# Table of Contents

Lab Overview - HOL-1857-04-UEM - Workspace ONE Productivity Apps ......................2  
Lab Guidance ...........................................................................................................3  
Module 1 - VMware Boxer (30 minutes) .................................................................9  
  Introduction ...........................................................................................................10  
  Login to the AirWatch Console ...........................................................................11  
  Configure VMware Boxer ....................................................................................15  
  Add VMware Browser as a Public App ..................................................................25  
  iOS Device Enrollment (Using the e-mail address from lab automation) ...............31  
  Exploring VMware Boxer .....................................................................................49  
  Un-enrolling Your Device .....................................................................................71  
  Conclusion .............................................................................................................80  
Module 2 - VMware AirWatch School Manager (45 Minutes) .................................81  
  Introduction ..........................................................................................................82  
  Login to the AirWatch Console ..........................................................................84  
  Enabling VMware AirWatch School Manager .......................................................88  
  Creating the Class List ..........................................................................................91  
  Publish the Classroom Application .......................................................................96  
  Enroll Class Devices ..............................................................................................104  
  Control Student Devices with Classroom App .....................................................119  
  Un-enrolling Your Device .....................................................................................123  
  Conclusion .............................................................................................................132  
Module 3 - VMware Browser (45 Minutes) ............................................................134  
  Introduction ..........................................................................................................135  
  Login to the AirWatch Console ..........................................................................137  
  AirWatch Console Configuration ...........................................................................141  
  iOS Device Enrollment ..........................................................................................163  
  Explore VMware Browser .....................................................................................178  
  Un-enrolling Your Device .....................................................................................185  
  Conclusion .............................................................................................................194
Lab Overview - HOL-1857-04-UEM - Workspace ONE Productivity Apps
Lab Guidance

NOTE - It will 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.

AirWatch productivity apps are engaging and intuitive with a consumer-simple experience and enterprise-grade security. VMware Boxer provides better-than-native email experience with turbo-charged productivity features and integrated mail, calendar and contacts. AirWatch School Manager allows organizations to configure and deploy the Apple Classroom app for organizations ineligible to use Apple School Manager. VMware Browser provides you with an intuitive browsing experience and seamless access to backend services while protecting sensitive corporate data. Take this lab to learn how to setup and configure these productivity apps that your employees actually want to use.

Lab Module List:

- **Module 1 - VMware Boxer** (30 minutes) (Basic) Configure and explore VMware Boxer integration with AirWatch on an iOS device.
- **Module 2 - VMware AirWatch School Manager** (45 minutes) (Basic) AirWatch School Manager is designed to let organizations leverage Apple's Classroom application in organizations that are not eligible for Apple School Manager.
- **Module 3 - VMware Browser** (45 Minutes) (Basic) Configure and explore VMware Browser for iOS and learn how to utilize the features to meet your business requirements.

Lab Captains:

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

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

http://docs.hol.vmware.com

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

Location of the Main Console

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

Alternate Methods of Keyboard Data Entry

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

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

Accessing the Online International Keyboard

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

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

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

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

Click on the @ key

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

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

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

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

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

This cosmetic issue has no effect on your lab.

Look at the lower right portion of the screen
Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes your lab has not changed to "Ready", please ask for assistance.
Module 1 - VMware Boxer (30 minutes)
Introduction

As part of the Workspace ONE suite of apps, VMware 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 VMware Browser 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 VMware Boxer.
Login to the AirWatch Console

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

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.

Authenticate to the AirWatch Administration Console

Username

Your VLP Email Address

Password

VMware1!

Login

Trouble Logging In
The default home page for the browser is https://hol.awmdm.com. Enter your AirWatch Admin Account information and click the Login button.

