# Table of Contents

- **Lab Overview** - HOL-1851-09-ADV - Horizon 7.1 Advanced: Security Concepts ........................................ 3
  - Lab Guidance ........................................................................................................................................ 4
- **Module 1 - Security Considerations** (15 minutes) ............................................................................ 10
  - Introduction & Overview ....................................................................................................................... 11
  - Device Protection Capabilities ........................................................................................................... 13
  - Network Protection Considerations .................................................................................................... 14
  - OS Protection Suggestions .................................................................................................................. 16
  - Application Protection .......................................................................................................................... 17
  - User Environment Protection ............................................................................................................. 18
  - General Protection ................................................................................................................................ 19
  - Module Conclusion .............................................................................................................................. 20
- **Module 2 - VMware Unified Access Gateway** (30 minutes) ............................................................ 22
  - Introduction & Overview ....................................................................................................................... 23
  - UAG Appliance Review and Settings in vSphere .................................................................................. 25
  - Unified Access Gateway Integration with Horizon Configuration ..................................................... 33
  - User Demonstration Connecting to Horizon With Unified Access Gateway ....................................... 36
  - Module Conclusion .............................................................................................................................. 41
- **Module 3 - SSL Certificates** (30 minutes) ....................................................................................... 43
  - Introduction & Overview ....................................................................................................................... 44
  - Introduction to SSL Certificates in VMware Horizon ......................................................................... 45
  - SSL Setup for VMware Horizon Connection Servers ......................................................................... 46
  - Module Conclusion .............................................................................................................................. 81
- **Module 4 - True SSO** (30 minutes) .................................................................................................. 83
  - Introduction & Overview ....................................................................................................................... 84
  - Benefits of True SSO ............................................................................................................................. 85
  - How True SSO Works ............................................................................................................................ 86
  - Supported Authentication Methods for Identity Manager ...................................................................... 88
  - Infrastructure Requirements ................................................................................................................ 89
  - Desktop OS Support .............................................................................................................................. 90
  - True SSO Deployment Walk Through and Demonstration .................................................................... 91
  - Module Conclusion .............................................................................................................................. 109
- **Module 5 - Governance and Compliance** (30 minutes) ................................................................ 111
  - Introduction & Overview ....................................................................................................................... 112
  - Healthcare Compliance ....................................................................................................................... 114
  - Government Compliance ..................................................................................................................... 121
  - Finance Compliance ............................................................................................................................. 131
  - Energy Compliance .............................................................................................................................. 139
  - Module Conclusion .............................................................................................................................. 147
- **Module 6 - Multifactor Authentication** (30 minutes) ..................................................................... 149
  - Introduction & Overview ....................................................................................................................... 150
  - Horizon 7 Multi-Factor Features ......................................................................................................... 151
  - VMware Identity Manager Multi-Factor Features ............................................................................... 161
Multi-Factor Demonstration and Walkthrough with VMware Identity Manager .......................... 163
Module Conclusion ............................................................................................................. 183
Module 7 - NSX for Horizon (60 minutes) ........................................................................ 185
Introduction & Overview .............................................................................................. 186
Fast and Simple VDI Networking .................................................................................. 188
Automated Policy Provisioning ...................................................................................... 189
Platform for Advanced Security .................................................................................... 190
Distributed Firewall Configuration Walkthrough and Demonstration ..................... 191
Module Conclusion ......................................................................................................... 262
Lab Overview - HOL-1851-09-ADV - Horizon 7.1 Advanced: Security Concepts
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 explore various use cases and security considerations of the Horizon suite. It is the intent of this lab to provide concise references to some of the security features and technologies built into and supported throughout the Horizon suite portfolio.

Lab Module List:

- **Module 1 - Security Considerations** (15 minutes) (Basic) This module will explore various use cases and security considerations of Horizon 7. It is the intent of this lab to provide concise references to some of the security features and technologies supported for Horizon 7. *(Informational Module)*

- **Module 2 - VMware Unified Access Gateway** (30 minutes) (Advanced) Within this section of the lab it will be shown how using VMware Unified Access Gateway will secure remote access to VMware end-user computing resources. There will be a walk through and demonstration lesson in this module you can follow.

- **Module 3 - SSL Certificates** (30 minutes) (Intermediate) This module will demonstrate securing various VMware Horizon server components with SSL certificates. There will be a walk through and demonstration lesson in this module you can follow.

- **Module 4 - True SSO** (30 minutes) (Intermediate) This module will review and demonstrate configuring True SSO (single sign-on) features in Horizon 7 while securing and adhering to Microsoft Windows (AD) Domain rights and authentication privileges. There will be a walk through and demonstration lesson in this module you can follow.

- **Module 5 - Governance and Compliancy** (30 minutes) (Basic) VMware governance and compliancy delivers the ability for customers to confidently and quickly secure mission critical virtualized workloads throughout many critical industries. This portion of the lab will provide guidance and information on these topics to assure compliance against many regulation requirements throughout various, unique industries. *(Informational Module)*

- **Module 6 - Multifactor Authentication** (30 minutes) (Intermediate) This module will provide information supporting multi-factor authentication with Horizon 7 to include SmartCard, RSA, RADIUS technologies. There will be a walk through and demonstration lesson specifically on RADIUS in this module you can follow.
• **Module 7 - NSX for Horizon** (60 minutes) (Advanced) This module will demonstrate how VMware End User Computing and NSX Security solutions can provide a customized desktop experience, doing so while maximizing operational efficiencies and security leveraging pure stateless VDI. There will be a walk through and demonstration lesson in this module you can follow to deploy Distributed Firewalls, configure firewall rules and test those rules against two different user groups.

**Lab Captains:**

• Chris Betz - Staff Systems Engineer - Federal System Engineering Team
• Trevor Davis - Senior Systems Engineer - SLED System Engineering Team

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 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 start-up 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 - Security Considerations (15 minutes)
Introduction & Overview

Within this section of the lab you will explore various use cases and security considerations of Horizon 7. It is the intent of this module to provide concise references to some of the security features and technologies supported within Horizon 7. This module is informational only and requires no interaction within the lab environment itself.

This Module contains the following lessons:

- **Device Protection Capabilities** - Overview of methodologies to protect devices
- **Network Protection Overview** - Leveraging VMware Networking technologies to secure the network
- **OS Protection Overview** - Protecting operating systems
- **User Environment Protection Overview** - Protecting user data and application data
- **Application Protection** - Securing Applications for end users
- **General Protection** - Miscellaneous technologies also leveraged to secure the Horizon environment

VMware Horizon deployments coupled with other VMware vSphere products offer many options for securing the end user environment. End users can access their desktops, applications and data from supported Web browsers, laptops, and a range of other devices, including a wide variety of operating systems inside or outside the corporate firewall, while corporate data and resources remain protected within the virtual datacenter. VMware Horizon deployments also provide a great deal of flexibility. For example, when accessing their virtual desktops, end users can redirect multimedia and USB devices for use within their Horizon View desktops as well as maintain personal profiles, which enable them to customize and maintain their desktops look and feel. With a personal profile, a user can also check a virtual desktop out to a local device, whether Bring Your Own Device (BYOD) or corporate-issued, and continue to work while mobile. Due to this flexibility, you must exercise vigilance in order to keep access to user data both secure and unimpeded. As a safeguard against loss or theft, for instance, you can set controls to disable a device in local mode if it is not synchronized within a certain time interval. Hackers and other potential intruders are always exploring new ways to circumvent the security process. This module will explore and provide overviews of many of the security options to consider when deploying Horizon. Within this lab we will break these technologies up into six major sections. This will include: device protection, network protection, OS protection, user environment protection,
application protection and overall general protection throughout the Horizon environment.

After reviewing all of the lessons throughout this module, you will have a better understanding of all the technologies that make VMware Horizon a secure working environment for end users.
Device Protection Capabilities

Within this lesson you will review the technologies and capabilities built into VMware Horizon that protect devices. It is only the intent to describe features available to the Horizon Suite to secure the end user environment.

- **Client Device Certificate Authentication**: VMware UAG (Unified Access Gateway) is a component within the Horizon Suite and it functions as a secure gateway for users who want to access remote desktops and apps outside the corporate firewall. A feature in UAG is for the silently authenticates only trusted client machines (endpoints that have the client device certificate installed). The certificate can be delivered as part of an enrollment process with VMware AirWatch (outside of the scope of this lab) or configured within Horizon covered in a later module of this lab. Click here for setup of SSL certificates within Horizon, also found in another module of this lab.

- **VMware Horizon Toolbox**: The Horizon Toolbox web portal is an extension to Horizon View in Horizon 6 and up. Within this portal includes “Device Access Policy” that limits access to the broker based on the media access control (MAC) address of a device. In a high-security environment, security organizations may want extra control on not only who connects to the system but also from which device. This is a very effective way to accomplish this task.

- **VMware NSX**: NSX makes “Zero Trust” model a reality. With the VMware Security Partner Ecosystem provides out-of-the-box endpoint security capabilities include: quarantining machines, killing processes, disabling network connections, changing registry data, uninstalling applications, resetting credentials, shutting down systems and even reimaging Windows endpoints at scale.

- **VMware ThinAapp**: Another option is to deliver your Horizon Client as a ThinAapp isolated app. This ensures the Horizon Client will not be changed, nor its configurations that might allow the attacker to abuse its code.
Network Protection Considerations

This lesson discusses some of the various technologies used to address network concerns within the Horizon environment.

- **VMware NSX for Horizon**: NSX allows administrators to create policies and security rules based on logical objects such as a specific virtual machine (VM) and/or folder to bring agility and control to your Horizon environment. This capability can complement a design with more security around Horizon. In addition, micro-segmentation within Horizon can make provide the back end network infrastructure with a zero-trust network. No resources will be able to contact other resources over network or any other unnecessary enterprise resources. NSX technologies and methodologies are covered more in depth within the Network Virtualization Tracks (NET) within Hands On Labs.

![Network Protection Considerations Diagram](image-url)
• **VMware Instant Clone Technology:** Instant Clone Technology allows admins to rapidly clone and deploy a VM in less than a few seconds (“just in time”). For example, administrators can decide to provision or decommission VM's only around users’ login time. Because the servers don’t exist until IT deploys them, there is no IP addresses to ping until then, no MAC etc... nothing exists. Because of this there's zero attack surface.

• **UAG:** Unified Access Gateway (UAG) acts as a proxy host for connections inside your company’s trusted network. This additional layer of security shields virtual desktops, application hosts and servers from the public-facing internet. The only remote desktop and application traffic that can enter the corporate data center is traffic on behalf of a strongly authenticated user.
OS Protection Suggestions

Within this lesson you will learn about some of VMware recommendations and best practices to protect the OS.

- **VMware OS Optimization Tool**: Optimize Windows 7, 8 and 10, as well as Windows Server 2008 and 2012, for View. With customizable templates, you can easily enable or disable Windows services and features (often enabled by default) to improve performance and enhance the security of the end user desktop.

- **Instant Clones & View Composer**: In addition to the network benefits of Instant Clones, View Composer supports recomposing (cleaning and redeploying from a standard snapshot). The desktop pools stay clean and up-to-date based on the setup (e.g. force clean desktop pools daily, weekly, etc.).

- **Disable vSphere Console Access**: In VDI, the user’s session can be viewed from the vSphere console for administrators creating a security breach and privacy issues. This is disabled by default and can be managed under the GPO ADM or registry (Software\Policies\Teradici\PCoIP\pcoip_admin pcoip.enable_console_access=0).

- **ThinApp Containerized Apps**: ThinApp isolation benefits apps management and ensures local OS resources are not available to the app itself. If the app is isolated from the host, any changes, deletions or additions made by the app to the file system or registry are recorded in the sandbox, instead of to the host OS.

- **Disable Peripherals on the VM**: Any external device or external interface can be used to bypass all software and OS security, so peripherals should be individually managed and disabled. Extract devices such as USB and serial ports and CD and floppy disk drives from the VM settings, and manually disable capabilities like hot plugging and VMware Tools.[Quick Tips: On the VM advanced settings, set “devices.hotplug” to “disable.” Edit “HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order” delete the “vmhgfs” string.]

- **VMware User Environment Manager (UEM)**: UEM simplifies end-user profile management, and, with the following features, gives you more control over the OS environment: DirectFlex, Environment Variables, application blocking (for example, regedit.exe, cmd.exe, powershell and other editors), hide drives, policy settings (such as hide “Run” and prohibit access to the control panel). Another best practice: Create a mandatory profile instead of using the defaults. (Note: This is officially supported by Microsoft only for Win2008R2 servers.)
Application Protection

This lesson will explain some of the considerations administrators should take when trying to secure the application environment.

- **VMware App Volumes AppStacks**: Read-only objects, AppStacks cannot be modified by the user (elevated or not) or the administrator. This helps administrators maintain a unified, standard end user environment while protecting the OS and applications from malware attempting to hijack the application environment.

- **NSX for App Volumes**: NSX for App Volumes enables IT to manage network policies associated with apps in App Volumes. This provides micro-segmentation from an application perspective while providing the same application firewall rules.

- **ThinApp Containerized Apps**: ThinApp protects apps from modifications and changes while running. Just enable the “Delete sandbox on exit.” Once enabled, each time a user runs Chrome, it will be a new install, keeping it secure and fresh.

- **UEM**: The user’s profile also holds a link to the app, as the application loads it corresponds with the AppData required to run (unless you defined zero customization for user, which will mitigate this risk, as well). With UEM, control a big part of the user’s profile and AppData when considering the following options: 1) Control and enforce predefined settings and 2) DirectFlex profile delivery. For example, block advanced configuration and appearance with predefined settings and not saving user changes on log off. This way IT can control the profile the user gets upon login.
User Environment Protection

This is a quick lesson that will provide guidance and suggestions to secure the user environment.

- **USB and Serial Redirection**: Map required USB devices Vendor ID (VID) and Product ID (PID), and use the whitelisting option in the Horizon GPO. If not needed, you can block it entirely using the same GPO.
- **Client Driver Redirection**: This is another bridge from the client to the Datacenter. Block this feature, or even better, don’t install the agent.
- **Disable Clipboard**: Horizon View Client and Agent have corresponding GPO settings to allow one or bi-directional clipboard usage.
- **Printing Redirection**: Printing can be used as a channel to transfer data and exploit the system. Disable where needed or use network-managed printers.
- **UEM**: Part of the user is his or her profile (%APPDATA%), which is directly managed by UEM. To strengthen security, consider using UEM Profile Backups, predefined settings and advanced settings (exclusion of files based on size and date). In addition, use the “Remove local profile at logoff” feature to clear the local copy after logoff. UEM also has “Horizon Smart Policy” feature so you can control all of the above for PCoIP.
General Protection

In the below lesson you will learn about miscellaneous considerations administrators should take to further secure and protect the Horizon environment.

- **vRealize Log Insight Windows Agent:** A Windows event channel is a pool for collecting related events in a Windows system. By default, the Log Insight Windows Agent collects events from the application, system and security channels. In a Windows system, applications can store log data in flat text files on the file system. The Log Insight Windows Agent can monitor directories and collect events from flat text log files.
- **Antivirus with NSX Integration:** With NSX, utilize the hypervisor level antivirus with third-party vendors. This offloading ensures each VM is protected and up-to-date with virus definition from the moment its created. [Click here for help installing NSX components.](#)
- **Disable Remote Desktop Protocol (RDP):** To make sure no RDP connections will override PCoIP and Blast protocols, disable the option to log in with RDP, even for administrators.
- **Windows Updates:** Regularly update your RDS server for critical and security updates. Refresh all servers from the image using Composer in a managed way and not individually with System Center Configuration Manager (SCCM) or Windows Server Update Services (WSUS), which can fail or be blocked by a malicious user.
- **Remove Unnecessary Software:** Remove unnecessary software like PowerShell, admin tools and debug tools.
- **Disconnect Idle Sessions:** With this internal tool, you can disconnect users not performing any jobs and idling on the system.
Module Conclusion

You have completed the Security Considerations Module of this lab. This module reviewed many suggestions and VMware best practices to secure the end user environment. Topics reviewed were Device Protection, Network Protection, OS Protection, User Protection, Application Protection and General protection. These recommendations can be deployed individually or together but should be delivered on top of Microsoft security best practices concerning the New Technology File System (NTFS), ports, services, etc. In addition, follow security hardening guides, like VMware vSphere and NSX, and follow each product minimal user rights required.

You've finished Module 1

Congratulations on completing Module 1.

If you are looking for additional information on Horizon 7, try one of these:

- Click on this [HOL-1851-09-ADV](http://bit.ly/VMwareHorizon7)
- Or use your smart device to scan the above QRC Code.

Proceed to any module below which interests you most. [Add any custom/optional information for your lab manual.]
• **Module 1 - Security Considerations** (15 minutes) (Basic) This module will explore various use cases and security considerations of Horizon 7. It is the intent of this lab to provide concise references to some of the security features and technologies supported for Horizon 7. *(Informational Module)*

• **Module 2 - VMware Unified Access Gateway** (30 minutes) (Advanced) Within this section of the lab it will be shown how using VMware Unified Access Gateway will secure remote access to VMware end-user computing resources.

• **Module 3 - SSL Certificates** (30 minutes) (Intermediate) This module will demonstrate securing various VMware Horizon server components with SSL certificates.

• **Module 4 - True SSO** (30 minutes) (Intermediate) This module will review and demonstrate configuring True SSO (single sign-on) features in Horizon 7 while securing and adhering to Microsoft Windows (AD) Domain rights and authentication privileges.

• **Module 5 - Governance and Compliancy** (30 minutes) (Basic) VMware governance and compliancy delivers the ability for customers to confidently and quickly secure mission critical virtualized workloads throughout many critical industries. This portion of the lab will provide guidance and information on these topics to assure compliance against many regulation requirements throughout various, unique industries. *(Informational Module)*

• **Module 6 - Multifactor Authentication** (30 minutes) (Intermediate) This module will provide information supporting multifactor authentication with Horizon 7 to include SmartCard, RSA, RADIUS technologies.

• **Module 7 - NSX for Horizon** (60 minutes) (Advanced) This module will demonstrate how VMware End User Computing and NSX Security solutions can provide a customized desktop experience, doing so while maximizing operational efficiencies and security leveraging pure stateless VDI.

**How to End Lab**

To end your lab click on the **END** button.
Module 2 - VMware Unified Access Gateway (30 minutes)
Introduction & Overview

VMware Unified Access Gateway (UAG) is a virtual appliance primarily designed to allow secure remote access to VMware end-user-computing resources from authorized users connecting from the Internet. UAG provides this secure connectivity to desktops and applications that are either cloud-hosted through Horizon Air or on-premises in a customer datacenter through VMware Horizon.

UAG functions as a secure gateway for users who want to access application and desktop resources from outside the corporate firewall. A UAG appliance typically resides within a network demilitarized zone (DMZ) and acts as a proxy host for connections inside your organizations trusted network. This design provides an additional layer of security by shielding VMware Identity Manager, virtual desktops, application hosts, and servers from the public-facing Internet.

UAG directs authentication requests to the appropriate server and discards any unauthenticated requests. The only VMware Identity Manager, virtual desktop, and hosted application traffic that can enter the organizations data center is traffic on behalf of a strongly authenticated user. Users can access only the resources that they are authorized to access.

UAG provides very similar functionality to View security server for Horizon 7 but does not need 1-to-1 pairing with a View Connection Server. UAG is also capable of proxying sessions to other VMware products and providing more advanced security options including authentication in the DMZ. If you are running View security servers, take the time to look at replacing them with UAG appliances.

This portion of the lab will show how the appliance has been deployed into the environment, review the appliance settings in vSphere. Demonstrate how UAG is tied into View Administrator console and configured. Then a walk-through of the steps of a user connecting into the environment with a view client logging into UAG.
This Module contains the following lessons:

- **Appliance review and settings in vSphere**
- **Demonstration of UAG Integration with Horizon**
- **Demonstration of a user connecting into the environment using UAG**
UAG Appliance Review and Settings in vSphere

This lesson will provide an overview of what Unified Access Gateway is, how its deployed and configured within vSphere. You will also login to Unified Access Gateway to review various configuration options for the appliance.

