# Table of Contents

Lab Overview - HOL-1857-06-UEM - Workspace ONE UEM Configuration, AD Integration/Certificates................................................................................................................................. 2  
Lab Guidance ........................................................................................................................................................................ 3  
Module 1 - Advanced Workspace ONE UEM Configuration, AD Integration/Certificates (60 minutes)........................................................................................................................................ 9  
  Introduction........................................................................................................................................................................... 10  
  VMware Enterprise Systems Connector Setup .................................................................................................................. 11  
  Login to the AirWatch Console ........................................................................................................................................ 13  
  Directory Services Integration................................................................................................................................................ 17  
  Configuring an Enterprise Certificate Authority .................................................................................................................. 24  
  Create an iOS Profile with a Credential Payload .................................................................................................................. 44  
  iOS Device Enrollment With Directory Account .................................................................................................................... 51  
  View the Certificate on the Device ....................................................................................................................................... 66  
  Un-enrolling Your Device ..................................................................................................................................................... 72  
  Conclusion.................................................................................................................................................................................. 81
Lab Overview - HOL-1857-06-UEM - Workspace ONE UEM Configuration, AD Integration/Certificates
Lab Guidance

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

The Advanced AirWatch lab targets some of more advanced features such as active directory integration and certificate authority integration. AD integration allows the admin and end users to use their corporate AD credentials, without having to create local accounts in the AirWatch console. Certificate based authentication is not only one of the more secured forms of authentication but it also enables better end user experience on their mobile devices.

Each Module can be taken independently or you can start at the beginning and work your way through each module in sequence. In most cases, a unique "sandbox" instance of AirWatch will be created just for you when you begin a Module. When the Module has ended, this sandbox will be deleted and the device that you are enrolling in the lab will be returned to the state that it was in prior to the lab. The approximate time it will take to go through all the modules is around 1 hours.

Lab Module List:

- **Module 1 - Advanced Workspace ONE UEM Configuration, AD Integration/Certificates** (60 minutes) (Advanced) Integrate with your active directory and configure AirWatch to seamlessly integrate with certificate authority to distribute certificates for authentication.

Lab Captains:

- All modules: Roger Deane, Shardul Navare, Justin Sheets.

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:

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

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

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

This cosmetic issue has no effect on your lab.

**Look at the lower right portion of the screen**
Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes you lab has not changed to "Ready", please ask for assistance.
Module 1 - Advanced Workspace ONE UEM Configuration, AD Integration/Certificates (60 minutes)
Introduction

AirWatch 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 authority with AirWatch, 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 - 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.

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 AirWatch Console

To perform most of the lab you will need to login to the AirWatch Management Console.

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.

Authenticate to the AirWatch Administration Console

Username
Your VLP Email Address

Password
VMware1!

Login

Trouble Logging In
The default home page for the browser is https://hol.awmdm.com. Enter your AirWatch 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 AirWatch Hands On Labs server.**

Accept the End User License Agreement

You must accept the following AirWatch software license agreement to use AirWatch Mobile Device Management.

**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 AirWatch Terms of Use. Click the Accept button.
Address the Initial Security Settings

After accepting the Terms of Use, you will be presented with a Security Settings popup. The Password Recovery Question is in case you forget your admin password and the Security PIN is to protect certain administrative functionality in the console.

1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a question from the Password Recovery Question drop-down (default selected question is ok here).
3. Enter "VMware1!" in the Password Recovery Answer field.
4. Enter "VMware1!" in the Confirm Password Recovery Answer field.
5. Enter "1234" in the Security PIN field.
6. Enter "1234" in the Confirm Security PIN field.

After accepting the Terms of Use, you will be presented with a Security Settings popup. The Password Recovery Question is in case you forget your admin password and the Security PIN is to protect certain administrative functionality in the console.

1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a question from the Password Recovery Question drop-down (default selected question is ok here).
3. Enter "VMware1!" in the Password Recovery Answer field.
4. Enter "VMware1!" in the Confirm Password Recovery Answer field.
5. Enter "1234" in the Security PIN field.
6. Enter "1234" in the Confirm Security PIN field.

After accepting the Terms of Use, you will be presented with a Security Settings popup. The Password Recovery Question is in case you forget your admin password and the Security PIN is to protect certain administrative functionality in the console.

1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a question from the Password Recovery Question drop-down (default selected question is ok here).
3. Enter "VMware1!" in the Password Recovery Answer field.
4. Enter "VMware1!" in the Confirm Password Recovery Answer field.
5. Enter "1234" in the Security PIN field.
6. Enter "1234" in the Confirm Security PIN field.
7. Click the **Save** button when finished.

