# Table of Contents

Lab Overview - HOL-1957-06-UEM - Workspace ONE UEM - Android Management........2
  Lab Guidance .................................................................................................................3
Module 1 - Introduction to Android Enterprise ...............................................................8
  Introduction..........................................................................................................................9
  Conclusion............................................................................................................................13
Module 2 - Android Enterprise - Work Profile.................................................................14
  Introduction........................................................................................................................15
  Login to the Workspace ONE UEM Console .................................................................16
  Configuring Android Enterprise in the Console.........................................................22
  Device Enrollment with Android Enterprise (Work Profile)........................................29
  Android Enterprise Profiles..............................................................................................57
  Approving Applications .....................................................................................................66
  Verify Work Apps ...............................................................................................................77
  Un-enrolling Your Android Device ..................................................................................81
  Learn More about Android Enterprise............................................................................85
  Conclusion............................................................................................................................86
Module 3 - Android Enterprise Work Managed Enrollment ..............................................87
  PLEASE READ - DISCLAIMER BEFORE TAKING THIS MODULE.................................88
  Introduction........................................................................................................................89
  Work Managed Enrollment Methods..............................................................................90
  Login to the Workspace ONE UEM Console.................................................................92
  Configuring Android Enterprise in the Console.........................................................98
  Device Enrollment with Android Enterprise (Work Managed) Identifier
  Enrollment .........................................................................................................................105
  Un-enrolling Your Android Device ................................................................................142
  Conclusion............................................................................................................................146
Lab Overview - HOL-1957-06-UEM - Workspace ONE UEM - Android Management
Lab Guidance

Note: It may take more than 90 minutes to complete this lab. You should expect to only finish 2-3 of the modules during your time. The modules are independent of each other so you can start at the beginning of any module and proceed from there. You can use the Table of Contents to access any module of your choosing.

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

Explore the management options that Workspace ONE UEM provides with Android Enterprise and how these options impact enrolling, managing, and securing your Android devices. Learn about the various management options available for Android and how these impact your management capabilities with Workspace ONE UEM to decide which option is optimal for your desired experience and use case. Additionally, review how Remote Management can be used with Android devices for remote troubleshooting and assistance.

Lab Module List:

- **Module 1 - Introduction to Android Enterprise** (15 minutes) (Beginner) Learn the fundamentals of Android Enterprise and device enrollment with Workspace ONE UEM to secure your Android devices using modern device management APIs.
- **Module 2 - Android Enterprise - Work Profile** (30 minutes) (Beginner) Work Profile is a feature of Android Enterprise that allows device administrators to manage business applications and data while leaving the device under the user's control. It provides several features and configurations when integrated with Workspace ONE, which secures and manages devices in your organization including application management for enterprise and public apps, device profile configurations to enhance security and functionality.
- **Module 3 - Android Enterprise Work Managed Enrollment** (30 minutes) (Beginner) Enroll an Android device for Work Managed mode, which is designed for corporate-owned devices. Explore how Workspace ONE UEM and Work Managed enrollment grants a wider range of policies and controls to manage your corporate-owned devices.

Lab Captains:

- Roger Deane, Sr. Manager, Technical Marketing, USA
- Shardul Navare, Sr. Technical Marketing Architect, USA
- Chris Halstead, EUC Staff Architect, USA
- Andreano Lanusse, EUC Staff Architect, USA
- Justin Sheets, Sr. Technical Marketing Architect, USA

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

http://docs.hol.vmware.com

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


**Location of the Main Console**

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

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

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

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

Click and Drag Lab Manual Content Into Console Active Window

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

Accessing the Online International Keyboard

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

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

Click once in active console window

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

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

1. Click on the "@ key".

Notice the @ sign entered in the active console window.

Activation Prompt or Watermark

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

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

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

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

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

What is Android Enterprise?

Android enterprise debuted with 5.0 Lollipop in 2014 as an optional solution manufacturers could add to their OS images in order to integrate a common set of device management and Enterprise Mobility Management (EMM) APIs. From 6.0 Marshmallow, it was no longer optional and has since been a mandatory component for all Google Mobile Service (GMS) certified manufacturers.

What does Android Enterprise Offer?

