



THE CLOUD STRATEGY COMPANY™

# **Mobile Device Management (MDM)**

---

Administrator Quick Reference Guide

## Contents

Overview.....	3
Login .....	3
Main Menu.....	3
Supported Devices.....	4
Adding Users and Devices.....	4
Apple Push Notification Service (APNs) for MDM.....	4
Manually Adding Users.....	5
Batch Import .....	5
Enrollment .....	6
The Device List View.....	6
Managing devices with Profiles: Restricting the camera on iOS devices .....	7
Create a Profile: Restricting the camera on iOS devices.....	9
Updating Profiles: The Add Version feature .....	10
Additional help.....	11

## 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.

- 


GETTING  
STARTED

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.
- 


HUB

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.
- 

DEVICES

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 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.
- 

ACCOUNTS

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

GROUPS &  
SETTINGS

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 options.

### Main Menu

## Supported Devices

MDM supports the following devices and operating systems.

Android 4.0+	Tizen 2.3+
Apple iOS 7.0+	Windows Desktop (8/8.1/RT/10)
Apple macOS 10.9+	Windows 7 (Windows 7 or higher)
Chrome OS (latest)	Windows Phone (Windows Phone 8/8.1, Windows 10 Mobile)
QNX 6.5+	Windows Rugged (Mobile 5/6 and Windows CE 4/5/6)

## 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.

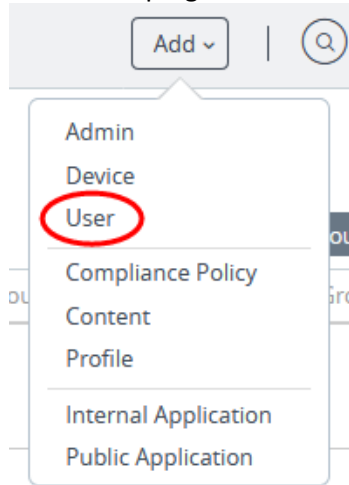
### Apple Push Notification Service (APNs) for MDM

If you plan on managing iOS devices, then you will need an Apple Push Notification service (APNs) certificate in order for iOS device users to 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. Under **General** tab > **Notification**
5. Click **Save**

## Batch Import

1. Navigate to **Accounts > Users > Batch Status or Devices > Lifecycle > Enrollment Status > 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 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.

Please see our “Workspace ONE MDM Enrollment – End-user guide” for instructions on how end-users can enroll their devices.

## 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, and more. You can also filter this list by various criteria.

AirWatch Console EvolveIP, LLC (MSP) - CN700 Add

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
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
38m	Everett's iPhone EvolveIP, LLC (MSP) - CN700 / EvolveIP Internal MDM   Undefined	Apple iOS iPhone 6 Plus 11.0.3
43m	EIP-BFREILEY EvolveIP, LLC (MSP) - CN700 / EvolveIP Internal MDM   Undefined	Windows Desktop Latitude E5450 10.0.15063
50m	EVERETT-LAPTOP EvolveIP, LLC (MSP) - CN700 / EvolveIP Internal MDM   Undefined	Windows Desktop 423946U 10.0.10586
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
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.

Settings EvolveIP, LLC (MSP) - CN700

System  
Devices & Users  
General  
Enrollment  
Friendly Name  
Lookup Fields  
Message Templates  
Notifications  
Privacy  
Passwords  
Shared Device  
Advanced  
Android  
Apple  
BlackBerry  
QNX

Devices & Users > General > Privacy

Current Setting  Inherit  Override

Collect and Display  Collect Do Not Display  Do Not Collect

Corporate - Dedicated Corporate - Shared Employee Owned Unassigned

GPS

GPS Data

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.

The screenshot shows the 'Agent Settings' page for Apple iOS. The left sidebar contains a navigation menu with 'Agent Settings' selected. The main content area shows the 'General' tab with various settings. The 'Collect Location Data' checkbox is checked and circled in red. Other settings include 'Disable Unenroll Option in Agent', 'Background App Refresh', 'Detect iBeacon Area', 'Collect Cellular Data Usage', and 'Self Service Setting'. The 'Child Permission\*' section at the bottom has radio buttons for 'Inherit only', 'Override only', and 'Inherit or Override'.

## Android

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

The screenshot shows the 'Settings' page for EvolveIP, LLC (MSP) - CN700 / E... The left sidebar contains a navigation menu with 'Agent Settings' selected. The main content area shows the 'Location' section with three settings: 'Collect Location Data' (set to 'Enabled' and circled in red), 'Force GPS On' (set to 'Disabled'), and 'GPS Time Poll Interval (min)\*' (set to '60').



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**

- The **General** payload form will show. Please fill it out as per the below screenshot.

The screenshot shows the 'Add a New Apple iOS Profile' form in the MDM console. The 'General' tab is selected, and the form is filled out as follows:

- 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:** (Empty field, with a callout box indicating that the company name should be shown in parentheses)
- Assigned Groups:** All Devices (Selected group, with a callout box indicating that the company name should be shown in parentheses)
- Exclusions:** No
- Additional Assignment Criteria:**
  - Install only on devices inside selected areas
  - Enable Scheduling and install only during selected time periods
- Removal Date:** M/D/YYYY

At the bottom of the form, there are buttons for 'Save & Publish' and 'Cancel'.

