

Android Platform

VMware Workspace ONE UEM 1903



vmware®

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

<https://docs.vmware.com/>

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

docfeedback@vmware.com

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

Copyright © 2019 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

1 Overview 6

- [Integrating Workspace ONE UEM with Android](#) 6
- [Deployment Requirements for Android](#) 6
- [Network Requirements for Android](#) 8
- [Enrollment Restrictions for Android](#) 9
- [Key Terms for Android](#) 9
- [Understanding Android Device Modes](#) 10

2 Registering Android with Workspace ONE UEM 13

- [Register Android EMM with Managed Google Play Account](#) 14
- [Register Android EMM with Managed Google Domain \(G-Suite Customers\)](#) 14
 - [Setup Google Service Account](#) 15
 - [Setup Google Admin Console](#) 16
 - [Generate EMM Token](#) 17
 - [Upload EMM Token](#) 17
 - [Setup Users](#) 18
- [Unbind Domain from AirWatch](#) 20

3 Android Device Enrollment Overview 21

- [Devices & Users / Android / Android EMM Registration](#) 21
- [Device Protection for Android Devices](#) 22
- [Autodiscovery Enrollment](#) 23
 - [Configure Autodiscovery Enrollment from a Child Organization Group](#) 23
 - [Configure Autodiscovery Enrollment from a Parent Organization Group](#) 24
- [Configuring Work Managed Device Enrollment](#) 24
 - [Enroll Work Managed Device with AirWatch Relay](#) 27
 - [Enroll Android Devices Using VMware Workspace ONE Intelligent Hub Identifier](#) 37
 - [Enroll Android Device Mode Using a QR Code](#) 37
 - [Enroll Android Device Using Zero Touch Portal](#) 39
- [Configuring Corporate Owned Personally-Enabled Enrollment](#) 43
- [Enroll Android Device into Work Profile Mode](#) 45
- [Zebra Stage Now](#) 46

4 Android Profiles Overview 49

- [Passcode Profile \(Android\)](#) 51
 - [Enforce Passcode Settings \(Android\)](#) 51
 - [Configure Lockscreen Overlay \(Android\)](#) 53
- [Enforce Chrome Browser Settings \(Android\)](#) 55

- Chrome Browser Settings Matrix (Android) 57
- Restrictions Profile (Android) 59
 - Enforce Restrictions (Android) 59
- Enable Exchange Active Sync (Android) 60
- Auto Update Profile 61
- Credentials (Android) 62
 - Deploy Credentials (Android) 62
- Create Custom Messages 63
- Application Control (Android) 63
 - Configure Application Control (Android) 63
- Configure Proxy Settings (Android) 64
- Enable System Updates (Android) 64
- Wi-Fi Profile (Android) 65
 - Configure Wi-Fi Access (Android) 65
- Configure VPN (Android) 66
 - Configure Per-App VPN (Android) 67
- Set Permissions (Android) 68
- Configure Single App Mode (Android) 69
 - Best Practices for Single App Mode (Android) 69
- Set Date/Time 70
- Create Workspace ONE Launcher Profile (Android) 71
- Configure Firewall Rules (Android) 72
- Configure APN Profile 73
- Enterprise Factory Reset Protection 74
 - Configure Enterprise Factory Reset Protection(Android) 74
- Configure Zebra MX Profile (Android) 74
- Using Custom Settings (Android) 76

5 Shared Devices 78

- Configure Android for Shared Device Use 79
- Configure Shared Devices 80
- Define the Shared Device Hierarchy 81
- Log In and Log Out of Shared Android Devices 82

6 Application Management for Android 83

- Workspace ONE Intelligent Hub for Android 84
- Internal Apps with Android 86
- Add Public Applications for Android 86
- Assign Applications for Android 87
- Enable Play for Work 89
- Integration Features 89

- [Samsung Native Email with Android](#) 90
- [Set up App Configuration for Samsung Email](#) 90

7 Android Device Management Overview 92

- [Device Management Commands \(Android\)](#) 92
- [Device Details Apps Tab](#) 93
- [Android Updates Overview](#) 93
 - [Publish Firmware Updates \(Android\)](#) 93
 - [Samsung Enterprise Firmware Over The Air \(EFOTA\) Updates](#) 94
- [SafetyNet Attestation](#) 95
- [Enable SafetyNet Attestation](#) 96
- [Specific Profiles Features for Android](#) 96
- [Specific Restrictions for Android](#) 98

Overview

This chapter includes the following topics:

- [Integrating Workspace ONE UEM with Android](#)
- [Deployment Requirements for Android](#)
- [Network Requirements for Android](#)
- [Enrollment Restrictions for Android](#)
- [Key Terms for Android](#)
- [Understanding Android Device Modes](#)

Integrating Workspace ONE UEM with Android

VMware 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.

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.

Deployment Requirements for Android

Before deploying Android devices, 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)

Note : Workspace ONE UEM supports product provisioning on Android 4.1+ devices. For more information, see the VMware AirWatch Product Provisioning for Android Guide.

Android 6.X.X

Android 7.X.X

Android 8.X.X

Android 9.X.X

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 device

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 Workspace ONE Intelligent Hub 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.

Network Requirements for Android

End-user devices must be able to reach certain endpoints for access to apps and services. The Network Requirements for Android is a list of known endpoints for current and past versions of enterprise management APIs.

Table 1-1. Firewall Rules

Destination Host	Ports	Purpose
play.google.com, android.com, google-analytics.com, googleusercontent.com, *gstatic.com, *gvt1.com*, *ggpht.com, dl.google.com, dl-ssl.google.com	TCP/443 TCP, UDP/5228-5230	Google Play and updates gstatic.com, googleusercontent.com - contains User Generated Content (e.g. appicons in the store) *gvt1.com, *ggpht, dl.google.com, dl-ssl.google.com, android.clients.google.com - Download apps and updates, PlayStore APIs
*.googleapis.com	TCP/443	EMM/Google APIs/PlayStore APIs
accounts.google.com, accounts.google.[country]	TCP/443	Authentication For accounts.google.[country], use your local top-level domain for [country]. For example, for Australia use accounts.google.com.au, and for United Kingdom use accounts.google.co.uk.
fcm.googleapis.com, fcm-xmpp.googleapis.com	TCP/443, 5228-5230	Firebase Cloud Messaging (e.g. Find My Device, EMM Console <-> DPC communication, like pushing configs)
fcm-xmpp.googleapis.com, gcm-xmpp.googleapis.com	TCP/5235, 5236	When using persistent bidirectional XMPP connection to FCM and GCM servers
pki.google.com, clients1.google.com	TCP/443	Certificate Revocation list checks for Google-issued certificates
clients2.google.com, clients3.google.com, clients4.google.com, clients5.google.com, clients6.google.com	TCP/443	Domains shared by various Google backend services such as crash reporting, Chrome Bookmark Sync, time sync (tlsdate), and many others
omahaproxy.appspot.com	TCP/443	Chrome updates
android.clients.google.com	TCP/443	CloudDPC download URL used in NFC provisioning
connectivitycheck.android.com www.google.com	TCP/443	Connectivity check prior to CloudDPC v470 Android connectivity check starting with N MR1 requires https://www.google.com/generate_204 to be reachable, or for the given WiFi network to point to a reachable PAC file.

This list is not exhaustive and is subject to change.

Enrollment Restrictions for Android

Enrollment restrictions allows you to provision enrollment such as restricting enrollment to known users, user groups, and number of enrolled devices allowed.

You can create enrollment restrictions based on Android manufacturer and model to ensure only approved devices are

These options are available by navigating to **Groups & Settings > All Settings > Devices & Users > General > Enrollment** and choosing the **Restrictions** selecting the Restrictions tab allows you to customize enrollment restriction policies by organization group and user group roles.

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. For more information, see [Understanding Android Device Modes](#) .
- **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 Workspace ONE Intelligent Hub 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 Workspace ONE Intelligent Hub and grants the Workspace ONE Intelligent Hub full control of the entire device. For more information, see [Understanding Android Device Modes](#) .
- **Corporate Owned Personally Enabled** – Corporate Owned Personally (COPE) refers to company-owned devices, similar to Work Managed Device, but is provisioned with a Work Profile which leverages both personal and corporate use. For more information, see [Understanding Android Device Modes](#)
- **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 admin's 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) applications.

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. **Corporate Owned Personally-Enabled (COPE)** mode refers to company-owned devices, similar to Work Managed Device, but is provisioned with a Work Profile which uses both personal and corporate use.

Work Profile Mode Functionality

Applications in the Work Profile are differentiated by a red briefcase icon, called badged applications, and are shown in a unified launcher with the user's personal applications. 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 application is only installed once with business data stored separately from personal data.

The Workspace ONE Intelligent Hub is badged and exists only within the Work Profile data space. There is no control over personal applications and the Workspace ONE Intelligent Hub does not have access to personal information.

There are a handful of system applications 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 applications like Work Profile mode.
- Users have access to various pre-loaded applications upon activation of the device. Additional applications can only be approved and added through the Workspace ONE UEM console.
- The Workspace ONE Intelligent Hub 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.

Corporate Owned Personally Enabled (COPE) Mode

When devices are enrolled using COPE mode, you still control the entire device. The unique capability with COPE mode is that it allows you to enforce two separate sets of policies, such as restrictions, for the device and inside a Work profile.

COPE mode is only available on Android 8.0+ devices. If you enroll Android devices below Android 8.0, the device automatically enrolls as Work Managed Device.

There are some caveats to consider when enrolling devices into COPE mode:

- Pin Based encryption and AirWatch Single Sign On by using SDK is not supported for Corporate Owned Personally Enabled devices. A work passcode can be enforced to ensure that the use of work applications requires the use of a passcode.
- Single user staging and Multi-user staging are not supported for COPE enrollments.
- Internal applications (hosted in AirWatch) and public applications deployed to COPE devices are shown in the application Catalog within the Work Profile.
- Similar to Work Profile only enrollments, Corporate Owned Personally Enabled devices provide users the option to disable the Work Profile (for example, if the user is on vacation). When the Work Profile is disabled, the work applications no longer present notifications and cannot be launched. The status (Enabled or Disabled) of the Work Profile is presented to the admin on the Device Details page. When the Work Profile is disabled, the latest application and profile information cannot be retrieved from the Work Profile.
- The Workspace ONE Hub exists in the Work Managed and the Work Profile sections of the Corporate Owned Personally Enabled device. By existing both inside and outside the Work Profile, management policies can be applied within the Work Profile and the entire device. However, the Workspace ONE Hub is only visible within the Work Profile.
- When push notifications are sent to the device, the Workspace ONE Hub outside the Work Profile is temporarily available for the user to view messages, ensuring that critical messages reach the user even if the Work Profile is temporarily disabled.

- Assigned profiles can be viewed through the Workspace ONE Hub in the Work Profile.
- Compliance policies for application management (such as block/ remove applications) are only supported for applications within the Work Profile. Applications can be blacklisted on the device (outside the Work Profile) by using Application Control profiles.
- An enterprise wipe will factory reset Corporate Owned Personally Enabled devices.
- Product Provisioning is not supported on COPE enrollments.

Registering Android with Workspace ONE UEM

2

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.

This chapter includes the following topics:

- [Register Android EMM with Managed Google Play Account](#)
- [Register Android EMM with Managed Google Domain \(G-Suite Customers\)](#)

- [Unbind Domain from AirWatch](#)

Register Android EMM 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.

Prerequisites

If 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

Procedure

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

What to do next

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.

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

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.

Prerequisites

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

Procedure

- 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:
 - a Generate Token: Obtain your enterprise token by registering your enterprise domain with Google.
 - b Upload Token: Enter the EMM Token into the Android setup wizard.
 - c 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.

Procedure

- 1 Navigate to the [Google Cloud Platform- Google Developers Console](#).
- 2 Sign in with your Google credentials.

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.
- 8 Navigate to **APIs & Services > Credentials > Create Credentials > Service Account Key > New Service Account**.
- 9 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.
- 10 Use the drop-down menu to select the **Role > Project** as **Owner**.

- 11 Select the **Key Type** as **P12**.
- 12 Select **Create**. The identity certificate gets automatically created and downloaded to your local drive. Be sure to save your identity certificate and password for when you upload the certificate into the Workspace ONE UEM console.
- 13 Select **Manage service accounts** from the **Service Account Keys** list which opens the Service Accounts page.
- 14 Select the menu button (three vertical dots) beside your service account and select **Edit**.
- 15 Select **Enable G Suite Domain-wide Delegation**.
- 16 Enter a **Product name** in order change settings for G Suite Domain. Consider using AndroidEMM-CompanyName as the naming convention.
- 17 Select **Save**.
- 18 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](#)

What to do next

For steps to configure the Google Admin Console, see [Setup Google Admin Console](#)

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).

Procedure

- 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.

Procedure

- 1 Complete the following fields:
 - a **About You** – Enter your admin contact information.
 - b **About Your Business** – Fill out your company information.
 - c **Your Google Admin Account** – Create a Google admin account.
 - d **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. If you encounter problems during this step, refer to Google support using the number and unique PIN listed.
- 5 Copy the generated EMM token and select **Finish**.

