# Table of Contents

Lab Overview - HOL-1851-05-ADV - VMware Workspace ONE and VMware Horizon 7.1 ... 2

Lab Guidance ................................................................................................................. 3

Module 1 - Install and Configure Identity Manager and Workspace ONE (30 minutes) ..... 9
  Introduction......................................................................................................................... 10
  Download and Deploy VMware Identity Manager Appliance ...................................... 15
  Initial Configuration of the VMware Identity Manager Appliance ........................... 20
  VMware Identity Manager Admin Console Configuration .............................................. 29
  Admin Console walk-through ......................................................................................... 41
  Conclusion......................................................................................................................... 60

Module 2 - Integrating Identity Manager with Horizon 7.1 (30 minutes) ...................... 61
  Introduction......................................................................................................................... 62
  Enabling View Applications for Use with VMware Identity Manager ......................... 65
  Enable SAML Authentication in Horizon 7 .................................................................. 69
  Configuring Horizon 7 Application Pools ....................................................................... 74
  Synchronize VMware Identity Manager with Horizon 7 ............................................... 79
  Check Entitlements for Horizon 7 Application Pools via VMware Identity Manager ........ 83
  Conclusion......................................................................................................................... 94

Module 3 - Integrating Identity Manager with ThinApp (30 minutes) ............................ 95
  Introduction......................................................................................................................... 96
  Configure ThinApp Repository ....................................................................................... 97
  Entitle ThinApp Packages to Users ............................................................................. 108
  Configure vIDM Desktop Client and Verify ThinApp Package Install .......................... 113
  Updating ThinApp Packages ......................................................................................... 118
  Conclusion......................................................................................................................... 135

Module 4 - Multifactor Authentication using RADIUS (30 minutes) ............................... 136
  Introduction......................................................................................................................... 137
  Setup RADIUS as Authentication Adapter ................................................................... 139
  Create Network Range and modify policy ................................................................... 143
  Verify functionality ........................................................................................................ 150
  Conclusion......................................................................................................................... 159

Module 5 - Integrating Identity Manager with SAML-based Web App (30 minutes) ...... 161
  Introduction......................................................................................................................... 162
  Create Web Based Application Shortcut ..................................................................... 163
  Add SAML based Web Application and SSO Configuration ...................................... 170
  Conclusion......................................................................................................................... 187

Lab Conclusion .............................................................................................................. 188

Conclusion......................................................................................................................... 189
Lab Overview - HOL-1851-05-ADV - VMware Workspace ONE and VMware Horizon 7.1
Lab Guidance

Note: It will likely 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-prem, how to integrate it with Horizon 7, ThinApp, SaaS and Web Applications. You will also learn about configuring vIDM with a RADIUS-based 2-Factor Authentication solution.

Lab Module List:

- **Module 1 - Introduction to Identity Manager and Workspace ONE (30 minutes)** (Beginner) Learn how to install and perform initial configuration of vIDM
- **Module 2 - Integrating Identity Manager with Horizon 7.1 (30 minutes)** (Advanced) Integrate vIDM with Horizon 7
- **Module 3 - Integrating Identity Manager with ThinApp (30 minutes)** (Advanced) Integrate vIDM with ThinApp
- **Module 4 - Multifactor Authentication using RADIUS (15 minutes)** (Advanced) How to configure RADIUS authentication to work with vIDM
- **Module 5 - Integrating Identity Manager with SAML-based Web App (15 minutes)** (Advanced) Integrating vIDM with SaaS and Web Applications

Lab Captains:

- Karsten Giessen, Sr. Systems Engineer, United States
- Peter Schraml, Sr. Solution Architect, EUC Cloud Services, EMEA

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

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

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

Please take a look at HOL-1851-08-ADV for more information on installing VMware Identity Manager / Workspace ONE as part of a Cloud Pod Architecture deployment.

Any App, Any Device

VMware Identity Manager (vIDM) is the authentication engine powering VMware's Workspace ONE portal, allowing users a seamless experience to access their applications or virtual desktops from any device. In this lab we will show you how to perform a simple setup of the vIDM Appliance, integrate with Horizon View for hosted applications and virtual desktops, leverage Workspace ONE to deploy ThinApps and present web-based applications, leveraging SAML integration. You will also learn how to use a RADIUS-based 2-factor authentication method. While not shown in this lab, you can also present Citrix XenApps through Workspace ONE or present mobile application via Integration with VMware AirWatch (take a look at the HOL-1857-xx-UEM labs).

Before starting with the actual lab, please make yourself familiar with the specifics of the Hand-On-Labs environment. If you are familiar with Lab-Status, drag and copy etc, feel free to skip the next steps and proceed directly to the Module you want to take.

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.
Location of the Main Console

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

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 10 minutes your lab has not changed to "Ready", please ask for assistance.
Module 1 - Install and Configure Identity Manager and Workspace ONE (30 minutes)
Introduction

This module will cover the installation and configuration of the on-prem version of VMware Identity Manager (vIDM). vIDM 2.8.1 appliance features include the portal (which users will see labeled as Workspace ONE), AirWatch Directory integration, access policy integration, and Horizon True SSO support. It provides a simple and secure enterprise platform that delivers and manages any app on any device by integrating, application and mobility management.

In this module you will review the prerequisites and configure the vIDM appliance for a simple install, as you would for a POC or test environment. Once the configuration is complete, you will take a tour of the interface and view what additional features and functionality are available.

Please note in this module we recommend using Chrome for the best experience. The browser has been configured to ignore self signed certs.

If you are interested in more advanced options for installing, e.g. installing vIDM as part of Cloud Pod Architecture (CPA), we recommend looking at HOL-1851-08-ADV.

What is VMware Identity Manager?

VMware Identity Manager is identity management for the mobile cloud era that delivers on consumer-simple expectations like one-touch access to nearly any app, from any
device, optimized with AirWatch Conditional Access. Empower 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 are the Key Benefits?

• Empower employees to 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.

More Information

You can find more information, including links to the vIDM Datasheet and documentation on our website. Use the QR-Code above or click here.
Lab Ready?

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.

Start vidm-02a appliance
To prepare the interactive part of the lab, we need to start vidm-02 using vSphere Client.

1. Open Chrome and click on **HOL-1851 Admin** in the bookmark
2. Select **vCenter HTML5 Client**

### Log in to vSphere Web Client

![vCenter Single Sign-On](image)

1. User name: **administrator@corp.local**
2. Password: **VMware1!**
3. Click **Login**

Note: You can also click "use Windows session authentication" instead of entering username/password.
Power on vidm-02a

1. Right-click on vidm-02a
2. Select Power
3. Select Power On

It will take a couple of minutes for the appliance to boot, please proceed to the next step and read through the initial download and deployment process, the appliance should be ready by the time you get to the hands-on portion.
Download and Deploy VMware Identity Manager Appliance

vIDM deploy

In this chapter, we will discuss the prerequisites for successfully deploying the Identity Manager (vIDM) appliance. This chapter is strictly theoretical module, with no steps to be performed.

vIDM appliance prerequisites are:

1. DNS records (both A and PTR-records)
2. ESXi host to be time synced

A default TLS/SSL server certificate is generated when you deploy a vIDM appliance. For production environments, VMware strongly recommends that you replace the default certificate as soon as possible.

It is important to use Fully Qualified Domain Name (FQDN) during installation of vIDM!

Configure DNS
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.

Within this Lab environment the corp.local domain is the main domain.

