# Table of Contents

Lab Overview - HOL-1957-02-UEM - Workspace ONE UEM - Identity Management .......... 3
  Lab Guidance ........................................................................................................... 4
Module 1 - Install, Configure and Manage VMware Identity Manager ......................... 9
  Introduction .......................................................................................................... 10
  Connect to the Conn-01a Server ........................................................................ 11
  Install and Configure the VMware Identity Manager Connector .......................... 12
  Return to the Main Console ............................................................................... 23
  Login to the Workspace ONE UEM Console .................................................... 24
  Login to the VMware Identity Manager Console ............................................. 30
  Configure Your VMware Identity Manager Tenant ............................................ 35
  Create and Configure the VMware Identity Manager Connector ....................... 37
  Sync Directory Users to VMware Identity Manager ........................................... 43
  Setup an Identity Provider to use Password Cloud Deployment ....................... 50
  Setup a Weblink Application and Entitle Users ............................................... 61
  Setup Kerberos Authentication Adapter ....................................................... 73
  Setup RADIUS Authentication ...................................................................... 86
  Instructions for Taking Additional Lab Modules .............................................. 119
  Conclusion ........................................................................................................ 120

Module 2 - On-Premises Install for VMware Identity Manager .................................. 121
  Introduction ...................................................................................................... 122
  Lab Architecture ............................................................................................... 123
  Create VMware Identity Manager SQL Database .......................................... 125
  Install the VMware Identity Manager Service ............................................... 130
  Navigate to the VMware Identity Manager Admin Console ......................... 160
  Install the VMware Identity Manager Connector ......................................... 163
  Activate the VMware Identity Manager Connector ....................................... 182
  Sync Directory Users to VMware Identity Manager ....................................... 188
  Login as a Domain User .................................................................................. 195
  Setup Kerberos Authentication Adapter ....................................................... 200
  Instructions for Taking Additional Lab Modules .............................................. 215
  Conclusion ........................................................................................................ 216

Module 3 - Third party Identity Provider Integration with ADFS .............................. 217
  Introduction ...................................................................................................... 218
  AD FS Overview ................................................................................................ 219
  Install and Configure AD FS (Video Walkthrough) ......................................... 220
  Download the AD FS Federation Metadata XML .......................................... 221
  Connect to the Conn-01a Server .................................................................... 226
  Install and Configure the VMware Identity Manager Connector ..................... 227
  Return to the Main Console ............................................................................ 238
  Login to the Workspace ONE UEM Console ................................................ 239
  Login to the VMware Identity Manager Console .......................................... 245
  Configure Your VMware Identity Manager Tenant ....................................... 250
Create and Configure the VMware Identity Manager Connector ........................................ 252
Sync Directory Users to VMware Identity Manager ...................................................... 258
Create a Third Party Identity Provider ........................................................................ 265
Configure Access Policies in VMware Identity Manager ........................................... 275
Configure Relying Party Trust in AD FS ..................................................................... 280
Login as a Domain User ............................................................................................... 299
Troubleshooting ............................................................................................................ 309
Instructions for Taking Additional Lab Modules ......................................................... 315
Conclusion .................................................................................................................... 316
Module 4 - VMware Identity Manager REST API ......................................................... 317
  Introduction .................................................................................................................. 318
  Login to the Workspace ONE UEM Console ......................................................... 319
  Login to the VMware Identity Manager Console .................................................. 325
  Open Postman ............................................................................................................ 330
  Request an oAuth SessionToken .............................................................................. 331
  Create a Local User in Identity Manager ............................................................... 335
  List Users in Identity Manager ................................................................................ 341
  Create a Weblink Application in Identity Manager ............................................... 342
  Entitle the Local User to the Weblink App ............................................................ 347
  Instructions for Taking Additional Lab Modules .................................................... 354
  Conclusion .................................................................................................................. 355
Lab Overview - HOL-1957-02-UEM - Workspace ONE UEM - Identity Management
Lab Guidance

Note: It may 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.

Learn how VMware Identity Manager can act as the primary Identity Provider or federate your authentication to other 3rd Party Identity Providers to provide Single Sign-On capabilities and rich access policies for your workforce. Learn how to configure and manage VMware Identity Manager for both Software-as-a-Service (SaaS) and on-premises scenarios. Lastly, explore how the VMware Identity Manager REST APIs can assist in automating common tasks and procedures.

Lab Module List:

- **Module 1 - Install, Configure and Manage VMware Identity Manager** (60 minutes) (Beginner) Learn the fundamental principles of how to install, configure and manage VMware Identity Manager and the VMware Identity Manager Connector for SaaS, including authentication methods and identity providers.
- **Module 2 - On-Premises Install for VMware Identity Manager** (60 minutes) (Intermediate) Learn how to properly install and configure VMware Identity Manager for an on-premises Windows installation.
- **Module 3 - 3rd party Identity Provider Integration with ADFS** (60 minutes) (Beginner) Learn how to leverage your existing ADFS deployment as a 3rd Party Identity Provider with VMware Identity Manager to federate user authentication.
- **Module 4 - VMware Identity Manager REST API** (30 minutes) (Beginner) Explore the VMware Identity Manager REST APIs and how they can be used to automate common tasks and procedures.

Lab Captains:

- Roger Deane, Sr. Manager, Technical Marketing, USA
- Shardul Navare, Sr. Technical Marketing Architect, USA
- Chris Halstead, EUC Staff Architect, USA
- Andreano Lanusse, EUC Staff Architect, USA
- Justin Sheets, Sr. Technical Marketing Architect, USA

Subject Matter Experts:

- Camilo Lotero, Senior Technical Marketing Manager, USA
This lab manual can be downloaded from the Hands-on Labs Document site found here:

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 startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes you lab has not changed to "Ready", please ask for assistance.
Module 1 - Install, Configure and Manage VMware Identity Manager
Introduction

This lab will review how to install, configure, and manage VMware Identity Manager. These exercises included:

1. Setup and Install the VMware Identity Manager Connector
2. Configure, Sync, and Manage Directories and Users
3. Configuring Identity Providers (IdP) and Authentication Methods for Kerberos and Radius
4. Configuring and Entitling Applications
Connect to the Conn-01a Server

Double-click the conn-01a.rdp link on the Desktop to connect to the Conn-01a Server.

For the initial part of this lab, you will be installing the VMware Identity Manager Connector on the designated server. It is recommended to install the VMware Identity Manager Connector on a dedicated server or Virtual Machine (VM).
Install and Configure the VMware Identity Manager Connector

The VMware Enterprise Systems Connector has already been downloaded for you. The VMware Enterprise Systems Connector contains both the AirWatch Cloud Controller (ACC) and VMware Identity Manager Connector services. For this lab, you will only be installing the VMware Identity Manager Connector service in order to sync and authenticate Active Directory users with your VMware Identity Manager Tenant.

Start the VMware Enterprise Systems Connector Installer

1. Click the File Explorer icon from the taskbar.
2. Click Documents.
3. Click HOL.

4. Click VMware Enterprise Systems Connector.
4. Double-click the **VMware Enterprise Systems Connector 9.4.0.0 Installer.exe** file.

**Confirm Security Warning and Run**

Click **Run**.

*NOTE - The Installer may take a minute or two to start after clicking run.*
Start the VMware Enterprise Systems Connector Installer

Click **Next**.

Accept the License Agreement Terms

1. Select **I accept the terms in the license agreement**.
2. Click **Next**.

**Disable the AirWatch Cloud Connector Feature**

![AirWatch Cloud Connector Feature Diagram]

1. Click the dropdown by the **AirWatch Cloud Connector** component.
2. Click **This feature will not be available.**
Enable the VMware Identity Manager Connector Feature

1. Click the dropdown by the VMware Identity Manager Connector component.
2. Click This feature will be installed on local hard drive.

Accept the Default Destination Folder

1. Click the dropdown by the VMware Identity Manager Connector component.
2. Click This feature will be installed on local hard drive.
3. Accept the Default Destination Folder C:\VMware\.
Click **Next** to accept the default destination folder of `C:\VMware\`

**Configure the SSL Certificate**

1. Check the **Would you like to use your own SSL Certificate?** option
2. Click **Browse...**
Browse to the Connector SSL Certificate

1. Click **Documents**
2. Click **HOL**
3. Click **conn-01a**
4. Click **Open**
Enter SSL Certificate Password

1. Enter VMware1! for the Certificate Password
2. Click Next

Continue without Activating the Connector
1. Select No for **Would you like to activate the Connector now**
2. Click **Next**

In this lab, we are only interested in installing the VMware Identity Manager Connector at this point. We will activate the Connector later once we have setup the Connector in our VMware Identity Manager Admin Console and have access to the Activation Code. As stated by the installer, this can be updated later by accessing the Connector settings at [https://{hostname}:8443](https://{hostname}:8443), which will be [https://conn-01a.corp.local:8443](https://conn-01a.corp.local:8443).

**Setup the Service Account Configuration**

1. Ensure the **Would you like to run the Connector service as a domain user account** option is enabled.
2. Enter **CORP\Administrator** for the User name.
3. Enter **VMware1!** for the Password.
4. Click **Next**.
Start the Install Process

Click Install.

*NOTE - The Installer may take a few minutes to complete. Please be patient while the service installs.*
Close the VMware Enterprise Systems Connector After It Completes

Click **Finish**.
Return to the Main Console

With the VMware Identity Manager Connector installed, you will configure the remainder of the requirements for this lab from the Main Console.

Click the Close (X) button on the Remote Desktop Connector bar at the top of your screen.

*NOTE: If you do not see the Remote Desktop Connection bar, you may have un-pinned the bar. Hover your mouse over the top and center part of the screen to reveal it.*
Login to the Workspace ONE UEM Console

To perform most of the lab, you will need to login to the Workspace ONE UEM Admin Console.

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.
Authenticate to the Workspace ONE UEM Admin Console

![Workspace ONE UEM Login Form]

The default home page for the browser is https://labs.awmdm.com. Enter your Workspace ONE UEM Admin Account information and click the Login button.

**NOTE - If you see a Captcha, please be aware that it is case sensitive!**

1. Enter your **Username**. This is your email address that you have associated with your **VMware Learning Platform (VLP) account**.
2. Enter **VMware1!** for the **Password** field.
3. Click the **Login** button.

**NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the Workspace ONE UEM Hands On Labs server.**
Accept the End User License Agreement

Terms of Use

You must accept the following VMware End User License Agreement to use Workspace ONE UEM.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If you are licensing the Software for evaluation purposes, your use of the Software is only permitted in a non-production environment and for the period limited by the license key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls

NOTE - The following steps of logging into the Administration Console will only need to be done during the initial login to the console.

You will be presented with the Workspace ONE UEM Terms of Use. Click the Accept button.
Address the Initial Security Settings

Security Settings

Password Recovery Question 1

Password Recovery Question *

Password Recovery Answer *

Confirm Password Recovery Answer *

Security PIN

A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).

Security PIN *

Confirm Security PIN *

After accepting the Terms of Use, you will be presented with a Security Settings popup. The Password Recovery Question is in case you forget your admin password and the Security PIN is to protect certain administrative functionality in the console.
1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a question from the Password Recovery Question drop-down (default selected question is ok here).
3. Enter VMware1! in the Password Recovery Answer field.
4. Enter VMware1! in the Confirm Password Recovery Answer field.
5. Enter 1234 in the Security PIN field.
6. Enter 1234 in the Confirm Security PIN field.
7. Click the Save button when finished.

Close the Welcome Message

Workspace ONE UEM Console Highlights

Powered by VMware AirWatch!

Workspace ONE is powered by VMware AirWatch Unified Endpoint Management (UEM) technology, a unified digital workspace platform delivering a single, secure experience for app management, single sign-on (SSO), and conditional access.

Workspace ONE UEM transforms your business so you can:

- Configure, manage and support devices from any endpoint
- Increase productivity with seamless access to any app
- Safeguard company data at every layer
- Access identity and access management tools with ease
- Enjoy a simplified, consistent look and feel across Workspace ONE

Don’t show this message on login
After completing the Security Settings, you will be presented with the Workspace ONE UEM Console Highlights pop-up.

1. Click on the **Don't show this message on login** check box.
2. Close the pop-up by clicking on the **X** in the upper-right corner.
Login to the VMware Identity Manager Console

A temporary VMware Identity Manager tenant has been generated for you to use throughout this lab. The VMware Identity Manager tenant URL and login details were uploaded to the Content section in the Workspace ONE UEM Console at the start of the lab.

Accessing Your Tenant Details in the Workspace ONE UEM Console

In the Workspace ONE UEM Console:

1. Click Content.
2. Expand Content Locker.
3. Click List View.
4. Find the text file named `viDM Tenant Details for your@email.shown.here.txt` and click the toggle button beside it to select the file.
5. Click Download.

Open the Downloaded Text File
After the file downloads, click the **viDM Tenant Details for your@email.shown.here.txt** file from the download bar to open it.

**Copy the Tenant URL**

1. Select the **Tenant URL** text and right-click.
2. Click **Copy**.

You will navigate to this Tenant URL in the next step to login to your VMware Identity Manager tenant.

**NOTE:** Your tenant name will match your Group ID in the Workspace ONE UEM Console.

**Login to Your VMware Identity Manager Tenant**

You will now login to your VMware Identity Manager tenant for the following steps.

**Launch Google Chrome (If Needed)**

If Google Chrome is not already open, launch **Google Chrome** by double-clicking the icon from the desktop.

**NOTE:** If Google Chrome is already open, skip this step.
Open a New Browser Tab

Click the Tab space to open a new tab.

Navigate to Your VMware Identity Manager Tenant

Paste or enter the Tenant URL into the navigation bar and press Enter to continue.

NOTE: This is the Tenant URL you received from the previous steps. If you did not copy or note this information from the previous step, return to those previous steps and note your Tenant URL.

NOTE: Your tenant name will match your Group ID found in the Workspace ONE UEM Console.
Login to Your VMware Identity Manager Tenant

1. Enter Administrator for the Username.
2. Enter VMware1! for the Password.
3. Click Sign In.

Navigate to the Administrator Console (If Necessary)
If you see the User Portal as pictured above, you will need to navigate to the Administrator Console.

1. Click the **User dropdown**.
2. Click **Administration Console**.

This will open the Administration Console in a separate tab in your browser.

*NOTE - If you do not see the above view, you are already in the Administration Console and can skip this step.*
Configure Your VMware Identity Manager Tenant

Before configuring the Directory Services and the VMware Identity Manager settings in the AirWatch Console, you will need to make some configurations your VMware Identity Manager tenant to ensure our Active Directory users are imported and mapped properly based on our configuration.

Continue to the next step.

Edit User Attributes

![Image of user attributes page]

1. Identity & Access Management
2. Manage
3. Setup
4. Check for required attributes:
   - distinguishedName
   - firstName
   - lastName
   - userPrincipalName

5. Keep other attributes unchecked.
1. Click **Identity & Access Management**.
2. Click **Setup**.
3. Click **User Attributes**.
4. Enable **distinguishedName** by clicking the checkbox next to the field.
5. Enable **userPrincipalName** by clicking the checkbox next to the field.

   **NOTE** - You may need to scroll down to find the distinguishedName and userPrincipalName attributes.

### Save User Attribute Changes

1. Scroll down to the bottom of the page.
2. Click **Save**.
Create and Configure the VMware Identity Manager Connector

In the VMware Identity Manager Administrator Console,

1. Click **Identity & Access Management**.
2. Click **Setup**.
3. Click **Connectors**.
4. Click **Add Connector**.

Generate the Connector Activation Code

1. Enter **Lab** for the Connector ID Name.
2. Click **Generate Activation Code**.
Copy the Connector Activation Code

1. Double-click the **Connector Activation Code** textbox to select the code.
2. **Right-click** and click **Copy**.
3. Click **OK**.

Activate the Connector

To activate the VMware Identity Manager Connector, you can connect to the hostname over port 8443 where the VMware Identity Manager Connector service was installed. You installed the VMware Identity Manager Connector service on conn-01a.corp.local in earlier steps.

