# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab Overview - HOL-1957-07-UEM - Workspace ONE UEM - Productivity Apps</td>
<td>3</td>
</tr>
<tr>
<td>Lab Guidance</td>
<td>4</td>
</tr>
<tr>
<td>Module 1 - Workspace ONE Boxer</td>
<td>9</td>
</tr>
<tr>
<td>Introduction</td>
<td>10</td>
</tr>
<tr>
<td>Login to the Workspace ONE UEM Console</td>
<td>11</td>
</tr>
<tr>
<td>Configure Workspace ONE Boxer</td>
<td>17</td>
</tr>
<tr>
<td>Add Workspace ONE Web as a Public App</td>
<td>28</td>
</tr>
<tr>
<td>iOS Device Enrollment (Using the e-mail address from lab automation)</td>
<td>35</td>
</tr>
<tr>
<td>Exploring Workspace ONE Boxer</td>
<td>56</td>
</tr>
<tr>
<td>Un-enrolling Your Device</td>
<td>82</td>
</tr>
<tr>
<td>Conclusion</td>
<td>91</td>
</tr>
<tr>
<td>Module 2 - Workspace ONE Web</td>
<td>92</td>
</tr>
<tr>
<td>Introduction</td>
<td>93</td>
</tr>
<tr>
<td>Login to the Workspace ONE UEM Console</td>
<td>95</td>
</tr>
<tr>
<td>Workspace ONE UEM Console Configuration</td>
<td>101</td>
</tr>
<tr>
<td>iOS Device Enrollment</td>
<td>128</td>
</tr>
<tr>
<td>Explore Workspace ONE Web</td>
<td>147</td>
</tr>
<tr>
<td>Un-enrolling Your Device</td>
<td>157</td>
</tr>
<tr>
<td>Conclusion</td>
<td>166</td>
</tr>
<tr>
<td>Module 3 - Workspace ONE Tunnel</td>
<td>167</td>
</tr>
<tr>
<td>Introduction</td>
<td>168</td>
</tr>
<tr>
<td>Login to the Workspace ONE UEM Console</td>
<td>169</td>
</tr>
<tr>
<td>Create Per-App VPN Profile</td>
<td>175</td>
</tr>
<tr>
<td>Publish VMware Tunnel as a Public App</td>
<td>181</td>
</tr>
<tr>
<td>Configure Workspace ONE Web for Per-App VPN</td>
<td>188</td>
</tr>
<tr>
<td>iOS Device Enrollment</td>
<td>195</td>
</tr>
<tr>
<td>Testing Per App VPN</td>
<td>214</td>
</tr>
<tr>
<td>Safari Domain Profile Configuration</td>
<td>221</td>
</tr>
<tr>
<td>Testing Safari Domains with Per App Tunnel</td>
<td>225</td>
</tr>
<tr>
<td>Un-enrolling Your Device</td>
<td>232</td>
</tr>
<tr>
<td>Conclusion</td>
<td>241</td>
</tr>
<tr>
<td>Module 4 - Workspace ONE App Catalog</td>
<td>242</td>
</tr>
<tr>
<td>Introduction</td>
<td>243</td>
</tr>
<tr>
<td>Different types of applications - Internal / Public / Purchased / Web Apps</td>
<td>244</td>
</tr>
<tr>
<td>Login to the Workspace ONE UEM Console</td>
<td>245</td>
</tr>
<tr>
<td>Download AppLifecycle Apps</td>
<td>251</td>
</tr>
<tr>
<td>iOS Device Enrollment With Directory Account</td>
<td>253</td>
</tr>
<tr>
<td>Internal App Deployment</td>
<td>272</td>
</tr>
<tr>
<td>Public App Deployment - Workspace ONE Catalog</td>
<td>284</td>
</tr>
<tr>
<td>Log into Workspace ONE Catalog</td>
<td>294</td>
</tr>
<tr>
<td>Internal App Versioning</td>
<td>301</td>
</tr>
<tr>
<td>Web App Deployment</td>
<td>315</td>
</tr>
</tbody>
</table>
Remove Apps via Workspace ONE UEM Console .................................................. 324
Assume Management ......................................................................................... 326
Un-enrolling Your Device .................................................................................. 343
Conclusion ........................................................................................................... 352
Lab Overview - HOL-1957-07-UEM - Workspace ONE UEM - Productivity Apps
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.

The Workspace ONE UEM solution also includes productivity apps to enable your workforce and provide a unified experience across your devices for core components. Learn how Workspace ONE Web and Workspace ONE Boxer can provide secure access to cross-platform browser and email platforms, and how Workspace ONE Tunnel allows your users to securely access internal resources from any device to empower your digital workforce.

Lab Module List:

- **Module 1 - Workspace ONE Boxer** (30 minutes) (Beginner) As part of the Workspace ONE suite of Productivity Apps, Workspace ONE Boxer combines consumer simplicity with enterprise security. The app provides frictionless access to enterprise email, calendar and contacts across both corporate-owned and employee-owned devices. In this lab, we will perform Workspace ONE Web setup in AirWatch Console for Data Loss Prevention (DLP) and a mail account configuration. We will then validate those configurations while highlighting some exclusive features of Workspace ONE Boxer.

- **Module 2 - Workspace ONE Web** (30 minutes) (Beginner) Workspace ONE Web is an Enterprise-grade mobile browser that can be configured to meet your business requirements with features like kiosk mode, bookmarks and tunneling. Let's see how to configure Workspace ONE Web and experience those configurations on an enrolled device.

- **Module 3 - Workspace ONE Tunnel** (30 minutes) (Beginner) Leveraging Per-App VPN allows you to control which applications on a device have access to your VPN by automatically enabling disabling VPN access based on which applications are active. This prevents you from needing to provide a device wide VPN on your devices, which allow unintended apps or processes to access your VPN and ensures only authorized apps have access to your VPN. Let's see how we can leverage Workspace ONE Tunnel to enable per-app VPN on an enrolled device.

- **Module 4 - Workspace ONE App Catalog** (45 minutes) (Beginner) Explore the basic concepts of Mobile Application Management (MAM) with Workspace ONE UEM and learn how to deploy applications to the Workspace ONE Catalog for your users to access on any device from anywhere.

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

http://docs.hol.vmware.com

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


Location of the Main Console

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

Alternate Methods of Keyboard Data Entry

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

Click and Drag Lab Manual Content Into Console Active Window

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

Accessing the Online International Keyboard

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

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

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

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

### Click on the @ key

1. Click on the "@ key".

Notice the @ sign entered in the active console window.

### Activation Prompt or Watermark

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

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

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

This cosmetic issue has no effect on your lab.

**Look at the lower right portion of the screen**

![Lab Status Screen]

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

As part of the Workspace ONE suite of Productivity Apps, Workspace ONE Boxer combines consumer simplicity with enterprise security. The app provides friction-less access to enterprise email, calendar and contacts across both corporate-owned and employee-owned devices.

We will configure and deploy Workspace ONE Boxer with Data Loss Prevention (DLP) settings and then validate those configurations while highlighting some exclusive features of Workspace ONE Boxer.
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

<table>
<thead>
<tr>
<th>Password Recovery Question 1</th>
<th>What was your childhood nickname?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Recovery Question  *</td>
<td>VMware!</td>
</tr>
<tr>
<td>Password Recovery Answer</td>
<td>VMware!</td>
</tr>
<tr>
<td>Confirm Password Recovery Answer *</td>
<td>VMware!</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>1234</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm Security PIN *</td>
<td>1234</td>
</tr>
</tbody>
</table>

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.
Configure Workspace ONE Boxer

In this chapter, you will configure and deploy the Workspace ONE Boxer client to the device.

Add the Workspace ONE Boxer Client as an iOS Public Application

We can leverage Workspace ONE UEM to deploy and automatically configure the VMware email client on the device through Workspace ONE UEM. This step will walk you through the process of adding an application from the iOS Public App store.

Add a New Public Application

1. Click Add
2. Click Public Application
Search for the Application to Add

1. Select Apple iOS from the Platform dropdown.
2. Enter VMware Boxer in the Name field.
3. Click Next.

Select the Application from the Search Results

VMware Boxer

VMware Boxer is the most innovative email, calendar and contacts app available for iPhone! Here’s what people are saying about our app: The Webby Awards Nominated Boxer for Best Mobile Productivity App of the Year! ***** “If you like to have a lot of control over how your app works, including the ability to customize swipe gestures, you should check out Boxer. With its fast notifications, plentiful customization options, and integrated calendar and contacts list, this iPhone app has a lot to o...

Click Select on the VMware Boxer application.
Save and Assign VMware Boxer

Add Application - VMware Boxer
Public | Managed By: snavare@vmware.com | Application ID: com.air-watch.boxer ...

Details
Terms of Use
SDK

Name * VMware Boxer

View in App Store

Categories
Start Typing to Select Category ...

Supported Models
iP...
Add Assignment for VMware Boxer

Configure VMware Boxer Assignment Settings

1. Click in the **Selected Assignment Groups** field. This will pop-up the list of created Assignment Groups. Start Typing **All Devices** and select the **All Devices (your@email.shown.here)** Group.
2. Select **Auto** for the **App Delivery Method**.
Configure VMware Boxer Email Settings

VMware Boxer - Add Assignment

1. Find the Email Settings section, you may need to scroll down.
2. Enter **HOL Email** for the **Account Name**. This is a friendly name used to identify this email account configuration.
3. Enter **https://sme.airwlab.com** for the **Exchange ActiveSync Host**.
4. Enter **hol** for the **Domain**.
5. Enter the lookup value `{UserPrincipalName}` for the **User**.
6. Enter the lookup value `{EmailAddress}` for the **Email Address**.
# Configure the Passcode Settings

## VMware Boxer - Add Assignment

1. Scroll down to find the More Email Settings section.
2. Click **More Email Settings** to expand the section.
3. Select **Numeric** for the **Type** under the Passcode section.
4. Enter **4** for the Minimum Length. This will require that we setup a **4 digit PIN** to access the Boxer app on our device.
Configure the Data Loss Prevention (DLP) Settings

VMware Boxer - Add Assignment

1. Scroll down to find the Data Loss Prevention section.
2. Set **Copy Paste** to **RESTRICTED**: This restricts Copy/Paste to other applications. This setting allows copy/paste to Personal Accounts if Unrestricted.
3. Set **Hyperlinks** to **RESTRICTED**: Sets all URL’s to open in Workspace ONE Web.
4. Set **Sharing** to **WHITELIST**:
   - Preview Only - allows viewing of files in Boxer only;
   - Whitelist - select specific applications that can open files from Boxer;
   - Unrestricted - attachments can be opened in all applications from Boxer.
   By default, when you select Whitelist, a default set of whitelisted applications are configured automatically. We are mostly concerned with whitelisting `com.air-watch.content.locker` to allow Content Locker to be able to open attachments from Workspace ONE Boxer.
5. Enter **com.air-watch.content.locker** for **Whitelisted Applications**, if not whitelisted already. This allows Workspace ONE Boxer to open files and attachments in the Content Locker app.
6. Set **Caller ID** to **RESTRICTED**: Allows your saved Outlook contacts to be exported to the device so when a saved contact calls you, their name displays on your device. Only Name and phone number are exported to the local contacts.