### Close the Welcome Message

After completing the Security Settings, you will be presented with the AirWatch Console Welcome pop-up.

1. Click on the **Don't show this message again** 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 AirWatch MDM. If you haven’t yet opened the console, please do so now by following the instructions in "Login to the AirWatch 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.

Server Setup

1. Click the **Server** tab.
2. Select **controlcenter.corp.local** for the server.
3. Select **None** for the encryption type.
4. Configure the LDAP settings as needed.
Configure the Server section of Directory Services as follows:

1. Confirm that the **Server** tab is selected.
2. Enter "**controlcenter.corp.local**" in the **Server** box.
3. Confirm that the **Encryption Type** is set to **None**.
4. Scroll down to continue configuring the Server section.

**Server Setup (continued)**

1. Enter "**389**" for the **Port** field.
2. Enter "**3**" for the **Protocol Version** field.
3. Select **GSS-NEGOTIATE** for the **Bind Authentication Type**. *NOTE - You may need to scroll to the right to see this option.*
4. Enter "**corp\administrator**" for the **Bind Username** field.
5. Enter "**VMware1!**" for the **Bind Password** field.
6. Enter "**corp.local**" in the **Domain** field.
Configure the User section of Directory Services as follows:

1. If necessary, 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 **Save**.

Confirm Directory Services Saved Successfully

After the Saving loading wheel finishes, you should see the **Saved Successfully** confirmation appear.
Test Directory Services Connection

1. Scroll down to the bottom of the Group section again.
2. Click the Test Connection button.
3. Confirm that the Connection successful with the given Servername, Bind Username and Password message is displayed.

Close Directory Services

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 AirWatch as well as how to integrate the Certificate Authority on your domain with AirWatch 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 AirWatch and assign security permissions to allow a service account to make requests to the CA. If you already have a PKI in your enterprise, AirWatch 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 AirWatch, 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 AirWatch. 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 AirWatch.

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

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

Getting the Certificate Authority Server Name

The first item that you will need when integrating AirWatch 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**

![Image of CONTROLCENTER-CA Properties window with options highlighted]

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 AirWatch. 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 AirWatch. The template you choose depends on the function being configured in AirWatch. 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](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**".
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. 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

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 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 X 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.

Add the Certificate Authority in AirWatch

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

In order for AirWatch to retrieve a certificate from a Certificate Authority (CA), you must configure the AirWatch 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 AirWatch Console in your browser tab.
Login to the AirWatch Console (IF NEEDED)

If your AirWatch Console login session has expired, enter your AirWatch Admin Account information and click the Login button. Otherwise, skip this step and continue.

**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 AirWatch Hands On Labs server.**
Configuring the CA in AirWatch

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 AirWatch

1. Enter "CONTROLCENTER-CA" for the Name.
2. Enter "Control Center Certificate Authority" for the Description.
3. Select Microsoft ADCS for the Authority Type.
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. Select **Service Account** for the Authentication.
2. Enter "imaservice" for the Username.
3. Enter "VMware1!" for the Password.
4. Enter "VMware1!" for the Confirm Password.
5. Select **None** for Additional Options.
6. Click Test Connection and ensure the "Test is Successful!" prompt displays at the top of the menu.
7. Click Save and Add Template.

**Setup the Certificate Template**

- **Name**: your@email.shown.here
- **Description**: Mobile User
- **Certificate Authority**: CONTROLCENTER-CA
- **Issuing Template**: MobileUser
- **Subject Name**: CN={EnrollmentUser}
- **Private Key Length**: 2048
1. Enter your VLP email address for the Name.
2. Enter "Mobile User" for the Description.
3. Select CONTROLCENTER-CA for the Certificate Authority.
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.
4. Enter "5" for Auto Renewal Period (days).
5. Enable the Enable Certificate Revocation option.
6. Click Save.
Close the Certificate Authorities Settings Page

Click **Close** on the **Certificate Authorities** page.

**Conclusion and Wrap Up**

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

Proceed to the next chapter to define an AirWatch 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.

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.

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**

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

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

You should now see your Restrictions Profile, named "iOS Certificate", within the List View of the Devices Profiles window.

**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

You will now enroll your iOS device by using a directory account for use with this module.

Download/Install AirWatch MDM Agent Application from App Store - IF NEEDED

NOTE - Checked out devices will likely have the AirWatch MDM Agent already installed. You may skip this step if your device has the AirWatch MDM agent installed.
At this point, if using your own iOS device or if the device you are using does NOT have the AirWatch MDM Agent Application installed, then install the AirWatch Application.

