Table of Contents

Lab Overview - HOL-1951-03-VWS - VMware Workspace ONE Advanced .......................... 2
   Lab Guidance ................................................................................................................. 3
Module 1 - Installation and Configuration of VMware Identity Manager (30 minutes) ........... 9
   Introduction .................................................................................................................... 10
   Power on Appliance ....................................................................................................... 12
   Deployment Options for On-Premise VMware Identity Manager .................................. 14
   Deploy VMware Identity Manager Appliance .............................................................. 15
   Run Setup Wizard ......................................................................................................... 24
   Configuration of VMware Identity Manager ............................................................... 31
   Administration Console Walk-Through ........................................................................... 54
   Conclusion ..................................................................................................................... 72

Module 2 - Integrating Workspace ONE with Horizon 7 (60 Minutes) ................................ 74
   Introduction .................................................................................................................... 75
   Prepare for Horizon Integration with Identity Manager .................................................. 77
   Configure SAML Authentication .................................................................................... 80
   Configure Horizon Pods and Pod Federations in VMware Identity Manager ................. 89
   Launching Horizon Desktops and Applications from Workspace ONE .......................... 102
   Configure Access and Network Policies and Client Access URL .................................. 115
   Launching Horizon Desktops with Deny Access Policy Rule ......................................... 134
   Conclusion ..................................................................................................................... 138

Module 3 - Configure MFA using RADIUS in Workspace ONE (15 Minutes) ....................... 140
   Introduction .................................................................................................................... 141
   Setup RADIUS as an Authentication Adapter .............................................................. 143
   Create Network Range and modify policy .................................................................... 148
   Verify functionality ....................................................................................................... 158
   Conclusion ..................................................................................................................... 167

Module 4 - Integrating Workspace ONE with SAML Based Web Applications (30 minutes) ... 169
   Introduction .................................................................................................................... 170
   Create Web Based Application Shortcut ...................................................................... 172
   Add SAML based Web Application and SSO Configuration .......................................... 183
   Conclusion ..................................................................................................................... 201

Module 5 - Configure Failover and Redundancy for Workspace ONE (15 Minutes) ............... 204
   Introduction .................................................................................................................... 205
   Configure Highly Available Single Site ......................................................................... 206
   Configure Highly Available Multi-Site .......................................................................... 210
   Conclusion ..................................................................................................................... 212
Lab Overview - HOL-1951-03-VWS - VMware Workspace ONE Advanced
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.

In this lab you will learn how to install and configure VMware Identity Manager (vIDM) on-premise deployment. How to integrate Workspace ONE with Horizon 7 and Web Applications. You will also learn about configuring Workspace ONE with a RADIUS-based 2-Factor Authentication solution. Followed by walking through the process of configuring Workspace ONE for high availability.

Lab Module List:

- **Module 1 - Installation and Configuration of VMware vIDM** (30 minutes)  
  (Advanced) Walk through the installation and configuration of the VMware Identity Manager
- **Module 2 - Integrating Workspace ONE with Horizon** (60 minutes)  
  (Advanced) Walk through the integration of Horizon 7 with Workspace ONE to deliver desktops and apps
- **Module 3 - Configure MFA using RADIUS in Workspace ONE** (15 minutes)  
  (Advanced) Learn how to configure a RADIUS compatible authentication adapter
- **Module 4 - Integrating Workspace ONE with SAML Based Web Applications** (30 minutes)  
  (Advanced) Learn how to add web applications and configure single-sign-on with SAML 2.0
- **Module 5 - Configure Failover and Redundancy or Workspace ONE** (15 minutes)  
  (Advanced) Learn how to design a highly available Workspace ONE deployment in both single- and multi-site implementations

Lab Captains:

- **Module 1 - Pamela Norris, Staff TAM/DWS TAS, USA**
- **Module 2 - Josh Spencer, EUC Tech Marketing Architect, USA**
- **Module 3 - Karsten Giessen, Staff Solutions Engineer, USA**
- **Module 4 - Karsten Giessen, Staff Solutions Engineer, USA**
- **Module 5 - Josh Spencer, EUC Tech Marketing Architect, USA**

This lab manual can be downloaded from the Hands-on Labs Document site found here:
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 cannot 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 your lab has not changed to "Ready", please ask for assistance.
Module 1 - Installation and Configuration of VMware Identity Manager (30 minutes)
Introduction

In the module you will cover the installation and configuration of a single, on-premise version of VMware Identity Manager (vIDM). Once the configuration has been completed, you will review features and functionality available in the Administration Console.

What is Workspace ONE?

Workspace ONE provides the ability to simply deliver and manage any app on any device. It delivers on consumer-simple expectations like one-touch access to nearly any app, from any device, optimized with AirWatch Conditional Access. Empowering employees to get productive quickly with a self-service app store while giving IT a central place to manage user provisioning and access policy with enterprise-class directory integration, identity federation and user analytics expected from the leader of hybrid cloud infrastructure.
What is VMware Identity Manager?

VMware Identity Manager (vIDM) is the name of the appliance that runs Workspace ONE. It is also a software layer that resides in the appliance that provides identity-related components, including authentication for users who single sign-on to resources in VMware Workspace ONE. You can create a set of policies that relate to networking and authentication to control access to these resources.

What are the Key Benefits?

Providing an environment where employees can be both happy and productive; removing the traditional barriers to mobility like complex passwords, configuration steps, traditional VPNs and tokens by uniquely optimizing authentication for each device type rather than the lowest common denominator. Free the business to roll out new SaaS and mobile apps and services immediately to forever change business processes and customer engagement while maintaining a single point of user entitlement and license monitoring. Simplify IT by leveraging existing directory infrastructure and extend to SaaS and mobile apps with automated provisioning, utilization reporting and conditional access policies.
Power on Appliance

Due to the length of time it takes to power on the appliance in a lab environment, you will execute that task first. Once you have powered on the appliance, continue on with the lab while the boot process is taking place.

Launch Browser

1. From the main console, double-click on **Google Chrome**

Login to the vSphere Client

The vSphere HTML client login screen should appear. If not navigate to https://vcsa-01.corp.local

1. Select **Use Windows session authentication**
2. Click on **Login**
Power On the VM

1. Under the RegionA01-COMP01 cluster, right click on the **vIDM-02** vm
2. Select **Power**
3. Select **Power On**

This process may take up to 15 minutes in this lab environment. Please continue on with the lab. You will navigate back to the appliance at a later point in time.
Deployment Options for On-Premise VMware Identity Manager

VMware Identity Manager (vIDM) offers both a Windows and Linux deployment option. The Windows version can be installed on Windows Server 2008 R2, 2012 R2, or 2016. The Linux based virtual appliance runs SUSE Linux Enterprise 11, and comes as a virtual appliance. In this case we will be using the Linux based virtual appliance.

In this lab, we have a single node vIDM deployment, which is common during a proof of concept. In a production environment VMware recommends a 3 node clustered configuration to maintain full functionality. More information on clustering vIDM can be found in the module 5 of this lab to get more information on how to deploy vIDM for high availability.
Deploy VMware Identity Manager Appliance

In this chapter, we will walk through the process of deploying the Identity Manager (vIDM) Linux appliance. This chapter is strictly theoretical with no steps to be performed.

Configure DNS

![Forward Lookup Zone]

These steps are not to be performed in the Lab environment.

The vIDM appliance requires both forward (A-record) and reverse (PTR-record) DNS records.

As you can see, both have been configured for the vIDM appliance vIDM-02.

Time Sync

![Time Configuration]

vIDM is sensitive to time differences between the systems it integrates with. For example, the maximum skew time for SAML is 30 seconds.
You should confirm Time Configuration is set up and running on the ESXi host(s) in which vIDM will reside. The appliance will pick up the correct time from the ESXi host. When integrating vIDM with Active Directory it is important that the ESXi hosts and your domain controllers are time synced to the same source.

Note: The following screen captures used the vSphere Web Client.

**These steps are not to be performed in the Lab environment.**

To confirm the host has time configured:

1. Within vCenter, click on `esxi-03a.corp.local`
2. Select the **Configure** tab
3. Expand **System**
4. Select **Time Configuration**

As you can see NTP Client is running on the host, configured with IP Address 192.168.100.1.

**Deploy the Virtual Appliance**

Once all prerequisites are in place and you have downloaded the vIDM Storage Virtual Appliance (SVA) from [my.vmware.com](http://my.vmware.com), you are ready to begin the deployment process. In this lab the appliance has been uploaded for you. For informational purposes you will review the process for uploading the appliance.

The vSphere Flash Client, was used for this example of deploying the vIDM appliance.

**These steps are not to be performed in the Lab environment.**

1. Right click on `esx-03a.corp.local`
2. Select **Deploy OVF Template**
These steps are not to be performed in the Lab environment.

1. Select Choose Local File, then Browse. Navigate to the OVA file
2. Click on Next

Select Datacenter to place Appliance

Now you need to select the datacenter where the virtual appliance will be placed.

These steps are not to be performed in the Lab environment.

1. Select RegionA01
2. Click on Next
Select Cluster to place Appliance

Then you will select the cluster

**These steps are not to be performed in the Lab environment.**

1. Select the **RegionA01-COMP01** cluster
2. Click on **Next**

Review Details

<table>
<thead>
<tr>
<th>Product</th>
<th>IdentityManager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>3.2.0.1</td>
</tr>
<tr>
<td>Vendor</td>
<td>VMware, Inc.</td>
</tr>
<tr>
<td>Publisher</td>
<td><strong>VMware, Inc.</strong> (Trusted certificate)</td>
</tr>
<tr>
<td>Download size</td>
<td>2.6 GB</td>
</tr>
<tr>
<td>Size on disk</td>
<td>3.9 GB (thin provisioned)</td>
</tr>
<tr>
<td></td>
<td>60.2 GB (thick provisioned)</td>
</tr>
</tbody>
</table>

**These steps are not to be performed in the Lab environment.**

1. Review Details, click on **Next**
Accept License Agreements

These steps are not to be performed in the Lab environment.

1. **Accept** License Agreement
2. Click on **Next**
Select Storage Placement

These steps are not to be performed in the Lab environment.

1. Select **ESX02a-Local**
2. Click on **Next**

Note: Local storage was used for the purposes of this lab. In a production environment, shared storage should be selected.
Select Network

Choose the Destination Network you would like vIDM to use.

These steps are not to be performed in the Lab environment.

1. Select the drop down in the Destination Network field
2. Click on VM-RegionA01-vDS-COMP
3. Click Next
These steps are not to be performed in the Lab environment.

On the Customize Template screen:

1. **Scroll Down**
2. Enter the correct **networking information**
3. Click on **Next**
Complete Deployment

These steps are not to be performed in the Lab environment.

