## Table of Contents

Lab Overview - HOL-1851-04-ADV - Horizon 7.1: User Environment Manager - Getting Started

Module 1 - Introduction to User Environment Manager ( 60 minutes )
  Introduction
  Introduction to VMware User Environment Manager
  Introduction to Application Profiling
  Introduction to Application Personalization
  Introduction to Conditions and Environment Personalization
  Conclusion

Module 2 - Application Blocking ( 30 minutes )
  Introduction
  Introduction to Application Blocking
  Application Blocking - Global Configuration
  Application Blocking - A Practical Walkthrough
  Conclusion

Module 3 - Privilege Elevation ( 30 minutes )
  Introduction
  Introduction to Privilege Elevation
  Privilege Elevation - Global Configuration
  Privilege Elevation - A Practical Walkthrough
  Conclusion

Module 4 - Horizon Smart Policies ( 45 minutes )
  Introduction
  Introduction to Horizon Smart Policies
  Horizon Smart Policies - Creation and Execution
  Conclusion
Lab Overview - HOL-1851-04-ADV - Horizon 7.1: User Environment Manager - Getting Started
Lab Guidance

Note: It will take more than 90 minutes to complete this lab. You should expect to only finish 2-3 of the modules during your time. The modules are independent of each other so you can start at the beginning of any module and proceed from there. You can use the Table of Contents to access any module of your choosing.

The Table of Contents can be accessed in the upper right-hand corner of the Lab Manual.

This lab will provide an overview of VMware User Environment Manager. Discover how User Environment Manager manages profiles and policies as part of the Just-In-Time Management Platform (JMP). Configure user environment settings such as shortcuts, printer mappings, and folder redirection using context based conditions. Complete exercises in application and privilege elevation. Learn about Horizon Smart Policies and see how the user experience can be controlled based upon changing context.

Lab Module List:

- **Module 1 - Introduction to VMware User Environment Manager** (60 minutes) (Basic) This module will look at Application Profiling, Personalization, and Conditions.
- **Module 2 - Application Blocking** (30 minutes) (Beginner) This module will walk through the basics of Application blocking and whitelisting.
- **Module 3 - Privilege Elevation** (30 minutes) (Beginner) This module will walk through the basics of Privilege Elevation.
- **Module 4 - Smart Policies** (45 minutes) (Advanced) This module will walk through Horizon Smart Policies, Printer Mapping and Condition Sets.

Lab Captains:

- **Module 1-4 Captain - Michael McDonnell, Senior Systems Engineer, US**
- **Module 1-4 Captain - Vernon Lihou, Senior TAM PSO, United Kingdom**

This lab manual can be downloaded from the Hands-on Labs Document site found here:

[http://docs.hol.vmware.com](http://docs.hol.vmware.com)

This lab may be available in other languages. To set your language preference and have a localized manual deployed with your lab, you may utilize this document to help guide you through the process:

Location of the Main Console

1. The area in the RED box contains the Main Console. The Lab Manual is on the tab to the Right of the Main Console.
2. A particular lab may have additional consoles found on separate tabs in the upper left. You will be directed to open another specific console if needed.
3. Your lab starts with 90 minutes on the timer. The lab can not be saved. All your work must be done during the lab session. But you can click the \textbf{EXTEND} to increase your time. If you are at a VMware event, you can extend your lab time twice, for up to 30 minutes. Each click gives you an additional 15 minutes. Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.

Alternate Methods of Keyboard Data Entry

During this module, you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.
Click and Drag Lab Manual Content Into Console Active Window

You can also click and drag text and Command Line Interface (CLI) commands directly from the Lab Manual into the active window in the Main Console.

Accessing the Online International Keyboard

You can also use the Online International Keyboard found in the Main Console.

1. Click on the Keyboard Icon found on the Windows Quick Launch Task Bar.
Click once in active console window

In this example, you will use the Online Keyboard to enter the "@" sign used in email addresses. The "@" sign is Shift-2 on US keyboard layouts.

1. Click once in the active console window.
2. Click on the Shift key.

Click on the @ key

1. Click on the "@ key".

Notice the @ sign entered in the active console window.
Activation Prompt or Watermark

When you first start your lab, you may notice a watermark on the desktop indicating that Windows is not activated.

One of the major benefits of virtualization is that virtual machines can be moved and run on any platform. The Hands-on Labs utilizes this benefit and we are able to run the labs out of multiple datacenters. However, these datacenters may not have identical processors, which triggers a Microsoft activation check through the Internet.

Rest assured, VMware and the Hands-on Labs are in full compliance with Microsoft licensing requirements. The lab that you are using is a self-contained pod and does not have full access to the Internet, which is required for Windows to verify the activation. Without full access to the Internet, this automated process fails and you see this watermark.

This cosmetic issue has no effect on your lab.

Look at the lower right portion of the screen
Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes your lab has not changed to "Ready", please ask for assistance.
Module 1 - Introduction to User Environment Manager ( 60 minutes )
Introduction

In this Module the user can expect to learn the following:

• [Part 1] Introduction to VMware User Environment Manager
• [Part 2] Introduction to Application Profiling
• [Part 3] Introduction to Application Personalization
• [Part 4] Introduction to Conditions and Windows Personalization
Introduction to VMware User Environment Manager

VMware User Environment Manager™ offers personalization and dynamic policy configuration across any virtual, physical and cloud-based Windows desktop environment. User Environment Manager simplifies end-user profile management by providing organizations with a single, light-weight and scalable solution that leverages existing infrastructure. It accelerates time-to-desktop and time-to-application by replacing bloated roaming profiles and unmaintainable, complex logon scripts. It maps environmental settings (such as networks and printers), and dynamically applies end-user security policies and personalizations. This focused, powerful and scalable solution is engineered to deliver workplace productivity while driving down the cost of day-to-day desktop support and operations, and is a key component of JMP - the next generation of desktop and application delivery.

Introducing the Just in Time Management Platform (JMP)

Just-In-Time Management Platform or 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 RDSH provisioning
- VMware App Volumes for real-time application delivery
VMware 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 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.

**User Environment Manager**

When it comes to desktop virtualization, many organizations have traditionally had to choose between deploying persistent desktops (desktops that are tied to a specific user) and non-persistent desktops (generic desktops that get destroyed every time a user logs off). And while persistent desktops provide end users with a personalized desktop experience, they also come at a higher cost. Conversely while non-persistent desktops help drive down costs for IT, they do nothing to support end users with a customized experience.

This has led many to look for a middle ground—a truly “stateless” desktop that addresses both the needs of IT to drive down costs as well as the requirements of end users for a better desktop experience. This “stateless” desktop is the way forward—and VMware is uniquely positioned to deliver this solution to customers across virtual and cloud-hosted environments.
A Closer Look

Centralized and Simplified User Environment Management

VMware User Environment Manager provides IT with a robust solution for profile and persona management. Simple by design, this solution can easily be managed without scripting or complex user interfaces. And customers can get started with very little investment in infrastructure. The solution simply requires one central configuration share and one network folder per user.

Consistent and Personalized End-User Experience

With User Environment Manager, IT can deliver a consistent and personalized user experience for end users to maximize productivity. End users are productive because of a consistent feel to their workspace. Contextual policies for user persona management ensure that IT can map policy settings that tie directly to the end user’s device and location. This allows IT to respond to rapidly changing business dynamics.

Enterprise-Grade Scalability

With VMware User Environment Manager, IT can quickly and cost-effectively scale to support over a hundred thousand end users across virtual, physical and cloud-hosted environments. IT can add or remove profile and personalization services across the organization as required, to better respond to changes in the workforce and the overall business.

Building block for JMP

The next-generation desktop and application delivery platform included in VMware Horizon Enterprise. JMP (pronounced jump) leverages Instant Clones, App Volumes, and User Environment Management technologies to untangle the operating system, applications, and user personalization. By doing so, all the component pieces together can be reconstituted on-demand to deliver Just-in-Time desktops and apps across any infrastructure topologies—delivered to any device.
User Environment Manager clients are installed on RDS or VDI hosts, and devices such as desktops and laptops. Clients are enabled and configured through central GPOs in Active Directory that IT sets up with User Environment Manager. IT can then set up policies and settings using the management console.

When a user logs onto their laptop or virtual desktop for example, policy settings such as network and printer mappings and shortcuts are automatically configured according to the set policy. IT can even create dynamic contextual policies based on condition statements from the management console.

Application settings can also be predefined such that when a user opens up an application, the application configuration settings are automatically configured for quick application access. Settings can be applied to published applications and virtual desktops, such as VMware Horizon 6, RDSH desktops and apps, or Citrix XenApp and XenDesktop.
Launch the Management Console

1. On the Main Console desktop - Double click on the "Management Console"
Logging into the Management console for the first time will immediately show a plethora of options.

The first tab selected by default is **Personalization**. Each of the applications and settings listed underneath are applications and settings that have been profiled by UEM to allow administrators the ability to build a policy that can either enable users to maintain their personalization settings from device to device, or that same policy can
prevent users from making changes that hinder them, such as deleting a setting or overwriting a saved password.

Users can learn about Application Profiling in the Introduction To Application Profiling.

Users can learn about Application Personalization in the Introduction to Application Personalization.

1. Click on the User Environment tab to continue.
This tab is the **User Environment** tab. In this section of the Management Console, users will be able to set up policies that directly interact with the user environment. Some key tasks to note are [Display Language] settings.