Unified Access Gateway is an appliance that is normally installed in a demilitarized zone (DMZ).

Unified Access Gateway is used to ensure that the only traffic entering the corporate data center is traffic on behalf of a strongly authenticated remote user.

Unified Access Gateway directs authentication requests to the appropriate server and discards any unauthenticated request. Users can access only the resources that they are authorized to access.

Unified Access Gateway also ensure that the traffic for an authenticated user can be directed only to desktop and application resources to which the user is actually entitled. This level of protection involves specific inspection of desktop protocols and coordination of potentially rapid changing policies and network addresses, to accurately control access.

Unified Access Gateway acts as a proxy host for connections inside your company's trusted network. This design provides an extra layer of security by shielding virtual desktops, application hosts, and servers from the public-facing Internet.

Unified Access Gateway is designed specifically for the DMZ. The following hardening settings are implemented.

- Up-to-date Linux Kernel and software patches
- Multiple NIC support for Internet and intranet traffic
- Disabled SSH
- Disabled FTP, Telnet, Rlogin, or Rsh services
- Disabled unwanted services

Deploying Unified Access Gateway

Unified Access Gateway is packaged as an OVF and is deployed onto a vSphere ESX or ESXi host as a pre-configured virtual appliance.

Two primary methods can be used to install the Unified Access Gateway appliance on a vSphere ESX or ESXi host. Microsoft Server 2012 and 2016 Hyper-V roles are supported.
The vSphere Client or vSphere Web Client can be used to deploy the Unified Access Gateway OVF template. You are prompted for basic settings, including the NIC deployment configuration, IP address, and management interface passwords. After the OVF is deployed, log in to the Unified Access Gateway admin user interface to configure Unified Access Gateway system settings, set up secure edge services in multiple use cases, and configure authentication in the DMZ.

PowerShell scripts can also be used to deploy Unified Access Gateway and set up secure edge services in multiple use cases. You download the ZIP file, configure the PowerShell script for your environment, and run the script to deploy Unified Access Gateway.

For the purpose of this lesson the vSphere method will be discussed.

**Deploying Unified Access Gateway Using the OVF**

Due to the UAG appliance already being deployed within this lab, the first portion of the lesson will simply review the steps of deploying the OVF into the virtual environment.

You can deploy the Unified Access Gateway appliance by logging in to vCenter Server and using the Deploy OVF Template wizard.

Two versions of the Unified Access Gateway OVA are available, standard OVA and a FIPS version of the OVA. The FIPS 140-2 version runs with the FIPS certified set of ciphers and hashes and has restrictive services enabled that support FIPS certified libraries. When Unified Access Gateway is deployed in FIPS mode, the appliance cannot be changed to the standard OVA deployment mode.

Use the native vSphere Client or the vSphere Web Client to log in to a vCenter Server instance. For an IPv4 network, use the native vSphere Client or the vSphere Web Client. For an IPv6 network, use the vSphere Web Client.

1. Select a menu command for launching the **Deploy OVF Template** wizard.
2. On the Select Source page, browse to the .ova file that you downloaded or enter a URL and click Next. Review the product details, version, and size requirements.
3. Follow the wizard prompts and take the following guidelines into consideration as you complete the wizard.
   - Name and Location (Enter a name for the appliance)
   - Deployment Configuration (Here you can select the number of NICs needed for both IPv4 and IPv6)
   - Host/Cluster (Select the host or cluster to deploy to)
   - Disk Format
   - Setup Networks/Network Mapping
   - Customize Network Properties
4. On the Ready to Complete page, select Power on after deployment, and click Finish.
5. When deployment is complete, verify that end users can connect to the appliance by opening a browser and entering the following URL:
Login and Configure UAG appliance

Please follow along within the console for this portion of the lab.

Once the UAG appliance has been deployed you can login to the appliance to review and configure various settings based on use case.

Launch Google Chrome

- Open Google Chrome from the desktop
Launch vCenter Web Client

- Select **HOL-1851 Admin**
- Next Select **vCenter WebClient**

![Image of vCenter Web Client login]

Login

- Select Use **Windows session authentication** and **Login**

![Image of Login screen]

Power On UAG Appliance

From the navigator pane, expand RegionA01, Expand RegionA01-COMP01 Cluster
• Right Click **ap-02a**
• Select **Power**
• Power on **ap-02a**

Browse to UAG Appliance

• Wait about 1 minute for the **ap-02a** to power on and open a new browser tab to login to **https://ap-02a.corp.local:9443/admin**
• Proceed to **ap-02a.corp.local (unsafe)**
Login UAG Appliance

- Login with **Admin**
- Password **VMware1!**

![VMware Unified Access Gateway login screen](image)
Configure Manually

- **Configure Manually** and **Select**

Review all of the settings and various Use Cases for UAG on both the General and Advanced Settings pages.

The General Settings and Advanced Settings pages include the following:

- Unified Access Gateway system configuration and SSL server certificate
- Edge service settings for Horizon, Reverse Proxy, and VMware Tunnel
- Authentication settings for RSA SecurID, RADIUS, X.509 Certificate, and RSA Adaptive Authentication
- SAML identity provider and service provider settings
- Identity Bridging setting configuration

The following options can be accessed from the Support Settings pages:
• Download Unified Access Gateway log zip files
• Export Unified Access Gateway settings to retrieve the configuration settings
• Set the log level settings
• Import Unified Access Gateway settings to create and update an entire Unified Access Gateway configuration

**Conclusion**

This lesson provided instruction to deploy the UAG appliance with a OAV file and logging into the UAG appliance to review various configuration options.

Moving onto the next lesson will dive deeper into configuring UAG for Horizon.
Unified Access Gateway Integration with Horizon Configuration

This lesson will provide you the steps needed to integrate UAG with Horizon View

Configure Horizon Settings

Please follow along on the console for this portion of the lab.

You can deploy Unified Access Gateway from Horizon View and Horizon Cloud with On-Premises Infrastructure. For the View component of VMware Horizon, the Unified Access Gateway appliance fulfills the same role that was previously played by the View security server.

To login to the UAG appliance please follow the steps outlined in the previous lesson, "UAG Appliance Review and Settings in vSphere."

General Settings

In the General Settings > Edge Service Settings line, click **Show**.

Horizon Settings

Click the **Horizon Settings** gearbox icon.
Change Settings

In the Horizon Settings page, change **NO** to **YES** to enable Horizon

![Enable Horizon](image)

Configuration Settings

The Following List of settings can be configured:

- Identifier
- Connection Server URL
- Proxy Destination URL Thumb Prints
- Auth Methods
- Health Check URL
- SAML SP
- PCOIP Enabled
- Proxy External URL
- Smart Card Hint Prompt
- Blast Enabled
- Blast External URL
- UDP Tunnel Server Enabled
- Tunnel Enabled
- Tunnel External URL
- Proxy Pattern
- Match Windows User Name
- Gateway Location
- Windows SSO Enabled
- Host Entries

For the purpose of this lesson configure the following for Horizon integration.

- Connection Server URL to [https://view-02a.corp.local:443](https://view-02a.corp.local:443)
- Proxy Destination URL Thumb Prints to 7e 39 0c e2 7f 7c 2a 3b 1f 52 51 00 bf 30 ea a1 c5 47 dd b8
- Enable PCOIP
- Enable BLAST
• Enable **UDP Tunnel Server Enabled**
• Select **Save**

**Conclusion**

This lesson provided you the steps necessary to integrate the Unified Access Gateway with Horizon.
User Demonstration Connecting to Horizon With Unified Access Gateway

This lesson will demonstrate a user logging into the UAG portal through the VMware Horizon Client and the VMware Horizon Web Client.

Login with VMware Horizon Client

- Launch the **VMware Horizon Client** from the Desktop

Select UAG

- Select the Unified Access Gateway **ap-01a.corp.local** server that is already configured for you.

Login

Login to the client by inputting:

HOL-1851-09-ADV

Page 36
• User Name: \texttt{lab1user}
• Password: \texttt{VMware1!}
• Domain: \texttt{CORP}
• Select \texttt{Login}

![Login to any Available Entitlement](image)

**Login to any Available Entitlement**

You are now logged into the Horizon View environment through the Unified Access Gateway! You can log into any of the available entitlements presented with the VMware Horizon Client.
Login with VMware Horizon Web Client

This section will show you how to login to the VMware Horizon Web Client.

- Select **Google Chrome** from the Desktop

VMware Horizon HTML Access

- In the Address Bar type: [https://ap-01a.corp.local](https://ap-01a.corp.local)
- Select **VMware Horizon HTML Access**

Login to Web Client

Login to the web client by inputting:
• User Name: **lab1user**
• Password: **VMware1!**
• Domain: **CORP**
• Select **Login**
Login to any Available Entitlement

You are now logged into the Horizon View environment through the Unified Access Gateway using the web client! You can login to any of the available entitlements presented with the VMware Horizon Web Client.

Lesson Conclusion

This concludes the steps required to login to the UAG appliance through both the VMware Horizon Client and VMware Horizon Web Client.
Module Conclusion

You have completed the VMware Unified Access Gateway Module of this lab. This module reviewed the appliance and settings within vSphere, demonstrated UAG integration with Horizon and demonstrated a user connecting into the environment with UAG through the VMware Horizon Client and VMware Horizon Web Client.

You've finished Module 2

Congratulations on completing Module 2.

If you are looking for additional information on Horizon 7, try one of these:

- Click on this [HOL-1851-09-ADV](#)
- Or use your smart device to scan the above QRC Code.
Proceed to any module below which interests you most. [Add any custom/optional information for your lab manual.]

- **Module 1 - Security Considerations** (15 minutes) (Basic) This module will explore various use cases and security considerations of Horizon 7. It is the intent of this lab to provide concise references to some of the security features and technologies supported for Horizon 7. (Informational Module)
- **Module 2 - VMware Unified Access Gateway** (30 minutes) (Advanced) Within this section of the lab it will be shown how using VMware Unified Access Gateway will secure remote access to VMware end-user computing resources.
- **Module 3 - SSL Certificates** (30 minutes) (Intermediate) This module will demonstrate securing various VMware Horizon server components with SSL certificates.
- **Module 4 - True SSO** (30 minutes) (Intermediate) This module will review and demonstrate configuring True SSO (single sign-on) features in Horizon 7 while securing and adhering to Microsoft Windows (AD) Domain rights and authentication privileges.
- **Module 5 - Governance and Compliancy** (30 minutes) (Basic) VMware governance and compliancy delivers the ability for customers to confidently and quickly secure mission critical virtualized workloads throughout many critical industries. This portion of the lab will provide guidance and information on these topics to assure compliance against many regulation requirements throughout various, unique industries. (Informational Module)
- **Module 6 - Multifactor Authentication** (30 minutes) (Intermediate) This module will provide information supporting multifactor authentication with Horizon 7 to include SmartCard, RSA, RADIUS technologies.
- **Module 7 - NSX for Horizon** (60 minutes) (Advanced) This module will demonstrate how VMware End User Computing and NSX Security solutions can provide a customized desktop experience, doing so while maximizing operational efficiencies and security leveraging pure stateless VDI.

**How to End Lab**

To end your lab click on the **END** button.
Module 3 - SSL
Certificates (30 minutes)
Introduction & Overview

In this lesson you will learn how VMware Horizon 7 leverages SSL Certificates and how to create, sign and install the necessary certificates.

This Module contains the following lessons:

- Introduction to SSL Certificates in VMware Horizon
- SSL Setup for VMware Horizon Connection Servers

With VMware Horizon, all communication channels between the Horizon components are secured with SSL authentication mechanisms. Starting with Horizon 5.1, upgrades or new installs, you will find a higher security standard for SSL certificates than in previous releases. In this module you will learn how VMware Horizon 7 leverages SSL Certificates and how to create, sign and install the necessary certificates on various Horizon Server components.
Introduction to SSL Certificates in VMware Horizon

With VMware Horizon, all communication channels between the Horizon components are secured with SSL authentication mechanisms. Starting with Horizon 5.1, upgrades or new installs, you will find a higher security standard for SSL certificates than in previous releases.

When you install the VMware Horizon servers in your environment, each one includes a default self-signed certificate. Self-signed certificates are issued by the server itself, not by a Certificate Authority. The server identifies and validates itself, which results in an untrusted certificate. Self-signed certificates provide very low-level security because untrusted server certificates are at risk of having traffic intercepted between the client and the servers. If an unauthorized server steps into the middle of a transaction and responds to the same IP address as the organizations server, the administrator receives no additional warning beyond the original warning resulting from the self-signed certificate.

Self-signed certificates are acceptable only for a testing environment, and are not secure enough for a production environment. VMware Horizon now makes using the default self-signed certificates more difficult to use by warning users and administrators if certificates are not signed by a Certificate Authority. To ensure a secure production environment, you need to install SSL certificates that are signed by a Certificate Authority (CA).

SSL certificates signed by a CA protect communications against tampering, eavesdropping, and man-in-the-middle (MITM) attacks. These certificates provide a secure channel between VMware Horizon clients and VMware Horizon servers for passing of private information, such as passwords and PINs. If you use the default self-signed certificates installed with VMware Horizon servers, communication between VMware Horizon servers and VMware Horizon clients can be compromised.
SSL Setup for VMware Horizon Connection Servers

In the following steps you will configure the VMware Horizon Connection Server with an SSL Certificate using the built-in Microsoft Active Directory Certificate Services, which issues certificates for public key security programs.

Microsoft Certificate Authority

The Microsoft Certificate Authority service has already been installed and configured to issue certificates for the corp.local domain.

In your organization you might use the MCA, or a third-party signing authority.


SSL certificate security is enhanced in VMware Horizon 5.1 and later

Warnings to users if the VMware Horizon Server certificate is not signed
Warnings to users if the VMware Horizon Server certificate is not signed by a Certificate Authority

VMware Horizon Clients include improved mechanisms to check certificates and to give warnings when the identity of the VMware Horizon server cannot be fully validated. All VMware Horizon servers are installed with default self-signed certificates. In VMware Horizon 5.1 and later, users by default receive warnings if you do not upgrade the default certificates to ones signed by a CA.

Newer VMware Horizon Clients can communicate only over HTTPS (HTTP over SSL). HTTP communication is no longer permitted. All VMware Horizon Client communication is encrypted.

Enhanced VMware Horizon component certificate-checking displayed

Enhanced VMware Horizon component certificate-checking displayed in the VMware Horizon Administrator dashboard

VMware Horizon now does more certificate checking to verify the identity of connected components. The VMware Horizon Administrator dashboard displays a red warning symbol next to VMware Horizon servers that do not have certificates signed by a trusted CA (a CA present in the Trusted Certificate Authorities store).
Support of the Windows Certificate Store

VMware Horizon supports only the Windows Certificate Store for managing certificates on VMware Horizon components. VMware Horizon formerly allowed JKS and PKCS certificate stores, or keystores, which use complex Java Keytool and command-line tools to generate certificate requests and import the resulting certificates back into the keystore. Windows administrators were less familiar with these tools than with Windows tools. You can use the Microsoft Management Console (MMC) Certificates Snap-In to perform part of the process of obtaining and importing certificates. The Windows Certificate Store is installed by default with the Windows operating system on both servers and desktops, and is a familiar certificate management interface for administrators.

This change to using the Windows Certificate Store allows you to better protect the private key for the certificate. The encryption password of the keyfile was stored in a text file if you used other certificate stores. In addition, with the Windows Certificate Store, the process of managing SSL server certificates is simplified and more likely to be accurate. The prior Java Keytool method for generating a CSR, creating a keystore, and importing the certificate into the keystore was more complex.
SSL Certificates Required for VMware Horizon Servers

The following VMware Horizon components require SSL certificates:

- VMware Horizon Connection Server
- VMware Horizon Security Server
- VMware Horizon Access Point
- VMware Horizon Composer server
- Intermediate servers that terminate SSL connections from VMware Horizon Clients
- vCenter Server

Certificate Types

With your Certificate Signing Request, you can ask for a single-server or multiple-server certificate:

- Single-server certificate You receive a certificate for a single specified server. This server can be either a VMware Horizon Connection Server or a load balancer.
VMware Horizon Clients access their desktops with a single URL to the Connection Server or load balancer.

- **Multiple-server certificates** The two common types of multiple-server certificates are SAN certificate and wildcard certificate.
  - Subject alternative name certificate (SAN) You receive a certificate valid for a single name, such as:
    - `desktops.<my_company>.com`
    - When you request this kind of certificate, you specify alternative server URLs to be allowed for this certificate, such as:
      - `vcs1.<my_company>.com`
      - `vcs2.<my_company>.com`
      - `vcs3.<my_company>.com`
    - You can place the same SAN certificate on each of several specified Horizon servers.
  - A SAN certificate is more secure than a wildcard certificate because you specify ahead of time the possible servers to be certified, but a SAN certificate is less expensive than a wildcard certificate because it is less extensible.

- **Wildcard certificate** You receive a certificate for all servers in your organizations domain: `*.<my_company>.com`
  - This wildcard certificate can be used for any server within a single domain level in your environment. For example, the `*.<my_company>.com` certificate can be used for the subdomain:
    - `<department>.<my_company>.com`
    - but not for
    - `<department>.it.<my_company>.com`
  - A wildcard certificate is the most flexible type of certificate, and therefore the most expensive. However, a wildcard certificate is considered less secure than a SAN certificate because the servers to be certified do not need to be specified ahead of time. An administrator could place the certificate on any server in the domain. In addition, with a wildcard certificate, more of your environment is exposed in the event of a compromise.

**Confirm Self-Signed Certificate with the VMware Horizon Administrator Console**

This lab is already configured for SSL but we will confirm the status of the connection server to show that the SSL cert is valid and working, remove the SSL cert to show how it breaks connectivity and then generate a new SSL certificate and verify that the new certificate is valid.
Launch Google Chrome

Log in to the VMware Horizon Administrator Console

- From the Main Console desktop, double click on Google Chrome
Login to View Administrator Console

- Select **View-02A Admin** from the tool bar
- Enter **User name: Administrator**
- Enter **Password: VMware1!**
- **Log In**
Verify Certificate

- Select **Dashboard**
- Expand **View Components**
- Select **View-02A**
- Verify SSL Certificate is **Valid**

Now that we have verified a good certificate, we are going to break connectivity by revoking and deleting the certificate associated to this Connection Server.
Remote into the Connection Server

- **RDP to the Connection Server**
  - From the Main Console desktop
    - Click on the Windows **Start** icon
    - Enter `mstsc /c` in the search window
    - Press the **Enter** key
Remote Desktop Connection

- Enter **view-02a.corp.local**
- Click **Connect**

![Remote Desktop Connection Window]

User Name

- User name: **CORP\administrator**
- Password: **VMware1!**
- Click **OK**

![Windows Security Window]
Launch the Microsoft Management Console (MMC)

From the **view-02a** desktop

- Right click on the **Windows Start** icon
- Select **Run**
- Type **mmc**
- Click **OK**
*Note* - Make sure you are launching MMC from within the remote desktop session to **view-02a** and not on the Main Console.
Add Snap-in

MMC - Add Snap-in

We need to add the Certificate Snap-in to MMC

- Choose **File**
- Select **Add/Remove Snap-in**

![Add Snap-in Diagram](image)

Add Certificates Snap-in

To manage the local Certificates, you need to install/enable the snap-in
• Click **Certificates**
• Click **Add**
• Click **Computer account**
• Click **Next**

Select Computer and Finish Snap-in Install

• Click **Local computer**
• Click **Finish**
• Click **OK** to close the Snap-ins window
Delete Trusted Cert

- Expand the **Certificates (Local Computer)**
- Expand the **Personal** folder
- Click on the **Certificates** folder
- Highlight both **view-02a.corp.local** certificates
- Delete
Restart VMware Horizon Connection Server

- From the **Start Menu** Type **Services**
- Click **Services**
Find Service

- Find the service **VMware Horizon View Connection Server**
- **Restart** Service

Service Restarting

- Wait for the service to restart

Verify SSL is Broken

Now we will check to see if we can still hit the **view-02a View Admin Console**

Minimize RDP window
Verify SSL is Broken

- Click **Google Chrome**
- Select **View-02A Admin** from the tool bar
- **Notice** you can no longer connect to the page due to an invalid cert

Create a New Certificate

Now you will step through the process of creating a new cert for view-02a so that we can connect to the View Admin Console again.

