# Table of Contents

Lab Overview - HOL-1857-07-UEM - Workspace ONE UEM - Android Management ........2
   Lab Guidance .................................................................................................................. 3
Module 1 - Android Enterprise - Work Profile (30 minutes) ........................................... 9
   Introduction ....................................................................................................................... 10
   Login to the AirWatch Console .................................................................................... 11
   TUTORIAL FOLLOW ALONG - Configuring Android Enterprise in the Console ...... 15
   Device Enrollment with Android Enterprise (Work Profile) ...................................... 22
   Android Enterprise Profiles ........................................................................................... 43
   Approving Applications ................................................................................................. 53
   Verify Work Apps .......................................................................................................... 65
   Un-enrolling Your Android Device .............................................................................. 69
   Learn More about Android Enterprise ............................................................................. 72
   Conclusion ....................................................................................................................... 73
Module 2 - Android Enterprise Work Managed Enrollment (30 minutes) ...................... 74
   PLEASE READ - DISCLAIMER BEFORE TAKING THIS MODULE ......................... 75
   Introduction ....................................................................................................................... 76
   Work Managed Enrollment Methods ............................................................................. 77
   Login to the AirWatch Console ..................................................................................... 79
   TUTORIAL FOLLOW ALONG - Configuring Android Enterprise in the Console ....... 83
   Device Enrollment with Android Enterprise (Work Managed) Identifier Enrollment ........ 90
   Un-enrolling Your Android Device .............................................................................. 117
   Conclusion ....................................................................................................................... 120
Lab Guidance

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.

Dive deep into how to provide a separation of work and personal information and apps at the Android operating system level while maintaining the consistent native user experience. Learn how to deploy Android apps while protecting your enterprise data with security policies.

Lab Module List:

- **Module 1 - Android Enterprise - Work Profile** (30 minutes) Enroll your Android and configure applications and restrictions to experience how these configurations apply on the device to provide a separate of work and personal apps.
- **Module 2 - Android Enterprise Work Managed Enrollment** (30 minutes) Learn how to configure and enroll your Android device by using the AirWatch Identifier.

**WARNING - Module 2 requires that your Device must be in Out of Box mode after a Factory Reset. Please DO NOT factory reset your personal device to take this lab. Refer to the help desk to acquire a device that is already factory reset and ready to enroll into Work Managed mode. Only use devices from help desk to enroll into Work Managed mode.**

- **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](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:

1. The area in the RED box contains the Main Console. The Lab Manual is on the tab to the Right of the Main Console.

2. A particular lab may have additional consoles found on separate tabs in the upper left. You will be directed to open another specific console if needed.

3. Your lab starts with 90 minutes on the timer. The lab can not be saved. All your work must be done during the lab session. But you can click the **EXTEND** to increase your time. If you are at a VMware event, you can extend your lab time twice, for up to 30 minutes. Each click gives you an additional 15 minutes. Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.

**Alternate Methods of Keyboard Data Entry**

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

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

Accessing the Online International Keyboard

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

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

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

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

Click on the @ key

1. Click on the "@" key.

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

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

One of the major benefits of virtualization is that virtual machines can be moved and run on any platform. The Hands-on Labs utilizes this benefit and we are able to run the labs out of multiple data centers. 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 - Android Enterprise - Work Profile (30 minutes)
Introduction

Android Enterprise, is the feature developed by Google to make Android devices (running 5.0 or later versions). It provides several features and configurations when integrated with AirWatch, which secures and manages devices in your organization.

Some of the features supported by Android in the enterprise are:

- Hosting your enterprise apps in Play Store
- Installing apps (both Play Store and enterprise apps) without user intervention.
- Manage license of paid apps.
- Modify app-specific configurations and permissions.
- Customize Play Store.
- Enhance data security using AirWatch restrictions and configurations.

AirWatch can configure both a Work Profile and a Work managed mode. You will be going through the Work Profile mode in this lab.
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 1

Password

VMware1! 2

Login 3

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

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

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

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

**Accept the End User License Agreement**

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

**End User License Agreement**

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

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 by the terms and conditions hereof, in which case all references to Customer

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

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

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

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

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.
TUTORIAL FOLLOW ALONG - Configuring Android Enterprise in the Console

In this Lab we will be covering some of the Android For Work basic functionality.

When running on Android 5.0 Lollipop devices, Android for Work is built into the operating system with no need for an additional application.