Users can learn more about many of the User Environment features (and more!) by checking out the [VMware User Environment Manager YouTube Channel](https://www.youtube.com/watch?v=dQw4w9WgXcQ).
1. Click on **Condition Sets** to continue

**UEM Management Console Walkthrough - Condition Sets**

This tab is the **Condition Sets** tab. In this section of the Management Console, users will be able to set up collections of reusable conditions that may be used across multiple policies. This allows for faster policy creation. Conditions and Conditions set information can be found in detail in the [Introduction to Conditions and Environment Personalization](#) lab.

1. Click on **Application Migration** to continue
This tab is the Application Migration tab. As applications need to be upgraded over time, and settings need to be maintained as users move from Application Version 1 to Application Version 2, User Environment Manager can help create a seamless migration experience by allowing Administrators to develop migration plans that occur based on policy.

To see this in action - check out the VMware User Environment Manager - Office 2010 to 2013 Application Settings Migration video on YouTube.

Summary

At this point in the lab, users should have a very basic understanding of the lay out of User Environment Manager. Throughout the course of the other modules and exercises within the lab, users will be learning more about the various feature sets and abilities built into VMware User Environment Manager through the Management Console.
Introduction to Application Profiling

Windows is an open platform and as such gives application developers a great deal of flexibility in the way applications they design behave. While guidelines and best practices have been established over the years, one still can occasionally find an application which writes a log file to C:\Temp!

Understanding the behavior of an application, not just during installation, but as the application is opened, modified, updated, and so on, is critical to successfully managing the application lifecycle. There are a number of tools available that help administrators understand how an application behaves. These are powerful tools, but can be time-consuming and cumbersome to use.

The VMware User Environment Manager Application Profiler tool is purpose-built to help users easily understand how an application behaves. With real-time application analysis capabilities, Application Profiler automatically generates configuration files which enable application management.

Profiling an Application

While an application is being used, Application Profiler monitors the changes that the application makes to the registry and the file system. It is important that the application saves its configuration during the analysis session.

Only .EXE files are supported for analysis. Some applications install shortcuts in the start menu that refer to an application document instead of to the executable file of the application. Administrators can profile these applications by browsing to the executable and adding any additional arguments after the application path.

Usually, it is sufficient to modify a few of the settings of the profiled application. Many applications save their full configuration whenever a change is made. Some changes
may need to be made to more of the application features and settings, so that the corresponding files are written to disk. For example, administrators might change settings such as creating a signature in an email client or adding an entry to the custom dictionary in a word processor.

**Keeping the changes isolated**

Application Profiler monitors the application selected and all of the child processes started by that application. Monitoring stops when the main application and all child processes are stopped. As a result - keeping an image whose sole purpose is application profiling is important to confirm that only the application itself is modifying the behavior of the filesystem and registry and nothing else.

In this lab, users will be using a VM with a snapshot that has the Application Profiler installed. This will allow for a total environment cleanup between profiling sessions.

**Launch UEM**
1. On the Main Console desktop - Double click on the **Management Console**

![Management Console](image)

1. Expand the Applications folder.

Note the applications listed under Applications folder. Notably for this lab - WinSCP is missing and needs to be added to the list.
Minimize UEM

1. Minimize UEM by clicking the _ in the top right hand corner.

Launch Google Chrome

1. On the Main Console Desktop - Double click on the Google Chrome icon.
Log into App Volumes

1. Click on the App Volumes Admin in the Bookmarks Toolbar
2. Log into App Volumes using Username: Administrator
3. Password: VMware1!
4. Confirm Domain is CORP
5. Click Login
Assign Appstack

1. Click on the Volumes tab
2. Click the checkbox to the right of Sample Apps
3. Click Assign
Search for the Base W10 Template

1. Type in **base-w** in the Search Active Directory bar.
2. Select the checkbox on the left of **CORP\BASE-W10-X64-01$**.
3. Click **Assign**.
Confirm Appstack Assignment

1. Verify that Attach AppStacks on next login or reboot is selected.
2. Click Assign to finish the assignment.
1. Click on **HOL-1851 Admin** Folder in the Bookmarks Toolbar
2. Click on **vCenter Web Client**
3. Sign in with username: **administrator@vsphere.local**
4. Password: **VMware1!**
5. Click **Login** to continue.
Revert Snapshot to App Profiler

1. (If needed) Expand Datacenter **RegionA01**
2. (If needed) Expand Cluster **RegionA01-IC01**
3. Click on **base-w10-x64-01**
4. Click on the **Snapshots** tab in the right panel.
5. Click on **Application Profiler**
6. Click on the **Revert** icon to revert the VM to its Application Profiler state.

1. Click **Yes** to revert the VM to the Application Profiler snapshot.
1. Right click on **base-w10-x64-01**
2. Mouse over **Power**
3. Click on **Power On**
1. Right click on **base-w10-x64-01**
2. Click on **Open Console**

**Log In as Local Administrator**

Note: Be sure to log in as the local administrator as opposed to CORP\Administrator due to Active Directory trust issues. The CORP\Administrator account will not be able to log in successfully.

1. Click **Send Ctrl+Alt+Delete** to start login prompt.
2. Click on the Username: **Administrator**
3. Type in the Password: **VMware1!**

**Launch Profiler and Set Default Save Path**
1. On base-w10-x64-01 desktop, double click on the **Application Profiler** icon

![Application Profiler Window](image1)

Application profiles need to be saved in a place where UEM has access to them as these profiles are what enable the next lab in this module: [Application Personalization](#)

1. In the Application Profiler window - click on the **Settings** tab.
2. Click on the **Default Save Path** icon
3. In the Default save path type in `\controlcenter\config\general\Applications`
4. Click **OK** to save

![Specify Default Save Path](image2)
1. Click on the **Program Analysis** tab
2. Click on **Start Session**
3. **Scroll** to the bottom of the list
4. Click on **WinSCP**
5. Click on **OK**
Customize WinSCP Step 1 - Add ESX-01A

As soon as the user clicks OK on the previous step, WinSCP will launch and immediately go into a personalization / customization mode. In order to show how Application Profiler will detect and save these changes, this lab will guide users through the process of customizing WinSCP.

1. Modify the File protocol by changing the dropdown to **SCP**
2. Set the Host name to **esx-01a.corp.local**
3. Set the User name to **root**
4. Set the password to **VMware1!**
5. Click **Save** to preserve the profile
Customize WinSCP Step 2 - Save Session Entry and Login

1. In order to expedite future connections to esx-01a.corp.local click **Save password** even though it's not recommended.
2. Click **OK** to continue.
3. Click **Login** to test and to continue customizing WinSCP.
Accept the ESX-01A Certificate to Cache

1. Click Yes to accept the certificate to cache.

Customize WinSCP Step 3 - Preferences
Once connected - users will be given a rich set of options to choose from.

1. For the purposes of this lab, users will be changing some of the key preferences of WinSCP - Click **Options**.
2. Click **Preferences** to load the preferences screen.

1. On the preferences screen click **Panels**.
2. Click **Show hidden files**
3. Click **OK** to save the preferences.
Exit WinSCP and Finish Profiling

When exiting WinSCP - note the hidden files that have suddenly appeared in the My documents folder on the left side of WinSCP. This is a good indication of the application settings in action.

1. Close WinSCP by clicking the X on the top right corner of the window.

   ![Confirmation dialog]

1. In order to expedite the usage of WinSCP - check the box that says Never ask me again
2. Click OK to exit WinSCP
**Finished Profiling**

When Application Profiler is done inspecting all of the changes WinSCP has made to the registry and the filesystem and all child processes have exited Application Profiler will announce its completed Profiling.

1. Click **OK** to continue.

1. Click on the **Save** Button
2. Click **Save Config File with Predefined Settings** to save the WinSCP configuration file.
   This will produce four files:
   - INI – User Environment Manager configuration file containing the import and export locations. This file defines the parameters for User Environment Manager to manage the application.
   - ICO – Icon used by User Environment Manager Management Console and the Self-Support tool.
   - FLAG – Flag file for FlexEngine, when DirectFlex is enabled (default).
   - ZIP – Contains the predefined user settings.
Save Application Profile

1. Type WinSCP in the File name box
2. Click **Save** to save the profile with predefined settings.

A note will appear letting users know that WinSCP.zip was saved on the share.

1. Click **OK** to continue
Users may be tempted to open and edit the ZIP file directly from Windows Explorer, it is critical that the **Edit Profile Archive** button be used instead. User Environment Manager uses the standard ZIP file format to prevent the creation of proprietary file formats, but the writes to and reads from the ZIP files are optimized for performance. Using tools outside of User Environment Manager to edit these ZIP files makes them unreadable by FlexEngine.

1. To view the profile archive just created. Click **Edit Profile Archive**
2. Select **WinSCP**
3. Click **Open**
Navigating the Profile Archive - Part 1

In the Profile - users will note 2 folders. **AppData** and **Registry**.

1. Start by navigating to the **AppData** folder by double clicking.

In AppData, users will note a **winscp.rnd** file. This file is a blob and unreadable by anything in the lab. It is used to seed WinSCP's encryption random number generator.

Navigating the Profile Archive - Part 2

Next - navigate into the Registry folder.
1. Click on VMware **UEM Profile Archive Settings**
2. Double click on **Registry**

In the Registry folder there will be a Flex Profiles.reg file. This is the registry file that will get merged with the registry on the fly when WinSCP is used on UEM enabled machines in the future.