Maximize the view-02a RDP session that we minimized previously to Request New SSL Certificate. Your MMC console with the certificates add in should still be open.

To start the Certificate Enrollment

- Right click on **Certificates**
- Choose **All Tasks**
• Select Request New Certificate...
Begin Enrollment

- Click **Next** to begin the enrollment

Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate
Active Directory Enrollment

- Select the **Active Directory Enrollment Policy**
- Click **Next**
Certificate Box

- Select the VMware Certificate box.
- Click the link for **More information is required to enroll this certificate under the Web Server checkbox.**

![Certificate Enrollment](image)

Certificate Properties

On the Subject Tab of the properties of the certificate request
• Change the **Subject name** type to **Common name** from the drop-down list.
• In the **Value** field add the server name by entering: **view-02a.corp.local**
• Click **Add**
• Change the Alternative name type to **DNS** from the drop-down list.
• In the **Value** field add the FQDN by entering **view-02a.corp.local**
• Click **Add**
• Click **Apply** but do NOT click OK yet.
Certificate Properties Cont...

- Select the **General** tab
- Add the name to the **Friendly name** field by entering **vdm**
- Click **Apply** but do NOT click OK yet.
Certificate Properties Cont...

• Select the **Private Key** tab.
• Expand **Key Options**
• Check the box **Make private key exportable**
• Click **Apply**
• Click **OK**
Enroll Certificate

- Click **Enroll** to have the certificate issued from the CA
Verify Success

- You should receive a "Succeeded" message like this.
- Click Finish
View New Certificate
- Expand the **Certificates (Local Computer)**
- Expand the **Personal** folder
- Click on the **Certificates** folder
- Notice the new certificate has been issued by the Control Center-CA
- Close **MMC** when finished reviewing and DO NOT disconnect your RDP connection
- Select **No** to save console settings
- Note: Be careful not to close your remote connection to view-02a.corp.local
Restart VMware Horizon Connection Server

- From the **Start Menu** Type **Services**
- Click **Services**
Restart Service

- Find the service **VMware Horizon View Connection Server**
- **Restart** Service

Restart Service Cont...

- Wait for the service to restart

Minimize RDP

Now we will check to see if we can still hit the view-02a View Admin Console

- Minimize RDP window
Verify SSL Cert Works

- Click **Google Chrome**
- Select **View-02A Admin** from the tool bar
- *Notice* you can now connect to the View Admin Console with a valid cert. **This can take up to a minute for the connection to establish, keep refreshing your page until the page loads.**
Login View Administrator Conosle

- Enter **User name**: Administrator
- Enter **Password**: VMware1!
- **Log In**
Confirm Valid Certificate

- You can confirm that the new SSL Certificate is **Valid** and **green**

![VMware Horizon 7 Administrator](image)

Lesson Conclusion

You have successfully stepped through the process of installing and verifying SSL certs on a Connection Server.
Module Conclusion

You have completed the SSL Certificates module of this lab. This module reviewed SSL certificates as it pertains to the Horizon Suite and also demonstrated some of the components of Horizon and the use of those SSL certificates.

You've finished Module 3

Congratulations on completing Module 3.

If you are looking for additional information on Horizon 7, try one of these:

- Click on this [HOL-1851-09-ADV](#)
- Or use your smart device to scan the above QRC Code.

Proceed to any module below which interests you most.

- **Module 1 - Security Considerations** (15 minutes) (Basic) This module will explore various use cases and security considerations of Horizon 7. It is the intent of this lab to provide concise references to some of the security features and technologies supported for Horizon 7. *(Informational Module)*
- **Module 2 - VMware Unified Access Gateway** (30 minutes) (Advanced) Within this section of the lab it will be shown how using VMware Unified Access Gateway will secure remote access to VMware end-user computing resources.
- **Module 3 - SSL Certificates** (30 minutes) (Intermediate) This module will demonstrate securing various VMware Horizon server components with SSL certificates.
- **Module 4 - True SSO** (30 minutes) (Intermediate) This module will review and demonstrate configuring True SSO (single sign-on) features in Horizon 7 while securing and adhering to Microsoft Windows (AD) Domain rights and authentication privileges.
- **Module 5 - Governance and Compliancy** (30 minutes) (Basic) VMware governance and compliancy delivers the ability for customers to confidently and
quickly secure mission critical virtualized workloads throughout many critical industries. This portion of the lab will provide guidance and information on these topics to assure compliance against many regulation requirements throughout various, unique industries. (Informational Module)

- **Module 6 - Multifactor Authentication** (30 minutes) (Intermediate) This module will provide information supporting multifactor authentication with Horizon 7 to include SmartCard, RSA, RADIUS technologies.
- **Module 7 - NSX for Horizon** (60 minutes) (Advanced) This module will demonstrate how VMware End User Computing and NSX Security solutions can provide a customized desktop experience, doing so while maximizing operational efficiencies and security leveraging pure stateless VDI.

**How to End Lab**

To end your lab click on the **END** button.
Module 4 - True SSO (30 minutes)
Introduction & Overview

True SSO provides the ability to seamlessly sign onto a virtual desktop a single time using two-factor authentication via Identity Manager or Workspace ONE. True SSO separates authentication and access to Horizon-based desktops and applications.

Throughout this module are the following lessons (Select Links to Review the Lesson):

- Benefits of True SSO
- How True SSO Works
- Supported Authentication Methods for Identity Manager
- Infrastructure Requirements
- Desktop OS Support
- True SSO Walk-through and Demonstration

True SSO provides a way to authenticate to Microsoft Windows, retaining all of the users’ normal domain privileges, without requiring them to provide AD credentials! True SSO is a VMware Horizon technology that integrates VMware Identity Manager 2.6 with Horizon 7. VMware Identity Manager Standard is included in VMware Horizon 7 Advanced and Enterprise Editions.

With True SSO, a user can log into Identity Manager using any non-AD method (for example, RSA SecurID credentials) and once authenticated, the user is able to launch any entitled desktop or app (hosted from any domain) without ever being prompted for a password again!

True SSO uses SAML (Security Assertion Markup Language) to send the User Principal Name (for example, jdoe@example.com) to the identity provider’s authentication system to access AD credentials. Horizon 7 then generates a unique, short-lived certificate for the Windows login process.
Benefits of True SSO

True SSO

- Separates authentication (validating a user’s identity) from access (such as to a specific Windows desktop or application).
- Provides enhanced security. User credentials are secured by a digital certificate. No passwords are vaulted or transferred within the data center.
- Supports a wide range of authentication methods. Selecting or changing authentication protocols has a limited impact on the infrastructure of the enterprise.
How True SSO Works

Figure 1: The True SSO Authentication Process

Figure 1 shows the flow of data in True SSO:

1. A user authenticates to VMware Identify Manager. The administrator can select from an extensive set of authentication methods (RSA SecurID, RADIUS, Biometric, and so on). After authentication, the user selects a desktop or application to launch from VMware Identity Manager.
2. Horizon Client is launched with the user’s identity, and credentials are directed to the View Connection Server, the broker for Horizon 7.
3. The broker validates the user’s identify with Identify Manager by sending a SAML assertion.
4. Using the certificate Enrollment Service, Horizon 7 requests that the Microsoft Certificate Authority (CA) generate a temporary, short-lived certificate on behalf of that user.
5. Horizon 7 presents the certificate to the Windows operating system.
6. Windows validates the authenticity of the certificate with Active Directory.
7. The user is logged in to the Windows desktop or application, and a remote session is initiated on the Horizon Client.

True SSO does not rely on password vaulting, which risks compromising the credentials or having them become out of date, for example, with password changes. All
authentication and access to enterprise assets are provided by digitally signed credentials and certificates.
Supported Authentication Methods for Identity Manager

Identity Manager supports the following authentication methods in conjunction with True SSO:

- RSA SecurID
- Kerberos
- RADIUS authentication
- RSA Adaptive Authentication
- Standards-based third-party identity providers

Identity Manager also supports integration with third-party identity providers to federate authentication across the enterprise.

Of course, Identity Manager also supports user name and password credentials as well as smart card logins, but for either of these, True SSO is not needed.
Infrastructure Requirements

True SSO requires a Horizon 7 environment, which includes the View Connection Server and Horizon Agent, as well as a new service called the Enrollment Service. The Enrollment Service can run on Windows Server 2008 R2 or Windows Server 2012 R2 (4 GB RAM is sufficient).

In addition, a Microsoft CA is required. The CA can run on Windows Server 2008 R2 or Windows Server 2012 R2.

For high availability (HA), VMware recommends a minimum of 2 certificate authorities and 2 Enrollment Servers.
Desktop OS Support

True SSO is supported on all Windows guest operating systems that are supported for Horizon 7 desktops, from Windows 7 to Windows 10, along with Windows Server 2008 R2 and Windows Server 2012 R2. In addition, True SSO is supported on desktops and apps provided by Microsoft Remote Desktop Session Hosts running Windows Server 2008 R2 or Windows Server 2012 R2.

True SSO is supported with all display protocols, including Blast Extreme and HTML Access.
True SSO Deployment Walk Through and Demonstration

This lesson will provide you the steps needed to deploy and configure True SSO in a Horizon environment. A demonstration to confirm and validate SSO in the environment will also be provided.

True SSO provides the ability to seamlessly sign onto a virtual desktop a single time using two-factor authentication via Identity Manager or Workspace ONE. True SSO separates authentication and access to Horizon-based desktops and applications.

This lesson will provide you an overview of the components that are required to deploy True SSO within Horizon and take you through the steps to verify that True SSO is running within the environment.

Setting Up True SSO

Following is a list of tasks you must perform to set up your environment for True SSO:

- Determining an Architecture for True SSO
- Set Up an Enterprise Certificate Authority
- Create Certificate Templates Used with True SSO
- Install and Set Up an Enrollment Server
- Export the Enrollment Service Client Certificate
- Configure SAML Authentication to Work with True SSO
- Configure View Connection Server for True SSO

Many of these steps have already been deployed for you within the lab, please read each component for an overview of the steps needed to deploy SSO.

Determining an Architecture

To use True SSO, you must have or add a certificate authority and create an enrollment server. These two servers communicate to create the short-lived Horizon virtual certificate that enables a password-free Windows logon. You can use True SSO in a single domain, in a single-forest with multiple domains, and in a multiple-forest, multiple-domain setup.
For the purpose of this lab we have chosen to use a simple True SSO architecture.

**Set up an Enterprise Certificate Authority**

If you do not already have a certificate authority set up, you must add the Active Directory Certificate Services (AD CS) role to a Windows server and configure the server to be an enterprise CA.

If you do already have an enterprise CA set up, verify that you are using the settings described in this procedure.

You must have at least one enterprise CA, and VMware recommends that you have two for purposes of failover and load balancing. The enrollment server you will create for True SSO communicates with the enterprise CA. If you configure the enrollment server to use multiple enterprise CAs, the enrollment server will alternate between the CAs available. If you install the enrollment server on the same machine that hosts the enterprise CA, you can configure the enrollment server to prefer using the local CA. This configuration is recommended for best performance.

Part of this procedure involves enabling non-persistent certificate processing. By default, certificate processing includes storing a record of each certificate request and issued certificate in the CA database. A sustained high volume of requests increases the CA database growth rate and could consume all available disk space if not monitored. Enabling non-persistent certificate processing and can help reduce the CA database growth rate and frequency of database management tasks.
Create Certificate Templates Used with True SSO

You must create a certificate template that can be used for issuing short-lived certificates, and you must specify which computers in the domain can request this type of certificate.

You can create more than one certificate template, but you can configure only one template to be used at any one time.

Install and Set Up an Enrollment Server

You run the Connection Server installer and select the Horizon 7 Enrollment Server option to install an enrollment server. The enrollment server requests short-lived certificates on behalf of the users you specify. These short-term certificates are the mechanism True SSO uses for authentication to avoid prompting users for Active Directory credentials.

You must install and set up at least one enrollment server, and the enrollment server cannot be installed on the same host as View Connection Server. VMware recommends that you have two enrollment servers for purposes of failover and load balancing. If you have two enrollment servers, by default one is preferred and the other is used for failover. You can change this default, however, so that the connection server alternates sending certificate requests to both enrollment servers.

Export the Enrollment Service Client Certificate

To accomplish pairing, you can use the MMC Certificates snap-in to export automatically generated, self-signed Enrollment Service Client certificate from one connection server in the cluster. This certificate is called a client certificate because the connection server is a client of the Enrollment Service provided by the enrollment server.

Enrollment Service must trust the VMware Horizon View Connection Server when it prompts the Enrollment Servers to issue the short lived certificates for Active Directory users. Hence, the VMware Horizon View Connection Server clusters or pods must be paired with Enrollment Servers.

The Enrollment Service Client certificate is automatically created when a Horizon 7 or later connection server is installed and the VMware Horizon View Connection Server service starts. The certificate is distributed through View LDAP to other Horizon 7 connection servers that get added to the cluster later. The certificate is then stored in a custom container (VMware Horizon View Certificates\Certificates) in the Windows Certificate Store on the computer.
Import the Enrollment Service Client Certificate on the Enrollment Server

To complete the pairing process, you use the MMC Certificates snap-in to import the Enrollment Service Client certificate into the enrollment server. You must perform this procedure on every enrollment server.

Configure SAML Authentication to Work with True SSO

With the True SSO feature introduced in Horizon 7, users can log in to VMware Identity Manager 2.6 and later releases using smart card, RADIUS, or RSA SecurID authentication, and they will no longer be prompted for Active Directory credentials, even when they launch a remote desktop or application for the first time.

With earlier releases, SSO (single sign-on) worked by prompting users for their Active Directory credentials the first time they launched a remote desktop or hosted application if they had not previously authenticated with their Active Directory credentials. The credentials were then cached so that subsequent launches would not require users to re-enter their credentials. With True SSO, short-term certificates are created and used instead of AD credentials.

Although the process for configuring SAML authentication for VMware Identity Manager has not changed, one additional step has been added for True SSO. You must configure VMware Identity Manager so that password pop-ups are suppressed.

Configure View Connection Server for True SSO

You can use the vdmutil command-line interface to configure and enable or disable True SSO.

This procedure is required to be performed on only one connection server in the cluster.

SSO Additional Steps and Validation

These next few steps will take you through the process to configure vIDM for True SSO integration with Horizon. These would be required steps needed once vIDM has been deployed and configured.
• Open Google Chrome from the desktop.

**Login**

• Input user name:  
  ◦ **Admin**

• Input Password:  
  ◦ **VMware1!**

• Select **Sign in**
Select Catalog

- Select the **Catalog** tab
- Select **Manage Desktop Applications**
- Select **View Application**

### Suppress Password Popup

For True SSO to work with vIDM and Horizon 7, we need to log into the vIDM administration page of the View Pools and enable Suppress Password Popup.
• Verify **Suppress Password Popup** is selected

Without doing this, vIDM will prompt the user for a password when launching a Horizon desktop or app if it doesn’t already have a password cached. For True SSO we do not need to cache passwords or request this, hence the option to suppress the password popup.

**Launch RDP for View-01a.RDP**

We will set up Horizon Connection Server to use True SSO for a certain domain by using a command line tool called vdmUtil.

vdmUtil is located in the Horizon Connection Server folder. Typically, it can be found here on the Connection Server:

%PROGRAMFILES%\VMware\VMware View\Server\tools\bin

When launching the console, the following commands would be used to configure the Connection server for True SSO:
• Select the **View-01a.RDP** icon from the desktop

![View-01a.RDP icon](image)

**Open Command Prompt**

• Start typing **"cmd"** from the **Start Menu** and hit enter

![Start Menu with cmd](image)

**vdmutil Command**

• From the Command Prompt type **vdmutil**
• This will display all of the command line options available to vdmutil
vdmUtil List Information

Here we will find out detailed info about how to identify various components of the environment which will be useful for configuring True SSO.

• List information from the cmd for the Enrollment Server
  ◦ vdmUtil --authAs administrator --authDomain corp.local --authPassword VMware1! --truesso --environment --list --enrollmentServer truesso-01a.corp.local --domain corp.local

List SAML Authenticators

• List all SAML Authenticators available in the Horizon View environment.
  ◦ vdmUtil --authAs administrator --authDomain corp.local --authPassword VMware1! --truesso --list --authenticator

• Looking at the output you will notice that True SSO is enabled for the Horizon environment
Test SSO

When you successfully verify the steps above, True SSO should now be correctly configured for domain corp.local. To verify the state of True SSO, we can now go to the admin page of the Horizon Connection Server and check the Dashboard.

From the desktop select **Google Chrome**
Test SSO Cont...

- Select **View-01A Admin** from the tool bar
- Input User Name:
  - **Administrator**
- Input Password
  - **VMware1!**
- Domain = Corp.local
- Select **Log In**
Test SSO Cont...

- With **Dashboard** highlighted, select **True SSO**
- Select **corp.local**

Make sure that the True SSO Domain Details are all green

---

Testing SSO...

Now we can launch a web browser and connect to vIDM. Once authenticated, we should be able to see all entitled desktops and apps.
We can launch any desktop or app with a click on the icons. The user should not be prompted for AD credentials and will be logged into the desktop or app with an interactive session.
Testing SSO Cont...

- Log in with User name:
  - lab1user

- Password:
  - VMware1!

- Domain:
  - Corp
Login to Entitlement

- Select any of your entitlements and you will see True SSO log you into any instance.
SSO is Working

If you reached this stage, True SSO is working! We can now check the logs on the desktop where the user logged in to verify that True SSO worked as expected.

After logon is completed we can open the debug logs for Horizon View Agent. This will typically be:

\%PROGRAMDATA\%\VMware\VDM\logs\debug-<date>-<pid>.txt

**From the Main Console we will access the logs from the Windows 10 desktop that we logged into with True SSO**

- On a Run line type `\W10-ic-01\c$\programdata\VMware\VDM\logs`

Filter the files to show the latest modified and open the latest debug log file.
Right click the file and **Edit with Notepad++**
• Now you can search through the file for the below syntax

Lesson Conclusion

This concludes the steps required setting up True SSO with Horizon View.
Module Conclusion

You have completed the True SSO module of this lab. This module reviewed True SSO and demonstrated how the True SSO integrates into the Horizon Suite. It was also demonstrated how True SSO delivers a fast, secure, streamlined experience for the end user.

You've finished Module 4

Congratulations on completing Module 4.

If you are looking for additional information on Horizon 7, try one of these:

- Click on this [HOL-1851-09-ADV](http://bit.ly/VMwareHorizon7)
- Or use your smart device to scan the above QR Code.

Proceed to any module below which interests you most.