Android Enterprise offers a wide variety of rich features that cover numerous device management scenarios:

- A rich Enterprise Mobility Management (EMM) experience. This allows device administrators to send configurations, applications, and policies down to any Android Enterprise (AE) device, providing a secure method of managing devices and corporate data no matter where your devices are.
- **Work Profile** mode for BYOD (Bring Your Own Device) scenarios, which allows for a device to have a separate work container from their personal apps and data.
- **Work-Managed** mode (previously called device owner), which provides corporations a larger suite of options for securing corporate owned devices that are not intended for personal use.
- **Corporately Owned, Single Use** (COSU) mode, which provides corporations with a kiosk-like experience. The Work-Managed device is locked down in a Kiosk-like state, granting access to a few applications or resources instead of the entire underlying device operating system.
- **Corporate Owned, Personally Enabled** (COPE) joins the Work Profile and Work-Managed modes to provide a fully managed device with personal space.
- **Zero-Touch Enrollment** for out of the box Android 8.0 and higher devices, providing a streamlined enrollment experience for end users.
- A corporate-managed Managed Google Play portal, allowing administrators to explicitly approve applications to an application store that can be accessed by end users.
- **Silent Application Installation** without requiring a user provided Google account on the device.
- **App Configuration**, enabling device administrators to deploy key-value pairs to managed applications to modify the end user experience.
- **Mandatory Device Encryption** to ensure that your corporate resources are secured and protected on the device.
Understanding Device Management Scenarios

The above graphic shows the big picture differences between various device management scenarios.

**Bring Your Own Device (BYOD):**

- Commonly used where employees or end users have their own personal devices that need access to corporate resources.
- To avoid managing the end user's personal data or apps, a **Work Profile** can be deployed to keep the corporate apps and data separate from their personal apps and data.
- This grants device administrators the ability to securely control access to corporate resources from a personal device without managing the full personal device.

**Corporate Owned:**

- Commonly used where corporations own devices that are given to employees or end users to fulfill their role or task.
- **Work-Managed** mode allows for the entire device to be managed and controlled, allowing for a wider range of configurations.
- **Work-Managed** mode does not provide an un-managed personal space and should only be used for corporate owned devices.

**Corporate Owned Single Use (COSU):**
• Commonly used where corporations own devices that are used as Kiosks or have Kiosk-like applications running on them.
• Corporate Owned Single Use leverages **Work-Managed** mode to manage the entire device, but does not grant the end user access to the full underlying device operating system.

**Corporate Owned, Personally Enabled (COPE):**

• Commonly used where corporations own devices that are given to employees or end users that permits some level of personal usage while still being corporately controlled.
• Corporate Owned, Personally Enabled leverages a **Work-Managed** personal space for varying amounts of personal usage while employing a **Work Profile** to control corporate resources, data, and apps.
• This joins the ideas of **Work Profile** and **Work-Managed** modes into a single device.

**Different Enrollment Methods**

In addition to providing different device management scenarios, there are also multiple ways in which devices can be enrolled into Android Enterprise.

**Near-Field Communication (NFC) Enrollment**

With the Near-Field Communication (NFC) bump method, a NFC programmer app is setup on a designated programmer device. Subsequent devices are “bumped” into the programmer device to pass the necessary initial policies (such as Wi-Fi, device configurations, etc.) to the bumped device via NFC.

The process will vary slightly in terms of pre-applied settings, what agent is downloaded in order to enroll the device on the relevant platform, etc. AirWatch allows for the additional configuration of a named account to directly enroll the device against.

**Hashtag (#) Enrollment or Device Policy Controller (DPC) Identifier Enrollment**

This method was introduced in Android 6.0 Marshmallow. When prompted to add or create an account on a freshly wiped (or directly from the box) device, rather than enter in a Google account, the administrator would type in `afw#airwatch` and then the device would download the AirWatch Agent and begin the enrollment process with the correct configurations.
**QR Enrollment**

By tapping on **Welcome** 6 times when the device boots into the setup Wizard, it will prompt the device to connect to Wi-Fi and start QR enrollment.

In Android 9.0 P, the QR payload is bundled into the system and therefore doesn’t require a download. This offers faster provisioning as the device no longer needs to connect to the internet to download the QR package and the ability to add Wi-Fi credentials to the QR code.

