



THE CLOUD STRATEGY COMPANY™

Mobile Device Management (MDM)

Administrator Quick Reference Guide

Contents

Overview	3
Login.....	3
Main Menu.....	3
Supported Devices	4
Creating Administrative Users	4
Email enrollment setup.....	5
Adding Users and Devices	5
Apple Push Notification Service (APNs) for MDM	5
Manually Adding Users	6
Batch Import	6
Enrollment	7
The Device List View	7
GPS tracking	9
iOS	9
Android	10
Managing devices with Profiles: Restricting the camera on iOS devices	11
Profile example: Restricting the camera on iOS devices	11
Updating Profiles: The Add Version feature	12
Enterprise Wipe and Device Wipe	13
How to prevent user-initiated Device Wipes.....	14
You can adjust the following restrictions when setting up profiles for iOS and Android. This will prevent users from completely erasing their devices back to factory default.	14
iOS	14
Android	15
Disable admin-initiated Device Wipe for BYOD Devices.....	15
Reports & Analytics.....	17
More features	17
How to whitelist and blacklist apps	17
Additional help.....	17

Overview

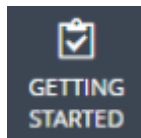
This guide discusses the most common tasks and tools you can use to manage your Workspace ONE MDM environment. For a complete administrator guide discussing all features of AirWatch MDM please see the Additional Help section at the bottom of this document.

Login

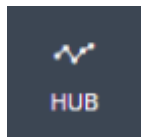
Open your web browser and navigate to <https://cn700.awmdm.com>. Your username and password will be provided by Evolve IP.

Main Menu

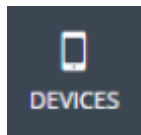
The Main Menu contains all options and features to govern your environment. The following options in the main menu relate to MDM and are relevant to your environment.



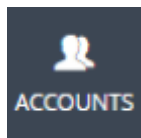
Ensure that all aspects of a basic successful deployment are established. Getting Started is organized to reflect only those modules within an AirWatch Console deployment that you are interested in. Getting Started produces an on-boarding experience that is more tailored to your actual configuration.



Ensure that all aspects of a basic successful deployment are established. Getting Started is organized to reflect only those modules within an AirWatch Console deployment that you are interested in. Getting Started produces an on-boarding experience that is more tailored to your actual configuration.



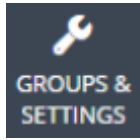
Access an overview of common aspects of devices in your fleet, including compliance status, ownership type breakdown, last seen, platform type, and enrollment type. Swap views according to your own preferences including full Dashboard, list view, and detail view. Access additional tabs, including all current profiles, enrollment status, Notification, Wipe Protection settings, compliance policies, certificates, product provisioning, and printer management.



Survey and manage users and administrators involved with your MDM deployment. Access and manage user groups, roles, batch status, and settings associated with your users. Also, access and manage admin

[Most recent date the document was updated – Initials of the updater]

groups, roles, system activity, and settings associated with your administrators.



Manage structures, types and statuses related to organization groups, smart groups, app groups, user groups, and Admin Groups. Configure entire system settings or access settings related to all **Main Menu**

options.

Supported Devices

MDM supports the following devices and operating systems.

Android 4.0+

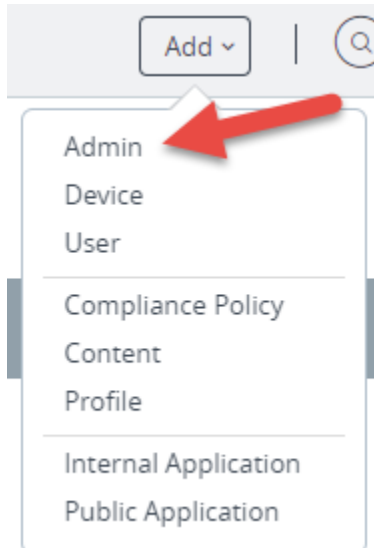
Apple iOS 7.0+

Chrome OS (latest)

Creating Administrative Users

If you wish to add additional administrative users to your organization, you can do so easily by following these instructions.

