Mobile Device Management Guide

Managing your organization's mobile devices

AirWatch v8.0

Table of Contents

What's New

This guide has been updated with the latest features and functionality from the most recent release of AirWatch, AirWatch v8.0. The list below includes these new features and the sections and pages on which they appear.

- The Getting Started wizard has been redesigned to better reflect the purchased SKUs within an AirWatch Admin Console deployment. This produces an onboarding experience that feels more tailored to your actual AW configuration. The location of the Getting Started button has also been moved to the main menu. See Using the Getting Started Wizard on page 14.
- A new selection has been added in the Admin Console's Hub called Admin Panel, which contains a summary of AirWatch licenses (MDM, AirWatch Container, App Categories, Inbox, App Wrapping, App Reputation Scanning, Browser, Content Locker, etc.) condensed into two separate sections, Active Products and Deployed Components. See Using the Admin Panel Dashboard on page 134.
- A new design has been introduced to the Users List View that combines Action Menu availability with selecting devices in bulk, making the steps for applying and affecting Actions and other changes to multiple (bulk) devices the same as those used to change a single device. See Managing User Accounts on page 57.
- A new Bulk Import template choice is available under the Batch Type 'Users And/Or Devices.' Select the information icon to access the help topic which contains links to both the new template (Simple) and the old template (Advanced). See Using the Batch Import Feature on page 58.
- The Self-Service Portal has been enhanced with several new features including a Change button on the password field allowing users to change their own password and an easy way to change the Friendly Name of a device. See Using the My Devices Page of the SSP on page 138.
- You may now select an Initial Landing Page for the Self Service Portal on new User Roles. Existing User Roles will get the default Initial Landing Page of My Devices, although this can be edited as well. See Defining User Roles on page 56.
- You may now require the addition of a note when an admin decides to implement a Lock SSO (single sign on) on a device. See Configuring Restricted Actions on page 32.
- Usability improvements have been implemented to the OG Comparison tool, including the insertion of column labels, automatically highlighted differences, and empty setting labels. See Comparing Organization Groups Using Settings Comparison on page 39.
- Global Search has been made much faster by implementing a tabbed interface. See Using the Global Search on page 18.
- You will now be notified when any of your Apple Push Notification Service (APNs) certificates are in jeopardy of expiring with the new Notifications section, located next to Global Search in the console header. See Viewing Notifications on page 19
- During those cases in which profiles do not install on targeted devices, the View Devices screen enables you to see the specific reason why. You can also export the entire View Devices page to a .csv file (comma-separated values) which you can analyze using Excel. See Profile Installation Logging and Reporting with View Devices on page 95.

- The Device List View has been enhanced with a Custom view option which you can use to modify which columns you want to see. New columns are available as well: Tags and Wi-Fi MAC Address. Additionally, a new filter has been added, User Groups. See Using the Device List View on page 117
- A new tool has been introduced, the Admin Role Comparison Tool, which can be used to audit and analyze all your Admin Roles and make changes where necessary. See Comparing Admin Roles on page 75
- Several improvements have been made to the Smart Group system, including the addition of a new column in the main SG listing, several convenience features during the editing and creation of smart groups, and a new assignment category, Channels. See Smart Groups on page 41
- In addition to making background task optimizations, the Compliance Engine has received a new platform, QNX, which can now be the focus of a new compliance policy. There are also two new compliance rules: Vendor Application Blacklist and Roaming Cell Data Usage. See Adding a Compliance Policy on page 109 and see Compliance Policies by Platform on page 107
- Lifecycle Notifications can be configured to notify the user, the admin, and anyone else with an email address when a device is enrolled into AirWatch successfully or is successfully unenrolled from AirWatch. See Lifecycle Notifications on page 87
- Administrators can now take advantage of Android's Auto-Enrollment capabilities. See End User Device Registration on page 83
- A Mobile Console has been established, allowing administrators to access a mobile version of the AirWatch Admin Console and enabling them to perform basic device management remotely while they themselves are using a mobile device. See Using the Mobile Console on page 21.

Introduction to Mobile Device Management (MDM)

Overview

This guide outlines how to effectively create, configure and maintain your MDM deployment.

Mobile devices are valuable enterprise tools, allowing immediate access to your internal content and resources. However, the diversity of mobile platforms, operating systems and versions can make managing a uniform set of devices difficult. Mobile Device Management (MDM) solves this problem by enabling you to configure, secure, monitor and manage all types of mobile devices in the enterprise.

- Manage large-scale deployments of mobile devices from a single console.
- Enroll devices in your enterprise environment quickly and easily.
- Configure and update device settings over-the-air.
- Enforce security and compliance policies.
- Secure mobile access to corporate resources.
- Lock and wipe managed devices remotely.

Tailor your MDM environment to gain immediate access to device locations, current users and content. Automate your MDM deployment to enforce security and compliance settings 24/7 with rules and warnings unique to each user or Organization Group. Make certain content and features are available and establish restrictions based on a device's geographic location.

In This Guide

- Before You Begin – Details useful background information and things to keep in mind before diving into AirWatch and MDM, including prerequisites and suggested reading.
- Getting Started with AirWatch – Introduces the AirWatch Admin Console and provides a detailed walkthrough of its main pages, menus and functions.
- Setting Up Your Environment – Covers aspects of preparing your MDM deployment, including privacy settings, Terms of Use and various environment setup options.
- Organization Groups – Summarizes how Organization Groups are used to manage MDM and how to maintain Organization Groups in the AirWatch Admin Console.
- Device Users – Details how to create user accounts within AirWatch or integrate with your existing directory service.
- User Groups – Details how to create user groups within AirWatch for assignment or integrate with your existing directory service groups.
- Administrators and Role-Based Access – Explains how Administrators and role-based access are used to customize features and settings for specific users in the AirWatch Admin Console.

- Device Enrollment – Covers each of the enrollment options available in AirWatch, including single- and multi-user devices, staging devices for other users, and various enrollment options and restrictions.
- Profiles – Details each of the profile options available in the AirWatch Admin Console to secure your devices, including enforcing passcodes, geofences, timefences and restrictions.
- Geofences – Covers geofences and how they are defined and applied to profiles.
- Time Schedules – Details time schedules and how they are created and applied to profiles.
- Compliance – Explains how the AirWatch Compliance Engine works and how to create compliance policies.
- Managing Devices – Explains how to manage all aspects of your MDM deployment from the AirWatch Admin Console (Hub and Device Control Panel) and Self-Service Portal (SSP).

Before You Begin

Overview

Before configuring your AirWatch MDM deployment, you should consider the following prerequisites, requirements, supporting materials, and helpful suggestions from the AirWatch team. Familiarizing yourself with the information available in this section will help prepare you for configuring your MDM deployment.

In This Section

- Supported Browsers – View a comprehensive list of supported browsers.
- Supported Devices – View a comprehensive list of supported devices.

Supported Browsers

The AirWatch Admin Console supports the following web browsers:

- Internet Explorer 9+
- Firefox 3.x+
- Google Chrome 11+
- Safari 5.x

Note: If using IE to access the Console, navigate to **Settings > Internet Options > Security** and ensure you have a security level or custom security level that includes the **Font Download** option being set to **Enabled**.

If you are using a browser older than those listed above, we recommend upgrading to a newer browser to guarantee all the features and functionality available in the AirWatch Admin Console. Comprehensive platform testing has been performed to ensure functionality using these web browsers. The AirWatch Admin Console may still function in non-certified browsers with minor issues.

Supported Devices

AirWatch supports the following devices and operating systems:

- Android versions 2.3+
- BlackBerry versions 5+
- BlackBerry 10
- Chromebook 39.0+
- iOS versions 4.0+
- Mac OS X 10.7+
- QNX 6.5+
- Symbian OS ^3 and S60
- Windows Mobile 5/6 and Windows CE 4/5/6
- Windows Phone 7 and 7.5 Mango
- Windows Phone 8
- Windows 8/8.1/RT
- Win32

Note: Limited support may be available for other devices/operating systems. Please refer to each platform's specific User Guide, available via AirWatch Resources, or contact AirWatch Support for more information.

Getting Started with AirWatch

Overview

The AirWatch Admin Console provides a centralized solution to view and manage every aspect of your Mobile Device Management (MDM) deployment. Quickly and easily add new devices and users to your fleet, manage profiles and configure system settings all within a single, web-based resource.

In This Section

- Logging into the AirWatch Admin Console – Explains how to log into your environment and where to obtain login credentials.
- Setting Your Security PIN – Details the initial security PIN prompt and how to manage actions requiring the Security PIN.
- The AirWatch Admin Console at a Glance – Provides information for all available menus and main features within the AirWatch Admin Console.
- Using the Global Search – Details the function and behavior of the Global Search feature, including areas searched and search result sorting.
- Using the Getting Started Wizard – Explores the Getting Started Wizard and helps understand how the tool is used to configure your environment and deployment.

Logging into the AirWatch Admin Console

Before logging into the AirWatch Admin Console, you must have the **Environment URL** and **login credentials** provided to you by your AirWatch administrator, account representative or free trial. Where you obtain this information depends on your type of deployment. For example:

- **SaaS Deployment** – Your **Account Manager** will provide your Environment URL and username/password. The URL is not customizable and generally follows the format of **awmdm.com**.
- **On-Premise** – Your **Consultant** will provide your Environment URL and username/password. The URL is customizable and generally follows the format of **awmdm.<MyCompany>.com**.

Your Account Manager provides initial setup credentials for your environment. Admins who create additional accounts to delegate management responsibility may also create and distribute credentials for their environment. See Creating an Admin Account for details.

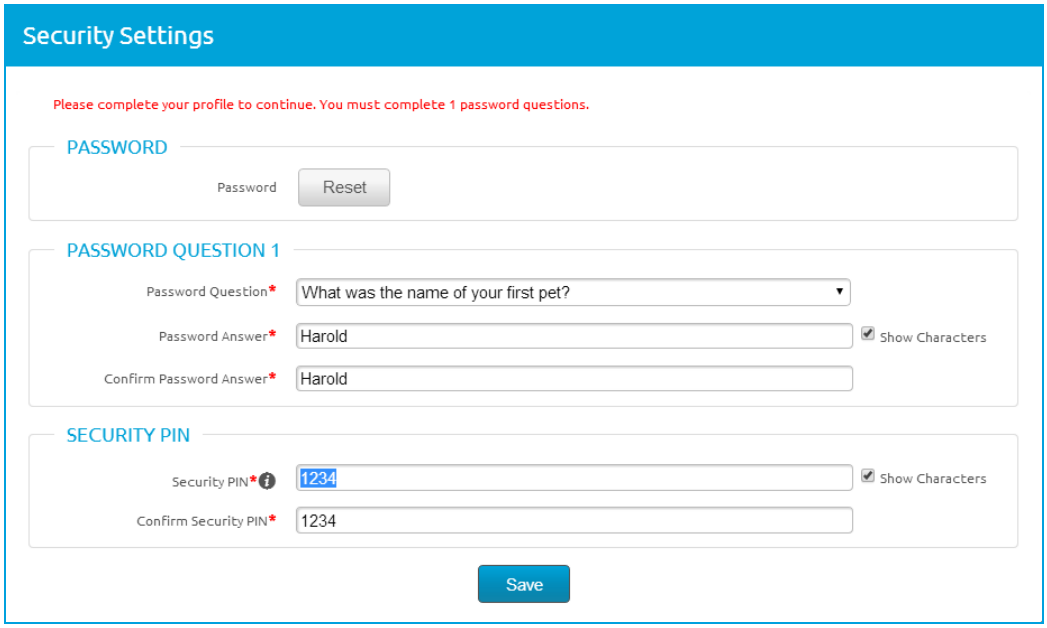
Once your browser has successfully loaded the **Environment URL** where the AirWatch Console resides, logging in is simply a matter of entering your **Username** and **Password** provided by your AirWatch Administrator.

Note: Passwords are case-sensitive.

Setting Your Security PIN

Upon first logging into the AirWatch Admin Console, you must establish a Security PIN. The Security PIN acts as a safeguard against accidental device wipes or deletion of major MDM-related aspects of your environment, including users and Organization Groups.

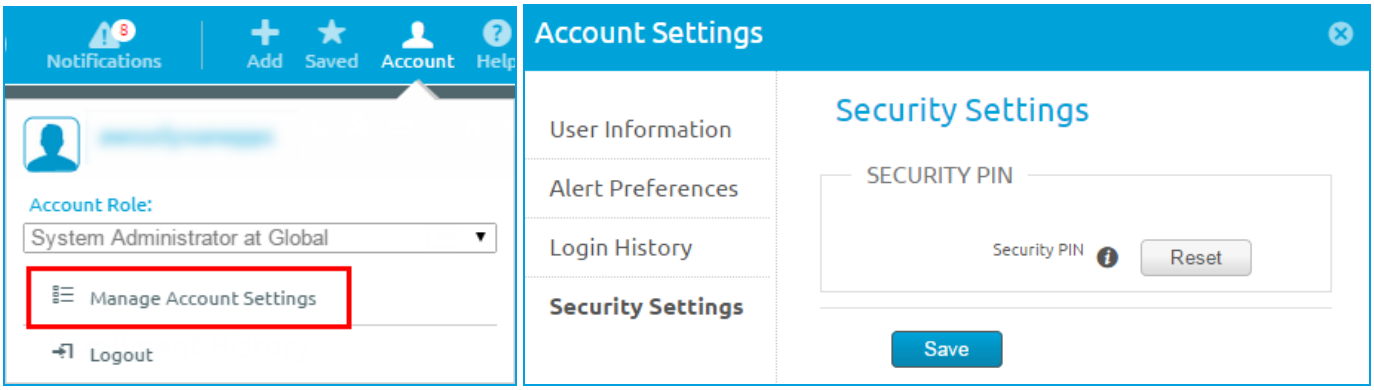
The Security PIN also serves as a second layer of security, presenting an additional point of authentication by blocking actions made by unapproved users if the AirWatch Admin Console is left open and unattended. Enter and confirm your four-digit Security PIN when presented with the Security Settings page and save this PIN for future use. You may not bypass this page or proceed to any area within the AirWatch Admin Console before creating this PIN.



Resetting Your PIN

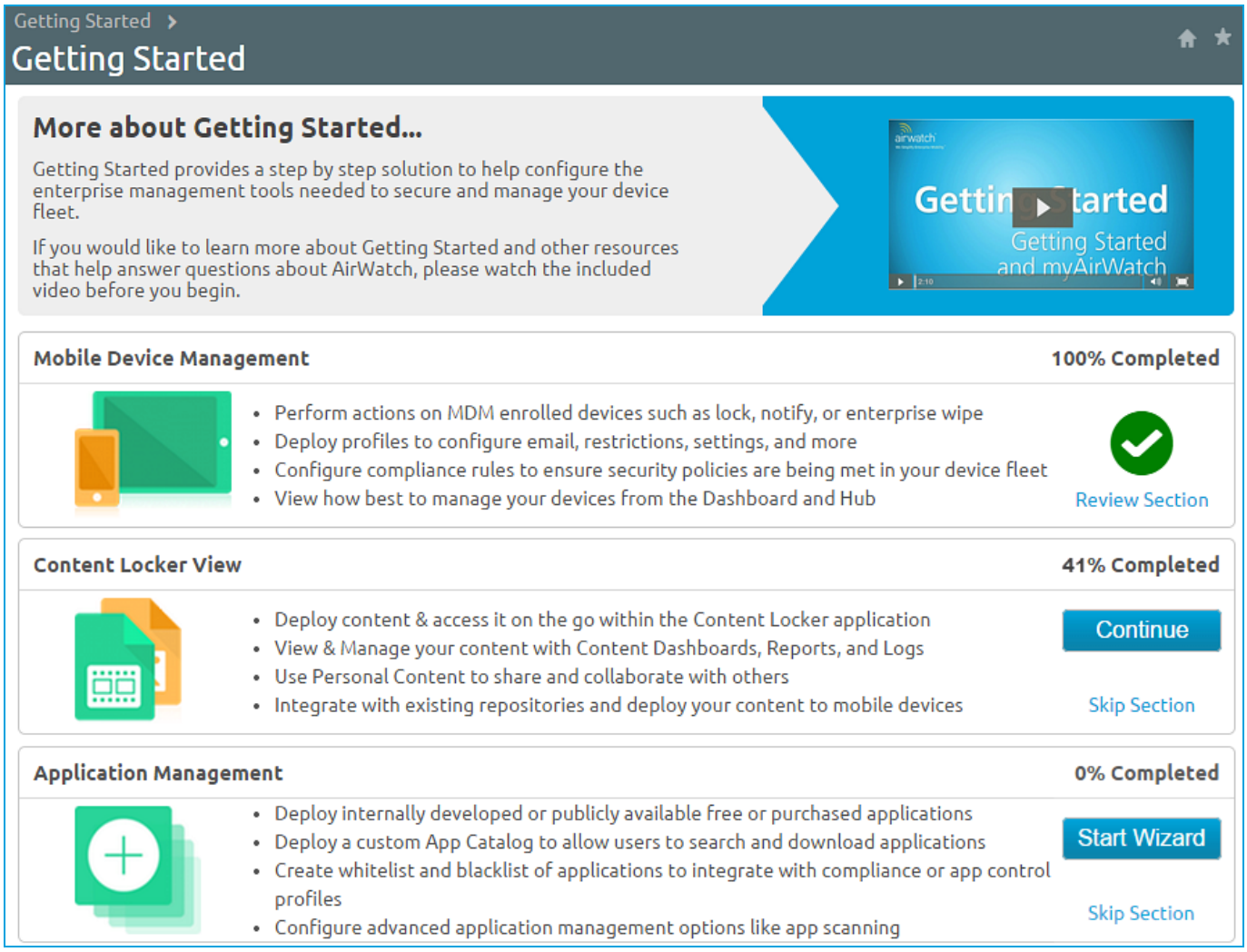
Once your PIN is set, revisit the **Security Settings** page to reset the PIN by selecting the **Account** icon in the top-right corner of the AirWatch Admin Console and then selecting **Manage Account Settings**.

Select **Reset** from the Security Settings menu to reset your PIN, log out of the AirWatch Admin Console and present the PIN creation prompt upon logging back in.



Using the Getting Started Wizard

The **Getting Started Wizard** serves as a checklist that ensures all aspects of a successful deployment are established. It is organized by module to accurately reflect the modules within an AirWatch Admin Console deployment. This produces an on-boarding experience that is tailored to your configuration.



The **Getting Started** page is split into three sections: **Mobile Device Management**, **Mobile Content Management** and **Mobile Application Management**, each with their own set of steps. Steps that are shared among the three sections are kept track of automatically so you never have to take the same step twice.

- **Mobile Device Management** (MDM) – Establish the level of control you wish to have over your devices, add users and enroll devices into the AirWatch system.
- **Mobile Content Management** (MCM) – Identify content, add users, secure personal content and configure content management specifications.
- **Mobile Application Management** (MAM) – Determine how users will install recommended apps, identify and install public apps to enrolled devices.

Review your responses to any module at any time by selecting **Review Section** from each completed module. Additionally, opt out of any module by selecting **Skip Section**, which temporarily disables the **Continue** button and inserts a **Resume Section** link. Select this link to enable the **Continue** button once more.

Select **Start Wizard** to initiate the first steps in a module, answering questions and accessing the exact pages within the AirWatch Admin Console to configure settings for each feature. As you answer each question, the percentage counter will progress, displaying how far along you are in completing the module. If you stop a module before completing, you may return to where you left off by selecting **Continue**.

As each substep in the module is completed, a small check-mark is placed in the header bar representing that substep and the green status bar at the top representing the whole module progresses further.

Select the **Back** button at any time to return to the previously-answered question or screen.

Manually Enabling the Getting Started Wizard

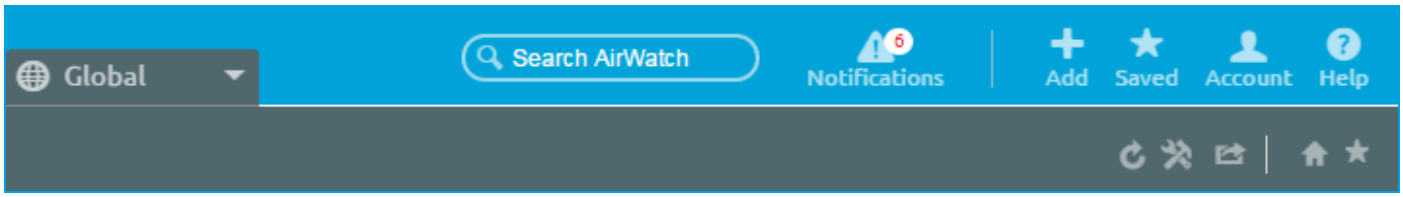
For a new AirWatch implementation, the Getting Started page is accessed from the main menu, above the **Hub** icon on the far-left side of the console screen. However, you can manually enable the Getting Started Wizard at any time, thereby restarting the walk through.

Do this by performing the following steps:

1. Select any **Organization Group** other than the top-level group. You can also easily create a new Organization Group.
2. Navigate to **Groups & Settings** ▸ **Groups** ▸ **Organization Groups** ▸ **Organization Group Details**. Ensure you are currently at a customer-level Organization Group and **Save** your changes.
3. Navigate next to **Groups & Settings** ▸ **All Settings** ▸ **System** ▸ **Getting Started**.
4. Select 'Enable' for each of the fields on this page: **Getting Started Device Status**, **Getting Started Content Status** and **Getting Started Application Status** and **Save** changes to the page.

The AirWatch Admin Console at a Glance

The AirWatch Admin Console has several key components, which are described below.



Header Menu

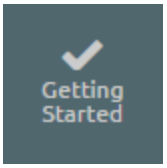
The header menu options, shown above, provide access to:

- **Organization Group** – Select the organization group (the tab labeled "Global") you wish to apply changes to. See Organization Groups for details.
- **Global Search** – Search all aspects of your AirWatch deployment within the AirWatch Admin Console, including devices, users, content, applications, configuration settings admins, pages and more.
- **Notifications** – Stay informed about expired APNs certificates with Notifications. The red number badge hovering over the Notifications button indicates the number of alerts you should see.

- **Add** – Quickly add an admin, device, user, compliance policy, content, profile, internal application or public application.
- **Saved** – Access your favorite and most-utilized features within the AirWatch Admin Console.
- **Account** – View your account information. Change roles that you are assigned to within the current environment. Customize preferences, including contact information, AirWatch Admin Console settings and preferences and login history. Log out of the AirWatch Admin Console and return to the Login screen.
- **Help** – Launch the online help portal to browse or search the available guides and feature documentation.
- **Refresh** – Executes a screen refresh (to see updated stats and info) without leaving the current view.
- **Available Sections** – Customize the sections you want to see with the Available Sections icon. Accessible only on the Hub Overview.
- **Export** – Produce a .pdf version of the console screen with the Export button. Accessible only on Hub Overview.
- **Home** – Assign any screen in the AirWatch Admin Console as your home page by selecting the home icon. The next time you open the Admin Console, your selected screen will be the first to display.
- **Save** – Saves the current page or view for quick access from your list of Saved pages.

Main Menu

Additionally, the **Main Menu** allows quick navigation to all features available within your role and Mobile Device Management (MDM) deployment. These options generally include:



Getting Started – Start off right with Getting Started which serves as a checklist ensuring all aspects of a basic successful deployment are established. It is organized by module to accurately reflect the modules within an AirWatch Admin Console deployment. This produces an on-boarding experience that is more tailored to your actual AW configuration.

Hub – View and manage MDM information that drives decisions you need to make. Gain a quick overview of specific information such as the most blacklisted apps that violate compliance, Admin Panel Dashboard to keep track of module licenses or all devices that are currently out of compliance. Review the Using the Hub section for more information.

Devices – Access the Devices Dashboard for a detailed overview of common aspects of devices in your fleet, including compliance status and breakdown of ownership type, last seen, platform type and enrollment type. Easily swap views according to your own preference, including full Dashboard, list view or detail view. Drill down to additional tabs, including all current profiles, enrollment status, 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. Additionally, access and manage admin groups, roles, system activity and settings associated with your administrators.

Apps & Books – Access and manage the app catalog, book catalog and Volume Purchase Program (VPP) orders. Also view application analytics and logs along with application settings, including app categories, Smart Groups, app groups, featured apps, geofencing and profiles associated with apps.

Content – Access the Content Dashboard for a detailed overview of content usage including storage history trends, user/content status, engagement and user breakdown. Manage and upload content available to users and devices. Additionally, access batch import status, content categories, content repositories, user storage, AirWatch Content Locker homescreen configuration and all other content-specific settings.

Email – Access the Email Dashboard for a detailed overview of email information related to your deployment, including email management status, managed devices, email policy violations, deployment type and time last seen.

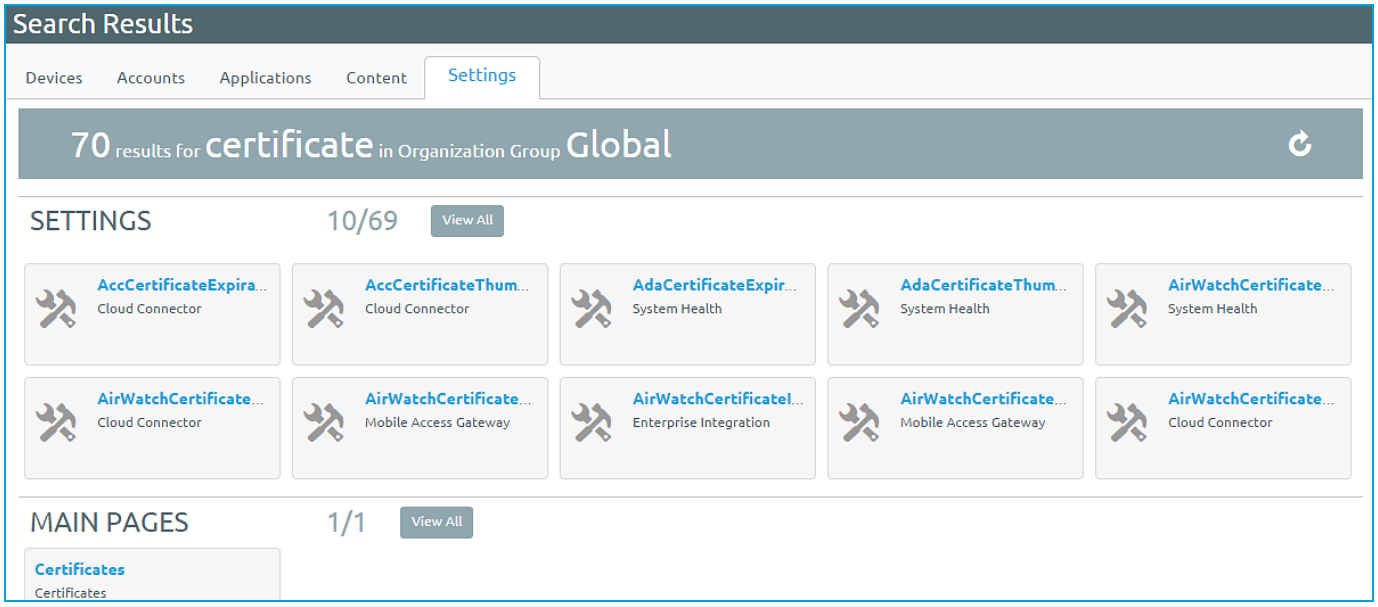
Telecom – Access the Telecom Dashboard to see a detailed overview of telecom-enabled devices including plan utilization, usage history and roaming data. View and manage telecom usage and roaming tracking, including call, Short Message Service (SMS) and content settings.

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 **Main Menu** options outlined above.

Click the bottom-left arrow  to toggle the Secondary Menu view on or off.

Using the Global Search

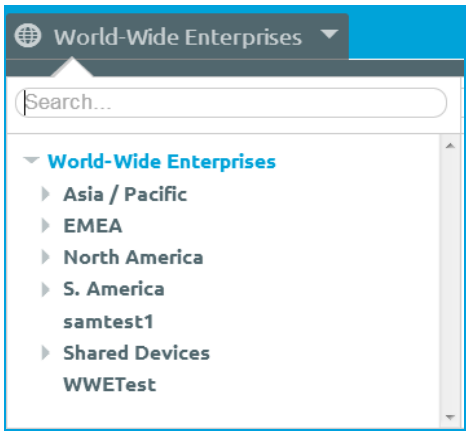
The AirWatch Admin Console's Global Search box returns quick-access information for your entire deployment. Global Search uses a modular design with a tabbed interface, applying your search to a single tab at a time, which produces fast results. Select another tab to apply the same search parameters.



After executing a Global Search, select the following tabs to view the results:

- **Devices** – Returns matches to Device friendly name as well as Device Profile name.
- **Accounts** – Returns matches to User names and Administrator names.
- **Applications** – Returns matches to Internal, Public and Purchased Applications.
- **Content** – Returns matches to any content that appears on devices.
- **Settings** – Returns matches to individual settings and console main pages.

You can also perform a search for an Organization Group by selecting the Organization Group drop-down menu, which displays the Search bar above the listing.



Viewing Notifications

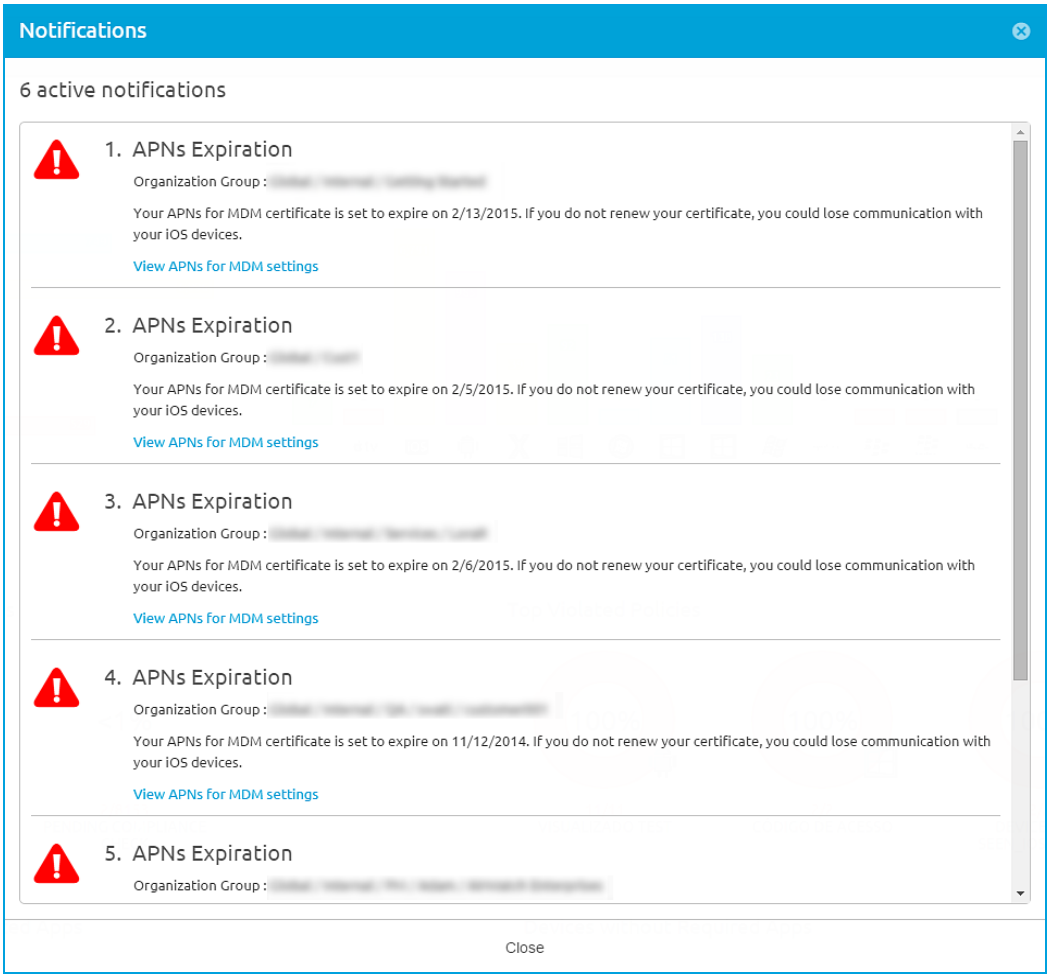
Next to the Global Search bar is the **Notifications** button, which alerts you when APNs for MDM certificates are set to expire within 30 days. This is valuable because it enables you to avoid the hassles involved with expired certificates and keeps your devices in communication with the AirWatch Admin Console.