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

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

**NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the AirWatch Hands On Labs server.**

**Accept the End User License Agreement**

**Terms of Use**

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

**End User License Agreement**

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

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

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

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

### Close the Welcome Message

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

1. Click on the **Don't show this message again** check box.
2. Close the pop-up by clicking on the **X** in the upper-right corner.
Configure VMware Boxer

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

Add the VMware Boxer Client as an iOS Public Application

We can leverage AirWatch to deploy and automatically configure the VMware email client on the device through AirWatch. 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

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

Click **Save & Assign**.

Add Assignment for VMware Boxer

Click **+ Add Assignment**.

Click + **Add Assignment**.
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

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 identity this email account configuration.
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**

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.

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

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 AirWatch browser.
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 VMware Boxer.
5. Enter "com.air-watch.content.locker" for **Whitelisted Applications**, if not whitelisted already. This allows VMware 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

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
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**
Add VMware Browser as a Public App

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

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 Browser” in the Name field.
3. Click Next

Select the Application From the Search Results

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

Click **Save & Assign**

Add Assignment for VMware Browser
Click + Add Assignment.

**Configure VMware Browser 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 Policies for VMware Browser**

- **Managed Access**
  - Enabled
- **Remove On Unenroll**
  - Enabled
- **Prevent Application Backup**
  - Enabled
- **Make App MDM Managed if User Installed**
  - Enabled
- **App Tunneling**
  - Enabled
- **Application Configuration**
  - Enabled
1. Scroll down to find the Policies section.
2. Select **Enabled** for **Remove On Unenroll**
3. 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 email address from lab automation)

A temporary Exchange mailbox has been generated for you to use throughout this lab. The account credentials were emailed to the email address associated with your VMware Learning Platform (VLP) account at the start of the lab and also uploaded to the AirWatch Content section of the AirWatch Console.

Locate Your Exchange Account Details

If you have access to your email account, continue to the next step to retrieve your Exchange account details. If you do not have access to your email account, continue to the step titled "Accessing Your Exchange Account Details in the AirWatch Console" for instructions.

Accessing Your Exchange Account Details by Email

Hello,

Due to your recent enrollment in HOL-1857-MDM-04, you have received a temporary Exchange mailbox that is necessary to complete the lab!

- **Email Address:** yourid1234@hol.airwlab.com
- **Password:** VMware1!
- **Domain:** HOL

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

The subject of the email will be titled "HOL-1857-04-UEM". After opening the email, note the **Email Address** field provided as you will need this during the following steps for device enrollment.

You can now continue to the "Enroll Your iOS Device" section.

Accessing your Exchange Account Details in the AirWatch Console

First, return to the AirWatch Console.
Download the Text File From AirWatch Content

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.
Copy the Email Address

1. Select the Email Address text and right-click.
2. Click Copy.

You will use this Email Address in the next step to enroll your iOS Device.

Enroll Your iOS Device

You are now going to enroll your iOS device for use with this module.
Download/Install AirWatch MDM Agent Application from App Store - IF NEEDED

NOTE - Checked out devices will likely have the AirWatch MDM Agent already installed. You may skip this step if your device has the AirWatch MDM agent installed.

At this point, if using your own iOS device or if the device you are using does NOT have the AirWatch MDM Agent Application installed, then install the AirWatch Application.

To Install the AirWatch MDM Agent application from the App Store, open the App Store application and download the free AirWatch MDM Agent application.
Find your Group ID from AirWatch 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.

Launching the AirWatch MDM Agent

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

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

Welcome to AirWatch!

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

The multi-step enrollment process begins with authentication.

Choose authentication method:

- Email Address
- Server Details
- QR Code

Click on the Server Details button.
Attach the AirWatch MDM Agent to the HOL Sandbox

Once the Agent has launched you can enroll the device. To do so, follow the below steps.

1. Enter "hol.awmdm.com" for the Server field.
2. Enter your Group ID for your Organization Group for the Group ID field. Your Group ID was noted previously in the Finding your Group ID step.
3. Tap the Go button.

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

1. Enter your **Username**, which will be the Email Address ending in "@hol.airwlab.com" that was sent to your VLP email address or retrieved via the AirWatch Console.

