# Table of Contents

   Lab Guidance ........................................................................................................... 4

**Module 1 - Introduction to Apple iOS Management** ................................................. 9
   Introduction ............................................................................................................ 10
   Login to the Workspace ONE UEM Console .......................................................... 11
   Add A Basic User Account ...................................................................................... 17
   Create a Device Restriction Profile ........................................................................ 20
   Validate Device Before Restriction Profile .............................................................. 26
   iOS Device Enrollment using basicuser ................................................................... 28
   Validate the Restriction Profile .............................................................................. 47
   Un-enrolling Your Device ....................................................................................... 48
   Conclusion ............................................................................................................. 57

**Module 2 - Introduction to Apple macOS Management** ......................................... 58
   Introduction ........................................................................................................... 59
   Login to the Workspace ONE UEM Console .......................................................... 60
   Retrieving the Group ID ........................................................................................ 66
   Installing the Workspace ONE Intelligent Hub ...................................................... 67
   Enroll a macOS Device ......................................................................................... 74
   Creating a Device Profile for macOS ...................................................................... 83
   Creating a User Profile for macOS ........................................................................ 91
   Reviewing New Payloads for macOS High Sierra Profile ...................................... 97
   Configuring Device Lock ....................................................................................... 104
   macOS Application Management (MAM) ............................................................... 108
   Managing macOS Custom Attributes .................................................................... 145
   Enterprise Wipe a macOS Device ......................................................................... 154
   Validate the Enterprise Wipe on the macOS Device ............................................ 157
   Conclusion ............................................................................................................ 160

**Module 3 - Software Distribution with macOS** ..................................................... 161
   Introduction ........................................................................................................... 162
   Login to the Workspace ONE UEM Console .......................................................... 163
   Installing the Workspace ONE Intelligent Hub ...................................................... 169
   Enroll a macOS Device ......................................................................................... 176
   Software Distribution Methods ............................................................................. 185
   VIDEO: Deploying macOS Volume-Purchased Apps ............................................. 189
   Deploying macOS Applications via Internal Applications (using Munki) ............... 190
   Deploying macOS Applications via Product Provisioning (legacy support) .......... 228
   Enterprise Wipe a macOS Device ....................................................................... 256
   Conclusion ............................................................................................................ 259

**Module 4 - AirWatch School Manager** ................................................................. 260
   Introduction ........................................................................................................... 261
   Login to the Workspace ONE UEM Console .......................................................... 263
   Enabling VMware AirWatch School Manager ...................................................... 269
Creating the Class List .................................................................................................................. 273
Publish the Classroom Application ............................................................................................. 277
Enroll Class Devices .................................................................................................................... 285
Control Student Devices with Classroom App .............................................................................. 305
Un-enrolling Your Device ............................................................................................................. 311
Conclusion .................................................................................................................................. 320
Lab Overview - HOL-1957-05-UEM - Workspace ONE UEM - Apple 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.

Discover how Workspace ONE UEM with iOS and macOS provides a wide array of management capabilities for your Apple devices. This lab focuses on how to manage device restrictions, application distribution, and modifying aspects of the end user experience. In addition, learn how Apple School Manager can be used to control and manage Apple devices for the classroom. Lastly, explore how Ground Control, a partner solution, can be used with Workspace ONE UEM to for zero-touch provisioning with shared devices.

Lab Module List:

- **Module 1 - Introduction to Apple iOS Management** (30 minutes) (Beginner) This lab module will focus on introducing the concepts of Unified Endpoint Management (UEM) with Workspace ONE. This lab will walk you through how to enroll an iOS device and deploy device profiles to configure your iOS devices to leverage UEM functionality.

- **Module 2 - Introduction to Apple macOS Management** (30 minutes) (Beginner) Explore key Workspace ONE administration features and concepts available for the macOS platform. This lab will give you a better understanding of how macOS devices are enrolled, what management options you have available, and how these options can improve and impact the user experience by configuring macOS and publishing applications.

- **Module 3 - Software Distribution with macOS** (30 minutes) (Beginner) Learn how to deploy various types of software applications to your macOS devices with Workspace ONE UEM and any caveats associated with these deployments.

- **Module 4 - Apple School Manager** (45 minutes) (Beginner) Learn how to deploy Apple School Manager with Workspace ONE UEM, then explore the various features that empower classrooms by enrolling two iOS devices to simulate a classroom scenario.

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

Subject Matter Experts:

• Robert Terakedis, Sr. Technical Marketing Manager, 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 cannot be saved. All your work must be done during the lab session. But you can click the **EXTEND** to increase your time. If you are at a VMware event, you can extend your lab time twice, for up to 30 minutes. Each click gives you an additional 15 minutes.
Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.

Alternate Methods of Keyboard Data Entry

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

Click and Drag Lab Manual Content Into Console Active Window

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

Accessing the Online International Keyboard

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

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

Click once in active console window

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

**Click on the @ key**

1. Click on the "@ key".

Notice the @ sign entered in the active console window.

**Activation Prompt or Watermark**

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

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

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

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

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

This lab module will focus on introducing the concepts of Unified Endpoint Management (UEM) with Workspace ONE UEM, using the Workspace ONE UEM Console, and how to enroll an iOS device into Workspace ONE. By the end of this lab, you should have a better understanding of why Unified Endpoint Management is important and how Workspace ONE UEM can manage your iOS devices.
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, OR COPY THE SOFTWARE. IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN FORTY-FIVE (45) 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 *
VMware!

Confirm Password Recovery Answer *
VMware!

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.
Add A Basic User Account

Basic accounts are the accounts which are created locally in the AirWatch admin console, as opposed to the accounts which are imported from an active directory. In this section, we will create a Basic User account which we will use for enrollment in the following section.

Click on Add / User

In the top right corner of the AirWatch console,

1. Click **Add**.
2. Click **User**.

---

In the diagram shown above:

1. Click **Add** to open the dropdown menu.
2. Click **User** to select the account type.
Add User information

In the pop-up window,

1. Ensure that security type is **Basic**
2. Enter the username as **basicuser**
3. Enter the password as **VMware1!**
4. Confirm the password as **VMware1!**
5. Enter the first name as **basic**
6. Enter the last name as **user**
7. Enter the e-mail address as **basicuser@corp.local**

*NOTE - Use the scroll bar if you don't see the option to enter email address*

8. Click on **Save**
You should see a confirmation that user is created successfully. If the user is already created with the same username then you can use the existing user in the following section.
Create a Device Restriction Profile

In this section, we will create a restriction profile that will disable the camera on the device. We will set the profile for auto-deployment, so that the profile to disable the camera will install automatically when the device is enrolled.

Add A Profile

In the top right corner of the AirWatch console,

1. Click Add.
2. Click Profile.
Select Platform as Apple iOS

Click Apple iOS.

Configure General Payload

1. Select the General tab.
2. Enter the Name as 'iOS Restriction Profile'.
3. Select 'All Devices (your@email.shown.here)' for Assigned Groups.
4. Ensure that the Exclusions are set as needed.
1. Select **General** if not selected already.
2. Enter **iOS Restriction Profile** for the **Name** field.
3. Click the **Assigned Groups** dropdown field to view all available assignment groups.
   
   *NOTE - You may need to scroll down to find the Assigned Groups dropdown.*
4. Select **All Devices (your@email.shown.here)** from the list.

**Configure Restriction Payload**

1. Click on the **Restrictions** payload in the left panel.
2. Click **Configure**.
Disable Allow use of camera

1. Uncheck the **Allow use of Camera** checkbox.
2. Click **Save & Publish**.
Publish the Profile

Click Publish.
Validate profile creation

1. Click **Devices**.
2. Expand **Profiles & Resources**.
3. Click **Profiles**.
4. Validate that you see **iOS Restriction Profile** in the Profiles List View.
Validate Device Before Restriction Profile

Before enrolling your device, confirm that the Camera app is available on your iOS device.

Find the Camera App

Press the **Home** button on your device and find the **Camera** app. Take note of the location of the app, as we will confirm the removal of the app in a later step after enrollment.
Search for the Camera App (Optional)

1. Swipe down to show the Search bar.
2. Enter "camera" in the Search bar.
3. Ensure the Camera app displays, confirming the app exists on the device.
iOS Device Enrollment using basicuser

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**

![Workspace ONE Intelligent Hub icon]

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

1. Enter **basicuser** 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 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

<table>
<thead>
<tr>
<th>Device Manager</th>
<th>Workspace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signed by</td>
<td>awmdm.com</td>
</tr>
<tr>
<td>Verified</td>
<td>✔</td>
</tr>
<tr>
<td>Description</td>
<td>Device Management profile to manage and activate access to work applications and services on your device.</td>
</tr>
<tr>
<td>Contains</td>
<td>Device Enrollment Challenge</td>
</tr>
</tbody>
</table>

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.
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

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.
Validate the Restriction Profile

Now that the device is enrolled, the restriction profile we created will be installed on the device and the Camera app will be disabled. Continue to the next steps to verify that the Camera app is successfully disabled.

Return to the Camera App

If you located the Camera app on the device earlier, return to your device and navigate back to where the Camera app previously was. Notice that the Camera app is now disabled and is no longer displayed on the device.

Search for the Camera App (Optional)

1. Swipe down to show the Search bar.
2. Enter **camera** in the Search bar.
3. Notice that the Camera app is disabled and no longer displays in the search results.
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. \textit{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
### Settings

<table>
<thead>
<tr>
<th>Airplane Mode</th>
<th>Wi-Fi</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bluetooth</td>
<td>Cellular Data</td>
</tr>
</tbody>
</table>

### General

#### Use Side Switch To:
- Lock Rotation
- Mute

Rotation Lock is available in Control Center.

#### iPad Storage
- Background App Refresh

#### Restrictions
- Off

#### Date & Time
- Keyboard
- Language & Region
- Dictionary

#### iTunes Wi-Fi Sync
- Not Connected

#### Device Management
- Device Manager

#### Regulatory

#### Reset
- Shut Down
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](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

Managing your devices with Workspace ONE UEM empowers your administrators to ensure devices are operating and accessing corporate resources securely without violating user privacy. Now that you know how to enroll a device a push a profile, consider exploring the other lab topics available in this module to further expand your Workspace ONE UE< knowledge.

This concludes the Introduction to Apple iOS Management module.
Module 2 - Introduction to Apple macOS Management
Introduction

In this lab module, we will explore some Workspace ONE administration features and concepts available for the macOS platform. This lab will give you a better understanding of how macOS devices are enrolled, what management options you have available, and how these options can improve and impact the user experience by configuring macOS and publishing applications.

Before you can start the lab, make sure you review the next page to ensure you can successfully complete the lab.