When there are active notifications that require your attention, a red numeral badge appears on the button-face indicating how many alerts there are. Select the **Notifications** button to display the **Notifications** screen.

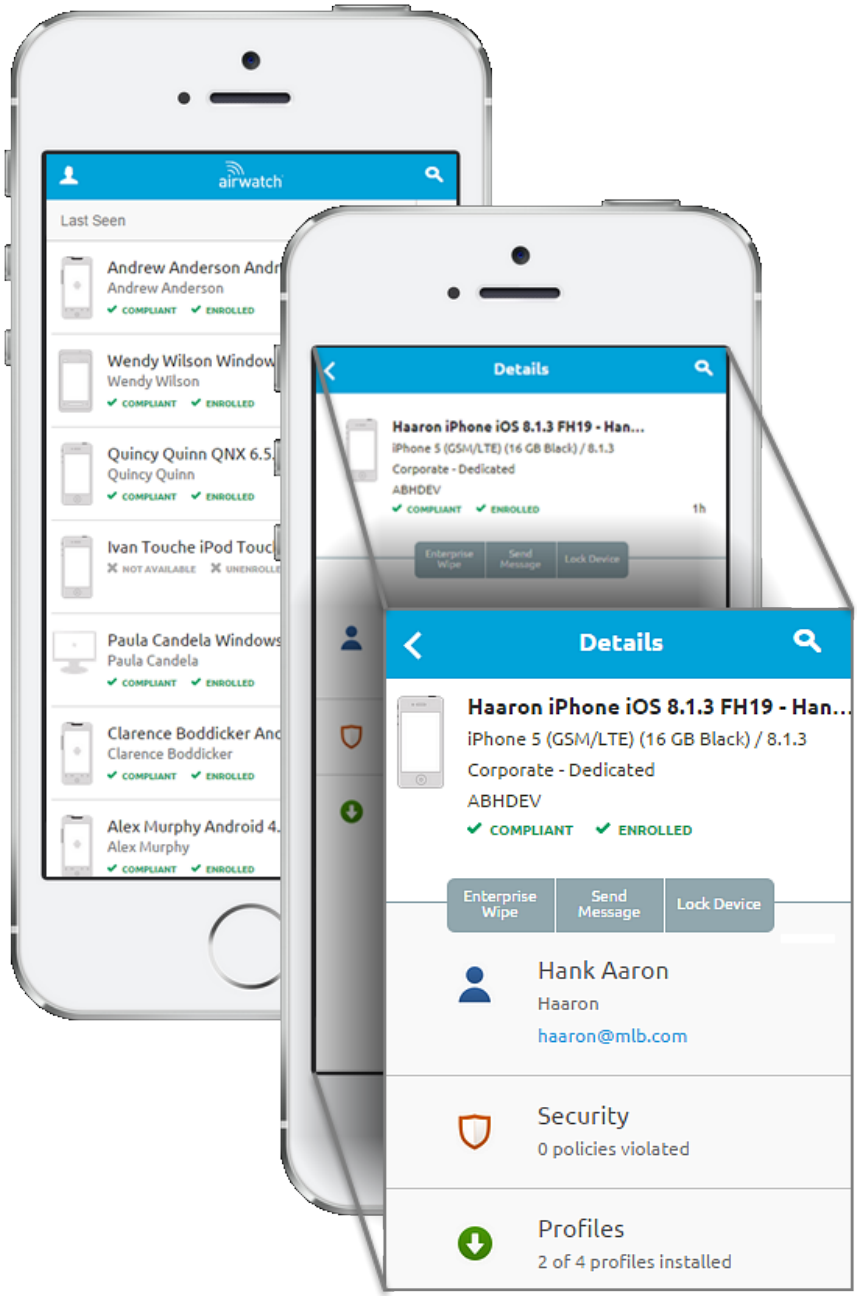
Each alert displays the organization group under which the APNs for MDM certificate is located, the date the certificate is due to expire as well as a link to the **System Settings** page for APNs.

Note: selecting the **View APNs for MDM settings** link will display the **System Settings** page for the Organization Group (OG) you are currently in.

Before you are able to take action in **System Settings** on the specific certificate due to expire, you must manually navigate to the OG reported in the **Notifications** screen.



Using the Mobile Console



A mobile-friendly console view is available including **Device List** and **Details** views. You may initiate several different kinds of actions, all remotely through your mobile device.

The Admin Console will automatically invoke the correct version (Mobile vs. Full) depending upon the device you are using. Tablet devices are able to run the full version in its default browser and mobile phones will display the **Mobile Console** view. For either type of device, enter the default login URL **https://<AirWatchEnvironment>/AirWatch** and the console will do the rest.

The **Device List** view features sorting (ascending and descending) by User, Friendly Name and Last Seen. It also displays whether or not the device is compliant and whether the device has been enrolled. The **Device List** view displays how much time has elapsed since the device was last seen in the listing. Additionally, there is an icon in the top-left corner that allows you to **Logout** and to **Switch to desktop version**.

The **Details** view displays the Friendly Name, Model and OS info, Device Ownership, and Username. You can also see how many profiles are installed as well as security violations and the user's email.

Tapping the gray buttons at the top of the **Details** view will initiate actions on the selected device including **Enterprise Wipe**, **Send Message**, and **Lock Device**.

Environment Setup

Overview

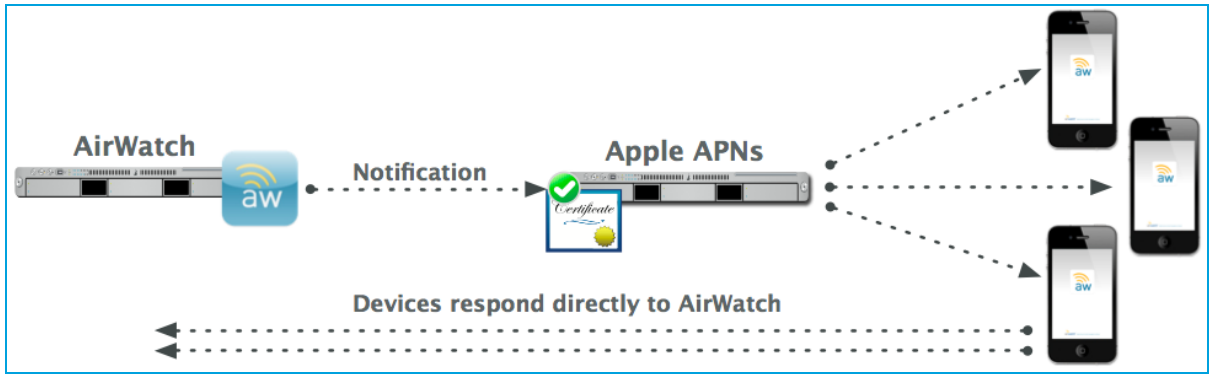
The next step to establishing your AirWatch deployment is setting up your AirWatch environment and laying the groundwork for your deployment, including establishing certificates for managing certain platforms and configuring telecom and privacy settings.

In This Section

- Generating an APNs Certificate – Details how to generate an Apple Push Notification service certificate, in case you will be managing Apple devices.
- Configuring Privacy Settings – Covers the various privacy options available in the AirWatch Admin Console.
- Setting Up Autodiscovery – Explains how to configure auto discovery with a single organization email address to streamline enrollment.
- Configuring Terms of Use – Details how to customize Terms of Use presented to users upon enrolling their device, logging into the AirWatch Admin Console and using applications.
- Configuring Console Branding – Provides information regarding customizing your environment with branding and theme options.
- Integrating with Other Systems – Describes how you can connect AirWatch with your other enterprise systems.

Generating an APNs Certificate

If you are planning on managing iOS devices, you must first obtain an Apple Push Notification Service (APNs) certificate. APNs allow AirWatch to securely communicate to Apple devices and report information back to AirWatch.



To generate an APNs Certificate, follow the simple steps outlined in the Getting Started Wizard or navigate to **Groups & Settings ▸ All Settings ▸ Devices & Users ▸ Apple ▸ APNs for MDM**.

The Notifications button in the header bar of the console will alert you if your APNs for MDM certificates are in jeopardy of expiring, allowing you to take early action. See Notificationsfor details about this feature.

For more information, please see the **Generating and Renewing an APNs Certificate for AirWatch** document, available via AirWatch Resources.

Configuring Privacy Settings

Configure Privacy Settings to define how device and user information are handled in the AirWatch Admin Console. This is particularly useful in bring your own device (BYOD) deployments.

The AirWatch Admin Console enables you to:

- Review and adjust privacy policies according to device ownership, which lets you easily adhere to data privacy laws in other countries or legally-defined restrictions.
- Ensure certain IT checks and balances are in place, preventing overload of servers and systems.

See Privacy Best Practices for tips about configuring data collection for GPS, Telecom and application usage.

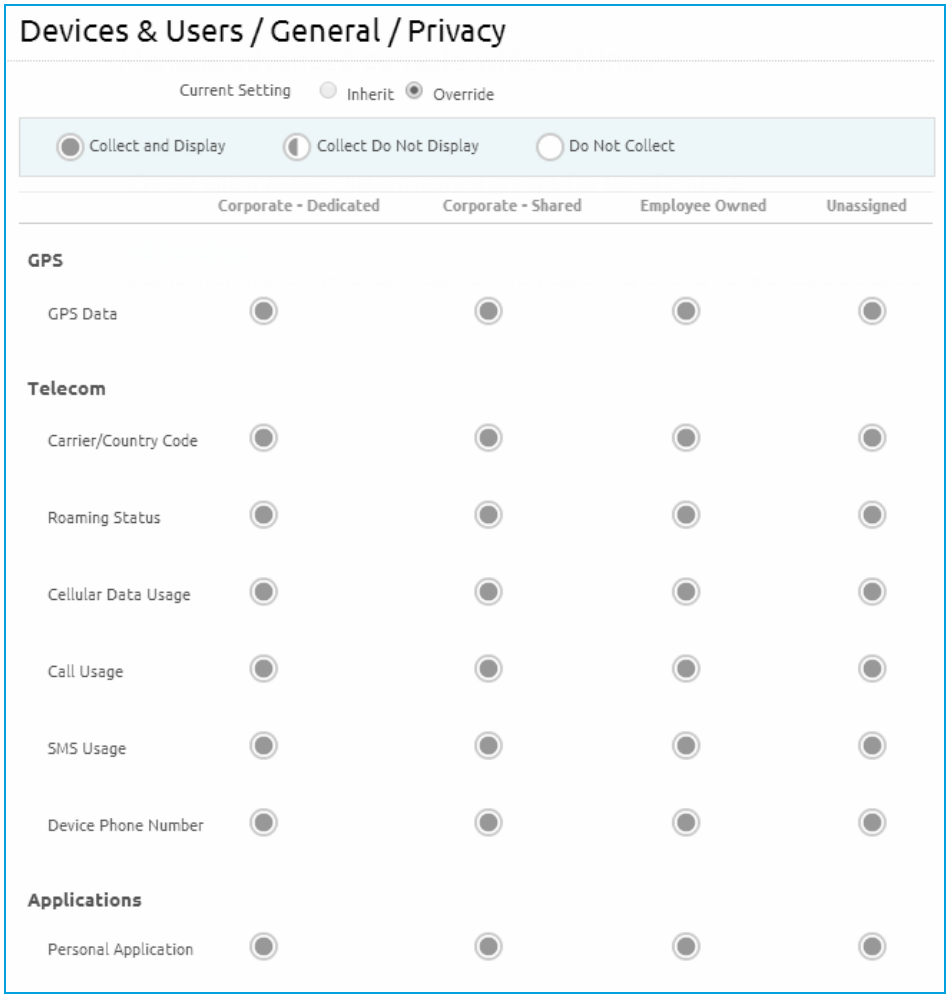
To set up privacy settings:

1. Navigate to **Devices** ▸ **Device Settings** ▸ **Devices & Users** ▸ **General** ▸ **Privacy**.
2. Select one of the following options for the various settings for **GPS**, **Telecom** and **Applications:**

   Collect and Display – Collect user data and display it in the AirWatch Admin Console.

   Collect Do Not Display – Collect user data for use in reports but do not display it in the AirWatch Admin Console.

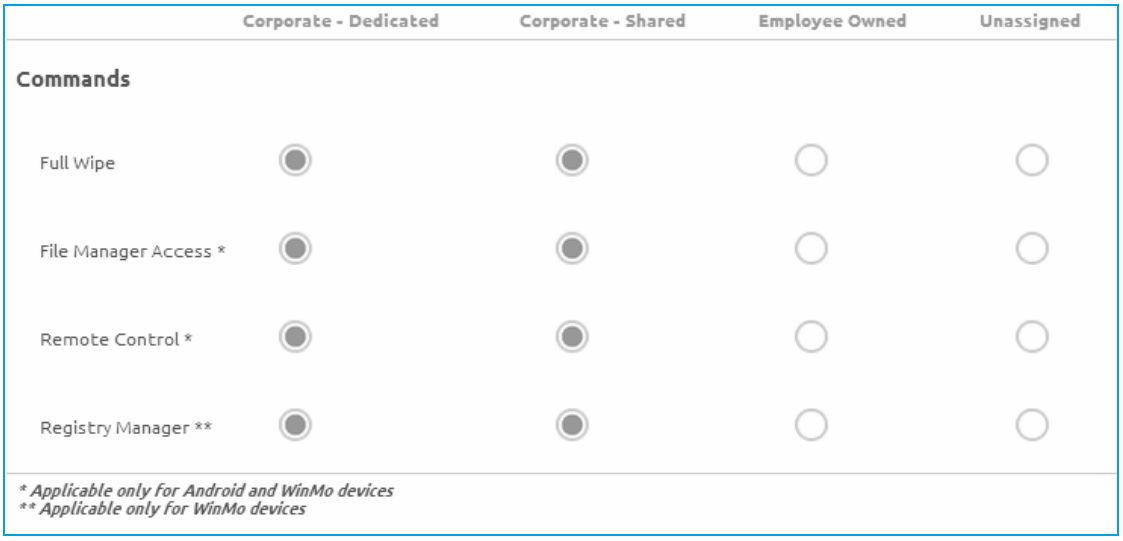
   Do Not Collect – Do not collect user data.



1. For more information on privacy within AirWatch, see recommended best practices.
2. Select the **Commands** that can be performed on devices.

   Consider disabling all remote commands for employee-owned devices – especially full wipe. This prevents inadvertent deletion or wiping of an end user's personal content.

   If you are going to allow remote control, file manager, or registry manager access for Android/Windows Mobile devices, you should consider using the **Allow With User Permission** option. This requires the end user to consent to admin access on their device via message prompt before the action is performed. If you opt to allow use of any commands, explicitly mention these in your Terms of Use agreement.

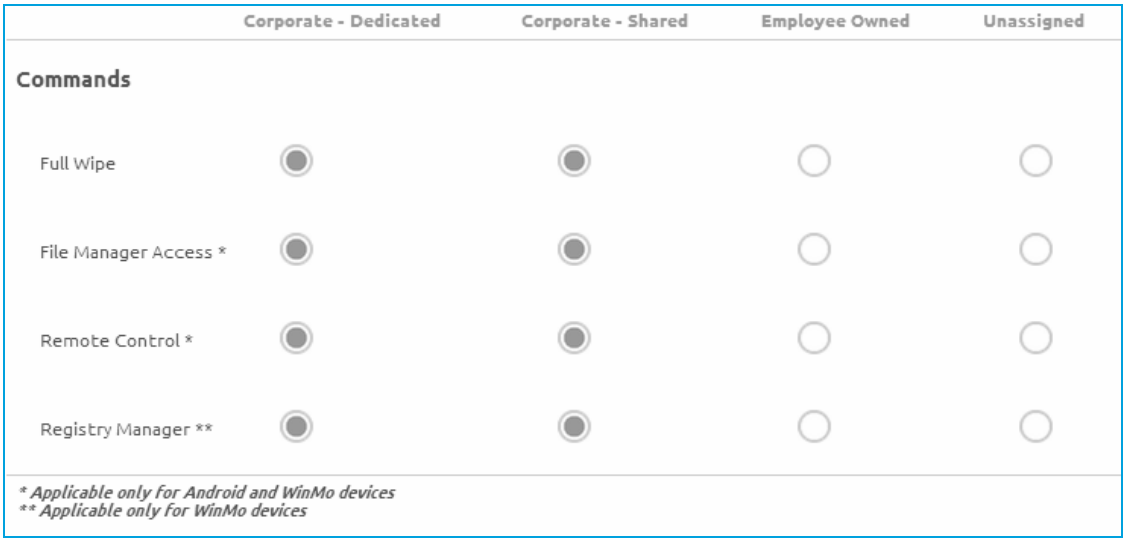


3. Select the **Commands** that can be performed on devices.

   Consider disabling all remote commands for employee-owned devices – especially full wipe. This prevents inadvertent deletion or wiping of an end user's personal content.

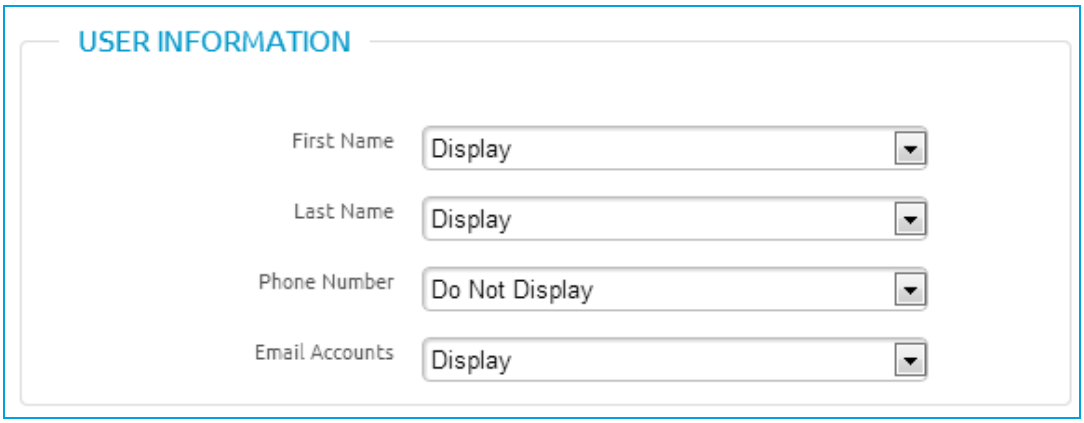
   Note for iOS devices: If you disable full wipe as a command for select ownership types, then users who enroll under that ownership type will not see the "Erase all content and settings" permission displayed during MDM profile installation when enrolling with the AirWatch Agent.

   If you are going to allow remote control, file manager, or registry manager access for Android/Windows Mobile devices, you should consider using the **Allow With User Permission** option. This requires the end user to consent to admin access on their device via message prompt before the action is performed. If you opt to allow use of any commands, explicitly mention these in your Terms of Use agreement.



4. For **User Information**, select whether to **Display** or **Do Not Display** in the AirWatch Admin Console information for **First Name, Last Name, Phone Number**, and **Email Accounts**.

If a field is set to **Do Not Display**, then it displays as "Private" wherever it appears in the AirWatch Admin Console. This means you are not be able to search for fields you set to **Do Not Display**.



Note: If desired, you can encrypt personally identifiable information, including first name, last name, email address and telephone number. Navigate to **Groups & Settings ▸ All Settings ▸ System ▸ Security ▸ Data Security** from the Global or Customer-level Organization Group you want to configure encryption for. Enabling encryption, selecting which user data fields to encrypt, and clicking **Save** encrypts user data. Doing so limits some features in the AirWatch Admin Console, such as search, sort and filter.

5. Click **Save** when finished.

For more information about leveraging bring your own device, please see the .**AirWatch BYOD Guide** document, available via AirWatch Resources.

Privacy Best Practices

AirWatch recommends a few simple best practices for managing Privacy Settings. Note, however, that every deployment is different and you should consult with your own legal, human resource and management teams to tailor these settings to best suit your organization.

GPS Coordinates

In general, it is not appropriate to collect GPS data for employee-owned devices. The following notes apply to corporate-owned devices:

- GPS Data – Information collected includes location data and a time-stamp indicating when this information was sent to AirWatch.
    - For iOS devices, GPS data is reported automatically by opening any AirWatch application or internal applications with an AirWatch software development kit (SDK) set to capture GPS data.

      When this happens, AirWatch defines a 1 kilometer region around this location and reports location information whenever the device moves outside this 1 kilometer region or whenever the user opens an AirWatch or internal

application. No new GPS data is reported unless one of these actions occurs.

- Location Services must be enabled on the iOS device. AirWatch cannot force this setting.

- While GPS data is typically used for lost or stolen devices, it can also be used for any situation where knowing a device's location is useful.

User Information

In general, you will display user information such as first name and last name for both employee-owned and corporate-owned devices, since you need to know who you are managing. This information includes First Name, Last Name, Phone Number and Email Address.

Telecom Data

In general, it is only appropriate to collect telecom data for employee-owned devices that are a part of a stipend program where you subsidize an end user's cellphone plan. In this case, or for corporate-owned devices, the following notes apply:

- **Carrier/Country Code** – Carrier and Country Code are recorded and can be used for telecom tracking purposes. Telecom plans can be set up and devices can be assigned to the appropriate plan based on their carrier and country. This information can also be used to track devices by home carrier and home country or by current country and current carrier if the device is traveling.

- **Roaming Status** – Roaming Status is either "Roaming" or "Not Roaming" in AirWatch. This can be used to track which devices are in a roaming state. Compliance policies can be set up to disable voice and data usage while the device is roaming or perform other compliance actions. Additionally, if the device is assigned to a telecom plan, AirWatch can track data usage while roaming. Collecting and monitoring roaming status can be helpful in preventing large carrier charges due to roaming.

- **Cellular Data Usage** – Cellular Data Usage refers to data usage in terms of total bytes sent and received. This data can be collected for each cellular device. If the device is assigned to a telecom plan within AirWatch, you can monitor data usage based on a percentage of a total amount of data for a billing cycle. This allows you to create compliance policies based on the percentage of data used. This can be helpful in preventing large carrier overage charges.

- **Cell Usage** – Cell Usage refers to the voice minutes that can be collected for each cellular device. Similar to Data Usage, if the device is assigned to a telecom plan within AirWatch, you can monitor voice usage based on a percentage of a total amount of minutes for a billing cycle. This allows you to create compliance policies based on the percentage of minutes used. This can be helpful in preventing large carrier overage charges.

- **SMS Usage** – SMS Usage refers to the short message service data that can be collected for each cellular device. Similar to Data Usage, if the device is assigned to a telecom plan within AirWatch, you can monitor SMS usage based on a percentage of a total amount of messages for a billing cycle. This allows you to create compliance policies based on the percentage of messages used. This can be helpful in preventing large carrier overage charges.

Application Information

In general, it is appropriate to set the collection of application information to either **do not collect** or **collect and do not display** for employee-owned devices. This is because public apps installed on a device, if viewed, can be considered personally identifiable information. For corporate-owned devices, all installed applications on the device will be reported to AirWatch.

If “Do Not Collect” is selected, only personal application information will not be collected. All managed applications, whether public, internal or purchased will still be collected by AirWatch.

Remote Commands

Consider disabling all remote commands for employee-owned devices. However, if you are going to allow remote actions or commands, you will want to explicitly mention these in your Terms of Use agreement.

Setting Up Autodiscovery

AirWatch makes the enrollment process as simple as possible, leveraging an autodiscovery system to associate and enroll devices to intended environments using end users' email addresses. It can also be used to allow end users to authenticate into the Self-Service Portal (SSP) using their email address. The server checks for email domain uniqueness, only allowing a domain to be registered at one Organization Group in one environment. It is therefore recommended that your domain is registered at your highest Organization Group.

Note: Autodiscovery is configured automatically for new software as a service (SaaS) customers.

Note: To enable autodiscovery for on-premise environments, ensure your environment can communicate with the AirWatch Autodiscovery servers. For the latest on-premise requirements, refer to the AirWatch **Installation Guide**, available via AirWatch Resources.

Autodiscovery Enrollment from a Parent Organization Group

To enable autodiscovery enrollment:

1. Navigate to **Devices** ▸ **Device Settings** ▸ **Devices & Users** ▸ **General** ▸ **Enrollment**, select the **Authentication** tab and then select **Add Email Domain**.
2. Select the **Organization Group** you want to associate with this domain and then enter your **Business Email Domain** and **Confirmation Email Address**. This Organization Group associates end users to your environment and serves as the starting point for possible Group ID selection prompts.
3. Verify your email address by clicking the confirmation link in the email sent to the address you provided.
4. Add more **Business Email Domains** as required, such as "us.example.com" or "eu.example.com."
   - Multiple email domains can be added to the same Organization Group level.
   - Consider adding alternative email domains to other Organization Groups to facilitate multi-tenancy.
5. Select **Save** to complete autodiscovery setup.

Instruct end users who enroll themselves to enter their email address for authentication instead of entering an environment URL and Group ID. When users enroll devices using the email address prompt, those devices will be enrolled into the same group that is listed in the **Enrollment Organization Group** field of the associated AirWatch user account.

Autodiscovery Enrollment from a Child Organization Group

If you expect your users to enroll devices into a child Organization Group below the Enrollment Organization Group of the user, then you should prompt users to select a Group ID during enrollment. You can enable this by navigating to **Devices ▸ Device Settings ▸ General ▸ Enrollment ▸ Grouping** and selecting **Prompt User to Select Group ID**. For additional enrollment considerations and details about configuring enrollment options, refer to the **AirWatch Enrollment Processes Guide**, available via AirWatch Resources.

Configuring Terms of Use

Define and enforce Terms of Use to ensure all users with managed devices agree to the policy. If required, users must accept the Terms of Use before proceeding with enrollment, installing apps, or accessing the AirWatch Admin Console. The AirWatch Admin Console allows you to fully customize and assign a unique Terms of Use to each Organization Group and Child Organization Group.

Creating Enrollment Terms of Use

The Terms of Use displays during each device's enrollment. Set version numbers, set platforms to receive the Terms of Use, set to notify users by email if the Terms of Use is updated and create language-specific copies of the Terms of Use.

You can create multiple Terms of Use agreements and assign them to Organization Groups based on ownership type or platform. This lets you tailor each agreement to meet the legal and liability requirements of specific groups, including users enrolled in your BYOD program.

1. Ensure your current active Organization Group is the correct one for the terms of use you are creating.
2. Navigate to **Devices ▸ Device Settings ▸ Devices & Users ▸ General ▸ Enrollment** and select the **Terms of Use** tab.
3. Select **Add New Enrollment Terms of Use**.
4. Set the Terms of Use to trigger depending on platform type by toggling the **Platforms** option from **Any** to **Selected Platform** and checking each desired platform.
5. Set the Terms of Use to trigger depending on ownership type by toggling the **Device Ownership** option from **Any** to **Selected Ownership Types** and checking each desired type of ownership.
6. Set the Terms of Use to trigger depending on enrollment type by toggling the **Enrollment Type** option from **Any** to **Selected Enrollment Types** and checking the desired type of enrollment.
7. Enter your Terms of Use in the text field provided.

   This is where you may want to mention any specific privacy settings and any applicable restrictions or compliance policies. The editor provides a basic text entry tool to create a new Terms of Use or paste in an existing Terms of Use. If pasting in text from external content, right-click the text box and choose **Paste as plain text** to prevent any HTML or formatting errors.
8. Select **Save**.

Note: You can enforce MDM Terms of Use acceptance by creating a compliance policy for **MDM Terms of Use Acceptance**.

Creating Application or Console Terms of Use

You can also create application-based Terms of Use to notify end users when a specific application collects data or when it imposes restrictions. When users launch these applications from your enterprise App Catalog, they must accept the agreement to access the application. For applications, you can set Terms of Use version numbers, create language-specific copies of the Terms of Use, and set a grace period to remove associated apps if the Terms of Use isn't accepted.

Console Terms of Use display when an administrator logs in to the AirWatch Admin Console for the first time. For the AirWatch Admin Console, you can set Terms of Use version numbers and create language-specific copies of the Terms of Use.

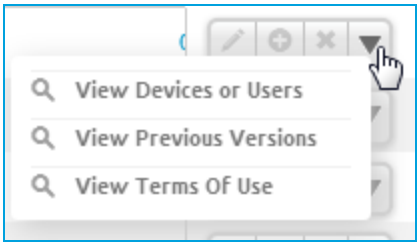
1. Navigate to **Groups & Settings** ▸ **All Settings** ▸ **System** ▸ **Terms of Use**.
2. Select **Add Terms of Use**.
3. Enter a **Name** for the Terms of Use and select the **Type**, which can be **Console**, **Enrollment** or **Application**.
4. Configure settings such as **Version** number and **Grace Period**, depending on the **Type** you selected.
5. Enter your Terms of Use in the text field provided. The editor provides a basic text entry tool to create a new Terms of Use or paste in an existing Terms of Use. If pasting in text from external content, right-click the text box and choose **Paste as plain text** to prevent any HTML or formatting errors.
6. Select **Save**.

For Applications, assign the Terms of Use when adding or editing an application using the **Terms of Use** tab. For more information, please see the **Mobile Application Management Guide** document, available via AirWatch Resources.

View Terms of Use Acceptance

While compliance policies can be set up to help enforce Terms of Use acceptance, you can also view a summary page of exactly who has and has not accepted the agreement. Then, if necessary, you can contact those individuals directly.

1. Navigate to **Groups & Settings** ▸ **All Settings** ▸ **System** ▸ **Terms of Use**. A list of Terms of Use agreements displays.
2. Use the **Type** drop-down list to filter based on agreement type, for example, Enrollment. The **Users / Devices** column displays devices that have accepted/not accepted/been assigned the Terms of Use.
3. Select the appropriate number in the **Devices** column for the applicable Terms of Use row to see device information pertaining to that agreement. Optionally, access the drop-down menu for the row and click one of the following:



- **View Devices or Users** – Display a complete list of devices and their acceptance statuses. You can filter by Organization Group.

- **View Previous Versions** – View previous iterations of the agreement.
- **View Terms of Use** – View the Terms of Use agreement.

Tracking Terms of Use Acceptance via Reports

Track user acceptance for each Terms of Use by accessing the **Hub** ▸ **Reports & Analytics** ▸ **Reports** ▸ **List View** page and generating the **Terms of Use Acceptance Detail** report. View details regarding specific Organization Groups and drill down to view AirWatch Admin Console acceptances or Device Enrollment acceptances. View the acceptances directly in the Admin Console or export the report in either PDF, CSV and Excel formats.

Note: AirWatch does not provide legally binding sample text and any text examples provided must be reviewed by your own company/legal team.

Configuring Console Branding

The AirWatch Admin Console allows extensive customization options, which provides a way to completely brand aspects of your AirWatch tools and resources according to your organization's color scheme, logo and overall aesthetic.

Additionally, branding can be configured in support of multi-tenancy, so different divisions of your enterprise can have their unique look and feel at their Organization Group level.

To configure branding settings:

1. Select the Organization Group you want to brand and then navigate to **Groups & Settings** ▸ **All Settings** ▸ **System** ▸ **Branding**.
2. Configure the settings on the **Branding** tab:
   - Upload a primary logo, secondary logo and Login page image and set a destination hyperlink for each image. Set the image by either uploading a file saved on your computer or inserting a link to an external source that can be automatically updated at any time.
   - You may also customize the SSP title by filling in the **Self Service Portal Title** field.
   - Upload a background for the Login page. Set the image by either uploading a file saved on your computer or inserting a link to an external source that can be automatically updated at any time.
   - Enable branding of reports generated in the AirWatch Admin Console.
3. Configure the settings on the **Theme** tab:
   - Set overall color theme from preset AirWatch colors or upload your own organization's colors by selecting the **Customize Field** option.
4. Configure the settings on the **Advanced** tab:
   - Enter custom CSS code for advanced branding customization.
5. Select **Save**.

Configuring Restricted Actions

In a scenario where the Admin Console is left opened and unattended, AirWatch provides an additional safeguard against actions that, undertaken by a malicious user, could be possibly destructive. You have the option to place those actions out of reach from those users by requiring an additional PIN authentication and required note entry.

Configure settings for restricted actions by navigating to **Groups & Settings** ▸ **All Settings** ▸ **System** ▸ **Security** ▸ **Restricted Actions**. From here you can require that certain actions require admins to enter a PIN and/or enter a note of explanation.