   **NOTE** - If you forgot the email address you received, revisit the previous steps "Locate Your Exchange Account Details" to retrieve it.

2. Enter "**VMware1!**" for the **Password**.

3. Tap the **Go** button.
Redirect to Safari and Enable MDM Enrollment in Settings

Enable Device Management

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

Why?

- Access your company resource
- Remove company data in the event of loss or theft

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

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

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

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

*NOTE - If a PIN is requested, it is the current device PIN. Provided VMware devices should not have a PIN.*
You should now see the iOS Profile Installation warning explaining what this profile installation will allow on the iOS device.

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

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

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

You should now see the iOS Profile successfully installed.

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

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

Authentication Complete

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

Click on Done to continue.

Accept Notification Prompt (IF NEEDED)

Tap Allow if you get a prompt for Notifications.

Accept the App Installation (IF NEEDED)
You may be prompted to install a series of applications depending on which Module you are taking. If prompted, tap **Install** to accept the application installation.
Exploring VMware Boxer

In this series of steps you will sync email to a sample account and get introduced to a few of the features in VMware 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 VMware Boxer

Return to the Launchpad of your iOS device and select the **Boxer** icon.

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 VMware 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 VMware Boxer. Continue to the next step.

Accept Boxer permissions

"Boxer" Would Like to Send You Notifications

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

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 **Sent Items**.
2. Verify the name has been entered.
3. Verify Background Sync is enabled.
4. Select the `< 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 Inobx.

**Open a link into AirWatch Browser**

Earlier we set Boxer to open all links into AirWatch Browser 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 AirWatch Browser

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

Edit your Swipe actions

<table>
<thead>
<tr>
<th>Swipe actions</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Left Short Swipe</td>
<td>Read/Unread</td>
</tr>
<tr>
<td>Left Long Swipe</td>
<td>Delete</td>
</tr>
<tr>
<td>Right Short Swipe</td>
<td>Read/Unread</td>
</tr>
<tr>
<td>Right Long Swipe</td>
<td>Actions</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.
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 VMware Boxer in the AirWatch Console we set attachments to open into white listed applications like AirWatch Content Locker. In this section we will show how to use this feature.
Return to your inbox

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 permissions requests for Content Locker

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

Welcome to

content locker

Securely view, share and collaborate on content.

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.

Conclusion of Intro to Boxer Lab

This concludes the Intro to Boxer lab. You may continue to explore 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 AirWatch.

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

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

Enterprise Wipe (un-enroll) your iOS device

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

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

1. Click Devices on the left column.
2. Click List View.
3. Click the checkbox next to the device you want to Enterprise Wipe.

NOTE - Your Device Friendly Name will very likely be different than what is shown. It will, however, be in the same location as shown on image in this step.
Find the Enterprise Wipe Option

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

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

1. Enter "1234" for the **Security PIN**. You will not need to press enter or continue, the console will confirm your PIN showing "Successful" below the Security PIN input field to indicate that an Enterprise Wipe has been requested. **NOTE:** If "1234" does not work, then you provided a different Security PIN when you first logged into the AirWatch Console. Use the value you specified for your Security PIN.

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

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

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

Feel free to continue to the "**Force the Wipe**" step to manually uninstall the AirWatch services from the device if network connectivity is failing.
Verify the Un-Enrollment

Press the Home button on the device to go back to the home screen. The applications pushed through AirWatch should have been removed from the device.

**NOTE** - The applications and settings pushed through AirWatch management should have been removed. The Agent will still be on the device because that was downloaded manually from the App Store. Due to lab environment settings, it may take some time for the signal to traverse through the various networks out and back to your device. Continue on to the next step to force the wipe if the needed.
If your device did not wipe, follow these instructions to ensure the wipe is forced immediately. Start by opening the iOS Settings app.
1. Tap **General** in the left column.
2. Scroll down to view the **Device Management** option.
3. Tap **Device Management** at the bottom of the list of General settings.