**Configure Personal and Work Separation Settings**

1. Scroll down to find the Personal and Work Separation section.
2. Set **Personal Accounts** to **RESTRICTED**. This prevent personal accounts from being added to the Boxer app and deletes any personal data already entered in the app.
3. Set **Personal Contacts** to **RESTRICTED**. This prevent personal contacts from being added to the Boxer app and deletes any personal data already entered in the app.
Configure Policies for VMware Boxer

VMware Boxer - Add Assignment

1. Scroll down to find the Policies section.
2. Select **ENABLED** for **Device must be MDM Managed to install this App**
3. Select **ENABLED** for **Remove on Unenroll**
4. Select **ENABLED** for **Prevent Application Backup**
5. Click **ADD**

---

**Policies**

- **Device must be MDM Managed to install this App**: **ENABLED**
- **Remove On Unenroll**: **ENABLED**
- **Prevent Application Backup**: **ENABLED**
- **Make App MDM Managed if User Installed**: **ENABLED**
- **App Tunneling**: **ENABLED**
Confirm Assignment and Save

VMware Boxer - Update Assignment

Please note that the newly added assignments will be added at the bottom of the priority list. The assignments can now be moved up or down in the priority list. 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. Confirm that the Assignment you just configured is displayed.
2. Click **SAVE & PUBLISH**
Preview Assigned Devices and Publish

Preview Assigned Devices

Assignment Status  All

Search List

No Records Found

Click **PUBLISH**
Add Workspace ONE Web as a Public App

VMware Boxer also supports Workspace ONE Web for opening links and other features, so in order to demo this functionality, we will be publishing Workspace ONE Web to the iOS device.

Add A New Public Application

1. Click Add
2. Click Public Application
Search for the Application to Add

Add Application

1. Select Apple iOS from the Platform dropdown.
2. Enter Workspace ONE Web in the Name field.
3. Click Next

Select the Application From the Search Results

Click Select on the Web - Workspace ONE application.
Save and Assign Workspace ONE Web

Add Application - Web - Workspace ONE

Details | Terms of Use | SDK

Name * Web - Workspace ONE

View in App Store

Categories
Start Typing to Select Category ...

Supported Models
iPad
iPhone
iPod Touch

Click SAVE & ASSIGN
Add Assignment for Workspace ONE Web

Configure Workspace ONE Web Assignment Settings

1. Click in the **Selected Assignment Groups** field. This will pop-up the list of created Assignment Groups. Start Typing **All Devices (your@email.shown.here)** and select the **All Devices (your@email.shown.here)** Group.

2. Select **AUTO** for the **App Delivery Method**.
Configure Policies for Workspace ONE Web

1. Scroll down to find the Policies section.
2. Select **ENABLED** for **Remove On Unenroll**
3. Select **ENABLED** for **Make App MDM Managed if User Installed**
4. Click **ADD**
Confirm Assignment and Save

1. Confirm that the Assignment you just configured is displayed.
2. Click **SAVE & PUBLISH**
Preview Assigned Devices and Publish

Click **PUBLISH**
iOS Device Enrollment (Using the e-mail address from lab automation)

A temporary Exchange mailbox has been generated for you to use throughout this lab. The account credentials are uploaded to the Content section of the Workspace ONE UEM Console.

**Locate Your Exchange Account Details**

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

Return to the Workspace ONE UEM Console,

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

After the file downloads, click the Mailbox Details for your@email.shown.here.txt file from the download bar to open it.

Note the Email Address

You will use this Email Address in the next step to enroll your iOS Device. Leave this Notepad file open and refer to the Email Address as needed in the following steps.

Enroll Your iOS Device

In this section, we are going to enroll an iOS device to complete the steps on the device side.
Download and Install Workspace ONE Intelligent Hub from App Store (IF NEEDED)

NOTE - Checked out devices will likely have the Workspace ONE Intelligent Hub already installed. You may skip this step if your device has the Workspace ONE Intelligent Hub installed.

At this point, if you are using your own iOS device or if the device you are using does NOT have the Workspace ONE Intelligent Hub Application installed, then install the application from the App Store.

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

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

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

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

Click on the \texttt{Server Details} button.

Find Your Group ID From the Workspace ONE UEM Console

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

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

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

![Workspace ONE Intelligent Hub icon](image)

labs.awmdm.com

{Your Group ID}  

Next

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 User Credentials

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

1. Enter the email address copied from the previous steps in the **Username** field. This will be in the format `yourid1234@hol.airwlab.com`.
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

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

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

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

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

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

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

Congratulations!

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

You may navigate away from this page.

Open this page in “Hub”?

Open

Cancel

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/helpprivacy.html

I agree

Not now

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

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.
Exploring Workspace ONE Boxer

In this series of steps you will sync email to a sample account and get introduced to a few of the features in Workspace ONE Boxer that make it the top choice for enterprise productivity.

Sync your HOL email account

In this step you will sync the Boxer client with the HOL Exchange server and receive email.

Open Workspace ONE Boxer

Return to the Launchpad of your iOS device and select the Boxer icon.
Accept the Privacy Prompt

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 Boxer 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 Boxer
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.

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

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

Tap **I understand** to accept the Privacy prompt.
Agree to the Data Sharing Prompt

Tap **I agree** to accept the Data Sharing Prompt

**Enter your password**

An email account has been created for your in the format seen above. This email account will remain active for the duration of the lab.

1. Enter **VMware1!** in the password field.
2. Select **Get started** to continue.
Create your Passcode

You will be asked to configure a PIN for Boxer.

1. The Passcode requirements shown here will match what you configured for the Passcode settings in the Boxer configuration within AirWatch Console.
2. Enter 1234 for your Passcode.
3. Tap Next to continue.

*NOTE - If you do not see this step, then you did not configure a passcode for Workspace ONE Boxer. Continue to the next step.*
Confirm your Passcode

You will be prompted to confirm your passcode.

1. Enter **1234** for the Passcode.
2. Tap **Next**.

*NOTE - If you do not see this step, then you did not configure a passcode for Workspace ONE Boxer. Continue to the next step.*

Accept Boxer permissions

Tap **Allow** to accept Boxer's request for permissions for all pop-up messages on the iPad.
Accept Boxer permissions for Caller ID (If Configured)

If you enabled Caller ID, you must grant Boxer permissions to your Contacts.

Click **OK** to accept Boxer's request for permissions for all pop-up messages on the iPad.

**Create a new Custom Box to sync your Sent Items in the Background**

In this step you will add a Custom Box to your boxer folders. This is really just a group of folders that can be set to sync in the background just like your Inbox.

*NOTE - It may take around 1 -2 minutes for Boxer to sync and populate emails in your mailbox.*
Edit your folder list

NOTE - It may take around 1 -2 minutes for Boxer to sync and populate emails in your mailbox.

1. Open the folder list by selecting the **3 bars** in the upper left of the screen.
2. Select **Edit**.
Select **Add custom box**.
Customize the box

1. Select \textbf{Sent Items}
2. Verify the name has been entered.
3. Verify \textbf{Background Sync} is \textbf{enabled}.
4. Select the \textbf{< arrow}. 
Sort your folders

1. Verify the custom box has been added.
2. Optional: Reorder the folders as you’d like by long pressing on the hamburger icon in front of the folder.
3. Tap Done when you are ready to move on.
4. Click on the hamburger menu key to go back to Inbox.

Open a link into Workspace ONE Web

Earlier we set Boxer to open all links into Workspace ONE Web which has been delivered to your device. We will now demo this functionality.
Open an email and select a link

1. Find and tap the email with subject Link support
2. Tap the first link http://www.vmware.com

Accept Browser Notification Permissions

"Browser" Would Like to Send You Notifications
Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.

Tap Allow when prompted to allow Browser Notifications.
Verify website opened in Workspace ONE Web

View the website and then tap < **Boxer** in the upper left of the iPad screen.

**NOTE - The Home Page for the website may be different than what you are seeing in the screenshot.**

**Explore Settings and Advanced Options**

This is a dive into the some of the available settings options for the Boxer email client. Feel free to explore on our own as well!
Edit your Swipe actions

1. Tap **Settings** from toolbar at the bottom.
2. Tap **Swipe actions**

---

<table>
<thead>
<tr>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Left Short Swipe</strong></td>
</tr>
<tr>
<td><strong>Left Long Swipe</strong></td>
</tr>
<tr>
<td><strong>Right Short Swipe</strong></td>
</tr>
<tr>
<td><strong>Right Long Swipe</strong></td>
</tr>
</tbody>
</table>
1. Explore options for swipe actions. **NOTE - This options may be different than the screenshot. Feel free to customize them as per your preference.**
2. Tap Back to return to the Settings menu.

You can return to your mailbox and test out the swipe actions now if you'd like. Continue to the next step when ready.

**Respond to an email with a Quick Response**

Boxer has a unique feature that allows you to quickly respond to an email with either a **Quick Response** or your **availability** by interactively selecting available times directly on your calendar. We'll see how these features work in the next steps.

**Return to your Inbox**

1. Select **Mail** from the toolbar at the bottom.
2. Select the email with subject **Availability Request**.
3. Select **Reply**
Add a quick response

Select the **Quick response icon**.

**Select a Quick response**

Choose from any of the quick responses. In the settings menu, you can add your own custom quick responses that will then show here!
Open the interactive availability menu

Select the **Calendar** icon.

**Select Send Availability**

Select **Send Availability**
Select availability

1. Select **Friday** to let the administrator know when you have some free time. **NOTE - The dates available in the calendar may be different for you.**
2. Select some available time slots, note here that I have selected two separate blocks of time.
3. Select the **checkmark**.
1. Note your quick response and your availability that has been summarized.
2. Send the response.
Verify Sent Items Custom Box is syncing in the background

1. Tap the 3 Bars to access the folder list again.
2. Note that the Sent Items folder has 1 item in it now and is syncing on the background.
3. Close the folder list by selecting the 3 Bars again.
4. Click Inbox

Open a file into Content Locker

When we configured the settings for Workspace ONE Boxer in the Workspace ONE UEM Console we set attachments to open into white listed applications like VMware Content Locker. In this section we will show how to use this feature.
1. Select the **Mail** icon.
2. Select the email with subject **PDF and Image files** (or any email with an attachment).
3. Select the **SamplePDF.pdf** file (or any supported file).
Open the File Options

1. Tap the **File Options** button (triple dots).
2. Tap **Open in**
Open the file into Content Locker

Tap **Copy to Content** to open the file in Content Locker.
Accept the Privacy Prompt

Tap **I understand** to accept the Privacy prompt.
Agree to the Data Sharing Prompt

Tap **I agree** to accept the Data Sharing Prompt.

Accept permissions requests for Content Locker

Select **OK** for any pop up permission requests for Content Locker.
Dismiss intro to Content Locker

Welcome to

Content

Securely view, share and collaborate on content.

