MANAGING BRING-YOUR-OWN ANDROID DEVICES: VMWARE WORKSPACE ONE
OPERATIONAL TUTORIAL
VMware Workspace ONE
Table of Contents

Overview

– Introduction
– Audience

Getting Started with Android Device Management

– Introduction
– Prerequisites
– Understanding Android Device Modes
– Logging In to the Workspace ONE UEM Console
– Registering for Android EMM

Enrolling Bring-Your-Own Android Devices

– Introduction
– Prerequisites
– Enrolling an Android Device into Work Profile Mode
– Navigating Android Work Profile

Configuring Profiles for Bring-Your-Own Android Devices

– Introduction
– Prerequisites
– Understanding Configuration Options for Android Profiles
– Configuring Restriction Profiles
– Testing Android Restriction Settings
Managing Applications for Bring-Your-Own Android Devices

- **Introduction**
- **Prerequisites**
- Deploying VMware Workspace ONE Web to an Android Device
- Verifying Workspace ONE Web on an Android Device

Summary and Additional Resources

- **Conclusion**
- Terminology Used in This Tutorial
- Additional Resources
- About the Author
- Feedback
OT-WS1-And-BYOD

Overview

Introduction
VMware provides this operational tutorial to help you with your VMware Workspace ONE® environment. In this tutorial, you enroll a bring-your-own-device (BYOD) Android device using the VMware Workspace ONE® Intelligent Hub, configure and test a restrictions profile, and deploy VMware Workspace ONE® Web to a BYOD Android device.

Audience
This operational tutorial is intended for IT professionals and Workspace ONE administrators of existing production environments. Both current and new administrators can benefit from using this tutorial. Familiarity with networking and storage in a virtual environment is assumed, including Active Directory, identity management, and directory services. Knowledge of additional technologies such as VMware Identity Manager™ and VMware Workspace ONE® UEM (unified endpoint management), powered by VMware AirWatch, is also helpful.

Getting Started with Android Device Management

Introduction
This exercise walks-through deploying a bring-your-own Android device in Work Profile mode. The Work Profile creates a dedicated device container for business applications and content. Although this mode enables you to manage the business data and applications in the container, you cannot manage the user's personal data and apps. To help end users distinguish business apps from their personal apps, the business apps are marked with a briefcase icon.

Prerequisites
Before you can perform this exercise, you must meet the following requirements.

- Workspace ONE UEM version 9.4 or later

This exercise requires specific account information. Gather the required account information, and record it in the following table. The account information provided in the table is based on a test environment. Your account details will differ.

<table>
<thead>
<tr>
<th>Workspace ONE UEM Account Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Server URL</td>
<td>https://&lt;WorkspaceONEUEMHostname&gt;</td>
</tr>
<tr>
<td>User name</td>
<td>administrator</td>
</tr>
<tr>
<td>Password</td>
<td>VMware1!</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Google Admin Account Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td><a href="mailto:WorkspaceONEadmin@gmail.com">WorkspaceONEadmin@gmail.com</a></td>
</tr>
</tbody>
</table>

Understanding Android Device Modes
To address a variety of device-ownership use cases, Workspace ONE UEM supports multiple management modes for Android. The easiest way to determine which device mode is the most appropriate for your organization is to evaluate your device-ownership use case.
The following table pairs each device-ownership use case with its coordinating device mode. Review this table, and double-check that the tutorial you are reading will best address your use case.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Device Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>BYOD</td>
<td>Work Profile</td>
</tr>
<tr>
<td>Corporate-Owned</td>
<td>Work Managed</td>
</tr>
<tr>
<td>Hybrid</td>
<td>COPE</td>
</tr>
</tbody>
</table>

Each device mode offers a unique device-side user experience. After you have determined which device mode best addresses your use case, it is important to understand the user experience that mode offers. To help you understand their key similarities and differences, the following table outlines some of the primary device-side capabilities of each mode.

<table>
<thead>
<tr>
<th></th>
<th>Work Profile</th>
<th>Work Managed</th>
<th>COPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entire Device</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Badged Enterprise</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Apps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dedicated Personal</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Apps</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Logging In to the Workspace ONE UEM Console
To perform most of the steps in this exercise, you must first log in to the Workspace ONE UEM Console.