1. Click the **Options** button
2. Click **New Tab**
Create the Administrator Account Credentials

First you will configure the Appliance Administrator Account (admin) for future logins:

1. Enter `VMware1!` for the Password
2. Enter `VMware1!` to confirm the password
3. Click `Continue`
Paste the Activation Code

1. Right-Click inside the Activation Code textbox and click **Paste** to paste the Activation Code we copied from the previous step when creating the "Lab" Connector from the VMware Identity Manager Console
2. Click **Continue**

**NOTE - While the page loads and refreshes, DO NOT close or manually refresh the page until you see the Setup is Complete screen shown in the next step!**
Confirm the Setup Completed

When the configuration has saved successfully, you should see the Setup is complete page. Continue to the next step when this screen is displayed.
Verify the Connector Activated

Back in the VMware Identity Manager Console,

1. Click the **Refresh** button in the browser.
2. Click **Identity & Access Management**.
3. Click **Setup**.
4. Click **Connectors**.
5. Confirm that the Connector now shows the Hostname as `conn-01a.corp.local` and the Worker named **Lab**.

This confirms that you have successfully setup and installed the VMware Identity Manager Windows Connector.
Sync Directory Users to VMware Identity Manager

This section will review how to add a new Directory in VMware Identity Manager and then sync users from our Active Directory into our VMware Identity Manager tenant.

Add an Active Directory over LDAP

In the VMware Identity Manager Administrator Console,

1. Click **Identity & Access Management**
2. Click **Directories**
3. Click **Add Directory**
4. Click **Add Active Directory over LDAP/IWA**

Configure the Directory Details

1. Enter `corp.local` for the Directory Name.
2. Select **Active Directory (Integrated Windows Authentication)**.
Configure the Directory Sync and Authentication Settings

1. Scroll down to find the Directory Sync and Authentication section.
2. Select the `conn-01a.corp.local` connector as the Sync Connector.
3. Select **Yes** to allow this Connector to perform authentication.
4. Select `sAMAccountName` for the Directory Search Attribute.

Configure the Bind User Details

1. Scroll down to find the Bind User Details section.
2. Enter `administrator@corp.local` for the Bind User UPN.
3. Enter `VMware1!` as the Bind DN Password.
4. Click **Save & Next**.
Select the Domains

1. Ensure the corp.local domain is selected.
2. Click Next.

Review the User Attribute Mappings

Review the User Attribute Mappings as desired, we won’t need to make any changes to the default mappings for this lab. Click Next.
Find Groups to Sync

Select the groups you want to sync

1. Click the Green Plus (+) button to add a new Group DN.
2. Enter `dc=corp,dc=local` for the group DN.
3. Click Find Groups.

Select the Groups to Sync

1. Click Select All to select all groups.
2. Click Next.
Select the Users to Sync

1. Click the Green Plus (+) button to add a new User DN.
2. Enter `cn=users,dc=corp,dc=local` for the user DN.
3. Click Next.

Review and Initiate Sync

Once the Review page loads and shows the number of Users and Groups being added, click Sync Directory.
Confirm Sync Started and Refresh to Check Status

1. Click the X to close the message confirming that the Sync has started.
2. Click Refresh Page to see if the Sync has completed.

**NOTE** - The sync may take a minute or two to complete. Keep clicking Refresh Page until the sync shows as completed with a green checkbox as shown in the next step.

Confirm the Sync Completes Successfully

Confirm that the **corp.local** directory shows synced groups, synced users, and that the Refresh Page notification is gone and replaced by a green checkbox to indicate the sync has completed.
### Confirm the Synced Users Exist

1. Click **Users & Groups**.
2. Confirm the **corp.local** users have synced and are displayed here.

This confirms that you have successfully added a directory to your VMware Identity Manager tenant and you were able to use your previously installed Connector to sync Active Directory users to the directory.
Setup an Identity Provider to use Password Cloud Deployment

This section will review how to configure the Built-In Identity Provider (IdP) to allow your corp.local domain users to provide their AD credentials to sign in to the VMware Identity Manager tenant.

Configure the Built-In Identity Provider

1. Click **Identity & Access Management**.
2. Click **Identity Providers**.
3. Click **Built-In**.

---

Click **Identity & Access Management**.

Click **Identity Providers**.

Click **Built-In**.
Configure the Identity Provider

1. Scroll down to find the Users, Network and Authentication Methods sections.
2. Click to enable the corp.local users.
3. Click to enable the ALL RANGES network range.

Associate Connector with Identity Provider

1. Scroll down to find the Connector(s) section.
2. Select conn-01a.corp.local from the list.
3. Click Add Connector.

**NOTE - If you don't see a list of available connectors, you may need to wait a few moments until the connectors are queried.**
1. Scroll down to the bottom.
2. Click the checkbox by Password (cloud deployment) for the Connector Authentication Methods to associate this authentication method with the Identity Provider.
3. Click Save.

Confirm the Identity Provider Was Created

The list of Identity Providers should now show your Built-In Identity Provider as having the Password (cloud deployment) authentication method for the corp.local directory and using the conn-01a.corp.local connector.
Configure the Access Policy

1. Click **Identity & Access Management**
2. Click **Policies**
3. Click **Edit Default Policy**

Add New Policy Rule

1. Click **Configuration**
2. Click **Add Policy Rule**
Configure Policy Rule Details

1. Select **ALL RANGES** for the network range.
2. Select **All Device Types** for the device type.
3. Type **Domain Users@corp.local** for the user group.
4. Click the **Domain Users@corp.local** result.

Configure the Authentication Method

1. Scroll down to the bottom.
2. Select **Authenticate using...** for the action.
3. Select **Password (cloud deployment)** for the authentication method.
4. Click **Save**.
Re-Order the Access Policy Rules

1. Click and drag the created policy rule, which has Any configured for the Device Type, to the top of the list.
2. Click **Next**.
Review and Save

Review as desired and click **Save**.

Your Policies and Identity Providers are now configured to authenticate your Domain Users@corp.local group using Password (cloud deployment) through your conn-01a.corp.local connector. Your tenant local users will continue to be authenticated with their default methods (Password and Password (Local Directory)) as we did not modify those policies.

**Verify that corp.local Users Can Login**

1. Click Options
2. Click New incognito window
3. Enter **https://{yourtenant}.vidmpreview.com** to navigate back to the login screen of your VMware Identity Manager tenant

*NOTE - Replace {yourtenant} with your tenant name!*
Login as aduser

1. Enter **aduser** for the username.
2. **Uncheck** Remember this setting.
3. Click **Next**.
Enter the Domain User's Password

1. Enter **VMware1!** for the password.
2. Notice that the domain shows as **corp.local**, verifying that aduser belongs to corp.local instead of the System Domain.
3. Click **Sign in**.
Open the Settings Page

1. Click the **User Dropdown**.
2. Click **Settings**.

Confirm the User Details

1. Click the **Account** tab.
2. Confirm the **Profile** for the user shows you've signed in as **aduser@corp.local**.
3. Click **Sign Out**.
This confirms that you have successfully allowed the Identity Provider to use the Connector we installed and configured earlier to use the Password (cloud deployment) authentication method to authenticate your Active Directory users.

Continue to the next steps to log back in as your local Administrator account.

**Close the Incognito Session**

Click the **Close** button in the top-right corner of the Incognito session to return to the VMware Identity Manager Administration Console.
Setup a Weblink Application and Entitle Users

This section will review how to create a Weblink Application and how to entitle your synced users to access the application.

Create a Weblink Application

In the VMware Identity Manager Administrator Console,

1. Click Catalog.
2. Click New.
Configure Weblink Application Definition

1. Enter **Workspace ONE UEM** for the Name.
2. Enter **Workspace ONE UEM Login Page** for the Description.
3. Click **Select File...** for the Icon.
Choose the Google.png File

1. Click **Documents**
2. Click **HOL**
3. Click **VMware Identity Manager**
4. Click **hol_logo.png**
5. Click **Open**
Complete Application Definition

Click **Next**.
1. Select **Web Application Link** as the Authentication Type.
2. Enter [https://labs.awmdm.com](https://labs.awmdm.com) for the Target URL.
3. Click **Next**.
Save and Assign

Review the configuration as desired and then click **Save & Assign**.
Entitle All Users to the Application

1. Enter **ALL USERS** in the Users / User Groups search bar.
2. Click the **ALL USERS** result.

Set the Deployment Type to Automatic

1. Select **Automatic** for the Deployment Type.
2. Click **Save**.

Selecting Automatic will place the application in the user's catalog.
Verify the Weblink Application

1. Click Options
2. Click New incognito window
3. Enter https://{yourtenant}.vidmpreview.com to navigate back to the login screen of your VMware Identity Manager tenant
   
   NOTE - Replace {yourtenant} with your tenant name!

Login as aduser

1. Enter aduser for the username.
2. Uncheck Remember this setting.
3. Click Next.
1. Enter **VMware1!** for the password
2. Notice that the domain shows as **corp.local**, verifying that aduser belongs to corp.local instead of the System Domain
3. Click **Sign in**
Open the Weblink Application

1. Click **Catalog**
2. Click **Open** for the Workspace ONE UEM Weblink Application
Confirm the Google Weblink Application Launches


This confirms that you were able to successfully create the Weblink Application, entitle it to your ALL USERS user group, and successfully launch the application for a user.
Close the Incognito Session

Click the **Close** button in the top-right corner of the Incognito session to return to the VMware Identity Manager Administration Console.
Setup Kerberos Authentication Adapter

This section will review how to configure Kerberos authentication through the IDM Connector to enable Windows Single Sign On.

Enable the Kerberos Authentication Adapter on the Connector

The setupKerberos.bat file that needs to be run to enable Kerberos Authentication for our VMware Identity Manager Connector is on the server where the VMware Identity Manager Connector service was installed, which was conn-01a.corp.local.

Double-click the conn-01a.rdp link on the Main Console Desktop to connect to the conn-01a server.
Run the setupKerberos.bat file

1. Click the File Explorer icon from the task bar.
2. Click Local Disk (C:).
3. Click VMware.
4. Click IDMConnector.
5. Click usr.
6. Click local.
7. Click horizon.
8. Click scripts.
9. Right-click the setupKerberos.bat file.
10. Click Run as Administrator.
Enter the User Credentials (IF NEEDED)

1. Enter **CORP\Administrator** for the Username.
2. Enter **VMware1!** for the Password.
3. After the PowerShell window closes and the process finishes, press any key to continue.

Return to the Main Console

After the setupKerberos.bat file has completed running, return to the Main Console in order to save the KerberosIdpAdapter.

Click the **Close (X)** button on the Remote Desktop Connector bar at the top of your screen.

*NOTE: If you do not see the Remote Desktop Connection bar, you may have un-pinned the bar. Hover your mouse over the top and center part of the screen to reveal it.*
Navigate to the Lab Connector

In the VMware Identity Manager Administration Console,

1. Click **Identity & Access Management**
2. Click **Setup**
3. Click **Connectors**
4. Click the **Lab** worker link

Navigate to the KerberosIdpAdapter

1. Click the **Auth Adapters** tab.
2. Click **KerberosIdpAdapter**.

**NOTE - The page may take several seconds to load after clicking the KerberosIdpAdapter link. Please be patient while it loads!**
Configure KerberosIdpAdapter Authentication Adapter

1. Enter **sAMAccountName** for the Directory UID Attribute.
2. **Check** Enable Windows Authentication.
3. Click **Save**.

**NOTE** - The KerberosIdpAdapter may take several minutes to save. Please do not navigate away from the page or refresh while this completes!
Confirm the KerberosIdpAdapter is Enabled

1. The KerberosIdpAdapter should now show as Enabled.
2. Click Admin Console to return.

Update the Policy Rules

1. Click Identity & Access Management
2. Click Manage
3. Click Policies
4. Click Edit Default Policy
Add Policy Rule

1. Click **Configuration**.
2. Click **Add Policy Rule**.

Configure Policy Rule Details

1. Select **ALL RANGES** for the Network Range.
2. Select **Windows 10** for the Device Type.
Configure Policy Rule Authentication

1. Scroll down to the bottom.
2. Select **Authenticate using...** for the action.
3. Select **Kerberos** for the authentication action.
4. Select **Password (cloud deployment)** for the fallback authentication action.
5. Click **Save**.

Update the Policy Rule Order

1. Select the policy rule to be updated.
2. Click **Next** to proceed.
1. Click and drag the created **Windows 10** policy rule to the top of the list.
2. Click **Next**.

**Review and Save the Policy Rule Changes**

![Configuration screenshot](image)

Review the configuration as desired and click **Save**.

You have now configured your Policies to authenticate all Windows 10 Devices using Kerberos and failover to Password (cloud deployment) if Kerberos isn't applicable or fails.

**Authenticate with Kerberos using the Workspace ONE App**

![Win10-01a.rdp shortcut](image)

From the Desktop, double-click the **Win10-01a.rdp** shortcut.
Use the Workspace ONE App to Connect To Your Tenant

1. Click the **Workspace ONE App** from the task bar.
2. Enter **https://{yourtenant}.vidmpreview.com** for the URL.
   
   **NOTE - Replace** `{yourtenant}` **with your actual tenant name that you accessed in previous steps!**
3. Click **Continue**.
Select the corp.local Domain

1. Select corp.local for the Domain.
2. Click Next.

Enter Workspace

Click Enter after the workspace finishes building.
Confirm User Details

Notice that you were authenticated via Kerberos without having to enter any additional credentials.

1. Click the **User** icon.
2. Click the **Account** tab.
3. Confirm that the User details show that we successfully signed in as holuser@corp.local. This is the user account that is signed in to the Windows 10 virtual machine you have connected to.

This confirms that we were able to successfully enable Kerberos authentication for our Connector, configure our Policy Rules to authenticate our Windows 10 users via Kerberos, and then authenticate using Windows Authentication via Kerberos from our Windows 10 device by leveraging the Workspace ONE application.

**Return to the Main Console**

Click the X on the Remote Desktop session at the top of your screen to return to the Main Console.
Setup RADIUS Authentication

This section will detail how to install and configure a RADIUS server and client for Windows, and how to integrate RADIUS with IDM by enabling the RADIUS Cloud Deployment authentication method.

Connect to the Conn-01a Server

You will configure the RADIUS server and client on the conn-01a.corp.local server for this exercise.

Double-click the conn-01a.rdp link on the Desktop to connect to the Conn-01a Server.
1. Click **Server Manager** from the task bar.
2. Click **Manage**.
3. Click **Add Roles and Features**.
Enable Network Policy and Access Services

1. Click **Server Selection**.
2. Click **Server Roles**.
3. You may need to scroll down to find Network Policy and Access Services.
4. Click the checkbox to enable **Network Policy and Access Services**.
Add Features for Network Policy and Access Services

Click **Add Features**.
Install the New Roles and Features

1. Click **Confirmation**.
2. Click **Install**.

Wait for the installation to complete. This may take several minutes to complete.
Close the Installation Window

1. Ensure the Feature Installation shows the **installation succeeded**.
2. Click **Close**.
Configure Network Policy Server

Within Server Manager,

1. Click **Tools**.
2. Click **Network Policy Server**.

Register Network Policy Server in Active Directory

1. Click **Action**.
2. Click **Register server in Active Directory**.

**Authorize to Read User's Dial-In Properties**

1. Click **OK** to authorize this computer to read user's dial-in properties.
2. Click **OK** to confirm that the computer is not authorized.

**Add a new RADIUS Client**
1. Click the caret next to RADIUS Clients and Servers to expand the folder.
2. Right-click **RADIUS Clients**.
3. Click **New**.