To Install the AirWatch MDM Agent application from the App Store, open the App Store application and download the free **AirWatch MDM Agent** application.

**Launching the AirWatch MDM Agent**

Launch the **AirWatch Agent** app on the device.

*NOTE - If you have your own iOS device and would like to test you will need to download the agent first.*
Choose the Enrollment Method

Welcome to AirWatch!

AirWatch helps your IT Department to provide your device with secure access to resources.

The multi-step enrollment process begins with authentication.

Choose authentication method:

- Email Address
- Server Details
- QR Code

Click on the Server Details button.
Find your Group ID from AirWatch Console

The first step is to make sure you know what your Organization Group ID is.

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 AirWatch MDM Agent to the HOL Sandbox

Once the Agent has launched you can enroll the device. To do so, follow the below steps.
1. Enter "hol.awmdm.com" for the Server field.
2. 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.
3. Tap the Go button.

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

Authenticate the AirWatch MDM Agent

On this screen, enter the Username and Password for the basic user account.

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

Enable Device Management

To enable your device, you will be redirected to Safari and Settings

Why?

- Access your company resource
- Remove company data in the event of loss or theft
Allow Website to Open Settings (IF NEEDED)

Process will begin shortly...

Tap Here if you are not prompted automatically.

This website is trying to open Settings to show you a configuration profile. Do you want to allow this?

Ignore  Allow

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**

The AirWatch Agent will now redirect you to Safari and start the process of enabling MDM in the device settings.

Tap on **Redirect & Enable** at the bottom of the screen.
Install the MDM Profile

Tap **Install** in the upper right corner of the Install Profile dialog box.
Install and Verify the AirWatch MDM Profile

Tap **Install** when prompted at the Install Profile dialog.

*NOTE - If a PIN is requested, it is the current device PIN. Provided VMware devices should not have a PIN.*
iOS MDM Profile Warning

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

The administrator may collect personal data, add/remove accounts and restrictions, and list, install and manage apps 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.
iOS Profile Installation Complete

You should now see the iOS Profile successfully installed.

Tap Done in the upper right corner of the prompt.
AirWatch Enrollment Success

Your enrollment is now completed. Tap **Open** to navigate to the AirWatch Agent.
Accept the Authentication Complete Prompt

![Configure with Done button]

Authentication Complete

- You will receive company resources and settings assigned to your device by your IT department
- You will receive a notification if further action is required

Click on **Done** to continue.

Accept Notification Prompt (IF NEEDED)

![Notification prompt]

Tap **Allow** if you get a prompt for Notifications.

Accept the App Installation (IF NEEDED)

![App installation dialog]

VMware AirWatch: Directory and Certificate Authority
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.
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 AirWatch. 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** - **AirWatchMDM/V_6** 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 **AirWatchMDM/V_6**
Select More Details to view additional configuration.

<table>
<thead>
<tr>
<th>Settings</th>
<th>12:29 PM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Airplane Mode</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Wi-Fi</strong> vmwareguest</td>
<td></td>
</tr>
<tr>
<td><strong>Bluetooth</strong> On</td>
<td></td>
</tr>
<tr>
<td><strong>Cellular Data</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Notifications</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Control Center</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Do Not Disturb</strong></td>
<td></td>
</tr>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
</tbody>
</table>

- **AirWatchMDM/V_G**
- Signed by: *autmdm.com*
- Verified: ✔
- Description: AirWatchMMDMDescription
- Contains: Mobile Device Management 3 Certificates

More Details

Remove Management
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 **imauser** that has been issued from the CONTROLCENTER-CA that we previously integrated into AirWatch. 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 AirWatch 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 AirWatch.

**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 MDM Agent application from the device as this was downloaded manually before AirWatch 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 AirWatch 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.
After selecting **Enterprise Wipe**, you will be prompted to enter your Security PIN which you set after your logged into the console ("1234").

1. 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 AirWatch 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 AirWatch services from the device if network connectivity is failing.
Press the Home button on the device to go back to the home screen. The applications pushed through AirWatch should have been removed from the device.

**NOTE** - The applications and settings pushed through AirWatch management 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.
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 Management** at the bottom of the list of General settings.

**Force the Wipe - IF NECESSARY**

Tap the **Workspace Services** profile that was pushed to the device.
Force the Wipe - IF NECESSARY

1. Tap **Remove Management** on the Workspace Services 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 Workspace Services 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 AirWatch 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-1857-06-UEM

Version: 20180323-184034