**Zero-Touch Enrollment**

Devices are purchased through authorized resellers, assigned to AirWatch and then later, when the end-user first takes the device freshly out of the box, will be ready to enroll as a work-managed device straight away. With Zero-Touch enrollment, administrators can send enrolled and configured devices directly to end-users to authenticate with.
Conclusion

Let's summarize what we have learned from the new Android Enterprise Implementation:

- Prior to Android enterprise the Android devices had to deal with inconsistent management capabilities across various Android manufacturers and app developers
- Android enterprise offers a set of consistent APIs for device management and app management
- Android enterprise securely separates corporate and personal data, or enables a purely corporately-owned profile without a user space
- Once enrolled, an Android enterprise-enabled device no longer needs a Google account in order to install applications
- More features are coming in future to expand capabilities and enable more management types
Introduction

Android Enterprise is developed by Google to allow organization to securely manage Android devices (running 5.0 or later). It provides several features and configurations when integrated with Workspace ONE UEM, 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 Workspace ONE UEM restrictions and configurations.

Workspace ONE UEM 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 Workspace ONE UEM Console

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

Launch Chrome Browser

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

The default home page for the browser is https://labs.awmdm.com. Enter your Workspace ONE UEM Admin Account information and click the Login button.

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

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

NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the Workspace ONE UEM Hands On Labs server.
Accept the End User License Agreement

Terms of Use

You must accept the following VMware End User License Agreement to use Workspace ONE UEM.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT (“EULA”). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

“Affiliate” means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls

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

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

Security Settings

Password Recovery Question 1

Password Recovery Question *
What was your childhood nickname?

Password Recovery Answer *
VMware!

Confirm Password Recovery Answer *
VMware!

Security PIN

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

Security PIN *
1234

Confirm Security PIN *
1234

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

Close the Welcome Message

Workspace ONE UEM Console Highlights

Powered by VMware AirWatch!

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

Workspace ONE UEM transforms your business so you can:

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

We will be covering some of the Android basic functionality.

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

To begin using Android Enterprise inside the Workspace ONE UEM Console, you need to register your enterprise with Google. This creates your Android Enterprise admin account which connects with Workspace ONE UEM to manage your enterprise devices. Users will not be able to use Android Enterprise features from their devices until registered with Workspace ONE UEM. The Android Enterprise 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 Workspace ONE UEM Sales Engineer or Representative.

NOTE - Once a Google Admin Account is bound to Workspace ONE UEM, 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 Workspace ONE UEM for this lab.
Open Settings (FOLLOW ALONG)

NOTE - The following changes have already been configured for you as part of the lab!

1. Click **Groups & Settings**
2. Click **All Settings**
Open Android Enterprise Configuration (FOLLOW ALONG)

1. Click Devices & Users
2. Expand Android
3. Click Android Enterprise
4. Click Register with Google

NOTE - The following changes have already been configured for you as part of the lab!

1. Click Devices & Users
2. Expand Android
3. Click Android Enterprise
4. Click Register with Google
Provide Google Admin Account (FOLLOW ALONG)

1. Confirm you are logged into your Google Admin Account that you wish to associate with your Android Enterprise configuration.
   
   *NOTE - Once you register a Google Admin Account to Android Enterprise, 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

**NOTE - The following changes have already been configured for you as part of the lab!**
Provide your Organization Details (FOLLOW ALONG)

NOTE - The following changes have already been configured for you as part of the lab!

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

Set up complete
Thanks for choosing Android

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

COMPLETE REGISTRATION

NOTE - The following changes have already been configured for you as part of the lab!

Click Complete Registration to return to the Workspace ONE UEM Android Enterprise configuration
Confirm Android Enterprise Integration (FOLLOW ALONG)

Back in the Workspace ONE UEM Console,

1. On the Android Enterprise Configuration 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 Enterprise configuration step is displayed here.
3. Confirm that your **Android Enterprise 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 Enterprise or the Google Developers Console are required.

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

In this section, we will be enrolling your device with Workspace ONE UEM and get it set up with Android Enterprise.

NOTE - The screenshots in this article will differ depending on the make and model of the Android device you are using.
Download the Workspace ONE Intelligent Hub (IF NEEDED)

If you do not have the Workspace ONE Intelligent Hub app on your device, you will need to download it the app before continuing.
To install the Workspace ONE Intelligent Hub app, you can open the Google Play Store app and download the free **Workspace ONE Intelligent Hub** app or navigate to [https://www.getwsone.com](https://www.getwsone.com) in your device browser and follow the **Get it on Google Play** link to the **Workspace ONE Intelligent Hub** page in the Google Play Store.

