Application Management for Android

VMware Workspace ONE UEM 2001

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

1 Application Management for Android 4

- Application Types and Suported OS Versions for Android 5
- Workspace ONE Intelligent Hub for Android 5
- Deploying Internal Application on Android Devices 7
- Deploy Application on your Android Devices through Managed Google Play Store 8
  - Deploy Public Applications through Managed Google Play Store 8
  - Deploy Private Applications through Managed Google Play Store 9
  - Deploy Web Applications through Managed Google Play Store 10
  - Organizing your Applications in the Managed Play Store 11
- Assign Applications on your Android Devices to Smart Groups 11
- Enable Google Play for Work in the Workspace ONE UEM console 13
- Configure Samsung Native Email in the Workspace ONE UEM console 14
- OEMConfig on Android Enterprise Devices 14
  - Configure OEM settings in the Workspace ONE UEM console 15

Application Management for Android

1

Use the Workspace ONE UEM powered by AirWatch to push Android public applications, internal applications, and web apps to Android devices.

After approval, assign the application to devices using smart groups, a Workspace ONE UEM system that allows you to group devices on criteria you set. The final step is to assign the Terms of Use.

Applications that you push through the integration of Workspace ONE UEM and Android have the same functionality as their counterparts from the Google Play Store.

However, you can use Workspace ONE UEM features to apply policies to the applications. For example, you can add configurations that make using the application more convenient and you can configure settings that make using the application more secure.

- 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 with the application. Examples of supported values may include user names, passwords, and VPN settings. Support value depends upon the application.
- To add secure features, use Workspace ONE UEM profiles for Android. Profiles let you set passcodes, apply restrictions, and use certificates for authentication.

The Workspace ONE UEM console allows you to push alpha, beta, or production versions of apps. Using alpha and beta versions of apps allows for testing for compatibility and stability before pushing the production version. You can select specific smart groups for testing and use flexible deployment to determine which users receive which version of the app. If you don't select whether to push the alpha or beta version, the production version is automatically assigned.

For more information on application assignment, see Assign Applications on your Android Devices to Smart Groups .

Important VMware productivity apps (Browser, Boxer, Content Locker, etc) are not supported with Android (Legacy) Knox container deployments, such as Dual Persona or Container Only Mode, due to technical limitations with Knox container data separation. The Workspace ONE Intelligent Hub manages the container from the outside, and is not able to communicate with apps on the inside. Since the apps require a direct link to the Workspace ONE Intelligent Hub in order to communicate with the Workspace ONE UEM console, the apps cannot be configured inside the container. In order to use productivity apps with Knox, the device must be enrolled using Android Enterprise on a device running Knox 3.x or higher.

Web Links for Android Devices

Web links applications function much like an application on a device. They provide end users a way to access a URL directly from an icon on the menu of their device. The end user sees the web links application icon and title, selects the application, and connects directly to a specified URL.

Web links applications are useful for navigation to extended URLs with many characters. You can place web links application icons on the springboard. These icons connect end users to internal content repositories or login screens, so end users do not open a browser and type out a long URL.

You can add web links as an application in the Apps & Books section of the Workspace ONE UEM console. For more information on adding web links for Android, see Add Web Links Applications .

This chapter includes the following topics:

- Application Types and Suported OS Versions for Android
- Workspace ONE Intelligent Hub for Android
- Deploying Internal Application on Android Devices
- Deploy Application on your Android Devices through Managed Google Play Store
- Assign Applications on your Android Devices to Smart Groups
- Enable Google Play for Work in the Workspace ONE UEM console
- Configure Samsung Native Email in the Workspace ONE UEM console
- OEMConfig on Android Enterprise Devices

Application Types and Suported OS Versions for Android

Workspace ONE UEMclassifies applications as native (internal, public, purchased), SaaS, and Web. You upload applications depending on the type. Workspace ONE UEM supports the following OS Versions for Android applications based on the application type.