**Force the Wipe - IF NECESSARY**

Tap the **Workspace Services** profile that was pushed to the device.
1. Tap **Remove Management** on the Workspace Services profile.  
   *NOTE - If prompted for a device PIN, enter it to continue. VMware provisioned devices should not have a device PIN enabled.*
2. Tap **Remove** on the Remove Management prompt.
After removing the Workspace Services profile, the device will be un-enrolled. Feel free to return to the "Verify the Un-Enrollment" step to confirm the successful un-enrollment of the device.
Conclusion

VMware 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 - VMware AirWatch School Manager (45 Minutes)
Introduction

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

What is AirWatch School Manager

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

Requirements

AirWatch School Manager requires the following software and hardware:

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

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

Optional Functionality

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

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

Differences from Apple Education

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

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

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

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

### Typical Uses for AirWatch School Manager

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

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

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

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.

Authenticate to the AirWatch Administration Console

Username

Your VLP Email Address

Password

VMware1!

Login

Trouble Logging In
The default home page for the browser is https://hol.awmdm.com. Enter your AirWatch Admin Account information and click the Login button.

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

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

**NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the AirWatch Hands On Labs server.**

**Accept the End User License Agreement**

![End User License Agreement]

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

You will be presented with the AirWatch Terms of Use. Click the **Accept** button.
## Address the Initial Security Settings

### Security Settings

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

### Security PIN

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

<table>
<thead>
<tr>
<th>Security PIN</th>
<th>Show</th>
<th>Confirm Security PIN</th>
<th>Show</th>
</tr>
</thead>
<tbody>
<tr>
<td>1234</td>
<td>Show</td>
<td>1234</td>
<td>Show</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. Save
7. Click the **Save** button when finished.

### Close the Welcome Message

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

1. Click on the **Don't show this message again** check box.
2. Close the pop-up by clicking on the **X** in the upper-right corner.
Enabling VMware AirWatch School Manager

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

Enter Devices Settings

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

1. Under **Devices & Users**, click **Apple**.
2. Click **Education**.
3. Select **Override** for **Current Setting**.
4. Select **Enabled** for **Enable Education Features**.
5. Select **AirWatch** for the Class Source.
6. Click **Save**.
Enter Security PIN

You are about to perform the Education Settings Change action. Please review all the information below carefully and then enter your Security PIN to proceed.

Disabling Education setting will remove all data tied to this component including classes and app assignment. Any apps, profiles or content assigned to a device will be removed from those devices as well. Any DEP profiles with the "Shared" option enabled will be deleted as well.

This action cannot be undone. Please proceed with caution.

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

Close Device Settings

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

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

The Education Overview Hub

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

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

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

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

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

Add a Public Application

In the top-right corner of the AirWatch Console:

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

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

Select the Classroom App

1. Find the Apple **Classroom** app in the list. The identifier will be **com.apple.classroom**.
NOTE - It may not be the first result and may require you to scroll down to find it!

2. Click **Select** on the Apple Classroom app.
Review Classroom Application Information
Review the information about the application you've selected and click **Save & Assign**
Configure the Classroom Assignment Settings

Classroom - Update Assignment

1. On the "Update Assignment" screen, click **Add Assignment**.
Create the Classroom Configuration.

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

1. Assign to your "All Device" smart group.
2. Set the app delivery method as "Auto".
3. Scroll down to the policies section and select **Enabled** for Remove On Unenroll.
4. Click Add.
Finish the Classroom Configuration and Save

Classroom - Update Assignment

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).

Add Assignment

<table>
<thead>
<tr>
<th>Name</th>
<th>Priority</th>
<th>App Delivery Method</th>
<th>Managed Access</th>
<th>Remove On Unenroll</th>
<th>Prevent Application Backup</th>
<th>VPN Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Devices</td>
<td>0</td>
<td>Auto</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Save & Publish

Click **Save & Publish**.