**Launching the Workspace ONE Intelligent Hub App**

Launch the **Hub** app on the device.
Provide the Workspace ONE UEM Server URL

Email address or server

labs.awmdm.com

QR CODE

NEXT
1. Enter `labs.awmdm.com` for the Server URL.
2. Tap NEXT.

**Allow Phone Permission for Hub (IF NEEDED)**

![Allow Hub to make and manage phone calls?](image)

Tap Allow.

**Find your Group ID from Workspace ONE UEM Console**

The first step is to make sure you know what your Organization Group ID is. In the Workspace ONE UEM Console,

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

**NOTE** - The Group ID is required when enrolling your device in the following steps.
Attach the Workspace ONE Intelligent Hub to the HOL Sandbox

Email address or server
https://ds1193.awmdm.com

Group ID
{Your Group ID}

1. Enter your **Group ID** for the **Group ID** field. This was noted previously in the **Finding your Group ID** step.
2. Tap **NEXT**.
Provide User Credentials

1. Enter **testuser** for the **Username** field.
2. Enter **VMware1!** for the **Password** field.
3. Tap **Continue**.
Confirm the Privacy Policy
Your privacy matters.

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

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

Data Collected by Hub

Tap here for an overview of the data that this app may collect about device hardware, diagnostics and user information to function properly, and to secure
Accept the Data Sharing Policy
Data Sharing

Want an even better app experience?
Help us improve and develop new app features and functionality that will make you even more productive.

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

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

I AGREE

NOT NOW
Tap **I Agree** for the Data Sharing Policy.
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 the Android Enterprise Work Profile
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:

Hub
Tap **NEXT**.

**NOTE - This may take some time, please be patient while the Setup process completes.**
(Optional) Device Encryption
Set up work 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 Enterprise 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 Workspace ONE Intelligent Hub app confirming your enrollment (next page).*
Confirm Device Enrollment
Account

Test User
testuser@vmworldhol.com

This Device

Support

About

Congratulations! You have successfully enrolled your device.
You have now completed enrolling your device using the Workspace ONE Intelligent Hub. After the enrollment process completes, the Workspace ONE Intelligent Hub app will display the notification **Congratulations! You have successfully enrolled your device.**

You can now **Exit** the Workspace ONE Intelligent Hub app.

**Badged Apps**

On your Android device, you should now see the new Work applications. Android Enterprise 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 Workspace ONE Intelligent Hub is badged and exists only within the Work Profile data space.

**IMPORTANT** - There is no control over personal apps nor will the Hub app 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 Diagram]

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 Enterprise profiles to modify devices restrictions and to assist in protecting sensitive data. Profiles serve many different purposes, from letting you enforce corporate rules and procedures to tailoring and preparing Android Enterprise capable devices for how they will be used.

**IMPORTANT - If your device is enrolled with Android Enterprise, then ONLY Android Enterprise 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 Enterprise devices and vary based on device enrollment.

Create a New Profile

In the Workspace ONE UEM Console,

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

Click Android
Configure the General Settings

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. Enter **All Devices** and select the **All Devices (your@email.shown.here)** group.
Configure Restrictions

1. Click the **Restrictions** payload.
2. Click **Configure**.

Configure Screen Capture Restrictions

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

Click Publish.
Verify the Android Enterprise 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 Enterprise 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 Workspace ONE UEM and Android Enterprise. Applications that you push through the integration of Workspace ONE UEM and Android Enterprise have the same functionality as their counterparts from the Google Play Store. However, you can use Workspace ONE UEM 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 depends upon the application.
- To add secure features, use Workspace ONE UEM profiles for Android Enterprise. Profiles allow you to set passcodes, apply restrictions, and use certificates for authentication.

Add Public Application

In the Workspace ONE UEM Console,

1. Select Add.
2. Select Public Application.
1. Select **Android** from the Platform drop-down menu.
2. Select **Search App Store** for the Source.
3. Enter **VMware Browser** in the Name text box.
4. Click **Next**.
Select the VMware Browser App

Click the **VMware Browser** app.

**Approve VMware Browser (IF NEEDED)**

Click **Approve**.
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 pop-up window.

Note: Scroll down if you do not see the pop-up window.
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

VMware Browser - Update Assignment

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

Click **Add Assignment**.
Configure Assignment

VMware Browser - Add Assignment

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

2. Select **Auto** for the App Delivery Method.

3. Click **Add**.

Adaptive Management Level: **Open Access**

Apply policies that give users open access to apps with minimal administrative management.