Table 1-1. Application Types and Supported OS Versions for Android

Application Type	Supported Platforms
Internal	Android v4.0+
Public (Free and Paid)	Android v4.0+
Web Links	Android v4.0+
SaaS	Android v4.0+

Workspace ONE Intelligent Hub for Android

The Workspace ONE Intelligent Hub for Android is an application that enables the Native Android SDK API layer of management to which Workspace ONE UEM connects. Workspace ONE UEM engages Native Android SDK APIs on Android devices for management and tracking capabilities. **Native Android**

SDK APIs are available to any third-party application, including the Workspace ONE Intelligent Hub and any other application using the AirWatch Software Development Kit (SDK).

With the AirWatch SDK, applications can take advantage of key MDM features that are available such as:

- Compromised Device Detection
- GPS Tracking
- Additional Telecom Detail
- Additional Network Details such as IP address
- Additional Battery and Memory statistics
- Native number badging

After enrolling, use the Workspace ONE Intelligent Hub to access and manage device information and settings. Access device information from the following tabs on the left of the device display:

- **This Device** – Displays the name of the enrolled end user, the device-Friendly Name, current enrollment status, connectivity method, and compliance status.
- **Device Status** – Displays the current enrollment status including:
  - The server to which the device is connected.
  - The organization group to which the device is enrolled.
  - The current network status including the active Wi-Fi SSID to which the device is connected.
- **Compliance** – Displays a list of compliance policies currently active for the device.
- **Profiles** – Displays a list of profiles currently installed on the device. From the profiles list, you can refresh and reapply profiles from your device that might be out of sync or uninstalled.
- **Managed Apps** – Displays a list of apps managed by Workspace ONE UEM installed on the device and their install status.
- **About** – Displays the version number of the Workspace ONE Intelligent Hub installed on the device and provides a hyperlink to the associated Privacy Policy agreed to upon device enrollment.

Perform basic device management functions from the Workspace ONE Intelligent Hub menu at the top of the display:

- **Sync Device** – Sync latest device information and receive updates from IT admin.
- **App Catalog** – Launch the application catalog within the Workspace ONE Intelligent Hub or the native web browser, if applicable.

Additional functionality is accessible from the application menu in the upper-right corner of the display:

- **Edit Phone Number** – Modify the assigned phone number, if applicable.
- **Send Debug Log** – Transmit a debug log for the device to Workspace ONE UEM.
- **Remove Device** – Unenroll the device from Workspace ONE UEM.

Android devices running Android 6.0 (Marshmallow) and above use the power saving options for idle apps and devices. If a user unplugs a device and leaves it stationary, with its screen off, for a period, the device goes into **Doze** mode, where it attempts to keep the device in a sleep state. There will be no network activity during this time. Doze mode affects how the Workspace ONE Intelligent Hub reports information back to Workspace ONE UEM.

When a device is on battery power, and the screen has been off for a certain time, the device enters Doze mode and applies a subset of restrictions that shut off app network access and defer jobs and syncs. After a device is in doze mode for a period, the system sends the remaining Doze restrictions to wake locks, alarms, GPS, and Wi-Fi settings.

Additionally, **App Standby** mode allows the device to determine that an app is idle when the user is not actively using it. When devices are in either state, the Workspace ONE UEM console will not receive reports on device details. When the user plugs a device in to charge or opens an app, the device will resume normal operations and reporting from AirWatch apps installed on the device to the Workspace ONE UEM console resumes.

The Hub and SDK-Built Applications

AirWatch offers an SDK to integrate into applications you build for the Android platform. Integrating the SDK into your applications enables the application to use AirWatch features. These features include controlling authentication to SDK-built applications and sharing a single-sign on session between applications that use the SDK.

However, you must enable **Key Encryption with User Input** so that the Workspace ONE Intelligent Hub can care share an application passcode or an SSO session with other SDK applications.

For information on the AirWatch SDK for Android, see AirWatch SDK for Android documentation.

For information on SDK features in the Workspace ONE UEM console , see MAM Features With SDK Functions documentation.

For information on the option **Key Encryption with User Input**, see Devices & Users / Android / Security in the Workspace ONE UEM System Settings documentation.