Enabling Send Message to All

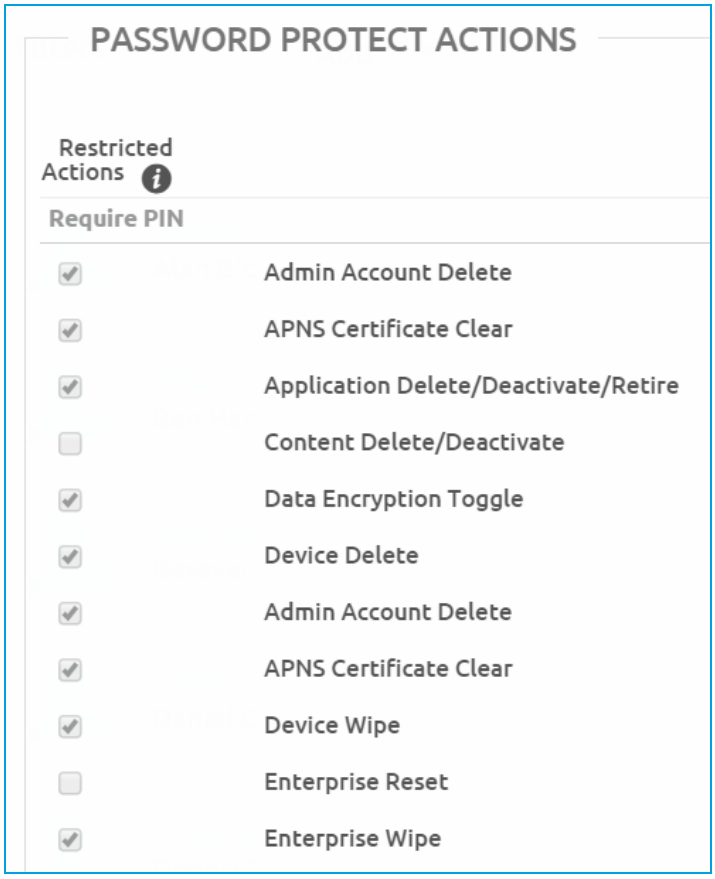
Enable this setting to allow a System Administrator to send a message to all devices in your deployment from the Device List View. See Using the Device List View for more information.

Selecting Password Protect Actions

For each action you choose to protect, select the appropriate **Require PIN** check box. This provides you with granular control over which actions you would like to make more secure. Note that some grayed out actions always require a PIN and thus you cannot de-select them.

Set the maximum number of failed attempts the system will accept before automatically logging out the session. If the max number of failed accepts is reached, you will need to log back into the AirWatch Admin Console and set a new Security PIN.

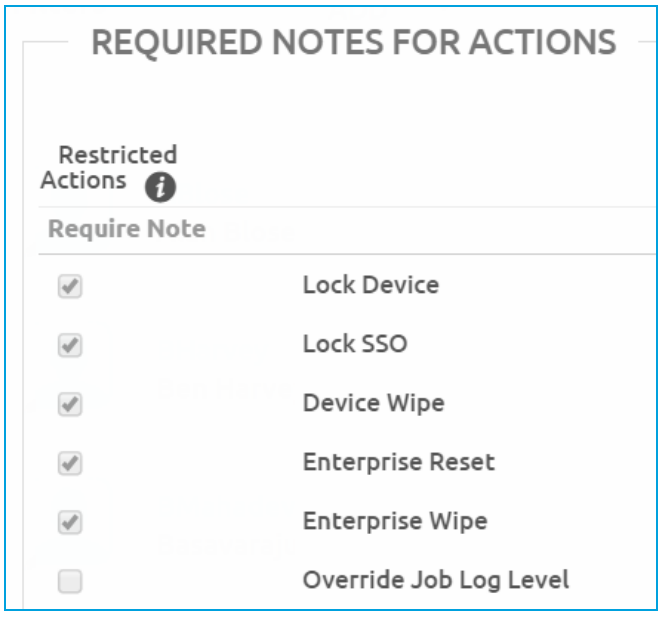
Note: The **Maximum invalid PIN attempts** setting must be between 1 and 5.



- **Admin Account Delete** – Protects from the deletion of an admin user account in **Accounts** ▸ **Administrators** ▸ **List View**.
- **APNs Certificate Clear** – Protects from the disabling of APNs for MDM in **Groups & Settings** ▸ **All Settings** ▸ **Devices & Users** ▸ **Apple** ▸ **APNs For MDM**.
- **App Scan Vendor Reset/Toggle** – Protects from the resetting (and subsequent wiping) of your app scan integration settings. This action is performed in **Groups & Settings** ▸ **All Settings** ▸ **Apps** ▸ **Application Integration** ▸ **App Scan**.
- **Application Delete/Deactivate/Retire** – Protects from the deletion, deactivation or retirement of an application in **Apps & Books** ▸ **Applications** ▸ **List View**.
- **Content Delete/Deactivate** – Protects from the deletion or deactivation of a content file in **Content** ▸ **List View**.
- **Data Encryption Toggle** – Protects from the Encryption of User Information setting in **Groups & Settings** ▸ **All Settings** ▸ **System** ▸ **Security** ▸ **Data Security**.
- **Delete Telecom Plan** – Protects the deletion of a telecom plan in **Telecom** ▸ **Plan List**.
- **Device Delete** – Protects from the deletion of a device in **Devices** ▸ **List View**.
- **Device Wipe** – Protects from any attempt to perform a device wipe from the Device List View or Device Details screens.
- **Enterprise Reset** – Protects from any attempt to enterprise reset a device from the **Devices Details** page of a Windows Mobile, rugged Android device, or QNX devices.

- **Enterprise Wipe** – Protects from any attempt to enterprise wipe a device from the **Devices Details** page of a device.
- **Enterprise Wipe (Based on User Group Membership Toggle)** – Protects from the enterprise wiping of a device when they are removed from user groups. This is an optional setting that you can configure under **Groups & Settings ▸ All Settings ▸ Devices & Users ▸ General ▸ Enrollment** on the **Restrictions** tab. If you **Restrict Enrollment to Configured Groups** on this tab, then you have the added option of enterprise wiping a device when they are removed from a group. For more information, see the Configuring Enrollment Restrictions section.
- **Organization Group Delete** – Protects from any attempt to delete the current Organization Group from **Groups & Settings ▸ Groups ▸ Organization Groups ▸ Organization Group Details**.
- **Profile Delete/Deactivate** – Protects from any attempt to delete or deactivate a profile from **Devices ▸ Profiles ▸ List View**.
- **Provisioning Product Delete** – Protects from any attempt to delete a provisioning Product from **Devices ▸ Products ▸ List View**.
- **Provisioning Product (New) Delete** – Protects from any attempt to delete a provisioning Product from **Devices ▸ Products (New) ▸ List View**.
- **Revoke Certificate** – Protects from any attempt to revoke a certificate from **Devices ▸ Certificates ▸ List View**.
- **Secure Channel Certificate Clear** – Protects from any attempt to clear an existing secure channel certificate from **Groups & Settings ▸ All Settings ▸ System ▸ Advanced ▸ Secure Channel Certificate**.
- **User Account Delete** – Protects from any attempt to delete a user account from **Accounts ▸ Users ▸ List View**.

In addition, you can require admins to enter notes via the **Require Note** check box and explain their reasoning when performing these actions.



- **Lock Device** – Require a note for any attempt to lock a device from the **Device List** View or **Device Details** screens.
- **Lock SSO** – Require a note for any attempt to lock an SSO session from the **Device List** View or **Device Details** screens.
- **Device Wipe** – Require a note for any attempt to perform a device wipe from the **Device List** View or **Device Details** screens.
- **Enterprise Reset** – Require a note for any attempt to enterprise reset a device from the **Devices Details** page of a Windows Mobile or rugged Android device.
- **Enterprise Wipe** – Require a note for any attempt to enterprise wipe a device from the **Devices Details** page of a device.

Integrating with Other Enterprise Systems

Take advantage of advanced MDM functionality by integrating your AirWatch environment with other existing enterprise infrastructure, such as email management with SMTP, Directory Services and content management with repositories such as SharePoint and other network file shares.

AirWatch can integrate with the following internal components:

- **Email Relay (SMTP)** – Provide highest level of security, visibility and control for mobile email.
- **Directory Services (LDAP/AD)** – Take advantage of existing corporate groups to manage users and devices.
- **Microsoft Certificate Services** – Utilize existing Microsoft certificate infrastructure for AirWatch deployment.
- **Simple Certificate Enrollment Protocol (SCEP PKI)** – Configure certificates for Wi-Fi, VPN, Microsoft EAS and more.
- **Email Management Exchange 2010 (PowerShell)** – Securely connect AirWatch to enforce policies with corporate email servers.
- **BlackBerry Enterprise Server (BES)** – Integrate with BES for streamlined BlackBerry management.
- **Third-party Certificate Services** – Import existing certificate management systems to be managed within the AirWatch Admin Console.
- **Lotus Domino Web Service (HTTPS)** – Access established Lotus Domino content and features through your AirWatch deployment.
- **Content Repositories** – Integrate with SharePoint, Google Drive, SkyDrive, file servers and network shares.
- **Syslog (Event log data)** – Export event log data to be viewed across all integrated servers and systems.
- **Corporate Networks** – Configure Wi-Fi and VPN network settings and provision device profiles containing user credentials for access.
- **System Information and Event Management (SIEM)** – Record and compile device and console data to ensure security and compliance with regulations and corporate policies.

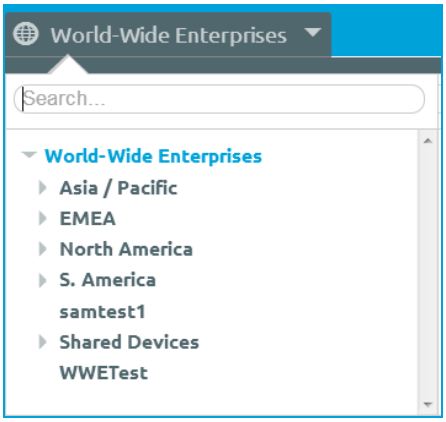
For more information on how to integrate AirWatch with these infrastructures, see the **AirWatch Cloud Connector Guide**, the **AirWatch Mobile Access Gateway Guide** and the Syslog section of the **Reports & Analytics Guide**, available via AirWatch Resources.

Organization Groups

Overview

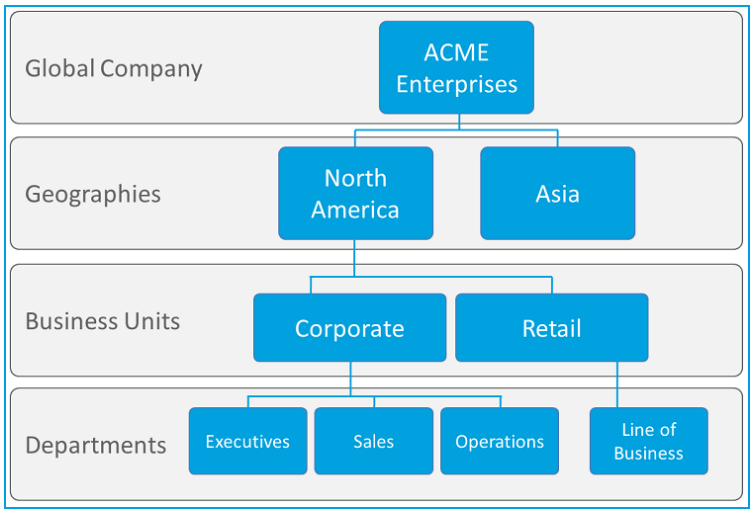
AirWatch identifies users and establishes permissions using Organization Groups, which you can view by navigating to **Groups & Settings ▸ Groups ▸ Organization Groups ▸ List View** or via the Organization Group drop-down list.

With Organization Groups, you can establish an MDM hierarchy identical to your organization's internal hierarchy. Alternatively, you may choose to establish Organization Groups depending on features and content that will be accessed from sets of devices.



Organization groups allow you to:

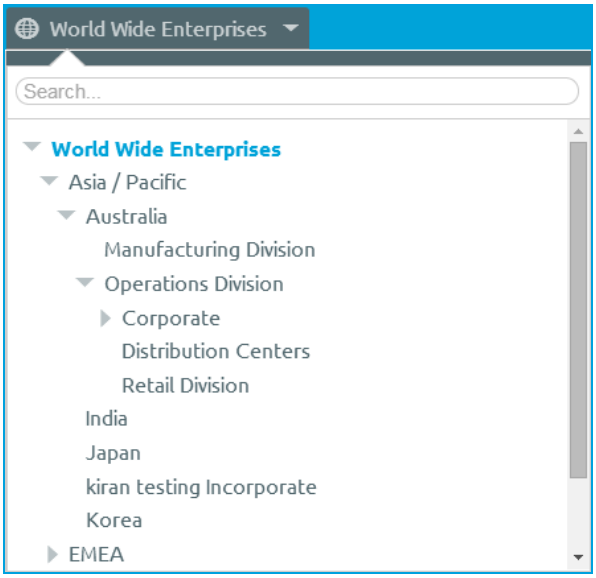
- Build groups for entities within your organization.
- Customize hierarchies with parent and child levels.
- Integrate with multiple internal infrastructures at the tier level.
- Delegate role-based access and management based on multi-tenant structure.



Accommodating functional, geographic and organization entities, the use of Organization Groups enables a multi-tenancy solution, such as:

- **Scalability** – Flexible support for exponential growth.
- **Multi-tenancy** – Create groups that function as independent environments.
- **Inheritance** – Streamline the setup process by setting child groups to inherit parent configurations.

Organization Group Setup Considerations



Using the example of the Organization Group drop-down list to the left, any profiles, features, applications and other MDM settings can be set at the top World-Wide Enterprises level.

Then, settings can be inherited down to child Organization Groups, such as **Asia/Pacific** and **EMEA** or even further down to **Australia ▸ Manufacturing Division** or **Australia ▸ Operations Division ▸ Corporate**.

Alternatively, you may choose to override settings at a lower level and alter only settings you want to change or keep. These settings can be altered and/or carried down at any level.

Before setting up your Organization Group hierarchy in the AirWatch Admin Console, decide the layout of the groupings first to best make use of settings, applications and resources. For example, review the following configuration options:

- **Delegated Administration** – Do you want a subgroup to be maintained by a sub-administrator? You can delegate administration of sub-groups to lower level administrators by restricting their visibility to a lower Organization Group.

Retail Company
LA store
NY store

– **Corporate administrators** have access here, and can view everything in the environment.
– **LA manager** has access here and can manage only those devices.
– **NY manager** has access here and can manage only those devices.

- **System Settings** – Settings can be applied at different levels in the Organization Group tree and inherited down. They can also be overridden at any level. Settings include device enrollment options, authentication methods, privacy settings and branding.

Shipping Company
Delivery Drivers
Warehouse Scanners

– **Overall company** establishes enrollment against the company Acitve Directory server.
– **Driver devices** override the parent's authentication and allows token enrollment.
– **Warehouse devices** inherit the AD settings from the parent group.

- **Device Use Case** – Are there different device configurations to consider? Is there a particular group of devices that will receive access to certain configurations/applications/resources? A profile can be assigned to one or several Organization Groups. Devices in those groups can then receive that profile. Refer to the Profiles section for more information.

  Additionally, AirWatch recommends configuring devices using profile, application and content settings according to attributes such as device make and model, ownership type or user groups before creating organization groups.

– **Executive** devices cannot install applications and have access to the Wi-Fi sales network.

– **Sales** devices are allowed to install applications and have VPN access.

Override vs Inherit Setting

The hierarchy of your structure determines which Organization Groups are children and which Organization Groups are parents but only with the addition of repositories and applications can you elect to override this native inheritance.

Adding repositories and applications can be done such that they inherit parent group settings down through all child groups below. Alternatively, you may override inheritance at each group level, if you so choose. For more information on setting up repositories and applications, please see the **Mobile Content Management (MCM) Guide** and the **Mobile Application Management (MAM) Guide** respectively, each available via AirWatch Resources.

In This Section

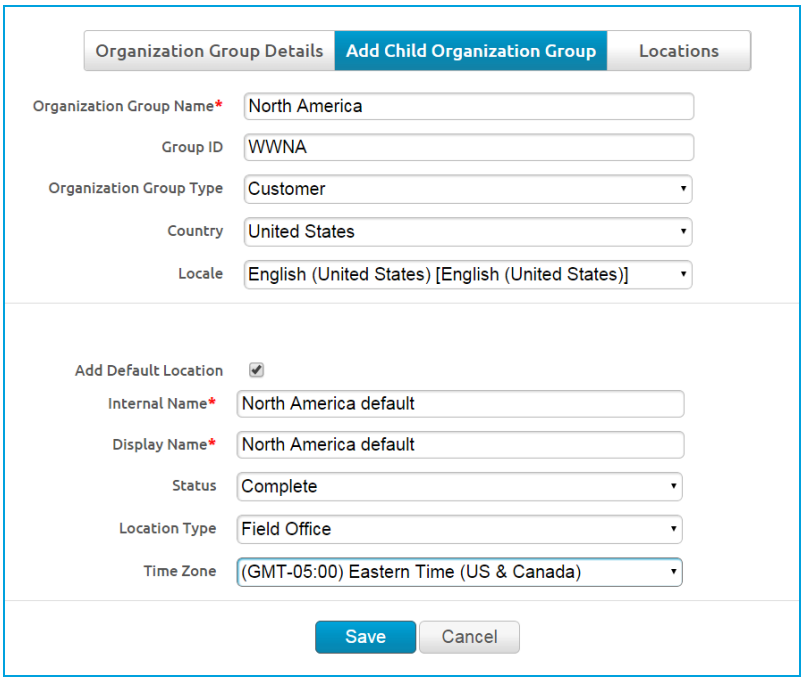
- Creating Organization Groups – Walks through the steps to create a new Organization Groups as well as child Organization Groups.
- Comparing Organization Groups Using Settings Comparison – Enables you to compare one organization group's entire list of settings with another organization group, including an option to only show the differences.

Creating Organization Groups

Create an Organization Group for each business entity where devices are deployed:

1. Navigate to **Groups & Settings** ▸ **Groups** ▸ **Organization Groups** ▸ **Organization Group Details**
2. Select the **Add Child Organization Group** tab.
3. Specify the **Organization Group Name** and **Group ID** for the new group. Group IDs are used during enrollment to group devices to the appropriate Organization Group.

   See Configure Enrollment Options for details about Group IDs as used in Organization Groups.
4. Select the **Organization Group Type**. Certain system settings, such as Wipe Protection, and certain features, such as Personal Content, DEP, Telecom, and so on, can only be configured at **Customer** level organization groups. In addition, Global is only available for certain deployments. Other than Customer, Partner, and Global, the types are simply for metadata purposes and do not serve a specific purpose.
5. Add region information and select **Save**.



Comparing Organization Groups Using Settings Comparison

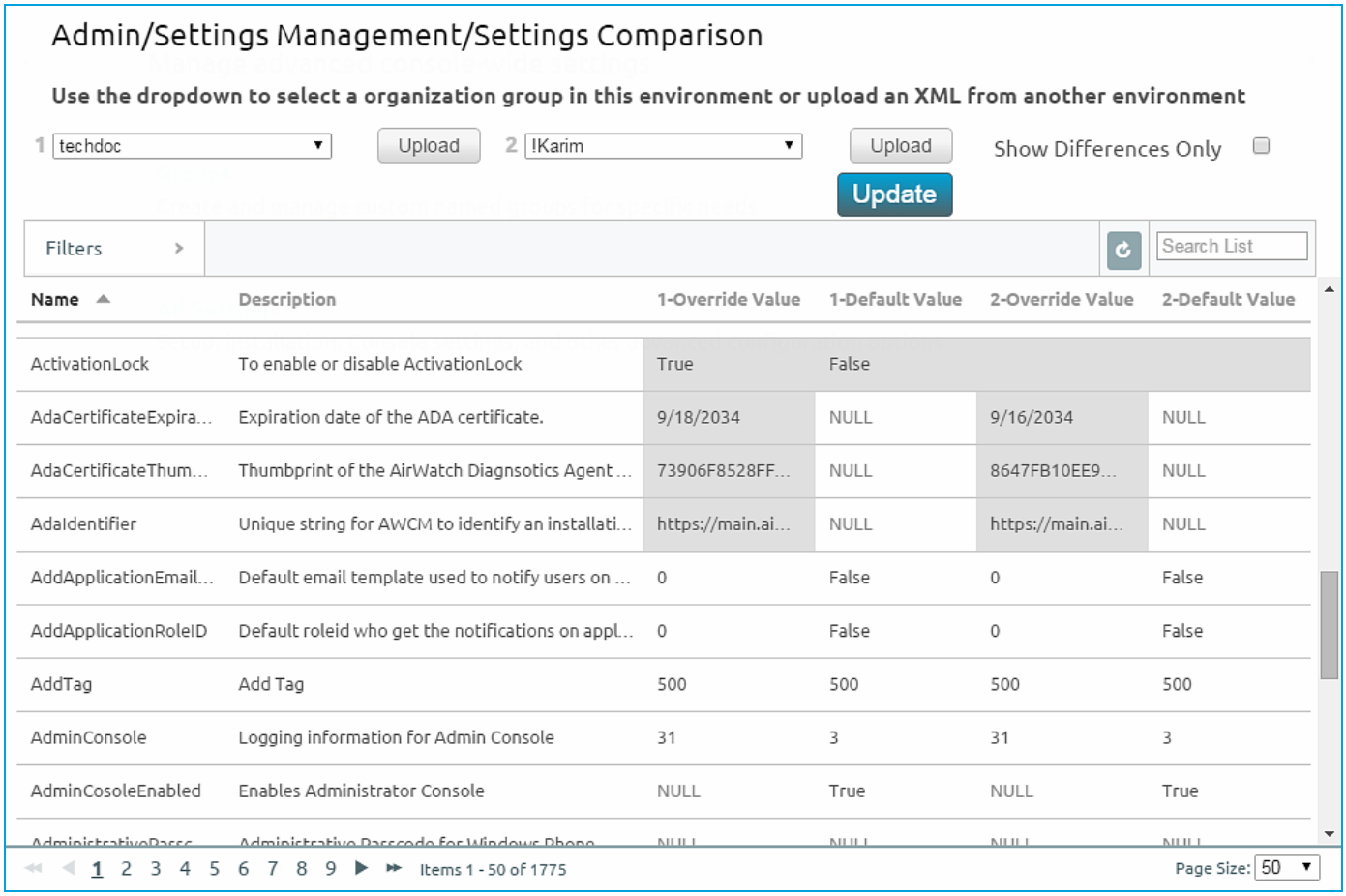
Note: This Organization Group Compare feature is only available for On-Premise customers.

As an AirWatch Administrator, you may find it useful to compare the settings of one Organization Group to another. This may be for troubleshooting purposes or to simply check for consistency.

In addition to being able to compare two Organization Groups in your environment, you can upload XML files containing the OG settings from different AirWatch software versions.

For example, once a User Acceptance Testing (UAT) server has been configured and tested and the production server is ready for an upgrade, the Settings Comparison feature will enable the UAT settings to be compared with the production settings directly, eliminating the possibility of a difference in configuration causing problems.

A **Filter** can be applied to the comparison results enabling you to display only those groups of settings you are interested in comparing. A **Search** function is also available if you want to check a single setting by name.



Compare two Organization Groups by taking the following steps:

1. Navigate to **Groups & Settings** ▸ **All Settings** ▸ **Admin** ▸ **Settings Management** ▸ **Settings Comparison**.
2. Select an Organization Group in your environment from the left drop-down menu (labeled with the numeral **1**) or upload the XML settings file by selecting the **Upload** button and choosing an exported Organization Group setting XML file.
3. Select the Organization Group to which you would like to compare on the right drop-down menu (labeled with the numeral **2**).
4. Select the **Update** button to display a listing of all settings for both selected organization groups. Differences between the two sets of OG settings will automatically be highlighted, as shown above. You may optionally enable the **Show Differences Only** check box, which displays only those settings that apply to one Organization Group but not the other. Individual settings that are empty (or not specified) will display in the comparison listing as 'NULL'.

Smart Groups

Smart Groups are customizable groups you define that determine which platforms, devices and end users receive an application, book, compliance policy, device profile, video channel or product provision. While Organization Groups are typically defined by geographical location, business unit and department, Smart Groups provide you the flexibility to deliver content and settings by device platform, model, operating system, device tag or user group. You can even deliver content to individual users across multiple Organization Groups.

While you can create Smart Groups when you upload content and define settings, their modular nature means you can create them at any time so they are available to be assigned later.

The main benefit of Smart Groups is their re-usability. Rather than specifying a new assignment every time you add new content or define a new profile or policy, you can configure a Smart Group once and apply it where needed.

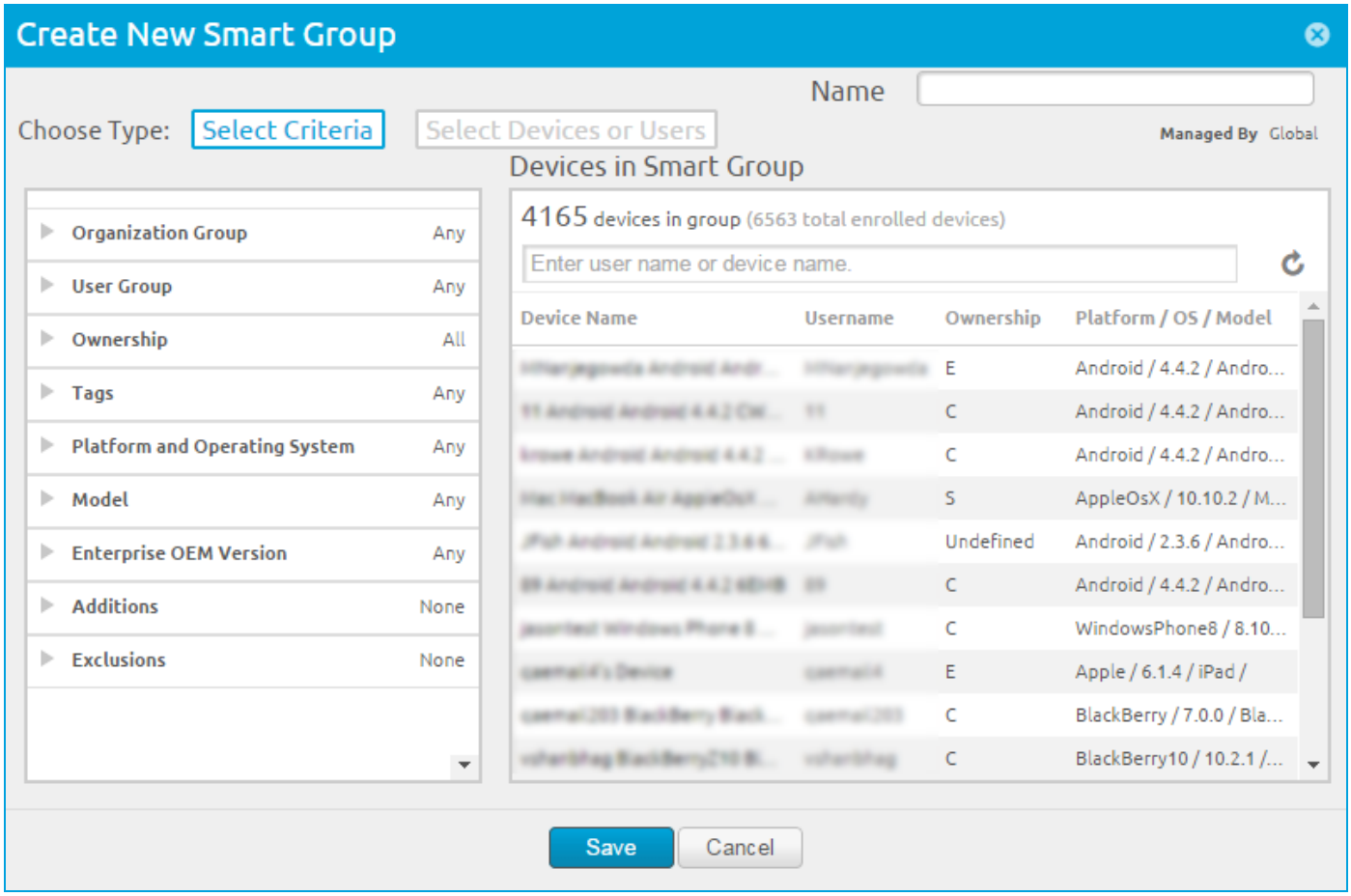
Note: For detailed instructions on how to integrate your pre-7.3 policies and profiles to utilize Smart Groups, see the Smart Groups Migration tech note (https://resources.air-watch.com/view/m99rhmjrrdb4dfk92bcz/en), available via AirWatch Resources.

In This Section

- Creating a Smart Group – Explains how to create a new Smart Group.
- Assigning a Smart Group – Details how to assign a Smart Group to applications, books, profiles, policies and provisions; also, how excluding Smart Groups can be beneficial.
- Managing Smart Groups – Explores how to edit, delete and unassign Smart Groups and how to view Smart Group assignments.

Creating a Smart Group

Before you can assign a Smart Group to an application, book, compliance policy, device profile, video channel or product provision, you must first create one.

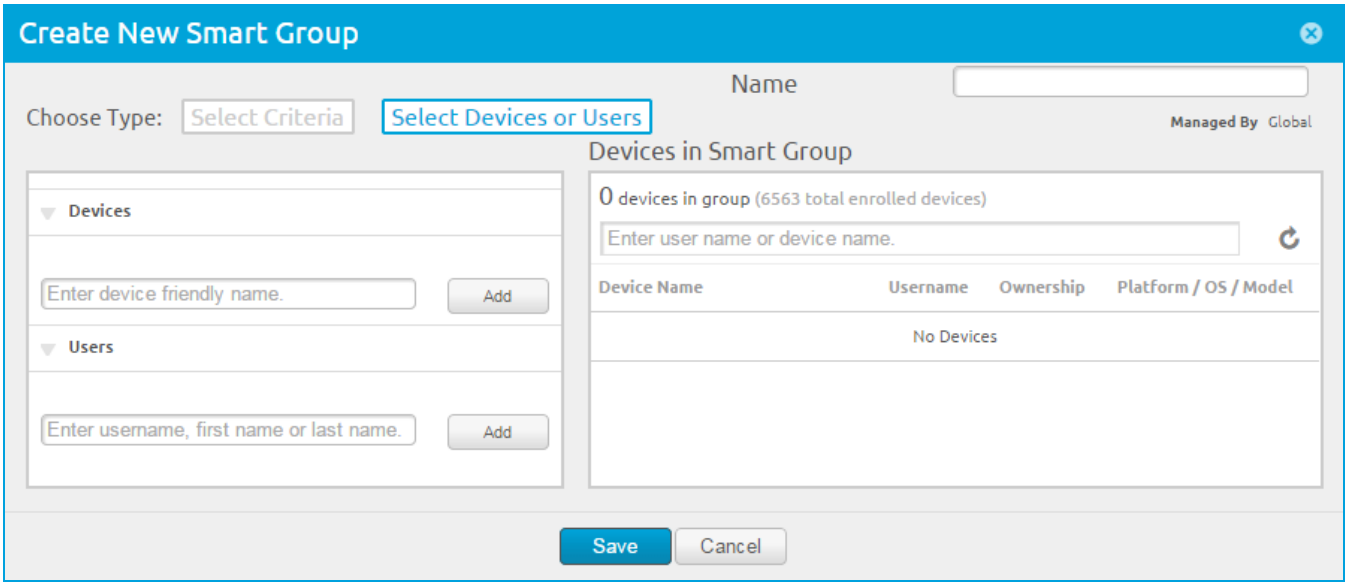


Take the following steps to create a Smart Group:

1. Choose the applicable **Organization Group** to which your new Smart Group will apply and be managed from.
2. Navigate to **Groups & Settings** ▸ **Groups** ▸ **Smart Groups** and then select **Add Smart Group**.
3. Enter a **Name** for the Smart Group.
4. Configure the Smart Group type by choosing between **Select Criteria** and **Select Devices or Users**.

- The **Select Criteria** option works best for groups with large numbers (more than 500 devices) that receive general updates because the inherent details of these groups can reach all endpoints of your mobile fleet.
    - In the **Select Criteria** type, select qualifying parameters to add in the Smart Group. Parameters include **Organization Group**, **User Group**, **Ownership**, **Tags**, **Platform and Operating System**, **Model**, and **Enterprise OEM (Original Equipment Manufacturer) Version**. You can also add and exclude specific devices and users in the **Additions** and **Exclusions** sections.