1. **Launch Chrome Browser**

   On your desktop, double-click the **Google Chrome** icon.

2. **Navigate to the VMware Workspace ONE UEM Console**

   For example, navigate to `https://WorkspaceONEUEMHostname` where `WorkspaceONEUEMHostname` is the host name of the Workspace ONE UEM console.

3. **Authenticate In to the Workspace ONE UEM Console**
1. Enter your Username, for example, administrator.
2. Click Next. After you click Next, the Password text box is displayed.
Enter your **Password**, for example, VMware1!

1. Click **Login**.

**Note**: If you see a Captcha, be aware that it is case sensitive.

### Registering for Android EMM
After logging into the Workspace ONE UEM console, you register your enterprise with Google. This creates an admin account that connects Google with Workspace ONE UEM.

**1. Navigate to Android EMM Registration Settings**
In the Workspace ONE UEM console, at the appropriate Organization Group level:

1. Click Groups & Settings.
2. Click All Settings.

2. Begin Google Registration

- Select Devices & Users.
- Expand Android.
- Select Android EMM Registration.
- Click Register with Google.

3. Provide a Google Admin Account
1. Confirm you are logged into your Google Admin Account that you want to associate with your Android for Work configuration. For example, enter WorkspaceONEadmin@gmail.com. **Note:** After 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 want to associate with your Organization.

2. Click **Get Started**.

**4. Provide Organization Details**
Enter your Organization Name.

1. Enter your Organization Name.
2. Select the Google Play Agreement.
3. Click Confirm.

5. Complete Registration

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

Click Complete Registration to return to the Workspace ONE UEM Android Enterprise configuration.

6. Confirm Integration in the Workspace ONE UEM Console
Return to the Android EMM Registration page in the Workspace ONE UEM Console:

1. On the Configuration tab, scroll down to the Google Admin Console Settings section. Note that the account information you provided to Google displays here.
2. Confirm the Android Enterprise Registration Status is shown as Successful.
3. Note how the Client ID and Google Service Account Email Address have been automatically created and configured.

Enrolling Bring-Your-Own Android Devices

Introduction
Device enrollment establishes communication with the Workspace ONE UEM console and allows devices to access internal resources. In this exercise, you enroll an Android device in Work Profile mode—which sets the device up with a special type of administrator. You begin enrollment with a device that already has a user account associated with it. Then, you enroll the device which installs the Work Profile and adds the Workspace ONE Intelligent Hub as the profile owner.

Prerequisites
Before you can perform the exercises in this tutorial, you must meet the following requirements.

- Android device running version 5.0 or later
- Ensure this device has an associated personal user account
- Retrieve the Group ID from Workspace ONE UEM Console

This exercise requires a user to enroll their device into Workspace ONE UEM. Note the user account information in the following table. The details provided in this table are based on a test environment. Your user account details will differ.
<table>
<thead>
<tr>
<th>User Account Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>testuser</td>
</tr>
<tr>
<td>Password</td>
<td>VMware1!</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Workspace ONE UEM Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace ONE Server URL</td>
<td>labs.awmdm.com</td>
</tr>
</tbody>
</table>

**Enrolling an Android Device into Work Profile Mode**

In this section, enroll your device in Workspace ONE UEM and set it up in Work Profile mode. You need to encrypt data on your device during this process. Depending on the amount of data on your device, this can take some time. Be patient until you see the next enrollment prompt.

**Note:** Screenshots may differ due to differences in device models and operating system versions.

**1. Download the Workspace ONE Intelligent Hub**

Navigate to [https://www.getwsone.com](https://www.getwsone.com) to download the latest version of Workspace ONE Intelligent Hub (formerly the AirWatch Agent).

**2. Launch the Workspace ONE Intelligent Hub**

![Hub](image)

Launch the *Hub* app on the device.

**3. Enter the Server URL**
1. Enter the Server URL for your Workspace ONE UEM environment.
2. Tap Next.

4. Enter the Group ID for Workspace ONE Intelligent Hub
Return to the Workspace ONE Intelligent Hub application on your Android device,

1. Enter your Group ID for your Organization Group for the Group ID text box. See Retrieving the Group ID from Workspace ONE UEM Console.
2. Tap the Next.