Publish the Classroom App

Preview Assigned Devices

No Records Found

Publish

Click **Publish**.
Enroll Class Devices

You are now going to enroll your iOS device for use with this module.

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

NOTE - Checked out devices will likely have the AirWatch MDM Agent already installed. You may skip this step if your device has the AirWatch MDM agent installed.

At this point, if using your own iOS device or if the device you are using does NOT have the AirWatch MDM Agent Application installed, then install the AirWatch Application.

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

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

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

Welcome to AirWatch!

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

The multi-step enrollment process begins with authentication.

Choose authentication method:

- Email Address
- Server Details
- QR Code

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

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

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

Attach the AirWatch MDM Agent to the HOL Sandbox

Once the Agent has launched you can enroll the device. To do so, follow the below steps.
1. Enter "hol.awmdm.com" for the Server field.
2. Enter your Group ID for your Organization Group for the Group ID field. Your Group ID was noted previously in the Finding your Group ID step.
3. Tap the Go button.

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

Authenticate the AirWatch MDM Agent

On this screen, enter the Username and Password as shown below.

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

1. Type in the Basic User Account Username i.e. "imateacher".
2. Type in the Basic User Account Password. This should be "VMware1!".
3. Tap the Go button.
Redirect to Safari and Enable MDM Enrollment in Settings

Enable Device Management

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

Why?

- Access your company resource
- Remove company data in the event of loss or theft

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

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

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

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

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

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

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

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

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

You should now see the iOS Profile successfully installed.

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

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

Accept Notification Prompt (IF NEEDED)

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.

**REMINDER - Enroll TWO Devices**

1. Type in the Basic User Account Username i.e. "imastudent".
2. Type in the Basic User Account Password. This should be "VMware1!".
3. Tap the **Go** button.

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

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

1. Type in the Basic User Account Username i.e. "imastudent".
2. Type in the Basic User Account Password. This should be "VMware1!".
3. Tap the **Go** button.
On either the Student or Teacher iPad:

1. Click on the **Settings** app
2. Click on **General** then scroll and click **Profiles & Device Management**
3. Click the **Workspace Services** profile
4. Click **More Details**
5. Note the Education Configuration profile (e.g. AirWatch School Manager####)
Control Student Devices with Classroom App

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

Open Classroom App

Return to the Teacher iPad. On the Teacher iPad:

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

Accept Notification Prompt (IF NEEDED)

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

Click on **1st Grade - Mr Jones**

**Explore Classroom Interface**

Note the following areas of the Classroom app interface:

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

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

Control Single iPad

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

**Control Multiple Devices**

1. Select a Group from the list of Device Groups.
2. Note that you can now take actions against the group, such as Open, Navigate, Lock, and Screen Viewing.
3. Click **Screens** on the Teacher device.
4. Note the icon for the student device in the Classroom app now displays the screen capture of the device. Also note on the student device that the status bar is now blue and there is also an airplay icon displayed.
5. Click the **Screens** button to end screen viewing. Note the icon returns to normal in the Classroom app and the student device status bar returns to normal.
Un-enrolling Your Device

You are now going to un-enroll the iOS device from AirWatch.

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

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

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

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

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

1. Click **Devices** on the left column.
2. Click **List View**.
3. Click the **checkbox** next to the device you want to Enterprise Wipe.

**NOTE - Your Device Friendly Name will very likely be different than what is shown. It will, however, be in the same location as shown on image in this step.**
Find the Enterprise Wipe Option

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

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

1. Enter "1234" for the **Security PIN**. You will not need to press enter or continue, the console will confirm your PIN showing "Successful" below the Security PIN input field to indicate that an Enterprise Wipe has been requested.  **NOTE:** if "1234" does not work, then you provided a different Security PIN when you first logged into the AirWatch Console. Use the value you specified for your Security PIN.

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

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

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

Feel free to continue to the "**Force the Wipe**" step to manually uninstall the AirWatch services from the device if network connectivity is failing.
Verify the Un-Enrollment

Press the Home button on the device to go back to the home screen. The applications pushed through AirWatch should have been removed from the device.