1. Click the “Add” button near the top-right hand corner of the page, and select **Admin**




2. You will see the Add/Edit Admin window, with Basic, Details, Roles, API, and Notes tabs.
3. Under the Basic tab, set the user to Basic and fill out the rest of the required fields as appropriate.
4. If you wish to set up Two-Factor Authentication Method or Notifications, then click the drop-down arrow next to those respective options and fill out the forms as appropriate.
5. If you wish to fill out the Details tab with more information about the user, you may do so
6. Click the Roles tab.
7. Click the “Select Organization Group” field and select your company name.

8. Click the “Role” field and select the appropriate role. Choose Console Administrator if you want the user to have total administrative capabilities. You can find out more about the additional roles in the Mobile Device Management Guide.
9. Click Save.

Email enrollment setup

During enrollment your users will be asked to authenticate using their email account or with a Server ID. The more user-friendly option is by using their email account. You can add your company’s email domain to MDM to allow this.

1. Go To **Groups & Settings > All Settings > Devices & Users > General > Enrollment**
2. Click the **Add Email Domain** button 
 - a. **Organization Group:** This should be prepopulated with your organization
 - b. **Business email Domain:** Enter in an email address with the email domain that you want to include
 - c. **Confirmation email address:** Retype the email address
 - d. Click **SAVE**

After this is completed your users will be able to enroll their devices using their email address.

Adding Users and Devices

The first thing you will want to do is get your users’ devices enrolled into your MDM environment. The simplest way to add devices is to add the actual user of that device. The user will then receive an email invitation to enroll their device. After the user has followed the steps for enrollment, their device will show in the AirWatch Console.

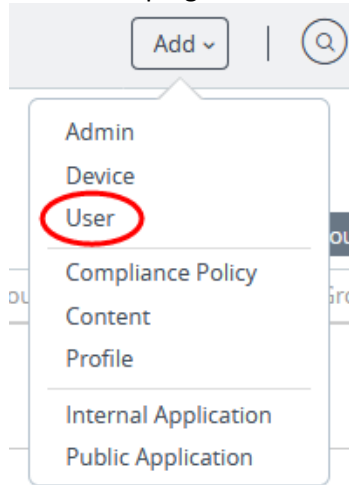
Apple Push Notification Service (APNs) for MDM

If you plan on managing iOS devices, then you will need an Apple Push Notification service (APNs) certificate so that iOS device users can enroll their devices. You will need an Apple ID to obtain this certificate. Please follow these instructions to obtain and install it.

1. Get your [Apple ID](#)
2. In the AirWatch Console, go to **Groups & Settings > All Settings > Devices & Users > Apple > APNs For MDM**
3. Click the blue **Generate New Certificate** button and follow the instructions to complete the process.

Manually Adding Users

1. Near the top right-hand corner of the web page, click the **Add** drop-down menu and choose **User**



2. Under the **General** tab, fill out the following fields with appropriate end user information:
 - a. Username
 - b. Password
 - c. Confirm Password
 - d. Full Name
 - e. Display Name
 - f. E-mail Address
3. Under **General** tab > **Enrollment**:
 - a. Verify the **Enrollment Organization Group** is set correctly
 - b. Set **Allow user to enroll into additional Organization Groups** to "Disabled"
 - c. Set the **User Role** to "Basic Access"
4. Leave **General** tab > **Notification** as is. This will send out an email to the user with instructions to enroll.
5. Click **Save**

Batch Import

1. Navigate to **Accounts > Users > List View**. Then select the **Add** and select **Batch Import**.
2. Enter the basic information including a Batch Name and Batch Description in the AirWatch Console.
3. Select the applicable batch type from the Batch Type drop-down menu.
4. Select and download the template that best matches the kind of batch import you are making.
 - Blacklisted Devices** – Import a list of known, non-compliant devices by IMEI, Serial Number, or UDID. Blacklisted devices are not allowed to enroll. If a blacklisted device attempts to enroll, it is automatically blocked.
 - Whitelisted Devices** – Import pre-approved devices by IMEI, Serial Number, or UDID. Use this import a list of known, trusted devices. The ownership and group ID associated to this device is automatically applied to the device during enrollment.
 - User / Device** – Choose between a Simple and an Advanced CSV template. The simple template features only the most often-used options and the Advanced template features the full, unabridged compliment of options.