Deploying Internal Application on Android Devices

Internal apps are company-specific apps developed by your organization that you might not necessarily want to be searchable in the public app store, but you want your users to have access to this application from their device.

There are two options for deploying internal apps:

- Add it Google Play as a private application. These applications are added as public applications in the Workspace ONE UEM console after publishing in Google Play.
- Host the application .apk file as a local file. For Android 6.0+ devices only.

For information on uploading internal apps for the Work managed devices (Android 6.0+), see Add and Deploy Internal Applications as a Local File available in the Mobile Application Management(MAM) documentation. Follow all directions in this section to get these apps approved, uploaded, and assigned to your users.

If you are deploying internal apps on Android Work profile devices, add internal apps to Google Play for Work so that they are available to the Android specific users. Upload your application by logging into the Google Play Developer Console with your enterprise credentials. There is an option to enable, Restrict Distribution, which only allows users of your domain to view this application on Google Play for Work (the badged play store). Once you have added your internal application to the developer console, these apps are treated as public applications.

Deploy Application on your Android Devices through Managed Google Play Store

The managed Google Play Store is the recommended way to manage all your application deployment use-cases for Android devices. Managed Google Play loads in an iframe within the Workspace ONE UEM console whenever a public application is added and when an Android Enterprise EMM Registration is configured. The iframe is opened through the API integration with Google Play and is not hosted by VMware.

Deploy Public Applications through Managed Google Play Store

Search the Google Play Store directly from the Workspace ONE UEM console to add applications to the Managed Google Play Store for your users.

Procedure

1 Navigate to **Apps & Books > Public > Add Application**.

2 Select **Android** from the **Platform** drop-down menu.

3 Select one of the following options to add an application:

Setting	Description
Search App Store	Select to search for the application in the app store. Google Play launches within the Workspace ONE UEM console through an iFrame.
Enter URL	Enter the URL of the app.
Import From Play	Select to import previously approved applications.

4 Select **Next** or enter the **Name** of the applications you want to add to the integration. Google Play will open directly from the Workspace ONE UEM console.

5 Find desired apps by using the **Search** field or browsing through the apps section.

6 Review the permissions the application requires on the device, and select **Approve**.

7 Future updates to the application may require further permissions on the device. If you choose to approve the updates automatically and allow them to be pushed to devices, consider selecting **Keep approved when app requests new permissions**.

   If an application is updated, ensure it does not need to get reapproved in the Google Play Store.

8 Configure options on the **Details** tab.

Setting	Description
Name	View the name of the application.
View in App Store	View the store record for the application where you can download it and get information about it.
Categories	Use categories to identify the use of the application. You can configure custom application categories or keep the application's pre-coded category.
Supported Models	Select all the device models that you want to run this application.
Is App Restricted to Silent Install Android	Assign this application to those Android devices that support the Android silent uninstallation feature. Workspace ONE UEM cannot silently install or uninstall public applications. However, you can control what applications you push to your Android standard devices or your Android enterprise devices. Android enterprise devices support silent activity.
Managed By	View the organization group (OG) that the application belongs to in your Workspace ONE UEM OG hierarchy.

9 (Optional) Assign a **Required Terms of Use** for the application on the **Terms of Use** tab.

   Terms of use state specifically how to use the application. They make expectations clear to end users. When the application pushes to devices, users view the terms of use page that they must accept to use the application. If users do not accept the terms of use, they cannot access the application.

10 Select the **SDK** tab and assign the default or custom **SDK Profile** and an **Application Profile** to the application. SDK profiles apply advanced application management features to applications.

11 Select **Save & Assign** to configure flexible deployment options for the application.

What to do next

Check to make sure the application has been imported after approval. The console will direct you to the next step to designate assignment groups.

For more information on assigning apps, see Assign Applications on your Android Devices to Smart Groups

Deploy Private Applications through Managed Google Play Store

You can publish applications developed by your organization or the applicatons that are developed for your organization can be hosted and distributed through the Managed Play Store. While adding a public app on an organization group with Android Enterprise enabled, the iframe is loaded and the private apps

are available in the left menu. Additional information such as a description, images, and more can be added in the Advanced options after uploading. Private apps uploaded through the iframe can never be made public apps.

