EVOLVE IP

THE CLOUD STRATEGY COMPANY™

# Workspace ONE MDM

## Administrator Quick Reference Guide

## Contents



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

## Overview

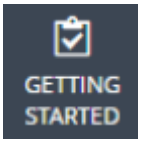
This guide discusses the most common tasks and tools you can use to manage your Workspace ONE MDM environment.

## Login

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

## Main Menu

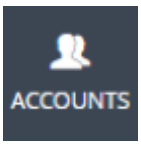
The Main Menu contains all options and features to govern your environment. The following options in the main menu relate to MDM and are relevant to your environment.



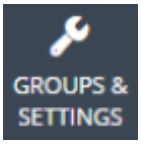

Ensure that all aspects of a basic successful deployment are established. Getting Started is organized to reflect only those modules within an AirWatch Console deployment that you are interested in. Getting Started produces an on-boarding experience that is more tailored to your actual configuration.


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
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.

## 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.

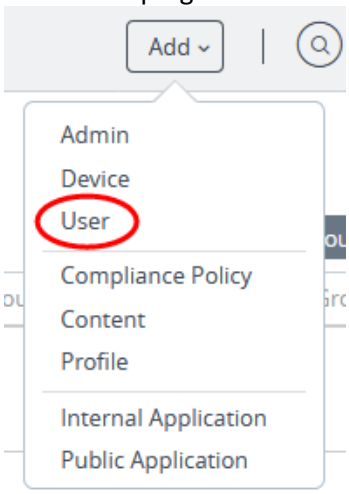
### Apple Push Notification Service (APNs) for MDM

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**

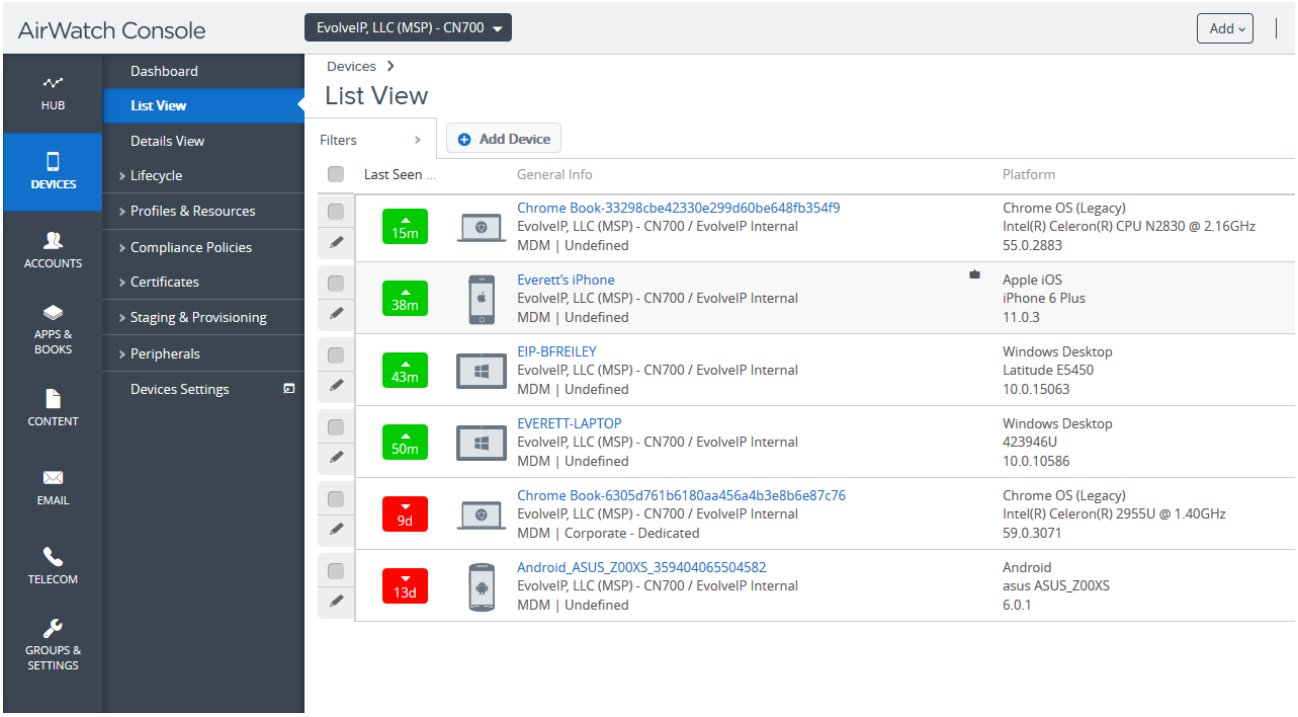
## Enrollment

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 specifc 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.