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

If your device did not wipe, follow these instructions to ensure the wipe is forced immediately. Start by opening the iOS **Settings** app.
1. Tap **General** in the left column.
2. Scroll down to view the **Device Management** option.
3. Tap **Device Management** at the bottom of the list of General settings.

**Force the Wipe - IF NECESSARY**

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

1. Tap **Remove Management** on the Workspace Services profile.  
   *NOTE - If prompted for a device PIN, enter it to continue. VMware provisioned devices should not have a device PIN enabled.*
2. Tap **Remove** on the Remove Management prompt.
After removing the Workspace Services profile, the device will be un-enrolled. Feel free to return to the "Verify the Un-Enrollment" step to confirm the successful un-enrollment of the device.
Conclusion

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

Requirements and Optional Add-ons for AirWatch School Manager

AirWatch School Manager requires the following software and hardware:

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

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

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

Typical Uses for AirWatch School Manager

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

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

For additional information on AirWatch School Manager, please speak with your Account Executive or refer to the documentation on MyAirWatch.
Module 3 - VMware Browser (45 Minutes)
Introduction

VMware Browser 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.

VMware Browser Feature Overview

Before diving in, explore the features available in VMware Browser to better understand the use cases that could benefit from deploying VMware Browser 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 VMware Browser 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 VMware Browser 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 AirWatch Console

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

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.

Authenticate to the AirWatch Administration Console

Username

Your VLP Email Address

Password

VMware1!

Login

Trouble Logging In
The default home page for the browser is https://hol.awmdm.com. Enter your AirWatch Admin Account information and click the Login button.

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

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

**NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the AirWatch Hands On Labs server.**

**Accept the End User License Agreement**

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

**End User License Agreement**

**IMPORTANT:** READ THIS DOCUMENT CAREFULLY.

The terms and conditions of this End User License Agreement (the "EULA") constitute a legal agreement between you (either an individual or, if purchased or otherwise acquired by or for an entity, such entity) ("CUSTOMER") and AirWatch with respect to use of the proprietary AirWatch Software. By (1) executing an AirWatch Order, (2) installing, copying, downloading or otherwise accessing the Software, (3) electronically accepting, or (4) executing this EULA, CUSTOMER completely and unequivocally agrees to be bound by the terms of this EULA without modification. If Customer does not intend to be legally bound to the terms and conditions of this EULA, CUSTOMER MAY NOT ACCESS OR OTHERWISE USE THE SOFTWARE AND MUST PROMPTLY RETURN OR DELETE ALL COPIES OF THE SOFTWARE AND DOCUMENTATION IN THE MANNER PROVIDED HEREIN.

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

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

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

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

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

<table>
<thead>
<tr>
<th>Security Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password Recovery Question</strong></td>
</tr>
<tr>
<td><strong>What was your childhood nickname?</strong></td>
</tr>
<tr>
<td><strong>Password Recovery Answer</strong></td>
</tr>
<tr>
<td>VMware1!</td>
</tr>
<tr>
<td><strong>Password Recovery Answer</strong></td>
</tr>
<tr>
<td>VMware1!</td>
</tr>
<tr>
<td><strong>Security PIN</strong></td>
</tr>
<tr>
<td>1234</td>
</tr>
<tr>
<td><strong>Confirm Security PIN</strong></td>
</tr>
<tr>
<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

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

1. Click on the **Don't show this message again** check box.
2. Close the pop-up by clicking on the **X** in the upper-right corner.
AirWatch Console Configuration

This section will explain what configurations must be made in the AirWatch 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 VMware Browser to connect to an intranet site.

Add a Profile

1. Click Devices.
2. Expand Profiles & Resources.
3. Click Profiles.
4. Click ADD to expand the dropdown.
5. Click Add Profile.

Select the Platform

Select a platform to start:

- iOS
- Android
- Apple iOS
Click **Apple iOS**.

