# Table of Contents

Lab Overview - HOL-1857-03-UEM - Workspace ONE UEM with App & Access Management .................................................................................................................... 2  
Lab Guidance ........................................................................................................ 3  
Module 1 - Workspace ONE Setup and Configuration ............................................ 9  
  Introduction ........................................................................................................ 10  
  VMware Enterprise Systems Connector Setup .................................................... 11  
  Login to the AirWatch Console ......................................................................... 13  
  Login to the VMware Identity Manager Console ............................................ 17  
  Configure Your VMware Identity Manager Tenant ......................................... 22  
  Configure Directory Services and VMware Identity Manager User Sync ........ 25  
  Review Your Configuration in VMware Identity Manager ................................ 38  
  Integrate AirWatch and VMware Identity Manager using the Cloud Kerberos Key Distribution Center (KDC) ................................................................. 42  
  iOS Device Enrollment With Directory Account .............................................. 63  
  SSO Validation ................................................................................................. 78  
  Un-enrolling Your Device ................................................................................ 89  
  Conclusion ........................................................................................................ 98
Lab Overview - HOL-1857-03-UEM - Workspace ONE UEM with App & Access Management
Lab Guidance

NOTE - 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.

Explore Workspace ONE configuration and how it simplifies authentication by leveraging Single Sign On. Setup the VMware Enterprise Systems Connector, AD integration and provide ease of use by leveraging Cloud KDC for signing in automatically. The approximate time required to finish all the modules in this lab is 1 hour.

Lab Module List:

• **Workspace ONE Setup and Configuration** (60 minutes) (Advanced) Configure VMware Enterprise Systems Connector, AD integration and complete Identity manager configuration. The goal of this lab is to perform the setup which will offer automatic signing in. Validate the setup on an iOS device by performing Single Sign On.

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:

Location of the Main Console

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

Alternate Methods of Keyboard Data Entry

During this module, you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.
Click and Drag Lab Manual Content Into Console Active Window

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

Accessing the Online International Keyboard

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

1. Click on the Keyboard Icon found on the Windows Quick Launch Task Bar.
Click once in active console window

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

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

Click on the @ key

1. Click on the "@" **key**.

Notice the @ sign entered in the active console window.
Activation Prompt or Watermark

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

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

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

This cosmetic issue has no effect on your lab.

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

VMware AirWatch 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 AirWatch 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 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 - 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 subtitiles 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.

**IMPORTANT:** READ THIS DOCUMENT CAREFULLY.

The terms and conditions of this end user license agreement (the “EULA”) constitute a legal agreement between you (either an individual or, if purchased or otherwise acquired by or for an entity, such entity) (“CUSTOMER”) and AIRWATCH with respect to the use of the Proprietary AIRWATCH SOFTWARE. BY (1) EXECUTING AN AIRWATCH ORDER, (2) INSTALLING, COPYING, DOWNLOADING OR OTHERWISE ACCESSING THE SOFTWARE, (3) ELECTRONICALLY ACCEPTING, OR (4) EXECUTING THIS EULA, CUSTOMER COMPLETELY AND UNCONDITIONALLY AGREES TO BE BOUND BY THE TERMS OF THIS EULA WITHOUT MODIFICATION. IF CUSTOMER DOES NOT INTEND TO BE LEGALLY BOUND TO THE TERMS AND CONDITIONS OF THIS EULA, CUSTOMER MAY NOT ACCESS OR OTHERWISE USE THE SOFTWARE AND MUST PROMPTLY RETURN OR DELETE ALL COPIES OF THE SOFTWARE AND DOCUMENTATION IN THE MANNER PROVIDED HERETO.

In consideration of the mutual covenants herein expressed, and other true and valuable consideration, the receipt and adequacy of which are hereby acknowledged, the parties hereby agree as follows:

1. **Definitions.** The following capitalized terms shall have the meanings and applications set forth below:

   1.1 “Affiliate” means any entity controlling, under common control with or controlled by a party, such common control or control being defined as ownership of more than fifty percent (50%) of the voting equity of the entity or ownership of securities through which are attached voting rights capable of electing more than fifty percent (50%) of the entity’s board of directors. Any Affiliate of Customer may use a Software License granted hereunder and, by doing so, agrees to be bound to the terms and conditions hereof, in which case all references to Customer

**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 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. Save
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.
Login to the VMware Identity Manager Console

A temporary VMware Identity Manager tenant has been generated for you to use throughout this lab. The tenant URL and login details were emailed to the email address associated with your VMware Learning Platform (VLP) account and uploaded to the AirWatch Content section in the AirWatch Console at the start of the lab.

