Android (Legacy) Platform

VMware Workspace ONE UEM 2011

vmware®

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

https://docs.vmware.com/

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

Contents

Workspace ONE UEM Integration with Android(Legacy)

1

Workspace ONE UEM powered by AirWatch ™ provides you with a robust set of mobility management solutions for enrolling, securing, configuring, and managing Android devices.

Android (Legacy) refers to the integrating Android devices with Workspace ONE UEM that:

- Opt out of using Google registration
- Devices that are unable to communicate with Google Play
- Android devices running Android 5.0 or lower.

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.

An important part of managing a device fleet is ensuring devices are compliant and secure. You can assign compliance policies and security profiles to specific groups and individuals in your organization. For application integration, you can integrate any of your existing enterprise apps with the AirWatch Software Development Kit (SDK) to enhance their functionality. You can also enable end users to perform task themselves through the Self-Service Portal (SSP) and user enrollment, which saves you vital time and resources. Finally, custom reporting tools and a searchable, customizable dashboard make it easy for you to perform ongoing maintenance and management of your device fleet.

Android Name Change

Android for Work was introduced in 2015 to boost enterprise adoption for Android devices. Since that time, Google has worked to implement features in Android for Work available in the majority of 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. If you are an existing Workspace ONE UEM customer, you can continue with your Android deployment using Android (Legacy) for managing your device fleet.

This guide covers integrating Workspace ONE UEM with Android (Legacy) Platform.

This chapter includes the following topics:

- Android (Legacy) Device Administrator Migration

Supported Devices and OS Versions for Android (Legacy) Deployment

Before deploying Android devices with Android (Legacy) enrollment, consider the following pre-requisites, requirements, supporting materials, and helpful suggestions from the Workspace ONE UEM team. Familiarizing yourself with the information available in this section helps prepare you for deploying devices Android (Legacy).

Supported Operating Systems

- 4.4.X Kit Kat
- 5.0.X Lollipop
- 5.1.X Lollipop
- 6.0.X Marshmallow
- 7.0.X Nougat
- 8.0.X Oreo
- 9.0 Pie
- 10.0

OEMs that offer more management capability

- Samsung
- LG

  Note If you are deploying LG devices on Android 9.0 or later using the Android Legacy enrollment method will not be able to take advantage of the added capabilities of LG Service. If you need advanced capabilities, consider migrating to Android Enterprise.

- Lenovo
- HTC
- Motorola
- Amazon
- Barnes and Noble Nook
- Sony
- Panasonic
- Asus
- Intel

- Nexus

Caution To ensure successful installation and running of the Workspace ONE Intelligent Hub on your Android (Legacy) device, the device needs a minimum of 60 mb of space available. CPU and Run Time Memory are allocated per app on the Android platform. If an app uses more than allocated, Android (Legacy) devices optimize by killing the app.

Requirements for Configuring Devices with Android (Legacy) Deployment

The following are requirements needed for a successful deployment of Workspace ONE UEM to your devices with Android (Legacy).

Requirements

- **Google ID with a corresponding device UID** – Allows you to integrate with and search applications in the Google Play Store.
- **Appropriate Admin Permissions** – Allows you to create profiles, policies, and manage devices within the Workspace ONE UEM console.
- **Enrollment URL** – Links to your enrollment environment and takes you directly to the enrollment screen. For example, **mdm.acme.com/enroll**
- **Group ID** – Associates your device with your corporate role and is defined in the Workspace ONE UEM console.
- **Credentials** – Authenticates you as an end user in your Workspace ONE UEM environment. These credentials may be the same as your network directory services or may be uniquely defined in the Workspace ONE UEM console.

Product Provisioning with Android (Legacy) Devices

Product Provisioning allows you to manage rugged devices by using products. These products act as nannies for the devices ensuring that the assigned profiles, apps, and files/actions remain installed on the devices. By using relay servers, a form of FTP(S) servers, the products automatically push provisioned content to devices as they are needed. This system helps ensure that your devices remain up-to-date with content and limits bandwidth demand on your network.

Android (Legacy) Device Administrator Migration

Device administrator is the legacy method of enrolling Android devices with the Workspace ONE UEM console after Android's Work Managed and Work Profile modes were introduced in Android 5.0. Customers who are enrolled into Workspace ONE UEM using Android (Legacy) deployment can migrate to Android Enterprise to take advantage of device functionality for the enterprise.

This section gives you information and best practices on how to move from the Android (Legacy) deployment to Android Enterprise.

Google deprecated certain device administrator APIs in favor or more up-to-date device functionality because device administrator is not well suited to support current enterprise requirements. Workspace ONE UEM customers can adopt Work Managed (ideal for corporate owned devices), Work Profile (ideal for BYOD deployments), and Corporate Owned Personally Enabled (COPE) modes to manage their Android devices by migrating from Android (Legacy) to Android Enterprise. For more information on device modes, see Understanding Android Device Modes.

Have more questions? See our Frequently Asked Questions for Android (Legacy) Migration sections to help.

Migrate from Android (Legacy) to Android Enterprise into Work Managed Mode Using Zebra Android Devices

Zebra devices running Android 7 and higher and MXMF 7 and higher support a migration from Android (Legacy) to Android Enterprise Work Managed mode. The migration features from this flow include:

- The migration is done remotely and silently.
- Devices do not power off, reboot, or reset during the migration ensuring app data to remains intact.
- Wi-Fi connectivity is maintained during the migration.
- Products which do not contain profiles remain installed.
- Migration to AOSP/Closed Network mode is fully supported.

To get started, see Migrate to Work Managed Enrollment Using Android Legacy Migration Tool.

Migrate from Android (Legacy) to Android Enterprise with BYOD Devices

The Workspace ONE UEM console provides a seamless process that helps you migrate all devices from Android (Legacy) to a Work Profile for Android Enterprise. The migration features in the UEM console help you to make sure that:

- Your legacy administration remains intact until migration is complete.
- Devices not being migrated are never affected.
- Monitor which devices are complete, in progress, and assigned.
- Create staging or test Smart Groups to make sure that all user devices successfully migrate before migrating your entire device fleet.

To get started, see Migrating to Work Profile From Android (Legacy) Using Migration Tool.

Migrate from Android (Legacy) to Android Enterprise with Corporate Owned Devices

You can migrate from Android (Legacy) to Android Enterprise with your corporate owned devices into Work Managed Mode or Corporate Owned Personally Enabled (COPE). The enrollment and migration options vary depending on Android OS, device type, and whether the devices have access to Google Services. This scenario is best for migrating non- Zebra Android devices.

The migration and enrollment options are:

- Use Fully Managed enrollment for Android 8.0+ devices. To get started, see Migrate to Android Enterprise Using Zero Touch Enrollment
- Use Knox Mobile Enrollment for Samsung Android 8.0+ devices. To get started, see Samsung Knox Mobile Enrollment documentation.
- Follow the Cap and Grow strategy and continue to use your current Android devices enrolled through Android (Legacy). A Cap and Grow strategy means that any new device rollouts are automatically enrolled into Android Enterprise and managed simultaneously with older deployments (Android (Legacy) until your organization is ready to move all devices to Android Enterprise.

Migrate from Android (Legacy) to Android Enterprise Without Google Services

If you are currently enrolled into Workspace ONE UEM with Android devices deployed through Android (Legacy) and want to switch to Android Enterprise without Google Services, we offer Closed Network support for corporated owned devices and unmanaged enrollment for BYOD devices.

If you have a device that has no network connectivity or the device can connect to a network but has no Google services (a non-GMS certified device), you can enroll these devices into Android Enterprise into Work Managed Mode and push internal applications and apply policies with Android profiles.

If you have a device that has network connectivity but has restrictions on Google Services, for example devices being in China, you can use Closed Network support for corporate devices. For BYOD devices, you can use SDK-based MAM only mode called Registered Mode to enable unmanaged enrollment for Android devices.

For more information on Closed Network support for corporate owned devices. see Devices & Users / Android / Android EMM Registration to configure these settings.

To configure your BYOD devices without Google services, see Enable Unmanaged Unenrollment for Android Devices for steps to enroll.

Impact on APIs

Google deprecated certain device administrator APIs in favor of more up-to-date device functionality because device administrator is not well suited to support current enterprise requirements. The following APIs available with device administrator no longer function on devices running Android 10 and above. Devices remaining on Android 9.0 and below are not impacted:

- USES_POLICY_DISABLE_CAMERA
- USES_POLICY_DISABLE_KEYGUARD_FEATURES
- USES_POLICY_EXPIRE_PASSWORD
- USES_POLICY_LIMIT_PASSWORD

Create Smart Group to Migrate from Android (Legacy) to Android Work Profile

Workspace ONE UEM customers currently deployed under Android (Legacy) can migrate to Android Work profile mode to manage their Android devices. This use case walks you through the creating Smart Groups, creating a new migration, and tracking the status of the migration.

The Workspace ONE UEM console provides a seamless process that helps you create Smart Groups to migrate all devices from Android (Legacy) to Android Work Profile deployment.

Prerequisites

Before you migrate, you will need to create Smart Groups for all devices that are being migrated. You can create separate groups for staging a small number of devices for testing purposes before you deploy to all your devices.

Procedure

1. Select the applicable **Organization Group (OG)** to which your new smart group applies and from which it can be managed. Selecting an OG is optional.
2. Navigate to **Groups & Settings > Groups > Assignment Groups** and then select **Add Smart Group**
3. Enter a **Name** for the smart group.
4. Configure the Smart Group type:
    - **Criteria**: This option works best for groups with large numbers of devices (more than 500) that receive general updates. This method works best because the inherent details of these groups can reach all endpoints of your mobile fleet.

- **Devices or Users**: This option works best for groups with smaller numbers of devices (500 or fewer) that receive sporadic, although important, updates. This method works best because of the granular level at which you can select group members.

Note Switching between the two smart group types will erase any entries and selections you might have made.

At least one device deployed as Android (legacy) needs to be selected as eligible for migration or you will get errors while setting up the migration.

5 Select **Save**.

What to do next

After your Smart Groups are created, you are ready to walk through the prerequites to begin the migration.

Prerequisites for Migrating to Android Enterprise to Work Profile Android (Legacy) Migration

To provide an intuitive end user experience for the migration, this page will guide you through a successful migration. Not completing these steps could result in a failed migration or users not being able to access all apps they need.

Device Eligibility

Device needs to be eligible for migration. For example. Samsung devices with Knox Container enabled cannot be migrated.

Check eligibility for migration by navigating to **Device Details > Custom Attributes** and make `sure migration.eligible` attribute has a value of `True`.

Recreate Profiles for Android

Android Enterprise profiles are separate from device administrator, or Android (Legacy) profiles. You must re-create profiles for Android enterprise. These profiles are available for configuration after completing the Android enterprise registration.

On UEM consoles lower than 9.4.0, Android enterprise profiles are available under `Devices > Profiles & Resources > Profiles > Add > Add Profile > Android > Android for Work`.

On UEM consoles 9.4.0 and higher, Android enterprise profiles are available under `Devices > Profiles & Resources > Profiles > Add > Add Profile > Android`.

Note If the Wi-Fi profile was configured for your Android (Legacy) deployment, you must create and assign an Android Wi-Fi profile to the devices selected for migration before you can create a migration.

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

Configure Application Management

Once an application is added to the Workspace ONE UEM console, it can be distributed to device administrator, also known as Android (Legacy), and Android enterprise enrollments. If a public application has been added to the UEM console prior to Android enterprise registration, the application management section of this guide will help you configure settings so there will be no disruption to existing app assignments.

Internal applications cannot be managed for Work Profile management mode under Android Enterprise. In order to make sure internal applications are available for devices that have migrated to Work Profile, you must upload the application to the Managed Google console as a private application prior to migration.

Use Workspace ONE UEM to manage the deployment and maintenance of publicly available mobile applications from Google Play Store. Make sure every public app is approved for your organization to ensure seamless migration.

Verify Network Settings

The Network Requirements for Android is a list of known endpoints for current and past versions of enterprise management APIs. Check your network settings to ensure a connection between Workspace ONE, the Google Play Store, and Android devices. For more information, see Network Requirements for Android.

Manage Public Apps for Android (Legacy) Migration

If a public app has been added to the UEM console prior to the Android (Legacy) migration and Android Enterprise registration, this task will help you make sure all apps are imported after the migration.

These steps simply ensure the UEM console is aware the app has been approved on managed Google Play. It is now possible to assign this app to Android enterprise enrollments after the migration has completed.

Procedure

1. Navigate to https://play.google.com/work (log in with the same Gmail account used to configure Android enterprise), search for the app(s) and approve it for your organization.
2. In the UEM console, navigate to `Apps & Books > Native > Public > Add Application > Android > Import from Play` .
3. Select Import once the list of approved apps displays

   After migration, the app cache is cleared and users will have to re-enter there credentials.

Migrating to Work Profile From Android (Legacy) Using Migration Tool

The Workspace ONE UEM console provides a migration tool that allows you to complete all prerequisites, select smart groups, configure a custom message for your users, and a dashboard to view a summary page of the migrated devices including eligilibity status and reason for failure or success.

Prerequisites

Be sure to have completed the prerequisites to avoid failed migration or users not being able to access all apps they need. For more information on prerequisites see: Prerequisites for Migrating to Android Enterprise to Work Profile Android (Legacy) Migration .

Procedure

1 Navigate to **Devices > Lifeycle > Legacy Android Migration** and select **New Migration**.

2 Complete the prerequisites and select **Next** to move to the **Details** tab.

Details	The details tab allows you to select the Smart Groups you want to migrate
Name	Enter a friendly name for the migration group.
Description	Enter detailed description of the migration group.
Smart Groups	Specify which smart groups to receive the migration. Smart Groups must include Android (Legacy) deployments. You will receive an error message if a Smart Group is not eligible to be included in the migration.
Message	After users have chosen to upgrade to Android Enterprise, this message will inform them about the migration and prompt them to take action to proceed.

3 Select **Validate**. Selecting validate retrieves the number of devices eligible for migration.

4 Select **Continue** once all devices are validated for migration. You cannot continue until a valid Smart Group is selected.

A **Summary** page displays showing details such as list of devices, migration eligibility, and reason the device is not eligible, when applied

5 Select **Create** to create the migration.

A notification is sent to eligible devices in the selected Smart Groups informing users about migration and prompting them to perform necessary actions to proceed. You can monitor progress on the Legacy Android Migration page. From this page you can select migrations from the list view to display the Migration Details page.

Note During Android (Legacy) migration to Android Enterprise, based on the setting in the Scheduler the migration command is automatically sent for the first batch size (300) of devices instantly. After the first 300 devices, the remaining devices will receive the command at the determined intervals. You can view the settings in the UEM console under **Admin > Scheduler.**

What to do next

See the Migration Details Page for more information

Migrate to Android Enterprise Using Zero Touch Enrollment

Zero-touch enrollment allows Android devices to be configured in bulk with Workspace ONE UEM as your EMM provider right out of the box without having to manually setup each device. Using Zero-touch enrollment with your Android (Legacy) migration allows you to move your devices to Fully Managed mode with ease and ensuring the migration is completed securely.

TBD

Procedure

1 Setup the Workspace ONE UEM console by completing the prerequisites for Android (Legacy) Migration. Find the steps Prerequisites for Migrating to Android Enterprise to Work Profile Android (Legacy) Migration .

2 Complete Zero-Touch enrollment to get your devices added into the Zero-Touch portal. To get started, see Enroll Android Device Zero Touch Portal

3 Test and make sure the migration flow works for your test devices.

Note Remember a Wi-Fi profile has to be created for the migration to be successful.

4 Send a "Device Wipe" command to the devices previously managed under Android (Legacy).

Migration Details Page

The **Migration Details** pages allow you to track the migration by migration group, details, status, and list view of devices included in migration.

Legacy Android Migration List View

The Legacy Android Migration List View automatically displays after you create a new migration page. The list view helps you to view all the real-time updates of your end user devices that you are migrating with the Workspace ONE UEM console. The list view allows you to:

- Edit specific migrations by selecting the radio button on the desired migration friendly name. You can update the migration for new devices added to the Smart Group by selecting **Edit**.
- Delete migration groups which prevents devices in queue from migrating from Legacy Android by withdrawing the persistent notification. Android Work Profile is not removed from devices that have already migrated.
- Search and narrow down a device using the Search option.

Legacy Android Migration Details Page

The Migration Details page is accessed by selecting a migration Friendly Name from the Legacy Android Migration List View with the Workspace ONE UEM console to review the status of the migration. You can view a graphical overview, status, and reason for the migration failing or succeeding.

Use the Migration Details page to push the migration command to the device with the **Retry** button if the migration fails.

Customize a message to the devices in the migration batch with the **Notify** button. Configure the field as followed:

- **Message Type**: Select the message type (email, SMS, or push) that Workspace ONE UEM uses for this template.
- **Subject**: Enter the message subject.
- **Message Body**: Enter the message Workspace ONE UEM displays on the end-user devices for each message type.

Frequently Asked Questions for Android (Legacy) Migration

To help you better understand the Android (Legacy) migration, here are some commonly asked questions and best practices to make for a successful migation.

FAQ's

- **When I enable Android enterprise in an organization group, does it affect my existing device administrator enrollments?**
  - Current device administrator enrollments will remain enrolled and will receive all assigned profiles and apps. Enabling Android enterprise will affect new enrollments only; when a new Android enterprise-capable device enrolls it will use Android enterprise. If a device is not Android enterprise capable, it will enroll using device administrator.

- **Can device administrator and Android enterprise co-exist in the same UEM console?**
  - Device administrator enrollments and Android enterprise enrollments can co-exist in the same organization group. Profile management is separated as Android and Android (Legacy) for Android enterprise and device administrator enrollments respectively.

    Additionally, with UEM console v9.2.0+ it is possible to override Android enterprise enrollments at specific organization groups, or even limit it to specific smart groups.
- **Can I use Product Provisioning with Android enterprise?**
  - Product Provisioning is supported on Fully Managed devices.
- **Are OEM-specific management capabilities available on devices enrolled through Android enterprise?**
  - OEM-specific management capabilities are possible through OEMConfig. OEMs such as Samsung and Zebra have created public apps that can be added to the Workspace ONE UEM console. These apps provide app configuration key-value pairs that can alter device capabilities.
- **Does Workspace ONE Assist work with Android Enterprise?**
  - Workspace ONE Assist is compatible with all Android Enterprise enrollment options.
- **Can new customers use Android (Legacy)?**
  - New Workspace ONE UEM customers must setup Android Enterprise to deploy Android devices.
  - Existing customers can disable and re-enable Android (Legacy) as desired.