What to do next

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.

Procedure

- 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.

- 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. This final step in the Android EMM Registration wizard 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.

The format for the user name is `username@<your_enterprise_domain>.com`.

Procedure

- 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.

Procedure

- 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.

Procedure

- 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.

Procedure

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

Android Device Enrollment Overview

3

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 Workspace ONE Intelligent Hub provides a single resource to enroll a device and provides device and connection details. Hub-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 three enrollment options: Work Managed Device, Work Profile, and Corporate Owned Personally-Enabled enrollment with unique enrollment options for each mode.

Android (Legacy) deployment allows you to enroll Android devices with the Workspace ONE Intelligent Hub as the device administrator if you've opted out of Google registration. For enrolling devices using Android (Legacy) deployment, see [Android \(Legacy\) Enrollment Overview](#) in the [Workspace ONE Android \(Legacy\) documentation](#).

This chapter includes the following topics:

- [Devices & Users / Android / Android EMM Registration](#)
- [Device Protection for Android Devices](#)
- [Autodiscovery Enrollment](#)
- [Configuring Work Managed Device Enrollment](#)
- [Configuring Corporate Owned Personally-Enabled Enrollment](#)
- [Enroll Android Device into Work Profile Mode](#)
- [Zebra Stage Now](#)

Devices & Users / Android / Android EMM Registration

Android EMM Registration 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.

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 (non-G suite only)	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.
Fully-Managed Device Enrollments	Choose whether enrolled devices will use Work Managed Device or Corporate Owned Personally Enabled mode. <ul style="list-style-type: none"> ■ Work Managed Device is a fully-managed device that will be locked down providing employees with access to corporate apps only and no access to personal apps through the Google Play Store. ■ Corporate Owned Personally Enabled provides all the benefits of complete device management, but employees will receive a Work Profile to access corporate apps and will still have access to their personal Google Play Store outside of the Work Profile. This enrollment type is only available on Android 8.0+.

For more information on Android Device modes, see Understanding Android Device Modes available through docs.vmware.com.

Enrollment Restrictions

Setting	Description
Define the enrollment method for this Organization Group	Select whether to Always use Android , or Always Use Android (Legacy) , Define assignment group that use Android . If you select Define Assignment Group that use Android , all unassigned devices default to use 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 For more information on Smart Groups, see Smart Groups Overview in the Mobile Device Management (MDM) documentation.

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 Workspace ONE Intelligent Hub 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.

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.

Force users to select a Group ID during enrollments.

Procedure

- 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.

Procedure

- 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.workspaceone.com/set-discovery-password> to set the password for Auto Discovery service. Once you have registered and selected **Set Identity**, the **HMAC Token** auto-populates. 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, and also can **Replace** and **Clear** these existing certificates.
- 3 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 select the cert on your device.
- 4 Select **Save** to complete an autodiscovery setup.

What to do next

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.

Configuring 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 a 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 [Chapter 2 Registering Android with Workspace ONE UEM](#) 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 earlier versions, then enroll Android using the Legacy enrollment method in the VMware AirWatch Android (Legacy) Platform Guide.

Enrolling with 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 Workspace ONE Intelligent Hub for Android.
- Silently set the Workspace ONE Intelligent Hub 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 Workspace ONE Intelligent Hub. 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](#).

Enrolling with 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 Workspace ONE Intelligent Hub. The user only has to enter server details, user name, and password. For AirWatch Identifier enrollment, see [Enroll Android Devices Using VMware Workspace ONE Intelligent Hub Identifier](#).

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.

For more information on Single-User Device Staging, see [Stage a Single-User Device](#) in the Mobile Device Management (MDM) documentation.

Enrolling with 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 Android Device Mode Using a QR Code](#).

Enrolling with Zero Touch

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 Workspace ONE Intelligent Hub is automatically downloaded and enrollment details are automatically passed to enroll the device with no user interaction.

Zero Touch enrollment is supported by a limited number of mobile carriers and OEMs. Customers 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 Android Device Using Zero Touch Portal](#)

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 [Enroll Android Device with AirWatch Relay for Android 6.0+](#)

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 [Enroll Work Managed Device with AirWatch Relay for Android 5.0 and Android 6.0](#).

Enroll Android Device with AirWatch Relay for Android 6.0+

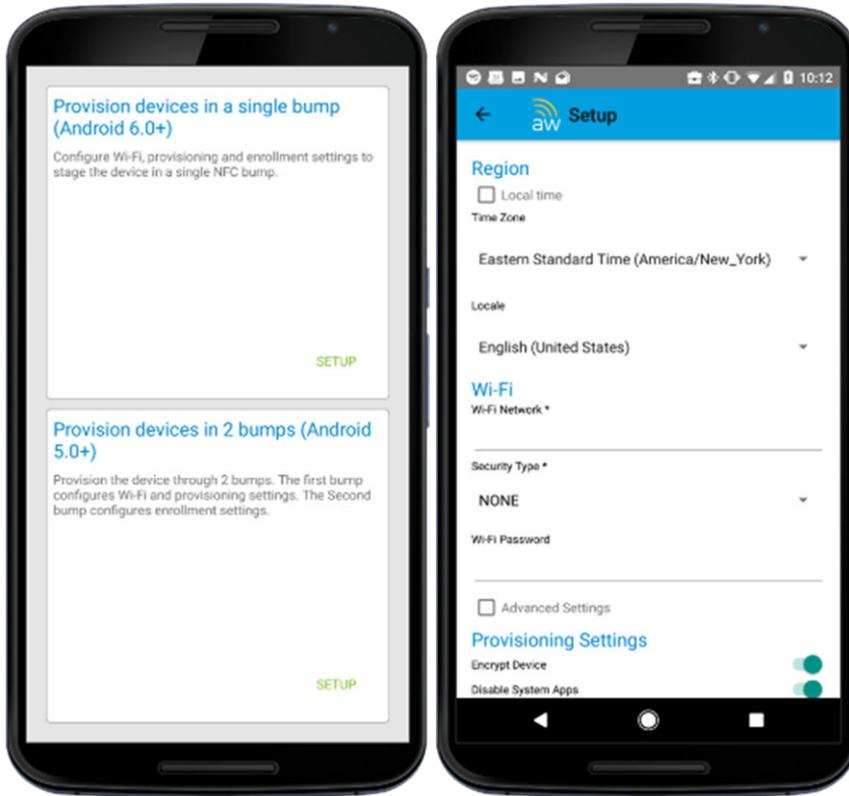
For Android 6.0+, the AirWatch Relay app provides a single bump option which configures region, Wi-Fi, provisioning settings, and enrollment settings in the single bump.

Procedure

- 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
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 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.
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 Workspace ONE Intelligent Hub from disabling system apps during set up.
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.
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.

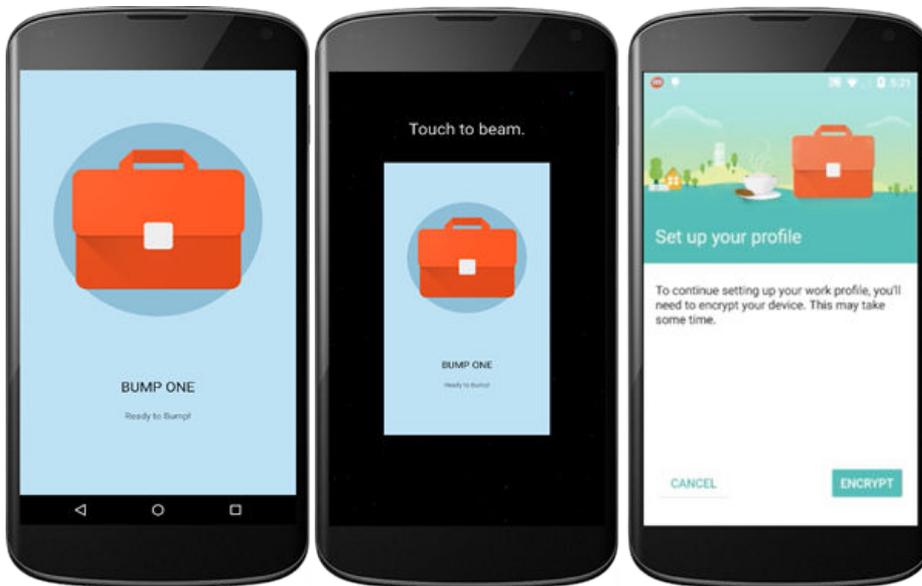
- 6 Perform the NFC bump by touching the parent and child device back to back. The child device should be in factory reset mode which will ensure the device is not being used for personal use.

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 users 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.

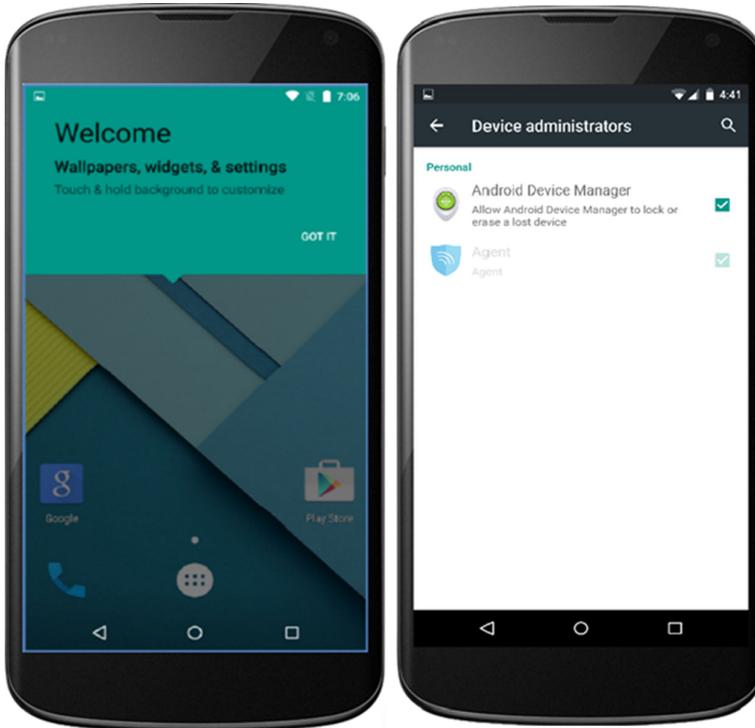
- 7 Tap **Touch to Beam** on the parent device with the devices still back to back.
- 8 Tap **Encrypt** on the child device with the devices still back to back.

The child device will automatically:

- a Connect to the Wi-Fi network defined in the AirWatch Relay app.
- b Download and silently install the Workspace ONE Intelligent Hub.
- c Set the Workspace ONE Intelligent Hub 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 Workspace ONE Intelligent Hub 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.

Alternatively, you can choose to enroll the child devices manually and skip the second NFC bump steps outlined below. You will need to enter enrollment details manually on each device. For additional enrollment flows, see [Additional Enrollment Workflows](#) in the [Mobile Device Management \(MDM\)](#) documentation.

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.

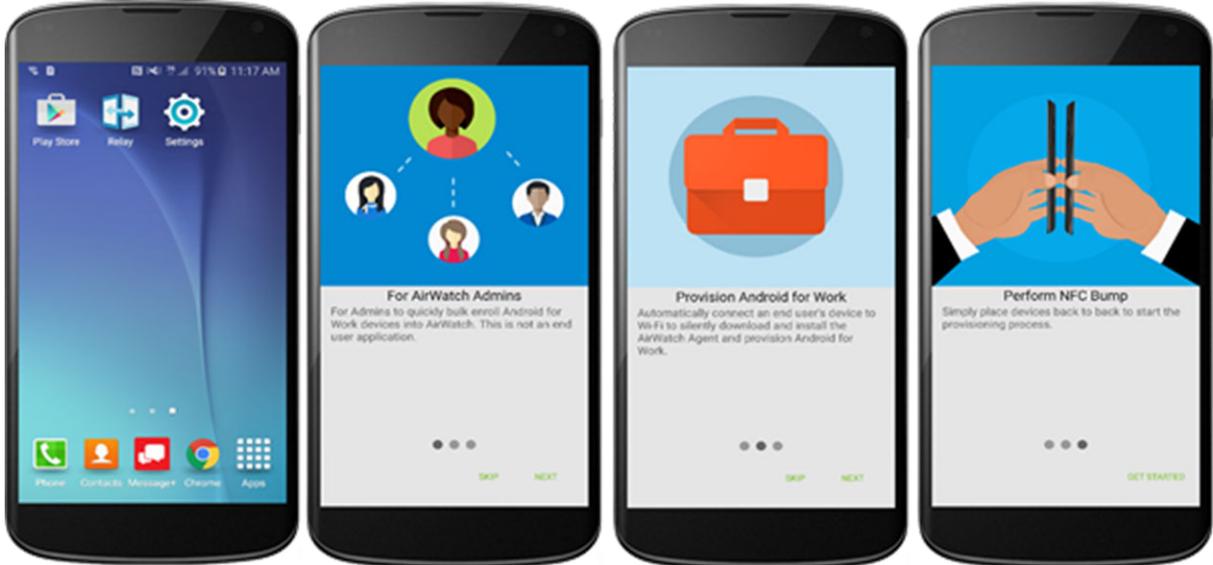
Navigate to **Devices > Details View > Summary** and view the **Security** section of the page to view the status. A green check verifies Android activation.