To begin using Android for Work inside the AirWatch Admin Console, you need to register your enterprise with Google. This creates your Android for Work admin account which connects with AirWatch to manage your enterprise devices. Users will not be able to use Android for Work features from their devices until registered with AirWatch. The Android for Work setup wizard simplifies the process. To simplify your experience, this initial process has been done for you. If you are interested in learning more about this process please talk to your AirWatch Sales Engineer or Representative.

Overview

IMPORTANT - You will not be able to make the configurations shown in the following steps within your lab!

This section is designed to only walk you through the process of configuring Android for Work so you can become familiar with the administrative process behind configuring Android for Work for AirWatch. Android for Work has already been configured for you in your lab environment, so no action is required on your part for this section.

Once a Google Admin Account is bound to AirWatch, you cannot reuse this Google Admin for another organization. Due to this limitation, you would be unable to use the Google Admin Account we have already bound to AirWatch for this lab.

AirWatch Android for Work Configuration

This section will demonstrate how to configure Android for Work within the AirWatch Console.

IMPORTANT - Remember, you will not be able to make the configurations shows in the following steps within your lab! This is for demonstration purposes only so that you can become familiar with the process.
Open Settings

1. Click **Groups & Settings**.
2. Click **All Settings**.
Open Android for Work Configuration

1. Click Devices & Users.
2. Expand Android.
3. Click Android For Work.
4. Click Configure.
Provide Google Admin Account

1. Confirm you are logged into your **Google Admin Account** that you wish to associate with your Android for Work configuration.

   *NOTE - Once you register a Google Admin Account to Android for Work, you cannot disassociate your Google Admin Account from that Organization. Ensure the Google Admin Account shown is the account you wish to associate with your Organization!*

2. Click **Get Started**
Provide your Organization Details

1. Enter your Organization Name.
2. Check the Google Play Agreement checkbox.
3. Click Confirm.
Complete Registration

Set up complete
Thanks for choosing Android

You now need to return to your EMM provider to complete your registration.

Click Complete Registration to return to the AirWatch Android for Work configuration.
Confirm Android for Work Integration

1. On the Android for Work Settings page, scroll down until you see the **Google Admin Console Settings** and **Google API Settings** sections.
2. Under Google Admin Console Settings, note that the account information you provided during the Android for Work configuration step is displayed here.
3. Confirm that your **Android for Work Registration Status** is shown as **Successful**.
4. Note that the **Client ID** and **Google Service Account Email Address** have been created and configured for you automatically. No additional configurations with Android for Work or the Google Developers Console are required.

Your Organization Group is now successfully configured with Android for Work!
Device Enrollment with Android Enterprise (Work Profile)

In this section, we will be enrolling your device with AirWatch and get it set up with Android for Work.

Launching the AirWatch MDM Agent

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

If you have your own Android device and would like to test you will need to download the agent first. Navigate to **https://www.awagent.com** to download the latest version of the AirWatch Agent.
Select AirWatch MDM Agent Authentication Method

Welcome to AirWatch!

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

You will be guided through a three part process to authenticate, secure and configure your device.

Choose Authentication Method:

- ✉️ EMAIL ADDRESS
- 🌐 SERVER DETAILS
- 📅 QR CODE

Once the Agent has launched you can enroll the device. To do so, you must first select the AirWatch authentication method.

Tap Server Details
Find your Group ID from AirWatch Console

The first step is to make sure you know what your **Organization Group ID** is.

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

*NONE* - The Group ID is required when enrolling your device in the following steps.

Attach the AirWatch MDM Agent to the HOL Sandbox

After selecting the Server authentication method, you need to supply the information to authenticate. To do so, follow the below steps.

1. Enter **hol.awmdm.com** for the **Server** field.
2. Enter your **Group ID** for the **Group ID** field. This was noted previously in the **Finding your Group ID** step.
3. Tap **Continue**.

**Authenticate the AirWatch MDM Agent**

1. Enter "**testuser**" for the **Username** field.
2. Enter "**VMware1!**" for the **Password** field.
3. Tap **Continue**.
Accept the Terms and Conditions
Terms and Conditions

Please read the following carefully before downloading and installing Android for Work on your device.

Samsung provides the Trusted Boot, as one of its security features, to detect rooting and custom ROM (i.e., not Samsung official firmware) installed in your device during boot time. After Android for Work is installed, and if such rooting or custom ROM is detected, your device will automatically enter factory reset mode and the data or application you stored or installed in your device will be deleted. You are strongly advised to back up important data or information in other devices such as your personal computer. Samsung shall not be responsible for any loss of data or
Tap **Agree.**
Set Up Android for work
Set up work profile

Your organization controls this profile and keeps it secure. You control everything else on your device.