## Managing devices with Profiles: Restricting the camera on iOS devices

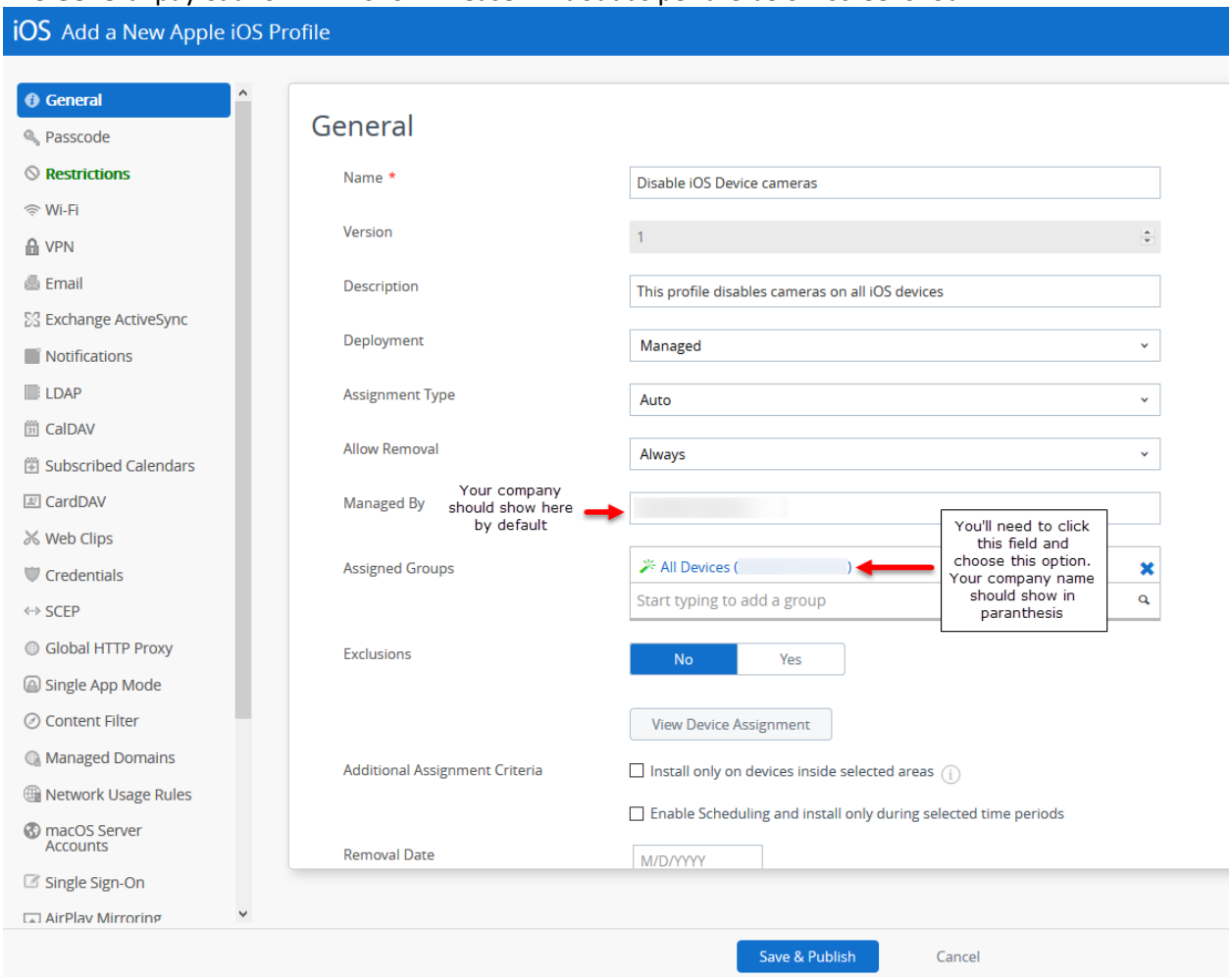
After enrollment, your users' devices will be managed by a default device profile. This initial profile imposes no restrictions on devices. If you wish to apply restrictions to your device fleet, you can do so with **Profiles**.