**Configure the RADIUS Client**

![New RADIUS Client dialog box](image)

1. Enter `conn-01a.corp.local` for the Friendly Name.
2. Enter `conn-01a.corp.local` for the Address (IP or DNS).
3. Enter `VMware1!` for the Shared Secret.
4. Enter `VMware1!` for the Confirm Shared Secret.
5. Click **OK**.
Add a New Network Policy

1. Click the caret next to Policies to expand it.
2. Right-click Network Policies.
3. Click New.
Configure Policy Name and Connection Type

1. Enter **IDM Authentication** for the Policy name.
2. Select **Unspecified** for the Type of Network access server.
3. Click **Next**.
Add Conditions

Click **Add**.
Add a User Groups Condition

1. Click **User Groups**.
2. Click **Add**.

**Add Groups**

Click **Add Groups**.
Select the Domain Users Group

1. Enter **Domain Users** into the search field.
2. Click **Check Names**. Ensure the Domain Users group is found.
3. Click **OK**.

Confirm User Groups

Click **OK**.
Continue after specifying User Groups Condition

Click **Next**.
Specify Access Granted Permission

1. Select **Access Granted**.
2. Click **Next**.
Configure Authentication Methods

1. Under the Less secure authentication methods, ensure that **ALL of the options are checked EXCEPT for Perform machine health check only.**
2. Click **Next**.
Close Help Popup

Click **No**.

Accept the Default Constraints
Click **Next** to accept the default Constraints.

**Accept the Default Settings**

Click **Next** to accept the default Settings.
Complete the New Network Policy

Click Finish.

Return to the Main Console

With the RADIUS client configured, you will configure the remainder of the requirements from the Main Console.

Click the Close (X) button on the Remote Desktop Connector bar at the top of your screen.
NOTE: If you do not see the Remote Desktop Connection bar, you may have un-pinned the bar. Hover your mouse over the top and center part of the screen to reveal it.

Configure the RADIUS Authentication Method for VMware Identity Manager

In the VMware Identity Manager Administration Console,

1. Click **Identity & Access Management**
2. Click **Setup**
3. Click **Connectors**
4. Click **Lab**
Select the RADIUSAuthAdapter

1. Click the Auth Adapters tab.
2. You may need to scroll down.
3. Click the RADIUSAuthAdapter link.
Configure the RADIUSAuthAdapter Details

1. Click to enable the Enable RADIUS Adapter option.
2. Enter 5 for the Number of attempts to RADIUS server.
3. Enter 20 for the Server timeout in seconds.
4. Enter conn-01a.corp.local for the RADIUS server hostname/address.
5. Select MSCHAPv2 for the Authentication type.
6. Enter VMware!! for the Shared secret.
Save the RADIUSAuthAdapter

1. Scroll down to the bottom.
2. Click **Save**.
Return to the VMware Identity Manager Admin Console

1. Confirm the **RADIUSAuthAdapter** shows as **Enabled**.
2. Click **Admin Console**.

Configure the Identity Providers

1. Click **Identity & Access Management**
2. Click **Identity Providers**
3. Click **Built-In**
**Associate the RADIUS Authentication Method**

1. Scroll down to the bottom.
2. Click to **enable** the RADIUS (cloud deployment) authentication method for this Identity Provider.
3. Click **Save**.

**Configure the Policy Rules**

1. Click **Identity & Access Management**.
2. Click **Policies**.
3. Click **Edit Default Policy**.

1. Click **Identity & Access Management**.
2. Click **Policies**.
3. Click **Edit Default Policy**.
Add Policy Rule

1. Click **Configuration**.
2. Click **Add Policy Rule**.

Configure Policy Rule

- If a user's network range is **ALL RANGES**.
- and user accessing content from **Web Browser**.
- and user belongs to group(s) **Select Groups**.
- Then perform this action **Authenticate using...**.
- then the user may authenticate using **RADIUS (cloud deployment)**.
- If the preceding method fails or is not applicable, then **Password (cloud deployment)**.

Add fallback method
1. Select **ALL RANGES** for the Network Range.
2. Select **Web Browser** for the Device type.
3. Select **Authenticate using...** for the action.
4. Select **RADIUS (cloud deployment)** for the authentication type.
5. Select **Password (cloud deployment)** for the fallback authentication type.

**Save the Policy Rule**

1. Scroll down to the bottom.
2. Click **Save**.

**Move the Policy Rule to the Top**

1. Drag the policy rule to the top of the list.
2. Click **Next**.
1. Move the Policy Rule for the RADIUS (cloud deployment) authentication to the top.
2. Click Next.

**Review and Save**

![Configuration screenshot](image)

Review the configuration as desired and click Save.

**Test RADIUS Authentication from a Web Browser**

1. Click Options
2. Click New incognito window
3. Enter `https://{yourtenant}.vidmpreview.com` to navigate back to the login screen of your VMware Identity Manager tenant

*NOTE - Replace `{yourtenant}` with your tenant name!*
Navigate to the Identity Manager Tenant

1. Select corp.local for the Domain.
2. Click Next.
Authenticate using RADIUS

1. Notice we are being prompted to authenticate with our RADIUS passcode.
2. Enter **aduser** for the username.
3. Enter **VMware1!** for the RADIUS Passcode.
4. Click **Sign In**.
Navigate to the User Settings

1. Click the User dropdown.
2. Click Settings.

Confirm RADIUS Authentication was Successful

1. Confirm the User Profile shows as aduser@corp.local.
2. Click the X to close the incognito browsing session and return to the VMware Identity Manager Administration Console.

This confirms that we were able to successfully install and configure our RADIUS Server on the Windows server, and then enabled and configured our RADIUS authentication.
method and Policy Rules to allow our users to authenticate using their RADIUS passcode when accessing the tenant from a Web Browser.
Instructions for Taking Additional Lab Modules

If you are interested in taking additional modules for this lab, please click the END button in the VMware Learning Platform and then relaunch the lab.

Since each module in this lab takes advantage of configuring VMware Identity Manager and the VMware Identity Manager Connector for different use cases, the quickest way to start with a clean infrastructure to complete the next module is to restart the lab. Once you restart, navigate to the next module using the Table of Contents as shown in the Lab Guidance section.
Conclusion

In this exercise, you learned how to:

- Install and Configure the VMware Identity Manager Connector
- Sync Users and Groups to VMware Identity Manager using the VMware Identity Manager Connector
- Configure various Authentication Methods for the VMware Identity Manager Connector for user authentication, including Active Directory Password, Kerberos and RADIUS.

This first look into installing, configuring and managing VMware Identity Manager showcases the flexibility and customization you have for creating access policies based on the needs of your enterprise. Your Identity Providers and Access Policies can be setup to allow your users to authenticate in ways they are familiar with, without needing to spend time re-building these authentication policies from the ground up.

Be sure to check out the additional VMware Identity Manager exercises for additional learning and authentication possibilities.
Module 2 - On-Premises Install for VMware Identity Manager
Introduction

VMware Identity Manager is the identity component of VMware Workspace ONE. This service is available as both a SaaS (Software as a Service) or on-premise service. The on-premise distribution can be deployed as either a Linux based OVA or installed on a Windows server.

This hands-on lab will walk you through the installation of the VMware Identity Manager service on a Windows server, as well as the integration of it to an on-premises Active Directory environment for user sync and authentication.

This exercise will follow an architecture in which the different components of VMware Identity Manager are distributed across separate dedicated Windows servers. This allows for a more flexible architecture, in which the main VMware Identity Manager service is placed in a public facing DMZ, while the Active Directory connector and SQL database are maintained within the internal network.

A reference architecture of the VMware Identity Manager service and other service in the Workspace ONE platform can be found in the VMware TechZone: https://techzone.vmware.com/resource/vmware-workspace-one-and-vmware-horizon-7-enterprise-edition-premises-reference
Lab Architecture

We have simplified the architecture to limit the scope for this lab. Let's take a look at what are the different components involved.

Components and sub-systems

Main Console (192.168.110.10)

- Windows 2012R2 Server for Active Directory (AD), Domain Name System (DNS), and Certificate Authority (CA).

vidm-01a (192.168.110.14)

- Windows 2012R2 Server for hosting the VMware Identity Manager service. This server will communicate with the sql-01a server where the VMware Identity Manager database will be installed.
- Not joined to corp.local domain.

conn-01a (192.168.110.15)

- Windows 2012R2 Server for hosting the VMware Identity Manager Connector. This server will be responsible for using a domain service account to sync users and groups and provide authentication methods that require a domain joined account, such as Kerberos.
- Joined to corp.local domain.
sql-01a (192.168.110.13)

- Windows 2012R2 Server for hosting the SQL database which will be utilized by the VMware Identity Manager service installed on vidm-01a.
- Joined to corp.local domain.

**Use Case and Requirements**

For this exercise, the following use cases apply:

- Utilize the VMware Identity Manager Connector for syncing Active Directory users and groups to VMware Identity Manager
- Utilize the VMware Identity Manager Connector domain joined service account to perform Kerberos Authentication for Windows 10 devices

For these use cases, the following requirements and decisions are made:

- **The VMware Identity Manager service IS NOT required to be domain joined**: The VMware Identity Manager Connector will be domain joined and will handle syncing users and authentication.
- **The VMware Identity Manager Connector IS domain joined**: Since we are relying on the Connector to sync users from Active Directory and handle authentication, the Connector server will be domain joined.

The benefits of this setup are:

- **Reduced Firewall Requirements**: The VMware Identity Manager service can sit in your DMZ while the VMware Identity Manager Connector can be installed on the intranet in outbound-only mode, not requiring inbound port 443 to be opened to provide secure Active Directory user-sync and authentication for your external users.
- **Eliminate Domain Joined Servers in DMZ**: The VMware Identity Manager service can remain unjoined while relying on the VMware Identity Manager Connector to handle user-sync and authentication.
Create VMware Identity Manager SQL Database

In this exercise, we are going to create a SQL Database for VMware Identity Manager. During the VMware Identity Manager installation process, we will be referencing this database as the target database.

Copy the CreateVidmDb Script

1. Click the File Explorer icon from the taskbar
2. Click Documents
3. Click HOL
4. Click VMware Identity Manager
5. Right-Click CreateVidmDb.txt
6. Click **Edit with Notepad++**

**Copy the CreateVidmDb Contents**

1. Right-click within the CreateVidmDb.txt text field and click **Select All**
2. Right-click within the CreateVidmDb.txt text field and click **Copy**

**Run the CreateVidmDb Script**

From the Desktop, double-click **SQL Server 2014 Management Studio**
Connect to the SQL Database Engine

1. Enter `sql-01a.corp.local` for the Server name.
2. Select **Windows Authentication**.
3. Click **Connect**.

Create a New Query

1. Click **Databases**.
2. Click **New Query**.
1. Ensure that the database selected is master.
2. Right click in the area for New Query.
3. Click Paste.

Execute the Create DB Script

Once the script is pasted, click on Execute to run the script.

These commands are accomplishing the following tasks:

1. Creating the vidmdb database.
2. Setting the necessary collation and configurations for the vidmdb database.
3. Creating a user (vidmuser) with a password (VMware1!).
4. Assigning the vidmuser the appropriate roles for the vidmdb database.
Refresh the Database List

1. Right-click the `sql-01a.corp.local` server.
2. Click Refresh.

Validate that the `vidmdb` Database Was Created

1. Expand Databases.
2. Confirm the `vidmdb` Database exists.
Install the VMware Identity Manager Service

In this exercise, we are going to run the VMware Identity Manager service application installer to install the VMware Identity Manager service. As discussed in the introduction, we have a dedicated server, vidm-01a.corp.local, setup to host the VMware Identity Manager service and will be installing the service on that server.

Connect to VIDM-01 RPD

From the Desktop, click the vidm-01a.rdp shortcut.
1. Click the **File Explorer icon** from the taskbar on the vidm-01a.corp.local server.
2. Click **Documents**.
3. Click **HOL**.
4. Right-click the **VMware_Identity_Manager_3.2.0.1_Full_Install.exe** file.
5. Click **Run as administrator**.
Complete the VMware Identity Manager Service Install

Click **Next**.

**NOTE:** It might take a **couple of minutes** for the installer to load.
Accept License Agreement

1. Check the **I accept the terms in the license agreement** button.
2. Click **Next**.
Continue Without Participating in the CEIP

The Customer Experience Improvement Program (CEIP) uses non-personally identifiable information to improve products and services. For the purposes of this exercise, you will opt-out of the program.

1. Select No.
2. Click Next.

The Customer Experience Improvement Program (CEIP) uses non-personally identifiable information to improve products and services. For the purposes of this exercise, you will opt-out of the program.
Installation Wizard Prerequisites

Click **Next**.

The installation wizard will automatically install the missing software prerequisites. For the purposes of this exercise, the prerequisites have already been installed for you to reduce the installation time.

**NOTE:** It is not recommended to pre-install Java 8 and to instead allow the installer to install the recommended Java 8 version.
Destination Folder

We will install this on the default destination folder `C:\VMware`.

Click **Next**
Click **Next** to continue without joining an existing VMware Identity Manager cluster.

**NOTE:** If you were configuring an additional VMware Identity Manager instance to provide high availability or to load balance existing traffic, you would provide your cluster configuration package at this step.
Provide the Hostname

1. Enter `vidm-01a.corp.local` for the Hostname.  
   **NOTE:** The Hostname should always be provided as the fully qualified domain name (FQDN).  
   **NOTE:** The provided hostname is the hostname of the vidm-01a server that you are currently connected to.  
2. Click **Next**.
VMware Identity Manager Database Server

1. Enter `sql-01a.corp.local` as the VMware Identity Manager Database server.
2. Select **SQL Server authentication using Login ID and password below**.
3. Enter `vidmuser` as the Login ID.
4. Enter `VMware1!` as the Password.
5. Click on **Browse**.

Remember that during our vidmdb database setup earlier, our script created the `vidmuser` user with the `VMware1!` password for use with the vidmdb database. This is why we choose to use these credentials here in order to authenticate to the vidmdb in the following steps.

**NOTE:** After clicking Browse, it may take 30 - 60 seconds to populate the list of databases.
Select VIDMDB

1. Select the **vidmdb** database.
2. Click **OK**.
Click **Next**.
VMware Identity Manager Service Account Information

1. **Uncheck** the option for **Would you like to run the VMware Identity Manager server as a domain user account.**
2. Click **Next**.

As mentioned in the introduction, this setup will not utilize a domain user account for the VMware Identity Manager service since the server is not domain joined. Instead, you will configure the VMware Identity Manager Connector in a later step to use a domain user account for Active Directory user sync and authentication.
Confirm User Account Question

![Image of VMware Identity Manager Installation Wizard]

Click Yes.

As noted, Integrated Windows Authentication (IWA) and Kerberos authentication require a domain user account for authentication. In this setup, you are electing that these authentication methods will be unavailable to your VMware Identity Manager service. However, you will configure the setup to authenticate users with the VMware Identity Manager Connector rather than the VMware Identity Manager service in later steps.

If you wished to authenticate your users using IWA or Kerberos from your VMware Identity Manager service without using the VMware Identity Manager Connector or without running the VMware Identity Manager Connector with a domain user account, you would need to supply a domain user account for the VMware Identity Manager service instead.
Begin the Installation

Click **Install** to begin the installation of the VMware Identity Manager service.

**NOTE:** The installation may take around 8 - 10 minutes to fully complete, please be patient while the installer finishes.
Install Completed

Click **Finish** to close the install wizard.
Open the VMware Identity Manager Setup Wizard

When prompted, click **Yes** to open the VMware Identity Manager Setup Wizard at https://vidm-01a.corp.local:8443/cfg.
Complete the VMware Identity Manager Setup Wizard

1. Click Advanced.
2. Click Proceed to vidm-01a.corp.local (unsafe).

Why are you seeing an invalid certificate error? If you recall, we do not provide a SSL certificate as part of the VMware Identity Manager Service installer. You will be uploading the SSL certificate after the Setup Wizard, which you are accessing now.
Setup the Appliance Administrator Password

1. Enter **VMware1!** for the password.
2. Enter **VMware1!** to confirm the password.
3. Click **Continue**.
Setup the Database Connection

1. Enter \texttt{VMware1!} for the database password. This is the password for the vidmuser connecting to our vidmdb database.
2. Click \texttt{Continue}.
Confirm Setup Completed Successfully

After a few minutes, you should see the Setup is Complete screen. Click **Log in to the administration console**.