Best Practices for Android (Legacy) Migration

When to migrate to Android Enterprise is at the discretion of your business needs and timing of the actual migration depends on you organization's use cases. Here are a few considerations:

- If your current devices are unlikely to receive Android 10, or the OS updates are controlled by your organization, it is not necessary to migrate these devices. You can deploy Android enterprise for newly purchased devices.
- BYOD devices are the most vulnerable as end users are likely to update their devices to the latest operating system. A migration from device administrator to work profile can be achieved using the Android Legacy Migration feature in the Workspace ONE UEM console. To get started, see Migrating to Work Profile From Android (Legacy) Using Migration Tool.

Android (Legacy) Enrollment 2

Each Android device in your deployment must be enrolled before it can communicate with Workspace ONE UEM and access internal content and features. Enrollment is facilitated with the Workspace ONE Intelligent Hub for Android as the Device Administrator for Android (Legacy) deployment.

You can enroll devices using a web-based process that automatically detects if the Workspace ONE Intelligent Hub is already installed. Additionally, you can pre-enroll devices for end users, or end users can enroll their own devices.

Available for download from the Google Play Store and the Amazon App Store, the Workspace ONE Intelligent Hub for Android provides a single resource to enroll a device as well as provide device and connection details. Additionally, 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.

Note Certain Android OEM vendors offer features and capabilities that you can enable in the Workspace ONE UEM console. See Install the Platform OEM Service

Note: Looking for Android with Google Registration?, see the VMware AirWatch Android Platform Guide.

Requirements for Enrollment

Autodiscovery is a simplified approach that leverages information end users likely already know for enrollment purposes. For more information, see Email Autodiscovery

Enrollment Restrictions

You can create enrollment restrictions based on Android (Legacy) manufacturer and model to ensure only approved devices are allowed to enroll with Workspace ONE UEM.

Android (Legacy) Enrollment with the Workspace ONE Intelligent Hub

The Workspace ONE Intelligent Hub application facilitates enrollment and allows for real-time management and access to relevant device information. The enrollment process secures a connection between Android (Legacy) devices and your Workspace ONE UEM environment. For more information, see Enrolling an Android Device with the Workspace ONE Intelligent Hub.

Workspace ONE Intelligent Hub Sideloading to Android Devices

Sideloading allows you to deploy the Workspace ONE Intelligent Hub to Android devices asd device administrator without using the Google Play Store. For more information, see Workspace ONE Intelligent Hub Sideloading for Android (Legacy) Deployment.

OEM Service App

The OEM Service app is a plug-in app that is only installed and used in combination with Workspace ONE Intelligent Hub enrollment. It allows for additional MDM capabilities that only pertain to a specific OEM device. For more information, see Chapter 9 OEM Service App.

Platform OEM Service

The Platform OEM Service is an additional app that allows Workspace ONE UEM to provide extended management capabilities to any Android device deployment. For more information, see Chapter 10 Platform OEM Service.

Email Autodiscovery

Autodiscovery is a simplified approach that leverages information end users likely already know this information.

You can associate an email domain to your environment for Auto Discovery, which requires users to enter only an email address and credentials (and in some cases select a Group ID from a list) to complete enrollment.

Alternatively, if you do not set up an email domain for enrollment, end users are prompted for the Enrollment URL and Group ID, which must be given to them. See the Auto Discovery section of the **VMware AirWatch Mobile Device Management Guide** for more information on setting up auto discovery enrollment.

This chapter includes the following topics:

- Enrollment Restrictions for Android
- Enrolling an Android Device with the Workspace ONE Intelligent Hub
- Workspace ONE Intelligent Hub Sideloading for Android (Legacy) Deployment
- Hub-Based Sideload Enrollment

Email Autodiscovery

Autodiscovery is a simplified approach that leverages information end users likely already know this information.

You can associate an email domain to your environment for Auto Discovery, which requires users to enter only an email address and credentials (and in some cases select a Group ID from a list) to complete enrollment.

Alternatively, if you do not set up an email domain for enrollment, end users are prompted for the Enrollment URL and Group ID, which must be given to them. See the Auto Discovery section of the **VMware AirWatch Mobile Device Management Guide** for more information on setting up auto discovery enrollment.

Requirements for Android (Legacy) Enrollment

Before enrolling your Android (Legacy) method, you must have credentials and enrollment URL.

If an email domain is associate with your environment with Auto Discovery:

- **Email address** – This is your email address associated with your organization. For example, **JohnDoe@acme.com**.
- **Credentials** – This **username** and **password** allows you to access your Workspace ONE UEM 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, you are still prompted to enter your email domain. Since auto discovery is not enabled, you are then prompted for the following additional 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 UEM console.
- **Credentials** – This unique username and password pairing allows you to access your Workspace ONE UEM environment. These credentials may be the same as your network directory services or may be uniquely defined in the UEM console.

To download the Workspace ONE Intelligent Hub for Android and subsequently enroll an Android (Legacy) device, you'll need the **Enrollment URL**. The **Enrollment URL** is AWAgent.com for all users, organizations, and devices enrolling into Workspace ONE UEM.

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.

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

You can create enrollment restrictions based on:

- Android manufacturer and model to ensure only approved devices are enrolled into Workspace ONE UEM.

  Note Some devices are manufactured by other vendors. You can create a policy with the actual manufacturer of the device for policies to come into effect.The following are some ways to identify the device manufacture:

  - Navigate to the **About** page in device settings.
  - With an adb command: `adb shell getprop | grep "manufacturer"`.

- Allow or deny devices by UDID, IMEI, and serial number.

  Note When enrolling Android 10 or later devices into Work Profile mode, the devices are held in a pending status until the UEM console is able to retrieve the IMEI or Serial Number from the the devices to see if they are allowed or denied. Until this is verified, the device will not be fully enrolled nor any work data sent until enrollment is complete.

For more information, see Create an Enrollment Restriction Policy.

Enrolling an Android Device with the Workspace ONE Intelligent Hub

The Workspace ONE Intelligent Hub is the application that facilitates enrollment and allows for real-time management and access to relevant device information.

Procedure

1 Navigate to **AWAgent.com** from your browser. You can also send the enrollment URL to devices using SMS text message.

  Workspace ONE UEM automatically detects if the Workspace ONE Intelligent Hub is installed on your device and, if it is not, redirects you to the App Store to download it. A Google ID is required to download the Workspace ONE Intelligent Hub from the Google Play store

2 Download and install the Workspace ONE Intelligent Hub from the App Store, if needed.

   To ensure successful installation and running of the Workspace ONE Intelligent Hub on your Android device, the device will need to have a minimum of 60mb of space available. CPU and Run Time Memory are allocated per app on Android platform. If an app uses more than allocated, Android devices will optimize by killing the app.

3 Launch the Workspace ONE Intelligent Hub or return to your browser session to continue enrollment.

   a If you have configured email autodiscovery, then it 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, you can select Server Details or QR code enrollment options.

   c At first launch, the Workspace ONE Intelligent Hub asks the user to accept permissions where the app requests to use specific device features. Permissions for camera, phone, location, and storage will need to be turned on or it will affect functionality. This applies to devices running Android 6.0+ with Workspace ONE Intelligent Hub v5.3 for Android.

   d The permissions include granting Workspace ONE UEM permission to collect user data to optimize security and productivity for your device. The information to be collected includes: Phone Number, Installed Applications, Serial Number, UDID (Universal Device Identifier),IMEI (International Mobile Equipment Identity), SIM Card Identifier, Mac Address, Currently Connected SSID.

4 Enter your username and password

5 Follow the remaining prompts to complete enrollment.

   You may be notified at this time if your user account is not allowed or blocked because your account is blacklisted and not approved for enrollment.

Workspace ONE Intelligent Hub Sideloading for Android (Legacy) Deployment

Sideloading allows you to deploy the Workspace ONE Intelligent Hub to devices using Android (Legacy) management without using the Google Play Store.

Sideload the Workspace ONE Intelligent Hub in the following situations:

- Sideload the Workspace ONE Intelligent Hub on to the following devices because these devices do not have access to the Google Play Store:
- Sideload the Workspace ONE Intelligent Hub if the company prohibits the use of Google Accounts. Users need a Google Account to access the Google Play Store.

Hub-Based Sideload Enrollment

The process of sideloading an Android (Legacy) device affects the device's ability to upgrade the Workspace ONE Intelligent Hub version.

For the sideloaded Android (Legacy) device to receive the Workspace ONE Intelligent Hub upgrade, you must deploy the new Hub version as an internal application through the Workspace ONE UEM console. You can get the upgrade file from your Workspace ONE UEM Account Manager.

You do not need to deploy the Workspace ONE Intelligent Hub as an internal application for upgrade if the company does not prohibit the use of Google Accounts. When users receive staged devices, they can download personal Google Accounts to the staged devices. With their personal Google Accounts, they can access the Google Play Store to upgrade the Workspace ONE Intelligent Hub.

Sideload Workspace ONE Intelligent Hub Using a USB Port

Drag and drop the Workspace ONE Intelligent Hub from a computer to Android devices. Use this method to stage the Workspace ONE Intelligent Hub on a small number of devices.

Procedure

1. Put the Workspace ONE Intelligent Hub .apk file on a computer for easy access.

   If you do not have the latest version, ask your Workspace ONE UEM Account Manager for it.
2. Prepare the Android (Legacy) device for sideloading. On the device, navigate to **Settings > Security > Unknown sources** and select **Allow installation of non-Market apps**.
3. Connect a device to the computer using the USB port and a USB cable.
4. For the computer to communicate with the device, select the **Turn on USB storage** button on the device.

   The computer detects the device drive.
5. Select the **Open folder to view files** option on the computer to open the device drive.
6. From the computer, drag and drop the Workspace ONE Intelligent Hub .apk file to the device.

   Do not put the .apk file in the device's USB Storage folder because you cannot access the USB Storage folder from the device.
7. Disconnect the device from the computer.
8. Using the native file manager or the **Files** application on the device, select the **AirWatchAgent_x.x.apk** file.
9. Select install.

What to do next

After the installation completes, select the prompt to open the Workspace ONE Intelligent Hub and begin enrollment.

Sideload Workspace ONE Intelligent Hub Using a Hosted Download Site

Send users a link that connects their Android (Legacy) devices to the Workspace ONE Intelligent Hub .apk file that you host on an internal server. Use this method to deploy the Workspace ONE Intelligent Hub to a large number of devices.

Procedure

1. Host the Workspace ONE Intelligent Hub .apk file on an internal server that is accessible by devices for download.

   If you do not have the latest version, ask your Workspace ONE UEM Account Manager for it.
2. Instruct users to prepare the device for sideloading.
3. On the device, users navigate to **Settings > Security > Unknown sources** and select **Allow installation of non-Market apps**.
4. Send an email or text message that contains a direct link to the Workspace ONE Intelligent Hub .apk file to applicable users.
5. Direct users to navigate to and select the hosted file to install the Workspace ONE Intelligent Hub.
6. Instruct users to select the Workspace ONE Intelligent Hub download notification in the download notifications area on the device.
7. Instruct users to select the **AirWatchAgent_x.x apk** file.

   If users miss the download notification, they can find the Workspace ONE Intelligent Hub .apk file in the **Download** folder. The Download folder is in the native file manager or the **Files** application.
8. Direct users to select install.

What to do next

After installation completes, have users select the prompt to open the Workspace ONE Intelligent Hub and begin enrollment.

Profiles for Android (Legacy) 3

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

The individual settings you configure, such as passcodes, Wi-Fi, VPN, and email, are called payloads. When creating profiles, consider configuring one payload per profile, which means you can have multiple profiles for the different settings you want to push to devices. For example, you can create a profile to integrate with your email server and another to connect devices to your workplace Wi-Fi network.

It is important to note that if two profiles are applied with conflicting restrictions, then the device will implement the most restrictive setting.

Device Profiles and Container Profiles

Note When you apply a device profile to a Samsung Knox enabled device, it will take effect but apply to the entire device – not just the container – by default.

Note Android M devices uses power-saving options for idle apps and devices. If a user unplugs a device and leaves it stationary, with its screen off, the device goes into **Doze** mode, where it attempts to keep the device in a sleep state. There is no network activity during this time. Also, **App Standby** mode allows the device to determine that an app is idle when the user is not actively using it. When device is in either state, the Workspace ONE UEM console does not receive reports on device details. When the user plugs a device in to charge or opens an app, the device resumes normal operations and reporting from AirWatch apps installed on the device to the Workspace ONE UEM console resumes.

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.

Device Access

Some device profiles configure the settings for accessing an Android (Legacy) 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 Device Passcode Profile (Android (Legacy))
- Specify and control how, when and where your employees use their devices. For more information, see Configure Restrictions Profile (Android Legacy)) .

Device Security

Ensure that your Android (Legacy) devices remain secure through device profiles. These profiles configure the native Android (Legacy) 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 Create a VPN Profile (Android (Legacy)).
- Take administrative actions when a user installs or uninstalls certain applications. For more information, see Application Control Profile (Android (Legacy)).

Device Configuration

Configure the various settings of your Android (Legacy) 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 (Legacy)) .
- Access a URL directly from an icon on the device's menu. For more information, see Bookmarks for Android (Legacy) Devices

This chapter includes the following topics:

- Device Passcode Profile (Android (Legacy))
- Configure Restrictions Profile (Android Legacy))

- Wi-Fi Profile (Android (Legacy))
- Create a VPN Profile (Android (Legacy))
- Forcepoint Content Filter Profile (Android (Legacy))
- Deploy Email Account Settings (Android)
- Exchange Active Sync Profile (Android (Legacy))
- Application Control Profile (Android (Legacy))
- Bookmarks for Android (Legacy) Devices
- Credentials Profile
- Workspace ONE Launcher
- Configure Firewall Rules for Android Devices
- Configure a Global Proxy (Android)
- Set Date/Time (Android)
- Configure Sound Profiles (Android)
- Configure Firewall Rules (Android(Legacy))
- Configure a Display Profile (Android)
- Deploy Advanced Profile (Android)
- Configure Custom Settings (Android)

Device Passcode Profile (Android (Legacy))

The passcode policy requires users to protect their devices with a passcode each time they return from an idle state. This policy ensures that all sensitive corporate information on managed devices remains protected.

The complexity of the passcode can vary. You can set simple passcodes so that users can quickly access device content or set complex alphanumeric passcodes for an added layer of security. Fingerprint authentication can be set as a primary method of authentication but most devices require a backup to also be entered when using fingerprint.

Important For Samsung devices supporting Fingerprint Authentication, it is required for the device to have a backup password. If the device already has a passcode prior to enrolling, and a fingerprint passcode requirement is enforced from the Workspace ONE UEM console, the end user will be prompted to set a complex passcode as a back up.

You can enforce two types of passcode policies: one for devices and another for access to applications in the event there is a container on a device.

Enforce Device Passcode (Android (Legacy))

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 **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.

2 Select **Device** to deploy your profile to a device.

3 Configure the **General** profile settings.

4 Configure the following Passcode settings.

Setting	Description
Minimum Passcode Length	Ensure passcodes are appropriately complex by setting a minimum number of characters.
Passcode Content	Ensure the passcode content meets your security requirements by selecting **Any**, **Numeric**, **Alphanumeric**, **Alphabetic**, or**Complex** or **Fingerprint** from the drop-down menu. The Fingerprint Authentication is only available on SAFE v5.0+ devices. Do not use Fingerprint authentication as a classic password when you are checking security requirements. When you are enabling fingerprint authentication to unlock the device or container, a PIN or password is also required. A PIN or passcode is required for recovery when enabling fingerprint authentication. Two factor authentication is not the default setting for a device or container. You cannot enforce fingerprint authentication without requiring a PIN or passcode. **Important** For Safe v5.2 and above, if the minimum number of complex characters in the password set by the profile is greater than 4, then at least one lowercase character and one uppercase character are required. **Note** If the passcode is not compliant, access to company resources, such as email, may be restricted and profiles are removed.
Pre-Define Passcode	This setting is only available on Android Work-managed or COPE enrolled devices with Android 8.0 or later and Workspace ONE Intelligent Hub 8.0 or later for Android. Consider Android (Legacy) Device Administrator Migration to Android Enterprise for more control, consistency and better security across all OEM devices.
Passcode	This setting is only available on Android Work-managed or COPE enrolled devices with Android 8.0 or later and Workspace ONE Intelligent Hub 8.0 or later for Android. Consider Android (Legacy) Device Administrator Migration to Android Enterprise for more control, consistency and better security across all OEM devices.
Maximum Number of Failed Attempt	Specify the number of attempts allowed before the device is wiped.
Grace Period for Passcode Change	Amount of time prior to the expiration of the passcode that the end user is notified to change their passcode

Setting	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.
Maximum Passcode Age (days	Specify the maximum number of days the passcode can be active.
Passcode History	Set the number of times a passcode must be changed before a previous passcode can be used again.
Device Lock Timeout (in Minutes)	Set the period of inactivity before the device screen locks automatically. If the device time-out set on the profile is greater than maximum time-out on the device, Workspace ONE Intelligent Hub will not be able set that value for device time-out.
Enable Passcode Visibility	Enable to make the passcode visible to users as it is entered on their devices.
Allow Fingerprint Unlock	Enable to allow users to use their fingerprint to unlock their devices and prevents using fingerprint as the primary method of authentication and instead requires that the end user enter the specified type of password in the profile instead.
Require Storage Encryption	Indicate if internal storage requires encryption.
Require SD Card Encryption	Indicate if the SD card requires encryption.
Lockscreen Overlay	Enable to push information to the end user devices and display this information over the lock screen. ■ **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. 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.

5 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 **Resources > Profiles & Baselines > 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 and available across several OEMs.

The Lockscreen Overlay settings for **Android** profiles on only 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**.

Configure Restrictions Profile (Android Legacy))

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.

Procedure

1. Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.
2. Select **Device** to deploy your profile to a device.
3. Configure the profile's **General** settings.
4. Select the **Restrictions** payload from the list. You can select multiple restrictions as part of a single restrictions payload.
5. Configure **Restrictions** settings as needed for your enterprise.
6. Select **Save & Publish**.

Restrictions Profile Overview (Android (Legacy))

Restriction profiles lock down native functionality of Android (Legacy) devices and vary significantly based on OEM. Removing the restrictions profile is the recommended method for removing the restrictions from the device.