1. To Complete the deployment, click on **Finish**
Run Setup Wizard

Once the OVA file has been deployed, the remainder of the initial setup takes place in the GUI based Identity Manager Appliance Setup Wizard.

Note: All additional steps moving forward are to be done in the lab unless otherwise noted.

Confirm you are still logged into the vSphere Client

First we must confirm that the virtual appliance vIDM appliance vIDM-02 has booted up.

1. Confirm you are still logged into the vSphere Client

If you are logged in go directly to the Navigate to the vIDM Appliance step. If you need to log back into the vSphere Client, continue on to the next step.

Navigate to the vSphere Client

1. If you are not logged into the vSphere client, from Google Chrome, click on the vCenter bookmark
2. Select the RegionA vSphere Client (HTML) shortcut
Login to the vSphere Client

1. Select the **Use Windows session authentication** check box
2. Click on **Login**

Navigate to the vIDM Appliance

1. Right click on **vIDM-02**
2. Select **Open Remote Console**

Confirm Boot Up Process is Complete

If you see a plain black screen you can continue on to **Open Additional Browser Tab** step.

1. If the console states **Waiting for Application Server to start**, wait for the boot up process to be completed. Note the entire boot up process can take 5-10 minutes in this lab.
2. Once completed the blue login screen will appear, and you can continue
Open Additional Browser Tab

1. From Google Chrome, open another tab

Launch Administration Console

1. Open the WS1 shortcut folder
2. Select the New vIDM shortcut
Google may warn you that the connection to vIDM is not secure. This is due to the fact that we use self signed certs that were configured automatically when the appliance was deployed. VMware highly recommends replacing self signed certs with ones that are assigned by a Certificate Authority when running in production. More information on SSL can be found later on in this lab.

1. Select **Advanced**
2. Click on **Proceed to vidm-02.corp.local (unsafe)**
VMware Identity Manager Appliance Setup Wizard

Welcome to VMware Identity Manager Appliance Setup wizard.
You will be guided through the steps necessary to set up the appliance.
To complete the configuration, make sure you have this information available:
- Database configuration information

1. To start the VMware Identity Manager Appliance Setup wizard, click on **Continue**

Specify Administrative Passwords

Your first task is to set passwords for different administrative accounts. It is important to note, that by default, the root account is not granted SSH access to the appliance.
1. Specify **VMware1**! as the password for the Admin user - This is the built in account for the Web Admin User
2. Specify **VMware1**! as the password for the root user - Root account for the vIDM appliance
3. Specify **VMware1**! as the password for the sshuser - This account has has shell access to the appliance
4. Click **Continue**

**Select Database**

vIDM comes with an embedded PostgreSQL database. VMware also supports various versions of SQL. Please review the [Interoperability Matrices](#) for information on specific versions of SQL supported. The embedded database is not recommended for a production environment. For high availability or multi-datacenter deployments with the SQL database, please consult SQL documentation.

For the purposes of this lab you will be using the embedded database.

1. Confirm the **Internal Database** is selected
2. Click on **Continue**

**Processing the Database**

Processing...

```
Configuration of the database and application setup is in progress. 
Do not press the Back button. This process can take some time.
Configuring database connection...
```
Setting up the database can take up to 5 minutes. Please be patient. Do not navigate away or refresh this page, until the creation process has finished.

Initial Setup Completed

1. Confirm the Setup is complete
2. Click on the Log into the administration console link
Configuration of VMware Identity Manager

In this chapter you will learn how to complete the configuration process using the Administration Console.

Log into the Administration Console

Here you have the login screen for the Administration Console

1. Specify **admin** as the user. This is the Appliance Administrator Account.
2. Type **VMware1!** as the password
3. Click **Sign in**
Modify User Attribute Requirements in VMware Identity Manager

vIDM utilizes User Attributes, defined in your identity source, to filter which users and groups should be synchronized with vIDM.

1. Confirm you are on the **Identity & Access Management** tab
2. Click on **Setup**
3. Select **User Attributes**
Select Attribute

In certain cases, a specific User Attribute will be required to integrate with another solution. The distinguishedName needs to be set for the vIDM directory that is mapped to Active Directory. The integration of Horizon requires the userPrincipalName attribute. A required attributes can not be changed from optional to required after a directory has been created.

1. Scroll down
2. Select the check box next to distinguishedName
3. Select the check box next to UserPrincipalName
4. Click on Save

Click on Manage

1. In the upper right hand corner, click on Manage
Add Directory

Add Directory supports Active Directory, LDAP, or Local Users directories. In this lab we use Active Directory. If you choose to use LDAP in your environment as your identity source, be aware there are certain limitations that exist, such as you can not join vIDM to an LDAP domain. To find out more on the restrictions when using LDAP click [here](#).

1. Select **Add Directory**
2. Click on **Add Active Directory over LDAP/IWA**

Add Directory Name

Add Directory

Directory Name*

1. Enter **corp.local**

Active Directory over LDAP binds the vIDM connector to AD using simple BIND authentication.

Active Directory (Integrated Windows Authentication) binds the vIDM connector to AD using Integrated Windows Authentication.

2. Select **Active Directory (Integrated Windows Authentication)**
Join Domain Details

1. Scroll down
2. Confirm you are on the **Join Domain Details** section
3. Enter Domain Name: **corp.local**
4. Enter Domain Admin Username: **administrator**
5. Enter Domain Admin Password: **VMware1!**

Bind User Details

1. Scroll down
2. Confirm you are on **Bind User Details** section

vIDM does not have the ability to write or modify objects within Active Directory. So the Bind user accounts only requires read access to the User and Group accounts you wish to sync. If the BIND user account expires, it must be reset in Active Directory. VMware recommends using a BIND password that does not expire in order to avoid affecting the health of the vIDM environment.

3. Enter the Bind User UPN: **administrator@corp.local**
4. Enter Password: **VMware1!**
5. Click on **Save & Next**
Select Domain

1. Confirm corp.local is checked
2. Click on Next

Confirm User Attributes

<table>
<thead>
<tr>
<th>Attribute Name in VMware Identity Manager</th>
<th>Attribute Name in Active Directory</th>
<th></th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>lastName</td>
<td>sn</td>
<td></td>
<td></td>
</tr>
<tr>
<td>firstName</td>
<td>givenName</td>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>email</td>
<td>mail</td>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>userName</td>
<td>sAMAccountName</td>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>phone</td>
<td>telephoneNumber</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Make note how the User Attributes align with what had been configured previously in this lab.

1. Click on Next
### Add Groups DN

Select the groups you want to sync

Enter the Group DN 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. Confirm **Sync nested group members** is checked
2. Click on the green + symbol
3. Enter: `cn=users,dc=corp,dc=local`
4. Click on **Find Groups**

#### Select Group

Select the groups you want to sync

Enter the Group DN 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.

<table>
<thead>
<tr>
<th>Specify the group DN</th>
<th>Select All</th>
<th>Groups to sync</th>
<th>Mapped Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn=users,dc=corp,dc=local</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The list of groups that meet the DN criteria is 29. Now you need to specify out of the 29 groups, which one(s) would you like to sync to vIDM.

1. Click on Select

Define Group

29 Group(s) found for: cn=users,dc=corp,dc=local

1. Enter Domain Users in the search box
2. Check the box next to Domain Users
3. Click on Save

Verify Groups DN

1. Notice how Groups to sync is now listed at 1 of 29, reflecting the Domain Users group you choose
2. Confirm **cn=users,dc=corp,dc=local** is listed under the Group DN
3. Click on **Next**

### Specify Users DN

Enter the User DNs to sync, for example, **CN=Username,CN=Users,DC=example,DC=company,DC=com**. All users found under the DN are also synced. To exclude any users from syncing, provide exclusion filters.

1. Click on the green **+** sign
2. Enter **cn=Users,dc=corp,dc=local**
3. Click on **Next**

Now you are ready to specify the Active Directory user accounts you want to sync with vIDM.

1. Click on the green + sign
2. Enter **cn=Users,dc=corp,dc=local**
3. Click on **Next**
# Review Sync Operation

<table>
<thead>
<tr>
<th></th>
<th>Add</th>
<th>Remove</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>34</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Groups</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

1. Verify number of objects for Users and Groups matches what is shown in the picture
2. Click on **Sync Directory**

Note: If you do not see the correct number of objects listed, click on the Edit User or Group DNs, and check for typographical errors in the DN names.

## Import Status

A message will appear indicating a directory sync has started. The sync operation is very quick in this small lab environment. You do not have to wait until sync status is changed in order to move ahead to next step.
Role Based Access Control

1. Click on the Roles tab

Note: Roles may be hidden behind the search box, depending on what your screen resolution is set to.

Role Based Access Control (RBAC), allows you to define specific roles that an administrator is granted within vIDM. Starting with vIDM 3.2, you can control what a given administrator can and cannot modify within the console. By default there are three different levels of administrators.

- The Super administrator role is granted full access to the console.
- Directory Admin has the ability to manage users, groups, and directories. However they are not permitted to make modifications to settings such as authentication policies and application configurations.
- A read-only administrator is granted read access to the Administrator Console.

Assign User Account to an Existing Role

In this lab we will be using a domain administrator account to complete the configuration of vIDM. By default, a domain administrator account from a domain
defined in vIDM will be given ReadOnly Admin role rights in vIDM. For the purposes of this lab, we will be adding the domain administrator account "administrator" to the Super Admin role. In a production environment, you would typically assign a group to this role.

1. Check **Super Admin**
2. Click on **Assign**

### Enter User Account

![Image showing user account entry]

1. Enter **administrator**
2. Select **Corp, Administrator**

### Confirm Assignment

![Image showing assignment confirmation]

1. Confirm **Corp, Administrator** is listed
2. Click on **Save**
Create a Custom Role

You also have the ability to create a custom role.

Note: Depending on your screen resolution, the Roles tab may be hidden behind the search box.

1. Confirm you are still on the Roles tab
2. Click on Add

Add Role

1. Enter the Role Name: vIDM Lab Admin
2. Description: vIDM Lab Admin Role
3. Click on Next
Service Definition

You will now define what service(s) the role will have access to.

1. Click on pencil next to Role Administration

Assign Resources

1. Click on the drop down arrow, in the Actions box.
2. Select Read
3. Click on Save
Confirm Definition

1. Confirm Actions and Resources is set to **Read All**
2. Anyone assigned to this role would be limited to viewing the Roles and corresponding assignments.
3. Click on **Save**

Assign Role

Now you will assign the role you just created to a user.