Dismiss

Select **Dismiss**.
Return to Boxer

You can now view or save the file to a store in Content Locker. When you are ready to return to Boxer tap the < Boxer button in the upper left corner of the screen.

Workspace ONE Boxer Conclusion

This concludes the Introduction to Workspace ONE Boxer. You may continue to explore Workspace ONE Boxer and move to the next step when you are ready.
Un-enrolling Your Device

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

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

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

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

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

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

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

Find the Enterprise Wipe Option

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

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

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

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

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

1. On your device, open the AirWatch **Agent** application.
2. Tap the **Device** section (under **Status**) in the middle of the screen.
3. Tap **Send Data** near the top of the screen. If this does not make the device check in and immediately un-enroll, continue to Step #4.
4. If the above doesn't make it immediately un-enroll, then tap **Connectivity [Status]** under Diagnostics.
5. Tap **Test Connectivity** at the top of the screen.

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

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

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

**NOTE - The applications and settings pushed through Workspace ONE UEM should have been removed. The Agent will still be on the device because that was downloaded manually from the App Store. Due to lab environment settings, it may take some time for the signal to traverse through the various networks out and back to your device. Continue on to the next step to force the wipe if the needed.**
Force the Wipe - IF NECESSARY
Settings

- Airplane Mode
- Wi-Fi
- Bluetooth
- Cellular Data

Notifications

Control Center

Do Not Disturb

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

Passcode

VPN

- Not Connected

Device Management

- Device Manager

Battery

Privacy

iTunes & App Store

Accounts & Passwords

Mail

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 Manager](image)

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

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

2. Tap **Remove** on the Remove Management prompt.

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

Workspace ONE Boxer is an industry leading e-mail app with features and functionality targeted towards increased productivity. As we saw in this lab, the containerization of business data from personal data enables IT organizations to exceed their enterprise security, compliance, data loss prevention (DLP) and user privacy requirements.
Module 2 - Workspace

ONE Web
Introduction

Workspace ONE Web is an Enterprise-grade mobile browser that can be configured to meet your business requirements by providing a streamlined and productive browsing experience for your employees without sacrificing security and compliance by providing features like kiosk mode, bookmarks and tunneling. Learn how to configure and deploy Workspace ONE Web to an iOS device and explore the configurations from an end-user perspective.

Workspace ONE Web Feature Overview

Before diving in, explore the features available in Workspace ONE Web to better understand the use cases that could benefit from deploying Workspace ONE Web to their mobile workforce.

Productivity:

1. Per-App VPN allows employees to access corporate web apps and intranet sites without manually connecting.
2. Corporate home pages and bookmarks can be pre-configured for a no-hassle setup.
3. Personal bookmarks can be synced across devices automatically.
4. Utilize built-in SSO to eliminate authentication issues and challenges.
5. Seamlessly access web app links from business emails by integrating with VMware Boxer.

Security:

1. End-to-end encryption of data at rest and in-transit with AES 256-bit encryption.
2. Separate business and personal data, allowing you to manage security policies while keeping individual information private.
3. Employ Data Loss Prevention (DLP) controls to determine whitelisting/blacklisting, cut/copy/paste restrictions, cookie behaviour, and more.
4. Trigger manual or automatic compliance actions to block or wipe enterprise data based on flexible policies.

Line of Business:

1. Lock the device into a single, configurable web application kiosk.
2. Control browsing to specific home pages, web apps, and links.
3. Remove the navigation bar for a controlled browsing experience.
4. Enable shared device modes using Workspace ONE Web as the central point for users to log in and out.
Lab Overview

In this lab, you will be configuring a few of the features in Workspace ONE Web that will showcase:

• Automatic Per-App VPN access to intranet sites
• Data Loss Prevention (DLP) controls
• Kiosk mode browsing
• Configuring bookmarks for easy access
• Whitelisting/Blacklisting sites for a controlled browsing experience
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

- 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
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.
Workspace ONE UEM Console Configuration

This section will explain what configurations must be made in the Workspace ONE UEM Console to achieve the features and restrictions that were outlined in the Introduction section.

iOS Per-App VPN Profile

This section will explain how to create a Per-App VPN profile, which will be used to allow Workspace ONE Web to connect to an intranet site.

Add a Profile

1. Click **Add**
2. Click **Profile**
Select the Platform

Add Profile

Select a platform to start:

Android

Apple iOS

Click Apple iOS
Configure the General Properties of the Profile

1. Enter \textit{Per-App VPN} as the Name.
2. Select \textit{All Devices (your@email.shown.here)} as the Assigned Group.
Enable the VPN Payload

1. Click the **VPN** payload tab.
2. Click **CONFIGURE**
Configure the VPN Payload

VPN

Connection Info

Connection Name *: VPN Configuration

Connection Type *: VMware Tunnel

Server *: TCP://holtunnel.airwlab.com:4025

Per-App VPN Rules:

Enable VMware Tunnel:

Provider Type: AppProxy

Safari Domains:

1. Set **Connection Type** to **VMware Tunnel**.
2. Set **Enable VMware Tunnel** to enabled.
3. Click **SAVE & PUBLISH**
Publish the VPN Profile

Click PUBLISH

Configure Security Policies

This section will explain how to configure the default Security Policies to determine DLP controls.
Navigate to All Settings

1. Click Groups & Settings
2. Click All Settings
Navigate to Security Policies

1. Click Apps
2. Expand Settings & Policies
3. Click Security Policies
4. Set Current Setting to Override

Configure Data Loss Prevention

1. Data Loss Prevention
   2. ENABLED
   3. Enable Bluetooth
   4. Enable Camera
   5. Enable Composing Email
   6. Enable Copy and Paste Out
1. Scroll down to find the **Data Loss Prevention** section.
2. Click **ENABLED** for **Data Loss Prevention**.
3. Ensure **Enable Printing** is set to **NO**
4. Ensure **Enable Camera** is set to **NO**
5. Ensure **Enable Composing Email** is set to **NO**
6. Ensure **Enable Copy and Paste** is set to **NO**

### Save Security Policies Settings

![Image of security settings with options to inherit, override, or inherit or override]

1. Scroll down to the bottom of the Security Policies menu.
2. Click **SAVE**

### Confirm Saved Security Policies

![Image of saved successfully prompt]

Confirm that the **Saved Successfully** prompt shows.

### Configure Workspace ONE Web Settings

This section will explain how to configure the Workspace ONE Web settings, including security settings, whitelisted and blacklisted sites, bookmarks and kiosk mode.
Navigate to Browser Settings

If you already closed the All Settings menu, reopen it by click Groups & Settings > All Settings.

1. Click Apps
2. Click Browser
3. Set Current Setting to Override
Configure Kiosk Mode Settings

<table>
<thead>
<tr>
<th>Mode</th>
<th>Kiosk Mode</th>
<th>Return Home After Inactivity</th>
<th>Clear Cookies and History with Home</th>
<th>Enable Multiple Tabs Support</th>
<th>Home Page URL</th>
<th>Selection Mode</th>
<th>Denied Site URLs</th>
</tr>
</thead>
</table>

1. Scroll down to find the **Mode** section.
2. Select **Enabled** for **Kiosk Mode**.
3. Select **Enabled** for **Enable Multiple Tabs Support**.
4. Enter **https://internal.airwlab.com** for the **Home Page URL**.
5. Select **Deny** for **Selection Mode**. This enables Blacklisting for the included site URLs, where selecting Allow would enable Whitelisting for the included site URLs.
6. Enter ***.airwatch.com** for the **Denied Site URLs**. This will allow traffic to all URLs except the *.airwatch.com domain.

**NOTE - Normally, Kiosk Mode would restrict Workspace ONE Web to a single page and it’s available links. For the purposes of the lab, we enable Multiple Tabs Support to showcase multiple bookmarks. In this mode, the navigation bar returns and bookmarks can be selected from the menu, but other items are still restricted in this mode.**
Save Browser Settings

1. Scroll down to the bottom of the Browser Settings page.
2. Click **SAVE**

Navigate to the Bookmarks Tab

1. The menu will return to the top, and you should see the Saved Successfully prompt display.
2. Click **Bookmarks**
Add New Bookmark

1. Select Current Settings as Override
2. Enter name as Internal Splash Page
3. Enter URL as https://internal.airwlab.com
4. Click ADD BOOKMARK
5. Enter name as AirWatch Home
6. Enter URL as https://www.airwatch.com
7. Click Save.
Close the Browser Settings Page

1. Confirm the **Saved Successfully** prompt shows.
2. Click X to close the pop-up window.

Add Workspace ONE Web as a Public App

1. Click **Add**
2. Click **Public Application**
Search for the Application to Add

Add Application

1. Select Apple iOS from the Platform dropdown.
2. Enter Workspace ONE Web in the Name field.
3. Click Next

Select the Application From the Search Results

Click Select on the Workspace ONE Web application.
Save and Assign Workspace ONE Web

Add Application - Web - Workspace ONE

Public | Managed By: your@email.shown.here | Application ID: com.air-watch.security

Details | Terms of Use | SDK

Name* Web - Workspace ONE

View in App Store

Categories
Start Typing to Select Category...

Supported Models
iPad
iPhone
iPad Touch

Click SAVE & ASSIGN
Add Assignment for Workspace ONE Web

Click + ADD ASSIGNMENT

Configure Workspace ONE Web Assignment Settings

1. Click in the Selected Assignment Groups field. This will pop-up the list of created Assignment Groups. Start Typing All Devices (your@email.shown.here) and select the All Devices (your@email.shown.here) Group.
2. Select AUTO for the App Delivery Method.
Configure Policies for Workspace ONE Web

1. Scroll down to find the Policies section.
2. Select **ENABLED** for **Remove On Unenroll**
3. Select **ENABLED** for **App Tunneling**
4. Select the profile named **Per-App VPN** you created in the earlier section.
5. Click **ADD**
Confirm Assignment and Save

1. Confirm that the Assignment you just configured is displayed.
2. Click **SAVE & PUBLISH**
Preview Assigned Devices and Publish

In order to leverage the Per-App VPN profile we created for Workspace ONE Web, we will need to also publish VMware Tunnel to the device.

Add the VMware Tunnel Client as a Public Application

In order to leverage the VPN profile, the VMware Tunnel Client must be installed on your device. We can leverage AirWatch to deploy the client as a managed application to the device. This step will walk you through the process of adding the client application to the AirWatch Console to automatically install on enrolled devices. Please note, while it is required that the Tunnel client application is installed on any device using Per App Tunnel, it does not have to be a managed application. Users can download the VMware Tunnel client from the App Store.