**NOTE:** DO NOT manually refresh or navigate away from the page during the final setup. You will be automatically re-directed to the page when the setup is completed.
Perform Initial Configuration in the Administration Console

1. Enter admin for the username.
2. Enter VMware1! for the password.
3. Click Sign in.

These credentials are for the Appliance Administrator you configured in the previous steps during the Setup Wizard.
Open System Configuration

1. Click **Appliance Settings**.
2. Click **Manage Configuration**.
Open the Certificate Chain Text File

1. Click the File Explorer icon from the taskbar of the vidm-01a.corp.local server.
2. Click Documents.
3. Click HOL.
4. Double-click the wildcard_corp_local.txt file to open it in Notepad.
Copy the Certificate Chain

Copy the full Certificate Chain text. This will be used to paste into the VMware Identity Manager system configuration.

1. Click **Edit**.
2. Click **Select All**.
3. Click **Edit**.
4. Click **Copy**.
Update the SSL Certificate Chain for the VMware Identity Manager Server Certificate

1. Click the **Install SSL Certificate** tab.
2. Click the **Server Certificate** tab.
3. Select Custom Certificate for the SSL Certificate.
4. Right-click inside the SSL Certificate Chain textbox and click **Select All**.
5. Right-click inside the SSL Certificate Chain textbox and click **Paste**.

This will replace the existing SSL Certificate Chain with the one you copied in the previous step. The SSL Certificate Chain you copied is comprised of a wildcard corp.local certificate and the root certificate used for this exercise.

Return to the System Configuration page for VMware Identity Manager in Google Chrome.

1. Click the **Install SSL Certificate** tab.
2. Click the **Server Certificate** tab.
3. Select Custom Certificate for the SSL Certificate.
4. Right-click inside the SSL Certificate Chain textbox and click **Select All**.
5. Right-click inside the SSL Certificate Chain textbox and click **Paste**.

This will replace the existing SSL Certificate Chain with the one you copied in the previous step. The SSL Certificate Chain you copied is comprised of a wildcard corp.local certificate and the root certificate used for this exercise.
Open the Private Key Text File

1. Click the File Explorer icon from the taskbar of the vidm-01a.corp.local server.
2. Click Documents.
3. Click HOL.
4. Double-click the wildcard_corp_local_key.txt file to open it in Notepad.
Copy the Private Key

Copy the full Private Key text. This will be used to paste into the VMware Identity Manager system configuration.

1. Click **Edit**.
2. Click **Select All**.
3. Click **Edit**.
4. Click **Copy**.
Update the Private Key

Return to the System Configuration page for VMware Identity Manager in Google Chrome.

1. Scroll down to find the Private Key textbox.
2. Right-click inside the Private Key textbox and click Select All.
3. Right-click inside the Private Key textbox and click Paste.
4. Click Add.

This will replace the existing Private Key with the one you copied in the previous step. The Private Key you copied is comprised of a wildcard corp.local private key paired with the SSL Certificate used in this exercise.

Confirm Identity Manager Service Restart

Click OK to confirm that updating the certificate will cause the Identity Manager Service to restart.
Wait for the Server to Restart

You will see a loading screen while the certificate installs and the server restarts. Please wait until this has completed before continuing.

**NOTE:** This process may take 10 - 12 minutes to complete.

Once the server has restarted, you will have provided your own SSL certificate chain and private key. This concludes the initial configuration of your newly installed VMware Identity Manager service, additional steps will be taken from the Main Console where you will validate that the certificate error is no longer shown.

**NOTE:** When the process finishes, you will return to the Server Certificate tab of the System Configuration screen.

Return to the Main Console

You will return to the Main Console to complete additional exercises. Click the **Close (X)** button on the Remote Desktop Connection bar at the top of your screen.
Navigate to the VMware Identity Manager Admin Console

Double-click the Chrome Browser on the lab desktop.

1. Click **Options**.
2. Click **New tab**.
3. Enter `https://vidm-01a.corp.local` and press **ENTER**.

Remember that you installed the VMware Identity Manager service with the hostname as vidm-01a.corp.local. This is where your users will navigate to in order to access to administration console.
Login to the VMware Identity Manager Administration Console

1. Enter **admin** for the Username.
2. Enter **VMware1!** for the Password.
3. Click **Sign in**.

These are the administrator credentials you created during the VMware Identity Manager service installation.
If the VMware Identity Manager Administration Console loads as shown above, then you were able to authenticate successfully. You will be returning to the Administration Console in later steps for additional configuration.
Install the VMware Identity Manager Connector

The VMware Identity Manager Connector will be responsible for integrating VMware Identity Manager with the on-premises Active Directory. This exercise will guide you through install the VMware Identity Manager Connector with the proper configurations to meet the use case and requirements we discussed in the introduction.

Connect to the Conn-01a Server

Double-click the conn-01a.rdp link on the Desktop to connect to the Conn-01a Server.

You will be installing the VMware Identity Manager Connector on the designated server. It is recommended to install the VMware Identity Manager Connector on a dedicated server or Virtual Machine (VM).

Start the Computer Browser Service

Click the Windows Start Button from the task bar of the conn-01a Server.
Open Services

1. Start typing `Services` to search.
2. Click on the `Services` result.
Open the Computer Browser Properties

1. Right-click the **Computer Browser** service.
2. Click **Properties**.
Start the Computer Browser Service

1. Select **Automatic** for the Startup type.
2. Click **Apply**.
3. Click **Start**.
4. Click **Close**.

The Browser service or Computer Browser Service is a feature of Microsoft Windows to let users easily browse and locate shared resources in neighboring computers. This allows the installer to discover and aggregate the domains that are available for authentication within the network.
Ensure the Computer Browser Service is Running

1. Confirm that the **Computer Browser** status shows as **Running**.
2. Click **Close**.
Enable NetBIOS over TCP/IP

1. Right-click the **Network** icon.
2. Click **Open Network and Sharing Center**.
3. Click **Ethernet0 2** from the Network and Sharing Center.
Open the IPv4 Properties

1. Click **Properties** for the Ethernet0 2 Status.
2. Click **Internet Protocol Version 4 (TCP/IPv4)** to select it.
3. Click **Properties**.
Enable NetBIOS over TCP/IP

1. Click Advanced.
2. Click the WINS tab.
3. Select Enable NetBIOS over TCP/IP.
4. Click OK.
Start the VMware Enterprise Systems Connector Installer

1. Click the **File Explorer icon** from the taskbar.
2. Click **Documents**.
3. Click **HOL**.
4. Right-click the **VMware Enterprise Systems Connector Installer.exe** file.
5. Click **Run as Administrator**.

1. Click the **File Explorer icon** from the taskbar.
2. Click **Documents**.
3. Click **HOL**.
4. Right-click the **VMware Enterprise Systems Connector Installer.exe** file.
5. Click **Run as Administrator**.
Confirm Security Warning and Run

Click **Run**.

*NOTE - The Installer may take a minute or two to start after clicking run.*

Start the VMware Enterprise Systems Connector Installer
Click **Next**.

**Accept the License Agreement Terms**

1. Select **I accept the terms in the license agreement**.
2. Click **Next**.
Disable the AirWatch Cloud Connector Feature

1. Click the dropdown by the AirWatch Cloud Connector component.
2. Click This feature will not be available.

Enable the VMware Identity Manager Connector Feature
1. Click the dropdown by the **VMware Identity Manager Connector** component.
2. Click **This feature will be installed on local hard drive.**

**Accept the Default Destination Folder**

![Destination Folder dialog box](image)

Click **Next** to accept the default destination folder of C:\VMware\
Configure the SSL Certificate

1. Check the **Would you like to use your own SSL Certificate?** option
2. Click **Browse...**
Browse to the Connector SSL Certificate

1. Click **Documents**
2. Click **HOL**
3. Click **conn-01a**
4. Click **Open**
Enter SSL Certificate Password

1. Enter **VMware1!** for the Certificate Password
2. Click **Next**

Continue without Activating the Connector

1. Click **[ ] No**
2. Click **Next**
1. Select No for Would you like to activate the Connector now
2. Click Next

In this lab, we are only interested in installing the VMware Identity Manager Connector at this point. We will activate the Connector later once we have setup the Connector in our VMware Identity Manager Admin Console and have access to the Activation Code. As stated by the installer, this can be updated later by accessing the Connector settings at \[https://\{hostname\}:8443\], which will be \[https://conn-01a.corp.local:8443\].

**Setup the Service Account Configuration**

![VMware Enterprise Systems Connector - Installation Wizard]

1. Ensure the Would you like to run the Connector service as a domain user account option is enabled.
2. Enter corp\administrator for the User name.
3. Enter VMware1! for the Password.
4. Click Next.
Start the Install Process

Click **Install**.

*NOTE - The Installer may take a few minutes to complete. Please be patient while the service installs.*
Close the VMware Enterprise Systems Connector After It Completes

Click Finish.

Return to the Main Console

With the VMware Identity Manager Connector installed, you will configure the remainder of the requirements for this exercise from the Main Console.

Click the Close (X) button on the Remote Desktop Connector bar at the top of your screen.

NOTE: If you do not see the Remote Desktop Connection bar, you may have un-pinned the bar. Hover your mouse over the top and center part of the screen to reveal it.
Activate the VMware Identity Manager Connector

In the previous exercise, we completed the installation of the VMware Identity Manager Connector, but we did not activate the Connector yet. In this exercise, you will activate and register the VMware Identity Manager Connector from the VMware Identity Manager Administration Console.

Add a Connector

Return to Google Chrome. In the VMware Identity Manager Administrator Console,

1. Click **Identity & Access Management**.
2. Click **Setup**.
3. Click **Connectors**.
4. Click **Add Connector**.
Generate the Connector Activation Code

1. Enter **Lab** for the Connector ID Name.
2. Click **Generate Activation Code**.

Copy the Connector Activation Code

1. Double-click the **Connector Activation Code** textbox to select the code.
2. **Right-click** and click **Copy**.
3. Click **OK**.
Activate the Connector

To activate the VMware Identity Manager Connector, you can connect to the hostname over port 8443 where the VMware Identity Manager Connector service was installed. You installed the VMware Identity Manager Connector service on conn-01a.corp.local in earlier steps.

1. Click the **Options** button
2. Click **New Tab**

Create the Administrator Account Credentials

First you will configure the Appliance Administrator Account (admin) for future logins:

1. Enter **VMware1!** for the Password
2. Enter **VMware1!** to confirm the password
3. Click **Continue**
Paste the Activation Code

1. Right-Click inside the Activation Code textbox and click Paste to paste the Activation Code we copied from the previous step when creating the "Lab" Connector from the VMware Identity Manager Console
2. Click Continue

NOTE - While the page loads and refreshes, DO NOT close or manually refresh the page until you see the Setup is Complete screen shown in the next step!
Confirm the Setup Completed

When the configuration has saved successfully, you should see the Setup is complete page. Continue to the next step when this screen is displayed.
Verify the Connector Activated

Back in the VMware Identity Manager Console,

1. Click the **Refresh** button in the browser.
2. Click **Identity & Access Management**.
3. Click **Setup**.
4. Click **Connectors**.
5. Confirm that the Connector now shows the Hostname as **conn-01a.corp.local** and the Worker named **Lab**.

This confirms that you have successfully setup and installed the VMware Identity Manager Windows Connector.
Sync Directory Users to VMware Identity Manager

This section will review how to add a new Directory in VMware Identity Manager and then sync users from our Active Directory into our VMware Identity Manager tenant.

Add an Active Directory over LDAP

In the VMware Identity Manager Administrator Console,

1. Click Identity & Access Management
2. Click Directories
3. Click Add Directory
4. Click Add Active Directory over LDAP/IWA

Configure the Directory Details

1. Enter corp.local for the Directory Name.
Configure the Directory Sync and Authentication Settings

1. Scroll down to find the Directory Sync and Authentication section.
2. Select the **conn-01a.corp.local** connector as the Sync Connector.
3. Select **Yes** to allow this Connector to perform authentication.
4. Select **sAMAccountName** for the Directory Search Attribute.

Configure the Bind User Details

1. Scroll down to find the Bind User Details section.
2. Enter **administrator@corp.local** for the Bind User UPN.
3. Enter **VMware1!** as the Bind DN Password.
4. Click **Save & Next**.
Select the Domains

1. Ensure the **corp.local** domain is **selected**.
2. Click **Next**.

Review the User Attribute Mappings

Review the User Attribute Mappings as desired, we won't need to make any changes to the default mappings for this lab. Click **Next**.
Find Groups to Sync

Select the groups you want to sync

1. Click the **Green Plus (**) button to add a new Group DN.
2. Enter `dc=corp,dc=local` for the group DN.
3. Click **Find Groups**.

Select the Groups to Sync

Select the groups you want to sync

Enter the Group DNs to sync, for example, `CN=users,DC=example,DC=company,DC=com`. Select the Active Directory groups that you want to sync to the directory. When you select a group, the group names are synced immediately. Memberships of these groups will be synced when the group is entitled to a resource.

1. Click **Select All** to select all groups.
2. Click **Next**.
Select the Users to Sync

1. Click the **Green Plus (+) button** to add a new User DN.
2. Enter `cn=users,dc=corp,dc=local` for the user DN.
3. Click **Next**.

Review and Initiate Sync

Once the Review page loads and shows the number of Users and Groups being added, click **Sync Directory**.
1. Click the X to close the message confirming that the sync has started.
2. Click Refresh Page to see if the sync has completed.

**NOTE - The sync may take a minute or two to complete. Keep clicking Refresh Page until the sync shows as completed with a green checkbox as shown in the next step.**

**Confirm the Sync Completes Successfully**

Confirm that the corp.local directory shows synced groups, synced users, and that the Refresh Page notification is gone and replaced by a green checkbox to indicate the sync has completed.
Confirm the Synced Users Exist

1. Click **Users & Groups**.
2. Confirm the **corp.local** users have synced and are displayed here.

This confirms that you have successfully added a directory to your VMware Identity Manager tenant and were able to use your previously installed Connector to sync Active Directory users to the directory.
Login as a Domain User

Now that you have successfully synced your corp.local domain users to VMware Identity Manager by using the VMware Identity Manager Connector, you will confirm that you are able to authenticate to the VMware Identity Manager Console by providing credentials for a corp.local domain user.

Verify that corp.local Users Can Login

1. Click Options
2. Click New incognito window
3. Enter [https://vidm-01a.corp.local](https://vidm-01a.corp.local) to navigate back to the login screen of your VMware Identity Manager Console.
Select the Corp.Local Domain

1. Select the **corp.local** domain.
2. Uncheck the **Remember this setting** option.
3. Click **Next**.
Login as aduser

1. Enter **aduser** for the username.
2. Enter **VMware1!** for the password.
3. Click **Sign in**.
Open the Settings Page

1. Click the **User Dropdown**.
2. Click **Settings**.

Confirm the User Details

1. Click the **Account** tab.
2. Confirm the **Profile** for the user shows you've signed in as **aduser@corp.local**.
3. Click **Sign Out**.
This confirms that you have successfully authenticated as a corp.local domain user for your VMware Identity Manager Console.

**Close the Incognito Session**

Click the **Close** button in the top-right corner of the Incognito session to return to the VMware Identity Manager Administration Console.
Setup Kerberos Authentication Adapter

This section will review how to configure Kerberos authentication through the IDM Connector to enable Windows Single Sign On.

Setup Kerberos Authentication using the Batch File

The setupKerberos.bat file that needs to be run is on the server where the VMware Identity Manager Connector service was installed, which was conn-01a.corp.local.

Double-click the conn-01a.rdp link on the Desktop to connect to the conn-01a server.
Run the `setupKerberos.bat` file

1. Click the **File Explorer** icon from the task bar.
2. Click **Local Disk (C:)**.
3. Click **VMware**.
4. Click **IDMConnector**.
5. Click **usr**.
6. Click **local**.
7. Click **horizon**.
8. Click **scripts**.
9. Right-click the `setupKerberos.bat` file.
10. Click **Run as Administrator**.
Enter the User Credentials (IF NEEDED)

1. Enter "corp\administrator" for the Username.
2. Enter "VMware1!" for the Password.
3. After the PowerShell window closes and the process finishes, press any key to continue.