1. Check the **vIDM Lab Admin** role
2. Select **Assign**
Enter Username

1. Enter user3mod1 in the search box
2. Select User3, mod1

Confirm Username

1. Confirm User3, mod1 is listed
2. Click on Save

Confirm Role has been Applied

Now you will test if the new role has been applied.
Logout as Current Admin

1. Click on the arrow next to Local Admin
2. Select Logout

Navigate to Login Page

1. Click on Go back to login page

Select Domain

Notice how you now have a domain option when logging into vIDM. This is because you added it to Active Directory earlier in this lab.

1. Confirm corp.local is listed as the domain you want to login to
2. Click on Next
Sign in as User

1. Enter username: **user3mod1**
2. Password: **VMware1!**
3. Click on **Sign in**

Navigate to Administration Console

1. Click on the **drop down arrow** next to the profile picture
2. Select **Administration Console**
Create New Role

Now you will try to create a new role using the user3mod1 account

Note: Depending on resolution the Roles button may be behind the search bar.

1. Click on the Roles Tab
2. Click on Add

Name Role

1. Enter the Role Name: Test Role 2
2. Click on Next
Select Service

1. Click on the pencil next to **Role Administration**

Select Resource

1. Click the arrow in the **Actions** field
2. Select **Read**
3. Click on **Save**
Verify Action

1. Confirm the Role Administration Action is set to **Read**
2. Click on **Save**

Exit Role Manager

1. You will see a pop up at the top of your screen informing you that **You don't have permission to perform this operation.** This is because user1mod3 only has Read Access to the Role Administration Role.
If you do not see the pop up, click on Save again. The warning is only displayed for about 2 seconds.

2. Click on **Cancel**

**Log Out**

1. In the upper right had side, click on the drop down arrow next to **User3mod1**
2. Select **Logout**

**Sign In**

You will need to be signed in as administrator in order to complete the remainder of the lab.

1. Click on **Sign in**
Sign in as Administrator

1. Enter username: administrator
2. Enter password: VMware1!
3. Click on Sign in

Navigate to Administration Console

1. Click on the drop down arrow next to the profile
2. Click on Administration Console
Administration Console Walk-Through

The VMware Identity Manager (vIDM) Administration Console provides you the ability to manage users, groups, resources, entitlements, and access policies. In this chapter we will take a tour of the features and functionality of Administration Console

Dashboard

The dashboard section of the Administration Console is where you go to gain an overview of utilization, health, and wellness of your environment.

User Engagement Dashboard

The very first thing that an administrator sees when they logon to the administration console is the User Engagement Dashboard. This dashboard is used to monitor user and resource usage.

In the Users and Groups window, you see 41 Users and 2 groups. This is the comprised list of users and groups from the system and Active Directory domain.

You may also have noticed that the Application and Client activity windows have no information listed. That is because applications have not been configured or accessed yet.
Systems Diagnostics Dashboard

1. Click on Dashboard
2. Select System Diagnostics Dashboard

Review Dashboard

The System Diagnostics Dashboard shows the status of the appliance, if any modules are not functional, which database you are using, if any admin passwords are expiring, and so on.
Reports

1. Select the down arrow next to **Dashboard**
2. Click on **Reports**

Select Report

As you can see, vIDM comes with a variety of built-in reports. These reports can be used to view resource usage along with tracking user and group activates.

2. Click on **Recent Activity**

Select Activity Range

1. Confirm **Past day** is selected
2. Click on **Show**
Review Recent Activity

There are various tasks listed. You could click on Show Events for more information on a particular event or Export the Recent Activity list to a CSV.

Note: If you do choose to explore other reports, please be aware there may be no data available, due to the fact the vIDM deployment is new, the data required for said reports has not been generated yet.

Users and Groups

1. Click on the Users & Groups tab
2. Note the ones that list Domain as **corp.local**. These are the accounts that were imported from Active Directory when you added the Directory earlier in the lab
3. The accounts labeled as **System Domain** are the local vIDM accounts
4. Click on Add User
Add User

1. Click on the drop down arrow in the Directory List search box

Notice how you can only add a user to the System Directory. That is because vIDM can only read from Active Directory (AD), it can not write or modify an object. If you needed to add a new user or group to vIDM from AD, you would need to add them to AD first then sync the directory.

2. Click on Cancel

Password Settings

1. Click on Settings
Password Policy

Password Policy for Local Users

Password Restrictions

The default password policy requires 8 characters. Configure the fields to include a combination of uppercase, lowercase, numerical, and special characters to add more restrictions.

- Minimum length for passwords: 6
- Lowercase characters: 0

The Password Policy for Local Users allows you to configure the password policies for the accounts that reside in the System Directory.

Catalog

1. Click on drop down arrow next to catalog Catalog

The catalog tab allows you to define your Web Apps and Virtual Apps that you wish to publish on the Workspace ONE portal.

Web Apps are considered Software as a Service (SaaS) based applications. With Web Apps, you have the ability to enable approvals. Once approvals have been activated, vIDM can integrate with a third party approval system. As soon as a user makes a request for an application that is located in the catalog an approval sequence is initiated. The request must then be approved before a user will be allowed to launch the application.

Virtual Apps are published applications such as Horizon, Horizon Cloud, or Citrix-Published Applications. To walk through the process of publishing a Horizon desktop please review Module 2 of this lab.
Navigate to Settings

1. Under Catalog, click on **Settings**

**Global Settings**

Settings are where you go to define the look and feel of the Workspace ONE portal.

1. Under **Global Settings**, the Disable launcher feature prevents the user from being prompted every time they access Workspace ONE from said device. This is a good option, when users are accessing Workspace ONE from a Workspace ONE UEM managed device.
Remote App Access

1. Click on Remote App Access

When configured, Remote App Access provides a group of clients the ability to register dynamically with Workspace ONE.

User Portal Branding

1. Click on User Portal Branding

User Portal Branding is where you can modify the colors and company logo to be used on the Workspace ONE portal.
User Portal Configuration

Starting with vIDM 3.2 you can control what tabs the user sees when they logon to the Workspace ONE portal.

1. **Click on User Portal Configuration**

2. **Hide Catalog tab** prevents users from adding additional applications to their Bookmark tab. This would limit the users to only see the applications that have been predefined by the administrator.

3. **Hide Bookmark tab** prevents users from viewing a subset of applications they or the administrator has identified as frequently used apps.

4. **Show recommended apps in Bookmarks tab** populates the Bookmark tab with applications that are labeled as recommended.

If either the Catalog or Bookmark tab is hidden, a user will no longer have the ability to bookmark an application.

A user portal view is refreshed to reflect the changes made in this section every 24 hours. You can also perform a manual sync via CLI.
New End User Portal UI

1. Click on **New End User Portal UI**.

After you have upgraded your vIDM environment, you can click on Enable New Portal UI to enable the latest user interface that is available when applicable.

People Search

1. Click on **People Search**

People Search allows employees in an organization to search for their colleagues and view user details. The AirWatch People Search application is required. For more information on how to configure People Search please consult the [VMware People Search Admin Guide](#).
1. Click on the **Identity & Access Management** tab

The Identity & Access Management tab contains options for how a user will access the environment. You visited this section earlier when integrated Active Directory with vIDM. We will now take a look at some additional features.

**Identity Provider**

1. Click on **Identity Providers**

Identity Providers are systems used to authenticate a user. The built-in System Identity Provider and the Active Directory for corp.local are listed.

<table>
<thead>
<tr>
<th>Identity Provider Name</th>
<th>Auth Methods</th>
<th>Directory</th>
<th>Network Ranges</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Identity Provider</td>
<td>Password (Local Directory)</td>
<td>System Directory</td>
<td>ALL RANGES</td>
</tr>
<tr>
<td>Built-In</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WorkspaceIDP_1</td>
<td>Password</td>
<td>corp.local</td>
<td>ALL RANGES</td>
</tr>
</tbody>
</table>
Password Recovery Assistant

1. Click on **Password Recovery Assistant**

Here we can provide information to a user who is unable to login due to a password issue. When a user clicks on Forgot Password on the main login page, the message you define will be displayed. A message typically can contain information on where to go to get their Active Directory account reset. Possibly an email address of the help desk or a link to a third party that allows the user to do password resets or unlock themselves.

2. Click on **Custom Message**

3. Enter a message you feel would be appropriate

4. Check **Show detailed message to End User when authentication fails**

5. Click **Save**
In this case, I want the user to know why they are unable to login

5. Click on **Save**

**Authentication Methods**

The Authentication Methods for Built-in Identity Providers page is used to configure authentication methods that can be associated with identity providers defined in vIDM. Once configured, you then create access policies to apply to the authentication method.

1. Click on **Authentication Methods**

Navigate to Setup

1. Click on **Setup**
Custom Branding

1. Select **Custom Branding**

Custom Branding allows you to modify the look and feel of the tabs within the browser as well as the Workspace ONE sign-in screen.

2. Notice how the browser tab states **VMware Workspace ONE**
3. For Company Name enter: **My Company**
4. Product Name enter: **WO**
5. Click on **Save**

Refresh Browser

1. Click on **refresh** button of your browser
2. Notice the tab has changed to **My Company WO**
Navigate to Setup

When you refreshed your browser to reflect the name change vIDM automatically switches you back to the Manage option.

1. Under the Identity & Management Access Tab click on Setup

Terms of Use

1. Click on Terms of Use
2. Check box to Enable Terms of Use
3. Click on OK to Enable Terms of Use

Once the Terms of Use has been enabled, a user will not be able to access their application catalog until they have accepted the agreement. This setting only applies to the Workspace ONE client. It does not apply when accessing the Workspace ONE Portal through a web browser.
Add Terms of Use

1. Select **Add New Terms of Use**

Example of Terms of Use

Here is where you would enter the terms of use. This picture shows an example of terms of use.

1. Since we will not be using a Terms of Use in this lab, click on **Cancel**.
Appliance Settings

1. Click on the **Appliance Settings** tab

In this tab you have the option to configure the appliance, enter the license number, configure SMTP alerts, as well as choose if you would like to participate in the user experience program (Telemetry).

2. Click on **Manage Configuration**

**Navigate to Appliance Settings**

1. Click **here** on the redirection link to expedite the process.
Review Settings

The Virtual Appliance configuration page allows you to modify components of managing the virtual appliance.

As you see there is a variety of configurations options. We are going to go through these settings, and highlight a few of the options.

1. **Install SSL Certificates** allows you to replace the self signed certificate that is generated during the deployment of VMware Identity Manager (vIDM). VMware recommends replacing the self signed certificate with one signed by a Certificate Authority (CA) in a production environment. It is important to note that the CA certificate will only work if you include the entire certificate chain in the correct order. Details on how to do so can be found in the [VMware vIDM Installation Guide](#).

