# Table of Contents

Lab Overview - HOL-1957-01-UEM - Workspace ONE UEM with App & Access Management

Lab Guidance................................................................................................................................. 2

Module 1 - Workspace ONE Setup and Configuration................................................................. 8

Introduction....................................................................................................................................... 9
VMware Enterprise Systems Connector Setup............................................................................... 10
Login to the Workspace ONE UEM Console ............................................................................ 12
Login to the VMware Identity Manager Console ...................................................................... 18
Configure Your VMware Identity Manager Tenant.................................................................... 23
Configure Directory Services and VMware Identity Manager User Sync............................... 25
Review Your Configuration in VMware Identity Manager......................................................... 40
Integrate Workspace ONE UEM and VMware Identity Manager using the Cloud Kerberos Key Distribution Center (KDC) .................................................................................. 43
iOS Device Enrollment With Directory Account........................................................................... 67
SSO Validation................................................................................................................................. 86
Un-enrolling Your Device ............................................................................................................... 97
Conclusion...................................................................................................................................... 106

Module 2 - Workspace ONE UEM Configuration, AD Integration/Certificates.......................... 107

Introduction...................................................................................................................................... 108
VMware Enterprise Systems Connector Setup........................................................................... 109
Login to the Workspace ONE UEM Console ............................................................................ 111
Directory Services Integration....................................................................................................... 117
Configuring an Enterprise Certificate Authority ........................................................................ 124
Login to the Workspace ONE UEM Console (IF NEEDED)...................................................... 138
Add the Certificate Authority in Workspace ONE UEM........................................................... 141
Create an iOS Profile with a Credential Payload....................................................................... 148
iOS Device Enrollment With Directory Account .......................................................................... 156
View the Certificate on the Device.............................................................................................. 175
Un-enrolling Your Device ............................................................................................................. 179
Conclusion...................................................................................................................................... 188
Lab Overview - HOL-1957-01-UEM - Workspace ONE UEM with App & Access Management
Lab Guidance

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

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

Looking for the latest on the VMware Workspace ONE solution? Integrate Workspace ONE UEM and Workspace ONE Identity Manager to enable Single Sign-On from any device to any application, and deploy applications through Workspace ONE. Learn how Workspace ONE provides a best-in-class user experience without sacrificing enterprise security.

Lab Module List:

- **Module 1 - Workspace ONE Setup and Configuration** (60 minutes) (Intermediate) Configure the VMware Enterprise Systems Connector, Active Directory, and VMware Identity Manager integrations with AirWatch to enable Single Sign-On (SSO) for your users on an iOS device.
- **Module 2 - Workspace ONE UEM Configuration, AD Integration/ Certificates** (45 minutes) (Intermediate) Integrate your Active Directory and Certificate Authority with Workspace ONE UEM to seamlessly distribute certificates for authentication.

Lab Captains:

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

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

http://docs.hol.vmware.com

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

Location of the Main Console

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

Alternate Methods of Keyboard Data Entry

During this module, you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.

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

**Accessing the Online International Keyboard**

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

1. Click on the Keyboard Icon found on the Windows Quick Launch Task Bar.

**Click once in active console window**

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

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

1. Click on the "@ key".

Notice the @ sign entered in the active console window.

Activation Prompt or Watermark

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

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

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

This cosmetic issue has no effect on your lab.
Look at the lower right portion of the screen

Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes your lab has not changed to "Ready", please ask for assistance.
Module 1 - Workspace ONE Setup and Configuration
Introduction

Workspace ONE UEM integrated with VMware Identity Manager is the core of Workspace ONE, providing Single Sign-On access to applications by providing various authentication mechanisms to ensure secure access and improving user experience. This module will detail how to configure VMware Identity Manager with Workspace ONE UEM and how to enable Single Sign-On access into the VMware Identity Manager console from the iOS device.

Although the focus of this module highlights the iOS implementation and functionality, you can provide Single Sign-On capabilities for other devices (like Android, macOS, and Windows 10) as well.
VMware Enterprise Systems Connector Setup

The VMware Enterprise Systems Connector allows organizations to integrate AirWatch with back-end enterprise systems without exposing or compromising the security of these systems. The VMware Enterprise Systems Connector runs in the internal network and acts as a proxy that securely transmits requests from AirWatch to enterprise infrastructure components.

For the purposes of the lab, the VMware Enterprise Systems Connector is already setup and configured for you. The following steps will review the architecture and show a demo video of how to install the VMware Enterprise Systems Connector.

Architecture Overview

The simple architecture diagram above demonstrates the following concepts:

- The VMware Enterprise Systems Connector is installed on the internal network where it is able to access your Active Directory.
- The VMware Enterprise Systems Connector requires no inbound access from the internet, requiring no additional inbound ports to be exposed on your firewall.
- When deploying the VMware Enterprise Systems Connector with only the AirWatch Cloud Connector component installed, AirWatch can securely sync your Directory and users to your VMware Identity Manager tenant.

Continue to the next step when you are ready.
Video Demo of Installation

**NOTE:** The video contains no spoken instructions. Please refer to the subtitles for instructions about the installation process.

Please watch this short demonstration of how to install the VMware Enterprise Systems Connector before continuing to the next step.

**NOTE:** Do not attempt to make any of the configurations or changes shown in the demo video! This demonstration is only to highlight the configuration and installation process for your knowledge.
Login to the Workspace ONE UEM Console

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

Launch Chrome Browser

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

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

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

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

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

Terms of Use

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

VMWARE END USER LICENSE AGREEMENT

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

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

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

1. DEFINITIONS.

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

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

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

Security Settings

Password Recovery Question 1

Password Recovery Question *
What was your childhood nickname?

Password Recovery Answer *

VMware1!

Confirm Password Recovery Answer *

VMware1!

Security PIN

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

Security PIN *
1234

Confirm Security PIN *
1234

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

Close the Welcome Message

Workspace ONE UEM Console Highlights

Powered by VMware AirWatch!

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

Workspace ONE UEM transforms your business so you can:

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

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

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

Accessing Your Tenant Details in the Workspace ONE UEM Console

In the Workspace ONE UEM Console:

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

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

## Copy the Tenant URL

![Image of selecting and copying text](image)

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

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

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

## Login to Your VMware Identity Manager Tenant

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

## Launch Google Chrome (If Needed)

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

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

Click the Tab space to open a new tab.

Navigate to Your VMware Identity Manager Tenant

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

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

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

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

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

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

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

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

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

Continue to the next step.

Edit User Attributes

![Image of VMware Identity Manager user attributes settings]

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

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

### Save User Attribute Changes

1. Scroll down to the bottom of the page.
2. Click **Save**.
Configure Directory Services and VMware Identity Manager User Sync

You will now use the Workspace ONE Getting Started Wizard to configure Directory Services and to sync a directory to VMware Identity Manager.

Continue to the next step.

Setup Directory Services

You will now configure Directory Services through the Workspace ONE Getting Started Wizard to sync AD users to the Identity Manager tenant.

Return to the Workspace ONE UEM Console,

1. Click Getting Started.
2. Expand Getting Started.
3. Click Workspace ONE.
4. If the Setup section is minimized, click the + button to expand it.
   
   NOTE - You may need to scroll to the right to see the + button on the Setup bar.

5. Click Configure for the Enterprise Connector & Directory section under Setup.
   
   NOTE - You may need to scroll to the right to see the "Configure" button.
Configure Active Directory Server Settings

1. Enter `controlcenter.corp.local` for the **Server**.
2. Select **None** for the **Encryption Type**.
3. Enter **389** for the **Port**.
4. Enter **3** for **Protocol Version**.

Enter the Active Directory Binding Information Settings

1. Scroll down to find the **Binding Information** section.
2. Select **GSS-NEGOTIATE** for the **Bind Authentication Type**.
3. Enter `corp\administrator` for the **Bind Username**.
4. Enter `VMware1!` for the **Bind Password**.
5. Enter `corp.local` for the **Domain**.
6. Click **Save**.