Enroll Work Managed Device with AirWatch Relay for Android 5.0 and Android 6.0

For Android v5.0 and Android v6.0, the AirWatch Relay app provides a 2 bump option that configures region, Wi-Fi, provisioning settings, and enrollment settings.

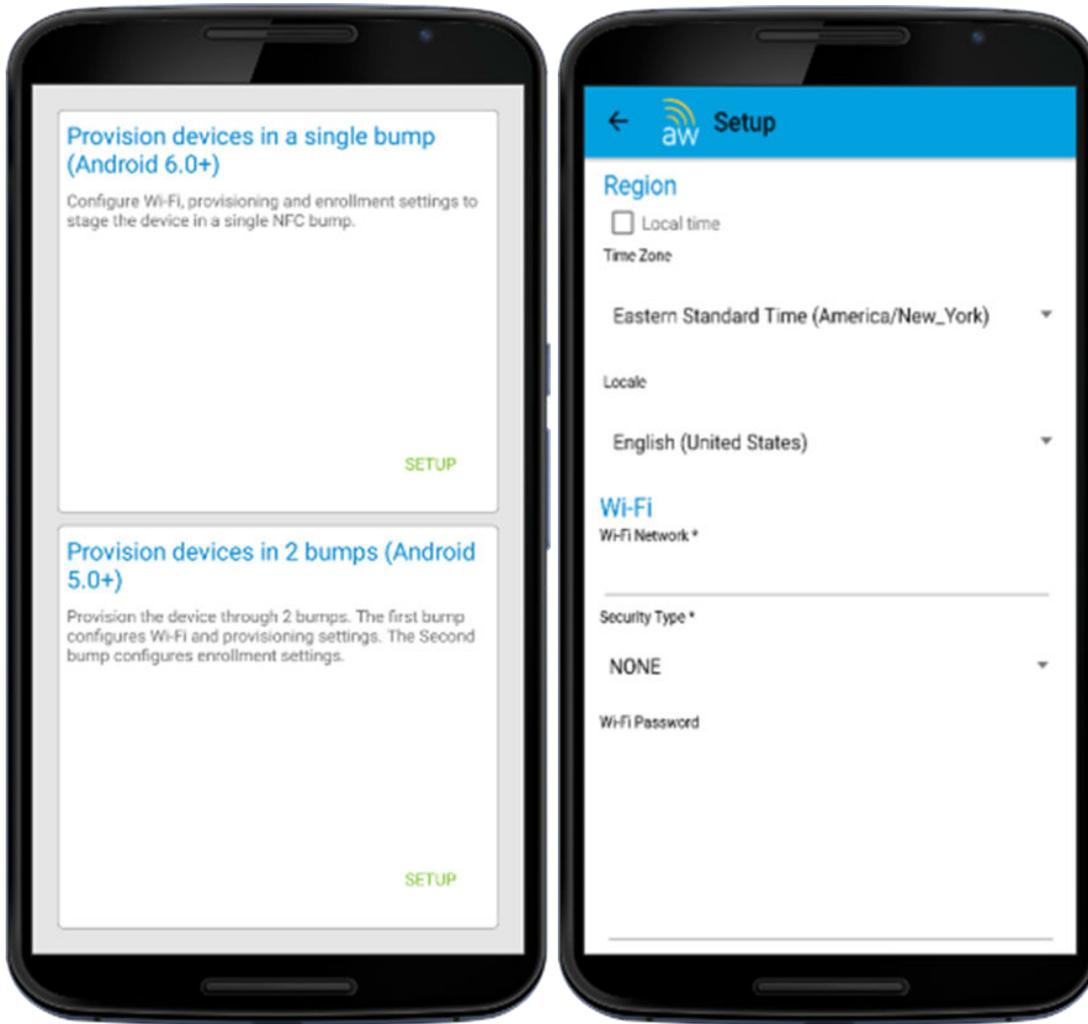
Procedure

- 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 v5.0- 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 [Enroll Android Device with AirWatch Relay for Android 6.0+](#).



4 From the parent device, define the following settings:

Setting	Description
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 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.
Skip Device Encryption Requirement for Provisioning	Enable this field to indicate that device encryption can be skipped as part of Work Managed device provisioning.
Do Not Disable System Apps During Provisioning	Enable this field to skip the Workspace ONE Intelligent Hub from disabling system apps during set up.

5 Tap **Ready** from the parent device to perform bump one.

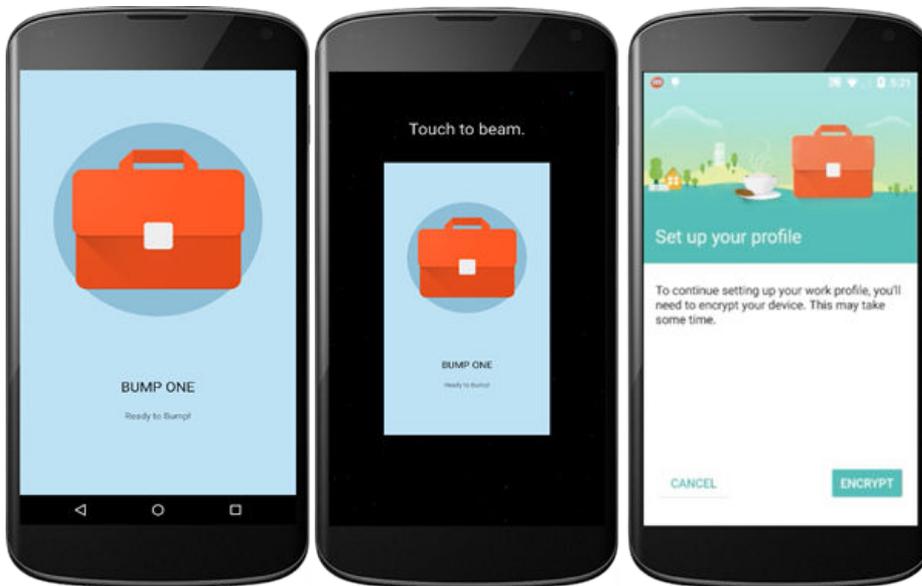
- 6 Perform the first NFC bump by touching the parent and child device back to back. The child device should be in factory reset mode which will ensure the device is not being used for personal use.

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 users 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.

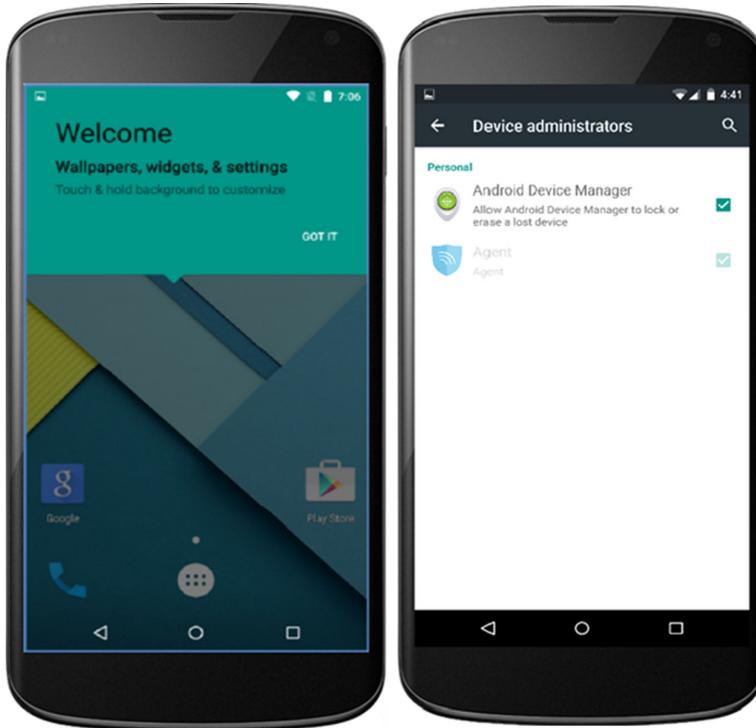
- 7 Tap **Touch to Beam** on the parent device with the devices still back to back.
- 8 Tap **Encrypt** on the child device with the devices still back to back.

The child device will automatically:

- Connect to the Wi-Fi network defined in the AirWatch Relay app.
- Download and silently install the Workspace ONE Intelligent Hub.
- Set the Workspace ONE Intelligent Hub 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 Workspace ONE Intelligent Hub listed as the device administrator. End users will not be able to deactivate this setting.

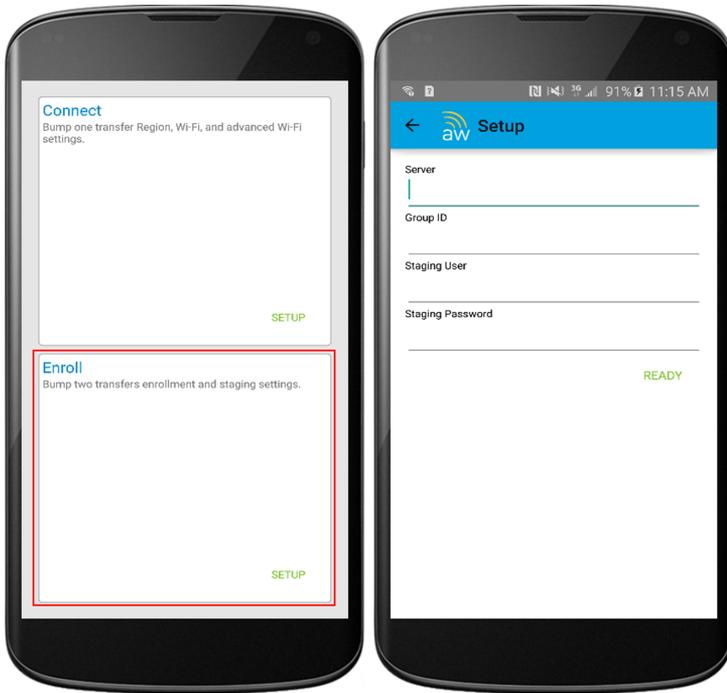


You will also notice on the device homescreen the pre-downloaded apps allowed. Any other applications will need to be approved by the administrator from the Workspace ONE UEM console .

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.

Alternatively, you can choose to enroll the child devices manually and skip the second NFC bump steps outlined below. You will need to enter enrollment details manually on each device. For additional enrollment flows, please see Additional Enrollment Workflows in the Mobile Device Management (MDM) documentation.

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.

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 Workspace ONE Intelligent Hub.



- 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).

What to do next

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. A green check verifies Android activation.

Enroll Android Devices Using VMware Workspace ONE Intelligent Hub Identifier

During Work Managed Device and Corporate Owned Personally enabled (COPE) 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 UEM as your EMM provider.

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

Procedure

- 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#hub” 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.

If the identifier is entered incorrectly, you are prompted to re-enter it.
- 4 Tap **Install** to begin configuration of the Workspace ONE Intelligent Hub to the device. The Hub will automatically open after install is complete.
- 5 Choose the **Authentication Method** to continue enrollment:
 - a Select **Email Address** if you have configured Autodiscovery. In addition, you may be prompted to select your Group ID from a list.
 - b Choose **Server Details** and enter Server, Group ID, and user credentials.
 - c Choose **QR Code** if you have created a QR Code in the UEM console.
- 6 Follow the remaining prompts to complete enrollment.
- 7 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.
- 8 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 Android Device Mode Using a QR Code

The QR code enrollment method sets up and configures Work Managed Device and Corporate Owned Personally Enabled (COPE) modes 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.

Prerequisites

Use the Workspace ONE UEM console to create the QR code before starting enrollment. Alternatively, you can use any online QR Code generator, such as Web Toolkit Online, to create your QR code.

To use the UEM console to create the QR code, see the Enrollment Configuration Wizard in Staging & Provisioning. For more information on the Enrollment Configuration Wizard, see, [Generate a QR Code Using the Enrollment Configuration Wizard](#).

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.

Procedure

- 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.
 - a For Android 8.0+ devices, proceed to step 2 in order to download the QR Code reader.
 - b For Android 9.0+ devices, the camera will open automatically after you complete the six taps.
- 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. For Android 9.0+ devices, use the QR code option on the camera to scan. You can use any online QR Code generator, such as Web Toolkit Online, to create your unique QR code. For more information, see [Configuring Work Managed Device Enrollment](#).
- 4 The setup wizard automatically downloads the Workspace ONE Intelligent Hub 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.

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

Generate a QR Code Using the Enrollment Configuration Wizard

After selecting QR Code enrollment in the Enrollment Configuration wizard, create a QR Code to scan with your Android 7.0 or later devices to stage the device quickly. The wizard simplifies the staging configuration process.

Procedure

- 1 After taking note of the prerequisites, select **Configure** to begin.

- You can connect the device to **Wi-Fi** prior to enrollment by enabling the Wi-Fi toggle. This enabling action displays the following options.