> **Note:** While Platform is a criterion within a Smart Group, the Platform configured in the device profile or compliance policy will always take precedence over the Smart Group's platform. For instance, if a device profile is created for the iOS platform, the profile will only be assigned to iOS devices even if the Smart Group includes Android devices.



- The **Select Devices or Users** option works best for groups with smaller numbers (500 or less devices) that receive sporadic, although important, updates because of the granular level at which you can select group members.
    - In the **Select Devices or Users** type, which you utilize to assign content and settings to special cases *outside* of the general enterprise mobility criteria, enter the device friendly name in **Devices** and username (first name or last name) in **Users**. You must **Add** at least one device or user or you cannot save the Smart Group.

> **Note:** Switching between **Select Criteria** and **Select Devices or Users** erases any entries and selections you may have made.

> **Note:** A 500 device maximum has been placed on the **Select Devices or Users** option of creating Smart Groups. If you encounter a scenario where you must add more than 500 devices while utilizing the **Select Devices or Users** option, consider instead enabling the **Select Criteria** option for the main bulk of devices that share a general criteria and, if required, create a separate **Select Devices or User** smart group for those devices that fall outside the general criteria.

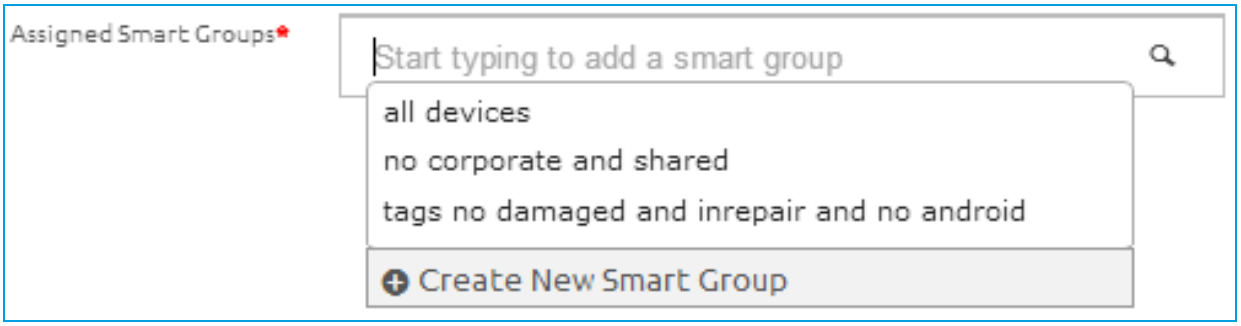
5. Click **Save** when finished.

Assigning a Smart Group

Before Smart Groups take effect, you must assign them to an application, book, compliance policy, device profile, video channel or product provision.

Take the following steps to assign a Smart Group:

1. Complete the **Assigned Smart Groups** drop-down field as it appears during the process of adding or creating an application, book, compliance policy, device profile, video channel or product provision.

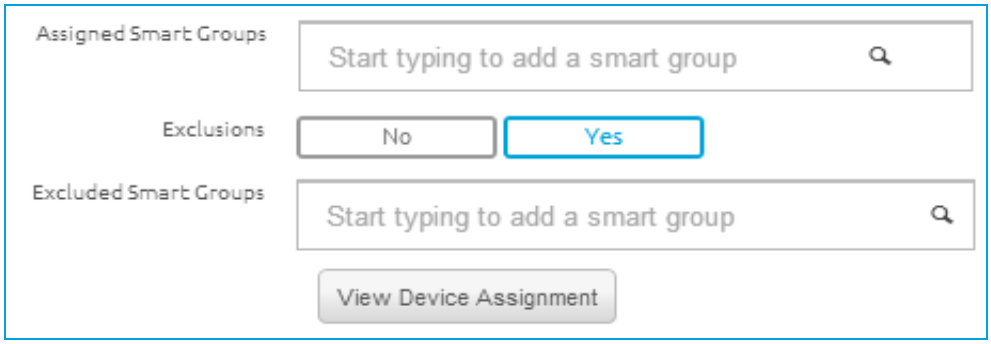


2. Select a Smart Group from the drop-down list. Smart Groups available for selection are only those managed within the Organization Group (OG) to which the application, book, compliance policy, device profile, video channel or product provision is being added, or to a child OG below it.
3. If no smart group matches the desired assignment criteria, then select the **Create New Smart Group** option. You can assign more than one Smart Group per application, book, compliance policy, device profile, video channel or product provision.
4. Select **Save** to include the assignment.

Excluding Smart Groups in Profiles and Compliance Policies

Since Smart Groups apply to not only apps, books, video channels and products but also device profiles and compliance policies, the ability to exclude selected Smart Groups provides you with greater flexibility.

For example, if you want a compliance policy for all users in the company except executives, you can easily accomplish this by assigning a smart group to the policy that includes all users, and exclude a smart group that contains only the executives.



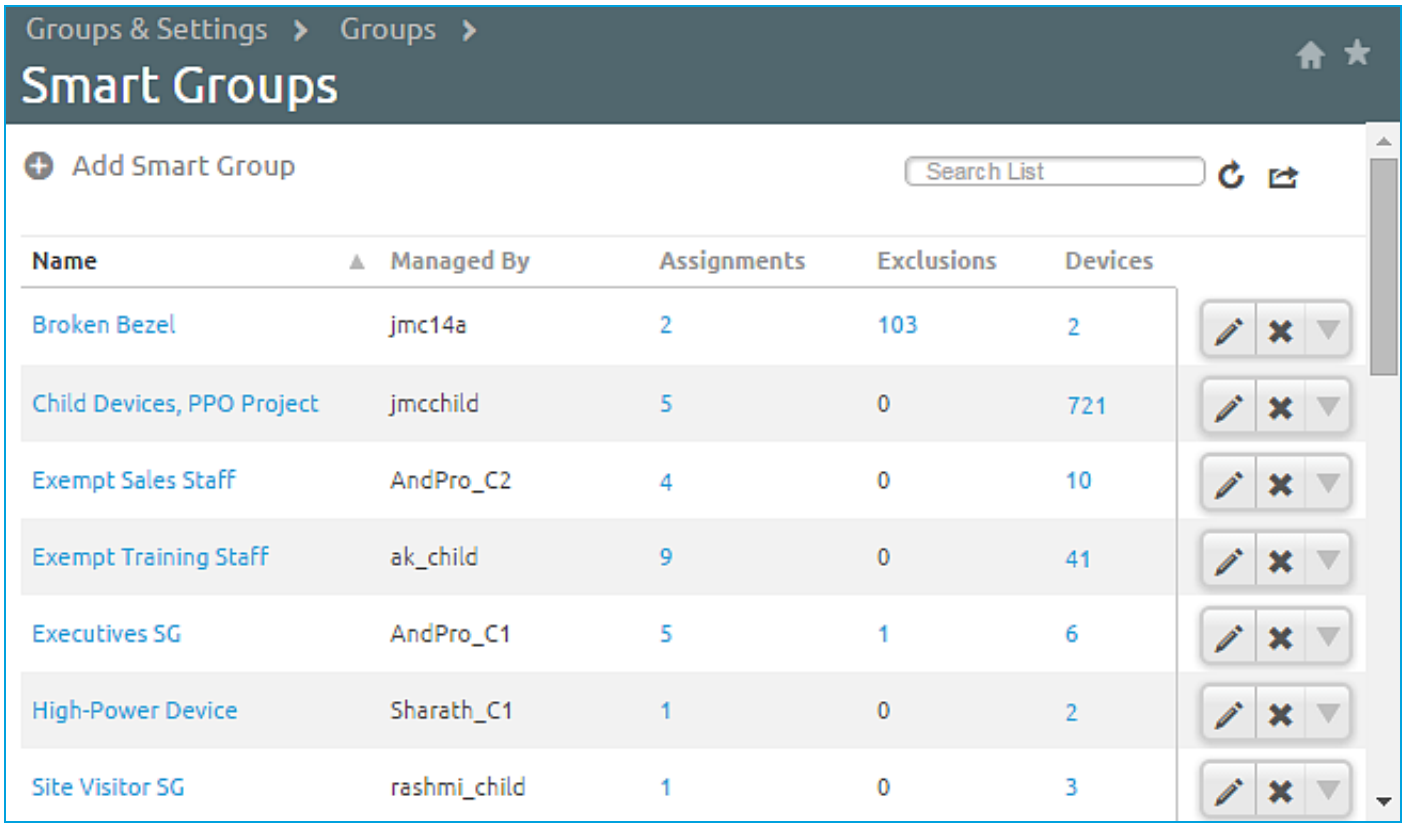
To exclude a Smart Group while adding an app, book, video channel, product provision or creating a profile or policy:

1. Select **Yes** next to the **Exclusion** field and a new field will appear titled **Excluded Smart Groups**.
2. Select those Smart Groups you wish to exclude from the assignment of this profile or policy.
3. Select the **View Device Assignment** button to preview the affected devices.

> **Note:** If you select the same smart group in both the **Assigned Smart Groups** and **Excluded Smart Groups** fields, then the profile or policy will fail to save.

Managing Smart Groups

Manage your Smart Groups by Editing, Assigning, Unassigning, Excluding and Deleting them with the AirWatch Admin Console. Navigate to **Groups & Settings** ▸ **Groups** ▸ **Smart Groups** to view the entire listing of Smart Groups.



The columns **Name**, **Assignments**, **Exclusions** and **Devices** each feature selectable links which you can use to view detailed information. Selecting links in the **Assignments** or **Exclusions** columns display the **View Smart Group Assignments** screen.

Selecting a link in the **Devices** column loads up the **Devices** ▸ **List View** with only those devices included in the Smart Group.

Editing a Smart Group

Any edits you apply to a Smart Group will affect all policies and profiles to which that Smart Group is assigned.

For example, a Smart Group for executives is assigned to a compliance policy, device profile, and two internal apps. If you wish to exclude some of the executives, then simply edit the smart group by specifying **Exclusions**. This action will have the effect of removing not only the two internal apps but also the compliance policy and device profile from those excluded devices.

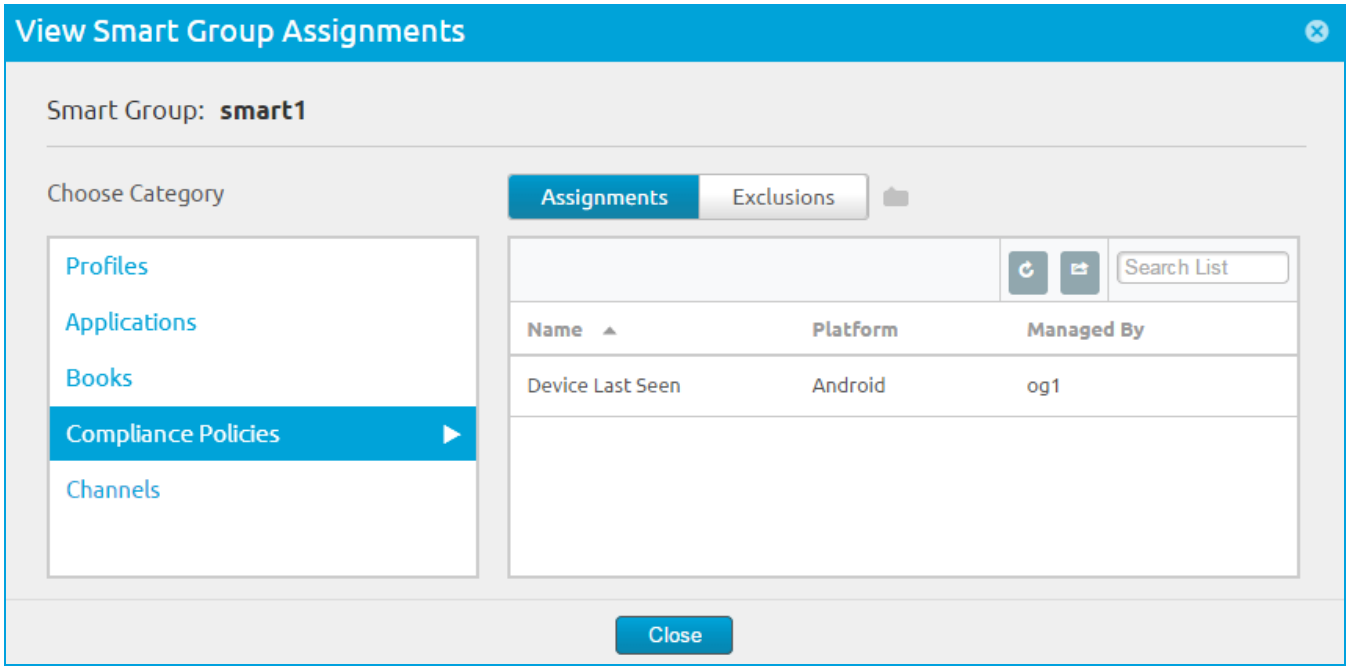
Take the following steps to edit a Smart Group:

1. Navigate to **Groups & Settings** ▸ **Groups** ▸ **Smart Groups**.
2. Select the **Edit** icon  from the **Action** menu to the right of the listed Smart Group that you want to edit. The **Edit Smart Group** screen will display with its existing settings.

3. Make changes to either the **Criteria** or the **Devices and Users** (depending upon which type the Smart Group was saved with).
4. Select the **Next** button and the **View Smart Group Assignments** page displays, allowing you to review which profiles, apps, books, provisions and policies may be added or removed from the devices as a result.
5. Save your Smart Group edits by selecting the **Publish** button on the View Smart Group Assignments page. All profiles, apps, books, provisions and policies tied to this smart group will now change its device assignment based on this edit.

View Smart Group Assignments

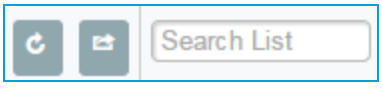
As a convenience, you can confirm the specific profile, app, book, channel and compliance policy that are included in (as well as excluded from) the assigned Smart Group.



Navigate to the Smart Group listing in **Groups & Settings** ▸ **Groups** ▸ **Smart Groups** and locate a Smart Group that has been assigned to at least one device. Look in the **Assignments** column for a clickable, hyperlinked number and select it to open the **View Smart Groups Assignments** screen.

Only those categories that contain **Assignments** or **Exclusions** in the Smart Group are displayed.

Above the header row in the **View Smart Group Assignments** screen are three new tools to help you confirm the specific profile, app, book, channel and compliance policy.



- There is a **Refresh** button which re-sends a query to retrieve an up-to-date listing of assignments and exclusions.
- An **Export** button enables you to produce a full listing of profiles, apps, books, channels or policies to a .csv file (comma-separated values) that you can view and analyze within Excel.
- A **Search List** bar helps you locate a specific assignment or exclusion.

Deleting a Smart Group

Navigate to **Groups & Settings** ▸ **Groups** ▸ **Smart Groups** and locate the Smart Group you wish to delete from the listing. Select Delete (**X**) from the actions menu.

Note: You cannot delete a Smart Group if it is currently assigned.

Unassigning a Smart Group

You may unassign a Smart Group from an application, book, channel, policy, profile or product because you wish to remove the Smart Group from those settings or because you simply wish to delete the Smart Group.

1. Navigate to the edit screens (paths below) to unassign Smart Groups from applications, books, compliance policies, device profiles or product provisions:
   - **Applications** – Navigate to **Apps & Books** ▸ **Applications** ▸ **List View** and select the **Public** or **Internal** tab.
   - **Books** – Navigate to **Apps & Books** ▸ **Books** ▸ **List View** and select the **Public** or **Internal** tab.
   - **Channels** – Navigate to **Content** ▸ **Video** ▸ **Channels**.
   - **Compliance Policy** – Navigate to **Devices** ▸ **Compliance Policies** ▸ **List View**.
   - **Device Profile** – Navigate to **Devices** ▸ **Profiles** ▸ **List View**.
   - **Product Provision** – Navigate to **Devices** ▸ **Products** ▸ **List View**.
2. Locate the content or setting from the listing and select the **Edit** icon  from the actions menu.
3. Select the **Assignment** tab or locate the **Assigned Smart Groups** field.
4. Select Delete (**X**) next to the Smart Group you wish to unassign. This action will not delete the Smart Group, rather it simply removes the Smart Group assignment from the saved setting.
5. Take the normal steps to **Save** your changes.

Device Users

Overview

AirWatch manages devices by keeping track of the users of each device. Therefore, user accounts must also be created or integrated for devices to enroll into AirWatch. The AirWatch Admin Console allows you to establish a complete user infrastructure by providing configuration options for user authentication types, enterprise integration and ongoing maintenance.

In This Section

- Choosing User Security Types – Presents the pros and cons for the authentication options available to your organization.
- Creating Basic User Accounts – Walks through the simple steps to create a new User in the AirWatch Admin Console.
- Creating Directory-Based User Accounts – Walks through the process of adding a user from an existing directory service into AirWatch.
- Defining User Roles – Details how to set a default user role or change the role of a specific user.
- Managing User Accounts – Details the various management options for user accounts, including adding, importing, removing, deactivating and more.
- Using the Batch Import Feature – Details how to use the batch import feature to add multiple users or user groups at once.

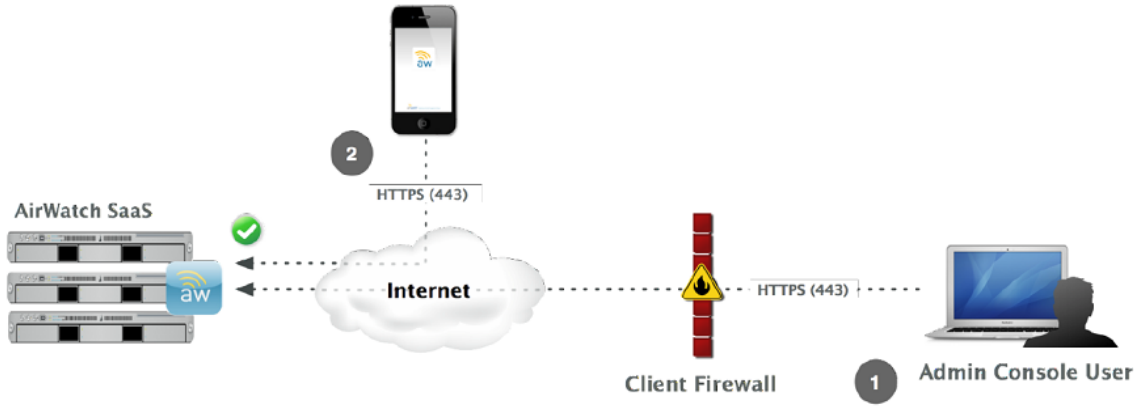
Choosing User Authentication Types

The type of user authentication you choose depends on the amount of back-end setup work required by the administrator and the amount of login steps required by the end user on the device at enrollment. If you want the enrollment process to be as simple as possible for the end user, the administrator must do more work to set up the process. Likewise, a lighter workload for the administrator means there is more setup to do by the end user.

Basic Authentication

Basic Authentication can be utilized by any AirWatch architecture but offers no integration to existing corporate user accounts.

- **Pros** – Can be used for any deployment method, requires no technical integration, and requires no enterprise infrastructure.
- **Cons** – Credentials only exist in AirWatch and do not necessarily match existing corporate credentials. Offers no federated security or single sign on. AirWatch stores all username and passwords.

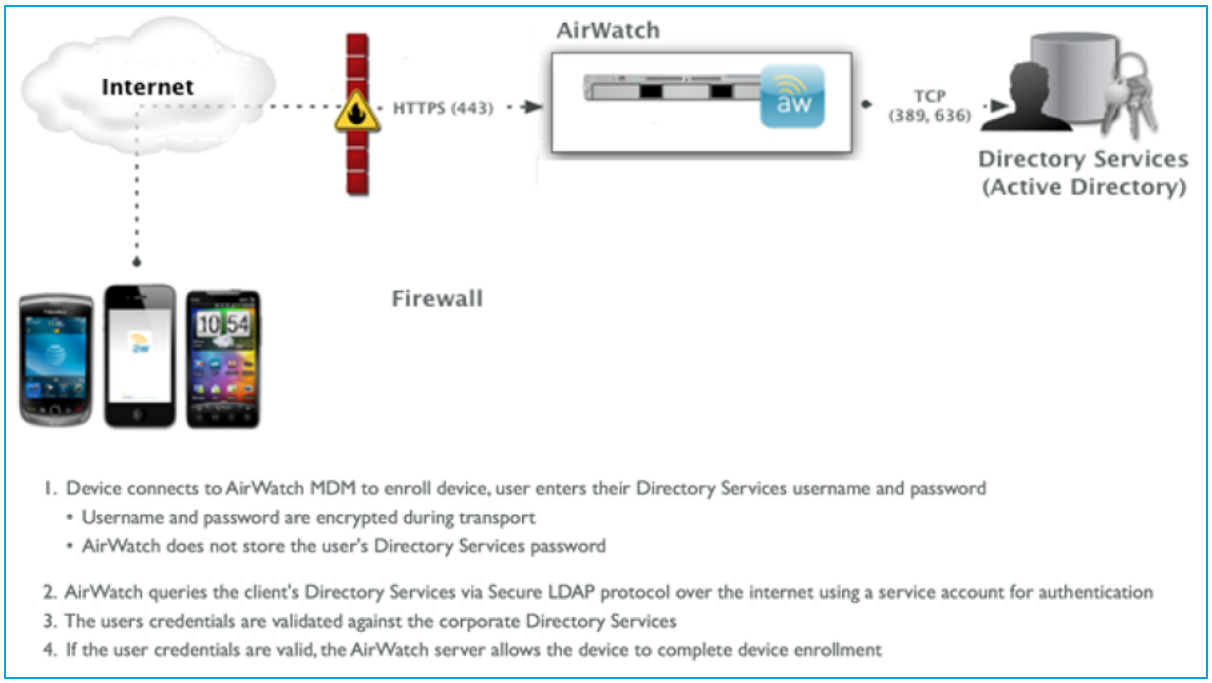


1. Console user logs into AirWatch SaaS using local AirWatch account for authentication (Basic Authentication)
   - Credentials are encrypted during transport
   - (e.g. username: jdoe@air-watch.com, password: abcd)
2. Device user enrolls device using local AirWatch account (Basic Authentication) credentials
   - Credentials are encrypted during transport
   - (e.g. username: jdoe2, password: 2557)

Active Directory / LDAP Authentication

Active Directory / Lightweight Directory Access Protocol (LDAP) authentication is utilized to integrate user and admin accounts of AirWatch with existing corporate accounts.

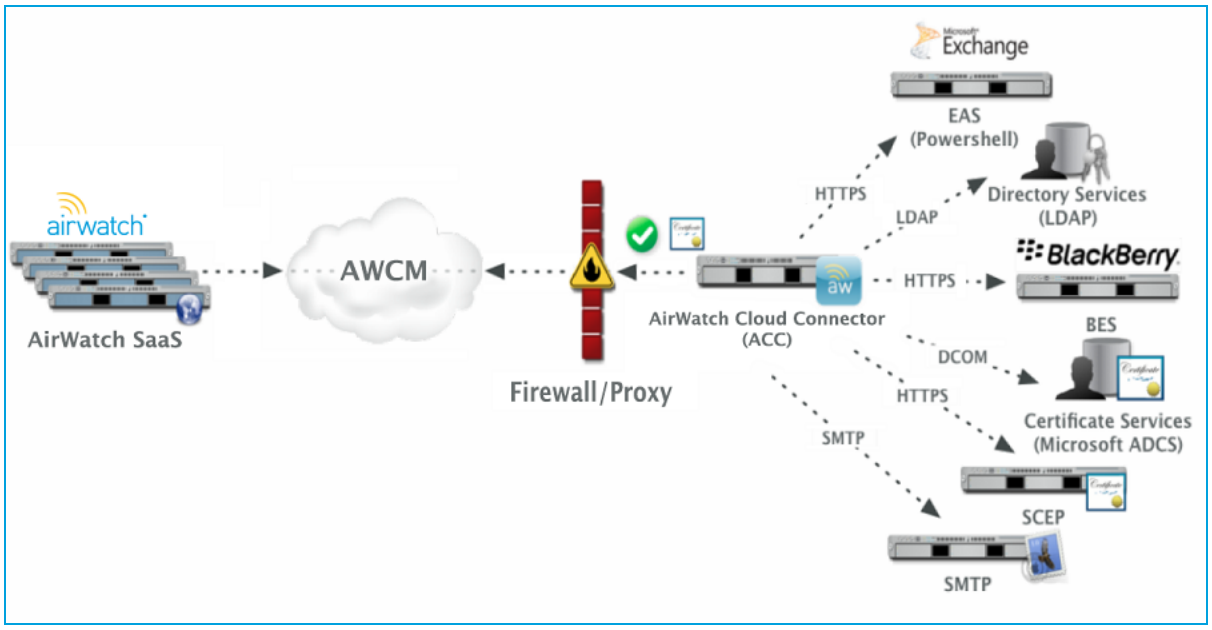
- **Pros** – End users now authenticate with existing corporate credentials. Secure method of integrating with LDAP / AD. Standard integration practice.
- **Cons** – Requires an AD or other LDAP server.



Active Directory / LDAP Authentication with AirWatch Cloud Connector

Active Directory / LDAP authentication with the AirWatch Cloud Connector provides the same functionality as traditional AD/LDAP authentication, but allows this model to function across the cloud for Software as a Service (SaaS) deployments. The Enterprise Integration Service also offers a number of other integration capabilities as shown below.

- **Pros** – End users authenticate with existing corporate credentials. Requires no firewall changes, as communication is initiated from the AirWatch Cloud Connector (ACC) within your network. Transmission of credentials is encrypted and secure. Also offers secure configuration to other infrastructure such as BES, Microsoft ADCS, SCEP and SMTP servers.
- **Cons** – Requires ACC to be installed behind the firewall or in a DMZ. Requires additional configuration.

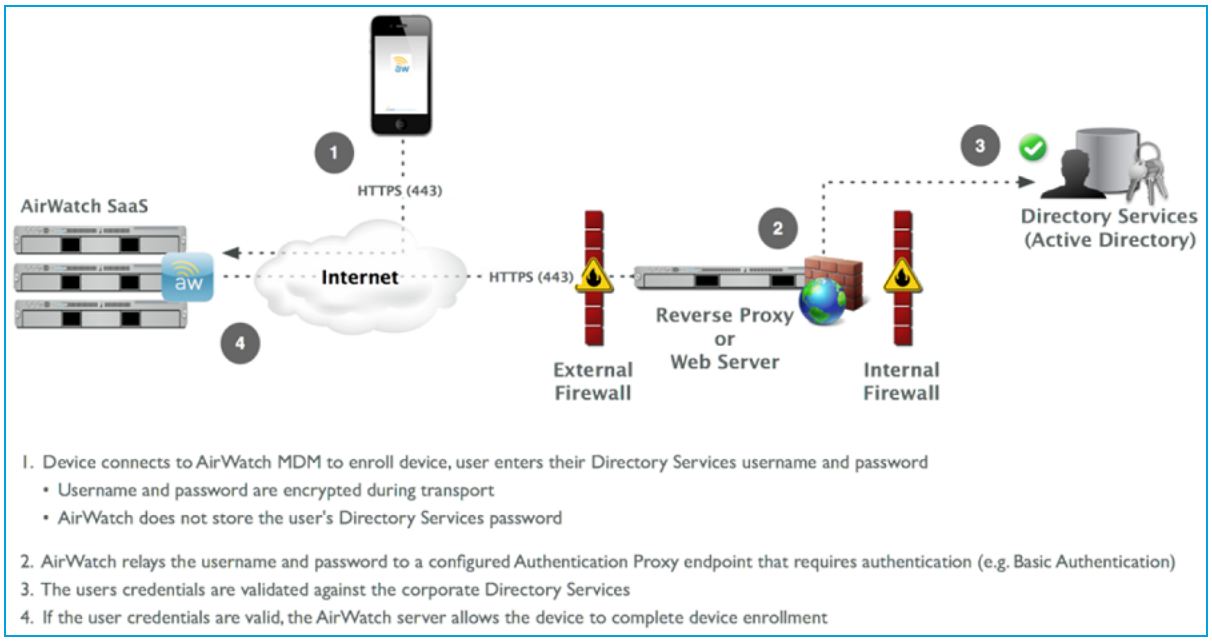


Note: For information on how to integrate yourAirWatch environment with these infrastructures, see the **AirWatch Cloud Connector Guide** document, available via AirWatch Resources.

Authentication Proxy

Authentication Proxy is an AirWatch proprietary solution delivering directory services integration across the cloud or across hardened internal networks. In this model, the AirWatch MDM server communicates with a publicly-facing web server or an Exchange ActiveSync Server that is able to authenticate users against the domain controller. This method can only be used when organizations have a public-facing web server with hooks into the corporate domain controller.

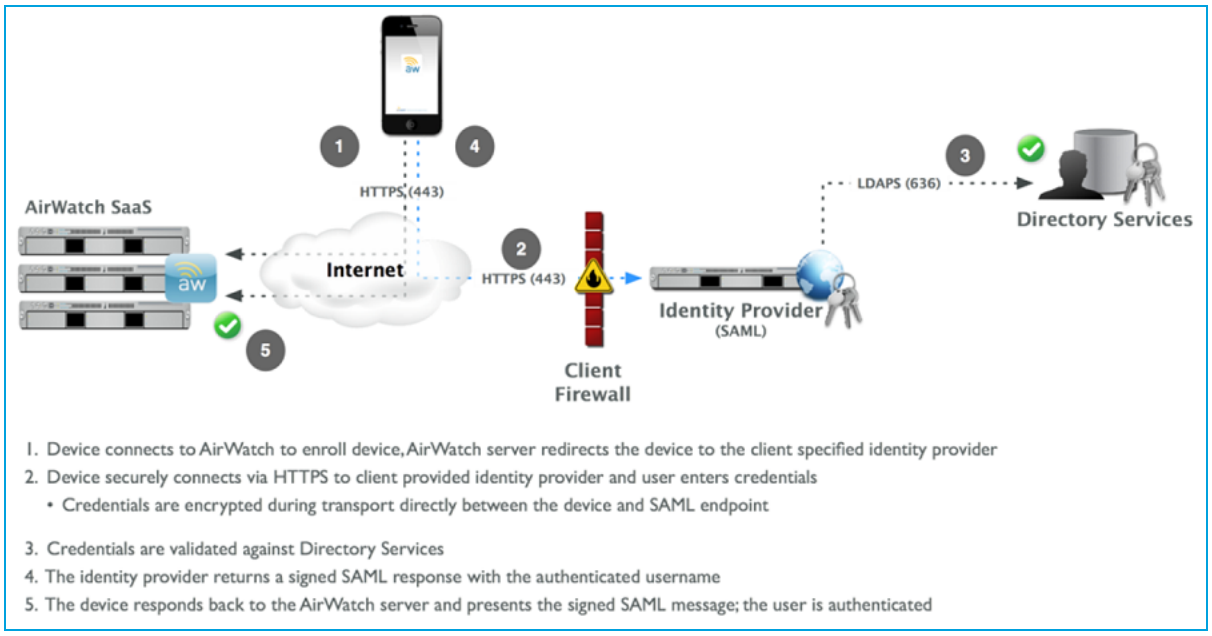
- **Pros** – Offers a secure method to proxy integration with AD/LDAP across the cloud. End users can authenticate with existing corporate credentials. Lightweight module that requires minimal configuration.
- **Cons** – Requires a public facing web-server or an Exchange ActiveSync server which ties into an AD/LDAP server. Only feasible for specific architecture layouts. Much less robust solution than ACC.



SAML 2.0 Authentication

Security Assertion Markup Language (SAML) 2.0 Authentication offers single sign on support and federated authentication. AirWatch never receives any corporate credentials. If an organization has a SAML Identity Provider server, SAML 2.0 integration is recommended.

- **Pros** – Offers single-sign on capabilities, authentication with existing corporate credentials and AirWatch never receives corporate credentials in plain-text.
- **Cons** – Requires corporate SAML Identity Provider infrastructure.



For information on how to integrate your AirWatch environment with a SAML provider, see the **AirWatch SAML Guide** document, available via AirWatch Resources.