### Test the Active Directory Connection

1. Click **Test Connection**.
2. Confirm the **Connection successful with the given Servername, Bind Username and Password** message appears.
3. Click **Continue**.
4. Click **Close**.

We are not finished with the Workspace ONE Getting Started Wizard yet, however, additional Directory Services configuration options must be made in order to find the correct groups for the Active Directory users in our Lab infrastructure. We will return to the Workspace ONE Getting Started Wizard after modifying our Group properties for our Active Directory configuration.
Open All Settings

Advanced Directory Services configurations will need to be made for the purpose of this lab.

1. Click **Groups & Settings**
2. Click **All Settings**
Configure the Directory Services Group Settings

1. Click **System**.
2. Expand **Enterprise Integration**.
3. Click **Directory Services**.
4. Click the **Group** tab.
5. Enter `container` for the Organizational Unit Object Class.
6. Expand **Advanced**.
Configure the Organizational Unit

1. Scroll down to the bottom of the page.
2. Click the Pencil (Edit) icon next to the Organizational Unit field. This allows the Organizational Unit field to be edited.
3. Enter `cn` for the Organizational Unit.
4. Click Save.
5. Click Test Connection.
6. Confirm the Connection successful with given Servername, Bind Username and Password message appears.

Close the Directory Services Menu

Click Close in the top right corner.
Setup the VMware Identity Manager Settings

With the Directory Services integration completed, return to the Workspace ONE Getting Started Wizard to integrate your VMware Identity Manager tenant.

1. Click **Getting Started**.
2. Expand **Getting Started**.
3. Click **Workspace ONE**.
4. If the **Setup** section is minimized, click the + button to expand it.
   
   *NOTE - You may need to scroll to the right to see the + button on the Setup bar.*
5. Click **Configure** for the **Enterprise Connector & Directory** section under Setup.
Enter the VMware Identity Manager Connection Details

1. Enter your Tenant URL in the Tenant URL field. 
   **NOTE** - Details on retrieving your Tenant URL were listed in the Login to the VMware Identity Manager Console section, please return to that step if you do not remember your Tenant URL. 
   **NOTE** - Please ensure that there is no trailing slash at the end of your Tenant URL to avoid any connection issues.

2. Enter Administrator for the Username.

3. Enter VMware1! for the Password.

4. Click Test Connection and ensure the Test connection successful! prompt displays.

5. Click Continue.
Configure and Save the VMware Identity Manager Settings

1. Select Yes for Do you want to use AirWatch to authenticate users?
2. Click Save.
   
   **NOTE** - The Save process may take several seconds to complete, please be patient. The Finish button will become clickable once the process finishes.
3. Click Finish.

Add A New User Group

Next, you will create a User Group from our AD users for use within our VMware Identity Manager tenant.

1. Click Accounts.
2. Expand User Groups.
3. Click List View.
4. Mouse over Add.
5. Click **Add User Group**.

**Enter the Users Group Details**

1. Select Type as **Directory**
2. Select **Organizational Unit** for the **External Type**
3. Enter **Users** for the **Search Text**
4. Click **Search**
5. Select the **Users** option under **Group Name**.

**NOTE - Do NOT click Save yet! Additional configurations will be made in the next step for this group.**
Modify the User Group Settings

1. Scroll down to the bottom.
2. Select **Custom** for User Group Settings.
3. Select **Enabled** for Auto Merge Changes.
4. Enter **100** for Maximum Allowable Changes.
5. Select **Enabled** for Add Group Members Automatically.
6. Click **Save**.
Sync AD Users

1. Click the **Check box** next to the **Users** user group to select it.
2. Click on the **Sync** button. This will add all the users in our Users group from Active Directory to Workspace ONE UEM.

**Acknowledge Sync**

Click **OK** from the popup to proceed the sync.
Confirm Sync

1. To view the number of Users synced to the Users user group, you may need to scroll your screen to the right.
   
   NOTE - It may take 20-30 seconds to complete the user sync. Please use the refresh button to check the status.

2. Confirm that you see 27 Users synced for the group.
Confirm User Sync in VMware Identity Manager

1. Click **Identity & Access Management**.
2. Click **Directories**.
3. Locate the Directory that was synced from Workspace ONE UEM. The Workspace ONE Getting Started Wizard will generate a unique name, which will be **Company_Directory_{GroupID}**. Ensure that you have 1 synced domain and 5 **synced users**.

Return to your VMware Identity Manager to confirm that the corp.local domain and users successfully synced.
Force a Sync (IF NEEDED)

If the domain and users have not synced to your directory in VMware Identity Manager, you can force a sync to occur from the Workspace ONE UEM Console.

Navigate back to the Workspace ONE UEM Console, and go to Groups & Settings > All Settings.

1. Click **System**
2. Click **Enterprise Integration**
3. Click **VMware Identity Manager**
4. Click **Configuration**
5. Scroll down to the bottom of the VMware Identity Manager settings page
6. Click **Sync Now**
Review Your Configuration in VMware Identity Manager

In one of the previous sections, we configured Workspace ONE Getting Started Wizard from the console. The Getting Started Wizard generates an AirWatch API admin key and an AirWatch API Enrollment User Key. These API keys are used by Identity Manager to communicate with Workspace ONE UEM and populate the related configurations within Identity Manager console.

Let's review our configuration in VMware Identity Manager to see where these changes are made.

Navigate to the VMware Identity Manager Tab

Click to navigate to VMware Identity Manager Admin Console in Google Chrome.

Validate the Configuration for AirWatch
In your VMware Identity Manager Tenant,

1. Click on **Identity & Access Management**
2. Click on **Setup**
3. Click **AirWatch** to view the related configurations
4. Validate that you are seeing **AirWatch API URL** as https://as1193.awmdm.com
5. Validate that you are seeing an **API Key** populated
6. Validate that you have **AirWatch Enrolled User API Key** is also populated

**NOTE - API key and AirWatch Enrolled User API Key will be different for each lab session.**

### Confirm Group ID and Save

1. Scroll down if needed.
2. Ensure that you are seeing your Group ID getting populated. 
   
   *(NOTE - You can find your Group ID by hovering over your organization group name in the Workspace ONE UEM Console)*
3. Click **Save**

### Enable App Catalog (IF NEEDED)

1. Scroll down if needed until you see a section for **Workspace ONE Catalog**.
2. Ensures the boxes for the options **Fetch from IDM** and **Fetch from AirWatch** are checked. If they are not checked, click each box to select them.

3. Click **Save**.

**Validate Compliance Check and Password Authentication**

1. Scroll down if needed.
2. Validate that **Compliance Check** is **Enabled**
3. Click **Save**
4. Validate that **User Password Authentication through AirWatch** is **Enabled**
5. Click **Save**

**Return to the Workspace ONE UEM Console**

For the next steps, we will return to the Workspace ONE UEM Console and complete the Workspace ONE Getting Started wizard.

Click the Workspace ONE UEM tab, which should be the first tab, on your browser to return to the Workspace ONE UEM Console Login page.

*NOTE - Your Workspace ONE UEM tab may not be at the Login page as shown in the picture depending on your previous steps.*
Integrate Workspace ONE UEM and VMware Identity Manager using the Cloud Kerberos Key Distribution Center (KDC)

This section will review how to integrate the Cloud Kerberos Key Distribution Center (KDC) between Workspace ONE UEM and VMware Identity Manager. Continue to review the necessary steps.
The first steps for configuring the Cloud Kerberos Key Distribution Center (KDC) is to setup the VMware Identity Manager Certificate in Workspace ONE UEM.

1. Click **Groups & Settings**.
2. Click **All Settings**.
Enable the Certificate

1. Click **System**
2. Click **Enterprise Integration**
3. Click **VMware Identity Manager**
4. Click **Configuration**
5. Scroll down to the **Certificate** section
6. Click **Enable**
Export the Certificate

1. Scroll back down to the Certificate section again.
2. Click the Export button.

The Certificate (VidmAirWatchRootCertificate.cer) will be saved in the Downloads folder. You will need this certificate in an upcoming step.

