VMware AirWatch Android Platform Guide

Managing and Deploying Android Devices with Workspace ONE UEM

Workspace ONE UEM v9.4

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Table of Contents

Chapter 1:
Overview

Introduction to Workspace ONE UEM Integration with Android

Workspace ONE UEM provides you with a robust set of mobility management solutions for enrolling, securing, configuring, and managing your Android device deployment. Through the Workspace ONE UEM console, you have several tools and features at your disposal for managing the entire life cycle of corporate and employee owned devices.

The guide explains how to integrate Workspace ONE UEM as your Enterprise Mobility Manager (EMM) with Android devices for work profile and work managed device.

Android Name Change

Android for Work was introduced in 2015 to boost enterprise adoption for Android devices. Google has worked to implement features in Android for Work available for most Android devices. Starting with Workspace ONE UEM console release v9.4, Workspace ONE UEM has adopted the simplified naming convention. Android for Work has been renamed to Android and is the default deployment method for new enrollments. This guide covers this deployment method. If you are an existing VMware AirWatch customer, you can continue with your Android deployment using Android (Legacy) for managing your device fleet. For documentation on Android (Legacy) management, see VMware AirWatch Android (Legacy) Platform Guide.

Requirements for Deploying Android

Before deploying Android devices, you should consider the following pre-requisites, requirements for enrollment, supporting materials, and helpful suggestions from the AirWatch team.

Supported Operating Systems

Android 5.X.X (Lollipop)

Android 6.X.X (Marshmallow)

Android 7.X.X (Nougat)

Android 8.X.X (Oreo)

Your Android device must be able to communicate with the Google Play Store. If your devices do not support Google Play Integration, refer to Android (Legacy) deployment.

Enrollment Requirements

Each Android device in your organization's deployment must be enrolled before it can communicate with AirWatch and access internal content and features. The following information is required prior to enrolling your devices.

If an email domain is associated with your environment – If Using Auto Discovery

- **Email address** – This is your email address associated with your organization. For example, **JohnDoe@acme.com**.
- **Credentials** – This **username** and **password** allow you to access your AirWatch environment. These credentials may be the same as your network directory services or may be uniquely defined in the Workspace ONE UEM console .

If an email domain is not associated with your environment – If Not Using Auto Discovery

If a domain is not associated with your environment, you are still prompted to enter your email address. Since auto discovery is not enabled, you are then prompted for the following information:

- **Enrollment URL** – This URL is unique to your organization's enrollment environment and takes you directly to the enrollment screen. For example, **mdm.acme.com/enroll**.
- **Group ID** – The Group ID associates your device with your corporate role and is defined in the Workspace ONE UEM console .
- **Credentials** – This unique username and password pairing allows you to access your AirWatch environment. These credentials may be the same as your network directory services or may be uniquely defined in the Workspace ONE UEM console .

To download the Agent and subsequently enroll an Android device, you'll need the following information:

- **Enrollment URL** – The enrollment URL is AWAgent.com for all users, organizations and devices enrolling into AirWatch.

Key Terms for Android

These key terms associated with Android will help you in understanding how to configure and deploy settings to your users.

- **Work Profile**– Work Profile mode, also known as Profile Owner, creates a dedicated container on your device for only business applications and content. Work Profile mode allows organizations to manage the business data and applications but not have access to the user's personal data and apps. The Android apps are denoted with a briefcase icon so they are distinguishable from the personal apps.
- **Work Managed Device**– Work Managed Device mode, also referred to as Device Owner, is scoped to the whole device. There is no personal side to the device and APIs pushed from the AirWatch Agent apply to the entire device. Work Managed Device mode applies to a device which starts in an unprovisioned state and, through a separate provisioning process, installs the AirWatch Agent and grants the Agent full control of the entire device.
- **Managed Google Account** – Refers to the Google account registered to the device used for Android and provides Android app management through Google Play. This account is managed by the domain that manages your Android configuration.
- **Google Service Account** – The Google Service Account is a special Google account that is used by applications to access Google APIs recommended for G Suite customers.
- **EMM Token** – Unique ID that Workspace ONE UEM uses to connect the Workspace ONE UEM console to the Managed Google Account.
- **Managed Google Domain** – Domain claimed for enabling Android associated with your enterprise.
- **Google Domain Setup** – Google process for claiming a managed Google domain.
- **G Suite** – A brand from Google from which you can push cloud computing, productivity and collaboration tools, software and products developed by Google.
- **AirWatch Relay** – The Workspace ONE UEM application admins use to bulk enroll Android Devices into Workspace ONE UEM.
- **NFC Bump** – This is done while using the AirWatch Relay app to pass information from the parent device to the child device.

Understanding Android Device Modes

Android's built-in management features enable IT admins to fully manage devices used exclusively for work.

Android offers two modes depending on the ownership of the device being used within your organization. The **Work Profile**(also called the Profile Owner) creates a dedicated space on the device for only work applications and data. This is the ideal deployment for Bring Your Own Device (BYOD) programs. For devices that are being deployed to end users as corporate owned, **Work Managed Device** mode allows Workspace ONE UEM and IT admin to control the entire device and enforce an extended range of policy controls unavailable to work profiles, but restricts the device to only corporate use.

Work Profile Mode Functionality

Apps in the Work Profile are differentiated by a red briefcase icon, called badged apps, and are shown in a unified launcher with the user's personal apps. For example, your device shows both a personal icon for Google Chrome and a separate icon for Work Chrome denoted by the badge. From an end-user perspective, it looks like two different applications, but the app is only installed once with business data stored separately from personal data.

The AirWatch Agent is badged and exists only within the Work Profile data space. There is no control over personal apps and the Agent does not have access to personal information.

There are a handful of system apps that are included with the Work Profile by default such as Work Chrome, Google Play, Google settings, Contacts, and Camera – which can be hidden using a restrictions profile

Certain settings show the separation between personal and work configurations. Users see separate configurations for the following settings:

- **Credentials** – View corporate certificates for user authentication to managed devices.
- **Accounts** – View the Managed Google Account tied to the Work Profile.
- **Applications** – Lists all applications installed on the device.
- **Security** – Shows device encryption status.

Work Managed Device Mode Functionality

When devices are enrolled in Work Managed Device mode, a true corporate ownership mode is created. Workspace ONE UEM controls the entire device and there is no separation of work and personal data.

Important things to note for the Work Managed mode are:

- The homescreen does not show badged apps like Work Profile mode.
- Users have access to various pre-loaded apps upon activation of the device. Additional applications can only be approved and added through the Workspace ONE UEM console.
- The AirWatch Agent is set as the device administrator in the security settings and cannot be disabled.
- Unenrolling the device from with from Work Managed mode prompts device factory reset.

Chapter 2:
Android Setup

Android EMM Registration Overview

To start managing Android devices, you'll need to register Workspace ONE UEM as your Enterprise Mobility Management (EMM) provider with Google. The Getting Started page in the Workspace ONE UEM console provides a step by step solution to help configure the enterprise management tools needed to secure and manage your device fleet.

There are two ways to configure Android: by using a Managed Google Play account (preferred) or using a managed Google domain (recommended by Google for G Suite customers). A Managed Google Play account is used when your business does not use G Suite and allows for multiple configurations of Android within your organization using a personal Google account. Workspace ONE UEM manages this account and requires no Active Directory sync or Google verification.

Setting up Android using managed Google domain (G Suite) requires your enterprise to set up a Google domain and must follow a verification process to prove that you own the domain. This domain can only be linked to one verified EMM account. The setup includes creating a Google Service Account and configuring Workspace ONE UEM as your EMM provider. Consider creating a Google account specifically for Android for your organization to use so as not to conflict with any existing Google accounts.

The Google Service Account is a special Google account that is used by applications to access Google APIs and is required when setting up Android using the managed Google domain method for your business. The Google Service Account credentials are automatically populated when configuring Android Accounts when registering using managed Google play account. If you encounter an error while setting Android Accounts, clear your settings in the Workspace ONE UEM console and try again or create the account manually. For Google Accounts, consider creating your Google Service Account before either setup method.

To change the Google account or make changes to your admin settings, you have to unbind the account from the Workspace ONE UEM console.

Important: The setup of Android includes the integration of third-party tools that is not managed by VMware AirWatch. The information in this guide for the Google Admin Console and Google Developer Console has been documented with the available version as of January 2018. Integration with a third-party product is not guaranteed and is dependent upon the proper functioning of the third-party solutions.

Android EMM Registration with Managed Google Play Account

The Workspace ONE UEM console allows you to complete a simplified setup process to bind the UEM console to Google as your EMM provider.

To start Android setup in the UEM console, complete the following:

1. Navigate to **Getting Started > Workspace ONE > Android EMM Registration**.
2. Select **Configure** and you are redirected to the Android EMM Registration page.

   Note: If for some reason, the Android EMM Registration page is blocked, make sure you've enabled the Google URLs in your network architecture to communicate with internal and external endpoints. For more information, see the Recommended Architecture Guide.

3. Select **Register with Google**. If you are already signed in with your Google credentials, you are redirected back to the Workspace ONE console.

4. Select **Sign In**,if you are not already, and enter your Google credentials and then select **Get Started**.
5. Enter your **Organization Name**. The Enterprise Mobility Manager (EMM) provider field populates automatically as AirWatch.
6. Select **Confirm > Complete Registration**. You are redirected to the Workspace ONE Console, and your Google Service Account credentials are automatically populated.
7. Select **Save > Test Connection** to ensure the service account is set up and connected successfully.

Note: If your settings in the UEM console have been cleared, when you navigate to register with Google, you will see a message that prompts you to complete setup. You are redirected back to the Workspace ONE console, to finish setup.

Android EMM Registration with Managed Google Domain (G-Suite Customers)

Setting up your account with managed Google domain requires the organization to set up a Google domain if they do not already use one.

You are to complete several manual tasks, such as verifying domain ownership with Google, obtaining an EMM token, and creating an enterprise service account to use this type of setup.

To start Android setup in the Workspace ONE UEM console using managed Google domain method, complete the following:

1. Navigate to **Getting Started > Workspace ONE > Android EMM Registration**.
2. Select **Register** to be redirected to the Android Setup Wizard to complete three steps:
   - **Generate Token**: Obtain your enterprise token by registering your enterprise domain with Google.
   - **Upload Token**: Enter the EMM Token into the Android setup wizard.
   - **Setup Users**: Configure how users will be created for your entire enterprise.
3. Select **Go To Google**. You are redirected to the G Suite site.
4. Register your enterprise and verify your domain.

Setup Google Service Account

The Google Service Account is a special Google account that is used by applications to access Google APIs. You should create this account after you generate your EMM token so you can upload all information at one time. The account is only required if you are using the Google Accounts method for deploying Android.

1. Navigate to the Google Cloud Platform- Google Developers Console.
2. Sign in with your Google credentials.

Note: The Google Admin credentials do not have to be associated with your business domain. Consider creating a Google account specifically for Android for your organization to use so as not to conflict with any existing Google accounts.

3. Use the drop-down menu from the Select a project menu and select **Create a project**.
4. Enter a **Project Name** to create your API project in the New project window. Consider using *Android EMM-CompanyName* as the naming convention.
5. Agree to the terms and conditions and select **Create**.

   Your project generates and the Google Developer Console redirects you to the API Manager page.
6. Select **Enable APIS and Services** for Android from the **APIs & Services Dashboard**.
7. Search and enable the following APIs: **Google EMM API** and **Admin SDK API**.

   After creating your project and enabling APIs, create your service account in the Google Developer's Console.

Create Service Account

Remain in the Google Developer's Console to create the service account.

1. Navigate to **APIs & Services > Credentials > Create Credentials >Service Account Key > New Service Account**.
2. Define the **Service Account name** for your service account. Consider following the Android naming convention and be sure to note the name you choose as you will need it in further steps.
3. Use the drop-down menu to select the **Role > Project** as **Owner**.
4. Select the **Key Type** as **P12**.
5. Select **Create**. The identity certificate gets automatically created and downloaded to your local drive.

   Caution: You must save your identity certificate and password for when you upload the certificate into the Workspace ONE UEM console .
6. Select **Manage service accounts** from the **Service Account Keys** list which opens the Service Accounts page.
7. Select the menu button (three vertical dots) beside your service account and select **Edit**.
8. Select **Enable G Suite Domain-wide Delegation**.
9. Enter a **Product name** in order change settings for G Suite Domain. Consider using *AndroidEMM-CompanyName* as the naming convention.
10. Select **Save**.
11. Select **View Client ID** under the **Options** field. The details of your service account displays. From here, you will leave the Developer Console and input your credentials into the Google Admin Console.

    Be sure to save your client ID before navigating away from the Developer's Console. You will also use these credentials in the Workspace ONE UEM console when you upload your EMM token. For more information, see

Upload EMM Token on page 13

For steps to configure the Google Admin Console, see Setup Google Admin Console on page 12

Setup Google Admin Console

The Google Admin Console is where administrators manage Google services for users in an organization. AirWatch uses the Google Admin Console for integration with Android and Chrome OS.