1. Right click on **Flex Profiles**
2. Click **Edit**

**Know Thine App**

```plaintext
[HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Configuration]
"JumpList"="root@esx-01a.corp.local"
"SelectMask"="%ZA.%ZA"
"ShowHiddenFiles"=dword:00000001
"FastFileButtons"=dword:00000001
```
Scrolling through the registry settings, users will note that WinSCP appears to save their settings in the registry. To confirm the changes made in this lab, search for **JumpList** and **ShowHiddenFiles** as seen in the collective screenshots above. Sometimes knowing what changes the profiled application made can be crucial to developing advanced profiles and understanding the needs of the end users.

1. Close Notepad by clicking the X on the top right corner of the window. If any changes were made - please discard them.
2. Close the explorer window by clicking the X on the top right corner of the window.

Return to Application Profiler

1. Click **Done** to continue
At this point the Application Profiling process is complete. There is no need to clean up anything, as this environment is snapshotted, and will be reverted as needed. Everything else can be left behind with no problems.

**Close Chrome**

1. Close Chrome by clicking the X in the top right corner of the window.

**Bring back VMware UEM**
1. If the application is still minimized - click on **VMware User Environment Manager** in the Task Bar

Users may note after all that hard work of Profiling WinSCP - its not there!

1. Click on **Refresh Tree**
2. Click on **WinSCP**
Import / Export Screen looks like Application Profiler Screen!

Users will note that the profiling just completed will have imported the settings that the Application Profiler was able to derive from WinSCP usage.

**Summary**

At this point in the lab, users should understand the basics of Application Profiling, what it does, and how it gets the data it uses. For a more indepth view of Application Profiler and possibly a lab to try, please see [Profiling Applications with Vmware User Environment Manager Part 2](#).
**Introduction to Application Personalization**

User Environment Manager Application Configuration Management enables users to configure the initial settings of an application without having to rely on the defaults of the application. Predefined Settings can be configured as one-time defaults, fully enforced (application starts each time in desired state), or partially enforced where the application starts each time in a desired state but allows partial personalization by the user.

In the previous section of the lab, users learned how to use VMware UEM Application Profiler to capture predefined settings for an application. For more information - please see *Introduction to Application Profiling*.

In this section of the lab, users will learn how to utilize User Environment Managers Administrative Console to allow user settings to migrate from application instance to application instance. They will also learn how to enforce settings so users cannot change them.

**Launch Horizon Client**

1. On the Main Console Desktop - Double click on the *VMware Horizon Client*
1. Double click on **view-01a.corp.local**

![Login Screen]

1. Log In as **lab1user**
2. Password: **VMware1!**
3. Click **Login**

![Windows 10 Instant Clone]

1. Double Click **Windows 10 Instant Clone**

**Launch WinSCP**

![WinSCP Icon]

1. On the VDI Desktop - double click on the WinSCP icon
Login to ESX-01A

1. Select the **root@esx-01a.corp.local** site
2. Click **Login**
Check and modify preferences

Users will immediately note that WinSCP still believes that **administrator.CORP** is the user logged in even though the user logged in is **lab1user**. In a future module, users will learn how to dig deep into the the application profile and modify that username with a variable. For now - to continue the lab, users will modify the preferences of WinSCP to stop showing hidden files, and modify the current local directory WinSCP is pointed at.

1. Click on **Options**.
2. Click on **Preferences**.
Stop showing Hidden Files

1. Click on Panels on the left.
2. Click on Show hidden files.
3. Click OK to continue
1. Click on the **Home** button to point the application back to C:\
2. Close WinSCP by clicking the X in the top right corner of the window.
Log out of the Desktop

1. On the top of the VDI Desktop screen - Click **Send Ctrl-Alt-Delete**
2. Click **Sign out**
Close the VMware Horizon Client

1. Close the Horizon Client by clicking the X in the top right corner of the window.

Publish WinSCP as an RDS Application

This lab is based on Instant Clones. Theoretically speaking - as soon as the user logs out and logs in - the user will get a new desktop, and that will show that the settings follow the user. However one of the goals of this lab is to show that UEM is cross platform. To show this in a lab scenario is slightly difficult due to limitations in the environment. In this specific case, the lab will be quickly guiding users through the process to publish WinSCP as an RDS application. If a full explanation to the process is needed, please check out [MBL-1851-02 -Module 2 -RDS Farm Provisioning (30 minutes)](MBL-1851-02 -Module 2 -RDS Farm Provisioning (30 minutes))
1. On the Main Console Desktop - Double click on the Google Chrome icon.

Log in to the View-01A Admin Page

![Log in to the View-01A Admin Page](image-url)
1. Click the **View-01A Admin** link in the bookmark toolbar
2. Sign in with Username: **Administrator**
3. Password: **VMware1!**
4. Click **Log In**

**Add a new Application Pool**

![Application Pools](image)

1. Expand **Catalog**
2. Click on **Application Pools**
3. Click **Add**
Search and Select WinSCP

1. In the Filter type **WinSCP**.
2. Click **Find**.
3. Select the checkbox to the left of **WinSCP**.
4. Click **Next**.
**Name the RDS Pool**

1. Leave the ID at defaults - in this case it is WinSCP.
2. Double-check that Entitle users after this wizard finishes is selected.
3. Click **Finish** to continue

**Entitle Horizon Users to WinSCP**
1. On the Add Entitlements screen click **Add**
1. Search for **Horizon**
2. Click **Find**
3. Select **Horizon Users**
4. Click **OK**

1. Click **OK** to continue with the UEM portion of the lab.
Close Chrome

1. Close Chrome by clicking the X in the top right corner of the window.

Launch Horizon Client

1. On the Main Console Desktop - Double click on the **VMware Horizon Client**
1. Double click on **view-01a.corp.local**

1. Log In as **lab1user**
2. Password: **VMware1!**
3. Click **Login**

1. Double Click **WinSCP** to launch as an RDS Desktop
Login to ESX-01A

1. Select the root@esx-01a.corp.local site
2. Click Login
Users will immediately note that WinSCP now reflects the state of the last time it was used. The Local Working Directory is set to C:\ instead of C:\Users\administrator.CORP.

1. To further validate these changes, click on **Options**.
2. Click on **Preferences**.
No Hidden Files Shown

Users will again note that all changes made in the last session are sticky.

1. Click on **Panels** on the left.
2. Click **OK** to continue
Clone to a new Site

1. Click the **New Session** tab.
2. Click on **root@esx-01a.corp.local**.
3. Click on **Manage**
4. Click on **Clone to a New Site**.
Modify Site Details

1. Change the Host name to **esx-02a.corp.local**
2. Click **Save** to preserve the profile.

1. Change the Site name to **root@esx-02a.corp.local**
2. In order to expedite future connections to esx-02a.corp.local, click **Save password** even though its not recommended.
3. Click **OK**
Delete ESX-01A Entry

Now that the ESX-02A entry has been created, the ESX-01A entry can be deleted.

1. Right click on the `root@esx-01a.corp.local` Site
2. Click **Delete**

1. Confirm the delete of esx-01a.corp.local by clicking **OK**.
Log In to ESX-02A

1. Click on `root@esx-02a.corp.local`.
2. Click `Login`.
Accept the ESX-02A Certificate to Cache

1. Click **Yes** to accept the certificate to cache.

Close WinSCP

1. Now that WinSCP is finished being configured again. Click the **X** in the top right hand corner of the window to exit.
1. Minimize the Horizon Client by clicking the _ in the top right corner of the window.
What happened?

1. As users log on to VDI, Physical Devices, RDS Apps, etc., the base profile is loaded and all the Predefined Windows settings, keyboard, mouse, language, etc. are injected by FlexEngine.
2. When WinSCP started, settings were automatically injected into the profile.
3. When the user then used the application, settings were updated during the session.
4. When the user closed WinSCP, the settings were written back to the share where they are stored.

Administratively Enforced Application Settings

During the previous section of this lab, users created a site setting for esx-01a.corp.local. This section of the lab has had lab1user destroy that entry. The rest of this lab will be devoted to allowing the users a certain level of personalization, but also enforcing specific settings within an application.
1. On the Main Console desktop - Double click on the Management Console

1. Expand Applications
2. Click on WinSCP
3. Click on the Predefined Settings tab
4. Click on Default Settings
5. Click on Edit
Predefined Settings

The edit screen has 2 tabs: Settings and Conditions. This lab will be focused on the Settings portion. For more details on the conditions - jump forward in this lab to Conditions and Environment Personalization.

As seen earlier in the process of Application Profiling - users learned that they could set up custom settings for an application and push those settings "by default" to the end user. During that profiling process - the user saved the configuration with Predefined settings that were later navigated and inspected. In VDI and RDS, the end user was shown to have the capability to override those settings and create their own personalized version of the application.
What if Administrators needed to guarantee a partial state of the application. In the case of WinSCP - that root@esx-01a.corp.local site that was just deleted could be a costly customization lost to a busy end user. To solve that problem, UEM introduced Predefined Settings. There are 4 modes to Predefined Settings:

- **Default Settings**: Default settings are only applied if no user profile archive exists.
- **Partially Enforced Settings**: Partially enforced settings are applied after the user profile archive, if any, has been imported.
- **Default Settings with Partial Enforcement**: The Default settings are applied if no user profile archive exists, then the user profile archive, if any, is imported, and finally the Partially Enforced Settings are applied.
- **Fully Enforced Settings**: Fully enforced settings are applied always and no user profile archive is created.