The following app will need to access this profile:

Agent

NEXT >
Tap **NEXT**.

*NOTE - This may take some time, please be patient while the Setup process completes.*

**(Optional) Device Encryption**

Set up your profile

To continue setting up your work profile, you'll need to encrypt your device. This may take some time.

For lab purposes, you should not see this screen and should continue to the next step. If you do see this screen, read the notes below.
NOTE - Android for Work enabled devices must be encrypted. If you are using a VMware provisioned device, you should not see this message, as all devices have been encrypted prior to the lab.

IMPORTANT - If you are using a VMware provisioned or personal device that shows this message, you should request a test device from the lab staff. Encrypting your devices can take some time depending on the amount of data on your device.
Administrator Rights
Your admin has the ability to monitor and manage settings, corporate access, apps, permissions, and data associated with this profile, including your network activity, as well as your device's location, call history, and contact search history.

Contact your admin for more information, including your organization's privacy policies.

Learn more
Tap **OK** to confirm the Privacy Policy.

**NOTE - Enrollment time may vary depending on your network connectivity. Typically, it takes around 1 minute to complete. Please be patient while this process completes.**

**IMPORTANT - During the enrollment process, you will see several processing screens. Please note that you do not need to interact with the device further until you see the AirWatch Agent app confirming your enrollment (next page).**
Wait for Device Connectivity (IF NEEDED)
Agent

My Device

Owner: testuser
samsung SM-G920V
Android for Work - Work Profile

Connectivity Issue
Compliant

Device Status
Information on the current state of this device

Compliance
Information on compliance status of this device

Profiles
A list of profiles installed on this device

Managed Apps
A list of managed Apps on this device

About
Information about the agent

Send Data  Sync  App Catalog
If you see a Connectivity Issue notification, the device may be taking several minutes to establish a connection to Google Cloud Messaging. Please wait until you see the Connectivity Issue notification change to Connectivity Normal before continuing.

**NOTE - If you do not see any Connectivity Issue notifications, please continue to the next step.**

**Confirm Device Enrollment**

![Device Enrollment Screen]

- **Owner**: testuser
  - LGE Nexus 5
  - Android for Work - Work Profile
  - Connectivity Normal
  - Compliant

- **Device Status**: Information on the current state of this device

- **Compliance**: Information on compliance status of this device

- **Profiles**: A list of profiles installed on this device

- **Managed Apps**: A list of managed Apps on this device

---

**Congratulations! You have successfully enrolled your device.**
You have now completed the AirWatch MDM Agent configuration wizard. After the enrollment process completes, the AirWatch Agent will display the notification *Congratulations! You have successfully enrolled your device.*

You can now **Exit** the AirWatch Agent.
Badged Apps
On your Android device, you should now see the new Work applications. Android for Work apps are differentiated by an orange briefcase icon also referred to as **Badged Apps**.

In the Applications view, your Work apps and Personal apps are shown in a unified launcher. For example, your device will show both a personal icon for Google Chrome and a separate icon for Work Chrome denoted by the badge. The AirWatch Agent is badged and exists only within the Work Profile data space.

**IMPORTANT - There is no control over personal apps nor will the Agent have access to personal information. There are a handful of system apps that come with the Work Profile by default such as Work Chrome, Google Play, Google settings, Contacts and Camera.**

**Work Container**

![Work Container](image)

On some devices, you may also notice the **Work** container on your device depending on the OS version. This Work container can be utilized for quick access to your **Work (Badged) Apps**.
Android Enterprise Profiles

In this section, we are going to create Android for Work profiles to ensure proper usage of devices and protection of sensitive data. Profiles serve many different purposes, from letting you enforce corporate rules and procedures to tailoring and preparing Android for Work capable devices for how they will be used.

**IMPORTANT - If your device is enrolled with Android for Work, then ONLY Android for Work profiles will take effect on the device, Android device profile will NOT take effect.**

Verify Restrictions

Restrictions profiles provide a second layer of device data protection by allowing you to specify and control how, when and where your employees use their devices. The Restrictions profiles lock down native functionality of Android for Work devices and vary based on device enrollment.

