VMware AirWatch Android Platform Guide

Deploying and managing Android devices

AirWatch v9.3

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

Table of Contents

Chapter 4: Compliance Policies 47

Chapter 5: Applications for Android Devices 49

Chapter 6: Shared Devices 59

vmware airwatch

vmware airwatch

4

Chapter 1:
Overview

vmware airwatch

Introduction to the Android Platform

AirWatch provides you with a robust set of mobility management solutions for enrolling, securing, configuring, and managing your Android device deployment. Through the AirWatch 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.

Supported Devices and OS Versions for Android Devices

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

Supported Operating Systems

- 4.0.X Ice Cream Sandwich
- 4.1.X Jelly Bean
- 4.2.X Jelly Bean
- 4.3.X Jelly Bean
- 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

OEMs that offer more management capability

- Samsung
- LG
- Lenovo
- HTC
- Motorola

- Amazon

- Barnes and Noble Nook

- Sony

- Panasonic

- Asus

- Intel

- Nexus

> **Caution**: To ensure successful installation and running of the AirWatch Agent on your Android 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 devices optimize by killing the app.

Requirements for Deploying Android Devices with AirWatch

The following are requirements needed for a successful deployment of AirWatch to your Android devices.

- **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 AirWatch 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 AirWatch Console.

- **Credentials** – Authenticates you as an end user in your AirWatch environment. These credentials may be the same as your network directory services or may be uniquely defined in the AirWatch Console.

Product Provisioning with Android 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.

Chapter 2:
Android Device Enrollment

Android Enrollment Overview

Each Android device in your deployment must be enrolled before it can communicate with AirWatch and access internal content and features. Enrollment is facilitated with the AirWatch Agent for Android. You can enroll devices using a web-based process that automatically detects if the AirWatch Agent is already installed. Additionally, you can pre-enroll devices for end users, or end users can enroll their own devices.

> **Note:** Certain Android OEM vendors offer features and capabilities that you can enable in the AirWatch Console. See Install an OEM Service App

Android devices must begin communicating with AirWatch to access internal content and features, which is facilitated using the AirWatch Agent. Available for download from the Google Play Store and the Amazon App Store, the AirWatch Agent provides a single resource to enroll a device as well as provide device and connection details. Additionally, agent-based enrollment allows you to:

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

> **Note**: **Looking for Android for Work?**, see the VMware Integration with Android for Work 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 on page 11

Enrollment Restrictions

You can create enrollment restrictions based on Android manufacturer and model to ensure only approved devices are allowed to enroll with AirWatch.

Android Device Enrollment with the AirWatch Agent

The AirWatch Agent application facilitates enrollment and allows for real-time management and access to relevant device information. The enrollment process secures a connection between Android devices and your AirWatch environment. For more information, see Android Device Enrollment with the AirWatch Agent on page 12.

AirWatch Agent Sideloading to Android Devices

Sideloading allows you to deploy the AirWatch Agent to Android devices without using the Google Play Store. For more information, see AirWatch Agent Sideloading to Android Devices on page 13.

Agent-Based Sideload Enrollment

Platform OEM Service

The Platform OEM Service is an additional app that allows AirWatch to provide extended management capabilities to any Android device. For more information, see Platform OEM Service Overview.

Email Autodiscovery

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.

Autodiscovery is a simplified approach that leverages information end users likely already know this information. See Setting up Autodiscovery for more information. 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 Enrolling Android Devices

The following information is required prior to enrolling your Android device.

If an email domain is associated 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 AirWatch environment. These credentials may be the same as your network directory services or may be uniquely defined in the AirWatch 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 AirWatch Console.

- **Credentials** – This unique username and password pairing allows you to access your AirWatch environment. These credentials may be the same as your network directory services or may be uniquely defined in the AirWatch Console.

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

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

vmware airwatch

Enrollment Restrictions

You can create enrollment restrictions based on Android manufacturer and model to ensure only approved devices are allowed to enroll with AirWatch.

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

Android Device Enrollment with the AirWatch Agent

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

Android devices use the Enrollment URL to first check and then download the AirWatch Agent. The AirWatch Agent provides a single resource to enroll a device as well as provides device and connection details. Additionally, the enrollment process allows you to:

- Authenticate users using basic or directory services, such as AD/LDAP/Domino, SAML, tokens or proxies.

- Authenticate users using pass through authentication using Single Sign On.

- Register devices in bulk or allow users to self-register.

- Define approved OS versions, models and maximum number of devices per user.

Enrolling an Android Device with the AirWatch Agent

The AirWatch Agent is the application that facilitates enrollment and allows for real-time management and access to relevant device information.

To enroll a device using the AirWatch Agent:

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

   AirWatch automatically detects if the AirWatch Agent 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 AirWatch Agent from the Google Play store.

2. Download and install the AirWatch Agent from the App Store, if needed.

> **Important:** To ensure successful installation and running of the AirWatch Agent 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 AirWatch Agent or return to your browser session to continue enrollment.

   - 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.

- If you have not configured email autodiscovery, then it will prompt you for the Enrollment URL and a Group ID.

- At first launch, the AirWatch Agent will ask 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 AirWatch Agent v5.3 for Android.

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.

AirWatch Agent Sideloading to Android Devices

Sideloading allows you to deploy the AirWatch Agent to Android devices without using the Google Play Store.

Sideload the Agent in the following situations:

- Sideload the Agent on to the following devices because these devices do not have access to the Google Play Store:

  - Motorola ET1

  - Motorola MC40

- Sideload the Agent if the company prohibits the use of Google Accounts. Users need a Google Account to access the Google Play Store.