2. **Identity Manager FQDN** allows you to change the FQDN of the appliance

3. **Configure Syslog** is where you would navigate to have a copy of the logs sent to an external syslog server

4. **Change Password** to change the admin account password

5. **System Security** to change the root and Ssh user passwords

6. **Log File Locations** is where you go to create a log bundle. This is often used for diagnostic and troubleshooting purposes.
Conclusion

Congratulations! You have now completed Module 1. You should be familiar with the initial setup and configuration of VMware Identity Manager.

VMware Identity Manager Document Library

If you are looking for additional information on how to configure

- Click on this link
- Or use your smart device to scan the QRC Code.

Proceed to any module below which interests you most.

Lab Module List:

Module 2 - Integrating Workspace ONE with Horizon (60 minutes) (Advanced)
Walk through the integration of Horizon 7 with Workspace ONE to deliver desktops and apps

Module 3 - Configure MFA using RADIUS in Workspace ONE (15 minutes) (Advanced) 
Learn how to configure a RADIUS compatible authentication adapter

Module 4 - Integrating Workspace ONE with SAML Based Web Applications (30 minutes) (Advanced) 
Learn how to add web applications and configure single-sign-on with SAML 2.0

Module 5 - Configure Failover and Redundancy or Workspace ONE (15 minutes) (Advanced) 
Learn how to design a highly available Workspace ONE deployment in both single- and multi-site implementations
How to End Lab

To end your lab click on the **END** button.
Module 2 - Integrating Workspace ONE with Horizon 7 (60 Minutes)
Introduction

*PLEASE NOTE* - This module is dependent on the Workspace ONE Identity Manager configuration that was done in Module 1 of this lab.

Please be sure that you have completed the following sections of Module 1 before continuing with this module:

- Module 1 - Power on Appliance
- Module 1 - Run Setup Wizard
- Module 1 - Configuration of VMware Identity Manager

The Identity Manager server you configure in Module 1 will be used for Horizon integration in this module.

In the module you will integrate VMware Horizon 7 with an on-premise installation of VMware Identity Manager. The Identity Manager appliance has already been deployed, and you will configure it for Horizon integration.

- Lesson 1 - Prepare for Horizon integration with Identity Manager
- Lesson 2 - Configure SAML authentication
- Lesson 3 - Configure Horizon Pods and Pod Federations in VMware Identity Manager
- Lesson 4 - Launching Horizon desktops and applications from Workspace ONE
- Lesson 5 - Configure Access and Network Policies and Client Access URL
- Lesson 6 - Launching Horizon Desktops with Deny Access Policy Rule

Please note in this module we recommend using Google Chrome for the best experience. This browser has been configured to ignore self-signed certificates.

Integrating Horizon 7 with Identity Manager

Integrating VMware Horizon 7, Horizon 6, or View with the VMware Identity Manager service lets you provide users the ability to access their entitled Horizon desktops and applications from the Workspace ONE portal or app. You can integrate independent Horizon pods, which consist of Horizon Connection Server instances, and pod federations, which contain multiple pods and can span multiple sites and data centers.

You deploy and manage desktop and application pools in the Horizon Administrator interface. You also create entitlements for Active Directory users and groups in Horizon, not in VMware Identity Manager. You must sync these users and groups to the VMware Identity Manager service from Active Directory before integrating with Horizon.

To integrate Horizon pods and pod federations with VMware Identity Manager, you create one or more virtual apps collections in the VMware Identity Manager administration console. The collections contain the configuration information for the
pods and pod federations, as well as sync settings. You then sync the Horizon resources and entitlements to VMware Identity Manager.

In the VMware Identity Manager administration console, you can view the Horizon desktops and applications. You can also view user and group entitlements.

End users can run their entitled desktops and applications from the Workspace ONE portal or app. These desktops and apps can be accessed over HTML in a browser or over a supported display protocol in the Horizon Client.
Prepare for Horizon Integration with Identity Manager

In Module 1 you configured an Identity Manager appliance, which is not yet configured for Horizon integration. Please be sure you completed Module 1 of this lab before continuing with this module.

Integrating Horizon with Identity Manager enables you to sync desktop and application resources, along with entitlements (assignments) to these resources to Identity Manager.

Installing and configuring VMware Horizon 7 is outside the scope of this lab. In this section you will use the Horizon Administrator console to verify desktop entitlements, which will be used for Identity Manager integration.

Launch Chrome Browser

1. From the Desktop of the Main Console, double-click Google Chrome

Navigate to Horizon Administrator

1. Select Horizon from the bookmarks bar
2. Select Horizon-02-Admin
Login to Horizon Administrator

1. User name: **administrator**
2. Password: **VMware1!**
3. Verify Domain: **CORP**
4. Select **Log In**

Navigate to Desktop Pool

1. Expand **Catalog** and select **Desktop Pools**
2. Click *twice* on the **Manual** pool to open the properties page
Review Entitlements

1. Select **Entitlements**
2. Verify the **Domain Users** group has been entitled to the Desktop Pool

**Leave Horizon Administrator Open**

Leave the VMware Horizon 7 Administrator tab open in Chrome, as you will use it in the next lesson.
Configure SAML Authentication

Workspace ONE provides users with the ability to run Horizon applications and desktops from a user portal. Identity Manager provides single sign-on to these applications and desktops by sending SAML assertions to VMware Horizon.

In this section, you will configure SAML authentication in Horizon.

Navigate to Horizon View Administrator Tab in Chrome

1. From the Chrome browser, select the View Administrator tab

Chrome should already be running with the View Administrator tab available. If so, you can skip the following steps and proceed to Configure SAML Authentication on Horizon Connection Server.

Launch Chrome Browser

1. From the Desktop of the Main Console, double-click Google Chrome
Navigate to Horizon View Administrator

1. Select Horizon from the bookmarks bar
2. Select Horizon-02-Admin

Log In to Horizon View Administrator

1. User name: administrator
2. Password: VMware1!
3. Verify Domain: CORP
4. Select Log In

Configure SAML Authentication on Horizon Connection Server

To launch remote desktops and applications from VMware Identity Manager or to connect to remote desktops and applications through a third-party load balancer or gateway, you must create a SAML authenticator in Horizon Administrator.

A SAML authenticator contains the trust and metadata exchange between Horizon 7 and the device to which clients connect.
You associate a SAML authenticator with a Connection Server instance. If your deployment includes more than one Connection Server instance, you must associate the SAML authenticator with each instance.

**Edit Horizon Connection Server**

1. Expand View Configuration and select Servers
2. Select Connection Servers
3. Select HORIZON-02
4. Select Edit...
1. Select **Authentication**

**Workspace ONE mode**

1. Review the options on the Authentication page.

Note there are options to configure **Workspace ONE mode**.

Workspace ONE, or VMware Identity Manager (vIDM) administrators can configure access policies to restrict access to entitled desktops and applications in Horizon 7. To enforce policies created in vIDM you put Horizon client into **Workspace ONE mode** so that Horizon client can push the user into Workspace ONE client to launch entitlements. When you log in to the Horizon Client, the access policy directs you to log in through Workspace ONE to access your published desktops and applications.
In order to enable and use this feature, the **Delegation of authentication to VMware Horizon** must be set to **required**.

Workspace ONE mode will not be used in this lab.

### Enable SAML

1. Click the drop-down menu
2. Select **Allowed**

### Manage SAML Authenticator

1. Select **Manage SAML Authenticators...**
Add SAML Authenticator

1. Select Add

SAML Authenticator Form

1. Label = vIDM
2. Left-click right in the middle of the text YOUR SAML AUTHENTICATOR NAME
   Only the portion of the Metadata URL that needs to be modified will be highlighted
Metadata URL

1. Enter `vidm-02.corp.local`
   
   Be careful not to modify the rest of the Metadata URL.

2. Select **OK**

Self-Signed Certificate Warning

1. Select **View Certificate**
Accept Certificate

1. Select **Accept**

Authenticator Status - Enabled

1. Once the Authenticator is ready, select **OK**
Complete SAML Authenticator

1. Select **OK** to close the **Edit Connection Server Settings** window

**SAML Configuration Complete**

You have successfully configured your Horizon 7 Connection Server for SAML authentication.
Configure Horizon Pods and Pod Federations in VMware Identity Manager

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

You can integrate the following types of resources with VMware Identity Manager:

- Web applications
- VMware Horizon Cloud Service applications and desktops
- VMware Horizon 7, Horizon 6, and View desktop and application pools
- Citrix-published resources
- VMware ThinApp packaged applications

In this module you will configure Identity Manager for integration to an existing, on-premises VMware Horizon 7 pod.

Integrate Horizon Cloud Pod Architecture Pod Federations with Identity Manager

The Horizon Cloud Pod Architecture (CPA) feature links together multiple Horizon pods to form a single, large desktop and application brokering and management environment called a pod federation. A pod federation can span multiple sites and data centers.

While CPA is outside the scope of this lab, note that Identity Manager can be integrated with both single Horizon pods as well as CPA pod federations.
If you would like to learn more about Horizon Cloud Pod Architecture, please visit lab 1951-02.

**Integrate an Independent Horizon Pod with Identity Manager**

To integrate Horizon pods in VMware Identity Manager, you create one or more *virtual apps collections* in the VMware Identity Manager administration console. The collections contain the configuration information for the Horizon Connection Servers as well as sync settings.

**Open a New Tab in Chrome**

1. Open a **New Tab** in the Chrome browser.

You should already have Chrome running from the previous less. If so, open the new tab and proceed to [Navigate to the Identity Manager Login Page](#).

**Launch Chrome Browser**

1. From the Desktop of the Main Console, double-click **Google Chrome**
Navigate to the Identity Manager Login Page

1. Select **WS1** from the shortcut menu
2. Select **New vIDM**
Change Authentication Domain

1. The logon page is currently configured to authenticate to the corp.local domain
2. Select Change to a different domain
Choose System Domain

1. Click the drop-down menu to select a domain
2. Select **System Domain**
3. Clear the checkbox for **Remember this setting**
4. Select **Next**

The **System Directory** is a local directory that is automatically created in the service when Identity Manager is first set up. This directory has the domain **System Domain**. You cannot change the name or domain of the System Directory, or add new domains to it. Nor can you delete the System Directory or the System Domain.

The local administrator user that is created when you first set up the VMware Identity Manager appliance is created in the System Domain of the System Directory.

The System Directory is typically used to set up a few local administrator users to manage the service. In the following step you will authenticate with a local administrator account called **admin**.
Sign In to Workspace ONE as Admin

1. username = admin
2. password = VMware1!
3. Select Sign in

Forgot Password?
Change to a different domain
Verify User Attributes

1. Select Identity & Access Management
2. Select Setup
3. Select User Attributes
4. Verify distinguishedName and userPrincipalName are selected

When configuring Identity Manager to sync user accounts from Active Directory or another directory service, specific user attributes are required for Horizon integration.