- **Module 1 - Security Considerations** (15 minutes) (Basic) This module will explore various use cases and security considerations of Horizon 7. It is the intent of this lab to provide concise references to some of the security features and technologies supported for Horizon 7. *(Informational Module)*
- **Module 2 - VMware Unified Access Gateway** (30 minutes) (Advanced) Within this section of the lab it will be shown how using VMware Unified Access Gateway will secure remote access to VMware end-user computing resources.
- **Module 3 - SSL Certificates** (30 minutes) (Intermediate) This module will demonstrate securing various VMware Horizon server components with SSL certificates.
- **Module 4 - True SSO** (30 minutes) (Intermediate) This module will review and demonstrate configuring True SSO (single sign-on) features in Horizon 7 while securing and adhering to Microsoft Windows (AD) Domain rights and authentication privileges.
- **Module 5 - Governance and Compliancy** (30 minutes) (Basic) VMware governance and compliancy delivers the ability for customers to confidently and
quickly secure mission critical virtualized workloads throughout many critical industries. This portion of the lab will provide guidance and information on these topics to assure compliance against many regulation requirements throughout various, unique industries. (Informational Module)

- **Module 6 - Multifactor Authentication** (30 minutes) (Intermediate) This module will provide information supporting multifactor authentication with Horizon 7 to include SmartCard, RSA, RADIUS technologies.
- **Module 7 - NSX for Horizon** (60 minutes) (Advanced) This module will demonstrate how VMware End User Computing and NSX Security solutions can provide a customized desktop experience, doing so while maximizing operational efficiencies and security leveraging pure stateless VDI.

How to End Lab

To end your lab click on the **END** button.
Module 5 - Governance and Compliance (30 minutes)
Introduction & Overview

Within this section of the lab you will explore various use cases and security considerations of Horizon 7 as they pertain to various industries. It is the intent of this module to provide concise references to some of the compliance programs, features and technologies supported within Horizon 7 across those industries. This module is informational only with no interaction within the lab environment itself.

Within this module you will find the following lessons:

- **Healthcare Compliance** - Review of Healthcare compliance within Horizon
- **Government Compliance** - Review of Government (Federal\State & Local) compliance within Horizon
- **Finance Compliance** - Review of Finance Compliance within Horizon
- **Energy Compliance** - Review of Energy Compliance

Many organizations have initiatives to virtualize their Information Technology (IT) infrastructure, or to move to a Cloud Computing model. However, these initiatives are often complicated by the increasing number of regulatory compliance requirements, which require protection of data such as 1PCI, 2HIPAA, 3FISMA, 4DIACAP, 5FedRAMP, 6GLBA, and other State and Federal requirements. Organizations are increasingly concerned with the complexity, risk, and impact that a new technology can bring to their existing environment(s).

Historically, most organizations have had to gradually gather solutions from a variety of vendors and best practices in order to create an entire IT architecture that can meet their business compliance needs. While each vendor may have their own specific guidance on how to meet compliance, they often do not have guidance on how to meet controls that were not addressed by their specific solutions. This can lead to a delay in the adoption of cloud and virtualization initiatives as it often requires a significant investment in time, resources, and technical capabilities.

VMware has addressed these challenges by establishing a Compliance Reference Architecture Framework (RAF) that provides a consistent way for VMware, its partners, and organizations to assess and evaluate the impact of regulations on virtual and cloud environments. The intent of the RAF is to provide a single framework for VMware, its partners, and organizations to address a variety of compliance requirements across an IT infrastructure. The RAF is comprised of four primary components:

- **Use Case** - Provides a business description of an organization and how it has designed its IT architecture to meet specific regulatory and compliance requirements.
- **VMware Product Suites** - VMware’s recommended product suites designed to help meet compliance requirements.
VMware Partner Products Provides a framework for partners to address controls that are not covered by VMwares product suites.

Organizational Requirements _ Provide guidance on adjacent control requirements not addressed by VMware or Partner solutions such as physical security.

The main focus on this module is for the Horizon stack and how these various compliance challenges are addressed and solved with VMware solutions.
Healthcare Compliance

As part of the VMware Compliance Reference Architecture Framework, VMware has developed these documents are must reads for anyone interested in compliance and cybersecurity for HIPAA.

Information security design and architectural requirements, driven by regulatory compliance, are common but critical aspects that organizations should consider when migrating from traditional IT environments to cloud computing environments. Helping organizations with the arduous tasks of meeting and maintaining HIPAA and the HITECH act regulatory compliance, VMware and its partners provide suites of industry-leading, virtualization solutions which address the confidentiality, integrity and availability requirements of HIPAA/HITECH.

This module will explain how VMware meets HIPAA Requirements within a Cloud Computing Environment” by providing helpful information to VMware architects, the HIPAA/HITECH community, business stakeholders and third parties.

Due to the broad context of the HIPAA and HITECH acts it is prudent to properly define and detail the scope of this module and the approach that has been taken in defining such scope. The scope is divided between the VMware components that are included, reviewed and considered highly relevant as part of this guide and the governing sections of the HIPAA and HITECH Acts that pertain to electronic data, information technology and thus network and electronic information security. While this module provides specific technical opinions regarding the applicability of VMware solutions to HIPAA’s regulations the guide is neither comprehensive in its coverage of the entire HIPAA regulation nor prescriptive. It does not define a single implementation strategy that assures compliance but simply explains work that is done from a Horizon perspective to meet these Healthcare requirements.

Highlights

- Security and Compliance Thought Leadership
- VMware and Partner Product Applicability
- Independently Audited and Validated Guidance

Overview

VMware recognizes the following as critical areas that must be addressed by each covered entity and business associate in the operation of healthcare information systems: security and compliance; the criticality and vulnerability of the assets needed to manage electronic protected health information (ePHI) impacting infrastructures; and the risks to which they are exposed. By standardizing an approach to compliance and expanding the approach to include partners, VMware provides its customers a proven solution that more fully addresses their compliance needs. This approach provides
management, IT architects, administrators, and auditors a high degree of transparency into risks, solutions, and mitigation strategies for moving critical applications to the cloud in a secure and compliant manner. This is especially important when the outcomes for noncompliance are extremely critical due to civil and criminal penalties imposed by the Office for Civil Rights (OCR) Department of Health and Human Services (HHS) and the U.S. Department of Justice (DOJ); not to mention, there is a high probability for collateral impact due to failure to protect patient privacy, institutional trust and economics. In extreme cases of breach or data loss, the fines and penalties are minor compared to the potential for litigation, recompense and/or public relations improvements.

For these reasons, VMware enlisted its audit partner, Coalfire Systems, to engage in a programmatic approach to evaluate VMware products and solutions for HIPAA Security Rule requirements capabilities and document these capabilities into a set of reference architecture documents. This document presents Coalfire’s evaluation of the different VMware applications available to organizations that use (or are considering using) VMware software-defined data center (SDDC) and end-user computing EUC environments to host or access ePHI impacting critical cyber assets. Specifically, this document focuses on the SDDC and EUC solutions available. The software-defined data center is defined as a platform, which brings together best-in-class compute, storage, networking, security and technical management, virtualized and delivered as a service. A unified hybrid cloud lets you rapidly develop, automatically deliver, and manage all of your enterprise applications, no matter where they reside, from one, unified platform. To that end, Coalfire highlights the specific HIPAA Security Rule requirements that these applications address and/or support. The applications outlined in this product applicability guide can be considered in evaluation of the initial sourcing of technologies to build a platform which helps covered entities and business associates meet HIPAA requirements.

Most organizations begin the compliance process by mapping the mandated requirements to their specific organizational needs and capabilities. This is usually a difficult task that can utilize significant time and resources. To streamline the process, VMware has established a single holistic approach that can be used to evaluate the VMware environment, partner solutions, and end user tools. This Product Applicability Guide, the first in a series of white papers that make up the reference architecture framework, maps HIPAA Security Rule requirements to VMware's software-defined data center and end-user computing technology platforms.

Organizations can significantly reduce the complexity and cost of HIPAA Security Rule compliance by replacing traditional non-integrated products with integrated solutions. As most organizations know, there is no single product or vendor that can meet all of an organization’s needs. To further address this gap, VMware, together with the VMware partner ecosystem delivers compliance-oriented integrated solutions, enabling compliance by automating the deployment, provisioning and operation of regulated environments. VMware provides the solution reference architecture, HIPAA Security Rule specific guidance, and software solutions that businesses require to be able to achieve continuous compliance, along with breakthrough speed, efficiency and agility for their deployments. These solutions directly address agency needs for:
The VMware compliance reference architecture framework provides a programmatic approach to map VMware and partner products to regulatory controls, from an independent auditor perspective. The result is valuable guidance that incorporates best practices, design, configuration and deployment with independent auditor oversight and validation.

VMware illustrates measures of capability with respect to security, confidentiality, and integrity that make up a trusted cloud implementation in the below graphic. The graphic illustrates the specific solution categories that can be addressed with VMware solutions and VMware's extensive partner ecosystem.

By addressing and implementing the security solutions within the framework of the regulated infrastructure many of the technical control requirements for any particular regulation are addressed. By integrating these security solution components together in a cohesive manner, the outcome is a compliance-capable, audit-ready platform upon which the covered entity or business associate can overlay its business systems and data.
VMware illustrates the alignment of system security solutions with compliance frameworks and gives examples of VMware technologies and solutions that are capable of addressing the solution. End User Computing technologies are outlined in RED.

### VMware Workspace ONE

VMware End-User computing products allow IT organizations to pro-actively deliver consistent and intuitive services to their customers. Driven by the demands of users for immediate access to applications and data from any device, at any time, and from any place, services can be orchestrated to meet these demands without sacrificing...
compliance requirements. As a result, the user is able to work more efficiently in a manner that best suits his or her needs, while IT is able to manage that experience to ensure confidentiality, integrity and availability. VMware Workspace ONE combines end-user computing technologies from VMware and AirWatch by VMware to unify the end-user experience for secure access to applications and content from laptops, desktops, zero or thin-clients, and mobile devices and tablets.

**VMware Horizon 7 Enterprise Edition**

- vSphere Desktop and vCenter Desktop
- Horizon with View
- Horizon for Linux
- vSphere and vCenter for Desktop
- vRealize Operations for Horizon
- User Environment Manager
- Mirage
- App Volumes
- ThinApp

**AirWatch Enterprise Mobility Manager**

VMware AirWatch is a scalable enterprise mobility management platform that integrates with existing enterprise systems and allows you to manage all devices, regardless of type, platform or ownership, from one central console. Included with AirWatch Enterprise Mobility Manager are the tools necessary to allow end users, regardless of their device, to securely interact with HIPAA compliant workloads. The ability for administrators to manage and control the device ensures the integrity of the device and security of the data that these devices are accessing.

- AirWatch Container Management
- AirWatch Mobile Device Management
- VMware AirWatch Mobile Applications Management
- AirWatch Mobile Content Management
- VMware AirWatch Mobile Email Management
- AirWatch Mobile Browsing Management
**VMware Identity Manager**

VMware Identity Manager is an Identity as a Service (IDaaS) offering, providing application provisioning, self-service catalog, conditional access controls and Single Sign-On (SSO) for SaaS, web, cloud and native mobile applications. Identity Manager delivers on consumer-grade expectations like one-touch access to apps. This delivery of applications can be optimized with AirWatch Conditional Access and backed by a self-service catalog with enterprise-class management and security.

**VMware Horizon FLEX**

VMware Horizon FLEX provides the flexibility IT needs to serve BYO users, Mac users, contractors and road warriors while ensuring security, control and compliance for the corporate desktop. Horizon FLEX containerizes corporate windows desktops that are then distributed to these various devices. This containerization of the desktop allows for IT to implement all of the security measures required by the organization and to confirm that these measures are properly securing the workload and any data contained therein.

**VMware Approach**

The HIPAA Security Rule Solutions Applicability Matrix, found in the sections following this module, maps specific requirements of the HIPAA Security Rule to VMware’s solutions suites, their component technologies, and partner technologies where specifically integrated with made use of by the VMware technologies.

The understanding of the HIPAA Security Rule requirements is supported by NIST SP 800-66 and NIST 800-53 revision 4. Based on available product documentation, a notional determination of capabilities with respect to the requirement allowed for the alignment process to determine the extent of attainability of the technology or the solution as a whole to address the HIPAA requirement. The inferences drawn upon by this common understanding support cases where the technology is specifically capable of attaining control enablement, the technology partially supports control enablement, and/or the technology does not undermine the requirement. Though HIPAA does not specifically include guidance relative to cloud and virtualization, the concepts of controls relative to confidentiality, integrity and availability are applicable to the software-defined data center.
The below graphic illustrates the VMware's complete approach to compliance.

**Conclusion**

There is no doubt that the transformation of business to the digital world presents exciting opportunities for businesses around the world. New businesses have emerged in recent years that have shifted the paradigm for how things are traditionally done. Among these transformations is the concept introduced by VMware of “One Cloud, Any Application, Any Device” architecture. Alone, this capability presents opportunities for improvements in how people interact with information. Improvements in speed and the availability of information can assist people in business and the health care industry with making informed decisions. This flexibility also presents the possibility for greater risk. It isn’t uncommon for security to follow in the footsteps of a brave new frontier as the awareness for the need of security paces behind the benefit for the new technology. Even with the benefits from accelerated innovation and mobile cloud applications, security of electronic protected health information is still of utmost concern. This product applicability guide identified ways in which VMware’s software-defined data center and end-user computing platforms help to govern risk and support a responsible participation in ongoing and continuing innovation.
Government Compliance

As part of the VMware Compliance Reference Architecture Framework this module includes the latest core Reference Architecture information for Federal Risk Authorization and Management Program (FedRAMP) and Criminal Justice Information Services (CJIS)

FedRAMP

The Federal Risk Authorization and Management Program (FedRAMP) was created to provide a streamlined and standardized process along with a “do once, use many times” approach to the authorization of commercial cloud services.

This program enables US Government agencies to take full advantage of the benefits of migrating their IT assets and infrastructure to the cloud, as they work to meet the goals of the Federal Cloud Computing Strategy published by the White House in February 2011.

The FedRAMP program provides an avenue for Cloud Service Providers (CSPs) to obtain a provisional Authorization To Operate (p-ATO) after undergoing an independent third-party security assessment that has been reviewed by the JAB. By assessing security controls on candidate platforms, and providing P-ATOs on platforms that have acceptable risk, FedRAMP significantly reduces the time and cost to agencies by removing the assessment and authorization requirements of the underlying cloud vendor services on a system-by-system basis. This minimizes the work each Consumer of FedRAMP Cloud resources must undergo to receive an actual ATO for the workloads running applications that process sensitive data and transactions.

CJIS

The Federal Bureau of Investigation (FBI) established the Criminal Justice Information Services (CJIS) Division in 1992 to meet the need for criminal justice information to be available 24/7 in order for law enforcement, national security, and the intelligence community partners to protect the United States while preserving civil liberties.

Today, CJIS is FBI's largest division and processes millions of transactions on a daily basis, with response times ranging from minutes to seconds. The CJIS Division is responsible for many information technology-based systems like the National Crime Information Center (NCIC), National Instant Criminal Background Check System (NICS), Interstate Identification Index (III), National Data Exchange (N-DEx), Uniform Crime Reporting (UCR) Program, and the Next Generation Identification (NGI). These systems provide state, local, and federal law enforcement and criminal justice agencies with timely and secure access to critical, personal information such as fingerprint records, criminal histories, and sex offender registrations.

Description
This module will explain how VMware meets FedRAMP and CJIS requirements within a computing environment by providing helpful information to VMware architects, the FedRAMP and CJIS communities, business stakeholders and third parties specifically within the mobility and end user computing space.

VMware recognizes the tremendous opportunity that FedRAMP and CJIS provides customers wishing to leverage VMware vCloud-powered FedRAMP and CJIS environments for hosting their enterprise applications. For an entity wishing to host applications in a FedRAMP-accredited or CJIS-accredited VMware vCloud hosting provider, or for the vCloud hosting provider itself, it is beneficial to understand which features of the VMware stack may apply in gaining and maintaining FedRAMP and CJIS compliance. In addition to VMware Products and Suites VMware's Technology Partners' solutions may also be used to provide this goal of ongoing FedRAMP accreditation with the greatest security, agility and cost savings.

**Highlights**

- Security and Compliance Thought Leadership
- VMware Solutions for FedRAMP and CJIS
- Independently Audited and Validated Guidance

**FedRAMP Overview**

The United States Federal Government’s cloud first policy presents tremendous opportunities for cloud service providers wishing to host IT operations for Federal Government agencies. According to a paper written by the U.S. Chief Information Officer, Vivek Kundra, dated February 8th, 2011,

“The Federal Government’s current Information Technology (IT) environment is characterized by low asset utilization, a fragmented demand for resources, duplicative systems, environments which are difficult to manage, and long procurement lead times. These inefficiencies negatively impact the Federal Government’s ability to serve the American public. Cloud computing has the potential to play a major part in addressing these inefficiencies and improving government service delivery. The cloud computing model can significantly help agencies grappling with the need to provide highly reliable, innovative services quickly despite resource constraints.” (Kundra, 2011)

Service providers wishing to deploy workloads look for compliant, cost effective, flexible, and highly scalable designs. However, building and operating a cloud can be a complex undertaking. The process involves integrating hardware, installing and configuring software, optimizing and securing the overall infrastructure for performance, scale and reliability. From start to finish, the deploying of these solutions can take several months from purchase to deployment utilizing a specialized team of IT professionals, including networking, storage, virtualization, operating system, and security experts. Once the underlying infrastructure is configured, a service catalog must be created, requiring additional time and investment. A service catalog can be created not only for a cloud
service provider, but can also be created to service the needs of the cloud service provider tenants as well. For a cloud service provider wishing to host regulated tenants, all of this must be done within the framework of compliance from IT security standards such as FedRAMP, PCI DSS, ISO 27001, or HIPAA. The cloud service provider must balance the infrastructure requirements, security requirements, workload requirements and compliance requirements in a cohesive way that still maintains the principles of cloud computing. Many cloud service providers have adopted the VMware vCloud Suite and VMware technology partner solutions in order to service the Federal Government and related customers with Infrastructure-as-a Service (IaaS) cloud offerings.

Prior to hosting federal systems, the cloud system must be compliant with the Federal Risk and Authorization Management Program (FedRAMP).

It is compliant when it meets the following requirements:

- The system security package has been created using the required FedRAMP templates
- The system meets the FedRAMP security control requirements
- The system has been assessed by an independent assessor
- A provisional Authorization, and/or an Agency ATO, has been granted for the system
- An authorization letter for the system is on file with the FedRAMP Program Management Office (PMO, 2014)

In order to further assist cloud service providers through the complex process and to facilitate validation decisions, VMware, and its third party assessment organization (3PAO) partner Coalfire are presenting this module “VMware Joint Validated Reference Architecture for FedRAMP 2.0.” The purpose of the FedRAMP joint reference architecture validation is to portray the provider infrastructure consisting of these components in a way that is consistent with controls set forth in FedRAMP version 2.0. It is presented to guide cloud customers and cloud service providers wishing to capitalize on the many features and benefits offered by a VMware based Software-Defined Data Center. This is the third and final document in a series of documents comprising what is known as the VMware FedRAMP reference architecture framework. This paper builds on two previously published papers, the product applicability guide and the architectural design guide.

VMware, the leader in cloud computing software for enterprises and cloud service providers alike, recognizes the tremendous opportunity that FedRAMP provides customers seeking to leverage VMware vCloud environments for hosting of federal agency IT infrastructure. The intent of this module is to demonstrate the capabilities of the VMware and certain third party technologies to adhere to and/or enable FedRAMP compliance. By turning these VMware solutions capabilities into a FedRAMP compliant delivered service, both the cloud service provider and our federal government customers can achieve a consistent experience that satisfies and exceeds mission goals and objectives. Additionally, the principles and demonstrated capabilities outlined in this guide are beneficial to all markets concerned with private, public or hybrid cloud security. As an integral part of this ongoing analysis, VMware has partnered with Intel, HyTrust and VCE for the goal of meeting FedRAMP compliance capabilities with the
greatest security, agility and costs savings possible. This guide represents a cross section of the specific capabilities that VMware and these specific partner solutions have to meet FedRAMP compliance. More information about VMware’s partner network is available on the VMware Solution Exchange. In an ongoing effort, VMware and Coalfire will utilize this information to create new “joint” reference architectures based on the VMware reference architecture for FedRAMP where technology partner products and solutions are combined and lab validated to further ease the adoption for CIOs, IT managers, architects, IT auditors and security practitioners involved with a VMware vCloud Suite based cloud computing architecture.