Setting	Description
SSID	Enter the Service Set Identifier, more commonly known as the name of the Wi-Fi Network.
Password	Enter the Wi-Fi password for the entered SSID.

- Select **Next**.
- Select the Workspace ONE Intelligent Hub to push to devices during staging. The default selection is Use latest Workspace ONE Intelligent Hub.

If you do not have an Workspace ONE Intelligent Hub added, select **Hosted on an external URL** and enter the address in the **URL** text box to point to an externally-hosted Workspace ONE Intelligent Hub Package.

- Select **Next**.
- Set the **Enrollment Details** settings. To use token-based authentication, leave both options disabled.

Setting	Description
Organization Group	Enable and select the organization group the QR Code staging package uses.
User name	Enable to configure login credentials. Enter the Workspace ONE UEM account user name.
Password	Enter the corresponding password.

- Select **Next**.
- The **Summary** page allows you to **Download File** of the PDF. You can also **View PDF** to see a preview of your **QR Code Format** selections.

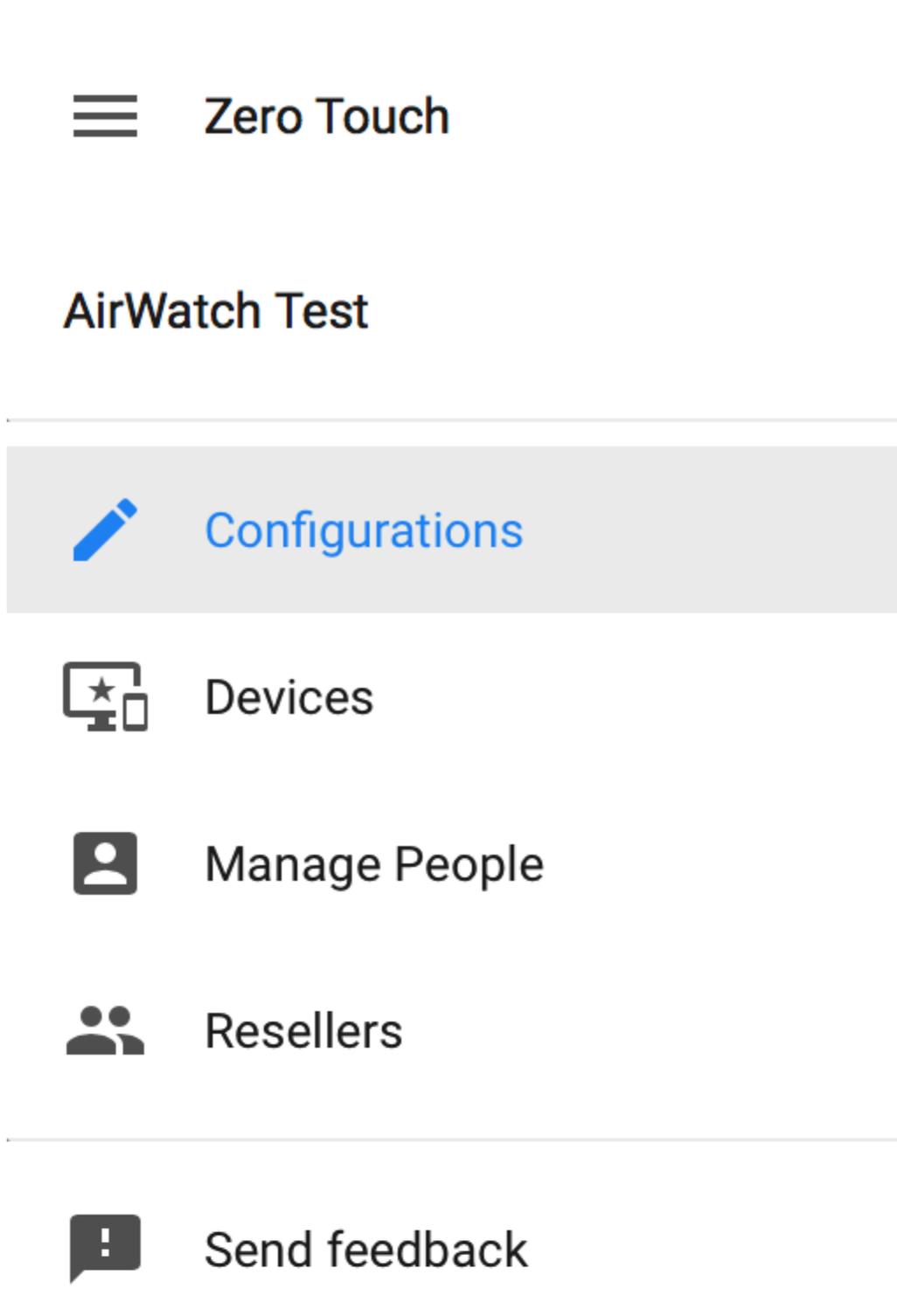
Enroll Android Device Using Zero Touch Portal

In the Zero Touch Portal, add enrollment configurations that should be applied on the device as soon as the Workspace ONE Intelligent Hub is downloaded.

Note Zero Touch enrollment is only supported on Android 8.0 (Oreo) devices. For Samsung devices, use Knox Mobile Enrollment.

Procedure

- 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 'Workspace ONE Intelligent Hub'. This will ensure that the Workspace ONE Intelligent Hub is downloaded as part of factory setup
DPC Extras	<p>Enter the enrollment credentials that will be configured in the Workspace ONE Intelligent Hub. You can include the Workspace ONE UEM console Server URL, Group ID, enrollment username, and password.</p> <p>End user provisions device: In this scenarios, exclude the username and password and the user enters them at device setup when prompted.</p> <pre>{ "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": { "serverurl": "https://airwatch.console.com", "gid": "groupID"} }</pre> <p>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.</p> <pre>{ "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": { "serverurl": "https://airwatch.console.com", "gid": "groupID", "un":"username", "pw":"password" } }</pre>
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 Workspace ONE Intelligent Hub.

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.

Zero Touch

AirWatch Test



Configurations



Devices



Manage People



Resellers

Configuring Corporate Owned Personally-Enabled Enrollment

Android Corporate Owned Personally-Enabled(COPE) mode gives Workspace ONE UEM control of the entire device while still deploying a Work profile for the user to use the device as a personal device. COPE is a hybrid between Work Profile and Work Managed Device modes.

There are several ways to enroll COPE 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 [Chapter 2 Registering Android with Workspace ONE UEM](#) to complete registration.

Android 8.0+ is required to use COPE deployment on your device fleet. If you attempt to enroll a device that is not running Android 8.0, the device will automatically be enrolled as a Work Managed device. For information on Work Managed Device enrollment, see [Configuring Work Managed Device Enrollment](#).

If the Android devices you are using are on a closed network, unable to communicate with Google Play, or are running Android 7.0 or lower, then enroll Android using the Legacy enrollment method in the VMware AirWatch Android (Legacy) Platform Guide.

Enroll with 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 Workspace ONE Intelligent Hub for Android.
- Silently set the Workspace ONE Intelligent Hub 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 a COPE device.

The NFC bump process depends on the Android OS version . Since COPE is only supported on Android 8.0+ only, enrollment with AirWatch relay will perform a single bump to connect and enroll child devices in one step.

For AirWatch Relay enrollment, see [Enroll Android Device with AirWatch Relay for Android 6.0+](#)

Enroll with AirWatch Identifier

The AirWatch Identifier enrollment method is a simplified approach to enrolling COPE enabled 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 Workspace ONE Intelligent Hub. The user only has to enter server details, user name, and password. For AirWatch Identifier enrollment, see [Enroll Android Devices Using VMware Workspace ONE Intelligent Hub Identifier](#).

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.

For more information on Single-User Device Staging, see [Stage a Single-User Device](#).

Enroll with QR Code

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 generate the QR Code using the Enrollment Configuration Wizard in the Workspace ONE UEM console. For more information, see [Generate a QR Code Using the Enrollment Configuration Wizard](#).

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 QR Code 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 Android Device Mode Using a QR Code](#).

Enroll with Zero Touch

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 Workspace ONE Intelligent Hub is automatically downloaded and enrollment details are automatically passed to enroll the device with no user interaction.

Here are some prerequisites to consider:

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 Android Device Using Zero Touch Portal](#).

Note Zero Touch enrollment is only supported on Android 8.0 (Oreo) devices. For Samsung devices, use Knox Mobile Enrollment.

Enroll Android Device into Work Profile Mode

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

Use the following instructions to install the Workspace ONE Intelligent Hub and authenticate users based on the enrollment flow.

Procedure

- 1 Download and install the Workspace ONE Intelligent Hub from the Google Play Store.
- 2 Launch the Workspace ONE Intelligent Hub.
 - a If you have configured email autodiscovery, then the Workspace ONE Intelligent Hub prompts you for your email address. In addition, you may be prompted to select your Group ID from a list.
 - b 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 accept the settings. The Workspace ONE Intelligent Hub will close after accepting the encryption settings. Tap the **Encryption Complete** notification to return to the Workspace ONE Intelligent Hub to continue enrollment.

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**.
- 10 To continue with **Directory Service Sync**:
 - a Enter your **Password** and tap **Next**.
 - b Select **Continue**.
 - c Select **Exit**.
- 11 To follow the **SAML** enrollment flow:
 - a Enter the **User Name** and **Password** and tap **Login**. The user will be redirected to the Workspace ONE Intelligent Hub.

If successful, the Work Profile is configured for the device and displays the Workspace ONE Intelligent Hub settings page. The device is ready for use according to Android settings for the Work Profile.

Zebra Stage Now

The Stage Now staging client is Zebra's next generation Android solution for staging Zebra devices and preparing them for production use.

Workspace ONE UEM supports Stage Now given the following conditions and limitations.

For more information on Zebra Mobility, see [Zebra Mobility Extensions \(MX\)](#) and [Full MX Feature Matrix](#).

If you plan to enroll Zebra devices in Work Managed Device Mode with a Stage Now barcode, take the following steps.

Prerequisites

- Zebra devices must be running Android Nougat with MX version 7.1 or later.

- If you want to enroll your Zebra devices using a Stage Now barcode, you must have Android Hub version 8.2 or later uploaded to the console as the Workspace ONE Intelligent Hub Package.
- Zebra devices running Android Marshmallow and below must continue to use Rapid Deployment as the default staging client.
- Relay Servers set to passive mode only are supported. Relay servers in active mode are not supported and do not function with the Stage Now client.
- Ensure the **Stage Now URL** setting, found in **Groups & Settings > All Settings > System > Advanced > Site URLs**, is set to the appropriate URL.
 - If your on premises environment is configuring your own Stage Now server, then place your custom URL in this field.
 - If your on premises environment is not configuring your own Stage Now server, then you simply must open your networks to allow access to the URL listed here.
 - SaaS environments do not need to change this text box.
- There must be no Google account present on the device while attempting Stage Now enrollment in Work Managed Mode.

Procedure

- 1 Use the Organization Group selector to select the OG you want to configure for your Android devices.
- 2 Navigate to **Groups & Settings > All Settings > Devices & Users > Android > Android EMM Registration** and select the **Enrollment Restrictions** tab.
- 3 Complete the following settings.

Setting	Description
Current Setting	Select Override to affect changes to the OG you selected in step 1.
Define devices that will use Android (Legacy) in this organization group	<p>This setting determines how this OG treats Android (Legacy) devices. Select from among the following settings.</p> <p>Don't use Android (Legacy) – This setting enables the Device Owner Mode slider on the Generate Stage Now Barcode screen and makes it uneditable. This forces all Android (Legacy) devices that enroll in this OG to be in Device Owner Mode (or Work Managed Device Mode).</p> <p>Always use Android (Legacy) – This setting disables the Device Owner Mode slider from the Generate Stage Now Barcode screen and makes it uneditable. This forces all Android (Legacy) devices that enroll in this OG to be in Device Admin Mode.</p> <p>Exempt smart groups from Android (Legacy) – This setting enables the Device Owner Mode slider on the Generate Stage Now Barcode screen and makes it editable, allowing you the choice of enrolling Android devices in Device Owner Mode (Work Managed Device Mode) or enrolling them in Device Admin Mode.</p>

- 4 Direct your end-user to take the following steps once they take possession of the newly-enrolled device.
 - a Start the device from a "factory settings" state.
 - b Ensure there is no Google account on the device.
 - c Proceed through the Setup Wizard or scan the "skip setup wizard" barcode provided by Zebra.
 - d Open the Stage Now app.
 - e Scan the barcode.

The device is automatically enrolled into Work Managed mode.

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). Select the Android profile option if you have completed the Android EMM Registration. 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 [Chapter 2 Registering Android with Workspace ONE UEM](#)

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 Workspace ONE Intelligent Hub 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 Workspace ONE Intelligent Hub the Work Managed device. The Workspace ONE Intelligent Hub 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 \(Android\)](#).
- Specify and control how, when and where your employees use their devices. For more information, see [Restrictions Profile \(Android\)](#).

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 \(Android\)](#).
- Take administrative actions when a user installs or uninstalls certain applications. For more information, see [Application Control \(Android\)](#).

