# Table of Contents

Lab Overview - HOL-1857-08-UEM - Workspace ONE UEM - Technology Partner Integration ................................................................. 2  
Lab Guidance .................................................................................................................. 3  
Module 1 - F5 Integration with Workspace ONE UEM (30 min)........................................... 9  
  Introduction ................................................................................................................. 10  
  F5 BigIP Configuration............................................................................................... 12  
  Login to the Workspace ONE UEM Console ........................................................... 27  
  iOS Device Enrollment ............................................................................................... 33  
  AirWatch Console Configuration ............................................................................... 48  
  Testing Per App VPN ............................................................................................... 69  
  Un-enrolling Your Device ....................................................................................... 74  
  Conclusion ............................................................................................................... 83
Lab Overview - HOL-1857-08-UEM - Workspace ONE UEM - Technology Partner Integration
Lab Guidance

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

AirWatch has native integration with many other technology vendors. This lab explores the configurations between F5 and AirWatch to deliver secure access to your applications.

Each Module can be taken independently or you can start at the beginning and work your way through each module in sequence. In most cases, a unique "sandbox" instance of AirWatch will be created just for you when you begin a Module. When the Module has ended, this sandbox will be deleted and the device that you are enrolling in the lab will be returned to the state that it was in prior to the lab. The approximate time it will take to go through all the modules is around 2.5 hours.

Lab Module List:

- **Module 1 - F5 Integration with AirWatch** (30 minutes) (Advanced) Configure access policies in F5 and provide Per-App VPN on an iOS device through AirWatch by leveraging the F5 VPN capabilities.

Lab Captains:

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

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

### Accessing the Online International Keyboard

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

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

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

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

Click on the @ key

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

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

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

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

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

This cosmetic issue has no effect on your lab.

Look at the lower right portion of the screen
Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes you lab has not changed to "Ready", please ask for assistance.
Module 1 - F5 Integration with Workspace ONE UEM (30 min)
Introduction

With F5 BIG-IP APM, you may provide AirWatch mobile users unmatched secure remote access, performance, and availability. This module guides you through the configuration details required to integrate F5 BIG-IP APM with AirWatch. The steps are a series of recommended practices to follow in order to build an integrated solution. As with any system deployment, the steps are examples and the deployed environment may not exactly match these examples.

What to Expect

After completing this guide, you will be able to:

• Use the F5 BIG-IP APM as an AirWatch access gateway.
• Use the iOS BIG-IP Edge Client for Per-App VPN access with iOS 7 or later.
• Authenticate AirWatch MDM users via the BIG-IP APM.
• Initiate on-demand VPN tunnels by domain query.
• Use BIG-IP APM as a Microsoft Active Sync Proxy for Android and iOS email synchronization.
• Manage AirWatch MDM devices through the BIG-IP APM access gateway.

Requirements

This section covers various requirements for implementing in your own environment. These include prerequisites, product licensing, software, and/or hardware requirements. All prerequisites will be provided for use during this module.

Prerequisites:

This solution utilizes the following ancillary infrastructure:

• An authentication server
• An email server
• An application server
• An NTP time server
• Globally Routable IP addresses
• Mobile device(s) with network access (iOS and Android devices only)
• Internet access
• Administrator login credentials
• SSL Certificate and Key (please reference F5 solution article SOL14499 for how to create a certificate authority and client certificates)

AirWatch

• AirWatch service subscription required.
F5 BIG-IP

- Either a physical or a virtual instance of BIG-IP is required.
- This guide is based on BIG-IP software release 11.5.0.
- This solution relies on F5 Access Policy Manager (APM) and requires an APM software license.
F5 BigIP Configuration

This section covers the steps required to be performed within the BigIP web configuration utility. The BigIP you will be accessing for this lab has been pre-configured for the lab environment.

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.
Open F5 Web Admin Console

1. Select the "BIG-IP" shortcut from the bookmarks bar or navigate to "https://bigip-01.corp.local".
2. Enter "admin" for the Username field.
3. Enter "VMware1!" for the Password field.
4. Click Login.