Sideload AirWatch Agent Using a USB Port

Drag and drop the Agent from a computer to Android devices. Use this method to stage the agent on a small number of devices.

1. Put the Agent .apk file on a computer for easy access. Ask you AirWatch Account Manager for the latest version if you do not have it.

2. Prepare the Android 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. In order 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 Agent .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. After the installation completes, select the prompt to open the Agent and begin enrollment.

Sideload Using a Hosted Download Site

Send users a link that connects their Android devices to the Agent .apk file that you host on an internal server. Use this method to deploy the Agent to a large number of devices.

1. Host the Agent .apk file on an internal server that is accessible by devices for download. Ask your AirWatch Account Manager for the latest version if you do not have it. Instruct users to prepare the device for sideloading.

2. On the device, users navigate to **Settings > Security > Unknown sources** and select **Allow installation of non-Market apps**.

3. Send an email or text message that contains a direct link to the Agent .apk file to applicable users.

4. Direct users to navigate to and select the hosted file to install the Agent.

5. Instruct users to select the Agent download notification in the download notifications area on the device.

6. Instruct users to select the **AirWatchAgent_x.x apk** file.

   If users miss the download notification, they can find the Agent .apk file in the **Download** folder. The Download folder is in the native file manager or the **Files** application.

7. Direct users to select install. After installation completes, have users select the prompt to open the Agent and begin enrollment.

Sideload Upgrade

The process of sideloading an Android device affects the device's ability to upgrade the Agent version. In order for the sideloaded Android device to receive an Agent upgrade, you must deploy the new Agent version as an internal application through the AirWatch Console. You can get the upgrade file from your AirWatch Account Manager.

You do not need to deploy the Agent 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 Agent.

Chapter 3:
Android Device Profiles

vmware airwatch

16

Android Profiles Overview

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.

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 Access

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

Some examples of device access profiles include:

- Secure a device with a Passcode profile. For more information, see Device Passcode Profile (Android) on page 17
- Specify and control how, when and where your employees use their devices. For more information, see Configure Restrictions Profile (Android) on page 22.

Device Security

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

- Access internal resources such as email, files, and content. For more information, see Create a VPN Profile (Android) on page 25.
- Take administrative actions when a user installs or uninstalls certain applications. For more information, see Application Control Profile (Android) on page 34.

Device Configuration

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

- Connect your device to internal WiFi automatically. For more information, see Wi-Fi Profile (Android) on page 23.
- Access a URL directly from an icon on the device's menu. For more information, see Bookmarks for Android Devices on page 37

Device Passcode Profile (Android)

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 AirWatch 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)

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

To create a device passcode profile:

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

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

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

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

4. Configure the following Passcode settings.

Setting	Description
Minimum Passcode Length	Ensure passcodes are appropriately complex by setting a minimum number of characters.

Setting	Description
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	Enable to set a predefined passcode for use on devices with multiple end users. Complex Passcode Policies require a minimum Operating System of Android 3.0. This passcode must match the passcode requirements that you set in the profile. If the passcode does not meet the predefined requirements, the device prompts the end user to change the passcode to meet the requirements.
Passcode	Enter the predefined passcode that you want to use.
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
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.

Setting	Description
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.
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.

To configure the lockscreen overlay:

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

2. Select the **Passcode** profile from the list.

3. Enable the **Lockscreen Overlay** field.

4. Select your desired lockscreen overlay type: **Image Overlay** or **Company Information**.

5. 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	Uploadan 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**.

6. 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**.

7. Select **Save & Publish**.

Configure Restrictions Profile (Android)

Restrictions profiles provide a second layer of device data protection by allowing you to specify and control how, when and where your employees use their devices.

To create a Restrictions profile:

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

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

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

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

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)

Restriction profiles lock down native functionality of Android 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 Devices on page 79

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.

vmware airwatch

Setting	Description
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.
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)

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.

AirWatch 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)

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

To configure the Wi-Fi profile:

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

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

3. Configure the **General** profile settings as appropriate.

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

4. Select the **Wi-Fi** payload.

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

Setting	Description
Wi-Fi	
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.

Setting	Description
Fusion	
Include Fusion Settings	Enable to expand Fusion options for use with Fusion Adapters for Motorola devices.
Set Fusion 802.11d	Enable to use the Fusion 802.11d to set the Fusion 802.11d settings.
Enable 802.11d	Enable to use 802.11d wireless specification for operation in additional regulatory domains.
Set Country Code	Enable to set the Country Code for use in the 802.11d specifications.
Set RF Band	Enable to choose 2.4 GHz, 5 Ghz, or both bands and any channel masks applicable.
Proxy	
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.

Note: Fusion Settings apply only to Motorola Rugged devices. For more information about AirWatch support for Android Rugged devices, see the Rugged Android Platform Guide via AirWatch Resources.

6. Select **Save & Publish**.

Create a VPN Profile (Android)

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.

To create a VPN profile:

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

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

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

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

4. Select **VPN**and configure the settings. The Authentication settings that display vary based on the Connection Type selected from the Connection Info section.

5. The table below defines all settings that can be configured based on the VPN client.

Setting	Description
Connection Info	
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) on page 28 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 Configuring Per-app VPN for Android Devices. Per-app VPN is supported on Android 5.0+devices.
Authentication Info	
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.

Setting	Description
Realm	Define the server used to authenticate the device.
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.
VPN On Demand	
Enable VPN On Demand	Enable VPN On Demand to use certificates to automatically establish VPN connections.
Proxy	
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.

6. 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.