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 \(Android\)](#).
- Manage how Android OS update notifications and the actual updates are controlled. For more information, see [Enable System Updates \(Android\)](#).

Note Some profiles display the following tags: **AFW v1+** and **AFWAPP**. The Android App (AFWAPP) is the Pre-Lollipop solution for Android coming soon.

This chapter includes the following topics:

- [Passcode Profile \(Android\)](#)
- [Enforce Chrome Browser Settings \(Android\)](#)
- [Restrictions Profile \(Android\)](#)
- [Enable Exchange Active Sync \(Android\)](#)
- [Auto Update Profile](#)
- [Credentials \(Android\)](#)
- [Create Custom Messages](#)
- [Application Control \(Android\)](#)

- [Configure Proxy Settings \(Android\)](#)
- [Enable System Updates \(Android\)](#)
- [Wi-Fi Profile \(Android\)](#)
- [Configure VPN \(Android\)](#)
- [Set Permissions \(Android\)](#)
- [Configure Single App Mode \(Android\)](#)
- [Set Date/Time](#)
- [Create Workspace ONE Launcher Profile \(Android\)](#)
- [Configure Firewall Rules \(Android\)](#)
- [Configure APN Profile](#)
- [Enterprise Factory Reset Protection](#)
- [Configure Zebra MX Profile \(Android\)](#)
- [Using Custom Settings \(Android\)](#)

Passcode Profile (Android)

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 (Android)

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

Procedure

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

Settings	Description
Maximum Number of Repeating Characters	Prevent your end users from entering easily cracked repetitive passcodes like '1111' by setting a maximum number of repeating characters.
Maximum Length of Numeric Sequences	Prevent your end user from entering an easily cracked numeric sequence like 1234 as their passcode.
Allow Iris Scanner	Disable to prevent the Iris Scanner method from being configurable or selectable on the Samsung device.
Allow Face Unlock	Disable to prevent the Face Unlock method from being configurable or selectable on the Samsung device.
Lockscreen Overlay	<p>Enable to push information to the end user devices and display this information over the lock screen.</p> <ul style="list-style-type: none"> ■ Image Overlay – Upload images to display over the lock screen. You can upload a primary and secondary image and determine the position and transparency of the images. ■ Company Information – Enter company information to display over the lock screen. This can be used for emergency information in the event the device has been lost or reported stolen. <p>The Lockscreen Overlay setting is for Safe 5.0 devices and above only. The Lockscreen Overlay settings remains configured on the device while in use and cannot be changed by the end user.</p> <p>For more information on Lockscreen Overlay settings, see Configure Lockscreen Overlay (Android)</p>

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.

Configure Lockscreen Overlay (Android)

The **Lockscreen Overlay** option in the passcode profiles gives you the ability to overlay information over the screen lock image to provide information to the end user or anyone who may find a locked device. Lockscreen Overlay is a part of the Passcode profile.

Procedure

- 1 Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
- 2 Select **Android** or **Android (Legacy)** depending on your enrollment configuration.
- 3 Configure the **General** profile settings as appropriate.

Lockscreen Overlay is a native functionality for Android (Legacy) and available across several OEMs.

The Lockscreen Overlay settings for **Android** profiles on displays when the **OEM Settings** field is toggled to **Enabled** and Samsung is selected from the **Select OEM** field. The OEM settings field in the General profile only applies to Android profiles and not Android (Legacy) configurations.

- 4 Select the **Passcode** profile from the list.
- 5 Enable the **Lockscreen Overlay** field.
- 6 Select your desired lockscreen overlay type: **Image Overlay** or **Company Information**.
- 7 Configure the settings for Image Overlay as desired.

Setting	Description
Image Overlay Type	Select Single Image or Multi Image to determine the number of overlay images required.
Primary Image	Upload an image file.
Primary Image Top Position in Percent	Determine the position of the top image from 0-90 percent.
Primary Image Bottom Position in Percent	Determine the position of the bottom image from 0-90 percent.
Secondary Image	Upload a second image if desired. This field only displays if Multi Image is selected from the Image Overlay Type field.
Secondary Image Position in Percent	Determine the position of the top image from 0-90 percent. Only application if Multi Image is selected from the Image Overlay Type field.
Secondary Image Bottom Position in Percent	Determine the position of the bottom image from 0-90 percent. Only applicable if Multi Image is selected from the Image Overlay Type field.
Overlay Image	Determine the transparency of your image as Transparent or Opaque .

- 8 Configure the settings for **Company Information** as desired.

Setting	Description
Company Name	Enter your company name for display.
Company Logo	Upload the company logo with an image file.
Company Address	Enter the company office address.
Company Phone Number	Enter the company phone number.
Overlay Image	Determine the transparency of your image as Transparent or Opaque .

- 9 **Save & Publish.**

Enforce Chrome Browser Settings (Android)

The Chrome Browser Settings profile helps you to manage settings for the Work Chrome app.

Chrome is Google's web browser. Chrome offers a number of features such as search, the omnibox (one box to search and navigate), auto-fill, saved passwords, and Google account sign-in to instantly access recent tabs and searches across all your devices. The work Chrome app functions the same as the personal version of Chrome. 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.

Procedure

- 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.

Setting	Description
Allow Cookies	Enable to determine browser cookies settings.
Allow Cookies On These Sites	Specify URLs which are allowed to set cookies.
Block Cookies On These Sites	Specify URLs which are not allowed to set cookies.
Allow Session Only Cookies On These Sites	Specify sites which are allowed to set session only cookies.
Allow Images	Enable to determine which sites allow images.
Allow Images On These Sites	Specify a list of URLs which are allowed to display images.
Block Images On These sites	Specify a list of URLs which are not allowed to display images.
Allow JavaScript	Enable JavaScript browser settings.
Allow JavaScript On These Sites	Specify sites which are allowed to run JavaScript.
Block JavaScript On These Sites	Specify sites which are not allowed to run JavaScript.
Allow Pop-Ups	Enable pop-up browser settings.
Allow Popups On These Sites	Specify sites which are allowed to open popups.
Block Popups On These sites	Specify sites which are not allowed to open popups.
Allow Track Location	Set whether websites are allowed to track the users' physical location.
Proxy Mode	Specify the proxy server used by Google Chrome and prevents users from changing proxy settings.
Proxy Server URL	Specify the URL of the proxy server.
Proxy PAC File URL	Specify a URL to a proxy .pac file.
Proxy Bypass Rules	Specify which proxy settings to bypass. This policy only takes effect if you have selected manual proxy settings.
Force Google SafeSearch	Enable to force search queries in Google web search to be done with SafeSearch.

Setting	Description
Enable Touch to Search	Enables the use of Touch to Search in Google Chrome's content view.
Enable Default Search Provider	Specify the default search provider.
Default Search Provider Name	Specify the name of the default search provider.
Default Search Provider Keyword	Specify the keyword search for the default search provider.
Default search provider search URL	Specify the URL of the search engine used when doing a default search.
Default search provider suggest URL	Specify the URL of the search engine used to provide search suggestions.
Default Search Provider Icon	Specify the favorite icon URL of the default search provider.
Default Search Provider Encodings	Specify the character encodings supported by the search provider. Encodings are code page names like UTF-8, GB2312, and ISO-8859-1. If not set, the default will be used which is UTF-8.
List Of Alternate URLs For The Default Search Provider	Specify a list of alternate URLs that can be used to extract search terms from the search engine.
Search Provider Image URL	Specify the URL of the search engine used to provide image search.
New Tab URL	Specify the URL that a search engine uses to provide a new tab page.
POST URL Search Parameters	Specify the parameters used when searching a URL with POST.
POST Suggestion Search Parameters	Specify the parameters used when doing image search with POST.
POST Image Search Parameters	Specify the parameters used when doing image search with POST.
Enable The Password Manager	Enable saving passwords to the password manager.
Enable Alternate Error Pages	Enable to use alternate error pages that are built into Google Chrome (such as 'page not found').
Enable Autofill	Enable to allow users to auto complete web forms using previously stored information such as address or credit card information.
Enable Printing	Enable to allow printing in Google Chrome.
Enable Safe Browsing	Enable to activate Google Chrome's Safe Browsing.
Disable Saving Browser History	Enable to disable saving browser history in Google Chrome.
Prevent Proceeding After Safe Browsing Warning	Enable to prevents users from proceeding from the warning page to malicious sites.
Enable Network Prediction	Enable network prediction in Google Chrome.
Enable Deprecated Web Platform Features For A Limited Time	Specify a list of deprecated web platform features to re-enable temporarily.
Incognito Mode Availability	Specify whether a user can open pages in Incognito mode in Google Chrome.
Enable Search Suggestions	Enable search suggestions in Google Chrome's omnibox.
Enable Translate	Enable the integrated Google Translate service on Google Chrome.
Enables or Disables Bookmark Editing	Enable to allow bookmarks to be added, removed, or modified.
Managed Bookmarks	Specify a list of managed bookmarks.
Block Access To A List Of URLs	Enter URLs to prevents the user from loading web pages from blacklisted URLs.
Exceptions to blocked list of URLs	Enter blacklist exception URLs.

Setting	Description
Minimum SSL Version Enabled	Selected the minimum SSL version from the dropdown.
Minimum SSL Version To Fallback To	Select the minimum, SSL version to fallback to from the dropdown.

4 Select **Save & Publish**.

Chrome Browser Settings Matrix (Android)

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 matrix details the available settings in the Chrome Browser profile.

Setting	Description
Content Settings	
Allow Cookies	Applies to the native Android browser to allow or prevent any website from storing cookies related to the website on the device.
Allow Cookies On These Sites	Allows you to set a list of URL patterns that specify sites which are allowed to set cookies.
Block Cookies On These Sites	Allows you to set a list of URL patterns that specify sites which are not allowed to set cookies.
Allow Session Only Cookies on These Sites	Allows you to set a list of URL patterns that specify sites which are allowed to set session only cookies.
Allow Images	Allows you to set whether websites are allowed to display images.
Allow Images On These Sites	Allows you to set a list of URL patterns that specify sites which are allowed to display images.
Block Images On These Sites	Allows you to set a list of URL patterns that specify sites which are not allowed to display images.
Allow JavaScript	Applies to the native Android browser to allow or prevent the browser from running JavaScript code for a website.
Allow JavaScript On These Sites	Allows you to set a list of URL patterns that specify sites which are allowed to run JavaScript.
Block JavaScript On These Sites	Allows you to set a list of URL patterns that specify sites which are not allowed to run JavaScript.
Allow Pop-Ups	Pop-up browser setting to allow or prevent any website from popping up new browser windows when the user navigates to a website that invokes such action.
Allow Pop-Ups On These Sites	Allows you to set a list of URL patterns that specify sites which are allowed to open popups.
Allow Track Location	Allows you to set whether websites are allowed to track the users' physical location.
Proxy Settings	
Proxy mode	Select how your desired proxy flow.
Proxy Server URL	Specify a URL to a proxy .pac file.

Setting	Description
Proxy PAC File URL	Enter your Proxy PAC file URL, if applicable.
Proxy Bypass Rules	Enter any applicable bypass rules to direct requests from certain clients or to particular origin servers around the proxy.
Search Settings	
Force Google SafeSearch	
Force YouTube Safety Mode	
Enable Touch to Search	
Enable Default Search Provider	Enable to set a default search provide on the browser.
Default Search Provider Name	Specifies the name of the default search provider.
Default Search Provider Keyword	Specifies the keyword, which is the shortcut used in the address bar to trigger the search for this provider.
Default search provider search URL	Specifies the URL of the search engine used when doing a default search.
Default search provider suggest URL	Specifies the URL of the search engine used to provide search suggestions.
Default Search Provider Icon	Specifies the favorite icon URL of the default search provider.
Default Search Provider Encodings	Specifies the character encodings supported by the search provider.
List Of Alternate URLs For The Default Search Provider	Specifies a list of alternate URLs that can be used to extract search terms from the search engine.
Search Terms Replacement Key	Enter search terms that will display instead of the URL.
Search Provider Image URL	Specifies the URL of the search engine used to provide image search.
New Tab URL	Specifies the URL that a search engine uses to provide a new tab page.
POST URL Search Parameters	Specifies the parameters used when searching a URL with POST.
POST Suggestion Search Parameters	Specifies the parameters used when doing suggestion search with POST.
POST Image Search Parameters	Specifies the parameters used when doing image search with POST.
Password Manager	
Enable the password manager	Enable to allow web forms to store passwords.
Start Up Pages	
Enable alternate error pages	Controls whether the browser shows suggestions for the page you were trying to reach when it is unable to connect to a web address such as 'Page Not Found.'
Enable autofill	Enable to allow the browser to automatically complete any online forms from stored information.
Other Settings	
Enable Printing	Enable to allow printing from the device.
Enable Data Compression Proxy Feature	Enable to allow webpages to compress pages which reduces data usage.
Enable Safe Browsing	Enable to remove Chrome's Safe Browsing feature
Disable saving browser history	Select to prevent the browsing history from being saved

Setting	Description
Prevent Proceeding After Safe Browsing Warning	Enable to stop users from proceeded past the warning page to malicious sites.
Disable SPDY protocol	Enable to disable the SPDY protocol which manipulates HTTP traffic, with particular goals of reducing web page load latency and improving web security.
Enable Deprecated Web Platform Features For A Limited Time	Specify a list of unapproved web platform features to re-enable temporarily.
Force Safe Search	Enable for all Google web searches to be done with SafeSearch set to active.
Incognito Mode Availability	Specifies whether the user may open pages in Incognito mode in Chrome.
Allows sign in to Chromium	Enable to allow user to sign in to Chromium.
Enable Search Suggestions	Allows for search suggestions in the Chrome address bar.
Enable Translate	Set which integrates Google Translate into Chrome which will offer to translate a page for the user when appropriate.
Enables or disables bookmark editing	Set this field to restrict the use of the bookmarks editor.
Managed Bookmarks	Enter any applicable URL's that will be managed from the browser. Managed bookmarks allow the administrator to push out a fixed set of bookmarks to all users.
Allows Access To A List Of URLs	Specify a list of whitelisted URLs that can be accessed from the device.
Block Access To A List Of URLs	Specify a list of blacklisted URLs.
Minimum SSL Version Enabled	Set the minimum Secure Socket Layer version.
Minimum SSL Version to Fallback To	Set the minimum Secure Socket Layer version that the browser will revert to.