Create A Network Access Policy

This step will use the BIG-IP configuration utility wizard to assist you in creating a remote access configuration using Access Policy Manager (APM).
Start the Network Access Policy Wizard

1. Click Wizards.
2. Click Device Wizards.
4. Click Next.

Set the Basic Properties

1. Enter "f5_airwatch_policy" for the Policy Name field.
2. Enter "f5_airwatch_policy" for the Caption field.
3. Uncheck Enable Antivirus Check in Access Policy.
4. Enter "192.168.120.1" for the IPv4 Gateway Address field.
5. Click "Next".

Select Access Policy Authentication

![Select Authentication screenshot]

We will be setting the authentication type at a later step.

1. Select **No Authentication** for the Select Authentication choice.
2. Click **Next**.
A lease pool is a pool of available IP addresses that BIG-IP will assign to remote clients for network access. The size of this pool needs to be large enough to provide enough address space for the total concurrent connections licensed by APM.

1. Enter "192.168.2.100" for the Start IP Address field.
2. Enter "192.168.2.199" for the End IP Address field.
3. Click Add.
4. Click Next.
Configure Network Access Settings

The client settings should be set according to the deployment scenario requirements. In this example, all traffic will be forced through the SSL VPN tunnel.

1. Ensure that for **Traffic Options**, the preselected option is **Force all traffic through tunnel**.
2. Click **Next**.
Configure DNS Hosts

1. Enter "192.168.110.10" for the first Primary Name Server field.
2. Enter "corp.local" for the DNS Default Domain Suffix field.
3. Scroll down if necessary.
4. Click Next.

Enter the Virtual Server IP Address

Finally, the Virtual Server IP Address needs to be defined.

1. Enter "192.168.5.11" for the Virtual Server IP Address field.
2. Uncheck the Create Redirect Virtual Server checkbox.
3. Click **Next**.

Review & Confirm Configuration

Review your settings, scroll down and select **Next**
Review Summary of F5 Network Access Configuration

Review your configuration again and click on Finished

NOTE - You may need to click on the image to enlarge it.

Adjust the Access Policy to Authenticate Client Certificates for Access
The Network Access Wizard created several components and we will now need to make a few changes to the default settings of those components to enable per-app VPN. Please note that the configuration we are setting up here is as basic as possible. Your organization can configure a more advanced security and access policy that suits your needs.

1. Click **Access Policy**.
2. Click **Access Profiles**.
3. Click **Edit...** on the **f5_airwatch_policy** Access Policy.

### Add a Node to the Access Policy

Click the first + in front of **Logon Page**,
Enable Client Certificate Authentication

1. Click **Authentication**.
2. Select **On-Demand Cert Auth**.
3. Click **Add Item**.
Set Cert Auth Mode to Require

1. Set **Auth Mode** to **Require**.
2. Click **Save**.

Apply the Access Policy Updates

1. Click **Apply Access Policy**.
2. Close the **Access Policy Editor** tab in the browser to return the F5 Admin Console.
Configure Advanced Settings of the Virtual Server

1. Click **Local Traffic**.
2. Click **Virtual Servers**.
3. Click **f5_airwatch_policy_vs**.
Change the Service Port

Enter "5011" for the Service Port field.

Edit the Virtual Server Settings
We will need to change the SSL Profile on the F5 Virtual Server to accept Client Certificates from our Enterprise PKI and enable a few options that are required for Per-App VPN.

1. Scroll down to find the **SSL Profile (Client)** section.
2. Select `clientssl` in the **Selected** list under **SSL Profile (Client)**.
3. Click the `>>` button to remove `clientssl` from the **Selected** list.
4. Select `clientssl_holcertreq` in the **Available** list under **Client Profile (Client)**.
5. Click the `<<` button to move `clientssl_holcertreq` to the **Selected** list.
6. Select **Auto Map** for the **Source Address Translation** dropdown.