Enable and Setup Cloud Kerberos Key Distribution Center (KDC)

With the Certificate exported from Workspace ONE UEM, return to your VMware Identity Manager tenant to continue the Cloud Kerberos Key Distribution Center (KDC) configuration.

Switch to VMware Identity Manger Console
Click on the **VMware Workspace ONE** tab to return to the **VMware Identity Manager Administration Console**.

**Navigate to the Built-in Kerberos Configuration Page**

1. Click **Identity & Access Management**.
2. Click **Authentication Methods**.
3. Click on the Edit icon for **Mobile SSO (for iOS)**.
Configure Mobile SSO (for iOS)

1. Enable the **Enable KDC Authentication** check box.
2. Click the **Select File** button for the **Root and Intermediate CA Certificates**.

Upload the Root Certificate

1. Select the **YidmAirWatchRootCertificate.cer** file in the Downloads folder.
2. Click **Open** to upload the file.
1. Select the **Downloads** folder.
2. Select the **VidmAirWatchRootCertificate.cer** file that was downloaded previously.
3. Click **Open**.

### Confirm the Authentication Adapter Update

![Confirmation dialog box](image)

Click **OK** in the confirmation dialog box.

### Save the Kerberos Auth Settings

1. Confirm the **Certificate** was uploaded.
2. Click **Save**.
Navigate to the Identity Providers page

1. Click **Identity Providers**
2. Click **Built-in**

Download the KDC Server Root Certificate

1. Scroll down to the bottom of the page to find the **KDC Certificate Export** section.
2. Click the **Download Certificate** link.
The Certificate (KDC-root-cert.cer) will be saved in the Downloads folder. You will need this certificate in an upcoming step.

**Update the Access Policy**

1. Click Policies.
2. Click Edit Default Policy.

With the Identity Provider (IdP) configured, we now need to update the Policies to use our Identity Provider (IdP).

1. Click Policies.
2. Click Edit Default Policy.

**Create a new Policy Rule**

1. Click Configuration.
2. Click Add Policy Rule.
Configure the new Policy Rule

1. Select **ALL RANGES** for the *If a user's network range is* dropdown.
2. Select **iOS** for the *and user accessing content from* dropdown.
3. Select **Authenticate using...** for the *Then perform this action* dropdown.
4. Select **Mobile SSO (for iOS)** for the *then the user may authenticate using* dropdown.
5. Select **Password (Local Directory)** for the *If the preceding method fails or is not applicable, then* dropdown.

Save the New Policy Rule

1. You may need to scroll down to find the Save button.
2. Click **Save**.
Update the Policy Rules Order

1. Click and drag the **Mobile SSO (for iOS) handle** to the top of the list. This causes our **Mobile SSO (for iOS) Policy** to be processed first.
2. Click **Next**.
Save the Policy Rule Updates

1. You may need to scroll down to find the Save button.
2. Click **Save**.

Create Workspace ONE UEM Profiles for Single Sign-On

With our Access Policies and Identity Providers (IdP) configured, we now need to create a profile to enable our iOS device to Single Sign-on into our VMware Identity Manager tenant.

Click on the **Workspace ONE UEM** tab to return to the **Workspace ONE UEM Console**.

Close the Settings Page

If necessary, close the **Settings** page that was left open on a previous step by clicking on the X.
Create a Credentials Profile

1. Click Devices
2. Click Profiles & Resources
3. Click Profiles
4. Hover the mouse over Add
5. Click Add Profile

Select Apple iOS platform

Click Apple iOS.
1. Click **General**.
2. Enter **iOS Identity KDC Cert** in the **Name** field.
3. Click in the **Assigned Groups** field and a list of groups will appear.
4. Click **All Devices (your@email.shown.here)**.
Configure the Credentials Payload

1. Click the **Credentials** payload.
2. Click **Configure**.

Upload the KDC Root Certificate
1. Ensure **Upload** is selected for the **Credential Source** field.
2. Click **Upload**.

**Browse for the KDC Root Certificate to Upload**

Click **Choose File** in the Add popup.
Select the KDC Root Certificate to Upload

1. Click the Downloads folder.
2. Select the KDC-root-cert.cer file by clicking on it.
3. Click Open.
Save the KDC Root Certificate

Click Save.
Configure the SCEP Payload

1. Scroll down to find the <-> SCEP payload.
2. Click <-> SCEP.
3. Click Configure.
Confirm SCEP Settings

1. Select **Workspace ONE UEM Certificate Authority** for the **Credential Source** dropdown.
2. Select **Workspace ONE UEM Certificate Authority** for the **Certificate Authority** dropdown.
3. Select **Single Sign On** for the **Certificate Template** dropdown.
Create the Single Sign-On Payload

1. Scroll down to view the **Single Sign-On** payload.
2. Click **Single Sign-On**.
3. Click **Configure**.
Configure the Single Sign-On Connection Info

1. Enter a friendly name like `testsso` in the **Account Name** field.
2. Enter the `{EnrollmentUser}` lookup value in the **Kerberos Principal Name** field.
3. Enter `VIDMPREVIEW.COM` in the **Realm** field.
   
   **NOTE** - The value for Realm is case sensitive and it needs to be all upper case.
4. Select `SCEP #1` from the **Renewal Certificate** dropdown.
Configure the Single Sign-On URL Prefixes and Applications

1. Scroll down until you see the **URL Prefixes** and **Applications** sections.
2. Enter your VMware Identity Manager URL (https://{tenantName}.vidmpreview.com) in the **URLs** field.  
   **NOTE** - This is the VMware Identity Manager URL you’ve logged into during previous lab steps.
3. Enter com.apple.mobilesafari for the **Application Bundle ID** field.
4. Click **Save & Publish**.
Click **Publish**.
iOS Device Enrollment With Directory Account

In this section, we are going to enroll an iOS device. The upcoming steps will need to be completed from an iOS device.

Download and Install Workspace ONE Intelligent Hub from App Store (IF NEEDED)

NOTE - Checked out devices will likely have the Workspace ONE Intelligent Hub already installed. You may skip this step if your device has the Workspace ONE Intelligent Hub installed.
At this point, if you are using your own iOS device or if the device you are using does NOT have the Workspace ONE Intelligent Hub Application installed, then install the application from the App Store.

To Install the Workspace ONE Intelligent Hub application from the App Store, open the App Store application and download the free Workspace ONE Intelligent Hub application.

Launching the Workspace ONE Intelligent Hub

Launch the Hub app on the device.

*NOTE - If you have your own iOS device and would like to test you will need to download the Workspace ONE Intelligent Hub app first.*
Enter the Server URL

1. Enter \texttt{labs.awmdm.com} for the Server URL.
2. Click \texttt{Next}.

Click on the \texttt{Server Details} button.

Find Your Group ID From the Workspace ONE UEM Console

Return to the Workspace ONE UEM Console,
1. To find the Group ID, hover your mouse over the Organization Group tab at the top of the screen. Look for the email address you used to log in to the lab portal.  
2. Your **Group ID** is displayed at the bottom of the Organization Group pop up.

**NOTE** - The Group ID is required when enrolling your device in the following steps.

**Attach the Workspace ONE Intelligent Hub to the HOL Sandbox**

1. Enter your **Group ID** for your Organization Group for the **Group ID** field. Your Group ID was noted previously in the **Finding your Group ID** step.  
2. Tap the **Next** button.

**NOTE** - If on an iPhone, you may have to close the keyboard by clicking **Done** in order to click the **Next** button.

Return to the Workspace ONE Intelligent Hub application on your iOS Device,

1. Enter your **Group ID** for your Organization Group for the **Group ID** field. Your Group ID was noted previously in the **Finding your Group ID** step.  
2. Tap the **Next** button.
Enter User Credentials

You will now provide user credentials to authenticate to Workspace ONE UEM.