For further special considerations for enabling certain restrictions, see Best Practices for Configuring Restrictions with Android (Legacy) Devices

Setting	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.
Sync and Storage	Control how information is stored on devices, allowing you to maintain the highest balance of productivity, security, and firmware updates. For example disabling Google or USB Backup keeps corporate mobile data on each managed device and out of the wrong hands.
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.+
Bluetooth	Limit file sharing through bluetooth by disallowing bluetooth behaviors such as outgoing calls and data transfer.
Network	Prevent devices from accessing Wi-Fi and data connections to ensure that end users are not viewing sensitive information using an insecure connection.
Roaming	Allow/disallow device functionality while roaming to configure telecom settings for your devices.
Tethering	Prevent end users tethering with other devices to keep unmanaged devices from viewing sensitive information about your device fleet.
Browser	Limit the behavior of your browser to maximize security. If implementing VMware Browser, ensure you disable Allow Native Android Browser to restrict browsing activity to the VMware Browser.
Location Services	Determine the hard keys end users can utilize to limit the level of device functionality to a level that is appropriate for your organization.

Setting	Description
Phone and Data	Configure phone and data limits and restrictions to keep device usage within the parameters of your organizations plan. You can also allow or prevent incoming and outgoing calls and SMS messages by selecting **Add** underneath **Call And SMS Restriction** and selecting the direction, type, and restriction. Set **Maximum Data Usage** to determine the amount of data network usage per day, week, or month. The Frequency, Size and Maximum fields will report one month usage from the time the profile was pushed to the device. Set MMS restrictions to allow incoming and outgoing MMS messages.
Miscellaneous	Configure the font and font size for your device to give it a customized look and feel.
Hardware Restrictions	Determine the hard keys end users can utilize to limit the level of device functionality to a level that is appropriate for your organization.
Security Restrictions	Allow/disallow security functionality such as forcing fast encryption and firmware recovery. **Important** If the administrator wants to disable upgrading OS using firmware over the air, they cannot do so if they disable Firmware Recovery. Firmware Recovery must be enabled in order for the restriction on OS upgrades to work.

Wi-Fi Profile (Android (Legacy))

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

The Wi-Fi profile also automatically configures devices to connect to the appropriate wireless network while in an office. For end users who travel to various locations, the Wi-Fi profile ensures that they have their own unique wireless networks.

Workspace ONE UEM cannot change the Wi-Fi configuration if a user already has their device connected to a Wi-Fi network through a manual setup. If the Wi-Fi password has been changed the updated profile is pushed to enrolled devices, some users have to update their device with the new password manually.

Configure Wi-Fi Profile (Android (Legacy))

The Wi-Fi profile must be configured for a device that has no previously been configured on an existing network.

Procedure

1. Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.
2. Select **Device** to deploy your profile to a device.
3. Configure the **General** profile settings as appropriate.
4. Select the **Wi-Fi** payload.

5 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 connects to the network with no end-user interaction.
Security Type	Specify the access protocol used and whether certificates are required. Depending on the selected security type, the displayed fields will change. If **None, WEP,or WPA/WPA 2)** are selected; the **Password** field will display. If **WPA/WPA 2 Enterprise** is selected, the Protocols and Authentication fields display. ■ **Protocols** ■ Use Two Factor Authentication ■ SFA Type ■ **Authentication** ■ Identity ■ Anonymous Identity ■ Username ■ Password ■ Identity Certificate ■ Root Certificate
Password	Provide the required credentials for the device to connect to the network. The password field displays when **WEP, WPA/WPA 2, Any (Personal), WPA/WPA2 Enterprise** are selected from the **Security Type** field.
Include Fusion Settings	Enable to expand Fusion options for use with Fusion Adapters for Motorola devices. **Note** Fusion Settings apply only to Motorola Rugged devices.
Set Fusion 802.11d	Enable to use the Fusion 802.11d to set the Fusion 802.11d settings. **Note** Fusion Settings apply only to Motorola Rugged devices.
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.
Proxy Type	Select the Proxy Type as **Manual Proxy** or **Proxy Auto Configuration** to configure proxy settings.
Proxy Server	Enter the host name of IP address for the proxy server.
Proxy Server Port	Enter the target port for the proxy server.
Exclusion List	Add hostnames to the Exclusion List to prevent them from routing through the proxy.
PAC URL	Enter the URL which defines how web browsers and other user agents can automatically choose the appropriate proxy server (access method). This field displays if Proxy Auto Configuration is selected.

6 Select **Save & Publish**.

Create a VPN Profile (Android (Legacy))

Virtual private networks (VPNs) provide 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.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.

2 Select **Device** to deploy your profile to a device.

3 Configure the profile's **General** settings.

4 Select **VPN**and configure the settings. The Authentication settings that display vary based on the Connection Type selected from the Connection Info section. The table below defines all settings that can be configured based on the VPN client.

Setting	Description
Connection Type	Choose the VPN client that is used to connect VPN sessions. **Important** **Cisco AnyConnect**, **Juniper Junos Pulse** and **F5 SSL** 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. Additionally, a Forcepoint specific **Certificate Authority** must be established to enable a **Websense (Forcepoint)** VPN connection. See Forcepoint Content Filter Profile (Android (Legacy)) for more information.
Connection Name	Enter the display name of the connection to be displayed on the device.
Server	Enter the hostname or IP address for the server used for VPN connections.
Per-app VPN Rules	Enable Per App VPN that allows you to configure VPN traffic rules based on specific applications. This field only displays for supported VPN vendors. If you are using VPN connections for specific managed apps, see Configure Per-App VPN (Android). Per-app VPN is supported on Android 5.0+devices.
Username	Provide the credentials required for end-user VPN access. Depending on the connection type and authentication method, use lookup values to automatically fill user name info to streamline the login process.
Shared Secret	Provide the encrypted key stored on the VPN server and used by the profile for VPN access.
Encryption	Enable to encrypt traffic on this connection.
Identify Certificate	Enter the certificate credentials used to authenticate the connection.
Use Web Logon for Authentication	Enable to redirect users to the web page of the selected VPN client for the user to enter their user credentials for authentication.
Realm	Define the server used to authenticate the device.

Setting	Description
Role	Defines the network resources that the device can access.
Password	Provide the credentials required for end-user VPN access.
Server	Enter the hostname or IP address of the server for connection.
User Authentication	Choose **Password** or **Certificate** as the method required to authenticate the VPN session.
Enable VPN On Demand	Enable VPN On Demand to use certificates to automatically establish VPN connections.
Proxy	Select either **Manual** or **Auto** proxy type to configure with this VPN connection.
Server	Enter the URL of the proxy server.
Port	Enter the port used to communicate with the proxy.
Username	Enter the user name to connect to proxy server.
Password	Enter the password for authentication.

5 Select **Save & Publish**.

Configure Per-App VPN (Android)

Per-app VPN allows you to configure VPN traffic rules based on specific applications. When configured, the VPN can automatically connect when a specified app is launched as well as send the application traffic through the VPN traffic but no traffic from other applications.

Prerequisites

Per- App VPN is supported on Android 5.0+ devices.

Procedure

1 Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.

2 Select the **VPN** payload from the list.

3 Configure your Create a VPN Profile (Android (Legacy)) settings. Per-app VPN displays on supported vendors selected from the Connection Type field.

4 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.

5 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.

Configure Public Apps to use the VPN Profile (Android)

To be able to enforce VPN on public apps, you will have to perform a few additional steps.

Procedure

1 Navigate to **Apps & Books > List View**.

2 Select the **Public** tab

3 Select **Add Application** and add an Android app or **Edit** an existing Android app.

4 On the Deployment tab, select **Use VPN** and then select the **Per App VPN Profile** client you created above.

5 **Save & Publish**.

Forcepoint Content Filter Profile (Android (Legacy))

Forcepoint lets you leverage your existing content filtering categories in Forcepoint and apply those to devices you manage within the Workspace ONE UEM console .

Directory users enrolled in Workspace ONE UEM are validated against Forcepoint to determine which content filtering rules to apply based on the specific end user. You can enforce content filtering with Forcepoint in one of two ways:

- Use a VPN profile, which applies to all web traffic using browsers other than the VMware Browser. This method is described below.
- Use the **Settings and Policies** page, which applies to all web traffic using the VMware Browser.

Directory-based end users will now have access to permitted sites based on your Forcepoint categories. If you enable SSL decryption for the Android (Legacy) devices, you will need to download a Forcepoint root certificate from the Forcepoint cloud service. You will upload the certificate to the Workspace ONE UEM console . Consider using the same profile that you used for your VPN settings. Navigate to **Devices > Profiles > List View** and select the VPN profile you created. Then, on the **Credentials** payload, upload your Forcepoint root certificate.

TRITON AP-MOBILE App

For Android (Legacy) device users, the TRITON AP-MOBILE app is required for TRITON AP-MOBILE to begin protecting their devices with Forcepoint. You will need to add the app as a public app to the Workspace ONE UEM console.

After the app is deployed to Android (Legacy) devices, device users receive a “Forcepoint VPN configuration” notification. Tapping the notification displays a second notification that “Forcepoint VPN configuration is ready.” Tapping the second notification launches the Forcepoint app. Device users then receive a request to allow TRITON AP-MOBILE to create a VPN connection. They should check the box that says, “I trust this application,” and then tap **OK**. To confirm that TRITON AP-MOBILE is protecting their device, the app homescreen should show Security as “ON.” If it does not, device users should try tapping the “Forcepoint VPN configuration is ready” notification again.

Configure Forcepoint Content Filter Profile (Android)

Allow or block access to websites according to the rules you configure in Forcepoint and then deploy a VPN payload to force devices to comply with those rules.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.

2 Select **Device** to deploy your profile to a device.

3 Configure the profile's **General** settings.

4 Select **VPN**.

5 Select **Websense (Forcepoint)** as the **Connection Type**.

6 Configure the Authentication settings:

Setting	Description
Server	Enter the connection URL that was provided in the Forcepoint cloud service.
Username	Enter your username for the Fuser namet administrator's cloud service account.
Password	Enter your password used for the Forcepoint administrator's cloud service account. If your VPN connection password changes or expires, be sure to enter your new password in the VPN section to maintain the integration of Workspace ONE UEM with the Forcepoint cloud service. For this reason, consider setting your password to not expire.

7 Select **Test Connection** to make sure your authentication settings are able to connect successfully.

8 Select **Save & Publish**.

Deploy Email Account Settings (Android)

You can configure email settings externally from Exchange Active Sync (EAS) by deploying an **Email Settings** profile payload. This profile creates an IMAP or POP account using your individual email settings and your devices native mail client.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.

2 Select **Device** to deploy your profile to a device.

3 Configure the profile's **General** settings.

4 Select the **Email Settings** profile payload.

5 Configure **Email Setting** settings to specify the basic rules for an email account and its interaction with the mail client including, including:

Setting	Description
Email Account	Enter the email service provider.
Email Address	Enter the user email address. You can use lookup values to use the device specific value.
Email Sync Interval	Determine how often email is synced to devices.
Sender's Name	Determine the displayed name on sent emails.
Signature	Enter an email signature to be displayed for all outgoing emails.
Set as Default Account	Enable to set this account as the default account used to send outgoing email.
Max Emails to Show	Determine the maximum amount of emails downloaded on the device.
Allow Attachments	Specify if attachments will be allowed to be included in emails.
Maximum Attachment Size	Enter the maximum attachment size allowed to be sent.
Use SSL	Enable to use Secure Socket Layer when sending/receiving emails.
Use TLS	Enable to use Transport Layer Security for authentication for sending/ receiving emails.
Protocol	Select the email protocol for incoming/outgoing mail.
Host Name	Enter the email server URL for incoming mail.
Port	Enter the number of the port assigned to mail traffic.
Username	Enter the username for the email account. Note that re-applying or re-pushing the email profile will prompt the end users for credentials again. Email will not be received until the credentials have been provided.
Password	Enter the password required to authenticate the end user. Note that re-applying or re-pushing the email profile will prompt the end users for credentials again. Email will not be received until the credentials have been provided.
Path Prefix	Enter the name of the root folder for the email account (IMAP only)
Ignore SSL Errors	Enable to allow devices to ignore SSL errors for Agent processes.
Use SSL	Enable to use Secure Socket Layer when sending/receiving emails.
Use TLS	Enable to use Transport Layer Security for authentication for sending/ receiving emails.
Protocol	Select the email protocol for incoming/outgoing mail.
Host Name	Enter the email server URL for incoming mail.
Port	Enter the number of the port assigned to mail traffic.
Username	Enter the username for the email account.
Password	Enter the password required to authenticate the end user.

Setting	Description
Path Prefix	Enter the name of the root folder for the email account (IMAP only)
Ignore SSL Errors	Enable to allow devices to ignore SSL errors for Agent processes.

6 Select **Save & Publish**.

Exchange Active Sync Profile (Android (Legacy))

The industry standard protocol designed for email synchronization on mobile devices is called **Exchange Active Sync (EAS)**. To guarantee a secure connection to internal email, calendars and contacts, Workspace ONE UEM integrates with multiple mail clients that configure EAS accounts on Android (Legacy) devices.

You have the option to configure the **EAS** profile payload using NitroDesk TouchDown, Lotus Notes, the AirWatch Inbox or the mail client native to the device.

Generic EAS Profile for Multiple Users

The generic EAS profile applies to all devices registered, but specific items such as username and password, are pulled using lookup values. Before you create an EAS profile that automatically enables devices to pull data from your mail server, you must first ensure End Users have the appropriate information in their user account records. For **Directory Users**, or those users who enrolled with their directory credentials, such as Active Directory, this information is automatically populated during enrollment. However, for **Basic Users** this information is not automatically known and must be populated in one of two ways:

- You can edit each user record and populate the **Email Address** and **Email Username** fields.
- You can prompt users to enter this information during enrollment by navigating to **Devices > Device Settings > General > Enrollment** and under the **Optional Prompt** tab, checking the **Enable Enrollment Email Prompt** box.

Deploy Exchange ActiveSync (EAS) Mail using Native Mail Client (Android (Legacy))

Create a configuration profile for the Native Mail Client.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.

2 Select **Device** to deploy your profile to a device.

3 Configure the profile's **General** settings.

4 Select the **Exchange ActiveSync** payload.

5 Configure Exchange ActiveSync settings:

Setting	Description
Mail Client	Select **Native Mail Client** as the account type.
Account Name	Enter a description for the mail account.
Exchange ActiveSync Host	Enter the external URL of your company's ActiveSync server. The ActiveSync server can be any mail server that implements the ActiveSync protocol, such as IBM Notes Traveler, Novell Data Synchronizer, and Microsoft Exchange.
Ignore SSL Errors	Enable to allow devices to ignore SSL errors for Agent processes.
Domain	Enter the end-user's domain. You can use the Lookup Values instead of creating individual profiles for each end user.
User	Enter the end-user's username. You can use the Lookup Values instead of creating individual profiles for each end user.
Email Address	Enter the end-user's email address. You can use the Lookup Values instead of creating individual profiles for each end user.
Password	Enter the password for the end user. You can use the Lookup Values instead of creating individual profiles for each end user.
Identity Certificate	Select (if desired) an Identity Certificate from the drop-down if you require the end user to pass a certificate in order to connect to the Exchange ActiveSync, otherwise select **None** (default). For more information needed to select a certificate for this payload, see Deploy Credentials (Android (Legacy)) profile.
Past Days of Mail to Sync	Select the number of days worth of past mail to sync with device.
Past Days of Calendar to Sync	Select the number of past days to sync on the device calendar.
Sync Calendar	Enable to allow calendars to sync with device.
Sync Contacts	Enable to allow contacts to sync with device.
Allow Sync Tasks	Enable to allow tasks to sync with device.
Maximum Email Truncation Size	Specify the size beyond which e-mail messages are truncated when they are synced to the devices.
Email Signature	Enter the email signature to be displayed on outgoing emails.
Allow Attachments	Enable to allow attachments with email.
Maximum Attachment Size	Specify the maximum attachment size in MB.
Allow Email Forwarding	Enable to allow email forwarding.
Allow HTML Format	Specify whether e-mail synchronized to the device can be in HTML format. If this setting is set to false, all e-mail is converted to plain text.
Disable screenshots	Enable to disallow screenshot to be taken on the device.
Sync Interval	Enter the number of minutes between syncs.

Setting	Description

Peak Days for Sync Schedule	■ Schedule the peak week days for syncing and the **Start Time** and **End Time** for sync on selected days.
	■ Set the frequency of **Sync Schedule Peak** and **Sync Schedule Off Peak**.
	  ■ Choosing **Automatic** syncs email whenever updates occur.
	  ■ Choosing **Manual** only syncs email when selected.
	  ■ Choosing a time value syncs the email on a set schedule.
	■ Enable **Use SSL**, **Use TLS** and **Default Account**, if desired.

S/MIME Settings	Select **Use S/MIME** From here you can select an S/MIME certificate you associate as a **User Certificate** on the **Credentials** payload. ■ **S/MIME Certificate** – Select the certificate to be used. ■ **Require Encrypted S/MIME Messages** – Enable to require encryption. ■ **Require Signed S/MIME Messages** – Enable to require S/MIME signed messages. Provide a **Migration Host** if you are using S/MIME certificates for encryption. Select **Save** to save the settings or **Save & Publish** to save and push the profile settings to the required device.

6 Select **Save** to save the settings or **Save & Publish** to save and push the profile settings to the required device.

Deploy Exchange ActiveSync (EAS) Mail Using IBM Notes Traveler (Android(Legacy))

Create a configuration profile for IBM Notes Traveler.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.

2 Select **Device** to deploy your profile to a device.

3 Configure the profile's **General** settings.

4 Select the **Exchange ActiveSync** payload.

5 Select **IBM Notes Traveler** for the **Mail Client** and configure the settings:

Settings	Description
Account Name	Fill in the field with a description of this mail account.
Exchange ActiveSync Host	Fill in the with the external URL of your company's ActiveSync server. The ActiveSync server can be any mail server that implements the ActiveSync protocol, such as Lotus Notes Traveler, Novell Data Synchronizer and Microsoft Exchange.
User	Fill in the field using look-up values. Look-up values pull directly from the user account record. To use the {EmailUserName} look-up values, ensure your Workspace ONE UEM user accounts have an email username defined.

a

6

7 Select **Save & Publish**.

Application Control Profile (Android (Legacy))

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, prevent a certain game application from ever installing on a device, or force the Workspace ONE Intelligent Hub to remain on a device.

Application Control is available only for specific device models. For a full list, please see the Android (Legacy) OEM Specific Profiles Matrix.

Configure Application Control (Android (Legacy))

To allow or prevent installation of applications on devices, you can enable Application Control to whitelist and blacklist specific applications.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.