Create a New Profile

Back in the AirWatch Console:

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

Click **Android**

Select the Android for Work Configuration Type

Click **Android for Work**

*NOTE - We are selecting the Android for Work configuration here because we want to modify the Android for Work functionality, apps, and restrictions on the enrolled device. If we wanted to modify the unbadged apps or base Android functionality, we would select 'Device' here instead.*
Configure the General Settings

Add a New Android Profile

1. Ensure the **General** payload is selected.
2. Enter "**AfW Restrictions**" for the Name field.
3. Click **Assigned Groups** to display the list of available assignments.
4. Select **All Devices**
Configure Restrictions

Add a New Android Profile

1. Click the **Restrictions** payload.
2. Click **Configure**.
## Configure Screen Capture Restrictions

<table>
<thead>
<tr>
<th>Device Functionality</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Factory Reset</td>
<td>✔</td>
</tr>
<tr>
<td>Allow screen capture</td>
<td>✔</td>
</tr>
<tr>
<td>Allow adding Google accounts</td>
<td>✔</td>
</tr>
<tr>
<td>Allow removing the Android Work account</td>
<td>✔</td>
</tr>
<tr>
<td>Allow Outgoing Phone Calls</td>
<td>✔</td>
</tr>
</tbody>
</table>

Uncheck the **Allow Screen Capture** checkbox.
Configure Camera Restrictions

1. Scroll down to find the **Applications** section.
2. Uncheck the **Allow Camera** checkbox.
3. Click **Save & Publish**
### Publish the Profile

#### View Device Assignment

<table>
<thead>
<tr>
<th>Assignment Status</th>
<th>Friendly Name</th>
<th>User</th>
<th>Platform / OS / Model</th>
<th>Phone Number</th>
<th>Organization Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added</td>
<td>testuser</td>
<td>testuser</td>
<td>Android / Android 6.0.1</td>
<td></td>
<td><a href="mailto:your@email.shown.here">your@email.shown.here</a></td>
</tr>
</tbody>
</table>

Items 1-1 of 1

---

Click **Publish**.
Verify the Android For Work Camera Restrictions

On your device, notice that after we push the profile your device will no longer have the badged camera application available but your personal side (unbadged) camera will still be available for usage. This shows the camera restriction that we applied on the AirWatch profile created previously.

**NOTE - Due to lab network limitations, it may take a few minutes for the badged Camera application to be removed. If you still see it on your device, please wait until the application is successfully removed.**
1. Open your **non-badged Contacts** apps.
2. Take a screen shot (Power button and volume down / Power Button + Home Button at the same time for 2 seconds).

**NOTE - The shortcut to change screenshot may vary depending on your device model. Please see a lab assistant in case assistance is required.**

Notice that the screen shot was successful.
Verify the Android for Work Screenshot Restriction

1. Open the **badged Contacts** app.
2. Attempt taking a screen shot within the app and notice that it is not allowing you to take the screenshot and flashing a toast message depending on the device model and OS version.

This shows the screenshot restriction that we applied on the AirWatch profile created previously.
Approving Applications

This section is designed to walk you through the process of approving applications for integration between AirWatch and Android for Work. Applications that you push through the integration of AirWatch and Android for Work have the same functionality as their counterparts from the Google Play Store. However, you can use AirWatch features to add functionality and security to these applications.

- To add convenience of use, configure the Send Application Configuration option. Application configurations allow you to pre-configure supported key-value pairs and to push them down to devices along with the application. Examples of supported values may include usernames, passwords, and VPN settings. Support values depend upon the application.
- To add secure features, use AirWatch profiles for Android for Work. Profiles let you set passcodes, apply restrictions, and use certificates for authentication.

Add Public Application

Back in the AirWatch Console:

1. Click on **Add**
2. Click on **Public Application**
## Search for Public Application

<table>
<thead>
<tr>
<th>Add Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed By</td>
</tr>
<tr>
<td>Platform</td>
</tr>
<tr>
<td>Source</td>
</tr>
<tr>
<td>Name*</td>
</tr>
</tbody>
</table>

1. Select **Android** from the **Platform** dropdown.
2. Select **Search App Store** for the **Source**.
3. Enter "**VMware Browser"** for the **Name** field.
Select the VMware Browser App

Click the **VMware Browser** app.
Approve VMware Browser (IF NEEDED)

Click **Approve** if not approved already.
Confirm Approval for VMware Browser (IF NEEDED)

1. You may need to scroll down to view the Approve button.
2. Click Approve.

Click Approve again in the Application Popup.