Procedure

1. Navigate to **Apps & Books > Public > Add Application**.
2. Select **Android** from the **Platform** drop-down menu.
3. Select **Search App Store** to search for the application in the app store. Leave the **Name** blank and select **Next**. Google Play opens directly from the Workspace ONE UEM console.
4. Access the **Private Apps** from the left menu.
5. Enter the **Title** and upload the **APK** file.

Note

- Uploading through the iframe publishes the application in as little as 10 minutes and waives the one-time fee that is charged to create a Google Developer account.
- Private applications can never be uploaded more than once as the Google Play ensures that each of the application has a unique package name.
- Deleted Private applications cannot be reuploaded with the same package name. Delete the private applications only if you never want to use the same package name again. The package name is a unique name to identify a specific app.

Deploy Web Applications through Managed Google Play Store

Web applications are shortcuts on android devices that the users can open to navigate to the pre-defined URLs. Web applications can be managed on the android devices similarly to public applications. To do so, administrators need to set the title, URL, display mode, and the icon. The managed Google Play store loads in an iframe that creates a Web App object that is treated by the Workspace ONE UEM, Google Play, and the Android OS as if it were a Public application.

Procedure

1. Navigate to **Apps & Books > Public > Add Application**.
2. Select **Android** from the **Platform** drop-down menu.
3. Select **Search App Store** to search for the application in the app store. Leave the **Name** blank and select **Next**. Google Play opens directly from the Workspace ONE UEM console.
4. Access the **Web Apps** from the left menu.
5. Create a **Web App**.
   a. Enter the **Title** and the **URL**.
   b. Select the **Display Mode**.
   c. Upload the **Icon**.

d Select **Create**.

e After you **Save** the Web App, select the **Back** arrow at the top-left of the screen.

6 Select the **Web App**.

7 Choose the **Select** option at the bottom of the screen.

8 Select **Save & Assign** to configure flexible deployment options for the Web App.

Note Publishing the web application creates the application. However, publishing to users does not happen until you assign the application within the Workspace ONE UEM console.

Organizing your Applications in the Managed Play Store

Workspace ONE UEM administrators can simplify access to recommended apps by adding applications into collections which are displayed as rows on the managed Play Store. After enabling this feature, there is a minimum requirement of one collection at all times. Apps which have not been assigned to a collection can only be found in the managed Play Store using the search functionality.

Prerequisites

Once an environment has begun using collections, the managed Google Play cannot be reverted to an earlier state. Because the change to collections cannot be rolled back, customers are highly encouraged to test the feature in a sandbox environment to ensure it aligns with the desired end-user experience and functionality before rolling it out to any production environments.

Procedure

1 Navigate to **Apps & Books > Public > Add Application**.

2 Select **Android** from the **Platform** drop-down menu.

3 Select **Search App Store** to search for the application in the app store. Leave the **Name** blank and select **Next**. Google Play opens directly from the Workspace ONE UEM console.

4 Access the **Organize Apps** from the left menu.

5 Create collections and add apps to your collection to set the Play Store layout.

Assign Applications on your Android Devices to Smart Groups

After you approve the application from the Google Play Store, you will be redirected to the Workspace ONE UEM console to assign the applications to smart groups on the assignment tab.