1. Enter **aduser** in the **Username** field.
2. Enter **VMware1!** in the **Password** field.
3. Tap the **Next** button.
Redirect to Safari and Enable MDM Enrollment in Settings

Workspace Services

This is required before the app can be installed. You automatically receive:

- Direct installation of all corporate resources.
- Secured corporate network access.
- Synchronized apps and content on all of your devices.
- An enhanced app experience that will make you more productive.

The Workspace ONE Intelligent Hub will prompt you to enable Workspace Services to enroll your device into Workspace ONE UEM.

Tap Next to begin.
Allow Website to Open Settings (IF NEEEDED)

If you prompted to allow the website to open Settings to show you a configuration profile, tap **Allow**.

**NOTE - If you do not see this prompt, ignore this and continue to the next step. This prompt will only occur for iOS Devices on iOS 10.3.3 or later**
Install the Workspace ONE MDM Profile

Tap **Install** in the upper right corner of the Install Profile dialog box.
Enter Device Passcode (IF NEEDED)

If prompted, enter your device passcode to continue.
If you do NOT receive this prompt, continue to the next step.

Install and Verify the Workspace ONE MDM Profile

Tap **Install** when prompted at the Install Profile dialog.
iOS MDM Profile Warning

You should now see the iOS Profile Installation warning explaining what this profile installation will allow on the iOS device.

Tap **Install** in the upper-right corner of the screen.
Trust the Remote Management Profile.

You should now see the iOS request to trust the source of the MDM profile.

Tap **Trust** when prompted at the Remote Management dialog.
iOS Profile Installation Complete

You should now see that the iOS Profile was successfully installed.

Tap **Done** in the upper right corner of the prompt.
Workspace ONE UEM Enrollment Success

Congratulations!
You have completed the initial configuration for your device. You will receive a notification prompt if further action is required.
You may navigate away from this page.

Open this page in “Hub”?

Cancel! Open

Your enrollment is now completed! Tap **Open** to navigate to the Workspace ONE Intelligent Hub.
Accept the Workspace ONE Intelligent Hub Notice

Your IT department will provide you access to a wide variety of company resources and apps and notify you if further action is required.

Tap **Done** to confirm the notice and continue.

**Accept Notifications for Hub (IF NEEDED)**

“Hub” Would Like to Send You Notifications

Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.

Tap **Allow** if you get a prompt to allow notifications for the Hub app.
Accept the App Installation (IF NEEDED)

You may be prompted to install a series of applications depending on which Module you are taking. If prompted, tap **Install** to accept the application installation.
Confirm the Privacy Policy
Privacy

Your privacy matters.

VMware Workspace ONE collects information to provide secure access to your work data and applications. Below you will find an overview of data collected by Workspace ONE and Hub to provide optimal performance, security and support. For information about how your company handles information collected by Workspace ONE, please contact your company.

Contact your company's IT administrator if you want to find out how to un-enroll your device and discontinue access to this app.

Data collected by Hub
Tap here for an overview of the data that this app may collect about device hardware, diagnostics and user information to function properly, and to secure company data stored on this device. Your company has access to this data and some data collected may be visible to your IT administrator.

Hub permissions
Tap here for an overview for the device permissions that this app will require to function properly. These permissions can be changed at any time within your device settings but may impact app functionality.

Your company's privacy policy
Contact your IT administrator for information about how your company handles information collected by this app.

I understand
Tap **I Understand** when shown the Privacy policy.

**Accept the Data Sharing Policy**

Data sharing

Want an even better app experience?

Help us improve and develop new app features and functionality that will make you even more productive.

We would like to collect information about your usage of our app to better understand how users interact with our apps and how we can improve the app experience. We analyze this usage data in the aggregate and not in any way that identifies you. If you change your mind, you can change this setting at any time.

For information about how VMware handles your usage data if you elect to share this data with VMware, visit [https://www.vmware.com/help/privacy.html](https://www.vmware.com/help/privacy.html)

I agree

Not now

Tap **I Agree** for the Data Sharing policy.
Confirm the Device Enrollment in the Hub App

Account

aduser
Directory Account
Updated Today at 8:56 AM

This Device

Support

About

Confirm that the Hub app shows the user account that you enrolled with.

You have now successfully enrolled your iOS device with Workspace ONE UEM! Continue to the next step.
SSO Validation

In this section, we will validate that the SSO configuration is working on our iOS device.

Open Settings

Tap Settings on the iOS device.
Navigate to General Settings, Digital Workspace
1. Tap **General**.
2. Scroll down to find the **Device Management** option.
3. Tap **Device Management**.

**Open the Digital Workspace profile**

![Device Manager profile]

Tap the **Device Manager** profile.

**View More Details**

![More Details]

Tap **More Details**.
Open the Single Sign On Account

You should see the Single Sign On Account that you added in the Profile created in the previous section.

Tap testssso.
Verify Settings

Verify the following Single Sign-On settings are correct:

1. Principal Name is set to aduser.
2. Realm is set to VIDMPREVIEW.COM.
3. URL Prefix Matches is set to https://{tenantName}.vidmpreview.com/.
   This URL will be your VMware Identity Manager Tenant URL.
4. Eligible App IDs includes com.apple.mobilesafari.

**NOTE** - If any of these settings are incorrect, return to the AirWatch Console and inspect your iOS Identity KDC Cert Profile that was previously created.
Clear the Safari Cache

Navigate back to the main Settings page.

1. Scroll down to find the Safari settings.
2. Tap Safari.
3. Scroll down to find Clear History and Website Data.
4. Tap Clear History and Website Data.
Confirm the Clear History and Data Prompt

Click **Clear**.

Launch Safari on the iOS Device

Tap the **Safari** icon, it should be on the bottom tray.
1. Enter the URL of your Identity Manager tenant in the URL bar.
2. Click Go
Notice that Identity Manager is signing you in without requiring any authentication.
Identity Manager Application Catalog

You are now signed into Workspace ONE using Single Sign On automatically without having to enter any credentials!

There are no applications visible because they haven't been added in VMware Identity Manager or Workspace ONE UEM.

It doesn't look like you've been assigned any apps yet. They should be coming shortly, so check back soon.
Un-enrolling Your Device

You are now going to un-enroll the iOS device from Workspace ONE UEM.

NOTE - The term "Enterprise Wipe" does not mean reset or completely wipe your device. This only removes the MDM Profiles, Policies, and content which the AirWatch MDM Agent controls.

It will NOT remove the AirWatch Agent application from the device as this was downloaded manually before Workspace ONE UEM had control of the device.

Enterprise Wipe (un-enroll) your iOS device

Enterprise Wipe will remove all the settings and content that were pushed to the device when it was enrolled. It will not affect anything that was on the device prior to enrollment.

To Enterprise Wipe your device you will first bring up the Workspace ONE UEM Console in a web browser. You may need to re-authenticate with your credentials (VLP registered email address and VMware1 as the password).

1. Click Devices on the left column.
2. Click List View.
3. Click the checkbox next to the device you want to Enterprise Wipe.
NOTE - Your Device Friendly Name will very likely be different than what is shown. It will, however, be in the same location as shown on image in this step.

Find the Enterprise Wipe Option

1. Click More Actions. NOTE - If you do not see this option, ensure you have a device selected by clicking the checkbox next to the device.
2. Click Enterprise Wipe under Management.
Enter your security PIN

After selecting Enterprise Wipe, you will be prompted to enter your Security PIN which you set after your logged into the console (1234).

1. Scroll down until you see the option for entering Security PIN
2. Enter 1234 for the Security PIN. You will not need to press enter or continue, the console will confirm your PIN showing "Successful" below the Security PIN input field to indicate that an Enterprise Wipe has been requested.

**NOTE** - If 1234 does not work, then you provided a different Security PIN when you first logged into the Workspace ONE UEM Console. Use the value you specified for your Security PIN.