**NOTE - Scroll down if you do not see the pop-up screen.**
Click Save (IF NEEDED)

1. You may need to scroll down to view the Approval Settings button.
2. Select **Keep approved when app requests new permissions**.
3. Click **Save**.
Select the Approved App (IF NEEDED)

if the application was already approved, click SELECT. If you had to approve the application in the previous step, skip to the next step.
Publish Public App

Click **Save & Assign**.
Add Assignment

Click **Add Assignment**.
Configure Assignment

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**.
3. Click **Add**.
Save and Publish VMware Browser

Click Save & Publish.
Preview Assigned Devices and Publish

Click **Publish**.
Verify Work Apps

In the previous section, we learned how we can approve and push an Android application from the AirWatch Console. In this section, we will verify that Work apps installed correctly on our enrolled Android device.

Confirm the Published VMware Browser Application Downloaded

Return to your testing Android device and confirm that the VMware Browser application has downloaded and displays as a Work app.

*NOTE - Depending on lab network traffic, you may need to wait several minutes for the download to complete.*

Using this process, you can rapidly approve new applications and deploy them to your users.

Open the Badged Android for Work Play Store App

Open your Work Play Store application on your Android device.

*NOTE - The screenshot may differ depending on device model and OS.*
Accept Google Play Terms of Service (IF NEEDED)

Work account

Terms of Service

Google Play gives you access to millions of apps to use or install. Links to instant apps will open without requiring installation, when available. Learn more

By using Google Play, you agree to the Google Play Terms of Service.

DECLINE  ACCEPT

If you are prompted with the Google Play Terms of Service, tap Accept. Otherwise, continue to the next step.

Open Play Store Menu

Tap the Menu button in the top-left corner.

NOTE - The screenshot may differ depending on device model and OS.
**View Play Store Work Apps**

Tap **My Work Apps** from the menu.

*NOTE - The screenshot may differ depending on device model and OS.*
Verify VMware Browser Is Available As A Work App

1. Tap Installed.
2. Confirm that the **VMware Browser** application is in your list of Work applications. You may need to scroll down to find the application.

**NOTE - The screenshot may differ depending on device model and OS.**

The VMware Browser app is listed as a Work app because it was approved as a Work app through the AirWatch Console while adding and assigning the application to your users. This streamlines and rapidly improves the process of approving and deploying Work apps to your Android devices!
Un-enrolling Your Android Device

You are now going to un-enroll the Android 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 Android 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.

1. Click **Devices**
2. Expand **List View**
3. Click on the **checkbox** next to the testuser device to select the device.

**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 the More Actions drop down.
2. Click Enterprise Wipe under the Management menu.
Enter your security PIN

Restricted Action - Enterprise Wipe

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

An Enterprise Wipe will unenroll and remove all managed enterprise resources from the selected device(s), including applications and profiles. This action cannot be undone and re-enrollment will be required for AirWatch to manage these device(s) again.

Enter Security PIN:

Forgot Security PIN?

Cancel

After selecting Enterprise Wipe, you will be prompted to enter your Security PIN which you set after your logged into the console. Note, on the screen you will see a check box to Prevent Re-Enrollment. **Do NOT check this check box.**

Enter your PIN ("1234") in the boxes. You will not need to press enter or continue, the console will confirm your PIN showing **Successful** and then pop up the window showing that an Enterprise Wipe has been requested.

Your Android device has now been successfully un-enrolled from AirWatch.
Learn More about Android Enterprise

This is just a sampling of the functionality you will see with Android Enterprise integrated with AirWatch. To learn more about features and functions please contact your AirWatch representative or visit our website at https://www.air-watch.com or the website for Android Enterprise at https://www.android.com/enterprise.
Conclusion

The work profile is designed specifically for personal (BYOD) devices. Using Android in the enterprise, AirWatch creates a "Work profile", a container which separates the personal space and the corporate space in a device. AirWatch can fully control the work profile but has zero control over the personal profile.
Module 2 - Android Enterprise Work Managed Enrollment (30 minutes)
PLEASE READ - DISCLAIMER BEFORE TAKING THIS MODULE

Work Managed mode requires the following software and hardware:

1. Android device 5.0 or higher.
2. Device must be factory reset in out of the box mode.

Please read the warning from the next step.

WARNING - Please DO NOT factory reset your personal device to take this lab. Refer to the the help desk to acquire a device that is already factory reset and ready to enroll into Work Managed mode. Only use devices from help desk to take this module.
Introduction

Android Enterprise, is the feature developed by Google to make Android devices (running 5.0 or later versions). It provides several features and configurations when integrated with AirWatch, which secures and manages devices in your organization.