If the required attributes are not populated and synced, Horizon desktops and applications may not work properly.

Create Virtual Apps Collection

You can integrate Horizon desktops and applications, Horizon Cloud desktops and applications, Citrix published resources, and ThinApp applications with VMware Identity Manager.

Beginning with the 3.1 release, these resources are managed with the new Virtual Apps Collections feature.
Navigate to Virtual Apps

1. Select the **Catalog** tab, being sure to click on the down arrow
2. Select **Virtual Apps**

Open Virtual App Configuration

1. Select **Virtual App Configuration**

Review Virtual Apps Collection Info

1. Review the **Introducing Virtual Apps Collection** page and select **Get Started** to begin configuration
Add Virtual Apps for Horizon View On-Premises

1. Select **Add Virtual Apps**
2. Select **Horizon View On-Premises**

**Configure Horizon View Virtual Apps**

There are a number of configurable options when configuring **Horizon View Virtual Apps**. Only some of these will be used for this lab. Any options not specified in the lab manual should be left as default.

**Virtual Apps Name**

![Virtual Apps Name Definition](image)
1. In the **Name** field, enter `corpHorizonApps`
2. Verify the **Sync Connector** selected is `vidm-02.corp.local`

## Horizon Pods Configuration

![Horizon Pods Configuration](image)

1. **Connection Server** = `horizon-02.corp.local`
2. **Username** = **administrator**
   - This is a domain account with administrative privileges in Horizon
3. **Password** = **VMware1!**
4. Check the box for **Sync Local Entitlements**

**Local Entitlements** refer to the desktop and application entitlements for a given Horizon pod. **Global Entitlements** refer to desktop and application entitlements across Horizon pods in a Cloud Pod Architecture (multiple pod) implementation.

In this lab you are working with a single Horizon pod so all entitlements are local.

The **Connection Server** field must use the FQDN of one of the Horizon Connection Servers.

In production Horizon implementations, it is common to configure a load-balancer virtual IP (VIP) in front of your Connection Servers. Do **not** use the VIP for this configuration step. You will configure the **Client Access URL** with the load-balancer VIP in a later exercise.
Save the Virtual Apps Configuration

1. Select **Save**

Success Message

It may take several minutes for the **virtual apps saved successfully** notification to appear, and it will only be displayed briefly.

Sync Horizon Resources to Identity Manager

1. Select **Sync** to begin syncing Horizon desktops, apps, and user entitlements to Identity Manager
Wait for Sync

It may take several minutes for the Calculating Sync Actions step to complete.

Begin Sync of Horizon Resources

1. Notice the desktop and entitlement that will sync. This is the Manual desktop pool with entitlement Domain Users you reviewed in a previous exercise.
2. Select Save to continue

Successful Sync

It may take a few minutes for the sync to start.
Wait for Sync to Complete

1. Wait for the **SYNC STATUS** to report **Started**
2. Select **Refresh**

You may need to click **Refresh** more than once. If the status does not change to **Completed**, wait a few seconds and click **Refresh** again.

Successful Sync of Horizon Resources

1. Wait for the **SYNC STATUS** to report **Completed**

Virtual Apps Sync Complete

You have successfully synced Horizon applications, desktops, and user entitlements to Identity Manager.

Leave the Workspace ONE Management Console Open

Leave the Workspace ONE Management Console tab open in Chrome, as you will use it in the next lesson.
Launching Horizon Desktops and Applications from Workspace ONE

Workspace ONE provides users with the ability to run Horizon applications and desktops from a user portal. Identity Manager provides single sign-on to these applications and desktops by sending SAML assertions to VMware Horizon.

In this section you will authenticate to Workspace ONE as an end user, then launch Horizon resources.

Log Out of Previous Workspace ONE Sessions

In this exercise you will connect to Workspace ONE using end user credentials. To do this, it is important that any existing Workspace ONE sessions are logged off.

Navigate to Existing Workspace ONE Tab in Chrome

1. Navigate to the VMware Workspace ONE tab in Chrome.

You should still have Chrome opened with a tab for VMware Workspace ONE. If so, proceed to Logout of VIDM-02. If you closed Chrome, proceed to the next step.

Launch Chrome Browser

1. From the Desktop of the Main Console, double-click Google Chrome
Navigate to Workspace ONE

1. Select WS1 from the Chrome bookmarks bar
2. Select New vIDM

Logout of VIDM-02

1. Select the drop-down menu next to the logged on user
2. Select Logout
1. Select **Go back to login page**
Verify Authentication Domain

1. Verify the domain selected is **corp.local**
2. Select **Next**
Authenticate to Workspace ONE as an End User

1. username = user1mod1
2. password = VMware1!
3. Select Sign in

Review Workspace ONE Preferences

Once logged on to Workspace ONE, your catalog of applications and desktops is available.
Navigate to User Settings

1. Select the drop-down menu next to the user avatar
2. Select **Settings**

User Preferences

1. Select **Preferences**
Review Horizon Remote Apps Configuration

Horizon Remote Apps

Opening the Horizon remote apps in the Horizon Client will give you a better experience than the browser. How would you like to launch the Horizon remote apps?

Workspace ONE is currently configured to launch apps and desktops using the Horizon Client.

While this option provides the best overall user experience, Horizon also supports HTML access for added flexibility.

Configure Horizon Remote Apps for Browser

Horizon Remote Apps

Opening the Horizon remote apps in the Horizon Client will give you a better experience than the browser. How would you like to launch the Horizon remote apps?

Successfully saved selected preference.
1. Select **Browser**
2. Select **Save**
3. Note the **Successfully saved selected preference** message.

Back to Catalog

1. Select **Back**

Launch Remote Desktop
1. Select **Open** on the **Man-Pool1** desktop pool

Identity Manager checks the network and access policy rules, then passes a SAML token to Horizon to start and authenticate to the remote desktop or application.

**VMware Horizon HTML Access**

1. The remote desktop is opened in a new **Chrome tab**
2. Click to expand the **Horizon Client** controls
Log Out of Windows

1. Select **Options** for the running VM
2. Select **Log Off**
Confirm Log Off

Log Off Desktop

Are you sure you want to log off from Man-Pool1?  
Warning: you may lose unsaved work.

1. Select **OK**
2. Select **Close**

Disconnected

You have been disconnected.

1. Select **OK**
2. Select **Close**

Sign out of Horizon HTML Access

1. Select **Options** for Horizon
2. Select **Log out**
Confirm Log Off

1. Select OK

Sign Out of Workspace ONE

1. Expand the drop-down menu
2. Select Sign Out
1. Select **Go back to login page**

Leave this page open as you will use it in the next exercise.
Configure Access and Network Policies and Client Access URL

The VMware Identity Manager service attempts to authenticate users based on the authentication methods, the default access policy, network ranges, and the identity provider instances you configure.

A policy rule can also be configured to deny access to users by network range and device type.

When users attempt to log in, the service evaluates the default access policy rules to select which rule in the policy to apply. The authentication methods are applied in the order they are listed in the rule. The first identity provider instance that meets the authentication method and network range requirements of the rule is selected. The user authentication request is forwarded to the identity provider instance for authentication. If authentication fails, the next authentication method configured in the rule is applied.

You should already be at the Workspace ONE login page. If so, skip to the Change Authentication Domain step.

Launch Chrome Browser

1. From the Desktop of the Main Console, double-click Google Chrome

Navigate to the Identity Manager Login Page
1. Select **WS1** from the shortcut menu
2. Select **VIDM-02**

**Change Authentication Domain**

1. The logon page is currently configured to authenticate to the **corp.local** domain
2. Select **Change to a different domain**
Choose System Domain

1. Click the drop-down menu to select a domain
2. Select System Domain
3. Clear the checkbox for Remember this setting
4. Select Next

The System Directory is a local directory that is automatically created in the service when Identity Manager is first set up. This directory has the domain System Domain. You cannot change the name or domain of the System Directory, or add new domains to it. Nor can you delete the System Directory or the System Domain.

The local administrator user that is created when you first set up the VMware Identity Manager appliance is created in the System Domain of the System Directory.

The System Directory is typically used to set up a few local administrator users to manage the service. In the following step you will authenticate with a local administrator account called admin.
Sign In to Workspace ONE

Authenticate to the System Domain as admin.

1. username = admin
2. password = VMware1!
3. Select Sign in
Navigate to Policies

1. Select **Identity & Access Management**
2. Select **Policies**

Network Ranges

1. Select **Network Ranges**
Add Network Range

A default network range containing all IP addresses is created by default. You can modify the existing range, and/or add new ranges.

In this lesson, you will create a new network range and use it to apply policies.

Complete Add Network Range Form

1. Name: Corporate Network
2. IP Ranges: 192.168.0.0 to 192.168.255.255
3. Select Save
Successfully Added Network Range

Verify Default Access Policy Settings

The VMware Identity Manager service includes a default access policy that controls user access to their Workspace ONE portals and their Web applications. You can edit the policy to change the policy rules as necessary.

When you enable authentication methods other than password authentication, you must edit the default policy to add the enabled authentication method to the policy rules.

Each rule in the default access policy requires that a set of criteria be met to allow user access to the applications in the portal. You apply a network range, select which type of user can access the content, and select the authentication methods to use.

Navigate to default_access_policy_set
1. Select `default_access_policy_set`

**Review default_access_policy_set**

1. The default access policy applies to 1 application in the catalog. This is the Horizon Desktop Pool as a result of the sync operation you completed.
2. There are two policy rules created by default, controlling the access behavior when users logon from a **Web Browser** or the **Workspace ONE App**
3. Select **Edit**
Edit Policy - Configuration

1. Select **Configuration**

Review Policy Configuration Settings

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

<table>
<thead>
<tr>
<th>Network Range</th>
<th>Device Type</th>
<th>Authentication</th>
<th>Re-authenticate</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL RANGES</td>
<td>Web Browser</td>
<td>Password+1</td>
<td>8 Hour(s)</td>
</tr>
<tr>
<td>ALL RANGES</td>
<td>Workspace ONE App</td>
<td>Password+1</td>
<td>2160 Hour(s)</td>
</tr>
</tbody>
</table>

Add Policy Rule
1. Select **Cancel** as no changes are necessary for this lab.

The default policy can be modified as needed.

**Create a New Access Policy to Deny Application Access**

A policy rule can be configured to deny access to users by network range and device type.

You will create a rule to deny access to a Horizon published application when it is accessed from a specific network.

**Add Policy**

1. Select **Add Policy**
Complete Policy Definition

1. Policy Name: **Internal Network**
2. Click in the **Select applications from your catalog...** window to bring up a list of available applications

If the application list does not populate immediately, wait a few seconds and click in the **Select applications from your catalog...** window again.