The Manage API client access page allows you to control custom internal application and third-party application access to supported Google APIs (scopes).

To set up your Google Admin Console:

1. Login to the Google Admin Console and navigate to **Security > Settings > Advanced Settings > Manage API Client Access**.
2. Fill in the following details:

Setting	Description
Client Name	Enter the Client ID obtained from AirWatch. Paste the ID from your service account.
One or More API Scopes	Copy and paste the following Google API scopes for Android: **Android:** https://www.googleapis.com/auth/admin.directory.user

3. Select **Authorize**.

Generate EMM Token

Your unique EMM token binds your domain for Android management to AirWatch. You are directed to the G Suite setup site after selecting **Go to Google** from the previous task to begin.

1. Complete the following fields:
   - **About You** – Enter your admin contact information.
   - **About Your Business** – Fill out your company information.
   - **Your Google Admin Account** – Create a Google admin account.
   - **Finishing Up** – Enter the security verification data.
2. Select **Accept & create your account** after reading and agreeing to terms set by Google.
3. Follow the remaining prompts to **Verify domain ownership** and **Connect with your provider**. Once verified, this becomes your managed Google domain.

   To verify domain ownership, the following options are available: **add a meta tag to your homepage**, **add a domain host record**, or **upload HTML file to your domain site**. Configure settings for the available options.
4. Select **Verify** to proceed. If this process is successful, the **Connect with your provider** section displays your EMM token. This token is valid for 30 days.

> **Note:** If you encounter problems during this step, please refer to Google Support using support number and unique PIN listed.

5. Copy the generated EMM token and select **Finish**.

AirWatch recommends that you create your Google Service Account before you return to the Workspace ONE UEM console to upload the EMM token, so that you can upload all credentials at one time.

Upload EMM Token

After you have finished all tasks in the Google Admin Console and the Google Developer Console, you are redirected to the Workspace ONE UEM console to finish binding your G Suite domain with AirWatch for Android EMM.

1. Navigate to **Getting Started > Workspace ONE > Android EMM Registration**. If you have closed the window or are not automatically redirected back to AirWatch.
2. Select **Upload Token** from the Android Setup wizard.
3. Complete the following fields:

Setting	Description
Domain	Domain claimed for enabling Android associated with your enterprise. **Important:** If your domain has already been registered with another EMM provider, you will not be allowed to upload a new EMM token.
Enterprise Token	Unique identifier that links AirWatch to your G Suite configuration.
Google Admin Email Address	Admin email created in the Google Admin Console. The email address displays from the View Client ID from where you created your service account. For more information, see Setup Google Admin Console on page 12

4. Enter the **Directory Access Credentials**, if needed. You only need to configure this if you plan to create users automatically. For manual creation, you do not have to enter these credentials.
5. Proceed to upload your **Google Developer Console Settings** retrieved from your Google Service Account.

Setup Users

All users in your enterprise using Android will need Google accounts created to connect with their devices. The format will be username@<your_enterprise_domain>.com. This screen allows you to determine which setup method you prefer for creating users. Admins have two options for creating users under Android:

- Create users manually by logging into the Google Admin Console or using the Google Active Directory Sync Tool (GADS).
- Allow AirWatch to automatically create Google accounts during enrollment.

To configure these settings:

1. Select **Yes** or **No** on the **Create accounts during enrollment based on enrolled users' email** prompt.

   If yes, the next prompt will ask if you desire to use SAML to authenticate the accounts.

   If no, the Workspace ONE UEM console directs you to the alternative method of creating Google accounts by the Google Active Directory Sync Tool or the Google Admin Console.

2. Select **Finish**.

Creating Android Enrollment Users Automatically

AirWatch suggests that you create users for Android automatically during enrollment. The Android setup wizard allows you to specify if you want to automatically create user accounts during enrollment, and if so, to use SAML to authenticate the accounts. If you have not set up SAML previously, the wizard will display a link that directs you to configure your settings.

If you wish to use create users automatically:

1. Select **Yes** to **Create accounts during enrollment based on users' emails**.

   If you select yes, you will need configure the Directory Access Credential settings in the setup wizard. Upload a Directory Access Certificate and enter a Service Account Email Address and Admin Email Address to configure these settings.

2. Select **Yes** to **Use SAML endpoint to authenticate accounts**.

   If you have not setup SAML, the wizard will prompt you to configure SAML authentication settings.

3. Select **Finish** to complete Android setup.

Creating Android Enrollment Users Manually

You can manually create user accounts for your entire enterprise outside of the Workspace ONE UEM console by either using either the Google Cloud Directory Sync (GCDS) tool or the Google Admin Console. To access the Google Admin Console , you can click the link provided in the setup wizard. You will need to contact Google for further instructions on how to use the console.

The GCDS method requires you to use similar settings as the AirWatch Directory Services. Access the Directory Services settings by navigating to **Groups & Settings** ▸ **All Settings** ▸ **System** ▸ **Enterprise Integration** ▸ **Directory Services**.

You can access the GCDS tool by clicking the link posted in the setup wizard or by downloading the tool directly to your computer from the Google Support page.

The GADS tool allows you to manually create Google accounts for every employee in your enterprise in one bulk creation. The accounts are created by synchronized with the information from your AirWatch Directory Services.

Note: The information discussed here is up to date as of latest version of GCDS v4.4.0 for March 2017.

To create users using this method, complete the following:

1. Select the link from the setup wizard or download the GADS tool directly from Google.
2. Open the tool from your desktop and select **User Accounts** and **Groups** to synchronize.
3. Select the **Google Apps Configuration** tab and enter the following:
   a. Enter **Primary Domain Name**.

b. Select to **Replace domain names in LDAP email address (of users and groups) with this domain name**. This will ensure that all user email addresses match the domain name.

4. Select the **Authorize Now** button.
5. Follow the steps to continue the authorization process when the **Authorize Google Apps Directory Sync** dialog displays.
   a. Sign-in to your Android admin account.
   b. Enter the verification received in email.
   c. Select **Validate** to confirm these settings.
6. Select the **LDAP Configuration** tab to enter the connection settings to sync the AirWatch Directory Services with Google.

   From here, you can enter the same settings saved in the AirWatch Directory Services to sync with this tool. To access these settings, navigate to **Groups & Settings ▸ All Settings ▸ System ▸ Enterprise Integration ▸ Directory Services**.
7. Select **Test Connection.** If the sync is successful, this will auto create the linked Active Directory accounts and corporate Google accounts in Google.

   You will be directed back to the setup wizard to finish setup.

Unbind Domain from AirWatch

You can unbind the Android admin account in the Workspace ONE UEM console in the event you need to make a change or change Google accounts.

1. Navigate to **Devices > Device Settings > Devices & Users > Android > Android EMM Registration**.
2. Select **Clear Settings** from the Android EMM Registration page.

Chapter 3:
Android Enrollment

Android Enrollment

Each Android device in your organization's deployment must be enrolled before it can communicate with the Workspace ONE UEM console and access internal content and features.

The AirWatch Agent provides a single resource to enroll a device and provides device and connection details. Agent-based enrollment allows you to:

- Authenticate users using basic or directory services, such as AD/LDAP/Domino, SAML, tokens, or proxies.
- Register devices in bulk or allow users to self-register.
- Define approved OS versions, models, and maximum number of devices per user.

Android has two enrollment options: Work Managed Device enrollment and Work Profile enrollment with additional enrollment options for each mode.

Work Managed Device Enrollment

Work Managed Device mode, also called Device Owner, gives Workspace ONE UEM control of the entire device. This mode is ideal for corporate owned device configurations that require a parent staging process. For more information, see Work Managed Device Enrollment on page 20.

Work Profile Enrollment

Work Profile enrollment, also known as Profile Owner, is facilitated with the AirWatch Agent which secures a connection between the Android device and the Workspace ONE UEM console. For more information, see Enrolling Android Device into Work Profile Mode on page 34.

Enrollment Settings

The Android EMM Registration page lets you configure the various options for integrating with Android. This page uses a wizard to help you set up the integration for devices. Enable these settings before beginning enrollment.

Device Protection

Android OS 5.1 and above have a feature called Device Protection which requires Google credentials to be entered before and after a device can be reset. When a device is ready to be enrolled as a Work Managed device for Android, the device must be factory reset. This feature impacts Android enrollment. For more information, see Device Protection for Android Devices on page 18.

Autodiscovery Enrollment

Workspace ONE UEM makes the enrollment process simple, using an autodiscovery system to enroll devices to environments and

organization groups (OG) using user email addresses. For more information, see Autodiscovery Enrollment on page 19

Devices & Users / Android / Android EMM Registration

The Android settings page lets you configure the various options for integrating with Android prior to enrolling Android devices. Android configuration uses a wizard to help you set up the integration for devices.

Configuration

The **Configuration** page shows Google Admin Console Settings and Google API settings after successful Android EMM registration.

Enrollment Settings

Setting	Description
Work Managed Enrollment Type	Choose if devices should be associated with the enrollment user or device. When using paid apps, User Based is preferred for optimal license allocation and most BYOD use cases. For scenarios where a single user will not be associated with the device (such as Kiosks), Device Based is preferred.

Enrollment Restrictions

Setting	Description
Define devices that will use Android (Legacy) in this organization group	Select whether to **Don't use Android (Legacy)**, **Always use Android (Legacy)**, or **Exempt smart groups from Android (Legacy)**.
Assignment Groups	Select a smart group from the drop-down menu. When a smart group(s) is selected, devices or users that do not belong to that group(s) will go through Android legacy enrollment (device administrator). Devices that belong to smart group will enroll in Work Profile or Work Managed assuming they support these enrollment modes

Device Protection for Android Devices

Android OS 5.1 and above have a feature called Device Protection which requires Google credentials to be entered before and after a device can be reset. When a device is ready to be enrolled as a Work Managed device for Android, the device must be factory reset.

Any existing Google account has to be removed from the device and the secure lock screen disabled to avoid triggering Device Protection so that the AirWatch Agent can be installed during enrollment. Using the device from the factory reset state also prevents the new user from being locked out of the device.

In the event the previous owner changed the Google account password, you must wait three days before factory resetting any of your Android 5.1+ devices for enrollment unless you have explicitly disabled Android Device Protection on them. If you factory reset one of your Android devices before those three days are up and then attempt to sign into that device with your Google account, you will be met with an error message and not allowed to log into the device with any account until 72 hours after the password reset occurred.

Autodiscovery Enrollment

Workspace ONE UEM makes the enrollment process simple, using an autodiscovery system to enroll devices to environments and organization groups (OG) using user email addresses. Autodiscovery can also be used to allow end users to authenticate into the Self-Service Portal (SSP) using their email address.

Note: To enable an autodiscovery for on-premises environments, ensure that your environment can communicate with the Workspace ONE UEM Autodiscovery servers.

Registration for Autodiscovery Enrollment

The server checks for an email domain uniqueness, only allowing a domain to be registered at one organization group in one environment. Because of this server check, register your domain at your highest-level organization group.

Autodiscovery is configured automatically for new Software as a Service (SaaS) customers.

Autodiscovery Enrollment

Workspace ONE UEM makes the enrollment process simple, using an autodiscovery system to enroll devices to environments and organization groups (OG) using user email addresses. Autodiscovery can also be used to allow end users to authenticate into the Self-Service Portal (SSP) using their email address.

Note: To enable an autodiscovery for on-premises environments, ensure that your environment can communicate with the Workspace ONE UEM Autodiscovery servers.

Registration for Autodiscovery Enrollment

The server checks for an email domain uniqueness, only allowing a domain to be registered at one organization group in one environment. Because of this server check, register your domain at your highest-level organization group.

Autodiscovery is configured automatically for new Software as a Service (SaaS) customers.

Configure Autodiscovery Enrollment From a Child Organization Group

You can configure Autodiscovery Enrollment from a child organization group below the enrollment organization group. To enable an autodiscovery enrollment in this way, you must require users to select a Group ID during enrollment.

1. Navigate to **Devices > Device Settings > General > Enrollment** and select the **Grouping** tab.
2. Select **Prompt User to Select Group ID**.
3. Select **Save**.

Configure Autodiscovery Enrollment From a Parent Organization Group

Autodiscovery Enrollment simplifies the enrollment process enrolling devices to intended environments and organization groups (OG) using end-user email addresses.

Configure an autodiscovery enrollment from a parent OG by taking the following steps.

1. Navigate to **Groups & Settings > All Settings > Admin > Cloud Services** and enable the **Auto Discovery** setting. Enter your login email address in **Auto Discovery AirWatch ID** and select **Set Identity**.

a. If necessary, navigate to https://my.air-watch.com/set-discovery-password to set your myAirWatch password for Auto Discovery service. Once you have registered and selected **Set Identity**, the **HMAC Token** autopopulates. Click **Test Connection** to ensure that the connection is functional.

2. Enable the **Auto Discovery Certificate Pinning** option to upload your own certificate and pin it to the auto discovery function.

   You can review the validity dates and other information for existing certificates, where you also have the option to **Replace** and **Clear** these existing certificates.

   Select **Add a certificate** and the settings **Name** and **Certificate** display. Enter the name of the certificate you want to upload, select the **Upload** button, and choose the cert located on your device.