> **Note:** Per- App VPN is supported on Android 5.0+ devices.

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

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

3. Configure your VPN profile 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 **Save & Publish**.

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

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.

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)

Forcepoint lets you leverage your existing content filtering categories in Forcepoint and apply those to devices you manage within the AirWatch Console.

Directory users enrolled in AirWatch 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 devices, you will need to download a Forcepoint root certificate from the Forcepoint cloud service. You will upload the certificate to the AirWatch Console. AirWatch recommends that you use 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 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 AirWatch.

After the app is deployed to Android 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.

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

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

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

    These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

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 Forcepoint 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 AirWatch MDM with the Forcepoint cloud service. For this reason, AirWatch recommends that you set 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.

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

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

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

    These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

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.

Setting	Description
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.
Incoming Mail	
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.
Outgoing Mail	
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.

Setting	Description
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.
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)

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, AirWatch integrates with multiple mail clients that configure EAS accounts on Android 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 EAS Mail using Native Mail Client (Android)

Use the following steps to create a configuration profile for the Native Mail Client:

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

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

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

    These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

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.
Login Information	
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 Deploying Credentials profile.
Settings	
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.

Setting	Description
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.
Restrictions	
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.
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.

vmware airwatch

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

Deploy EAS Mail Using IBM Notes Traveler (Android)

Use the following steps to create a configuration profile for IBM Notes Traveler:

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

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

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

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

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 AirWatch user accounts have an email username defined.

6. Select **Save & Publish**.

Application Control Profile (Android)

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 AirWatch Agent to remain on a device.

Application Control is available only for specific device models. For a full list, please see the Android OEM Specific Profiles Matrix on page 79.

Configure Application Control (Android)

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

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

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

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

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

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 Application Groups. **Note:** For instructions on creating application groups, see Mobile Application Management Guide available on AirWatch Resources.
Prevent Un-Installation of Required Apps	Enable to prevent the un-installation of required apps defined in Application Groups
Only Allow installation of Whitelisted Apps	Enable to prevent the installation of any application that is not a whitelisted app defined in Applications Groups

6. Select **Save & Publish**.

Configure an 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.

> **Note**: 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.

1. Navigate to **Apps & Books > Applications > Applications 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 AirWatch Console.

Setting	Description
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.
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.

   See the applicable platform guide for information on configuring application control profiles.

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.

Edit App Groups and the Application Control Profile

When you edit app groups for Android and Windows phone, follow these steps to reflect the update on devices.

1. Edit the app group first.

2. Edit the application profile to create a new version of it.

3. Save and publish the new version of the application profile to devices.

   The system does not reflect the changes to the app group unless the new version of the application control profile deploys to devices.

Bookmarks for Android 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)

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.

To add Bookmarks:

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

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

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

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

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)

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

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

Configure the following options to create certificate enabled profile:

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

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

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

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.

AirWatch Launcher (Android)

AirWatch Launcher allows your organization to completely customize the look and behavior of managed Android devices. The AirWatch Launcher app will replace your device's graphical user interface with one that has been custom tailored to your organization's specifications.

Even more, the AirWatch 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 AirWatch Launcher at this time.

> AirWatch Launcher is compatible with Android 3.0.

Create AirWatch Launcher Profile (Android)

To configure the settings of the AirWatch Launcher profile:

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

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

    These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

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 AirWatch or **Save & Publish** to add the profile and immediately deploy it to applicable Android devices.

Launcher Version Settings (Android)

After you configure the AirWatch Launcher settings, navigate to **Service Applications** in the AirWatch 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 AirWatch Launcher app to selected devices using organization groups. For more information on deploying profiles by organization group, please see the **Mobile Device Management Guide** available on AirWatch Resources.

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.

To configure this profile:

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

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

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

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

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.

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

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

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

    These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

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 AirWatch 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.

> **Important**: This profile can only be used by Motorola Rugged devices running Android.

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

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

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

    These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

4. Configure the Sound settings, including:

Setting	Description
Volumes	
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.
System	
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.

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

Configure Firewall Rules (Android)

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

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

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

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

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

These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

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**.

> **Note:** 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.

> **Note**: This profile can only be used by Motorola Rugged devices running Android.

To configure a Display profile, follow the steps detailed below:

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

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

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

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

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.

Setting	Description
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.

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

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

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

    These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

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

Setting	Description
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**.

Use Custom Settings (Android)

The **Custom Settings** payload can be used when new Android functionality releases or features that AirWatch 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.

To configure custom settings:

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

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

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

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

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

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

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. Since the code is now custom, you should test the profile devices with older versions to verify expected behavior.

12. Select **Save & Publish**.

Chapter 4:
Compliance Policies

Compliance Policy Overview

The compliance engine is an automated tool by AirWatch that ensures all devices abide by your policies. These policies may include basic security settings such as requiring a passcode and having a minimum device lock period. For certain platforms, you may also decide to set and enforce certain precautions. These precautions include setting password strength, blacklisting certain apps, and requiring device check-in intervals to ensure that devices are safe and in-contact with AirWatch.

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.

For more information about compliance policies, including which policies and actions are supported for a particular platform, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

Chapter 5:
Applications for Android Devices

Applications for Android Devices Overview

You can use AirWatch applications in addition to AirWatch 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.

AirWatch Agent for Android

The **AirWatch Agent for Android** is an application that enables the Native Android SDK API layer of management to which AirWatch connects.

AirWatch 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 AirWatch Agent 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 AirWatch Agent to access and manage device information and settings. Access device information from the following tabs on the left of the device display:

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

- **About** – Displays the version number of the AirWatch Agent 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 AirWatch Agent menu at the top of the display:

- **Send Data** – Transmit the latest device data to AirWatch.