Click **PUBLISH**

**Publish the VMware Tunnel Application**

In order to leverage the Per-App VPN profile we created for Workspace ONE Web, we will need to also publish VMware Tunnel to the device.
Add VMware Tunnel as a Public App

1. Click Add
2. Click Public Application

Search App Store for VMware Tunnel

Add Application

- Managed By: your@email.shown.here
- Platform*: Apple iOS
- Source: SEARCH APP STORE
- Name*: VMware Tunnel

Next
1. Select **Apple iOS** for the **Platform**.
2. Enter **VMware Tunnel** for the **Name**.
3. Click **NEXT**

**Select the VMware Tunnel Result**

Search

<table>
<thead>
<tr>
<th>VMware Tunnel</th>
<th>Country</th>
<th>United States</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.vmware.ios-tunnel</td>
<td>Free</td>
<td></td>
</tr>
<tr>
<td>Category: Business</td>
<td>Current Version: 3.0.0</td>
<td></td>
</tr>
</tbody>
</table>

VMware Tunnel securely connects both internally built and public App Store applications to corporate resources within a secure network. Using the Network Extensions framework, VMware Tunnel allows you to access corporate resources behind the firewall, giving you easy access to what you need to be productive. Only managed applications can establish a connection with corporate resources, ensuring your personal privacy is maintained. Note: VMware Tunnel will not operate without the required AirWa...
Save and Assign VMware Tunnel

Click **SAVE & ASSIGN**
Add Assignment for VMware Tunnel

Click + Add Assignment.

Configure VMware Tunnel Assignment Settings

1. Click in the Selected Assignment Groups field. This will pop-up the list of created Assignment Groups. Start Typing All Devices (your@email.shown.here) and select the All Devices (your@email.shown.here) Group.
2. Select Auto for the App Delivery Method.
Configure Policies for VMware Tunnel

1. Scroll down to find the Policies section.
2. Select **ENABLED** for **Remove On Unenroll**.
3. Click **ADD**
Confirm Assignment and Save

VMware Tunnel - 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 the Assignment you created is displayed.
2. Click **SAVE & PUBLISH**
Preview Assigned Devices and Publish

Preview Assigned Devices

Assignment Status | All | Search List

| Assignment Status | Friendly Name | User | Platform/OS/Model | Organization Group |

No Records Found

Click **PUBLISH**
iOS Device Enrollment

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

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

NOTE - Checked out devices will likely have the Workspace ONE Intelligent Hub already installed. You may skip this step if your device has the Workspace ONE Intelligent Hub installed.

At this point, if you are using your own iOS device or if the device you are using does NOT have the Workspace ONE Intelligent Hub Application installed, then install the application from the App Store.
To Install the Workspace ONE Intelligent Hub application from the App Store, open the App Store application and download the free *Workspace ONE Intelligent Hub* application.

**Launching the Workspace ONE Intelligent Hub**

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

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

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

Click on the Server Details button.

Find Your Group ID From the Workspace ONE UEM Console

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

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

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

![Workspace ONE Intelligent Hub](image)

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

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

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

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

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

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

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

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

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

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

Congratulations!

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

You may navigate away from this page.

Open this page in “Hub”?  

Open

Cancel!

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 NECED)

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**

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)

Tap **I agree** for the Data Sharing policy.
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.
Explore Workspace ONE Web

We will now launch and explore Workspace ONE Web to confirm that the settings we've configured are controlling the application as expected.

Confirm Intranet Access in Safari

Let's try to access internal web page from Safari Browser first to ensure that we can't connect it without any VPN.

Launch Safari

Tap Safari.
Attempt to Navigate to the Intranet Site

1. Navigate to https://internal.airwlab.com
2. Tap Go.

Confirm Safari Cannot Access the Intranet Site

![Safari error message](image)

Confirm that Safari cannot open the intranet site.

**Confirm the Workspace ONE Web Configurations**

Now, let's access the same link from Workspace ONE Web.

**Launch the Workspace ONE Web app**

![Workspace ONE Web app icon](image)

Tap the **Workspace ONE Web** app.
Accept the Privacy Prompt

Tap I understand to accept the Privacy prompt.
Agree to the Data Sharing Prompt

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.

Tap I agree to accept the Data Sharing Prompt
Confirm Automatic Per-App VPN

We configured our Home Page URL for Workspace ONE Web to load our intranet site (http://internal.airwlab.com). Notice that upon launch, Workspace ONE Web is able to successfully connect to the intranet site due to the Per-App VPN profile and application configuration that was created earlier in the Workspace ONE UEM Console.

**NOTE - In this case, VPN is only authorized for the Workspace ONE Web application based on the configuration in the Workspace ONE UEM Console. There are no additional steps were required from the device user in order to activate or connect to the VPN. The VPN is only available to the Workspace ONE Web app instead of functioning as a device wide VPN, which was demonstrated by Safari being unable to connect to the intranet site.**
Confirm Data Loss Prevention (DLP)

Tap and hold over the **Welcome** text for about 2 seconds to select the text.

Notice that after selecting the text, you do not receive the standard Cut/Copy/Paste or Share options. This is due to the Data Loss Prevention settings that were configured in the Workspace ONE UEM Console to disable Copy and Paste and Printing functionalities.

Confirm Kiosk Mode
1. For reference, the first screenshot is when Kiosk Mode is Disabled. Notice that the Options menu that is available when Kiosk Mode is Disabled.
2. On our device, notice that the Options menu is missing from the navigation bar.

Normally, Kiosk Mode would prevent users from interacting with the navigation bar at all, restricting them to a single page. Since we enabled Multiple Tabs Support for Workspace ONE Web, our Kiosk Users are still able to interact with the navigation bar, but they are not able to modify any of the settings provided through the Options menu, ensuring the initial configuration pushed to the device remains the same.

Confirm Bookmarks

Let's validate the bookmarks we configured for Workspace ONE Web in Workspace ONE UEM Console.

Open a New Browser Tab

1. Click the Tabs button in the top-right corner.
2. Click the Add button to open a new tab.
Open AirWatch Home Bookmark

Notice that our two configured bookmarks, **Internal Splash Page** and **AirWatch Home**, are available on the device.

Tap **AirWatch Home** to load the AirWatch website (https://www.airwatch.com).

Confirm Denied Sites

Upon loading the AirWatch Home bookmark, notice that we instead receive a page notifying us that the website has been blocked by the administrator. This occurs because we configured the Denied Site URLs within the Workspace ONE Web configuration to deny access to the *.airwatch.com sites.
Review

You've now confirmed all of the configurations we deployed to Workspace ONE Web during our setup in the Workspace ONE UEM Console. Feel free to explore any other features of Workspace ONE Web and continue to the next step when you are ready.
Un-enrolling Your Device

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

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

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

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

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

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

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

Find the Enterprise Wipe Option

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

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

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

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

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

1. On your device, open the AirWatch Agent application.
2. Tap the Device section (under Status) in the middle of the screen.
3. Tap **Send Data** near the top of the screen. If this does not make the device check in and immediately un-enroll, continue to Step #4.
4. If the above doesn't make it immediately un-enroll, then tap **Connectivity [Status]** under Diagnostics.
5. Tap **Test Connectivity** at the top of the screen.

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

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

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

**NOTE - The applications and settings pushed through Workspace ONE UEM should have been removed. The Agent will still be on the device because that was downloaded manually from the App Store. Due to lab environment settings, it may take some time for the signal to traverse through the various networks out and back to your device. Continue on to the next step to force the wipe if the needed.**
Force the Wipe - IF NECESSARY
<table>
<thead>
<tr>
<th>Settings</th>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airplane Mode</td>
<td>USE SIDE SWITCH TO:</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Lock Rotation</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>Mute</td>
</tr>
<tr>
<td>Cellular Data</td>
<td>Rotation Lock is available in Control Center.</td>
</tr>
<tr>
<td>Notifications</td>
<td>iPad Storage</td>
</tr>
<tr>
<td>Control Center</td>
<td>Background App Refresh</td>
</tr>
<tr>
<td>Do Not Disturb</td>
<td>Restrictions</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>Not Connected</td>
</tr>
<tr>
<td></td>
<td>Device Management</td>
</tr>
<tr>
<td></td>
<td>Device Manager</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**

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

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

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

Workspace ONE Web has a wide variety of configurations that can be adjusted to meet your business needs across multiple platforms. We explored a few options through this lab, but there are more features that can provide a higher quality user experience at the level of security that your business requires. Consider how Workspace ONE Web can improve your productivity by providing a secure and configurable browsing experience!

This concludes this lab module.
Module 3 - Workspace
ONE Tunnel
Introduction

Leveraging Per-App VPN allows you to control which applications on a device have access to your VPN by automatically enabling or disabling VPN access based on which applications are active. This prevents you from needing to provide a device-wide VPN on your devices, which allows unintended or unauthorized apps or processes to access your VPN. Explore how to configure and deploy Workspace ONE Tunnel to enable per-app VPN on an enrolled device.
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 VMware! in the Password Recovery Answer field.
4. Enter VMware! 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.
Create Per-App VPN Profile

For iOS 7 and higher devices and Android Enterprise devices, you can force selected applications to connect through your corporate VPN. Your VPN provider must support this feature, and you must publish the apps as managed applications.

Create an iOS VPN Profile

In this step you will configure the iOS profile that will be delivered to the device to configure the VMware Tunnel Client on the device to allow only designated applications to access content on internal servers.

Add a New Profile

1. Click Add
2. Click Profile
Select the OS the profile will be used for.

Add Profile

Select a platform to start:

- Android
- Apple iOS

Click Apple iOS
Configure the General Properties of the Profile

1. Enter **Per-App VPN** as the Name.
2. Select **All Devices (your@email.shown.here)** as the Assigned Smart Group.
Add a VPN Payload

1. Click **VPN** from the Payload menu.
2. Click **CONFIGURE** to access the VPN payload settings.
Configure the VPN Payload

1. Select **VMware Tunnel** from the **Connection Type** dropdown.
2. Check the **Enable VMware Tunnel** box.
3. Click **SAVE & PUBLISH**
Publish the VPN Profile

View 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>
</table>

No Records Found

Click **PUBLISH**

[Image of a form with a Publish button and a message saying 'No Records Found']
Publish VMware Tunnel as a Public App

In this section you will create a Per-App VPN profile and deploy an Application configured to use the VPN Tunnel on iOS.

Add the VMware Tunnel Client as a Public Application

In order to leverage the VPN profile, the VMware Tunnel client must be installed on your device. We can leverage Workspace ONE UEM to deploy the client as a managed application to the device.

This step will walk you through the process of adding the client application to the Workspace ONE UEM Console to automatically install on enrolled devices. Please note, while it is required that the VMware Tunnel client application is installed on any device using Per App Tunnel, it does not have to be a managed application.

Users can download the VMware Tunnel client from the App Store.

Add VMware Tunnel as a Public App

1. Click Add
2. Click Public Application
Search App Store for VMware Tunnel

1. Select **Apple iOS** for the **Platform**.
2. Enter **VMware Tunnel** for the **Name**.
3. Click **NEXT**

**Select the VMware Tunnel Result**

VMware Tunnel

- **Free**
- **Category:** Business
- **Current Version:** 3.0.0

VMware Tunnel securely connects both internally built and public App Store applications to corporate resources within a secure network. Using the Network Extensions framework, VMware Tunnel allows you to access corporate resources behind the firewall, giving you easy access to what you need to be productive. Only managed applications can establish a connection with corporate resources, ensuring your personal privacy is maintained. Note: VMware Tunnel will not operate without the required AirWatch...
Click **SELECT** for the **VMware Tunnel** result.