This lab will be focused on Partially Enforced Settings to show how even though a root@esx-02a.corp.local site was created, the root@esx-01a.corp.local site is still considered needed by Administrators.

1. Click on the dropdown for Type and select **Partially Enforced Settings**.
2. Click **Save**.

**Save Changes and Minimize**

![Save changes and minimize screen](image)

This is the first change in this lab made directly within UEM regarding policy. As a rule of thumb, if a change is made; always **Save the Config File**.

1. Be sure to **Save the Config File** before going any further.
2. Minimize the Management Console by clicking the _ button in the top right corner of the window.
Relaunch Horizon Client

1. If the Horizon Client is now closed, please re-launch the Horizon Client by double clicking on the **VMware Horizon Client** on the Main Console desktop.

1. Double click on **view-01a.corp.local**
1. Log In as **lab1user**
2. Password: **VMware1!**
3. Click **Login**

1. Double Click **WinSCP** to launch as an RDS Desktop

... and then there were two!

Users will immediately note the esx-01a.corp.local entry has returned to the Sites list. This is due to the Partial Policy Enforcement mixing with the users personal settings.
1. Click on either site.
2. Click **Login**.

**Did the settings revert?**

Users will again immediately note that WinSCP believes that *administrator.CORP* is the user logged in even though the user logged in is *lab1user*. Previously - users had selected *C:\* as the home folder for WinSCP.
1. Click **Options**
2. Click **Preferences**

Users will immediately note that **Show hidden files** has also been rechecked.

2. Click **OK** to continue.

**Why did that happen?**

This was by the design of the lab and by the design of UEM. The policy chosen: **Partially Enforced Settings**, specifically applies the pre-packaged settings created during application profiling after the user profile archive, if any, has been imported.

Had the user chosen **Fully Enforced Settings**, all user customizations would have been completely dropped and only the pre-designed package would have been usable.
Any customizations during that specific application session would have been dropped the following session.

**Clean Up**

1. Click the X in the top right hand corner of the window to close WinSCP.
2. Click the X in the top right hand corner of the window to close the VMware Horizon Client.
3. Click the X in the top right hand corner of the window to close VMware User Environment Manager Management Console.

**Summary**

At this point in the lab, users should understand the basics of Application Personalization and Settings Policy Enforcement. For a more indepth view of Application Personalization and so much more, please see the [VMware User Environment Manager YouTube Channel](#) or the [VMware EUC Blog surrounding User Environment Manager](#).
Introduction to Conditions and Environment Personalization

User Environment Manager conditions and condition sets enable granular control over the user experience. They can be used to apply initial settings, or enforce specific settings. Doing this allows administrator to easily and quickly enforce policies based on very specific details. Need to limit a user's Clipboard access when they are connecting from a 32 bit Windows 7 over the PCoIP protocol on a Sunday while they are running on Battery but only if the time is somewhere between 3:00 AM and 6:00 AM? VMware UEM can help build that policy quickly and clearly.

In the previous section of this lab, users learned how to enable Application personalization across multiple platforms. For more information - please see Introduction to Application Personalization.

In this section of the lab, users will learn about the power of conditions. They will then take that knowledge and build out a policy that changes the language of a user based on Group Membership in Active Directory.

Launch Horizon Client

1. On the Main Console Desktop - Double click on the VMware Horizon Client
1. Double click on **view-01a.corp.local**

1. Log In as **lab1user**
2. Password: **VMware1!**
3. Click **Login**

1. Double Click **Windows 10 Instant Clone**
**Generic Windows Desktop in English**

This lab is designed to give users the ability to change the language for a user dynamically based on policy. Right now, this desktop is in its default state using English as the primary language.

Users will note the use of the English language in the start menu and the Ctrl-Alt/Delete menu.

1. On the top of the VDI Desktop screen - Click **Send Ctrl-Alt-Delete**
2. Click **Sign out**
Minimize the VMware Horizon Client

1. Minimize the Horizon Client by clicking the _ in the top right corner of the window.

Launch the Management Console

1. On the Main Console desktop - Double click on the Management Console
Navigate to Language Settings

Due to the limited nature and size of the labs only one language pack (German) was installed to show the capabilities of User Environment Manager.

VMware User Environment Manager has the ability to modify many parts of windows on the fly. This HOL has many settings that get automatically injected. There are automated folder redirections, drive mappings, printer mappings, registry settings, shortcuts, and many more. This lab will focus on the section referred to as **Display Language**.

1. After launching the Management Console, click on the **User Environment** tab.
2. Click on **Display Language** to pull up the different display language policies.
3. Select the **German** option under Display Language.
4. Click on **Edit**.
Introducing Conditions

Note: The next several steps in this manual are not steps for users. They are merely explanations of features and capabilities. To skip ahead - go to the page titled Build A Condition

1. When the German - Display Language screen appears, click on the Conditions tab.
2. Click on Add
User Environment Manager operates on a policy of "Apply To Everyone Unless I Shouldn't". This means if this setting were enabled right now, every user in the entire environment would be trying to navigate their windows desktop that has been localized to the German Language. To prevent UEM from being too helpful, Conditions must be added to limit the scope of a policy.

**Featured Conditions - Active Directory Site Name**

Conditions at their most basic level are very simple. They either evaluate to **TRUE** or **FALSE**. To start that can allow for very high level generalizations. For example in this HOL there is only one Site within Active Directory.

In a global environment there are likely more Sites within Active Directory, and because Sites are part of the replication scheme between controllers, those Sites can be named in reference to a geographical location. Imagine a corporation with a Berlin branch. It may be safe to assume that those users speak German. As of VMware User Environment Manager 9.2, a new condition option is **Active Directory Site Name**.

User Environment Manager has a rich string parsing feature that allows administrators to easily pick out partial strings or full strings. If an administrator had several sites all named **DE-<City>-Branch** it would be simple for UEM to just search for any site starting with "DE-".
Featured Conditions - Remote Display Protocol

Just because a group of individuals may all speak the same language, does not guarantee they have an Active Directory Site that is local to their region. They may be people logging in to systems remotely utilizing a VDI tool such as VMware Horizon. One of the ways to tell that a user is logging into a given computer remotely is by detecting the Remote Display Protocol.

![Remote Display Protocol](image)

VMware UEM supports 4 popular remote protocols:

- Citrix ICA
- Microsoft RDP
- PCoIP
- VMware’s own Blast protocol

Detecting these protocols could help an administrator identify specific sets of users based on the platform they are logging in on and set different policies for the UEM administrated machine as a result.

Featured Condition - Horizon Client Property

VMware User Environment Manager is the centerpoint of the Just-in-time Management Platform. Making a UEM deployment Horizon-aware allows administrators the ability to quickly and flexibly build policies based on Horizon Specific constructs.

![Horizon Client Property](image)

As a user logs into a Horizon Pool, knowing the location of Internal or External will allow administrators to specify policies that flex with the users. For example, a user
logging on from a location external to the home office may not get internal printers mapped to their desktop.

**Launch tags** are metadata tags on a Horizon Pool. When a pool is tagged, UEM can detect that tagging and apply policy on the fly. This allows for pools to be tagged and policy updated quickly based solely around metadata. In some cases, just having Launch tags could be needed to set a policy.

**Pool name** is the final Horizon Client Property option. This property can do a partial or full match based on Horizon Pool name. Users will see this many times throughout the lab.
Featured Condition - Group Membership

The Group Membership condition allows UEM to automatically match users based on their membership to a given group either via Active Directory or locally (when No-AD Mode is enabled). The condition dialog actually allows for an Active Directory search so the Group Membership can be matched on Group SID.

This lab will feature the group membership condition by validating a user's membership in an Active Directory Group DE Speakers.
**Condition Chaining**

Conditions can be chained together to take several high level states and narrow down the scope of a policy. This allows for extremely granular control over policies, enabling administrators to make changes at a microlevel as necessary.
Note the AND on the front of each condition. This shows that each condition must be met for the policy to be implemented. Sometimes conditions need to be explicitly negated.

Selecting a condition and clicking edit gives the options to modify the logic, allowing administrators to get extremely specific in the details necessary to build a policy - such as would be necessary when attempting to enforce a language onto a users machine.
Condition Sets

Occasionally - there will be a specific set of conditions used over and over again. Those conditions can be grouped together into what is called a Condition Set. A Condition Set can be used as part of a condition for a specific policy.
Seen above: a **Condition Set** stating that if an IP for either the local device or the endpoint (VDI/RDS) is somewhere in a 10.0/8 or a 14.0/8, it is in Headquarters. As stated before, those condition sets can be used in other conditions.

Seen above: A **Condition Set** integrated into the Display Language Setting.
**Condition Groups**

**Condition Groups** are different from Condition Sets in that they are logical groupings of conditions that allow for *scoping* conditions in a factor similar to using parenthesis in scripting.

![Image of condition group setup](image-url)

Seen above: a complex nested set of condition groups allowing administrators to develop very specific policies.

For those wondering, the condition above states:

If a user is a member of CORP\DE Speakers AND (The remote display protocol is Blast and they are connected to the Horizon Pool BerlinBranchPool) OR (The connecting endpoint IP is on the 192.168.10.0/24 network and the remote protocol is RDP)

Then give them a desktop with German Language set as default.
Build A Simple Condition

1. If the add menu has since been closed, click the Add menu again.
2. Select Group Membership
Search for Group

1. Click on **Browse**
1. Search for **DE Speakers**
2. Click **Check Names**
3. Click **OK**

Note the SID filled in under CORP\DE Speakers. That is the exact reference to the Active Directory Group.