Some of the features supported by Android in the enterprise are:

- Hosting your enterprise apps in Play Store
- Installing apps (both Play Store and enterprise apps) without user intervention.
- Manage license of paid apps.
- Modify app-specific configurations and permissions.
- Customize Play Store.
- Enhance data security using AirWatch restrictions and configurations.

AirWatch can configure both a Work profile and a Work managed mode. You will be going through the Work managed mode in this lab.
Work Managed Enrollment Methods

Work Managed Device mode gives AirWatch control of the entire device.

There are several ways to enroll Work Managed devices: using AirWatch Relay to perform NFC bump, using an AirWatch Identifier or token code, or scanning a QR code. Your business requirements determine which enrollment methods you will want to use.

AirWatch Relay

AirWatch Relay is an application that passes information from parent devices to all child devices being enrolled into Android for Work. This process is done through and NFC bump and provisions child devices to:

- Connect to the parent device to Wi-Fi network and region settings including the device date, time and location.
- Download the latest production version of AirWatch Agent for Android.
- Silently set the AirWatch Agent as device administrator.
- Automatically enroll into AirWatch.

AirWatch Relay allows you to bulk enroll all child devices at the same time before deploying them to end users and eliminates end users from having to enroll their own devices. All child devices must be in factory reset mode and have NFC enabled by default in order to be enrolled as Work Managed Device for Android for Work. This helps ensure that devices are not set up for personal use.

AirWatch Identifier

The AirWatch Identifier enrollment method is a simplified approach to enrolling Work Managed devices. You will enter a simple identifier, or hash value, on a factory reset device. After the identifier is entered, the enrollment is automated pushing down the AirWatch Agent. The user only has to enter server details, username and password.

Along with the identifier, you can also enroll on behalf of the end user by doing Single-User Device Staging. This method is particularly useful for administrators who set up multiple devices for an entire team or single members of a team. Such a method saves the end users the time and effort of enrolling their own devices.

QR Code

Devices such as tablets do not support NFC, so these devices cannot use the AirWatch Relay enrollment method which requires NFC bump.
QR code provisioning is an easy way to enroll a fleet of devices that do not support NFC. The QR code contains a payload of key-value pairs with all the information that is needed for the device to be enrolled. QR Code enrollment does not require a managed Google domain or a Google account. You should create the QR code before starting enrollment. You can use any online QR Code generator, such as Web Toolkit Online, to create your unique QR code. The QR code should include the Server URL and Group ID information. You can also include the username and password or the user will have to enter their credentials.
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](image)

**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.
TUTORIAL FOLLOW ALONG - Configuring Android Enterprise in the Console

In this Lab we will be covering some of the Android For Work basic functionality.

When running on Android 5.0 Lollipop devices, Android for Work is built into the operating system with no need for an additional application.

To begin using Android for Work inside the AirWatch Admin Console, you need to register your enterprise with Google. This creates your Android for Work admin account which connects with AirWatch to manage your enterprise devices. Users will not be able to use Android for Work features from their devices until registered with AirWatch. The Android for Work setup wizard simplifies the process. To simplify your experience, this initial process has been done for you. If you are interested in learning more about this process please talk to your AirWatch Sales Engineer or Representative.

Overview

**IMPORTANT** - You will not be able to make the configurations shown in the following steps within your lab!

This section is designed to only walk you through the process of configuring Android for Work so you can become familiar with the administrative process behind configuring Android for Work for AirWatch. Android for Work has already been configured for you in your lab environment, so no action is required on your part for this section.

Once a Google Admin Account is bound to AirWatch, you cannot reuse this Google Admin for another organization. Due to this limitation, you would be unable to use the Google Admin Account we have already bound to AirWatch for this lab.

AirWatch Android for Work Configuration

This section will demonstrate how to configure Android for Work within the AirWatch Console.

**IMPORTANT** - Remember, you will not be able to make the configurations shows in the following steps within your lab! This is for demonstration purposes only so that you can become familiar with the process.
Open Settings

1. Click **Groups & Settings**.
2. Click **All Settings**.
Open Android for Work Configuration

1. Click **Devices & Users**.
2. Expand **Android**.
3. Click **Android For Work**.
4. Click **Configure**.
Provide Google Admin Account

1. Confirm you are logged into your Google Admin Account that you wish to associate with your Android for Work configuration.