2 Select **Device** to deploy your profile to a device.

3 Configure the profile's **General** settings.

4 Select the **Application Control** payload.

5 Enable or disable the following settings to set the level of control for your application deployments:

Settings	Description
Prevent Installation of Blacklisted Apps	Enable to prevent the installation and enforce the automatic removal blacklisted apps defined in Configure your Application Group **Note** For instructions on creating application groups, see Mobile Application Management Guide.
Prevent Un-Installation of Required Apps	Enable to prevent the un-installation of required apps defined in Configure your Application Group
Only Allow installation of Whitelisted Apps	Enable to prevent the installation of any application that is not a whitelisted app defined in Configure your Application Group

6 Select **Save & Publish**.

Configure your Application Group

Configure application groups, or app groups, so that you can use the groups in your compliance policies. Take set actions on devices that do not comply with the installing, updating, or removing applications.

You assign application groups to organization groups. When you assign the application group to a parent organization group, the child organization groups inherit the application group configurations.

Procedure

1 Navigate to **Resources > Apps > Settings > App Groups**.

2 Select **Add Group**.

3 Complete options on the **List** tab.

Setting	Description
Type	Select the type of application group you want to create depending on the desired outcome: allow applications, block applications, or require application installations. If your goal is to group custom MDM applications, select **MDM Application**. You must enable this option for it to display in the menu.
Platform	Select the platform for the application group.
Name	Enter a display name for the application group in the Workspace ONE UEM console.
Add Application	Display text boxes that enable you to search for applications to add to the application group.
Application Name	Enter the name of an application to search for it in the respective app store.

Setting	Description
Application ID	Review the string that automatically completes when you use the search function to search for the application from an app store.
Add Publisher - Windows Phone	Select for Windows Phone to add multiple publishers to application groups. Publishers are organizations that create applications. Combine this option with **Add Application** entries to create exceptions for the publisher entries for detailed whitelists and blacklists on Windows Phone.

4 Select **Next** to navigate to an application control profile. You must complete and apply an application control profile for Windows Phone. You can use an application control profile for Android devices.

5 Complete settings on the **Assignment** tab.

Setting	Description
Description	Enter the purpose of the application group or any other pertinent information.
Device Ownership	Select the type of devices to which the application group applies.
Model	Select device models to which the application group applies.
Operating System	Select operating systems to which the application group applies.
Managed By	View or edit the organization group that manages the application group.
Organization Group	Add more organization groups to which the application group applies.
User Group	Add user groups to which the application group applies.

6 Select **Finish** to complete configurations.

Bookmarks for Android (Legacy) Devices

Bookmarks function much like an app on a device, providing end users a simple way to access a URL directly from an icon on their device's menu. The end user sees the bookmark icon and title, selects the bookmark and connects directly to a specified URL.

Bookmarks are particularly useful for easy navigation to extended URLs with a large amount of characters. Bookmark icons can be placed on an end user's springboard directly next to the app. These icons can be used to connect to internal content repositories or login screens without having to open a browser and type out a long URL.

Bookmarks configured in this profile will display in the Launcher profile to allow admins to determine position of bookmarks while using Multi App mode.

Configure Bookmarks (Android (Legacy))

Bookmarks configured in this profile will display in the Launcher profile to allow admins to determine position of bookmarks while using Single App, Multi App, and Template Mode.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.

2 Select **Device** to deploy your profile to a device.

3 Configure the profile's **General** settings.

4 Select the **Bookmarks** payload.

5 Configure the **Bookmarks** settings, including:

Setting	Description
Label	Provide the name that appears on the device menu.
URL	Specify the link destination that the user is brought to upon selecting the Bookmark.
Icon	Upload an image for the bookmark as it appears on the device springboard.
Add to Homescreen	Determine whether the bookmark appears on the device's homescreen (first page of the device men).
Show in App Catalog/Container	Enable to allow the app to be displayed in the App Catalog and Container.

6 Select **Save & Publish**.

Credentials Profile

Even if you protect your corporate email, Wi-Fi, and VPN with strong passcodes, and with other restrictions, your infrastructure still remains vulnerable to attack, in addition to employee error. You can implement digital certificates, known as certificates, to protect corporate assets.

To do this, you must first define a certificate authority, then configure a **Credentials** payload alongside your EAS, Wi-Fi, or VPN payload. Each of these payloads has settings for associating the certificate authority defined in the **Credentials** payload.

Deploy Credentials (Android (Legacy))

Credentials profiles deploy corporate certificates for user authentication to managed devices.

When deploying this profile for Smart Glasses configuration, there is a limit of two credentials supported.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.

2 Configure the profile's **General** settings.

3 Select the **Credentials** payload.

4 Configure the **Credentials** settings, including:

Settings	Description
Credential Source	**Upload** a certificate from your local machine or define a **Defined Certificate Authority**, or upload a **User Certificate**. ■ If you choose to **Upload** a certificate, complete the following: ■■ **Credential Name** – Enter the name of the credential or select on the information symbol to view acceptable lookup values like {EmailDomain} and {DeviceModel} to find the credential file to use. ■■ **Certificate** – **Upload** the new certificate or lookup values. ■ If you choose to use a **Defined Certificate Authority**, complete the following: ■■ **Certificate Authority** for the **Defined Certificate Authority** – Select the external or internal CA issuing encryption keys for the PKI. ■■ **Certificate Template** for the **Defined Certificate Authority** – Select the predefined template for the CA to use when requesting a certificate. ■ If you choose upload a **User Certificate**, select either **S/MIME Certificate** or **S/MIME Encryption Certificate**. ■ If you choose **Derived Credentials**, make sure to select the appropriate Key Usage which can be either **Authentication**, **Signing**, or **Encryption**.

5 Navigate back to the previous payload for EAS, Wi-Fi, or VPN.

6 Specify the Identity Certificate in the payload:

Setting	Description
EAS	Select the **Identity Certificate** under Login Information.
WiFi	Select a compatible **Security Type** (WEP Enterprise, WPA/WPA2 Enterprise or Any (Enterprise)) and select the **Root Certificate** under **Authentication**.
VPN	Select a compatible **Connection Type** (for example, CISCO AnyConnect, F5 SSL) and select the **Identity Certificate**.

7 Select **Save & Publish** after configuring the remaining settings.

Workspace ONE Launcher

Workspace ONE Launcher allows your organization to completely customize the look and behavior of managed Android (Legacy) devices. The Workspace ONE Launcher profile replaces your device's graphical user interface with one that has been custom tailored to your organization's specifications.

Even more, the Workspace ONE UEM console provides an easy-to-follow configurations page to configure and manage layout and display settings in a centralized environment.

Note The Kindle Fire HD is not supported by the Workspace ONE Launcher at this time.

Create Workspace ONE Launcher Profile

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 replaces your device interface with one that is custom- tailored to your business needs.

You can configure Android 6.0 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.

Procedure

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

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

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

Launcher Version Settings (Android)

After you configure the Workspace ONE Launchersettings, navigate to **Service Applications** in the Workspace ONE UEM console to determine which version of the profile you want to deploy to your device fleet.

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

If you do not want to deploy the Launcher to your entire fleet, provision the Workspace ONE Launcher to selected devices using organization groups. For more information on deploying profiles by organization group, please see the **Mobile Device Management Guide**.

Configure Firewall Rules for Android Devices

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

This profile is available when **OEM Settings** is enabled and the **Select OEM** field is set to Samsung in the General profile settings.

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

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android**.

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.

2 Select **Device** to deploy your profile.

3 Configure the **General** profile settings.

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.
Redirect Exception Rules	Avoids traffic from being redirected.

6 Select **Save & Publish**.

Configure a Global Proxy (Android)

Global Proxy settings is 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 **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.

2 Select **Device** to deploy your profile to a device.

3 Configure the profile's **General** settings.

4 Configure the **Global Proxy** settings, including:

Proxy Type	Select the as **Manual** or **Auto**: ■ If set as **Auto**enter the following : ■ **Proxy PAC File URL** – Enter your Proxy PAC file URL, if applicable. ■ If set to **Manual**, provide the complete the following fields: ■ **Proxy Server**– Host name of IP address for the proxy server. ■ **Proxy Server Port** – Target port for the proxy server.
Enable HTTPS Proxy	Select to utilize global proxy for HTTPS traffic.
Exclusion List	Add hostnames to this list to prevent them from routing through the proxy.

5 Select **Save & Publish**.

Set Date/Time (Android)

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

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.

2 Select **Device** to deploy your profile to a device.

3 Configure the profile's **General** settings.

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

6 Select **Save & Publish**.

Configure Sound Profiles (Android)

Deploy a Sound profile to control on an admin level the volume for ring tones, voice, and music. You can also use this profile to enable and disable other phone sounds such as touch tone or screen lock sounds.

This profile can only be used by Motorola Rugged devices running Android.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.

2 Select **Device** to deploy your profile to a device.

3 Configure the profile's **General** settings.

4 Select the Sound payload.

5 Configure the Sound settings, including:

Setting	Description
Music, Video, Games, and 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.

6 Select **Save & Publish** to push the profile to the device.

Configure Firewall Rules (Android(Legacy))

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

The Firewall payload only applies to SAFE 2.0+ devices.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.

2 Select **Device** to deploy your profile.

3 Configure the profile's **General** settings.

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.
Redirect Exception	Avoids traffic from being redirected.

6 Select **Save & Publish**.

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

Configure a Display Profile (Android)

Deploy a display profile to devices to control the brightness of the display. You can also set how long the device stays awake before shutting off the screen.

This profile can only be used by Motorola Rugged devices running Android.

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.

2 Select **Device** to deploy your profile to a device.

3 Configure the profile's **General** settings.

4 Configure the Display settings, including:

Setting	Description
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.
Enable Stay Awake	Allow the device to not go to sleep mode.

5 Select **Save & Publish** to push the profile to devices.

Deploy Advanced Profile (Android)

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

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.

2 Select **Device** to deploy your profile to a device.

3 Configure the profile's **General** settings.

4 Select the **Advanced** payload.

5 Configure the Advanced settings, including:

Setting	Description
Display Name	Provide a user friendly name of the access name.
Access Point Name	Enter the name of the carrier.
Access Point Type	Set as **default**, **mms** or **supl**.
Mobile Country Code	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.
Server	Enter the name or address used for the connection.
Proxy Server	Enter the Host name of IP address for the proxy server.
Proxy Server Port	Enter the target port for the proxy server.
Access Point Username	Specify the username that connects to t he access point.
Access Point Password	Specify the password that authenticates t he access point.
Authentication Type	Select the authentication type to be used with applications.
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.
+/-	Add or delete additional APN settings by using the plus/minus buttons located on the bottom right corner.

6 Select **Save & Publish**.

Configure Custom Settings (Android)

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

Procedure

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > Android (Legacy)**.

2 Select **Device** to deploy your profile to a device.

3 Configure the profile's **General** settings.

4 Configure the applicable payload (for example, Restrictions or Passcode).

To avoid affecting other users before you are ready to Save and Publish, work on a copy of your profile saved under a "test" organization group.

5 **Save**, but do not publish, your profile.

6 Select the radio button from the **Profiles List View** for the row of the profile you want to customize.

7 Select the **XML** button at the top to view the profile X.

8 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.

9 Copy this section of text and close the XML View. Open your profile.

10 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>.

11 Remove the original payload you configured by selecting the base payload section and selecting the minus [-] button.

You can now enhance the profile by adding custom XML code for the new functionality.

Important Any device not upgraded to the latest version ignores the enhancements you create. Because the code is now custom, you should test the profile devices with older versions to verify expected behavior.

12 Select **Save & Publish**.

Compliance Policies

4

The compliance engine is an automated tool by Workspace ONE UEM powered by AirWatch that ensures all devices abide by your policies. These policies can include basic security settings such as requiring a passcode and having a minimum device lock period.

Compliance Policies in Workspace ONE UEM

For certain platforms, you can also decide to set and enforce certain precautions. These precautions include setting password strength, blocking certain apps, and requiring device check-in intervals to ensure that devices are safe and in-contact with Workspace ONE UEM. Once devices are determined to be out of compliance, the compliance engine warns users to address compliance errors to prevent disciplinary action on the device. For example, the compliance engine can trigger a message to notify the user that their device is out of compliance.

In addition, devices not in compliance cannot have device profiles assigned to it and cannot have apps installed on the device. If corrections are not made in the amount of time specified, the device loses access to certain content and functions that you define. The available compliance policies and actions vary by platform.

Dell BIOS Verification for Workspace ONE UEM

Ensure that your Dell Windows Desktop devices remain secure with Dell Trusted Device (formerly, Dell BIOS Verification). This service analyses the BIOS of your Dell devices and reports the status to Workspace ONE UEM so you can act against any compromised devices.

Benefits of Dell Trusted Device

The BIOS is a part in maintaining the overall device health and security. Modern computer systems rely on BIOS firmware to initialize hardware during the boot process and for runtime services that support the operating system and applications. This privileged position within the device architecture makes unauthorized modification of the BIOS firmware a significant threat. The Dell Trusted Device service provides secure BIOS validation using a secure signed response model. The status of the secure validation helps you act on compromised devices with the compliance policy engine.

Prepare Your Devices for Dell Trusted Device

To use Dell Trusted Device on your Windows Desktop devices, you must install the Dell Trusted Device service on the device. You must download the latest client from Dell (https://www.dell.com/support/home/product-support/product/trusted-device/drivers). Consider using Software Distribution to install the client on your Dell Windows Desktop devices.

Dell BIOS Verification Statuses

After you install the client onto your devices, you can see the reported status in the Device Details page. The statuses are as follows:

- Pass - The Dell Trusted Device client is installed on the device and the device is secure.
- Fail - The Dell Trusted Device client is installed and one of the following issues is present:
  - The Pre-Check event returns a fail result. This result happens when the client detects an invalid binary signature.
  - The BIOS Utility event returns a fail result for the validation test.
  - The BIOS Server Processing event returns a fail result for an invalid signature, invalid exit code, or the payload status is out of sync.
- Warning - The Dell Trusted Device is installed and the client detects an issue. The device might not be secured, so investigate the issue. Causes for a Warning status might include the following list.
  - No network connection
  - Invalid command-line argument
  - Application is running with insufficient privileges.
  - Internal errors in the client
  - Server responds with an error.
  - Driver issues with the client
  - Unknown results in the BIOS verification
- If you see a gray warning icon, the Dell Trusted Device client is not installed on the device.

Compromised Device Detection with Health Attestation

In both BYOD and Corporate-Owned device deployments, it is important to know that devices are healthy when accessing corporate resources. The Windows Health Attestation Service accesses device boot information from the cloud through secure communications. This information is measured and checked against related data points to ensure that the device booted up as intended and is not victim to security vulnerabilities or threat. Measurements include Secure Boot, Code Integrity, BitLocker, and Boot Manager.

Workspace ONE UEM enables you to configure the Windows Health Attestation service to ensure device compliance. If any of the enabled checks fail, the Workspace ONE UEM compliance policy engine applies security measures based on the configured compliance policy. This functionality allows you to keep your enterprise data secure from compromised devices. Since Workspace ONE UEM pulls the necessary information from the device hardware and not the OS, compromised devices are detected even when the OS kernel is compromised.

Configure the Health Attestation for Windows Desktop Compliance Policies

Keep your devices secured by using Windows Health Attestation Service for compromised device detection. This service allows Workspace ONE UEM to check the device integrity during startup and take corrective actions.

Procedure

1 Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Desktop > Windows Health Attestation**.

2 (Optional) Select **Use Custom Server** if you are using a custom on-premises server running Health Attestation. Enter the **Server URL**.

3 Configure the Health Attestation settings.

Settings	Descriptions
Use Custom Server	Select to configure a custom server for Health Attestation. This option requires a server running Windows Server 2016 or newer. Enabling this option displays the Server URL field.
Server URL	Enter the URL for your custom Health Attestation server.
Secure Boot Disabled	Enable to flag compromised device status when Secure Boot is disabled on the device. Secure Boot forces the system to boot to a factory trusted state. When Secure Boot is enabled, the core components used to boot the machine must have the correct cryptographic signatures that the OEM trusts. The UEFI firmware verifies the trust before it allows the machine to start. Secure boot prevents the startup if any it detects any tampered files.
Attestation Identity Key (AIK) Not Present	Enable to flag compromised device status when the AIK is not present on the device. Attestation Identity Key (AIK) is present on a device, it indicates that the device has an endorsement key (EK) certificate. It can be trusted more than a device that does not have an EK certificate.

Settings	Descriptions
Data Execution Prevention (DEP) Policy Disabled	Enable to flag compromised device status when the DEP is deacivated on the device. The Data Execution Prevention (DEP) Policy is a memory protection feature built into the system level of the OS. The policy prevents running code from data pages such as the default heap, stacks, and memory pools. Hardware and software both enforce DEP.
BitLocker Disabled	Enable to flag compromised device status when BitLocker encryption is deactivated on the device.
Code Integrity Check Disabled	Enable to flag compromised device status when the code integrity check is deactivated on the device. Code integrity is a feature that validates the integrity of a driver or system file each time it is loaded into memory. Code integrity checks for unsigned drivers or system files before they load into the kernel. The check also scans for users with administrative privileges running system files modified by malicious software.
Early Launch Anti-Malware Disabled	Enable to flag compromised device status when the early launch anti-malware is deactivated on the device. Early launch anti-malware (ELAM) provides protection for the computers in your network when they start up and before third-party drivers initialize.
Code Integrity Version Check	Enable to flag compromised device status when the code integrity version check fails.
Boot Manager Version Check	Enable to flag compromised device status when the boot manager version check fails.
Boot App Security Version Number Check	Enable to flag compromised device status when the boot app security version number does not meet the entered number.
Boot Manager Security Version Number Check	Enable to flag compromised device status when the boot manager security version number does not meet the entered number.
Advanced Settings	Enable to configure advance settings in the Software Version Identifiers section.

4 Select **Save**.

Applications for Android (Legacy) Overview

5

You can use AirWatch applications in addition to Workspace ONE UEM MDM features to further secure devices and configure them with added functionality.

Two features you can use for advanced app management are Software Development Kits (SDKs) and App Wrapping. Both enable you to integrate the same MDM functionality provided by AirWatch into your own internal applications. SDKs must be developed new, and let you perform more extensive device, application, and content management. App wrapping, by contrast, gives you the ability to inject functionality into internal apps without the need for development or code changes. Both serve to bolster the security of internal applications and thus increase their value to your company.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Configure Workspace ONE Intelligent Hub Settings

The settings configured for the Workspace ONE Intelligent Hub determines how reports and metrics are reported back to Workspace ONE UEM from the device.

Procedure

1 Navigate to **Devices > Device Settings > Android > Hub Settings**.

Adjusting these intervals can impact battery life, with smaller values equating to more frequent pings and greater power consumption.