1. Click **OK** to continue.
Create a Second Condition - Horizon Client Property

1. Once again on the conditions screen - Click **Add**
2. Click **Horizon Client Property**

This lab is focused around VDI and JMP. As such the policy should verify that the users are logging into the Windows 10 Instant Clone Pool to use this.

1. Set the Property to **Pool name**.
2. Set the comparison operator to **is equal to**.
3. Type **Win10-IC** in the text box.
4. Click **OK**.

**Review the condition**

As of the last step - the conditions for this policy to be applied are

- User is a member of **CORP\DE Speakers**
- AND the user is connected to the Horizon Pool **Win10-IC** the Windows 10 Instant Clone Pool.

1. Click on the **Settings** tab to continue.

This concludes the detailed deep dive on conditions. If a more detailed run down is needed, please see the **VMware User Environment Manager Administration Guide**.
Run Once

This dialog allows administrators to choose a specific language for an endpoint. It also has a Run once checkbox. The Run once checkbox will set the display language for a given user only once allowing them the capacity to change it later.

1. Click Save to continue
Enable the German Display Language Policy

Now that the policy has been fleshed out, the German Display Language policy can be safely enabled.

1. Right click on German.
2. Click Enable.

Minimize the UEM Management Console

1. Minimize the Management Console by clicking the _ button in the top right corner of the window.
Validate User Membership

Once of the conditions set for the German Display Language was the user had to be a member of DE Speakers. The user used in this lab is lab1user, and to make this lab successful the user's membership needs to be validated.
1. On the control center desktop - double click on **Active Directory Users and Computers**.

1. Under corp.local click on **Users**.
2. Right Click on **Lab 1 User**.
3. Click on **Add to a group...**
Add to DE Speakers

1. Search for **DE Speakers**
2. Click **Check Names**
3. Click **OK**

A dialog will appear to show that the Add to Group operation was successful.

1. Click **OK** to continue.
2. Close the Active Director Users and Computers snapin by clicking the X in the top right corner of the window.

Relaunch Desktop to Validate Changes

1. If the Horizon Client is now closed, please re-launch the Horizon Client by double clicking on the VMware Horizon Client on the Main Console desktop.

1. Double click on **view-o1a.corp.local**

![Login](image-url)
1. Log In as **lab1user**
2. Password: **VMware1!**
3. Click **Login**

1. Double Click **Windows 10 Instant Clone**

**Note:** Sometimes the Desktop is not immediately available after a log out due to the fact that this is a lab and the instant clones do take a little more time than usual to regenerate.

1. Click **Try Again** in the top right corner after about a minute.
Users will note the use of the English language in the start menu and the Ctrl-Alt-Delete menu.

1. On the top of the VDI Desktop screen - Click **Send Ctrl-Alt-Delete**
2. Click **Abmelden** to sign out.
1. Close the Horizon Client by clicking the X in the top right corner of the window.

**Clean Up - Disable Policy**

In order to avoid having to translate everything from German for the remaining modules in this lab, the German Display Language policy should be disabled.
1. If the Management Console is now closed - Double click on the **Management Console** on the Main Console Desktop.

   ![Management Console](image)

   1. Click on the **User Environment** tab.
   2. Right click on **German**.
   3. Click **Disable**.

**Summary**

At this point in the lab, users should understand the basics of Conditions and Environment Personalization. For a more indepth view of Environment Personalization along with much more, please see [VMware User Environment Manager Environment - Personalization Part 2 on YouTube](https://www.youtube.com/watch?v=example_video_id).
Conclusion

Congratulations, you've finished Module 1

Congratulations on completing Module 1.

If you are looking for additional information on VMware User Environment Manager, try one of these:

- Click on this link
- Or go to http://bit.ly/VMwareUEM
- Or use your smart device to scan the QRC Code.

Proceed to any module below which interests you most.

- Module 2 - Application Blocking
- Module 3 - Privilege Elevation
- Module 4 - Horizon Smart Policies
Module 2 - Application Blocking (30 minutes)
Introduction

In this Module the user can expect to learn the following:

- [Part 1] Introduction to Application Blocking
- [Part 2] Application Blocking - Global Configuration
Introduction to Application Blocking

Application Blocking 101

VMware User Environment Manager Application Blocking Policies can be created based on Hash, Path or Publisher. Application blocking allows administrators to trust or deny particular applications on a varied set of conditions. UEM takes a whitelist approach to any executables outside of Windows and Program Files. This means that Administrators have the ability to create a whitelist of trusted executables that are not pre-installed. It also gives administrators the ability to explicitly blacklist any unnecessary executables to a given user based on a rich set of conditions.

Application Blocking starts disabled by default when UEM is initially installed. When it's enabled, it has a global scope across all UEM enabled devices. It gives the ability right off the bat to only block based on certain conditions, allowing for policies to be built out in a smaller more granular scope and then slowly widen the scope until all users are able to be covered.
Due to the possibility of overlapping rules, administrators will want to understand the idea of precedence in their rule making. In the chart above, green check boxes show when an application will be allowed to execute vs when an application will *not* be allowed to execute regardless of location. Note that Hash-based blocking for an EXE will block an executable - in the case of a pre-installed app such as Visual Studio or Rational Application Developer - Application Blocking can possibly help alleviate a licensing issue by guaranteeing that any user NOT allowed to use an application will have absolutely no ability to access it.

**Conclusion**

At this point in the lab, users should have a high level understanding of Application Blocking. Continuing through this lab will allow users to learn the specifics of implementation and policy development.
Application Blocking - Global Configuration

In the previous section of this lab, users were able to get a high level overview of Application Blocking and whitelisting. Using that understanding, this section of the lab will focus on building upon that knowledge to enable the Application Blocking part of UEM while scoping it only for specific users.

Launch the Management Console

1. On the Main Console desktop - Double click on the Management Console
Navigate to Application Blocking

Users will note from the beginning that Application Blocking is already enabled. This is due to the fact that there are applications running on the VDI desktops that need to be unblocked specifically for the labs. Please do not modify these policies as doing so may hinder the lab.

1. Click on the **User Environment** tab.
2. Click on **Application Blocking**.
3. Click on **Global Configuration**.
**Application Blocking - Global Configuration**

Users will note from the beginning that Application Blocking is already enabled. This is due to the fact that there are applications running on the VDI desktops that need to be unblocked specifically for the labs. In a default setup, this would not be the case.

The **Global Configuration** screen immediately presents administrators with the ability to restrict in what situations applications MAY be whitelisted or blocked. Conditions are not necessarily required to allow Application Blocking / Whitelisting, though it will affect all users without any regard to scope for an initial deployment. Furthermore - when administrator click **OK** on this screen, if no Application Blocking / Whitelisting policies are defined, the defaults will go into effect immediately for all users who have a **policy refresh** (log On or unlock workstation event) from that moment on. This means that any application who is launched OUTSIDE of \Windows, \Program Files, or \Program Files (x86) will be blocked. For more information on Conditions please see the **Introduction to Conditions and Environment Personalization** lab.
For the sake of this lab - Application Blocking was reduced in scope to only affect members of the group *CORP\UEM Users*.

**Application Blocking - Global Configuration Part 2**

![Application Blocking - Global Configuration](image)

The second half of the **Global Configuration** screen focuses on messaging to users when a process is blocked.
The executables section specifically designates the parent process that will spawn off all child processes. These processes will be the ones that will show a **Process Blocked** like in the image below. Most commonly in today's modern user environments the parent applications used are explorer.exe and cmd.exe. If one of the configured parent application(s) (like explorer.exe listed above) attempts to start a blocked application, the configured message is displayed instead of the windows default message as seen below.

![Image of Process Blocked window](image)

This message is derived from the **Message Title**, and the **Message Text**.

The message text section by default starts with the phrase **Process '\[PROCESSNAME\]' blocked from running from '\[PROCESSFOLDER\]'**. Users should note the use of bracket-based variables \[PROCESSNAME\] and \[PROCESSFOLDER\], those are variables specific to UEM. Users can also inject environment variables in to this message on the fly using standard \%VariableName\% notation.

The message is set to **Hide after** 10 seconds in this example. This allows administrators to give users a note without them having necessarily click "OK" to continue. This time limit can be set to an astronomically long time if necessary if administrators want users to know they're specifically being blocked. It can also be set to 0 if administrators do **not** want to give users any notification what so ever.
Once the **Global Configuration** is complete for Application Blocking - enabling and setting the policies for everyone is as easy as a click of button.

1. Click **OK** to save all changes and enforce Application Blocking for all users who are members of the group CORP\UEM Users.

**Summary**

At this point in the lab, users should have the ability to configure and turn on Application Blocking. To learn more about configuring Application Blocking, please see the [VMware User Environment Manager Administrator Guide](#).
Application Blocking - A Practical Walkthrough

In the previous section of this lab, users learned how to enable and configure Application Blocking and whitelisting. Using that understanding, this section of the lab will focus on building upon that knowledge to practically demonstrate the capabilities and limits of Application Blocking and Whitelisting.