- **Sync** – Synchronize corporate directory services data and resources on the device.

- **App Catalog** – Launch the application catalog within the AirWatch Agent 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 AirWatch.

- **Un-enroll** – Unenroll the device from AirWatch.

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

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

Additionally, **App Standby** mode allows the device to determine that an app is idle when the user is not actively using it. When devices are in either state, the AirWatch 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 AirWatch Console resumes.

Configure AirWatch Agent Settings

The settings configured for the AirWatch Agent determines how reports and metrics are reported back to AirWatch from the device.

Customize the capability of the Agent.

1. Navigate to **Devices > Device Settings > Android > Agent 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	Description
Heartbeat Interval (min)	Enter the heartbeat time interval, which is how frequently the Agent checks in with the AirWatch server. Reports beacon data to the AirWatch Console. The primary purpose of this report is to show compromised device status. However, beacon data also includes GPS, IP address and other minor data, such as model and OS version.

Setting	Description
Data Sample Interval (min)	Enter the data sample time interval, which is how frequently the Agent collects data from the device. Collects interrogator data and reports all data collected by the Agent, including Telecom and Network data, as well as the battery, power and memory status.
Data Transmit Interval (min)	Enter the data transmit time interval, which is how frequently the Agent sends data to the AirWatch server. Reports interrogator data to the AirWatch 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 AirWatch server. Checks in with the AirWatch 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 AirWatch 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.

4. 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 (**min**)	Enter the frequency at which the AirWatch Agent checks the application list.

5. 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**.

6. 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**, available on AirWatch Resources.

Setting	Description
Enable Containers	Select **Enabled** to allow profile creation for Samsung Knox Containers and to allow the Android Agent to create application containers for Samsung Knox devices.
Knox License Key	Enter your Samsung Knox License Key.

Setting	Description
Enable Audit Logging	Select **Enabled** to turn on audit logging and the related settings below.
	The AirWatch 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 AirWatch 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. The log levels are: • **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** – The log file will never be sent transmitted to the console. • **Critical** – The log file needs be at critical size to be transmitted to the console. • **Maximum** – The log file needs be at maximum size to be transmitted to the console. • **Full** – The log file needs be at full size to be transmitted to the console.

7. 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 AirWatch Console according to the Data Transmit Interval.

Setting	Description
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.

8. 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 AirWatch.
Enable SMS Logs	Reports that log any incoming and outgoing SMS messages to devices.
Enable Cellular Data Usage	Allows the AirWatch Console to create reports which details data usage.

9. Configure AWCM Settings, if applicable:

AirWatch Cloud Messaging (AWCM) provides an internal communication solution for the entire AirWatch 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.

10. Configure the **Remote Management** settings:

Setting	Description
Download Remote Control Cab	Select this link to download the cabinet (CAB) installer file for AirWatch Remote Management.

Setting	Description
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.
Advanced	
Remote Management Port	Enter the port used to communicate between the Remote Management Agent and the Tunnel Agent on the end-user device. This port is responsible for caching the different frames on the device for use with the screen sharing function. The default port is 7775. Consider leaving the default setting unless port 7775 is in use for other uses in your organization.
Device Log Level	Set the Device Log Level to control the verbosity of the remote management application on the device.
Log Folder Path	Define the Log Folder Path where the application saves the remote management log file on the device.
Display Tray Icon	Enable Display Tray Icon to show the remote management applet on the device.
Max Sessions	Enter the maximum number of concurrent sessions allowed on a device.
Number of Retries	Enter the number of retries allowed before communication attempts stop.
Retry Frequency (Seconds)	Enter the amount of time between attempts to communicate.
Heartbeat Interval (Seconds)	Enter the amount of time (in seconds) that passes between status updates that are sent from the device.
Connection Loss Retry Frequency (Seconds)	Enter the amount of time (in seconds) that passes between attempts to reestablish the connection.

See the VMware AirWatch Remote Management Guide available on AirWatch Resources for more information.

11. 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 agent settings.

    • **SDK Profile V2** – Select the profile that will provide the AirWatch Agent with the SDK settings configured for that organization group.

12. Select **Save**.

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

Configure Service Applications

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

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.
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.**
AirWatch Launcher Version	Select the desired Launcher version.

1. Select **Save**.

VMware Content Locker for Android

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 Admin Console, content from synced corporate repositories, or their own personal content.

Use the AirWatch 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. For more information about configuring and deploying the VMware Content Locker, see the **Mobile Content Management (MCM) Guide** available in the Resources Portal.

vmware airwatch

VMware Browser for Android

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, AirWatch recommends deploying the VMware Browser in conjunction with a restrictions profile blocking the native browser.

AirWatch Container for Android

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 AirWatch 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 **AirWatch Container User Guide for Android.**

VMware Boxer for Android

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 AirWatch apps, wrapped apps, and SDK-enabled apps without entering credentials for each application. Using the AirWatch Agent 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 AirWatch apps, wrapped apps, and SDK-enabled apps using a Default SDK Profile. To enable SSO:

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 AirWatch applications and maintain a persistent login.

3. Optionally set **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 AirWatch account) to authenticate, and an SSO Passcode does not exist.

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.

Chapter 6:
Shared Devices

Shared Devices Overview

Issuing a device to every employee in certain organizations can be expensive. AirWatch MDM 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.