3. Select **Save** to complete an autodiscovery setup.

Instruct end users who enroll themselves to select the email address option for authentication, instead of entering an environment URL and Group ID. When users enroll devices with an email address, they enroll into the same group listed in the **Enrollment Organization Group** of the associated user account.

Work Managed Device Enrollment

Android Work Managed Device mode gives Workspace ONE UEM control of the entire device. Using a factory reset device helps ensure that devices are not set up for personal use.

There are several ways to enroll Work Managed devices:

- Using AirWatch Relay to perform an NFC bump
- Using an unique identifier or token code
- Scanning a QR code
- Using Zero Touch enrollment

Your business requirements determine which enrollment methods you want to use. You cannot enroll devices until you have completed Android EMM Registration. See Android EMM Registration Overview to complete registration.

If the Android devices you are using are on a closed network, unable to communicate with Google Play, or are running Android 5.0 or lower, then enroll Android using the Legacy enrollment method in the VMware AirWatch Android (Legacy) Platform Guide.

Enrollment Settings

The Android EMM Registration page lets you configure the various options for integrating with Android. This page uses a wizard to help you set up the integration for devices. Enable these settings before beginning enrollment.

AirWatch Relay

AirWatch Relay is an application that passes information from parent devices to all child devices being enrolled into Workspace ONE UEM with Android. 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 Workspace ONE UEM.

AirWatch Relay allows you to bulk enroll all child devices 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 to be enrolled as Work Managed Device for Android.

The NFC bump process depends on the Android OS. Devices running Android 6.0+ perform one bump to connect and enroll child devices in one step. Devices running Android OS versions between v5.0 and v6.0 perform two NFC bumps. The first bump is to connect the parent device to Wi-Fi network and region settings including the device date, time, and location and download the AirWatch Agent. The second NFC bump is to enroll all child devices before deploying them to end users.

For AirWatch Relay enrollment, see Enroll Work Managed Device with AirWatch Relay on page 22.

AirWatch Identifier

The AirWatch Identifier enrollment method is a simplified approach to enrolling Work Managed devices for Android 6.0+ devices. 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, user name, and password. For AirWatch Identifier enrollment, see Enroll Work Managed Devices Using AirWatch Identifier on page 31.

With the identifier, you can also enroll on behalf of the end user by doing Single-User Device Staging. This method is 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 for Android 7.0+ devices.

QR code provisioning is an easy way to enroll a fleet of devices that do not support NFC and the NFC bump. 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. 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 includes the Server URL and Group ID information. You can also include the user name and password or the user has to enter their credentials.

Here is the format of the text to paste into the generator:

```
{
"android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.airwatch.androidagent/com.airwatch.agent.DeviceAdministratorReceiver",

"android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
"6kyqxDOjgS30jvQuzh4uvHPk-0bmAD-1QU7vtW7i_o8=\n",

"android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://awagent.com/mobileenrollment/airwatchagent.apk",
"android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,
"android.app.extra.PROVISIONING_WIFI_SSID": "Your_SSID",
"android.app.extra.PROVISIONING_WIFI_PASSWORD": "Password",
"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
```

```
"serverurl": "Server URL",
        "gid": "Group ID",
        "un":"Username",
        "pw":"Password"
}
}
```

For QR Code enrollment, see Enroll Work Managed Device Mode Using a QR Code on page 31.

Zero Touch Enrollment

Zero Touch enrollment allows for Android 8.0+ devices to be configured with Workspace ONE UEM as the enterprise mobility management provider out the box.

When the device is connected to the Internet during the device setup, the AirWatch Agent is automatically downloaded and enrollment details are automatically passed to enroll the device with no user interaction.

Prerequisites

Zero Touch enrollment is only supported by a limited number of mobile carriers and OEMs. Customers need to work with their carrier to ensure that zero touch provisioning is supported. Learn more about supported carriers and devices on the Google website.

For Zero Touch enrollment steps, see Enroll Work Managed Device Using Zero Touch on page 1.

Note: Zero Touch enrollment is only supported on Android 8.0 (Oreo) devices.

Enroll Work Managed Device with AirWatch Relay

Enrolling the Work Managed Device mode using AirWatch Relay varies depending on the Android OS version.

If you are using Android 6.0+, the AirWatch Relay app provides a single NFC bump option which configures Wi-Fi, provisioning, and enrollment settings. For provisioning Work Managed Devices with AirWatch Relay on Android 6.0+ devices, please see Provisioning Work Managed Device with AirWatch Relay for Android 6.0+ on page 22

Enrolling the Work Managed Device mode for devices running Android OS version between v5.0 and v6.0 is completed in two NFC bump. Bump one configures region, Wi-Fi, and any applicable advanced settings applied to all the devices in your fleet. Bump two configures the enrollment settings and automates the enrollment process. See Enrolling Work Managed Device with AirWatch Relay for Android v5.0 and Android v6.0 on page 25.

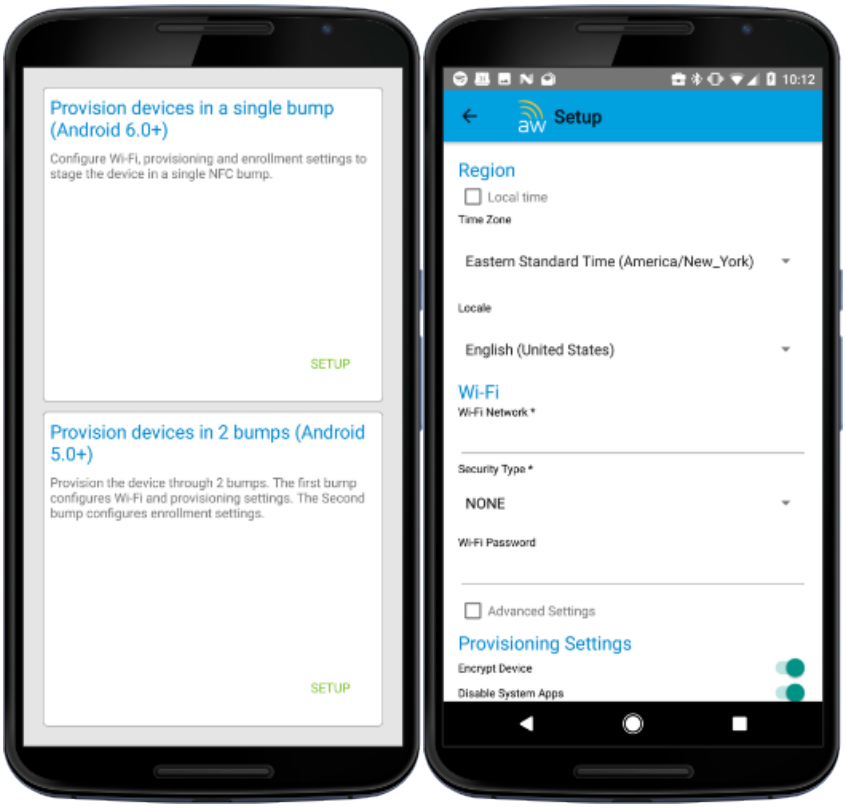
Provisioning Work Managed Device with AirWatch Relay for Android 6.0+

For Android 6.0+, the AirWatch Relay app provides a single bump option which configures region, Wi-Fi, provisioning settings, and enrollment settings in the single bump.

For provisioning Work Managed Devices with AirWatch Relay on Android 6.0+ devices:

1. Download the AirWatch Relay app from the Google Play Store to the parent device and launch the app once complete.
2. Review the 'For AirWatch Admins' screen and select **Next** to proceed to the wizard.

   This screen will allow you to view or skip to a setup wizard which provides a descriptions of the purpose of the app and a tutorial of the NFC bump.
3. Tap **Setup** on Provision devices in a single bump (Android 6.0+).



4. From the parent device, define the following settings:

Setting	Description
Region	
Local Time	Enable this field for the device to automatically configure with local time.
Time Zone	Select the time zone.
Locale	Select the location your device will be enabled.
Wi-Fi	
Wi-Fi Network	Specify the Wi-Fi network the device will connect to.
Security Type	Determine the encryption type for the connection.
Wi-Fi Password	Enter the Wi-Fi Password.
Provisioning (Advanced)	
Encrypt Device	Enable this field to indicate that device encryption can be skipped as part of Work Managed device provisioning.
Disable System Apps	Enable this field to skip the agent from disabling system apps during set up.
Enrollment Settings	
Server	Enter the server URL or hostname.

Setting	Description
Group ID	Enter an identifier for the organization group for the end users to use for device to log in.
Username	Enter the credentials for the user the child device will be enrolled.
Password	Enter the credentials for the user the child device will be enrolled.

5. Tap **Ready** from the parent device.
6. Perform the NFC bump by touching the parent and child device back to back. The child device should be in factory reset mode which will ensure the device is not being used for personal use.
7. Tap **Touch to Beam** on the parent device with the devices still back to back.
8. Tap **Encrypt** on the child device with the devices still back to back.

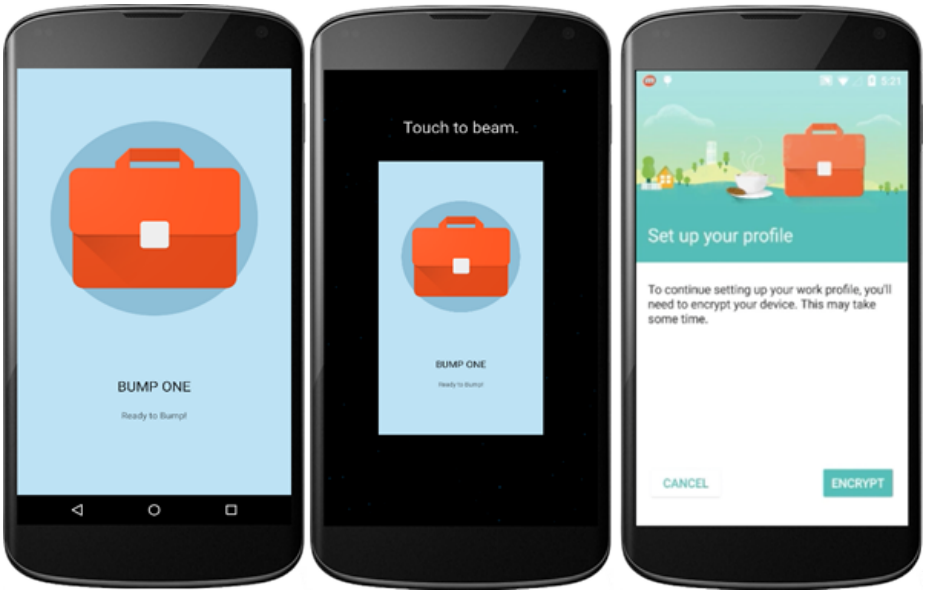
   The child device will automatically:

   a. Connect to the Wi-Fi network defined in the AirWatch Relay app.

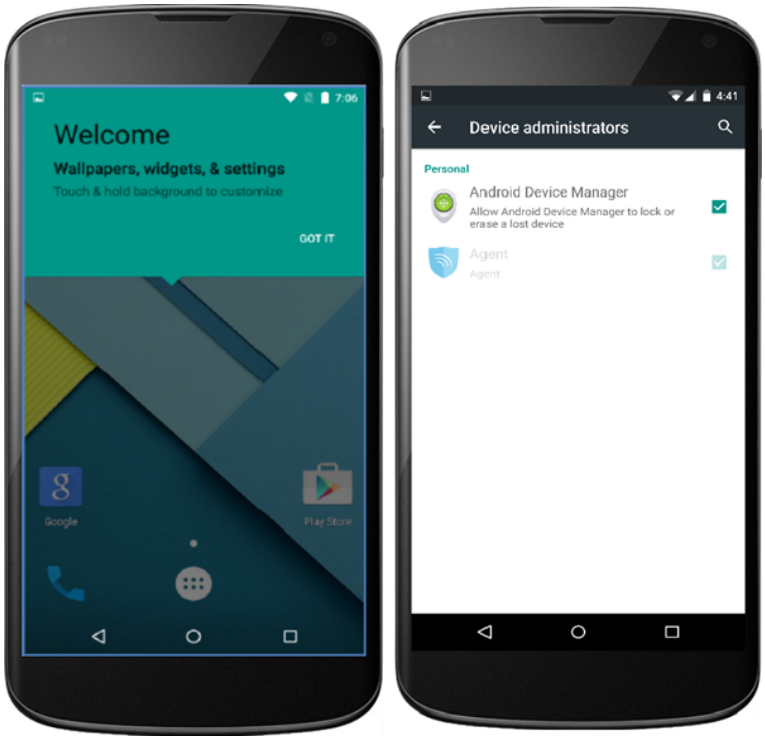
   b. Download and silently install the AirWatch Agent.

   c. Set the AirWatch Agent as device administrator.

   d. Reset the device.



After the child device has reset, the device is provisioned for Work Managed Mode. A welcome screen displays on your child device. To verify this from the child device, navigate to **Device Settings > Security > Device Administrators** to view AirWatch Agent listed as the device administrator. End users will not be able to deactivate this setting.