Return to the Main Console

After the setupKerberos.bat file has completed running, return to the Main Console in order to save the KerberosIdpAdapter.

Click the Close (X) button on the Remote Desktop Connector bar at the top of your screen.

NOTE: If you do not see the Remote Desktop Connection bar, you may have un-pinned the bar. Hover your mouse over the top and center part of the screen to reveal it.
Enable the Kerberos Authentication Adapter on the Connector

In the VMware Identity Manager Administration Console,

1. Click **Identity & Access Management**
2. Click **Setup**
3. Click **Connectors**
4. Click the **Lab** worker link

Navigate to the KerberosIdpAdapter

1. Click the **Auth Adapters** tab.
2. Click **KerberosIdpAdapter**.
NOTE - The page may take several seconds to load after clicking the KerberosIdpAdapter link. Please be patient while it loads!

Allow Auth Adapter Popup (IF NEEDED)

If the Auth Adapter pop-up does not load and the pop-up shows it has been blocked, follow these steps. Otherwise, continue to the next step.

1. Click the Pop-up blocked button.
2. Select Always allow pop-ups.
3. Click Done.
Configure KerberosIdpAdapter Authentication Adapter

1. Enter **sAMAccountName** for the Directory UID Attribute
2. **Check** Enable Windows Authentication
3. **Check** Enable Redirect
4. Enter **conn-01a.corp.local** for the Redirect Host Name
5. Click **Save**

**NOTE - The KerberosIdpAdapter may take several minutes to save. Please do not navigate away from the page or refresh while this completes!**
Confirm the KerberosIdpAdapter is Enabled

1. The KerberosIdpAdapter should now show as Enabled.
2. Click Admin Console to return.

Update the Policy Rules

1. Click Identity & Access Management.
2. Click Manage.
3. Click Policies.
4. Click Edit Default Policy.
Add Policy Rule

1. Click the **Configuration** tab.
2. Click **Add Policy Rule**.

Configure Policy Rule Details

1. Select **ALL RANGES** for the Network Range.
2. Select **Windows 10** for the Device Type.
3. Select **Kerberos** for the primary Authentication Method.
4. Select **Password** for the fallback Authentication Method.
Save the New Policy Rule

1. Scroll down to find the Save button.
2. Click **Save**.

Update the Policy Rule Order

1. Click and drag the created **Windows 10** policy rule to the top of the list.
2. Click **Next**.
The order of the Policy Rules determines in which order they are processed when users authenticate. For this exercise, you want the newly policy rule to process first.

Save Default Access Policy Set Changes

Click **Save**.

Authenticate with Kerberos using the Workspace ONE App

From the Desktop, double-click the **Win10-01a.rdp** shortcut.
Use the Workspace ONE App to Connect To Your Tenant

1. Click the **Workspace ONE App** from the task bar.
2. Enter [https://vidm-01a.corp.local](https://vidm-01a.corp.local) for the URL.
3. Click **Continue**.
Select the corp.local Domain

1. Select corp.local for the Domain.
2. Click Next.
Enter Credentials for Windows Authentication

1. Enter `aduser@corp.local` for the username.
2. Enter `VMware1!` for the password.
3. Click `OK`.

Enter Workspace

Click `Enter` after the workspace finishes building.
Confirm User Details

1. Click the **User** icon.
2. Click the **Account** tab.
3. Confirm that the User details show that we successfully signed in as **aduser@corp.local**.

This confirms that we were able to successfully enable Kerberos authentication for our Connector, configure our Policy Rules to authenticate our Windows 10 users via Kerberos, and then authenticate using Windows Authentication via Kerberos from our Windows 10 device by leveraging the Workspace ONE application.

**Return to the Main Console**
Click the X on the Remote Desktop session at the top of your screen to return to the Main Console.
Instructions for Taking Additional Lab Modules

If you are interested in taking additional modules for this lab, please click the END button in the VMware Learning Platform and then relaunch the lab.

Since each module in this lab takes advantage of configuring VMware Identity Manager and the VMware Identity Manager Connector for different use cases, the quickest way to start with a clean infrastructure to complete the next module is to restart the lab. Once you restart, navigate to the next module using the Table of Contents as shown in the Lab Guidance section.
Conclusion

In this exercise, you have completed the process of deploying VMware Identity Manager on-premise. This deployment followed the standard architecture in which the different components of VMware Identity Manager are installed on separate dedicated servers. This architecture was composed of the main VMware Identity Manager service running a non-domain joined Windows server, and the VMware Identity Manager Connector and SQL database running on dedicated, domain-joined Windows servers.

After successful installation of the different components, VMware Identity Manager was integrated to an on-premises Active Directory server for both user sync and authentication. Authentication for LDAP and Kerberos protocols were configured and tested successfully.

This concludes this lab.
Module 3 - Third party Identity Provider Integration with ADFS
Introduction

Active Directory Federation Services (AD FS) is a Windows Server component that provides single sign-on access to applications and systems for users using claims-based authentication. You can configure VMware Identity Manager to use Active Directory Federation Service (AD FS) as the third-party identity provider for authentication. In this lab, we'll review how to install and configure AD FS and how to add AD FS as a 3rd party IdP in VMware Identity Manager.

Prerequisites

- **VMware Identity Manager Tenant**: SaaS or On-Premise instance of VMware Identity Manager that you have administrator access to. For this lab, use the VMware Identity Manager tenant that is provided to you (details to access are contained in later steps).
- **Synced Domain**: Utilize the VMware Enterprise Systems Connector to sync a domain and at least a single domain user to login with.
- **Install AD FS**: Install AD FS on a server you have access to. This will require administrator access.

For this exercise, all of the prerequisites will be available to you.
AD FS Overview

AD FS utilizes claims-based authorization to implement identity federation. By default, VMware Identity Manager uses Security Assertion Markup Language (SAML), which is an assertion-based form of authorization. Conceptually, there are many parallels between SAML and AD FS. Use these similarities, outlined in the above table, as a foundation for understanding VMware Identity Manager and AD FS integration.

AD FS Claims

A claim is a statement about a user that includes values about the user (ie: user principal name (UPN), email address, role, group, windows account name, etc.) which are contained in a trusted token. Trusted parties, called relying parties, use the values stored in the claim to determine how to authorize the request.

Claims providers, such as your Active Directory, source and sign these claims. The Federation Service brokers trust between claims providers and relying parties by processing and exchanging claims between these parties to allow for authorization decisions to be made based on the statements of the claim.

1. The client requests a trusted token for access to a relying party, such as a web-hosted application.
2. The client authenticates against AD FS, validated by the trusted attribute store.
3. A trusted token is returned to the client upon successfully authenticating, which presents the trusted token to the relying party.
4. The relying party validates that the trusted token and allows access.
Install and Configure AD FS (Video Walkthrough)

For this exercise, you will need AD FS installed and configured to authenticate our domain users. Since the focus of this exercise is to integrate VMware Identity Manager with an existing AD FS deployment, you will not be installing the AD FS instance from scratch.

The below video will demonstrate how to install and configure a basic AD FS deployment, which has already been configured for you. If you are interested in seeing the initial installation, please watch the below video for a step-by-step walk-through of the process. Otherwise, please continue to the next step to continue with the exercise.
Download the ADFS Federation Metadata XML

To establish trust between VMware Identity Manager and our ADFS instance, you will need to download the ADFS Federation Metadata.

**Download the Federation Metadata XML**

Double-click the **Chrome** Browser on the lab desktop.

**Navigate to the Federation Metadata XML Endpoint**

Enter `https://adfs.corp.local/FederationMetadata/2007-06/FederationMetadata.xml` into the navigate bar and press **ENTER**.

The FederationMetadata.xml will appear in your downloads bar and will be stored in your Downloads folder. You will access the file later on when configuring VMware Identity Manager.
Finding the Federation Metadata Endpoint

Before continuing, you may be wondering how to get the Federation Metadata endpoint. Review the next steps to see how to retrieve the Federation Metadata endpoint from your ADFS server.

Connect to the adfs-01a Server

Double click the adfs-01a.rdp link from the Desktop.

For this exercise, ADFS is installed on the adfs-01a server. The hostname for this server is adfs.corp.local.
Open AD FS Management

1. Click the **Server Manager icon** from the taskbar.
2. Click **Tools**.
3. Click **AD FS Management**.

Alternatively, you can search for **AD FS Management** from the Start menu.
Locate FederationMetadata.xml Endpoint

1. Expand Service under AD FS.
2. Click Endpoints.
3. Scroll down to find the Metadata section.
4. Locate the Metadata object with the type Federation Metadata. Note the URL Path.

The link you used to download the Federation Metadata XML was your ADFS hostname ([https://adfs.corp.local](https://adfs.corp.local)) followed by your Federation Metadata endpoint found above ([/FederationMetadata/2007-06/FederationMetadata.xml](/FederationMetadata/2007-06/FederationMetadata.xml)). This is how the Federation Metadata endpoint was found.

Return to the Main Console
Click the **Close (X)** button on the Remote Desktop Connection bar at the top of the screen to return to the Main Console.

The remainder of the exercise will continue from the Main Console.
Connect to the Conn-01a Server

Double-click the conn-01a.rdp link on the Desktop to connect to the Conn-01a Server.

For the initial part of this lab, you will be installing the **VMware Identity Manager Connector** on the designated server. It is recommended to install the VMware Identity Manager Connector on a dedicated server or Virtual Machine (VM).
Install and Configure the VMware Identity Manager Connector

The VMware Enterprise Systems Connector has already been downloaded for you. The VMware Enterprise Systems Connector contains both the AirWatch Cloud Controller (ACC) and VMware Identity Manager Connector services. For this lab, you will only be installing the VMware Identity Manager Connector service in order to sync and authenticate Active Directory users with your VMware Identity Manager Tenant.

Start the VMware Enterprise Systems Connector Installer

1. Click the File Explorer icon from the taskbar.
2. Click Documents.
3. Click HOL.

1. Click the File Explorer icon from the taskbar.
2. Click Documents.
3. Click HOL.

**Confirm Security Warning and Run**

Click **Run**.

*NOTE - The Installer may take a minute or two to start after clicking run.*
Start the VMware Enterprise Systems Connector Installer

Click Next.

Accept the License Agreement Terms

1. Select I accept the terms in the license agreement.
2. Click **Next**.

**Disable the AirWatch Cloud Connector Feature**

1. Click the dropdown by the **AirWatch Cloud Connector** component.
2. Click **This feature will not be available**. 
Enable the VMware Identity Manager Connector Feature

1. Click the dropdown by the VMware Identity Manager Connector component.
2. Click This feature will be installed on local hard drive.

Accept the Default Destination Folder
Click **Next** to accept the default destination folder of C:\VMware\ 

**Configure the SSL Certificate**

1. Check the **Would you like to use your own SSL Certificate?** option
2. Click **Browse...**
Browse to the Connector SSL Certificate

1. Click **Documents**
2. Click **HOL**
3. Click **conn-01a**
4. Click **Open**
Enter SSL Certificate Password

1. Enter VMware1! for the Certificate Password
2. Click Next

Continue without Activating the Connector
1. Select No for Would you like to activate the Connector now
2. Click Next

In this lab, we are only interested in installing the VMware Identity Manager Connector at this point. We will activate the Connector later once we have setup the Connector in our VMware Identity Manager Admin Console and have access to the Activation Code. As stated by the installer, this can be updated later by accessing the Connector settings at [https://{hostname}:8443](https://{hostname}:8443), which will be [https://conn-01a.corp.local:8443](https://conn-01a.corp.local:8443).

**Setup the Service Account Configuration**

![VMware Enterprise Systems Connector - Installation Wizard](image)

1. Ensure the Would you like to run the Connector service as a domain user account option is enabled.
2. Enter corp\administrator for the User name.
3. Enter VMware1! for the Password.
4. Click Next.
Start the Install Process

Click **Install**.

*NOTE - The Installer may take a few minutes to complete. Please be patient while the service installs.*
Close the VMware Enterprise Systems Connector After It Completes

Click **Finish**.
Return to the Main Console

With the VMware Identity Manager Connector installed, you will configure the remainder of the requirements for this lab from the Main Console.

Click the Close (X) button on the Remote Desktop Connector bar at the top of your screen.

**NOTE - If you do not see the Remote Desktop Connection bar, you may have un-pinned the bar. Hover your mouse over the top and center part of the screen to reveal it.**
Login to the Workspace ONE UEM Console

To perform most of the lab, you will need to login to the Workspace ONE UEM Admin Console.

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.
Authenticate to the Workspace ONE UEM Admin Console

The default home page for the browser is https://labs.awmdm.com. Enter your Workspace ONE UEM Admin Account information and click the Login button.

NOTE - If you see a Captcha, please be aware that it is case sensitive!

1. Enter your Username. This is your email address that you have associated with your VMware Learning Platform (VLP) account.
2. Enter VMware1! for the Password field.
3. Click the Login button.

NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the Workspace ONE UEM Hands On Labs server.
Accept the End User License Agreement

Terms of Use

You must accept the following VMware End User License Agreement to use Workspace ONE UEM.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If you are licensing the Software for evaluation purposes, your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls

NOTE - The following steps of logging into the Administration Console will only need to be done during the initial login to the console.

You will be presented with the Workspace ONE UEM Terms of Use. Click the Accept button.
Address the Initial Security Settings

Security Settings

Password Recovery Question 1

Password Recovery Question *
What was your childhood nickname? 

Password Recovery Answer *
VMware1! 

Confirm Password Recovery Answer *
VMware1! 

Security PIN 

A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).

Security PIN *
1234 

Confirm Security PIN *
1234 

After accepting the Terms of Use, you will be presented with a Security Settings popup. The Password Recovery Question is in case you forget your admin password and the Security PIN is to protect certain administrative functionality in the console.
1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a question from the Password Recovery Question drop-down (default selected question is ok here).
3. Enter VMware1! in the Password Recovery Answer field.
4. Enter VMware1! in the Confirm Password Recovery Answer field.
5. Enter 1234 in the Security PIN field.
6. Enter 1234 in the Confirm Security PIN field.
7. Click the Save button when finished.

Close the Welcome Message

Workspace ONE UEM Console Highlights

Powered by VMware AirWatch!

Workspace ONE is powered by VMware AirWatch Unified Endpoint Management (UEM) technology, a unified digital workspace platform delivering a single, secure experience for app management, single sign-on (SSO), and conditional access.

Workspace ONE UEM transforms your business so you can:

- Configure, manage and support devices from any endpoint
- Increase productivity with seamless access to any app
- Safeguard company data at every layer
- Access identity and access management tools with ease
- Enjoy a simplified, consistent look and feel across Workspace ONE
After completing the Security Settings, you will be presented with the Workspace ONE UEM Console Highlights pop-up.

1. Click on the **Don't show this message on login** check box.
2. Close the pop-up by clicking on the X in the upper-right corner.
Login to the VMware Identity Manager Console

A temporary VMware Identity Manager tenant has been generated for you to use throughout this lab. The VMware Identity Manager tenant URL and login details were uploaded to the Content section in the Workspace ONE UEM Console at the start of the lab.

Accessing Your Tenant Details in the Workspace ONE UEM Console

In the Workspace ONE UEM Console:

1. Click **Content**.
2. Expand **Content Locker**.
3. Click **List View**.
4. Find the text file named `vIDM Tenant Details for your@email.shown.here.txt` and click the toggle button beside it to select the file.
5. Click **Download**.

Open the Downloaded Text File
After the file downloads, click the viDM Tenant Details for your@email.shown.here.txt file from the download bar to open it.

**Copy the Tenant URL**

1. Select the **Tenant URL** text and right-click.
2. Click **Copy**.

You will navigate to this Tenant URL in the next step to login to your VMware Identity Manager tenant.