**NOTE - If the Enterprise Wipe does not immediately occur, follow the below steps to force a device sync:**

1. On your device, open the AirWatch Agent application.
2. Tap the Device section (under Status) in the middle of the screen.
3. Tap **Send Data** near the top of the screen. If this does not make the device check in and immediately un-enroll, continue to Step #4.

4. If the above doesn't make it immediately un-enroll, then tap **Connectivity [Status]** under Diagnostics.

5. Tap **Test Connectivity** at the top of the screen.

*NOTE - Depending upon Internet connectivity of the device and responsiveness of the lab infrastructure, this could take a couple of minutes or more if there is excessive traffic occurring within the Hands On Lab environment.*

Feel free to continue to the "**Force the Wipe**" step to manually uninstall the Workspace ONE UEM services from the device if network connectivity is failing.

**Verify the Un-Enrollment**
Press the Home button on the device to go back to the home screen. The applications pushed through Workspace ONE UEM should have been removed from the device.

**NOTE - The applications and settings pushed through Workspace ONE UEM should have been removed. The Agent will still be on the device because that was downloaded manually from the App Store. Due to lab environment settings, it may take some time for the signal to traverse through the various networks out and back to your device. Continue on to the next step to force the wipe if the needed.**
Force the Wipe - IF NECESSARY
If your device did not wipe, follow these instructions to ensure the wipe is forced immediately. Start by opening the iOS Settings app.

1. Tap General in the left column.
2. Scroll down to view the Device Management option.
3. Tap Device Manager at the bottom of the list of General settings.

**Force the Wipe - IF NECESSARY**

![Device Manager Profile](image)

Tap the Device Manager profile that was pushed to the device.
Force the Wipe - IF NECESSARY

1. Tap Remove Management on the Device Manager profile. **NOTE - If prompted for a device PIN, enter it to continue. VMware provisioned devices should not have a device PIN enabled.**
2. Tap Remove on the Remove Management prompt.

After removing the Device Manager profile, the device will be un-enrolled. Feel free to return to the Verify the Un-Enrollment step to confirm the successful un-enrollment of the device.
Conclusion

Workspace ONE enables users to access their applications from any device at any time, providing a rich user experience while ensuring corporate resources and apps are accessed securely and by the appropriate users. Integrating VMware Identity Manager with Workspace ONE UEM allows administrators to control what authentication methods are available to users to access and download apps while providing Single Sign-On for secure and quick access.

This concludes this module.
Module 2 - Workspace
ONE UEM Configuration, AD Integration/Certificates
Introduction

Workspace ONE UEM can integrate with your Certificate Authority to provide certificates to your enrolled devices. This enables your users to utilize certificates for authentication and other purposes for increased security and providing a better user experience by eliminating the need to authenticate with credentials.

This lab module will explore how to integrate a Certificate Authority with Workspace ONE UEM, configure the templates, and distributing a certificate to a device by using a Profile.
VMware Enterprise Systems Connector Setup

The VMware Enterprise Systems Connector allows organizations to integrate AirWatch with back-end enterprise systems without exposing or compromising the security of these systems. The VMware Enterprise Systems Connector runs in the internal network and acts as a proxy that securely transmits requests from AirWatch to enterprise infrastructure components.

For the purposes of the lab, the VMware Enterprise Systems Connector is already setup and configured for you. The following steps will review the architecture and show a demo video of how to install the VMware Enterprise Systems Connector.

Architecture Overview

The simple architecture diagram above demonstrates the following concepts:

- The VMware Enterprise Systems Connector is installed on the internal network where it is able to access your Active Directory.
- The VMware Enterprise Systems Connector requires no inbound access from the internet, requiring no additional inbound ports to be exposed on your firewall.
- When deploying the VMware Enterprise Systems Connector with only the AirWatch Cloud Connector component installed, AirWatch can securely sync your Directory and users to your VMware Identity Manager tenant.

Continue to the next step when you are ready.
Video Demo of Installation

**NOTE:** The video contains no spoken instructions. Please refer to the subtitles for instructions about the installation process.

Please watch this short demonstration of how to install the VMware Enterprise Systems Connector before continuing to the next step.

**NOTE:** Do not attempt to make any of the configurations or changes shown in the demo video! This demonstration is only to highlight the configuration and installation process for your knowledge.
Login to the Workspace ONE UEM Console

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

Launch Chrome Browser

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

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

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

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

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

Terms of Use

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

VMWARE END USER LICENSE AGREEMENT

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

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

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

1. DEFINITIONS.

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

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

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

Security Settings

Password Recovery Question 1

Password Recovery Question *

What was your childhood nickname?  

Password Recovery Answer *

VMware1!  

Confirm Password Recovery Answer *

VMware1!  

Security PIN

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

Security PIN *

1234  

Confirm Security PIN *

1234  

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

Close the Welcome Message

Workspace ONE UEM Console Highlights

Powered by VMware AirWatch!

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

Workspace ONE UEM transforms your business so you can:

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

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

1. Click on the Don't show this message on login check box.
2. Close the pop-up by clicking on the X in the upper-right corner.
Directory Services Integration

In this chapter, you will setup Active Directory Services to work with Workspace ONE UEM. This will allow Workspace ONE UEM to import your Active Directory Users and Groups.

If you haven't yet opened the console, please do so now by following the instructions in Login to the Workspace ONE UEM Console.

Open All Settings

1. Click the Groups & Settings button on the left menu.
2. Click the All Settings button from the middle menu.
Selecting Directory Services

1. Click the **System** section to expand the section.
2. Click the **Enterprise Integration** dropdown section.
3. Click the **Directory Services** button.
4. Click the **Skip wizard and configure manually** link.
Configure the Server section of Directory Services as follows:

1. Confirm that the **Server** tab is selected.
2. Enter `controlcenter.corp.local` for the **Server**.
3. Confirm that the **Encryption Type** is set to **None**.
4. Enter `389` for the **Port**.
5. Enter `3` for the **Protocol Version**.
1. Set **Disabled** for **Use Service Account Credentials**.
2. Select **GSS-NEGOTIATE** for the **Bind Authentication Type**.
3. Enter **corp\administrator** for the **Bind Username** field.
4. Enter **VMware1!** for the **Bind Password** field.
5. Enter **corp.local** in the **Domain** field.
Configure the User section of Directory Services as follows:

1. Scroll back to the top of the menu where the **Server, User, and Group** tabs are.
2. Click the **User** tab.
3. Enter `dc=corp,dc=local` for the **Base DN** box.
Configure the Group section of Directory Services as follows:

1. Click the **Group** tab.
2. Enter `dc=corp,dc=local` for the **Base DN** field.

**Save Directory Services Configuration**
1. Scroll down to find the Save button if it is not visible on your screen.
2. Click **Test Connection**.
3. Ensure the **Connection successful with the given server name, bind user name, and password** success message is displayed.
4. Click **Save**.

**Confirm Directory Services Saved Successfully**

![Image of Directory Services Saved Successfully]

1. After the Saving loading wheel finishes, you should see the **Saved Successfully** confirmation appear.
2. Click the **Close (X)** button in the top-right corner.
Configuring an Enterprise Certificate Authority

This module will walk through the configuration of a newly installed Enterprise Certificate Authority for use with Workspace ONE UEM as well as how to integrate the Certificate Authority on your domain with Workspace ONE UEM SaaS services using the VMware Enterprise Systems Connector.

Configure the Certificate Authority

The first step in this process is to prepare your Certificate Authority, create a template for use with Workspace ONE UEM and assign security permissions to allow a service account to make requests to the CA. If you already have a PKI in your enterprise, Workspace ONE UEM can seamlessly connect with your current infrastructure.

For this lab, the Certificate Authority has already been configured for you. To better learn and understand the configurations made to integrate the Certificate Authority with Workspace ONE UEM, you can choose between watching a demo video on how to configure the Certificate Authority, or you can practice the steps hands-on using a local Certificate Authority.

- If you wish to watch a demo video, click here.
- If you wish to step through a hands-on example using a local Certificate Authority, click here.