**Edit the Virtual Server Settings**

1. Scroll down to the section **Access Policy**
2. Set **Application Tunnels** to **Enabled** by checking the box.
3. Click **Update**

**F5 Configuration Wrap-Up**

We've now completed configuration of the F5 Big IP. We have created a basic Network Access Policy that will allow us to connect our devices with the F5 Edge Client and securely access internal resources. Our next steps are to configure AirWatch to push all the necessary configurations and activate specified applications to leverage the VPN connection while ensuring other device applications are blocked from accessing your internal network.
Login to the Workspace ONE UEM Console

To perform most of the lab you will need to login to the Workspace ONE UEM Management Console.

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.
Authenticate to the Workspace ONE UEM Administration Console

The default home page for the browser is https://hol.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 that party, and here "control" means an ownership, voting or similar interest representing fifty percent (50%) or

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 popup. The Password Recovery Question is in case you forget your admin password and the Security PIN is to protect certain administrative functionality in the console.
1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a question from the Password Recovery Question drop-down (default selected question is ok here).
3. Enter "VMware1!" in the Password Recovery Answer field.
4. Enter "VMware1!" in the Confirm Password Recovery Answer field.
5. Enter "1234" in the Security PIN field.
6. Enter "1234" in the Confirm Security PIN field.
7. Click the Save button when finished.

Close the Welcome Message

Workspace ONE UEM Console Highlights

Powered by VMware AirWatch!

Workspace ONE is powered by VMware AirWatch Unified Endpoint Management (UEM) technology, a unified digital workspace platform delivering a single, secure experience for app management, single sign-on (SSO), and conditional access.

Workspace ONE UEM transforms your business so you can:

- Configure, manage and support devices from any endpoint
- Increase productivity with seamless access to any app
- Safeguard company data at every layer
- Access identity and access management tools with ease
- Enjoy a simplified, consistent look and feel across Workspace ONE

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.
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.**
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.
AirWatch Console Configuration

In this chapter you create a Per-App VPN profile and deploy an Application configured to use the F5 Access app on iOS.

Create an iOS VPN Profile

In this step you will configure the iOS profile that will be delivered to the device to configure the F5 Access app 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.
Click **Apple iOS**.

**Configure the General Properties of the Profile**

1. Select General.
2. You may need to scroll down to view the **Name** and **Assigned Groups** fields.
3. Enter "**F5 Per-App VPN**" as the **Name**.
4. Click the **Assigned Groups** field.
5. Select "**All Devices @ yourname@email.com**" as the Assigned Smart Group.
Add a Credentials Payload

1. Click **Credentials** from the Payload menu.
2. Click **Configure** to go to the Credential configuration menu.
Configure the Credentials Payload

For the purposes of this lab, a Certificate Authority has already been configured for you to use. We have connected this Microsoft CA to AirWatch to allow AirWatch to issue and manage client certificates for use with the F5 SSL VPN. This allows users to seamlessly connect to the VPN and authenticate without the need for entering username and password. As soon as the designated application is opened on the device, the VPN connection will be established.

1. Select **Defined Certificate Authority** for the Credential Source field.
2. Select **HOL.AIRWLAB.COM HOL CA** for the Certificate Authority field.
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 **F5 SSL** from the Connection Type dropdown.
3. Check the Per-app VPN checkbox.
4. Check Connect Automatically checkbox, which should auto-enable after enabling the Per-App VPN Rules checkbox.
Configure the VPN Payload

1. Scroll down to find the **Authentication** section.
2. Select **Certificate** for the **User Authentication** dropdown.
3. Select **Certificate #1** for the **Identity Certificate** dropdown.
4. Click **Save & Publish**.
Publish the VPN Profile

Click **Publish**

**Add the F5 Access App as a Public Application**

In order to apply the VPN profile, the F5 Access app needs to be installed on your device. We can leverage AirWatch to deploy the F5 Access app to the device through MDM. This step will walk you through the process of adding an application from the Public App store.
Add a New Public Application

1. Click **Add**
2. Click **Public Application**

Search for the Application to Add

**Add Application**

- **Managed By**: your@email.shown.here
- **Platform**: Apple iOS
- **Source**: Search App Store
- **Name**: F5 Access

[Next]  [Cancel]
1. Select Apple iOS from the Platform dropdown.
2. Ensure Search App Store is set for the Source option.
3. Enter "F5 Access" in the Name field.
4. Select Next

Select the F5 Access App from the Search Results

Click Select on the F5 Access for iOS application.
Save and Assign F5 Access

Click **Save & Assign**.
Add Assignment for F5 Access

Click + Add Assignment.