1. As shown in this screen capture, there is an Host (A) record for **vidm-02a**
2. Looking in the reverse look up zone for the 192.168.110, you can see the PTR record has been created

**Time Sync**

![Time Configuration Screen](image)

vIDM is very sensitive to time differences between systems with which it integrates. vIDM uses SAML for a lot of its functionality. Therefore a maximum of 30 second drift is often enough to break functionality.

You should confirm Time Configuration is set up and running on the host(s). The appliance will pick up the correct time from the ESXi host. Since you often join vIDM to a Microsoft Active Directory domain, it is important the ESXi host and your domain controllers are time synced to the same source. Many times you can specify one of your domain controllers as the time source for your ESXi host.

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

To confirm the host has time configured:

1. Within vCenter, click on your host
2. Select Configure
3. Select Time Configuration

**Deploy the VMware Identity Manager Appliance**

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

Once all prerequisites are in place and you have downloaded the vIDM Connector from VMware.com you are ready to deploy

1. From the vSphere Web Client, right click on the cluster you would like to deploy to
2. Select **Deploy OVF Template**
3. Select **Local File**, then **Browse**. Navigate to the OVA file
4. Click on **Next**
Specify OVA Properties

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

Now you must specify the properties that will be applied to the appliance.

Follow the Wizard, entering the correct information for your environment. Once you have entered the correct information, click on Next. Then click on Finish.
VMware Identity Manager up and running

Once the appliance is fully powered on it will display a screen similar to above.

The rest of the configuration is done using the web interface.
Initial Configuration of the VMware Identity Manager Appliance

Once the VMware Identity Manager appliance has been deployed and powered on, the remainder of the configuration process is done using a web interface. The first portion of the setup will utilize the Setup Wizard.

These steps ARE to be performed in the Lab environment.

Configure Administrator User

1. Open Active Directory Users and Computers

Note: When synchronizing Workspace ONE with Active Directory, certain user attributes are expected/required. The following steps will walk you through adding some of the attributes we will require (name, username) later in this lab.
Modify Administrator Name

1. Double-Click on Administrator User
2. Select General
3. Enter First name: Admin
4. Enter Last name: Admin
5. Click on Account
Modify Administrator Account

1. Enter **administrator** as the user logon name
2. Select **@corp.local** from the drop-down menu
3. Click **OK**
Close Active Directory Users And Computers

1. Close **Active Directory Users and Computers** console
Use the VMware Identity Manager Appliance Setup Wizard

Launch Chrome Browser and browse to the new vIDM appliance

1. Enter **https://vidm-02a.corp.local** as the URL
2. As the appliance is new and no certificates have been installed yet, we receive a warning, click **ADVANCED**
3. Click **Proceed to vidm-02a.corp.local (unsafe)**

**Note:** Please make sure to enter https and use vidm-02a NOT vidm-1a.
vIDM Appliance Setup

1. Click Continue
Specify administrative passwords

Your first task is to set passwords for different administrative accounts. The Admin account is the built-in web admin user. Root is the root on the appliance Operating System. Sshuser is the user who has SSH access to the appliance. By default root does not have SSH access.

1. Specify **VMware1!** as the password for the Appliance Administrator Account - This is the built-in account for the Web Admin User
2. Specify **VMware1!** as the password for the Appliance Root Account - The root account for the vIDM appliance OS
3. Specify **VMware1!** as the password for the Remote User Account - This account has remote shell access to the appliance
4. Click **Continue**
vIDM comes with a built in vPostgres database server. We also support using external Microsoft SQL, Oracle, and VMware vFabric PostgreSQL databases as well. VMware recommends that you configure your database for high availability. To configure the embedded database for High Availability, please review KB 2094258


In the lab we will be using the embedded vPostgres database.

1. Select **Internal Database**
2. Click **Continue**

Due to time and resource limitations in this lab we chose a simple deployment, using a single appliance and the internal Posgres-DB, which is typical for test/POC deployment. In a production deployment scenario, you would deploy a minimum of 3 (more if required for scalability) appliances behind a load balancer.
Waiting for the database to be configured

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...
Database connection configuration has not changed.
Initializing database...
Successfully initialized database.
Activating connector...

Setting up the database takes some time (5-10min). Please be patient. Please do not navigate away or refresh this page.

Initial setup completed

Setup is complete
You can now begin using the Service.

What to do next?

1. Log in to the administrative console

Once the database is setup the initial setup is complete.

1. Click on the Log in to the administrative console link
VMware Identity Manager Admin Console Configuration

In this section you will learn how to perform some additional configurations including adding Active Directory, as well as adding users and groups to the appliance.

Login into the Portal

If you have not closed your web browser, you should now have the login page of Workspace ONE in front of you.

1. Specify **admin** as the user (this is the built in web administrative account)
2. Type **VMware1!** as the password
3. Click **Sign in**
Modify User Attributes

In the portal you can modify the Attributes that are used to sync to Active Directory. Based on how current attributes are configured in the lab, we will modify which attributes users are mapped to:

1. Click on **Identity & Access Management** tab
2. Select **Setup**
3. Select **User Attributes** tab
4. Uncheck all the boxes except userName
5. Scroll down, and click on **Save**

**Note:** We are de-selecting the other user attributes, as in our test-environment some (like phone number etc.) are not set in Active Directory, if a checked attribute is not set for the user in AD, the user would not get imported to vIDM.

During the VMware Identity Manager service directory setup, you select Active Directory user attributes and filters to select which users sync in the VMware Identity Manager.
directory. You can change the user attributes that sync from the administration console, Identity & Access Management tab, Setup > User Attributes.

Changes that are made and saved in the User Attributes page are added to the Mapped Attributes page in the VMware Identity Manager directory. The attributes changes are updated to the directory with the next sync to Active Directory.

The User Attributes page lists the default directory attributes that can be mapped to Active Directory attributes. You select the attributes that are required, and you can add other attributes that you want to sync to the directory. When you add attributes, the attribute name you enter is case-sensitive. For example, address, Address, and ADDRESS are different attributes.

**Important**

If you plan to sync XenApp resources with VMware Identity Manager, you must make distinguishedName a required attribute. You must make this selection before creating a directory as attributes cannot be changed from optional to required after a directory is created.

**Add User Directory**

1. Confirm you are on the **Identity & Access Management** tab
2. Click on **Manage**
3. Click **Add Directory**
4. Select **Add Active Directory over LDAP/IWA**
Configure Directory Access

1. Type **corp.local** as the Directory Name
2. Scroll down

**Configure Directory Access - Continued**

- **Base DN**: `cn=Users,dc=corp,dc=local`
- **Bind DN**: `cn=administrator,cn=Users,dc=corp,dc=local`
- **Bind DN Password**: Enter your Active Directory bind account password.
1. In the Base DN field paste `cn=Users,dc=corp,dc=local` (The Base DN is the root from which vIDM will search the directory.)

2. In the field for Bind DN (user account vIDM uses to communicate with the directory) drag&drop or enter `cn=administrator,cn=Users,dc=corp,dc=local` (Workspace One only reads from the AD. It never updates it. So the Bind DN only has to have read access to the objects you want to sync to Workspace One.)

3. Specify `VMware1!` as the Bind DN's password

4. Click **Test Connection** and make sure you get a **successful** test reported back

5. Click **Save & Next**

Using Base DN, allows to filter OUs, especially in larger environments you might want to use a specific container only.