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

When administering shared devices, you must first provision the devices with applicable settings and restrictions before deploying them to end users. Once deployed, AirWatch uses a simple login/logout 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/logout functions are self-contained within the AirWatch Agent. Self-containment ensures that the enrollment status is never affected, and that AirWatch can manage the device whether it is in use or not.

Shared Devices Capabilities

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

- **Functionality**

  - Personalize each end-user experience without losing corporate settings.

  - Logging in a device automatically 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 AirWatch Agent.

  - 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 AirWatch.

  - Authenticate end users during a login with directory services or dedicated AirWatch credentials.

  - 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 2.3+,

- iOS devices with AirWatch Agent v4.2+,

- MacOS devices with AirWatch Agent v2.1+.

When provisioning shared Android devices, enroll the device using the AirWatch Agent and set the AirWatch Launcher application as the default home screen. Next, specify which version of AirWatch Launcher to push to the device. Finally,

create the Launcher profile in the AirWatch Console. The AirWatch Launcher application replaces the Android native launcher.

For more information, see .

Define the Shared Device Hierarchy

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

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 any 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 may be required for the device to log in depending on your Shared Device configuration.
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.

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

   - 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.

   - 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 on page 62.

6. Select **Save**.

61

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.

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 AirWatch 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	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.

Setting	Description
Require Special Characters	Require special characters in the shared device passcode, which includes characters such as @, %, &, and so forth.
Shared Device Passcode Minimum Length	Set the minimum character length of the shared passcode.
Shared Device Passcode Expiration Time (days)	Set the length of time (in days) the shared passcode expires.
Keep Shared device Passcode for minimum time (days)	Set the minimum amount of time (in days) the shared device passcode must be changed.
Passcode History	Set the number of passcodes that are remembered by the system, providing a more secure environment by preventing the user from reusing old passcodes.
Auto Log out Enabled	Configure an automatic log out after a specific time period.
Auto Log out After	Set the length of time that must elapse before the **Auto Log out** function activates in **Minutes**, **Hours**, or **Days**.
Enable Single App Mode	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. Enabling Single App Mode also disables the Home button on the device.
Clear Device Passcode on Logout (Android Only)	This setting controls whether the current device passcode is cleared when the user logs out (checks in) a multi-user shared device.
Clear App Data on Logout (Android Only)	Select this checkbox to clear the app data when the user logs out of a shared device (checks it in).

4. Click **Save**.

For specific information about provisioning devices for single-user and multi-user device staging, see the **Mobile Device Management (MDM) Guide** available on AirWatch Resources..

Configure Android for Shared Device Use

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

To configure Launcher version settings:

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. See Create AirWatch Launcher Profile (Android) on page 39 for further details on the Launcher profile. 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.

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

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 AirWatch Agent and set the Android Launcher application as the default home screen. The Launcher application 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 AirWatch Console.

Log in to an Android device

1. From the 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, then end users are required to enter a **Group ID** to log in.

2. Tap **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.

Log out of an Android device

1. Tap the **Settings** button.

2. Select **log out**.

Chapter 7:
Product Provisioning for Android Devices

Product Provisioning for Android Devices Overview

Product provisioning allows you to create, through AirWatch, products containing profiles, applications, and files/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 AirWatch 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 AirWatch Agent, Wi-Fi profile, and any other important content. The methods of staging a device vary by platform.

Chapter 8:
Android Device Management

vmware airwatch

Android Device Management Overview

After your devices are enrolled and configured, manage the devices using the AirWatch 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 VMware AirWatch Dashboard. 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 AirWatch environment and their status. The Device Details page provides device-specific information such as profiles, apps, AirWatch Agent version and which version of any applicable OEM service currently installed on the device. You can also perform remote actions on the device from the Device Details page that are platform-specific.

Device Dashboard

As devices are enrolled, you can manage them from the AirWatch **Device Dashboard**. 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.

Device List View

Select **Devices > List View** to see a full listing of all devices.

The **Last Seen** column displays an indicator showing the number of minutes elapsed since the device has checked-in.

Select a device in the **General Info** column at any time to open the details page for that device.

Sort by columns and configure information filters to review device 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 choose 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. For instance, you can hide 'Asset Number' from the **Device List**.

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

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.

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 AirWatch 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 AirWatch 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 AirWatch 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 AirWatch Agent 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 (More ▼).

- **Network** – View current network (Cellular, Wi-Fi, Bluetooth) status of a device.

- **Security** – View current security status of a device based on security settings.

- **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.

- **Provisioning** – View complete history and status of all packages provisioned to the device and any provisioning errors.

- **Terms of Use** – View a list of End User License Agreements (EULAs) which have been accepted during device enrollment.

- **Alerts** – View all alerts associated with the device.

- **Shared Device Log** – View history of device in terms of Shared Device, including past check-ins and check-outs and current status.

- **Event Log** – View history of device in relation to MDM, including instances of debug, information and server check-ins.

- **Status History** – View history of device in relation to enrollment status.

- **Management** – Lock or perform Enterprise Wipe on all selected devices.

  When you lock a SAFE 4 device, you can configure a customized lock screen. Set the **Message Template** to **Custom Message**. Then, in the **Message** field, provide your text and provide a **Phone Number**.

- **Support** – Send a message to email AirWatch Technical Support regarding selected device. Also, locate the device according to its current GPS location.

- **Admin** – Change AirWatch Console settings, including changing organization group of selected devices or deleting devices from AirWatch MDM.

- **Advanced** – Perform a warm boot on devices to remotely reboot those devices. Select **Provision Now** to perform a number of configurations for selected devices.

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, AirWatch 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.

- **AirWatch Agent (Query)** – Send a query command to the device's AirWatch Agent to ensure it has been installed and is functioning normally.