Launch Horizon Client

Run Client Launcher

1. On the Main Console Desktop - Double click on the VMware Horizon Client

Connect to View-01a

1. Double click on view-01a.corp.local
Login as Lab 1 User

1. Log In as lab1user
2. Password: VMware1!
3. Click Login

Launch Instant Clone Desktop

1. Double Click Windows 10 Instant Clone
Applications to Test

In the VDI desktop there are 2 applications that will be tested.

• C:\Windows\System32\cmd.exe or more commonly known as the Command Prompt.
• T:\putty.exe or more commonly known as Putty.

Based on what has been stated about UEM's application blocking and white listing thus far, users will note that the Command Prompt should always run unless we explicitly say not to run. Putty should never run unless it is explicitly whitelisted.

To reiterate: Application Blocking will by default only allow applications to run from C:\Program Files, C:\Program Files (x86), and C:\Windows. That means anything running out of the Tools drive (T:) will be blocked by default.

This lab will focus on reversing the situation; that means it will show users how to block the Command Prompt, and allow Putty to be run.
Launch Command Prompt

1. In the VDI Desktop - Right click the **Start Button**.
2. Click on **Command Prompt**

Command Prompt Successfully launches

The command prompt successfully launches as expected.

1. Type in **exit** and hit **<Enter>** in the command prompt to continue.
Launch Putty
1. Click on the **Folder** Icon on the Task Bar
2. Expand **This PC** on the left panel if it is not already expanded.
3. Click on the **Tools** drive.
4. Double click on **Putty** to launch.

**Putty fails to launch**

![Open File - Security Warning]

1. Click **Run** to continue.

![VMware HOL Demo - Process Blocked]

As established in the global configuration; UEM will launch a dialog showing the process being blocked. If users did not change the default text in the global config, the above
image will be exactly what is shown on the VDI desktop. Note the 10 second count down timer.

Time for a choose-your-own adventure:

- **Wait 10 seconds** and the Process Blocked box will go away on its own.
- Click **OK** to force the box to disappear immediately.

Time to create some application blocking and whitelisting rules

### Log out of the Desktop

1. On the top of the VDI Desktop screen - Click **Send Ctrl-Alt-Delete**
2. Click **Sign out**
Minimize the VMware Horizon Client

1. Minimize the Horizon Client by clicking the _ button.

Launch Management Console

1. On the Main Console desktop - Double click on the Management Console
Navigate to Application Blocking

Users will note from the beginning that Application Blocking is already enabled. This is due to the fact that there are applications running on the VDI desktops that need to be unblocked specifically for the labs. Please do not modify these policies as doing so may hinder the lab.

1. Click on the **User Environment** tab.
2. Click on **Application Blocking**.
3. Click on **Create**.
Block the Command Prompt via Path
1. General Settings
   - Name: Block Command Prompt
   - Label:
   - Tag:

2. Application Blocking Settings
   - Type: Path-based
   - Allow:
   - Block:

   Add...  Edit...  Remove...
This lab will start by showing a Path-based blocking of the Command Prompt. Path-based blocking is great for applications that have a consistent path such as C:\Windows\System32\cmd.exe across multiple systems. Doing a path-based blocking is convenient for administrators trying to block a pre-installed application as a security measure or utilizing conditions to help alleviate a licensing issue.

1. Start by giving the Application Blocking policy a name: **Block Command Prompt**
2. Click **Add** under the Block box.

**Select a path to block**

![Select path to block window](image)
1. Click Select file.

1. Click on **Local Disk (C:)** on the left pane.
2. Double click on **Windows**.
Selecting Command Prompt
1. Scroll to find and double click on **System32**.

1. Scroll to find and click on **cmd.exe**.
2. Click **Open**.

**Save File Selection**
1. Now that C:\Windows\System32\cmd.exe is in the Path, click OK to continue.
Review and Save Application Blocking Setting
Review the appropriate fields on the Application Blocking Dialog.

1. Is the **Name** correct and does it clearly define the policy's function?
2. Is `C:\Windows\System32\cmd.exe` next to **Block**?
3. Click **Save** to continue.

## Whitelist Putty

Now that the Block Command Prompt policy has been created, the Allow Putty policy needs to be created.

1. Click **Create** to start the process.
Hash-based vs Path-based
In this policy, given that Putty is easily downloadable and can be located anywhere on a given machine, relying on it being in a specific path is a difficult proposition. Maintaining a list of possible locations would be cumbersome and difficult. It would also allow for users to potentially move and rename apps into a potentially whitelisted app space just to force them into running. Hash-based blocking and whitelisting solves that in a big way by guaranteeing that the application in question is indeed the application desired to be white-listed / blocked.

1. Set the name to **Allow Putty**.
2. Click on **Type**.
3. Select **Hash-based**.
4. Click **Add** under the Allow box.

### Navigate and select Putty

1. Click on **tools** in the left pane.
2. Click on **putty.exe**.
3. Click **Open** to continue.
Review Putty Hash

Upon selecting Putty, users will note that the Hash is immediately generated. This hash will be compared every time an application is run to validate it is allowed to be run.

Something to note: There is a checkbox for **Path-specific**. This will allow for a "best of both worlds" approach, it will enforce a specific path and validate that the application ran is the application administrators intended to be run.

Also to note: the path of this version of Putty is **C:\tools\putty.exe**. The version of Putty ran in the VDI desktop is **T:\**. The path does **not** need to remain the same.

1. Click **OK** to continue.
Review and Save Application Allow Policy
Review the appropriate fields on the Application Blocking Dialog.

1. Is the **Name** correct and does it clearly define the policy's function?
2. Is **putty.exe** next to **Allow**?
3. Click **Save** to continue.

**Relaunch Desktop to Validate Changes**

1. If the Horizon Client is now closed, please re-launch the Horizon Client by double clicking on the **VMware Horizon Client** on the Main Console desktop.

1. Double click on **view-01a.corp.local**

1. Log In as **lab1user**
2. Password: **VMware1!**
3. Click **Login**

1. Double Click **Windows 10 Instant Clone**

**Note:** Sometimes the Desktop is not immediately available after a log out due to the fact that this is a lab and the instant clones do take a little more time than usual to regenerate.

1. Click **Try Again** in the top right corner after about a minute.
Launch Command Prompt

1. In the VDI Desktop - Right click the **Start Button**.
2. Click on **Command Prompt**

Command Prompt Denied!

A familiar dialog appears, this time blocking `cmd.exe` out of `C:\Windows\System32`.

Time for a choose-your-own adventure:

- **Wait 10 seconds** and the Process Blocked box will go away on its own.
- Click **OK** to force the box to disappear immediately.
Launch Putty
1. Click on the **Folder** Icon on the Task Bar
2. Expand **This PC** on the left panel if it is not already expanded.
3. Click on the **Tools** drive.
4. Double click on **Putty** to launch.

**Putty Success!**
1. Click **Run** to continue.

This time Putty launches immediately, showing the Application Blocking and Whitelisting policies created in this lab were completely successful.
Log out of the Desktop

1. On the top of the VDI Desktop screen - Click **Send Ctrl-Alt-Delete**
2. Click **Sign out**

**Summary**

At this point in the lab, users should have a clear understanding about how Application Blocking and whitelisting works within UEM. For more information on Application Blocking and Whitelisting, please check out the [VMware User Environment Manager Administrator Guide](#) or the [VMware User Environment Manager YouTube Channel](#).
Conclusion

Congratulations, you've finished Module 2

Congratulations on completing Module 2.

If you are looking for additional information on VMware User Environment Manager, try one of these:

- Click on this link
- Or go to http://bit.ly/VMwareUEM
- Or use your smart device to scan the QRC Code.

Proceed to any module below which interests you most.

- Module 1 - Introduction to VMware User Environment Manager
- Module 3 - Privilege Elevation
- Module 4 - Horizon Smart Policies
Module 3 - Privilege Elevation ( 30 minutes )
Introduction

In this Module the user can expect to learn the following:

- [Part 1] Introduction to Privilege Elevation
- [Part 2] Privilege Elevation - Global Configuration
- [Part 3] Privilege Elevation - A Practical Walkthrough
Users in a modern environment want and need a certain level of autonomy to do their jobs effectively. Sometimes this means installing applications, sometimes this means activating features in their environment that require administrative privileges. A new feature as of VMware User Environment Manager 9.2 is Privilege Elevation. UEM now allows administrators to pre-define applications for end users to run or install using...
elevated privileges. Standard user accounts can run applications as if they were a member of the local administrators group.

This helps improve security posture in an end user environment by removing local administrator privilege from domain users, while enabling elevation only for specific apps in specific instances.

**Privilege Elevation Use Cases**

Privilege Elevation can be extremely effective in today's enterprise IT environment.

- Older legacy applications requiring administrative rights just to run.
- Application Installers - especially in combination with [Writable App Volumes](#).
- Application Repositories - Shares with IT-Approved Applications.
- Power Users - Users who have specific rights on their machines such as developers to modify OS settings for their application.
Elevated Applications

Elevated Applications are pre-existing applications that can be elevated by 3 potential mechanisms:

- Path-Based Elevation
- Hash-Based Elevation
- Publisher-Based Elevation

To be an Elevated Application, the process MUST be an executable. MSI's cannot be elevated as an Application. Also - child processes that come off of Elevated Applications are elevated on a \textit{per-rule} basis. This means that while an administrator may say Application A is elevated to admin rights, its sub processes are not necessarily elevated to the same level.
Privilege Elevation with User-installed Apps (UIAs) are different from Elevated Applications (EAs) in that they are not application or process specific. Privilege Elevation for UIAs is path-based, and is designed for an entire folder. This allows for administrators to set up an installer share or an application share where apps that need privilege could live. Applications that live in this folder can be either executables (EXE's) or installers (MSI's).