The use of a specific Bind DN user account, with a non-expiring password is recommended.
Select the Domains

1. Since we only have one domain in this Lab, click **Next** in the Select the Domains step.
2. Here you see a list of user's attributes that you could choose whether or not to sync to your objects by. If an attribute is required, users without this attribute won't be synced to Workspace One. Some User Attributes are required for integrating with other solutions. For example, integration with Citrix requires that
the distinguishedName attribute be selected. For the purposes of this lab, userName is the only required attribute. Accept what is configured and click Next.

Select the Groups to Sync

You can specify from where Workspace One will sync AD groups and which groups to be synced.

1. Click the + sign
2. Drag&drop or enter \texttt{cn=Users,dc=corp,dc=local} as the Group DN
3. Select Find Groups
Select the Groups to Sync - Continued

Select the groups (users) you want to sync

Enter the Group DNs to sync, for example. CN=users,DC=example,DC=company,DC=com. Select the Active Directory groups that you want to sync to the directory. When you select a group, users of that group are also synced.

- Sync nested group members

<table>
<thead>
<tr>
<th>Specify the group DNs</th>
<th>Select All</th>
<th>Groups to sync</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn=Users,dc=corp,dc=local</td>
<td>✓</td>
<td>0 of 23</td>
</tr>
</tbody>
</table>

1. Click on the Select button
2. Scroll down
3. Select **Domain Users**

4. Save
4. Click **Save**

**Verify Managed Groups**

Select the groups (users) you want to sync

Enter the Group DNs to sync, for example, CN=users,DC=example,DC=company,DC=com. Select the Active Directory groups that you want to sync to the directory. When you select a group, users of that group are also synced.

- Sync nested group members

#### Specify the group DNs

<table>
<thead>
<tr>
<th>Group DN</th>
<th>Mapped Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn=Users,dc=corp,dc=local</td>
<td>CN=Domain Users,CN=Users,DC=corp,DC=local</td>
</tr>
</tbody>
</table>

1. Make sure the Domain group **Domain Users** are listed under Mapped Groups
2. Click **Next**
Select users to sync

All users in the locations you specified will be synced as long as they have all the required attributes. The Bind DN account is listed by default to make sure it's being synced. Do not delete the Bind DN since it will become the admin user. You can always access the vIDM console using the built in Admin user. You can later promote other user accounts to become portal administrators.

1. Select the + sign to add additional users
2. Drag&drop or enter `cn=Users,dc=corp,dc=local`
3. Click Next
Review sync operation

The Directory Sync window will show you how many users and groups were added, removed, or updated. Should the information not be what you expected, you can simply select Edit User DNs or Edit Group DNs to make additional adjustments to the DN path.

1. Based on the criteria we set you should see 12 user objects and 1 group object listed.
2. Click **Sync Directory**

**NOTE:** If you do not see the correct number of objects listed, click on the corresponding edit button to confirm you do not have a typo.

Sync Started

You should see a status message indicating 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.
Verify Users

1. Click on **Users & Groups** tab
2. Verify you have some users listed

Verify Groups

1. Click on **Groups**
2. Verify **Domain Users** are listed
Admin Console walk-through

This section is aiming to familiarize you with the different parts of the administrative console and where to find a certain settings.

Please feel free to navigate through the admin console in the lab environment.

User Engagement Dashboard

The very first thing that an administrator sees when accessing the administrator console is the **User Engagement Dashboard**. Here you get a quick overview of the system. For example how many users and groups your system has. Which applications are used the most. How many logins and much more.

1. Click on **Dashboard**
Navigate to the System Diagnostics Dashboard

1. Click on down arrow next to Dashboard
2. Choose the System Diagnostics Dashboard

System Diagnostics Dashboard

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

1. Select the down arrow next to Dashboard
2. Select Reports

Reports

1. vIDM comes with a variety of reports built in. This picture shows you the list of reports. Feel free to investigate further. Please note that since this a newly deployed environment some reports may have no entries.

Portal Catalog Settings
1. Click **Catalog**, and choose **Settings**

**SAML Metadata**

Here we see the SAML Metadata and certificate listed. SAML is an open standard often used to exchange authentication/authorization data between a service provider and an identity provider. You can configure vIDM to act as your identity provider for many components of your enterprise utilizing SAML. The SAML information is needed when integrating vIDM with a SAML enabled web application. To find out more on configuring SAML integration please review: [http://blogs.vmware.com/euc/2016/06/identity-manager-vrealize-automation-sso-single-sign-on-saml-integration.html](http://blogs.vmware.com/euc/2016/06/identity-manager-vrealize-automation-sso-single-sign-on-saml-integration.html)
1. Select Approvals: Once approvals have been activated, vIDM can integrate with a third party approval system. So if a user adds an application using the application catalog you can have an approval sequence being initiated. Not until the approval
sequence sends back that the request has been approved can the user launch the application.

2. Auditing: Is enabled by default. But you can turn it off if needed.
3. User Portal Branding: In this section you an add your logo, company name or product name. Giving the portal a real customized look and feel.

### Identity & Access Management - Directories

In this section of the console you can not only confirm the domain(s) and the vIDM appliance are in sync but also add additional domains as well.

1. Click on **Identity & Access Management**
2. Confirm you are in the **Manage** section
3. Confirm you are on the **Directories** tab
Let's review the additional Tabs that reside in Identity & Access Management.
1. Identity Providers: Are systems authenticating users. vIDM comes with its built in iDP but you can also add third party Identity Providers.
2. Password Recovery Assistant: If users have forgotten their password you can customize the message / link to a web page you display to users. vIDM cannot reset nor change a AD user's password.
3. Policies: vIDM comes with a default policy called `default_access_policy_set`. This policy decides if users gets access to the portal itself or not. You can add your own application policies for SAML/WS-Fed based web applications. Using policies you can grant access to the portal from Internet but launching a specific SAML integrated Web application may require users to be on the LAN. Therefore launching the SAML based application form Internet wont work. Policies can use both authentication type and location to base its rules.

**Identity & Access Management - Setup**

![Identity & Access Management Setup](image)

Now we will review options that reside in Setup under the Identity & Access Management section.

1. Confirm you are on **Identity & Access Management**, select **Setup**
2. First we see the Connectors tab. This is where you would go to add additional vIDM connectors/appliances as well as adding or changing domain membership
Add vIDM to Active Directory

You can integrate VMware identity Manager with Active Directory in a single Active Directory domain, multiple domains in a single Active Directory forest, or multiple domains across multiple Active Directory forests configurations. Adding vIDM to Active Directory is required for functionality such as integration with Horizon 7, ThinApp, etc. This is due to the fact that user entitlements need to be verified. More information can be found: http://tinyurl.com/htk97t4. Adding vIDM to the domain also allows administrators to logon with their AD account vs using local accounts.

To add vIDM to the domain

1. Click on Join Domain
2. Enter Domain: corp.local
3. Domain User: administrator
4. Password: VMware1!
5. Click on Join Domain
Verify Active Directory Membership

1. You will now notice that the Domain now list **corp.local**.
2. Available Actions has changed to **Leave Domain**
3. Select the dropdown box arrow next to Local Admin and select Logout
4. Select Go back to login page
Login using AD Credentials

1. Confirm Remember this setting box is selected
2. Click on Next

Forgot password?
3. Notice how `corp.local` is now listed above the Sign in button.
4. During the module you logged in using the local account `admin`. Now we will login using a domain account. Enter the username: `administrator` password: `VMware1!`
5. Click on **Sign in**

### Navigate Back to Identity and Access Management

1. In the upper right hand corner, click on the drop down arrow net the your user name
2. Select **Administration Console**
3. **Identity & Access Management**
4. Select **Setup**
5. Select **Custom Branding** tab

You will notice the login screen now looks a little different now that it has been added to the domain
Next we have the **Custom branding** tab. This allows you to change the company name and name that appears on your browser page title.