5. Open the CSV file, which consists of a CSV (comma-separated values) file that is populated with a single row completed with a sample device data. The CSV file features several columns corresponding to the setting that display on the Add / Edit User page. The **GroupID** column corresponds to the **Enrollment Organization Group** setting on the **Add / Edit** User page.
You can confirm whether or not users are part of the enrollment organization group (OG).
 - a. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment** and check the **Grouping** tab.
 - b. If the **Group ID Assignment Mode** is set to **Default**, then your users are part of the enrollment OG.
 - c. For a directory-based enrollment, the **Security Type** for each user must be **Directory**.
6. Enter data for your organization's users, including device information (if applicable) and save the file.
7. Return to the Batch Import page and select **Choose File** to locate and upload the CSV file that you had previously downloaded and filled out.
8. Select **Save**

Enrollment

After adding users in the AirWatch Console, users will receive an email that invites them to enroll their device. The link will direct them to download and install steps specific to their devices. For example, if the user has an Android or Chromebook device, the link will direct users to the Google Play store. If the user has an iOS device, it will direct them to the Apple App Store. After following the steps for enrolling, an AirWatch agent application will be installed on their device as well as a Profile.

Android users may also receive a notification to install com.airwatch.rm.agent. This additional agent allows administrators to remotely control these devices via the Remote Management feature. You may direct your end-users to Skip or Install this agent. Please note that Remote Management is a feature that Evolve IP does not support.

The Device List View

Once enrolled, your users' devices will show in the Device List View. To see this list, go to **Devices > List View**. From this list you can view your entire device fleet, drill down on device names to see their details, launch Remote Management sessions for supported devices, add Tags, and more. You can also filter this list by various criteria.

AirWatch Console EvolveIP, LLC (MSP) - CN700 Add

HUB

DEVICES

ACCOUNTS

APPS & BOOKS

CONTENT

EMAIL

TELECOM

GROUPS & SETTINGS

Dashboard

List View

Details View

> Lifecycle

> Profiles & Resources

> Compliance Policies

> Certificates

> Staging & Provisioning

> Peripherals

Devices Settings

Devices >

List View

Filters + Add Device

		Last Seen ...	General Info	Platform
<input type="checkbox"/>		15m	Chrome Book-33298cbe42330e299d60be648fb354f9 EvolveIP, LLC (MSP) - CN700 / EvolveIP Internal MDM Undefined	Chrome OS (Legacy) Intel(R) Celeron(R) CPU N2830 @ 2.16GHz 55.0.2883
<input type="checkbox"/>		38m	Everett's iPhone EvolveIP, LLC (MSP) - CN700 / EvolveIP Internal MDM Undefined	Apple iOS iPhone 6 Plus 11.0.3
<input type="checkbox"/>		43m	EIP-BFREILEY EvolveIP, LLC (MSP) - CN700 / EvolveIP Internal MDM Undefined	Windows Desktop Latitude E5450 10.0.15063
<input type="checkbox"/>		50m	EVERETT-LAPTOP EvolveIP, LLC (MSP) - CN700 / EvolveIP Internal MDM Undefined	Windows Desktop 423946U 10.0.10586
<input type="checkbox"/>		9d	Chrome Book-6305d761b6180aa456a4b3e8b6e87c76 EvolveIP, LLC (MSP) - CN700 / EvolveIP Internal MDM Corporate - Dedicated	Chrome OS (Legacy) Intel(R) Celeron(R) 2955U @ 1.40GHz 59.0.3071
<input type="checkbox"/>		13d	Android_ASUS_Z00XS_359404065504582 EvolveIP, LLC (MSP) - CN700 / EvolveIP Internal MDM Undefined	Android asus ASUS_Z00XS 6.0.1

GPS tracking

GPS settings need to be set up in multiple areas of the MDM console in order for GPS tracking to work properly.

1. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Privacy**
2. Set **Current Setting** to **Override**
3. Here you will see the **GPS Data** feature. By default, **Corporate Dedicated** and **Corporate – Shared** are set to “Collect and Display”. If you wish to apply GPS tracking to Employee Owned and Unassigned devices too, then set them to “Collect and Display” as well.

The screenshot shows the 'Privacy' settings page in the MDM console. The breadcrumb trail is 'Devices & Users > General > Privacy'. The 'Current Setting' is set to 'Override'. Below this, there are three radio button options: 'Collect and Display', 'Collect Do Not Display', and 'Do Not Collect'. The 'Collect and Display' option is selected. Below these options, there are four columns representing device types: 'Corporate - Dedicated', 'Corporate - Shared', 'Employee Owned', and 'Unassigned'. Under the 'GPS Data' row, there are radio buttons for each device type. Red arrows point to the 'Collect and Display' radio buttons for 'Employee Owned' and 'Unassigned' device types.

4. Click **Save** (at the bottom of the page).

You will also need to enable “Collect Location Data” on both iOS and Android devices.

iOS

Go to **Apple/Apple iOS/Agent Settings** and you will see **Collect Location Data** checkbox. Checkmark the box to enable the feature.

System

Devices & Users

- General
- Android
- Apple
 - APNs For MDM
 - Apple iOS
 - APNs For Applications
 - Agent Settings
 - Managed Settings
 - Apple macOS
 - AppleCare
 - Automated Enrollment
 - Device Enrollment Program
 - SCEP
 - Install Fonts
 - Education
 - VPP Managed Distribution
 - BlackBerry
 - QNX
 - Tizen
 - Chrome OS
 - Windows
 - Peripherals
 - Advanced

- Apps
- Content
- Email
- Telecom
- Admin

Devices & Users > Apple > Apple iOS > Agent Settings

General Notification

Current Setting Inherit Override

General

Disable Unenroll Option in Agent

Background App Refresh

Area

Collect Location Data ⓘ

Detect iBeacon Area ⓘ

Telecom

Collect Cellular Data Usage

Self Service Setting

Self Service Enabled ⓘ

SDK Profile

SDK Profile (Legacy)

SDK Profile V2

Child Permission* Inherit only Override only Inherit or Override

Android

Go to **Android > Agent Settings** and you will see **Collect Location Data**. Choose “Enabled.”

Settings

EvolveIP, LLC (MSP) - CN700 / E...

System

Devices & Users

- General
- Android
 - Agent Settings
 - Auto-Enrollment
 - Google Play Integration
 - Android for Work
 - Service Applications
 - Security
 - Samsung Enterprise FOTA
- Apple

Location

Collect Location Data Enabled Disabled

Force GPS On Enabled Disabled

GPS Time Poll Interval (min)*

After enabling these GPS features the user will get a request for authorization to collect location information. If the user authorizes this, GPS tracking for that device will begin working and will show under the device’s Location tab.

Managing devices with Profiles: Restricting the camera on iOS devices

After enrollment, your users' devices will be managed by a default device profile. This initial profile imposes no restrictions on devices. If you wish to apply restrictions to your device fleet, you can do so with **Profiles**.

Here is a brief list of features and applications you can restrict or govern:

Camera	Device and Enterprise Wipes
Screen capture	Multiplayer gaming
iMessage	Safari
In-app purchases	Keychain sync
AirDrop	Movies based of rating type
YouTube	Apps based of age

Profile example: Restricting the camera on iOS devices

The below example shows how to restrict the use of the camera on iOS devices using a custom Profile.