2 Configure the following **General** settings:

Setting	Descriptions
Heartbeat Interval (min)	Enter the heartbeat time interval, which is how frequently the Workspace ONE Intelligent Hub checks in with the Workspace ONE UEM server. Reports beacon data to the Workspace ONE UEM console. The primary purpose of this report is to show compromised device status. However, beacon data also includes IP address and other data, such as model and OS version.
Data Sample Interval (min)	Enter the data sample time interval, which is how frequently the Workspace ONE Intelligent Hub collects data from the device. Collects interrogator data and reports all data collected by the Workspace ONE Intelligent Hub, including Telecom and Network data, as well as the battery, power and memory status.

Setting	Descriptions
Data Transmit Interval (min)	Enter the data transmit time interval, which is how frequently the Workspace ONE Intelligent Hub sends data to the Workspace ONE UEM server. Reports interrogator data to the Workspace ONE UEM console. This value should always be greater than the Data Sample Interval value.
Profile Refresh Interval (min)	Enter the profile refresh time interval, which is how frequently the device profile list for the device is refreshed on the Workspace ONE UEM server. Checks in with the Workspace ONE UEM console for profile updates or new profiles.
Require Google Account	Require a Google Account to leverage Google Cloud Messaging (GCM) to send remote commands to devices. Only deselect this option if you are utilizing AWCM.
Require Phone Number	Enable an additional prompt during enrollment. This phone number is recorded in Workspace ONE UEM to serve as a backup contact number in case devices are lost, turned off or do not have access to Internet.
Block User Unenrollment	Select this option to ensure end users cannot unenroll their devices by disabling the 'Unenroll' option in the Workspace ONE Intelligent Hub menu. On Samsung devices using Android Legacy, this will also prevent Device Administrator deactivation for the Workspace ONE Intelligent Hub.
Device Services Version	Displays OEM service version.

3 Configure **Application List** settings:

The Application List detects specific, blacklisted apps that are installed on a device, or detect all apps that are not whitelisted. You can either specifically prohibit certain apps, such as social media or entertainment apps, or specifically permit only the apps you specify, such as internal applications for business use.

Setting	Description
Application List Interval	Enter the frequency at which the Workspace ONE Intelligent Hub checks the application list.

4 Configure **Internal Applications** settings:

Setting	Description
Install Options	Select how end users will be prompted to install new internal applications. You can provide a **Direct Prompt**, a **Status Bar Notification**, or opt to have **No Notification**.
SafetyNet App Verification	Enable to allow app verification which scans apps installed on the device before they are downloaded to detect potentially harmful apps. When enabled: ■ The scan runs whenever an app is installed or removed from device. ■ Users cannot disable app verification on device. This setting also works in conjuction with the restriction setting in the Android Restrictions profile in the UEM console.

5 Configure **Samsung Knox** settings, if applicable:

For more information about these settings or Samsung Knox in general, refer to the **VMware AirWatch Containerization with Samsung Knox Guide**.

Setting	Description
Enable Containers	Select **Enabled** to allow profile creation for Samsung Knox Containers and to allow the Android Hub to create application containers for Samsung Knox devices.
Knox License Key	Enter your Samsung Knox License Key.
Enable Audit Logging	Select **Enabled** to turn on audit logging and the related settings below. The Workspace ONE UEM console has the ability to monitor errors that might prevent successful creation of the Knox container. The log provides the cause of the error and what needs to be resolved for successful Knox deployment. The audit logs are sent to the UEM console from the Knox enabled devices and stored in the Device Details page. The **Transmits Logs Automatically** setting determines the threshold at which the log file is reported to the device details.
Logging Level	Determines how severe an error has to be in order for it to be sent to the log file. The logging levels are listed in order or severity where notice is the least severe and alert is the highest. ■ **Alert** ■ **Critical** ■ **Error** ■ **Warning** ■ **Notice**
Critical Log Size	Enter a percentage (up to 70 percent) to define the critical log size. When the log file passes this percentage, a critical log size alert is sent to the admin.
Maximum Log Size	Enter a percentage (up to 90 percent) to define the maximum log size. When the log file passes this percentage, a maximum log size alert is sent to the admin.
Full Log Size	Set to 97 percent by default. When the log file reaches this percentage, a full log size alert is sent to the admin and immediate action is required.
Transmits Logs Automatically	Determines when the audit logs are to be transmitted to the console to notify the admins of errors. ■ **Never** â€“ The log file will never be sent transmitted to the console. ■ **Critical** â€“ The log file needs be at critical size to be transmitted to the console. ■ **Maximum** â€“ The log file needs be at maximum size to be transmitted to the console. ■ **Full** â€“ The log file needs be at full size to be transmitted to the console.

6 Configure **Location** settings:

Setting	Description
Collect Location Data	Select whether to collect location data from devices. Location is determined based on a device's Wi-Fi network. When it is available, it is reported to the Workspace ONE UEM console according to the Data Transmit Interval.
Force GPS On	Prevent the user from turning off GPS for certain devices.
GPS Time Poll Interval (min)	Enter the interval, in minutes, for which a time sample gets signaled. The minimum time is five minutes.

7 Configure **Telecom** settings:

Enable specific Telecom settings like Call Logs, SMS Logs and Cellular Data Usage to allow logging and tracking of device use.

Setting	Description
Enable Call Logs	Collects information from incoming and outgoing phone calls made devices registered with Workspace ONE UEM.
Enable SMS Logs	Reports that log any incoming and outgoing SMS messages to devices.
Enable Cellular Data Usage	Allows the Workspace ONE UEM console to create reports which details data usage.

8 Configure AWCM Settings, if applicable:

AirWatch Cloud Messaging (AWCM) provides an internal communication solution for the entire Workspace ONE UEM solution as a comprehensive replacement for Google Cloud Messaging (GCM).

Setting	Description
Use AWCM Instead of C2DM As Push Notification Service	Set to **Enabled** to enable AWCM.
AWCM Client Deployment Type.	Set to Always Running if you want the system and device have a constant and ongoing line of communication.
AWCM Client Timeout Value (Mins)	Determines how much idle time can pass before the client responds to the AWCM server.

9 Configure the **Remote Management** settings:

Setting	Description
Download Remote Control Cab	Select this link to download the cabinet (CAB) installer file for Workspace ONE UEM Remote Management.
Seek Permission	Enable Seek Permission if you want to prompt the end user to accept or decline the remote management request from the admin. ■ Enter a **Seek Permission Message** that the end user sees when a remote request is sent. ■ Enter the **Yes Caption** message for the accept button the end user sees on the Seek Permission request. ■ Enter the **No Caption** message for the decline button the end user sees on the Seek Permission request.

See the **VMware AirWatch Remote Management Guide**.

10 Configure SDK Profile settings:

Enterprises can integrate any existing company specific apps with the use of an AirWatch Software Development Kit (SDK). Select which SDK profile to deploy to your devices by using the SDK Profile V2 option in the Workspace ONE Intelligent Hub settings.

a **SDK Profile V2** â€“ Select the profile that will provide the Workspace ONE Intelligent Hub with the SDK settings configured for that organization group.

11 Select **Save**.

What to do next

There are additional options available for the above devices with Product Provisioning. For more information, please see the Rugged Android Platform Guide.

Configure Service Applications

The OEM Service application is a plug-in app that is only installed and used in combination with Workspace ONE Intelligent Hub enrollment. It allows for additional MDM capabilities that only pertain to a specific OEM device.

Service Application allow you to customize how your end users get the specified service application to their device.

Procedure

1 Navigate to **Devices > Device Settings > Android > Service Applications**.

2 Enable the following features:

Setting	Description
Require Service App	Select to ensure end users get the Service App.
Push Service App from Play Store	Select to install the OEM service through the Google Play Store before or during enrollment. Pushing the Service App simplifies enrollment for your end users by removing the need to accept "unknown sources" during the enrollment process.

Setting	Description
Download Folder	Provide a location for the file download. This option only appears if **Push Service App from Play Store** is disabled.
Always use the Latest Version of Telecom Sampler	Select to use latest or de-select to choose a specific **Telecom Sampler Version**.
Telecom Sampler Version	Select the desired Telecom Sampler version.
Always use the Latest Version of AirWatch Launcher	Select to use latest or de-select to choose a specific **AirWatch Launcher Version**. Once this setting is enabled, it applies across all devices you have enrolled into Workspace ONE UEM using Launcher.
AirWatch Launcher Version	Select the desired Launcher version.

3 Select **Save**.

VMware Content Locker for Android (Legacy)

VMware Content Locker is an application that enables your end users to access important content on their devices while ensuring file safety for your organization.

From the VMware Content Locker, end users can access content you upload in the UEM console, content from synced corporate repositories, or their own personal content.

Use the UEM console to add content, sync repositories and configure the actions that end users can take on content opened within the application. These configurations prevent content from being copied, shared, or saved without approval.

VMware Browser for Android (Legacy)

The VMware Browser is a safe, accessible and manageable Internet browser for your devices.

You can customize and configure the VMware Browser to meet unique business and end user needs, restrict web access to certain websites, provide a secure Internet portal for devices used as a mobile point-of-sale and more. For maximum security, consider deploying the VMware Browser in conjunction with a restrictions profile blocking the native browser.

AirWatch Container for Android (Legacy)

AirWatch Container offers a flexible approach to Bring Your Own Device (BYOD) management by pushing a secure work space to a personal device. Businesses can distribute Workspace ONE UEM applications and internal applications to the AirWatch Container for employees to use on their mobile devices.

Applications are visible inside and outside the AirWatch Container, but the enterprise applications are secure through a common SDK framework and a container passcode. These apps can interact seamlessly using single sign on authentication and can connect securely to the Internet through an app tunnel VPN. For instructions on how to use the AirWatch Container on a device, see the **VMware AirWatch Container User Guide for iOS** or the **VMware AirWatch Container User Guide for Android.**

VMware Boxer for Android (Legacy)

VMware Boxer is an email application that offers a consumer-centric focus on mobile productivity with enterprise-grade security in the form of AES 256-bit encryption. This app containerizes business data from personal data, providing frictionless access to enterprise email, calendar, and contacts across corporate-owned and employee owned.

Boxer allows users to personalize the app to meet their needs with features like custom swipe gestures, contact avatars, custom smart folders, and account color preferences. The all-in-one email, calendar, and contacts app provides an intuitive user experience following native design paradigms on Android devices.

Enforcing Application-Level Single Sign On Passcodes

Single sign on (SSO) allows end users to access Workspace ONE UEM apps, wrapped apps, and SDK-enabled apps without entering credentials for each application. Using the Workspace ONE Intelligent Hub or the AirWatch Container as a "broker application," end users authenticate once per session using their normal credentials or an SSO Passcode.

Enable SSO as part of the **Security Policies** that you configure to apply to all Workspace ONE UEM apps, wrapped apps, and SDK-enabled apps using a Default SDK Profile.

Procedure

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.
2. Set **Single Sign On** to **Enabled** to allow end users to access all Workspace ONE UEM applications and maintain a persistent login.
3. (Optional) **Authentication Type** to **Passcode** and set the **Passcode Mode** to either **Numeric** or **Alphanumeric** to require an SSO Passcode on the device. If you enable SSO but do not enable an Authentication Type, end users use their normal credentials (either directory service or Workspace ONE UEM account) to authenticate, and an SSO Passcode does not exist.

Results

Once an end user authenticates with an application participating in SSO, a session establishes. The session is active until the **Authentication Timeout** defined in the SDK profile is reached or if the user manually locks the application.

Shared Devices

6

Shared Device/Multi-User Device functionality in Workspace ONE UEM powered by AirWatch ensures that security and authentication are in place for every unique end user. Shared devices can also allow only specific end users to access sensitive information.

Issuing a device to every employee in certain organizations can be expensive. Workspace ONE UEM powered by AirWatch 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 Device capabilities are also possible natively on Apple iPads integrated with Apple Business Manager. This functionality called Shared iPads for Business leverages the user's Managed Apple ID for login and does not take place in the Workspace ONE Intelligent Hub for login and logout. To know more about configuring Shared iPads for Business with Apple Business Manager and steps to achieve this functionality, see **Shared iPads for Business** in *Introduction to Apple Business Manager Guide* available on docs.vmware.com.

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 Workspace ONE Access.
- 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 Workspace ONE Access.
- 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 or later
- iOS devices with Workspace ONE Intelligent Hub 4.2 or later.
  - For details about logging in and out of shared iOS devices, see the topic *Log In and Log Out of Shared iOS Devices* in the **iOS Platform Guide**, available on docs.vmware.com.
- MacOS devices with Workspace ONE Intelligent Hub 2.1 or later.

Define the Shared Device Hierarchy

While strictly optional, making an organization group (OG) specific to shared devices offers many benefits due to multi-tenancy and inherited device settings.

If you have a large number of shared devices in your fleet and you want to manage them apart from single user devices, you can make a shared device-specific OG. Making a shared device hierarchy in your OG structure is optional. Features like smart groups and user groups mean you do not have to rely strictly on OG hierarchy design to simplify device management.

However, having a shared device OG (or nested OGs) simplifies device management by enabling you to standardize device functionality through profiles, policies, and device inheritance without the processing overhead required by a smart group or a user group.

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	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. 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. 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.
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 macOS Devices

Multiple users can log in to and out of a macOS shared device, activating the automatic push of device profiles.

Log In to a macOS Device - Using assigned Network credentials, log in to a macOS device that has been staged and you receive the profiles assigned to your account in Workspace ONE UEM.

Log out of a macOS Device - The standard macOS log-out procedure also logs the device out of your assigned Workspace ONE UEM user profile.

This chapter includes the following topics:

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

Define the Shared Device Hierarchy

While strictly optional, making an organization group (OG) specific to shared devices offers many benefits due to multi-tenancy and inherited device settings.

If you have a large number of shared devices in your fleet and you want to manage them apart from single user devices, you can make a shared device-specific OG. Making a shared device hierarchy in your OG structure is optional. Features like smart groups and user groups mean you do not have to rely strictly on OG hierarchy design to simplify device management.

However, having a shared device OG (or nested OGs) simplifies device management by enabling you to standardize device functionality through profiles, policies, and device inheritance without the processing overhead required by a smart group or a user group.

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	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. 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. 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.
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 Build out your corporate hierarchical structure by creating more groups and subgroups in the same manner.

a If you are configuring a **Fixed Organization Group**, then ensure that you create the single organization group for end users to log in or log out.

b If you configure **Prompt Users for Organization Group**, then ensure that you have created the multiple OGs for end-user roles for logging in or logging out. For more information, see Configure Shared Devices.

6 Select **Save**.

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

1 Navigate to **Groups & Settings > All Settings > Devices & Users > General > Shared Device**.

2 Select **Override** and complete the **Grouping** section.

Setting	Description
Group Assignment Mode	Configure devices in one of three ways: ■ Select **Prompt User for Organization Group** to have the end user enter a Group ID for an organization group upon login. With this method, you have the flexibility to provide access to the settings, applications, and content of the organization group entered. Using this approach, an end user is not restricted to accessing only the settings, applications, and content for the organization group to which they are enrolled. ■ Select **Fixed Organization Group** to limit your managed devices to settings and content applicable to a single organization group. Each end user who logs in to a device has access to the same settings, applications, and content. This method can be beneficial in a retail use case where employees use shared devices for similar purposes such as checking inventory. ■ Select **User Group Organization Group** to enable features based on both user groups and organization groups across your hierarchy. When an end user logs in to a device, they have access to specific settings, applications, and content based on their assigned role within the hierarchy. For example, an end user is a member of the 'Sales' user group, and that user group is mapped to the 'Standard Access' organization group. When that end user logs in to the device, the device is configured with the settings, applications, and content available to the 'Standard Access' organization group. You can map user groups to organization groups on the UEM console. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment**. Select the **Grouping** tab and fill in the required details.
Always Prompt for Terms of Use	Prompts the end users to accept your **Terms of Use** agreement before they log in to a device.

3 Complete the **Security** section, as applicable.

Setting	Description
Require Shared Device Passcode	**(For iOS devices only)**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.

Setting	Description
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.
Auto Logout	Configure an automatic log out after a specific time period.
Auto Logout After	Set the length of time that must elapse before the **Auto Log out** function activates in **Minutes**, **Hours**, or **Days**.
iOS Single App Mode	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. 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. Enabling Single App Mode also deactivates the Home button on the device. **Note** Single App Mode applies only to Supervised iOS devices.

4 Configure the **Logout Settings**, as applicable.

Setting	Description
Clear Android App Data	Clear the app data when the user logs out of a shared device (checks it in).
Reinstall Android Apps	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.
Clear Android Device Passcode	This setting controls whether the current Android device passcode is cleared when the user logs out (checks in) a multi-user shared device.
Allow PIN at Startup	Activate or deactivate Android Secure Startup, which requires an initial PIN entry to boot up the device. If deactivated, users cannot enable Secure Startup during passcode setup. If Secure Startup is already deactivated on the device, the device must be factory reset to enable it. This feature applies only to Android devices that do not have file-based encryption.
Clear iOS Device Passcode	This setting controls whether the current iOS device passcode is cleared when the user logs out (checks in) a multi-user shared device.

5 Select **Save**.

What to do next

For specific information about provisioning devices for single-user and multi-user device staging, see the topics Stage a Single-User Device and Stage a Multi-User Device.

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 installs and the login screen appears, by default.

Note The Launcher .apk needs to be installed before the Launcher profile is pushed as a part of the Shared Device settings.

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.

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 **Launcher Settings** and select **Log Out** (door icon).

Product Provisioning for Android (Legacy) Devices Overview

7

Product provisioning enables you to create, through Workspace ONE ™ UEM, products containing profiles, applications, files/actions, and event actions (depending on the platform you use). These products follow a set of rules, schedules, and dependencies as guidelines for ensuring your devices remain up-to-date with the content they need.

Product provisioning also encompasses the use of relay servers. These servers are FTP(S) servers designed to work as a go-between for devices and the UEM console. Create these servers for each store or warehouse to store product content for distribution to your devices.

Another product provisioning feature is the staging methods of enrollment. Depending on the device type, you can perform device staging that quickly enrolls a device and downloads the Workspace ONE Intelligent Hub, Wi-Fi profile, and any other important content. The methods of staging a device vary by platform.

Android (Legacy) Device Management Overview

8

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 Dashboard

As devices are enrolled, you can manage them from the **Device Dashboard** in Workspace ONE UEM powered by AirWatch.

The **Device Dashboard** provides a high-level view of your entire fleet and allows you to act on individual devices quickly.