Watch a Certificate Authority Configuration Demo
NOTE - You may need to scroll to the right to view the full screen button on the video above.  
NOTE - The video contains no sound. Please note the subtitles for details the installation process.

The embedded video will showcase the configurations to the Certificate Authority used for this lab to integrate with Workspace ONE UEM. After finishing the video, click here to continue.

Configure an Example Certificate Authority

In this section, you will utilize a local Certificate Authority provided to better learn how to configure the Certificate Authority to interact with Workspace ONE UEM.

NOTE - The Certificate Authority that this lab accesses to issue certificates has already been configured, you are only editing a local Certificate Authority that will not impact the ability to issue certificates for this lab.

Opening the Microsoft Certificate Authority Application

![Certification Authority](image)

On the Main Console server, double-click the Certification Authority shortcut on the desktop.

Getting the Certificate Authority Server Name

![Certificate Authority Server Name](image)

The first item that you will need when integrating Workspace ONE UEM to ADCS is the name of CA. The name of the instance is the top most attribute on the configuration screen, in this case it is **CONTROLCENTER-CA** as we have already pre-configured it to be a Certificate Authority.
Navigate to Properties of CA

1. Right click on **CONTROLCENTER-CA**.
2. Click on **Properties**.

Configure Security

1. Click **Security**
2. Click **Add**
Add the Imaservice account

1. Type `imaservice` in the **Enter the object names to select** embedded window.
2. Click the **Check Names** button to validate.
3. If no errors appear, click the **OK** button to add the **IMASERVICE** user account.
Set the IMASERVICE Account Permissions

After completing the previous step to add the IMASERVICE user to the CONTROLCENTER-CA Properties permissions, you need to modify the permissions to allow the user to issue, manage, and request certificates.

1. Click on the **ima service (imaservice@corp.local)** user in the **Group or user names** embedded window.
2. In the **Permissions for Authenticated Users** check box, ensure the **Request Certificates** box is checked.
3. Check the **Issue and Manage Certificates** box.
4. Click the **OK** button.
Manage Certificate Templates

Now you will create a new certificate template for use with Workspace ONE UEM. In order to do so, you need to open the Manage Certificate Templates menu.

1. In the left pane, click on **CONTROLCENTER-CA** to select it.
2. Right-click on the **Certificate Templates** folder to bring up the context menu.
3. Select **Manage**. This will open a new MMC Snap-in window titled **Certificate Templates Console**.

Duplicate the Certificate Template

The Certificate Templates Console window displays.

1. In **Template Display Name** column, scroll down and select the **User** template.
2. Right-click on the **User** template.
3. From the context menu, select **Duplicate Template**.

**NOTE** - *This duplicate certificate template will be used by Workspace ONE UEM. The template you choose depends on the function being configured in Workspace ONE UEM. For example, for Wi-Fi, VPN, or Exchange Active Sync (EAS) client authentication you would select the CEP Encryption template instead.*

**Define New Certificate Template Settings**

![Properties of New Template dialog box](image)

The **Duplicate Template** dialog box displays.

1. Click on the **General** tab.
2. In the **Template display name** field, type the name of the template that will display to users. For this lab, type **Mobile User**.

---

HOL-1957-01-UEM
3. The **Template name** field auto-fills with the same name as above, only without spaces. For this lab, leave it as **MobileUser**.
4. Un-check the **Publish certificate in Active Directory** checkbox.
5. Click **OK**.

### Open the Mobile User Template Properties

1. Right click on the new template **Mobile User** which was just created
2. Select **Properties** from the context menu. The **Mobile Users Properties** window will appear.

### Edit the Security of Mobile User Template

1. Click on the **Security** tab
2. Add **Authenticated Users**, **Administrator**, **Domain Admins** (CORP\Domain Admins), **Domain Users** (CORP\Domain Users), and **Enterprise Admins** (CORP\Enterprise Admins).
1. Select the **Security** tab in the **Mobile User Properties** window.
2. Click the **Add...** button below the embedded **Group or user names** window. The "Select Users, Computers, Service Accounts, or Groups" dialog box displays.

### Add the account Imaservice

![Screen capture of the Select Users, Computers, Service Accounts, or Groups dialog box]

1. Type the previously created user service account **IMASERVICE** in the **Enter the object names to select** embedded window.
2. Click the **Check Names** button to verify the account was typed correctly. If typed correctly, you will see it change to **ima service (imaservice@corp.local)**.
3. Click the **OK** button on the **Select Users, Computers, Service Accounts, or Groups** dialog box.
Apply Read and Enroll permissions

1. Back on the Mobile User Properties window, select the ima service (imaservice@corp.local) user account.
2. In the Permissions for ima service embedded window, ensure the Allow checkbox for Read permissions is selected.
3. In the Permissions for ima service embedded window, click the Allow checkbox for Enroll permissions to enable it.
4. Click the Apply button. DO NOT click OK yet.
Configure Subject Name Properties

1. Select the **Subject Name** tab in the Mobile User Properties window.
2. Select the **Supply in the request** radio button.
3. Click the **OK** button on the **Certificates Templates** prompt.
4. Click the **OK** button on the **Mobile User Properties** window.
Close the Certificate Template Console

Close the Certificate Template Console by clicking on \( \times \) sign.

Add new certificate template to issue

Switch back to the **CERTSRV - Certificate Authority window** shown in this step.

In the left window pane, single click to select the **Certificate Template** folder.

1. Click on the twisty to expand options for CA.
2. Right click the **Certificate Template** folder
3. Select **New** in the context menu which appears.
4. Click on **Certificate Template to Issue** which appears to the right of **New**.

## Enabling the Mobile User Certificate Template

1. In the **Enable Certificates Templates** dialog box, select the name of the certificate template - in this case, **Mobile User** - which you previously created.
2. Click the **OK** button.
Accept the Updating Template Prompt (IF NEEDED)

If you see a prompt for Updating Templates, click Yes to continue.
Login to the Workspace ONE UEM Console (IF NEEDED)

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

Launch Chrome Browser

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

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

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

1. Enter your **Username**. This is your **email address** that you have associated with your **VMware Learning Platform (VLP) account**.
2. Enter **VMware1!** for the **Password** field.
3. Click the **Login** button.
NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the Workspace ONE UEM Hands On Labs server.
Add the Certificate Authority in Workspace ONE UEM

Now that the configuration of the Certificate Authority itself is done, you will now be configuring the Certificate Authority within Workspace ONE UEM.

In order for Workspace ONE UEM to retrieve a certificate from a Certificate Authority (CA), you must configure the Workspace ONE UEM console to use the communicate with the CA. There are two steps to this process:

- Add the Certificate Authority
- Add the Certificate Template

Return to the Workspace ONE UEM Console in your browser tab.
Add the Certificate Authority in Workspace ONE UEM

1. Click **Groups & Setting**.
2. Click **All Settings**.
Navigating to the CA Settings

1. Click **System**.
2. Expand **Enterprise Integration**.
3. Click **Certificate Authorities**.
4. Ensure the **Certificate Authorities** tab is selected.
5. Click the + **Add** button.

Define the CA Settings in Workspace ONE UEM

1. Enter **CONTROLCENTER-CA** for the **Name**.
2. Enter **Control Center Certificate Authority** for the **Description**.
3. Select **Microsoft ADCS** for the **Authority Type**.
4. Select **ADCS** for the **Protocol**.
5. Enter **controlcenter.corp.local** for the **Server Hostname**.
6. Enter **CONTROLCENTER-CA** for the **Authority Name**.
NOTE - Do NOT click Save yet! There are additional CA settings that need to be configured in the next step.