1. Notice the current tab for your vIDM appliance says **VMware Workspace One**
2. For Company Name: Confirm it says VMware
3. For Product Name: Replace what is currently there with **VMworld**
4. Click on **Save**
5. Select the refresh button on your browser
6. It should now say VMware VMworld
Network Ranges

1. Click on **Setup**. The refresh of the browser causes the appliance to go back to Manage.

2. With **Network Ranges** you can create ranges to reflect for example LAN users or VDI desktops. With a network range specified you can define access policies based on the range. An important setting is the View Client Access URL Host. This is the address clients will use to connect to View if you are brokering View entitlements using the portal. Client Access URL Host setting is only displayed if you have configured Horizon/View integration. Each network range has its own Client access URL. So make sure you edit the URL to reflect your networks configuration.
1. Select Appliance Settings
2. Within this tab you can specify the license key and a SMTP server. But most likely you want to configure more so then you need to click on **Manage Configuration**. This will cause an additional tab in your browser to be opened.
3. Enter **VMware1**!
4. Click on **Login**
Manage Configuration for vIDM Appliance

Once you clicked on Manage Configuration, you get access settings for the management of the appliance itself. These settings are typically one time only settings that you configure once per installation.

1. **Database Connection**: Here you specify which database to use. This is the same setting as you where asked during the initial web wizard.
Install Certificate and FQDN

1. Install Certificate: You can leave vIDM using its own self signed certificate. If you want to change the certificate you can do it here. You must upload the whole certificate chain. More information how to configure certificates can be found in the VMware Identity Manager Connector Installation and Configuration Guide.

2. Identity Manager FQDN: Changing the vIDM FQDN is often done to allow for external access. The FQDN should point to your reverse proxy or load balancer placed in the DMZ. The DMZ component terminates certificate and forwards traffic to vIDM by initiating a new session. In order to change the FQDN of vIDM you must trust the certificate used on your DMZ component and must be able to do a roundtrip communication through the DMZ component all the way to itself.
Configure Syslog and Change Appliance Password

The Manage Configuration section is also where you would go to perform tasks that may need to be done on a manual basis within your environment.

1. **Configure Syslog**: Allows for a copy of the vIDM logs files to be sent to an external source
2. **Change Password**: This is where you would go to change the local appliance admin password.
System Security and Log File Locations

1. **System Security**: Here is where you would go to change the root and ssh password

2. **Log Files Locations**: From here you can not only locate where your log files currently reside, but also create a log bundle for trouble shooting purposes
Conclusion

You have now completed Module 1. You should now be familiar with the initial setup and configuration of VMware Identity Manager for a simple install.

Please close all browser windows before proceeding to the next Module.

For More Information

Additional information on installation or configuration of VMware Identity Manager can be found:

- Click on this [https://www.vmware.com/support/pubs/identitymanager-pubs.html](https://www.vmware.com/support/pubs/identitymanager-pubs.html)
- Or use your smart device to scan the QRC Code.

Proceed to any module below which interests you most:

- **Module 2 - Integrating Identity Manager with Horizon 7.1 (30 minutes)** (Advanced) Integrate vIDM with Horizon 7
- **Module 3 - Integrating Identity Manager with ThinApp (30 minutes)** (Advanced) Integrate vIDM with ThinApp
- **Module 4 - Multifactor Authentication using RADIUS (15 minutes)** (Advanced) How to configure RADIUS authentication to work with vIDM
- **Module 5 - Integrating Identity Manager with SAML-based Web App (15 minutes)** (Advanced) Integrating vIDM with SaaS and Web Applications

The HOL-1851-8-ADV Lab will cover setup of vIDM with an external database and as part of Cloud Pod Architecture (CPA).
Module 2 - Integrating Identity Manager with Horizon 7.1 (30 minutes)
**Introduction**

VMware Identity Manager lets you build a self-service app store, so users can access virtually any application on any device from a single portal. This allows for better control for admins and better ease of use for the end-user.

With support for Bring Your Own Device (BYOD) initiatives, Workspace ONE lets IT centrally deliver, manage and secure these assets across devices. It reduces employee on-boarding time, consolidates access to corporate resources for better intellectual property protection and reduces helpdesk calls.

In this module you will learn how to integrate Horizon 7 with VMware Identity Manager to access hosted applications.

**VMware Identity Manager and Horizon SSO**

1. A user authenticates to VMware Identify Manager. The administrator can select from an extensive set of authentication methods (RSA SecurID, RADIUS,
Biometric, and so on). After authentication, the user selects a desktop or application to launch from VMware Identity Manager.

2. Horizon Client is launched with the user’s identity, and credentials are directed to the View Connection Server, the broker for Horizon 7.

3. The broker validates the user’s identity with VMware Identity Manager by sending a SAML assertion.

4. Using the certificate Enrollment Service, Horizon 7 requests that the Microsoft Certificate Authority (CA) generate a temporary, short-lived certificate on behalf of that user.

5. Horizon 7 presents the certificate to the Windows operating system.

6. Windows validates the authenticity of the certificate with Active Directory.

7. The user is logged in to the Windows desktop or application, and a remote session is initiated on the Horizon Client.

**Lab Ready?**

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.

**Note:** It can take 10-20 minutes for the Lab Status to be **ready** in case of a "cold vPOD". Typically we aim to have several vPODs for each lab ready to go. If your lab is **not ready**, please wait a couple minutes before calling for help.
If you went through Module 1 prior to this Module, please be sure to close all browser windows prior to proceeding. We will NOT use the vIDM instance (vidm-02a) from Module 1 for this module. Modules 2-5 will use a pre-configured instance of vIDM (vidm-01a).
Enabling View Applications for Use with VMware Identity Manager

To enable Horizon 7 Machines or Applications Pools in VMware Identity Manager (vIDM), we have to switch to the Catalog and add a View Application.

As this vPOD is used by other Labs, vIDM has been configured for use with Horizon View already, but we will walk through the steps to verify the necessary steps.

Open Workspace ONE Admin Console

1. Open Chrome and select **WS1 Admin** Bookmark

Login to Workspace ONE
Sign in to Workspace ONE

1. User **admin**
2. Password **VMware1!**

Note: For this lab we are using the admin user from the **System Domain** of vIDM, not a domain user. You can configure a domain user or group to be admin users if you prefer.

**Add View Application**

1. Switch to **Catalog**
2. Click **Manage Desktop Applications**
3. Select **View Application**
Enable View Pools

1. Verify **Enable View Pools** is checked
2. Verify Connection Server is set to: `view-01a.corp.local`
3. Verify user is set to: `administrator`
4. Scroll down
5. Verify **Suppress Password Popup** and **Sync Local Entitlements** are set
6. Verify **Deployment Type** is set to **Automatic**
7. Click **Save**

The default setting for **Deployment Type** is **Automatic**, this will automatically add applications and virtual desktops entitled via Horizon 7 to the user's Portal

### Change to Horizon View Admin Console

1. Click on **Admin Console** to open Horizon View Administrator Console

**Note:** In a new setup, the SSL Cert of the Horizon View Server would need to be accepted and SAML Authentication would need to be enabled before proceeding, in this lab we have already done this for you.
Enable SAML Authentication in Horizon 7

In this step we will verify that SAML Authentication between Horizon 7 and VMware Identity Manager has been enabled.