You can view graphical representations of relevant device information for your fleet, such as device ownership type, compliance statistics, and platform and OS breakdowns. You can access each set of devices in the presented categories by selecting any of the available data views from the **Device Dashboard**.

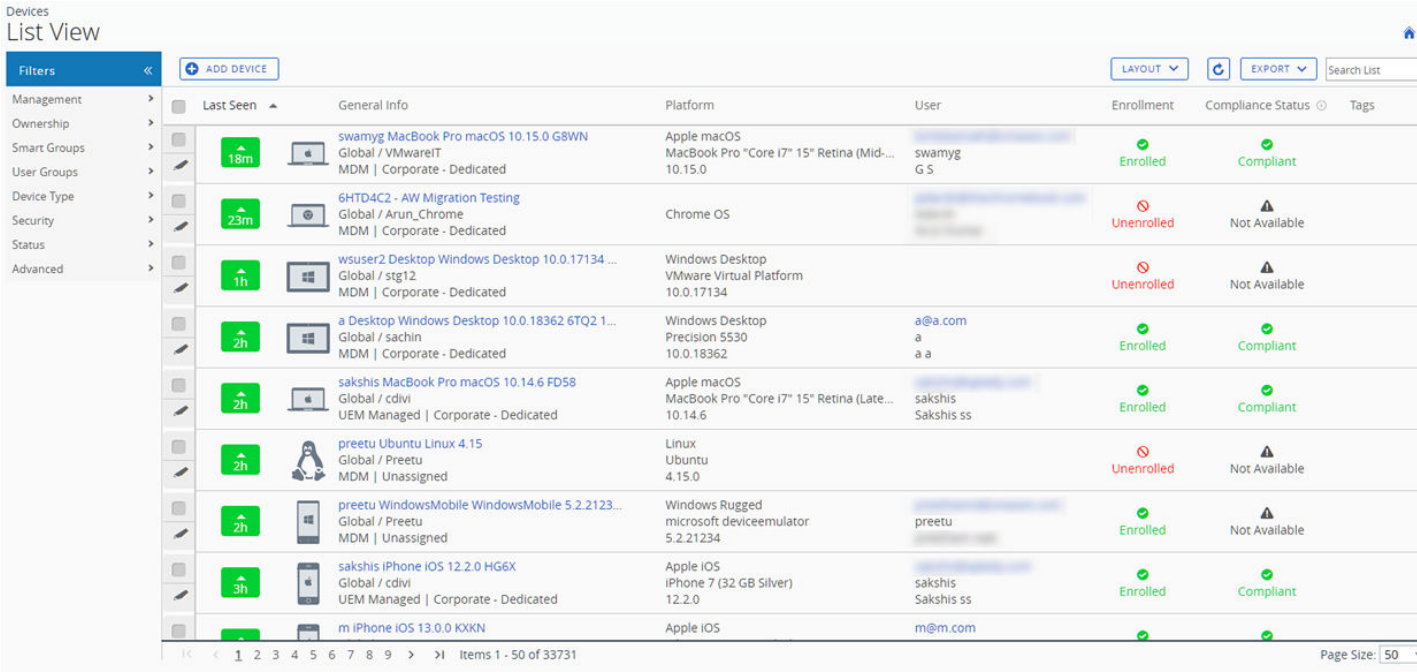
From the **List View**, you can take administrative action: send messages, lock devices, delete devices, and change groups associated with the device.

- **Security** – View the top causes of security issues in your device fleet. Selecting any of the doughnut charts displays a filtered **Device List** view comprised of devices affected by the selected security issue. If supported by the platform, you can configure a compliance policy to act on these devices.
  - **Compromised** – The number and percentage of compromised devices (jailbroken or rooted) in your deployment.
  - **No Passcode** – The number and percentage of devices without a passcode configured for security.
  - **Not Encrypted** – The number and percentage of devices that are not encrypted for security. This reported figure excludes Android SD Card encryption. Only those Android devices lacking disc encryption are reported in the donut graph.

  Ownership – View the total number of devices in each ownership category. Selecting any of the bar graph segments displays a filtered **Device List** view comprised of devices affected by the selected ownership type.
- **Last Seen Overview/Breakdown** – View the number and percentage of devices that have recently communicated with the Workspace ONE UEM MDM server. For example, if several devices have not been seen in over 30 days, select the corresponding bar graph to display only those devices. You can then select all these filtered devices and send out a query command so that the devices can check in.
- **Platforms** – View the total number of devices in each device platform category. Selecting any of the graphs displays a filtered **Device List** view comprised of devices under the selected platform.
- **Enrollment** – View the total number of devices in each enrollment category. Selecting any of the graphs displays a filtered **Device List** view comprised of devices with the selected enrollment status.
- **Operating System Breakdown** – View devices in your fleet based on operating system. There are separate charts for each supported OS. Selecting any of the graphs displays a filtered **Device List** view comprised of devices running the selected OS version.

Device List View

Use the Device List View in Workspace ONE UEM powered by AirWatch to see a full listing of devices in the currently selected organization group.



The **Last Seen** column displays an indicator showing the number of minutes elapsed since the device has checked-in. The indicator is red or green, depending on how long the device is inactive. The default value is 480 minutes (8 hours) but you can customize this by navigating to **Groups & Settings > All Settings > Devices & Users > General > Advanced** and change the **Device Inactivity Timeout (min)** value.

Select a device-friendly name in the **General Info** column at any time to open the details page for that device. A **Friendly Name** is the label you assign to a device to help you differentiate devices of the same make and model.

Sort by columns and configure information filters to review activity based on specific information. For example, sort by the **Compliance Status** column to view only devices that are currently out-of-compliance and target only those devices. Search all devices for a friendly name or user name to isolate one device or user.

Customize Device List View Layout

Display the full listing of visible columns in the **Device List** view by selecting the **Layout** button and select the **Custom** option. This view enables you to display or hide Device List columns per your preferences.

There is also an option to apply your customized column view to all administrators at or below the current organization group (OG). For instance, you can hide 'Asset Number' from the **Device List** views of the current OG and of all the OGs underneath.

Once all your customizations are complete, select the **Accept** button to save your column preferences and apply this new column view. You can return to the **Layout** button settings at any time to tweak your column display preferences.

Some notable device list view custom layout columns include the following.

- Android Management
- SSID (Service Set Identifier or Wi-Fi network name)
- Wi-Fi MAC Address
- Wi-Fi IP Address
- Public IP Address

Exporting List View

Select the **Export** button to save an XLSX or CSV (comma-separated values) file of the entire **Device List View** that can be viewed and analyzed with MS Excel. If you have a filter applied to the **Device List View**, the exported listing reflects the filtered results.

Search in Device List View

You can search for a single device for quick access to its information and take remote action on the device.

To run a search, navigate to **Devices > List View**, select the **Search List** bar and enter a user name, device-friendly name, or other device-identifying element. This action initiates a search across all devices, using your search parameter, within the current organization group and all child groups.

Device List View Action Button Cluster

With one or more devices selected in the Device List View, you can perform common actions with the action button cluster including Query, Send [Message], Lock, and other actions accessed through the **More Actions** button.

Available Device Actions vary by platform, device manufacturer, model, enrollment status, and the specific configuration of your Workspace ONE UEM console.

Remote Assist

You can start a **Remote Assist** session on a single qualifying device allowing you to remotely view the screen and control the device. This feature is ideal for troubleshooting and performing advanced configurations on devices in your fleet.

To use this feature, you must satisfy the following requirements.

- You must own a valid license for Workspace ONE Assist.
- You must be an administrator with a role assigned that includes the appropriate Assist permissions.
- The Assist app must be installed on the device.

- Supported device platforms:
  - Android
  - iOS
  - macOS
  - Windows 10
  - Windows Mobile

Select the check box to the left of a qualifying device in the **Device List View** and the **Remote Assist** button displays. Select this button to initiate a Remote Assist session.

For more information, see the Workspace ONE Assist Guide.

Using the Device Details Page

The **Device Details** page allows you to track detailed device information and quickly access user and device management actions.

You can access the **Device Details** page by either selecting a device's Friendly Name from the **Device Search** page, from one of the available Dashboards or by using any of the available search tools with the Workspace ONE UEM console.

Android devices running Android M 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.

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.

Use the **Device Details** menu tabs to access specific device information, including:

- **Summary** – View general statistics such as enrollment status, compliance, last seen, platform/model/OS, organization group, contact information, serial number, power status including battery health, storage capacity, physical memory and virtual memory. Zebra devices feature a panel displaying detailed battery information. You can also view the Workspace ONE Intelligent Hub and which version of any applicable OEM is currently installed on the device.
- **Compliance** – Display the status, policy name, date of the previous and forthcoming compliance check and the actions already taken on the device.
- **Profiles** – View all MDM profiles currently installed on a device.
- **Apps** – View all apps currently installed or pending installation on the device.
- **Content** – View status, type, name, priority, deployment, last update, and date and time of views, and provide a toolbar for administrative action (install or delete content).

- **Location** – View current location or location history of a device.
- **User** – Access details about the user of a device as well as the status of the other devices enrolled to this user.

The menu tabs below are accessed by selecting **More** from the main Device Details tab.

- **Network** – View current network (Cellular, Wi-Fi, Bluetooth) status of a device.
- **Telecom** – View all amounts of calls, data and messages sent and received involving the device.
- **Notes** – View and add notes regarding the device. For example, note the shipping status or if the device is in repair and out of commission.
- **Certificates** – Identify device certificates by name and issuant. This tab also provides information about certificate expiration.
- **Products** –View complete history and status of all packages provisioned to the device and any provisioning errors.
- **Custom Attributes** – Enable you to use advanced product provisioning functionality.
- **Files/Actions** – View the files and other actions associated with the device.
- **Event Actions** – Allows you to take action on a device when predetermined conditions are met
- **Shared Device Log** – View history of device in terms of Shared Device, including past check-ins and check-outs and current status.
- **Troubleshooting** – View **Event Log** and **Commands** logging information. This page features export and search functions, enabling you to perform targets searches and analysis.
    - **Event Log** – View detailed debug information and server check-ins, including a **Filter** by **Event Group Type**, **Date Range**, **Severity**, **Module**, and **Category**.

      In the **Event Log** listing, the **Event Data** column may display hypertext links that open a separate screen with even more detail surrounding the specific event. This information enables you to perform advanced troubleshooting such as determining why a profile fails to install.
    - **Commands** – View detailed listing of pending, queued, and completed commands sent to the device. Includes a **Filter** enabling you to filter commands by **Category**, **Status**, and specific **Command**.
- **Compromised Detection** – View details about the compromised status of the device including the specific **Reason** for the status and how **Severe** the status is.
- **Status History** – View history of device in relation to enrollment status.
- **Targeted Logging** - View the logs for the Console, Catalog, Device Services, Device Management, and Self Service Portal. You must enable Targeted Logging in settings and a link is provided for this purpose. You must then select the **Create New Log** button and select a length of time the log is collected.

- **Attachments** – Use this storage space on the server for screenshots, documents, and links for troubleshooting and other purposes without taking up space on the device itself.

Remote Actions for Android Devices

The **More drop-down** on the Device Details page enables you to perform remote actions over-the-air to the selected device. The actions listed below vary depending on factors such as device platform, Workspace ONE UEM console settings, and enrollment status.

Note Device admins can no longer send the Clear Device Passcode or Change Device Passcode once a passcode is already set for devices running Android 7.0 (Nougat). Admins can still set a passcode, but only when the device has no passcode, PIN, or pattern .

- **Add Tag** – Assign a customizable tag to a device, which can be used to identify a special device in your fleet.
- **Workspace ONE Intelligent Hub Query** – Send a query command to the Workspace ONE Intelligent Hub on the device to ensure it has been installed and is functioning normally.
- **Change Device Passcode** – Replace any existing device passcode used to access the selected device with a new passcode. The new passcode is displayed on the Change Passcode screen.
  - Take note of the passcode *before* clicking the **Change Passcode** button.
  - Select the **Change Passcode** button to proceed.

    - You can close the window or select **Cancel** and check back later, meaning: if you are unable to notate the passcode or relay the passcode to the end user, you can re-initiate a Change Device Passcode action at a later time.
- **Change Organization Group** – Change the device's home organization group to another existing OG. Includes an option to select a static or dynamic OG.
    - If you want to change the organization group for multiple devices at a time, you must select devices for the bulk action using the Block selection method (using the shift-key) instead of the Global check box (next to the Last Seen column heading in the device list view).
- **Change Ownership** – Change the Ownership setting for a device, where applicable. Choices include Corporate-Dedicated, Corporate-Shared, Employee Owned and Undefined.
- **Clear Passcode (Container)** – Clear the container-specific passcode. To be used in situations where the user has forgotten their device's container passcode.
- **Clear Passcode (Device)** – Clear the device passcode. To be used in situations where the user has forgotten their device's passcode.
- **Clear Passcode (SSO)** – Clear the SSO passcode, for situations where the user has forgotten their single sign-on passcode.
- **Delete Device** – Delete and unenroll a device from the console. Sends the enterprise wipe command to the device that gets wiped on the next check-in and marks the device as **Delete In Progress** on the console. If the wipe protection is turned off on the device, the issued command immediately performs an enterprise wipe and removes the device representation in the console.
- **Device Information (Query)** – Send an MDM query command to the device to return information on the device such as friendly name, platform, model, organization group, operating system version, and ownership status.
- **Device Wipe** – Send an MDM command to wipe a device clear of all data and operating system. This action cannot be undone.
- **Edit Device** – Edit device information such as **Friendly Name**, **Asset Number**, **Device Ownership**, **Device Group Device Category**.
- **Enroll** – Send a message to the device user to enroll their device. You can optionally use a message template that can include enrollment information such as step-by-step instructions and helpful links. This action is only available on unenrolled devices.
- **Enterprise Reset** – Enterprise Reset a device to factory settings, keeping only the Workspace ONE UEM enrollment.
    - **Windows Desktop Only:** Enterprise Reset restores a device to a Ready to Work state when a device is corrupted or has malfunctioning applications. It reinstalls the Windows OS while preserving user data, user accounts, and managed applications. The device will resync auto-deployed enterprise settings, policies, and applications after resync while remaining managed by Workspace ONE.

- **Enterprise Reset** – Enterprise Reset a device to factory settings, keeping only the Workspace ONE UEM enrollment.
  - **Windows Desktop Only:** Enterprise Reset restores a device to a Ready to Work state when a device is corrupted or has malfunctioning applications. It reinstalls the Windows OS while preserving user data, user accounts, and managed applications. The device will resync auto-deployed enterprise settings, policies, and applications after resync while remaining managed by Workspace ONE.
- **Find Device** – Send a text message to the applicable Workspace ONE UEM application together with an audible sound designed to help the user locate a misplaced device. The audible sound options include playing the sound a configurable number of times and the length of the gap, in seconds, between sounds.
- **Location** – Reveal a device's location by showing it on a map using its GPS capability enabled on the macOS Workspace ONE Intelligent Hub. This device action requires user approval to enable the functionality in macOS System Preferences.
  - If you want to display the location for multiple devices at a time, you must select devices for the bulk action using the Block selection method (using the shift-key) instead of the Global check box (next to the Last Seen column heading in the device list view).
- **Lock Device** – Send an MDM command to lock a selected device, rendering it unusable until it is unlocked.
- **Lock SSO** – Lock the device user out of Workspace ONE UEM Container and all participating applications.
- **Mark Do Not Disturb** – Mark the device not to be disturbed, preventing it from receiving messages, emails, profiles, and any other type of incoming interaction. Only those devices that are actively Marked Do Not Disturb have the action **Clear Do Not Disturb** available, which removes the restrictions.
- **Override Job Log Level** – Override the currently specified level of job event logging on the selected device. This action sets the logging verbosity of Jobs pushed through Product

Provisioning and overrides the current log level configured in Android Hub Settings. Job Log Level Override can be cleared by selecting the drop-down menu item **Reset to Default** on the action screen. You can also change the Job Log Level under the Product Provisioning category in Android Hub Settings.

- **Query All** – Send a query command to the device to return a list of installed applications (including Workspace ONE Intelligent Hub, where applicable), books, certificates, device information, profiles, and security measures.
- **Reboot Device** – Reboot a device remotely, reproducing the effect of powering it off and on again.
- **Remote Management** – Take control of a supported device remotely using this action, which starts a console application that enables you to perform support and troubleshoot on the device. Android devices require Remote Control Service to be installed on the device.
- **Request Device Log** – Request the debug log for the selected device, after which you can view the log by selecting the **More** tab and selecting **Attachments > Documents**. You cannot view the log within the Workspace ONE UEM console. The log is delivered as a ZIP file that can be used to troubleshoot and provide support.

  When you request a log, you can select to receive the logs from the **System** or the **Hub**. **System** provides system-level logs. **Hub** provides logs from the multiple agents running on the device.

  Android Only: you can retrieve detailed logs from corporate-owned Android devices and view them in the console to resolve issues on the device quickly.

For more information, see Request Device Log.

- **Send Message** – Send a message to the user of the selected device. Select between **Email**, **Push Notification** (through AirWatch Cloud Messaging), and **SMS**. Push notification requires Airwatch applications like Hub, Boxer etc which must have been launched at least once.
- **Start/Stop AWCM** – Start/Stop the Cloud Messaging service for the selected device. VMware AirWatch Cloud Messaging (AWCM) streamlines the delivery of messages and commands from the Admin Console. The AWCM eliminates the need for end users to access the public Internet or use consumer accounts such as Google IDs.
- **Sync Device** – Synchronize the selected device with the UEM console, aligning its **Last Seen** status.

Request Device Log

The Request Device Log command allows you to retrieve Workspace ONE Intelligent Hub or detailed system logs from corporate-owned devices and view them in the console to quickly resolve any issues on the device. The Request Device Log dialog box allows you to customize your logging request for Android devices.

Procedure

1 Navigate to **Groups & Settings > All Settings > Devices and Users > General > Privacy** and enable Request Device Log in the privacy settings.

   Employee- owned devices are not allowed to be selected due to privacy concerns

2 Navigate to **Devices > List View > Select device from list > More Actions > Request Device Log**.

3 Customize the log settings:

Setting	Description
Source	Select **Hub** to collect logs generated by Workspace ONE Intelligent Hub. Select **System** to include all applications and events on the device. System is available based on your privacy settings and is limited to device manufacturers with specific platform service applications. **Note** Available on devices running Platform OEM Service v3.3+, MSI Service v1.3+, and Honewell Service v3.0+. Select **Network** to record DNS requests and network connections from apps to a log file for the specified duration. **Note** Available on Work Managed devices running Android 8 or higher. **Note** Collect Public IP Address must be enabled in Privacy Settings.
Type	Select **Snapshot** to retrieve the latest log records available from devices. Select **Timed** to collect a rolling log over a specified period. Multiple log files may be sent to UEM console. The 'Level' option will not be available when Network is selected
Duration	Specify the duration of time for the device to collect and report logs to the console.
Level	Determine the level of detail included in the log (Error, Warning, Info, Debug, Verbose).