Pre-Requisites

To successfully complete this Hands-On Lab, you'll need to ensure you have the following pre-requisites:

- An Apple device running macOS version 10.13.5 (High Sierra) or later.
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.

```text
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

<table>
<thead>
<tr>
<th>Password Recovery Question 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Recovery Question *</td>
<td>What was your childhood nickname?</td>
</tr>
<tr>
<td>Password Recovery Answer *</td>
<td>VMware1!</td>
</tr>
<tr>
<td>Confirm Password Recovery Answer *</td>
<td>VMware1!</td>
</tr>
</tbody>
</table>

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).

<table>
<thead>
<tr>
<th>Security PIN *</th>
<th>Show</th>
</tr>
</thead>
<tbody>
<tr>
<td>1234</td>
<td></td>
</tr>
<tr>
<td>Confirm Security PIN *</td>
<td>Show</td>
</tr>
<tr>
<td>1234</td>
<td></td>
</tr>
</tbody>
</table>

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

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.
Retrieving the Group ID

Before enrolling your device, retrieve your Group ID from the Workspace ONE UEM Console.

Point to the Organization Group

Select the email address you used to log in to the Workspace ONE UEM Console.

Copy the Group ID

Copy the Group ID from the Organization Group tab.
Installing the Workspace ONE Intelligent Hub

In this exercise, download and install the Workspace ONE Intelligent Hub on your macOS device.

Log In to the MacBook - If Needed

Login to the macOS device. If you are using a VMworld provided device, the login details are below.

1. Enter `administrator` for the username.
2. Enter `VMware1!` for the password.
3. Press the continue button or press `ENTER`.
Download the Workspace ONE Intelligent Hub

Click the **Safari icon** (blue compass) to open the Safari browser.

**Initiate Download**

1. Enter [https://www.getwsone.com](https://www.getwsone.com) in the URL field, then press **ENTER**.
2. Click **Download Hub for macOS**. The Workspace ONE Intelligent Hub installer begins to download and will save to the downloads folder by default.
Install the Workspace ONE Intelligent Hub

1. Click the **Downloads** folder in the dock (next to the Trash Bin).
2. Click the **VMwareWorkspaceONEIntelligentHub.pkg** file to begin the installer.
Continue at Introduction Screen

Welcome to VMware Workspace ONE Intelligent Hub Installer

Welcome to VMware Workspace ONE UEM!

This process will install an application that further enhances MDM capabilities on this device and will assist you in maintaining compliance with all security and information management policies. It may also configure resources to assist you in performing your work responsibilities. This is required to complete the enrollment process. Please follow all prompts to continue.

Click **Continue**.
Continue and Agree to Terms

1. On the License page, click **Continue**.
2. Click **Agree** (to the license terms).
Provide Credentials for the Installer

1. Click **Install**. You are now prompted to enter the computers administrator credentials.
2. Enter **administrator** in the Name field.
3. Enter **VMware1!** in the Password field.
4. Click the **Install Software** button.
Close and Move to Trash

1. Click **Close** when the installer finishes.
2. Click **Move to Trash** to move the installer to the trash.
Enroll a macOS Device

In this exercise, you enroll a macOS device into Workspace ONE UEM. Enrollment is the action that brings a device under management and control by Workspace ONE UEM. There are a number of ways to enroll the various platforms (macOS included), but for this exercise we cover a basic enrollment scenario.

Enroll the macOS Device

This enrollment flow is considered *User-Approved* per the functionality introduced in macOS High Sierra.

Begin macOS Enrollment Process

The Enrollment Wizard should start automatically. From within the Enrollment wizard window, click **Server Detail**.
**Note:** The Enrollment Wizard may take several minutes to launch. If you do not see the Enrollment Wizard immediately, be patient and wait for it to appear.

**Enter Enrollment Server Details**

1. Enter `labs.awmdm.com` for your Server URL.

2. Enter `{Your Group ID}`.
2. Enter your **Group ID**. This was documented in the previous steps titled **Retrieve Your Group ID**.
3. Click the **Continue** button.

### Enter Enrollment Credentials

1. Enter **testuser** for the enrollment staging username.
2. Enter **VMware1!** for the password.
3. Click the **Continue** button.
Enable Device Management

Enable Device Management

You are now ready to configure your device!

To complete this process, follow the System Preferences prompts and enter your computer password when prompted.

Click **Enable** to enable device management.
Install Device Manager Profile

Click **Install**.

Install Profile for User-Approved Enrollment

Click **Install**.
Enter Administrative Credentials for Profile Install

When prompted, enter the credentials for the macOS device.

1. Enter **administrator** for the username.
2. Enter **VMware1!** for the password.
3. Click **OK**.
Quit Profiles Preference Panel

Click the **Close** button (red dot) to close the Profiles panel.
Quit the Enrollment Wizard

Congratulations!

✓ Your device has been successfully enrolled!

✓ You now have secure access to your corporate resources.

✓ You may Quit to exit this installer or view your enrollment status by opening the Agent.

Click Quit when the installation completes.
Validate Mac Enrollment

Follow the next steps to verify that the Mac has been successfully enrolled.

In upper-right corner:

1. Note the shield icon in the menu bar. Click the **AirWatch Agent** icon.
2. Note the menu shows your device as **Enrolled**.
3. Click **Preferences** and review the options available to you in the agent.

Key Takeaways

- Agent-based macOS enrollment is streamlined and intuitive.
- Workspace ONE UEM supports a number of enrollment methods for macOS devices: web-based, agent-based, staged (pre-installed agent), enrollment on-behalf, and enrollment using the Apple Device Enrollment Program.
- Agent logs can be collected directly from the Workspace ONE Intelligent Hub. This eases helpdesk troubleshooting by allowing end-user to quickly send diagnostic information to helpdesk and/or administrative users.
Creating a Device Profile for macOS

This exercise explores how to modify the macOS device behavior using Profiles.

Profiles are the mechanism by which Workspace ONE UEM manages settings on a macOS device. macOS profile management is done in two ways: device level and enrollment-user level. You can set appropriate restrictions and apply appropriate settings regardless of the logged-on user. You can also apply settings specific to the logged-on user on the device.

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 some filters on what device will get it.
- 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.

Device Profiles are typically used to control settings that apply system-wide. Device profiles can include items such as VPN and Wi-Fi configurations, Global HTTP Proxy, Disk Encryption, and/or Directory (LDAP) integration. In this exercise, we create a profile that modifies the dock for all users on the machine.

Close System Preferences if opened

This section helps you to create a device profile which will change some system preferences in your Mac. However, to see those changes take place, you must first close any existing System Preference sessions if they are already open.

If System Preferences are opened, click X to close.
Add a macOS Device Profile

In the Workspace ONE UEM console:

1. Select **Devices**.
2. Select **Profiles & Resources**.
3. Select **Profiles**.
4. Select **Add**.
5. Select **Add Profile**.

**Select Profile Platform**

Add Profile

Select a platform to start:

- Android
- iOS
- macOS

Select the **macOS** icon.
Select the Profile Context

Select Context

Select the **Device Profile** icon.

**Profile General Settings**

Configure the device profile as follows:
1. Select **General** if it is not already selected.
2. Enter **macOS Device Restrictions** for the profile name.
3. Select **Auto** for the Assignment Type.
4. Scroll down to view the **Assigned Groups** field, and click in the search box. This will pop-up the list of created Assignment Groups. Enter **All Devices** and select **All Devices (your@email.shown.here)**.

**Note**: You do not need to click Save or Save & Publish at this point. This interface allows you to move around to different payload configuration screens before saving.

### Select the Restrictions Payload

**macOS** Add a New Apple macOS Profile

- **General**
- Passcode
- Network
- VPN
- Credentials
- SCEP
- Dock

1. Select **Restrictions**.
2. Click the **Configure** button.

**Note**: When initially setting most payloads a Configure button will show to reduce the risk of accidentally setting a payload configuration.
Configure the Restrictions Payload

macOS Add a New Apple macOS Profile

1. Select **Restrict System Preference Panes**
2. Select **Disable Selected Items**
3. Enable the **Bluetooth** checkbox.
4. Enable the **Energy Saver** checkbox.
Save and Publish

Click **Save and Publish**
Publish the Device Profile

View Device Assignment

Click the Publish button.

Verify the Device Profile Now Exists

You should now see your macOS Device Restrictions Device Profile within the list of the Profiles window.

Note: If you need to edit the Profile, this is where you would return in order to do so.
Validate Applied Profiles

1. Click the Apple icon in the upper-left corner
2. Click System Preferences.
3. If System Preferences shows you a specific subpanel, such as Time Machine, click the back button.
4. Note you cannot modify the settings for Bluetooth and Energy Saver as those icons are grayed-out.

Key Takeaways

- You can use a combination of Device-level and User-level profiles for flexibility when configuring your macOS devices.
- Profiles can be targeted against Assignment Groups for granular control.
Creating a User Profile for macOS

User Profiles are typically used to control settings that apply to the enrolled user. User profiles can include items such as Email configurations, web clips (URL shortcuts), credentials (certificates), and content filtering settings. In this exercise, we create restrictions for system preferences panes for the enrolled user on this machine.

Add a macOS User Profile

1. Select **Add**.
2. Select **Add Profile**.

Select Profile Platform

Select a platform to start:

- Android
- iOS
- macOS

Select Click on the **macOS** icon.
Select the Profile Context

Select Context

Select the **User Profile** icon.

Profile General Settings

Configure the profile as follows:
1. Click on **General** if it is not already selected.
2. Enter **macOS User Dock** in the Name text box.
3. Ensure the assignment type is set to **Auto**.
4. Click in the Assigned Groups field. This will pop-up the list of created Assignment Groups. Enter **All Devices** and select the **All Devices (your@email.shown.here)** Group.

**Note:** You do not need to click Save or Save & Publish at this point. This interface allows you to move around to different payload configuration screens before saving.

**Select the Dock Payload**

1. Select **Dock**
2. Click the **Configure** button.
Configure the Dock Payload

1. Change the Dock Size to be smaller
2. Change the Dock Position to Left

Save & Publish

Click Save & Publish
Publish the User Profile

Select the Publish button.

Verify the User Profile

You should now see your macOS User Dock User Profile within the List of the Profiles window.

Note: If you need to edit the Profile, this is where you would return in order to do so.
Validate the Dock has changed size and moved to the left side of the screen.
Reviewing New Payloads for macOS High Sierra 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 some filters on what device will get it.
- 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.

**Add a macOS Device Profile**

In the Workspace ONE UEM console:

1. Select **Devices**.
2. Select **Profiles & Resources**.
3. Select **Profiles**.
4. Select **Add**
5. Select **Add Profile**.
Select Profile Platform

Add Profile

Select a platform to start:

Android  
iOS  
macOS

Select the macOS icon.

Select the Profile Context

Select Context

User Profile  
Device Profile

Select the Device Profile icon.
Configure Security & Privacy Payload

macOS Add a New Apple macOS Profile

1. Select Security & Privacy
2. Click Configure.
Review Security & Privacy Payload Settings

macOS Add a New Apple macOS Profile

Security & Privacy

OS Updates

1. Select the **Delay Updates** check box.
2. Note the box where you can specify how long (1 to 90 days) to delay updates.

**Note:** The delay starts from the day the update is released. For example, if Apple publishes an update and the device is offline for the first 30 days the update is released, a 90-day update delay period would end 60 days later (even though technically the device has only known about the update for 60 days).
Review the Kernel Policy Extension Payload

macOS Add a New Apple macOS Profile

1. Select the **Kernel Extension Policy** payload.
2. Click **Configure**.

In the same profile screen:
1. Note the User Override setting. You can allow the user to add their own Kernel Extensions.
2. Click **Add** under Allowed Team Identifiers.
3. Note the Allowed Team identifier setting. This allows all Kernel Extensions signed by that team identifier.
4. Click **Add** under Allowed Kernel Extensions.
5. Note the Allowed Kernel Extensions setting. You can enter a constrained list of Kernel Extension bundle IDs and their associated developer.

**Note**: The Kernel Extension Policy requires the device to be enrolled through *User Approved MDM Enrollment* methods.

**Note**: To facilitate admins discovering Kernel Extensions (KEXTs) in their environment, VMware created a script that writes details about kernel extensions found in three common folders to the Custom Attributes database.

Download the [KEXT Custom Attributes via Products](#) script from GitHub.
Close Profile Window

1. Click the X in the upper-right corner to close the Add Profile window.
2. Click OK to confirm and discard your changes.
Configuring Device Lock

Device lock for macOS devices causes the machine to reboot into a firmware-lock screen. This lock screen occurs at the firmware level prior to OS boot.

Open macOS Device Details

1. Select Devices.
2. Select List View.
Select macOS Device

Select your enrolled macOS device.

**Note:** In this exercise we are using MacBooks—ensure that you are selecting your enrolled macOS device.

**Lock Device**

Click **Lock** in the upper-right corner of your device details view.
Enter Device Lock Code

Lock Device

You are about to perform the Lock Device action. Please enter a 6-digit unlock PIN below.

<table>
<thead>
<tr>
<th>Set Unlock PIN:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 1 1 1 1 1 1</td>
</tr>
</tbody>
</table>

Warning: This device cannot be unlocked remotely and can only be unlocked using 6-digit pin entered above. Write this PIN down and store it in a safe place. If you forget your PIN you must contact Apple to unlock your device.

1. Enter 111111 as the firmware lock code.
2. Click Lock Device.

Device Reboot

The device reboots after a short delay and the firmware will be locked.
Unlock The Device

1. At the System Lock screen, enter the unlock code 111111.
2. Click the Arrow (--> ) to boot the device.

Device lock for macOS devices causes the machine to reboot into a firmware-lock screen. This lock screen occurs at the firmware level prior to OS boot.

Key Takeaways

- Workspace ONE UEM supports a firmware-based device lock for macOS
- The device cannot be booted until the device lock code has been entered
macOS Application Management (MAM)

VMware AirWatch recently announced integration with the Open-Sourced "munki" project for third-party application management on enrolled macOS devices. With this integration, administrators can now manage third-party (non-AppStore) software using the internal apps view (closer aligning the admin experience to that of other platforms). The integration allows administrators to consume a global CDN for software delivery, without requiring the administrators to fully understand munki's inner workings and configuration.

In this exercise, you will enable the application catalog and deploy an Application to your device.

**Note:** All Workspace ONE UEM Console work for this section should be performed on a macOS device.

**Note:** Workspace ONE UEM also provides a second facility for delivering software/configurations and running scripts/commands on a macOS device. This method, known as Product Provisioning, is outside the scope of this exercise.

**Recommended Methods to Deliver Software**

Administrators can deliver software to macOS devices in numerous ways. As a quick reference, VMware recommends the following methods to deliver software to macOS devices:

- **MacOS App Store Application** — VMware recommends delivering any application that may be available on the macOS App Store be delivered as a "Purchased" application through the Volume Purchase Program. Apps should be assigned via device-based licenses and set to auto-update if the application is not business-critical.

- **Non-AppStore Applications** — Where possible, third-party applications which are not available through the app store should be delivered as an Internal Application (leveraging the AirWatch-Munki integration).

**Configure App Catalog**
On your macOS device, Open Safari by clicking the icon on the dock.

**View All Settings**

In the Workspace ONE UEM Console

1. Click on **Apps & Books**.
2. Click on **All Apps & Books Settings**.
Enable the Application Catalog

1. Expand **Workspace ONE**
2. Expand **AirWatch Catalog**
3. Click on **General**.
4. Click on the **Publishing** tab
5. Click **Override**
6. Enter the Catalog title as **App Catalog**
Select Platform as macOS and Save

1. Scroll down until you see the platform macOS.
2. Select **Enabled** for macOS.
3. Click on **Save**.
4. Scroll to the top and click on **X** to exit the pop-up screen.

Enable macOS Software Management

**NOTE:** The steps in this section have already been completed for you in the Hands-On Lab. You DO NOT need to Enable Software Management as it has already been completed on your behalf.

Prior to deploying a macOS Application, VMware AirWatch administrators must enable their environments for Software Management. The following items are pre-requisites for macOS Software Management:
1. For On-Premise Installations, "File Storage" must be enabled (Settings > Installation > File Path).
2. "Software Management" must be enabled (Settings > Devices & Users > Apple > Apple macOS > Software Management)
3. VMware AirWatch Agent for macOS version 3.0 (or newer)

### Access All Settings (FOLLOW ALONG)

![Screen capture showing access to All Settings]

**DO NOT** make the following configurations, they are shown only as an example of how to enable Software Management for macOS outside of the Hands on Labs environment!

1. Click Groups & Settings
2. Click All Settings
Enable File Storage (FOLLOW ALONG)

**Settings**

| ➔ System |
| ➔ Devices & Users |
| ➔ Apps |
| ➔ Content |
| ➔ Email |
| ➔ Telecom |
| ➔ Admin |
| ➔ Installation |

**File Storage Enabled**

1. **Ensure you are at the Global Organization Group unless your particular setup requires configuring at child Organization Groups.**
2. **Expand Installation**
3. **Click File Path**
4. **Scroll the file paths screen and click Enabled for File Storage Enabled**
5. **Enter the path of a file share accessible from your Device Services and Console servers.**
6. **Click Disabled for File Storage Caching Enabled unless you have planned and sized your Device Services server accordingly.**
7. **Click Enabled for File Storage Impersonation Enabled**
8. **Enter the username credentials to impersonate in order to access the file storage path**
9. **Enter the password for the impersonation user**
10. **Enter the password for the impersonation user**
11. **TEST CONNECTION**
12. **Connection Succeeded**
13. **SAVE**

**DO NOT** make the following configurations, they are shown only as an example of how to enable Software Management for macOS outside of the Hands on Labs environment!

1. Ensure you are at the **Global** Organization Group unless your particular setup requires configuring at child Organization Groups.
2. Expand **Installation**
3. Click **File Path**
4. Scroll the file paths screen and click **Enabled** for **File Storage Enabled**
5. Enter the path of a file share accessible from your Device Services and Console servers.
6. Click **Disabled** for **File Storage Caching Enabled** unless you have planned and sized your Device Services server accordingly.
7. Click **Enabled** for **File Storage Impersonation Enabled**
8. Enter the username credentials to impersonate in order to access the file storage path
9. Enter the password for the impersonation user
10. Confirm the password for the impersonation user
11. Click **Test Connection** and ensure you see **Connection Succeeded**
12. Click **Save**

**Enable Software Management**

DO NOT make the following configurations, they are shown only as an example of how to enable Software Management for macOS outside of the Hands on Labs environment!

1. Expand **Devices & Users**
2. Expand **Apple**
3. Expand **Apple macOS**
4. Click **Software Management**
5. Click **Override**
6. Click **Enabled** for **Enable Software Management**
7. Click **Save**
8. Ensure settings are **Saved Successfully**

**Prepare macOS Applications for Deployment**

In this section, you will download the VMware AirWatch Admin Assistant tool and use it to prepare another 3rd-Party application for deployment.
Open New Browser Tab

On your macOS device, Open a new Safari tab:

1. Within Safari, click **File**.
2. Click **New Tab**.

Download Skitch

1. Enter **https://evernote.com/products/skitch** in the URL bar. Press **ENTER**.
2. Click **Download for Mac**.
The zip file for Skitch will download to the Downloads folder.

**Download VMware AirWatch Admin Assistant Tool**

[Image: Link to VMware AirWatch Admin Assistant tool.

In the same tab as you downloaded Skitch, paste the link in Safari to download the VMware AirWatch Admin Assistant tool and press **ENTER** on the keyboard:

```
https://awagent.com/AdminAssistant/VMwareAirWatchAdminAssistant.dmg
```

The DMG file will download to the Downloads folder.

**Begin Installing VMware AirWatch Admin Assistant Tool**

On the dock, perform the following:

1. Click the **Downloads** folder (next to the Trash).
2. Click **VMwareAirWatchAdminAssistant.dmg**.

**Launch Installer Package**

[Image: VMware AirWatch Admin Assistant package.

```
Double-click the *VMware AirWatch Admin Assistant.pkg* file

**Continue Installer**

![Installer window with Continue button](image)

Click **Continue**
Review and Continue Installer

1. Review the License Agreement and click **Continue**
2. Click **Agree**.
Install Admin Assistant Tool

Click **Install**

**Enter Admin Credentials**

If prompted for administrative credentials, enter the credentials required to install.

1. Enter the **Administrator** as the Admin User Name on the macOS device
2. Enter the **VMware!** as the password for the admin user
3. Click **Install Software**

**Close the Installer**

1. Click **Close** when the installer completes
2. Click **Move to Trash** to clean up the installer
Launch VMware Admin Assistant Tool

1. Click the Launchpad on the Dock
2. Click **VMware AirWatch Admin Assistant**
1. Click the Downloads folder on the Dock (by the trash).
2. Click and Drag **Skitch**.
3. Drag and Drop **Skitch** onto the VMware AirWatch Admin Assistant app file upload section.

The VMware Admin Assistant Tool begins parsing the file to extract information necessary to deploy the software.
Monitor Process and Reveal Files

1. Monitor the progress of the parsing. When complete the wheel changes to a green checkmark.
2. In the pop-up window, click **Reveal in Finder**

Review Generated Files
In the Finder window:

1. Change to **Column** view
2. Note the Path of the Output for the Skitch files:  ~/Documents/VMware AirWatch Admin Assistant/Skitch-2.8.1
3. Note the output from the Assistant tool as described below:

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skitch-2.8.1.dmg</td>
<td>The Application has been packaged into a DMG file.</td>
</tr>
<tr>
<td></td>
<td>(Note: MPKG and PKG files will not be modified)</td>
</tr>
<tr>
<td>Skitch-2.8.1.plist</td>
<td>A metadata file (referenced as the pkginfo.plist in munki documentation)</td>
</tr>
<tr>
<td></td>
<td>which contains information used by the munki framework to determine how to</td>
</tr>
<tr>
<td></td>
<td>install/uninstall the software</td>
</tr>
<tr>
<td>Skitch.png</td>
<td>An icon image extracted from the app used for user-friendly display in the</td>
</tr>
<tr>
<td></td>
<td>console and Workspace ONE app for macOS</td>
</tr>
</tbody>
</table>

All output for the Admin Assistant tool follows the convention ~/Documents/VMware AirWatch Admin Assistant/{AppName-Version}. At the time this lab was created, Skitch was at version 2.8.1 but may be different depending on when you take this lab.

### Deploy a macOS Application

In Safari, Click on the tab labeled **Devices > Dashboard** to return to the Workspace ONE UEM Console.
View Native Internal Apps

1. Click on Apps & Books
2. Expand Applications
3. Click Native
4. Click Internal
5. Click Add Application

Begin Application File Upload

Add Application

Organization Group ID *

Application File *

Click Upload
Choose File

Add

Type  Local File  Link

Choose File  No file chosen

You have used 159 MB of 25000 MB

Click Choose File

Browse and Select Application File

1. Choose the Documents folder
2. Select **VMware AirWatch Admin Assistant**
3. Select **Skitch-{version}** (e.g. Skitch-2.8.1)
4. Select **Skitch-{version}.dmg**
5. Click **Choose**

**Save Local File**

Add

Type: [ ] Local File [ ] Link

Choose File: [ ] Skitch-{version}.dmg

You have used 159 MB of 25000 MB

Click **Save**

**Continue Adding Application**

Add Application

Organization Group ID: [ ]

Application File: [ ]

Click **Continue**
Upload Metadata File

Add Application

Application File

Skitch-2.8.1.dmg

This file is only eligible for full software lifecycle management. Click here for more info

1. Additional metadata is required to configure full software lifecycle management for this file.

   Download and install the VMware AirWatch Admin Assistant Tool to generate a metadata file (.plist), then upload the metadata file once complete. Click here for more info

Generate Metadata

[VMware AirWatch Assistant for macOS]

Metadata File *

UPLOAD

1. Note the link to directly download the VMware AirWatch Assistant (in case you forgot to generate the metadata file and are working from a computer where the VMware AirWatch Assistant is not installed).

2. Click Upload

Choose File

Add

Choose File

no file selected

Click Choose File
Browse and Select Plist File

1. Choose the **Documents** folder
2. Select **VMware AirWatch Admin Assistant**
3. Select **Skitch-{version}** (e.g. Skitch-2.8.1)
4. Select **Skitch-{version}.plist**
5. Click **Choose**

Save Plist File

Add

Choose File  Skitch...1.plist

SAVE  CANCEL
Click **Save**

**Continue Adding Application**

**Add Application**

1. **Application File**: Skitch 2.8.1.dmg

   This file is only eligible for full software lifecycle management. [Click here for more info](#)

   - Additional metadata is required to configure full software lifecycle management for this file.
   - Download and Install the VMware AirWatch Admin Assistant Tool to generate a metadata file (.plist), then upload the metadata file once complete. [Click here for more info](#)

2. **Generate Metadata**: [VMware AirWatch Assistant for macOS](#)

3. **Metadata File**: Skitch-2.8.1.plist

   - [UPLOAD]

   **CONTINUE** [CANCEL]

1. Note the Application File is shown
2. Note the Plist File is shown
3. Click **Continue**
Add Image File

1. Click on the **Images** tab
2. Click on **Click or Drag Files Here**
Browse and Select Image File

1. Choose the **Documents** folder
2. Select **VMware AirWatch Admin Assistant**
3. Select **Skitch-{version}** (e.g. Skitch-2.8.1)
4. Select **{App Name}.png** (e.g. Skitch.png)
5. Click **Choose**
Review Scripts Tab
Configure scripts to run for Installation, Uninstallation, or Verification. Click here for more info

Install Scripts

Define a pre-install script to run before attempting to install and/or a post-install script to run after a successful installation.