Login to Horizon View Console

1. User name: administrator
2. Password: VMware1!
3. Click Log In
Switch to Connection Servers

1. Underneath View Configuration, select Servers
2. Click Connection Servers
3. Select VIEW-01A
4. Click Edit
Verify SAML Authenticator Settings

1. Click **Authentication** tab
2. Verify **Allowed** is set in the drop down
3. Verify **VIDM-01A** is set as SAML Authenticator
4. Click **Manage SAML Authenticators...**
Verify SAML Authenticator

1. Verify Status is **Enabled**
2. Select **VIDM-01A**
3. Click **Edit...**

**Edit SAML Authenticator cont.**

1. Verify Label is set to: **VIDM-01A**
2. Verify Metadata URL is set to point to our vIDM appliance (https://vidm-01a.corp.local...)
3. Click **Cancel**

If you click **OK** you will receive a certificate warning and will have to accept the certificate before continuing.
Verify settings

1. Click **Cancel**
2. Click **Cancel**
Configuring Horizon 7 Application Pools

You will see there are some entitlement for applications (and Desktop Pools) available in Horizon View. We will add a new one for and walk you through the process of synchronizing with vIDM.

Add Application to Pool

1. Under Catalog select **Application Pools**
2. Click **Add**
Find VMware WordPad on RDSH Farm

1. Enter Filter: **word**
2. Click **Find**
3. Select **checkbox** next to the WordPad in search results
4. Click **Next**
Verify Display Name

1. Click Finish

Add Entitlements
1. Click **Add**

**Select Entitlement User**

1. Uncheck the checkbox next to **Groups**
2. Enter `lab1` in 'Name/User name:' (leave drop down set to **Contains**)
3. Click **Find**
4. Click on **Lab 1 User** to select
5. Click **OK**
Verify Entitlement

1. Verify `lab1user@corp.local` is listed as user who can use selected pool.
2. Click **OK**

Verify WordPad is available

1. Verify **Wordpad** is listed under Application Pools and has status **Available**
Synchronize VMware Identity Manager with Horizon 7

In order for changes from Horizon 7 Application Pools to appear in VMware Identity Manager, we need to synchronize the two.

Return to VMware Identity Manager

1. Click VMware Workspace ONE tab next to View Administrator in your browser to return to the VMware Identity Manager View Pools site
Synchronize View Pools

1. Scroll down
2. Click Sync Now
Verify Application Entitlement

1. Verify new entitlement has been added
2. Click Application

Verify Application Details

1. Click the x to close the window
Save Synchronization

1. Click **Save and Continue...** to commit changes.

Return to Admin Console

1. Click on the first browser TAB to return to the catalog
2. Refresh page
3. Scroll down
4. Verify WordPad is available in the catalog
Check Entitlements for Horizon 7 Application Pools via VMware Identity Manager

In this step we will check entitlements for Horizon View Pools in VMware Identity Manager

Verify View Pool App Details

1. Click on **WordPad**
Verify application entitlement

1. Verify Type is **View Hosted Application**
2. Verify the **User, Lab 1** is entitled and the deployment is set to **Automatic**

Verify Details
1. Click **Details**
2. Note some of the details listed for this app, including the **Connection Server** and **supported client types**

**Verify Licensing**

1. Click **Licensing**
2. Click **Edit**
Edit Licensing

1. Leave License approval required **unchecked**
2. set License Pricing to **Permanent**
3. set License Type to **Named User**
4. Set Cost per License to **10**
5. Set Number of Licenses to **5**
6. Click **Save**

**Note:**

- License approval requires an external approval REST-based approval system.
- While you can report on licenses, vIDM will not enforce licensing by blocking users from accessing apps.
- Licensing within vIDM is by no means a replacement for a full featured license management system.

**Access Application as user**
Open New Incognito Browser Window

Open a new Incognito Window in Chrome

1. Click the three vertical dots in the upper right corner of the Chrome Browser
2. Select New incognito window

Log In to WS!

1. Click on WS1 shortcut (not WS1 Admin)
Confirm Domain

1. 1. Confirm domain is set to corp.local
2. 2. Click Next

Log in As Lab1user

1. Username: lab1user
2. Password: **VMware1!**
3. Click **Sign in**

**Verify App is available**

1. Verify **WordPad** is available and click on it
Possible Error: Request not supported error

You might get an error message "the request is not supported"

NOTE: This is due to the time sync drift in the HOL lab and you would not see this error under normal conditions. The following steps will walk you through a quick fix.

If the app launched with no errors then please skip ahead

1. **Read** the error message "The request is not supported
2. **Close** the browser tab
Launch the Services on the Main Console

1. Click on the Windows icon
2. Enter services
3. Click on the Services icon
Restart the Active Directory Domain Services to Sync Time

Since time is out of sync in the HOL lab, the quickest way to rectify the situation is to restart the Active Directory Domain Services.

1. Right Click on the **Active Directory Domain Services** service
2. Click on **Restart**
3. Click **Yes** on the confirmation pop-up
4. Click the **X** to close the Services window when the service has restarted
Relaunch the Application

1. Verify **WordPad** is available and click on it

**WordPad will launch in Browser Tab**

1. Notice WordPad will be launched in a new Browser Tab
2. Close the Incognito Browser
Conclusion

In this module you have learned how to enable Horizon 7 Application Pools in VMware Identity Manager and configure SAML Authentication in Horizon View to allow single-sign-on.

VMware Identity Manager Resources

You can find more information on the vIDM website:

https://www.vmware.com/products/identity-manager

Choose Module to continue with

You can now proceed to the next module or any module below which interests you most:

- **Module 1 - Introduction to Identity Manager and Workspace ONE (30 minutes)** (Beginner) Learn how to install and perform initial configuration of vIDM
- **Module 2 - Integrating Identity Manager with Horizon 7.1 (30 minutes)** (Advanced) Integrate vIDM with Horizon 7
- **Module 3 - Integrating Identity Manager with ThinApp (30 minutes)** (Advanced) Integrate vIDM with ThinApp
- **Module 4 - Multifactor Authentication using RADIUS (15 minutes)** (Advanced) How to configure RADIUS authentication to work with vIDM
- **Module 5 - Integrating Identity Manager with SAML-based Web App (15 minutes)** (Advanced) Integrating vIDM with SaaS and Web Applications
Module 3 - Integrating Identity Manager with ThinApp (30 minutes)
Introduction

In this module you will learn how to configure a ThinApp repository in VMware Identity Manager and entitle users/user groups to access applications. You will learn how to modify existing ThinApp packages to work with VMware Identity Manager and handle updates for ThinApp packages presented via the VMware Identity Manager.

Lab Ready?

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.

Note: It can take 10-20 minutes for the Lab Status to be ready in case of a "cold vPOD". Typically we aim to have several vPODs for each lab ready to go. If your lab is not ready, please wait a couple minutes before calling for help.
Configure ThinApp Repository

In this step you will learn how to add a ThinApp Repository to VMware Identity Manager and entitle ThinApp-Packages to users.

Add ThinApp Application

1. Click **WS1 Admin** to open Admin Console in Chrome
2. User **admin**
3. Password **VMware1!**
4. Click **Sign In**

Add ThinApp Applications
1. In the Administrator Console click **Catalog** tab
2. Click **Manage Desktop Applications**
3. Select **ThinApp Application**

**Enable ThinApp Repository**

Verify the following settings:

1. Check box to enable packaged applications
2. Enter Path: `\Controlcenter\ThinAppRepository`
3. Check box to enable account based access. This is necessary in order to use HTTP download and DFS shares, which is what we want for this lab.
4. Enter Share User: `administrator`
5. Enter Share Password: `VMware1!`
6. Click **Save**

**Tip**

In a production environment, make sure to use a service account as the 'Share User' and be mindful of password changes etc.
Synchronize

1. Click **Sync Now**

**Verify Packaged Apps were detected**

Packaged Apps - ThinApp
1. Note **Upload failed** message for Notepad++ 7.4.1 and Orca
2. Click **OK**

### Switch to admin console

![Switch to admin console](image)

1. Click **VMware Workspace ONE** tab on the left

   Leave the other tab open, we will come back to it.