Define the CA Authentication Settings

1. Scroll down to find additional configuration options.
2. Select Service Account for the Authentication.
3. Enter imaservice for the Username.
4. Enter VMware1! for the Password.
5. Enter VMware1! for the Confirm Password.
6. Select None for Additional Options.
7. Click Test Connection and ensure the "Test is Successful!" prompt displays at the top of the menu.
8. Click Save and Add Template.
Setup the Certificate Template

1. Enter your VLP email address for the Name.
2. Enter Mobile User for the Description.
3. Select CONTROLCENTER-CA for the Certificate Authority. This is the Certificate Authority you created in the previous steps.
4. Enter MobileUser for the Issuing Template.
   **NOTE - Enter MobileUser as one word without spaces!**
5. Enter CN={EnrollmentUser} for the Subject Name.
6. Select 2048 for the Private Key Length.

**NOTE - Do NOT click Save yet! The next step includes additional settings.**
Complete and Save the Certificate Template

1. Enable **Signing** for the **Private Key Type**.
2. Enable **Encryption** for the **Private Key Type**.
3. Enable **Automatic Certificate Renewal**.
4. Enter **5** for **Auto Renewal Period (days)**.
5. Enable the **Enable Certificate Revocation** option.
6. Click **Save**.
Close the Certificate Authorities Settings Page

1. Click the Refresh button.
2. Ensure the CONTROLCENTER-CA Certificate Authority you created is displayed.
3. Click Close.

Conclusion and Wrap Up

This concludes the configuration of Microsoft Active Directory, Microsoft Certificate Authority, and Workspace ONE UEM with the VMware Enterprise Systems Connector.

Proceed to the next chapter to define an Workspace ONE UEM profile and configure your device for use with this enterprise certificate.
Create an iOS Profile with a Credential Payload

We will now walk through the creation of an iOS Profile for a Credential Payload which will deliver a unique enterprise certificate to the device. Please be sure you are logged into the AirWatch web console before continuing.

Navigate to the Devices Profile List View

1. Click **Devices**.
2. Expand **Profiles & Resources**.
3. Click on the **Profiles** option under Profiles & Resources.
4. Click on the **Add** dropdown.
5. Click **Add Profile**.

![Image showing the navigation steps]
Add an iOS Profile

You will now be presented with the Add Profile screen. Here you would select the operating system type of your device.

For this lab, select Apple iOS.
Configure the iOS Restriction Profile

After clicking on the iOS icon, you will be presented with the **Add a New Apple iOS Profile**. All profiles are broken down into two basic sections, the **General** section and the **Payload** section.

The **General** section has information about the Profile, its name and granular filters to determine which devices will receive the configurations in the profile.

The **Payload** sections define actions to be taken on the device.

Every Profile must have all *required* fields in the General section properly filled out and at least one payload configured.
**NOTE - In most cases, it is recommended a Profile contain only one Payload.**

## Define the General Settings for the Profile

Configure the profile as follows:

1. Click **General**.
2. Enter **iOS Certificate** for the **Name**.
3. Click in the **Assigned Smart Groups** field to view a list of available groups.
4. Click **All Devices (your@email.shown.here)** from the list.

**NOTE - You do not need to click SAVE or SAVE AND PUBLISH at this point. This interface allows you to move around to different payload configuration screens before saving.**

Continue to the next step in the lab manual to continue configuring this profile.
Select the Credentials Payload

NOTE - When initially setting a payload, a Configure button will show to reduce the risk of accidentally setting a payload configuration.

1. Click on the **Credentials** payload.
2. Click the **Configure** button to continue setting the Restrictions payload.
Configure the Credentials Payload

1. Select **Defined Certificate Authority** for the Credential Source.
2. Select **CONTROLCENTER-CA** for the Certificate Authority.
3. Select the Certificate Template named after your VLP email address.
4. Click **Save & Publish**.
After clicking on Save & Publish you will be presented with the Device Assignment screen. Click Publish.

Typically, you would see the devices that your profile would be assigned to here. This allows you to verify the filters you applied on the general tab are applied correctly before pushing the profile to devices. If you haven't enrolled a device, you won't see any devices here.
Verify the Certificate Profile Now Exists

1. You should now see your Credentials Profile, named **iOS Certificate**, within the List View of the Devices Profiles window.
2. If you do not see the Credentials Profile, click the **Refresh** button.

**NOTE - If you want to make changes to the profile, this is where you would do so. To edit a profile, click on the profile name and select Add Version, make your changes and then select Save & Publish.**
iOS Device Enrollment With Directory Account

In this section, we are going to enroll an iOS device. The upcoming steps will need to be completed from an iOS device.

Download and Install Workspace ONE Intelligent Hub from App Store (IF NEEDED)

NOTE - Checked out devices will likely have the Workspace ONE Intelligent Hub already installed. You may skip this step if your device has the Workspace ONE Intelligent Hub installed.
At this point, if you are using your own iOS device or if the device you are using does NOT have the Workspace ONE Intelligent Hub Application installed, then install the application from the App Store.

To Install the Workspace ONE Intelligent Hub application from the App Store, open the App Store application and download the free **Workspace ONE Intelligent Hub** application.

**Launching the Workspace ONE Intelligent Hub**

Launch the **Hub** app on the device.

**NOTE - If you have your own iOS device and would like to test you will need to download the Workspace ONE Intelligent Hub app first.**
Enter the Server URL

1. Enter **labs.awmdm.com** for the Server URL.
2. Click **Next**.

Click on the **Server Details** button.

Find Your Group ID From the Workspace ONE UEM Console

Return to the Workspace ONE UEM Console,
1. To find the Group ID, hover your mouse over the Organization Group tab at the top of the screen. Look for the email address you used to log in to the lab portal.
2. Your **Group ID** is displayed at the bottom of the Organization Group pop up.

**NOTE** - The Group ID is required when enrolling your device in the following steps.

**Attach the Workspace ONE Intelligent Hub to the HOL Sandbox**

1. Enter your **Group ID** for your Organization Group for the **Group ID** field. Your Group ID was noted previously in the Finding your Group ID step.
2. Tap the **Next** button.

**NOTE** - If on an iPhone, you may have to close the keyboard by clicking Done in order to click the Next button.
Enter User Credentials

1. Enter **aduser** in the **Username** field.
2. Enter **VMware1!** in the **Password** field.
3. Tap the **Next** button.

You will now provide user credentials to authenticate to Workspace ONE UEM.

1. Enter **aduser** in the **Username** field.
2. Enter **VMware1!** in the **Password** field.
3. Tap the **Next** button.
Redirect to Safari and Enable MDM Enrollment in Settings

Workspace Services

This is required before the app can be installed. You automatically receive:

- Direct installation of all corporate resources.
- Secured corporate network access.
- Synchronized apps and content on all of your devices.
- An enhanced app experience that will make you more productive.

Next

The Workspace ONE Intelligent Hub will prompt you to enable Workspace Services to enroll your device into Workspace ONE UEM.

Tap Next to begin.
Allow Website to Open Settings (IF NEEDED)

If you prompted to allow the website to open Settings to show you a configuration profile, tap **Allow**.

**NOTE - If you do not see this prompt, ignore this and continue to the next step. This prompt will only occur for iOS Devices on iOS 10.3.3 or later**
Install the Workspace ONE MDM Profile

Tap **Install** in the upper right corner of the Install Profile dialog box.
Enter Device Passcode (IF NEEDED)

Enter Passcode  

If prompted, enter your device passcode to continue.

If you do NOT receive this prompt, continue to the next step.

Install and Verify the Workspace ONE MDM Profile

Tap **Install** when prompted at the Install Profile dialog.
iOS MDM Profile Warning

MOBILE DEVICE MANAGEMENT

Installing this profile will allow the administrator at “https://ds1193.awmdm.com/DeviceServices/AppleMDM/Processor.aspx” to remotely manage your iPad.

The administrator may collect personal data, add/remove accounts and restrictions, install, manage, and list apps, and remotely erase data on your iPad.

You should now see the iOS Profile Installation warning explaining what this profile installation will allow on the iOS device.

Tap Install in the upper-right corner of the screen.
Trust the Remote Management Profile.

You should now see the iOS request to trust the source of the MDM profile.