1. Pre-Install Script
2. Post Install Script

Uninstall Scripts

Define a Pre-Uninstall script to run before an attempted uninstall and/or define a Post-Uninstall script to run after a successful uninstall. Uninstall Method should be automatically selected by default from the uploaded metadata. To override the default, select from dropdown and customize the behavior of the uninstallation procedure.

3. Pre-Uninstall Script
4. Post Uninstall Script
5. Uninstall Method: Remove Copied Items

Verification Scripts

Define an Install/Uninstall Check Script to determine if an item needs to be installed/uninstalled. The script should return an exit code of 0 to trigger the action, otherwise it will be skipped.

7.
1. Click the **Scripts** tab
2. The *Pre-Install Script* runs BEFORE the AirWatch Agent executes the dmg/pkg/mpkg file that installs the Application and can be used to set-up pre-requisite items before the installer runs. The Pre-install Script must have an exit code of zero (0) in order for the install to proceed.
3. The *Post-Install Script* runs AFTER the AirWatch Agent executes the dmg/pkg/mpkg file. This can be useful for applying configurations after the software completes the installation.
4. The *Pre-Uninstall Script* runs BEFORE the AirWatch Agent initiates the uninstall. The Pre-Uninstall script must have an exit code of zero (0) in order for the uninstall to proceed.
5. The *Uninstall Method* defines how the AirWatch Agent uninstalls software. Typically, "Remove Copied Items" is used for a DMG installer, and "Remove Packages" is used for a PKG installer.
6. The *Post-Uninstall Script* provides a method to validate an uninstall was completed and potentially handle any cleanup for the uninstall.
7. The *Install Check* script assists the AirWatch Agent with determining whether an install needs to happen. This script can be useful for "desired state" purposes and ensuring that a software install remains intact on a user's machine. If the script has an exit code of zero (0), the agent assumes an Install is needed.
8. The *Uninstall Check Script* validates whether an uninstall has occurred. If the script has an exit code of zero (0), the airwatch agent determines an uninstall is (or is still) required.

Use the pre and post install scripts to avoid repackaging installers. By including scripts, you can automate tasks that would normally be prompted for the user to resolve before/after an install. More info can be found in the munki Wiki: [https://github.com/munki/munki/wiki/Pre-And-Postinstall-Scripts](https://github.com/munki/munki/wiki/Pre-And-Postinstall-Scripts)

Scripts must include the shebang (#!) statement on the first line. Examples include the following:

```
#!/bin/bash
#!/bin/sh
#!/usr/bin/python
```
Review Deployment Tab

1. Click the Deployment tab
2. Note the different Restart actions
3. Note the section to include conditions which can further constrain the deployment.

For more information about Conditions, refer to the munki wiki: [https://github.com/munki/munki/wiki/Conditional-Items](https://github.com/munki/munki/wiki/Conditional-Items)

Review Terms of Use and Save Application

1. Click Terms of Use
2. Review the ability to add terms of use to a software title.
3. Click Save & Assign
Add Assignment

Skitch - Update Assignment

<table>
<thead>
<tr>
<th>Assignments</th>
<th>Exclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Devices will receive application based on the below configuration.
In the case where devices belong to multiple groups, they will receive policies from the grouping with highest priority (0 being highest priority).

Add Assignment

<table>
<thead>
<tr>
<th>Name</th>
<th>Priority</th>
<th>App Delivery Method</th>
<th>Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No Records Found

Click **Add Assignment**
1. For the Assignment Group, enter **All Devices** and select the **All Devices (your@email.shown.here)** group.
2. Click **Auto** for App Delivery Method
3. Click **Enabled** for Remove on Unenroll
4. Click **Add**
Save and Publish

1. Ensure your recently added Assignment shows in the list of Assignments
2. Click **Save & Publish**

Publish the Application

Click **Publish**
Review Published Application Information

Review the newly published application.

Validate Application Install

With the macOS device enrolled, the published application should begin downloading and installing immediately. This sections shows how you can manually validate the application is installing and/or installed.

Check the Agent Status

1. Click the Workspace ONE shield in the menu bar.
2. As the agent processes application installs, you will see a note about "Handling Application Updates." Depending on the speed of your connection, the agent may finish processing the install before you have a chance to see the status on the menu bar applet.
In a Workspace ONE UEM environment integrated with VMware Identity Manager, the end-user will see more verbose installation feedback from within the macOS native Workspace ONE application. Feedback using this method is outside the scope of this lab.

**Launch Terminal**

1. Click the **LaunchPad** on the Dock
2. Begin typing **terminal** to filter the LaunchPad apps
3. Click **Terminal**
1. Tail the ManagedSoftwareUpdate.log file by running the command line below. Note - the "-F" parameter means the tail command will continually monitor the file for updates (displaying progress as the software installation continues).

```
tail -n 20 -F /Library/Application\ Support/AirWatch/Data/Munki/Managed\ Installs/Logs/ManagedSoftwareUpdate.log
```

2. Look for a line in the results stating Skitch version [version] (or newer) is already installed. This indicates the software has been installed.

The VMware agent initiates a Managed Software Update within the munki framework multiple times. Depending on where the agent is within the process of the install the tail command may output lines similar to the following:

```
[Date/Time] Need to install Skitch
[Date/Time] Downloading Skitch-2.8.1.dmg from Skitch-2.8.1.dmg
[Date/Time] The following items will be installed or upgraded:
[Date/Time]   + Skitch-2.8.1
[Date/Time] Processing installs
[Date/Time] Installing Skitch (1 of 1)
[Date/Time] Mounting disk image Skitch-2.8.1.dmg
[Date/Time] The software was successfully installed.
```
Check for App in the Launchpad

1. Click the Launchpad icon on the Dock
2. Check for the existence of the **Skitch** application

View the Application Status in the AirWatch Application Catalog

1. Click on the **Application Catalog weblink** on the Dock
2. Note the Installation Status for **Skitch**.
Key Takeaways

- macOS Applications can be deployed using the munki framework (Internal Application) or a detailed manifest of scripts and packages (Product Provisioning - not covered in this lab).
- Detailed status on installation progress is delivered to the end-user via the Workspace ONE native application for macOS (not covered in this lab).
- AirWatch provides an Application Catalog to allow user and device specific self-service requests for application installation.
Managing macOS Custom Attributes

Custom attributes enable administrators to extract particular values from a managed device and return it to the Workspace ONE UEM Console. This can be particularly useful for device configuration auditing and Product sequencing.

Custom Attributes

Custom attributes are key-value pairs. These key value pairs are generated by scripting/commands which execute on the device and whose values are returned to the console through the Workspace ONE UEM Agent. The scripts/commands are delivered to the device using a custom attributes payload in a profile. The profile also allows scheduling of the script/command to re-occur on a schedule or based on an event. Additionally, custom attribute payloads execute in the root context on the device, which allows you to gather information about the device without requiring the enrolled user to have Administrative permissions.

Custom Attribute Profiles

Previously, custom attributes were sent to the console by creating a shell script to write values to a specific Plist file monitored by the agent. In AirWatch 8.2 and later, this functionality is now included as a profile and adds additional features such as scheduling.

Create Custom Attribute Profile

In the Workspace ONE UEM console:
1. Select **Devices**.
2. Select **Profiles & Resources**.
3. Select **Profiles**.
4. Select **Add**
5. Select **Add Profile**.

### Select Profile Platform

**Add Profile**

Select a platform to start:

- **Android**
- **iOS** (Apple iOS)
- **macOS** (Apple macOS)

Select the **macOS** icon.

### Select the Profile Context

**Select Context**

- **User Profile**
- **Device Profile**

Select the **Device Profile** icon.
Configure General Profile Settings

1. Select General if it is not already selected.
2. Enter macOS Device Custom Attributes in the Name text box.
3. Copy the profile name into the Description text box.
4. Ensure the Assignment Type is set to Auto.
5. Click in the Assigned Groups field. This will pop-up the list of created Assignment Groups. Enter All Devices and select the All Devices (your@email.shown.here) Assignment Group.

Note: You may need to scroll down to find the Assigned Groups field.

Note: You DO NOT need to click Save or Save & Publish at this point. This interface allows you to move around to different payload configuration screens before saving.
Configure Custom Attributes Payload

1. Scroll down the list of Payload Types on the left menu.
2. Select **Custom Attributes**.
3. Click **Configure**.
Enter Local Host Name Custom Attribute Command

1. Enter \texttt{LocalHostName} as the Attribute Name
2. Enter the following command: 
   \texttt{/usr/sbin/scutil --get LocalHostName}  
   Be sure to use the correct slash, two hyphens, and proper capitalization.
3. Select \texttt{1 Hour} as the Reporting
4. Click \texttt{Save & Publish}.

---

**macOS Add a New Apple macOS Profile**

- **Custom Attributes**
  - **Attribute Name**: LocalHostName
  - **Script/Command**: /usr/sbin/scutil --get LocalHostName
  - **Execution Interval**: SCHEDULE
  - **Report Every**: 1 Hour

---

**HOL-1957-05-UEM**

Page 149
Click **Publish**.

**Locating Custom Attributes**

After Workspace ONE UEM delivers a custom attributes profile/payload to a device, the agent will report the initial value of the Custom Attribute back to Workspace ONE UEM and begin the Schedule or Event monitoring. Custom attribute values that have been reported back to the console can be viewed in the device details.
Access Device List View

1. Select **Devices**.
2. Select **List View**.

**Select Your Device**

![Device Details]

- **User**: [User Name] (Email: user@email.stripped.here)
- **Device Details**: MacBook Pro "Core i7" 15"
  - **Model**: Apple macOS
  - **OS**: 10.12.1
  - **MDM Profile**: Corporate - Dedicated

Select your device.
Access Custom Attributes

1. Select **More**.
2. Select **Custom Attributes**.
Review Custom Attributes

1. Notice that the Source of the attributes is **Device Sourced**—this means the data was gathered from the device and sent to Workspace ONE UEM.
2. Note the list of Attributes.
3. Note the value of each Attribute. These values were generated by the output of your command/script in the Custom Attributes payload.
Enterprise Wipe a macOS Device

An Enterprise Wipe removes corporate data that was added to the device while leaving personal data intact.

View Device List

In the Workspace ONE UEM Console:

1. Select Devices
2. Select List View.
3. Select your macOS device in the List View to view details.
Initiate Enterprise Wipe

1. From the toolbar in the device details header, select **More Actions**.
2. Select **Enterprise Wipe** under the **Management** header in the drop-down menu.

Enter Security PIN to Confirm Wipe

Enter Security PIN:

1 2 3 4

Forgot Security PIN?

Cancel
1. Scroll down until you see the section to Enter Security PIN.
2. Enter your security PIN 1234 to initiate the Enterprise Wipe.
Validate the Enterprise Wipe on the macOS Device

1. On your device, select the Apple icon in the upper-left corner.
2. Select *System Preferences*. 
Verify Removal of System Preference Restrictions

Note you can now make modifications to **Energy Saver** and **Bluetooth** because the restriction created earlier has been removed.
1. Open Finder (Smiley Face) on the dock and select **Go**.
2. Select **Applications**.
3. Confirm that **Feedly** has been removed from your device.

On your device, also note that the dock preferences have been removed and the dock has returned to its original position.

**Note:** Due to network limitations, you may need to wait several minutes after un-enrolling before the Feedly application is removed and the dock is returned to the original position.
Conclusion

This lab covered basic macOS administration using AirWatch. You enrolled your macOS device, created profiles, deployed an application, locked the device, used Custom Attributes and then enterprise wiped the content and settings from the device.