4 Select **Save**.

5 To review the log files, navigate to **Device Details > More > Attachments > Documents**.

6 You can cancel the device log request after the logs have been received and there is no further need for log collection. Navigate to **Devices > List View > Select device from list > More Actions > Cancel Device Log** to cancel the device log request.

AirWatch Cloud Messaging

AirWatch Cloud Messaging (AWCM) provides an internal communication solution for the entire Workspace ONE UEM solution as a comprehensive replacement for Google Cloud Messaging (GCM).

AWCM provides real-time device management status and command pushes for:

- Devices that cannot be configured with a Google Account.
- Devices restricted to internal network communication.
- Devices without public Internet access.

Enable AWCM by navigating to **Devices > Device Settings > Android > Hub Settings > AirWatch Cloud Messaging**.

Select **Enabled** on **Use AWCM Instead of C2DM** to enable AWCM. Selecting this option locks the deployment type to **Always Running** so that the system and device have a constant and ongoing line of communication. You may also choose to leave the **Use AWCM Instead of C2DM** check box unchecked and decide to make the deployment type **Always Running** or **Manual**, with an associated timeout value.

Workspace ONE Assist

Workspace ONE Assist, previously named Advanced Remote Management (ARM), allows you to connect remotely to end-user devices so you can help with troubleshooting and maintenance. The Assist Server facilitates communication between the Workspace ONE UEM powered by AirWatch and the "host" device.

For more information, see VMware Workspace ONE Assist Documentation.

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 or later.

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

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.

Register Samsung Enterprise Firmware Over The Air Updates

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

This field in the Restrictions profile only becomes available when you select Samsung from the OEM Settings field.

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**.

Android System Updates with Workspace ONE UEM

You can review and push updates for Android devices using Workspace ONE UEM. This is helpful in allowing you to perform testing to resolve any compability issues and monitor available upates across devices before pushing firmware updates to your device fleet. 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.

For Samsung devices, you must register for a Samsung E-FOTA license in order to get updates. Features are not available until registered.

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 Device Updates**.

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 devices 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.

OEM Service App

9

The OEM Service app is a plug-in app that is only installed and used in combination with Workspace ONE Intelligent Hub enrollment. It allows for additional MDM capabilities that only pertain to a specific OEM device.

After you enroll, Workspace ONE UEM automatically detects if the device can take advantage of additional device capabilities, and deploys an Original Equipment Manufacturer (OEM) specific service application to your Android device.

Important To install the Samsung Service App, enable **Push Service App from Play Store** in the Workspace ONE UEM console under **Devices > Device Settings > Android > Service ApplicationsService Applications**. Otherwise, end users must first enable **Allow Non-Market Applications** in device settings. For more information on the Workspace ONE Intelligent Hub for Android, please see Workspace ONE Intelligent Hub for Android.

Samsung Enterprise License Management (ELM) Service

New enrollments for Samsung devices will begin using the new non-platform key signed Samsung Enterprise License Management (ELM)Service 3.0 application available on the Play Store. The Samsung Service application will no longer be platform-signed with the introduction of the new Enterprise License Management (ELM) APIs. The Samsung ELM Service 3.0 is a server-based access control mechanism for MDM administrators to access the Samsung Knox Standard (SAFE) APIs. These APIs support devices running SAFE 4.0+ only.

The current service on the Play Store, Service 2.2, will continue to remain on the Store for devices running SAFE 3.0 and below. This new application will support new APIs for SAFE 4.0, as well as Knox 2.0 and Knox 2.1.

This chapter includes the following topics:

Best Practices for Configuring Restrictions with Android (Legacy) Devices

The following are some considerations for implementing device restrictions for Android devices.

- We do not recommend the **Allow WiFi** restriction on devices, especially for those without any cellular data available, as this will result in the loss of connectivity on the device.
- For **Allow Headphones**, enabling headphones while they are still plugged in will not work because headphones need to be initialized by re-plugging in.
- With the **Enable Bluetooth Secure Mode** you can restrict different Bluetooth profiles and whitelist the devices based on the Bluetooth class, name and UUID of the Bluetooth devices. This setting takes effect after secure mode is enabled and Bluetooth is turned on the next time.
- For Android 4.0 onward, disabling background data with **Allow Background Data** works only when a mobile data limit is set. When the policy is enabled, the mobile data limit is set to 100GB; the user cannot disable the mobile data limit but can change the actual limit.
- For **Allow SD Card Write**, this policy is not applicable when the SD card is encrypted. If SD card is encrypted, the files in the SD card cannot be read by other devices or PCs except for the device that encrypted it. Hence SD card encryption takes priority over this policy.
- If **Allow Camera** has been turned off for the main device user, then the camera will be disabled for all the containers and users created on the device.
- If **Allow Microphone** has been turned off for the main device user, then the microphone will be disabled for all the containers and users created on the device.
- The **Allow Clipboard** policy only takes effect over native Android clipboard.
- Allow **Incoming MMS** and **Allow Outgoing MMS** applies to the native MMS client application.

Android (Legacy) OEM Specific Profiles Matrix

This matrix summarizes specific functionality and configurations, as available by OEM.

	Standard	Samsung	LG	Lenovo	HTC	Zebra	Panasonic	Amazon	Nook	Sony	Intel	ASUS
Email												
Native Email Configuration		v1.0+	v1.0+		v1.0+					v5.0+		
Allow Email Forwarding		v3.0+								v5.0+		
Disable Non-Enterprise Email Account Addition		v4.0+								v5.0+		

	Standard	Samsung	LG	Lenovo	HTC	Zebra	Panasonic	Amazon	Nook	Sony	Intel	ASUS
Prevent Enterprise Email Account Removal		v4.0+								v5.0+		
Application Control												
Prevent Installation of Blacklisted Apps		v2.0+	v1.0+					v1.0+	v1.0+	v3.0+	v1.0+	v1.0+
Prevent Un-Installation of Required Apps		v1.0+	v1.0+					v1.0+	v1.0+	v7.0	v1.0+	
Allow Only Whitelisted Apps		v2.0+								v3.0+	v1.0+	
Silent Application Install		v1.0+	v1.0+			MX v1.3+	v1.0+	v1.0+	v1.0+	v9.0	v1.0+	
Clear Specific Application Data Command		v2.0+	v1.0+			MX v1.3+		v1.0+				
Allow Voice Dialer		v2.0+										
Device Administration												
Silently Set Device Administrator					v1.0+	MX v1.3+		v1.0+				
Silently Remove Device Administrator					v1.0+	MX v1.3+		v1.0+				
Prevent Device Admin Removal by User					v1.0+			v1.0+				
Allow Activation Lock		v5.0+										
Allow Developer Mode		v5.0+										

	Standard	Samsung	LG	Lenovo	HTC	Zebra	Panasonic	Amazon	Nook	Sony	Intel	ASUS
Allow Firmware Recovery		v5.0+										
Headphone State		v5.0+										
Allow Fast Encryption		v5.0+										
Allow Device Administrator Deactivation										v5.0+		
Encryption												
Require Storage Encryption	v3.0+	v2.0+	v1.0+	v1.0+	v1.0+	MX v1.3+						
Require SD Card Encryption		v2.0+	v1.0+	v1.0+		MX v1.3+				v2.0+		
Remote Troubleshooting												
Remote Management		v4.0+	v1.0+			MX v1.3+	v1.0+					
Device Reboot		v3.0+				MX v1.3+		v1.0+				
Network												
Configure Basic Native VPN Types	v2.2-2.3.5	v2.0+	v1.0+		v1.0+			v1.0+				
Configure Advanced Native VPN Types		v3.0+	v1.0+		v1.0+							
Set Minimum Wi-Fi Security Level		v2.0+	v2.0+									
Certificate Management												
Silent Certificate Install		v2.0+	v1.0+			MX v1.3+		v1.0+		v2.0.1+		
Lock Screen Customization												
Set Enterprise Custom Images on Lock Screen		v4.0+										

	Standard	Samsung	LG	Lenovo	HTC	Zebra	Panasonic	Amazon	Nook	Sony	Intel	ASUS
Set Enterprise Contact Info on Lock Screen		v4.0+										
Allow Lock Screen Settings		v5.0+										

*For devices running Jelly Bean 4.3

‡For devices running Kit Kat

**Only supported on LG devices.

Android (Legacy) OEM Specific Restrictions Matrix

This matrix provides a representational overview of the restriction profile configurations available by OEM.

	Standard	Samsung	LG	Lenovo	HTC	Zebra	Panasonic	Amazon	Nook	Sony	Intel	ASUS	E
Device Functionality													
Allow Camera See Restrictions Best Practices for Configuring Restrictions with Android (Legacy) Devices	v4.0+	v2.0+		v1.0+		MX v1.3+					v1.0+		v
Allow Microphone See Restrictions Best Practices for Configuring Restrictions with Android (Legacy) Devices		v2.0+	v2.0+	v1.0+						v7.0			v
Allow Factory Reset		v2.0+	v1.0+					v1.0+				v1.0+	v
Allow Airplane Mode		v5.0	v2.0+										
Allow Screen Capture		v2.0+	v1.0+						v1.0+	v5.0+	v1.0+		
Allow Mock Locations		v2.0+	v2.0+			MX v1.3+							

	Standard	Samsung	LG	Lenovo	HTC	Zebra	Panasonic	Amazon	Nook	Sony	Intel	ASUS	E
Allow Clipboard See Restrictions Best Practices for Configuring Restrictions with Android (Legacy) Devices		v2.0+	v2.2+										
Allow USB Media Player		v2.0+	v2.2+										
Allow NFC			v2.0+							v7.0			
Allow NFC State Change		v5.0+											
Allow Home Key		v2.0+						v1.0+		v1.0+			
Allow Email Account Addition		v5.0+							v6.0+				
Allow Email Account Removal		v5.0+											
Allow Google Account Addition		v4.0+											
Allow POP / IMAP Email			v1.0+							v6.0+			
Allow Power Off		v3.0+	v4.0										
Allow Safe Mode		v4.0	v4.0										
Allow Status Bar		v3.0+	v2.2+										
Allow Notifications		v3.0+											
Allow Wallpaper Change		v3.0+											
Allow Audio Recording if Microphone is Allowed		v4.0+											
Allow Video Recording of Camera is Allowed		v4.0+											
Allow Ending Activity When Left Idle		v4.0+											

	Standard	Samsung	LG	Lenovo	HTC	Zebra	Panasonic	Amazon	Nook	Sony	Intel	ASUS	E
Allow User to Set Background Process Limit		v4.0+											
Allow Headphones See Restrictions Best Practices for Configuring Restrictions with Android (Legacy) Devices		v5.0+											
Allow All Local Services										v5.0+			
Allow Fingerprint Authentication		v5.0+											
Allow Deactivate Device Admin		v4.0+						v1.0+		v6.0+	v1.0+		
Sync and Storage													
Allow USB			v1.0+										v
Allow USB Debugging		v2.0+	v2.0+	v1.0+		MX v1.3+		v1.0+		v5.0+	v1.0+		v
Allow USB Mass Storage		v2.0	v2.2+	v1.0+		MX v1.3+			v1.0+	v5.0+			v
Allow Google Backup		v2.0+	v2.2+										
Allow Google Account Auto Sync		v5.0+								v7.0			
Allow SD Card Access		v2.0+	v1.0+	v1.0+		MX v1.3+			v1.0+	v2.0+	v1.0+		
Allow OTA Upgrade		v3.0+	v2.2+										v
Allow SD Card Write See Restrictions Best Practices for Configuring Restrictions with Android (Legacy) Devices		v3.0+											
Allow USB Host Storage		v4.0+	v2.2+										
Allow SD Card Move		v5.0											

	Standard	Samsung	LG	Lenovo	HTC	Zebra	Panasonic	Amazon	Nook	Sony	Intel	ASUS	E
Allow Local Desktop Sync										v1.0+			
Applications													
Allow Google Play		v2.0+	v1.0+								v1.0+		
Allow YouTube		v2.0+	v1.0+								v1.0+		
Allow Access to Device Settings		v2.0+	v1.0+							v7.0			
Allow Developer Options		v5.0+	v4.0+						v1.0+				
Allow Account Settings								v1.0+					
Allow Non-Market App Installation		v2.0+	v1.0+	v1.0+		MX v1.3+		v1.0+		v5.0			v
Allow Background Data See Restrictions Best Practices for Configuring Restrictions with Android (Legacy) Devices		v2.0+	v2.2+			MX v1.3+							
Allow Voice Dialer		v2.0+	v1.0+										
Allow Google Crash Report		v3.0+											
Allow Android Beam		v4.0+	v3.0+										
Allow S Beam		v4.0+											
Allow S Voice		v4.0+											
Allow Copy & Paste Between Applications		v4.0+									v1.0+		
Allow User to Stop System Signed Applications		v4.0+											
Bluetooth													
Allow Bluetooth		v2.0+	v1.0+	v1.0+		MX v.1.3+		v1.0+		v2.0+			v

	Standard	Samsung	LG	Lenovo	HTC	Zebra	Panasonic	Amazon	Nook	Sony	Intel	ASUS	E
Force Bluetooth On													v
Allow Outgoing Calls Via Bluetooth		v2.0+											
Allow Bluetooth Discoverable Mode		v2.0+	v2.0+										
Allow Bluetooth Limited Discoverable Mode		v2.0+											
Allow Bluetooth Pairing		v2.0+	v2.2++										
Allow Bluetooth Data Transfer			v2.2++										
Allow Desktop Connectivity via Bluetooth		v2.0+											
Enable Bluetooth Device Restrictions		v3.0+											
Enable Bluetooth Secure Mode		v4.0+											
See Restrictions Best Practices for Configuring Restrictions with Android (Legacy) Devices													
Network													
Allow Wi-Fi		v2.0	v1.0+					v1.0+			v1.0+		
See Restrictions Best Practices for Configuring Restrictions with Android (Legacy) Devices													
Allow Cellular Data		v2.0+	v1.0+					v1.0+			v1.0+		
Allow Wi-Fi Profiles		v2.0+	v2.2+										
Allow Wi-Fi Changes		v2.0+						v1.0+					

	Standard	Samsung	LG	Lenovo	HTC	Zebra	Panasonic	Amazon	Nook	Sony	Intel	ASUS	E
Allow Unsecure Wi-FI		v4.0+											
Allow Auto Connection Wi-Fi		v4.0+											
Allow Prompt for Credentials		v2.0+											
Minimum Wi-Fi Security Level		v2.0+	v2.0+										
Allow Only Secure VPN Connections		v4.0+											
Block Wi-Fi Networks by SSID		v2.0+	v1.0+										
Allow Sending SMS			v1.0+							v5.0+			v
Allow Native VPN		v2.0+	v4.0+										
Allow Wi-Fi Direct		v4.0+	v2.2+										
Allow Infrared			v4.0+							v4.0+			
Set Wi-Fi Sleep Setting						MX v1.3+							
Set Global HTTP Proxy		v4.0+						v1.0+	v1.0+			v1.0+	
Allow Cellular										v7.0			
Roaming													
Allow Data Usage on Roaming		v2.0+	v1.0+	v1.0+		MX v1.3+		v1.0+		v4.0+			v
Allow Automatic Sync on Roaming		v2.0+	v1.0+								v1.0+		
Allow Push Messages on Roaming		v2.0+											
Allow Roaming Voice Calls										v7.0			
Disable Voice Calls While Roaming		v3.0+	v2.2+										
Tethering													
Allow All Tethering		v2.0+	v1.0+	v1.0+						v2.0+	v1.0+		

	Standard	Samsung	LG	Lenovo	HTC	Zebra	Panasonic	Amazon	Nook	Sony	Intel	ASUS	E
Allow Wi-Fi Tethering		v2.0+	v2.0+	v1.0+			v1.1				v1.0+		
Allow Bluetooth Tethering		v2.0+	v2.0+				v1.1						
Allow USB Tethering		v2.0+	v2.0+				v1.1						
Browser													
Allow Native Android Browser		v2.0+	v1.0+							v2.0+			
Allow Pop-Ups		v2.0+											
Allow Cookies		v2.0+											
Enable Autofill for Android		v2.0+											
Enable JavaScript For Android		v2.0+											
Force fraud warning		v2.0+											
Location Services													
Allow GPS Location Services		v2.0+	v1.0+			MX v1.3+		v1.0+					v
Allow Wireless Network Location Services		v2.0+	v1.0+			MX v1.3+							
Allow Passive Location Services		v2.0+	v2.2+										
Phone and Data													
Allow Non-Emergency Calls (If disabled, then the device will not be able to send SMS/MMS messages as well.)		v2.0+	v2.2+										
Allow User to Set Mobile Data Limit		v4.0+											
Allow SMS with Storage		v4.0+											
Allow MMS with Storage		v4.0+											

	Standard	Samsung	LG	Lenovo	HTC	Zebra	Panasonic	Amazon	Nook	Sony	Intel	ASUS	E
Allow WAP Push		v4.0+											
Enable SIM PIN Lock		v4.0+											
Maximum Data Usage		v2.0+											
Call And SMS Limit		v4.0+											
Call Restriction		v5.0+											
SMS Restriction		v5.0+											
Miscellaneous													
Set Device Font		v4.0+											
Set Device Font Size		v4.0+											
Hardware Restrictions													
Allow System Bar		v3.0+	v2.2+										
Allow Task Manager		v3.0+	v2.2+										
Allow Menu Key		v3.0+	v2.2+										
Allow Back Key		v3.0+	v2.2+										
Allow Search Key		v3.0+											
Allow Volume Key		v3.0+											
Security													
Allow Activation Lock		v5.0+											
Force Fast Encryption		v5.0+											
Allow Firmware Recovery		v5.0+											
Allow Lock Screen Settings		v5.0+											
Allow User Creation (Requires Allow Multiple Users to be enabled)		v4.0+											

	Standard	Samsung	LG	Lenovo	HTC	Zebra	Panasonic	Amazon	Nook	Sony	Intel	ASUS	E
Allow User Removal (Requires Allow Multiple Users to be enabled)		v4.0+											
Allow Multiple User		v4.0+											
Allow Keyguard	v5.0+												
Allow Trusted Hub	v5.0+												
Allow Camera on Keyguard Screen	v5.0+												
Allow Fingerprint on Keyguard Screen	v5.0+												
Allow Notifications on Keyguard Screen	v5.0+												
Allow Un-redacted Notifications on Keyguard Screen	v5.0+												
Allow Fingerprint Unlock		v5.0+											

*For devices running Jelly Bean 4.3

‡For devices running Kit Kat

Supported Samsung Devices Matrix

The matrix below specifies which device types apply to each Samsung SAFE version.