### Check Log File

![Check Log File](image)

1. Select drop down menu next to Catalog
2. Select **Settings**
Open Alerts

1. Click ThinApp Application Alerts
2. Click Open Alerts
Notice Alerts

1. Scrolldown
2. Note Alerts related to the failed upload, indicating that something is wrong with our executable
3. This Error Message also indicates that the package is missing an **AppID**, indicating the package was not built to work with VMware Identity Manager when captured.

In the next steps we are going to fix this.
ThinApp packages have to be prepared to work with Workspace ONE, this can be done using `relink.exe`, recapturing the package with the option for vIDM selected or modifying the Package.ini of your ThinApp and rebuilding the package.

The KBAs below contain great information on this topic:

- Enabling VMware ThinApp virtual applications for Horizon Application Manager with the relink command (2021928)
- Enabling for Horizon a previously packaged VMware ThinApp virtual application, without relinking (2030595)

### Relink App to work with vIDM

1. Open Command Prompt

### Run relink for Orca

1. Type: `relink -h "C:\Tools\ThinApps\Orca\Orca.exe"` and hit ENTER

2. Verify output from command: "enabling package for Horizon" and the package AppID.
Tip

- Using `relink.exe -h` prevents us from having to re-capture/package the application.
- Relink will also create a backup (*.bak) of the existing *.exe-file in the folder.
- ThinApp Packages must not contain an *.alt-file used for packages containing Windows 32-bit and Windows 64-bit code. See KBA# 2089738 for more details.
- As we used a temporary license key for this lab the ThinApp Package will expire on the date the license key expires.
- For full transparency: to make things a little easier for this lab, the folder containing relink.exe was added to the PATH system variable, otherwise you would have to switch to the folder containing relink.exe or provide the full path when using it.

Switch to Catalog / Add ThinApp Application

1. Click on the browser TAB to the right to get to the ThinApp Configuration Page

Sync Now
1. Scroll Down
2. Click Sync Now

Verify Opera uploaded correctly

1. Verify Orca uploaded successfully this time
2. Click OK

Info

Please ignore the "upload fail" for Notepad++ 7.4.1 for now, we will address this later, when we show how to upgrade a ThinApp package.
Switch to Catalog

1. Click Admin Console

Verify Orca is available in Catalog

1. In the Administration Console click Catalog
2. Verify Orca is available in catalog now
Tip

Sometimes a generic logo is displayed for an app. This happens if InventoryIcon parameter in Package.ini of the ThinApp package is not set. You can also use this parameter to choose a specific Icon you want to be displayed, see Dean's Blog for details on how to set InventoryIcon.
Entitle ThinApp Packages to Users

After the sync with the ThinApp Repository, we need to entitle users to use them.

Switch to Catalog

1. In the Administrator Console click Catalog
2. Click the little arrow next Any Application Type
3. Select ThinApp Packages
4. Click on Safari
Add Entitlement

1. Click + **Add group entitlement**
Select Group
Add Group Entitlement:

1. Enter the user name: vtDM Users@corp.local
2. Select the user: vtDM Users@corp.local
3. Select the option: Automatic
4. Choose the type: User-Activated
5. Save the changes
1. Type 'v'
2. Select **vIDM User@corp.local**
3. Click **Save**
4. Select 'Automatic' for deployment type
5. Click **Save**

### Update Tables

1. Click **Done** to update tables
Configure vIDM Desktop Client and Verify ThinApp Package Install

For ThinApp entitlement and deployment to work, each client must have the VMware Identity Manager Desktop Agent installed. This lightweight Agent synchronizes entitlements from the central VMware Identity Manager Portal. The Agent keeps a local entitlement database so users can launch packages while offline. The local entitlement database is by default valid for 30 days. The Agent also enables distribution locally to the client. There is three deployment methods supported for ThinApp Packages; Local, Run From Share and HTTP delivery. Which delivery mechanism to use is specified during installation of the Agent and can be changed via registry keys after the Agent is installed.

**Local deployment** means clients will download the ThinApp packages to their hard drives from the ThinApp repository using SMB.

**Run From Share** means the ThinApp packages are never downloaded to the local client but executed over the network using ThinApp's streaming mechanism.

**HTTP delivery** downloads the packages to the local client using HTTPS as the protocol. This allows the clients to be non-domain members and located outside the firewall (clients do not need direct access to the ThinApp repository, Workspace proxies the file download).
Open Windows 10 Desktop

1. Open **Base-w10-x64-01** (Windows 10 Desktop)
2. Select other user: **corp\lab2user**
3. Password: **VMware1!**
4. Click **OK**
Identity Manager Desktop - Login

Upon first login of a user after Identity Manager Desktop has been installed, the user needs to authenticate. In this lab environment, we have installed Identity Manager Desktop on base-w10-x64-01 already, so you just need to authenticate the user.

1. Username **lab2user**
2. Password **VMware1!**
3. Click **Sign in**
Verify Identity Manager Desktop connection

With the previous step we authenticated our user to vIDM, you can verify that the VMware Identity Manager Desktop Client has been configured correctly via the task bar icon:

1. Click to **Show Hidden Icons** in task bar
2. Click on the **VMware Identity Manager Desktop Icon**
3. Verify you see **Next sync in xx seconds**

**Note:**

The default sync time is 5 minutes, for this lab we configured the Client to check for changes every 60 seconds.

In an enterprise environment, you likely would deploy the agent to all computers using your existing software deployment solution (i.e. Microsoft SCCM, Altiris etc.) or have it pre-installed for your VDI environment. The installer allows for silent install without interaction and all switches are well documented.

**Logged In Notification**

You will see a Status Notifications from the VMware Identity Manager Client in the lower right corner of your screen, confirming succesful log in.
Package Installed Notification

Depending on timing, you might have seen this before the last step, the VMware Identity Desktop Client controls ThinApp Packages for the user and since we set deployment to automatic, the Safari ThinApp Package will get installed for the user.

Confirm Safari Shortcut is available

Feel free to open Safari to test the application.

Minimize Remote session

1. Close Safari (if open)
2. Minimize (don't close!) the Remote Desktop session, to switch back to the Main Console
Updating ThinApp Packages

Now we will show you how to update a ThinApp Package in VMware Identity Manager. First we entitle Notepad++ 7.2 and then we’ll update it to Notepad++ 7.4.1. For VMware Identity Manager to discover a ThinApp package as an update to an existing package, the new package needs:

- the same ApplID
- a Version ID higher than the existing package
- both packages need to use the same package identifier/InventoryName

It is not necessary for the new package to be captured as update to an existing package, the necessary changes can be made by modifying the Package.ini and/or using relink.exe.