For more information, please register for a free account at https://my.air-watch.com (My AirWatch) in order to access AirWatch Academy and our Resources page. There you will find courses and documentation that can help you with advanced topics in macOS management, such as:

- Device Enrollment Program
- Device Staging and Enroll-on-Behalf
- Application Volume Purchase Program
- Kiosk Mode
- Certificates and Identity/Directory Integration
- Mail Integration
- Product Provisioning
- ... and More!

This concludes the Basic Apple macOS Management module.
Introduction

In this lab module, we will explore Workspace ONE features and concepts related to software distribution for the macOS platform. This lab will give you a better understanding of the software distribution options you have available, and what use cases are targeted by each deployment method.

Before you can start the lab, make sure you review the next page to ensure you can successfully complete the lab.

Pre-Requisites

To successfully complete this Hands-On Lab, you'll need to ensure you have the following pre-requisites:

- An Apple device running macOS version 10.13.5 (High Sierra) or later.
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
- What was your childhood nickname? (2)

Password Recovery Question *
- VMware1! (3)

Password Recovery Answer *
- VMware1! (4)

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 (5)

Confirm Security PIN *
- 1234 (6)

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

[Check] 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.
Installing the Workspace ONE Intelligent Hub

In this exercise, download and install the Workspace ONE Intelligent Hub on your macOS device.

Log In to the MacBook - If Needed

Login to the macOS device. If you are using a VMworld provided device, the login details are below.

1. Enter administrator for the username.
2. Enter VMware1! for the password.
3. Press the continue button or press ENTER.
Download the Workspace ONE Intelligent Hub

Click the Safari icon (blue compass) to open the Safari browser.

Initiate Download

1. Enter https://www.getwsone.com in the URL field, then press ENTER.
2. Click Download Hub for macOS. The Workspace ONE Intelligent Hub installer begins to download and will save to the downloads folder by default.
1. Click the **Downloads** folder in the dock (next to the Trash Bin).
2. Click the **VMwareWorkspaceONEIntelligentHub.pkg** file to begin the installer.
Continue at Introduction Screen

Click **Continue**.
Continue and Agree to Terms

1. On the License page, click **Continue**.
2. Click **Agree** (to the license terms).
Provide Credentials for the Installer

1. Click **Install**. You are now prompted to enter the computer's administrator credentials.
2. Enter **administrator** in the Name field.
3. Enter **VMware1!** in the Password field.
4. Click the **Install Software** button.
Close and Move to Trash

1. Click **Close** when the installer finishes.
2. Click **Move to Trash** to move the installer to the trash.
Enroll a macOS Device

In this exercise, you enroll a macOS device into Workspace ONE UEM. Enrollment is the action that brings a device under management and control by Workspace ONE UEM. There are a number of ways to enroll the various platforms (macOS included), but for this exercise we cover a basic enrollment scenario.

Enroll the macOS Device

This enrollment flow is considered *User-Approved* per the functionality introduced in macOS High Sierra.

Begin macOS Enrollment Process

The Enrollment Wizard should start automatically. From within the Enrollment wizard window, click **Server Detail**.
**Note:** The Enrollment Wizard may take several minutes to launch. If you do not see the Enrollment Wizard immediately, be patient and wait for it to appear.

**Enter Enrollment Server Details**

1. Enter `labs.awmdm.com` for your Server URL.

2. Enter your Group ID.

3. Continue.
2. Enter your **Group ID**. This was documented in the previous steps titled **Retrieve Your Group ID**.
3. Click the **Continue** button.

### Enter Enrollment Credentials

1. Enter **testuser** for the enrollment staging username.
2. Enter **VMware1!** for the password.
3. Click the **Continue** button.
Enable Device Management

You are now ready to configure your device!

To complete this process, follow the System Preferences prompts and enter your computer password when prompted.

Click **Enable** to enable device management.
Install Device Manager Profile

Click **Install**.

Install Profile for User-Approved Enrollment

Click **Install**.
Enter Administrative Credentials for Profile Install

When prompted, enter the credentials for the macOS device.

1. Enter **administrator** for the username.
2. Enter **VMware1!** for the password.
3. Click **OK**.
Quit Profiles Preference Panel

Click the **Close** button (red dot) to close the Profiles panel.
Quit the Enrollment Wizard

Congratulations!

Your device has been successfully enrolled!

You now have secure access to your corporate resources.

You may Quit to exit this installer or view your enrollment status by opening the Agent.

Click Quit when the installation completes.
Validate Mac Enrollment

Follow the next steps to verify that the Mac has been successfully enrolled.

In upper-right corner:

1. Note the shield icon in the menu bar. Click the AirWatch Agent icon.
2. Note the menu shows your device as Enrolled.
3. Click Preferences and review the options available to you in the agent.

Key Takeaways

- Agent-based macOS enrollment is streamlined and intuitive.
- Workspace ONE UEM supports a number of enrollment methods for macOS devices: web-based, agent-based, staged (pre-installed agent), enrollment on-behalf, and enrollment using the Apple Device Enrollment Program.
- Agent logs can be collected directly from the Workspace ONE Intelligent Hub. This eases helpdesk troubleshooting by allowing end-user to quickly send diagnostic information to helpdesk and/or administrative users.
Software Distribution Methods

Workspace ONE UEM supports a few different methods for delivering software to managed macOS devices. The distribution method you choose is highly dependent upon the type of software you wish to choose. This section is simply an overview of each different method and the caveats associated with each method.

Software Distribution encompasses delivery of a few different classes or types of software:

- Applications delivered from the macOS App Store
- Applications delivered by 3rd-Parties outside the App Store
- Scripts (such as Python or Shell scripts)

**NOTE:** Script deployment is outside the scope of this lab and will be included in a later release of the lab.
Workspace ONE UEM has supported application deployment from the macOS App Store via the Volume Purchase Program (VPP) for a number of releases. This support has also extended to VPP apps purchased through Apple School Manager (and now Apple Business Manager - shown above). In this case, Administrators may purchase licenses for macOS App Store applications and distribute them to users via device-based licensing. This allows administrators to deploy these apps to devices, without the need for the user to have an Apple ID.

Some applications that are commonly deployed this way include (but are not limited to):

- xCode
- Slack
- Microsoft Remote Desktop
- Pages, Numbers, etc (Apple's iWork suite)
- TextWrangler
- F5 Access (VPN)
3rd-Party Non-Store Applications

Workspace ONE UEM has also supported 3rd-Party Non-Store application deployment for a number of releases. Previous to Workspace ONE UEM (or AirWatch) 9.3, the primary method of deploying non-store applications was to use the Products engine. With the release of version 9.3 (and macOS Agent 3.0), Workspace ONE UEM included functionality to perform application install/uninstall using a built-in integration with the open-source framework Munki. You can optionally pair the munki integration with Workspace ONE UEM's CDN integration to enable in-region delivery of these non-store apps to the endpoint.
VMware has put considerable effort into making this integration "consumer simple" for admins which are new to Munki and/or macOS as a platform. This ensures administrators which are not experienced with Munki do not need to learn the framework to leverage its features and functionality.

Some applications that are commonly deployed this way include (but are not limited to):

- Adobe Creative Suite
- Microsoft Office 2016 for macOS
- BlueJeans
- Camtasia
- Audacity

Content Delivery Network (CDN) integration (via Akamai) is enabled by default for Workspace ONE UEM SaaS customers.
VIDEO: Deploying macOS Volume-Purchased Apps

Workspace ONE UEM has built-in support for Apple's Volume Purchase Program (including apps purchased in bulk via Apple School Manager and Apple Business Manager). In this section, you can view a video that demonstrates how content managers can purchase app licenses in Apple School Manager, then assign them to enrolled devices in Workspace ONE UEM.
Deploying macOS Applications via Internal Applications (using Munki)

VMware AirWatch recently announced integration with the Open-Sourced "munki" project for 3rd-party application management on enrolled macOS devices. With this integration, administrators can now manage 3rd-party (non-AppStore) software using the "internal apps" view (closer aligning the admin experience to that of other platforms). The integration allows administrators to consume a global CDN for software delivery, without requiring the administrators to fully understand munki’s inner workings and configuration.

In this exercise, you will enable the application catalog and deploy an Application to your device.

**NOTE - All AirWatch Management Console work for this section should be performed on a MacOS device.**

Recommended Methods to Deliver Software

As mentioned in the introduction to this section, administrators can deliver software to macOS devices in numerous ways. As a quick reference, VMware recommends using the following methods to deliver software to macOS devices:

- **MacOS App Store Applications**: VMware recommends delivering any application that may be available on the macOS App Store be delivered as a "Purchased" application through the Volume Purchase Program. Apps should be assigned via device-based licenses and set to auto-update if the application is not business-critical.
- **Non-AppStore Applications**: As much as possible, 3rd-Party applications which are not available through the app store should be delivered as an Internal Application (leveraging the AirWatch-Munki integration).

Configure App Catalog

On your macOS device, Open Safari by clicking the icon on the dock.
In the Workspace ONE UEM Console

1. Click on **Apps & Books**.
2. Click on **All Apps & Books Settings**.
Enable the Application Catalog

1. Click on **Apps**
2. Expand **Workspace ONE**
3. Expand **AirWatch Catalog**
4. Click on **General**
5. Click on the **Publishing** tab
6. Click **Override**
7. Enter the Catalog title as **App Catalog**
Select Platform as macOS and Save

1. Scroll down until you see the platform macOS.
2. Select Enabled for macOS.
3. Click on Save.
4. Scroll to the top and click on X to exit the pop-up screen.
Enable macOS Software Management

**NOTE:** The steps in this section have already been completed for you in the Hands-On Lab. You DO NOT need to Enable Software Management as it has already been completed on your behalf.

Prior to deploying a macOS Application, VMware AirWatch administrators must enable their environments for Software Management. The following items are pre-requisites for macOS Software Management:

1. For On-Premise Installations, "File Storage" must be enabled (Settings > Installation > File Path).
2. "Software Management" must be enabled (Settings > Devices & Users > Apple > Apple macOS > Software Management)
3. VMware AirWatch Agent for macOS version 3.0 (or newer)
Access All Settings (FOLLOW ALONG)

DO NOT make the following configurations, they are shown only as an example of how to enable Software Management for macOS outside of the Hands on Labs environment!

1. Click Groups & Settings
2. Click All Settings
Enable File Storage (FOLLOW ALONG)

**Settings**

1. Ensure you are at the **Global** Organization Group unless your particular setup requires configuring at child Organization Groups.
2. Expand **Installation**
3. Click **File Path**
4. Scroll the file paths screen and click **Enabled** for **File Storage Enabled**
5. Enter the path of a file share accessible from your Device Services and Console servers.
6. Click **Disabled** for **File Storage Caching Enabled** unless you have planned and sized your Device Services server accordingly.
7. Click **Enabled** for **File Storage Impersonation Enabled**
8. Enter the username credentials to impersonate in order to access the file storage path.
9. Enter the password for the impersonation user.
10. Click **TEST CONNECTION**
11. Connection Succeeded
12. **SAVE**

**DO NOT** make the following configurations, they are shown only as an example of how to enable Software Management for macOS outside of the Hands on Labs environment!
10. Confirm the password for the impersonation user
11. Click **Test Connection** and ensure you see *Connection Succeeded*
12. Click **Save**

**Enable Software Management**

1. Expand **Devices & Users**
2. Expand **Apple**
3. Expand **Apple macOS**
4. Click **Software Management**
5. Click **Override**
6. Click **Enabled** for *Enable Software Management*
7. Click **Save**
8. Ensure settings are *Saved Successfully*

**DO NOT** make the following configurations, they are shown only as an example of how to enable Software Management for macOS outside of the Hands on Labs environment!

1. Expand **Devices & Users**
2. Expand **Apple**
3. Expand **Apple macOS**
4. Click **Software Management**
5. Click **Override**
6. Click **Enabled** for *Enable Software Management*
7. Click **Save**
8. Ensure settings are *Saved Successfully*

**Prepare macOS Applications for Deployment**

In this section, you will download the VMware AirWatch Admin Assistant tool and use it to prepare another 3rd-Party application for deployment.
Open New Browser Tab

On your macOS device, Open a new Safari tab:

1. Within Safari, click **File**.
2. Click **New Tab**.

Download Skitch

2. Click **Download for Mac**.

Skitch

Get your point across with fewer words using annotation, shapes and sketches, so that your ideas become reality faster.