Elevating the child processes of these apps are limited to:

- Processes that exist in the same folder that the parent application lives.
- Processes that exist in the temporary folder of the user.
- Processes that exist in the temporary folder of the system.

The only exception to that rule is by enabling all child processes to be elevated in the global configuration of Privilege Elevation.

**Summary**

At this point in the lab, users should have a high level understanding the concepts and purposes of Privilege Elevation. Continuing through this lab will allow users to learn the specifics of implementation and policy development.
Privilege Elevation - Global Configuration

In the previous section of this lab, users were able to get a high level overview of Privilege Elevation and some of its use cases. Using that understanding, this section of the lab will focus on building upon that knowledge to enable Privilege Elevation and customize it's usage within the enterprise.

Launch the Management Console

1. On the Main Console desktop - Double click on the Management Console
Navigate to Privilege Elevation

1. Click on the **User Environment** tab.
2. Click on **Privilege Elevation**.
3. Click on **Global Configuration**.
The **Global Configuration** screen immediately presents administrators with the ability to enable Privilege Elevation and configure high level conditions for elevation conditions. Those conditions can be as granular or as wide spread as need be. In fact, conditions are not necessarily required, though it will affect all users without any regard to scope, and for an initial deployment - that may not be recommended. For more information on Conditions please see the [Introduction to Conditions and Environment Personalization](#) lab.

For the sake of this lab - Application Blocking was reduced in scope to only affect members of the group **CORP\UEM Users**.
After establishing the default conditions necessary for Privilege Elevation, users are then presented with the ability to automatically elevate all child processes for **User-installed Applications**. By default, UIA only elevates child processes that are located in the same folder as the elevated application, the temp folder of the user, or the temp folder of the system. This global setting will enable elevation for all child processes, regardless of location.

The final section of the global configuration is the Message section. Like application blocking, when there is an **Elevated Application** Privilege Elevation. This message does **not** apply to User-installed Apps. This allows UEM administrators to validate that users who want to use applications with administrative privileges understand the risk they’re about to take on.

1. Click **Enable Privilege Elevation**.
2. Click **OK** to continue.
Summary

At this point in the lab, users should have the ability to configure and turn on Privilege Elevation. To learn more about configuring Privilege Elevation, please see the VMware User Environment Manager Administrator Guide.
Privilege Elevation - A Practical Walkthrough

In the previous section of this lab, users learned how to enable and configure Privilege Elevation. Using that understanding, this section of the lab will focus on building upon that knowledge to practically demonstrate the capabilities and limits of Privilege Elevation.

Launch Horizon Client

1. On the Main Console Desktop - Double click on the VMware Horizon Client
1. Double click on **view-o1a.corp.local**

1. Log In as **lab1user**
2. Password: **VMware1!**
3. Click **Login**

1. Double Click **Windows 10 Instant Clone**
Launch Legacy App from T:\

1. Click on the **Folder** Icon on the Task Bar.
2. Expand **This PC** on the left panel if it is not already expanded.
3. Click on the **tools** drive.
4. Double click on **LegacyApp**.
Successful Launch with one caveat...

1. Click **Run** to continue.

Please note that this app is **NOT** running as admin.
Log out of the Desktop

1. On the top of the VDI Desktop screen - Click **Send Ctrl-Alt-Delete**
2. Click **Sign out**
Minimize the VMware Horizon Client

1. Minimize the Horizon Client by clicking the _ button.

Launch Management Console

1. On the Main Console desktop - Double click on the Management Console
Elevating an App based on Hash

1. Click the User Environment tab across the top of the window.
2. On the left panel - select Privilege Elevation.
   **Note:** There are other elevation policies in place that will be used and reviewed later in the lab.
3. Right Click on Elevate Legacy App
4. Click Enable
5. Click on Elevate Legacy App
6. Click the Edit on top row of icons.
Understanding Hash-based Privilege Elevation

1. Under the Allow box where LegacyApp.exe is listed, click **Edit**

   Users will note a Hash and Path for a specific application. This path is not actually something that has to be adhered to by UEM, but rather that path is used to generate the hash.
2. Click **Cancel** to close the Select executable to allow dialog.
3. Click **Cancel** to close the Application Blocking dialog.

**Minimize the UEM Management Console**

1. Close or minimize the Management Console by clicking either the X or the _ button in the top right corner of the window.

**Relaunch Desktop to Validate Changes**

1. If the Horizon Client is now closed, please re-launch the Horizon Client by double clicking on the **VMware Horizon Client** on the Main Console desktop.
1. Double click on `view-o1a.corp.local`

1. Log In as **lab1user**
2. Password: **VMware1!**
3. Click **Login**
1. Double Click **Windows 10 Instant Clone**

![Error Message](image)

**Note:** Sometimes the Desktop is not immediately available after a log out due to the fact that this is a lab and the instant clones do take a little more time than usual to regenerate.

1. Click **Try Again** in the top right corner after about a minute.
Relaunch Legacy App from T:\

1. Click on the **Folder** Icon on the Task Bar
2. Expand **This PC** on the left panel if it is not already expanded.
3. Click on the **tools** drive.
4. Attempt to run the LegacyApp by double clicking on **LegacyApp**
Run LegacyApp

1. Click **Run** to launch LegacyApp.exe

This time the LegacyApp launches in admin mode, as expected. Though to prove a point - it needs to be ran from multiple places to show that its a hash-based white list and not just a share with potentially special permissions.

1. Click the **X** on the top right corner of the window to close LegacyApp.
Copy LegacyApp from Tools

1. Select LegacyApp.exe.
2. Hold CTRL on the keyboard and select LegacyApp.exe.config.
3. Right click on LegacyApp.config and select Copy.
4. Click on Downloads on the left panel of the window.

Paste LegacyApp in Downloads
1. Right Click on any white space within the Downloads folder and select **Paste**.

![Image of Downloads folder with LegacyApp.exe highlighted]

1. Double Click on **LegacyApp.exe** to launch.
2. Select **Yes** to handle the power of the almighty admin.

**Review Legacy App**

![Image of Legacy App window showing running from folder and running as admin]

Note that Legacy App is STILL running in admin mode even without being in the original location. The same will be true no matter where this runs from.
Log out of the Desktop

1. On the top of the VDI Desktop screen - Click **Send Ctrl-Alt-Delete**
2. Click **Sign out**

**Summary**

At this point in the lab users should understand the basics setting up of Privilege Elevation for Elevated Apps. For more information on Privilege Elevation, please check out the [VMware User Environment Manager Administrator Guide](#) or the [VMware User Environment Manager YouTube Channel](#). If users would like details specifically Publisher-based Elevation - check out the video on [Publisher Based Application Blocking and Elevation](#).
Conclusion

Congratulations, you've finished Module 3

Congratulations on completing Module 3.

If you are looking for additional information on VMware User Environment Manager, try one of these:

- Click on this link
- Or go to http://bit.ly/VMwareUEM
- Or use your smart device to scan the QRC Code.

Proceed to any module below which interests you most.

- Module 1 - Introduction to VMware User Environment Manager
- Module 2 - Application Blocking
- Module 4 - Horizon Smart Policies
Module 4 - Horizon Smart Policies (45 minutes)
Introduction

In this Module the user can expect to learn the following:

- [Part 1] Introduction to Horizon Smart Policies
- [Part 2] Horizon Smart Policies - Creation and Execution
Introduction to Horizon Smart Policies

Horizon Smart Policies 101

User Environment Manager can interact with the Horizon Platform using Horizon Smart Policies. Horizon Smart Policies are simply Horizon-specific items that allow us to target very specific events and circumstances to apply policy. The great thing about UEM targeting is that it allows IT to use multiple pieces of information that are dynamic and that’s why we refer to them as ‘conditions’. Active Directory-based policy is fine for broad brush approaches, but isn’t always available or accurate enough for end-user computing (EUC) specific scenarios. We deal everyday with the nuances of multiple devices, locations, bring-your-own-X,\ and other factors that need to be considered.

The ability to control certain functionality inside a VDI or RDS session is driven by UEM as the Policy Engine. The integrations between UEM and Horizon allow for the use of the volatile environment variables that are passed by the client to the agent to form conditions. Thanks to triggered tasks, users can now refresh policies even on reconnect.
Smart Policies to control Bandwidth Profiles

The above image shows the detail of standard suggested PCoIP profiles used in real world circumstances. Now based on any number of conditions viewable by UEM, users are able to dynamically set the profile for the user and optimize the user experience on logon or unlock. This also works for the Blast Extreme protocol, meaning end users can always have the best user experience possible no matter what their connection conditions are like. For more information on Blast Extreme Adaptive Transport - start at this [Blog Post by Product Manager Kiran Rao](#).

Conclusion

At this point in the lab, users should have a high level understanding of the power and ideas behind Horizon Smart Policies. Moving forward in the lab will allow users to gain a better understanding of how UEM has the capacity to combine conditions with Triggered Tasks to show how Horizon Smart Policies can be truly "smart" and adaptive.
Horizon Smart Policies - Creation and Execution

In the previous section of this lab, users gained a high level overview of Horizon Smart Policies and how they drive the integration between User Environment Manager and Horizon. In this section of the lab, users will put Horizon Smart Policies into proactive by disabling USB Redirection, while conditionally enabling printing and clipboard use. This lab will feature Printer Mapping and Condition Sets in conjunction with Horizon Smart Policies.