Switch Back To Admin Console

1. Switch to Catalog
2. Select ThinApp Packages as filter
3. Click Notepad++ 7 (32-bit x86)
Add Entitlement

1. Notice Version is 1.0
2. Click + Add group entitlement
1. Type v
2. Select vIDM User@corp.local
3. Click Save
4. Set to 'Automatic' for deployment type
5. Click Save

**Update Tables**

1. Click Done to update tables
2. Leave Chrome running and switch to Remote Desktop base-w10-base-x64
Verify Notepad++ Gets Deployed

As mentioned before, Identity Manager Desktop will check every 60 seconds for updates, based on timing, you might have to wait a couple of seconds before Notepad++ will appear on the desktop.

1. Open NotePad++ from Desktop
2. Click the '?'
3. Select **About Notepad++**
Verify Version

1. Verify Version is v7.2
2. Click **OK**
3. Close Notepad++

Switch to Main Console

1. **Minimize** Remote Desktop (**do not close session**) to switch back to Main Console
Get AppID of previous Notepad++ version

Now let's go through the necessary steps to update an existing ThinApp Package within Workspace ONE. We already saw in the admin console that the Version of the existing Notepad++ package is 1.0, now we need to get the AppID of the package. There are different ways of getting the AppID (GUID) of the existing package, for example, you can run a relink -h on the package or get it from the Workspace ONE Admin Console, this is what we are doing for this lab:

Back on the Main Console, you should still see Modify application screen, if not, open the WS1 Admin console and go to Notepad++ in the Catalog again.
1. Click on Details
2. **Mark the GUID**, you can do this by clicking on the left bracket and and move the mouse to the right bracket while still pushing down the mouse button. Make sure to include both brackets.
3. **Right-click** on on the **marked GUID** to open the menu
4. select **Copy**

**Relink Notepad++ 7.4 as update to Notepad++ 7.2**

1. Open **Command Line**

**Relink Notepad++**

1. Switch to the project folder for the new version of Notepad++

```cmd
cd "c:\Tools\ThinApps\Notepad++ 7.4.1"
```
Relink Notepad++

1. Type relink command

```
relink -h -AppID
```

(do NOT hit enter yet)

2. **Right click** inside the Command Prompt Window and **paste** previously copied AppID

Run relink, verify AppID/Version ID

1. **continue** typing

```
-VersionID 2 "notepad++.exe"
```
the complete command line should like

```
relink -h -AppID {6E2C41A3-8462-473C-AD02-934FD4CCD5D2} -VersionID 2 "notepad++.exe"
```

hit ENTER

2. Verify **AppID** is set to the same AppID as the old package and **Version** is set to **2**

**Tip**

- Type relink without any parameters to get available options.
- VersionID needs to be an integer value between 2-99

**Re-Sync ThinApp Repository**

1. Open VMware Identity Manager Admin Console and switch to **Catalog**
2. Click on **Manage Desktop Applications**
3. Select **ThinApp Application**
Scroll Down to Sync

1. In the new tab, scroll down
2. Click Sync Now
Verify Notepad++ 7.4 Is Uploaded

1. Note **Notepad++ 7.4.1** is successfully uploaded
2. Click **OK**

**Note:** While we are detecting both version of Notepad++ in the ThinApp Repository (as shown in the screen above), you will notice only one will show in the catalog.

Switch Back to Admin Console

1. Click **Admin Console**
Verify Entitlement

1. Click on 'Notepad++ (32-bit x86)'

**Note:** Though both versions of Notepad++ were uploaded to VMware Identity Manager, only one version is displayed in the catalog. If you want both versions to show, you can do so, by using different values for the InventoryName in the Package.INI and AppIDs, you will have to manage the packages/entitlements independently.
Verify Version is 2.0 and Entitlement is unchanged

1. Verify Application Info: Version should now be 2.0
2. Verify entitlements are unchanged

Switch Back to Remote Desktop

1. Switch back to the Remote Desktop session

Package Updated Notification

If you are quick enough, you might see a **Package Updated** notification.
Verify new Version got installed

1. Open **Notepad ++**
2. Click on ?
3. Select **About Notepad++**
4. Verify Version is **7.4.1**
5. Click **OK**
6. Close Notepad++
Log Out from Remote Desktop

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

In this module you have learned how to add a ThinApp Repository to VMware Identity Manager and present ThinApp Packages to users. You have also learned how to use \texttt{Relink.exe} to modify existing ThinApp Packages to work with VMware Identity Manager and how to update an existing ThinApp Package with a new version.

VMware Identity Manager Resources

You can find more information on our website:

\url{http://www.vmware.com/products/identity-manager/}

Choose Module to continue with

You can now proceed to the next module or any module below which interests you most:

- **Module 1 - Introduction to Identity Manager and Workspace ONE (30 minutes)** (Beginner) Learn how to install and perform initial configuration of vIDM
- **Module 2 - Integrating Identity Manager with Horizon 7.1 (30 minutes)** (Advanced) Integrate vIDM with Horizon 7
- **Module 3 - Integrating Identity Manager with ThinApp (30 minutes)** (Advanced) Integrate vIDM with ThinApp
- **Module 4 - Multifactor Authentication using RADIUS (15 minutes)** (Advanced) How to configure RADIUS authentication to work with vIDM
- **Module 5 - Integrating Identity Manager with SAML-based Web App (15 minutes)** (Advanced) Integrating vIDM with SaaS and Web Applications
Module 4 - Multifactor Authentication using RADIUS (30 minutes)
Introduction

VMware Identity Manager allows for setting up Network Ranges and different authentication policies can be assigned to different network ranges.

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

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

Lab Ready?

1. Make sure the Lab Status is Ready
1. Open Start Menu
2. Select **FreeRADIUS START**
3. Verify FreeRADIUS is started and **Ready to process requests.**

**Warning**

Leave the FreeRADIUS START Window open or minimize it, but DO NOT close it.
Setup RADIUS as Authentication Adapter

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

Open Identity Manager console

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

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

Modify Authentication Adapters

1. Click Auth Adapters
2. Scroll down
3. Click RadiusAuthAdapter
Configure RADIUS

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

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

Define Network Range

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

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

This will add a "range" of one IP-Address (our Windows 10 VM)

**Info**

Step 3. and 4. are only visible/necessary if you have a Horizon View Connected to VMware Identity Manager.
Verify the new network range has been added

Change default access policy

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

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

1. Select RADIUS Test from dropdown menu
2. Select Web Browser from dropdown menu
3. Select RADIUS from dropdown menu
4. Click OK

Tip

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

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

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

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

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

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

Now we will verify the new policy is active.

Open New Incognito Windows

Open a new incognito browser window:

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

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

1. User **lab1user**
2. Click **VMware1!**

Verify Login

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

Test RADIUS Authentication from Windows10 VM

Now to the real test, minimize your browser windows.

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

1. Open Microsoft Edge browser
2. Browse to `vidm-01a.corp.local`
3. Click **Next**
Authenticate Using RADIUS

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

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

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

Verify you can access the portal successfully.
Disconnect and Log Off

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

We have shown how easy it is to integrate VMware Identity Manager with a RADIUS compatible 2FA solution. You can leave the FreeRADIUS running, if you are taking the Modules in a different order and the next Modules asks for login from the Windows 10 VM, please use the RADIUS Password 123456 instead of VMware1!

VMware Identity Manager also comes with a built-in 2FA solution, due to the networking limitation of this environment, we could not show it in this lab, but you can learn more about here: VMware Verify.

You can find a walkthrough of VMware Verify below:

http://support.vmtestdrive.com/article/252-vmware-verify-demo-walkthrough

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

Conclusion

You can find additional information on User Authentication options, including RADIUS, in the documentation for VMware Identity Manager.

The QR-Code will take you the link below:

Configuring RADIUS for VMware Identity Manager.