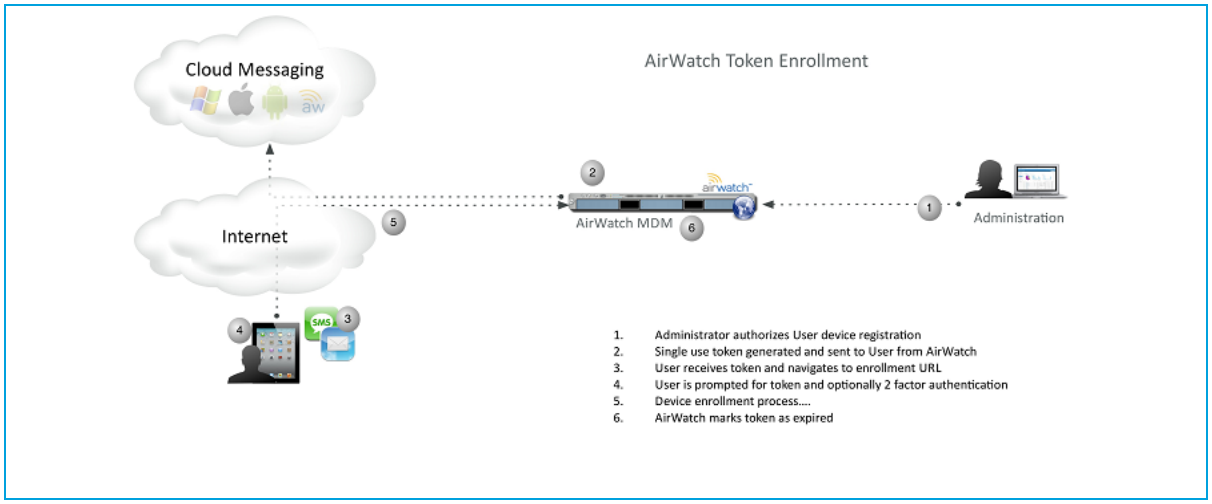
Token-based Authentication

Token-based authentication offers the easiest way for a user to enroll their device. With this enrollment setting, AirWatch generates a token, which is placed within the enrollment URL. For **single-token authentication**, the user accesses the link from the device to complete enrollment and the AirWatch server references the token provided to the user.

For additional security, set an expiration time (in hours) for each token to minimize potential for another user to take the device and gain access to any information and features available to that device.

You may also decide to implement two factor authentication to take end user identity verification a step further. With this authentication setting, the user must enter their username and password upon accessing the enrollment link with the provided token.

- **Pros** – Minimal work for end user to enroll and authenticate their device. Secure token usage by setting expiration. User doesn't need credentials for single-token authentication.
- **Cons** – Requires either Simple Mail Transfer Protocol (SMTP) or Short Message Service (SMS) integration to send tokens to device.



Note: SMTP is included with SaaS deployments.

Once AirWatch is integrated with a selected User Security Type, enable each security type for enrollment by navigating to **Devices ▸ Device Settings ▸ Devices & Users ▸ General ▸ Enrollment** in the **Authentication** tab and checking the appropriate check boxes for the **Authentication Mode(s)** field.

Creating Basic User Accounts

After you decide which Authentication Type you want to use, you can begin creating new users in the AirWatch Admin Console. How you do this will depend on which Authentication Type you use. For instance, if your authentication type is Basic, you would then create Basic User Accounts.

To add a Basic User account:

1. Navigate to **Accounts** ▸ **Users** ▸ **List View** ▸ **Add** ▸ **Add User**.
2. Fill in required fields, such as **Security Type**, **Username**, **Password**, **First Name**, **Last Name** and **Email Address**. You can also fill out additional information, such as a user's **Email Username** and **Email Password**.
3. Select the **Enrollment Organization Group**, which is the Organization Group that will be used to determine which profiles, apps, compliance policies, etc. apply to this user.
4. Select the **User Role**. To see the differences between Roles, navigate to **Accounts** ▸ **Users** ▸ **Roles** and select **View Role** for a particular role.
5. Select **Show advanced user details** to enter additional details, if necessary.
6. Leave **Enable Device Staging** unchecked unless this is a user who will be staging devices. See Device Staging for more information.
7. Select a **Message Template** that will be sent to the user for activation purposes.
8. Select **Save**.

Creating Directory-Based User Accounts

After you decide which Authentication Type you want to use, you can begin creating new users in the AirWatch Admin Console.

Every directory user you want to manage through AirWatch Mobile Device Management (MDM) must have a corresponding user account in the AirWatch Admin Console. You can directly add your existing directory services users to AirWatch using one of the following methods:

- Batch upload a file containing all your directory services users.
- Create AirWatch user accounts one at a time by entering the directory user's username and selecting **Check User** to auto-populate remaining details.

> **Note:** Do not import users and allow all directory users to self-enroll at the same time. The act of Batch importing automatically creates a user account.

This topic details creating user accounts one at a time. For an easy way to import Active Directory users in bulk, save time by Using the Batch Import Feature. To add a Directory-Based user account:

1. Navigate to **Accounts** ▸ **Users** ▸ **List View**.
2. Select **Add** ▸ **Add User**. The **Add / Edit User** page displays.
3. Select **Directory** as the **Security Type**.
4. Select the applicable domain from the **Domain** drop-down menu. The **Directory Name** field is pre-populated.
5. Enter the user's directory username in the **Username** field and select **Check User**. If the system finds a match, the user's information will be automatically populated. Ensure the **Enrollment Organization Group** and other details are correct.
6. Select **Save**.

Note: For more information about adding directory users to AirWatch, refer to the **AirWatch Directory Services Guide**, available via AirWatch Resources.

Defining User Roles

By defining user roles on the **Add/Edit Role** page you can set who has access to the Self Service Portal (SSP), what the initial SSP landing page will be and what actions logged-in users can perform. Creating multiple user roles is a time saving measure; making comprehensive configurations across different Organization Groups or changing the user role for a specific user at any time.

Define a User Role

In addition to the preset Basic Access and Full Access roles, you can also create customizable roles.

1. Navigate to **Accounts** ▸ **Users** ▸ **Roles** and click **Add**. Enter a **Name**, **Description** and select the **Initial Landing Page** of the SSP for users with this new role.

   Note: For existing User Roles, the default **Initial Landing Page** is the **My Devices** page.

2. Select from a list of options the level of access and control end users of this assigned role should have in the SSP.
3. Select **Save** when you are finished.

Configure a Default Role

A default role is the baseline role from which all user roles begin. Configuring a default role enables you to set the permissions and privileges users will automatically receive upon enrollment.

1. Navigate to **Devices** ▸ **Device Settings** ▸ **Devices & Users** ▸ **General** ▸ **Enrollment** and select the **Grouping** tab.
2. Select a **Default Role** to configure a default level of access end users should have in the SSP. These role settings are customizable by Organization Group.
3. Select **Save**.

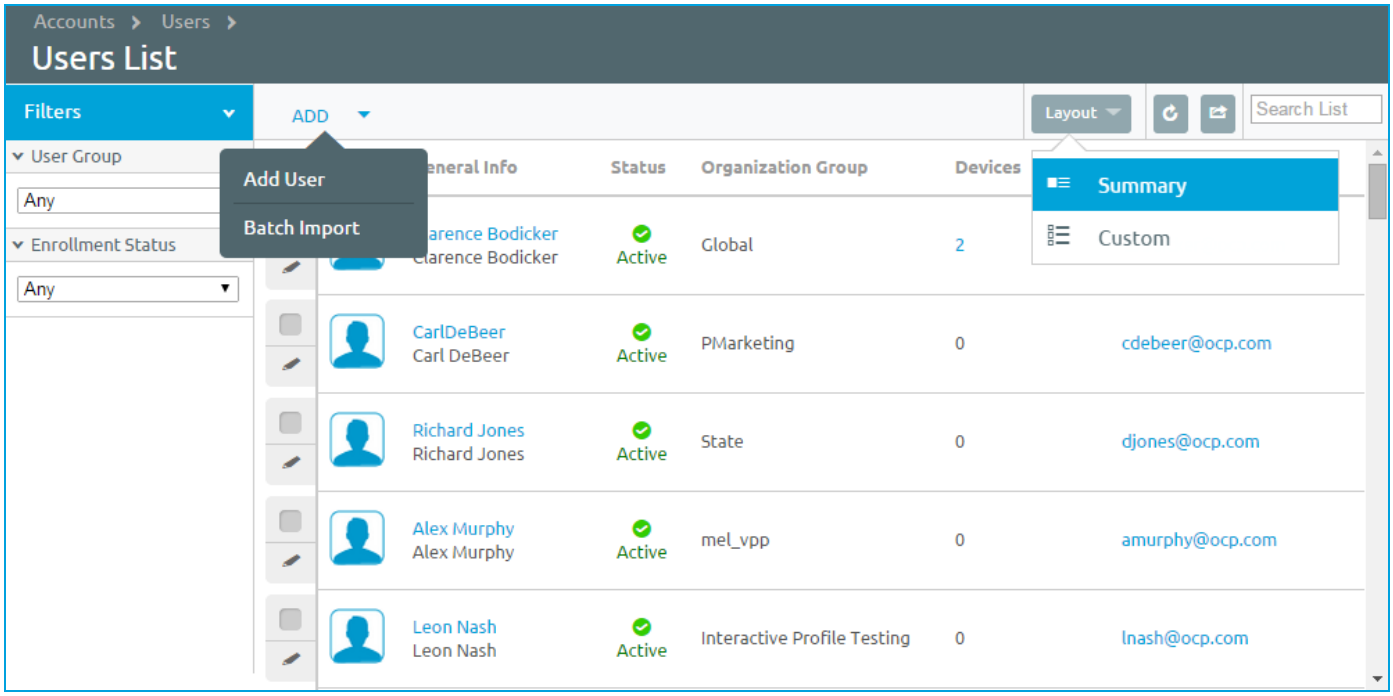
Set a Role for a Specific User

You can also edit the role for a specific user, for example, to grant or restrict access.

1. Select the appropriate Organization Group, navigate to **Accounts** ▸ **Users** ▸ **List View** and search for and select a user from the list. The **Edit User** screen displays.
2. Select **Edit**. Scroll down and select a **User Role** to set a role for this specific user.
3. Select **Save**.

Managing User Accounts

The **Users List** view page (**Accounts ▸ Users ▸ List View**) provides useful tools for common account maintenance and upkeep. Access the following options from the main **Users List**:

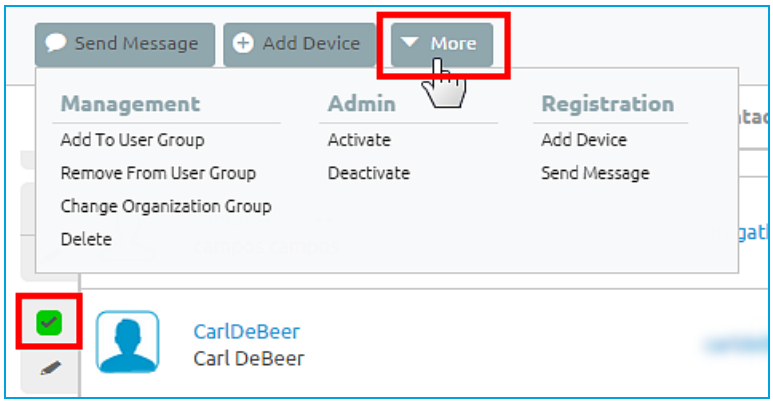


- **Filters** – Exclude entries from the **Users List** by selecting to view only the desired **User Groups** and/or **Enrollment Statuses**.
- **Add** button
  - **Add User** – Perform a one-off addition of a basic user account. Add a new employee or a newly-promoted employee that needs access to MDM capabilities.
  - **Batch Import** – Import new users in bulk by using a comma-separated values (.CSV) file. Enter a unique name and description to group and organize multiple users at a time.
- **Layout** button
  - **Summary** – View the **Users List** with the default columns and view settings.
  - **Custom** – Select only the columns in the **Users List** you wish to see. You also have the option to apply selected columns to all administrators at or below the current Organization Group.
- **Export** button – Save a .csv file (comma-separated values) of the entire **Users Listing** that can be viewed and analyzed in Excel.

The **User Listing** features a selection checkbox and **Edit** icon to the left of the user.

Selecting the **Edit** icon enables you to make basic changes to the User's account.

Selecting a single checkbox causes three buttons to appear above the listing:



- **Send Message** – Provide immediate support to a single user or group of users. Send a User Activation (user template) email to a user notifying them of their enrollment credentials.
- **Add Device** – Add a device to associate with the selected user. Only available for single user selections.
- **More**
  - **Add to User Group** – Add selected users to new or existing User Group for simplified user management.
  - **Remove from User Group** – Remove selected users from existing User Group.
  - **Change Organization Group** – Manually move user to a different Organization Group. Update the user's available content, permissions and restrictions if they change positions, get a promotion or change office locations or territory.
  - **Delete** – Delete a user account. Quickly and completely delete a user account if a member of your organization is fired or resigns from their position.
  - **Activate** – Activate user if a user returns to an organization or needs to be reinstated in the company.
  - **Deactivate** – Deactivate user if a user is missing in action, out-of-compliance or if their device is lost or stolen.

Note: You may select more than one user account by selecting the checkbox of as many users as you like. Doing so will modify the available action buttons and will also make those actions apply to multiple users and their respective devices.

Using the Batch Import Feature

From the **Batch Status** page you can create users in bulk or import them from your directory service in bulk, rather than creating them one at a time.

Creating Users and User Groups in Bulk

To save time and effort of importing your Lightweight Directory Access Protocol (LDAP)/Active Directory (AD) user groups into the AirWatch Admin Console, upload users and user groups in bulk through the batch import feature.

Upload users in bulk

1. Navigate to **Accounts** ▸ **Users** ▸ **Batch Status** and select **Batch Import**.
2. Enter the basic information including a **Batch Name** and **Batch Description** for reference in the AirWatch Admin Console.
3. Select the applicable batch type from the **Batch Type** drop-down menu.
4. Select the information icon ( ) to access available templates. Then, choose the applicable template for your environment, click **Download Template and Example for this Batch Type** and save the .csv file somewhere accessible.

   Note: For the **Batch Type** 'Users And/Or Devices,' you have the choice between a **Simple** .csv template, featuring only the most popular and most often-used fields and an **Advanced** .csv template, featuring the full, unabridged compliment of fields.

5. Open the .csv file, which has a number of columns corresponding to the fields that display on the Add / Edit User page. Columns with an asterisk are required and must be entered with data. The **GroupID** column corresponds to the **Enrollment Organization Group** field on the **Add / Edit User** page. This is the Organization Group in which the user will be enrolled if the **Group ID Assignment Mode** is set to **Default** in **Groups & Settings** ▸ **All Settings** ▸ **Devices & Users** ▸ **General** ▸ **Enrollment** in the **Grouping** tab.

   Note: For directory-based enrollment, the **Security Type** for each user should 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 screen in the AirWatch Admin Console, select **Choose File** to locate and upload the saved comma-separated values (.csv) file.
8. Click **Save**.

Upload user groups in bulk

1. Navigate to **Accounts** ▸ **Users** ▸ **User Groups**.
2. Select **Batch Import**.
3. Enter the basic information including a Batch Name and Batch Description for reference in the AirWatch Admin Console.
4. Select the information icon ( ) to access available templates. Then, under **User Group Import**, select **Download Template and Example for this Batch Type** and save the comma-separated values (.csv) file.
5. Open the .csv file, which has a number of columns corresponding to the fields that display on the **Add User Group** page. Columns with an asterisk are required and must be entered with data. Save the file.
6. Return to the User Groups screen in the AirWatch Admin Console and select **Batch Import**. Select **Choose File** and locate and upload the saved .csv file.
7. Select **Save**.

Note: If the Batch Import does not complete successfully, view and troubleshoot errors by selecting **Accounts** ▸ **Batch Status**. Click the **Errors** hyperlink to view the specific batch import errors.

Changes in External LDAP/AD User Directories

Once your user and user group batch list is uploaded, any changes to your external LDAP/AD user directories will not update in the AirWatch Admin Console. These user and user group changes need to be updated manually, or uploaded again as a new batch.

Editing Basic Users with Batch Import

The Batch Import feature also allows the ability to edit and move users and user details in groups rather than one at a time. If the users already exist in AirWatch, use batch import to upload the updated .CSV file to edit the following fields (applies to Basic Authentication and Authentication Proxy Users only):

- Password (Basic only)
- First Name
- Middle Name
- Last Name
- Email Address
- Phone Number
- Mobile Number
- Department
- Email Username
- Email Password
- Authorized LGs (at and below the given Group ID only)
- Enrollment user category (This category should be accessible to the user, otherwise, defaulted to 0)
- Enrollment user role (this role should be accessible to the user, otherwise, it assumes the default role of the Organization Group)

Moving Users with Batch Import

You may also use the Batch Import feature to move sets of users to a new Organization Group.

1. From the Batch Import screen, enter the basic information including a Batch Name and Batch Description for reference in the AirWatch Admin Console.
2. Choose **Change Organization Group** from the Batch Type drop-down menu. Select the information icon ( ) to access the Change Organization Group template and save the .CSV file somewhere accessible.
3. Enter the required applicable Group ID (Group ID of the current Organization Group of the user), Username (user to be moved), and Target Group ID (Group ID of the Organization Group where the user will be moved to).
4. Return to the Batch Import screen in the AirWatch Admin Console, select **Choose File** to locate and upload the saved .CSV file and click **Open**.
5. Click **Save**.

Shared Devices

Overview

Issuing a device to every employee in your organization can be expensive. With AirWatch MDM, you can share mobile devices among end users using either a single fixed configuration for all end users or a unique configuration setting for each individual end user. AirWatch's Shared Device/Multi-User Device functionality ensures security and authentication are in place for every unique end user, and if applicable, allows only specific end users to access sensitive information.

When administering shared devices, you must first provision devices with applicable settings and restrictions before deploying them to end users. Once deployed, AirWatch utilizes 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's role determines their level of access to corporate resources, including content, features, and applications. This 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, so the device's enrollment status is never affected, and the device can be managed in the AirWatch Admin Console whether it is in use or not.

System Capabilities

Functionality

- Configure a single managed device which can be used by multiple end users.
- Personalize each end user’s experience without losing corporate-wide settings.
- Configure corporate access, apps, files, and device privileges based on user or Organization Group.
- Allow for a seamless login/logout process that is self-contained in the AirWatch Agent.

Security

- Provision devices with the shared device settings before providing devices to end users.
- Login and logout devices without affecting device enrollment in AirWatch.
- Authenticate end users during device login with directory services or dedicated AirWatch credentials.
- Manage devices even when a device is not logged in.

Supported Platforms

Android 2.3+ , iOS devices with AirWatch Agent v4.2+, and Mac OS X devices with AirWatch Agent v2.1+ support shared device/multi-user device functionality.

In This Section

This document discusses the detailed setup and configuration of Shared Device mode. It is divided into the following sections:

- Organizing Shared Devices – Discusses how and where to create organization hierarchy to organize devices in the AirWatch Admin Console.
- Configuring Shared Devices – Details the multiple ways to configure shared device functionality on to the devices.
- Using Shared Devices – Explains how to use shared device functionality on the device.

Organizing Shared Devices

The easiest way to manage your mobile fleet is to organize the devices you administer based on your corporate hierarchy and geographic location, if applicable. Because employee permissions, device restrictions and corporate access are often based on defined roles within the hierarchy, it is both logical and beneficial for you to mirror this structure when organizing groups within the AirWatch Admin Console for the first time.

Defining the Device Hierarchy

In most cases, when you first log in to the AirWatch Admin Console, you will see a single Organization Group that has been created for you with the name of your organization. This group serves as your top-level Organization Group, and you will create subgroups underneath it to build out your company's hierarchical structure.

To define the device hierarchy:

1. Navigate to **Groups & Settings** ▸ **Groups** ▸ **Organization Groups** ▸ **Organization Group Details**. Here, you can see an Organization Group representing your company.
2. Ensure the **Organization Group Details** displayed are accurate and then use the available data entry fields and drop-down menus to make any modifications, if necessary. If you make changes, click **Save**.
3. Select **Add Child Organization Group**.
4. Enter the following information for the first Organization Group to reside within the top-level Organization Group:
   - **Organization Group Name** - Enter a name for the child Organization Group to be displayed within the AirWatch Admin Console.
   - **Group ID** – Enter an identifier for the Organization Group for the end users to use for device to log in.

     Note: Ensure the end users who share devices receive the **Group ID** as it may be required for device to log in depending on your Shared Device configuration.

   - **Organization Group Type** - Select the preconfigured Organization Group Type that reflects the category for the child Organization Group.
   - **Country** - Select the country where the Organization Group is based.

- **Locale** – Select the language classification for selected country.
- **Time Zone** – Select the time zone for this Organization Group.

5. Create additional groups and subgroups in the same manner as needed to build out your corporate hierarchical structure. If configuring a **Fixed Organization Group**, then ensure you have created the single Organization Group for end user to log in or log out. If you configure **Prompt Users for Organization Group**, then ensure you have created the multiple Organization Groups that are required for your various end-user log in or log out roles. For more information, see Configuring Shared Devices.
6. Select **Save**.

Configuring Shared Devices

You can utilize shared device functionality by navigating to **Groups & Settings ▸ All Settings ▸ Devices & Users ▸ General ▸ Shared Device**.

Configure devices in one of three ways:

- 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, for example, 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, the settings, applications, and content to which they have access are based on their specific role within the hierarchy. For example, if an end user is a member of the 'Sales' User Group, which is mapped to the 'Standard Access' Organization Group, then when that end user logs in to the device, the device will be configured with the settings, applications and content available to the 'Standard Access' Organization Group. Consider an other example, hospitals can utilize this method by configuring different device profiles for different employees. A doctor can log in to a device and have access to certain applications and information related to a patient's personal information, treatment, and diagnosis. A nurse can log in to the same device and have access to an entirely different set of resources applicable to their role.

- Select **Prompt User for Organization Group** to have the end user enter a Group ID for an Organization Group each time they log in to a device.

  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.

Configuring Shared Device Settings

1. Navigate to **Groups & Settings** ▸ **All Settings** ▸ **Devices & Users** ▸ **General** ▸ **Shared Device**.
2. Select the **Override** radio button.
3. Select any one of the following applicable radio button to enable the **Group Assignment Mode** that meets your shared device requirements:
   - **Prompt User for Organization Group** – Select to prompt the end user to enter a valid Group ID and credentials to log in to a device, thereby allowing the device to leverage the settings, applications, and content of a particular Organization Group.
   - **Fixed Organization Group** – Select to restrict the end user to a particular Organization Group when they log in to a device. A Group ID is not required, but an end user may be prompted to enter credentials to log in to a device.
   - **User Group Organization Group** – Select to use the User Group-to-Organization Group mapping configured in the AirWatch Admin Console to determine access to settings, applications, and content.

   Note: The User Group-to-Organization Group mapping is done on the AirWatch Admin Console. Navigate to **Groups & Settings** ▸ **All Settings** ▸ **Devices & Users** ▸ **General** ▸ **Enrollment**. Select the **Grouping** tab and fill in the required details.

   - **Always Prompt Terms of Use** – Select this checkbox to prompt the end user to accept **Terms of Use** agreement before logging into a device.
4. Select the **Auto Logout Enabled** check box to configure automatic logout after a specific time period.
5. Select the **Enable Single App Mode** check box to configure Single App Mode, which locks the device into a single application when an end user logs into the device.

   Note: Single App Mode applies only to Supervised iOS devices.

6. Click **Save**.

Enabling Multi-User Device Staging for iOS and Android

Note: When staging a device for a multi-user environment, it is important to make certain that the staging user (the individual tasked with prepping the device for users) is **not** part of the Smart Group to which any user-specific profile is assigned. For example, email profiles should not be assigned to the staging user. This ensures that the device profiles are removed when the device is checked in and the appropriate profiles are installed when checked out to each end user.

Similar to single-user device staging, multi-user – "shared device" – staging allows an IT administrator to provision devices intended to be used by more than one user. The first step is configuring this functionality in the AirWatch Admin Console. Follow the high-level steps below to create a staging user, enroll into AirWatch, and enable multi-user device staging.

1. Navigate to **Accounts** ▸ **Users** ▸ **List View** and select the **pencil** icon to edit the user account for which you want to enable device staging. Or, alternately, create the staging user.
2. On the Add / Edit User screen, select **Enable Device Staging** and then select the staging settings that will apply to this staging user. Select **Multi User Devices** to stage devices for use by multiple users. Select **Save**.
3. On the device, download and install the Agent by opening the device's Internet browser and navigating to **awagent.com** or by going to the enrollment URL (https://www.<environment_URL>.com/enroll).
4. Launch the Agent and enroll the device by entering the proper **Group ID** and **staging user credentials** as required.
5. During enrollment, when prompted, select **Multi-user** to determine how the device is staged.
6. Complete enrollment as the staging user you created and install the MDM profile by following the prompts.

The login/logout screen displays and prompts any users of the device to check out the device and to access the applications, settings and content for their Organization Group, which is assigned based on the **Group Assignment Mode** settings you specify under **Devices** ▸ **Settings** ▸ **Devices & Users** ▸ **General** ▸ **Shared Device**.

The device is now staged and ready for new users to log into it.

Using Shared Devices

Logging in a device automatically configures it with the specific settings, applications, and content based on the end-user's role. After the end user logs out of the device, the configuration settings of that session are wiped and the device is ready for login by another end user.

User Groups

You can group sets of users into user groups, which act as filters (in addition to Organization Groups) for assigning Mobile Device Management (MDM) profiles and applications. Use the **User Groups** page to manage them. When configuring your MDM environment, it is a best practice that user groups be used to define Security Groups and/or Business Roles within your organization.

It is also recommended that user groups be used to assign Profiles, Compliance Policies, Content, and Applications to users and devices. You can add your existing directory service groups into AirWatch or create user groups from scratch.

In This Section

- Adding User Groups without Directory Integration – Explains how to create a user group outside of your organization's existing directory service structure.
- Adding Directory-Based User Groups – Details how to integrate with your existing directory service infrastructure to add user groups.
- Editing User Group Permissions – Covers how to edit user group permissions, which determines which administrators have management permissions for a particular user group.

Adding User Groups Without Directory Integration

Creating a user group outside of your organization's existing Active Directory structure allows you to create specialized groups of users at any time. Add and tweak user groups that are not parallel to your existing user structure. Specifically design access to features and content and include basic and directory users to fully customize user groups according to your deployment. See Using the Batch Import Feature for more about adding user groups in bulk.

To establish a custom User Group without Active Directory integration:

1. Navigate to **Accounts** ▸ **Users** ▸ **User Groups** and select **Add**.
2. Change the User Group **Type** option to **Custom**.
3. Enter the **Group Name** and **Description** used to identify the User Group in the AirWatch Admin Console.
4. Confirm the Organization Group that will manage the User Group and select **Save**.
5. You can then add users to this new user group by navigating to **Accounts** ▸ **Users** ▸ **List View**, selecting users in bulk by clicking checkboxes to the far-left of each listed **Username**, hovering over the **Management** button above the column headings and choosing **Add to User Group**.

Adding Directory-Based User Groups

Another way to integrate your directory service users and groups with AirWatch is by utilizing user group integration. By importing your existing directory service groups into AirWatch for use as AirWatch user groups, you can perform tasks in the following areas:

- **User Management** – Reference your existing directory service groups (such as Security Groups or Distribution Lists) and align user management in AirWatch with the existing organizational systems.
- **Profiles and Policies** – Assign profiles, applications and policies across an AirWatch deployment to groups of users.
- **Integrated Updates** – Automatically update user group assignments based on group membership changes.
- **Management Permissions** – Set management permissions to only allow approved administrators to change policy and profile assignments for certain user groups.
- **Enrollment** – Allow users to enroll in AirWatch using their existing credentials and automatically assign them to the appropriate Organization Group.

Note: The administrator must designate an existing Organization Group as the primary root location group from which the administrator will manage devices and users. Directory Services must be enabled at the level of this root Organization Group. See the **AirWatch Directory Services Guide**, available via AirWatch Resources, for more information.

You can add your existing directory service groups into AirWatch. While this does not immediately create AirWatch user accounts for each of your directory service accounts, it does ensure AirWatch recognizes them as belonging to a configured group, which you can then use as a means of restricting who can enroll. See Using the Batch Import Feature for more about adding directory user groups in bulk.

To create a Directory-based User Group:

1. Navigate to **Accounts** ▸ **Users** ▸ **User Groups** and select **Add**.

   Note: For adding admins, use the same settings below except navigate to **Accounts** ▸ **Administrators** ▸ **Admin Groups**.

2. Enter the user group keywords in the **Search text** box and select **Search**.
3. Ensure the user group **Type** is **Directory**. Then, enter information for the following fields:
   - **External type** – Select the external type of group you are importing. For Custom Query, enter query logic in the section that displays.
   - **Search Text** – Enter a user group in your directory and select **Search** to search for it. If a directory group contains your search text, a list of **Group Names** displays.
   - **Directory Name** – Enter the address of your directory services server.
   - **Directory Name, Domain, Group Base DN** – This information will automatically populate based on the directory services server information you enter on the **Directory Services** page (**Accounts** ▸ **Settings** ▸ **Directory Services**).

     Select the **Fetch DN** information icon ( ) next to the **Group Base DN** field. This should display a list of Base Domain Names from which you can select to populate this field.
4. Select a **Group Name** from your **Search Text** results list.
5. Check the **Organization Group Assignment** check box to automatically assign users to the current Organization Group.

6. Leave the **Apply default settings** option enabled to save default settings, or switch the option to **Use Custom settings for this user group** to configure advanced settings.

   If configuring Custom Settings, consider the following:

   - **Management Permissions** – Allows all admins to manage the User Group.
   - **Default Role** – Assigns specific Role to all users in the User Group.
   - **Default Enrollment Policy** – Assigns a specific enrollment policy to all users in the User Group.
   - **Auto Sync with Directory** – Establishes automatic updates to directory.
   - **Auto Merge Changes** – Merges any changes in the existing and updated directory.
   - **Maximum Allowable Changes** – Restricts the number of allowable group membership changes to be merged. Any number of changes detected upon syncing with the directory service database that are less than this amount will be automatically merged (provided the **Auto Merge Changes** checkbox is selected). Amounts equal to or in excess of this amount will require Admin approval.
   - **Add Group Members Automatically** – Adds any members of the User Group automatically.
   - **Enable/Disable Sending Email to User when Adding Missing Users** – Sends correspondence to user if added to the User Group.

7. Select **Save**.

Editing User Groups Permissions

Fine-tuning user groups permissions allows you to reconsider who inside your organization can edit certain groups. For example, if your organization has a user group for company executives, you may not want lower level administrators to have management permissions for that user group.

Use the **Permissions** page to control who can manage certain user groups, and who can assign profiles, compliance policies and applications to user groups.

1. Navigate to **Accounts** ▸ **Users** ▸ **User Groups**.
2. Select **Edit** for an existing user group row.
3. Select the **Permissions** tab, then select **Add**.
4. Select the **Organization Group** for which you would like to define permissions.
5. Select the **Permissions** you would like to enable.
6. Select the **Scope** of these permissions, that is, which groups of administrators are allowed to manage or use this user group.
7. Select **Save**.

Accessing User Details

Once your users and user groups are in place, view all user information regarding user details, associated devices, and interactions. Access a user's information from any location in the AirWatch Admin Console where the username is displayed, allowing a single-page view of:

- All associated user groups.
- All Devices associated with the user over time and a link to complete history of enrolled devices.
- All devices a user has checked-out in a Shared Device Environment and a link to complete check-in/check-out device history.
- All device- and user-specific event logs.
- Summary of all assigned, accepted and declined Terms of Use.

Note: If desired, you can encrypt personally identifiable information, including first name, last name, email address and telephone number. Navigate to **Groups & Settings ▸ All Settings ▸ System ▸ Security ▸ Data Security** from the Global or Customer-level Organization Group for which you want to configure encryption.

Enabling encryption, selecting which user data fields to encrypt, and clicking **Save** encrypts user data so it is not accessible in the database. Note that doing so will limit some features in the AirWatch Admin Console, such as search, sort and filter.

Administrators and Role-Based Access

Overview

Similar to how AirWatch has user accounts to keep track of users with devices, AirWatch admin accounts keep track of those who have access to the AirWatch Admin Console. As an administrator, you can maintain Mobile Device Management (MDM) settings, push or revoke features and content and much more from the centralized AirWatch Admin Console.

Although many organizations have multiple administrators of their managed device fleet, each administrator requires different levels of access depending on their specific corporate role. Use Admin Account roles to provide the proper level of access for different administrators.