5. Enter User Credentials
You now provide user credentials to authenticate to Workspace ONE UEM.

1. Enter the Username. For example, testuser.
2. Enter the Password. For example, VMware1!.
3. Tap the Next button.

6. Accept Privacy Statement
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 use; information to function properly, and to secure.

Tap I Understand.

7. Accept Data Sharing Statement
8. Accept the Terms and Conditions
Tap **Agree**.

### 9. Set Up the Work Profile
Set up your 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:

Tap Set Up.

Note: This may take some time, be patient while the setup process completes.

10. Encrypt Device
Tap Encrypt.

After encryption has completed, enter your device PIN at the prompt to continue with enrollment.

11. Agree to Privacy Policy
Tap **OK** to confirm the Privacy Policy.

During the enrollment process, you will see several processing screens. You do not need to interact with the device further until you see the Hub app confirming your enrollment.

**12. Wait for Device Connectivity (IF NEEDED)**
If you see a Connectivity Issue notification, the device may be taking several minutes to establish a connection to Google Cloud Messaging. Wait until you see the Connectivity Issue notification change to Connectivity Normal before continuing.

**Note:** If you do not see any Connectivity Issue notifications, continue to the next step.

**13. Confirm Device Enrollment**
You have now completed the Hub configuration wizard. After the enrollment process completes, the Agent displays the notification Congratulations! You have successfully enrolled your device.

You can now Exit the agent.

Navigating Android Work Profile

After you have enrolled your Android device in Work Profile mode, 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. Depending on your device version, you might see a Work container with your badged apps. This section reviews both scenarios.

1. Badged Apps
In the Applications view, your Work apps and Personal apps are shown in a unified launcher. For example, your device shows both a personal icon for Play Store and a separate icon for Work Play Store 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 Workspace ONE Intelligent Hub 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.

## 2. Work Container
On some devices, you may also notice the Work container on your device depending on the OS version. This Work container can be used for quick access to your Work (Badged) Apps.

Configuring Profiles for Bring-Your-Own Android Devices

Introduction
Profiles are the mechanism by which Workspace ONE UEM manages settings on a device. In this exercise, you set up and configure a restrictions profile in Workspace ONE UEM to explore how enterprise profile settings apply on an Android device in Work Profile mode.

Prerequisites
Before you can complete this exercise, you must successfully enroll an Android device in Work Profile mode.

Understanding Configuration Options for Android Profiles
Profiles are the mechanism by which Workspace ONE UEM manages settings on a device. All profiles are broken down into two basic sections; the General section and the Payload section.

- The General section defines the profile's name and assignment settings.
- The Payload sections define actions to be taken on the device.

Every profile must have all required fields in the General section properly filled out and at least one payload configured.

To address multiple device ownership use cases, you can enable Android profile payload settings in Workspace ONE UEM at the Work Profile level and at the Work Managed device level.

- Work Profile-level configurations only apply restrictions and settings to the device's badged enterprise apps, and do not affect the users personal apps or settings.
- Work Managed device-level configurations apply restrictions and settings to the entire device.
- Corporate Owned Personally-Enabled devices use Work Profile-level and Work Managed device-level configurations.

Configuring Restriction Profiles
In this exercise, control camera settings by configuring a restrictions profile in the Workspace ONE UEM console.
1. Create a New Profile

In the Workspace ONE UEM Console:
1. Click Add.
2. Click Profile.

2. Select the Android Platform

Select a platform to start:

Select Android.
3. Configure the General Settings

1. Select General.
2. Enter a name for the Android Profile. For example, Android Restriction.
3. Click Assigned Groups to display the list of available assignments.
4. Select All Devices.

4. Open the Restrictions Payload
Select the Restrictions payload.
1. Click Configure.

5. Configure Screen Capture Restrictions

Device Functionality

<table>
<thead>
<tr>
<th>Allow Factory Reset</th>
<th>Allow Screen Capture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work Managed Device</td>
<td></td>
</tr>
<tr>
<td>Work Profile</td>
<td></td>
</tr>
</tbody>
</table>

Under Device Functionality:
1. In the Work Managed Device column, select the Allow Screen Capture check box.
2. In the Work Profile column, deselect the Allow Screen Capture check box.