Restrictions Profile (Android)

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 user's 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 (Android)

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.

Procedure

- 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.
Location Services	Configure Location Service settings for Work managed devices only.
Samsung Knox	Allows you to enable restrictions specifically for Android devices running Samsung Knox. This section of settings only applies when OEM Settings field in the General profile is toggled to enabled and Select OEM is set to Samsung. This section is only available when OEM Settings in the General Profile is enabled and Samsung is selected from the Select OEM field.

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

Enable Exchange Active Sync (Android)

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 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.

Prerequisites

Once each user has an email address and user name you can create an EAS profile.

Note The EAS profile applies towards the Work Profile and Work Managed Device mode types.

Procedure

- 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	<p>Enable to select an S/MIME certificate you associate as a User Certificate on the Credentials payload.</p> <ul style="list-style-type: none"> ■ 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.
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.
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.
Allow Contacts And Calendar Sync	Enable to allow contacts and calendar to sync with devices.

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

Auto Update Profile

The Auto update profile allows admins to configure auto updates and scheduling maintenance windows for public Android apps.

To configure an auto update policy:

Procedure

- 1 Navigate to Devices > Profiles & Resources > Profiles > Add > Add Profile > Android.
- 2 Configure the General profile settings as appropriate. These settings determine how the profile deploys and who receives it.

- 3 Select Auto Update from the payload list and configure the update settings:
 - Public Apps Auto Update Policy: Specify when Google Play allows auto-date. Select Allow user to configure, Always auto update, Update on Wi-Fi only, or Never auto update.
The default selection is Allow user to configure.
 - Start Time: Configure what the local time applications in the foreground should be allowed to auto update each day. Select a time between 00:30 to 23:30.
 - End Time: Configure what the local time applications in the foreground should be allowed to auto update each day. Select a time between 30 minutes to 24 hours.
- 4 Select Save and Publish to assign the profile to associated devices.

Based on time set, the applications will only auto update during the specified start and end times. For example, you would set kiosk devices to only update outside of business hours to not interrupt kiosk usage.

Credentials (Android)

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 (Android)

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.

Procedure

- 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**.

Create Custom Messages

The Custom Messages profile allows you configure messages that display on the device homescreen when important information needs to be relayed to the user.

The Custom messages profile allows you to set a lockscreen message, a message to display when users attempt to perform a blocked setting, or device user settings.

Procedure

- 1 Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
- 2 Select **Android**.
- 3 Configure the General profile settings as appropriate.
- 4 Select the Custom Messages profile and configure the messages settings:

Option	Description
Set a Lockscreen Message	Enter a message to display on the device homescreen when the device is locked. This is useful for a device that has been lost or stolen to display contact information of the user.
Set a short message for blocked settings	Enter a message to be displayed when a user tries to perform actions on a device that is blocked. Use the custom message to explain why the feature is blocked.
Set a long message for users to view in settings	Users can check this setting in Settings>Security>Device .

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

Application Control (Android)

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

For more information on Application Groups, see the [Mobile Application Management Documentation](#).

Configure Application Control (Android)

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

Procedure

- 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 (Android)

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.

Procedure

- 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 (Android)

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

Procedure

- 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 (Android)

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 (Android)

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

Procedure

- 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.

Setting>	Description
Security Type	<p>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.</p> <ul style="list-style-type: none"> ■ Protocols <ul style="list-style-type: none"> ■ Use Two Factor Authentication ■ SFA Type ■ Authentication <ul style="list-style-type: none"> ■ 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.
Proxy Type	<p>Enable to configure the Wi-Fi proxy settings.</p> <p>Note Wi-Fi Proxy Auto Configuration is not supported using Per-App VPN.</p>
Proxy Server	Enter the hostname or IP address for the proxy server.
Proxy Server Port	Enter the port for the proxy server.
Exclusion List	<p>Enter the hostnames to exclude from the proxy.</p> <p>Hostnames entered here will not be routed through the proxy.</p> <p>Use the * as a wild card for the domain. For example: *.air-watch.com or *air-watch.com.</p>

5 Select **Save & Publish**.

Configure VPN (Android)

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.

Note The VPN profile applies for both the Work Profile and Work Managed Device mode types.

Procedure

- 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 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	<p>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.</p> <p>Note Wi-Fi Proxy Auto Configuration is not supported using Per-App VPN.</p>
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 Deploy Credentials (Android) 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 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**.

Cisco AnyConnect and **Juniper Junos Pulse** connections require specific applications to be installed on each device before the VPN profile is deployed. These applications can be included as a **Recommended App** from the **App Catalog** for easy access.

Configure Per-App VPN (Android)

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.

Note Per-App VPN does not support internal apps.

Note Wi-Fi Proxy Auto Configuration is not supported using Per-App VPN.

Procedure

- 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.

What to do next

To configure public apps to use the Per-App VPN profile, see [Add Public Applications for Android](#)

Set Permissions (Android)

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.

Procedure

- 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 (Android)

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 \(Android\)](#).

Procedure

- 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. Apps are whitelisted in Apps & Books. For more information, see Add Public Applications for Android

Best Practices for Single App Mode (Android)

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.

Set Date/Time

Set the date and time as well as the display format to provide your fleet with the appropriate regional format.

Procedure

- 1 Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
- 2 Select **Device** to deploy your profile to a device.
- 3 Configure the profile's **General** settings. The **Date/Time** profile only displays when the **OEM Settings** field is toggled to **Enabled**.
- 4 Select the **Date/Time** payload.

5 Configure the Date/Time settings, including:

Setting	Description
Date Format	Set the to change the order that the Month, Day and Year display.
Time Format	Choose a of 12 or 24 Hours format.
Date/Time	<p>Set which data source your devices will pull from for the date and time settings:</p> <ul style="list-style-type: none"> ■ 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 . <ul style="list-style-type: none"> ■ 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. <ul style="list-style-type: none"> ■ 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 <ul style="list-style-type: none"> ■ 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.

6 Select **Save & Publish**.

Create Workspace ONE Launcher Profile (Android)

Workspace ONE 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 Workspace ONE 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 Workspace ONE Launcher profile in COSU mode, see the Workspace ONE Launcher publication.

Procedure

- 1 Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
- 2 Configure the profile's **General** settings.
These settings determine how the profile deploys and who receives it.
- 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 Firewall Rules (Android)

The **Firewall** payload allows admins to configure firewall rules for Android devices. Each firewall rule type allows you to add multiple rules.

Note The Firewall payload only applies to SAFE 2.0+ devices.

Procedure

- 1 Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android or Android (Legacy)**.
- 2 Select **Device** to deploy your profile.
- 3 Configure the **General** profile settings. The **Firewall** profile only displays for **Android** profiles when the **OEM Settings** field is enabled and Samsung is selected from the **Select OEM** field. The OEM Settings field in the General profile only applies to Android profiles and not Android (Legacy) configurations.

The General settings determine how the profile deploys and who receives it.

- 4 Select the **Firewall** profile.
- 5 Select the **Add** button under the desired rule to configure the settings:

Setting	Description
Allow Rules	Allows the device to send and receive from a specific network location.
Deny Rules	Blocks the device from sending and receiving traffic from a specific network location.
Reroute Rules	Redirects traffic from a specific network location to an alternate network. If an allowed website redirects to another URL, please add all redirected URLs to the Allow Rules section so it can be accessed.
Redirecaccessed.ion	Avoids traffic from being redirected.

6 Select **Save & Publish**.

The Firewall configuration is an IP Address based tool, and adding hostnames will not work and IP addresses. Services such as Google and Amazon do not always maintain static IP addresses so using hostnames is recommended, but can result in inconsistencies.

Configure APN Profile

Configure Android devices Access Point Name (APN) settings to unify device fleet carrier settings and correct misconfigurations.

Procedure

- 1 Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
- 2 Select **Device** to deploy your profile to a device.
- 3 Configure the profile's **General** settings. The APN profile only displays when the **OEM Settings** field is toggled to **Enabled** and Samsung is selected from the **Select OEM** field.

The General profile settings determine how the profile deploys and who receives it.

- 4 Select the **APN** payload.
- 5 Configure the **APN** settings, including:

Setting	Description
Display Name	Provide a user friendly name of the access name.
Access Point Name (APN)	Enter the APN provided by your carrier (For example: come.moto.cellular).
Mobile Country Code (MCC)	Enter the 3-digit country code. This values checks whether devices are roaming on a different carrier than entered here. This is used in combination with a mobile network code (MNC) to uniquely identify a mobile network operator (carrier) using the GSM (including GSM-R), UMTS, and LTE mobile networks.
Mobile Network Code (MNC)	Enter the 3-digit network code. This values checks whether devices are roaming on a different carrier than entered here. This is used in combination with a mobile country code (MCC) to uniquely identify a mobile network operator (carrier) using the GSM (including GSM-R), UMTS, and LTE mobile networks.
MMS Server (MMSC)	Specify the server address.
MMS Proxy Server	Enter the MMS port number.
MMS Proxy Server Port	Enter the target port for the proxy server.
Server	Enter the name or address used for the connection.
Proxy Server	Enter the proxy server details.
Proxy Server Port	Enter the proxy server port for all traffic. Select Add to continue this process.
Access Point User Name	Specify the username that connects to the access point.
Access Point Password	Specify the password that authenticates t he access point.

Setting	Description
Authentication Type	Select the authentication protocol.
Set as Preferred APN	Enable to ensure all end user devices have the same APN settings and to prevent any changes being made from the device or carrier.

- 6 Select **Save & Publish**.

Enterprise Factory Reset Protection

Factory Reset Protection (FRP) is a security method that was designed to make sure that someone cannot wipe and factory reset your device if it is lost or stolen.

You have to be signed in with the original Google account of the device (the one you used to set it up) to factory reset it. With the original Google account signed in, it presents a problem for the admin when a device is returned and a user has enabled FRP. When the device is returned to the organization (user leaves the company for example), the admin is unable to set up the device again.

Configure Enterprise Factory Reset Protection(Android)

The Enterprise Factory Reset Protection profile allows you to create Google userIDs that are to set up the device or complete reset. This Google User ID allows you to reset the device without the original Google account. Obtain your Google userID using the People:get API to configure the profile.

FRP can also be removed when performing a device wipe on the device from the device management commands. For more information on device management, see [Device Management Commands \(Android\)](#).

Procedure

- 1 Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
- 2 Configure the **General** profile settings as appropriate.
- 3 Select the **Enterprise Factory Reset Protection** payload.
- 4 Configure the following settings to set the level of control for your application deployments:

Setting	Description
Google user IDs	Enter the Google user ID obtained from Google People:get.

- 5 Select **Save & Publish**.

Configure Zebra MX Profile (Android)

The Zebra MX profile allows you take advantage of the additional capabilities offered with the Zebra MX service app on Android devices. The Zebra MX Service app can be pushed from Google Play and from AirWatch Resources distributed it as an internal app in the Workspace ONE UEM console in conjunction with this profile.

Procedure

- 1 Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.
- 2 Configure the **General** profile settings as appropriate. Enable the **OEM Settings** field and select Zebra from the **Select OEM** field to enable the Zebra MX profile.
- 3 Configure the Zebra MX profile settings:

Setting	Description
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.
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.
Allow Wi-Fi to Disconnect During Sleep	<p>Always On - Wi-Fi stays on when device goes to sleep.</p> <p>Only When plugged in - Wi-Fi stays on when device goes to sleep only if the device is charging.</p> <p>Never On - Wi-Fi turns off when the device goes to sleep.</p>
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.
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	<p>Set which data source your devices will pull from for the date and time settings:</p> <ul style="list-style-type: none"> ■ 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 . <ul style="list-style-type: none"> ■ 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. <ul style="list-style-type: none"> ■ 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 <ul style="list-style-type: none"> ■ 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.
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.
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 (Android)

The **Custom Settings** payload can be used when new Android functionality releases or features that Workspace ONE UEM console does not currently support through its native payloads. Use the **Custom Settings** payload and XML code to manually enable or disable certain settings.