- **App Remote View** – Take a series of screenshots of an installed application and send them to the Remote View screen in the Admin Console. You may choose the number of screenshots and the length of the gap, in seconds, between the screenshots.

  VMware Content Locker must be installed on the device to execute **App Remote View**.

- **Change Organization Group** – Change the device's home organization group to another pre-existing OG. Includes an option to select a static or dynamic OG.

- **Change Ownership** – Change the Ownership setting for a device, where applicable. Choices include Corporate-Dedicated, Corporate-Shared, Employee Owned and Undefined.

- **Delete Device** – Delete and unenroll a device from the Admin Console. This action does not remove any data from the device itself, only its representation in the console.

- **Device Information (Query)** – Send a query command to the device to return basic information on the device such as friendly name, platform, model, organization group, operating system version and ownership status.

- **Device Wipe** – Wipe a device clear of all data, including email, profiles and MDM capabilities and the device returns to a factory default state. This includes all personal user information if applicable. This action cannot be undone.

- **Edit Device** – Edit device information such as **Friendly Name**, **Asset Number**, **Device Ownership**, **Device Group** and **Device Category**.

- **Enroll** – Send a message to the device user to enroll their device. You may optionally use a message template that may 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 VMware AirWatch enrollment.

- **Enterprise Wipe** – Enterprise Wipe a device to unenroll and remove all managed enterprise resources including applications and profiles. This action cannot be undone and re-enrollment will be required for VMware AirWatch to manage this device again. Includes options to prevent future re-enrollment and a **Note Description** field for you to add any noteworthy details about the action.

  o Enterprise Wipe is not supported for cloud domain-joined devices.

- **File Manager** – Launch a File Manager within the AirWatch Console that enables you to remotely view a device's content, add folders, conduct searches and upload files.

- **Find Device** – Send a text message to the applicable VMware AirWatch application together with an audible sound (with options to repeat the sound a configurable number of times and the length of the gap, in seconds, between sounds). This audible sound should help the user locate a misplaced device.

- **Location** – Reveal a device's location by showing it on a map using its GPS capability.

- **Lock Device** – Lock the screen of a selected device, rendering it unusable until it is unlocked. Includes optional fields for a custom **Message**, **Phone Number**, and **Note Description**.

- **Lock SSO** – Lock the device user out of VMware AirWatch Container and all participating apps.

- **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 Agent Settings. Job Log Level Override can be cleared by selecting the drop-down menu item **Reset to Default** on the action screen, or by changing the Job Log Level under the Product Provisioning category in Android Agent Settings.

- **Query All** – Send a query command to the device to return a list of installed apps (including VMware AirWatch Agent, 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 Control** – Take control of a supported device remotely using this action, which launches a console application that enables you to perform support and troubleshooting on the device. This action requires Remote Control Service to be installed on the device.

- **Remote Management** – Take control of a supported device remotely using this action, which launches a console application that enables you to perform support and troubleshoot on the device. This action requires Remote Control Service to be installed on the device.

- **Request Device Log** – Request the debug log on the selected device, after which you may view the log by selecting the **More** tab and choosing **Attachments > Documents**. The log is delivered as a text file that can be used to troubleshoot and provide support. The device logs allow you to retrieve detailed logs from corporate-owned devices and view them in the console in order to quickly resolve any issues on the device.

  For more information, see .

- **Send Message** – Send a message to the user of the selected device. Choose between **Email**, **Push Notification** and **SMS**.

- **Start/Stop AWCM** – Start/Stop the AirWatch Cloud Messaging service for the selected device. VMware AirWatch Cloud Messaging (AWCM) streamlines the delivery of messages and commands from the Admin Console by eliminating the need for end users to access the public Internet or utilize consumer accounts, such as Google IDs.

- **Sync Device** – Synchronize the selected device with the AirWatch Console, aligning its **Last Seen** status.

AirWatch Cloud Messaging

AirWatch Cloud Messaging (AWCM) provides an internal communication solution for the entire AirWatch 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 > Agent 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.

Implement File Manager for AWCM Devices

This functionality is currently only available to Android devices utilizing AWCM, and allows you to gain additional management capability by accessing the device's file structure with File Manager.

To access File Manager:

1. Navigate to **Device Details** for an AWCM Android device.

2. Select **File Manager** from the **Support** tab.

3. From the **File Manager** area, utilize the following functions to edit the file structure and manage available content:

   - **Add Folder** – Create an additional file folder.

   - **Upload File** – Add a file to the selected folder.

   - **Refresh** – Regenerate the file list.

   - **Copy** – Create a copy of the selected file.

   - **Move** – Move the file to another folder.

   - **Download** – Download a local copy of the file.

Remote Control for Android Devices

Remote Control provides the ability to manipulate a remote device as if it were physically present. Remote Control capabilities directly saves time, and facilitates more efficient processing of help desk tickets.

Help desks often struggle to maximize their productivity because IT Administrators must rely on third party communication by employees with varying levels of technical knowledge to diagnose and correct device issues. This is a major strain, as figuring out the device issue by communicating with a third party is often time consuming; decreasing the number of tickets IT Administrators can close in a day.

Configure Remote Control for Android Devices

Remote Control eliminates the need to communicate device issues through email or phone calls. Once configured, IT admins can troubleshoot issues with user devices.

1. Verify prerequisites are met before implementing Remote Control.

   - Check for supported devices:

     - All Samsung devices (Samsung RC service in Play Store).

     - All LG devices (LG RC Service not in the store, distributed separately).