VMware contracted Coalfire, an independent FedRAMP 3PAO, to conduct a capability assessment of the vCloud based cloud service provider infrastructure’s FedRAMP capability. The final step in this study investigated different VMware, Intel, VCE and HyTrust solutions available to organizations that use (or are considering using) virtualization and cloud to support a FedRAMP compliant environment. VMware, VCE, HyTrust and Intel designed and built a lab to represent a cloud service provider public cloud offering. This public cloud lab was comprised of the hardware and software described in this module. Coalfire conducted an assessment of the lab to determine the combined capability of the hardware, software-defined data center, software-defined networking, and software-defined security solutions to support or enable FedRAMP control requirements. To that end, and with an eye towards building a FedRAMP-compliant environment, Coalfire has highlighted some of the specific FedRAMP requirements addressed by the applications and features discussed in this module. The controls selected in this paper are from FedRAMP security controls baseline version 2.02. It has been reviewed and authored by the staff of FedRAMP auditors in conjunction with VMware.

**CJIS Overview**

Per the Criminal Justice Information Services (CJIS) Security Policy version 5.5, “the essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of [Criminal Justice Information (CJI)], whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This policy applies to every individual contractor, private entity, noncriminal justice agency representative, or member of the criminal justice entity with access to, or who operate in support of, criminal justice services and information.” (CJIS Information Security Officer, 2016) The common framework for security of CJI as shared by participants with criminal justice services and information is useful for supporting the confidentiality, integrity, and availability of the information it serves. It provides a foundation of trust for access to CJI among various federal, state, and local agencies as well as outside supporting organizations. The readiness of this information is useful for the efficient enforcement of the law.

VMware recognizes the importance of the CJIS Security Policy and the role it plays for the protection of CJI. VMware also understands the relevance that information technology infrastructure, management, and end-user compute solutions play regarding
the security of critical digital assets. By standardizing an approach to compliance and expanding that approach to include technology partners, VMware provides its customers with a solution that may more fully address their compliance needs. This standardized approach provides management, IT architects, administrators, and security and compliance auditors more transparency into risks, solutions, and mitigation strategies for moving critical assets and data to the cloud in a secure and compliant manner in alignment with the recommendations and requirements of the CJIS Security Policy for the protection of CJI.

VMware enlisted its audit partner, Coalfire Systems, Inc. (Coalfire), to engage in a programmatic approach to assess VMware products and solutions for their capabilities to address CJIS Security Policy requirements and recommendations and to report these capabilities into a set of reference architecture documents. This is the second in a series of two documents representing Coalfire’s assessment of VMware technologies that are available to organizations that use (or are considering using) VMware Software-Defined Data Center (SDDC), Software-Defined Networking (SDN), and End-User Computing (EUC) platforms to host CJIS regulated applications and services. For this assessment, the SDDC, SDN, and EUC platforms have been designed and implemented in one of the Centers of Excellence to support testing of capabilities to address CJIS Security Policy requirements.

Coalfire has found that the assessed VMware Compliance Capable Solution, as described in this paper, provided sufficient control capabilities in support of the selected CJIS Security Policy requirements.
VMware Compliance Capable Solution for CJIS 5.5

The Center of Excellence used for this compliance capable validation exercise was a joint initiative by VMware and Intel. The hardware platform for the test lab was inclusive of Intel equipped SSDs, Network Controllers, and Intel Xeon based CPUs. The Center of Excellence follows the VMware Validated Design for Software Defined Data Center. The below graphic illustrates, at a high level, the conceptual design of the VMware Validated Design.

Layered on top of the VMware Validated Design for SDDC is VMware’s End-User Compute and Mobility Solutions, which form a comprehensive platform for end-user access to systems and data called VMware Workspace ONE. Workspace ONE includes virtual desktop infrastructure, secure data access options, identity management, and mobility management. VMware Workspace ONE provides several options for secure control enablement supporting end-user access and interaction with CJI. The Workspace ONE implementation follows VMware’s validated architecture and design criteria and best practices for practical, efficient deployment and delivery of end-user solutions.

To demonstrate functional control capability for operational workloads, VMware layered on workloads representative of multiple distinct security domains as may exist in a typical organization. In alignment with the topic of CJIS, the security domains were labeled as CJI and non-CJI. Each server workload further represented a multi-tier server architecture representing web, application, and database. Additional user access functionality was granted and made available through VMware Workspace ONE.

This section will provide a high-level summary of the architecture and design elements for the test lab made up of the VMware Validated Design for SDDC and VMware Workspace ONE. The focus in this section will be on the components that specifically relate to the aforementioned use cases. For more complete and detailed information about the VMware Validated Design for SDDC, please refer to the VMware Validated Design.
Design for SDDC documentation. For more complete and detailed information about a validated integration design for VMware Workspace ONE, please refer to the VMware Workspace ONE Reference Architecture: Validated Integration Design document.

**VMware Workspace One**

VMware NSX for vSphere can provide mechanisms to control the access to apps hosted on servers in the organization’s data center. VMware provides CJIS solutions for end-user computing to allow end users the freedom to securely access applications and data from any device from any location. The combined solution of VMware Horizon, VMware AirWatch, and VMware Identity Manager into a package called VMware Workspace ONE gives organizations greater control over the end-user experience without sacrificing the flexibility and agility that end users come to expect in the execution of their jobs.

Workspace ONE used in the environment to secure end-user access capabilities with respect to providing end-users, both remote and local, on end-user devices, PC, Mac and mobile devices and tablets, access to CJIS.
Workspace ONE provides secure delivery of access to information and applications that may be provided by the agency as a privately hosted SaaS application, cloud hosted application, or native mobile application. Delivery of applications includes client server applications that can be delivered for the use of end users using Horizon Apps or made available on Horizon Desktops.
The next graphic shows the flow of access from managed end user devices for access to Workspace ONE delivered applications, data repositories and virtual desktops. There are many options to deliver applications and data to end users. These options can vary by business use case or security requirement and can be adjustable based on specific scenarios or criteria applied to managed devices and end users. Relevant criteria can include geographic location of the accessing device, source IP address, logical location, security of the internet connection utilized by the accessing device and so forth.

After performing an analysis of VMware’s End User Compute and Mobility Solutions (VMware Workspace ONE, the configured VMware Validated Design for SDDC, the use cases layering of organizational workloads, and configurations specific to CJIS Security Policy requirements), Coalfire validated that the evaluated technical security control capabilities were addressed or addressable in a manner that supports and conforms to CJIS Security Policy requirements. Again, this module is specific to the End User Computing requirements of this testing.

Conclusion

This lesson provided information on Government compliance specifically within the End User Computing space.
It is without question that the transformation of business to the digital world represents exciting opportunities for industries around the world. As technology advances, new possibilities arise for how business is done. In support of these advances, VMware introduced the concept of “One Cloud, Any Application, Any Device”. Rapid change and advancements in technology bring new risk and this risk must be evaluated to determine the impact that it has on critical data. VMware has shown its commitment to security through innovations in network security and systems management. The security and control capabilities that VMware technologies enable support the flexible architecture and structure of the ever changing landscape of information technology. It is Coalfire’s opinion that the VMware software-defined data center (SDDC) and end-user computing (EUC) solutions discussed in this white paper could be used in a payment entity infrastructure and could be configured to address and/or support many of the FedRAMP and CJIS requirements.
Finance Compliance

As part of the VMware Compliance Reference Architecture Framework, VMware is addressing the issues of compliance and cybersecurity for the Payment Card Industry Data Security Standard (PCI DSS).

This is applicable to all types of environments that store, process, or transmit card holder data. This includes information such as Personal Account Numbers (PAN), as well as any other information that has been defined as Card Holder Data by the PCI DSS.

Cloud computing is no exception to the PCI DSS audit process, and many of the Cloud’s advantages over earlier paradigms -- sharing of resources, workload mobility, consolidated management plane, etc. -- themselves necessitate that adequate controls are adopted to help meet the PCI DSS audit.

PCI considerations are essential for assessors to help to understand what they might need to know about an environment in order to be able to determine whether a PCI DSS requirement has been met. If payment card data is stored, processed or transmitted in a cloud environment, PCI DSS will apply to that environment, and will typically involve validation of both the infrastructure and the applications running in that environment.

Many enterprise computing environments in various vertical industries are subject to PCI DSS compliance, and generally those that deal in any kind of financial transaction for exchanging goods and services rely on VMware and VMware Technology Partner solutions to deliver those enterprise computing environments. As such, these enterprises seek ways to reduce overall IT budget while maintaining an appropriate overall risk posture for the in-scope environment. One of the greatest challenges in hosting the next generation enterprise computing environment is consolidating many modes of trust required such as those required for a Cardholder Data Environment (CDE) and a Non-Cardholder Data Environment.

This module will explain how VMware meets PCI DSS Requirements within a Cloud Computing Environment” by providing helpful information to VMware architects, the PCI DSS community, business stakeholders and third parties.

VMware is addressing these challenges by establishing a Reference Architecture Framework (RAF) that provides a consistent way for VMware, its partners, and organizations to assess and evaluate the impact of PCI standards, regulations and best practices on virtual and cloud environments. The intent of the RAF is to provide a single framework for VMware, its partners, and organizations to address a variety of compliance and cyber security requirements across an IT infrastructure.

**Highlights**

- Security and Compliance Thought Leadership
- VMware and Partner Product Applicability
Independently Audited and Validated Guidance

Overview

Per the Payment Card Industry Security Standards Council (PCI SSC), “The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally.” (PCI SSC, 2016) The Payment Card Industry Data Security Standard version 3.2 (PCI DSS v3.2) is a proprietary information security standard that was created to reduce credit card fraud by stipulating a series of controls regulating the use of information systems that handle cardholder data (CHD) and sensitive authentication data (SAD). PCI DSS is not an optional standard. As stated, all entities who process, store, or transmit CHD and/or SAD must comply with the standard or they can be fined or refused access to the card brand’s payment system.

VMware recognizes the importance of PCI DSS and understands that the following critical areas must be addressed by each entity (merchants, processors, acquirers, issuers, and service providers) involved in payment card processing: security and compliance, the criticality and vulnerability of the assets needed to manage infrastructures impacting payment card processing, and the risks to which those assets are exposed. By standardizing an approach to compliance and expanding that approach to include technology partners, VMware provides its customers with a proven solution that more fully addresses their compliance needs. This approach provides management, IT architects, administrators, and assessors with a high degree of transparency into risks, solutions, and mitigation strategies for moving critical applications and data to the cloud in a secure and compliant manner in alignment with the recommendations and requirements of PCI DSS in order to protect CHD.

VMware enlisted its assessor partner, Coalfire Systems, Inc. (Coalfire), a QSA company, to engage in a programmatic approach to assess VMware products and solutions for their capabilities to address PCI DSS recommendations and requirements and to document these capabilities as a set of reference architecture documents. This is the second in a series of documents representing Coalfire’s assessment of the different VMware technologies available to organizations that use (or are considering using) VMware Software-Defined Data Center (SDDC), Software Defined Networking (SDN), and End User Computing (EUC) platforms to host PCI SSC regulated information. For this assessment, the SDDC and SDN platforms have been designed and implemented in one of the VMware Centers of Excellence to support demonstration and testing of capabilities to address PCI DSS requirements. The implementation follows a VMware Validated Design approach inclusive of best practices for practical deployment of VMware technologies in real-world installations. Coalfire highlights specific PCI DSS requirements and recommendations that these technologies address and/or support and has applied a testing methodology to validate VMware’s claims of compliance capability in this Compliance Capable Solutions document.
It is Coalfire’s opinion that the assessed VMware Compliance Capable Solution provided sufficient control capabilities in support of the selected PCI DSS requirements and recommendations.

**VMware Compliance Reference Architecture Framework**

The VMware Compliance Reference Architecture framework provides a programmatic approach to mapping VMware and partner products to regulatory controls from an independent auditor’s perspective. The result is valuable guidance that incorporates best practices, design, configuration, and deployment with independent auditor oversight and validation.

VMware, in the below graphic illustrates measures of capability with respect to security, confidentiality, and integrity that make up a trusted cloud implementation. This graphic illustrates the specific solution categories that can be addressed with VMware solutions and VMware’s extensive partner ecosystem. Those areas highlighted in **red** outline the components as they relate to the Horizon and Mobility components VMware develops.
By addressing and implementing the security solutions within the framework of the regulated infrastructure, many of the technical control requirements for any particular regulation are addressed. By integrating these security solution components together in a cohesive manner, the outcome is a compliance-capable platform upon which the covered entity or business associate can overlay its business systems and data.
VMware Workspace One

VMware end-user computing products allow IT organizations to pro-actively deliver consistent and intuitive services to their customers. Driven by the demands of users for immediate access to applications and data from any device at any time and from any location, services can be orchestrated to meet these demands without sacrificing security and compliance requirements. As a result, the user is able to work more efficiently in a manner that best suits his or her needs, while IT is able to manage that experience for confidentiality, integrity, and availability. VMware Workspace ONE combines end-user computing technologies such as VMware Horizon and AirWatch to unify the end-user experience for secure access to applications and content from laptops, desktops, zero or thin-clients, and mobile devices and tablets. This allows IT to deliver the digital workspace as a service, much like catalogs of infrastructure services can be delivered with the software-defined data center.

VMware Workspace ONE includes a unified app store for delivering a catalog of organization-approved applications. This unified app store provides controlled access to a variety of types of applications including mobile apps, client-server apps, web apps, web sites, and more. The apps are accessible through a catalog and is the central hub for end-user application delivery.

Workspace ONE also includes a single sign-on (SSO) capability, which allows for integrating with basic Active Directory Federation Services’ SSO, SSO with Custom Policies, Device Trust Authentication, Touch ID on iOS, and device-specific authentication provider integration as well as multi-factor authentication.

VMware Horizon 7 Enterprise Edition

- vCenter Server
- Horizon 7 Securely deliver virtualized desktops and published applications to end users across devices and locations through a single platform.
- Horizon for Linux Deliver, manage and access Linux virtual desktops.
• **Horizon FLEX** Give employees and contractors virtual desktops on Macs or PCs that they can use without a network connection with central control and strong security applied.

• vRealize Orchestrator + Desktop Plugin

• vRealize Automation for Horizon

• vRealize Operations for Horizon

• **User Environment Manager** Offers personalization and dynamic policy configuration across any virtual, physical, and cloud-based Windows desktop environment.

• **App Volumes** Deliver applications to desktop environments in seconds. With the click of a button, IT can provision applications to users and desktops at scale.

• VMware NSX for vSphere Horizon Edition

• **VMware Identity Manager (vIDM)** Identity as a Service (IDaaS) offering, providing application provisioning, self-service catalog, conditional access controls, and single sign-on (SSO) for SaaS, web, cloud, and native mobile applications. Identity Manager delivers on consumer-grade expectations like one-touch access to apps. This delivery of applications can be optimized with AirWatch Conditional Access and backed by a self-service catalog with enterprise-class management and security.

---

**VMware AirWatch Enterprise Mobility Manager**

VMware AirWatch is a scalable enterprise mobility management platform that integrates with existing enterprise systems and allows you to manage almost all devices, regardless of type, platform, or ownership, from one central console. Included with AirWatch Enterprise Mobility Manager are the tools necessary to allow end users, regardless of their device, to securely interact with PCI DSS 3.2 compliant workloads. The ability for administrators to manage and control the device helps to ensure the integrity of the device and security of the data that these devices are accessing.

• **VMware AirWatch Container Management** provides complete separation of corporate and personal data on mobile devices, securing corporate resources and maintaining employee privacy. AirWatch Container Management enables standardization of enterprise security and data loss prevention strategies across mobile devices. Corporate containers keep corporate applications and data separate from personal applications and data on mobile devices.

• **VMware AirWatch Mobile Device Management (MDM)** this is the foundation of a comprehensive Enterprise Mobility Management (EMM) platform. AirWatch MDM provides a simplified, efficient way to view and manage a diverse fleet of devices from a central admin console. AirWatch MDM enables enrollment of mobile devices in your enterprise environment quickly, configuring and updating device settings over-the-air, and securing mobile devices without hindering the user experience.

• **VMware AirWatch Mobile Applications Management** enables the concept of any application to any device. AirWatch Mobile Applications Management provides the framework to help the agency support the complete app lifecycle.
Beyond static app distribution, IT is able to source or develop apps, apply security policies, and deploy an app catalog, as well as analyze app metrics.

- **VMware AirWatch Content Locker** enables secure mobile access to content anytime, anywhere. AirWatch Content Locker protects your sensitive content in a corporate container and provides users with a central application to securely access, store, update, and distribute the latest documents from their mobile devices.

- **VMware AirWatch Mobile Email Management (VMware Boxer)** a mobile email solution that helps keep corporate data secure and compliant. VMware Boxer delivers fast email sync and an intuitive user experience with secure mobile access to corporate-owned and BYO devices while respecting user privacy.

- **VMware AirWatch Mobile Browsing Management** enables secure web browsing and provides organizations with the ability to configure customized settings to meet their unique business and end-user needs. AirWatch Mobile Browsing Management allows administrators to design and enforce secure browsing policies from a central admin console. It is pre-configured to use app tunneling through the AirWatch Mobile Access Gateway to proxy access to internal resources in the agency’s LAN. This is a secure point of entry for all compliant devices to access enterprise services.

![Diagram of VMware SDDC and EUC solutions](image-url)

**Overall Design**

The overall design of the VMware SDDC and **EUC** solutions has been considered for multiple purposes. Foremost, the design must support the function of the business. Secondly, the design must minimally meet security requirements for the impacted security framework. When deciding technologies to include in the design, these factors were considered.

**EUC** and mobility components were chosen for their ability to securely support end-user access to data and applications in a secure and controlled manner.
Software-defined data center components were chosen for the ability to achieve scalability and agility for the infrastructure.

Software-defined networking (not covered in this module), a component of the SDDC, was included due to the ability to provide secure networking capability to both the infrastructure and the end-user computing environments and the ability to segment workloads.

The VMware Validated Design for SDDC has been utilized to take advantage of a rigorously tested and consistently reproducible architecture that provides additional operational benefits for customers.

VMware has chosen to use a platform that includes Intel Trusted Execution Technology (Intel TXT) and Intel Advanced Encryption Standard New Instructions (Intel AES-NI) to form a strong hardware foundation for the software-defined data center.

The overall design is cohesive, comprehensive, and capable of being further enhanced by VMware partner solutions.

**Conclusion**

This lesson provided information on Finance compliance specifically within the End User Computing space.

It is without question that the transformation of business to the digital world represents exciting opportunities for industries around the world. As technology advances, new possibilities arise for how business is done. In support of these advances, VMware introduced the concept of “One Cloud, Any Application, Any Device”. Rapid change and advancements in technology bring new risk and this risk must be evaluated to determine the impact that it has on critical data. VMware has shown its commitment to security through innovations in network security and systems management. The security and control capabilities that VMware technologies enable support the flexible architecture and structure of the ever changing landscape of information technology. It is Coalfire’s opinion that the VMware software-defined data center (SDDC) and end-user computing (EUC) solutions discussed in this white paper could be used in a payment entity infrastructure and could be configured to address and/or support many of the PCI DSS recommendations and requirements.
Energy Compliance

VMware enlisted its audit partner, Coalfire Systems, to engage in a programmatic approach to evaluate VMware products and solutions for North American Electric Reliability Corporation Critical Infrastructure Protection, Version 5 (NERC CIP v5, or more simply CIP) (NERC, 2016) cybersecurity standards capabilities and document these capabilities into a set of reference architecture documents. The result is this Product Applicability Guide for NERC CIP v5.0.

VMware provides its customers a proven solution that more fully addresses their compliance needs. This approach provides management, IT architects, administrators, and auditors a high degree of transparency into risks, solutions, and mitigation strategies for moving critical applications to the cloud in a secure and compliant manner. This is especially important when the consequences of noncompliance can be extremely critical due to the penalties imposed by the Federal Energy Regulating Commission (FERC) and accompanying Canadian governmental regulating agencies.