Procedure

- 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.

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**.

Shared Devices

Shared Device/Multi-User Device functionality ensures that security and authentication are in place for every unique end user. And if applicable, shared devices allow only specific end users to access sensitive information.

Issuing a device to every employee in certain organizations can be expensive. Workspace ONE UEM lets you share a mobile device among end users in two ways: using a single fixed configuration for all end users, or using a unique configuration setting for individual end users.

When administering shared devices, you must first provision the devices with applicable settings and restrictions before deploying them to end users. Once deployed, Workspace ONE UEM uses a simple login or log-out process for shared devices in which end users simply enter their directory services or dedicated credentials to log in. The end-user role determines their level of access to corporate resources such as content, features, and applications. This role ensures the automatic configuration of features and resources that are available after the user logs in.

The login or log-out functions are self-contained within the Workspace ONE Intelligent Hub. Self-containment ensures that the enrollment status is never affected, and that the device is managed whether it is in use or not.

Shared Devices Capabilities

There are basic capabilities surrounding the functionality and security of devices that are shared across multiple users. These capabilities offer compelling reasons to consider shared devices as a cost-effective solution to making the most of enterprise mobility.

Functionality

- Personalize each end-user experience without losing corporate settings.
- Logging in a device configures it with corporate access and specific settings, applications, and content based on the end-user role and organization group (OG).
- Allow for a log in/log out process that is self-contained in the Workspace ONE Intelligent Hub or VMware Identity Manager.
- After the end user logs out of the device, the configuration settings of that session are wiped. The device is then ready for login by another end user.

Security

- Provision devices with the shared device settings before providing devices to end users.
- Log in and log out devices without affecting an enrollment in Workspace ONE UEM.
- Authenticate end users during a login with directory services or dedicated Workspace ONE UEM credentials.
- Authenticate end users using VMware Identity Manager.
- Manage devices even when a device is not logged in.

Platforms that Support Shared Devices

The following devices support shared device/multi-user device functionality.

- Android 4.3+
- iOS devices with Workspace ONE Intelligent Hub v4.2+,
- MacOS devices with Workspace ONE Intelligent Hub v2.1+.

This chapter includes the following topics:

- [Configure Android for Shared Device Use](#)
- [Configure Shared Devices](#)
- [Define the Shared Device Hierarchy](#)
- [Log In and Log Out of Shared Android Devices](#)

Configure Android for Shared Device Use

To use shared device functionality on Android devices, enroll the device using the Workspace ONE Intelligent Hub, set the Workspace ONE Launcher application as the default home screen, and create and assign the Launcher profile. Workspace ONE Launcher is automatically downloaded during enrollment, but you will need to determine which version of the Launcher is pushed to devices.

Procedure

- 1 Navigate to **Devices > Device Settings > Android > Service Applications**.
- 2 Configure the applicable settings:

Setting	Description
Always use the Latest Version of Launcher	If this setting is enabled, the latest version of the app automatically pushes to devices when it becomes available.
Launcher Version	Manually choose the version you want to deploy from the drop-down menu.

- 3 Select **Save**.

- 4 Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android > Launcher** and configure the Launcher profile at each child organization group. This profile should contain all of the necessary settings common to that organization group.

Important Make sure to enable the **Persist Admin Passcode If Launcher Profile Is Removed From Device setting**, as this will ensure that the staging user, as well as the shared device Users are not permitted to exit the Launcher without entering the Administrative Passcode.

Do not assign the Launcher profile to a staging user.

- 5 Enroll the device into the enrollment organization group using the staging user. The Launcher .apk will install and the login screen will appear, by default.

The Launcher .apk needs to be installed before the Launcher profile in the Staging Manifest.

- 6 Enter the shared device user Group ID, Name, and Password to log in, assigning the device to the Shared Device User and the proper child organization group. The Launcher profile will be applied to the device, and the console will reflect which user is logged in to the device.

Important Only enter the Group ID if you selected **Prompt for Organization Group** in the Group Organization Group assignment mode under the shared device settings.

- 7 Log out of the Launcher profile on the device. This reassigns the device back to the staging user, moves the device back to the original enrollment organization group, and removes the Launcher profile.

Configure Shared Devices

Similar to single-user device staging, multi-user staging (a "shared device") allows an IT administrator to provision devices to be used by more than one user.

Procedure

- ◆ Complete the **Security** section, as applicable.

Setting	Description
Require Shared Device Passcode.	Require users to create a Shared Device passcode in the Self-Service Portal to check out devices. This passcode is different from a Single Sign On passcode or a device-level passcode.
Require Special Characters.	Require special characters in the shared device passcode, which includes characters such as @, %, &, and so forth.
Shared Device Passcode Minimum Length	Set the minimum character length of the shared passcode.
Shared Device Passcode Expiration Time (days)	Set the length of time (in days) the shared passcode expires.
Keep Shared device Passcode for minimum time (days)	Set the minimum amount of time (in days) the shared device passcode must be changed.
Passcode History	Set the number of passcodes that are remembered by the system, providing a more secure environment by preventing the user from reusing old passcodes.

Setting	Description
Auto Log out Enabled	Configure an automatic log out after a specific time period.
Auto Log out After	Set the length of time that must elapse before the Auto Log out function activates in Minutes, Hours, or Days .
Enable Single App Mode.	<p>Select this check box to configure Single App Mode, which locks the device into a single application when an end user logs in to the device.</p> <p>To check out an iOS device in Single App Mode, end users log in using their credentials. When the device is checked in again, it returns to Single App Mode.</p> <p>Enabling Single App Mode also disables the Home button on the device.</p> <p>Note Single App Mode applies only to Supervised iOS devices.</p>
Clear Device Passcode on Logout (Android Only)	This setting controls whether the current device passcode is cleared when the user logs out (checks in) a multi-user shared device.
Clear App Data on Logout (Android Only)	Clear the app data when the user logs out of a shared device (checks it in).
Reinstall Apps on Logout (Android Work Managed Device and Android (Legacy) Only)	Use the drop-down to select whether to Always reinstall app between users or never reinstall app between users. For Android (Legacy) deployments, you can opt to reinstall app if the Hub cannot clear app data between users.

Define the Shared Device Hierarchy

Create the hierarchy of subgroups under a single organization group based on your company needs.

When you first log in to Workspace ONE UEM, you see a single organization group (OG) that has been created for you using the name of your organization. This group serves as your top-level OG. Below this top-level group you can create subgroups to build out your company hierarchical structure.

Procedure

- 1 Navigate to **Groups & Settings > Groups > Organization Groups > Organization Group Details**.
Here, you can see an OG representing your company.
- 2 Ensure the **Organization Group Details** displayed are accurate, and then use the available settings to make modifications, if necessary. If you make changes, select **Save**.
- 3 Select **Add Child Organization Group**.

4 Enter the following information for the first OG underneath the top-level OG.

Setting	Description
Name	Enter a name for the child organization group (OG) to be displayed. Use alphanumeric characters only. Do not use odd characters.
Group ID	<p>Enter an identifier for the OG for the end users to use during the device login. Group IDs are used during the enrollment of group devices to the appropriate OG.</p> <p>Ensure that users sharing devices receive the Group ID as it might be required for the device to log in depending on your Shared Device configuration.</p> <p>If you are not in an on-premises environment, the Group ID identifies your organization group across the entire shared SaaS environment. For this reason, all Group IDs must be uniquely named.</p>
Type	Select the preconfigured OG type that reflects the category for the child OG.
Country	Select the country where the OG is based.
Locale	Select the language classification for the selected country.
Customer Industry	This setting is only available when Type is Customer. Select from the list of Customer Industries.
Time Zone	Select the time zone for the OG's location.

5 Select **Save**.

Log In and Log Out of Shared Android Devices

To use shared device functionality on Android devices, enroll the device using the Workspace ONE Intelligent Hub and set the VMware Workspace ONE Launcher as the default home screen. The Workspace ONE Launcher is automatically downloaded during enrollment.

Once the application is installed and set as the default home screen, the device is in a checked-in state. While in this state, the end user is unable to navigate away from this page and the device prompts the user to check out. To remove the profile and make the entire device accessible again, perform an Enterprise Wipe on the staging user device from the Workspace ONE UEM console.

Procedure

- 1 From the Workspace ONE Launcher log in page, users must enter their Group ID, user name, and password. If **Prompt User for Organization Group** is enabled on the console, end users are required to enter a **Group ID** to log in.

- 2 Select **Login** and accept the terms of use, if applicable.

The device is configured. Once logged in, user profiles are pushed down based on the smart group and user group associations.

What to do next

To log out of an Android device, select the **Settings** button and select **log out**.

Application Management for Android

6

Use Workspace ONE UEM to push Android public and internal applications, and web apps 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.

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

For more information on application assignment, see [Assign Applications for Android](#).

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

This chapter includes the following topics:

- [Workspace ONE Intelligent Hub for Android](#)
- [Internal Apps with Android](#)
- [Add Public Applications for Android](#)
- [Assign Applications for Android](#)
- [Enable Play for Work](#)
- [Integration Features](#)
- [Samsung Native Email with Android](#)

Workspace ONE Intelligent Hub for Android

The Workspace ONE Intelligent Hub for Android is an application that enables the Native Android SDK API layer of management to which Workspace ONE UEM connects.

Workspace ONE UEM engages Native Android SDK APIs on Android devices for management and tracking capabilities. **Native Android SDK APIs** are available to any third-party application, including the Workspace ONE Intelligent Hub and any other application using the AirWatch Software Development Kit (SDK).

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

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

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

- **This Device** – Displays the name of the enrolled end user, the device Friendly Name, current enrollment status, connectivity method and compliance status.
- **Device Status** – Displays the current enrollment status including:
 - The server to which the device is currently connected.
 - The organization group to which the device is currently enrolled.
 - The current network status including the active Wi-Fi SSID to which the device is connected.
- **Compliance** – Displays a list of compliance policies currently active for the device.
- **Profiles** – Displays a list of profiles currently installed on the device. From the profiles list, you have the ability to refresh and reapply profiles from your device that might be out of sync or uninstalled.

- **Managed Apps** – Displays a list of apps managed by Workspace ONE UEM installed on the device as well as their install status.
- **About** – Displays the version number of the Workspace ONE Intelligent Hub installed on the device and provides a hyperlink to the associated Privacy Policy agreed to upon device enrollment.

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

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

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

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

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

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

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

The Hub and SDK-Built Applications

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

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

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

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

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

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.

There are two options for deploying internal apps:

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

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

If you are deploying internal apps on Android Work profile devices, add internal apps to Google Play for Work so that they are available to 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.

Add Public Applications for Android

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

Procedure

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

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

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

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.

What to do next

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

For more information on assigning apps, see [Assign Applications for Android](#)

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.

Procedure

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

Setting	Description
Assigned Smart Groups	Select an existing smart group or create a new one.
View Device Assignment	View the list of devices available by assigned smart groups.
App Delivery Method	<p>Set the application to install automatically (auto) or manually (on demand) when needed.</p> <ul style="list-style-type: none"> ■ On Demand – Deploys content to a catalog or other deployment agent and lets the device user decide if and when to install the content. This option is the best choice for content that is not critical to the organization. Allowing users to download the content when they want helps conserve bandwidth and limits unnecessary traffic. ■ Automatic – Deploys content to a catalog or other deployment Hub on a device upon enrollment. After the device enrolls, the system prompts users to install the content on their devices. This option is the best choice for content that is critical to your organization and its mobile users.
Managed Access	Enable adaptive management to set AirWatch to manage the device so that the device can access the application.
App Tunneling	Configure a VPN at the application level, and select the Per-App VPN Profile. Users access the application using a VPN, which helps ensure that application access and use is trusted and secure.
Android Legacy	Select the VPN configuration profile to use for this application. This field displays when App Tunneling is enabled.
Android	Select the VPN configuration profile to use for this application. This field displays when App Tunneling is enabled.
Pre-release Version	Select to push the Alpha or Beta version of app. Select None to automatically push the production version of the app.
Application Configuration	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.

Setting	Description
Application uses AirWatch SDK	<p>Identify whether the application uses AirWatch SDK functionality and whether it needs a profile to apply the features.</p> <p>This feature is optional and advanced. For more information on the default settings for profiles, see MAM Functionality with Settings and Policies and the AirWatch SDK in the Mobile Application Management (MAM) documentation.</p> <ul style="list-style-type: none"> ■ 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	<p>Deploy applications to those special use cases that can develop within an organization.</p> <ul style="list-style-type: none"> ■ Apply User Groups and Device Ownership types to your exceptions in the Criteria area. ■ Select an Override Value to create specific exceptions to the options. Override Value options vary depending on the platform.

- 2 Assign a **Required Terms of Use** for the application on the **Terms of Use** tab. Requiring a terms of use is optional. Terms of use state specifically how to use the application. They make expectations clear to end users. When the application pushes to devices, users view the terms of use page that they must accept to use the application. If users do not accept the terms of use, they cannot access the application.
 - a **On-demand**: The terms of use displays when the device user selects the install option in the app catalog.
 - b **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 v9.2. If you are deploying the Workspace ONE UEM console 9.3+, this option will not appear.