Would you like to enable Data Loss

ADD CANCEL
Save and Publish VMware Browser

VMware Browser - Update Assignment

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

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 Workspace ONE UEM 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 Enterprise 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 Workspace ONE UEM 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 Workspace ONE UEM.

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

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

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

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

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

To Enterprise Wipe your device you will first bring up the Workspace ONE UEM Console in a web browser. You may need to re-authenticate with your credentials (your 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 Workspace ONE UEM Console. Use the value you specified for your Security PIN.

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

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

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

This is just a sampling of the functionality you will see with Android Enterprise integrated with Workspace ONE UEM. To learn more about features and functions please contact your VMware End User Computing representative or visit our website at http://www.workspaceone.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, Workspace ONE UEM creates a "Work profile", a container which separates the personal space and the corporate space in a device. Workspace ONE UEM can fully control the work profile but has zero control over the personal profile.
Module 3 - Android Enterprise Work Managed Enrollment
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 developed by Google to allow organization to securely manage Android devices (running 5.0 or later versions). It provides several features and configurations when integrated with Workspace ONE UEM, 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 Workspace ONE UEM restrictions and configurations.

Workspace ONE UEM 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 Workspace ONE UEM Console

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

Launch Chrome Browser

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

The default home page for the browser is https://labs.awmdm.com. Enter your Workspace ONE UEM Admin Account information and click the Login button.

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

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

**NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the Workspace ONE UEM Hands On Labs server.**
Accept the End User License Agreement

Terms of Use

You must accept the following VMware End User License Agreement to use Workspace ONE UEM.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT (“EULA”). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If you are licensing the Software for evaluation purposes, your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided “AS-IS” without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 “Affiliate” means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls

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

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

Security Settings

Password Recovery Question 1

Password Recovery Question *

What was your childhood nickname?

Password Recovery Answer *

VMware1!

Confirm Password Recovery Answer *

VMware1!

Security PIN

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

Security PIN *

1234

Confirm Security PIN *

1234

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

Close the Welcome Message

Workspace ONE UEM Console Highlights

Powered by VMware AirWatch!

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

Workspace ONE UEM transforms your business so you can:

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

Don't show this message on login
After completing the Security Settings, you will be presented with the Workspace ONE UEM Console Highlights pop-up.

1. Click on the **Don't show this message on login** check box.
2. Close the pop-up by clicking on the **X** in the upper-right corner.
Configuring Android Enterprise in the Console

We will be covering some of the Android basic functionality.

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

To begin using Android Enterprise inside the Workspace ONE UEM Console, you need to register your enterprise with Google. This creates your Android Enterprise admin account which connects with Workspace ONE UEM to manage your enterprise devices. Users will not be able to use Android Enterprise features from their devices until registered with Workspace ONE UEM. The Android Enterprise 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 Workspace ONE UEM Sales Engineer or Representative.

**NOTE - Once a Google Admin Account is bound to Workspace ONE UEM, 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 Workspace ONE UEM for this lab.**
Open Settings (FOLLOW ALONG)

NOTE - The following changes have already been configured for you as part of the lab!

1. Click Groups & Settings
2. Click All Settings
Open Android Enterprise Configuration (FOLLOW ALONG)

1. Click Devices & Users
2. Expand Android
3. Click Android Enterprise
4. Click Register with Google

NOTE - The following changes have already been configured for you as part of the lab!

1. Click Devices & Users
2. Expand Android
3. Click Android Enterprise
4. Click Register with Google
Provide Google Admin Account (FOLLOW ALONG)

1. Confirm you are logged into your Google Admin Account that you wish to associate with your Android Enterprise configuration.
   
   NOTE - Once you register a Google Admin Account to Android Enterprise, 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

NOTE - The following changes have already been configured for you as part of the lab!
Provide your Organization Details (FOLLOW ALONG)

NOTE - The following changes have already been configured for you as part of the lab!

1. Enter your **Organization Name**.
2. Check the **Google Play Agreement** checkbox.
3. Click **Confirm**.
Complete Registration (FOLLOW ALONG)

Set up complete
Thanks for choosing Android

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

NOTE - The following changes have already been configured for you as part of the lab!