Choose Module to continue with

You can proceed to the next module or any module below which interests you most:
• **Module 1 - Introduction to Identity Manager and Workspace ONE (30 minutes)** (Beginner) Learn how to install and perform initial configuration of vIDM
• **Module 2 - Integrating Identity Manager with Horizon 7.1 (30 minutes)** (Advanced) Integrate vIDM with Horizon 7
• **Module 3 - Integrating Identity Manager with ThinApp (30 minutes)** (Advanced) Integrate vIDM with ThinApp
• **Module 4 - Multifactor Authentication using RADIUS (15 minutes)** (Advanced) How to configure RADIUS authentication to work with vIDM
• **Module 5 - Integrating Identity Manager with SAML-based Web App (15 minutes)** (Advanced) Integrating vIDM with SaaS and Web Applications
Module 5 - Integrating Identity Manager with SAML-based Web App (30 minutes)
Introduction

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

This will allow your users to have a single entry point for applications (ThinApps, Citrix XenApp, RDSH, SaaS) and VDI Desktops. With AirWatch you can even extend this to mobile apps.

Lab Ready?

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 Identity Manager.

Login to VMware Identity Manager

1. Open WS1 Admin in Chrome
2. Username: admin
3. Password: VMware1!
4. Click Sign in
Create New Web Application

1. Click 'Catalog'
2. Click 'Add Application'
3. Under Web Application select '...create new one'

Add Application

1. Enter Name: **vsphere Web Client**
2. Click on 'Choose File' select **vsphereLogo.jpeg** (C:\Tools\Icons)
3. Select Authentication Profile 'None'
4. Click 'Next'
Add Application Configuration

1. Enter Target URL: **https://vcsa-01a.corp.local/ui**  (Note: you can copy/paste from README.txt or existing bookmark in your browser)
2. Click 'Save

Add Entitlement

1. Click on 'Add group entitlement'
Select Admin

1. Type: a
2. Select ALL USERS

Switch to Automatic

1. Switch deployment type to 'Automatic'

This will automatically deploy the shortcut to the Admin's Workspace. If you chose 'User-Activated', the user will have to manually add the application from the App Center.

2. Click 'Save'
Update Tables

1. Click 'Done' to update entitlement tables.

Verify vSphere Web Client Shortcut is available

1. Click drop down menu next to user name
2. Select 'User Portal'
Verify new Shortcut has been added

1. Switch to LAUNCHER
2. Click vSphere Web Client

Note: Refresh the web site in case the logo does not appear automatically. If it still does not appear, go back to the CATALOG and add it, you might have missed switching to from 'user-activated' to 'automatic' when you created the entitlement.
Verify vSphere Web Client opens

Verify vSphere Web Client page comes up. As we didn't configure any SSO/SAML integration, we basically just created a bookmark within Workspace ONE and don't automatically log you in.

1. Close the tab
Add SAML based Web Application and SSO Configuration

In this lab we will add our SAML 2.0 Test-App and configure VMware Identity Manager to pass user information to the app. In preparation for this lab, we already configured the SAML Test-App to trust VMware identity Manager by adding the certificate to the Test App.

Switch back to Administration Console

1. Click the drop down menu next to the user name
2. Select 'Administration Console'
SAML 2.0 Preparation

SAML Integration requires configuration on the VMware Identity Manager 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. You can find the necessary information (signing certificate and IdP URL) in the Administration Console:

1. Click drop-down menu
2. Select 'Settings'
3. Click 'SAML Metadata'
4. SAML Metadata (IdP and SP) can be retrieved here
5. Signing Certificate
You don't have to perform this step in the lab.

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

1. Click on 'Catalog'
2. Click on 'Add Application'
3. Select '...create a new one'

Add SAML 2.0 App

1. Enter Name: **SAML 2.0 App**
2. Click on 'Choose File' and select 'SSO_NEW.jpg' from C:\Tools\Icons
3. Select 'SAML 2.0 POST profile' as Authentication Profile from the drop down menu
4. Click 'Next'
Application Configuration

1. Sign Assertion: click check box for 'Sign the assertion'
2. Include Cert: click check box for 'Include the signing certificate in the response'
3. Scroll down
Application Configuration cont.

1. Configure Via: switch to 'Manual configuration'
4. Enter Audience: php-saml
5. Scroll down

Note: You can drag&drop the input from the manual into the input fields, rather than typing it.
Attribute Mapping

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

1. Enter Name: **firstname**
2. Click drop down menu for Value
3. Select $${user.firstName}$$ from Value drop down
4. Click ‘Add another attribute’

**Note:** Depending on your screen resolution or browser zoom setting, you might have to scroll to the right.

Attribute Mapping continued

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 **Save**

**Add Entitlement**

1. **Click 'Add group entitlement'**
Entitle Domain Users

1. Type: a
2. Select 'ALL USERS'
Switch to Automated

1. Switch Deployment Type to 'Automatic'
2. Click 'Save'
Update Tables

1. Click 'Done' to update entitlement tables

Open New Incognito Browser Window

1. Click on the 3 vertical dots
2. Select 'New incognito window'
Test Accessing SAML-Test App directly

2. Notice "Unauthenticated User" message, click on VMware Workspace ONE

Note:
You can drag the URL from the manual to avoid typos.

Log In to Workspace ONE

1. Click Next
Authenticate User

1. Username **lab2user**
2. Password **VMware1!**
3. Click **Next**
Open SAML 2.0 APP

1. Click **SAML 2.0 App**
Verify attributes are displayed

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

For this to work, the necessary information must be available for each user in Active Directory and the attributes need to be synced with vIDM. If you make changes to attributes in AD, a sync between VMware Identity Manager and the Directory has to happen.
VMware Identity Manager also allows for adding 'Web Application from the cloud 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 90 (and growing) pre-configured templates for typically used web/SaaS applications such as ADP, Salesforce.com, Office 365, Workday, ServiceNow and many others more.

The steps below won't work in the HOL environment, as this environment is not connected to the Internet, they are ment just as a reference.

1. Add Application
2. Web Application ...from the cloud application catalog

Cloud Application Catalog
The list of out-of-the-box provided SaaS applications is constantly growing.

Just because an application is not listed, does not mean it is not supported/working with VMware Identity Manager, it might just be a little more work to set it up.
Conclusion

In this module you learned how 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 Identity Manager and your application. Always consult documentation for VMware Identity Manager and your application for details.

VMware Identity Manager Integration Documentation Library

You can find more information on our website:

https://www.vmware.com/support/pubs/vidm_webapp_sso.html

Choose Module to continue with

You can proceed to the next module or any module below which interests you most:

- **Module 1 - Introduction to Identity Manager and Workspace ONE (30 minutes)** (Beginner) Learn how to install and perform initial configuration of vIDM
- **Module 2 - Integrating Identity Manager with Horizon 7.1 (30 minutes)** (Advanced) Integrate vIDM with Horizon 7
- **Module 3 - Integrating Identity Manager with ThinApp (30 minutes)** (Advanced) Integrate vIDM with ThinApp
- **Module 4 - Multifactor Authentication using RADIUS (15 minutes)** (Advanced) How to configure RADIUS authentication to work with vIDM
- **Module 5 - Integrating Identity Manager with SAML-based Web App (15 minutes)** (Advanced) Integrating vIDM with SaaS and Web Applications
Lab Conclusion
Conclusion

This concludes lab 1851-05-MBL. Please make sure to fill out the survey at the end.
Conclusion

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

Lab SKU: HOL-1851-05-ADV

Version: 20180614-203637