**Save and Assign VMware Tunnel**

![Add Application - VMware Tunnel interface](image)

Click **SAVE & ASSIGN**
Add Assignment for VMware Tunnel

Click + Add Assignment.

Configure VMware Tunnel Assignment Settings

1. Click in the **Selected Assignment Groups** field. This will pop-up the list of created Assignment Groups. Start Typing **All Devices (your@email.shown.here)** and select the **All Devices (your@email.shown.here)** Group.
2. Select **Auto** for the **App Delivery Method**.
Configure Policies for VMware Tunnel

1. Scroll down to find the Policies section.
2. Select **ENABLED** for **Remove On Unenroll**.
3. Click **ADD**
1. Ensure the Assignment you created is displayed.
2. Click **SAVE & PUBLISH**
Preview Assigned Devices and Publish

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>
</table>

No Records Found

Click **PUBLISH**
Configure Workspace ONE Web for Per-App VPN

Now that the VMware Tunnel client is assigned to the appropriate group, this section walks through adding an application that is enabled to use Per App Tunnel. After enabling the setting that allows an application to use VPN, you must select the VPN profile that the app should use. This requires that any application you would like to leverage Per App VPN is pushed to the device from the Workspace ONE UEM Console as a managed app. There is one exception to this, which is the Safari application on iOS. This is covered in detail in a later section of this lab.

This step will walk you through the process of adding an application from the Public App store that will be associated to the VPN profile you created.

Add Workspace ONE Web as a Public App

1. Click Add
2. Click Public Application
Search for the Application to Add

Add Application

1. Select **Apple iOS** from the Platform dropdown.
2. Enter **Workspace ONE Web** in the Name field.
3. Click **Next**

Select the Application From the Search Results

Click **Select** on the **Workspace ONE Web** application.
Save and Assign Workspace ONE Web

Click **SAVE & ASSIGN**
Add Assignment for Workspace ONE Web

1. Click in the Selected Assignment Groups field. This will pop-up the list of created Assignment Groups. Start Typing All Devices (your@email.shown.here) and select the All Devices (your@email.shown.here) Group.

2. Select AUTO for the App Delivery Method.

Configure Workspace ONE Web Assignment Settings
Configure Policies for Workspace ONE Web

1. Scroll down to find the Policies section.
2. Select **ENABLED** for **Remove On Unenroll**
3. Select **ENABLED** for **App Tunneling**
4. Select the profile named **Per-App VPN** you created in the earlier section.
5. Click **ADD**
Confirm Assignment and Save

1. Confirm that the Assignment you just configured is displayed.
2. Click **SAVE & PUBLISH**
Preview Assigned Devices and Publish

Click PUBLISH
iOS Device Enrollment

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

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

NOTE - Checked out devices will likely have the Workspace ONE Intelligent Hub already installed. You may skip this step if your device has the Workspace ONE Intelligent Hub installed.

At this point, if you are using your own iOS device or if the device you are using does NOT have the Workspace ONE Intelligent Hub Application installed, then install the application from the App Store.
To Install the Workspace ONE Intelligent Hub application from the App Store, open the App Store application and download the free **Workspace ONE Intelligent Hub** application.

### Launching the Workspace ONE Intelligent Hub

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

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

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

Click on the Server Details button.

Find Your Group ID From the Workspace ONE UEM Console

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

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

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

![Workspace ONE Intelligent Hub](image)

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

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

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

1. Enter your **Group ID** for your Organization Group for the **Group ID** field. Your Group ID was noted previously in the **Finding your Group ID** step.
2. Tap the **Next** button.
You will now provide user credentials to authenticate to Workspace ONE UEM.

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

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

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

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

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

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

Congratulations!

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

You may navigate away from this page.

Open this page in “Hub”?

Open

Cancel

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.

[Button options: Don’t Allow, Allow]

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**

7:40 AM  Thu Oct 25

**Data sharing**

Want an even better app experience?

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

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

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

[I agree]

[Not now]

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

![Account](image)

**testuser**  
Basic Account  
Updated Today at 7:40 AM

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.
Testing Per App VPN

Now that the device is enrolled and has received the settings we configured in the Workspace ONE UEM Console, we are ready to begin testing the Per-App VPN functionality.

Testing Per App VPN on iOS

The applications assigned in the previous steps should push down during enrollment. The VMware Tunnel and Workspace ONE Web applications should be installed on your device.

Launch the Workspace ONE Web

Press the Home button on the iPad to return to the Launchpad. Swipe right to see the downloaded applications if needed.

Tap the Workspace ONE Web icon to launch the application. If prompted, select OK to allow the Web to send your device push notifications.
Accept the Privacy Prompt

Tap **I understand** to accept the Privacy prompt.
Agree to the Data Sharing Prompt

I agree

Tap I agree to accept the Data Sharing Prompt
Access the Internal Website with Workspace ONE Web

1. The application will launch and you will see the VPN icon appear indicating the connection is active. The application will now connect to Workspace ONE UEM and retrieve the settings for your Sandbox Organization Group. These settings include a default homepage that has been pre-configured for this lab. This website is available on an internal web server but not accessible from the public internet.

2. The website will load and you’ll see the Welcome message.

Attempt to Access the Website From Safari

We will now show that although the VPN connection is active, other applications on the device will not be able to access the Tunnel or the internal resources.
Select the URL from the Workspace ONE Web

1. **Press & hold** the Navigation Bar in Workspace ONE Web.
2. Choose **Select All** to highlight the URL for the internal site.

Copy the URL from the Workspace ONE Web

Select **Copy**.

Open Safari

Return to the launchpad by pressing the Home button on the iPad. Open **Safari** by selecting the icon from the Launcher.
Paste the URL Into the Safari Browser

1. Open a new tab by selecting the + sign on the navigation bar.
2. Select the entry box on the navigation bar.
3. Press & hold for a count of two then release on the entry box and select **Paste**.
4. Select **Go** on the keyboard.
Notice that the website does not load in the Safari browser due to DNS failure. The website is published to an internal DNS that can only be accessed when the VPN connection is being used. Although the VPN connection may remain active (look for the VPN icon in the status bar), Safari is not designated as an application that is allowed to use the Per-App VPN Tunnel. You may have multiple VPN configurations and multiple apps assigned for each VPN. Most Public applications (apps using Cocoa framework) are compatible with per-app VPN on iOS.
Safari Domain Profile Configuration

In this chapter you create a Per-App VPN profile and deploy an Application configured to use the VPN Tunnel on iOS.

Add a New Version to the iOS VPN Profile

In this step you will update the iOS profile created in the first step to include Safari domains.

Update the Per-App VPN Profile

Return to the Workspace ONE UEM Console.

1. Click Devices
2. Click Profiles & Resources
3. Click Profiles
4. Select the edit icon next to the Per-App VPN profile.
Add Version to update the existing profile

1. Click **ADD VERSION** to allow editing.
2. Select the **VPN** payload on the left hand side.
Configure Safari Domains

VPN

Connection Info

- **Connection Name**: VPN Configuration
- **Connection Type**: VMware Tunnel
- **Server**: TCP://holtunnel.airlab.com:4025
- **Per-App VPN Rules**: Checkered
- **Enable VMware Tunnel**: Checked
- **Provider Type**: AppProxy
- **Safari Domains**: airlab.com

Authentication

1. Enter airlab.com in the Safari Domains list.
2. Click SAVE & PUBLISH

**NOTE** - They syntax for Safari Domains does not require a wildcard character. Enter only the domain hostname to whitelist the entire domain to initiate VPN in Safari.
Publish the updated VPN Profile

View Device Assignment

Assignment Status | All | Filter Grid

<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>
</table>

No Records Found

Click PUBLISH
Testing Safari Domains with Per App Tunnel

Now that the VPN profile is updated to include the domain tested in the first example in the Safari Domains list, we can confirm these settings have updated on the device and test in the native Safari application.

Confirm the VPN Configuration Has Updated

This section will walk-through how to confirm that the VPN configuration has successfully updated on your device.

Open Device Settings

Tap Settings.
Open VPN Settings

1. Tap **General**.
2. Scroll down to find the VPN section.
3. Tap **VPN**.
Select Your VPN Configuration

Tap **VPN Configuration #819572** from your Per-App VPN profile.

---

**Tap VPN Configuration #XXXXXX** from your Per-App VPN profile.
### View Included Per-App VPN Apps

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>VMware Tunnel</td>
</tr>
<tr>
<td>Server</td>
<td>TCP://holttunnel.airlab.com:5065</td>
</tr>
</tbody>
</table>

To configure the settings for "VPN Configuration #60045", use the VMware Tunnel application.

- **Connect On Demand**: Off

#### INCLUDED APPS
- **Web**, airwlab.com
- **Safari**, airwlab.com

Note all managed applications from the Workspace ONE UEM Console enabled to use Per-App VPN and domains listed in **Safari Domains** in the VPN profile will appear in this list.

Whitelisting a domain in the **Safari Domains** list will initiate a VPN connection on demand whenever the user browses to a site within this domain.

**NOTE** - **Wildcards are not required when whitelisting a Safari Domain. The entire domain will automatically be whitelisted for VPN On Demand when added to VPN profile.**

### Attempt to Access the Website From Safari

We will now show that browsing to a site in the domain added to the "Safari Domains" list will initiate a VPN connection.
Open Safari

Return to the launchpad by pressing the Home button on the iPad. Open Safari by selecting the icon from the Launcher. The VPN icon should not be displayed in the toolbar.
Paste the URL Into the Safari Browser

1. Open a new tab by selecting the + sign on the navigation bar.
2. Select the entry box on the navigation bar.
3. Press & hold for a count of two then release on the entry box and select Paste or type https://internal.airwlab.com.
4. Select Go on the keyboard.
Browse to the Internal Webpage

Notice that the website now loads in the Safari browser after the VPN profile is updated to include airwlab.com in the Safari Domains list, whitelisting the domain for Per App VPN. The website is published to an internal DNS that can only be accessed when the VPN connection is being used.
Un-enrolling Your Device

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

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

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

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

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

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

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

Find the Enterprise Wipe Option

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

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

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

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

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

1. On your device, open the AirWatch Agent application.
2. Tap the Device section (under Status) in the middle of the screen.
3. Tap Send Data near the top of the screen. If this does not make the device check in and immediately un-enroll, continue to Step #4.
4. If the above doesn't make it immediately un-enroll, then tap Connectivity [Status] under Diagnostics.
5. Tap Test Connectivity at the top of the screen.