Choose Horizon Desktop Pool

1. Select **Man-Pool1**
2. Select **Next**
Add Policy Rule

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

1. Select **Add Policy Rule**

Configure Policy Rule

1. Choose **Corporate Network** from the drop-down list
2. Choose **Domain Users** from the drop-down list
3. Choose **Deny access** from the drop-down list

Save Policy Rule
1. Select **Save**

**Review Policy Rule**

**New Access Policy**

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

<table>
<thead>
<tr>
<th>Network Range</th>
<th>Device Type</th>
<th>Authentication</th>
<th>Re-authenticate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Net...</td>
<td>Any</td>
<td>Deny access</td>
<td></td>
</tr>
</tbody>
</table>

1. Select **Next**
Save

Successfully Added Policy

Configure Client Access URL

The client access URL is used to launch locally-entitled resources from the Horizon pod, when users request applications and desktops via Workspace ONE and Identity Manager.
In an earlier exercise you configured Horizon Virtual Apps, and supplied the FQDN of a single connection server to complete the Identity Manager integration with your Horizon pod.

In production Horizon implementations, it is common to configure a load-balancer virtual IP (VIP) in front of your Connection Servers or UAGs. The client access URL should be configured so it directs requests for Horizon resources to the VIP.

**Edit Virtual App Settings**

1. Select **Catalog**, making sure you click the down arrow
2. Select **Virtual Apps**

**Navigate to Virtual App Settings**

1. Note the **Horizon View Desktop** that is now available in Workspace ONE as a result of the sync operation you completed in a previous exercise

    Additional Horizon Desktops and Applications will be listed here, as they are created in Horizon, and synced to Workspace ONE

2. Select **Virtual App Settings**
Review Network Settings for Default ALL RANGES Network Range

1. Select **ALL RANGES**

Review Client Access URL Host

1. The **Client Access URL** defaults to the FQDN of the Horizon Connection Server you entered when configuring the **Virtual App**.

   If you have a load-balancer configured with a virtual IP address (VIP) in front of your Connection Servers or Unified Access Gateways (UAG), edit the **Client Access URL** to use the VIP.

   This lab does not contain a load-balancer, so the FQDN of the Connection Server will be used.

2. Select **Finish**
Configure Settings for Network Range Internal Network

1. Select **Corporate Network**

Identity Manager supports using different Client Access URLs for each network range. This provides the flexibility to direct users to internal Connection Servers, external UAGs, or different Horizon pods in a Cloud Pod Architecture (CPA) implementation.

**Review Client Access URL Host**

The **Client Access URL** for the Internal Network you created is blank by default. For the purposes of this lab, you will configure the Client Access URL to use the FQDN of the Horizon Connection Server.

It is important that each network range in your environment contains a client access URL.
Add Client Access URL Host and URL Port

1. Client Access URL Host: **horizon-02.corp.local**
2. URL Port: **443**
3. Select **Finish**

Logout of the Workspace ONE Admin Console

1. Select the drop-down menu next to **Local Admin**
2. Select **Logout**
1. Select **Go back to login page**

Leave this page open as you will use it in the next lesson.

**Configure Access and Network Policies and Client Access**

**URL Complete**

You have successfully:

- Added and configured a network range.
- Create an access policy to deny access to an application from a specific network range.
- Configured the client access URL access to your Horizon pod resources.
Launching Horizon Desktops with Deny Access Policy Rule

In the previous exercise you created a new network range for the corporate network, and a new policy to deny access for a specific Horizon resource when accessed from this network.

In this section you will authenticate to Workspace ONE as an end user, and attempt to launch the Horizon Desktop pool.

Navigate to VMware Workspace ONE Tab in Chrome

You should already have Chrome open with a tab to VMware Workspace ONE. If so, you can skip the next couple of steps and proceed to Authenticate to Workspace ONE as an End User.

Launch Chrome Browser

1. From the Desktop of the Main Console, double-click Google Chrome

Navigate to Workspace ONE

1. Select WS1 from the Chrome bookmarks bar
2. Select New vIDM
Verify Domain

1. Verify the domain selected is `corp.local`
2. Select **Next**
Authenticate to Workspace ONE as an End User

1. username = user1mod1
2. password = VMware1!
3. Select Sign in
Launch App

1. Select **Open**

Access Denied Due to Policy

1. Select **OK**

This time the Horizon Desktop can not be opened due to the deny rule you created in the previous exercise.
Conclusion

Congratulations! You have now completed Module 2. You should be familiar with the integration of Horizon 7 with VMware Workspace ONE Identity Manager.

Horizon Integration

If you are looking for additional information:

- Click on this link
- Or use your smart device to scan the QRC Code.

Proceed to any module below which interests you most.

Lab Module List:

**Module 1 - Installation and Configuration of VMware vIDM** (30 minutes)  
(Advanced) Walk through the installation and configuration of the VMware Identity Manager

**Module 3 - Configure MFA using RADIUS in Workspace ONE** (15 minutes)  
(Advanced) Learn how to configure a RADIUS compatible authentication adapter

**Module 4 - Integrating Workspace ONE with SAML Based Web Applications** (30 minutes)  
(Advanced) Learn how to add web applications and configure single-sign-on with SAML 2.0

**Module 5 - Configure Failover and Redundancy or Workspace ONE** (15 minutes)  
(Advanced) Learn how to design a highly available Workspace ONE deployment in both single- and multi-site implementations
How to End Lab

To end your lab click on the **END** button.
Module 3 - Configure MFA using RADIUS in Workspace ONE (15 Minutes)
Introduction

VMware Workspace ONE allows for setting up Network Ranges and different authentication policies that can be assigned to different network ranges.

For example, you might want your end-users to authenticate with their AD credentials when they are in the office and connected to the corporate network, while you might want them to use 2-factor authentication when working from home. Or you might have a group of users requiring MFA because of the applications they can access.

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

We will walk you through the configuration of the RADIUS authentication adapter within Workspace ONE and assign RADIUS authentication to all connections coming from a specific network range.

Lab Ready?

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

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

Attention!

Please leave the FreeRADIUS START Window open or minimize it, but **DO NOT** close it.
Setup RADIUS as an Authentication Adapter

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

Launch Browser

1. From the Main Console, open **Google Chrome**
Open Identity Manager console

1. Click **WS 1 and open VIDM-01 Admin** to open Management Console
2. Username: **administrator**
3. Password: **VMware1!**
4. Click **Sign in**

Setup Authentication Adapters

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

**Modify Authentication Adapters**

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

1. **Close this tab** to return to the Admin Console
Create Network Range and modify policy

To limit RADIUS authentication to clients in a specific network, we have to create a networks range and modify the default policy to use RADIUS for this specific range we create.

Switch To Policies

1. Click Manage
2. Click Policies
3. Click Network Ranges

Add Network Range

1. Click Add Network Range
Define Network Range cont.

1. Enter **RADIUS Test** as 'Name' for the network range
2. Provide a description **RADIUS Test** (optional)
3. Enter **192.168.100.1** as 'From'
4. Enter **192.168.100.255** as 'To'
5. Click **Save**

This will add all the 192.168.100.xxx IP addresses to the RADIUS Test network range and will include our test VM.

**Verify the new network range has been added**

1. **Verify** RADIUS Test IP Address Range was created
2. **Close** the Network Ranges Window
Change default access policy

1. Click **default_access_policy_set**

Edit Policy

1. Click **Edit**
Edit Policy

1. Click the X to ignore the warning about modifying the default policy
2. Click the Next

Add Policy Rule

You can create a list of rules to access the applications selected. For each rule, select the IP network range, the type of devices that can access the applications, the auth methods, and the maximum number of hours users can use the application before reauthenticating.
1. Click **Add Policy Rule**

**Configure Policy Rule**

![Add Policy Rule Form]

1. Select **RADIUS Test** from dropdown menu
2. Select **Web Browser** from dropdown menu
3. Select **RADIUS** from dropdown menu
4. Select **Password** from dropdown menu
5. **Scroll Down**
Advanced Properties

1. Click on **Advanced Properties**

Besides setting the time after which a user has to re-authenticate, you can configure a **Custom Error Message**, **Custom Error Link Text** and a **Custom Error Link URL**, where you could guide the user to a how-to document or further information on how to resolve any issues with authentication.

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

You can also combine multiple authentication methods if you need more than 2-factor authentication.

Click **Save**
Change Policy Rule Order
Edit Policy

1. Definition
2. Configuration
3. Summary

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

- Network Range: 
  - Device Type: 
    - Authentication: 
      - Re-authenticate:

1. All RA: Web Browser: Password+1
2. All RA: Workspac: Password+1
3. All RA: RADIUS Test

ADD POLICY RULE

ADD POLICY RULE

ADD POLICY RULE
1. Hover the mouse cursor over **RADIUS Test** until the cursor changes, then click on **RADIUS Test** and keep the button pushed
2. Drag the rule all the way to the top
3. Release the **RADIUS Test** Policy Rule

**Verify Rule Order**

1. Verify **Radius Test** is listed as the first rule
2. Click **Next**
Policy Summary

1. Verify Policy Rule
2. Click **Save**
Verify functionality

Now we will verify the new policy is active.

Open New Incognito Window

Open a new incognito browser window:

1. Click the vertical dots in the upper right corner
2. Select **New incognito window**
Log in to WS1

1. Click **WS1** and select **VIDM-01**
2. Click **Next**

Log In as user3mod3
1. Username **user3mod3**
2. Password **VMware1!**
3. Click **Sign in**

**Verify Login**

As you logged in from the Main Console (IP address 192.168.110.10), you should have successfully logged in to the Workspace ONE console using your **domain password**.

1. Close the Incognito Window

**Test RADIUS Authentication from Windows 10 VM**

Now let's test the RADIUS Authentication. For this we need to open our Windows 10 test VM via Horizon Client.
Open Horizon Client

1. Open Horizon Client from Start Menu or Menu Bar

Connect to Horizon-01

1. Click horizon-01.corp.local
Login to Horizon-01

1. User name: **user3mod3**
2. Password: **VMware1!**
3. Click **Login**

Open Instant Clone Pool

1. Double-Click **Instant Clone Pool** to open our Win10 test VM
Open Edge Browser

Wait for the Instant Clone VM to load, then

1. Notice the Subnet of the VM is 192.168.100.XXX (which is within the Network Range we defined earlier)
2. Open Microsoft Edge browser
3. Browse to vidm-01.corp.local (this should be the home page)
4. If prompted, confirm domain ist set to corp.local and click Next
Authenticate Using RADIUS

Since the IP address of our test VM is within the RADIUS Test network range (192.168.100.180 - 192.168.100.190) we defined earlier, we now - as expected - get prompted for the RADIUS Passcode instead of our CORP.LOCAL domain password.