Procedure

- 1 Navigate to **Groups & Settings > All Settings > Devices & Users > Android > Android EMM Registration**.
- 2 Select **Enable Play Store**. Once enabled, this option will disappear from the Settings page.

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.

Samsung Native Email with Android

Samsung Native Email enables users to manage multiple personal and business email accounts seamlessly. Samsung Native Exchange email is configurable within Android Fully managed, Work Profile, and Fully managed device with a work profile (previously COPE), enrollment modes using Application Configurations.

You can configure Samsung Native email with or without certificate based authentication.

The steps to configure Samsung Native email with Workspace ONE UEM console include:

- Create a Credentials Profile for Email authentication. For information on Credentials for Android, see [Deploy Credentials \(Android\)](#).
- Set up app configuration for Samsung email. For more information on App Configuration for Samsung Email, see [Set up App Configuration for Samsung Email](#).

Using Certificate Based Authentication (CBA)

In order to include Certificates in App Configuration, two pre-requisites must be met:

- The certificate(s) must be created and installed on the device, either via a Credentials Profile or manual install of certificates, before the app configuration is delivered.
- You must know the alias of the certificate(s) or use a lookup variable for the alias.

Note To prevent the email configuration from failing:

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

Set up App Configuration for Samsung Email

Configure default settings to define behaviors that apply to Samsung Native Email. Configure app specific system settings to define unique application behavior.

Configure Samsung Native Email settings on the UEM console.

Prerequisites

If you are using Certificate based authentication, be sure to create a Credentials profile prior to setting up app configuration. For more information, see [Deploy Credentials \(Android\)](#).

Procedure

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

The Google Play Store opens directly from the Workspace ONE UEM console.

- 4 Select the Samsung Email app and then click Approve.
- 5 Select Save & Assign to continue, then select Add Assignment.
- 6 Scroll down to Application Configuration and select Enabled to view and configure Exchange or Email settings.
- 7 Use lookup values to configure dynamic options, such as username, email address, or even certificate aliases.

Android Device Management Overview

7

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, Workspace ONE Intelligent Hub 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.

This chapter includes the following topics:

- [Device Management Commands \(Android\)](#)
- [Device Details Apps Tab](#)
- [Android Updates Overview](#)
- [SafetyNet Attestation](#)
- [Enable SafetyNet Attestation](#)
- [Specific Profiles Features for Android](#)
- [Specific Restrictions for Android](#)

Device Management Commands (Android)

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. If Enterprise Factory Protection is enabled, you will see a prompt that allows you to disable Enterprise Factory Reset Protection prior to the wipe.
- **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.

Android Updates Overview

Workspace ONE UEM supports reviewing and pushing Samsung Enterprise Firmware Over the Air (EFOTA) updates for Android devices. The Android Updates console page lists all firmware updates available for Android devices.

The updates are listed by release dates and details including information about specific OEMs, model, and carriers. Each model/carrier combination is a different firmware update. For example, you might see Samsung Galaxy S7 for T-mobile and a separate update for Samsung Galaxy S7 on Sprint. The list can be sorted by OEM and carrier.

Note Samsung EFOTA can only be configured at customer level Organization Group so all devices registered under that Organization Group receive updates. Consider creating a separate Organization Group for testing before pushing to all devices.

For more information on published Android firmware updates, [Publish Firmware Updates \(Android\)](#).

Publish Firmware Updates (Android)

The Android Updates console page lists all firmware updates available for Android devices and allows you to view specific firmware versions and select to prompt the user to install the update.

Procedure

- 1 Navigate to **Devices > Lifecycle > Updates** and select the **Android** tab.
- 2 View and select the radio button beside the desired update.
- 3 Select **Manage Update**.

4 Configure the settings:

Settings	Description
Install Method	Select Auto Install to select the timeframe to schedule updates. Select Install on Demand and users are prompted to accept firmware updates before it is installed on their device.
Deployment Start	Schedule the start date and time for update. Updates can be scheduled no more than 30 days in advance with a maximum update window of 7 days. Updates within this window will be published to devices every 4 hours in the server time zone.
Deployment End	Schedule the end date and time for update.
Server Time Zone	This field is read only as it generates from the server.
Network	Select whether to deploy the updates when the device are connected to Wi-Fi Only or Any network connection.

5 Select **Publish**. The Manage Updates window closes and the UEM console returns to the Updates page.

- a If for some reason you need to cancel or change the update: select the desired update and select **Cancel Schedule** from the Manage Update window.

Since the updates are batched into device groups, previous updated devices cannot be revoked.

Samsung Enterprise Firmware Over The Air (EFOTA) Updates

Samsung Enterprise Firmware Over the Air (EFOTA) allows you to manage and restrict firmware updates on Samsung devices running Android 7.0 Nougat and higher.

This is helpful in allowing you to perform testing to resolve internal application compatibility issues and monitor available updates across devices and carriers before pushing firmware updates to your device fleet.

The Samsung EFOTA flow involves registering your EFOTA settings provided by your licensed reseller, enabling "Register Enterprise FOTA" in the Android (Legacy) restrictions profile, viewing and selecting applicable updates to push to devices.

Note Samsung EFOTA can only be configured at customer level Organization Group, so all devices registered under that Organization Group receive updates. Consider creating a separate Organization Group for testing before pushing to all devices.

To configure Samsung EFOTA settings using AirWatch:

- 1 [Register Samsung Enterprise Firmware Over The Air Updates](#)

For more information, see [Devices & Users / Android / Samsung Enterprise FOTA](#)

- 2 [Configure Restrictions Profile \(Samsung EFOTA\)](#)

- 3 [Publish Firmware Updates \(Android\)](#).

For more information, see [Android Updates Overview](#).

Register Samsung Enterprise Firmware Over The Air Updates

Use the Devices & Users System Settings page to enter your EFOTA settings provided by your licensed reseller.

Procedure

- 1 Navigate to **Devices > Device Settings > Devices & Users > Android > Samsung Enterprise FOTA**.
- 2 Enter the settings:

Setting	Description
Customer ID	Enter the ID provided by your licensed reseller.
License	Enter the license provided by your licensed reseller.
Client ID	Enter the Client ID provided by your licensed reseller.
Client Secret	Enter the Client Secret provided by your licensed reseller.

- 3 Select **Save**.

Configure Restrictions Profile (Samsung EFOTA)

Restriction profiles lock down native functionality of Android devices and vary based on OEM. Enabling the "Register Enterprise FOTA" restriction locks down assigned devices to their current firmware version.

Procedure

- 1 Navigate to **Devices > Profile & Resources > Profiles > Add > Add Profile > Android > Restrictions**.
- 2 Select **Configure**
- 3 Enable **Register Enterprise FOTA**.
Allow OTA Upgrade must be enabled or firmware updates are blocked.
- 4 Select **Save & Publish**.

What to do next

For more information on restrictions for Android devices, see [Configure Restrictions Profile \(Android\)](#).

SafetyNet Attestation

SafetyNet Attestation is a Google API used to validate the integrity of the device ensuring the device is not compromised.

SafetyNet validates software and hardware information on the device and creates a profile of that device. This attestation helps determine if a particular device has been tampered or modified. When the Workspace ONE UEM console runs the SafetyNet Attestation API and reports the device has been compromised, the UEM console Device Details page reports the device as compromised.

SafetyNet Attestation is only supported with Workspace ONE Intelligent Hub and is not supported with Google Play Store version of the AirWatch Agent or Workspace ONE.

Note SafetyNet Attestation is not available for Android(Legacy) deployments.

Enable SafetyNet Attestation

Enable the SafetyNet Attestation API in the UEM console to validate the integrity of a device and determine if a device has been compromised.

Procedure

- 1 Navigate to **Groups & Settings > All Settings > Apps > Settings & Policies > Settings > Custom Settings**
- 2 Paste the following custom XML into the Custom Settings field: { "SafetyNetEnabled":true }
- 3 Save the Custom XML.
- 4 Verify SafetyNet from the Summary tab in the **Device Details** page in the UEM console. If you do not see the status of the SafetyNet Attestation, you can send a remote command to restart the device.

For more information on device commands, see [Chapter 7 Android Device Management Overview](#)

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 Managed	
	Work Profile	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	✓	✓

Feature	Work Managed	
	Work Profile	Device
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	✓	✓
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	✓	✓

Feature	Work Managed	
	Work Profile	Device
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	✓	✓
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	✓	✓
Allow Contacts and Calendar Sync	✓	✓
Network		
Configure VPN Types	✓	✓
Enable Per-app VPN (Only available for specific VPN clients)	✓	✓
Use Web Logon for Authentication (Only available for specific VPN clients)	✓	✓
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 Managed Device mode	Work Profile 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 Hub State	✓	✓
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	✓	✓
Prevent System UI (Toasts, Activities, Alerts, Errors, Overlays)	✓	
Application		
Allow Camera	✓	✓
Allow Google Play	✓	✓
Allow Chrome Browser	✓	
Allow Non-Market App Installation	✓	✓
Allow Modifying Application In Settings	✓	
Allow Installing Applications	✓	✓

Feature	Work Managed Device mode	Work Profile mode
Allow Uninstalling Applications	✓	✓
Allow Disabling Application Verification	✓	✓
Skip user tutorial and introductory hints	✓	✓
Allow Whitelist Accessibility Services	✓	
Sync and Storage		
Allow USB Debugging	✓	
Allow USB Mass Storage****	✓	
Allow Mounting Physical Storage Media	✓	
Allow USB File Transfer	✓	
Allow Backup Service (Android 8.0+)*****		
Network		
Allow Wi-Fi changes	✓	
Allow Bluetooth Pairing	✓	
Allow Bluetooth (Android 8.0+)	✓	
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 (Android 6.0+)	✓	
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		W
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+)		
Location Services		
Applies to Managed devices only.		
Allow No Location Access	✓	✓
Allow Location Access	✓	✓

Feature	Work Managed Device mode	Work Profile mode
Allow GPS Location Only	✓	✓
Allow Battery Saving Location Updates Only	✓	✓
Allow High Accuracy Location Only	✓	✓
Samsung Knox		
The Samsung Knox settings only displays for when the OEM Settings field is toggled to Enabled and Samsung is selected from the Select OEM field.		
Device Functionality		
Allow Airplane Mode	✓	
Allow Microphone	✓	
Allow Mock Locations	✓	
Allow Clipboard	✓	
Allow Power Off	✓	
Allow Home Key	✓	
Allow Audio Recording if Microphone is Allowed	✓	
Allow Video Recording if Camera is Allowed	✓	
Allow Email Account Removal	✓	
Allow Ending Activity When Left Idle	✓	
Allow User to Set Background Process Limit	✓	
Allow Headphones	✓	
Sync and Storage		
Allow SD Card Move	✓	
Allow OTA Upgrade	✓	
Allow Google Accounts Auto Sync	✓	
Allow SD Card Write	✓	
Allow USB Host Storage	✓	
Application		
Allow Settings Changes	✓	
Allow Developer Options	✓	
Allow Background Data	✓	
Allow Voice Dialer	✓	
Allow Google Crash Report	✓	
Allow S Beam	✓	
Allow Prompt for Credentials	✓	
Allow S Voice	✓	
Allow User To Stop System Signed Applications	✓	

Feature	Work Managed Device mode	Work Profile mode
Bluetooth		
Allow Desktop Connectivity Via Bluetooth	✓	
Allow Bluetooth Data Transfer	✓	
Allow Outgoing calls via Bluetooth	✓	
Allow Bluetooth Discoverable Mode	✓	
Enable Bluetooth Secure Mode	✓	
Network		
Allow Wi-Fi	✓	
Allow Wi-Fi Profiles	✓	
Allow Unsecure Wi-Fi	✓	
Allow Only Secure VPN Connections	✓	
Allow VPN	✓	
Allow Auto Connection Wi-Fi	✓	
Allow Cellular Data	✓	
Allow Wi-Fi Direct	✓	
Roaming		
Allow Automatic Sync on Roaming	✓	
Allow Auto Sync When Roaming Is Disabled	✓	
Allow Roaming Voice Calls	✓	
Data Usage on Roaming	✓	
Allow Push Messages on Roaming	✓	
Phone & Data		
Allow Non-Emergency Calls	✓	
Allow User to Set Mobile Data Limit	✓	
Allow WAP Push	✓	
Hardware Restrictions		
Allow Menu Key	✓	
Allow Back Key	✓	
Allow Search Key	✓	
Allow Task Manager	✓	
Allow System Bar	✓	
Allow Volume Key	✓	
Security		
Allow Lock Screen Settings	✓	

Feature	Work Managed Device mode	Work Profile mode
Allow Firmware Recovery	✓	
Tethering		
Allow USB Tethering	✓	
MMS Restrictions		
Allow Incoming MMS	✓	
Allow Outgoing MMS	✓	
Miscellaneous		
Set Device Font	✓	
Set Device Font Size	✓	
Allow User to Stop System Signed Applications	✓	
Allow Only Secure VPN Connections	✓	