FERC has mandated a single point of contact entity, specifically the North American Electric Reliability Corporation (NERC) as the international regulatory authority to monitor, educate, train, and certify organization participating in the “grid.” This single entity has additional responsibility to evolve and manage the Reliability Risk program by standards development and oversight – including investigation of operational status, impact of outage and events, and the capacity to levy fines on “grid” participants for outages, breaches of the FERC approved standards and other compliance-related events. Further, the aim of the NERC Risk Management program is to avoid or prevent additional impacts from litigation, recompense and/or negative public relations.

This module will explain how VMware meets NERC CIP Requirements within a Cloud Computing Environment” by providing helpful information to VMware architects, the NERC CIP community, business stakeholders and third parties.

Highlights

• Regulation specific guidance
• Independently validated compatibility and guidance
• Compliance and Cyber Risk thought leadership

Overview

VMware recognizes that security and compliance are critical areas that must be addressed by each covered entity in the operation of Bulk Electric Systems (BES) production, monitoring and distribution infrastructure, the criticality and vulnerability of the assets needed to manage BES impacting infrastructures, and the risks to which they are exposed. By standardizing an approach to compliance and expanding the approach
to include partners, VMware provides its customers a proven solution that more fully addresses their compliance needs. This approach provides management, IT architects, administrators, and auditors a high degree of transparency into risks, solutions, and mitigation strategies for moving critical applications to the cloud in a secure and compliant manner. This is especially important when the consequences of noncompliance can be extremely critical due to the penalties imposed by the Federal Energy Regulating Commission (FERC) and accompanying Canadian governmental regulating agencies; not to mention, there is a high probability for collateral impact due to failure to protect the North American Power “grid” privacy, institutional trust and economics. FERC has mandated a single point of contact entity, specifically the North American Electric Reliability Corporation (NERC) as the international regulatory authority to monitor, educate, train, and certify organization participating in the “grid.” This single entity has additional responsibility to evolve and manage the Reliability Risk program by standards development and oversight including investigation of operational status, impact of outage and events, and the capacity to levy fines on “grid” participants for outages, breaches of the FERC approved standards and other compliance-related events. Further, the aim of the NERC Risk Management program is to avoid or prevent additional impacts from litigation, recompense and/or negative public relations.
For these reasons, VMware enlisted its audit partner, Coalfire Systems, to engage in a programmatic approach to evaluate VMware products and solutions for North American Electric Reliability Corporation Critical Infrastructure Protection, Version 5 (NERC CIP v5, or more simply CIP) (NERC, 2016) cybersecurity standards capabilities and document these capabilities into a set of reference architecture documents. This document presents Coalfire’s assessment of different VMware applications available to organizations that use (or are considering using) software-defined data center (SDDC) environments to host or access NERC CIP critical cyber assets. Specifically, this document focuses on the VMware SDDC solutions available, and points out where additional, non-VMware vendor solutions may be required. The SDDC is defined as an architecture which brings together best-in-class compute, storage, networking virtualization and management offerings. Coalfire highlights the specific NERC CIP Version 5 standards that these applications address and/or support. These applications can be considered in evaluation of the initial sourcing or a systems refresh of technologies to build a NERC CIP v5 compliant environment.
VMware Scope and Approach

As the not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system in North America, NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system; and, educates, trains and certifies industry personnel. NERC is the private sector regulatory authority which, under the oversight of the United States Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada,
is chartered to direct, measure, mandate and regulate the cyber security systems used by users, owners and operators of the bulk power system for more than 334 million people in North America.

The scope of NERC oversight is vast, it includes Cyber Information Technology assets (cyber systems) that reside at a variety of North American Bulk Electric System (BES) contributors, as well as the physical, manpower, governance, economic and logistical components that are used to provide North American electrical power. NERC acts as a single point of contact for the relationship between FERC and the BES providers, and operates bi-directionally with stakeholders from both communities.

Due to the NERC CIP v5’s broad coverage of subjects relative to the Responsible Entity, it is necessary to identify the subjects that are relevant to the combined subject matter of this product applicability guide. The primary subjects include the NERC Critical Infrastructure Protection topics and the VMware software-defined data center (SDDC) platform and solutions.

This Product Applicability Guide (PAG) is focused on the VMware software-defined data center (SDDC), which is presented and described in the Creating a VMware Software-Defined Data Center Reference Architecture Version 1.5 (VMware, Inc., 2014) document. This technical white paper was created to convey details of the logical architecture and reflect nuances of the physical implementation.

**NERC CIP v5 Scope**

NERC CIP v5 is a body of ten standards that address Critical Cyber Infrastructure technologies, policies and procedures in a way that promotes (while not guaranteeing) a sound approach to risk avoidance for the Bulk Electric Systems providers to the North American power “grid.” While not specifically mandating a particular risk avoidance framework or underlying specific standard, much of NERC CIP is compatible with the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations (see NIST Special Publication 800-53 Revision 4) initiatives and philosophy.

The prescriptive methods present in other regulations, such as the Payment Card Industry Data Security Standard (PCI DSS), where specific guidance is provided on “how to secure”, are absent from the requirements section of CIP standards. Instead, the NERC CIP standards contain a section on Requirements and Measures, where specific outcome-based “shall” directives are stated and means to evaluate compliance with the “shall” directives are enumerated. The NERC CIP standards also contain a section titled Guidelines and Technical Basis which provides additional insights on how the “shall” directives may be arrived at. This additional information augments the requirements and measurement sections with insight that can direct the IT and InfoSec architects to concrete outcomes. The Guidelines... sections of each standard often provide similar details to what PCI DSS requirements specifically direct.
Coalfire has elected to put emphasis on both the Requirements and Measures and Guidelines and Technical Basis sections of the specific NERC CIP v5 standards, and to use these sections in combination to define what we will refer to hereafter as “requirements” or “controls” for the purposes of this Product Applicability Guide (PAG). Also, please be advised, this is our interpretation and not necessarily followed by all members of the audit community. We do not aim to mislead with this interpretation, but instead to seek to use the terms “control” and “requirement” in closer alignment with how they are meant in the Information Security community, without specific bias of NERC CIP regulatory meaning. From this point forward in this Product Applicability Guide, we will use “control” and “requirement” to mean the general InfoSec term, and the capitalized “Requirement(s)” to mean specifically a NERC CIP Requirement, per se. Similarly, we will use “Guideline(s)” and “Technical Basis (Bases)” to reflect NERC CIP elements from the Guidelines and Technical Basis section of the standards.

Sourcing the entire policy framework, we start with identification of North American Electric Reliability Corporation Critical Infrastructure Protection, Version 5 (NERC CIP v5) topics that are applicable to information technology that make up common infrastructure used for the storage, processing, transmission and destruction of electronic data.

We show an overview of the NERC CIP v5 Cyber Security Standards CIP-002 through CIP-011 which is in the following section. NERC CIP is a composite of technical requirements, which may be mapped against VMware SDDC and Partner technologies; and, a suite of policy requirements, which have no VMware SDDC direct requirement mapping, as they pertain to programs, personnel, procedures and policies.

Each CIP has a Section (B.) pertaining to Requirements and Measures, where the clear “shall” statements of what is required and how it may be evaluated for appropriate evidence is prescribed. CIP also contains Section (C.) which defines the Compliance Monitoring Process, and stating who enforces compliance, how evidence is retained, monitored and assessed. In Section C., tables enumerate the Violation Severity Levels (VSLs) on a per-requirement basis, which shows inadequate action to satisfy the requirement, and a ranking of the VSL as Lower, Moderate, High and Severe. The final two sections of each CIP are Guidelines and Technical Basis and Rationale where more detail and reasoning is provided to guide the responsible party with additional supporting information to make their tasks clear.

Our approach to interpreting these standards is based on an understanding the technical requirement policies, which are specifically restricted to CIP-005, CIP-007, CIP-009, CIP-010 and CIP-011, and focus on Electronic Security Perimeter(s), Systems Security Management, Recovery Plans for BES Cyber Systems, Configuration Change Management and Vulnerability and Information Protection, respectively. Where the Guidelines and Technical Basis section of a standard directs the responsible party toward NIST 800-53 and other guidance, we are interpreting the VMware and partner technical solutions in light of the requirement following that guidance. Where no such guidance is suggested, we will provide specific details of our cyber security “best practices,” as observed in a multitude of customer scenarios that we believe apply.
Unlike HIPAA/Hytrust, FedRAMP and other regulations, NERC standards committees and the FERC subject to enforcement regulation has been devoid of the strong hand of NIST.

In general, the following figure illustrates a regulation-agnostic approach to compliance, which we feel is an excellent overview of the relationship of the Authoritative Source through Audit business process and potential compliance outcome:

This compliance approach applies to the software-defined data center and end-user computing stack of VMware technologies which are integrated to formulate a total solution for the NERC CIP Responsible Entity. The comprehensive layering of these technologies is represented here:
Conclusion

Although the BES providers are focused on a more specific mission than most other regulatory required businesses (e.g. HIPAA for Healthcare, PCI-DSS for payment card merchants, etc.) they will still receive substantial benefits from the use of virtualized technologies from VMware. The VMware SDDC products have revolutionized cost and reliability in those other market segments; and, as NERC CIP regulated responsible BES entities move towards a more technologically sophisticated Cyber infrastructure with the onset of “Smart Grid” initiatives in the near future, those same advantages of velocity, flexibility and significantly reduced DevOps costs may be securely used by BES providers. Based on the “through the eyes of the auditor” review by Coalfire Systems, Inc., this product applicability guide identified ways in which VMware’s software-defined data center and end-user computing platforms help to govern risk and support a responsible participation in ongoing and continuing innovation.
Module Conclusion

You have completed the Governance and Compliance module of this lab. The VMware CCRS Reference Architecture Framework and Secure and Compliance Capable Platform can help an organization meet and maintain regulatory and policy requirements by providing a method to link integrated software and hardware features to specific regulatory controls with independent audit validation. Each VMware CCRS Reference Architecture Framework includes design, configuration and deployment guidance and best practices selected to help you maximize the use of your hardware and software while meeting compliance requirements and managing cyber risk. Design and operation of environments based on a VMware CCRS Reference Architecture Framework will enable effective use of reliable virtualization and cloud technologies that are validated to work together to provide breakthrough speed, efficiency and agility while securing data in the cloud.

You've finished Module 5

Congratulations on completing Module 5.

If you are looking for additional information on Horizon 7, try one of these:

- Click on this [HOL-1851-09-ADV](HOL-1851-09-ADV)
- Or use your smart device to scan the above QRC Code.

Proceed to any module below which interests you most.

- **Module 1 - Security Considerations** (15 minutes) (Basic) This module will explore various use cases and security considerations of Horizon 7. It is the intent of this lab to provide concise references to some of the security features and technologies supported for Horizon 7. (Informational Module)
• **Module 2 - VMware Unified Access Gateway** (30 minutes) (Advanced) Within this section of the lab it will be shown how using VMware Unified Access Gateway will secure remote access to VMware end-user computing resources.

• **Module 3 - SSL Certificates** (30 minutes) (Intermediate) This module will demonstrate securing various VMware Horizon server components with SSL certificates.

• **Module 4 - True SSO** (30 minutes) (Intermediate) This module will review and demonstrate configuring True SSO (single sign-on) features in Horizon 7 while securing and adhering to Microsoft Windows (AD) Domain rights and authentication privileges.

• **Module 5 - Governance and Compliancy** (30 minutes) (Basic) VMware governance and compliancy delivers the ability for customers to confidently and quickly secure mission critical virtualized workloads throughout many critical industries. This portion of the lab will provide guidance and information on these topics to assure compliance against many regulation requirements throughout various, unique industries. (Informational Module)

• **Module 6 - Multifactor Authentication** (30 minutes) (Intermediate) This module will provide information supporting multifactor authentication with Horizon 7 to include SmartCard, RSA, RADIUS technologies.

• **Module 7 - NSX for Horizon** (60 minutes) (Advanced) This module will demonstrate how VMware End User Computing and NSX Security solutions can provide a customized desktop experience, doing so while maximizing operational efficiencies and security leveraging pure stateless VDI.

---

**How to End Lab**

To end your lab click on the **END** button.
Module 6 - Multifactor Authentication (30 minutes)
Introduction & Overview

Multi-Factor or Two-Factor Authentication is a very secure way to protect your online accounts. It works by requiring you to identify yourself using two different things when you log-in to a site. The second factor is tied to something 'you have' (like a cellphone). So you can think of two-factor as something you know (your password) + something you have (your cellphone).

This Module contains the following lessons:

- **Horizon 7 Multi-Factor Features** - Overview of multi-factor features available with Horizon 7
- **VMware Identity Manager Multi-Factor Features** - Overview of multi-factor features available within VMware Identity Manager
- **Multi-Factor Demonstration and Walkthrough with VMware Identity Manager** - Walk through and Demonstration of VMware Identity Manager using Radius services
Horizon 7 Multi-Factor Features

Within this lesson you will review the technologies and capabilities built into VMware Horizon that protect devices. It is only the intent to describe features available to the Horizon Suite to secure the end user environment.

We will review Multi-Factor authentication methods for the Connection and Security Servers and the Unified Access Gateway.

Overview

VMware Horizon View enables you to access a virtual desktop from anywhere at anytime. Horizon offers you the possibility to move from one place to another: to work from your office, from a cybercafé, or from any other place, when you have a network connection that lets you connect to the Horizon View infrastructure.

Challenges occur when connecting externally, how to protect and secure? How to authorize only some users or groups of users to connect from an external network or Internet?

A method to use is multi-factor\2-Factor authentication. This lesson will describe the methods that Horizon 7 supports for multi-factor authentication and the associated technologies that enable these authentication methods.

This is informational only, a demonstration of multi-factor can be seen in the demo portion for RSA authentication in this module.

Connection\Security Server Multi-Factor

You can configure a View Connection\Security Server instance so that users are required to use multi-factor authentication.

Multi-Factor Authentication methods supported are:

- RADIUS
- RSA SecureID
- Certificate\SmartCard\PIV
- Biometrics

RADIUS support offers a wide range of alternative two-factor token-based authentication options.

View also provides an open standard extension interface to allow third-party solution providers to integrate advanced authentication extensions into View.
Because two-factor authentication solutions such as RSA SecurID and RADIUS work with authentication managers, installed on separate servers, you must have those servers configured and accessible to the View Connection Server host. For example, if you use RSA SecurID, the authentication manager would be RSA Authentication Manager. If you have RADIUS, the authentication manager would be a RADIUS server.

To use two-factor authentication, each user must have a token, such as an RSA SecurID token, that is registered with its authentication manager. A two-factor authentication token is a piece of hardware or software that generates an authentication code at fixed intervals. Often authentication requires knowledge of both a PIN and an authentication code.

If you have multiple View Connection Server instances, you can configure two-factor authentication on some instances and a different user authentication method on others. For example, you can configure two-factor authentication only for users who access remote desktops and applications from outside the corporate network, over the Internet.
View is certified through the RSA SecurID Ready program and supports the full range of SecurID capabilities, including New PIN Mode, Next Token Code Mode, RSA Authentication Manager, and load balancing.
Logging in with Multi-Factor

When a user connects to a View Connection Server instance that has multi-factor authentication enabled, a special login dialog box appears in Horizon Client.

Users enter their RSA SecurID or RADIUS authentication user name and passcode into a special login dialog box. A two-factor authentication passcode typically consists of a PIN followed by a token code.

If RSA Authentication Manager requires users to enter a new RSA SecurID PIN after entering their RSA SecurID username and passcode, a PIN dialog box appears. After setting a new PIN, users are prompted to wait for the next token code before logging in. If RSA Authentication Manager is configured to use system-generated PINs, a dialog box appears to confirm the PIN.

When logging in to View, RADIUS authentication works much like RSA SecurID. If the RADIUS server issues an access challenge, Horizon Client displays a dialog box similar to the RSA SecurID prompt for the next token code. Currently support for RADIUS challenges is limited to prompting for text input. Any challenge text sent from the RADIUS server is not displayed. More complex forms of challenge, such as multiple choice and image selection, are currently not supported.

After a user enters credentials in Horizon Client, the RADIUS server can send an SMS text message or email, or text using some other out-of-band mechanism, to the user's cell phone with a code. The user can enter this text and code into Horizon Client to complete the authentication.

Because some RADIUS vendors provide the ability to import users from Active Directory, end users might first be prompted to supply Active Directory credentials before being prompted for a RADIUS authentication user name and passcode.

Enable Multi-Factor Authentication

You enable a View Connection Server instance for RSA SecurID authentication or RADIUS authentication by modifying View Connection Server settings in View Administrator.

Prerequisites

Install and configure the two-factor authentication software, such as the RSA SecurID software or the RADIUS software, on an authentication manager server.

- For RSA SecurID authentication, export the sdconf.rec file for the View Connection Server instance from RSA Authentication Manager. See the RSA Authentication Manager documentation.
- For RADIUS authentication, follow the vendor's configuration documentation. Make a note of the RADIUS server's host name or IP address, the port number on which it is listening for RADIUS authentication (usually 1812), the authentication
type (PAP, CHAP, MS-CHAPv1, or MS-CHAPv2) and the shared secret. You will enter these values in View Administrator. You can enter values for a primary and a secondary RADIUS authenticator.

Procedure (Informational only)

1. In View Administrator, select View Configuration > Servers.
2. On the Connection Servers tab, select the server and click Edit.
3. On the Authentication tab, from the 2-factor authentication drop-down list in the Advanced Authentication section, select RSA SecureID or RADIUS.
4. To force RSA SecurID or RADIUS user names to match user names in Active Directory, select Enforce SecurID and Windows user name matching or Enforce 2-factor and Windows user name matching.
   - If you select this option, users must use the same RSA SecurID or RADIUS user name for Active Directory authentication. If you do not select this option, the names can be different.
5. For RSA SecurID, click Upload File, type the location of the sdconf.rec file, or click Browse to search for the file.
6. For RADIUS authentication, complete the rest of the fields:
   - Select Use the same username and password for RADIUS and Windows authentication if the initial RADIUS authentication uses Windows authentication that triggers an out-of-band transmission of a token code, and this token code is used as part of a RADIUS challenge.
     - If you select this check box, users will not be prompted for Windows credentials after RADIUS authentication if the RADIUS authentication uses the Windows username and password. Users do not have to reenter the Windows username and password after RADIUS authentication. From the Authenticator drop-down list, select Create New Authenticator and complete the page.
   - Set Accounting port to 0 unless you want to enable RADIUS accounting. Set this port to a non-zero number only if your RADIUS server supports collecting accounting data. If the RADIUS server does not support accounting messages and you set this port to a nonzero number, the messages will be sent and ignored and retried a number of times, resulting in a delay in authentication.
     - Accounting data can be used in order to bill users based on usage time and data. Accounting data can also be used for statistical purposes and for general network monitoring. If you specify a realm prefix string, the string is placed at the beginning of the username when it is sent to the RADIUS server. For example, if the username entered in Horizon Client is jdoe and the realm prefix DOMAIN-A\ is specified, the username DOMAIN-A\jdoe is sent to the RADIUS server. Similarly, if you use the realm suffix, or postfix, string @mycorp.com, the username jdoe@mycorp.com is sent to the RADIUS server.
7. Click **OK** to save your changes.

You do not need to restart the View Connection Server service. The necessary configuration files are distributed automatically and the configuration settings take effect immediately.

When users open Horizon Client and authenticate to View Connection Server, they are prompted for two-factor authentication. For RADIUS authentication, the login dialog box displays text prompts that contain the token label you specified.

Changes to RADIUS authentication settings affect remote desktop and application sessions that are started after the configuration is changed. Current sessions are not affected by changes to RADIUS authentication settings.