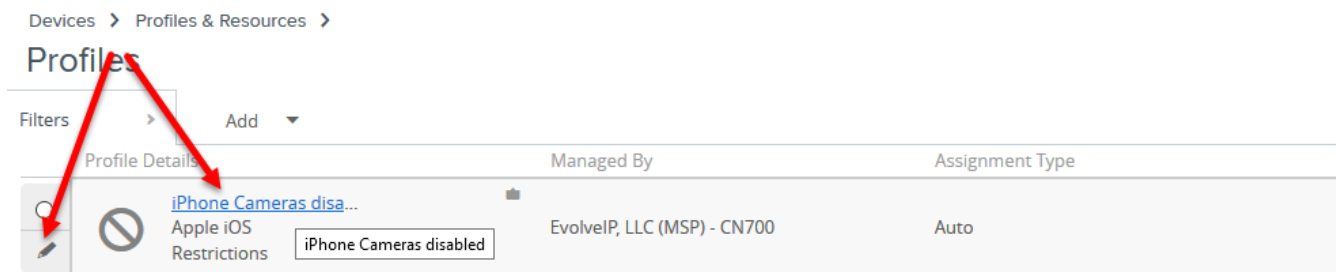
- Click the **Restrictions** option on the left of the screen, and then the **Configure** button. You will see a long list of functions and features that you can manage. The first option should be “Allow use of camera.”
- Uncheck the box next to “Allow use of camera” and click the **Save & Publish** button.
- 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.
- 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 is configured within the AirWatch Console.

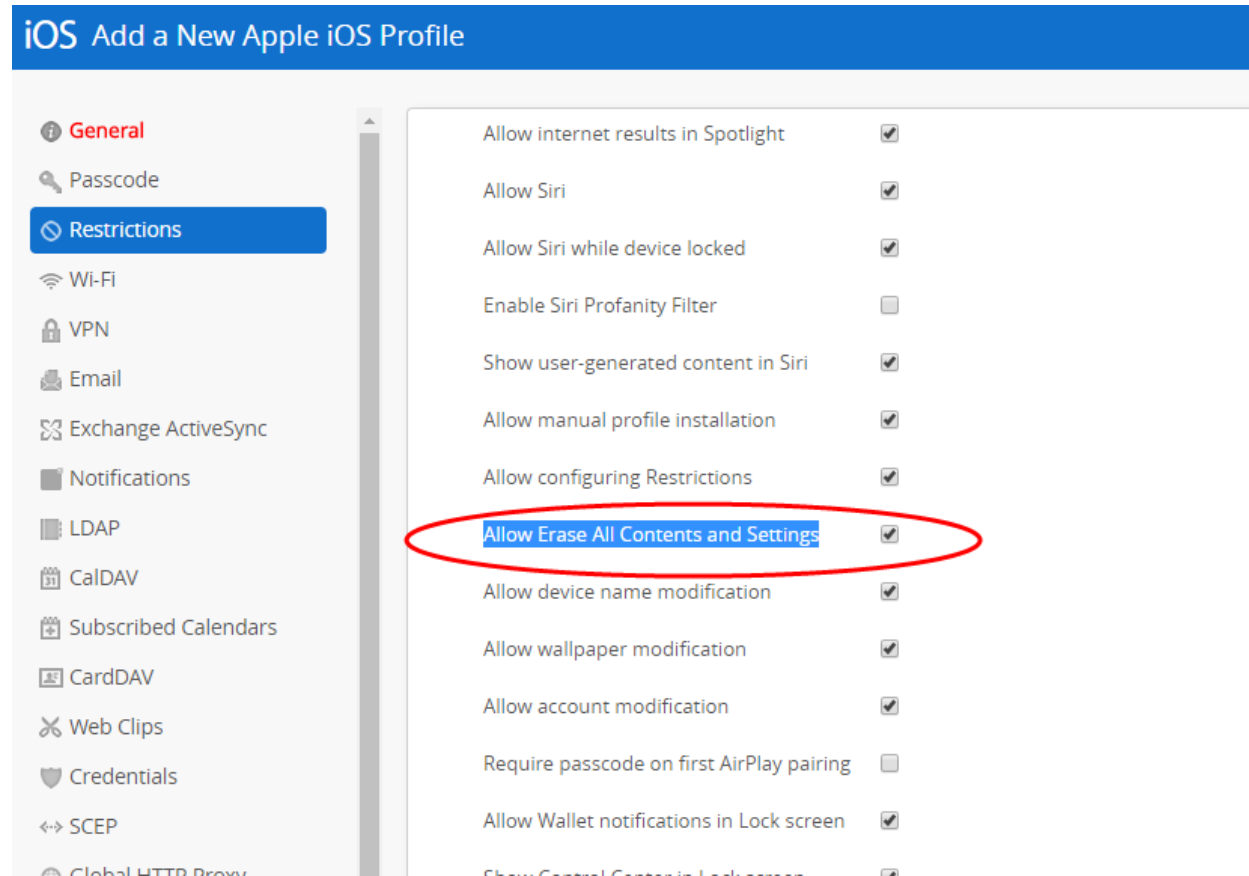
**Device Wipe:** A Device Wipe completely wipes a device and sets it back to default as if you pulled the device new out of its box.

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

## 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



**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

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"/>
<b>Allow Erase All Contents and Settings</b>	<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

Add a New Android Profile

- i General
- 🔑 Passcode
- 🔒 Restrictions
- 📶 Wi-Fi
- 🔒 VPN
- ✉️ Email Settings
- 🔄 Exchange ActiveSync
- ⊗ Application Control
- ✂️ Bookmarks
- 🔒 Credentials
- 📄 Launcher
- 🌐 Global Proxy
- 🕒 Date/Time

## Restrictions

### Device Functionality


- Allow Camera
- Allow Microphone
- Allow Factory Reset
- Allow Airplane Mode
- Allow Mock Locations
- Allow Clipboard
- Allow USB Media Player

### 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
<b>Devices &amp; Users</b>			
<b>Commands</b>			
Device Wipe	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Clear Device Passcode / Lock Device	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
File Manager Access *	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Remote Control *	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>



## 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>