**Enter the Profile Details**

1. Ensure the General payload tab is selected.
2. Enter "**iOS Per-App VPN**" for the **Name** field.
3. Click the **Assigned Groups** field.
4. Select **All Devices (your@email.shown.here)** from the list.
Enable the VPN Payload

1. Click the VPN payload tab.
2. Click Configure.

Configure the VPN Payload

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 Offline Access**

1. Scroll down to find the **Offline Access** section.
2. Click **Enabled** for **Offline Access**.
3. Enter "1" for **Maximum Period Allowed Offline**.
4. Select **day(s)** for the time period dropdown.

**Configure Data Loss Prevention**

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

**Save Security Policies Settings**

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

**Confirm Saved Security Policies**

Confirm that the Saved Successfully prompt shows.

**Configure VMware Browser Settings**

This section will explain how to configure the VMware Browser 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

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 VMware Browser to a single page and its 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

![Bookmark Settings](image)

The Internal Splash Page bookmark is already created for you, which is set to the Home Page.

1. Click **Add Bookmark**.
2. Enter "**AirWatch Home**" for the new bookmark **Name**.
3. Enter "**https://www.airwatch.com**" for the new bookmark **URL**.
4. Click **Save**.
Close the Browser Settings Page

1. Confirm the Saved Successfully prompt shows.
2. Click Close

Publish the VMware Browser Application

Let us add VMware Browser as a Public app to manage and configure.

Add a New Public Application

1. Click Apps & Books.
2. Expand Applications.
3. Click List View.
4. Click the Public tab.
5. Click + Add Application.
Search App Store for VMware Browser

1. Select Apple iOS for the Platform
2. Enter “VMware Browser” for the Name
3. Click Next

Select the VMware Browser Result

Click Select for the VMware Browser result.
Save and Assign VMware Browser

Click **Save & Assign**

Add Assignment for VMware Browser
Click + Add Assignment

Configure VMware Browser 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 Policies for VMware Browser

1. **Managed Access**: Enabled
2. **Remove On Unerroll**: Enabled
3. **App Tunneling**: Enabled (iOS 7+)
4. **Application Configuration**: Enabled
1. Scroll down to find the Policies section.
2. Select Enabled for Remove On Unenroll.
3. 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**.

Publish the VMware Tunnel Application

In order to leverage the Per-App VPN profile we created for VMware Browser, we will need to also publish VMware Tunnel to the device.
Add a New Public Application

1. Click **Apps & Books**.
2. Expand **Applications**.
3. Click **List View**.
4. Click the **Public** tab.
5. Click **+ Add 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

Click Select for the VMware Tunnel result.
Save and Assign VMware Tunnel

Click **Save & Assign**.

Add Assignment for VMware Tunnel

Devices will receive application based on the assigned priority.

In the case where devices belong to multiple groups, devices with the highest priority (0 being highest priority) will receive the application.

Click **Add Assignment**.
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" 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.

---

VMware AirWatch - Productivity Apps
2. Select **Enabled** for **Remove On Unenroll**.
3. Click **Add**.

**Confirm Assignment and Save**

1. Ensure the Assignment you created 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 to complete the steps on the device side.

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

*NOTE - Checked out devices will likely have the AirWatch MDM Agent already installed. You may skip this step if your device has the AirWatch MDM agent installed.*

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

**Launching the AirWatch MDM Agent**

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

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

Welcome to AirWatch!

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

The multi-step enrollment process begins with authentication.

Choose authentication method:

- Email Address
- Server Details
- QR Code

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

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

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

Attach the AirWatch MDM Agent to the HOL Sandbox

Once the Agent has launched you can enroll the device. To do so, follow the below steps.

1. Enter "hol.awmdm.com" for the **Server** field.
2. Enter your **Group ID** for your Organization Group for the **Group ID** field. Your Group ID was noted previously in the **Finding your Group ID** step.
3. Tap the **Go** button.