     - All Panasonic Toughpad.

     - All Motorola MX 1.3+ devices (The RC service is available on AirWatch Resources. The user's myAirWatch ID must be whitelisted for the download. This is done per request.).

   - Ensure active AirWatch Cloud Messaging (AWCM) Connection. Activate AWCM from the Advanced drop-down menu on the Device Details page.

   - Ensure you are operating AirWatch version 6.4 or greater.

   - Install the Remote Control app for your appropriate platform from the Play Store.

2. After AWCM is connected and the Remote Control app is installed, navigate to your Device Details view by selecting the Android device from the list view. Select **More** at the top right corner of the details view and select on **Remote Control** under the Support section.

3. Control the device remotely once the live image finishes loading.

   - Use the mouse to select hard keys.

   - Use the keyboard to type information into the device.

Remote Management

The Remote Management Service allows you to remotely connect to end-user devices so you can assist in troubleshooting and maintenance. The Remote Management Service requires your computer and the end user device to connect to the Remote Management Server to facilitate communication between the AirWatch Console and the end user device.

For more information on installing, configuring, and using the Remote Management Service, please see the **VMware AirWatch Remote Management Guide**, available on AirWatch Resources.

Samsung Enterprise Firmware Over The Air (EFOTA) Updates

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

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

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

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

Register Samsung Enterprise Firmware Over The Air Updates

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

To register Samsung EFOTA settings:

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.

To enable restrictions for Samsung EFOTA:

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

2. Select **Configure**

3. Enable **Register Enterprise FOTA**.

> **Note**: Allow OTA Upgrade must be enabled or firmware updates are blocked.

4. Select **Save & Publish**.

Android Updates Overview

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

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

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

For more information on published Android firmware updates, .

Publish Firmware Updates (Android)

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.

To push available updates on demand:

1. Navigate to **Devices > Lifecycle > Updates** and select the **Android** tab.

2. View and select the radio button beside the desired update.

3. Select **Publish > OK**. Users are prompted to accept the firmware update before it is installed on their device.

Appendix:
Android Features Matrices

Best Practices for Configuring Restrictions with Android 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.

- 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 OEM Specific Profiles Matrix

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

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Panasonic	Amazon	Nook	Sony	Intel	ASUS	Bluebird
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+			
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+	

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Panasonic	Amazon	Nook	Sony	Intel	ASUS	Bluebird
Prevent Un-Installation of Required Apps		v1.0+	v1.0+					v1.0+	v1.0+	v7.0	v1.0+		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+											
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+										

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Panasonic	Amazon	Nook	Sony	Intel	ASUS	**Bluebird**
Certificate Management													
Silent Certificate Install		v2.0+	v1.0+			MX v1.3+		v1.0+					
Lock Screen Customization													
Set Enterprise Custom Images on Lock Screen		v4.0+											
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 OEM Specific Restrictions Matrix

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

> **Looking for Knox restrictions?** See the AirWatch Containerization with Samsung Knox Guide, which contains a topic listing all of the available container restrictions.

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Panasonic	Amazon	Nook	Sony	Intel	ASUS	Bluebird
Device Functionality													
Allow Camera See Restrictions Best Practices	v4.0+	v2.0+		v1.0+		MX v1.3+					v1.0+		v1.0
Allow Microphone See Restrictions Best Practices		v2.0+	v2.0+	v1.0+						v7.0			v1.0
Allow Factory Reset		v2.0+	v1.0+					v1.0+				v1.0+	v1.0
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+							
Allow Clipboard See Restrictions Best Practices		v2.0+	v2.2+										

vmware airwatch

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Panasonic	Amazon	Nook	Sony	Intel	ASUS	Bluebird
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+	v2.2+						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+											
Allow User to Set Background Process Limit		v4.0+											
Allow Headphones See Restrictions Best Practices		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+										v1.0
Allow USB Debugging		v2.0+	v2.0+	v1.0+		MX v1.3+		v1.0+		v5.0+	v1.0+		v1.0
Allow USB Mass Storage		v2.0	v2.2+	v1.0+		MX v1.3+			v1.0+	v5.0+			v1.0

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Panasonic	Amazon	Nook	Sony	Intel	ASUS	Bluebird
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+										v1.0
Allow SD Card Write See Restrictions Best Practices		v3.0+											
Allow USB Host Storage		v4.0+	v2.2+										
Allow SD Card Move		v5.0											
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			v1.0
Allow Background Data See Restrictions Best Practices		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+											

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Panasonic	Amazon	Nook	Sony	Intel	ASUS	Bluebird
Bluetooth													
Allow Bluetooth		v2.0+	v1.0+	v1.0+		MX v.1.3+		v1.0+		v2.0+			v1.0
Force Bluetooth On													v1.0
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 See Restrictions Best Practices		v4.0+											
Network													
Allow Wi-Fi See Restrictions Best Practices		v2.0	v1.0+					v1.0+			v1.0+		
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+					
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+			v1.0

vmware airwatch

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Panasonic	Amazon	Nook	Sony	Intel	ASUS	Bluebird
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+			v1.0
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+		
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+					v1.0
Allow Wireless Network Location Services		v2.0+	v1.0+			MX v1.3+							

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Panasonic	Amazon	Nook	Sony	Intel	ASUS	Bluebird
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+											
Allow WAP Push		v4.0+											
Enable SIM PIN Lock		v4.0+											
Maximum Data Usage		v2.0+											
Call And SMS Limit		v4.0+											
Call Restriction	v4.0+												
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+											

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Panasonic	Amazon	Nook	Sony	Intel	ASUS	Bluebird
Allow User Creation (Requires Allow Multiple Users to be enabled)		v4.0+											
Allow User Removal (Requires Allow Multiple Users to be enabled)		v4.0+											
Allow Multiple User		v4.0+											
Allow Keyguard	v5.0+												
Allow Trusted Agent	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 2 10.1			✓ ‡		
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.