1. Go to **Devices > Profiles & Resources > Profiles**
2. Click the **Add** drop-down menu and select **Add Profile**
3. Choose **iOS**
4. The **General** payload form will show. Please fill it out as per the below screenshot.

iOS Add a New Apple iOS Profile

General

Passcode

Restrictions

Wi-Fi

VPN

Email

Exchange ActiveSync

Notifications

LDAP

CalDAV

Subscribed Calendars

CardDAV

Web Clips

Credentials

SCEP

Global HTTP Proxy

Single App Mode

Content Filter

Managed Domains

Network Usage Rules

macOS Server Accounts

Single Sign-On

AirPlay Mirroring

General

Name * Disable iOS Device cameras

Version 1

Description This profile disables cameras on all iOS devices

Deployment Managed

Assignment Type Auto

Allow Removal Always

Managed By Your company should show here by default

Assigned Groups All Devices ()

Exclusions No Yes

Additional Assignment Criteria

Install only on devices inside selected areas ⓘ

Enable Scheduling and install only during selected time periods

Removal Date M/D/YYYY

Save & Publish Cancel

You'll need to click this field and choose this option. Your company name should show in paranthesis

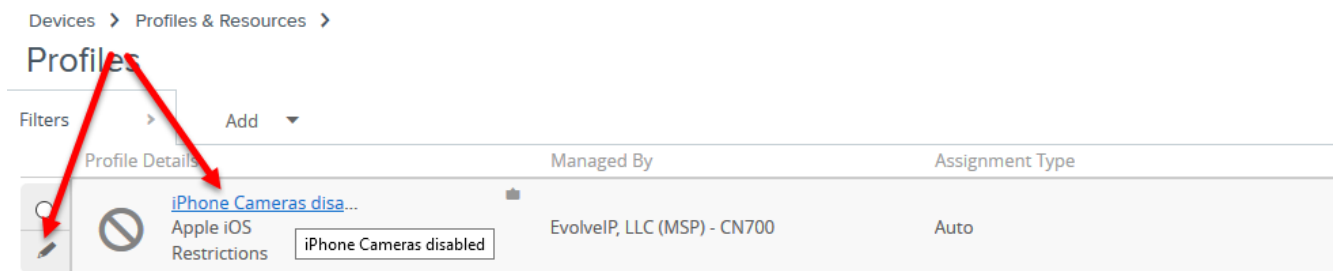
5. Click the **Restrictions** option on the left of the screen, and then the **Configure** button. You will see a long list of functions and features that you can manage. The first option should be “Allow use of camera.”
6. Uncheck the box next to “Allow use of camera” and click the **Save & Publish** button.
7. The “View Device Assignment” window will show, listing all the iOS devices in your fleet that will be affected by this change. Click the **Publish** button.
8. The **Profiles** screen will now show with the Profile that you just created.

This new Profile should push almost immediately to iOS devices in your fleet that are enrolled and active with an internet connection. They will push to inactive, enrolled iOS devices the next time they are on the internet.

Updating Profiles: The Add Version feature

This section discusses how to make changes to your custom Profiles. AirWatch uses versioning to track changes to profiles, so updating profiles uses a feature called **Add Version**.

1. Click the edit icon next to the profile that you want to update. You can also simply click on the Profile name.



2. Click the **Add Version** button. **Note: After clicking, this button will be replaced by the **Save & Publish** button. Do not click it just yet.*
3. Make your changes and then click **Save & Publish**.

Your changes should push almost immediately to iOS devices in your fleet that are enrolled and active with an internet connection. They will push to inactive, enrolled iOS devices the next time they are on the internet.

Enterprise Wipe and Device Wipe

This section discusses the differences between Device and Enterprise Wipe as well as preventative measures you can take to protect against accidental wipes initiated by employees and admins.

Enterprise Wipe: This will wipe a device of all company-related information and the AirWatch agent. The types of data that is removed are configured within the AirWatch Console.

Device Wipe: A Device Wipe completely wipes a device and sets it back to default as if you pulled the device new out of its box.

Both options are available under **More Actions > Management** in the Device Profile page.