You will also notice on the device homescreen the pre-downloaded apps allowed. Any other applications will need to be approved by the administrator from the Workspace ONE UEM console .

If you have several devices to enroll in your device fleet, then repeat NFC bump one on each child device to provision them in Work Managed Device mode.

If enrollment was successful, the **My Device** page will display on the child device (shown above). All profiles and applications will start to automatically push to the device. You will repeat the enrollment steps for each device needing to be enrolled in your device fleet.

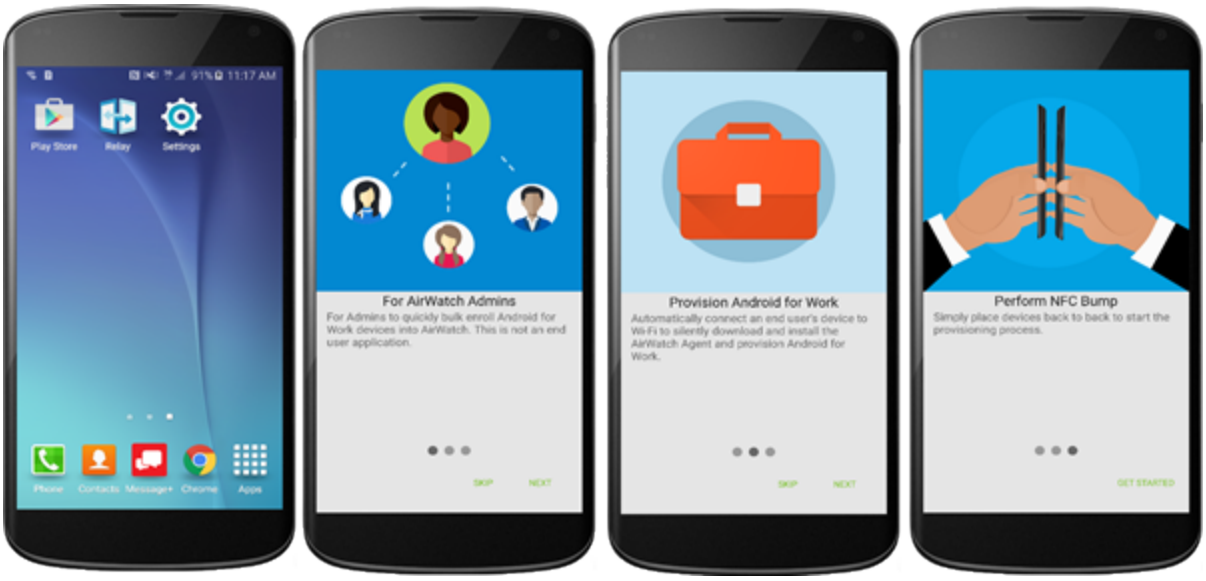
The Workspace ONE UEM console reports the status of Android on the users devices. You can check the **Details View** page to verify that Android was successfully created.

Navigate to **Devices > Details View > Summary** and view the **Security** section of the page to view the status. The should be a green check to verify Android activation.

Enrolling Work Managed Device with AirWatch Relay for Android v5.0 and Android v6.0

For instructions

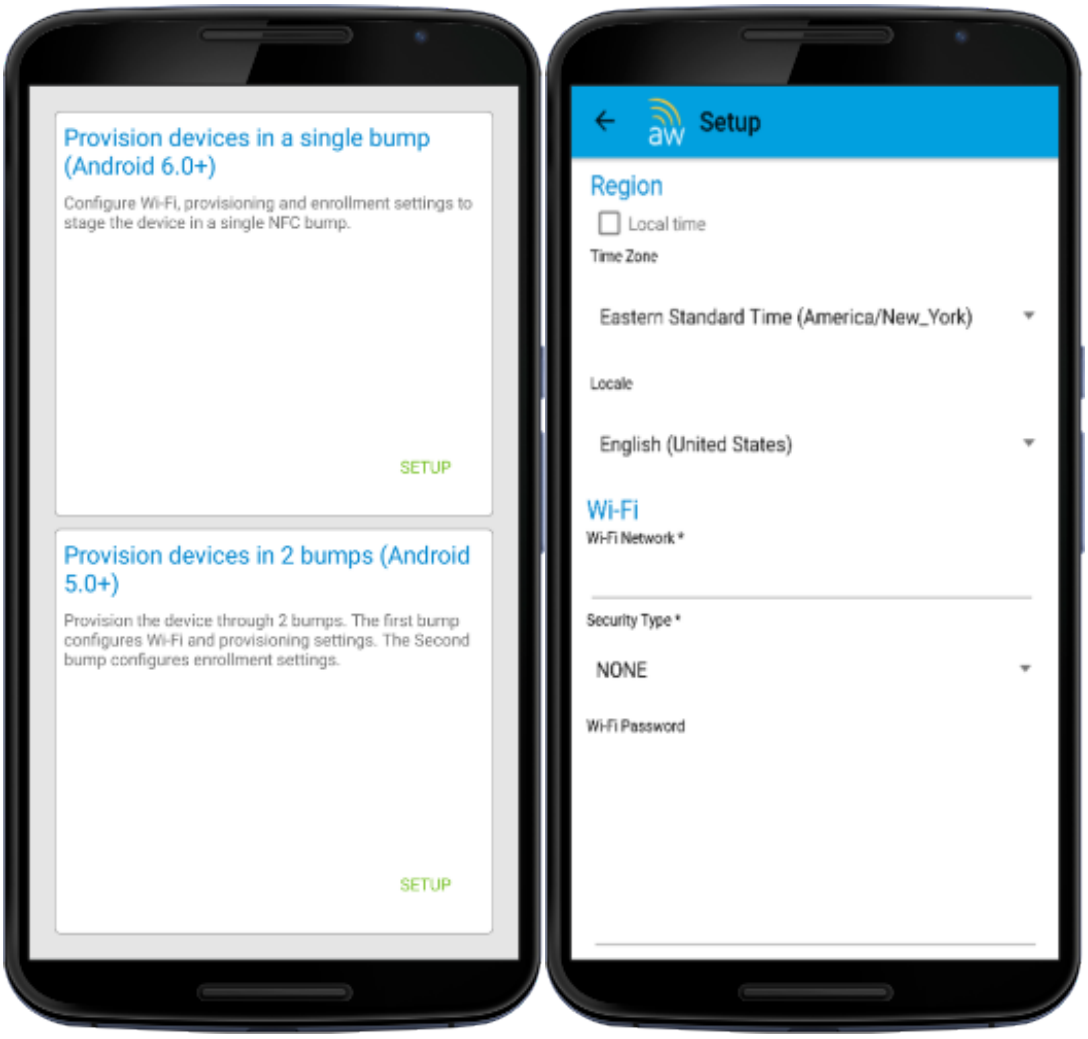
1. Download the AirWatch Relay app from the Google Play Store to the parent device and launch the app once complete.
2. Review the 'For AirWatch Admins' screen and select **Next** to proceed to the wizard.



This screen will allow you to view or skip to a setup wizard which provides a descriptions of the purpose of the app and a tutorial of the NFC bump.

3. Tap **Setup** on the desired option to **Provision devices in 2 bumps (Android v 5.0- Android v6.0+)**.

   If using Android 6.0+, select **Provisioning devices in a single bump(Android 6.0+).** For instructions for Android 6.0+ devices, please see Provisioning Work Managed Device with AirWatch Relay for Android 6.0+ on page 22.



4. From the parent device, define the following settings:

Setting	Description
Region	
Local Time	Enable this field for the device to automatically configure with local time.
Time Zone	Select the time zone.
Locale	Select the location your device will be enabled.
Wi-Fi	
Wi-Fi Network	Specify the Wi-Fi network the device will connect to.
Security Type	Determine the encryption type for the connection.
Wi-Fi Password	Enter the Wi-Fi Password.
Provisioning Settings	
Skip Device Encryption Requirement for Provisioning	Enable this field to indicate that device encryption can be skipped as part of Work Managed device provisioning.

Setting	Description
Do Not Disable System Apps During Provisioning	Enable this field to skip the agent from disabling system apps during set up.

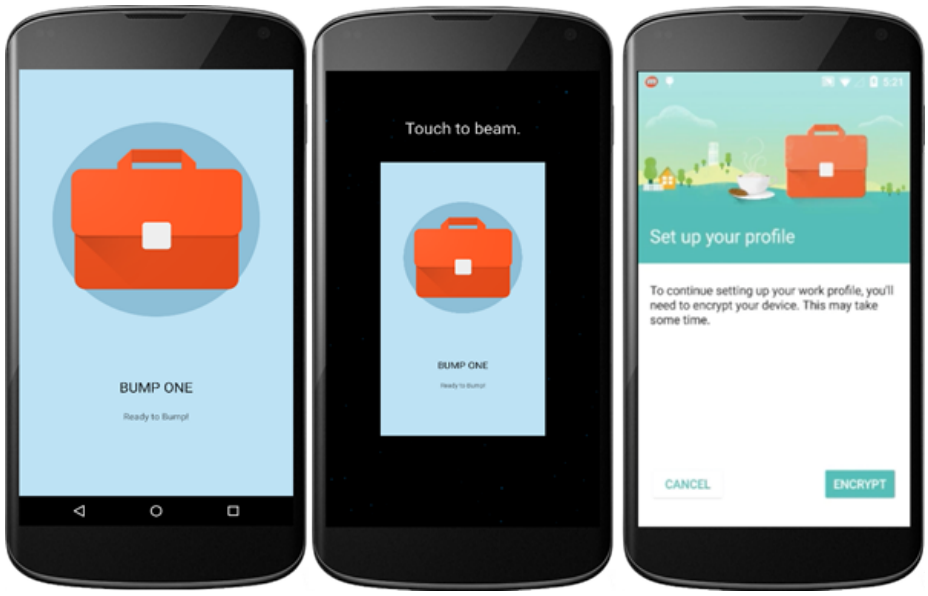
5. Tap **Ready** from the parent device to perform bump one.
6. Perform the first NFC bump by touching the parent and child device back to back. The child device should be in factory reset mode which will ensure the device is not being used for personal use.

> **Important**: Prior to performing a factory reset on child devices (if the device isn't new out of the box), disable the lock screen and remove any existing Google account configured on the device. Device Protection is a feature for Android 5.1 that requires uses to enter the Google account credentials prior to performing a factory reset. If you disable lock screen and remove existing Google account, you will not be prompted for credentials and enrollment will not be hindered.

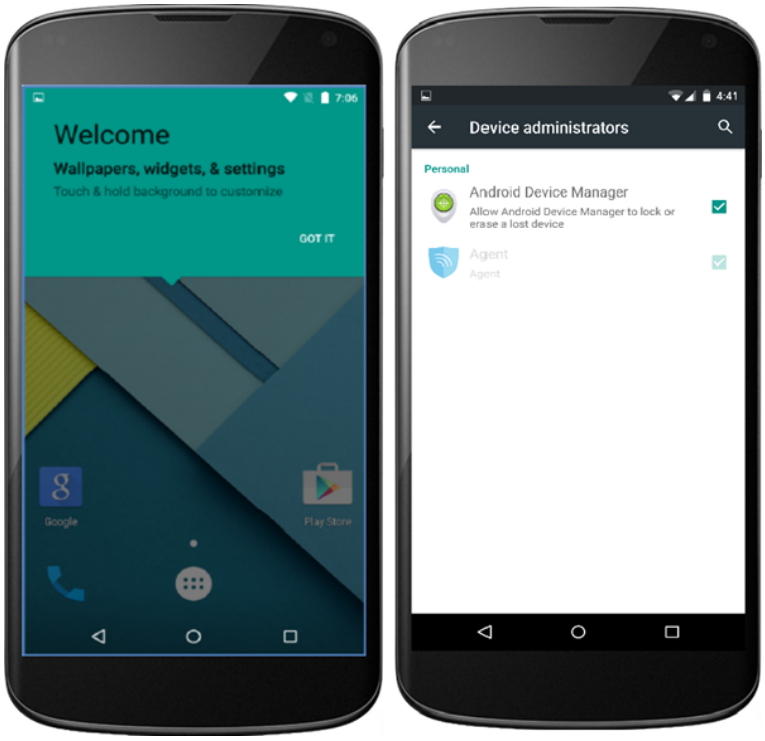
7. Tap **Touch to Beam** on the parent device with the devices still back to back.
8. Tap **Encrypt** on the child device with the devices still back to back.

   The child device will automatically:

   - Connect to the Wi-Fi network defined in the AirWatch Relay app.
   - Download and silently install the AirWatch Agent.
   - Set the AirWatch Agent as device administrator.
   - Reset the device.