Click Complete Registration to return to the Workspace ONE UEM Android Enterprise configuration
Confirm Android Enterprise Integration (FOLLOW ALONG)

Back in the Workspace ONE UEM Console,

1. On the Android Enterprise Configuration 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 Enterprise configuration step is displayed here.
3. Confirm that **your Android Enterprise 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 Enterprise or the Google Developers Console are required.

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

In this section, we will be enrolling your device with Workspace ONE UEM and get it set up with Android Enterprise on the Work Managed mode.

The Workspace ONE UEM 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 by pushing down the Workspace ONE Intelligent Hub.

Find your Group ID from Workspace ONE UEM 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

Welcome!

ENGLISH

START

EMERGENCY CALL

ACCESSIBILITY

Turn on your device from a factory reset state and tap Start.
Connect to WiFi

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

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.

Terms and conditions

I agree to the terms of the End User License Agreement.

DISAGREE  AGREE

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

NEXT  

Tap Agree.
Enter the AirWatch Identifier

Enter `afw#airwatch` into the Email or Phone field. This will automatically download the Workspace ONE Intelligent Hub app for you.
1. Review and configure the Google Services as desired and then scroll down to the bottom.
2. Tap Next.
Install the Workspace ONE Intelligent Hub
Android Enterprise

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

Intelligent Hub
Tap **Install**.
Confirm Workspace ONE Intelligent Hub Special Access and Install
Hub

Do you want to install this application? It does not require any special access.
Confirm the special access required by the Workspace ONE Intelligent Hub and tap **Install**.
Provide the Workspace ONE UEM Server URL

Email address or server

labs.awmdm.com

QR CODE

NEXT
1. Enter labs.awmdm.com for the Server URL.
2. Tap NEXT.

Allow Phone Permission for Hub (IF NEEDED)

Tap Allow.

Find your Group ID from Workspace ONE UEM Console

The first step is to make sure you know what your Organization Group ID is. In the Workspace ONE UEM Console,

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

NOTE - The Group ID is required when enrolling your device in the following steps.
Attach the Workspace ONE Intelligent Hub to the HOL Sandbox

Email address or server
https://ds1193.awmdm.com

Group ID
{Your Group ID}

1. Enter your Group ID for the Group ID field. This was noted previously in the Finding your Group ID step.
2. Tap NEXT.
Provide User Credentials

1. Enter testuser for the Username field.
2. Enter VMware1! for the Password field.
3. Tap Continue.
Confirm the Privacy Policy
Your privacy matters.
VMware Workspace ONE collects information that is required to provide secure access to your work data and applications. Below you will find an overview of data collected by Workspace ONE and Hub to provide optimal performance, security and support. For information about how your company handles information collected by Workspace ONE, please contact your company.

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

Data Collected by Hub
Tap here for an overview of the data that this app may collect about device hardware, diagnostics and user information to function properly, and to secure
Tap **I Understand** for the Privacy Policy.
Accept the Data Sharing Policy
Want an even better app experience?

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

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

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

I AGREE

NOT NOW
Tap **I Agree** for the Data Sharing Policy.
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 the Android Enterprise Work Profile
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:

Hub
Tap **NEXT**.

**NOTE** - *This may take some time, please be patient while the Setup process completes.*
(Optional) Device Encryption
Set up work 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 Enterprise 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 Workspace ONE Intelligent Hub app confirming your enrollment (next page).**
Confirm Device Enrollment
Account

Test User
testuser@vmworldhol.com

This Device

Support

About

Congratulations! You have successfully enrolled your device.
You have now completed enrolling your device using the Workspace ONE Intelligent Hub. After the enrollment process completes, the Workspace ONE Intelligent Hub app will display the notification *Congratulations! You have successfully enrolled your device.*

You can now **Exit** the Workspace ONE Intelligent Hub app.
Un-enrolling Your Android Device

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

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

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

Enterprise Wipe (un-enroll) your iOS device

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

To Enterprise Wipe your device you will first bring up the Workspace ONE UEM Console in a web browser. You may need to re-authenticate with your credentials (your 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 Workspace ONE UEM Console. Use the value you specified for your Security PIN.

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

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

**NOTE** - Depending upon **Internet connectivity of the device and responsiveness of the lab infrastructure, this could take a couple of minutes or more if there is excessive traffic occurring within the Hands On Lab environment.**
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-1957-06-UEM

Version: 20181104-164531