1. Notice "Please enter RADIUS Passcode" message
2. Username: user3mod3
3. RADIUS Passcode: 123456
4. Click Sign In
5. Click No to not save your password
Verify access

Verify you can access the portal successfully.

Disconnect and Log Off

1. Click **Options**
2. Select **Disconnect and Log Off**
3. Click **OK**

### Close Horizon Client

1. Click the **X** to close the Horizon Client
Conclusion

We have shown how easy it is to integrate VMware Workspace ONE with a RADIUS compatible 2FA solution.

VMware Workspace ONE also comes with a built-in 2FA solution, as this lab environment is not connected to the internet, we could not show it in this lab, but you can learn more about it here: VMware Verify.

VMware Verify uses mobile push tokens, leveraging the Verify app for iOS and Android.

**VMware Verify Video (1:43 min)**

If you are interested in learning more about VMware Verify, take a look at the short video above.

**Conclusion**
You can find additional information on User Authentication options, including RADIUS, in the documentation for VMware Workspace ONE.

The QR-Code will take you the link below:


You've finished Module 3

Congratulations on completing Module 3.

If you are looking for additional information on Workspace ONE, try one of these:

- Click on this [link](https://docs.vmware.com/en/VMware-Identity-Manager/3.2/idm-aw-administrator.pdf)
- Or go to https://techzone.vmware.com
- Or use your smart device to scan the QRC Code.

Proceed to any module which interests you most.

- **Module 1 - Installation and Configuration of VMware vIDM** (30 minutes) (Advanced) Walk through the installation and configuration of the VMware Identity Manager
- **Module 2 - Integrating Workspace ONE with Horizon** (60 minutes) (Advanced) Walk through the integration of Horizon 7 with Workspace ONE to deliver desktops and apps
- **Module 3 - Configure MFA using RADIUS in Workspace ONE** (15 minutes) (Advanced) Learn how to configure a RADIUS compatible authentication adapter
- **Module 4 - Integrating Workspace ONE with SAML Based Web Applications** (30 minutes) (Advanced) Learn how to add web applications and configure single-sign-on with SAML 2.0
- **Module 5 - Configure Failover and Redundancy or Workspace ONE** (15 minutes) (Advanced) Learn how to design a highly available Workspace ONE deployment in both single- and multi-site implementations

How to End Lab

To end your lab click on the **END** button.
Module 4 - Integrating Workspace ONE with SAML Based Web Applications (30 minutes)
Introduction

In this module you will learn how to configure Web and SaaS applications in VMware Workspace ONE. With VMware Workspace ONE, you can provide Single-Sign-On (SSO) for your users to any Web/SaaS application supporting Security Assertion Markup Language (SAML).

This will simplify a user's digital workspace experience by allowing the user to have a single entry point for all applications (ThinApps, Citrix XenApp, RDSH, SaaS) and VDI Desktops from any device offering a browser. With VMware AirWatch, you can even extend this to mobile apps.

The SSO into Horizon Published Apps and Desktops is shown in Module 2 - Workspace ONE Integration with Horizon 7.

Users can customize their portal by adding application bookmark from the catalog as shown in the sample picture of Workspace ONE portal above. In this lab, we will first walk you through adding a simple Web-Link (without SSO) to the catalog and in another example, add a SAML 2.0 enabled app with SSO.
1. Make sure the **Lab Status** is **Ready**

2. Open **README.txt**

3. Make yourself familiar with the content of **README.txt**, this will make your life easier by allowing you to copy/paste rather than typing, especially if you don't have a US keyboard.
Create Web Based Application Shortcut

In this example we will create a simple shortcut for a Web Application, without passing any user information for single-sign-on. This basically just creates a bookmark and is the simplest form of integrating a Web Application or Website into VMware Workspace ONE.

Launch Browser

1. From the Main Console, open Google Chrome
Login to VMware Identity Manager

1. Open **VIDM-01 Admin** in Chrome
2. Username: **administrator**
3. Password: **VMware1!**
4. Click Sign in
Switch To Catalog

1. Click on Catalog

Create New Web Application

1. Click New
Add Application

1. Enter Name: **vSphere Web Client**
2. Click on **Select File** and select **vsphere logo.jpg** (C:\Tools\Icons)
3. Click **Next**

**Note:** Depending on your screen resolution, you might have to scroll or reduce zoom in Chrome Browser.
Select Authentication Type

1. Click Dropdown
2. Select Web Application Link
Add Application Configuration

New SaaS Application

1. Enter Target URL: *https://vcsa-01a.corp.local/ui* (you can also click&drag from manual or copy from existing bookmark in your browser)
2. Click Next

Leave **Open in VMware Browser** set to 'no' (this setting will only apply to devices supporting VMware's secure Browser).
Add Entitlement

1. Click on **Save & Assign**

Assign Group

[Diagram showing the Assign Group interface with highlighted steps]
1. Type: `dom`
2. Select `Domain Users@corp.local`

**Verify and Save Assignment**

1. Verify the selected Users / User Groups shows `Domain Users@corp.local`
2. Leave Deployment Type set to `User-Activated`
3. Click `Save`
Open New Incognito Window

1. Click the **Customize And Control Google Chrome** Icon
2. Select **New Incognito Window**

Open VIDM-01

1. Open **VIDM-01**
Login as user3mod4

1. Click **Next**
2. Enter **user3mod4** as username
3. Password **VMware1!**
4. Click **Sign in**
Verify vSphere Web Client Shortcut is available

1. Select **Websites**
2. Click **Open**

Verify vSphere Web Client opens

Verify vSphere Web Client page comes up. As we didn't configure any SSO/SAML integration and basically just created a URL-bookmark within Workspace ONE, there is no single-sign-on.

1. **Close** the Incognito Browser
Add SAML based Web Application and SSO Configuration

In this lab we will add our SAML 2.0 Test-App and configure VMware Workspace ONE to pass user information to the app. In preparation for this lab, we have already configured the SAML Test-App to trust VMware Workspace ONE by adding the certificate to the Test App, as this is very specific to this app, we won't spend much time on that part and rather focus on the VMware Workspace ONE side.

Switch to Administration Console

1. Click **Settings**

If you have closed the Chrome browser Window/Tab with your Workspace ONE session, please re-open Chrome and login to VIDM-01 Admin as administrator.
SAML 2.0 Preparation

On this settings page, you can find and download the SAML Metadata. SAML Integration requires configuration on the Workspace ONE side and on the side of the application you want to integrate. For the SAML 2.0 test app we use later in this lab, this configuration was done for you. However, this is where you can find the necessary information (signing certificate and IdP URL etc.) in the Administration Console:

1. Click on **SAML Metadata**
2. Notice you could **Copy or Download** the Certificate for the Workspace ONE/vIDM Appliance
3. Click the **X** to close the window

**Note:** No need to copy or download the certificate for this lab, we have the test app already configured for you.
This is just to show how the setting files for our simple SAML-Test application look like. For this (very) simple app, we needed to provide the certificate of our Workspace ONE (vIDM) instance, the IdP SSO URL to get the application launched and the Assertion Return URL.

As the configuration is very specific to this simple test-app, we didn't add those steps to the lab. However, if you are really interested, you can use WinSCP or Putty to look at the settings.php file on saml-test.corp.local, the file is located under /var/www/html/saml/demo.
Add SAML Application

You should be on the Catalog page in the Administration Console

1. Click on New

Application Definition

1. Enter Name: **SAML 2.0 App**
2. Enter **SAML Test Application** in the description field
3. Click on Select File and select **SSO_NEW.jpg** from C:\Tools\Icons
4. Scroll Down
Select Category

1. Click **Dropdown**
2. Select **SaaS**
3. Click **Next**
1. Verify Authentication Type is set to **SAML 2.0**
2. Switch Configuration **Manual**
5. Application ID: enter **php-saml**
6. **Scroll down**
1. Click on **Advanced Properties**
2. **Scroll Down**
3. Switch **Sign Assertion** to **Yes**
4. Switch **Include Assertion Signature** to **Yes**
5. **Scroll Down**
1. Click **Add Row**
Attribute Mapping

Now we need to define the attributes we pass to the SAML Application

1. Enter Name: **firstname**
2. Start typing **fir** and select `{$user.firstName}` from Value list
3. Click **Add Row**

**Note:** Depending on your screen resolution or browser zoom setting, you might have to scroll to get to the fields.
1. Repeat previous steps and add the following attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>lastname</td>
<td>${user.lastName}</td>
</tr>
<tr>
<td>username</td>
<td>${user.userName}</td>
</tr>
<tr>
<td>principalname</td>
<td>${user.userPrincipalName}</td>
</tr>
</tbody>
</table>

2. Click Next

**Note:** It is important to use the exact names as listed above. Any typo will prevent the app from opening correctly later.
Access Policies

Leave the default_access_policy_set and

1. Click Next

**Note:** Access policies can be applied on the applications to control user access based on criteria such as the user's network range or device type. You can create access policies for a single application, a set of applications, or all applications in your catalog. When you add an application to the catalog, you select the access policy to use.
Add Entitlement

1. Click **Save & Assign**
Entitle Domain Users

1. Type: `dom`
2. Select `Domain User@corp.local`
3. Leave Deployment Type set to `User-Activated`
4. Click `Save`

Open New Incognito Browser Window

1. Click on the Customize and control Google Chrome Icon
2. Select `New incognito window`
Test Accessing SAML-Test App directly

1. Browse to http://saml-test.corp.local/saml/demo/samldispatch.php (you can click&drag the URL from the manual)
2. Notice the "Unauthenticated User" message we get from our SAML-Test Web Application, which is expecting proper metadata.
3. Click on the VMware Workspace ONE link

Note:
You can drag the URL from the manual to avoid typos or copy/paste from the Readme.txt.

Log In to Workspace ONE

1. Click Next
Authenticate User

1. Username **user3mod4**
2. Password **VMware1!**
3. Click **Sign in**

Open SAML 2.0 APP

Let's test the SAML 2.0 App:

1. Click **SaaS**
2. Click **Open**
After clicking open, you will notice the browser displaying the picture above, indicating that Workspace ONE is verifying your identity and passing your credentials to authenticate you to the SAML 2.0 Test App.
If you configured the app correctly, you should see the Success Window above.

1. Verify attributes **firstname/lastname**, **username** and **principalname** (=email) have been passed correctly to the SAML-Test App
2. **Close Incognito Window**

For this to work, the necessary information must be available for each user in Active Directory and the attributes need to be synced with Workspace ONE. If you make changes to attributes in AD, a sync between VMware Workspace ONE and the Directory has to happen.