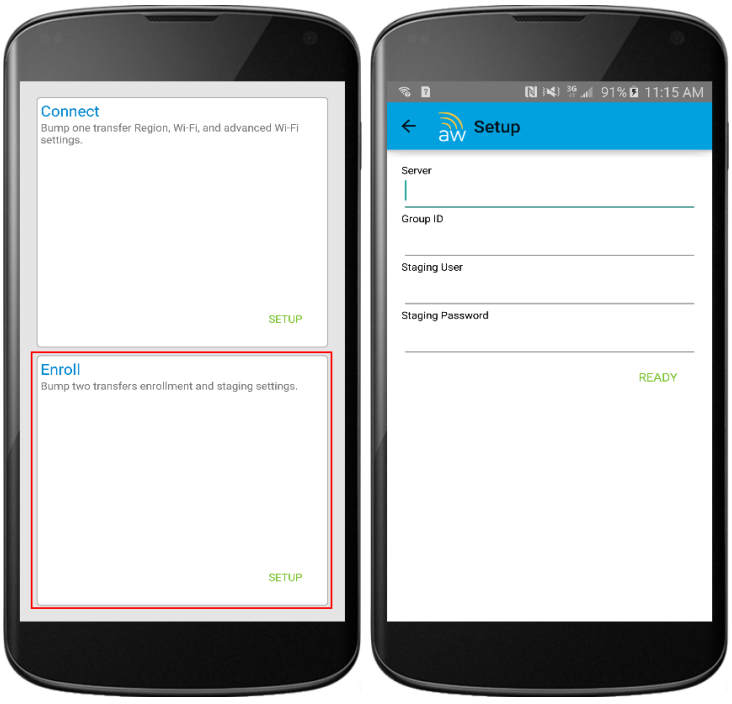
After the child device has reset, the device is provisioned for Work Managed Mode and bump one is complete. A welcome screen displays on your child device. To verify this from the child device, navigate to **Device Settings > Security > Device Administrators** to view AirWatch Agent listed as the device administrator. End users will not be able to deactivate this setting.



You will also notice on the device homescreen the pre-downloaded apps allowed. Any other applications will need to be approved by the administrator from the Workspace ONE UEM console .

If you have several devices to enroll in your device fleet, then repeat NFC bump one on each child device to provision them in Work Managed Device mode. If not, proceed to enrollment.

9. Return to the AirWatch Relay app, from the parent device, and tap **Enroll**.



10. Define the enrollment settings. These setting will be used to automate enrollment of child devices.

Setting	Description
Server	Enter the server URL or hostname.
Group ID	Enter an identifier for the organization group for the end users to use for device to log in.
parent User	Enter the credentials for the user the child device will be enrolled.
parent Password	Enter the credentials for the user the child device will be enrolled.

11. Tap **Ready**.

12. Perform the second NFC bump by bringing the parent and child device back to back and tap **Touch to Beam** on the child device to begin enrollment. The second NFC bump must be performed after the Setup Wizard has been completed. Wait until the Setup Wizard completes and directs you to the device home page before performing the second NFC bump to configure the AirWatch Agent.

13. Enter the credentials for the corporate Google account tied to the user. You will be prompted with the Google account password screen.

14. Tap **Next** to proceed to the **My Device** page (shown in the image above).

If enrollment was successful, the **My Device** page will display on the child device (shown above). All profiles and applications will start to automatically push to the device. You will repeat the enrollment steps for each device needing to be enrolled in your device fleet.

Navigate to **Devices > Details View > Summary** and view the **Security** section of the page to view the status. The should be a green check to verify Android activation.

Enroll Work Managed Devices Using AirWatch Identifier

During Work Managed Device enrollment, the user enters a special DPC-specific identifier token when they are prompted to add an account. A token is in the format “afw#EMM_Identifier” and automatically identifies Workspace ONE UEMas your EMM provider.

Important: This enrollment flow is only for Android accounts using Android 6.0 (M+) devices.

To enroll using the AirWatch Identifier:

1. Tap **Get Started** on your factory reset device.
2. Select your **Wi-Fi** network and login with your credentials to connect the device.
3. Enter the identifier “afw#airwatch” when prompted to add a Google account. The setup wizard adds a temporary Google Account to the device. This account is only used to download the DPC from Google Play and is removed upon completion.
4. Tap **Install** to begin configuration of the AirWatch Agent to the device. The Agent will automatically open after install is complete.
5. Choose the **Authentication Method** to continue enrollment:
   - Select **Email Address** if you have configured Autodiscovery. In addition, you may be prompted to select your Group ID from a list.
   - Choose **Server Details** and enter Server, Group ID, and user credentials.
6. Follow the remaining prompts to complete enrollment.

All profiles and applications start to automatically push to the device. The Workspace ONE UEM console reports the status of Android on the users devices. You can check the **Details View** page to verify that Android was successfully created.

Navigate to **Devices > Details View > Summary** and view the **Security** section of the page to view the status. A green check displays to verify Android activation.

Enroll Work Managed Device Mode Using a QR Code

The QR code enrollment method sets up and configures Work Managed Device mode by scanning a QR code from the setup wizard. This enrollment flow is ideal for an admin staging multiple devices before deploying to users or for the end user who will be enrolling their own device with the QR code provided by an IT admin.

Important: This enrollment flow is available for Managed Google Play and Managed Google Domain users. This enrollment flow is supported on Android 7.0+ devices.

1. Power on the device. The setup wizard prompts the user to tap the Welcome screen six times. The taps have to be done in the same place on the screen.
2. Connect to **Wi-Fi** and the setup wizard automatically downloads a QR code reader. The QR code reader app automatically starts once complete.

3. Scan your QR code.
4. The setup wizard automatically downloads the AirWatch Agent which should already be configured with Server URL and Group ID information.
5. Enter the user credentials.

If enrollment was successful, the **My Device** page displays on the device. All profiles and applications start to push automatically to the device.

The Workspace ONE UEM console reports the status of Android on the users devices. You can check the **Details View** page to verify that Android was successfully created.

Navigate to **Devices > Details View > Summary** and view the **Security** section of the page to view the status. The should be a green check to verify Android activation.

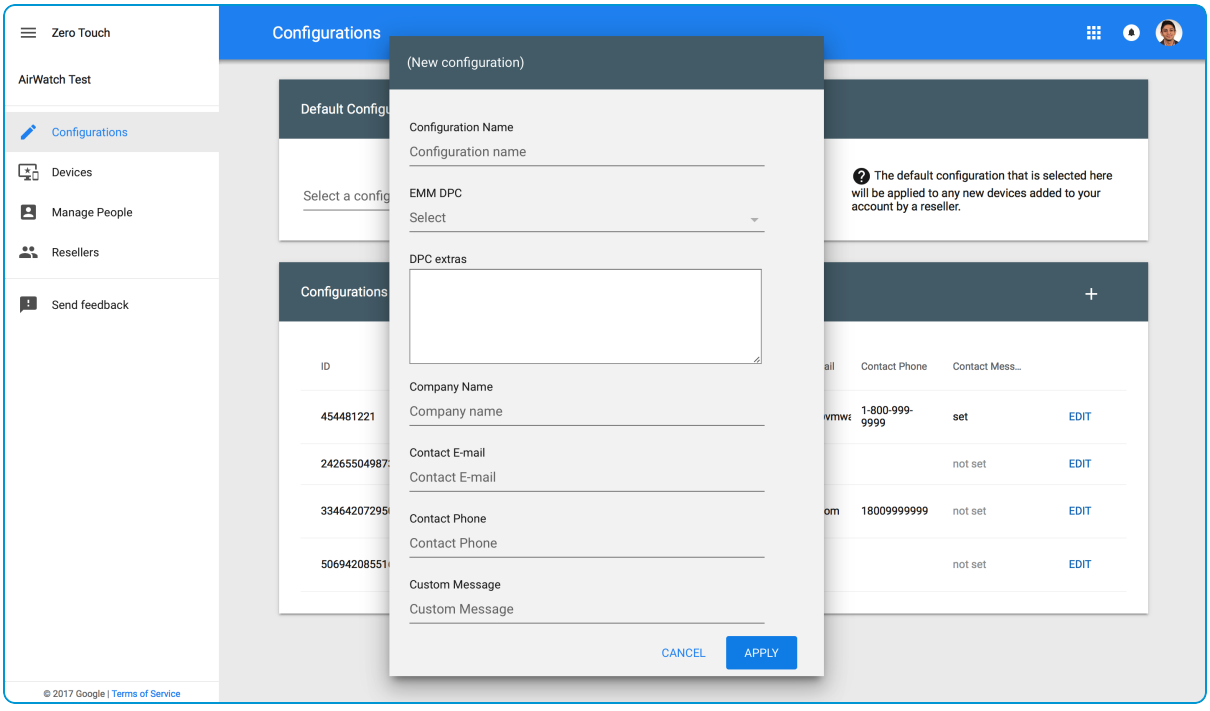
Enroll Work Managed Device Using Zero Touch Portal

In the Zero Touch Portal, add enrollment configurations that should be applied on the device as soon as the AirWatch Agent is downloaded.

Note: Zero Touch enrollment is only supported on Android 8.0+ devices.

To configure the portal:

1. Navigate to the **Configurations** tab and click the **+**.



2. Enter the following details for enrollment:

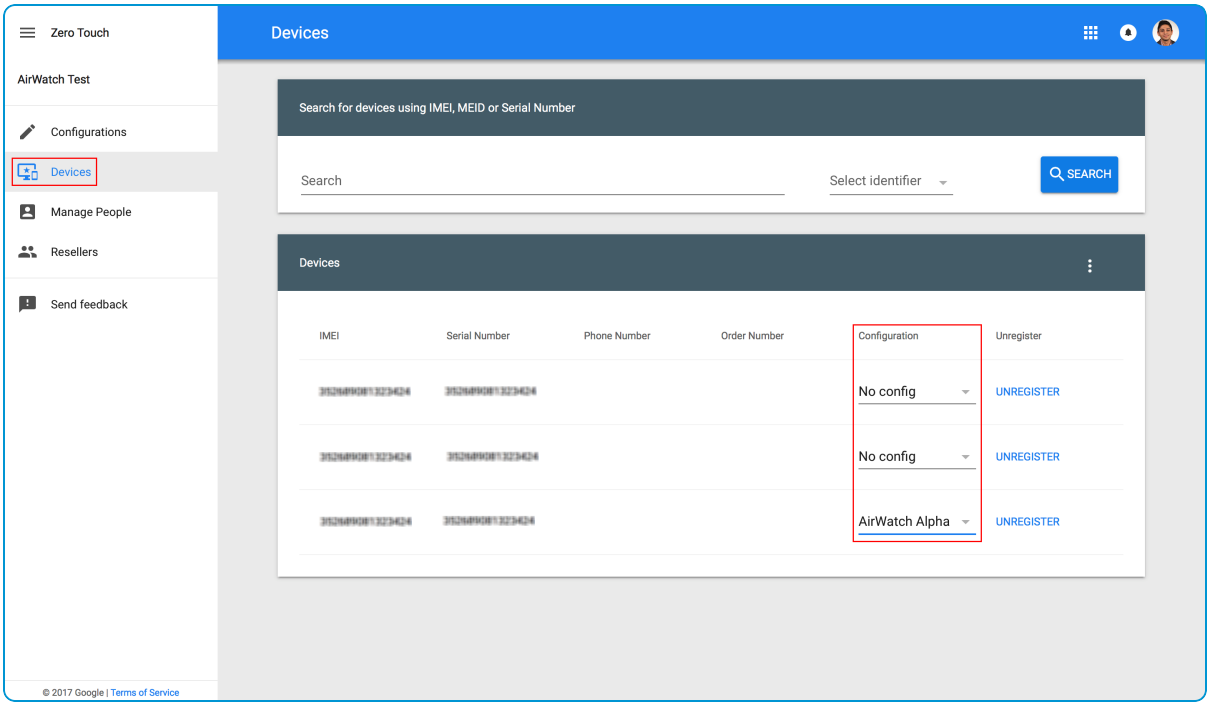
Setting	Description
Configuration Name	Enter a name for this configuration.
EMM DPC	Select 'AirWatch Agent'. This will ensure that the AirWatch Agent is downloaded as part of factory setup

DPC Extras	Enter the enrollment credentials that will be configured in the AirWatch Agent. You can include the Workspace ONE UEM console Server URL, Group ID, enrollment username, and password.
	End user provisions device:
	In this scenarios, exclude the username and password and the user enters them at device setup when prompted.
	`{ "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": { "serverurl": "https://airwatch.console.com", "gid": "groupID"} }`
	For Zero touch enrollment:
	This scenario is recommended if all devices are being staged to a single user or the enrollment username and password is known.
	`{ "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": { "serverurl": "https://airwatch.console.com", "gid": "groupID", "un":"username", "pw":"password" } }`

Company Name	Enter your organization name.
Contact E-mail	Enter the email that end users should contact if they run into issues.
Contact Phone	Enter the phone number that end users should call if they run into issues.
Custom Message	Enter a custom message to show to end users prior to downloading the AirWatch Agent.

3. Select **Apply**.
4. Assign configurations under the **Devices** tab by selecting the enrollment configuration that should be applied to the device.

   You will need to work with your carrier/ device reseller to retrieve IMEI and serial numbers for your devices.



Enrolling Android Device into Work Profile Mode

The enrollment process secures a connection between Android devices and your AirWatch environment. The AirWatch Agent facilitates enrollment and allows for real-time management and access to relevant device information.