In This Section

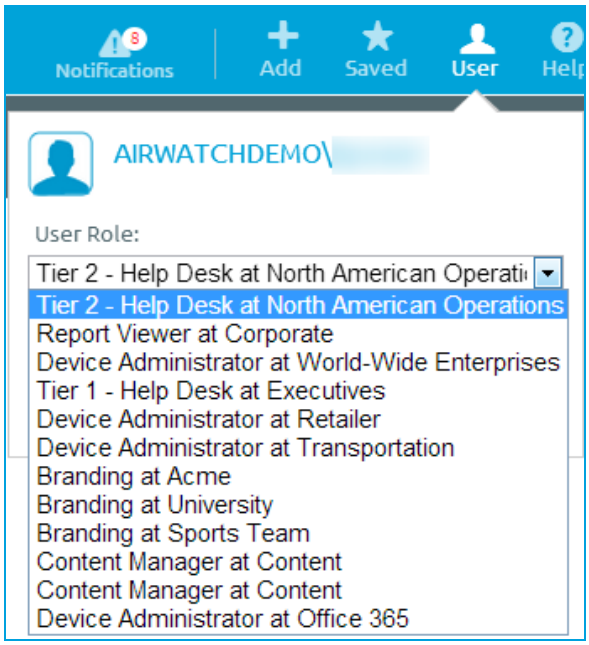
- Default and Custom Roles – Explains the difference between Default and Custom Roles and provides a list of Default Roles available in the AirWatch Admin Console.
- Creating a Custom Role – Details how to alter Default Roles to tailor Custom Roles.
- Creating an Admin Account – Walks through the steps required to create a new admin account as well as creating a Temporary Admin Account.
- Managing Admin Accounts – Lists the available actions you can take on existing admin accounts, such as view history, edit, change password, deactivate and delete admin accounts.

Default and Custom Administrator Roles

For ease of use, there are numerous **Default Roles** already provided by AirWatch. These default roles are available with every AirWatch upgrade and help to quickly assign appropriate roles to new users. If you require further customization, you always have the option to create **Custom Roles** to tailor user privileges and permissions. Unlike default roles, custom roles require manual updates with every AirWatch upgrade.

Each type of role comes with its own pros and cons to consider. **Default Roles** save time and effort in configuring a brand new role from scratch, logically suit a variety of administrative privileges and automatically update alongside new AirWatch features and settings. However, Default Roles may not be a precise fit for Administrators and Users in your organization and MDM deployment, which is why Custom Roles were created.

Custom Roles allow you to customize as many unique roles as you'd like and to tweak big or small changes across different users and administrators. However, Custom Roles must be manually maintained over time and updated with new AirWatch updates and features.



The following list of roles describes each Default Role currently available in the AirWatch Admin Console:

System Administrator

The System Administrator role provides complete access to an AirWatch environment. This includes access to the Password and Security settings, Session Management and AirWatch Admin Console audit information contained in the **Administration** tab under **System Configuration**.

Note: The System Administrator role is not available for software as a service (SaaS) customers.

AirWatch Administrator

The AirWatch Administrator role allows comprehensive access in the AirWatch environment. However, this access excludes the **Administration** tab under **System Configuration**, because that tab manages top-level AirWatch Admin Console settings.

Device Manager

The Device Manager role grants significant access to the AirWatch Admin Console. However, using this role to configure most System Configurations (Active Directory (AD)/Lightweight Directory Access Protocol (LDAP), Simple Mail Transfer Protocol (SMTP), Agents, etc.) is not recommended. Instead, it is more appropriate to use a top-tier role like the AirWatch Administrator or System Administrator.

Read Only

The Read Only role provides access to most of the AirWatch Admin Console, but limits access to read-only status. Use this role to audit or record the settings in place throughout an AirWatch environment. This role is not recommended for system operators or administrators.

Content Management

The Content Management role limits administrative access to AirWatch Content Locker management. This facilitates specialization of administrator(s) to uploading and managing the device fleet's content.

Application Management

The Application Management role grants access to deploy and manage the device fleet's internal and public apps. This role is limited in scope to facilitate the specialization of an application management administrator.

Help Desk

The Help Desk role provides the tools necessary for most Level 1 IT Help Desk functions. The primary tool available in this role allows AirWatch Administrators to see and respond to device info with remote actions. However, this role also contains report viewing and device searching abilities.

Report Viewer

The Report Viewer role allows viewing of the data captured through Mobile Device Management (MDM). This role limits access to generate, view, export, and subscribe to reports from the AirWatch Admin Console.

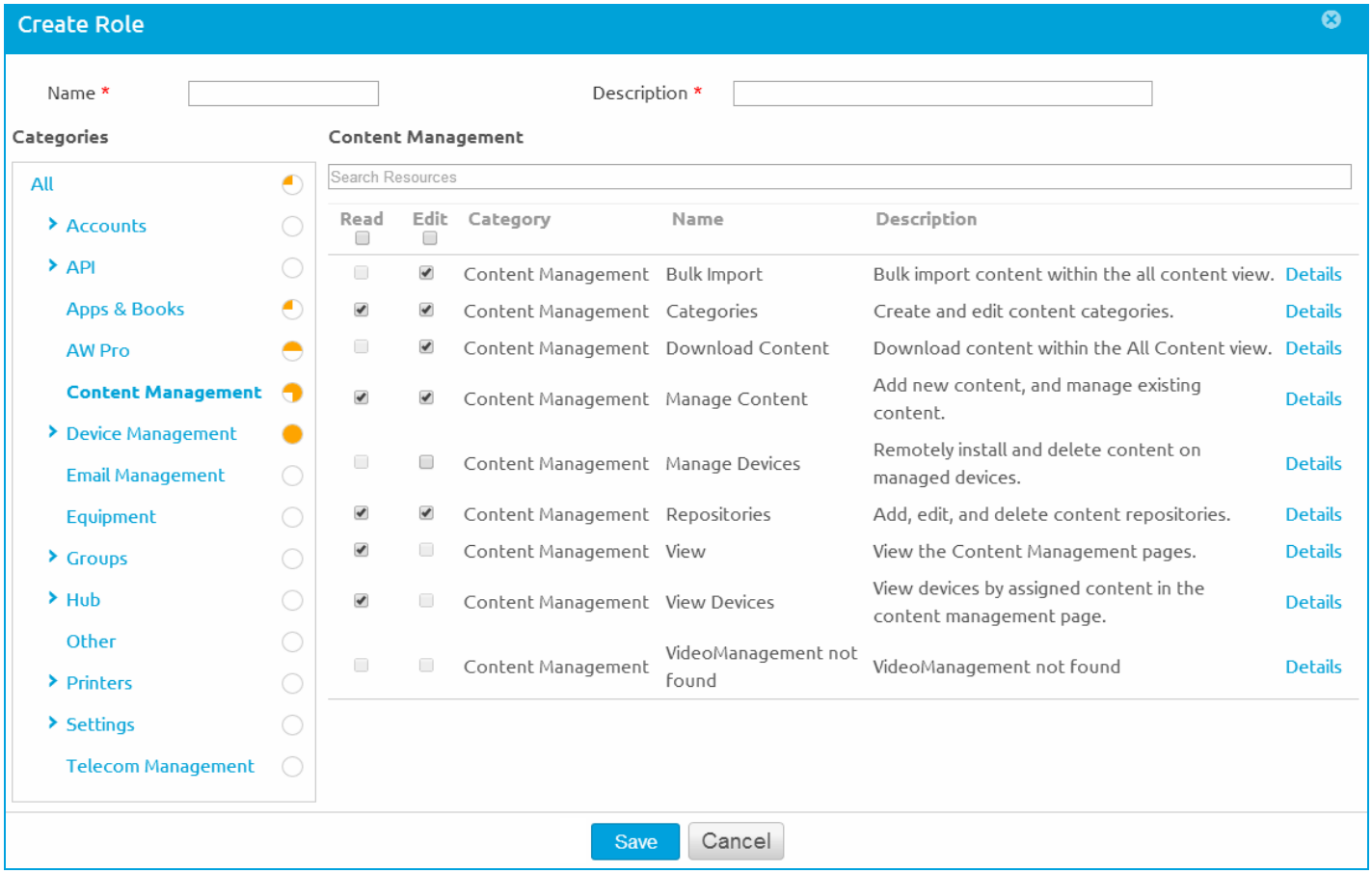
Creating a Custom Role

If none of the available Default Roles provide the proper fit for Admin and User resources in your organization, then consider creating a Custom Role from the **Admin Roles** listing page.

Determine the Default Role that best fits the role you want to create, select the **Copy** button from the actions menu and alter specific settings of the copy in the resulting **Add Role** screen, making sure to use a unique **Name** and **Role Description** prior to selecting the **Save** button.

Adding a New Administrator Role

Add a new administrator role from scratch by taking the following steps.



1. Navigate to **Accounts** ▸ **Administrators** ▸ **Roles** and select **Add Role** in the AirWatch Admin Console.
2. In the **Create Role** screen, enter the role's **Name** and **Role Description**.
3. Make a selection from the list of **Categories**.

   The **Categories** section organizes top-level categories such as **Device Management** under which are located subcategories including **Applications**, **Browser** and **Bulk Management** among others. This category subdivision enables an easy and quick role creation process. Each subcategory setting in the right panel has a **Read** and **Edit** check box.

   When you make a selection from the **Categories** section, its sub-categorized contents (individual settings) populate in the right panel. Each individual setting features its own **Read** and **Edit** check box (where applicable) in addition to a "select all" style **Read** and **Edit** check box in the column heading. This allows for a very flexible level of control and customization while creating roles.
4. Select the appropriate **Read** and/or **Edit** check box in the corresponding resource fields. You may also choose to clear any of the selected resources.

5. To make blanket category selections, select **None**, **Read** or **Edit** directly from the **Categories** section without ever populating the right panel. This is accomplished by selecting the circular icon to the right of the Category label, which is a drop-down menu. Use this selection method when you are certain you want to select none, read-only or edit capabilities for the entire category setting.

6. Select **Save** to finish creating the Custom Role. You can now view the added role in the list on the **Roles** page. From here, you can also edit the role details or delete the role.

Note: You will need to update the custom role after each AirWatch version update to account for the new permissions in the latest release. For a list of the latest added resources, see the **AirWatch Roles and Added Resources Guide** document, available via AirWatch Resources.

Read/Edit Indicator in Categories

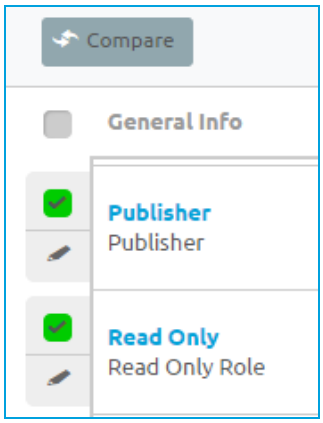
There is a visual indicator in the **Categories** section that serves to reflect the current selection of read-only, edit, or a selective combination of each. This indicator reports what the setting is without you having to open and examine the individual subcategory settings.

The indicator features a circular icon located to the right side of the Category listing that reports the following:

- All options in this category have the edit capability (which by definition means they also have read-only capability).
- The majority of category settings have the edit capability enabled but with at least one subcategory with edit disabled.
- All category settings have the read-only (edit disabled).
- The majority of category settings are read-only with at least one with read-only disabled.

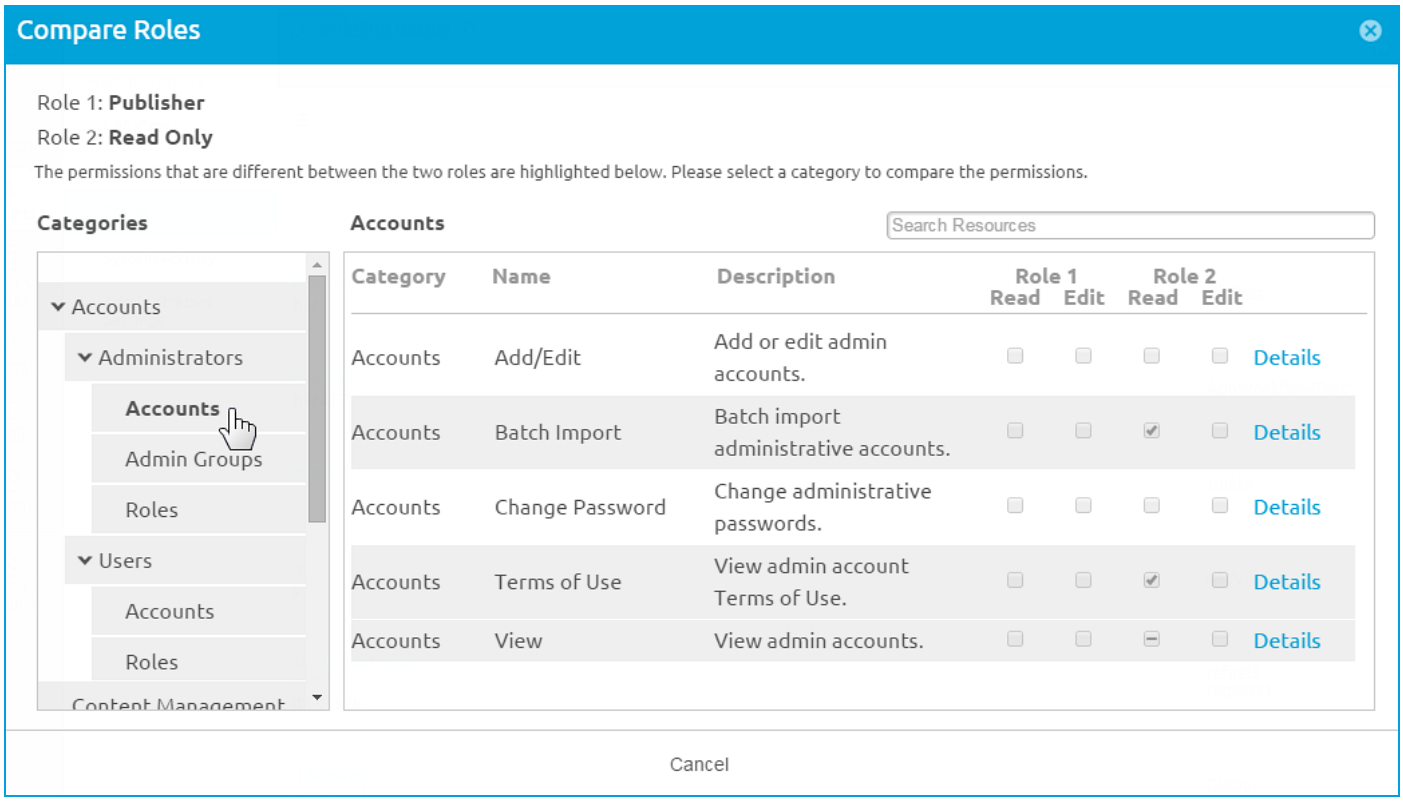
Comparing Admin Roles

Compare two Admin Roles with the **Compare Roles** tool, accessible by navigating to **Accounts** ▸ **Administrators** ▸ **Roles**. Choose any two listed roles and insert a check mark in those roles. Next, select the **Compare** button.



Note: The **Compare** button will not display if you have less than two or more than two roles checked.

Upon selecting the **Compare** button, the **Compare Roles** page displays featuring a list of Categories. Selecting a specific Category on the left populates all the details of that category on the right.



Differences between the two roles are highlighted in gray so you can see at-a-glance which categories and subcategories have different settings.

The roles you select are assigned to **Role 1** and **Role 2**, respectively, which enables you to easily identify which Read-only and Edit settings apply to the selected admin roles.

Creating an Admin Account

Administrators can maintain Mobile Device Management (MDM) settings, push or revoke features and content and much more from the centralized AirWatch Admin Console. Add Admin Accounts from the **Administrators List View** page

for each admin that maintain and supervise the Admin Console.

To add an admin account:

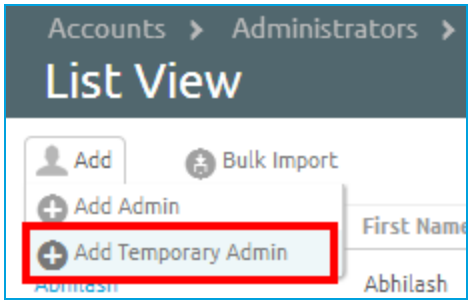
1. Navigate to **Accounts** ▸ **Administrators** ▸ **List View** and select **Add User**. You will notice that admins have additional tabs for configuration that normal users do not.
2. Select either **Basic** or **Directory** as the **User Type** on the **Basic** tab.
   - If you select Basic, then fill in all required fields on the **Basic** tab, including username/password and First Name/Last Name.
   - If you select Directory, then enter the **Domain** and **Username** of the admin user.
3. Select the **Details** tab and enter additional information, if necessary.
4. Select the **Roles** tab and select the **Organization Group** followed by the **Role** you want to assign to the new admin. Add new roles by using the **Add Role** button.
5. Select the **API** tab to choose the **Authentication** type.
6. Select the **Notes** tab to enter additional **Notes** for the admin user.
7. Choose **Save** to create the new Admin Account with every assigned role.

Creating a Temporary Admin Account

You may temporarily grant administrative access to your environment for support, demonstrations and other time-limited use cases.

A **Temporary Admin Account** enables a remote assistance feature within the AirWatch Admin Console.

These Temporary Admin Accounts, which have a configurable expiration, can be used to access areas normally reserved for permanent admin account-holders.



Create a **Temporary Admin Account** by taking the following steps:

1. Navigate to **Accounts** ▸ **Administrators** ▸ **List View** and select **Add**. Select the **Add Temporary Admin** option.
2. Complete the following required fields:
   - **Username**
   - **Password** and **Confirm Password**
   - **First Name** and **Last Name**
   - **Email Address**
   - **Initial Landing Page**
3. Select an **Expiration Time** which defaults to 6 hours. You may also set this field to **Inactive** for the purpose of creating the account now and activating it later.

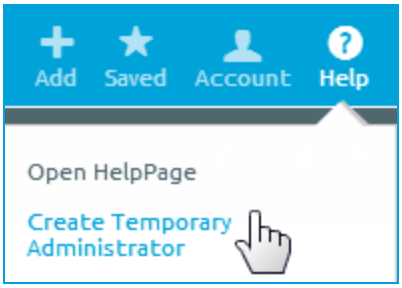
4. Select **Email** as a **Message Type** to send an optional email message to the user. This email notifies users of their new Temporary Admin Account, including credentials and expiration time.

   Select a template for the email via the **Email Message Template** drop-down field or configure a new template by selecting **Add Message Template**.

5. Select **Save**.

You may also create a temporary admin account by selecting the **Help** button and then selecting **Create Temporary Administrator**.

The **Add/Edit Admin** screen displays (commence step 2 above).



Managing Admin Accounts

Navigate to the Administrator Management page at **Accounts** ▸ **Administrators** ▸ **List View** and select from the actions drop-down menu to utilize key management functions for ongoing maintenance and upkeep, including:

- **Edit** – Alter admin information to keep current contact information or privileges if the Admin duties are delegated to another member of your organization.
- **View History** – Keep track of when admins log in and out of the AirWatch Admin Console.
- **Deactivate** – Change the status of an admin account from active to inactive. This feature allows you to temporarily suspend the management functions and privileges while at the same time keep the defined roles of the admin account for later use.
- **Activate** – Change the status of an admin account from inactive to active.
- **Change Password** – Reset a password that is compromised or forgotten by an Admin User.
- **Delete** – Ensure only the right users are accessing the AirWatch Admin Console. Immediately cancel and eliminate a user's account and revoke privileges if someone quits or is fired from their position.
- **Add/Edit Admin** – Quickly update current roles assigned to a user if the user is promoted or changes roles within your organization to keep their privileges up-to-date.

Device Enrollment

Overview

Use the organization groups, user groups and authentication established when setting up the environment in the AirWatch Admin Console to enable users to enroll their devices, providing access to content, features and applications from their mobile devices easily and securely.

Required Information

To enroll an iOS or Android device, you'll need the following information:

- **Enrollment URL** – This enrollment URL is AWAgent.com for all users, organizations and devices enrolling into AirWatch.
- **User Credentials** – This username and password confirm the identity of a user to allow login, authentication and enrollment. The credentials may be the same as the network directory services credentials, or may be AirWatch-specific credentials.

Note: For a step-by-step walkthrough of all of the enrollment options, refer to the **AirWatch Enrollment Processes Guide**, available via AirWatch Resources.

In This Section

- The Enrollment Process – Profiles the main enrollment process recommended by AirWatch.
- Additional Enrollment Workflows – Details all available routes for devices to enroll into AirWatch.
- Performing Device Staging – Describes how to stage devices as an administrator for end users.
- Registering Devices – Details how to register corporate devices, which offers the ability to lock down enrollment to only pre-approved devices.
- Configuring Enrollment Options – Explains the available options for customizing your enrollment process, including optional prompts, restrictions and groupings.
- Customizing Enrollment Messages and MDM Prompts – Explains how to create enrollment message prompts for end users.
- Blacklisting and Whitelisting Device Registration – Details the process of adding devices to a blacklist or whitelist, which lets you allow or deny them from enrolling.

The Enrollment Process

The enrollment process may differ slightly depending on the device platform (iOS, Android, Windows Phone).

- You can find platform-specific instructions for enrolling each type of device in the applicable **Platform Guides**.
- You can find a step-by-step walkthrough of the different enrollment options and how they affect device enrollment in the **AirWatch Enrollment Processes Guide**.
- To enroll with the AirWatch Container instead of the AirWatch Agent, refer to the **AirWatch Container Guide**, available via AirWatch Resources.

In general, enrollment via the AirWatch Agent tends to follow the workflow below:

1. Navigate to AWAgent.com from the native browser on the device that you are enrolling.

   AirWatch auto-detects if the AirWatch Agent is already installed and redirects to the appropriate mobile app store to download the Agent if needed.

   Note: Downloading the Agent from public application stores requires either an Apple ID or a Google Account.

2. Launch the Agent upon download completion or return to your browser session to continue enrollment.
3. Enter your email address. AirWatch checks if your address has been previously added to the environment in which case you are already configured as an end user and your Organization Group is already assigned.

   If AirWatch cannot identify you as a previously configured end user based on your email address, enter your **Environment URL**, **Group ID** and **Credentials** when prompted. Your AirWatch Administrator will provide you with the environment URL and Group ID if they are needed.

4. Follow all remaining prompts to finalize enrollment.

   Note: Each platform has slight variations in this process, so refer to each specific Platform Guide, available via AirWatch Resources, for more information.

Additional Enrollment Workflows

In some unique cases, the enrollment process must be adjusted for specific organizations and deployments. For each of the additional enrollment options below, you'll need the following information:

- **Environment URL** – The Environment URL brings you to the enrollment screen. It is specific to your organization's enrollment environment (e.g., **mdm.acme.com**). Your AirWatch Administrator will provide you with this URL if it is needed.
- **Group ID** – The Group ID determines what Mobile Device Management (MDM) resources and features the end user will have access to upon enrollment. Your AirWatch Administrator will provide you with this Group ID if it is needed.
- **User Credentials** – The username and password confirm the identity of a user to allow login, authentication and enrollment. The credentials may be the same as the network directory services credentials, or may be AirWatch-specific credentials.

Examples of other enrollment workflows include:

- **Notification-Prompt Enrollment** – End user receives notification (email and SMS) with Enrollment URL and enters their Group ID along with login credentials. As soon as the end user accepts the Terms of Use, the device

automatically enrolls and outfits with all MDM features and content, including apps and features from the AirWatch server.

- **Single-Click Enrollment** – Administrator sends an AirWatch-generated token to the user along with enrollment link URL. User only needs to click the provided link to authenticate and enroll the device. This is the easiest and fastest enrollment process for the end user and can be secured by setting expiration times.
- **Dual-Factor Authentication** – Administrator sends the same enrollment token generated by AirWatch but the user must also enter their login credentials. This method is just as easy to execute as the Single-Click Enrollment but adds one additional level of security by requiring the user to enter their unique credentials.
- **Web Enrollment** – There is an optional welcome screen that an administrator can invoke for web enrollments by appending "/enroll/welcome" to the active environment. For example, by supplying the URL **https://<custenvironment>/enroll/welcome** to users participating in Web Enrollment, they will see a Welcome to AirWatch screen with options to enroll with an Email Address or Group ID. This option is applicable to AirWatch version 8.0 and above.
- **End User Registration** – User logs into the Self-Service Portal (SSP) and registers their own device. Once registration is complete, the system sends an email to the end user including the enrollment URL and login credentials.
- **Single-User Device Staging** – Administrator enrolls devices on behalf of an end user. This method is particularly useful for administrators who need to set up multiple devices for an entire team or single members of a team to save time and effort of enrolling their own devices. The admin can also configure and enroll a device and mail it directly to a user who is off-site.
- **Multi-User Device Staging** – Administrator enrolls devices that will be used by multiple users. Each device is enrolled and provisioned with a specific set of features that can be accessed by users only after they log in with unique credentials.

Note: For a step-by-step walkthrough of all of these enrollment options, refer to the **AirWatch Enrollment Processes Guide**, available via AirWatch Resources.

Performing Device Staging

Device staging, while a simple process, can take time if you have thousands of devices to pre-enroll. Therefore it works best when you have a new batch of devices that are being provisioned, since you can gain access to the devices before employees receive them. Device staging can be performed for Android, Windows Phone 8, iOS and Mac OS X devices in the following ways:

- **Single User (Standard)** – Used when you are staging a device that will be enrolled later by any user.
- **Single User (Advanced)** – Used when you are staging and enrolling a device for a particular user.
- **Multi User** – Used when you are staging a device to be shared among multiple users.

Note: Windows Phone 8 currently only support Single User device staging.

Note: Staging Users can have both single and multi-user staging enabled using the steps below.

Single-User Device Staging

Particularly useful for IT administrators provisioning a fleet of devices, this feature of the AirWatch Admin Console allows a single administrator to outfit devices for other users on their behalf. To enable Device Staging:

1. Navigate to **Accounts** ▸ **Users** ▸ **List View** and select **Edit** for the user account for which you want to enable device staging.
2. Select **Enable Device Staging** and then select the staging settings that will apply to this staging user.

   Single User Devices – Stages devices for a single user. Toggle the type of Single User device staging mode to either **Standard** or **Advanced**. Standard staging requires an end user to enter login information after staging, while Advanced means the staging user will enroll the device on behalf of another user.
3. Enroll the device using one of the two following methods:
   - Enroll via the AirWatch Agent by entering a server URL and Group ID.
   - Open the device's Internet browser, navigate to the enrollment URL and enter the proper Group ID.
4. Enter your staging user's credentials during enrollment. If necessary, specify that you are staging for **Single User Devices**. You will only have to do this if Multi-User device staging is also enabled for the staging user.
5. Complete enrollment for either Advanced or Standard staging:
   - If performing Advanced staging, you will be prompted to enter the username of the end-user device owner who will be using the device. Proceed with enrollment by installing the Mobile Device Management (MDM) profile and accepting all prompts and messages.
   - If performing Standard staging, then upon completing enrollment the end user will be prompted to enter their own credentials.

The device is now staged and ready for use by the new user.

Multi-User Device Staging

Similar to single-user device staging, multi-user device/shared device staging allows an IT administrator to provision devices intended to be used by more than one user. However, multi-user devices require configuration of the device to accept any allowed users to sign-in and use the device as necessary.

For details on configuring multi-user staging, please see the Configuring Shared Devices section in the Mobile Device Management Guide, available via AirWatch Resources.

Registering Devices

Registering the devices involved in your Mobile Device Management (MDM) deployment provides additional detail when reviewing device information, while also providing an added level of secure authorization. Register devices through the AirWatch Admin Console before enrolling those devices so that only authorized devices can enroll. There are three ways to register devices depending on your unique needs and requirements:

- **Register individual devices in the Admin Console** – Enter important device and asset information such as Friendly name for easy recognition in the Admin Console, model, operating system, serial number, Unique Device Identifier (UDID) and asset number. This process may also be the final step when Adding a Single User by selecting **Save and**

Add Device rather than **Save**.

- **Register a list of devices** – Similar to adding users in bulk, this process streamlines the device registration process when adding multiple devices at a time and may be included with the **Bulk User Account Creation** process.
- **End User Device Registration** – You may choose to have end users register their own devices before enrolling into AirWatch if you are supporting BYOD in your deployment and yet still require devices to be registered before they can enroll.

Register Individual Device

To register an individual device, follow one of two options:

1. Navigate to **Accounts** ▸ **Users** ▸ **List View** and select a single user who is to receive a newly-registered device. Next, select the **Add Device** button, which is now displayed above the header in the listing. The **Add Device** page displays for you to enter **General** and **Message** information.

Or

2. Complete the New User Account Creation process and select **Save and Add Device** at the last step. This opens the **Add Device** page to enter **General** device and **Message** information.

- The basic device registration fields include information regarding:
  - **Friendly Name** – Name of the device displayed in the Admin Console for easy recognition.
  - **Ownership Type** – Ownership of the device, including Corporate-Dedicated, Corporate-Shared or Employee-Owned. This allows you to customize MDM policies based on ownership to maximize privacy and protection.
  - **Platform Type** – Platform of the device you're currently registering.
  - **Message** – Enrollment/welcome message sent to the user. This setting allows you to choose which message template is sent to the user, how the message is sent (either email or SMS) and to which email address or phone number the message is sent.
- You can also select **Show Advanced Device Information Options** to manually enter additional device information, including:
  - **Model / OS / UDID / Serial Number / Asset Number** – Additional device information for the device you're registering. These details help organize and manage devices in the Admin Console while also tailoring which policies and features are sent to specific sets of devices.

Once the device information is entered, select **Save** to complete the form and send the specified message to the end user.

Register a List of Devices

To register multiple devices:

1. Navigate to **Accounts** ▸ **Users** ▸ **List View** and select **Batch Import** from the **Add** menu to open the **Batch Import Form**.
2. Enter the basic information including a **Batch Name** and **Batch Description** for reference in the AirWatch Admin Console.

3. Select the information icon ( ) to access available **Batch Type** templates as well as a description of each. Next, choose the applicable template that best suits your environment by making a choice in the **Batch Type** drop-down field.

4. Select the information icon ( ) again to select the appropriate **Download Template and Example for this Batch Type** and save the comma-separated values (.CSV) file somewhere accessible.

5. Open this .CSV file and enter all relevant information for each device in the template.

   IMPORTANT: Enter all data for serial numbers, asset numbers, IMEI numbers, or any other number that contains numerical values only in double quote marks (ex: "123456") to avoid having the values truncated, which may result in devices being blacklisted by AirWatch MDM.

   Three sample users have been added to the top of the template to be used as a reference for the type of information intended to be placed in each column. To register a device, make sure that **column X (User Only Registration)** is set to **No**. To register an additional device to the same user account, make sure that all information in columns **A through W** is the same. The remaining columns are used to register each additional device. To store advanced registration information, make sure that **column AF (Store Advanced Device Info)** is set to **Yes**.

6. Save the completed template as a .CSV file, return to the AirWatch Admin Console, select **Choose File** from the Batch Import Form and select the completed .CSV file.

7. Select **Save** to complete registration for all listed users and corresponding devices.

End User Device Registration

You may also prefer to have end users register their own device prior to enrolling into AirWatch if the device details aren't known at setup, or if a bring your own device (BYOD) deployment is in effect and the end users opt-in various devices. In this case, you will need to notify your end users by either:

- Sending an email or intranet notification to users outside of AirWatch with the registration instructions. For this method, ensure enrollment authentication is enabled for either Active Directory or Authentication Proxy by navigating to **Devices ▸ Device Settings ▸ Devices & Users ▸ General ▸ Enrollment ▸ Authentication**. Also verify that the Deny Unknown Users is unchecked by navigating to **Devices ▸ Device Settings ▸ Devices & Users ▸ General ▸ Enrollment ▸ Restrictions**.

- Alternatively, you may first create user accounts for all of the end users to register their devices and then send User account activation messages to each user containing the registration instructions.

Note: If you are enrolling Android devices, be sure to take advantage of AirWatch support for Android's auto enrollment feature. See the **Android Platform Guide** for details, available via AirWatch Resources.

Both options require you to provide basic information to the end users, including:

- **Where to Register** – End users can register by navigating to the Self-Service Portal URL. This URL follows the structure of **https://<AirWatchEnvironment>/MyDevice** where **<AirWatchEnvironment>** is the enrollment URL.