Note: The matrix above applies to devices available as of January 2018

vmware airwatch

Samsung License Servers

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

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

- gslb.secb2b.com:443

- us-elm.secb2b.com:443

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

If you are in China, enable 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, enable 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 with 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

Samnsung Knox Servers

The device will need access to the Knox servers in order to activate the Knox license for creating the Samsung Knox container on the device.

Americas (USA, Canada, Brazil, etc..)

- 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

Appendix:
OEM Service Kit

Platform OEM Service Overview

The Platform OEM Service is an additional app that allows AirWatch to provide extended management capabilities to Android device.

After you enroll, AirWatch 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 AirWatch Agent 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:

Platform OEM 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

Platform OEM Service Versions

- Bluebird

- Cube

- Getac

- Honeywell

- HP

- Intermec

- Lenovo

- Mediawave

- Panasonic

- Sonim

- Zebra CC5000

Platform OEM Service Version Available on the Google Play Store

- Samsung

- Sony

- LG

- Huawei

- Zebra

- Honeywell

Install the Platform OEM Service

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

The workflow for installing the Platform OEM Service is as follows:

1. Download the appropriate Platform OEM Service from AirWatch Resources.

2. Enroll the Android device into the AirWatch Console.

3. Either sideload the Platform OEM Service onto the device or configure it to push as an internal application from the AirWatch Console.

4. If you push the Platform OEM Service as an internal app, users are prompted to install it.

The example below shows how to run the AirWatch Samsung Service for Android devices.
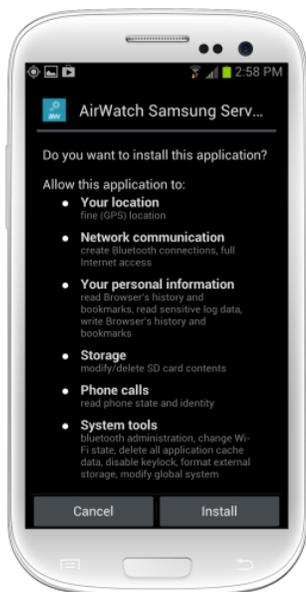
After installing the Agent, you are automatically prompted to begin installing the service app. Select **Install**, when prompted.
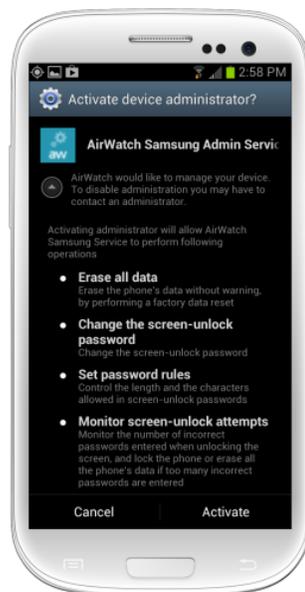
Once it installs, you are prompted to activate the device administrator. Select **Activate**.

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

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

> **Important:** In order to install the Samsung Service App, enable **Push Service App from Play Store** in the AirWatch Console under **Devices > Device Settings > Android > Service ApplicationsService 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 AirWatch 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
v1.0	- Silent App installation, uninstallation, and updates. - Silent Device Administrator Activation on launch. - Silent Device Administrator of Agent 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
v2.0	- 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
v3.0	- OS Upgrade - Enable/Disable SD Card

Version	Features
v3.2	• Send full device logs via Agent menu • Migration from Legacy Rugged Service • Allow SD card
v3.3	• Collect a rolling system log • Enabled Notification access for AirWatch Launcher

Honeywell Service Supported Features

Feature	Description	Supported Version
Enrollment		
Barcode Enrollment	Create barcode using EZ Config, device scans barcode to download agent and enroll.	1.0
Sideload Staging	Create sideload package manually, run batch file to install agent and enroll.	1.0
Client SDK Enrollment	Auto enrollment supported via Client SDK API. Agent and Service are silently activated and enrolled	1.0
Persistence	Agent and enrollment is persisted through an enterprise reset.	1.1
Security		
Silent Device Administrator Activation	Ability to activate the Agent and Service as device admin without user prompt.	1.0
Silently Set Default Launcher	Ability to set the default launcher without user prompt.	2.0
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

Feature	Description	Supported Version
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
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
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 AirWatch Agent and enrollment will be persisted.	1.1
Factory Reset	Send a Factory Reset from the Console and AirWatch Agent 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

Feature	Description	Supported Version
MDM Agent Upgrade	Upgrade the Agent 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
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

Feature	Description	Version
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 AirWatch Agent	View app logs inside the AirWatch and push them to the console or email the logs.	v1.3
Request Device Log Commands	Enable to request device log commands.	v1.3

Accessing Other Documents

While reading this documentation you may encounter references to documents that are not included here.

The quickest and easiest way to find a particular document is to navigate to https://my.air-watch.com/help/9.2/en/Content/Release_Notes/Doc_List_PDFs.htm and search for the document you need. Each release-specific document has a link to its PDF copy on AirWatch Resources.

Alternatively, you can navigate to AirWatch Resources on myAirWatch (resources.air-watch.com) and search. When searching for documentation on Resources, be sure to select your AirWatch version. You can use the filters to sort by PDF file type and AirWatch v9.3.