Designed for Mac, iPad, and iPhone:

![Download on the Mac App Store](https://www.evernote.com/products/skitch/mac-app-store-badge.png)
The zip file for Skitch will download to the Downloads folder.

**Download VMware AirWatch Admin Assistant Tool**

![Download Link](https://awagent.com/AdminAssistant/VMwareAirWatchAdminAssistant.dmg)

In the same tab as you downloaded Skitch, paste the link in Safari to download the VMware AirWatch Admin Assistant tool and press **ENTER** on the keyboard:

https://awagent.com/AdminAssistant/VMwareAirWatchAdminAssistant.dmg

The DMG file will download to the Downloads folder.

**Begin Installing VMware AirWatch Admin Assistant Tool**

On the dock, perform the following:

1. Click the **Downloads** folder (next to the Trash).
2. Click **VMwareAirWatchAdminAssistant.dmg**.

**Launch Installer Package**

![Installer Package]
Double-click the **VMware AirWatch Admin Assistant.pkg** file

**Continue Installer**

![Installer Screen]

Click **Continue**
1. Review the License Agreement and click **Continue**
2. Click **Agree**.
Install Admin Assistant Tool

Click Install

Enter Admin Credentials

If prompted for administrative credentials, enter the credentials required to install.

1. Enter the **Administrator** as the Admin User Name on the macOS device
2. Enter the **VMware1!** as the password for the admin user
3. Click **Install Software**

**Close the Installer**

1. Click **Close** when the installer completes
2. Click **Move to Trash** to clean up the installer
Launch VMware Admin Assistant Tool

1. Click the Launchpad on the Dock
2. Click **VMware AirWatch Admin Assistant**
Drag and Drop Skitch

1. Click the Downloads folder on the Dock (by the trash).
2. Click and Drag Skitch.
3. Drag and Drop Skitch onto the VMware AirWatch Admin Assistant app file upload section.

The VMware Admin Assistant Tool begins parsing the file to extract information necessary to deploy the software.
Monitor Process and Reveal Files

1. Monitor the progress of the parsing. When complete the wheel changes to a green checkmark.
2. In the pop-up window, click **Reveal in Finder**

Review Generated Files
In the Finder window:

1. Change to **Column** view
2. Note the Path of the Output for the Skitch files: ~/Documents/VMware AirWatch Admin Assistant/Skitch-2.8.1
3. Note the output from the Assistant tool as described below:

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skitch-2.8.1.dmg</td>
<td>The Application has been packaged into a DMG file. (Note: MPKG and PKG files will not be modified)</td>
</tr>
<tr>
<td>Skitch-2.8.1.plist</td>
<td>A metadata file (referenced as the pkginfo.plist in munki documentation) which contains information used by the munki framework to determine how to install/uninstall the software</td>
</tr>
<tr>
<td>Skitch.png</td>
<td>An icon image extracted from the app used for user-friendly display in the console and Workspace ONE app for macOS</td>
</tr>
</tbody>
</table>

All output for the Admin Assistant tool follows the convention ~/Documents/VMware AirWatch Admin Assistant/{AppName-Version}. At the time this lab was created, Skitch was at version 2.8.1 but may be different depending on when you take this lab.

**Deploy a macOS Application**

In Safari, Click on the tab labeled **Devices > Dashboard** to return to the Workspace ONE UEM Console.
View Native Internal Apps

1. Click on **Apps & Books**
2. Expand **Applications**
3. Click **Native**
4. Click **Internal**
5. Click **Add Application**

Begin Application File Upload

Add Application

- Organization Group ID * 
  - your@email.shown.here
- Application File *

Click **Upload**
Choose File

Add

Type  Local File  Link

Choose File  No file chosen

You have used 159 MB of 25000 MB

Click Choose File

Browse and Select Application File

1. Choose the Documents folder
2. Select **VMware AirWatch Admin Assistant**
3. Select **Skitch-{version}** (e.g. Skitch-2.8.1)
4. Select **Skitch-{version}.dmg**
5. Click **Choose**

### Save Local File

Add

- **Type**: Local File

Choose File  

Skitch-2.8.1.dmg

You have used 159 MB of 25000 MB

Click **Save**

### Continue Adding Application

Add Application

- **Organization Group ID**: your@email.shown.here
- **Application File**: Skitch-2.8.1.dmg

Click **Continue**
Upload Metadata File

Add Application

Application File

This file is only eligible for full software lifecycle management. Click here for more info

Additional metadata is required to configure full software lifecycle management for this file.

Download and install the VMware AirWatch Admin Assistant Tool to generate a metadata file (.plist), then upload the metadata file once complete. Click here for more info

Generate Metadata

VMware AirWatch Assistant for macOS

Metadata File *

1. Note the link to directly download the VMware AirWatch Assistant (in case you forgot to generate the metadata file and are working from a computer where the VMware AirWatch Assistant is not installed).

2. Click Upload

Choose File

Add

Choose File

Click Choose File
Browse and Select Plist File

1. Choose the Documents folder
2. Select VMware AirWatch Admin Assistant
3. Select Skitch-{version} (e.g. Skitch-2.8.1)
4. Select Skitch-{version}.plist
5. Click Choose

Save Plist File

Add

Choose File Skitch-...1.plist

SAVE CANCEL
Click **Save**

**Continue Adding Application**

**Add Application**

1. Note the Application File is shown
2. Note the Plist File is shown
3. Click **Continue**
Add Image File

macOS

Edit Application - Skitch

Internal | Managed By: your@email.shown.here | Application ID: com.vmware.macos.Skitch | App ...

Details | Files | Images | Scripts | Deployment | Terms of Use

1. Click on the Images tab
2. Click on Click or Drag Files Here
Browse and Select Image File

1. Choose the **Documents** folder
2. Select **VMware AirWatch Admin Assistant**
3. Select **Skitch-{version}** (e.g. Skitch-2.8.1)
4. Select **{App Name}.png** (e.g. Skitch.png)
5. Click **Choose**
Review Scripts Tab
Configure scripts to run for Installation, Uninstallation, or Verification. Click here for more info

### Install Scripts

1. Define a pre-install script to run before attempting to install and/or a post-install script to run after a successful installation.

   - **Pre-Install Script**
   - **Post Install Script**

### Uninstall Scripts

1. Define a Pre-Uninstall script to run before an attempted uninstall and/or define a Post-Uninstall script to run after a successful uninstall. Uninstall Method should be automatically selected by default from the uploaded metadata. To override the default, select from dropdown and customize the behavior of the uninstallation procedure.

   - **Pre-Uninstall Script**
   - **Uninstall Method**: Remove Copied Items
   - **Post Uninstall Script**

### Verification Scripts

1. Define an Install/Uninstall Check Script to determine if an item needs to be installed/uninstalled. The script should return an exit code of 0 to trigger the action, otherwise it will be skipped.
1. Click the **Scripts** tab
2. The **Pre-Install Script** runs BEFORE the AirWatch Agent executes the dmg/pkg/ mpkg file that installs the Application and can be used to set-up pre-requisite items before the installer runs. The Pre-install Script must have an exit code of zero (0) in order for the install to proceed.
3. The **Post-Install Script** runs AFTER the AirWatch Agent executes the dmg/pkg/ mpkg file. This can be useful for applying configurations after the software completes the installation.
4. The **Pre-Uninstall Script** runs BEFORE the AirWatch Agent initiates the uninstall. The Pre-Uninstall script must have an exit code of zero (0) in order for the uninstall to proceed.
5. The **Uninstall Method** defines how the AirWatch Agent uninstalls software. Typically, "Remove Copied Items" is used for a DMG installer, and "Remove Packages" is used for a PKG installer.
6. The **Post-Uninstall Script** provides a method to validate an uninstall was completed and potentially handle any cleanup for the uninstall.
7. The **Install Check** script assists the AirWatch Agent with determining whether an install needs to happen. This script can be useful for "desired state" purposes and ensuring that a software install remains intact on a user's machine. If the script has an exit code of zero (0), the agent assumes an Install is needed.
8. The **Uninstall Check Script** validates whether an uninstall has occurred. If the script has an exit code of zero (0), the airwatch agent determines an uninstall is (or is still) required.

Use the pre and post install scripts to avoid repackaging installers. By including scripts, you can automate tasks that would normally be prompted for the user to resolve before/after an install. More info can be found in the munki Wiki: [https://github.com/munki/munki/wiki/Pre-And-Postinstall-Scripts](https://github.com/munki/munki/wiki/Pre-And-Postinstall-Scripts)

Scripts must include the shebang (#!) statement on the first line. Examples include the following:

```
#!/bin/bash
#!/bin/sh
#!/usr/bin/python
```
Review Deployment Tab

1. Click the **Deployment** tab
2. Note the different **Restart** actions
3. Note the section to include conditions which can further constrain the deployment.

For more information about Conditions, refer to the munki wiki:  [https://github.com/munki/munki/wiki/Conditional-Items](https://github.com/munki/munki/wiki/Conditional-Items)

Review Terms of Use and Save Application

1. Click **Terms of Use**
2. Required Terms of Use: **None**
3. No terms of use selected

1. Click **Terms of Use**
2. Review the ability to add terms of use to a software title.
3. Click **Save & Assign**
Add Assignment

Skitch - Update Assignment

<table>
<thead>
<tr>
<th>Assignments</th>
<th>Exclusions</th>
</tr>
</thead>
</table>

Devices will receive application based on the below configuration.
In the case where devices belong to multiple groups, they will receive policies from the grouping with highest priority (0 being highest priority).

<table>
<thead>
<tr>
<th>Name</th>
<th>Priority</th>
<th>App Delivery Method</th>
<th>Effective</th>
</tr>
</thead>
</table>

No Records Found

Click Add Assignment
Select Assignment Group and Add

1. For the Assignment Group, enter [All Devices](your@email.shown.here) and select the All Devices (your@email.shown.here) group.
2. Click Auto for App Delivery Method
3. Click Enabled for Remove on Unenroll
4. Click Add
Save and Publish

Skitch - Update Assignment

Devices will receive application based on the below configuration. In the case where devices belong to multiple groups, they will receive policies from the grouping with highest priority (0 being highest priority).

1. Ensure your recently added Assignment shows in the list of Assignments
2. Click **Save & Publish**

Publish the Application

Preview Assigned Devices

Click **Publish**
Review Published Application Information

Native

Validate Application Install

With the macOS device enrolled, the published application should begin downloading and installing immediately. This section shows how you can manually validate the application is installing and/or installed.

Check the Agent Status

1. Click the Workspace ONE shield in the menu bar.
2. As the agent processes application installs, you will see a note about "Handling Application Updates." Depending on the speed of your connection, the agent may finish processing the install before you have a chance to see the status on the menu bar applet.
In a Workspace ONE UEM environment integrated with VMware Identity Manager, the end-user will see more verbose installation feedback from within the macOS native Workspace ONE application. Feedback using this method is outside the scope of this lab.

**Launch Terminal**

1. Click the **LaunchPad** on the Dock
2. Begin typing **terminal** to filter the LaunchPad apps
3. Click **Terminal**
Review ManagedSoftwareUpdate Log

1. Tail the ManagedSoftwareUpdate.log file by running the command line below. Note - the "-F" parameter means the tail command will continually monitor the file for updates (displaying progress as the software installation continues).

```
tail -n 20 -F /Library/Application\ Support/AirWatch/Data/Munki/Managed\ Installs/Logs/ManagedSoftwareUpdate.log
```

The VMware agent initiates a Managed Software Update within the munki framework multiple times. Depending on where the agent is within the process of the install the tail command may output lines similar to the following:

```
Apr 27 2018 11:09:33 -0700 Skitch version 2.8.1 (or newer) is already installed.
```

2. Look for a line in the results stating **Skitch version [version] (or newer) is already installed.** This indicates the software has been installed.