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

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

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

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

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

**Force the Wipe - IF NECESSARY**

![Screen shot of iOS Settings app showing Device Management]

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

1. Tap **Remove Management** on the Device Manager profile.

   *NOTE - If prompted for a device PIN, enter it to continue. VMware provisioned devices should not have a device PIN enabled.*

2. Tap **Remove** on the Remove Management prompt.

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

This lab module reviewed how to leverage native Per-App VPN capabilities by publishing Per-App VPN profiles to your devices to ensure that only authorized apps are accessing your VPN. This prevents users from needing to manually start and end VPN connections based on what apps they are accessing and provides an extra layer of security to your corporate resources by ensuring non-authorized apps are not able to connect to your VPN.

This concludes this lab module.
Introduction

The Workspace ONE App Catalog provides your users with a unified app catalog where they can access applications you deploy across all devices from anywhere and any time. This provides an identical experience across all your devices, streamlining this experience for your users.

In this exercise, you will explore the basic concepts of Mobile Application Management (MAM) with Workspace ONE UEM and learn how to deploy applications to the Workspace ONE App Catalog. You will enroll a device to explore the Workspace ONE App Catalog to see how users interact with and download apps from the App Catalog.
Different types of applications - Internal / Public / Purchased / Web Apps

Depending on the type and mode of deployment, Workspace ONE UEM classifies applications as Internal, Public, Purchased and Web apps.

- **Internal Apps** - These are internally developed apps and uploaded directly to the Workspace ONE UEM console or can also be imported from an external app repository. These applications are also known as Enterprise apps.
- **Public Apps** - These apps are available on respective app stores of the platforms i.e. App Store, Play Store, Windows Store etc.
- **Purchased Apps** - These apps are categorized as VPP (Volume purchased program) and Custom B2B apps. VPP allows businesses and educational institutions to purchase publicly available iOS applications. However, custom B2B apps are specifically developed third party iOS applications in volume for distribution to corporate devices.
- **Web Apps** - They provide end-users a way to access a URL directly from an icon on menu of their device.

<table>
<thead>
<tr>
<th>Platform/ Type</th>
<th>Internal</th>
<th>Public</th>
<th>Web</th>
<th>Purchased</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Desktop</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Google Chromebook</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

HOL-1957-07-UEM
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.

IF YOU HAVE PURCHASED VMware Identity Manager AS A SERVICE, YOUR USE OF VMware Identity Manager IS SUBJECT TO THE VMware Identity Manager TERMS OF SERVICE AVAILABLE AT: HTTP://WWW.VMWARE.COM/DOWNLOAD/EULA.HTML. IF YOU HAVE PURCHASED Workspace ONE AS A SERVICE, YOUR USE OF VMware Identity Manager IS SUBJECT TO THE WORKSPACE ONE TERMS OF SERVICE AVAILABLE AT:HTTP://WWW.VMWARE.COM/DOWNLOAD/EULA.HTML.

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

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.
Download AppLifecycle Apps

In this section, we are going to download AppLifecycle Apps that we will be using as Internal apps for this lab.

Download AppLifecycle 101

1. Open a new tab in Chrome Browser
2. Enter the following URL [https://hol.awmdm.com/MyDevice/s/2239/be759588-38d0-4ad4-949e-88a1f4398f4b](https://hol.awmdm.com/MyDevice/s/2239/be759588-38d0-4ad4-949e-88a1f4398f4b) and hit Enter
   
   **NOTE:** Remember that you can drag and drop text from the manual into the URL bar to avoid typing!
3. Validate that you have downloaded Applifecycle_101.ipa
Download AppLifecycle 102

1. Open a **new tab** in Chrome Browser.
2. Enter the following URL `https://hol.awmdm.com/MyDevice/s/2239/86896741-33e4-43fd-a843-6225742f002c` and hit **Enter**
   **NOTE:** Remember that you can drag and drop text from the manual into the URL bar to avoid typing!
3. Validate that you have downloaded **Applifecycle_102.ipa**
iOS Device Enrollment With Directory Account

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

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

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

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

**Launching the Workspace ONE Intelligent Hub**

Launch the [Hub](#) app on the device.

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

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

Click on the Server Details button.

Find Your Group ID From the Workspace ONE UEM Console

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

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

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

1. ![Image of Workspace ONE Intelligent Hub icon]
   - labs.awmdm.com
   - **{Your Group ID}**
   - Next

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

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

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

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

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

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

Workspace Services

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

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

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

Tap **Next** to begin.
Allow Website to Open Settings (IF 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.
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”?

Open

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

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

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

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

"Hub" Would Like to Send You Notifications

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

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

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

Your privacy matters.

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

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

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

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

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

**Accept the Data Sharing Policy**

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/helpl/about/company/privacy.html](https://www.vmware.com/helpl/about/company/privacy.html).

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.
Internal App Deployment

Use Workspace ONE UEM to distribute, track, and manage your internal applications. These are applications built in-house and not hosted on Public App Stores. You can upload the application files directly to Workspace ONE console for deployment. However, if you use an external repository to host your internal applications, then you can easily integrate that host with Workspace ONE UEM, instead of migrating the entire catalog to Workspace ONE UEM.

Supported File types for different platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>File Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>APK</td>
</tr>
<tr>
<td>iOS</td>
<td>IPA</td>
</tr>
<tr>
<td>macOS</td>
<td>APP Package Bundles</td>
</tr>
<tr>
<td>Windows Desktop</td>
<td>APPX, EXE, MSI, ZIP</td>
</tr>
<tr>
<td>Windows Phone</td>
<td>APPX, XAP</td>
</tr>
</tbody>
</table>

Once the application is installed, you can track the installation status and reason codes in case of failures.

Upload Internal Application with a Local File

In this section, you are going to add an IPA file to AirWatch console as an internal iOS app.

Add Internal Application
In the Workspace ONE UEM console,

1. Click on **Add**
2. Click **Internal Application**

**Upload**

Click **Upload**.

**Choose File**

Click **Choose File**.
Navigate to the iPA file

1. Click on **Downloads**
2. Select **AppLifecycle_101.ipa**
3. Click **Open**
Click **Save**.
Click Continue.
Application Details

1. Click the Details tab if it is not already selected.
2. Notice how Workspace ONE UEM can parse the Application bundle ID from the IPA File. All the application versioning within the Workspace ONE UEM Console is based on the Application ID.
3. Notice how Workspace ONE UEM can also parse the Application Version number from the IPA File.

Categories are useful to group the apps so that they are easy to find from the catalog.

Internal app version for iOS is determine by CFBundleVersion and CFBuildShortVersionString from info.plist
1. Scroll down on the Details page.
2. Select Category **Productivity (System)**. Categorizing apps allows you to filter them later in the Workspace ONE UEM Console or App Catalog.
3. You can also change the **minimum OS** requirement to be able install this app. For this lab, we are going to keep this value to default **iOS 9.0.0**.
4. Click on **Save & Assign**.

**Add an Assignment to the Internal Application**

We will now configure which devices will receive the internal application.
Add Assignment

Click **Add Assignment**.

**Add Delivery method**
1. All app assignments in Workspace ONE UEM are done via Assignment Groups. These assignment groups can be created by specifying different filter criteria on your devices and/or users. For this lab we are going to select our default group All Devices.

2. Your App Delivery method can be Auto where the application is installed automatically to the enrolled device. For this exercise, you are going to select On Demand to see how can we download these apps from Workspace ONE App Catalog instead.

3. You can also select the Deployment Begin Date for a particular app assignment. If you select a date in future, the app will not be available for download until that time. For this lab, we are going to keep the default value, which should reflect the current date.

Enable Remove on Unenroll

1. Scroll down until you see the Policies section.
2. Select **Enable** for Remove on Unenroll.
3. Click on **Add** to continue.

By enabling this option, you are flagging this app to be removed when the device is unenrolled after this lab is ended. You will have the same configuration for all the apps that we are going to deploy in this lab. You would enable this flag if you want to un-install the app so that the app data is not leaked when an employee leaves the organization or when the device is lost or stolen.

**Save & Publish**

![AppLifecycle - Update Assignment](image)

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).

Click on **Save & Publish** to continue.
Preview which devices fall under the All Devices assignment group and will have access to download this app. Click **Publish** to continue.
Provisioning Profiles for Enterprise Distribution

1. Click **Apps & Books**.
2. Expand **Applications**.
3. Click **Native**.
4. Click the **Internal** tab.
5. Validate that you have the application uploaded with the name as **AppLifecycle**.
6. In the **Version** column, you will see the version as **1.0.1**.
7. In the column **Renewal Date**, you will see when the provisioning profile is going to expire for this particular app.

You can renew this provisioning profile from the Workspace ONE UEM console (via the **Application Details > Files** menu), without having to rebuild and re-upload the app to the Workspace ONE UEM console. This simplifies the recurring task of profile renewal, without any intervention from App Developers and any interruption on the end user devices.

For this exercise, we are not going to renew the provisioning profile of this app.
Public App Deployment - Workspace ONE Catalog

Workspace ONE UEM offers two app catalogs - the Workspace ONE App Catalog and the AirWatch Catalog. Both catalogs support the features in the Apps Settings of the Workspace ONE UEM Console.

The Workspace ONE catalog integrates resources from environments that use VMware Identity Manager and Workspace ONE UEM. If your deployment does not use VMware Identity Manager, you still have access to the features previously released for the AirWatch Catalog.

In this lab, you are going to access the assigned apps via the Workspace ONE App Catalog, which is available as a public app from your device App Store.

Add Workspace One as a public app

1. Click Add.
2. Click Public Application.
1. Select **Apple iOS** for the platform.
2. Select **Search App Store** for the source.
3. Enter **VMware Workspace ONE** for the name.
4. Click **Next**.
Select Workspace ONE

Click **Select** for the VMware Workspace ONE app.
Save & Assign

Click **Save & Assign**
Add Assignment for Workspace ONE

Click **Add Assignment**.

**Select Group and Delivery Method**

1. Select **All Devices** for the Assignment Groups.
2. Select **Auto** for the App Delivery Method.

**TIP:** Automatic App Delivery ensures that the app is installed on the device automatically, without relying on end users to download it from the catalog. Use this setting for the apps that you want to make mandatory for your end users.
Modify Policies

1. Scroll down to the Policies section.
2. Select Enabled for Remove on Unenroll.
3. Select Enabled for Application Configuration.
Add Application Configuration

In this section, you are going to configure the Workspace ONE app so that it auto-populates the server URL and device UDID when the user launches the app.

**TIP:** Using Application Configuration (called **AppConfig**) to pre-configure apps reduces end user input requirements for a seamless end user experience!

1. Scroll down to the bottom of the page.
2. Click + Add to insert a second key value pair to configure.
3. Enter **AppServiceHost** for the first key.
4. Enter **https://hol-cn1193-** for the first configuration value. Don't change the Value Type from **String**.
   **NOTE:** This is the URL for the VMware Identity Manager tenant we have already configured for you to use with this exercise. This exercise will not cover setting up and configuring VMware Identity Manager, but other modules cover this topic if you are interested.
5. Enter **deviceUDID** for the second key.
6. Enter **{DeviceUid}** for the second configuration value. Don't change the Value Type from **String**.
7. Click **Add**.
NOTE: The {DeviceUid} is a lookup value, which means it will find the DeviceUDID at runtime and use the found value. There are dozens of Lookup Values available for you to use, and can be found by clicking the + Insert Lookup Value button besides the key value configurations.