Use the following instructions to install the AirWatch Agent and authenticate users based on the enrollment flow:

1. Download and install the AirWatch Agent from the Google Play Store.
2. Launch the AirWatch Agent.
   - If you have configured email autodiscovery, then the Agent prompts you for your email address. In addition, you may be prompted to select your Group ID from a list.
   - If you have not configured email autodiscovery, select desired enrollment method.
3. Tap **Server Details** and enter your **Server** and **Group ID**.
4. Enter **Username** and **Password** and tap **Continue**.
5. Accept the **Terms of Use**.
6. (Optional) Tap the **Encrypt** button and follow the remaining prompts to accepts the settings. The AirWatch Agent will close after accepting the encryption settings. Tap the **Encryption Complete** notification to return to the AirWatch Agent to continue enrollment.

   Note: The option to encrypt the device depends on the version of Android the device is running. Devices running Android Marshmallow are encrypted by default, so this option will not display during enrollment.

7. Tap **Set Up** to configure the Work Profile that will be associated with the device.

8. Tap **OK** on the Privacy Policy. Depending on how users are being created, the remaining screens for enrollment will vary.
   The enterprise settings from the Workspace ONE UEM console will be pushed to the device. **This ends enrolling devices for managed Google Play Accounts.**

9. For Google Accounts only, tap **Get Started** to create the Work Profile and connect the Managed Google Account to the device. These steps differ based on authentication method:

   To proceed with **User-defined** enrollment:

   a. Create the Password with your user credentials and tap **Next**.

   b. Enter the Managed Google Account **Password** and tap **Next**.

   To continue with **Directory Service Sync**:

   a. Enter your **Password** and tap **Next**.

   b. Select **Continue**.

   c. Select **Exit**.

   To follow the **SAML** enrollment flow:

   a. Enter the **User Name** and **Password** and tap **Login**. The user will be redirected to the AirWatch Agent.

If successful, the Work Profile is configured for the device and displays the AirWatch Agent settings page. The device is ready for use according to Android settings for the Work Profile.

Chapter 4:
Android Profiles

Android Profiles

Overview

Android profiles ensure proper use of devices and protection of sensitive data. Profiles serve many different purposes, from letting you enforce corporate rules and procedures to tailoring and preparing Android capable devices for how they are used.

Android Versus Android (Legacy) Profiles

When you go to deploy profiles for Android, you will see two platform types on the profiles page: Android and Android (Legacy). If you have completed the Android EMM Registration, select the Android profile option to configure profiles. If you have opted out of the EMM registration, then the Android (Legacy) profiles are available. When you select Android but have not walked through the Android EMM Registration, an error message displays prompting you to go to the settings page to complete EMM registration or proceed to Android (Legacy) profile deployment.

To walk through Android EMM Registration, see Android EMM Registration Overview on page 9

Work Profile vs. Work Managed Device Mode

A Work Profile is a special type of administrator. The user already has a personal device with their own account, and Workspace ONE UEM manages the Work Profile. Workspace ONE UEM enrollment will add a Work Profile and install the AirWatch Agent inside the Work Profile as the profile owner for that user.

The Work Managed device applies to devices that start in the unprovisioned state, and enrollment installs the AirWatch Agent the Work Managed device. The AirWatch Agent will have full control of the entire device. Some profiles will display the following tags: Work Profile and Work Managed Device.

Profiles configured for the Work Profile only apply to the Android badged apps and not affect the users personal apps or settings unless you configure profiles at the device level. For example, certain restrictions disable access to YouTube, Google Play. Restrictions only affect the Android badged apps and not the regular Play Store versions. Alternatively, profiles configured for Work Managed Device mode type apply to the entire device. Each profile discussed in this section indicates which device type the profile affects.

Device Access

Some device profiles configure the settings for accessing an Android device. Use these profiles to ensure that access to a device is limited only to authorized users.

Some examples of device access profiles include:

- Secure a device with a Passcode profile. For more information, see Passcode Profile on page 39.
- Specify and control how, when and where your employees use their devices. For more information, see Restrictions Profile on page 42.

Device Security

Ensure that your Android devices remain secure through device profiles. These profiles configure the native Android security features or configure corporate security settings on a device through Workspace ONE UEM.

- Access internal resources such as email, files, and content. For more information, see Configure VPN on page 48.
- Take administrative actions when a user installs or uninstalls certain applications. For more information, see Application Control on page 45.

Device Configuration

Configure the various settings of your Android devices with the configuration profiles. These profiles configure the device settings to meet your business needs.

- Connect your device to internal WiFi automatically. For more information, see Wi-Fi Profile on page 47.
- Manage how Android OS update notifications and the actual updates are controlled. For more information, see Enable System Updates on page 46.

Passcode Profile

You can set the Passcode profile for the settings to apply as a Work Passcode or Device Passcode.

The Work Passcode applies passcode policies only to work apps so users do not have to enter complex passwords each time they unlock their device when enrolled with a Work Profile. The Work passcode ensures that end users can access their private apps in any way they like while keeping corporate app data protected without the use of wrapping technologies. For Work Managed devices, this passcode policy applies to the device. The Work Passcode is available on Android 7.0 (Nougat) and above for Work Profile enrolled devices.

The Device Passcode applies passcode policies for the device enrolled with a Work Profile. This passcode needs to be entered each time the device is unlocked and can be applied in addition to the work passcode.

By default, when creating new profiles, only the work passcode is enabled (device passcode is enabled). The admin has to enable the device passcode manually.

Enforce Passcode Settings

Setting a passcode policy requires your end users to enter a passcode, providing a first layer of defense for sensitive data on devices.

To create a device passcode profile:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
2. Configure the **General** profile settings as appropriate.

3. Configure the Passcode settings:

Settings	Description
Work Passcode	
Enable Work Passcode Policy	Enable to apply passcode policies only to Android badged apps.
Minimum Passcode Length	Ensure passcodes are appropriately complex by setting a minimum number of characters.
Passcode Content	Ensure the passcode content meets your security requirements by selecting **Any**, **Numeric**, **Alphanumeric**, **Alphabetic**, **Complex**, or **Complex numeric** from the drop-down menu.
Maximum Number of Failed Attempts	Specify the number of attempts allowed before the device is wiped.
Maximum Passcode Age (days)	Specify the maximum number of days the passcode can be active.
Passcode History	Set the number of times a passcode must be changed before a previous passcode can be used again.
Device Lock Timeout Range (in Minutes)	Set the period of inactivity before the device screen locks automatically.
Device Passcode	
Enable Device Passcode Policy	Apply passcode policies for the device enrolled with a Work Profile. This passcode will need to be entered to unlock the device and can be applied in addition to the work passcode. For Work Managed devices, this passcode policy is applied to the device.
Minimum Passcode Length	Ensure passcodes are appropriately complex by setting a minimum number of characters.
Passcode Content	Ensure the passcode content meets your security requirements by selecting **Any**, **Numeric**, **Alphanumeric**, **Alphabetic**,**Complex**, or **Complex Numeric** from the drop-down menu.
Maximum Number of Failed Attempts	Specify the number of attempts allowed before the device is wiped.
Maximum Passcode Age (days)	Specify the maximum number of days the passcode can be active.
Passcode History	Set the number of times a passcode must be changed before a previous passcode can be used again.
Device Lock Timeout Range (in Minutes)	Set the period of inactivity before the device screen locks automatically.

The following settings apply if you select Complex from the **Passcode Content** text box.

Setting	Description
Maximum Number of Failed Attempts	Specify the number of attempts allowed before the device is wiped.
Minimum Number of Letters	Specify the number of letters that can be included in the passcode.
Minimum Number of Lower Case Letters	Specify the number of lowercase letters allowed in the passcode.
Minimum Number of Upper Case Letters	Specify the number of uppercase letters allowed in the passcode.
Minimum Number of Non-Letters	Specify the number of special characters allowed in the passcode.
Minimum Number of Numerical Digits	Specify the number of numerical digits allowed in the passcode.
Minimum Number of Symbols	Specify the number of symbols allowed in the passcode.
Maximum Passcode Age (days)	Set the maximum number of days the passcode can be active.

4. Select **Save & Publish** to assign the profile to associated devices.

Enforce Chrome Browser Settings

The Chrome Browser Settings profile helps you to manage settings for the Work Chrome app. Configuring this profile will not affect the user's personal Chrome app. You can push this profile in conjunction with a separate VPN or Credentials+Wi-Fi payload to ensure end-users can authenticate and log in to your internal sites and systems. This will ensure that users must use the Work Chrome app for business purposes.

To configure **Chrome Browser Restrictions**:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
2. Configure the profile's **General** settings as appropriate.
3. Select the **Chrome Browser Settings** payload and configure the settings as desired.
4. Select **Save & Publish**.

Restrictions Profile

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 devices and vary based on device enrollment. The Restrictions profile displays tags labeling the **Work Managed Device** and **Work Profile** modes.

The **Restrictions** profile displays tags that indicate if the selected restriction applies towards the Work Profile, Work Managed Device or both, however, that for Work Profile devices these only affect the Android badged apps. For example, when configuring restrictions for the Work Profile you can disable access to the work Camera. This only affects the Android badged camera and not the users personal camera.

Note, there are a handful of system apps included with the Work Profile by default such as Work Chrome, Google Play, Google settings, Contacts, and Camera – these can be hidden using the restrictions profile and does not affect the user's personal camera.

Enforce Restrictions

Deploy a restrictions payload for added security on Android devices. Restrictions payloads devices can disable end user access to device features to ensure devices are not tampered with.

To create a restrictions profile:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
2. Configure the profile's **General** settings as appropriate.
3. Select the **Restrictions** profile to configure the settings including:

Settings	Description
Device Functionality	Device-level restrictions can disable core device functionality such as the camera, screen capture and factory reset to help improve productivity and security. For example, disabling the camera protects sensitive materials from being photographed and transmitted outside of your organization. Prohibiting device screen captures helps protect the confidentiality of corporate content on the device.
Application	Application-level restrictions can disable certain applications such as YouTube, Google Play Store and native browser, which enables you to enforce adherence to corporate policies for device usage.
Sync and Storage	Control how information is stored on devices, allowing you to maintain the highest balance of productivity and security. For example disabling Google or USB Backup keeps corporate mobile data on each managed device and out of the wrong hands.
Network	Prevent devices from accessing Wi-Fi and data connections to ensure that end users are not viewing sensitive information through an insecure connection.
Work and Personal	Determine how information is accessed or shared between personal container and work container. These settings apply to the Work Profile Mode only.

4. Select **Save & Publish** to assign the profile to associated devices.

Enable Exchange Active Sync

AirWatch uses the Exchange ActiveSync (EAS) profile on Android devices to guarantee a secure connection to internal email, calendars, and contacts using mail client types such as AirWatch Inbox, Gmail, and Divide. For example, the configured EAS email settings for the Work Profile affects any email apps downloaded from the AirWatch App Catalog with the badged icon and not the user's personal email.

Once each user has an email address and user name you can create an EAS profile with the following steps:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
2. Configure the **General** profile settings as appropriate.
3. Select the **Exchange Active Sync** profile and configure the following settings.

Settings	Description
Mail Client Type	Use the drop-down menu to select a mail client that is being pushed to user devices.
Host	Specify the external URL of the company Active Sync server.
Server Type	Select between **Exchange** and **Lotus**.
Use SSL	Enable to encrypt EAS data.
Enable Validation Checks on SSL Certs	Enable to allow Secure Socket Layer certifications.
S/MIME	Enable to select an S/MIME certificate you associate as a User Certificate on the **Credentials** payload. • **S/MIME Signing Certificate** – Select the certificate to allow provision of S/MIME certificates to the client for message signing. • **S/MIME Encryption Certificate** – Select the certificate to allow provision of S/MIME certificates to the client for message encryption.
Login Information	
Domain	Use lookup values to use the device-specific value.
Username	Use lookup values to use the device-specific value.
Email Address	Use lookup values to use the device-specific value.
Password	Leave blank to allow end users to set their own password.
Login Certificate	Select the available certificate from the drop-down menu.
Settings	
Default Signature	Specify a default email signature to display on new messages.
Maximum Attachment Size (MB)	Enter the maximum attachment size that user is allowed to send.
Restrictions	
Allow Contacts And Calendar Sync	Enable to allow contacts and calendar to sync with devices.

4.

5. Select **Save & Publish** to assign the profile to associated devices.

Credentials

For greater security, you can implement digital certificates to protect corporate assets. To do this, you must first define a certificate authority, then configure a Credentials payload alongside your Exchange ActiveSync (EAS), Wi-Fi or VPN payload.

Each payload has settings for associating the certificate authority defined in the Credentials payload. Credentials profiles deploy corporate certificates for user authentication to managed devices. The settings in this profile vary depending on the device ownership type. The **Credentials** profile applies towards the Work Profile and Work Managed Device mode types.

Devices must have a device pin code configured before Workspace ONE UEM can install identity certificates with a private key.