The software was successfully installed.
Check for App in the Launchpad

1. Click the Launchpad icon on the Dock
2. Check for the existence of the **Skitch** application

View the Application Status in the AirWatch Application Catalog

1. Click on the **Application Catalog** weblink on the Dock
2. Note the Installation Status for **Skitch**.

   - **Installed**
   - version: 2.8.1
**Key Takeaways**

- macOS Applications can be deployed using the munki framework (Internal Application) or a detailed manifest of scripts and packages (Product Provisioning - not covered in this lab).
- Detailed status on installation progress is delivered to the end-user via the Workspace ONE native application for macOS (not covered in this lab)
- AirWatch provides an Application Catalog to allow user and device specific self-service requests for application installation.
Deploying macOS Applications via Product Provisioning (legacy support)

Workspace ONE UEM product provisioning is functionality that was originally created to support rugged devices but ported to provide support for macOS. While this software deployment strategy is less preferred than using the munki framework via Internal Apps, it can still be useful in some situations (and/or for problematic software installations). Product Provisioning can be thought of as a sequence of files and actions that together comprise the steps required to install a software package (the "product").

This section will walk you through the basic set of steps you can use to provision software to a macOS device.

Because products are considered a legacy form of software distribution, you will miss out on a number of features/benefits gained when deploying via Internal Applications. When deploying via Products, you will not have the following functionality:

- Content Distribution Network integration
- Mandatory Application Installs (e.g. mandatory apps re-installed if user-removed)
- Built-In Bandwidth Savings (e.g. munki only downloads files when install is required, products require custom scripting to prevent this)
- Controlled Install/Uninstall conditions based on real-time script exit code (e.g. munki’s "pre-install" and "pre-uninstall" scripts)

Create Custom Attribute Profile

Custom Attributes are a built-in function of the VMware Workspace ONE UEM agent for macOS. An administrator can deliver a shell script in a profile payload, and the echo result of that script is returned to the console as custom information about that device. In the context of product provisioning, one or more custom attributes can be used to further constrain product deployment to devices within an assignment group.

This section demonstrates how to create a custom attribute profile.
Create Custom Attribute Profile

In the Workspace ONE UEM console:

1. Select Devices.
2. Select Profiles & Resources.
3. Select Profiles.
4. Select Add.
5. Select Add Profile.

Select Profile Platform

Add Profile

Select a platform to start:

- Android
- iOS
- macOS

Select the macOS icon.
Select the Profile Context

Select Context

Select the **Device Profile** icon.
Configure General Profile Settings

1. Click on General if it is not already selected.
2. Enter BBEdit Version for the Name.
3. Select Auto for the Assignment Type.
4. Click in the Assigned Groups field. This will pop-up the list of created Assignment Groups. Enter All Devices and select the All Devices (your@email.shown_here) Smart Group.

NOTE - You may need to scroll down to find the Assigned Groups field.

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.
Configure Custom Attributes Payload

1. Scroll down on the list of Payload Types on the left side.
2. Click **Custom Attributes**.
3. Click **Configure**.
Enter Local Host Name Custom Attribute Command

1. Enter **BBEdit-Version** as the Attribute Name.
2. Enter the command shown below. Be sure to use the correct slash, two hyphens, and proper capitalization.
   
   ```
   if [-x "~/Applications/BBEdit.app"]; then
   /usr/bin/defaults read
   /Applications/BBEdit.app/Contents/Info.plist
   CFBundleShortVersionString; else echo "0.0"; fi
   ```

   **NOTE** - Remember you can drag and drop text from the manual to the text field to automatically populate the values!
3. Select **1 Hour** as the Reporting
4. Click **Save & Publish**.

**NOTE** - Please refer the Lab Guidance section in the beginning for how to copy text from manual to use in VLP.

Custom Attribute Command:
if [ -x "/Applications/BBEdit.app" ]; then /usr/bin/defaults read /Applications/BBEdit.app/Contents/Info.plist CFBundleShortVersionString ; else echo "0.0"; fi

Publish to Device Assignment

Locating Custom Attributes

Once Workspace ONE UEM delivers a Custom Attributes profile/payload to a device, the Agent will report the initial value of the Custom Attribute back to Workspace ONE UEM and begin the Schedule or Event monitoring. Custom Attribute values that have been reported back to the console can be viewed in the device details.
Select Your Enrolled Device

1. Click on **Devices**
2. Click on **List View**
3. Click on your **enrolled macOS** device to access the Device Details view.

Access Custom Attributes

1. Click on **More**.
2. Click on **Custom Attributes**.
Review Custom Attributes

1. Notice that the Source of the Attributes is **Device Sourced**, meaning it was gathered at the device and sent to AirWatch.
2. Note the list of **Attributes**.
3. Note the **value** of each Attribute. These values were generated by the output of your command/script in the Custom Attributes payload.

The value is currently **0.0** because BBEdit is not installed on the device.

**Download BBEdit Installer**

**Open Safari Browser**

If not already open, Click the Safari icon in the Dock
Browse to BareBones Software Website

In the URL box, enter [https://www.barebones.com/products/bbedit/download.html](https://www.barebones.com/products/bbedit/download.html) and press **ENTER** on the keyboard.

Download BBEdit 12 Evaluation for macOS

Click **Download**

Create Files/Actions

A product can comprise one or more Files/Actions. Files/Actions are the building blocks of a product, containing a set of files and a manifest of actions to take against those files. A Files/Actions set can also contain a corresponding *uninstall* manifest which directs the Workspace ONE UEM agent as to how a product should be removed during an Enterprise Wipe. This exercise illustrates how to create a basic set of files/actions in order to install and uninstall BBEdit.
In the Workspace ONE UEM Console, perform the following:

1. Select **Devices**
2. Expand **Staging & Provisioning**
3. Expand **Components**
4. Select **Files/Actions**
5. Click **Add Files/Actions**
Choose the macOS Platform

Select Apple macOS

Name the Files/Actions Item

1. Enter **BBEdit Install** as the Name
2. Select the **Files** tab
Add Files to Files/Actions

Add Files/Actions

<table>
<thead>
<tr>
<th>General</th>
<th>Files</th>
<th>Manifest</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image" alt="ADD FILES" /></td>
<td></td>
</tr>
</tbody>
</table>

File Name | Path
----------|---------

Select Add Files

Choose Files to Upload

Add Files

Add File* Choose Files no files selected

Select Choose Files
Select File from Finder

1. Click the Downloads folder
2. Select the BBEdit_<version>.dmg file
3. Select Choose

The BBEdit Installer will be in whichever folder your Internet browser used as a download destination. Common folders to check are the Desktop and Downloads folders.
Save the File to Files/Actions

Add File

Choose Files  BBEdit...1.4.dmg

SAVE  CANCEL

Select Save
1. Enter `/tmp` as the download path
2. Click Save

In this example, we use `/tmp` as the download path as it is automatically cleaned up by macOS. If you wish for Product Downloads to persist on the file system, you must choose a different download path.
Copy File Path

Add Files/Actions

1. Click and drag to highlight the Path field.
2. Right-click (or Control-click) the highlighted path and select Copy.
3. Select the Manifest tab.

Add Action to Install Manifest

Click Add Action under Install Manifest.
Configure Add Manifest Action

The Install Manifest comprises the sequence of actions that must be performed in order to install the files you've included in the Files/Actions. This could involve copying/moving files, installing dmg/pkgs, and running scripts.

1. Select **Install** as the action
2. Paste the File Path you copied previously: `/tmp/BBEdit_<version>.dmg`
3. Select **Save**

Add Action to Uninstall Manifest
Click **Add Action** under Uninstall Manifest.

**Add Action to Uninstall Manifest**

The Uninstall Manifest comprises the sequence of actions that must be performed in order to remove/revert the files and actions you've taken as part of an install. The Uninstall Manifest also instructs the agent how to remove the product during an *Enterprise Wipe*.

1. Select **Uninstall** as the action
2. Enter the name of the App as it appears in the list of Applications when installed: **BBEdit**
3. Select **Save**
Save File/Actions

Select Save

Create Product from Files/Actions
Add Product

In the Workspace ONE UEM Console:

1. Select Devices
2. Expand Staging & Provisioning
3. Select Product List View
4. Select Add Product

Choose Product Platform

Add Product

Select Apple macOS
Complete General Information

Add Product

1. Enter **Install BBEdit** for the Product Name
2. Click in the Assigned Groups field and select All Devices *(your@email.shown.here)*
3. Click **Add Rules**
Add Dependency Rules

1. Click **Add Rule**.
2. Select **BBEdit-Version @ AirWatchAgent** for the Attribute/Application.
3. Select **<>** for the Operator.
4. Select **Enter Manually** for the Value.
5. Enter **12.1.5** (or the most current version of BBEdit).
6. Notice that the Rule Logic field is built out automatically based on your selections and inputs.
7. Select **Save**.
Add Manifest to Product

Add Product

1. Select the **Manifest** tab
2. Select **Add**

Choose Manifest Item

1. Select **Install Files/Actions** in the action(s) menu
2. Select **BBEdit Install** as the Files/Actions item
3. Select **Save**
Set Product Type and Activate

1. Select the **Deployment** tab
2. Select **Required** as the product type
3. Select **Activate**
**Confirm Device Assignment**

<table>
<thead>
<tr>
<th>Assignment Status</th>
<th>Friendly Name</th>
<th>User</th>
<th>Platform/OS/Model</th>
<th>Phone Number</th>
<th>Organization Group</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Added</strong></td>
<td>testuser MacBook</td>
<td>testuser</td>
<td>AppleOSX / macOS H...</td>
<td><a href="mailto:your@email.shown.h">your@email.shown.h</a>...</td>
<td></td>
</tr>
</tbody>
</table>

Items 1-1 of 1

Page Size: 50

Select **Activate**
**Validate Product Installation**

After activating the Product, you will be taken back to the Product List View in the Workspace ONE UEM Console, which is located under Devices > Staging & Provisioning > Product List View.

1. You may need to click the Refresh button if the shown values are not populated.
2. Note the number of Compliant devices (The product installed successfully).
3. Note the number of devices where product installation is in progress.
4. Note the number of failed product installs.

All the status counts are clickable and will display a list view of all devices with that status (e.g. Compliant, In Progress, and Failed).
Validate Install on Managed macOS Device

1. Select the **Finder** icon in the Dock
2. Select **Applications**
3. Validate **BBEdit** is present in the application list
Enterprise Wipe a macOS Device

An Enterprise Wipe removes corporate data that was added to the device while leaving personal data intact.

View Device List

In the Workspace ONE UEM Console:

1. Select **Devices**
2. Select **List View**.
3. Select your macOS device in the List View to view details.
Initiate Enterprise Wipe

1. From the toolbar in the device details header, select More Actions.
2. Select Enterprise Wipe under the Management header in the drop-down menu.

Enter Security PIN to Confirm Wipe
1. Scroll down until you see the section to Enter Security PIN.
2. Enter your security PIN 1234 to initiate the Enterprise Wipe.
Conclusion

This lab covered basic macOS Software Distribution using Workspace ONE. You enrolled your macOS device, deployed software and then enterprise wiped the content and settings from the device.
Introduction

In this section we'll cover a basic introduction to AirWatch School Manager and it's requirements.

What is AirWatch School Manager

AirWatch School Manager is designed to let organizations leverage Apple's Classroom application in organizations that are not eligible for Apple School Manager.

Requirements

AirWatch School Manager requires the following software and hardware:

- AirWatch version **8.4 Feature Pack 4 or greater**.
- Apple devices running **iOS 9.3 or greater**.
- All Devices must be **supervised**.
- All Devices must have **beacon** capabilities.
- AirWatch School Manager utilizes the Apple Classroom application.
- **Apple Push Notification Services** must be **configured** in your AirWatch environment and **allowed** on your network/firewall/etc.

_NOTE - If your iOS Devices do not meet the above requirements, you will not be able to complete this entire module!