Launch Management Console

1. On the Main Console desktop - Double click on the Management Console
Create Condition Sets now to save time later

Condition Sets were introduced in Module 1 - Introduction to Conditions and Environment Personalization.

1. Click on the **Condition Set** tab.
2. Click **Create**.
Create a Condition Set to detect External Horizon Sessions.
1. Name: External Horizon Session

2. Add Condition

3. Horizon Client Property
1. Set the Name of the condition set to **External Horizon Session**.
2. Click **Add**.
3. Click **Horizon Client Property**.

1. Set the Property to **Client Location**.
2. Set the **Is equal to:** to **External**.
3. Click **OK** to continue.
1. Click on **Add**.
2. Select **Remote Display Protocol**.

1. Set the Remote display protocol to **Blast**.
2. Click **OK** to continue.

**Save the Condition Set.**
Click **Save** to continue.

**Create a second condition set**

1. Click **Create** again.
Create a Condition Set to detect Internal Horizon Sessions.
1. Name: Internal Horizon Session
2. Add Condition
3. Horizon Client Property
1. Set the Name of the condition set to **Internal Horizon Session**.
2. Click **Add**.
3. Click **Horizon Client Property**.

1. Set the Property to **Client Location**.
2. Set the **Is equal to:** to **Internal**.
3. Click **OK** to continue.
Condition Set for Internal Horizon Sessions - Part 2
1. Click on **Add**.
2. Select **Remote Display Protocol**.

![Remote Display Protocol settings]

1. Set the Remote display protocol to **Blast**.
2. Click **OK** to continue.

**Save the Condition Set.**

![Condition Set settings]

**Save the Condition Set.**
Click **Save** to continue.

**Create a Horizon Smart Policy**

1. Click on the **User Environment** tab.
2. Click on **Horizon Smart Policies**.
3. Click on **Create**.
Create an Internal VDI Policy

1. Give the Policy a Name: **Internal VDI Policy**.
2. Check the box for USB redirection and set it to **Disable**.
3. Check the box for Printing and set it to **Enable**.
4. Check the box for Clipboard and set it to **Allow All**.
5. Check the box for Bandwidth profile and set it to **High-speed LAN**.
6. Click **Conditions** to continue.
Utilize Internal Horizon Session Condition Set
1. Click **Add**.
2. Click **Condition Set**.

1. Select **Internal Horizon Session**.
2. Click **OK**.
Specify Policy for Pool Name

1. Click on Add.
2. Click on Horizon Client Property.

1. Set Property to Pool name.
2. Change Is Equal to to Contains.
3. Set the value of the text box to to **Win10**.

**Save the Policy**

1. Click **Save** to continue.
Create another Horizon Smart Policy

1. Click on **Create**.
Create an External VDI Policy
1. Give the Policy a Name: **External VDI Policy**.
2. Check the box for USB redirection and set it to **Disable**.
3. Check the box for Printing and set it to **Disable**.
4. Check the box for Clipboard and set it to **Disable**.
5. Check the box for Bandwidth profile and set it to **Broadband LAN**.
6. Click **Conditions** to continue.
Utilize External Horizon Session Condition Set
1. Click **Add**.
2. Click **Condition Set**.

![Select Condition Set](image)

1. Select **External Horizon Session**.
2. Click **OK**.
Specify Policy for Pool Name

1. Click on **Add**.
2. Click on **Horizon Client Property**.

1. Set Property to **Pool name**.
2. Change Is Equal to to **Contains**.
3. Set the value of the text box to **Win10**.

**Save the Policy**

1. Click **Save** to continue.
Configure Printer Mapping

1. Click on **Printer Mappings** on the left panel.
2. Click on **Create**.
Setting up a Printer Mapping

1. Set the name to **VDI Printer**.
2. Set the Remote Path to `\appvol-01a\Sales-Printer`
3. Check the box to the left of **Default Printer**.
4. Check the box to the left of **Undo at logoff**....
   This box will unmapi the printer every single time the user logs off or there is a policy refresh for printing. This gives administrators the ability to change out printers on users between logins or after unlocks.
5. Check the box to the left of **Run asynchronously**.
   This box will prevent the system from "hanging" and waiting for the printer to map before continuing to process other policies. This is especially useful when there is high latency between the printer and the user's VDI session.
6. Click on the **Conditions** tab.
Printer Policy

1. Click on Add.
2. Click on Horizon Client Property.

1. Set Property to Pool name.
2. Change 'Is Equal to' to Contains.
3. Set the value of the text box to \textbf{Win10}.
Utilize Internal Horizon Session Condition Set
1. Click **Add**.
2. Click **Condition Set**.

   ![Select Condition Set](image)

1. Select **Internal Horizon Session**.
2. Click **OK**.

**Save the Policy and Continue**

![Printer Mapping](image)
1. Click on **Save** to continue.

**Minimize the UEM Management Console**

1. Close or minimize the Management Console by clicking either the X or the _ button in the top right corner of the window.

**Gathering Data for Testing**
1. On the Control Center desktop - Double click on README.txt
2. Highlight the first paragraph of text as shown in the image.

1. Click Edit
2. Click Copy
3. Close Notepad by clicking either the X in the top right corner of the window.

**Time to test**

1. On the Main Console Desktop - Double click on the VMware Horizon Client
1. Double click on **view-01a.corp.local**

![Login Screen](image)

1. Log In as **lab1user**
2. Password: **VMware1!**
3. Click **Login**

![Windows 10 Instant Clone](image)

1. Double Click **Windows 10 Instant Clone**

**Launch WordPad**

![WordPad Icon](image)

1. On the VDI Desktop - double click on **WordPad (created by VMware UEM)**
Testing Copy / Paste

1. Click on the **Paste** button to copy the previously selected text into WordPad.

As per the internal policy - pasting into the environment was successful.

Testing Printing

1. Click on **File**.
2. Click on **Print**.

When the print dialog comes up - notice the HP Color LaserJet automatically added from appvol-01a

1. Click **Cancel** to continue.
Log out of the Desktop

1. On the top of the VDI Desktop screen - Click **Send Ctrl-Alt-Delete**
2. Click **Sign out**
Close the VMware Horizon Client

1. Close the Horizon Client by clicking the X in the top right hand corner of the window.

Update Blast Security Gateway Policy

Due to the configuration of the various 1851 labs in VMware Hands-On-Labs, tunneling has been enabled on both the UAG and the Connection Server. In a production design, the tunneling would only be enabled for a single path at either the edge or at the Connection Server(s). As a result - this lab needs to modify the configuration to appear as an external connection.

1. On the Main Console Desktop - Double click on the Google Chrome icon.
Log in to the View-01A Admin Page

1. Click the **View-01A Admin** link in the bookmark toolbar
2. Sign in with Username: **Administrator**
3. Password: **VMware1!**
4. Click **Log In**

**Edit the connection server.**

1. Expand **View Configuration**.
2. Select **Servers**.
3. Click on the **Connection Servers** tab.
4. Click on the **VIEW-01A** Connection Server.
5. Click on **Edit**.
Disable Blast Secure Gateway

1. Uncheck the box next to **Use Blast Secure Gateway for Blast connections to machine**.
2. Click **OK** to continue.
Close Chrome

1. Close Chrome by clicking the X in the top right corner of the window.

Return to the Horizon Client

1. Please re-launch the Horizon Client by double clicking on the **VMware Horizon Client** on the Main Console desktop.

Note: This time users are connecting to **ap-01a.corp.local** instead of view-01a.corp.local
1. Double click on **ap-01a.corp.local**

![Login screen]

1. Log In as **lab1user**
2. Password: **VMware1!**
3. Click **Login**

![Windows 10 Instant Clone]

1. Double Click **Windows 10 Instant Clone**
Launch WordPad

1. On the VDI Desktop - double click on **WordPad (created by VMware UEM)**

**No Copy/Paste Test Possible**

Immediately - due to the Clipboard Restrictions - users will see that the text originally copied to the clipboard is no longer accessible to the desktop.
Testing Printing
1. Click on **File**.
2. Click on **Print**.

When the print dialog comes up note there are no remote printers, only file based printers.

1. Click **Cancel** to continue.
Log out of the Desktop

1. On the top of the VDI Desktop screen - Click **Send Ctrl-Alt-Delete**
2. Click **Sign out**

**Summary**

At this point in the lab, users should have a detailed understanding of Horizon Smart Policies, Condition Sets and Horizon and UEM integration points. For more information, please check out the [VMware User Environment Manager Administrator Guide](#) or the [VMware User Environment Manager YouTube Channel](#).
Congratulations, you've finished Module 4

Congratulations on completing Module 4.

If you are looking for additional information on VMware User Environment Manager, try one of these:

- Click on this link
- Or go to http://bit.ly/VMwareUEM
- Or use your smart device to scan the QRC Code.

Proceed to any module below which interests you most.

- Module 1 - Introduction to VMware User Environment Manager
- Module 2 - Application Blocking
- Module 3 - Privilege Elevation
Conclusion

Thank you for participating in the VMware Hands-on Labs. Be sure to visit http://hol.vmware.com/ to continue your lab experience online.

Lab SKU: HOL-1851-04-ADV

Version: 20170920-142118