Procedure

1 From the **Assignments** tab select Add Assignment and configure the following details:

Setting	Description
Assigned Smart Groups	Select an existing smart group or create a one. **Note** When a device belongs to multiple assignment groups that have a different application configuration Key-Value pairs(KVP) with the same priority, the KVP from the smart group which is added first is sent to the devices. Currently, if the first smart group in the above scenario is removed from the assignment, the configuration from the second smart group is not applied automatically unless the application is repushed or until you click the **send app configuration** button.
Restrict To Devices That Support Silent Activity **Android**	Assign this application to those Android devices that support the Android silent uninstallation feature. AirWatch cannot silently install or uninstall public applications but this option lets you control what applications you push to your Android standard devices or your Android enterprise devices. Android enterprise devices support a silent activity.
View Device Assignment	View the list of devices available by assigned smart groups.,
App Delivery Method	Set the application to install automatically (auto) or manually (on demand) when needed. ■ **On Demand** – Deploys content to a catalog or other deployment agent and lets the device user decide if and when to install the content. This option is the best choice for content that is not critical to the organization. Allowing users to download the content when they want helps conserve bandwidth and limits unnecessary traffic. ■ **Automatic** – Deploys content to a catalog or other deployment Hub on a device upon enrollment. After the device enrolls, the system prompts users to install the content on their devices. This option is the best choice for content that is critical to your organization and its mobile users.
Managed Access	Enable the adaptive management to set AirWatch to manage the device so that the device can access the application.
App Tunneling	Configure a VPN at the application level, and select the Per-App VPN Profile. Users access the application using a VPN, which helps ensure that application access and use is trusted and secure.
Android Legacy	Select the VPN configuration profile to use for this application. This field displays when App Tunneling is enabled.
Android	Select the VPN configuration profile to use for this application. This field displays when App Tunneling is enabled.
Pre-release Version	Select to push the Alpha or Beta version of app. Select None to automatically push the production version of the app.
Application Configuration	Configure specific application options and send the configurations to devices with the application, automatically. Users do not have to configure these specified values on their devices manually.

Setting	Description
Application uses AirWatch SDK	Identify whether the application uses AirWatch SDK functionality and whether it needs a profile to apply the features. This feature is optional and advanced. For more information on the default settings for profiles, see MAM Functionality with Settings and Policies and the AirWatch SDK in the Mobile Application Management (MAM) documentation. ■ Select the profile from the **SDK Profile** drop-down menu. This profile applies the features configured in **Settings & Policies** (Default) or the features configured in individual profiles configured in **Profiles**. ■ Select the certificate profile from the **Application Profile** drop-down menu so that the application and AirWatch communicate securely.
Add Exception	Deploy applications to those special use cases that can develop within an organization. ■ Apply **User Groups** and **Device Ownership** types to your exceptions in the **Criteria** area. ■ Select an **Override Value** to create specific exceptions to the options. **Override Value** options vary depending on the platform.

2 Assign a **Required Terms of Use** for the application on the **Terms of Use** tab. Requiring a Terms of Use is optional. Terms of use state specifically how to use the application. They make expectations clear to end users. When the application pushes to devices, users view the terms of use page that they must accept to use the application. If users do not accept the terms of use, they cannot access the application.

   a **On-demand**: The terms of use display when the device user selects the install option in the app catalog.

   b **Auto**: The terms of use display when the device user opens the app catalog.

3 Select **Save & Publish** to make the application available to end users.

Enable Google Play for Work in the Workspace ONE UEM console

You need to enable Google Play for Work to display Android applications in the Work Play Store on assigned devices if you configured Android prior to AirWatch v9.2. If you are deploying the Workspace ONE UEM console 9.3+, this option will not appear.

Procedure

1 Navigate to **Groups & Settings > All Settings > Devices & Users > Android > Android EMM Registration**.

2 Select **Enable Play Store**. Once enabled, this option will disappear from the Settings page.

Configure Samsung Native Email in the Workspace ONE UEM console

Samsung Native Email enables users to manage multiple personal and business email accounts seamlessly. Samsung Native Exchange email is configurable within Android Fully managed, Work Profile, and Fully managed device with a work profile (previously COPE), enrollment modes using Application Configurations. You can configure Samsug Native email with or without certificate based authentication.

Complete the following steps to configure Samsung Native Email settings on the UEM console.

Prerequisites

- If you are using Certificate based authentication, be sure to create a Credentials profile prior to setting up app configuration. For more information, see Deploy Credentials.
- The certificate(s) must be created and installed on the device, either via a Credentials Profile or manual install of certificates, before the app configuration is delivered.
- You must know the alias of the certificate(s) or use a lookup variable for the alias.