Tap **Trust** when prompted at the Remote Management dialog.
You should now see that the iOS Profile was successfully installed.

Tap **Done** in the upper right corner of the prompt.
Workspace ONE UEM Enrollment Success

Congratulations!

You have completed the initial configuration for your device. You will receive a notification prompt if further action is required.

You may navigate away from this page.

Open this page in “Hub”? Cancel! Open

Your enrollment is now completed! Tap Open to navigate to the Workspace ONE Intelligent Hub.
Accept the Workspace ONE Intelligent Hub Notice

Your IT department will provide you access to a wide variety of company resources and apps and notify you if further action is required.

Tap **Done** to confirm the notice and continue.

**Accept Notifications for Hub (IF NEEDED)**

"Hub" Would Like to Send You Notifications

Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.

Tap **Allow** if you get a prompt to allow notifications for the Hub app.
Accept the App Installation (IF NEEDED)

You may be prompted to install a series of applications depending on which Module you are taking. If prompted, tap **Install** to accept the application installation.
Confirm the Privacy Policy
Privacy

Your privacy matters.

VMware Workspace ONE collects information to provide secure access to your work data and applications. Below you will find an overview of data collected by Workspace ONE and Hub to provide optimal performance, security and support. For information about how your company handles information collected by Workspace ONE, please contact your company.

Contact your company’s IT administrator if you want to find out how to un-enroll your device and discontinue access to this app.

Data collected by Hub

Tap here for an overview of the data that this app may collect about device hardware, diagnostics and user information to function properly, and to secure company data stored on this device. Your company has access to this data and some data collected may be visible to your IT administrator.

Hub permissions

Tap here for an overview for the device permissions that this app will require to function properly. These permissions can be changed at any time within your device settings but may impact app functionality.

Your company’s privacy policy

Contact your IT administrator for information about how your company handles information collected by this app.
Tap **I Understand** when shown the Privacy policy.

**Accept the Data Sharing Policy**

Tap **I Agree** for the Data Sharing policy.
Confirm the Device Enrollment in the Hub App

Confirm that the Hub app shows the user account that you enrolled with.

You have now successfully enrolled your iOS device with Workspace ONE UEM! Continue to the next step.
View the Certificate on the Device

You can now confirm the certificate was issued and installed on the device. When you enrolled your device, the profile containing a certificate from the CONTROLCENTER-CA will be pushed down to your device. The speed at which the profile is installed on the device is dependent on many variables outside of the control of Workspace ONE UEM. The profile with the certificate may arrive in few seconds or it may take a few minutes. We will go look in the settings for the certificate.

Navigate to Settings on the iOS device

On the iOS device, return to the launchpad by pressing the home button then select the Settings icon to open the menu.
Validate the Certificate is Pushed to the Device

1. Tap to select **General** settings in the left column.
2. Scroll to the bottom of the general menu and tap **Device Management** - **Device Manager** in the right side of the window. Here you will see details of the configuration information which has been pushed to the device.
Select Workspace Services

Select **Device Manager**

Select **More Details**

Select **More Details** to view additional configuration.
Select the MDM Profile

Look for the **Certificates** section in this menu. What is seen on your screen may differ from the image above depending on your lab configuration. You should see a certificate issued to your AD user named **aduser** that has been issued form the CONTROLCENTER-CA that we previously integrated into Workspace ONE UEM. This certificate can be used in conjunction with Email, Wi-Fi or VPN profiles. Certificates can also be used to authenticate to web resources or content repositories as well. You may select the certificate to view more details. When you are ready, continue to the next step.

Wrap Up

This concludes configuring Workspace ONE UEM to be used with an Enterprise Active Directory and Enterprise Certificate Authority for providing a single point of authentication and security using internal Enterprise security settings to ensure corporate data security is maintained even on end user personal devices. Please continue with the next steps to complete the module.
Un-enrolling Your Device

You are now going to un-enroll the iOS device from Workspace ONE UEM.

*NOTE - The term "Enterprise Wipe" does not mean reset or completely wipe your device. This only removes the MDM Profiles, Policies, and content which the AirWatch MDM Agent controls.*

It will NOT remove the AirWatch Agent application from the device as this was downloaded manually before Workspace ONE UEM had control of the device.

**Enterprise Wipe (un-enroll) your iOS device**

Enterprise Wipe will remove all the settings and content that were pushed to the device when it was enrolled. It will not affect anything that was on the device prior to enrollment.

To Enterprise Wipe your device you will first bring up the Workspace ONE UEM Console in a web browser. You may need to re-authenticate with your credentials (VLP registered email address and VMware1 as the password).

1. Click **Devices** on the left column.
2. Click **List View**.
3. Click the **checkbox** next to the device you want to Enterprise Wipe.
NOTE - Your Device Friendly Name will very likely be different than what is shown. It will, however, be in the same location as shown on image in this step.

Find the Enterprise Wipe Option

1. Click More Actions. NOTE - If you do not see this option, ensure you have a device selected by clicking the checkbox next to the device.
2. Click Enterprise Wipe under Management.
Enter your security PIN

After selecting Enterprise Wipe, you will be prompted to enter your Security PIN which you set after your logged into the console (1234).

1. Scroll down until you see the option for entering Security PIN
2. Enter 1234 for the Security PIN. You will not need to press enter or continue, the console will confirm your PIN showing "Successful" below the Security PIN input field to indicate that an Enterprise Wipe has been requested.

**NOTE** - If 1234 does not work, then you provided a different Security PIN when you first logged into the Workspace ONE UEM Console. Use the value you specified for your Security PIN.

**NOTE** - If the Enterprise Wipe does not immediately occur, follow the below steps to force a device sync:

1. On your device, open the AirWatch Agent application.
2. Tap the Device section (under Status) in the middle of the screen.
3. Tap **Send Data** near the top of the screen. If this does not make the device check in and immediately un-enroll, continue to Step #4.

4. If the above doesn't make it immediately un-enroll, then tap **Connectivity [Status]** under Diagnostics.

5. Tap **Test Connectivity** at the top of the screen.

**NOTE - Depending upon Internet connectivity of the device and responsiveness of the lab infrastructure, this could take a couple of minutes or more if there is excessive traffic occurring within the Hands On Lab environment.**

Feel free to continue to the "**Force the Wipe**" step to manually uninstall the Workspace ONE UEM services from the device if network connectivity is failing.

**Verify the Un-Enrollment**
Press the Home button on the device to go back to the home screen. The applications pushed through Workspace ONE UEM should have been removed from the device.

**NOTE - The applications and settings pushed through Workspace ONE UEM should have been removed. The Agent will still be on the device because that was downloaded manually from the App Store. Due to lab environment settings, it may take some time for the signal to traverse through the various networks out and back to your device. Continue on to the next step to force the wipe if the needed.**
Force the Wipe - IF NECESSARY
If your device did not wipe, follow these instructions to ensure the wipe is forced immediately. Start by opening the iOS *Settings* app.

1. Tap *General* in the left column.
2. Scroll down to view the *Device Management* option.
3. Tap *Device Manager* at the bottom of the list of General settings.

**Force the Wipe - IF NECESSARY**

![Device Management screen]

Tap the *Device Manager* profile that was pushed to the device.
Force the Wipe - IF NECESSARY

1. Tap **Remove Management** on the Device Manager profile.  
   *NOTE - If prompted for a device PIN, enter it to continue. VMware provisioned devices should not have a device PIN enabled.*  
2. Tap **Remove** on the Remove Management prompt.

After removing the Device Manager profile, the device will be un-enrolled. Feel free to return to the **Verify the Un-Enrollment** step to confirm the successful un-enrollment of the device.
Conclusion

This lab module reviewed how to integrate a Certificate Authority with Workspace ONE UEM to provision certificates to your enrolled devices. We were able to generate and deploy a certificate to our iOS device and confirm that the certificate was successfully downloaded.

This concludes this lab module.
Conclusion

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

Lab SKU: HOL-1957-01-UEM

Version: 20190109-165014