**SAML Test App**

**Verify attributes are displayed**

**Cloud Application Catalog**

![Application Catalog](image)

VMware Workspace ONE also allows for adding Web Application from the Application Catalog, since this environment is not connected to the Internet, you won't be able to test this option. The catalog currently consists of over 100 (and growing) pre-configured templates for typically used web/SaaS applications such as ADP, Salesforce.com, Office 365, Workday, ServiceNow and many others more.

Just because an application is not listed, does not mean it is not supported/working with VMware Workspace ONE it might just be a little more work to set it up.
External Application Sources

In addition to adding new applications manually or via our Application Catalog, it is possible to import applications from existing 3rd party Identity Managers such as OKTA, PING or ADFS. Yes, Workspace ONE can co-exist and play nicely with others.
Conclusion

In this module you learned how to add a simple shortcut for a web-based application and how to integrate a more complex SAML 2.0 based application, to which we passed certain user specific attributes. Depending on the application you want to integrate you might have to configure different settings in VMware Workspace ONE and your application. Always consult documentation for VMware Workspace ONE and your application for details or consider leveraging VMware Professional Service to assist.

VMware Workspace ONE - Techzone

You can find more information on VMware Workspace ONE on our Techzone Website:

https://techzone.vmware.com/resource/workspace-one
You've finished Module 4

Congratulations on completing Module 4.

If you are looking for additional information on Workspace ONE, try one of these:

• Click on this link
• Or go to https://techzone.vmware.com
• Or use your smart device to scan the QRC Code.

Proceed to any module previously which interests you most.

• **Module 1 - Installation and Configuration of VMware vIDM** (30 minutes) (Advanced) Walk through the installation and configuration of the VMware Identity Manager
• **Module 2 - Integrating Workspace ONE with Horizon** (60 minutes) (Advanced) Walk through the integration of Horizon 7 with Workspace ONE to deliver desktops and apps
• **Module 3 - Configure MFA using RADIUS in Workspace ONE** (15 minutes) (Advanced) Learn how to configure a RADIUS compatible authentication adapter
• **Module 4 - Integrating Workspace ONE with SAML Based Web Applications** (30 minutes) (Advanced) Learn how to add web applications and configure single-sign-on with SAML 2.0
• **Module 5 - Configure Failover and Redundancy or Workspace ONE** (15 minutes) (Advanced) Learn how to design a highly available Workspace ONE deployment in both single- and multi-site implementations
How to End Lab

To end your lab click on the **END** button.
Module 5 - Configure Failover and Redundancy for Workspace ONE (15 Minutes)
Introduction

In this module you will learn about how to implement a highly available Workspace ONE Identity Manager solution.

- Lesson 1 - Configure Highly Available Single Site
- Lesson 2 - Configure Highly Available Multi-Site

Please note this section of the lab is for informational purposes only. There are no associated lab steps.

Configure Highly Available Single Site

VMware Workspace ONE Identity Manager is the primary entry point for end users to consume all types of applications, including SaaS, web, Horizon 7 virtual desktops and published applications, Citrix XenApp, and mobile apps.

Therefore, it should be deployed to be highly available within a site, and also deployed in a secondary data center for failover and redundancy.

This lesson explores design considerations for implementing the Identity Manager components of Workspace ONE with HA for a single site.

Design Overview

VMware Identity Manager can be implemented using on-premises or SaaS-based implementation models. This lab focuses on the on-premises model.

The main components of Identity Manager on-premises are:

- **VMware Identity Manager appliance** - Runs the main VMware Identity Manager service.
- **VMware Identity Manager Connector** - Responsible for directory sync and authentication between on-premises resources such as Active Directory, Horizon 7, and the VMware Identity Manager service.
In an on-premises deployment, VMware Identity Manager is available as either a Linux-based virtual appliance or as a service installed in a Windows VM.

The Identity Manager Connector software can run on the same VM as the Identity Manager appliance. VMware recommends separating these services to separate appliances, as described in the following sections.

VMware Identity Manager can also be integrated with the rest of the Horizon 7 Enterprise components to provide access to Horizon 7 desktops and published applications. The VMware Identity Manager VM handles authentication and provides SSO services to applications and desktops.

Syncing resources such as Active Directory and Horizon 7 and can be done either by using a separate VMware Identity Manager Connector or by using the built-in connector of an on-premises VMware Identity Manager VM. The separate connector can run inside the LAN in outbound-only connection mode, meaning the connector receives no incoming connections from the DMZ.

**Database**

VMware Identity Manager can be set up with an internal or external database to store and organize server data. A PostgreSQL database is embedded in the VMware Identity Manager virtual appliance, but this internal database is not recommended for use with production deployments.

To use an external database, have your database administrator prepare an empty external database and schema before you use the VMware Identity Manager Setup wizard to connect to the external database. Licensed users can use an external Microsoft SQL Server 2012, 2014, or 2016 database server to set up a high-availability external database environment.

The database requires 64 GB of disk space for the first 100,000 users, and another 20 GB for each additional 10,000 users.
Scalability and Availability

VMware Identity Manager has been tested to 100,000 users per single virtual appliance installation. For a high-availability environment, at least three VMware Identity Manager appliances should be configured to ensure availability in the event of a failure of an appliance or ESXi host. After initial configuration, the virtual appliance is cloned twice and deployed with new IP addresses and host names.

For production implementations, VMware recommends Microsoft SQL Server 2016 along with its cluster offering Always On availability groups, which is supported with VMware Identity Manager. This allows the deployment of multiple instances of VMware Identity Manager, pointing to the same database protected by an availability group with an availability group listener as the single Java Database Connectivity (JDBC) target for all instances.

Windows Server Failover Clustering (WSFC) can also be used to improve local database availability and redundancy. In a WSFC cluster, two Windows servers are clustered together to run one instance of SQL Server, which is called a SQL Server failover cluster instance (FCI). Failover of the SQL Server services between these two Windows servers is automatic.

High Availability Design Recommendations

To provide high availability:

- Three VMware Identity Manager 3.x appliances are deployed in the DMZ.
- Two VMware Identity Manager 3.x Connectors are deployed inside the corporate LAN, configured to use an outbound-only connection mode.
- An external SQL Server 2016 database server is installed on a two-node Windows Server Failover Cluster, which uses a SQL Server Always On availability group.

**Load Balancing**

To remove a single point of failure, you can deploy more than one instance and use a third-party load balancer. This strategy not only provides redundancy but also allows the load and processing to be spread across multiple instances of the component. To ensure that the load balancer itself does not become a point of failure, most load balancers allow for setup of multiple nodes in an HA or master/slave configuration.

The following figure illustrates how load balancers distribute the load to a cluster of VMware Identity Manager appliances in the DMZ. VMware Identity Manager Connector virtual appliances are hosted in the internal network and use an outbound-only connection mode.

Split DNS is a requirement for VMware Identity Manager; that is, the same fully qualified domain name (FQDN) for VMware Identity Manager must be used both internally and externally for user access.
Configure Highly Available Multi-Site

This lesson explores design considerations for implementing Workspace ONE Identity Manager with HA in a multi-site configuration.

**Design Overview**

The failover process that makes the secondary sites VMware Identity Manager appliances active requires a change at the global load balancer to direct traffic of the namespace to the desired instance. You must also clear the caches on the original primary data center.

VMware Identity Manager consists of the following layers, which make up the service and need to be designed for redundancy:

- VMware Identity Manager appliances and connectors
- Database
- Unified app catalog that can contain SaaS, web, Horizon 7 published applications, Horizon 7 virtual desktops, Citrix XenApp, and mobile apps

**VMware Identity Manager Appliances and Connectors**

To provide site resilience, each site requires its own group of VMware Identity Manager virtual appliances to allow the site to operate independently, without reliance on another site. One site runs as the active VMware Identity Manager, while the second site has a passive group. The determination of which site has the active VMware Identity Manager is usually controlled by the global load balancers namespace entry or a DNS entry, which sets a given instance as the target for the namespace in use by users.

Within each site, VMware Identity Manager must be installed with a minimum of three appliances. This provides local redundancy and ensures that services such as
Elasticsearch function properly. The VMware Identity Manager appliances are hosted in the DMZ network.

A local load balancer distributes the load between the local VMware Identity Manager instances, and a failure of an individual appliance is handled with no outage to the service. Each local site load balancer is also load-balanced with a global load balancer.

At each site, two VMware Identity Manager Connector virtual appliances are hosted in the internal network and can use an outbound-only connection mode. These connectors point to the global load balancer.

**Multi-site Database**

VMware Identity Manager 2.9 (and later) supports Microsoft SQL Server 2012 (and later) and its cluster offering Always On availability groups. This allows us to deploy multiple instances of VMware Identity Manager, pointing to the same database protected by an availability group with an availability group listener as the single Java Database Connectivity (JDBC) target for all instances.

VMware Identity Manager is supported with an active/passive database instance with failover to the secondary site if the primary site is unavailable. Depending on the configuration of SQL Server Always On, inter-site failover of the database can be automatic, though not instantaneous.

Within a site, Windows Server Failover Clustering (WSFC) is used to improve local database availability and redundancy. In a WSFC cluster, two Windows servers are clustered together to run one instance of SQL Server, which is called a SQL Server failover cluster instance (FCI). Failover of the SQL Server services between these two Windows servers is automatic.

**Note:** All JDBC connection strings for VMware Identity Manager appliances should point to the SQL Server availability group listener (AGL) and not directly to an individual SQL Server node.

If your organization has already deployed Always On availability groups, consult with your database administrator (DBA) about the requirements for the database used with VMware Identity Manager.

The SQL Server Always On setup can be configured to automatically fail over and promote the remaining sites database to become the primary.
Conclusion

Congratulations! You have now completed Module 5. You should be familiar with how to configure failover and redundancy for Workspace ONE Identity Manager.

VMware Workspace ONE and VMware Horizon 7 Enterprise Edition On-premises Reference Architecture

If you are looking for additional information:

• Click on this link.
• Or use your smart device to scan the QRC Code.

Proceed to any module below which interests you most.

Lab Module List:

**Module 1 - Installation and Configuration of VMware vIDM** (30 minutes) (Advanced) Walk through the installation and configuration of the VMware Identity Manager

**Module 2 - Integrating Workspace ONE with Horizon** (60 minutes) (Advanced) Walk through the integration of Horizon 7 with Workspace ONE to deliver desktops and apps

**Module 3 - Configure MFA using RADIUS in Workspace ONE** (15 minutes) (Advanced) Learn how to configure a RADIUS compatible authentication adapter

**Module 4 - Integrating Workspace ONE with SAML Based Web Applications** (30 minutes) (Advanced) Learn how to add web applications and configure single-sign-on with SAML 2.0
How to End Lab

To end your lab click on the END button.
Conclusion

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

Lab SKU: HOL-1951-03-VWS

Version: 20190712-140802