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

### Authenticate the AirWatch MDM Agent

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

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

Enable Device Management

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

Why?

- Access your company resource
- Remove company data in the event of loss or theft

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

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

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

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

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

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

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

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

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

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

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

You should now see the iOS Profile successfully installed.

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

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

Authentication Complete

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

Click on **Done** to continue.

Accept Notification Prompt (IF NEEDED)

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

Accept the App Installation (IF NEEDED)
You may be prompted to install a series of applications depending on which Module you are taking. If prompted, tap **Install** to accept the application installation.
Explore VMware Browser

We will now launch and explore VMware Browser 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 webpage 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 "http://internal.airwlab.com".
2. Tap **Go**.

**Confirm Safari Cannot Access the Intranet Site**

![Safari error message]

Confirm that Safari cannot open the intranet site.

**Confirm the VMware Browser Configurations**

Now, let's access the same link from VMware Browser.

**Launch the VMware Browser app**

![VMware Browser app icon]

Tap the **VMware Browser** app.
Confirm Automatic Per-App VPN

We configured our Home Page URL for VMware Browser to load our intranet site (http://internal.airwlab.com). Notice that upon launch, VMware Browser 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 AirWatch Console.

**NOTE** - *In this case, VPN is only authorized for the VMware Browser application based on the configuration in the AirWatch 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 VMware Browser 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 AirWatch 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 VMware Browser, 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 VMware Browser in AirWatch 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 (http://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 VMware Browser configuration to deny access to the *.airwatch.com sites.

**Review**

You've now confirmed all of the configurations we deployed to VMware Browser during our setup in the AirWatch Console. Feel free to explore any other features of VMware Browser 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 AirWatch.

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

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

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

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

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

1. Click **Devices** on the left column.
2. Click **List View**.
3. Click the **checkbox** next to the device you want to Enterprise Wipe.

**NOTE - Your Device Friendly Name will very likely be different than what is shown. It will, however, be in the same location as shown on image in this step.**
Find the Enterprise Wipe Option

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

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

1. Enter "1234" for the **Security PIN**. You will not need to press enter or continue, the console will confirm your PIN showing "Successful" below the Security PIN input field to indicate that an Enterprise Wipe has been requested. **NOTE:** If "1234" does not work, then you provided a different Security PIN when you first logged into the AirWatch Console. Use the value you specified for your Security PIN.

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

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

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

Feel free to continue to the "**Force the Wipe**" step to manually uninstall the AirWatch services from the device if network connectivity is failing.
Verify the Un-Enrollment

Press the Home button on the device to go back to the home screen. The applications pushed through AirWatch should have been removed from the device.

**NOTE - The applications and settings pushed through AirWatch management should have been removed. The Agent will still be on the device because that was downloaded manually from the App Store. Due to lab environment settings, it may take some time for the signal to traverse through the various networks out and back to your device. Continue on to the next step to force the wipe if the needed.**
If your device did not wipe, follow these instructions to ensure the wipe is forced immediately. Start by opening the iOS **Settings** app.
1. Tap **General** in the left column.
2. Scroll down to view the **Device Management** option.
3. Tap **Device Management** at the bottom of the list of General settings.

**Force the Wipe - IF NECESSARY**

![Workspace Services profile]

Tap the **Workspace Services** profile that was pushed to the device.
1. Tap **Remove Management** on the Workspace Services profile.  
   **NOTE** - *If prompted for a device PIN, enter it to continue.*  
   **VMware provisioned devices should not have a device PIN enabled.**  
2. Tap **Remove** on the Remove Management prompt.
After removing the Workspace Services profile, the device will be un-enrolled. Feel free to return to the "Verify the Un-Enrollment" step to confirm the successful un-enrollment of the device.
Conclusion

VMware Browser 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 VMware Browser can improve your productivity by providing a secure and configurable browsing experience!

This concludes this lab module.
Conclusion

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

Lab SKU: HOL-1857-04-UEM

Version: 20180323-183916