If you have access to your email account, continue to the next step. If you do not have access to your email account, continue to the "Accessing Your Tenant Details in the AirWatch Console" for further instructions.

Accessing Your Tenant Details by Email

Continue to the next step for instructions on locating to the email containing your VMware Identity Manager tenant details.

Locate Email and Copy Details

Hello,

Due to your recent enrollment in HOL-1857-03-UEM, you have received a temporary VMware Identity Manager tenant that is necessary to complete the lab!

- **Tenant URL**: https://yourtenant.vimpreview.com
- **Admin Username**: Administrator
- **Admin Password**: VMware1!

To login to your VMware Identity Manager tenant, navigate to the Tenant URL and use the provided Admin Username and Password values on the login screen.

You will need to login to the email account that you associated with the VMware Learning Platform (VLP), which is also the email address you used to login to the AirWatch Console.

The subject of the email will be titled "HOL-1857-03-UEM". After opening the email, note the Tenant URL, Admin Username and Admin Password fields provided as you will need them to login in the following steps.

You may continue to the "Login to Your VMware Identity Manager Tenant" section.
Accessing Your Tenant Details in the AirWatch Console

Continue to the next step for instructions on locating your VMware Identity Manager details within the AirWatch Console.

Download the Text File From AirWatch Content

In the AirWatch Console:

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

Open the Downloaded Text File

After the file downloads, click the "vIDM Tenant Details for your@email.shown.here.txt" file from the download bar to open it.
Copy the Tenant URL

1. Click and drag to 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.

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 either by accessing the email sent to your email address associated with VLP or through the uploaded text file to the AirWatch Console. If you did not copy or note this information from the previous step, return to those previous steps and note your Tenant URL.*

**Login to Your VMware Identity Manager Tenant**

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

**Navigate to the Administrator Console (If Necessary)**

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

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

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

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

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

Continue to the next step.
Edit User Attributes

1. 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**.

Return to the AirWatch Console

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

Click the **AirWatch tab**, which should be the first tab, on your browser to return to the AirWatch Console Login page.

*NOTE - Your AirWatch tab may not be at the Login page as shown in the picture depending on your previous steps.*
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.

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.
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**.
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 we 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**.

---

VMware AirWatch - Workspace ONE, Single Sign-on and VMware Identity Manager
6. Click **Save**.

**Edit the User Group**

Click the **Edit (Pencil)** button next to the **Users** user group that was created.

**Update the User Group Settings**

1. You may need to scroll down to the bottom of the menu.
2. Enter "100" for the **Maximum Allowable Changes**
3. Enable **Add Group Members Automatically**
4. 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 AirWatch.

**Acknowledge Sync**

Click **OK**.

**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.
2. It may take 20-30 seconds to complete the user sync. Please use the refresh button to check the status.
3. Confirm that you see **26 Users** synced for the group.

**Confirm User Sync in VMware Identity Manager**

Return to your VMware Identity Manager to confirm that the corp.local domain and users successfully synced.

1. Click **Identity & Access Management**.
2. Click **Directories**.
3. Locate the Directory that was synced from AirWatch. 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 **4** synced users.
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 AirWatch Console. Navigate back to the AirWatch Console, and go to Groups & Settings > All Settings.

1. Click **System**
2. Click **Enterprise Integration**
3. Click **VMware Identity Manager**
4. Scroll down to the bottom of the VMware Identity Manager settings page
5. 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 AirWatch and populate the related configurations within Identity Manager console. Let's review our configuration in Identity Manager to see where these changes are made.

Navigate to Identity Manager Tab

Click to navigate to VMware Identity Manager Admin Console.