**NOTE:** Your tenant name will match your Group ID in the Workspace ONE UEM Console.

**Login to Your VMware Identity Manager Tenant**

You will now login to your VMware Identity Manager tenant for the following steps.

**Launch Google Chrome (If Needed)**

If Google Chrome is not already open, launch Google Chrome by double-clicking the icon from the desktop.

**NOTE:** If Google Chrome is already open, skip this step.
Open a New Browser Tab

Click the Tab space to open a new tab.

Navigate to Your VMware Identity Manager Tenant

Paste or enter the Tenant URL into the navigation bar and press Enter to continue.

NOTE: This is the Tenant URL you received from the previous steps. If you did not copy or note this information from the previous step, return to those previous steps and note your Tenant URL.

NOTE: Your tenant name will match your Group ID found in the Workspace ONE UEM Console.
Login to Your VMware Identity Manager Tenant

1. Enter Administrator for the Username.
2. Enter VMware1! for the Password.
3. Click Sign In.

Navigate to the Administrator Console (If Necessary)
If you see the User Portal as pictured above, you will need to navigate to the Administrator Console.

1. Click the **User dropdown**.
2. Click **Administration Console**.

This will open the Administration Console in a separate tab in your browser.

*NOTE - If you do not see the above view, you are already in the Administration Console and can skip this step.*
Configure Your VMware Identity Manager Tenant

Before configuring the Directory Services and the VMware Identity Manager settings in the AirWatch Console, you will need to make some configurations your VMware Identity Manager tenant to ensure our Active Directory users are imported and mapped properly based on our configuration.

Continue to the next step.

Edit User Attributes

1. Identity & Access Management
2. Manage
3. Setup

- disabled
- distinguishedName (Required)
- domain
- email
- employeeID
- firstName
- lastName
- phone
- userName
- userPrincipalName (Required)
1. Click **Identity & Access Management**.
2. Click **Setup**.
3. Click **User Attributes**.
4. Enable **distinguishedName** by clicking the checkbox next to the field.
5. Enable **userPrincipalName** by clicking the checkbox next to the field.

   **NOTE** - You may need to scroll down to find the **distinguishedName** and **userPrincipalName** attributes.

### Save User Attribute Changes

1. Scroll down to the bottom of the page.
2. Click **Save**.
Create and Configure the VMware Identity Manager Connector

In the VMware Identity Manager Administrator Console,

1. Click **Identity & Access Management**
2. Click **Setup**
3. Click **Connectors**
4. Click **Add Connector**

Generate the Connector Activation Code

1. Enter **Lab** for the Connector ID Name.
2. Click **Generate Activation Code**.

1. Enter **Lab** for the Connector ID Name.
2. Click **Generate Activation Code**.
Copy the Connector Activation Code

1. Double-click the **Connector Activation Code** textbox to select the code.
2. Right-click and click **Copy**
3. Click **OK**

Activate the Connector

To activate the VMware Identity Manager Connector, you can connect to the hostname over port 8443 where the VMware Identity Manager Connector service was installed. You installed the VMware Identity Manager Connector service on conn-01a.corp.local in earlier steps.

1. Click the **Options** button
2. Click **New Tab**
Create the Administrator Account Credentials

First you will configure the Appliance Administrator Account (admin) for future logins:

1. Enter **VMware1!** for the Password
2. Enter **VMware1!** to confirm the password
3. Click **Continue**
Paste the Activation Code

1. Right-Click inside the Activation Code textbox and click **Paste** to paste the Activation Code we copied from the previous step when creating the "Lab" Connector from the VMware Identity Manager Console
2. Scroll down until you see the option **Continue**
3. Click **Continue**

*NOTE - While the page loads and refreshes, DO NOT close or manually refresh the page until you see the Setup is Complete screen shown in the next step!*
Confirm the Setup Completed

When the configuration has saved successfully, you should see the Setup is complete page. Continue to the next step when this screen is displayed.
Verify the Connector Activated

Back in the VMware Identity Manager Console,

1. Click the **Refresh** button in the browser.
2. Click **Identity & Access Management**.
3. Click **Setup**.
4. Click **Connectors**.
5. Confirm that the Connector now shows the Hostname as **conn-01a.corp.local** and the Worker named **Lab**.

This confirms that you have successfully setup and installed the VMware Identity Manager Windows Connector.
Sync Directory Users to VMware Identity Manager

This section will review how to add a new Directory in VMware Identity Manager and then sync users from our Active Directory into our VMware Identity Manager tenant.

Add an Active Directory over LDAP

In the VMware Identity Manager Administrator Console,

1. Click Identity & Access Management
2. Click Directories
3. Click Add Directory
4. Click Add Active Directory over LDAP/IWA

Configure the Directory Details

1. Enter corp.local for the Directory Name.
Configure the Directory Sync and Authentication Settings

1. Scroll down to find the Directory Sync and Authentication section.
2. Select the `conn-01a.corp.local` connector as the Sync Connector.
3. Select **Yes** to allow this Connector to perform authentication.
4. Select `sAMAccountName` for the Directory Search Attribute.

Configure the Bind User Details

1. Scroll down to find the **Bind User Details** section.
2. Enter `administrator@corp.local` for the Bind User Name.
3. Enter `VMware1!` as the Bind DN Password.
4. Click **Save & Next**.
Select the Domains

1. Ensure the corp.local domain is selected.
2. Click Next

Review the User Attribute Mappings

Review the User Attribute Mappings as desired, we won't need to make any changes to the default mappings for this lab. Click Next.
Find Groups to Sync

Select the groups you want to sync

- Sync nested group members

Specify the group DNs | Select All | Groups to sync
---|---|---
[ ] dc=corp,dc=local

1. Click the **Green Plus (+)** button to add a new Group DN.
2. Enter `dc=corp,dc=local` for the group DN.
3. Click **Find Groups**.

Select the Groups to Sync

Select the groups you want to sync

- Sync nested group members

Specify the group DNs | Select All | Groups to sync
---|---|---
[ ] dc=corp,dc=local

1. Click **Select All** to select all groups.
2. Click **Next**.
Select the Users to Sync

1. Click the **Green Plus (+)** button to add a new User DN.
2. Enter `cn=users,dc=corp,dc=local` for the user DN.
3. Click **Next**.

Review and Initiate Sync

Once the Review page loads and shows the number of Users and Groups being added, click **Sync Directory**.
Confirm Sync Started and Refresh to Check Status

1. Click the X to close the message confirming that the sync has started.
2. Click Refresh Page to see if the sync has completed.

**NOTE** - The sync may take a minute or two to complete. Keep clicking Refresh Page until the sync shows as completed with a green checkbox as shown in the next step.

Confirm the Sync Completes Successfully

Confirm that the corp.local directory shows synced groups, synced users, and that the Refresh Page notification is gone and replaced by a green checkbox to indicate the sync has completed.
Confirm the Synced Users Exist

1. Click **Users & Groups**.
2. Confirm the **corp.local** users have synced and are displayed here.

This confirms that you have successfully added a directory to your VMware Identity Manager tenant and were able to use your previously installed Connector to sync Active Directory users to the directory.
Create a Third Party Identity Provider

In order for AD FS to authenticate our users, we need to create a Third Party Identity Provider (IdP) within VMware Identity Manager and use the FederationMetadata.xml downloaded from our Federation Service to establish trust between AD FS as the Identity Provider and VMware Identity Manager as the Service Provider.

Copy the ADFS Federation Metadata XML

1. Click the File Explorer icon from the taskbar.
2. Click Documents.
3. Right-click the FederationMetadata.xml.
4. Click the Edit with Notepad++.
Copy the Federation Metadata Contents

1. Right-click and click **Select All**.
2. Right-click and click **Copy**.

Create Third Party Identity Provider in VMware Identity Manager

1. Navigate to the **Identity & Access Management** section.
2. Select **Identity Providers**.
3. Click on **Add Identity Provider**.
4. Choose **Create Third Party IDP**.
Navigate to your VMware Identity Manager Administration Console in Chrome.

1. Click **Identity & Access Management**
2. Click **Identity Providers**
3. Click **Add Identity Provider**
4. Click **Create Third Party IDP**

**Enter Identity Provider Name and SAML Metadata**

Open the **FederationMetadata.xml** file you downloaded earlier and **copy the full XML text** contained within the document.

1. Enter **AD FS** for the Identity Provider Name. This is just a display name that will be used for this Third Party IDP.
2. Paste the XML text contained in your **FederationMetadata.xml** file into the SAML Metadata field.
3. Click **Process IdP Metadata**. This configures certain settings in your IDP based on the specifications that are noted within the Federation Metadata.
Confirm Processed IdP Metadata

After selecting to Process the IdP Metadata, notice that the SAML AuthN Request Binding and the Name ID format mappings have been automatically configured. These values were pulled from the `FederationMetadata.xml`, which informs VMware Identity Manager how to send requests to our Third Party IDP to process authentication requests.

Configure Users and Networks that can utilize this IDP

1. Select the checkbox for `ALL RANGES`.
2. Enable Just-in-Time User Provisioning.
3. Select `corp.local` as the user that can authenticate using this IdP.
1. Scroll down until you see the section for **Just-in-Time user Provisioning**.
2. Disable **Just-in-Time User Provisioning**.
   Just-in-Time user provisioning allows users to be created within VMware Identity Manager dynamically when they authenticate using this Third Party IDP if they do not already exist. This can be useful for dynamically adding any missed users or new users who have not been synced but still belong to your domain(s) that will be utilizing this Third Party IDP.
3. Select the **corp.local** users.
   This determines which users will be allowed to use this Third Party IDP when authenticating.
4. Select **ALL RANGES** for the Network.

**Configure Authentication Methods for this IDP**

![Authentication Methods Diagram](image)

We need to specify which authentication methods this Third Party IDP will utilize to authenticate our selected users.

1. Scroll down until you see the section for **Authentication Methods**
2. Enter **SAML Password** for the Authentication Method.
4. Click the **Add (+)** button to add another Authentication Method.
5. Enter **SAML Kerberos** for the Authentication Method.
7. Click the **Add (+)** button to add another Authentication Method.
8. Enter **Windows Authentication** for the Authentication Method.

The **Authentication Methods** column acts as a display name for the SAML Context. When creating Access Policies, the Authentication Methods column name will display as options for which authentication methods to use to authenticate our users. Note that these names must be unique across your VMware Identity Manager tenant, and cannot share names with the default Authentication Methods either!
The **SAML Context** informs the Identity Provider (AD FS in this instance) how the user should be authenticated. The SAML Context will be inserted as part of the SAML Assertion (under the AuthnStatement section). This SAML Assertion will be signed and sent to AD FS as a request to authenticate users when they attempt to login to VMware Identity Manager using this Third Party IDP.

For reference, here is a sample of a SAML Assertion that will be signed and sent to AD FS when users attempt to authenticate. Notice the AuthnStatement section, which details when the authentication request was made and contains how the user is attempting to authenticate (via Kerberos, in this case).

```xml
<saml:AuthnStatement
    AuthnInstant="2004-12-05T09:22:00"
    SessionIndex="b07b804c-7c29-ea16-7300-4f3d6f7928ac">
    <saml:AuthnContext>
        <saml:AuthnContextClassRef>
            urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
        </saml:AuthnContextClassRef>
    </saml:AuthnContext>
</saml:AuthnStatement>
```
1. Scroll down to find the additional configuration options.
2. Enable the **Single Sign-Out Configuration**, which will also sign users out of their IDP session when they sign out from Workspace ONE. You can optionally provide a Sign-Out URL, which will re-direct users to the provided URL upon logging out, and a Redirect Parameter, which will send URL parameters to the Sign-out URL which can be used by the IDP to perform certain actions based on the provided parameters. In our case, we just want our users to be re-directed to our Identity Provider (AD FS) using SAML single logout with no additional parameters so these will remain blank.
3. Right-click the **Service Provider (SP) Metadata** link.
4. Click **Save link as...**
   You will be providing the Service Provider Metadata XML file to ADFS in an upcoming step to establish trust between the two parties as an Identity Provider and Service Provider.
Save the Service Provider (SP) Metadata file

1. Click the Downloads folder.
2. Keep the default file name of sp.xml.
3. Click Save.

Add the Third Party Identity Provider

Click Add to save the configuration of our Third Party Identity Provider for AD FS.
Copy the sp.xml File

1. Click the down arrow button for the sp.xml download.
2. Click Show in Folder.

Copy the sp.xml File to the Clipboard

1. Right-click the sp.xml file
2. Click Copy.
You will be copying the Service Provider (SP) XML metadata file to the virtual machine that is hosting ADFS in an upcoming step in order to establish trust between ADFS and VMware Identity Manager.
Configure Access Policies in VMware Identity Manager

Now that we've created our Third Party IDP for AD FS in VMware Identity Manager, we need to use the Authentication Methods we created in our Access Policies to authenticate our domain users with our Third Party IDP authentication methods rather than using the default access policy rules for authenticating our domain users through the Password (AirWatch Connector) method.

Edit the Access Policy

1. Click Identity & Access Management
2. Click Policies
3. Click the default_access_policy_set to edit it
Create A New Policy Rule for Domain Users

1. Click the **Configuration** tab.
2. Click **Add Policy Rule**.

**Configure the Policy Rule**

This policy rule will be used to allow our Domain (corp.local) users to login by leveraging the AD FS authentication methods we setup earlier as part of our 3rd Party Identity Provider configuration.

1. Select **ALL RANGES** for the network range
2. Select **All Device Types** for the content origin
3. Enter **Domain Users** into the user groups search field
4. Click the **Domain Users@corp.local** result to select the group.
Configure the Authentication Methods for the Policy Rule

1. Scroll down to find the additional configuration options
2. Select **Authenticate using...** as the action
3. Set the 1st authentication method as **Windows Authentication**
4. Set the fallback authentication method as **SAML Kerberos**
5. Click **Add fallback method**
6. Set the 2nd fallback authentication method as **SAML Password**
7. Click **Save**

This Policy Rule will first attempt to authenticate our users via Kerberos with AD FS. Should that fail or be inapplicable, Windows Authentication will be attempted. Lastly, if all other methods have failed or been inapplicable, Password authentication will be attempted.
We need our policy rule that will handle AD FS authentication for our domain users to be processed first, otherwise our All Users policy that we configured for Password (Local Directory) will attempt to apply for our domain users instead of our intended policy.

1. Click and drag the handle for the policy rule we just created for AD FS to the top of the list.
   
   *NOTE - This will be the rule with the Authentication columned listed as Windows Authentication +2*

2. Click **Next**.
Save the Updated Policy Rules

Description
Default access policy set

Applications
0 Application(s)

Configuration

Policy Rule 1
If a user's network range is **ALL RANGES**
and the user is accessing content from **Web Browser**
and the user belongs to the group(s) **All Users**
then the user may authenticate using **Password**

Fallback method 1: **Password (Local Directory)**
Re-authenticate after **8 hour(s)**

Advanced Properties

Click **Save**
Configure Relying Party Trust in AD FS

With our Third Party IDP configured in VMware Identity Manager and our Service Provider Metadata in hand, we can now configure a Relying Party Trust in AD FS for our VMware Identity Manager tenant. This will utilize our Service Provider metadata to establish trust between AD FS as the Identity Provider and VMware Identity Manager as the Service Provider.

Connect to the adfs-01a Server

Double click the adfs-01a.rdp link from the Desktop.

You will need to modify your ADFS configuration to establish trust to VMware Identity Manager, which must be done from the server where we have installed ADFS.
1. Click the File Explorer icon on the taskbar.
2. Click Downloads.
3. Right-click within the Downloads folder and click Paste.
Add Relying Party Trust

Return to AD FS Management. If closed, you can either navigate to Server Manager and click Tools > AD FS Management or search for "AD FS Management" from the Start menu.

1. Expand Trust Relationships
2. Click Relying Party Trusts
3. Click Add Relying Party Trust

This will open the Add Relying Party Trust Wizard. Click Start to begin this process once the wizard displays.
Start Add Relying Party Trust Wizard

Click **Start**.
Select Data Source

You will now provide the Service Provider Metadata XML that you copied and pasted in the Downloads folder previously when creating your Third Party IDP in VMware Identity Manager to establish trust between ADFS and VMware Identity Manager.