The screenshot displays the AirWatch console interface for a device profile. At the top, the organization is identified as 'EvolveIP, LLC (MSP) - CN700'. The device is 'Everett's Android Asus tablet' (asus P01Z, 5.0.2, Corporate - Dedicated). The 'More Actions' menu is open, showing options like 'Clear Passcode', 'Device', 'Generate App Token', 'Management', 'Change Device Passcode', 'Enterprise Wipe', and 'Device Wipe'. The 'Enterprise Wipe' and 'Device Wipe' options are circled in red. Below the menu, the device status is shown as 'DEVICE IS NOT COMPROMISED', '0 COMPLIANCE VIOLATIONS', 'ENROLLED 3/27/2018', and 'LAST SEEN 27 MINUTE(S) AGO'. The 'Security' section shows 'Managed By MDM', 'Encryption Compliance', and 'Internal Storage Encryption'. The 'User Info' section shows 'USER NAME ecavazos' and 'NAME Everett Cavazos'. The 'ENTERPRISE VERSION' is 'Not Applicable' and the 'ORGANIZATION GROUP' is 'EvolveIP, LLC (MSP) - CN700 / EvolveIP Inte'.

How to prevent user-initiated Device Wipes

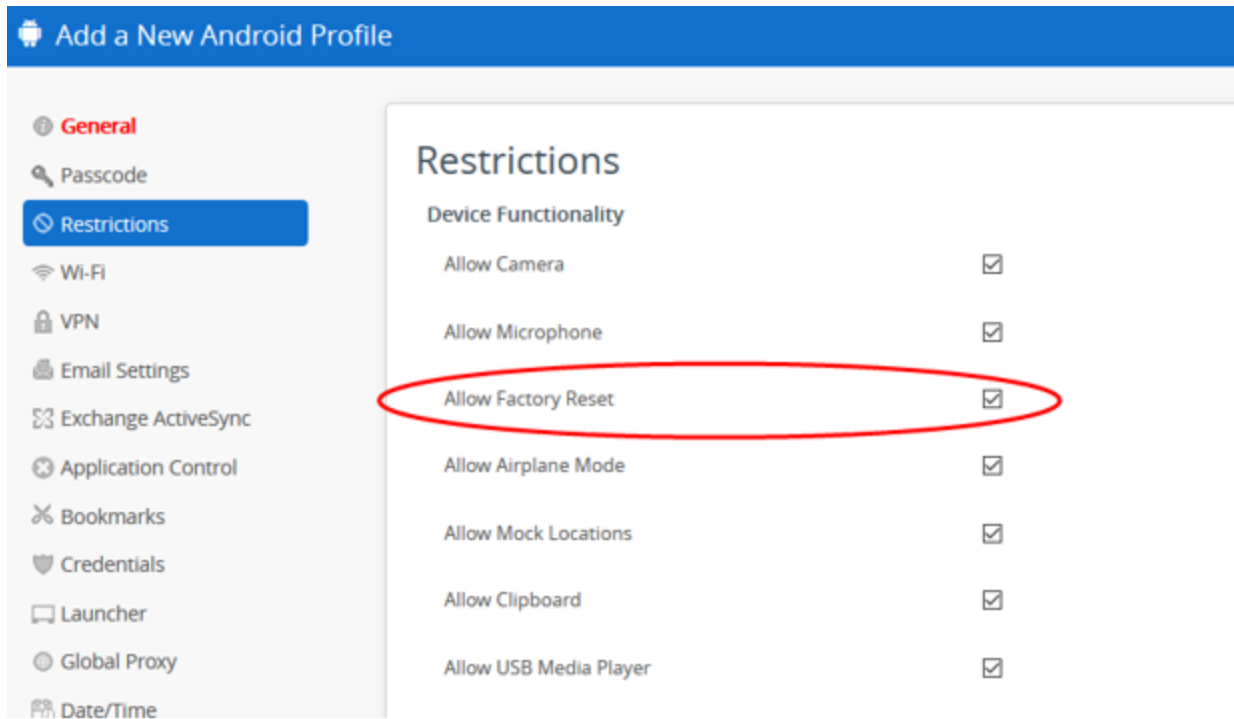
You can adjust the following restrictions when setting up profiles for iOS and Android. This will prevent users from completely erasing their devices back to factory default.