Navigate to Identity and Access Management Setup

In your VMware Identity Manager Tenant,

1. Click on **Identity & Access Management**
2. Click on **Setup**
Validate the Configuration for AirWatch

1. Click **AirWatch** to view the related configurations.
2. Validate that you are seeing **AirWatch API URL** as **https://hol.awmdm.com**
3. Validate that you are seeing an **API Key** populated.
4. 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. Enter the `AirWatch Group ID`.
3. Save changes.
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 AirWatch Console)
3. Click Save

**Enable App Catalog (IF NEEDED)**

1. Scroll down if needed until you see a section for *Unified Catalog*
2. Select Enable if not selected already.
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 AirWatch Console**

---

VMware AirWatch - Workspace ONE, Single Sign-on and VMware Identity Manager
For the next steps, we will return to the AirWatch Console and complete the Workspace ONE Getting Started wizard.

Click the **AirWatch tab**, which should be the first tab, on your browser to return to the AirWatch Console Login page.

*NOTE - Your AirWatch tab may not be at the Login page as shown in the picture depending on your previous steps.*
Integrate AirWatch 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 AirWatch and VMware Identity Manager. Continue to review the necessary steps.

Configure VMware Identity Manager Settings in AirWatch

The first steps for configuring the Cloud Kerberos Key Distribution Center (KDC) is to setup the VMware Identity Manager Certificate in AirWatch.
1. Click **Groups & Settings**.
2. Click **All Settings**.

Enable the Certificate

1. Click **System**
2. Click **Enterprise Integration**
3. Click **VMware Identity Manager**
4. Scroll down to the **Certificate** section
5. 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 AirWatch, return to your VMware Identity Manager tenant to continue the Cloud Kerberos Key Distribution Center (KDC) configuration.

Switch to VMware Identity Manager 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 on **Authentication Methods** section.
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. Locate the **VidmAirWatchRootCertificate.cer** file.
2. Select the file.
3. Click **Open**.

---

*VMware AirWatch - Workspace ONE, Single Sign-on and VMware Identity Manager*
1. Select the Downloads folder.
2. Select the VidmAirWatchRootCertificate.cer file that was downloaded previously.
3. Click Open.

Confirm the Authentication Adapter Update

![Update Auth Adapter dialog box]

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

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

1. Click **Policies**.
2. Click the checkbox to select the **default_access_policy_set**.
3. Click **Edit**.

### 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. 
2. 

---

**VMware AirWatch - Workspace ONE, Single Sign-on and VMware Identity Manager**
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 **Save**.

**Save the Policy Rule Updates**

![Save Policy Rule Updates](image)

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

**Create AirWatch 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 **AirWatch** tab to return to the AirWatch Console.

**Close the Settings Page**

![Close Settings](image)
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. Scroll down if needed.
4. Click in the **Assigned Groups** field and a list of groups will appear.
5. 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. Navigate to the Downloads folder.
2. Select the KDC root certificate file.
3. Click **Open**.
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**

```
Add

Certificate [Choose File] KDC-root-cert.cer

Save Cancel
```

Click **Save**.

**Configure the SCEP Payload**

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

SCEP

1. Select **AirWatch Certificate Authority** for the **Credential Source** dropdown.
2. Select **AirWatch 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 "testssso" 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 received in the email when starting the lab and also 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.
Publish the Profile

View Device Assignment

No Records Found

Click **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

Redirect & Enable
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**

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

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

Congratulations!
You have completed the initial configuration for your device. You may now proceed with further action as needed.

Open this page in “Agent”?

Cancel  Open

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

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)

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

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.
SSO Validation

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

Open Settings

Tap Settings.
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

![Open the Digital Workspace profile](image)

Tap the **Workspace Services** profile.

### View More Details

![View More Details](image)
Open the Singe 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 that 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

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.

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.
Navigate to Identity Manager in Safari

1. Enter the URL of your Identity Manager tenant in the URL bar.
2. Click **Go**
Workspace One Single Sign-On

Notice that Identity Manager is signing you in without requiring any authentication.
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 Identity Manager or AirWatch.
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**.
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. 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.
Verify the Un-Enrollment

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.**
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 Management** at the bottom of the list of General settings.

**Force the Wipe - IF NECESSARY**

![Screen with General and Device Management options]

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

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 AirWatch 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.
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-1857-03-UEM

Version: 20180323-183804