- **How to Authenticate into the Self-Service Portal** – End users need the Group ID, username and password to log into the Self-Service Portal (SSP) and register their device(s).

Once the end user receives the registration message, they will follow these simple steps to register their own device(s):

1. Navigate to the Self-Service Portal (SSP) URL: **https://<AirWatchEnvironment>/MyDevice**, where <AirWatchEnvironment> is the enrollment URL for your environment.
2. Enter the **Group ID** and credentials – either an email address or username and password – to login. (These can be directory service credentials for directory users.)
3. Select **Add Device** to launch the **Register Device** form.
4. Enter the device information by completing the required fields in the **Register Device** form.
5. Select **Save** to submit and register the device.

Device Registration Status

Occasionally, you may need to troubleshoot device registration or track the stage of the overall registration process. End users may accidentally delete the message containing registration instructions, or they might not redeem an authentication within the allotted expiration time. Manage registration status by accessing the **Registration Tab** on the left-panel menu of the **User Accounts** page. The options and actions available include:

- **Resend Message** – Simply resend the original message sent to a user, including Self-Service Portal URL, Group ID and login credentials.
- **Revoke Token** – Force the registration token status of selected devices to expire, essentially blocking access for unwanted users or devices.
- **Reset Token** – Reset a token's status if it has been revoked or is expired.
- **Delete Token** – Permanently delete the token for selected devices, forcing the user to re-register in order to enroll.

Blacklisting and Whitelisting Device Registration

Additional registration options provide control of the devices that end users are allowed to enroll. Particularly useful to BYOD deployments, prevent enrollment of blacklisted devices or restrict enrollment to only whitelisted devices by type, platform or specific device IDs and serial numbers. To blacklist and whitelist devices:

1. Navigate to **Devices** ▸ **Lifecycle** ▸ **Enrollment Status** and select **Add**.
2. Choose either **Blacklisted Devices** or **Whitelisted Devices** from the **Add** dropdown list.
3. Enter the list of device attributes (up to 30 at a time) and select the corresponding device attribute type, including IMEI, Serial Number or UDID.
4. Confirm which Organization Group the devices are blacklisted from or whitelisted to.
    - If blacklisting, check the **Additional Information** check box to attribute a **Platform** type to the list of devices to block devices by platform as well.
    - If whitelisting, choose **Ownership** from the dropdown menu to allow only devices according to ownership.
5. Select **Save** to confirm the settings.

Note: You can also upload a batch import of blacklisted and whitelisted devices by selecting the **Batch Import** option under **Add**.

Configuring Enrollment Options

Customize your enrollment workflow by incorporating advanced options available in the AirWatch Admin Console. Access additional Enrollment Options by navigating to **Devices ▸ Device Settings ▸ Devices & Users ▸ General ▸ Enrollment**.

Note: The **AirWatch Enrollment Processes Guide**, available via AirWatch Resources, walks you through these settings and gives additional context as to which you may want to configure.

Grouping

The **Grouping** tab allows you to view and specify basic information regarding Organization Groups and Group IDs for end users. Enable **Group ID Assignment Mode** allows you to choose how the AirWatch Mobile Device Management (MDM) environment assigns Group IDs to users:

- **Default** – Select this option if users are to be provided with Group IDs to use upon enrollment. The Group ID used determines what Organization Group the user is assigned to.
- **Prompt User to Select Group ID** – Enable this option to allow directory service users to select a Group ID from a list upon enrollment. The **Group ID Assignment** section lists available Organization Groups and their associated Group IDs. This does not require you to perform group assignment mapping, but does mean users have the potential to select an incorrect Group ID.
- **Automatically Select the Group ID** – This option only applies if you are integrating with user groups. Enable this option to ensure users are automatically assigned to Organization Groups based on their directory service group assignments. The **Group Assignment Settings** section lists all of the Organization Groups for the environment and their associated directory service user groups. Select **Edit Assignment** to modify the Organization Group/User Group associations and set the rank of precedence each group should have.

  For example, you have three groups, Executive, Sales, and Global, which are ranked in order of job role. Everyone is a member of Global, so if you were to rank that user group first it would put all of your users into a single Organization Group. By ranking Executives first, you ensure the few number of people belonging to that group are placed in their own appropriate Organization Group. By ranking Sales second, you ensure all Sales employees are placed in an Organization Group specific to sales. Ranking Global third means anyone not already assigned to a group – in this case executives and sales staff – will be placed in a separate Organization Group.

Restrictions

The **Restrictions** tab allows you to customize enrollment restriction policies by Organization Group and User Group roles, including the ability to:

- Create and assign existing enrollment Restrictions policies using the Policy Settings.
- Assign the policy to a User Group under the Group Assignment Settings area.
- Blacklist or whitelist devices by platform, operating system, UDID, IMEI, etc.

For more information, see Configuring Enrollment Restrictions.

Optional Prompt

Continuing to the **Optional Prompt** tab, you may decide to request additional device information or present optional messages regarding enrollment and MDM information. Choose one or multiple prompt options from the provided list, including:

- Prompt for Device Ownership Type
- Display Welcome Message
- Display MDM Installation Message
- Enable Enrollment Email Prompt

  Note: The Enrollment Email Prompt requests the email address from the end user in order to automatically populate that field in their user record. This is especially beneficial to organizations deploying email to devices using the {EmailAddress} lookup value.

- Enable Device Asset Number Prompt

Customization Options

Provide an additional level of end user support by configuring the **Customization** tab. Provide an enrollment support email address and phone number that the end user may use if they are unable to enroll their device for any reason. Additionally for iOS devices, provide a post-enrollment landing URL that the end user will be brought to upon successful enrollment. This URL may be a company resource, such as company website or login screen for additional resources.

Customizing Enrollment Messages and MDM Prompts

Customize the messages related to device enrollment and any future Mobile Device Management (MDM)-related prompts sent to a device. Customizing MDM messages reduces confusion of your users by showing a specific organization name in push notifications rather than an environment URL or simply "AirWatch."

To set up custom MDM enrollment messages:

1. Navigate to **Devices** ▸ **Device Settings** ▸ **General** ▸ **Enrollment** and select the **Customization** tab.
2. Select **Use specific Message Template for each Platform** and select a device activation message template from the drop-down for each platform. See **Creating Message Templates** below.
3. For iOS devices, optionally configure the following:
   - Enter a **post-enrollment landing URL** for iOS devices.
   - Enter an **MDM Profile message** for iOS devices, which is the message displayed in the install prompt for the MDM profile upon enrollment.
4. Select **Save**.

Creating Message Templates

You can create your own library of message templates customized by platform to cover the variety of enrollment scenarios you may encounter.

1. Navigate to **Devices** ▸ **Device Settings** ▸ **General** ▸ **Message Templates**. Select **Add**.
2. Set the **Category** field to match the category of your template. Options include **Administrator**, **Application**, **Compliance**, **Content**, **Device Lifecycle**, **Enrollment** and **Terms of Use**.
3. Set the **Type** that best corresponds to the subcategory. The **Type** field's options will depend upon the **Category** field setting.
4. Set the **Select Language** field. You may add languages to the drop-down listing by selecting the **Add** button next to the field.
5. You may optionally select the **Default** checkbox if you would like the template to be the default template for the chosen **Category**.
6. Choose the **Message Type** for the template. Your options are **Email**, **SMS** and **Push** notification.

   Note: You have two different environments while composing the **Email** message template, **Plain Text** and **HTML**. The **Plain Text** option features only a monospaced serif font (Courier) with no formatting options. The **HTML** option enables a **Rich Text** editing environment including fonts, formatting, heading levels, bullets, indentation, paragraph justification, subscript, superscript, image and hyperlink capability. The HTML environment supports basic HTML coding using the **Show Source** button which you can use to toggle between the **Rich Text** and source views.

7. Compose your message(s) by entering text to the **Message Body** field(s) and save your template by selecting the **Save** button.

Lifecycle Notifications

While the above procedure is used to customize a library of platform-specific messages and prompts, the **Lifecycle Notifications** setting enables you to deliver these customized messages after specific events during a device's lifecycle, including enrollment and unenrollment.

This optional setting can be configured by navigating to **Devices** ▸ **Lifecycle** ▸ **Setting** ▸ **Notifications** and enter the following fields for both **Enrollment** and **Unenrollment**.

Send Email To:

- **None** – Select this option to send no confirmation emails upon a successful device enrollment/unenrollment.
- **User** – Send a confirmation email to the device user informing them of the successful device enrollment/unenrollment.
  - **CC** – Send the same confirmation email to a single email address or multiple, comma-separated email addresses.

- **Message Template** – Select the desired message template from the drop-down listing. You have the option of adding a new message template or editing an existing template by selecting the "Click here..." hyperlink that takes you to the **Devices & Users** ▸ **General** ▸ **Message Templates** settings page.

- **Administrator** – Send a confirmation email to the AirWatch Administrator informing them of the successful device enrollment/unenrollment.
  - **To** – Send the same confirmation email to a single email address or multiple, comma-separated email addresses.

Blacklisting and Whitelisting Device Registration

Additional registration options enable you to control which devices are allowed to enroll.

For example, in a deployment of only corporate-owned devices, you might choose to create a whitelist of approved iOS devices. You can do this by adding a list of whitelisted devices by International Mobile Equipment Identity (IMEI), Serial Number, or Unique Device Identifier (UDID). This way, enrollment is restricted to only those devices you have identified, and AirWatch will not accept enrollment from employees' personal devices.

In addition, if a device is lost or stolen, you can add its IMEI, Serial Number, or UDID information to a list of blacklisted devices. This will unenroll the device, remove all MDM profiles and prevent enrollment until you remove the blacklist.

To blacklist or whitelist a device:

1. Navigate to **Accounts** ▸ **Users** ▸ **Enrollment Status** and select **Add**.
2. Choose either **Blacklisted Devices** or **Whitelisted Devices** from the **Add** dropdown list.
3. Enter the list of device attributes (up to 30 at a time) and select the corresponding device attribute type, including IMEI, Serial Number or UDID.
4. Confirm which Organization Group the devices are blacklisted from or whitelisted to.
   - If blacklisting, check the **Additional Information** check box to attribute a **Platform** type to the list of devices to block devices by platform as well.
   - If whitelisting, choose **Ownership** from the dropdown menu to allow only devices according to ownership.
5. Select **Save** to confirm the settings.

Note: You can also upload a batch import of blacklisted and whitelisted devices by selecting the **Batch Import** option under **Add**.

Configuring Enrollment Restrictions

You can set up additional enrollment restrictions to further control who can enroll and which device types are allowed. For example, you could create a restriction to only allow Android OS 4.0+ to enroll, which would be useful if you wanted to ensure email containerization for all Android devices with the AirWatch Email Container, which requires Android 4.0 and higher.

After your organization evaluates the number and kinds of devices your employees own and determines which ones make sense to use in your work environment, you can configure the following settings.

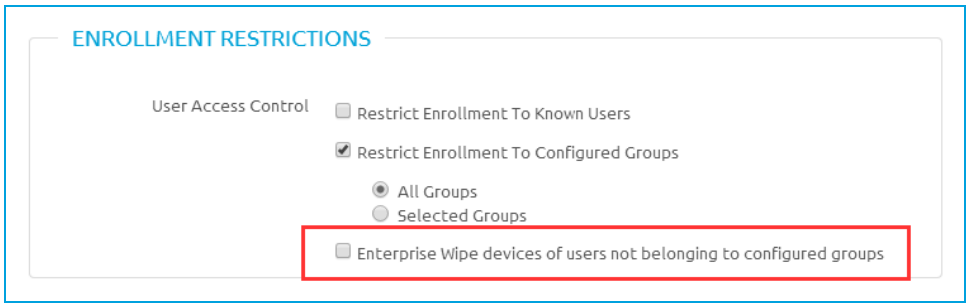
Enrollment Restrictions

When integrating AirWatch with directory services, you can choose whether or not to restrict enrollment to only known users or configured groups. Known users refers to users that already exist in the AirWatch Admin Console, while configured groups refers to users associated to directory service groups if you chose to integrate with user groups. These options are available by navigating to **Groups & Settings** ▸ **All Settings** ▸ **Devices & Users** ▸ **General** ▸ **Enrollment** and choosing the **Restrictions** tab.

- **Restrict Enrollment to Known Users** – Enable this option to restrict enrollment only to users that already exist in the AirWatch Admin Console. This applies to directory users you manually have added to the AirWatch Admin Console one by one or via batch import. It can also be used to lock down enrollment after an initial deployment that allowed anyone to enroll. This lets you to selectively allow only certain users to enroll.

  Leave this option unchecked to allow all directory users to create new AirWatch user accounts during enrollment. Since they do not already have an active AirWatch user account, they will use their directory service credentials to enroll.

- **Restrict Enrollment to Configured Groups** – Enable this option to restrict enrollment and only allow users belonging to All Groups or Selected Groups (if you have integrated with user groups) to enroll devices. You should not select this option if you have not integrated with your directory service user groups. Leave this option unchecked to allow all directory users to create new AirWatch user accounts during enrollment. In addition, you can select the **Enterprise Wipe devices of users not belonging to configured groups** option to automatically enterprise wipe any devices **not** belonging to any user group (if **All Groups** is selected) or a particular user group (if **Selected Groups** is selected).



Note: One option for integrating with user groups is to create an "MDM Approved" directory service group, import it to AirWatch, then add existing directory service user groups to the "MDM Approved" group as they become eligible for AirWatch MDM.

Note: For information about integrating your directory service groups with AirWatch, refer to the **AirWatch Directory Services Guide** document, available via AirWatch Resources.

Policy Settings

Save your enrollment restrictions as a policy by taking the following steps:

1. Navigate to **Devices** ▸ **Device Settings** ▸ **Devices & Users** ▸ **General** ▸ **Enrollment** and choose the **Restrictions** tab, then **Add Policy** located in the **Policy Settings** section. The **Add / Edit Enrollment Restriction Policy** screen will

display.

2. Enter an **Enrollment Restriction Policy Name** for your policy and select the **Organization Group** it should apply to.
3. Select the **Policy Type**, which can be either **Organization Group Default** to apply to the selected Organization Group, or **User Group Policy** to apply to specific User Groups via Group Assignment Settings on the **Restrictions** tab.
4. Identify the **Allowed Ownership Types**, which indicates whether you will permit or prevent bring your own device (BYOD).
5. Identify the **Allowed Enrollment Types**, which indicates whether you will permit or prevent enrollment through either the AirWatch Agent or AirWatch Container (for iOS/Android) apps.
6. Select the **Unlimited** check box for **Device Limit** to allow users to enroll as many devices as they want. Leave this box unchecked to enter values for the **Maximum Devices Per User** total or maximum devices per ownership type.
7. Select the **Limit enrollment to specific platforms, models or operating systems** option to add additional device restrictions based on device platform, device model, operating system version and, if applicable, enterprise version. You can also set a device limit. Choose one of two **Device Level Restriction Modes:**
   - **Only allow listed device types (Whitelist)** – Select this option to explicitly allow only devices matching the parameters you enter and to block everything else.
   - **Block listed device types (Blacklist)** – Select this option to explicitly block devices matching the parameters you enter and to allow everything else.

   Note: You can also block specific devices based on their IMEI, Serial Number or UDID by navigating to **Devices ▸ Lifecycle ▸ Enrollment Status** and selecting **Add**. This is an effective way to block a single device and prevent it from re-enrolling without affecting other users' devices. Preventing re-enrollment is also available as an option when performing an Enterprise Wipe.
8. Select **Save** and the **Add / Edit Enrollment Restriction Policy** screen will save your changes and close, taking you back to the **Devices & Users / General / Enrollment** screen.
9. Use the **Group Assignment Settings** section (scroll past the **Policy Settings** section) to assign customized policies to user groups. Set the rank of precedence and select a policy for each user group. This can be particularly useful if you are integrating with directory services.
10. Select **Save**.

Device Profiles

Profiles are the primary means by which you can manage devices. You can think of profiles as the settings and rules that, when combined with compliance policies, help you enforce corporate rules and procedures. They contain the settings, configurations and restrictions that you want to enforce on devices.

Create profiles for each platform type and configure a payload, which are the individual settings you configure (passcodes, Wi-Fi, restrictions or Virtual Private Networks (VPN)) for each one. Create a profile by navigating to **Devices** ▸ **Profiles** ▸ **List View**, selecting **Add** and choosing your appropriate platform.

Note: For step-by-step instructions on configuring a specific payload for a particular platform, please refer to the applicable **Platform Guide**, available via AirWatch Resources.

In This Section

- Configuring General Profile Settings – See how to set up a profile's **General** settings.
- Managing and Editing Device Profiles – See how to manage profiles from the **List View** after you create them.

Configuring General Profile Settings

The process for creating a profile consists of two parts. First, you must specify the **General** settings for the profile. The **General** settings determine how the profile is deployed and who receives it as well as other overall settings. Next, you must specify the **Payload** for the profile. The payload is the type of restriction or setting applied to the device when the profile is installed.

Note: The following profile settings and options apply to most platforms and can be used as a general reference. However, some platforms may offer different selections.

The general settings listed below apply to any profile:

1. Navigate to **Devices** ▸ **Profiles** ▸ **List View** and select **Add**.
2. Select the appropriate platform for the profile you wish to deploy.

   Depending on the platform you select, the following settings may vary.
3. Configure **General** settings on the applicable tab. These include:
   - **Name** – Name of the profile to be displayed in the AirWatch Admin Console.
   - **Version** – Read-only field that reports the current version of the profile as determined by the **Add Version** button.
   - **Description** – A brief description of the profile that indicates its purpose.
   - **Profile Scope** – Determines how the profile will be used.
     - **Production** – The profile is to be used as part of product provisioning.
     - **Staging** – The profile is to be used in staging configurations.
     - **Both** – The profile is to be used in both staging and provisioning.
   - **Deployment** – Determines if the profile will be automatically removed upon unenrollment:
     - **Managed** – The profile is removed.
     - **Manual** – The profile remains installed until removed by the end user.
   - **Assignment Type** – Determines how the profile is deployed to devices:
     - **Auto** – The profile is deployed to all devices automatically.
     - **Optional** – The end user can optionally install the profile from the Self-Service Portal (SSP) or can be deployed to individual devices at the administrator's discretion.
     - **Interactive** – This is a unique type of profile that is installed by end-users using the Self Service Portal. When installed, these special types of profiles interact with external systems to generate data to send to the device. This option will only be available if enabled in **Groups & Settings** ▸ **All Settings** ▸ **Devices & Users** ▸ **Advanced** ▸ **Profile Options**.

- **Compliance** – The profile is deployed when the end user violates a compliance policy applicable to the device.

- **Allow Removal** – Determines whether or not the profile can be removed by the device's end user:
  - **Always** – The end user can manually remove the profile at any time.
  - **With Authorization** – The end user can remove the profile with the authorization of the administrator. Choosing this option adds a required **Password** field.
  - **Never** – The end user cannot remove the profile from the device.
- **Managed By** – The Organization Group with administrative access to the profile.
- **Assigned Smart Group** – The Smart Group to which you want the device profile added. Includes an option to create a new Smart Group which can be configured with specs for minimum OS, device models, ownership categories, organization groups and more. See Smart Groups for more information.

  Note: While Platform is a criterion within a Smart Group, the Platform configured in the device profile or compliance policy will always take precedence over the Smart Group's platform. For instance, if a device profile is created for the iOS platform, the profile will only be assigned to iOS devices even if the Smart Group includes Android devices.

- **Exclusions** – If **Yes** is selected, a new field **Excluded Smart Groups** displays, enabling you to select those Smart Groups you wish to exclude from the assignment of this device profile. See Excluding Smart Groups in Profiles and Compliance Policies for details.
- **View Device Assignment** – After you have made a selection in the **Assigned Smart Group** field, you may select this button to preview a list of all devices to which this profile will be assigned, taking the Smart Group assignments and exclusions into account.
- **Additional Assignment Criteria** – These check boxes enable additional restrictions for the profile:
  - **Enable Geofencing and install only on devices inside selected areas** – Specify a configured geofence in which devices receive the profile only within the specified geographic limits. Selecting this option adds a required field **Assigned Geofence Areas**. See Geofences for more information.

    Note: Geofencing is available for Android and iOS only.

  - **Enable Scheduling and install only during selected time periods** – Specify a configured time schedule in which devices receive the profile only within that time-frame. Selecting this option adds a required field **Assigned Schedules**. See Time Schedules for more information.

    For more information on Time Schedules, please see the Mobile Device Management (MDM) Guide, available via AirWatch Resources
- **Removal Date** – The date the profile will be removed from the device. Must be a future date formatted as M/D/YYYY.

4. Configure a **Payload** for the device platform.

Note: For step-by-step instructions on configuring a specific **Payload** for a particular platform, please refer to the applicable **Platform Guide**, available via AirWatch Resources.

5. Select **Save & Publish**.

Configuring General Profile Settings for Product Provisioning Profiles

The product provisioning system allows you to create profiles for your devices.The profiles created for devices are installed or uninstalled as part of a product.

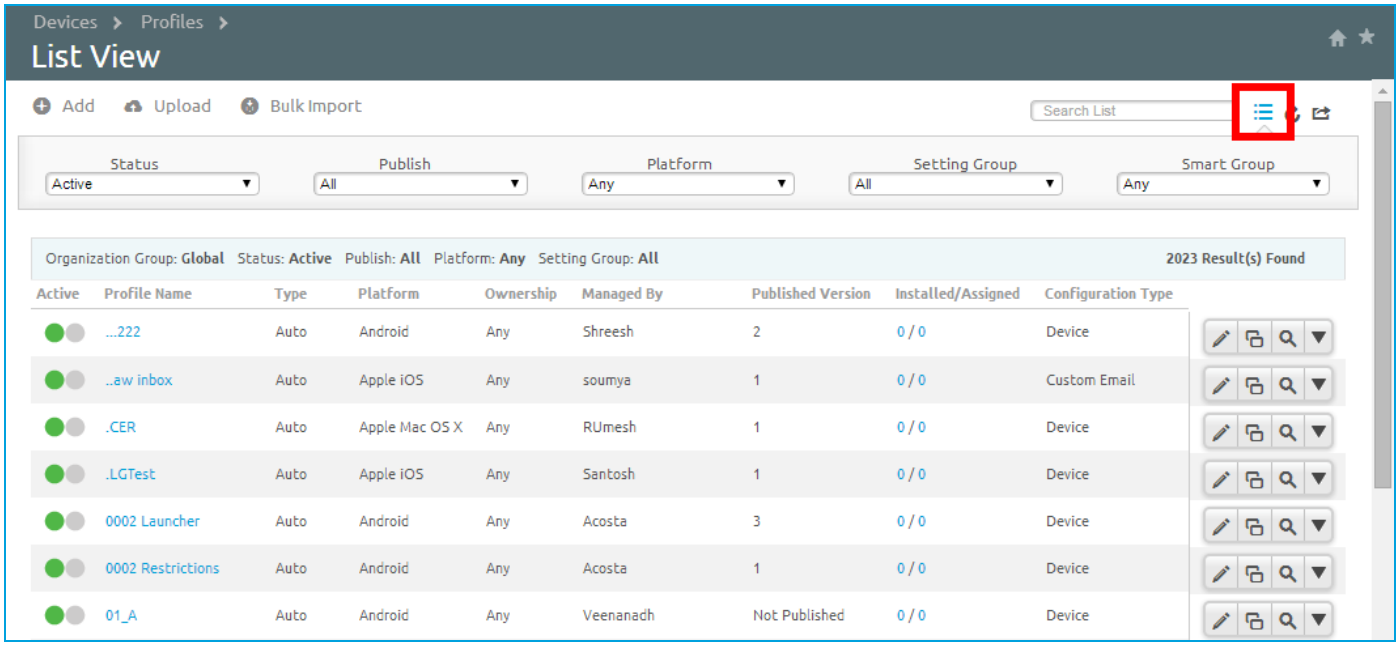
The process for creating a profile consists of two parts. First, you must specify the **General** settings for the profile. The **General** settings determine how the profile is deployed and who receives it as well as other overall settings.

Next, you must specify the **Payload** for the profile. The **Payload** is the type of restriction or setting applied to the device when the profile is installed.

To configure a profile, follow the steps detailed below:

Managing Device Profiles

After you have created profiles and assigned them to devices, you'll need a way to manage these settings one at a time and remotely from a single source. The **Devices ▸ Profiles ▸ List View** provides a centralized way to filter, sort and take actions on all profiles, including:



- **Toggle Filters** (highlighted above) – Filter the list of device profiles by status, platform, smart group and others.
- **Edit** – Customize an existing profile. Tweak major or minor settings in a profile to maintain the most effective Mobile Device Management (MDM) settings.

- **Publish** – Deploy the profile to all assigned devices. Update a device's profile settings depending on the user's (or device's) new role within your company.
- **View XML** – Display the XML code that AirWatch generates after profile creation. View and save the XML code to reuse or alter outside of the AirWatch Admin Console.
- **Edit Assignment** – Displays the General settings to change the Smart Group a profile is assigned to without republishing the profile to every assigned user.

  Note: Selecting the **Add Version** button will enable **Payload** editing and republish to all devices.

- **Delete** – Delete a profile and remove it from all devices. Maintain your roster of profiles by removing unnecessary profiles. For example, delete an outdated profile for roles or teams that do not exist anymore or have been phased out.
- **View Devices** – View devices that are available for that profile and whether the profile is currently installed and if not, see the reason why. Survey which devices are in your fleet and manually push profiles if necessary. For example, provide remote support for an end user who is requesting additional or necessary features.

Profile Installation Logging and Reporting with View Devices

During those infrequent cases in which profiles do not install on targeted devices, the **View Devices** screen enables you to see the specific reason why. Navigate to **Devices** ▸ **Profiles** ▸ **List View** and select the **View Devices** icon  .

The column **Command Status** reflects the current status of a profile's installation.

Command statuses include:

- **Error** – Displays as a link that, when selected, shows the specific error code applicable to the device.
- **Held** – Displays when the device is included in a certificate batch process that is currently underway.
- **Not Applicable** – Displays when a device is not impacted by the profile assignment but is nonetheless part of the Smart Group or deployment. For example, when the profile is not published to the device because of a deliberate profile assignment configuration.
- **Not Now** – Displays when the device is locked or otherwise occupied.
- **Pending** – Displays when the installation has been queued and is on schedule to be completed.
- **Success** – Displays when the profile has been successfully installed.

You also have the ability to produce a .csv (comma-separated value) file that can be read by Excel of the entire **View Devices** page. Select the **Export** icon  to take advantage of this new feature.

Additionally, you can customize which columns in the **View Devices** page you want to be visible. Select the **Available Columns** icon to utilize this feature.

Read-Only View

Device Profiles created in and managed by one Organization Group are in a read-only state when accessed by a logged-in administrator with lower-level privileges.

The profile window will reflect this by adding a special comment, “this profile is being managed at a higher organization group and cannot be edited.”

This read-only limitation applies to smart group assignments as well: when a profile is created at a parent organization group and is assigned to a smart group, a lower level OG admin logged in will be able to see the smart group to which the profile is assigned but the admin will not be able to edit it.

This maintains a hierarchy-based security while fostering communication among admins.

Editing Device Profiles

Using the AirWatch Admin Console, you can edit a device profile that has already been installed to devices in your fleet. There are two types of changes you can make to any device profile:

- **General** – Changes that serve to manage the profile's distribution: how the profile is assigned, by which Organization Group it is managed, to/from which Smart Group(s) it is assigned/excluded.
- **Payload** – Changes that affect the device itself: passcode requirement, device restrictions such as camera use or screen capture, Wi-Fi configs, VPN among others.

Since the operation of the device itself is not impacted, **General** changes can usually be made without re-publishing the profile. Saving such changes would result in the profile only being pushed to devices that were not already assigned to the profile.

Payload changes, however, must always be re-published to all devices, new and existing, since the operation of the device itself is affected.

To make **General** or **Payload** changes, edit an existing device profile by taking the following steps:

General Changes

1. Navigate to **Devices** ▸ **Profiles** ▸ **List View** and select the **Edit** icon  from the actions menu of the profile you wish to edit.

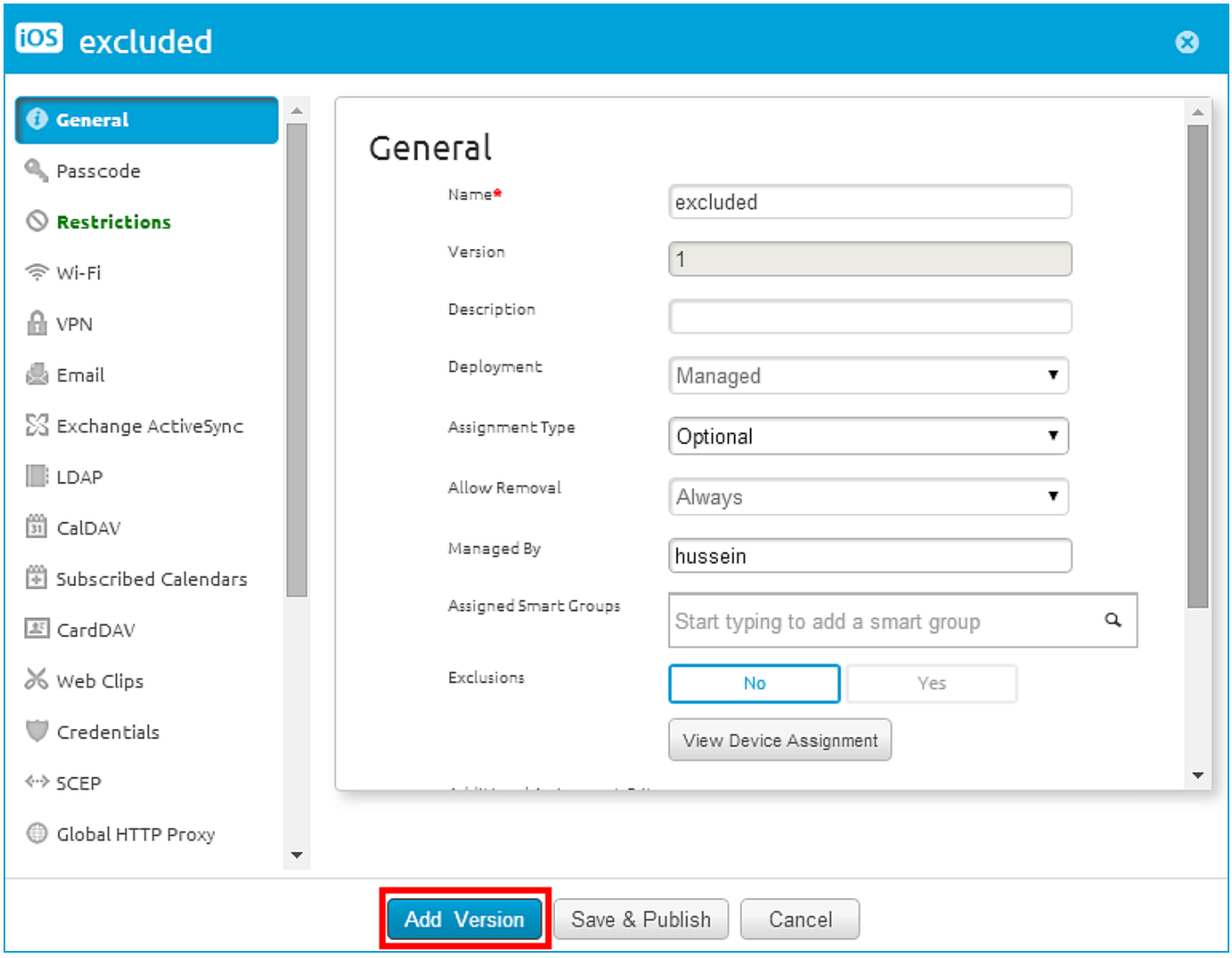
   Note: Only device profiles managed by that Organization Group or a child Organization Group below will be editable.

2. Make any changes you like in the **General** category. See Configuring General Profile Settings for a detailed listing of **General** category field descriptions.
3. After completing **General** changes, you may select **Save & Publish** to apply the profile to any *new* devices you may have added or removed. Devices already assigned with the profile will not receive the republished profile again. The **View Device Assignment** screen will appear, confirming the list of currently-assigned devices.

Payload Changes

Optionally, you may continue to make **Payload** changes:

The **Add Version** button enables you to create an increment version of the profile where settings in the **Payload** can be modified.