Devices that are SAFE 4.0 and above are also Knox compatible as long as they meet the minimum firmware requirements. Please contact your mobile device provider to ensure your devices meet these requirements.

Device	SAFE 1.0	SAFE 2.0	SAFE 3.0	SAFE 4.0	SAFE 5.0
Galaxy Tab	✓				
Galaxy Tab 10.1	✓*	✓‡			
Galaxy Tab 8.9	✓*	✓‡			
Galaxy Tab 7.0 Plus	✓*				
Galaxy Tab 7.7		✓			

Device	SAFE 1.0	SAFE 2.0	SAFE 3.0	SAFE 4.0	SAFE 5.0
Galaxy Tab 2 7.0			✓‡		
Galaxy Tab 210.1			✓‡		
Galaxy Note 10.1		✓‡	✓		
Galaxy Note 8.0		✓‡			
Galaxy Note		✓‡			
Galaxy Note 2			✓‡		
Galaxy Note 3				✓‡	
Galaxy S	✓				
Galaxy SII		✓			
Galaxy SIII			✓		
Galaxy S IV				✓	
Galaxy S5					✓
Galaxy Tab S					✓
Galaxy Tab 4					✓
Note 3				✓	
Tab 3 (10.1)				✓	
Galaxy S6					✓
Galaxy S6 Edge					✓
Galaxy S7					✓
Galaxy S7 Edge					✓
Galaxy Note 4					✓
Galaxy Note 5					✓

*For devices running Ice Cream Sandwich and below.

‡For devices running Ice Cream Sandwich and above.

Devices by Manufacturer and Version

Review this matrix as a quick glance at some of the supported devices by manufacturer and version.

Manufacturer	1.0+	1.3+	2.0+	3.0+	4.0+	5.0+	6.0+	7.0+
LG	LG Optimus G by Sprint LG Intuition by VzW		LG G2 LG G2 980	LG G-Flex– v3.1 LG G3– v3.2 LG G3 Beat– v3.2	LG G4 LG G5			
HTC	HTC One X HTC One X Plus HTC One S HTC One V HTC Evo 4g		HTC One HTC One M8					
Moto		ET1 N0 ET1 N1 MC40 TL55 ML67 TC70						
Panasonic	Toughpad							
Lenovo	Thinkpad Tablet							
Amazon	Kindle Fire HDX Kindle Fire HD Fire Phone							
Barnes and Noble	Nook HD							
Intel	Baytrail Grandhill Flaghill							

Manufacturer	1.0+	1.3+	2.0+	3.0+	4.0+	5.0+	6.0+	7.0+
Sony			Z Tablet Z ZL ZR A UL	Z1* Z Ultra* Z1Compact*	Z Tablet Z, ZL, ZR, A, UL Z1‡ Z Ultra‡ Z1 Compact, Xperia C4 Xperia E4g T2 Ultra Z2, Tablet Z2 C3, Z3 Z3 Compact Z3 Tablet Compact	Z2 Tablet Z2 Cosmos S50 Lavender Xperia M4 Aqua Ivy Karin Z2, Tablet Z2 T2 Ultra, C3 Z3 Z3 Compact Z3 Tablet Compact , Xperia E3, Xperia M2/ M2Aqua, Xperia T3	Z2 Tablet Z2, Z3, Z3 Compact, Z3 Tablet Compact, Xperia E4g, Z5 Premium	Z1, Z Ultra, Z1 Compact, Z2, Tablet Z2, Z3, Z3 Compact, Z3 Tablet Compact, Xperia Z3+, Z4 Tablet, Xperia M4 Aqua, S50, Lavender, Z5 Premium
Asus	Memopad Griffin							

*For devices running Jelly Bean 4.3

‡For devices running Kit Kat

Samsung License Servers

With the new Samsung ELM Service, the devices need access to the Samsung license servers. This is required so when you activate Knox services, devices can verify that their license keys devices periodically check their licenses a few times a week.

If you are in the Americas, configure access to these servers:

- gslb.secb2b.com:443
- us-elm.secb2b.com:443
- us-prod-klm.secb2b.com:443

If you are in China, configure access to these servers:

- china-gslb.secb2b.com.cn:443
- china-elm.secb2b.com.cn:443

- china-klm.secb2b.com.cn:443

If you are in Asia, Africa, Europe, or other regions, configure access to these servers:

- gslb.secb2b.com:443
- eu-elm.secb2b.com:443
- eu-prod-klm.secb2b.com:443

Note If your enterprise is highly regulated and does not allow communication to external servers, you can request the on-premises Knox server, which handles license verification within your firewall. Samsung charges an extra fee for this service. Samsung: https://www.samsungKnox.com/contact

Samsung Knox Servers

The device needs access to the Knox servers to activate the Knox license for creating the Samsung Knox container on the device.

Americas (USA, Canada, Brazil, and so on,..)

- gslb.secb2b.com:443
- us-elm.secb2b.com:443
- us-Knox.secb2b.com:443
- us-prod-klm.secb2b.com:443
- kaps.secb2b.com:443
- d28lmkz7f2awiw.cloudfront.net:443

China

- china-gslb.secb2b.com.cn:443
- china-elm.secb2b.com.cn:443
- china-Knox.secb2b.com.cn:443
- ch-prod-klm.secb2b.com:443
- china-kad.secb2b.com.cn:443
- bjprodkad.blob.core.chinacloudapi.cn:443

All other countries

- gslb.secb2b.com:443
- eu-elm.secb2b.com:443
- eu-Knox.secb2b.com:443
- eu-prod-klm.secb2b.com:443
- kaps.secb2b.com:443

- d28lmkz7f2awiw.cloudfront.net:443

Platform OEM Service

10

The Platform OEM (POEM) Service is an additional app that allows the Workspace ONE UEM console to provide extended management capabilities to Android devices.

After you enroll, the Workspace ONE UEM console automatically detects if the device can take advantage of additional device capabilities, and deploys an Original Equipment Manufacturer (OEM) specific service application to your Android. The OEM Service app is a plug-in app that is only installed and used in combination with Workspace ONE Intelligent Hub enrollment.

It allows for additional MDM capabilities that only pertain to a specific OEM device. All of these APKs are available through AirWatch Resources by request. There are a few service apps that we publish to the Google Play Store (see list below).

Here is a sample of supported features and available OEMs for the Platform OEM Service.

POEM Service Features

- Silent App installation, uninstallation, and updates
- Silent Device Administrator Activation on launch
- Date/Time configuration (date format, time format, time zone, server time, SNTP, HTTP URL, or Auto)
- Toggle Bluetooth on/off with the Disable Bluetooth restriction
- Disable installation from unknown sources on 5.0 Lollipop and above
- Device Reboot

POEM Service Versions

- Bluebird
- Kube
- Getac
- Honeywell
- HP
- Intermec

- Lenovo
- Mediawave
- Panasonic
- Sonim
- Zebra CC5000

POEM Service Version Available on the Google Play Store

- Samsung
- Sony
- LG
- Huawei
- Zebra
- Honeywell

This chapter includes the following topics:

Install the Platform OEM Service

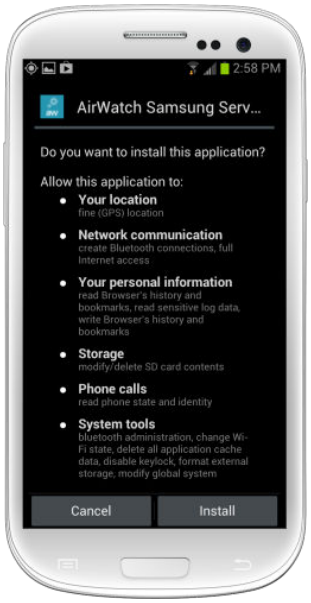
Install the Platform OEM Service (POEM) to gain additional MDM capabilities that only pertain to a specific OEM device.

The Platform OEM Service for each OEM is available on AirWatch Resources but requires you to be whitelisted (contact Workspace ONE Support). You must download the APK and either sideload it onto devices or configure it as an internal application in the Workspace ONE UEM console .

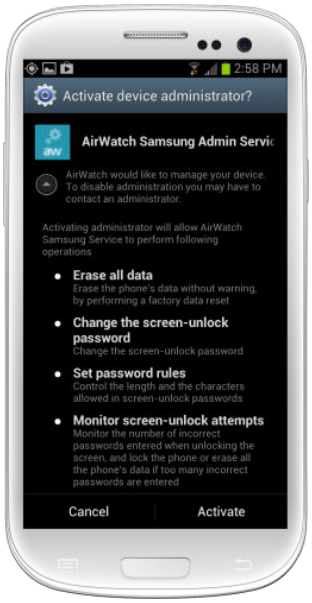
Procedure

1. Download the appropriate Platform OEM Service from AirWatch Resources.
2. Enroll the Android device into the Workspace ONE UEM console.
3. Either sideload the Platform OEM Service onto the device or configure it to push as an internal application from the Workspace ONE UEM console.
4. If you push the Platform OEM Service as an internal app, users are prompted to install it.

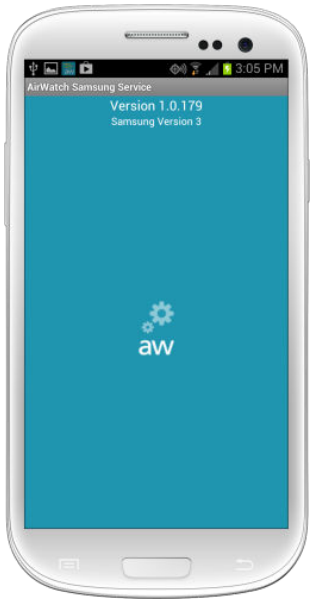
5 The example below shows how to run the AirWatch Samsung Service for Android devices.



After installing the Workspace ONE Intelligent Hub, you are automatically prompted to begin installing the service app. Select **Install**, when prompted.



Once it installs, you are prompted to activate the device administrator. Select **Activate**.



The blue screen indicates the **Service Application** upload is successful.

View the homepage to see the successfully downloaded **Hub** and **Service Application**.

In order to install the Samsung Service App, enable **Push Service App from Play Store** in the Workspace ONE UEM console under **Devices > Device Settings > Android > Service Applications Service Applications**. Otherwise, end users must first enable **Allow Non-Market Applications** in device settings.

Android Platform OEM (POEM) Service

The Android Platform OEM (POEM) Service is a service kit app that allows VMware AirWatch to provide extended management capabilities to generic Android devices.

When a customer has chosen a more cost-effective or "off brand" Android device to support their business need, the chances that the Workspace ONE UEM console supports advanced enterprise management features is very low, so the POEM Service allows customers to use these devices and support certain features which require minimal effort from the OEM or the customer.

Android Platform OEM (POEM) Features

Version	Features
1.0	■ Silent App installation, uninstallation, and updates. ■ Silent Device Administrator Activation on launch. ■ Silent Device Administrator of Hub during Auto Enrollment (client SDK) ■ Date/Time configuration (date format, time format, time zone, server time, SNTP, HTTP URL, or Auto). ■ Toggle Bluetooth on/off with the Disable Bluetooth restriction. ■ Enable/Disable installation from unknown sources on 5.0 Lollipop and above. ■ Device Reboot ■ Silent Certificate Install/removal
2.0	■ App whitelist - add/update/remove ■ App blacklist - add/update/remove, including system apps ■ Enable/Disable Google Play ■ Enable/Disable USB ■ Set & Get Default Launcher ■ Configure, update, remove, set default APN
3.0	■ OS Upgrade ■ Enable/Disable SD Card
3.2	■ Send full device logs via Hub menu ■ Migration from Legacy Rugged Service ■ Allow SD card
v3.3	■ Collect a rolling system log ■ Enabled Notification access for AirWatch Launcher
3.6	■ Automatically grant Usage Access for Launcher (requires Launcher 4.0.1 or higher)
4.0	■ Bug Fixes

Honeywell Service Supported Features

Feature	Description	Supported Version
Enrollment		
Barcode Enrollment	Create barcode using EZ Config, device scans barcode to download Hub and enroll.	1.0
Sideload Staging	Create sideload package manually, run batch file to install Hub and enroll.	1.0
Client SDK Enrollment	Auto enrollment supported via Client SDK API. Hub and Service are silently activated and enrolled	1.0
Persistence	Hub and enrollment is persisted through an enterprise reset.	1.1
Security		
Silent Device Administrator Activation	Ability to activate the Workspace ONE Intelligent Hub and Service as device admin without user prompt.	1.0

Feature	Description	Supported Version
Silently Set Default Launcher	Ability to set the default launcher without user prompt.	2.0
Migration from Legacy Rugged Service	Legacy Rugged Service will be removed when Honeywell Service is installed on the device	3.0
Notification Access for Launcher	Launcher is automatically granted Notification Access allowing for smoother setup process for user	3.1
Usage Access for Launcher	Automatically granted Usage Access allowing for complete silent setup . Requires Launcher 4.0.1+	3.3
Restrictions		
Allow Airplane Mode	Enable or disable airplane mode.	1.0
Allow Bluetooth	Enable or disable Bluetooth.	1.0
Force Bluetooth On	Forces Bluetooth on so user cannot turn it off.	1.0
Allow GPS	Enable or disable GPS Location on the device.	1.0
Force GPS On	Force GPS on so user cannot turn off.	1.0
Allow USB Debugging	Enable or disable USB Debugging found in Developer Options.	1.0
Allow USB Mass Storage	Enable or disables the ability to mount the device as storage to a PC. Affects both MTP & PTP.	1.0
Allow Wi-Fi	Enable or disable Wifi - when disabled, user cannot turn it on.	1.0
Force Wi-Fi On	Force Wifi on so user cannot turn it off.	1.0
Allow Safe Mode	Enable or disable the ability to reboot the device into Safe Mode.	1.1
Disable Guest Account Addition	Disable the ability to add a guest user on the device	3.1
Apps		
Silent Install/Uninstall/Update of Apps	Apps can be installed or uninstalled or updated without any user interaction.	1.0
App Whitelist	Only whitelisted applications will be able to be installed. Non-whitelisted applications will be disabled or removed from the device.	1.1
App Blacklist	Blacklisted Applications will be disabled or removed from the device and cannot be installed.	1.1
Date/Time		
Set Automatic Date/Time	Set the Date/Time and Timezone to Automatic on the device.	2.0
SNTP Time Server	Sync the Date/Time with a specific Time Server.	2.0
HTTP URL Time	Sync the Date/Time with any HTTP URL.	2.0
Server Time	Sync the Date/Time with the AW Console.	2.0
Set Date Format	Set the Date Format to various different options (12/12/2015, 31/12/2015, Sept 31, 2015, etc).	2.0
Set Time Format	Set the time to 12H or 24H.	2.0
Set Time Zone	Set the Time Zone on the device.	2.0

Feature	Description	Supported Version
Certificate Management		
Silent Certificate Install	Install certificates without user interaction.	1.0
Silent Certificate Removal	Remove/Uninstall certificates without user interaction.	1.0
File/Actioms		
Reboot	Send a reboot product or file/action.	1.0
Enterprise Reset	Send an Enterprise Reset from the Console and Workspace ONE Intelligent Hub and enrollment will be persisted.	1.1
Factory Reset	Send a Factory Reset from the Console and Workspace ONE Intelligent Hub and enrollment are not persisted.	1.1
Write Files to IPSM Directory	Push files down to the IPSM folder through file/actions.	1.0
OS Upgrade	Push an OS File to IPSM/autoinstall folder and reboot to perform OS upgrade.	1.0
MDM Hub Upgrade	Upgrade the Workspace ONE Intelligent Hub and HW Service via Files/Actions - New app versions are persisted.	1.1-KK 1.2 - M
Miscellaneous		
APN Configuration	Configure APN settings on the device.	1.1
VPN Configuration	Supported VPN types: PPTP L2TP/IPSEC PSK L2TP/IPSEC RSA IPSEC XAUTH PSK IPSEC XAUTH RSA IPSEC HYBRID RSA	1.1

MSI Service Features

Feature	Description	Version
Support for silent certificate install	Install Certificates without user interaction.	v1.0
Support for Allow Roaming Data restriction	Enable or disable Data Usage while Roaming.	v1.0
Set emergency button press interval	Specify length of time (between 1000-10000 milliseconds) required to hold down emergency button before emergency signal is sent. Once this setting is configured on the device, the user can send an emergency signal by holding down the emergency button for the specified amount of time.	v1.0
Support for Enable/disable all system certificates	Configure to determine the use of System Certificates (all the certificates listed in Settings > Certificates > System).	v1.0

Feature	Description	Version
Enable/disable specific applications on the device	All application listed can be enabled or disabled without being uninstalled.	v1.0
Allow application whitelisting	Enable to prevent the installation of any application that is not a whitelisted app defined in Applications Groups.	v1.0
allow Application Blacklisting	Enable to prevent the installation and enforce the automatic removal blacklisted apps defined in Application Groups.	v1.0
Allow USB	Enable or disable the connection to a PC over the USB port.	v1.0
Allow MTP	Enable or disable the “MTP” connection option when connected to a PC.	v1.0
Allow Tethering	Allow end users to tether their devices to other managed or unmanaged devices.	v1.0
Allow Voice Service	Enable or disable the ability to use voice services (make phone calls).	v1.0
Allow SD Card	Enable or disable access to external SD card.	v1.0
Allow Wi-Fi	Enable or disable Wifi - when disabled, user cannot turn it on.	v1.0
Allow Bluetooth	Enable or disable Bluetooth.	v1.0
Allow Camera	Enable or disable to allow use of the camera.	v1.0
Allow Mobile Data	Enable or disable data usage over the cellular network.	v1.0
Configure cellular APN Settings on device	Use the “Advanced” profile payload to create an Access Point Name for the device to connect to a cellular network. Set this APN as default so the device will automatically connect.	v1.0
Apply Custom Settings File/ Action	Install a Motorola custom device settings package.	v1.0
OS Upgrade File/Action	Enable to perform an over the air OS upgrade.	v1.0
Encrypt SD Card	Allow SD card encryption.	v1.2
Send full device logs with Workspace ONE Intelligent Hub	View app logs inside the Workspace ONE Intelligent Hub and push them to the Workspace ONE UEM console or email the logs.	v1.3
Request Device Log Commands	Enable to request device log commands.	v1.3