Deploy Credentials

Credentials profiles deploy corporate certificates for user authentication to managed devices. The settings in this profile will vary depending on the device ownership type. The **Credentials** profile will apply towards the Work Profile and Work Managed Device mode types.

Configure the following options to apply credentials:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
2. Configure the profile's **General** settings as appropriate.
3. Select the **Credentials** profile and select **Configure**.
4. Use the drop-down menu to select either **Upload** or **Defined Certificate Authority** for the **Credential Source**. The remaining profile options are source-dependent. If you select **Upload**, you must enter a **Credential Name** and upload a new certificate. If you select **Defined Certificate Authority**, you must choose a predefined **Certificate Authority** and **Template.**
5. Select **Save & Publish.**

Application Control

The Application Control profile allows you to whitelist or blacklist specific applications. While the compliance engine sends alerts and takes administrative actions when a user installs or uninstalls certain applications, Application Control prevents users from even attempting to make those changes.

For example, the AirWatch Agent is automatically pushed to the device as a badge app. Enabling the Prevent Un-Installation of Required Apps option prevents the uninstallation of the AirWatch Agent and other required apps configured in Application Groups. Whitelisting is enabled by default because only an admin can add apps to the Work Profile.

Configure Application Control

To limit app access to your Android devices, create a profile of blacklisted and whitelisted applications with the Application Control profile.

To configure application control settings:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**
2. Configure the **General** profile settings as appropriate.
3. Select the **Application Control** payload.
4. Enable or disable the following settings to set the level of control for your application deployments:

Setting	Description
Disable Access Blacklisted Apps	Enable to disable access to applications that are considered blacklisted which is defined in Application Groups. If enabled, this option does not uninstall the application from the device.
Prevent Un-Installation of Required Apps	Enable to prevent the uninstallation of required apps defined in Application Groups.
Enable System Apps inside Android	Enable to unhide pre-installed applications inside the Work Profile as defined in whitelisted apps in Application Groups.

5. Select **Save & Publish**.

Configure Proxy Settings

Global Proxy settings are configured to ensure that all the HTTP and HTTPS network traffic is passed only through it. This ensures data security since all the personal and corporate data will be filtered through the Global proxy profile.

To configure these settings:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
2. Configure the profile's **General** settings as appropriate.
3. Select the **Proxy Settings** profile.
4. Configure the Proxy settings as such:

Setting	Description
Proxy Mode	Select the desired proxy type.
Proxy PAC URL	Specify a URL to a proxy .pac file.
Proxy Server	Enter the host name of IP address for the proxy server.
Exclusion List	Add hostnames to prevent them from routing through the proxy.

5. Select **Save & Publish**.

Enable System Updates

AirWatch manages how OS update notifications and the actual updates are controlled. You can control OS updates with this profile in three ways.

To create a system update policy:

1. Navigate to**Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
2. Configure the **General** profile settings as desired.
3. Select the **System Updates** profile.

4. Use the drop-down menu from the **Automatic Updates** field to select the update policy.

Setting	Description
Install Updates Automatically	Automatically install updates when they become available .
Defer Update Notifications	Defer all updates. Send a policy that blocks OS updates for a maximum period of 30 days.
Set Update Window	Set a time window in which to update the device.

5. Select **Save & Publish**.

Wi-Fi Profile

Configuring a Wi-Fi profile lets devices connect to corporate networks, even if they are hidden, encrypted or encrypted, or protected. The Wi-Fi profile can be useful for end users who travel to various office locations that have their own unique wireless networks or for automatically configuring devices to connect to the appropriate wireless network while in an office.

When pushing a Wi-Fi profile to devices running Android 6.0+, if a user already has their device connected to a Wi-Fi network through a manual setup; the Wi-Fi configuration cannot be changed by Workspace ONE UEM. For example, if the Wi-Fi password has been changed and you push the updated profile to enrolled devices, some users have to update their device with the new password manually.

Configure Wi-Fi Access

Configuring a Wi-Fi profile lets devices connect to corporate networks, even if they are hidden, encrypted or password protected.

To configure the Wi-Fi profile:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
2. Configure the profile's **General** settings as appropriate.
3. Select the **Wi-Fi** payload.

4. Configure **Wi-Fi** settings, including:

Setting	Description
Service Set Identifier	Provide the name of the network the device connects to.
Hidden Network	Indicate if the Wi-Fi network is hidden.
Set as Active Network	Indicate if the device will connect to the network with no end-user interaction.
Security Type	Specify the access protocol used and whether certificates are required. Depending on the selected security type, this will change the required fields. If **None, WEP, WPA/WPA 2, or Any (Personal)** are selected; the **Password** field will display. If **WPA/WPA 2 Enterprise** is selected, the Protocols and Authentication fields display. • **Protocols** ◦ Use Two Factor Authentication ◦ SFA Type • **Authentication** ◦ Identity ◦ Anonymous Identity ◦ Username ◦ Password ◦ Identity Certificate ◦ Root Certificate
Password	Provide the required credentials for the device to connect to the network. The password field displays when **WEP, WPA/WPA 2, Any (Personal), WPA/WPA2 Enterprise** are selected from the **Security Type** field.

5. Select **Save & Publish**.

Configure VPN

A Virtual Private Network (VPN) provides devices with a secure and encrypted tunnel to access internal resources such as email, files, and content. VPN profiles enable each device to function as if it were connected through the on-site network.

Depending on the connection type and authentication method, use look-up values to auto-fill user name info to streamline the login process.

To create a VPN profile:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
2. Configure the **General** profile settings as appropriate.
3. Select **VPN** to edit the profile.
4. Configure **VPN** settings. The table below defines all settings that can be configured based on the VPN client.

Setting	Description
Connection Info	
Connection Type	Choose the protocol used to facilitate VPN sessions.
Connection Name	Enter the assigned to the connection created by the profile.
Server	Enter the name or address of the used for VPN connections.
Account	Enter the user account for authenticating the connection.
Always On VPN	Enable to force all traffic from work apps to be tunneled through VPN.
Set Active	Enable to turn VPN on after the profile applies to the device.
Per-App VPN Rules	Enable Per App VPN which allows you to configure VPN traffic rules based on specific applications. This text box only displays for supported VPN vendors.
Authentication	
User Authentication	Choose the method required to authenticate the VPN session.
Password	Provide the credentials required for end-user VPN access.
Client Certificate	Use the drop-down to select the client certificate. These are configured in the Credentials profiles.
Certificate Revocation	Enable to turn on certificate revocation.
Anyconnect Profile	Enter the AnyConnect profile name.
FIPS Mode	Enable to turn on FIPS Mode.
Strict Mode	Enable to turn on Strict Mode.
Vendor Configurations	
Vendor Keys	Create custom keys to go into the vendor config dictionary.
Key	Enter the specific key provided by the vendor.
Value	Enter the VPN value for each key.

5. Select **Save & Publish**.

Configure Per-App VPN

You can force selected applications to connect through your corporate VPN. Your VPN provider must support this feature, and you must publish the apps as managed applications.

1. Navigate to**Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
2. Select **Android** to configure the settings.
3. Select the **VPN** payload from the list.
4. Select your VPN vendor from the **Connection Type** field
5. Configure your VPN profile .
6. Select **Per-App VPN** to generate a VPN UUID for the current VPN profile settings. The VPN UUID is a unique identifier for this specific VPN configuration.
7. Select **Save & Publish**.

   If this was done as an update to an existing VPN profile, then any existing devices/applications that currently use the profile will be updated. Any devices/applications that were not using any VPN UUID whatsoever will also be updated to use the VPN profile.

To configure public apps to use the Per-App VPN profile, see Adding Public Applications for Android on page 58

Set Permissions

The Workspace ONE UEM console provides the admin the ability to view a list of all the permissions that an app is using and set the default action at run time of the app. The Permissions profile is available on Android 6.0+ devices using Work Managed device mode.

You can set run-time permission policies for each Android badged app. The latest permissions are retrieved when configuring an app at an individual app-level. Permissions apply to all Android badged apps.

Note: All permissions used by an app are listed when you select the app from the Exceptions list, however permission policies from the Workspace ONE UEM console only apply to dangerous permissions as deemed by Google. Dangerous permissions cover areas where the app requests data that includes the user's personal information, or could potentially affect the user's stored data. For more information, please reference the Android Developer website.

To create the Permissions profile:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
2. Configure the **General** profile settings as appropriate.
3. Configure the Permissions settings, including:

Settings	Description
Permission Policy	Select whether to **Prompt user for permission**, **Grant all permissions**, or **Deny all permissions** for all work apps.
Exceptions	Search for apps that have already been added into AirWatch (should only include Android approved apps), and make an exception to the permission policy for the app.

4. Select **Save & Publish** to assign the profile to associated devices.

Configure Single App Mode

Single App Mode allows you use Android devices for a single purpose such as kiosk mode by whitelisting supported internal and public applications.

Note: For more information on supported applications, see the link in the Single App Mode profile in the Workspace ONE UEM console which directs you to the Google Developer site for specifics.

Note: AirWatch application are not currently supported for Single App mode.

For optimal use of single app mode and best practices, see Best Practices for Single App Mode on page 52.

To configure Single App Mode:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
2. Configure the **General** profile settings as appropriate.
3. Configure the Single App Mode settings:

Settings	Description
Whitelisted Apps	Select the desired app to lock device into Single App Mode.

Best Practices for Single App Mode

Consider applying these policies and restrictions to ensure the best experience and maintenance for your single-purpose using single app mode policies. These recommendations are useful if you are deploying a single app mode profile for devices in kiosk and digital signage use cases where an end user is not associated with the device.

Create a "Restrictions" profile and configure the following within the profile:

- Disable the following options under **Device Functionality**:
  - **Allow Status Bar** - This ensures an immersive experience when the device is locked into a single app.
  - **Allow Keyguard** - This ensures that the device does not get locked.
- Enable the following options under **Device Functionality**:
  - Force Screen On when Plugged In on AC Charger
  - Force Screen On when Plugged In on USB Charge
  - Force Screen On when Plugged In on Wireless Charger

  These options ensure that the device screen is always turned on for interaction.

Deploy the System Update Policy profile to ensure the device receives the latest fixes with minimal manual intervention.

Create AirWatch Launcher Profile

AirWatch Launcher is an app launcher that enables you to lock down Android devices for individual use cases and customize the look and behavior of managed Android devices. The AirWatch Launcher app replaces your device interface with one that is custom- tailored to your business needs.

You can configure Android 6.0 Marshmallow and later devices as corporate-owned, single-use (COSU) mode. COSU mode allows you to configure devices for a single purpose such as kiosk mode by whitelisting supported internal and public applications. COSU mode is supported for Single App mode, Multi App Mode, and Template Mode. For more information on deploying AirWatch Launcher profile in COSU mode, see the AirWatch Launcher Guide.

To configure the settings of the AirWatch Launcher profile:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android (Legacy)**.
2. Configure the profile's **General** settings.
3. Select the **Launcher** profile.
4. Select app mode:

Setting	Description
Single App	Select to lock device into a mobile kiosk view for single app use.
Multi App	Select to restrict device to a limited set of apps.
Template	Select to customize the device home screen with images, text and apps.

5. Configure your selected app mode.
6. Click **Save** to add the profile to the Workspace ONE UEM console or **Save & Publish** to add the profile and immediately deploy it to applicable Android devices.

Configure Zebra MX Profile

The Zebra MX profile allows you take advantage of the additional capabilities offered with the Zebra MX service app on Android devices. You had to the Zebra MX Service app from AirWatch Resources and distribute it as an internal app in the Workspace ONE UEM console in conjunction with this profile.

To configure the Zebra MX profile for Android:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
2. Configure the **General** profile settings as appropriate.
3. Configure the Zebra MX profile settings:

Setting	Description
WiFi	
Include Fusion Settings	Enable to expand Fusion options for use with Fusion Adapters for Motorola devices.
Set Fusion 802.11d	Enable to use the Fusion 802.11d to set the Fusion 802.11d settings.
Enable 802.11d	Enable to use 802.11d wireless specification for operation in additional regulatory domains.
Set Country Code	Enable to set the Country Code for use in the 802.11d specifications.
Set RF Band	Enable to choose 2.4 GHz, 5 Ghz, or both bands and any channel masks applicable.
Restrictions	
Allow Airplane Mode	Enable to allow access to the Airplane Mode settings screen.
Allow Mock Locations	Enable or disable Mock Locations (in Settings > Developer Options).
Allow Background Data	Enable or disable background data.

Setting	Description
Allow Wi-Fi to Disconnect During Sleep	**Always On** - Wi-Fi stays on when device goes to sleep. **Only When plugged in** - Wi-Fi stays on when device goes to sleep only if the device is charging. **Never On** - Wi-Fi turns off when the device goes to sleep.
Data Usage On Roaming	Enable to allow data connection while roaming.
Force Wi-Fi On	Enable to force Wi-Fi on so user cannot turn it off.
Allow Bluetooth	Enable to allow the use of Bluetooth.
Allow Clipboard	Enable to allow copy/paste.
Allow Network Monitoring notification	Enable to allow Network Monitor Warning notification, which is normally displayed after installing certificates.
Date/Time	
Enable Date/Time Settings	Enable to set Date/Time settings.
Date Format	Determine the order that the Month, Day, and Year displays.
Time Format	Choose 12 or 24 Hours.