NOTE: ALL of the configuration keys and Lookup Values are case sensitive!

Save & Publish

Click **Save & Publish**.
Publish the app

Click **Publish** to continue.
Accept the app installation prompt

As soon as the device checks in after the app is assigned, you will see a prompt on the device to install the Workspace ONE app.

Click **Install** to continue.

**NOTE:** The push notification to install the application may take a minute or two to display on the device.

**NOTE:** If you are using a supervised device, such as a borrowed device at VMworld, you will not see the prompt and the app will be installed automatically.
Log into Workspace ONE Catalog

Launch Workspace App

Click on the **Workspace** app to launch.

Create a Passcode (IF-NEEDED)

If you do not already have a device passcode set on the iOS device, you will receive a warning message before being able to access the Workspace ONE app. Please navigate to **Settings > Passcode > Turn Passcode On**, to setup a new passcode, then return to Workspace ONE.
Validate App Service Host URL from AppConfig

1. Validate that the pre-populated URL is https://hol-cn1193-ws1mam.vidmpreview.com.
2. Tap Next to continue.

This is the value that you entered for the key AppServiceHost while configuring the deployment options for the Workspace ONE app. This is how easy it is to pre-configure the Workspace ONE app for a seamless end user experience.
Select domain as corp.local

1. Select the **hol** domain.
2. Click **Next**.
Enter Credentials

1. Enter **aduser** for the username.
2. Enter **VMware1!** for the password.
3. Ensure that you are seeing **hol** as the domain.
4. Tap **Sign in**.
Enter Workspace ONE

Your workspace is ready.

Enter

Whenever you see the message Your Workspace is ready, tap on Enter.

Accept the Notifications Prompt (IF NEEDED)

"Workspace" Would Like to Send You Notifications
Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.

Don’t Allow  Allow

If you are prompted to enable Notifications for Workspace, tap Allow.
Accept the Privacy Policy

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 Workspace 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.

Device Management
Tap here for an overview of data collected from this device to provide access to work resources and to secure company data stored on this device. The data collected is based on your company's configuration. Your company has access to this data and some or all of the data collected may be visible to your IT administrator.

Data collected by Workspace
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.

Workspace 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.

Tap I Understand when the Privacy Policy is displayed.
Accept Data Sharing

Tap I Agree when the Data Sharing prompt is displayed.
Internal App Versioning

Internal and Enterprise apps get updated on a regular basis to offer latest functionality and security enhancements. Workspace ONE makes it easy to update these apps on end user devices over-the-air automatically, without having to connect the device to a computer. In this section, we are going to add an internal app on-demand and install it from Workspace ONE catalog. You will also see how to update the app in the Workspace ONE UEM console so that it gets updated on the enrolled device without any app data loss.

Install the Internal app from Workspace ONE Catalog

Since you do not have many apps deployed in this lab, you can see all the apps from the default view. However, you are will still validate the app category we assigned while deploying our internal app.

Validate the Category of the internal app

![App View]

<table>
<thead>
<tr>
<th>All Apps</th>
<th>Productivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Apps</td>
<td>VMware</td>
</tr>
<tr>
<td>Recommended</td>
<td>Workspace ON</td>
</tr>
<tr>
<td></td>
<td>Installed</td>
</tr>
</tbody>
</table>

**NOTE:** The Menu icon only appears if your device is in portrait orientation. If you are holding your device in landscape orientation, you will need to rotate it to see the Menu icon.

1. Tap on the **Menu icon** in the top right corner.
2. Tap on **Productivity** to filter the apps with that category.
Install 1.0.1 version of the internal app

Validate that you only seeing AppLifecycle v1.0.1 for the Productivity category. Click on Install to continue.

Confirm Installation in Workspace ONE Catalog

Click on Install to initiate the app installation.
Accept the App Installation (IF NECESSARY)

Click on Install to accept OS prompt for installing the internal app.

**NOTE:** If your device is supervised, then you will not see the OS prompt for installing internal and enterprise apps. iOS device supervision enables the internal apps to be installed silently.

**Confirm app installation on the device**

Click on the Home button of the iPad to return to the springboard. Confirm that the app **AppLifecycle** was installed successfully.

**Add an updated version of the Internal app to the Workspace ONE UEM Console**

You will now upload a new version of our internal app to see how this reflects in the Workspace ONE UEM Console as well as on the device.
Navigate to the Internal app

Back to the Workspace ONE UEM console,

1. Click on Apps & Books.
2. Expand Applications.
3. Click on Native.
4. Click the Internal tab.
5. Click on the hyperlink for AppLifecycle.

Add Version

Click on Add Version in the top right corner.
Upload the new version

1. While updating the new version of the app, Workspace ONE UEM displays the current active version to help determine the app upgrade path.
2. Click **Upload**.

Choose File

Click **Choose File**.
Navigate to the iPA file

1. Click on **Downloads**
2. Select **AppLifecycle_102.ipa**
3. Click **Open**

Please ensure that you are uploading the ipa files from the Downloads folder.
Save

Click **Save**.

**NOTE**: The application may take around 45 - 60 seconds to upload.
Complete the app update

1. Validate that you have uploaded **AppLifecycle_102.ipa**
2. Click **Save** to continue.
Save & Assign

While retaining all the defaults, click on **Save & Assign**.
While retaining all the defaults, click on **Save & Publish**.
Publish to Devices

Preview Assigned Devices

Preview your device assignment and click **Publish** to continue.

**Install the updated version of the app from Workspace ONE Catalog**

Let's view the update process on the device in Workspace ONE when apps are updated through the AirWatch Console.
Launch Workspace ONE

Back to the enrolled iPad, tap on the icon to launch **Workspace ONE app**.

**Enter Passcode For Timeout (IF NEEDED)**

Enter iPad passcode for “Workspace”

![Passcode Keypad]

In case you encounter a timeout, enter the iPad passcode to log back into Workspace App.
Refresh Workspace ONE Catalog and update the app

You may be seeing the old version of the app (1.0.1) after launching the Workspace ONE app. Swipe down in the screen to refresh.

1. After the refresh, ensure that you are seeing v1.0.2 for AppLifecycle.
2. Click on Update.

Confirm Installation in Workspace ONE Catalog

You will be taken out of this catalog to the home screen on your device, and the download will begin automatically.

Click on Install to initiate app installation.
Confirm app update on the device

Click on the Home button of the iPad to return to the springboard. Confirm that you are seeing the blue dot next to the app **AppLifecycle** which indicates that app was updated successfully.

Uninstall the app from managed devices

As a part of the Workspace ONE UEM flexible deployment, the app removal from Workspace ONE UEM has three different phases:

1. **Retire** - Removes an application from all managed devices. For iOS devices, if an older version of the application exists in the Workspace ONE UEM solution, then this older version is pushed to devices.
2. **Deactivate** - Removes an application and all versions of it from all managed devices.
3. **Delete** - Deletes the app from Workspace ONE UEM Database. If the application is currently installed on any devices, it puts the app in the Deactivated state first. You can then remove the app by changing the filter to Inactive.

Use the **Retire** option if you want to revert to an earlier version, without uninstalling the app from all the enrolled devices.
Web App Deployment

Web applications are useful for navigating to complex URLs with many characters. You can place Web application icons on the springboard to minimize the frustration with accessing these websites. These icons connect end-users to internal content repositories or login screens, so end-users do not open a browser and type out a long or complex URL.

Add Web App to the Workspace ONE UEM Console

Continue to walk-through the process of adding a Web app through the Workspace ONE UEM Console.

Navigate to Web Apps

Back to the Workspace ONE UEM Console,

1. Click on Apps & Books.
2. Expand Applications.
4. Click Web Links.
5. Click on +Add Application.
Select Platform

1. Select platform as Apple iOS.
2. Click Continue.
Enter Details

1. Click on the Details tab if it is not selected already.
2. Enter VMware for the name.
3. Enter https://www.vmware.com for the URL.

Add an image

1. Click or drag files here
You can associate an icon with your web app so that it is easily distinguishable from the other native apps. Having an icon in alignment with your organization branding guidelines helps your end users to easily identify them and results in better end user experience.

1. Click on the **Images** tab.
2. Click on the icon section to add an image.

### Navigate to Image file

1. Expand **Documents**
2. Expand **HOL**
3. Click on **Intro to MAM**
4. Select **VMware.jpg**
5. Click **Open**
Validate the icon

Confirm that you are now seeing the VMware image file as the icon for the web app.
Configure Assignment

1. Click the Assignment tab.
2. Select All Devices (your@email.shown_here) for Assigned Groups.
3. Select Auto for Push Mode
4. Click Save & Publish.

By configuring the Push Mode to Auto, the web app will be installed automatically on the device.
Publish the Web App

View 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>Added</td>
<td>aduser iPad iOS 1...</td>
<td>aduser</td>
<td>Apple iOS / iOS 11.2...</td>
<td></td>
<td><a href="mailto:your@email.shown.h">your@email.shown.h</a>...</td>
</tr>
</tbody>
</table>

Page Size: 20

Items 1-1 of 1

Click on **Publish** to continue.
Validate the Web App in AirWatch Console

Validate that you are now seeing **VMware** web app for iOS added in Workspace ONE UEM Console.

**Access the Web App from enrolled device**

Now that the Web app is added to the AirWatch Console and published to devices, let's view and interact with the Web app from our device.

**Confirm the Web App Installation**

As soon as the device checks back in with Workspace ONE UEM, a bookmark/web-clip will be installed for the **VMware** web app you just configured.
Launch the Web App

Notice that Safari was opened and displayed the VMware homepage.

**NOTE:** The Homepage may differ from the screenshot.
Remove Apps via Workspace ONE UEM Console

So far, we have seen how to deploy apps using Workspace ONE UEM. Having the ability to remove the apps from a device is as important as deploying them, especially in the scenarios where a device is lost or stolen or if an employee leaves the organization. This not only clears the sensitive app data from the device but it also revokes access to the corporate resources and functionality that the app has access to.

Uninstall the Web App

In this section, we will see how to remove the apps from the enrolled devices.

Navigate to the Web App

Back in the Workspace ONE UEM Console,

1. Click on Apps & Books
2. Expand Applications
3. Expand Web
4. Click on Web Links
5. Click on Assigned Users icon showing a value of 1.
### Uninstall

1. Click on the X to the right of your device listing to remove the web app from your enrolled device.
2. Click OK from the pop-up window to confirm the action.
3. Click the X on the View Devices screen to close it.

### Validate Web App Removal on the device

Validate that the web app was removed from the enrolled device.

**NOTE:** The web app will not be removed until the device checks in with Workspace ONE UEM, so this may take several seconds after the command is issued.
Assume Management

Apple iOS enables Workspace ONE UEM to assume management of user-installed applications without requiring the deletion of the previously installed application from the device. In this section, we are going to install a public app from App Store and assume the management for it. This will enable us to perform all the mobile application management policies on this user-installed app, including removal upon un-enrollment. We will validate this in the next article.