iOS

The screenshot shows the 'Add a New Apple iOS Profile' configuration page. The left sidebar lists various settings categories, with 'Restrictions' selected. The main content area displays a list of restrictions, each with a checkbox. The 'Allow Erase All Contents and Settings' option is highlighted with a blue bar and circled in red, indicating it is selected. Other restrictions include 'Allow internet results in Spotlight', 'Allow Siri', 'Allow Siri while device locked', 'Enable Siri Profanity Filter', 'Show user-generated content in Siri', 'Allow manual profile installation', 'Allow configuring Restrictions', 'Allow device name modification', 'Allow wallpaper modification', 'Allow account modification', 'Require passcode on first AirPlay pairing', and 'Allow Wallet notifications in Lock screen'.

Restriction	Status
Allow internet results in Spotlight	<input checked="" type="checkbox"/>
Allow Siri	<input checked="" type="checkbox"/>
Allow Siri while device locked	<input checked="" type="checkbox"/>
Enable Siri Profanity Filter	<input type="checkbox"/>
Show user-generated content in Siri	<input checked="" type="checkbox"/>
Allow manual profile installation	<input checked="" type="checkbox"/>
Allow configuring Restrictions	<input checked="" type="checkbox"/>
Allow Erase All Contents and Settings	<input checked="" type="checkbox"/>
Allow device name modification	<input checked="" type="checkbox"/>
Allow wallpaper modification	<input checked="" type="checkbox"/>
Allow account modification	<input checked="" type="checkbox"/>
Require passcode on first AirPlay pairing	<input type="checkbox"/>
Allow Wallet notifications in Lock screen	<input checked="" type="checkbox"/>
Show Control Center in Lock screen	<input type="checkbox"/>

Android



Disable admin-initiated Device Wipe for BYOD Devices

Please follow these instructions if you wish to prevent other MDM Administrators from performing device wipes on BYOD Devices. This will remove the “Device Wipe” option from the **More Actions** menu located in devices’ profile screens.

1. Navigate to **Devices > Device Settings > Devices & Users > General > Privacy**.
2. Scroll down to the **Commands** section and find the **Employee Owned** column.
3. Set the **Device Wipe** option to **Prevent** and select **Save**.

System	Corporate - Dedicated	Corporate - Shared	Employee Owned
Devices & Users			
General			
Enrollment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Friendly Name			
Lookup Fields			
Message Templates			
Notifications			
Privacy			
Passwords			
Shared Device			
Advanced			
▶ Android			
▶ Apple			
▶ BlackBerry			
Commands			
Device Wipe	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Clear Device Passcode / Lock Device	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
File Manager Access *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Remote Control *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

The **Device Wipe** command will be removed from the **More Actions** menu as per this screenshot.

Device Wipe option removed

QUERY	SEND	MORE ACTIONS
		Clear Passcode Generate App Token
		Management Enterprise Wipe
		Support Find Device App Remote View Sync Device
		Admin Change Organization Group Add Tag Edit Device Delete Device Request Debug Log Override Job Log Level

Reports & Analytics

AirWatch has extensive reporting and event logging capabilities that provide administrators with actionable, result-driven statistics about device fleets. You can use these pre-defined reports or create custom reports based on specific devices, user groups, date ranges, or file preferences. Reports can be viewed by navigating to the Reports page at **Hub > Reports & Analytics > Reports > List View**. Added reports are accessible from the My Reports tab at the top of the Reports page for quick access.

Some examples of reports are:

Admin Login History	Content Details by Device	Count of Active Devices
Device Battery Log	Device Inventory	Device Wipe Log
Devices with User Details	Profile Configuration Details	Profile Details by Device

More features

How to whitelist and blacklist apps

Apps & Books > Applications > Application Settings > App Groups > Add Group

Additional help

For a comprehensive guide to all MDM features please see the VMware AirWatch Mobile Device Management Guide:

<https://resources.air-watch.com/view/4mrhbs2b7kygc2b5fkph/en>