Note To prevent the email configuration from failing:

- In the Certificate Request Template, use a Lookup Value to determine the certificate Subject Name. This will be used for the alias.
- In the App Configuration for Samsung Email, select the same Lookup Value as entered above for the necessary certificate settings.

Procedure

1. Navigate to **Apps & Books > Public > Add Application** .
2. Select Android from the Platform drop-down menu.
3. Select Search App Store from the Source field.

   The Google Play Store opens directly from the Workspace ONE UEM console.
4. Select the Samsung Email app and then click Approve.
5. Select Save & Assign to continue, then select Add Assignment.
6. Scroll down to Application Configuration and select Enabled to view and configure Exchange or Email settings.
7. Use lookup values to configure dynamic options, such as username, email address, or even certificate aliases.

OEMConfig on Android Enterprise Devices

OEMConfig is a standard solution for Android original equipment manufacturers (OEMs) to provide additional management capabilities to administrators, on top of what is natively offered by the Android Enterprise. OEMConfig is an application that is built and maintained by the OEM and hosted on Google

Play. The application takes advantage of AppConfig standards by allowing the administrator to dynamically configure any setting desired that the OEM offers in a data-driven user interface. Because the settings are data-driven and app-based, console upgrades are not required to access the latest settings offered by the OEM.

Use OEMConfig applications to add, create, and customize OEM-specific settings for Android Enterprise devices. The application is published to devices through UEM and silently installed using Android Enterprise Managed Google Play. Customized settings are delivered to the application during or post-install, and the application calls the corresponding, proprietary APIs on the device. Different OEMs might include different settings, and these settings might vary depending on the management mode (Work Managed, Work Profile, or COPE). The available settings depend on what the OEM includes in their OEMConfig app. Contact your OEM vendor for more information on their support of OEMConfig.

Configure OEM settings in the Workspace ONE UEM console

OEMConfig is typically used to configure settings that are not built in to Workspace ONE UEM. Different original equipment manufacturers (OEM) include different settings. The available settings depend on what the OEM includes in their OEMConfig application.

Complete the following steps to configure the OEM settings for an OEMconfig application in the Workspace ONE UEM console.

Prerequisites

Before you start configuring OEMConfig on your devices, consider the following caveats:

- OEM settings is a data-driven user interface that uses text boxes and support lookup values for the user or device-specific configurations.
- If any of the OEM settings is left blank, or is not selected, Workspace ONE UEM does not send the key-value pair to the device, and it is excluded from the configuration.
- **Clear** button clears all the values from the current configuration, including the default values.
- Use the **Clear** button to set a subset of configurations.
- Use the **Clear** button on each of the configuration page to clear the configuration settings.
- An OEMConfig app is built by the OEM, and uploaded to Google Play. If it is not on Google Play, contact the OEM for more information.

Procedure

1. Get the OEMConfig app from the Managed Google Play Store.
   a. Navigate to **Apps & Books > Public > Add Application**.
   b. Select **Android** from the **Platform** drop-down menu.

2 In the pop up, fill out the following text boxes with the supplied information:

Setting	Description
Managed by	Select the Organization Group that you set up to manage applications. Only IT Admins that belong to that Group can edit OEMconfig application configurations.
Platform	Android
Source	Search App Store
Name	OEMConfig App. For example, enter **`Knox Service Plugin`** if you are trying to configure OEM settings for the Knox Service Plugin.

3 Click **Approve** to add the OEMConfig application as an approved application.

4 Edit the **App Configurations** to enable or disable policies. From the **Assignments** tab, select Add Assignment.

   a In the detailed view page, click **Assign**.

   b Select your OEM Config App and click **Edit**.

   c **Edit** the **Application Configuration** to configure the OEM settings for the OEMconfig application.

5 In the app configuration screen, configure the OEM settings and modify the policies for your deployment.

6 On the Update Assignment pop-up window, click **Save and Publish**.

7 On the Preview Assigned Devices pop-up window, click **Publish**.