Consider the scenario where your employee has installed the app from App Store directly (very common in BYOD - Bring Your Own Device). In that case this app is unmanaged since it is not pushed down via Workspace ONE UEM. As a result, this app can not have MAM (Mobile Application Management) enhancements like per-app VPN (to connect to a backend resource), App Config (to auto-configure the app over-the-air), or Data Loss Prevention (removal of the app in case the device is stolen or compromised).

In this section, we will see how to convert such apps as managed apps so that they can leverage the above Workspace ONE UEM Mobile Application Management (MAM) enhancements and much more.

Install an unmanaged app from App Store

Begin by downloading and installing an unmanaged app from the App Store on our device. You will assume management of this app in an upcoming step.

Launch App Store

Tap on App Store to launch.
Search Salesforce

1. Enter Salesforce in the search box.
2. Tap on GET to initiate the install.

Install Salesforce

Tap on Install.
Open Salesforce

Once the download is completed, tap OPEN to launch the app.
Accept Salesforce EULA

Salesforce.com EULA

Order Form Supplement for Salesforce for iOS

This is a legally binding agreement. Please read it carefully. By clicking "I Accept"; or installing or using the Salesforce for iOS software and/or any updates to such software provided by salesforce.com (the "Software"), you:

- agree to the following terms on behalf of the Salesforce customer with which you are employed, affiliated or associated (the "Customer"),
- represent that you have the authority to bind the Customer to these terms, and
- represent that you are an authorized User under the master subscription agreement between salesforce.com and the Customer (the "Master Subscription Agreement").

If you do not have such authority, are not an authorized User, or do not agree to these terms, you may not install or use the Software.

Apple Inc. may, at any time and without notice, restrict, interrupt or prevent use of the Software, or delete the Software from your or the Customer’s Apple devices, or require salesforce.com to do any of the foregoing, without entitling the Customer or you to any refund, credit or other compensation from salesforce.com or any third party (including, but not limited to, Apple Inc. or your network connectivity provider).

This Order Form Supplement was last updated on July 14, 2016. It is effective between the Customer and salesforce.com as of the date you first download, install or use the Software, whichever is earliest.

1. THIS ORDER FORM SUPPLEMENT

This Order Form Supplement is a part of each order form by which the Customer ordered the Salesforce service (including, but not limited to, the Salesforce Files component of the Salesforce Chatter service), or a Salesforce service incorporating the Salesforce service (an "Order Form"). The Order Form and this Order Form Supplement are governed by the Master Subscription Agreement. This Order Form Supplement adjusts certain terms of the Master Subscription Agreement, solely with respect to the Software. Capitalized terms used but not defined in this Order Form Supplement have the meanings given to them in the Master Subscription Agreement.

2. THE SOFTWARE

The Software allows Salesforce customers to use the Salesforce service from Supported Devices. A "Supported Device" is a combination of an Apple device model and relevant iOS software version(s) that is supported by the Software. The Software is provided by salesforce.com as a component of the Salesforce service.

3. WHO YOU ARE CONTRACTING WITH

This Order Form Supplement is being entered into between the salesforce.com entity named on the Order Form (either salesforce.com, inc., salesforce.com Canada Corporation, salesforce.com EMEA Limited, salesforce.com Singapore Pte Ltd, or salesforce.com Kabushiki Kaisha ("salesforce.com") and the Customer. In this Order Form Supplement, the term "salesforce.com" means that entity.

4. SOFTWARE LICENSE

The Software, including software embedded in the Software, is licensed, not sold, to the Customer by salesforce.com only under the terms of the Master Subscription Agreement, the Order Form and this Order Form Supplement, and salesforce.com reserves all rights not expressly granted to the Customer. This Software may include some third-party software: please see the Documentation for additional notices required by our licensors. The Customer or you own the media or device on which the Software is recorded or stored but salesforce.com retains ownership of the Software itself.

5. PERMITTED LICENSE USES AND RESTRICTIONS

(a) This Order Form Supplement allows you, as an authorized User under the Master Subscription Agreement, to use the Software on any Supported Devices and on no other devices.
(b) You may not distribute, or make the Software available over a network where it could be used by multiple devices at the same time.
(c) With respect to updates to the Software that salesforce.com may make available for download, this Order Form Supplement allows you to download such Software updates to update or restore the Software on any Supported Device.
(d) Except as and only to the extent permitted by applicable law, or by licensing terms governing use of open-sourced components included with the Software, neither you nor any other Customer personnel may copy, decompile, reverse engineer, disassemble, attempt to derive the source code of, decrypt, modify, or create derivative works of the Software or Software updates, or any part thereof. Any attempt to do so is a violation of the rights of salesforce.com and its licensors. If you or any other Customer personnel violate this restriction, you or they, and the Customer, may be subject to prosecution and damages.

Tap I Accept to accept Salesforce EULA.
Accept the notification prompt for Salesforce

“Salesforce1” Would Like to Send You Notifications
Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.

Don’t Allow  OK

Tap OK to accept the notification prompt for Salesforce.
Validate Connection options

Tap on the gear icon to validate the available connections. Notice that you are seeing just the default connections, Production and Sandbox.
Add the same application as a public app from the Workspace ONE UEM Console

Now that you have downloaded an unmanaged app, we will publish the same app from the Workspace ONE UEM Console as part of the process of assuming management.

Add Salesforce as a public app

In the Workspace ONE UEM Console,

1. Click **Add**.
2. Click **Public Application**.
Search for Salesforce

1. Select Apple iOS for the Platform.
2. Select Search App Store for the Source.
3. Enter Salesforce for the Name.
4. Click Next.

Select the Salesforce Result

Click Select on the Salesforce result.
Save & Assign

Click **Save & Assign**.
Add Assignment

Click on Add Assignment.

Select Group and Delivery Method

1. Select All Devices (your@email.shown.here) for the Assignment Groups.
2. Select Auto for the App Delivery Method.

NOTE: Automatic App Delivery ensures that the app is installed on the device automatically, without relying on end users to download it from the catalog. Use this setting for the apps that you want to make mandatory for your end users.
Enable Flags

1. Scroll down to the Policies section.
2. Select **Enabled** for Remove on Unenroll.
3. Select **Enabled** for Make App MDM Managed if User Installed.
4. Select **Enabled** for Application Configuration.

**NOTE:** Enabling the Make App MDM Managed if User Installed is the policy used if you wish to manage apps that have already been installed by the user. This is useful to ensure that the apps you are pushing down with AppConfig (Application Configuration) settings are not being overridden by user installed apps which will not be able to access the AppConfig settings.
Add App Config

**NOTE - Now, we will configure Salesforce app to have a connection to a custom domain using App Config. We will validate this new connection on the device at a later step.**

1. Scroll down until you see the **Application Configuration** section.
2. Enter **AppServiceHost** for the Configuration Key.
3. Enter **vmtestdrive.my.salesforce.com** for the Configuration Value.
4. Click **Add**.

<table>
<thead>
<tr>
<th>Configuration Key</th>
<th>Value Type</th>
<th>Configuration Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppServiceHost</td>
<td>String</td>
<td>vmtestdrive.my.sfd</td>
</tr>
</tbody>
</table>
Click **Save & Publish**.
Publish the app

We will now see how the Salesforce app becomes managed by AirWatch on our device.

Click **Publish**

Salesforce as managed app
Close Salesforce app
Double press the Home button to launch app switcher. Swipe up the salesforce app to close Salesforce app.

Relaunch Salesforce app

Tap on the icon to relaunch Salesforce app.

Accept App Management Change prompt

Review the App Management Change prompt confirming the EMM is managing this app now. Tap Close to continue.
Review the Connection List

1. Click on the **Gear Icon** to view the connections that are available.
2. Validate that you are seeing the new connection **vmtestdrive.my.salesforce.com** which we add via App Config.

**NOTE** - Since we assumed the management of the Salesforce app, we could update the app over-the-air with Application Configuration. This app will also get removed automatically when we un-enroll the device preventing any data loss from an user-installed app.

**NOTE** - You are not expected to be able to authenticate to the vmtestdrive.my.salesforce.com endpoint, this is simply to demonstrate the Application Configuration values applying to the device!

**Conclusion**

This is how easy it is to manage a user installed device via Workspace ONE UEM. This feature is very powerful in a BYOD scenario to enhance functionality and ensure proper security of the user installed apps.
Un-enrolling Your Device

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

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

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

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

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

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

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

Find the Enterprise Wipe Option

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

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

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

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

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

1. On your device, open the AirWatch **Agent** application.
2. Tap the **Device** section (under **Status**) in the middle of the screen.
3. Tap **Send Data** near the top of the screen. If this does not make the device check in and immediately un-enroll, continue to Step #4.
4. If the above doesn't make it immediately un-enroll, then tap **Connectivity [Status]** under Diagnostics.
5. Tap **Test Connectivity** at the top of the screen.

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

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

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

**NOTE - The applications and settings pushed through Workspace ONE UEM should have been removed. The Agent will still be on the device because that was downloaded manually from the App Store. Due to lab environment settings, it may take some time for the signal to traverse through the various networks out and back to your device. Continue on to the next step to force the wipe if the needed.**
Force the Wipe - IF NECESSARY
<table>
<thead>
<tr>
<th>Settings</th>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airplane Mode</td>
<td>USE SIDE SWITCH TO:</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Lock Rotation</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>Mute</td>
</tr>
<tr>
<td>Cellular Data</td>
<td>Rotation Lock is available in Control Center.</td>
</tr>
<tr>
<td>Notifications</td>
<td>iPad Storage</td>
</tr>
<tr>
<td>Control Center</td>
<td>Background App Refresh</td>
</tr>
<tr>
<td>Do Not Disturb</td>
<td>Restrictions</td>
</tr>
<tr>
<td></td>
<td>Off</td>
</tr>
<tr>
<td>General</td>
<td>Date &amp; Time</td>
</tr>
<tr>
<td>Display &amp; Brightness</td>
<td></td>
</tr>
<tr>
<td>Wallpaper</td>
<td>Keyboard</td>
</tr>
<tr>
<td>Sounds</td>
<td>Language &amp; Region</td>
</tr>
<tr>
<td>Siri &amp; Search</td>
<td>Dictionary</td>
</tr>
<tr>
<td>Passcode</td>
<td>iTunes Wi-Fi Sync</td>
</tr>
<tr>
<td>Battery</td>
<td>VPN</td>
</tr>
<tr>
<td>Privacy</td>
<td>Not Connected</td>
</tr>
<tr>
<td></td>
<td>Device Management</td>
</tr>
<tr>
<td></td>
<td>Device Manager</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**

![Device Manager 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

In this exercise, you have learned how to deploy and manage different types of applications using Workspace ONE. We also saw how to remove a managed app from a device and how to assume management of apps installed by the end users.
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-1957-07-UEM

Version: 20181104-123713