**Unified Access Gateway Multi-Factor**

Unified Access Gateway is an appliance that is normally installed in a demilitarized zone (DMZ). Unified Access Gateway is used to ensure that the only traffic entering the corporate data center is traffic on behalf of a strongly authenticated remote user. Unified Access Gateway directs authentication requests to the appropriate server and discards any unauthenticated request. Users can access only the resources that they are authorized to access. Unified Access Gateway also ensure that the traffic for an authenticated user can be directed only to desktop and application resources to which the user is actually entitled. This level of protection involves specific inspection of desktop protocols and coordination of potentially rapid changing policies and network addresses, to accurately control access. Unified Access Gateway acts as a proxy host for connections inside your company's trusted network. This design provides an extra layer of security by shielding virtual desktops, application hosts, and servers from the public-facing Internet. Unified Access Gateway is designed specifically for the DMZ.

The following hardening settings are implemented:

- Up-to-date Linux Kernel and software patches
- Multiple NIC support for Internet and intranet traffic
- Disabled SSH
- Disabled FTP, Telnet, Rlogin, or Rsh services
- Disabled unwanted services

When you initially deploy Unified Access Gateway, Active Directory password authentication is set up as the default. Users enter their Active Directory user name and password and these credentials are sent through to a back-end system for authentication.

You can configure the Unified Access Gateway service to perform Certificate/Smart Card authentication, RSA SecurID authentication, RADIUS authentication, and RSA Adaptive Authentication.
Configuring Certificate or Smart Card Authentication on the Unified Access Gateway Appliance

You can configure x509 certificate authentication in Unified Access Gateway to allow clients to authenticate with certificates on their desktop or mobile devices or to use a smart card adapter for authentication.

Certificate-based authentication is based on what the user has (the private key or smart card), and what the person knows (the password to the private key or the smart card PIN). Smart card authentication provides two-factor authentication by verifying both what the person has (the smart card) and what the person knows (the PIN). End users can use smart cards for logging in to a remote View desktop operating system and to access smart-card enabled applications, such as an email application that uses the certificate for signing emails to prove the identity of the sender.

With this feature, smart card certificate authentication is performed against the Unified Access Gateway service. Unified Access Gateway uses a SAML assertion to communicate information about the end user's X.509 certificate and the smart card PIN to the Horizon server.

You can configure certificate revocation checking to prevent users who have their user certificates revoked from authenticating. Certificates are often revoked when a user leaves an organization, loses a smart card, or moves from one department to another. Certificate revocation checking with certificate revocation lists (CRLs) and with the Online Certificate Status Protocol (OCSP) is supported. A CRL is a list of revoked certificates published by the CA that issued the certificates. OCSP is a certificate validation protocol that is used to get the revocation status of a certificate.

You can configure both CRL and OCSP in the same certificate authentication adapter configuration. When you configure both types of certificate revocation checking and the Use CRL in case of OCSP failure check box is enabled, OCSP is checked first and if OCSP fails, revocation checking falls back to CRL. Revocation checking does not fall back to OCSP if CRL fails.

You can also set up authentication so that Unified Access Gateway requires smart card authentication but then authentication is also passed through to the server, which might require Active Directory authentication.

For full install instructions please refer to the following link for the deployment guide:

https://www.vmware.com/support/pubs/access-point-pubs.html

Configuring RSA and RSA Adaptive Authentication

RSA
After the Unified Access Gateway appliance is configured as the authentication agent in the RSA SecurID server, you must add the RSA SecurID configuration information to the Unified Access Gateway appliance.

**Prerequisites**

- Verify that RSA Authentication Manager (the RSA SecurID server) is installed and properly configured.
- Download the compressed sdconf.rec file from the RSA SecurID server and extract the server configuration file.

**Procedure**

1. In the admin UI Configure Manually section, click **Select**.
2. In the General Settings Authentication Settings section, click **Show**.
3. Click the gearbox in the RSA SecurID line.
4. Configure the RSA SecurID page.

Information used and files generated on the RSA SecurID server are required when you configure the SecurID

**RSA Adaptive Authentication**

RSA Adaptive Authentication can be implemented to provide a stronger multi-factor authentication than only user name and password authentication against Active Directory. Adaptive Authentication monitors and authenticates user login attempts based on risk levels and policies.

When Adaptive Authentication is enabled, the risk indicators specified in the risk policies set up in the RSA Policy Management application and the Unified Access Gateway configuration of adaptive authentication are used to determine whether a user is authenticated with user name and password or whether additional information is needed to authenticate the user.

**Supported RSA Adaptive Authentication Methods of Authentication**

The RSA Adaptive Authentication strong authentication methods supported in Access Point are out-of-band authentication via phone, email, or SMS text message and challenge questions. You enable on the service the methods of RSA Adaptive Auth that can be provided. RSA Adaptive Auth policies determine which secondary authentication method is used.

Out-of-band authentication is a process that requires sending additional verification along with the user name and password. When users enroll in the RSA Adaptive Authentication server, they provide an email address, a phone number, or both, depending on the server configuration. When additional verification is required, RSA adaptive authentication server sends a one-time passcode through the provided channel. Users enter that passcode along with their user name and password.
Challenge questions require the user to answer a series of questions when they enroll in the RSA Adaptive Authentication server. You can configure how many enrollment questions to ask and the number of challenge questions to present on the login page.

**Enrolling Users with RSA Adaptive Authentication Server**

Users must be provisioned in the RSA Adaptive Authentication database to use adaptive authentication for authentication. Users are added to the RSA Adaptive Authentication database when they log in the first time with their user name and password. Depending on how you configured RSA Adaptive Authentication in the service, when users log in, they can be asked to provide their email address, phone number, text messaging service number (SMS), or they might be asked to set up responses to challenge questions.

For full install instructions please refer to the following link for the deployment guide:

https://www.vmware.com/support/pubs/access-point-pubs.html

**Configuring RADIUS for Unified Access Gateway**

You can configure Unified Access Gateway so that users are required to use RADIUS authentication. You configure the RADIUS server information on the Unified Access Gateway appliance.

RADIUS support offers a wide range of alternative two-factor token-based authentication options. Because two-factor authentication solutions, such as RADIUS, work with authentication managers installed on separate servers, you must have the RADIUS server configured and accessible to the identity manager service.

When users sign in and RADIUS authentication is enabled, a special login dialog box appears in the browser. Users enter their RADIUS authentication user name and passcode in the login dialog box. If the RADIUS server issues an access challenge, Unified Access Gateway displays a dialog box prompting for a second passcode. Currently support for RADIUS challenges is limited to prompting for text input.

After a user enters credentials in the dialog box, the RADIUS server can send an SMS text message or email, or text using some other out-of-band mechanism to the user's cell phone with a code. The user can enter this text and code into the login dialog box to complete the authentication.

If the RADIUS server provides the ability to import users from Active Directory, end users might first be prompted to supply Active Directory credentials before being prompted for a RADIUS authentication username and passcode.

For full install instructions please refer to the following link for the deployment guide:

https://www.vmware.com/support/pubs/access-point-pubs.html
Conclusion

This lesson provided information on the multi-factor authentication methods supported within Horizon 7. This included Connection\Security Servers and the Unified Access Gateway Server.
VMware Identity Manager Multi-Factor Features

VMware Identity Manager is an Identity management platform, providing application provisioning, self-service catalog, conditional access controls and Single Sign-On (SSO) for SaaS, web, cloud and native mobile applications.

VMware Identity Manager supports multiple authentication methods. You can configure a single authentication method and you can set up chained, two-factor authentication. You can also use an authentication method that is external for RADIUS and SAML protocols.

The identity provider instance that you use with the VMware Identity Manager service creates an in-network federation authority that communicates with the service using SAML 2.0 assertions.

When you initially deploy the VMWare Identity Manager service, the connector is the initial identity provider for the service. Your existing Active Directory infrastructure is used for user authentication and management.

Authentication methods that are configured in a connector deployed in an outbound-only connection mode can be enabled in the Built-in identity provider in the admin console. When the authentication methods are enabled in the Built-in identity provider, the VMware Identity Manager service communicates through a Websocket-based communication channel with the connector to authenticate users.
The following multi-factor authentication methods that are configured in the connector can be enabled in the Built-in identity provider:

- **RSA SecurID** - When RSA SecurID authentication is configured, VMware Identity Manager is configured as the authentication agent in the RSA SecurID server. RSA SecurID authentication requires users to use a token-based authentication system. RSA SecurID is an authentication method for users accessing VMware Identity Manager from outside the enterprise network.

- **RADIUS** - RADIUS authentication provides two-factor authentication options. You set up the RADIUS server that is accessible to the VMware Identity Manager service. When users sign in with their user name and passcode, an access request is submitted to the RADIUS server for authentication.

- **RSA Adaptive Authentication** - RSA authentication provides a stronger multi-factor authentication than only user name and password authentication against Active Directory. When RSA Adaptive Authentication is enabled, the risk indicators specified in the risk policy set up in the RSA Policy Management application. The VMware Identity Manager service configuration of adaptive authentication is used to determine the required authentication prompts.

- **Certificate** - Certificate-based authentication (Smart Card\PIV) can be configured to allow clients to authenticate with certificates on their desktop and mobile devices or to use a smart card adapter for authentication. Certificate-based authentication is based on what the user has and what the person knows. An X.509 certificate uses the public key infrastructure standard to verify that a public key contained within the certificate belongs to the user.

- **VMware Verify** - VMware Verify can be used as the second authentication method when two-factor authentication is required. The first authentication method is user name and password, and the second authentication method is a VMware Verify request approval or code.

After the authentication methods are configured, you create access policy rules that specify the authentication methods to be used by device type. Users are authenticated based on the authentication methods, the default access policy rules, network ranges, and the identity provider instance you configure.

**Conclusion**

This lesson provided you information on multi-factor support and authentication methods for VMware Identity Manager.
Multi-Factor Demonstration and Walkthrough with VMware Identity Manager

In this lesson VMware Identity Manager will be used to demonstrate Multi-Factor Authentication and allows for setting up Network Ranges and different authentication policies can be assigned to different network ranges.

For example, you want your end-users to authenticate with their AD credentials while they are in the office and connected to the corporate network, while you might want them to use 2-factor authentication when working from home.

For this lab we are using FreeRADIUS.net, in a real-world scenario this could be your RSA Server or any other 2-factor authentication solution supporting RADIUS protocol. We have setup a different password (123456) other than the default AD-password (VMware1!) typically used in the HOL, consider this your RSA token.

Lab Ready?

1. Make sure the Lab Status is Ready
Start FreeRADIUS.net

1. Open Start Menu
2. Select **FreeRADIUS START**
3. Verify FreeRADIUS is started and **Ready to process requests**.

**Warning**

Leave the FreeRADIUS START Window open or minimize it, but DO NOT close it.

In this module we will setup RADIUS as an additional authentication adapter and configure it to work our FreeRADIUS.net.

**Configure Identity Manager for Radius**
Open Identity Manager console

Open Google Chrome from the Desktop

1. Click **WS 1 Admin** to open Management Console
2. Username: **admin**
3. Password: **VMware1!**
4. Click **Sign in**

Setup Authentication Adapters

1. Click **Identity & Access Management** tab
2. Click **Setup**
3. Click on **vidm-01a.corp.local**

**Modify Authentication Adapters**

![Auth Adapters button](image)

1. Click **Auth Adapters**
2. Scroll down
3. Click **RadiusAuthAdapter**

### Adapter Table

<table>
<thead>
<tr>
<th>Adapter Name</th>
<th>Authentication Method</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>KerberosIdpAdapter</td>
<td>um.oasis.names.tc:SAML 2.0 ac classes: Kerberos</td>
<td>Disabled</td>
</tr>
<tr>
<td>PasswordIdpAdapter</td>
<td>um.oasis.names.tc:SAML 2.0 ac classes:PasswordProtectedTransport</td>
<td>Enabled</td>
</tr>
<tr>
<td>RSAAdpAdapter</td>
<td>um.vmware.names.ac.classes.adaptive</td>
<td>Disabled</td>
</tr>
<tr>
<td>SecuridIdpAdapter</td>
<td>um.oasis.names.tc:SAML 2.0 ac classes:TimeSincToken</td>
<td>Disabled</td>
</tr>
<tr>
<td>RadiusIdpAdapter</td>
<td>um.vmware.names.ac.classes.radius</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Configure RADIUS

1. Check 'Enable RADIUS Adapter'
2. Check 'Enable direct authentication to Radius server during auth chaining'
3. Set 'Number of attempts to Radius server' to 5
4. Set 'Server timeout in seconds' to 5
5. Specify **192.168.110.10** as the RADIUS server ip
6. Scroll down
7. Set Accounting port to **1813**
8. Chose **PAP** as Authentication type
9. Enter **HOLrocks!** as the shared secret
10. Scroll down (leave configuration for secondary server empty)
11. Click **Save**
1. Close this tab to return to the Admin Console

Now we create a networks range for our test VM (Windows10-01a) and modify the default policy to use RADIUS for this specific range we create.

Now we will verify the new policy is active.

**Define Network Range**

1. Click **Network Ranges**
2. Click **Add Network Range**
Define Network Range cont.

1. Enter **RADIUS Test** as 'Name' for the network range
2. Provide a description **RADIUS Test** (optional)
3. Enter **view-01a.corp.local** as Client Access URL Host
4. Set URL Port to **443**
5. Enter **192.168.100.113** as 'From'
6. Enter **192.168.100.113** as 'To'
7. Click **Save**

This will add a "range" of one IP-Address (our Windows 10 VM)
Verify the new network range has been added

Change default access policy

1. Click Manage tab
2. Click Policies
3. Click default_access_policy_set
Add new Web browser rule

1. Scroll down
2. Click the '+' sign
Configure Policy Rule

Add a Policy Rule

If a user’s Network Range is...

and the user is trying to access content from...

then the user may authenticate using the following method...

Radius

If preceding Authentication Method fails or is not applicable, then:

- Select Authentication Method-

Re-authenticate after: 8 hours

1. Select **RADIUS Test** from dropdown menu
2. Select **Web Browser** from dropdown menu
3. Select **RADIUS** from dropdown menu
4. Click **OK**
### Change Policy Rule Order

**Policy Rules**

You can create a list of rules to access these applications. For each rule, select the IP network range, the type of devices that can access the applications, the methods and authentication order, and the maximum number of hours users can use the application before reauthenticating.

<table>
<thead>
<tr>
<th>Network Range</th>
<th>Device type</th>
<th>Authentication Method</th>
<th>Re-authenticate</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL RANGES</td>
<td>Workspace ONE App</td>
<td>First, try: Password and 1 more fallback(s)...</td>
<td>2160 Hour(s)</td>
</tr>
<tr>
<td>RADIUS Test</td>
<td>Web Browser</td>
<td>First, try: Password and 1 more fallback(s)...</td>
<td>8 Hour(s)</td>
</tr>
<tr>
<td>ALL RANGES</td>
<td>Web Browser</td>
<td>Radius</td>
<td>8 Hour(s)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Range</th>
<th>Device type</th>
<th>Authentication Method</th>
<th>Re-authenticate</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Test</td>
<td>Web Browser</td>
<td>Radius</td>
<td>8 Hour(s)</td>
</tr>
<tr>
<td>ALL RANGES</td>
<td>Workspace ONE App</td>
<td>First, try: Password and 1 more fallback(s)...</td>
<td>2160 Hour(s)</td>
</tr>
<tr>
<td>ALL RANGES</td>
<td>Web Browser</td>
<td>First, try: Password and 1 more fallback(s)...</td>
<td>8 Hour(s)</td>
</tr>
</tbody>
</table>

1. Click the icon in front of **RADIUS Test**
2. **Drag** the rule all the way to the top
3. Click **Save**
Verify authentication methods

1. Verify RADIUS is now the first authentication method to be tried for the Network Range RADIUS test, when connecting via a Web Browser.

**Tip**

Please take a minute to look at all the different "access content from" and authentication method options, allowing you to setup different authentication methods for different devices/access methods and locations (based on network range).

You can also combine multiple authentication methods if you need more than 2-factor authentication. If you scroll down, you can add custom error message and links to further information in case authentication fails.

**Open New Incognito Windows**
Open a new incognito browser window:

1. Click the vertical dots in the upper right corner
2. Select **New incognito window**

**Log in to WS1**

1. Click **WS1**
2. Click **Next**
Log In as lab1user

1. User lab1user
2. Click VMware1!

Verify Login

You should have successfully logged in to the Workspace ONE console using your domain password.
1. Close the Incognito Window

**Test RADIUS Authentication from Windows10 VM**

Now to the real test, minimize your browser windows.

1. Click **Base-w10 Shortcut**
2. Select corp\lab1user
3. Username **corp\lab1user**
4. Password **VMware1!**
5. Click **Login**
Open Edge Browser

1. Open Microsoft Edge browser
2. Verify URL is set to vidm-01a.corp.local/SAAS/auth/login... if not enter vidm-01a.corp.local
3. Click Next
Authenticate Using RADIUS

1. Notice "Please enter RADIUS Passcode"
2. Notice Authentication is set to RADIUS Passcode
Login using RADIUS

1. Username **lab1user** (all in lowercase)
2. Password **123456**
3. Click **Sign In**

**Note:** Lab1user's Active Directory password is **VMware1!** (as you verified before). The RADIUS server has **123456** configured as the lab1user's password, in a real-world scenario, this could be your RSA token.
Verify you can access the portal successfully.
Disconnect and Log Off

1. Click **Start Menu**
2. Click on **Lab 1 User**
3. Select **Sign out**

Lesson Conclusion

In this lesson we have shown how easy it is to integrate VMware Identity Manager with a RADIUS compatible 2FA solution.
Module Conclusion

You have completed the Multifactor Authentication module of this lab.

You've finished Module 6

Congratulations on completing Module 6.

If you are looking for additional information on Horizon 7, try one of these:

• Click on this [HOL-1851-09-ADV](#)
• Or use your smart device to scan the above QRC Code.

Proceed to any module below which interests you most.

• **Module 1 - Security Considerations** (15 minutes) (Basic) This module will explore various use cases and security considerations of Horizon 7. It is the intent of this lab to provide concise references to some of the security features and technologies supported for Horizon 7. (Informational Module)
• **Module 2 - VMware Unified Access Gateway** (30 minutes) (Advanced) Within this section of the lab it will be shown how using VMware Unified Access Gateway will secure remote access to VMware end-user computing resources.
• **Module 3 - SSL Certificates** (30 minutes) (Intermediate) This module will demonstrate securing various VMware Horizon server components with SSL certificates.
• **Module 4 - True SSO** (30 minutes) (Intermediate) This module will review and demonstrate configuring True SSO (single sign-on) features in Horizon 7 while securing and adhering to Microsoft Windows (AD) Domain rights and authentication privileges.
• **Module 5 - Governance and Compliancy** (30 minutes) (Basic) VMware governance and compliancy delivers the ability for customers to confidently and quickly secure mission critical virtualized workloads throughout many critical
industries. This portion of the lab will provide guidance and information on these topics to assure compliance against many regulation requirements throughout various, unique industries. (Informational Module)

- **Module 6 - Multifactor Authentication** (30 minutes) (Intermediate) This module will provide information supporting multifactor authentication with Horizon 7 to include SmartCard, RSA, RADIUS technologies.
- **Module 7 - NSX for Horizon** (60 minutes) (Advanced) This module will demonstrate how VMware End User Computing and NSX Security solutions can provide a customized desktop experience, doing so while maximizing operational efficiencies and security leveraging pure stateless VDI.

### How to End Lab

To end your lab click on the **END** button.
Module 7 -NSX for Horizon (60 minutes)
Introduction & Overview

Many organizations implement desktop and application virtualization to improve client-computing security and deliver greater enterprise mobility. Centralizing desktops and applications protects data at rest, prevents unauthorized application access, and provides a more efficient way to patch, maintain and upgrade images. However, with desktop and application virtualization, new security concerns can arise behind the data center firewall where hundreds or even thousands of desktops reside. These desktops sit in close proximity to other users and mission-critical workloads, making them much more susceptible to malware and other attacks. These attacks can move from desktop to server, exposing a large attack surface within the data center. This east-west threat scenario is a common one affecting many customers today, particularly those with stringent security and compliance mandates.