6. Configure Camera Restrictions

<table>
<thead>
<tr>
<th>Allow Camera</th>
<th>Work Managed Device</th>
<th>Work Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allow Google Play</th>
<th>Work Managed Device</th>
<th>Work Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
1. Scroll down to the Application section.
2. In the Work Managed Device column, select the Allow Camera check box.
3. In the Work Profile column, deselect the Allow Camera check box.
4. Click Save & Publish.

7. Publish the Profile

Click Publish.

Testing Android Restriction Settings

For Android, the various device modes change the way profile settings apply to devices. After configuring a restriction profile, test the profile settings to see how they applied on the Android device.

1. Verify Camera Restrictions

After the restrictions profile pushes to the device:

1. Notice that a badged enterprise version of the camera application is not available.
2. Notice that the unbadged personal camera remains available.
2. Test Screenshot Restrictions in Personal Contacts

Open your **non-badged Contacts** app, and try to take a screenshot within the app. Notice that the screen shot was **successful**.

3. Test Screenshot Restriction in Enterprise Contacts

Open the **badged Contacts** app, and try to take a screenshot within the app. Notice that the screenshot was unsuccessful. In certain device models and OS versions, a message may also appear.

Managing Applications for Bring-Your-Own Android Devices

**Introduction**

Work Profile applications are displayed in the unified launcher together with personal applications and are differentiated by a badged icon. To the user, it looks like two applications are installed. For example, a badged Chrome icon and an unbadged Chrome icon. However, the app is installed only once and business data is stored separately from personal data.

The Work Profile contains some default system applications such as Work Chrome, Google Play, Google settings, Contacts, and Camera. You can hide these apps using a restrictions profile. It is important to note that the Work Profile does not control any personal apps.

In this exercise, you deploy VMware Workspace ONE Web, a public application, to your Android device. 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 the Workspace ONE UEM features to add functionality and security to these applications.
Prerequisites
Before you can complete this exercise, you must successfully enroll an Android device in Work Profile mode.

Deploying VMware Workspace ONE Web to an Android Device
The following steps walk through deploying VMware Workspace ONE Web, a public application, to an Android device.

1. Add Public Application

   In the Workspace ONE UEM Console:
   1. Select Add.
   2. Select Public Application.

2. Search for Workspace ONE Web

   Add Application
   
   Managed By: Android Enterprise
   Platform: Android
   Source: SEARCH APP STORE
   Name: Web
1. Select Android from the Platform drop-down menu.
2. Select Search App Store for the Source.
3. Enter Web in the Name text box.
4. Click Next.

3. Select the Web - Workspace ONE App

Click the Boxer app.

4. Approve Web - Workspace ONE

If prompted, click Approve.
5. Confirm Approval for Boxer - Workspace ONE

Click Approve again in the Application pop-up window.

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

6. Save Approval Settings
How would you like to handle new app permission requests?

- **Keep approved when app requests new permissions.**
  
  Users will be able to install the updated app.

- **Revoke app approval when this app requests new permissions.**
  
  App will be removed from the store until it is reapproved.

You may need to scroll down to view the Approval Settings button.

1. Select **Keep approved when app requests new permission.**
2. Click **Save**.

### 7. Publish the App

Click **Save & Assign**.

### 8. Add 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**.

### 9. Configure Assignment

1. Click in the Selected Assignment Groups search box. From the list of Assignment Groups that appear, select the appropriate group. For example, select **All Devices (your@email.shown.here)**.

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

3. Click **Add**.

### Policies

**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**

1. Click in the Selected Assignment Groups search box. From the list of Assignment Groups that appear, select the appropriate group. For example, select **All Devices (your@email.shown.here)**.
2. Select **Auto** for the App Delivery Method.
3. Click **Add**.

### 10. Save and Publish Web - Workspace ONE App
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).

<table>
<thead>
<tr>
<th>Name</th>
<th>Priority</th>
<th>App Delivery Method</th>
<th>Managed Access</th>
<th>VPN Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Devices</td>
<td>0</td>
<td>Auto</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Click **Save & Publish**.