1. Select **Import data about the relying party from a file**.
2. Click **Browse...**
Provide Service Provider Metadata XML File

1. Click Downloads.
2. Click sp.xml.
3. Click Open.
Continue After Providing sp.xml File

Your sp.xml filepath will now be displayed in the Federation metadata file location field. Click **Next** to continue.
Specify Display Name

1. Enter `{YOUR_TENANT_NAME}.vidmpreview.com` for the Display Name, replacing `{YOUR_TENANT_NAME}` with the VMware Identity Manager tenant name you accessed in previous steps.
2. Click Next.

The Display Name has no impact on the Relying Party Trust, but it is recommended to name the trust accurately so you know which service it is integrated with.
Multi-factor Authentication (MFA) requires a user to complete two or more authentication challenges from multiple categories: Knowledge (something they know, like a password), possession (something they have, like a FOB or device), and inherence (something they are, such as biometrics).

Multi-factor Authentication configuration is out of scope for this exercise, so click **Next** to continue without configuring it.
Choose Issuance Authorization Rules

Issuance Authorization Rules specify if a user is permitted to receive claims, or authentication requests, for this relying party. We can either permit all users or deny all users from accessing this relying party.

1. Select **Permit all users to access this relying party**. In our case, we want our domain users to be able to use this relying party to authenticate.
2. Click **Next**.
Review and Continue with Relying Party Trust Wizard

Review any desired information about the relying party before clicking Next. Notice that certificates were also included with the Service Provider Metadata, which will be used to encrypt the SAML assertions from VMware Identity Manager.
Finish Relying Party Trust Wizard

1. Leave the **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** option enabled.
2. Click **Close**.

Add Claim Rules for Relying Party

In order to properly authenticate our users, we need to add Claim Rules for our relying party. Claim Rules control the flow of claims and are responsible for taking one or more incoming claims, applying conditions to these claims, and then producing one or more outgoing claims. Claim Rules and the Claims Engine are responsible for determining if incoming claims should be passed through as they are received, filtered to meet specific business logic criteria, or transformed into a new set of claims before they are issued as an outgoing claim.

In short, think of Claim Rules as the logic that inspects, processes, and transforms incoming claims to outgoing claims which determine who and how users are authenticated. For more detailed documentation, check out [the Role of Claim Rules](#).

In this lab, we'll need to create two types of Claim Rules.
1. **Send LDAP Attributes as Claims:** Meaning that the outgoing claim will contain LDAP attribute values from our attribute store (Active Directory, in this case) that can be used for authentication.

2. **Send Claims using a Custom Rule:** Will use the claim rule language to generate and transform our claim to handle specific business logic requirements needed to authenticate the user in VMware Identity Manager.

**Add Issuance Transform Rules for LDAP Attributes**

Claim Rules are processed in chronological order by the claims engine, so the order of our rules is important. For example, the output of one rule can be used as the input of the next rule, so depending on your business logic, you may need to carefully craft how your claims will be passed through, processed, or transformed.

**Add Issuance Transform Rule**

From the Edit Claim Rules dialog:

1. Ensure the **Issuance Transform Rules** tab is selected.
2. Click **Add Rule**.

**Choose Rule Type**

1. Select **Send LDAP Attributes as Claims** for the Claim Rule Template.
2. Click **Next**.
Configure Claim Rule

1. Enter **Get Attribute Email Address** for the Claim Rule Name.
2. Select **Active Directory** as the Attribute Store.
3. Select **E-Mail-Addresses** from the **LDAP Attribute** dropdown.
4. Select **E-Mail Address** from the **Outgoing Claim Type** dropdown.
5. Click **Finish**.

For this claim rule, we've mapped the E-Mail-Addresses LDAP attribute as E-Mail Address to our outgoing claim type and have issued the claim.
Add Issuance Transform Rules for Custom Claims Rule

Our Get Attribute Email Address Claims Rule is now created. Next, we'll create a Custom Claims Rule.

Click Add Rule to get started.

**NOTE:** Remember that you can highlight the text within the manual and drag-and-drop the selection into the terminal to paste the text.
Choose Rule Type

1. Select **Send Claims Using a Custom Rule** as the Claim Rule Template.
2. Click **Next**.
Configure Claim Rule

1. Enter Transform Email Address as the Claim Rule Name.
2. Enter the below text for the Custom rule.
3. You will need to replace the {YOUR_TENANT_NAME}.vidmpreview.com text at the end for the spnamequalifier with your VMware Identity Manage tenant! Otherwise this rule will not work. This rule transforms the outgoing Email Address claim and issues both the email.
   ```c:
   [Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>
   issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
   Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
   c.ValueType, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/
   format"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
   Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/
   spnamequalifier"] = "{YOUR_TENANT_NAME}.vidmpreview.com");
   ```
4. Click Finish.
Apply Claim Rules

1. Click **Apply**.
2. Click **OK** to close the Edit Claim Rules dialog.

Return to the Main Console

Click the **Close (X)** button on the Remote Desktop Connection bar to return to the Main Console.
Login as a Domain User

Now that we've established trust between AD FS as the Identity Provider and our VMware Identity Manager tenant as the Service Provider and configured our Relying Party Claim Rules to transform and issue the incoming claim to a format that our VMware Identity Manager tenant can process, we now need to attempt to login using the corp.local domain users and validate that our configurations are working.

Connect to the Windows 10 VM

Double-click the **Win10-01a.rdp** remote desktop connection shortcut from the Desktop.
Authenticate as a Domain User in the Browser

1. Open **Google Chrome**.
2. Navigate to your VMware Identity Manager tenant URL `(https://{yourtenant}.vidmpreview.com)`.  
   **NOTE:** Replace `{yourtenant}` with the name of your actual tenant!
3. Enter `holuser` for the username, which is one of the corp.local domain users we synced. This is also the user account that is currently logged into the win10-01a VM that you are connected to.
4. Uncheck **Remember this setting**.
5. Click **Next**.

**NOTE:** The authentication may take several seconds to process, please be patient after clicking Next.

**Confirm Authentication was Successful**

Notice that the user was logged into the VMware Identity Manager tenant without having to enter their credentials. Upon logging in as aduser, the 3rd party Identity Provider you configured attempted to authenticate the user using Kerberos first. After the Claim is processed in AD FS, the claim is transformed via the Claim Rules we created earlier and responds in a manner that VMware Identity Manager is able to process, thus authorizing the user to login using SAML.

1. Click the **User dropdown**.
2. Click **Sign Out**.

**NOTE:** Signing out may take several seconds to process from AD FS. Please wait until you are taken back to the VMware Identity Manager login page.

This will clear the login cookie for the aduser. The next exercise will showcase using the VMware Workspace ONE App to login, so the cookie needs to be cleared first.
Authenticate as a Domain User in the VMware Workspace ONE App

1. Launch the **VMware Workspace ONE app**.
2. Enter your VMware Identity Manager tenant URL
   ([https://yourtenant.vidmpreview.com](https://yourtenant.vidmpreview.com)).
   **NOTE:** Replace `{yourtenant}` with the name of your actual tenant!
3. Click **Continue**.
Login as a corp.local domain user

1. Enter `holuser` for the username. This is one of the corp.local domain users we synced.
2. Click **Next**.

**NOTE:** The authentication process may take several seconds after clicking **Next**. Please be patient and wait until the next page loads.
Confirm Authentication was Successful

As seen in your browser session, the claim is transformed and the outgoing claim authorizes the user to access Workspace ONE via SAML without having to enter their credentials.

After successfully authenticating, you should see a message indicating that your workspace is being configured, and eventually that the workspace is ready. Click Enter.
Clear Authorization Cookies (IF NEEDED)

The authorization cookies last 8 hours after you authenticate to VMware Identity Manager. If you need to re-authenticate again to test, you can either shorten the re-authentication timers of the Access Policy rules you configured, or you can clear your authorization cookies so that the browser and VMware Workspace ONE app sessions are removed which forces the user to authenticate again.

1. Open Google Chrome and click the Options button.
2. Click Settings.

The steps for clearing authorization cookies in Google Chrome are as follows:

1. **Open Google Chrome and click the Options button.**
2. **Click Settings.**

After clicking **Settings**, you will see a list of options. You can choose to clear cookies and other site data from here.
Navigate to Clear Browser History

1. Enter **Clear Browsing Data** in the search field.
2. Scroll down and click **Clear Browsing Data**.
Clear Cookies

1. Select the **beginning of time** for the period.
2. Ensure **Cookies and other site data** is checked.
3. Click **Clear Browsing Data**.
Confirm or Inspect Cookies

To check if any cookies exist or to see which cookies are being stored for your VMware Identity Manager session, navigate back to Google Chrome:

1. Right-click anywhere to pull up the options menu.
2. Click **Inspect**. Alternatively, you can use **Ctrl + Shift + i** to view the console.
3. Select the **Application** tab.
4. Find the **Cookies** section under Storage. If there are no cookies listed, then you currently have no authorization cookies for your VMware Identity Manager tenant. If they do exist, you'll be able to see them once you select your tenant URL under Cookies.
5. You can also use the **Delete** button from here to remove all cookies for this page.
Troubleshooting

This section will review a few issues you may experience while attempting to integrate a Third Party IDP with VMware Identity Manager and what troubleshooting steps you can take.

Cannot Login to the VMware Identity Manager Tenant

Problem:
When the Access Policies are configured incorrectly, authentication may fail for some or all users. This can cause even your local accounts to be unable to login to the tenant to resolve the issue.

Solution:
To login to the tenant and bypass the configured Access Policies causing the authentication issue, append `?login` to your default login URL:

```
https://<tenantURL>/SAAS/auth/login?login
```

VMware Identity Manager: Error: Cannot Update Identity Provider

Problem:
While adding or editing an Identity Provider and attempting to add or update an authentication method, you see the error "Cannot update Identity Provider". This prevents you from adding or editing authentication methods when you click save.

Solution:
The SAML context name must be unique in your VMware Identity Manager tenant, including names used by the default authentication methods. Rename your SAML context name for the chosen authentication method and click save.

VMware Identity Manager: 404.idp.not.found / federationArtifact.not.found Federation Artifact not found

Problem:
When attempting to login to VMware Identity Manager, an error message is displayed with "404.idp.not.found", "federationArtifact.not.found Federation Artifact not found", or another error that indicates that an Identity Provider or Federation Artifact
could not be found to authenticate the users. This occurs when no Access Policies are setup to handle authenticating the network range, device type, user group, or attempted authentication methods or if the Claim Rules for the relying party are misconfigured.

Solution:

• In the access policy rules, create an access policy that includes the network range, device type, user group and authentication method you are attempting to login with. Ensure these authentication methods are enabled and active for your Identity Providers and that they are applying to the network range and user group you are expecting.
• Ensure your Relying Party Trust claim rules were properly configured based on the examples provided. The claim values are case sensitive. Also ensure you properly replaced your spnameequalifier in the custom claims rule with your VMware Identity Manager tenant.

AD FS Error: Contact your Administrator

Problem:

When users attempt to authenticate using claims-based authentication to AD FS, they see a login page that says "Error: Contact your administrator". This occurs because AD FS cannot properly authenticate the claim.

Problem:

• Ensure you properly established trust between AD FS as the Identity Provider and VMware Identity Manager as the Service Provider. Re-export the FederationMetadata.xml files or URLs and ensure you uploaded the correct metadata for each component.
• Ensure your Relying Party Trust claim rules were properly configured based on the examples provided. The claim values are case sensitive, and ensure you properly replaced your spnameequalifier in the custom claims rule with your VMware Identity Manager tenant.
• Ensure your authentication methods configured for the access policies applied to your domain users are correctly using the authentication methods setup for the AD FS Identity Provider.
• Ensure you are not attempting to authenticate local users from VMware Identity Manager that do not exist within your Active Directory. Local users should be authenticated using the Password (Local Directory) authentication method, not authentication methods configured for AD FS since AD FS will fail to find these local user accounts in AD.
AD FS: Failed Authentication Requests and Viewing Logs
Problem:

When users attempt to authenticate using claims-based authentication to AD FS from VMware Identity Manager, they are being redirected to AD FS for their credentials appropriately but then receive an error that they could not be authenticated. AD FS may be configured incorrectly, causing issues with consuming incoming claims, generating outgoing claims, or other issues that would cause authentication to fail.

Solution:

- After installing and configuring AD FS, Server Manager will contain an AD FS Dashboard from the left menu. From here, an Events view is available which can be configured to log events of different severities (Informational, Warning, Error, or Critical) within a certain time period. This view can be configured by clicking Tasks > Configure Event Data, which is next to the Events view from this AD FS Dashboard.
- Alternatively, you can use Event Viewer to view the AD FS logs as well. From Event Viewer, you can find the logs by navigating to Applications and Services Logs > AD FS Tracing > Debug. To begin receiving logs, you will need to right-click the Debug file and select Enable Log. If you wish to stop tracking events
this way, you can right click the Debug file and select Disable Log to return it to the original state.

Both solutions will allow you to see traces of your authentication attempts. Failures and issues are typically noted with the severity levels of Error or Critical, so try inspecting your logs to see what is causing your authentication to fail. Typical authenticate issues could be:

- The Third Party IDP configuration in VMware Identity Manager is not sending a Name ID Format that the Identity Provider (AD FS) is expecting to query a user from the Attribute Store with.
- The Third Party IDP and/or Access Policies in VMware Identity Manager are using Authentication Methods that the Identity Provider (AD FS) is not handling or cannot handle due to the authentication methods allowed for Intranet vs. Extranet. These Intranet vs. Extranet authentication methods can be viewed in AD FS by going to AD FS Management > AD FS > Authentication Policies > Primary Authentication. By default, Extranet authentication uses Forms authentication while Intranet uses Windows authentication, so if you are attempting to authenticate users in your Intranet by using Forms authentication, this will fail until you update the Primary Authentication settings to also allow Forms authentication for Intranet requests.
- The Relying Party Trust was misconfigured in AD FS. If you imported the Service Provider Metadata from VMware Identity Manager, this shouldn't be an issue.
- The Relying Party Claim Rules were misconfigured. The exact configuration issues would depend on what Claim Rule templates you utilized, but double check that you have access to the attributes you're expecting in the claim as well as your Attribute Store. If you are using Custom Claim Rules, double check that your claim engine logic is correct and without syntax issues and that it is returning an outgoing claim that your Service Provider is expecting. Service Providers will require different configurations, so it's best to find documentation for that service (ie: VMware Identity Manager, Okta, Ping) and see what they are expecting in their claims from AD FS to properly authenticate users.
Instructions for Taking Additional Lab Modules

If you are interested in taking additional modules for this lab, please click the **END** button in the VMware Learning Platform and then relaunch the lab.

Since each module in this lab takes advantage of configuring VMware Identity Manager and the VMware Identity Manager Connector for different use cases, the quickest way to start with a clean infrastructure to complete the next module is to restart the lab. Once you restart, navigate to the next module using the Table of Contents as shown in the Lab Guidance section.
Conclusion

VMware Identity Manager can leverage AD FS as a third party identity provider to securely authenticate users via a claims-based access control authorization model. Consider how leveraging your existing AD FS deployment with VMware Identity Manager can be used to provide single-sign on access to systems and applications across your organization without re-creating your established authentication policies.

Additional AD FS documentation can be found through Microsoft’s documentation.
Module 4 - VMware Identity Manager REST API
Introduction

The VMware Identity Manager REST API allows you to automate a wide variety of administrative tasks. In this lab, we will review some sample actions you can perform using the REST API and how to properly authenticate using oAuth. The goal is to create a new local user account in Identity Manager, create a weblink application, and then update this application to be entitled to our created user.

At the end, we should be able to login to our Workspace ONE console using our generated user and launch our weblink application successfully.
Login to the Workspace ONE UEM Console

To perform most of the lab, you will need to login to the Workspace ONE UEM Admin Console.