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

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

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.



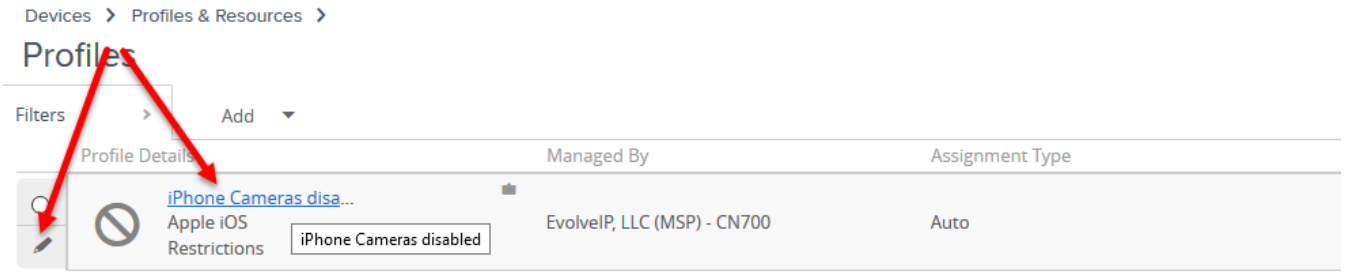

5. Click the **Restrictions** option on the left of the screen, and then the **Configure** button. You will see a long list of functions and features that you can manage. The first option should be "Allow use of camera."
6. Uncheck the box next to "Allow use of camera" and click the **Save & Publish** 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.

## Remote Management

You can use the Remote Management feature to view and control your users' devices to provide troubleshooting assistance.

### Supported Devices

**Android devices with AirWatch Agent v5.3.1+**

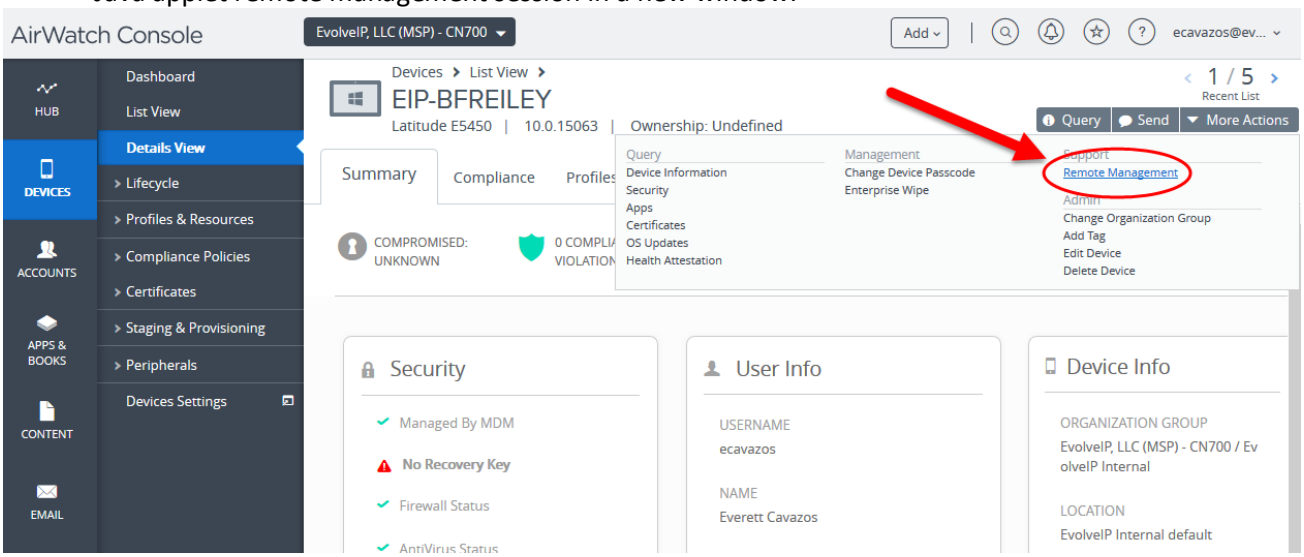
- Motorola/Zebra MX 1.3+ devices.
- Samsung with SAFE 4+.
- Panasonic.
- Honeywell.
- Kyocera.

**Additional devices**

- macOS with AirWatch Agent v2.2+.
- QNX.
- Windows Mobile/CE.
- Windows Desktop.
- Windows 7 with AirWatch Agent v7.2.0+.