**11. Preview Assigned Devices and Publish**
Click Publish.

Verifying Workspace ONE Web on an Android Device
After using the Workspace ONE UEM console to push Workspace ONE Web to your Android device, verify the Work app installed correctly on your device.

**Note:** Screenshots may differ depending on device model and OS.

1. **Confirm the Published Workspace ONE Web Application Downloaded**
Return to your testing Android device and confirm that the Workspace ONE Web application has downloaded and displays as a Work app.

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

2. Open the Badged Android for Work Play Store App
Open your Work Play Store application on your Android device.

3. 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.

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

4. Open Play Store Menu
Tap the **Menu** button in the upper-left corner.

### 5. View Play Store Work Apps

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

### 6. Verify Workspace ONE Web Is Available As A Work App
1. Tap **Installed**.
2. Confirm that the **Workspace ONE Web** application is in your list of Work applications. You may need to scroll down to find the application.

The Workspace ONE Web 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.
Summary and Additional Resources

Conclusion
This operational tutorial provided steps to manage Android BYOD devices.

Procedures included:

- Enrolling BYOD Android devices using the Workspace ONE Intelligent Hub
- Configuring and testing a restrictions profile
- Deploying Workspace ONE Web to Android BYOD and verifying the application

Terminology Used in This Tutorial
The following terms are used in this tutorial:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>application store</td>
<td>A user interface (UI) framework that provides access to a self-service catalog, public examples of which include the Apple App Store, the Google Play Store, and the Microsoft Store.</td>
</tr>
<tr>
<td>auto-enrollment</td>
<td>Auto-enrollment simplifies the enrollment process by automatically enrolling registered devices following the Out-of-Box-Experience.</td>
</tr>
<tr>
<td>catalog</td>
<td>A user interface (UI) that displays a personalized set of virtual desktops and applications to users and administrators. These resources are available to be launched upon selection.</td>
</tr>
<tr>
<td>cloud</td>
<td>Asset of securely accessed, network-based services and applications. A cloud can also host data storage. Clouds can be private or public, as well as hybrid, which is both private and public.</td>
</tr>
<tr>
<td>device enrollment</td>
<td>The process of installing the mobile device management agent on an authorized device. This allows access to VMware products with application stores, such as VMware Identity Manager.</td>
</tr>
<tr>
<td>identity provider (IdP)</td>
<td>A mechanism used in a single-sign-on (SSO) framework to automatically give a user access to a resource based on their authentication to a different resource.</td>
</tr>
<tr>
<td>mobile device management (MDM) agent</td>
<td>Software installed on an authorized device to monitor, manage, and secure end-user access to enterprise resources.</td>
</tr>
<tr>
<td>one-touch login</td>
<td>A mechanism that provides single sign-on (SSO) from an authorized device to enterprise resources.</td>
</tr>
<tr>
<td>service provider (SP)</td>
<td>A host that offers resources, tools, and applications to users and devices.</td>
</tr>
<tr>
<td>virtual desktop</td>
<td>The user interface of a virtual machine that is made available to an end user.</td>
</tr>
<tr>
<td>virtual machine</td>
<td>A software-based computer, running an operating system or application environment, that is located in the data center and backed by the resources of a physical computer.</td>
</tr>
</tbody>
</table>

For more information, see the VMware Glossary.

Additional Resources
For more information about Workspace ONE, you can explore the following resources:
VMware Workspace ONE Action Path
VMware Workspace ONE product page
VMware Workspace ONE Documentation
VMware Identity Manager product page
VMware Identity Manager Documentation
VMware Workspace ONE UEM, powered by VMware AirWatch product page
VMware AirWatch Documentation
VMware Workspace ONE free trial
VMware Workspace ONE Cloud-Based Reference Architecture
VMware Workspace ONE and VMware Horizon 7 Enterprise Edition On-premises Reference Architecture
VMware End-User-Computing Blogs
Workspace ONE UEM Hands-On Lab

About the Author
This tutorial was written by:
Karim Chelouati, Senior Technical Marketing Manager, End-User-Computing Technical Marketing, VMware

Feedback
The purpose of this tutorial is to assist you. Your feedback is valuable. To comment on this tutorial, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.