Configure F5 Access 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 F5 Access

1. Scroll down to find the Policies section.
2. Select **Enabled** for **Remove on Unenroll**.
3. Click **Add**.
1. Confirm the Assignment you created is displayed.
2. Click **Save & Publish**.
Preview Assignment and Publish

Click **Publish**.

**Add VMware Browser as a Public Application**

In order to associate the VPN profile to specific apps, you need to add the application through MDM. 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 a New Public Application

1. Click **Add**
2. Click **Public Application**

Search App Store for VMware Browser

1. **Managed By**: your@email.shown here
2. **Platform**: Apple iOS
3. **Source**: Search App Store
4. **Name**: VMware Browser
5. **Next**
1. Select **Apple iOS** for the **Platform**
2. Enter "**VMware Browser**" for the **Name**
3. Click **Next**

**Select the VMware Browser Result**

![VMware Browser search result]

Click **Select** for the **VMware Browser** result.

**Save and Assign VMware Browser**

![Edit Application - VMware Browser]

Click **Save & Assign** to save and assign the VMware Browser.
Click **Save & Assign**

**Add Assignment for VMware Browser**

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. Scroll down to find the Policies section.
2. Select Enabled for Managed Access.
5. Select the **F5 Per-App VPN** profile for Per-App VPN Profile.
6. 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.
Testing Per App VPN

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

Launch & Enable the F5 Access Application

This step is to enable the newly installed VPN client to handle network traffic and is required for the user to do only the 1st time that the application is installed.

Press the Home button on the iPad to return to the Launchpad. Swipe right if needed to see the downloaded applications. Select the F5 Access application to open it.
Accept the F5 User Agreement

Select **Enable** at the **User Agreement** prompt.

**Launch VMware Browser**

Press the Home button on the device to return to the Launchpad. Tap the **VMware Browser** icon to launch the application.
Allow Notifications from VMware Browser

If prompted to allow Notifications from VMware Browser, tap **Allow**.

Confirm VPN Connection and Navigate to Internal Website

1. The VPN icon notates that the VPN connection is active. This is established from our F5 Per-App VPN profile that we configured VMware Browser with.
2. Tap the "**internal.hol.airwlab.com**" bookmark to navigate to the internal website.
Confirm the Internal Website is Accessible

If your Per-App VPN connection is setup correctly, you should see a website with the Welcome message. Continue to the next step.

**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 internal network resources.
Open Safari

Return to the launchpad by pressing the Home button on the iPad. Open Safari by selecting the icon from the Launcher.

Attempt to Navigate to the Internal Resource From Safari

1. Open a new tab by selecting the + sign on the navigation bar.
2. Select the entry box on the navigation bar and enter the URL "internal.hol.airwlab.com" (this is the same URL we entered in VMware Browser).
3. Notice that the website does not load in the Safari browser due to a timeout.

Wrap-Up

The website is published to an internal web server 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 connection. You may have multiple VPN configurations and multiple apps assigned for each VPN. Most Public applications are compatible with per-app VPN on iOS. If desired, you can authorize the native browser on iOS to leverage the per-app VPN connection, we have chosen not to for the purposes of this lab.
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**

![Device Management Menu]

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

In addition to integrating with F5’s Access Client and Big-IP Edge Client, AirWatch can also integrate with a large number of other partners' VPN clients to provide per-app VPN functionality.

To learn more about AirWatch's own per-app VPN offering using AirWatch Tunnel, consider taking HOL-1857-05-UEM - Module 4 - Per-App VPN using AirWatch Tunnel.

This concludes the F5 Integration with AirWatch 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-1857-08-UEM

Version: 20180604-184151