If you have one of the above devices in your fleet then you should have a **Remote Management** option in the **Device View**.

1. Go to **Devices > List View**
2. Click on the device name that you want to remote to
3. Click on the **More Actions** drop-down menu and click **Remote Management**. This should initiate a Java applet remote management session in a new window.




### The Android Remote Management v3.0 Viewer

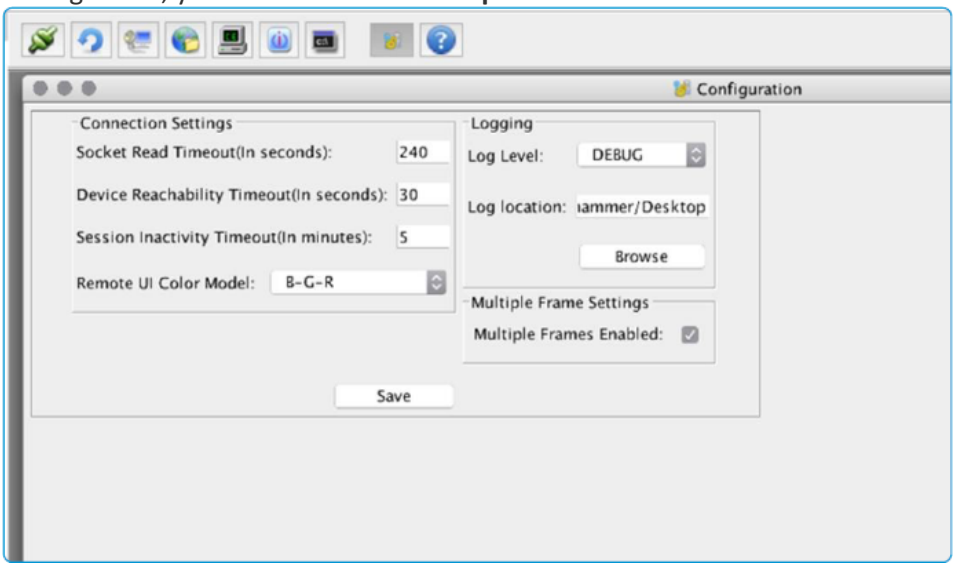
To manage Android devices remotely, start the remote management viewer Java applet. The viewer contains various
functions to control and manage Android devices.
To use Remote Management.

1. Navigate to **Devices > List View** and select the device you want to manage.
2. On the **Device Details View**, select the **More** option ( ) to display an expanded list of management options.
3. Select **Remote Management**. A new window opens listing the device details and showing the Remote Management window.

4. Use the Remote Management window to accomplish the tasks you want.
    - **Connection** – Shows the connection settings used to communicate with the device.
    - **Retry** – Attempts to connect with the device again.
    - **Screen Share** – Displays the device's screen so you can remotely view and control the device screen and receive any actions performed by the device user. The **Screen Share**toolbar also allows you to adjust the view depth and size. The toolbar also allows you to capture and save screenshots and videos to your computer. You can also record sequences of actions as

macros that can be used again later.


- **File Manager** – Displays the device file system so you can remotely manage by viewing, creating, copying, moving, and deleting files and directories. Files and directories can also be dragged and dropped between the file system on the device and the remote control admin's machine.
- **Task Manager** – Displays a list of the processes currently running on the device. Stop or kill a process by selecting the process from the list. You can also start an executable on the device by entering the full path and any parameters to be passed.
- **Applications** – Displays a list of any applications currently managed by the OS on the device. Uninstall a managed application by right-clicking on the listed application. You may also load a managed application from your local machine and install it to a specified directory on a device.
- **Command Prompt** – Displays the command prompt. For a full list of supported commands and details, type 'help' into the command prompt and press enter.
- **Applet Display and Log Settings** – Allows you to configure and save the settings for the remote management applet and the log.
    - If you want to see multiple frames at the same time while using remote management, you must select the **Multiple Frames Enabled** check box.




- **About** – Displays the version information about the remote management applet in use.

To disconnect from your Remote Management session click the **Cancel** button at the bottom of the applet window.

For Remote Management guidance on additional supported devices please consult the **Evolve IP Remote Management Guide**.

For guidance on all features of Workspace ONE MDM please consult the **Evolve IP Workspace ONE Mobile Device Management Guide**.

## Additional help

For a comprehensive guide to all MDM features please see the Evolve IP Mobile Device Management Guide.