   **NOTE** - Once you register a Google Admin Account to Android for Work, you cannot disassociate your Google Admin Account from that Organization. Ensure the Google Admin Account shown is the account you wish to associate with your Organization!

2. Click Get Started
Provide your Organization Details

1. Enter your Organization Name.
2. Check the Google Play Agreement checkbox.
3. Click Confirm.
Complete Registration

Set up complete
Thanks for choosing Android

You now need to return to your EMM provider to complete your registration.

Click **Complete Registration** to return to the AirWatch Android for Work configuration.
1. On the Android for Work Settings page, scroll down until you see the Google Admin Console Settings and Google API Settings sections.

2. Under Google Admin Console Settings, note that the account information you provided during the Android for Work configuration step is displayed here.

3. Confirm that your Android for Work Registration Status is shown as Successful.

4. Note that the Client ID and Google Service Account Email Address have been created and configured for you automatically. No additional configurations with Android for Work or the Google Developers Console are required.

Your Organization Group is now successfully configured with Android for Work!
Device Enrollment with Android Enterprise (Work Managed) Identifier Enrollment

In this section, we will be enrolling your device with AirWatch and get it set up with Android for Work on the Work Managed mode.

The AirWatch Identifier enrollment method is a simplified approach to enrolling Work Managed devices. You will enter a simple identifier, or hash value, on a factory reset device. After the identifier is entered, the enrollment is automated pushing down the AirWatch Agent.

Find your Group ID from AirWatch Console

The first step is to make sure you know what your **Organization Group ID** is.

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

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

Please Read - Before you proceed with Work Managed Identifier Enrollment

**WARNING** - Module 2 requires that your Device must be in Out of Box mode after a Factory Reset. Please DO NOT factory reset your personal device to take this lab. Refer to the help desk to acquire a device that is already factory reset and ready to enroll into Work Managed mode. Only use devices from help desk to enroll into Work Managed mode.

**NOTE** - Screenshots may differ due to differences in device models and operating system versions.
Out of Box Enrollment

Turn on your device from a factory reset state and tap **Start**.
1. Tap to connect to the appropriate WiFi network based on your location.
2. Tap **Next** after connecting to WiFi.
Review the Terms and Conditions

Terms and conditions

End User License Agreement

Read the End User License Agreement carefully. It contains important information.

Learn more

Diagnostic data

CONSENT TO PROVIDE DIAGNOSTIC AND USAGE DATA

Samsung Electronics Co., Ltd. and its affiliates (“Samsung”) would like your help in improving the quality and performance of its products and services. Your device includes diagnostic software that

Tap Next.
Accept the Terms and Conditions

Tap Agree.
Enter the AirWatch Identifier

Enter "afw#airwatch" into the Email or Phone field. This will automatically download the AirWatch Agent for you.
1. Review and configure the Google Services as desired and then scroll down to the bottom.
2. Tap Next.
Install the AirWatch Agent

This account requires mobile device management. Install the AirWatch Agent app to enforce security policies required by the account.

Tap Install.
Confirm the special access required by the AirWatch Agent and tap **Install**.
Enter AirWatch Server Details for Enrollment

Welcome to AirWatch!

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

You will be guided through a three part process to authenticate, secure and configure your device.

Choose Authentication Method:

✉️ EMAIL ADDRESS

.vs SERVER DETAILS

🔑 QR CODE

Once the Agent has launched you can enroll the device. To do so, you must first select the AirWatch authentication method.

Tap Server Details
Attach the AirWatch MDM Agent to the HOL Sandbox

After selecting the Server authentication method, you need to supply the information to authenticate. To do so, follow the below steps.

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

Allow Agent to Manage Phone Calls (IF NEEDED)

If prompted, tap **Allow** when the Agent requests permission to make and manage phone calls. Otherwise, continue to the next step.
Authenticate the AirWatch MDM Agent

1. Enter "testuser" for the Username field.
2. Enter "VMware1!" for the Password field.
3. Tap Continue.
Encrypt Device

Set up work device

To continue setting up your device, you'll need to encrypt it. This may take some time.

Tap Encrypt.
Review Encryption Requirements

You can encrypt accounts, settings, downloaded apps and their data, media, and other files.

Encryption takes an hour or more. Before you start, make sure that the battery is charged and keep the device plugged in until encryption is complete. Interrupting this process may lead to the loss of some or all of your data.