Optional Functionality

While not required, the following optional 3rd-party software features can augment the functionality of AirWatch School Manager. These 3rd-party features can help streamline your classroom setup and configuration:

- Apple's Device Enrollment Program.
- Apple's Volume Purchase Program.
- Student Images.
- LDAP / AD (with User Groups).

Differences from Apple Education

While employing similar concepts and functionality, AirWatch School Manager has a few differences from Apple Education.

1. **Apple School Manager is not required.** AirWatch School Manager can therefore be leveraged in countries where Apple School Manager is not available.
It also means AirWatch School Manager can be leveraged by entities (such as businesses) which are not eligible to enroll in Apple School Manager.

2. **Managed Apple IDs are not required.** AirWatch School Manager does not require Managed Apple IDs which can only be created via Apple School Manager. This means you can create a class device without the need for any Apple ID (if you leverage Device-Based Licensing via the Apple Volume Purchase Program).

3. **AirWatch School Manager does not require 32GB+ iPads.** This makes AirWatch School Manager work with a greater number of devices, including older 16GB iPads.

### Typical Uses for AirWatch School Manager

AirWatch School Manager is designed to let organizations leverage Apple's Classroom application in organizations that are not eligible for Apple School Manager. Some typical use cases are as follows:

- Educational institutions (such as daycares or continuing/career-oriented educators) which may not be eligible for Apple School Manager.
- Businesses with formalized onboarding/training programs that wish to leverage a digital classroom.
- School systems that ARE eligible for Apple School Manager but with a significant fleet of devices that do not meet the minimum requirements (e.g. 32GB) to use Apple School Manager.
- Organizations using AirWatch Teach/Learn applications looking to migrate to Apple's Classroom app.
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 *

Password Recovery Answer *

Confirm Password Recovery Answer *

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 *

Confirm Security PIN *

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.
Enabling VMware AirWatch School Manager

In this section we will enable AirWatch School Manager functionality in your AirWatch environment.

Enter Devices Settings

1. Click Devices
2. Click Devices Settings
Enable AirWatch School Manager

2. Click Education.
4. Select Enabled for Enable Education Features.
5. Select AirWatch for the Class Source.
6. Click Save.
Enter Security PIN

1. Enter the Security PIN (e.g. **1234**) that you entered when first logging into your AW environment.
2. After inputting your Security PIN, you should see the **Successful** confirmation appear and automatically closes the menu.
Close Device Settings

Click the ✗ in the top right corner of the Settings screen to return to the Device Dashboard.
Creating the Class List

In this section we'll walk through the initial stages of configuring AirWatch School Manager.

The Education Overview Hub

1. Click on **Hub**
2. Expand **Education**
3. Click **Overview**
4. Note the Overview page that details the AirWatch School Manager Setup and Use.

The Class List Page

1. Click on **Class List**
2. Click on **Add Class**
Add a Class

1. Enter a name for the class: **1st Grade - Ms Smith**
2. Click the Assigned Teachers box and select **imateacher**. **NOTE** - As you type the console will filter a list of users. **You can select the user without having to type the whole name.**
3. Click the Assigned Students box and select **imastudent**.
4. Click **Save**
Add Another Class

1. Click on Class List
2. Note the presence of the class you just created.
3. Click Add Class
Enter Class Information

Add Class

CLASS

Name *

1st Grade Mr Jones

TEACHERS

Assigned Teachers *

Search or create new users
Ima Teacher (imateacher) im...

STUDENTS

Assigned Students *

Search or create new users
Ima Student (imastudent) im...

1. Enter a name for the class: **1st Grade - Mr Jones**
2. Click the Assigned Teachers box and select **imateacher**. **NOTE - As you type the console will filter a list of users. You can select the user without having to type the whole name.**
3. Click the Assigned Students box and select **imastudent**
4. Click Save
Publish the Classroom Application

Next, we will publish the Classroom app so that our the Classroom functionality can be shown on devices that we will enroll in a later step.

Add a Public Application

In the top-right corner of the AirWatch Console:

1. Click **Add**.
2. Click **Public Application**.
Search for the Classroom App

1. Select Apple iOS for the Platform.
2. Enter Classroom for the Name.
3. Click Next.

Select the Classroom App

Classroom is a free service for schools, non-profits, and anyone with a personal Google account. Classroom makes it easy for learners and instructors to connect—inside and outside of schools. Classroom saves time and paper, and makes it easy to create classes, distribute assignments, communicate, and stay organized. Classroom is designed to help teachers create, collect, and grade assignments paperlessly, including time-saving features like the ability to automatically make a copy of a Google Doc...
1. Find the Apple **Classroom** app in the list. The identifier will be `com.apple.classroom`.

   **NOTE - It may not be the first result and may require you to scroll down to find it!**

2. Click **Select** on the Apple Classroom app.
Review Classroom Application Information

Review the information about the application you've selected and click Save & Assign
Configure the Classroom Assignment Settings

1. On the "Update Assignment" screen, click on the Assignments tab.
2. Click Add Assignment.
Create the Classroom Configuration.

Begin to fill-out your classroom configuration. Please ensure you've met the following:

1. Assign to your **All Devices (your@email.shown.here)** smart group.
2. Set the app delivery method as **AUTO**
3. Scroll down to the policies section and select **Enabled** for **Remove On Unenroll**.
4. Click **Add**

**Finish the Classroom Configuration and Save**

Click **Save & Publish**
Publish the Classroom App

Preview Assigned Devices

<table>
<thead>
<tr>
<th>Assignment Status</th>
<th>Friendly Name</th>
<th>User</th>
<th>Platform/OS/Model</th>
<th>Organization Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No Records Found

Click Publish
Enroll Class Devices

You are now going to enroll two iOS devices for use with this module. One device will act as a teacher, the other will act as a student.

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**

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.

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

You will now provide the Teacher account's user credentials to authenticate to Workspace ONE UEM on the first device.

1. Enter `imateacher` 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 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)

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”?

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.
Accept the Data Sharing Policy

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

I agree

Not now
Confirm the Device Enrollment in the Hub App

Account

Basic Account
Updated Today at 7:40 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.
REMINDER - Enroll TWO Devices

REMINDER - You will need to enroll one device as imateacher and another device as imastudent in order to complete the lab.

Please ensure you have completed the "ENROLL CLASS DEVICES" section twice and have a device enrolled as the teacher and another enrolled as the student!

1. Enter imastudent in the Username field.
2. Enter VMware1! in the Password field.
3. Tap the Next button.
Control Student Devices with Classroom App

This section is meant to give you a brief introduction to the Classroom application and its use within AirWatch School Manager. More details on the Classroom app can be found on Apple’s support website:  https://help.apple.com/classroom/ipad/1.1

Open Classroom App

Return to the Teacher iPad. On the Teacher iPad:

Tap the Classroom app to open it and click Continue at the Welcome Screen.

OPTIONAL: Configuration Invalid Error

If you receive a Configuration Invalid error message, you most likely have tried to open the Classroom application on the Student iPad.

1. Click OK
2. Swap iPads and restart this section at Open Classroom App from the TEACHER iPad.
Click Continue to launch the Classroom app.
Accept Notification Prompt (IF NEEDED)

Would Like to Send
You Notifications

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

Don’t Allow  Allow

You may see a prompt to allow notifications from Classroom app. Tap Allow if you get a prompt for Notifications.

Choose Class

Click on 1st Grade - Mr Jones
Explore Classroom Interface

Note the following areas of the Classroom app interface:

1. **Select** -- allows you to select multiple devices (#5) in order to apply commands (#3) to simultaneously.
2. **Action Buttons** -- The actions you can take against a group of devices (#4) or individual devices (#5)
3. **Device Groups** -- Groupings of devices (can be one or more). Classroom includes an **All** group by default.
4. **Individual devices** -- each device/user is shown in the classroom application.

Verify Student iPad Connectivity
1. If your student iPad displays as **Offline**, click the hardware power button the iPad to power it on.
2. You will see the status change to **Home Screen** (or whatever app is currently running in the foreground).
3. Note that the iPad is now displayed on the Device Groups bar based on the currently running app.

**Control Single iPad**

1. Click on the Student device. Note actions that are disabled - this functionality relates to Managed Apple IDs (requires Apple School Manager)
2. **Open** allows you to open an application on the student iPad. **NOTE** - **The app must already exist on the iPad.**
3. **Navigate** allows you to open a web location in Safari on the Student device.
4. **Lock** allows you to put the device into a "locked" state (such as for "eyes up front").
5. **AirPlay** allows you to force a device to send its screen to an AirPlay compatible device. You can populate the list of AirPlay destinations via an EMM Profile.
6. **Password** allows you to reset the device password if one has been set.
7. **View Screen** allows you to watch the screen on the device in real-time.
8. When choosing an action, completion of the action will display a **Done** link to return you to main Classroom App screen.
9. You can exit from the Actions list for a device by clicking outside the dialog screen.
Control Multiple Devices

1. Select a Group from the list of Device Groups.
2. Note that you can now take actions against the group, such as Open, Navigate, Lock, and Screen Viewing.
3. Click Screens on the Teacher device.
4. Note the icon for the student device in the Classroom app now displays the screen capture of the device. Also note on the student device that the status bar is now blue and there is also an airplay icon displayed.
5. Click the Screens button to end screen viewing. Note the icon returns to normal in the Classroom app and the student device status bar returns to normal.
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](mailto: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
<table>
<thead>
<tr>
<th>Settings</th>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airplane Mode</td>
<td>Lock Rotation</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Mute</td>
</tr>
<tr>
<td>Bluetooth On</td>
<td>Rotation Lock</td>
</tr>
<tr>
<td>Cellular Data</td>
<td>available in Control Center.</td>
</tr>
<tr>
<td></td>
<td>iPad Storage</td>
</tr>
<tr>
<td></td>
<td>Background App Refresh</td>
</tr>
<tr>
<td></td>
<td>Restrictions Off</td>
</tr>
<tr>
<td></td>
<td>Date &amp; Time</td>
</tr>
<tr>
<td></td>
<td>Keyboard</td>
</tr>
<tr>
<td></td>
<td>Language &amp; Region</td>
</tr>
<tr>
<td></td>
<td>Dictionary</td>
</tr>
<tr>
<td></td>
<td>iTunes Wi-Fi Sync</td>
</tr>
<tr>
<td></td>
<td>VPN Not Connected</td>
</tr>
<tr>
<td></td>
<td>Device Management</td>
</tr>
<tr>
<td></td>
<td>Regulatory</td>
</tr>
<tr>
<td></td>
<td>Reset</td>
</tr>
<tr>
<td></td>
<td>Shut Down</td>
</tr>
</tbody>
</table>
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**

1. 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 section will cover some key takeaways for you to remember before ending this lab.

Requirements and Optional Add-ons for AirWatch School Manager

AirWatch School Manager requires the following software and hardware:

- AirWatch version 8.4 Feature Pack 4 or greater.
- Apple devices running iOS 9.3 or greater.
- All Devices must be supervised.
- All Devices must have beacon capabilities.
- AirWatch School Manager utilizes the Apple Classroom application
- Apple Push Notification Services must be configured in your AirWatch environment and allowed on your network/firewall/etc.

You may also extend your AirWatch School Manager functionality by leveraging the following programs:

- Apple's Device Enrollment Program
- Apple's Volume Purchase Program
- LDAP or Active Directory Integration

Typical Uses for AirWatch School Manager

AirWatch School Manager is designed to let organizations leverage Apple's Classroom application in organizations that are not eligible for Apple School Manager. Some typical use cases are as follows:

- Educational institutions (such as daycares or continuing/career-oriented educators) which may not be eligible for Apple School Manager.
- Businesses with formalized onboarding/training programs that wish to leverage a digital classroom.
- School systems that ARE eligible for Apple School Manager but with a significant fleet of devices that do not meet the minimum requirements (e.g. 32GB) to use Apple School Manager.
- Organizations using AirWatch Teach/Learn applications looking to migrate to Apple's Classroom app.
For More Information

For additional information on AirWatch School Manager, please speak with your Account Executive or refer to the documentation on MyAirWatch.
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-1957-05-UEM

Version: 20181104-164221