Setting	Description

Date/Time	Set which data source your devices will pull from for the date and time settings:
	• **Automatic**Sets the date and time based on native device settings.
	• **Server Time** – Sets the time based on the server time of the Workspace ONE UEM console .
	  ◦ **Time Zone** – Specify the time zone.
	• **HTTP URL** – Sets the time based on a URL. This URL can be any URL. For example, you can use www.google.com for your URL.
	  ◦ **URL** – Enter the web address the Date/Time schedule.
	  ◦ **Enable Periodic Sync** – Enable to set the device to check date/time periodically in days.
	  ◦ **Set Time Zone** – Specify the time zone.
	• **SNTP Server**
	  ◦ **URL** – Enter the web address the Date/Time schedule. For example, you could enter time.nist.gov for your use.
	  ◦ **Enable Periodic Sync** – Enable to set the device to check date/time periodically in days.

Volumes	
Music, video, Games & Other Media	Set the slider to the volume level you want to lock-in on the device.
Ringtones & Notifications	Set the slider the volume you want to lock-in on the device
Voice Calls	Set the slider to the volume you want to lock-in on the device.
Enable Default Notifications	Allows default notifications on the device to sound.
Enable Dial Pad Touch Tones	Allows dial pad touch tones on the device to sound.
Enable Touch Tones	Allows touch tones on the device to sound.
Enable Screen Lock Sounds	Allows the device to play a sound when locked.
Enable Vibrate on Touch	Allows the vibrate settings to be activated.

Setting	Description
Display	
Enable Display Settings	Enable to set display settings.
Display Brightness	Set the slider to the brightness level you want to lock-in on the device.
Enable Auto-Rotate Screen	Allows the screen to auto-rotate.
Set Sleep	Choose the amount of time before the screen will set to sleep mode.

4. Select **Save & Publish**.

Using Custom Settings

The **Custom Settings** payload can be used when new Android functionality releases or features that AirWatch does not currently support through its native payloads. Uuse the **Custom Settings** payload and XML code to manually enable or disable certain settings. To do this you would use the following instructions:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
2. Configure the profile's **General** settings.
3. Configure the applicable payload (for example, Restrictions or Passcode).

   You can work on a copy of your profile, saved under a "test" organization group, to avoid affecting other users before you are ready to Save and Publish.
4. **Save**, but do not publish, your profile.
5. Select the radio button from the **Profiles List View** for the row of the profile you want to customize.
6. Select the **XML** button at the top to view the profile XML.
7. Find the section of text starting with <characteristic> ... <characteristic> that you configured previously, for example, Restrictions or Passcode. The section contains a configuration type identifying its purpose, for example, restrictions.
8. Copy this section of text and close the XML View. Open your profile.
9. Select the **Custom Settings** payload and select **Configure**. Paste the XML you copied in the text box. The XML code you paste should contain the complete block of code, from <characteristic> to <characteristic>.
10. Remove the original payload you configured by selecting the base payload section and selecting the minus [-] button. You can now enhance the profile by adding custom XML code for the new functionality.

    Important: Any device not upgraded to the latest version ignores the enhancements you create. Since the code is now custom, you should test the profile devices with older versions to verify expected behavior.
11. Select **Save & Publish**.

Chapter 5:
Application Management for Android

Application Management for Android Overview

Use Workspace ONE UEM to push Android public and internal applications to Android devices. This process includes adding and approving applications for integration between Workspace ONE UEM and the Google Play Store. 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.

Internal Apps with Android

Internal apps are company-specific apps developed by your organization that you may 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.

If you are using Android 6.0+ devices as Work managed devices, add these apps to Workspace ONE UEM console so that they are available to Android specific users. Once you have added your internal application to the UEM console, these apps are treated as public applications.

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 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.

Adding Public Applications for Android

Search the Google Play Store directly from the Workspace ONE UEM console to add apps to the Android integration.

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.
4. Select **Next** or enter the **Name** of the applications you want to add to the integration. The Google Play Store 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. Select **Approve**. Be sure to view the permissions for the applications and follow the prompts to confirm approval.

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

7. 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.

8. Assign a **Required Terms of Use** for the application on the **Terms of Use** tab. This setting 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.

9. 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.

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

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

Assign Applications for Android

After you approve the app 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.

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 new one.
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 agent 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 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.
Send Application Configuration	Enable this feature to 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.
Application uses AirWatch SDK	Identify whether the application uses AirWatch SDK functionality and whether it needs a profile to apply the features. • 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.

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

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

Enable Play for Work

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 v9.0.2.

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.

Integration Features

Integration of Android and Workspace ONE UEM Mobile Application Management provides the following features and behaviors.

Identifying Android Apps on Devices

The briefcase icon identifies applications that are part of the Android system.

Accessing Android Apps

Available through managed Google Play.

Chapter 6:
Android Management

Android Device Management Overview

After your devices are enrolled and configured, manage the devices using the Workspace ONE UEM console. The management tools and functions enable you to keep an eye on your devices and remotely perform administrative functions.

You can manage all your devices from the UEM console. The Dashboard is a searchable, customizable view that you can use to filter and find specific devices. This feature makes it easier to perform administrative functions on a particular set of devices. The Device List View displays all the devices currently enrolled in your Workspace ONE UEM environment and their status. The **Device Details** page provides device-specific information such as profiles, apps, AirWatch Agent version and which version of any applicable OEM service currently installed on the device. You can also perform remote actions on the device from the Device Details page that are platform-specific.

Device Management Commands

You can manage Android settings and configurations using the Workspace ONE UEM console .

Admins have the ability to perform one time commands including lock devices, wipe devices and change a passcode from the Workspace ONE UEM console. For Lollipop devices, these commands will apply at either the Work Profile or Work Managed Device level depending on the ownership of the device.

The following commands are available from this view:

- **Lock Device** – Lock all selected devices and force users to re-enter device security PIN. This option applies to the Work Profile and Work Managed Devices.
- **Device Wipe** – Wipes all data from the selected device, including all data, email, profiles and MDM capabilities and returns the device to factory default settings. This setting only applies to the Work Managed Device type.
- **Enterprise Wipe** – Remove the Work Profile and Work Managed Device capabilities from the Android device.

Device Details Apps Tab

The **Devices Details Apps Tab** in the Workspace ONE UEM console contains alternative options to control public applications by device. Admins can view information about the application including the installation status, the application type, the application version, and the application identifier.

The **Install** option from the actions menu allows admins to push the application to the Google Play for Work app. The device user can then install the application to the device. The **Remove** option from the actions menu to uninstall the application silently off the device.

Specific Profiles Features for Android

These features matrices are a representative overview of the key OS specific functionality available, highlighting the most important features available for device administration for Android.

Feature	Work Profile	Work Managed Device
Application Control		
Disable Access to Blacklisted Apps	✓	✓
Prevent uninstallation of Required Applications	✓	✓
Enable System Update Policy		✓
Runtime Permissions Management	✓	✓
Browser		
Allow Cookies	✓	✓
Allow Images	✓	✓
Enable Javascript	✓	✓
Allow Pop-Ups	✓	✓
Allow Track Location	✓	✓
Configure Proxy Settings	✓	✓
Force Google SafeSearch	✓	✓
Force YouTube Safety Mode	✓	✓
Enable Touch to Search	✓	✓
Enable Default Search Provider	✓	✓
Enable Password Manager	✓	✓
Enable alternate error pages	✓	✓
Enable Autofill	✓	✓
Enable Printing	✓	✓
Enable Data Compression Proxy Feature	✓	✓
Enable Safe Browsing	✓	✓
Disable saving browser history	✓	✓
Prevent Proceeding After Safe Browsing Warning	✓	✓
Disable SPDY protocol	✓	✓
Enable network prediction	✓	✓
Enable Deprecated Web Platform Features For a Limited Time	✓	✓
Force Safe Search	✓	✓
Incognito Mode Availability	✓	✓
Allows sign in to Chromium	✓	✓
Enable Search Suggestion	✓	✓

Feature	Work Profile	Work Managed Device
Enable Translate	✓	✓
Allow Bookmarks	✓	✓
Allow Access to Certain URLs	✓	✓
Block Access to Certain URLs	✓	✓
Set Minimum SSL Version	✓	✓
Passcode Policy		
Have User Set New Passcode	✓	✓
Maximum failed password attempts	✓	✓
Allow Simple Passcode	✓	✓
Alphanumeric password Allowed	✓	✓
Set Device Lock timeout (in minutes)	✓	✓
Set Maximum Passcode Age	✓	✓
Password History Length	✓	✓
Password History Length	✓	✓
Set Minimum Passcode Length	✓	✓
Set Minimum Number of Numerical Digits	✓	✓
Set Minimum Number of Lower Case Letters	✓	✓
Set Minimum Number of Upper Case Letters	✓	✓
Set Minimum Number of Upper Case Letters	✓	✓
Set Minimum Number of Special Characters	✓	✓
Set Minimum Number of Symbols	✓	✓
Allow Passcode Reset	✓	✓
Commands		
Allow Enterprise Wipe	✓	✓
Allow Device Wipe		✓
Allow Container or Profile Wipe	✓	
Allow SD Card Wipe		✓
Lock Device	✓	✓
Allow Lock Container or Profile		
Email		
Native Email Configuration	✓	✓

Feature	Work Profile	Work Managed Device
Allow Contacts and Calendar Sync	✓	✓
Network		
Configure VPN Types	✓	✓
Enable Per-app VPN*	✓	✓
Use Web Logon for Authentication*	✓	✓
Set HTTP Global Proxy	✓	✓
Allow Data Connection to Wi-Fi	✓	✓
Always on VPN	✓	✓
Encryption		
Require Full Device Encryption	✓	✓
Report Encryption Status		

Specific Restrictions for Android

This matrix provides a representational overview of the restrictions profile configurations available by device ownership type.

Feature	Work Profile mode	Work Managed Device mode
Device Functionality		
Allow Factory Reset		✓
Allow Screen Capture	✓	✓
Allow Adding Google Accounts	✓	✓
Allow Removing the Android Work Account		✓
Allow Outgoing Phone Calls		✓
Allow Send/Receive SMS		✓
Allow Credentials Changes		✓
Allow All Keyguard Features		✓
Allow Keyguard Camera		✓
Allow Keyguard Notifications		✓
Allow Keyguard Fingerprint Sensor		✓
Allow Keyguard Trust Agent State	✓	✓

Feature	Work Profile mode	Work Managed Device mode
Allow Keyguard Unredacted Notifications	✓	✓
Force Screen On when Plugged In on AC Charger (Android 6.0+)		✓
Force Screen On when Plugged In on USB Charger (Android 6.0+)		✓
Force Screen On when Plugged In on Wireless Charger (Android 6.0+)		✓
Allow Wallpaper Change (Android 7.0+)		✓
Allow Status Bar		✓
Allow Keyguard (Android 6.0+)		✓
Allow Adding Users		
Allow Removing Users		
Allow Safe Boot (Android 6.0+)		✓
Allow Wallpaper Change (Android 7.0+)		
Allow User Icon Change (Android 7.0+)		✓
Allow Adding/Deleting Accounts	✓	✓
Application		
Allow Camera	✓	✓
Allow Google Play	✓	✓
Allow Chrome Browser	✓	✓
Allow Non-Market App Installation	✓	✓
Allow Modifying Application In Settings		✓
Allow Installing Applications	✓	✓
Allow Uninstalling Applications	✓	✓
Allow Disabling Application Verification	✓	✓
Allow Whitelist Accessibility Services	✓	✓
Sync and Storage		
Allow USB Debugging	✓	✓
Allow USB Mass Storage		✓
Allow USB File Transfer		✓

Feature	Work Profile mode	Work Managed Device mode
Allow Backup Service (Android 8.0+)		
Network		
Allow Wi-Fi changes		✓
Allow Bluetooth		✓
Allow Bluetooth Contact Sharing (Android 8.0+)		✓
Allow Outgoing Bluetooth Connections		✓
Allow All Tethering		✓
Allow VPN Changes		✓
Allow Mobile Network Changes		✓
Allow NFC	✓	✓
Allow Managed Wi-Fi Profile Changes		✓
Location Services		
Allow No Location Access		✓
Allow Location Access		✓
Allow GPS Location Only		✓
Allow Battery Saving Location Updates Only		✓
Allow High Accuracy Location Only		✓
Work and Personal		
Allow Pasting Clipboard Between Work and Personal Apps	✓	
Allow Works Apps To Access Documents From Personal Apps	✓	
Allow Personal Apps to Access Documents From Work Apps	✓	
Allow Personal Apps to Share Documents With Work Apps	✓	
Allow Work Apps to Share Documents With Personal Apps	✓	
Allow Work Contact's Caller ID Info to Show in Phone Dialer	✓	
Allow Work Widgets To Be Added To Personal Home Screen	✓	
Allow Work Contacts in Personal Contacts App (Android 7.0+)	✓	