Tap **Encrypt Device**.
Confirm and Begin Encryption

1. If you are taking the Hands on Lab with a provided device, please tap to enable **Fast Encryption** to reduce the time required to encrypt the device.
2. Tap **Encrypt Device** to confirm and continue.
The device will begin encrypting and will restart as part of this process. Continue to the next step once the device has finished encrypting and restarts.
Complete Enrollment
Terms and Conditions

Please read the following carefully before downloading and installing Android for Work on your device.

Samsung provides the Trusted Boot, as one of its security features, to detect rooting and custom ROM (i.e., not Samsung official firmware) installed in your device during boot time. After Android for Work is installed, and if such rooting or custom ROM is detected, your device will automatically enter factory reset mode and the data or application you stored or installed in your device will be deleted. You are strongly advised to back up important data or information in other devices such as your personal computer. Samsung shall not be responsible for any loss of data or
Once the device restarts, you should see the Terms and Conditions for Android for Work. Tap **Agree**.
Set Up Android for work
Set up work profile

Your organization controls this profile and keeps it secure. You control everything else on your device.

The following app will need to access this profile:

Agent
Tap \textbf{NEXT}.  

\textit{NOTE - This may take some time, please be patient while the Setup process completes.}

\textbf{Administrator Rights}

Your admin has the ability to monitor and manage settings, corporate access, apps, permissions, theft-protection features, and data associated with this device, including network activity and your device's location information.

Contact your admin for more information, including your organization's privacy policies.

1. I consent

2. OK
1. Tap **I consent** to agree to the administrator rights terms.
2. Tap **OK** to confirm the Privacy Policy.

**NOTE** - Enrollment time may vary depending on your network connectivity. Typically, it takes around 1 minute to complete. Please be patient while this process completes.

**IMPORTANT** - During the enrollment process, you will see several processing screens. Please note that you do not need to interact with the device further until you see the AirWatch Agent app confirming your enrollment (next page).
Wait for Device Connectivity (IF NEEDED)
Agent

My Device

Owner: testuser
samsung SM-G920V
Android for Work - Work Profile

Connectivity Issue

Compliant

Device Status
Information on the current state of this device

Compliance
Information on compliance status of this device

Profiles
A list of profiles installed on this device

Managed Apps
A list of managed Apps on this device

About
Information about the agent
If you see a Connectivity Issue notification, the device may be taking several minutes to establish a connection to Google Cloud Messaging. Please wait until you see the Connectivity Issue notification change to Connectivity Normal before continuing.

**NOTE - If you do not see any Connectivity Issue notifications, please continue to the next step.**

**Confirm Device Enrollment**

![Device Status](Image)

**Device Status**
Information on the current state of this device

**Compliance**
Information on compliance status of this device

**Profiles**
A list of profiles installed on this device

**Managed Apps**
A list of managed Apps on this device

[Congratulations! You have successfully enrolled your device.]
You have now completed the AirWatch MDM Agent configuration wizard. After the enrollment process completes, the AirWatch Agent will display the notification **Congratulations! You have successfully enrolled your device.**

You can now **Exit** the AirWatch Agent.
Un-enrolling Your Android Device

You are now going to un-enroll the Android 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 Android 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.

1. Click **Devices**
2. Expand **List View**
3. Click on the **checkbox** next to the testuser device to select the device.

**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 the More Actions drop down.
2. Click Enterprise Wipe under the Management menu.
Enter your security PIN

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

An Enterprise Wipe will unenroll and remove all managed enterprise resources from the selected device(s), including applications and profiles. This action cannot be undone and re-enrollment will be required for AirWatch to manage these device(s) again.

Last Seen   Friendly Name   C/E/S   User   Platform   Model   Organization Group

Enter Security PIN: [ ] [ ] [ ] [ ]

Forgot Security PIN?

After selecting Enterprise Wipe, you will be prompted to enter your Security PIN which you set after your logged into the console. Note, on the screen you will see a check box to Prevent Re-Enrollment. Do NOT check this check box.

Enter your PIN ("1234") in the boxes. You will not need to press enter or continue, the console will confirm your PIN showing Successful and then pop up the window showing that an Enterprise Wipe has been requested.

Your Android device has now been successfully un-enrolled from AirWatch.
Conclusion

The Work managed profile is designed specifically for corporate owned devices. AirWatch provisions the devices as Device Owner ensuring the organization has full control of the device as it "owns the device" and provides more features to ensure the device and the confidential data in the device are secure. Device Owner supports all the Profile Owner-supported features as well as additional features.
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-1857-07-UEM

Version: 20180323-184049