This module will demonstrate how VMware End User Computing and NSX Security solutions can provide a customized desktop experience, doing so while maximizing operational efficiencies and security leveraging pure stateless VDI.

Throughout this module you can review the following lessons:

**Fast and Simple VDI Networking** - Simplify and accelerate administration of networking and security policy for users based on logical grouping, role, or tag

**Automated Policy Provisioning** - Automatically attach policy to a desktop as it is created, following the VM irrespective of the underlying infrastructure

**Platform for Advanced Security** - Integrate with industry-leading solutions for antivirus, malware, intrusion prevention, and next-gen security services

**Service Composer and Distributed Firewall Walkthrough and Demonstration** - This module will walk you through the requirements of configuring Service Composer and setting up the Distributed Firewall while applying that firewall to a VDI desktop.

VMware NSX for Horizon

How It Works

VMware NSX for Horizon improves desktop virtualization security and helps address east-west threats by enabling administrators to define policy centrally. That policy is then distributed to the hypervisor layer within every vSphere host, and automatically attached to each virtual desktop as soon as the desktop is created. To secure virtual desktops and adjacent workloads within the data center, VMware NSX implements micro-segmentation, giving each desktop its own perimeter defense. This shrink-
wrapped security uses VMware NSX distributed virtual firewalling capability to police traffic to and from each VM, eliminating unauthorized access between desktops and adjacent workloads. If the virtual desktop moves from one host to the next, or across the data center, policy will automatically follow it.
Fast and Simple VDI Networking

With VMware NSX for Horizon, administrators can create, change, and manage security policies across all virtual desktops with a few easy clicks. Security policies can be quickly mapped to user groups to speed virtual desktop onboarding. With the ability to deploy virtualized network functions (like switching, routing, firewalls, and load-balancing) administrators can build virtual networks for VDI without the need for complex VLANs, ACLs, or hardware configuration syntax.
Automated Policy Provisioning

Administrators can set policies that dynamically adapt to the end users computing environment, with network security services that map to the user based on role, logical grouping, desktop operating system, and more independent of the underlying network infrastructure. Centrally administered policy is automatically attached to each desktop VM as soon as the desktop is created, so organizations can scale with confidence, with security that persistently follows the virtual desktop across the data center.
Platform for Advanced Security

VMware NSX offers an extensible platform that can be integrated with best-in-class capabilities from an established ecosystem of security partners. By dynamically adding services, virtual desktop security can be extended from the data center to the desktop and the application. This ecosystem of partners, including Trend Micro, Intel Security, and Palo Alto Networks, offers solutions that protect the operating system, browser, email, and more with antivirus, malware, intrusion-prevention, and next-gen security services.
Distributed Firewall Configuration Walkthrough and Demonstration

Within this lesson you will review the steps required to deploy and configure the NSX Distributed Firewall. Once the Firewall is deployed you will create Firewall Rules and apply those rules to two different user groups. The specific use case in this lesson is to deploy rules to both Administrators and Normal Users restricting access to services each role should have access to while letting them use services they are entitled to.

Deploy NSX Firewall and Guest Introspection Services

Distributed firewall is a hypervisor kernel-embedded firewall that provides visibility and control for virtualized workloads and networks. You can create access control policies based on VMware vCenter objects like datacenters and clusters and virtual machine names; network constructs like IP or IPSet addresses, VLAN (DVS port-groups), VXLAN (logical switches), security groups, as well as user group identity from Active Directory. Firewall rules are enforced at the vNIC level of each virtual machine to provide consistent access control even when the virtual machine gets vMotioned. The hypervisor-embedded nature of the firewall delivers close to line rate throughput to enable higher workload consolidation on physical servers. The distributed nature of the firewall provides a scale-out architecture that automatically extends firewall capacity when additional hosts are added to a datacenter.
Launch vCenter Web Client

- Launch **Google Chrome** Browser
- Select the **HOL-1851 Admin** Folder
- Select **vCenter Web Client** Bookmark
- Login to the **vCenter Web Client** by selecting **Use Windows Authentication**
Browse to Networking & Security

- Select **Home**
- Select **Networking & Security**

Host Preparation

- Select **Installation**
- Select the **Host Preparation** Tab
Host Preparation Cont...

- Select RegionA01-IC01
- On the Actions Menu select Install

Host Preparation Cont...

- Select Yes

Host Preparation Cont...

- Wait for the Install Status to Complete
**Force Sync**

Once the installation is complete we need to sync services to show that the firewall has been configured on the hosts.

- On the **Actions** menu option select **Force Sync Services**

- Check the **Firewall** box

**Confirm Install**

- Confirm **Installation Status**

**Deploy Guest Introspection**

The Firewall service has been deployed and configured on the hosts. Next we need to deploy Guest Introspection throughout the environment.

Installing Guest Introspection installs a new vib and a service virtual machine on each host in the cluster. Guest Introspection is required for NSX Data Security, Activity Monitoring, and several third-party security solutions.

- Under the **Installation** area within the **Navigator**
- Select **Service Deployments** Tab
- Select the **Green +** icon
• Select the **Guest Introspection** Service
• Select **Next**
Deploy Guest Introspection Cont...

- Select **RegionA01-IC01**
- Select **Next**
Deploy Guest Introspection Cont...

- For the **Datastore** Select **COMP01-iscsi01**
- Select **VM-RegionA01-vDS-IC** for the **Network**
- Select **Next**
Deploy Guest Introspection Cont...

- Review configuration settings
- Select Finish
Verify Success for Guest Introspection

- Wait for the **Installation Status** to display **Succeeded**

Once this is done, Guest Introspection can be deployed to the VMs so that Firewall settings on those VMs can be configured.

**Deploy VM Guest Introspection Drivers**

**NOTE:**

Guest Introspection has already been deployed to all of the necessary VMs in this lab. The following steps will verify that the Guest Introspection has been properly deployed.
• Back in the vCenter Web Client and Within Hosts and Clusters, expand RegionA01 DataCenter and RegionA01-IC01 cluster

Open Console

• Right Click W10-IC-01
• Select Open Console
Send Ctrl-Alt-Delete

- Select Send Ctrl-Alt-Delete
Login

- Login with CORP\Administrator
- Password is VMware1!
Navigate to the Control Panel

- From the **Start Menu**
- Type **Control Panel**
- Select **Control Panel**
Programs and Features

• In the Control Panel find **Programs and Features** and launch it
VMware Tools

- Find **VMware Tools** and launch by selecting **Change**
Next

- Select Next
Modify

- Select **Modify**

![VMware Tools Setup](image)

Verify NSX Network Introspection

- Scroll down to **VMCI Driver** and expand
- Expand **NSX File Introspection Driver**
- Verify that **NSX Network Introspection** is installed
If Network Introspection is not installed, select the feature and install. This can also be deployed through the vSphere Web Client by deploying VMware Tools to the VM and selecting the same configuration options outlined in this step.

---

**Synchronize NSX Manager with Active Directory**

Once Guest Introspection is deployed and configured we need to register the NSX Manager with Active Directory.

You can register one or more Windows domains with an NSX Manager and associated vCenter server. NSX Manager gets group and user information as well as the relationship between them from each domain that it is registered with. NSX Manager also retrieves Active Directory (AD) credentials.

Once NSX Manager retrieves AD credentials, you can create security groups based on user identity, create identity-based firewall rules, and run Activity Monitoring reports. Some of these actions will be included in follow on steps.
• Select **Home**

![vmware vSphere Web Client](image)

**Browse Networking & Security**

• Select **Networking & Security**

![Inventory pane](image)
NSX Manager

Scroll down in the Navigator and select NSX Managers
Select corp.local

- Select 192.168.110.31
- Select Domains
- Select corp.local
- Select Edit

corp.local

- Leave the Domain Name as corp.local
- Leave the NetBIOS Name as CORP
- Select Next
LDAP Options

Within LDAP Options Configure the following options:

- Server: Controlcenter.corp.local
- Protocol: LDAP
- Port: 389
- User Name: administrator
- Password: VMware1!

Select Next
Next

• Select Next
Finish

• Select Finish

Update Local State

No we need to Update the local state of All AD Objects associated with this domain. This will synchronize the NSX Manager with Active Directory.

• Highlight corp.local
• Update the local state of All AD Objects associated with this domain
Refresh

- **Refresh** the page until you see **SUCCESS** and a **Time Stamp**

Now that the NSX Manager has been synchronized with Active Directory we can now create the Security Groups based on Active Directory Security Groups.

A security group is a collection of assets or grouping objects from your vSphere inventory and those objects that we have synchronized from Active Directory.

**We are going to create two security groups for an Administrators group and a normal Users Group. This will allow us to provide role based restrictions and capabilities against these groups when configuring the distributed firewall.**

**Create Security Groups**

- **Within the vSphere Web Client** Select **Home**
Browse Networking & Security

- Select **Networking & Security**

Add Security Group

- In **Navigator** Select **Service Composer**
- Add **New Security Group**
Add Security Group Cont...

- Within the New Security Group Wizard Provide the Name: **Administrator**
- Description: **Administrator Group**
- Select **Next**

![New Security Group Wizard](image1)

**Next**

- Select **Next** again

![Define dynamic membership](image2)
Add Objects

- Expand **Object Type** and select **Directory Group**
- Find **Administrator** in the **Available Objects** area
- Add to **Selected Object**
- Click **Next**
Finish

- Select Finish

Add User Group

We will now follow the same exact process for our User Group.
• In **Navigator** Select **Service Composer**
• Under the **Security Groups Tab** Add **New Security Group**

**User**

• Name: **User**
• Description: **User Group**
• Select **Next**
Next

- Select **Next** again

---

**Add User Group to Selected Objects**

- Expand **Object Type**
- Select **Directory Group**
- Find **Horizon Users** from the **Available**
- Select **Finish**
Verify Administrators and Users

- Verify that your two security groups for **Administrators** and **Users** was created

Now that we have created our security groups for Administrators and Users we can now apply dynamic role based firewall rules to these security groups. In the below steps you will test these user accounts prior to Firewall rule creation and distribution, deploy Firewall Rules to these security groups and then test those accounts once the Firewall setting have been deployed. Testing those accounts are in the steps to follow within the steps to follow.
Test User Accounts Pre-Firewall Rules

We will now test user accounts before we apply any Firewall rules to those users. This will demonstrate how we can dynamically assign Firewall rules to users whom log into the same exact machine.

We will test a User account vs a Administrator account. The Use Case is that Administrators should have access to tools like PING while restricting internet access so that an Administrator is not browsing the internet with admin privileges. Likewise, with our User account we will restrict access to Administrative tools like ping but allow Internet browsing. **Again, this first test is without Firewall rules being deployed and all services will work.**

- Still in the vSphere Web Client, select the Hosts and Clusters Tab
- Expand RegionA01 Datacenter
- Expand RegionA01-IC01
- Scroll and find W10-IC-01
- Right click on Open Console
Ctrl+Alt+Delete

- Select **Ctrl+Alt+Delete**
lab1user

- Select **Other user**
- Login: **lab1user**
- Password: **VMware1!**
- Login

![Login to CORP](image)

**Test Ping**

- Once logged on, open a **CMD** prompt
- Type **ping corp.local**
You can see as a normal user have rights to ping a domain controller in the environment. This is typically something you do not want to allow for normal users on the network. In steps later in this lesson we will create a firewall rule to prevent this from happening with normal users.

Test Internet Browsing

You can also test internet browsing to make sure that it is working for a normal user.

- Open Microsoft Edge
- Type in vmware.com into the address bar
Note Internet browsing works without issue

Log Off

Log off of the user account and login with an Administrator account.

- Select **Send Ctrl+Alt+Delete**
- **Sign Out**
Login with Administrator

- Select **Send Ctrl+Alt+Del**
- Select **Other User**
- Username: `administrator@corp.local`
- Password: `VMware1!`
- Login

Open CMD Prompt

- Open **CMD** prompt
- Type: `Ping corp.local`
You can see that the Administrator on the W10-IC-01 machine can ping a domain controller.

Test Internet Browsing

You can also open Microsoft Edge and test internet connectivity.

- Open Microsoft Edge
- Type: vmware.com in the address bar
Note that the Internet Browsing for the administrator also works

Log Off

Many organizations restrict internet access from Administrator accounts, so this would be a security finding in those environments.

We will setup those firewall rules to prevent this in the next part of the lesson.
• Next log off the VM by selecting **Send CTRL+ALT+DEL**
• Select **Sign Out**

Create Distributed Firewall Rules for Administrators and Users

Now you can see that both users and administrators have certain services available to them that they should not have permissions to. In this part of the lesson we will create the firewall rules to restrict access to those services. We will create rules to prevent Administrators from browsing the internet on a Win10 machine while allowing access to PING. Likewise, for a normal User we will restrict access to PING while allowing them to browse the internet on a Win10 machine.

• Within the **vSphere Web Client** Select **Home**
Browse Networking & Security

- Select **Networking & Security**

Select Firewall

- Select **Firewall**
- **Add a Section**

Horizon Section

In the New Section Wizard:
• Name: Horizon Rules
• Add Above

Add Rule

• Once the Section is created
• Add a Rule

Configure Rule

When the Rule is added we must configure the rule

Create the name
• Click the pencil in the Name Column to edit

ICMP Block

• Provide the name: **ICMP Block** (This rule will block PING and other ICMP protocols)
Create the Source

- Edit the **Source**

![Image of NSX Manager interface showing Horizon Rules (Rule 1) and Default Section Layer3 (Rule 2 - 4) with edit options highlighted.](image)

*Edit with the pencil*
Add Security Group

- Select Object Type: **Security Group**
- Select **User** (created in an earlier step)
- Add **User** to **Selected Objects**
- Hit **OK**
Configure the Service

• Edit Service

Specify Service

Object Type: Service

Filter: ICMP
Add **ALL ICMP** to the **Selected Objects**
Edit Action

• Edit the **Action**
Configure Rule

- Select **Action** and change to **Block**
- Direction: **In/Out**
- Packet Type: **Any**

![Image of ICMP Block - Edit Action dialog]

Add Another Rule

- Add a second **Rule** *(This rule will be created to block Http and Https traffic for Administrators)*

![Image of NSX Manager dashboard]

This rule set has unsaved changes. Click on Publish Changes button to start deploying or click Save Changes to save this configuration.
Configure Rule

When the Rule is added we must configure the rule

Create the name

  • Click the pencil in the Name Column to edit

![Edit with the pencil]

Name the Rule

  • Provide the name: Restrict HTTP, HTTPS (This rule will block HTTP and HTTPS)
Create the Source

- Edit the **Source**
Specify Source

- Select Object Type: Security Group
- Select Administrator (created in an earlier step)
- Add Administrator to Selected Objects
- Hit OK
Configure the Service

- Edit **Service**

Specify Service

Object Type: **Service**

Filter: **HTTP**
Add **HTTP & HTTPS** to the **Selected Objects**
Edit Action

• Edit the **Action**
Configure Action

- Select **Action** and change to **Block**
- Direction: **In/Out**
- Packet Type: **Any**

![Configure Action Image]

Publish Changes

Now that the two rules to restrict access to ICMP (Ping) for Users and to restrict access to HTTP\HTTPS for Administrators has been created Publish the Changes.

- **Publish Changes**

![Publish Changes Image]
Verify the Rules

- Verify that the rules have been created.

Test the Firewall Rules for Administrators and Users

Now that all of the rules to restrict access to ICMP for Users and HTTPS\HTTP traffic for Administrators, let's make sure that the rules work.

We will now test user accounts after we have created and applied Firewall rules to those users. This will demonstrate how we can dynamically assign Firewall rules to users whom log into the same exact machine.

We will test a User account vs a Administrator account. The Use Case is that Administrators should have access to tools like PING while restricting internet access so that an Administrator is not browsing the internet with admin privileges. Likewise, with our User account we will restrict access to Administrative tools like ping but allow Internet browsing. **This is the second test with Firewall rules being deployed and blocking the associated services.**

- Still in the **vSphere Web Client**, select the **Hosts and Clusters** Tab
- Expand **RegionA01** Datacenter
- Expand **RegionA01-IC01**
- Scroll and find **W10-IC-01**
- Right click on **Open Console**
Login with User Account

- Select Ctrl+Alt+Delete
Login with User Account Cont...

• Select **Other user**
• Login: **lab1user**
• Password: **VMware1!**
• Login

---

**Test Ping**

• Once logged on, open a **CMD** prompt
• Type **ping corp.local**
You can see as a normal user no longer has rights to ping a domain controller in the environment.

Test Internet Browsing

You can also test internet browsing to make sure that it is still working for a normal user.

- Open Microsoft Edge
- Type in vmware.com into the address bar
Internet browsing works without issue

Sign Out

Log off of the user account and login with an Administrator account.

• Select **Send Ctrl+Alt+Delete**
• **Sign Out**
Login with Administrator Account

- Select **Send Ctrl+Alt+Del**
- Select **Other User**
- Username: **administrator@corp.local**
- Password: **VMware1!**
- Login

Test Ping

- Open **CMD** prompt
- Type: **Ping corp.local**
You can see that the Administrator on the W10-IC-01 (Same exact VM) machine can ping a domain controller.

Test Internet Browsing

You can also open Microsoft Edge and test internet connectivity.

- Open Microsoft Edge
- Type: vmware.com in the address bar
Administrators no longer have access to browse the internet!

Log Off

Next log off the VM by selecting Send CTRL+ALT+DEL
Lesson Conclusion

This lesson has demonstrated how to deploy all of the necessary components for the Firewall operations within NSX and Horizon. We have demonstrated that two users based on Active Directory role can login to the same VM and have a totally unique set of Firewall rules applied to them. There are a number of other Security objects you can apply these rules to creating a true Role Based Firewall and desktop experience.
Module Conclusion

You have completed the NSX for Horizon module of this lab.

You've finished Module 7

Congratulations on completing Module 7.

If you are looking for additional information on Horizon 7, try one of these:

- Click on this [HOL-1851-09-ADV](#)
- Or use your smart device to scan the above QRC Code.

Proceed to any module below which interests you most.

- **Module 1 - Security Considerations** (15 minutes) (Basic) This module will explore various use cases and security considerations of Horizon 7. It is the intent of this lab to provide concise references to some of the security features and technologies supported for Horizon 7. *(Informational Module)*
- **Module 2 - VMware Unified Access Gateway** (30 minutes) (Advanced) Within this section of the lab it will be shown how using VMware Unified Access Gateway will secure remote access to VMware end-user computing resources.
- **Module 3 - SSL Certificates** (30 minutes) (Intermediate) This module will demonstrate securing various VMware Horizon server components with SSL certificates.
- **Module 4 - True SSO** (30 minutes) (Intermediate) This module will review and demonstrate configuring True SSO (single sign-on) features in Horizon 7 while securing and adhering to Microsoft Windows (AD) Domain rights and authentication privileges.
- **Module 5 - Governance and Compliancy** (30 minutes) (Basic) VMware governance and compliancy delivers the ability for customers to confidently and quickly secure mission critical virtualized workloads throughout many critical industries. This portion of the lab will provide guidance and information on these
topics to assure compliance against many regulation requirements throughout various, unique industries. (Informational Module)

- **Module 6 - Multifactor Authentication** (30 minutes) (Intermediate) This module will provide information supporting multifactor authentication with Horizon 7 to include SmartCard, RSA, RADIUS technologies.
- **Module 7 - NSX for Horizon** (60 minutes) (Advanced) This module will demonstrate how VMware End User Computing and NSX Security solutions can provide a customized desktop experience, doing so while maximizing operational efficiencies and security leveraging pure stateless VDI.

**How to End Lab**

To end your lab click on the **END** button.
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-1851-09-ADV

Version: 20181106-130632