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.
Authenticate to the Workspace ONE UEM Admin Console

The default home page for the browser is https://labs.awmdm.com. Enter your Workspace ONE UEM Admin Account information and click the Login button.

**NOTE - If you see a Captcha, please be aware that it is case sensitive!**

1. Enter your **Username.** This is your email address that you have associated with your **VMware Learning Platform (VLP) account.**
2. Enter **VMware1!** for the **Password** field.
3. Click the **Login** button.

**NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the Workspace ONE UEM Hands On Labs server.**
Accept the End User License Agreement

Terms of Use

You must accept the following VMware End User License Agreement to use Workspace ONE UEM.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If you are licensing the Software for evaluation purposes, your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls

NOTE - The following steps of logging into the Administration Console will only need to be done during the initial login to the console.

You will be presented with the Workspace ONE UEM Terms of Use. Click the Accept button.
Address the Initial Security Settings

Security Settings

Password Recovery Question 1

Password Recovery Question *

Password Recovery Answer *

Confirm Password Recovery Answer *

Password Recovery Question 1: What was your childhood nickname?

Password Recovery Answer 1: VMware1!

Confirm Password Recovery Answer 1: VMware1!

Security PIN

A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).

Security PIN *

Confirm Security PIN *

Security PIN: 1234

Confirm Security PIN: 1234

After accepting the Terms of Use, you will be presented with a Security Settings pop-up. The Password Recovery Question is in case you forget your admin password and the Security PIN is to protect certain administrative functionality in the console.
1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a question from the Password Recovery Question drop-down (default selected question is ok here).
3. Enter VMware! in the Password Recovery Answer field.
4. Enter VMware! in the Confirm Password Recovery Answer field.
5. Enter 1234 in the Security PIN field.
6. Enter 1234 in the Confirm Security PIN field.
7. Click the Save button when finished.

**Close the Welcome Message**

**Workspace ONE UEM Console Highlights**

**Powered by VMware AirWatch!**

Workspace ONE is powered by VMware AirWatch Unified Endpoint Management (UEM) technology, a unified digital workspace platform delivering a single, secure experience for app management, single sign-on (SSO), and conditional access.

Workspace ONE UEM transforms your business so you can:

- Configure, manage and support devices from any endpoint
- Increase productivity with seamless access to any app
- Safeguard company data at every layer
- Access identity and access management tools with ease
- Enjoy a simplified, consistent look and feel across Workspace ONE
After completing the Security Settings, you will be presented with the Workspace ONE UEM Console Highlights pop-up.

1. Click on the **Don't show this message on login** check box.
2. Close the pop-up by clicking on the **X** in the upper-right corner.
Login to the VMware Identity Manager Console

A temporary VMware Identity Manager tenant has been generated for you to use throughout this lab. The VMware Identity Manager tenant URL and login details were uploaded to the Content section in the Workspace ONE UEM Console at the start of the lab.

Accessing Your Tenant Details in the Workspace ONE UEM Console

In the Workspace ONE UEM Console:

1. Click Content.
2. Expand Content Locker.
3. Click List View.
4. Find the text file named vIDM Tenant Details for your@email.shown.here.txt and click the toggle button beside it to select the file.
5. Click Download.

Open the Downloaded Text File
After the file downloads, click the viDM Tenant Details for your@email.shown.here.txt file from the download bar to open it.

**Copy the Tenant URL**

![Image of Notepad with selected Tenant URL]

1. Select the **Tenant URL** text and right-click.
2. Click **Copy**.

You will navigate to this Tenant URL in the next step to login to your VMware Identity Manager tenant.

**NOTE:** Your tenant name will match your Group ID in the Workspace ONE UEM Console.

**Login to Your VMware Identity Manager Tenant**

You will now login to your VMware Identity Manager tenant for the following steps.

**Launch Google Chrome (If Needed)**

![Google Chrome icon]

If Google Chrome is not already open, launch **Google Chrome** by double-clicking the icon from the desktop.

**NOTE:** If Google Chrome is already open, skip this step.
Open a New Browser Tab

Click the Tab space to open a new tab.

Navigate to Your VMware Identity Manager Tenant

Paste or enter the Tenant URL into the navigation bar and press Enter to continue.

**NOTE:** This is the Tenant URL you received from the previous steps. If you did not copy or note this information from the previous step, return to those previous steps and note your Tenant URL.

**NOTE:** Your tenant name will match your Group ID found in the Workspace ONE UEM Console.
Login to Your VMware Identity Manager Tenant

1. Enter **Administrator** for the **Username**.
2. Enter **VMware1!** for the **Password**.
3. Click **Sign In**.

Navigate to the Administrator Console (If Necessary)
If you see the User Portal as pictured above, you will need to navigate to the Administrator Console.

1. Click the **User dropdown**.
2. Click **Administration Console**.

This will open the Administration Console in a separate tab in your browser.

*NOTE - If you do not see the above view, you are already in the Administration Console and can skip this step.*
Open Postman

We will be utilizing a REST client named Postman to setup and send API requests to VMware Identity Manager through the course of this lab.

Open Postman

Double-click the Postman icon from the desktop.

NOTE - Postman may take several seconds to launch after double-clicking the icon. Please wait a moment for the application to launch.

Note Your VMware Identity Manager Domain Name

The vIDM Tenant Details text file available from the Workspace ONE UEM Console contains a field titled Tenant URL.

Make note of this field, as further instructions in the lab will request that you substitute your VMware Identity Manager FQDN (Fully Qualified Domain name) to direct the API request to your tenant instance, which will be the Tenant URL field (ie: https://yourtenantname.vidmpreview.com).
Request an oAuth SessionToken

1. Select **POST** as the Verb.
2. Enter https://{your_tenant_fqdn}/SAAS/API/1.0/REST/auth/system/login for the Request URL.
   
   **NOTE** - Remember to replace {your_tenant_fqdn} with your VMware Identity Manager Tenant Fully Qualified Domain name (FQDN).
3. Click the **Headers** tab.
4. Enter **Content-Type** into the Key field.
5. Enter application/json into the Value field.
6. Enter **Accept** into the Key field.
7. Enter application/json into the Value field.

Setup the Request Body

1. Click the **Body** tab.
2. Select **Raw**.
3. Enter the below JSON data for the Body.
   ```json
   {"username":"Administrator", "password":"VMware1!","issueToken":"true"}
   ```
4. Click **Send**.
1. Scroll down to view the response.
2. Click the **Pretty** formatting option.
3. Ensure Word Warp is enabled to make the response easier to read.
4. In the response, you will see a `sessionToken` field. This is the OAuth key we will use to authenticate to the API for the remainder of this lab. **Highlight** the text (NOT the quotation marks) and **right-click**.
5. Click **Copy**.
Save the SessionToken Value

1. Click the Windows button.
2. Type Notepad to search.
3. Click Notepad from the list of results.

Enable Word Wrap

1. Click Format.
2. Click Word Wrap.
Paste the Session Token

1. Type `sessionToken:` into the Notepad file.
2. Right-click and click Paste.

If you need to refer back to your `sessionToken` for future steps, open your Notepad file and copy the `sessionToken` that is pasted here.
Create a Local User in Identity Manager

With a successful authentication returning a valid sessionToken, let's apply this to make an authenticated request to our VMware Identity Manager tenant and create a local user with the API.

Setup the Request Headers

1. Select **POST** as the verb.
2. Enter `https://{your_tenant_fqdn}/SAAS/jersey/manager/api/scim/Users` for the Request URL.  
   **NOTE** - Remember to replace `{your_tenant_fqdn}` with your VMware Identity Manager Tenant Fully Qualified Domain name (FQDN).
3. Click the Headers tab.
4. Enter **Authorization** for the **Key**.
5. Enter **HZN** for the **Value**.  
   **NOTE** - Include the extra space after "HZN"! We will be pasting the sessionToken after HZN and should appear as `HZN {sessionToken}`, otherwise the request will fail!
6. Click **Paste** to insert the copied `sessionToken`.
Setup the Request Body

1. Click the **Body** tab.
2. Select **Raw**.
3. Enter the below JSON data for the Body:
   ```json
   {"schemas": ["urn:scim:schemas:core:1.0"], "userName": "apiuser", "name": {"givenName": "API", "familyName": "User"}, "emails": [{"value": "apiuser@test.com"}], "password": "VMware1!"}
   ```
4. Click **Send**.
View the Response

1. Scroll down to view the response.
2. Confirm that the Status shows **201 Created**. This confirms the user was created.
3. Review the response of the API request to confirm that the created user details match the values provided in our Request Body from the previous step. Locate the apiuser data and then find the **id** field and **highlight** the text (NOT the quotation marks) and **right-click**.
4. Click **Copy**.
Save the ID of the Created User

1. Click the Notepad icon from the Task bar.
2. Enter **Created User ID:** into the Notepad file beneath your sessionToken.
3. **Right-click** and click **Paste**.
When asked for your **Created User ID** in future steps, refer to the pasted value here in your Notepad file.

**View the Created User in the Identity Manager Administrator Console**

![Workspace ONE Console](image)

1. Click **Users & Groups**.
2. Click the **User,API** entry.

Back in the VMware Identity Manager Administrator Console,

1. Click **Users & Groups**.
2. Click the **User,API** entry.
Confirm the User Details

1. Scroll through the User Details and confirm they match the values entered from our API request.
2. Click **Back to User List**.
List Users in Identity Manager

In addition to creating users, you can also query the list of users from Identity Manager.

Our Request URL will remain the same from the previous exercise, 
https://{your_tenant_fqdn}/SAAS/jersey/manager/api/scim/Users.

1. Select **GET** for the verb.
2. Click **Send**.
3. Scroll down to view the response.
4. Observe the results returned by the query,

Feel free to scroll through the response to confirm the other details of the returned users.
Create a Weblink Application in Identity Manager

You can also manage applications in Identity Manager using the API. Let's explore how to create a weblink type application using the APIs.

Setup the Request Headers

1. Select **POST** as the verb.
2. Enter `https://{your_tenant_fqdn}/SAAS/jersey/manager/api/catalogitems` for the request URL.  
   
   **NOTE** - Remember to replace `{your_tenant_fqdn}` with your VMware Identity Manager Tenant Fully Qualified Domain name (FQDN).
3. Click the **Headers** tab.
4. Change the **Content-Type** Header **Value** to `application/vnd.vmware.horizon.manager.catalog.webapplink+json`.
5. Change the **Accept** Header **Value** to `application/vnd.vmware.horizon.manager.catalog.webapplink+json`.
Setup the Request Body

1. Click the **Body** tab.
2. Select **Raw**.
3. Leave the Formatting as **Text**. Typically you would choose application/json or application/xml, depending on what format you were working in, but changing this to application/json will update the Content-Type header we just updated back to application/json, which will cause the request to fail. The formatting selection here is only for Postman to assist you in setting up the request correctly, the Text formatting option has no impact on the API request itself.
4. For the Body, enter the below JSON data.

   ```json
   { "catalogItemType": "WebAppLink", "uuid": "85c040cf-b389-41a0-9efe-c7ca64f985c4", "packageVersion": "1.0", "name": "API Generated Weblink", "productVersion": null, "description": "Web Link Generated by API Lab", "authInfo": { "type": "WebAppLink", "targetUrl": "https://www.vmware.com" } }
   ```
5. Click **Send**.
1. Scroll down to see the response.
2. Confirm the status shows **201 Created**, confirming the application was created.
3. Click the **Body** tab.
4. Find the **uuid** value in the response, it should match the uuid we provided in our request body (85c040cf-b389-41a0-9efe-c7ca64f985c4). **Highlight** this value (NOT including the quotation marks) and **right-click**.
5. Click **Copy**.

We will be using the uuid of the created weblink application
1. Click the **Notepad** icon from the Task bar.
2. Type `Created Application UUID:` and **right-click** at the end of the text.
3. Click **Paste** to insert the uuid.
In later steps when prompted to use the created application uuid, refer to the value you've pasted here.
Entitle the Local User to the Weblink App

Our created Weblink application currently has no entitled users, meaning no one can currently access our created application. We can update the entitlement of this application to include our created local user from earlier, allowing them to access the application in Identity Manager.

Setup the Request Headers

1. Select **POST** as the Verb.
2. Enter `https://{your_tenant_fqdn}/SAAS/jersey/manager/api/entitlements/definitions` for the Request URL.
   
   **NOTE** - Remember to replace `{your_tenant_fqdn}` with your VMware Identity Manager Tenant Fully Qualified Domain name (FQDN).
3. Click the **Headers** tab.
4. For the Content-Type Header **Value**, enter `application/vnd.vmware.horizon.manager.bulk.sync.response+json`
5. For the Accept Header **Value**, enter `application/vnd.vmware.horizon.manager.bulk.sync.response+json`
Setup the Request Body

1. Click the **Body** tab.
2. Select **Raw**.
3. Leave the Formatting as **Text**. Same as before, we don't want to change this as Postman will automatically update the Content-Type Header to reflect this field, and changing this back to application/json will cause the request to fail.
4. Enter the below JSON data for the Body.

   ```json
   { "returnPayloadOnError": true, "operations": [ { "method": "POST", "data": { "catalogItemId": "{YOUR_WEBLINK_UUID}", "subjectType": "USERS", "subjectId": "{YOUR_CREATED_USER_ID}", "activationPolicy": "AUTOMATIC" } } ], "_links": { } }
   ```
5. Replace the `{YOUR_WEBLINK_UUID}` text with the **Created Application UUID** value from your Notepad file. **DO NOT** remove the surrounding quotation marks!
6. Replace the `{YOUR_CREATED_USER_ID}` text with the **Created User ID** value from your Notepad file. **DO NOT** remove the surrounding quotation marks!
7. Click **Send**.
View the API Response

1. Scroll down to view the API response.
2. Ensure the Status shows 200 OK, confirming that the bulk operations request was completed successfully.
3. Click the **Body** tab.
4. Ensure the **code** field from the operations array shows **201**. This shows that our operation to update the catalogItemId with our subjectId was successful. If we had included multiple operations in our JSON body, you would see a status response for each operation noting the result.

Confirm the Application Entitlement in the Identity Manager Administrator Console
Return to the Identity Manager Administrator Console.

1. Click **Catalog**.
2. Click the **checkbox** next to **API Generated Weblink** to select it.
3. Click **Assign**.

### View the API Generated Weblink Assignments

1. Confirm that the **API User** is already included in the list of Users and that the Deployment Type is set to **Automatic**. This entitlement was added based on the specifications we included in our JSON Body with the API request.
2. Click **Close**.

### Test the Weblink Application as the Created user

We will now login to the Workspace ONE portal as our created user to confirm that we see the created application and that it launches successfully.

### Logout of the Identity Manager Administrator Account
1. In the top-right corner of the Identity Manager Administrator Console, click the **Tenant Admin** dropdown.
2. Click **Logout**.

**Go Back to the Login Page**

Click **Go back to the login page**.
Login as the Created User

1. Enter `apiuser` for the Username.
2. Enter `VMware1!` for the Password.
3. Click `Sign in`. 
View the Application Catalog

1. Click the Catalog tab if not already selected.
2. Confirm the API Generated Weblink application exists. Click Open.

Confirm the Weblink Application Opens

2. Click the Close button to close the tab.
Instructions for Taking Additional Lab Modules

If you are interested in taking additional modules for this lab, please click the END button in the VMware Learning Platform and then relaunch the lab.

Since each module in this lab takes advantage of configuring VMware Identity Manager and the VMware Identity Manager Connector for different use cases, the quickest way to start with a clean infrastructure to complete the next module is to restart the lab. Once you restart, navigate to the next module using the Table of Contents as shown in the Lab Guidance section.
Conclusion

In this lab, you've learned how the IDM API can be used to automate a variety of administrative tasks. For additional API documentation, be sure to check out the VMware Identity Manager API Reference page: https://code.vmware.com/apis/57/idm?h=Identity#/. 
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-1957-02-UEM

Version: 20190409-185430