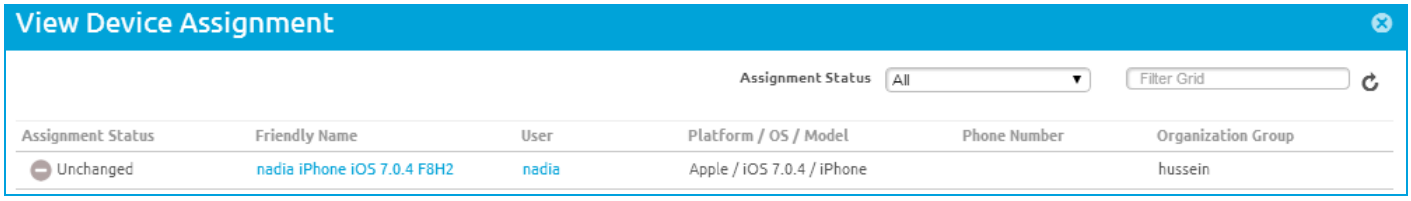
1. Select the **Add Version** button to enable **Payload** editing that impacts the operation of the device.

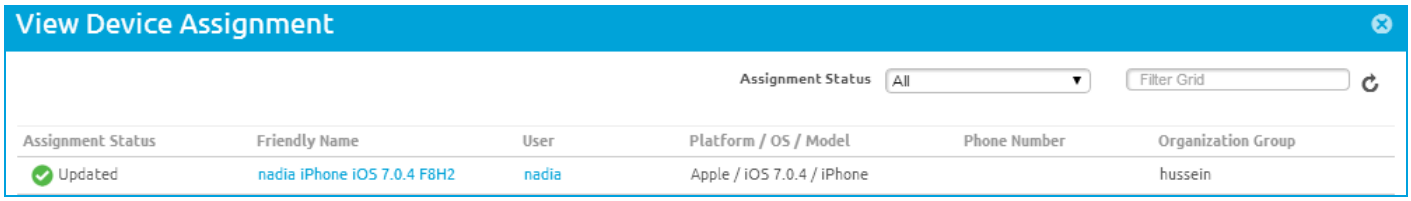
> **Note:** Selecting the **Add Version** button and saving your changes means re-publishing the device profile to *all* devices to which it is assigned, including devices that already have the profile. For step-by-step instructions on configuring a specific **Payload**, please refer to the applicable **Platform Guide**, available via AirWatch Resources.

2. After completing **Payload** changes, select **Save & Publish** to apply the profile to all assigned devices. The **View Device Assignment** screen will appear, enabling you to confirm the list of currently-assigned devices.

View Device Assignment

Selecting the **Save & Publish** button after configuring a profile displays the **View Device Assignment** screen and serves as a preview of affected (or unaffected) devices.





Depending upon which kind of change you make to the device profile, the **Assignment Status** column will reflect the following:

- **Added** – The profile will be added and published to the device.
- **Removed** – The profile will be removed from the device.
- **Unchanged** – Indicates the profile will not be republished to the device.
- **Updated** – Indicates the profile will be republished to a device that already has the profile assigned.

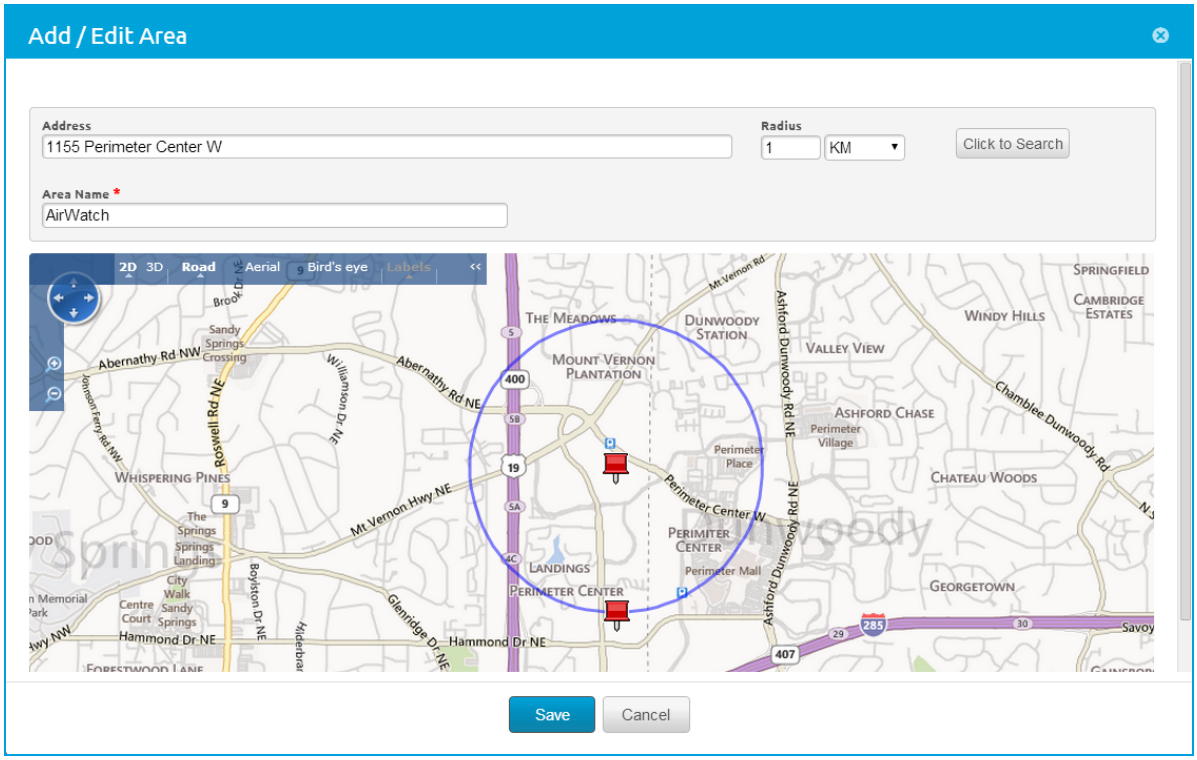
Select **Publish** to finalize the changes and, if necessary, re-publish any required profile.

Geofences

AirWatch enables you to define your profile with a Geofence, limiting the use of the device to specific areas including corporate offices, school buildings and retail department stores. You can think of a Geofence as a virtual perimeter for a real-world geographic area.

For example, a Geofence with a 1-mile radius could apply to your office, while a much larger Geofence could apply approximately to an entire state. Once you have defined a Geofence you can apply it to profiles, SDK applications, AirWatch apps such as the AirWatch Content Locker, and more.

Note: Geofencing is available for Android and iOS devices.



Enabling a Geofence is a two-step process:

1. Defining a Geofence
2. Applying a Geofence to a Profile

Supported iOS Devices

Geofencing for apps only works on iOS devices that have **Location Services** running. In order for location services function, the device must either be connected to either a cellular network or a Wi-Fi hotspot* or the device must have integrated GPS capabilities.

Devices in "airplane mode" result in location services (and therefore Geofencing) being deactivated.

Device	Wi-Fi*	Cellular Network	Built-In GPS
iPhone	✓	✓	✓
iPad Wi-Fi + 3G/4G	✓	✓	✓
iPad Wi-Fi	✓		
iPod Touch	✓		

*Wi-Fi hotspot must be in a location server database in order for the location services to retrieve a location.

Defining Geofences

Using geofencing profiles, you can allow or deny access to internal content and features based on a device's geographic location. For example, an organization may want to disable certain device features, enable VPN On Demand or automatically connect to Wi-Fi when inside its corporate offices.

Remember that while geofencing is combined with another payload to enable security profiles based on location, you should still only have one payload per profile.

To create a geofence:

1. Navigate to **Devices** ▸ **Profiles** ▸ **Profile Settings** ▸ **Geofencing** to access the Geofencing Settings page. Select **Add Area**.
2. Enter an **Address** and the initial **Radius** of the geofence.

   Additionally, you may double-click any area on the map to set the central location.
3. Select **Click to Search** to view on a map roughly where the geofence will be applied.

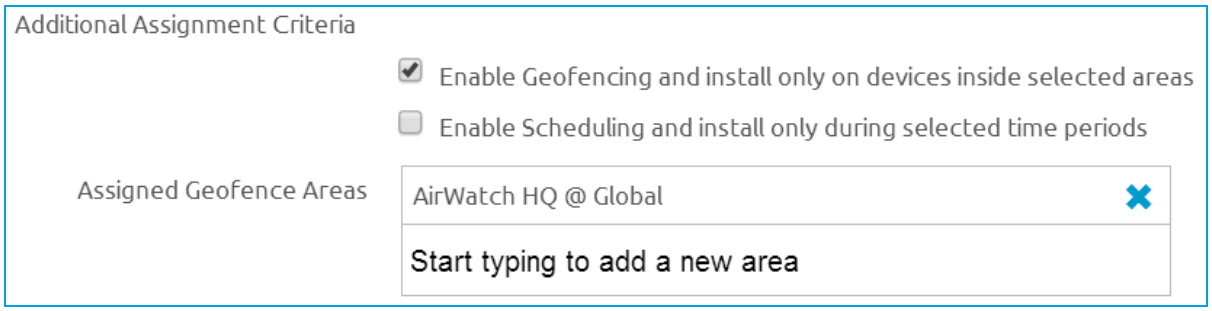
   Note: Integration with Bing maps requires that "insecure content" be loaded on this page. If location search does not load as expected, you may need to allow "Show all Content" for your browser.
4. Enter the **Area Name** (how it appears in the AirWatch Admin Console) and click **Save**.

Applying a Geofence to a Profile

Once you have defined a geofence area, you can apply it to a profile and combine it with other payloads to create more robust profiles.

For example, you can define geofence areas for each of your organization's offices and then add a Restrictions payload that disallows access to the Game Center, multiplayer gaming, YouTube content based on ratings and other settings. Once activated, the employees of the organization group to whom the profile was applied will no longer have access to these functions while in the office.

1. Navigate to **Devices** ▸ **Profiles** ▸ **List View** ▸ **Add** and select either **Android** or **iOS**.
2. Select **Enable Geofencing and install only on devices inside selected areas** on the **General** tab. An **Assigned Geofencing Area** box displays. If no Geofence Area has been defined, the menu directs you back to the Geofence Area creation menu.

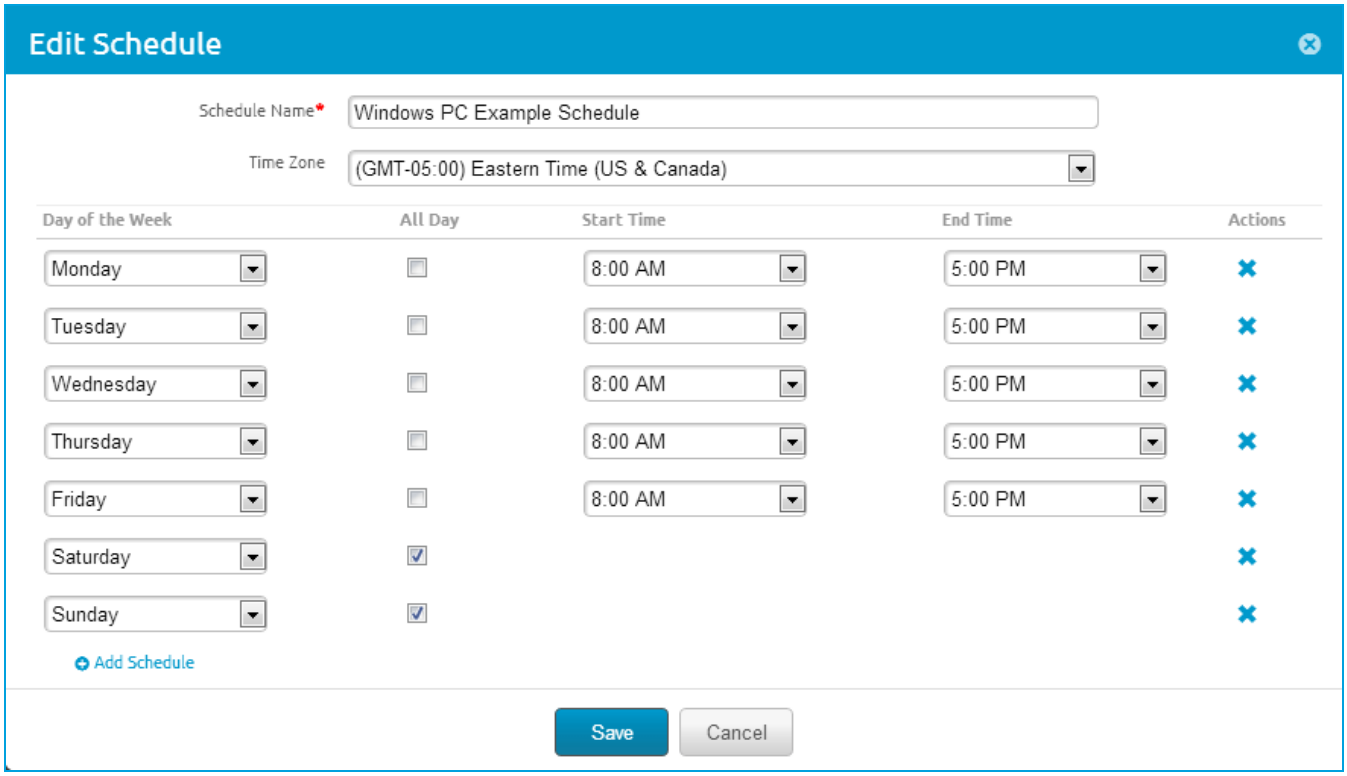


3. Enter one or multiple Geofencing areas to this profile.
4. Configure a payload such as Passcode, Restrictions or Wi-Fi that you want to apply only while devices are inside the selected geofencing areas.
5. Select **Save & Publish**.

Note: In the event that a user manually disables location services on their iOS device, AirWatch can no longer collect location updates and considers the device to be in the location where services were disabled.

Time Schedules

Time Schedules enable you to control *when* each device profile is active. Configure and apply time schedules to restrict when profiles are active on the device. Applying time schedules to profiles secures your corporate resources by only allowing employees access during the specific days and time frames. Conversely, applying time schedules can also limit personal content and access during work hours.



Once the time schedule is activated, the employees of the Organization Group to whom the profile was applied will no longer have access to these functions during the specified times.

Enabling a Time Schedule is a two-step process:

1. Defining a Time Schedule
2. Applying a Time Schedule to a Profile

Defining Time Schedules

You must define a time schedule before applying it to a device profile. To create a time schedule:

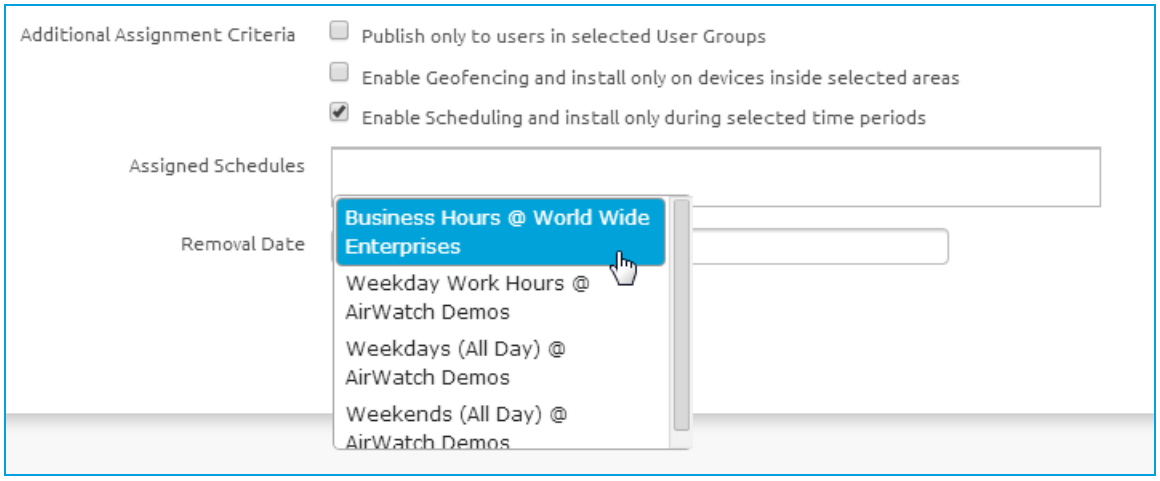
1. Navigate to **Devices** ▸ **Profiles** ▸ **Profile Settings** ▸ **Time Schedules**.
2. Select **Add Schedule** to launch the **Add Schedule** window.
3. Enter a name for the schedule in the **Schedule Name** field.
4. Select the applicable **Time Zone** using the drop-down menu.
5. Select the **Add Schedule** hyperlink.
6. Select the **Day of the Week**, **Start Time** and **End Time** using the applicable drop-down menus. You can also select the **All Day** check box to disable start and end times for the schedule.
   To remove a day from the schedule, select the applicable **X** under **Actions**.
7. Repeat steps 5 and 6 as many times as is necessary to add additional days to the schedule.
8. Select **Save**.

Applying a Time Schedule to a Profile

Once you have defined a time schedule, you can apply it to a profile and combine it with other payloads to create more robust profiles. For example, you can define time schedules for the normal work hours of different organization groups and add a Restrictions payload that denies access to the Game Center, multiplayer gaming or YouTube content based on ratings and other settings.

Once activated, the employees of the Organization Group to whom the profile was applied will no longer have access to these functions during the specified times.

1. Navigate to **Devices** ▸ **Profiles** ▸ **List View** ▸ **Add** and select your platform.
2. Select **Enable Scheduling and install only during selected time periods** on the **General** tab. An **Assigned Schedules** box displays.



3. Enter one or multiple Time Schedules to this profile.
4. Configure a payload, such as Passcode, Restrictions or Wi-Fi that you want to apply only while devices are inside the time frames.
5. Select **Save & Publish**.

Compliance

The **Compliance Engine** is an automated tool by AirWatch that ensures all devices abide by your policies, which may include basic security settings such as requiring a passcode and having a minimum device lock period. You may also decide to set and enforce password strength, blacklist certain apps and require device check-in intervals to ensure devices are safe and in-contact with the AirWatch servers.

Once configuration is complete and devices are found out of compliance, the Compliance Engine warns users to fix detected compliance errors to prevent disciplinary action on the device. For example, if a user loads blacklisted games or social media apps onto their device, the Compliance Engine sends a message to notify the user that their device is out of compliance. If the errors are not corrected in the amount of time specified, the device loses access to certain content and applications.

You may even automate the escalation process if corrections are not made. Lock down the device and notify the user to contact you to unlock the device. These escalation steps, disciplinary actions, grace periods and messages are all completely customizable with the AirWatch Admin Console.

Enforcing mobile security policies is as easy as:

- **Choosing your platform** – Determine on which platform you want to enforce compliance.
- **Building your policies** – Customize your policy to cover everything from application list, compromised status, encryption, manufacturer, model and OS version, passcode and roaming.
- **Defining escalation** – Configure time-based actions in minutes, hours or days and take a tiered approach to those actions.
- **Specifying actions** – Send SMS, email or push notifications to the user's device or send an email only to an Administrator. Request device check-in, remove or block specific profiles, install compliance profiles, remove or block apps and perform an enterprise wipe.
- **Configuring assignments** – Assign your compliance policy by organization group, Smart Group and confirm the assignment by device.

In This Section

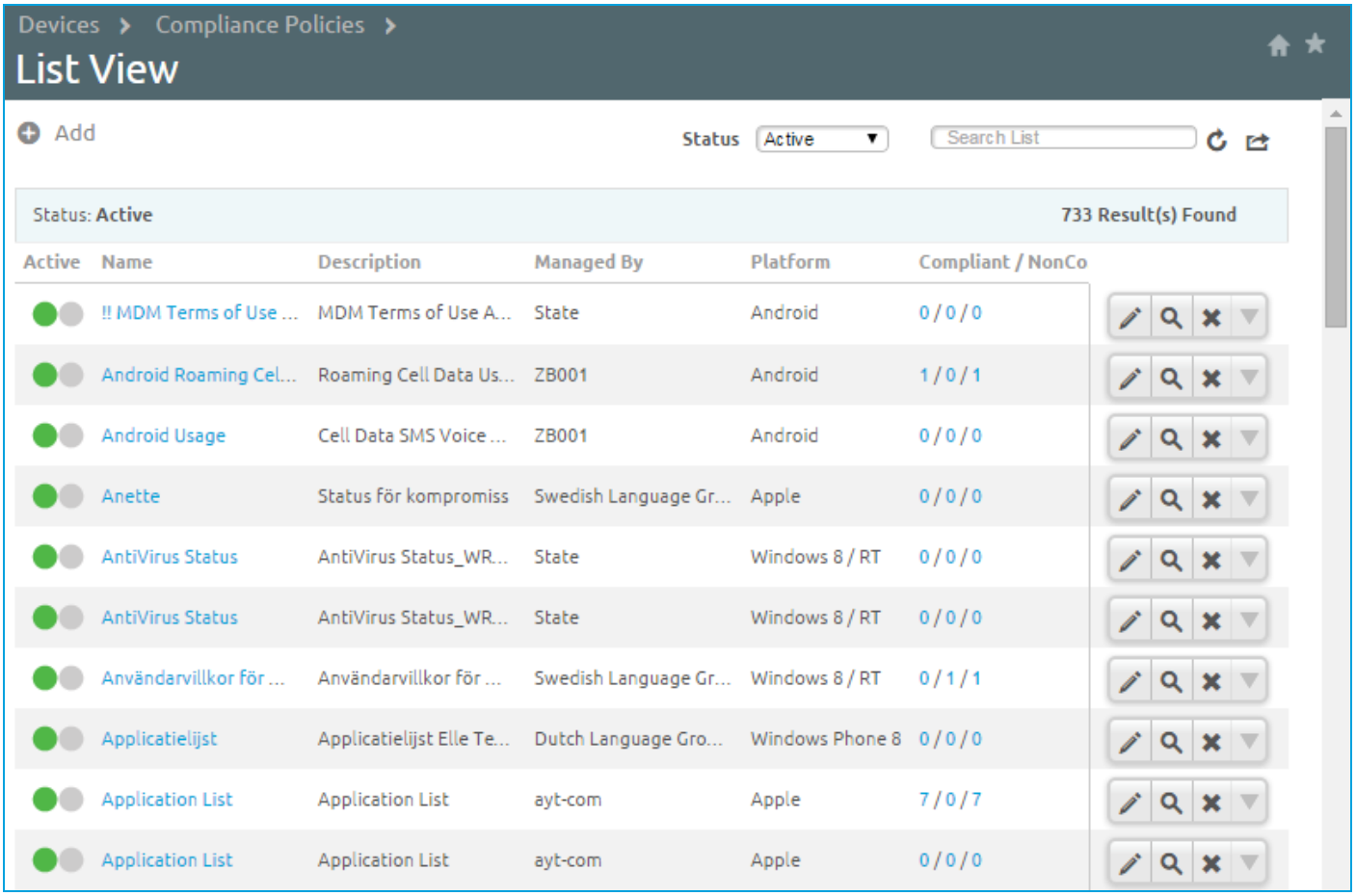
- Compliance Policies List View – Learn how to use the List View of Compliance Policies.
- Compliance Policies by Platform – Contains a table with each platform's supported compliance and a detailed description of each policy.
- Adding a Compliance Policy – Details the process of adding a new Compliance Policy.

Navigating Compliance Policies List View

The Compliance Policies List View lets you to see all the active and inactive compliance policies and their configurations.

The **Actions Menu**  enables you to view and edit individual policies, view devices to which the policy has

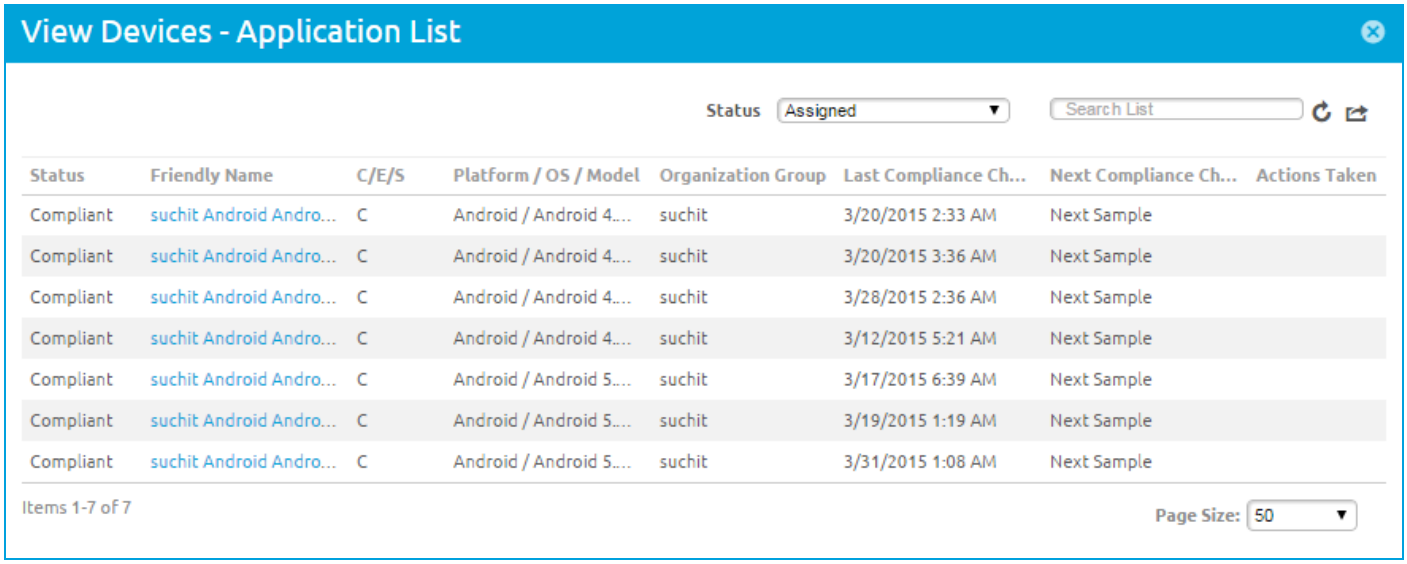
been assigned, and delete policies you no longer want to keep.



The three digits in the column titled **Compliant / NonCompliant / Assigned** features a hypertext link that, when selected, displays the **View Devices** page for the selected compliance policy.

View Devices

The **View Devices** page is used to view the assignment status for each device scheduled to receive the compliance policy.



Compliance Policies by Platform

The supported compliance policies by Platform are as follows:

Compliance Policy	Android	Apple iOS	Mac OS X	QNX	Windows Mobile	Windows PC (Win32)	Windows Phone 8	Windows 8/RT
Application List	✓	✓	✓					
Antivirus Status								✓
Cell Data Usage	✓	✓						
Cell Message Usage	✓							
Cell Voice Usage	✓							
Compromised Status	✓	✓						
Device Last Seen	✓	✓	✓	✓	✓	✓	✓	✓
Device Manufacturer	✓							
Encryption	✓	✓	✓			✓	✓	
Firewall Status								✓
Free Disk Space		✓						
Interactive Certificate Profile Expiry	✓	✓						
Last Compromised Scan	✓	✓						
MDM Terms of Use Acceptance	✓	✓	✓		✓	✓	✓	✓
Model	✓	✓	✓				✓	
OS Version	✓	✓	✓			✓	✓	✓
Passcode	✓	✓				✓	✓	
Roaming	✓	✓						✓
Roaming Cell Data Usage	✓	✓						
SIM Card Change	✓	✓					✓	
Windows Automatic Update Status								✓
Windows Copy Genuine Validation						✓		

Compliance Policies Detailed

- **Application List** – Detect 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, apps that have been blacklisted by the vendor, or specifically permit only the apps you specify, such as internal applications for

business use.

- **Antivirus Status** – Detect whether or not an antivirus program is running.
- **Cell Data/Message/Voice Usage** – Detect when end user devices exceed a particular threshold of their assigned telecom plan. For this policy to take effect Telecom must be configured. See the **AirWatch Telecom Guide**, available via AirWatch Resources, for more information.
- **Compromised Status** – Detect if the device is non-compliant when compromised.

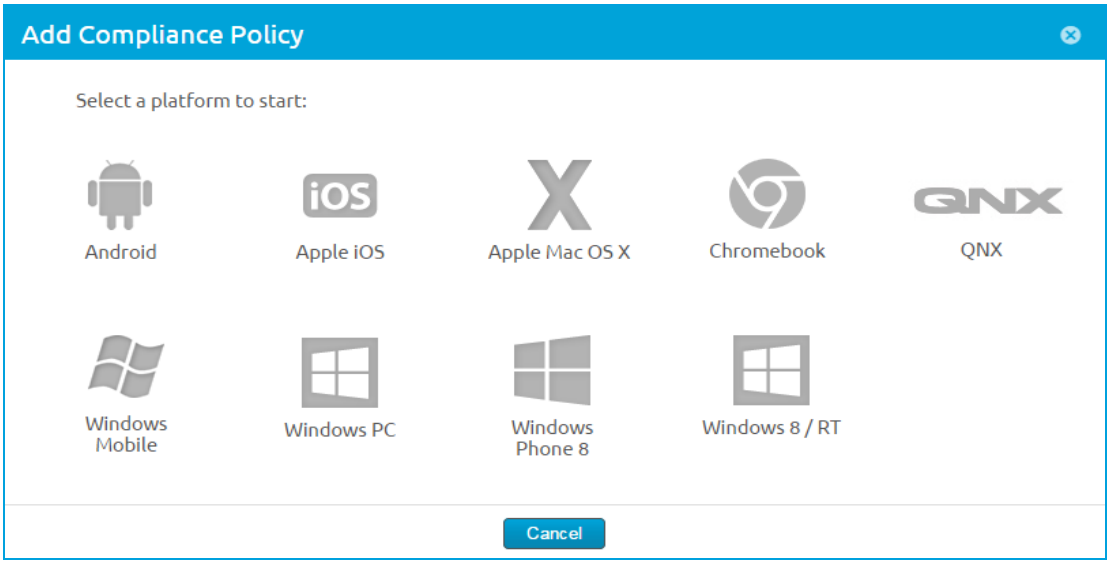
  Prohibit the use of jailbroken devices that are enrolled with AirWatch. Jailbroken devices strip away integral security settings and may introduce malware in your network and provide access to your enterprise resources. Monitoring for compromised device status is especially important in BYOD environments where employees have various versions of devices and operating systems. For more information, refer to the **Detecting Compromised Devices** document, available via AirWatch Resources.
- **Device Last Seen** – Detect if the device is non-compliant when the device fails to check in within an allotted time window.
- **Device Manufacturer** – Detect the manufacturer of the device allowing you to exclude certain devices.
- **Encryption** – Detect if the device is non-compliant when Encryption is not enabled.
- **Firewall Status** – Detect whether or not a firewall program is running.
- **Free Disk Space** – Detect the available storage space on the device.
- **Interactive Profile Expiry** – Detect if the device is non-compliant when an installed profile expires within the specified length of time.
- **Last Compromised Scan** – Detect if the device is non-compliant when AirWatch is unable to successfully query the device on schedule.
- **MDM Terms of Use Acceptance** – Detect if the device is non-compliant when the current MDM Terms of Use have not be accepted by the end user within a specified length of time.
- **Model** – Detect if the device is non-compliant based on a specific platform.
- **OS Version** – Detect if the device should be marked as non-compliant when it is within a certain window of OS versions that you configure.
- **Passcode** – Detect if the device is non-compliant when a passcode is not present.
- **Roaming** – Detect if the device is roaming.
- **Roaming Cell Data Usage** – Detect roaming cell data usage against a static amount of data measured in MB or GB.
- **SIM Card Change** – Detect if the device is non-compliant when the SIM Card has been replaced.
- **Windows Automatic Update Status** – Detect whether or not Windows Automatic Update has been activated.
- **Windows Copy Genuine Validation** – Detect whether or not the copy of Windows currently running on the device is genuine.

Note: Roaming, **Roaming Cell Data Usage**, and **Sim Card Change** is only be available for Telecom Advanced Users.

Adding a Compliance Policy

Follow the steps below to set up and initiate the Compliance Engine complete with profiles and automated escalations:

1. Navigate to **Devices** ▸ **Compliance Policies** ▸ **List View** and select **Add**.
2. Select a platform from the **Add Compliance Policy** screen on which to base your compliance policy. The available listing of rules, escalations and actions are platform-specific.

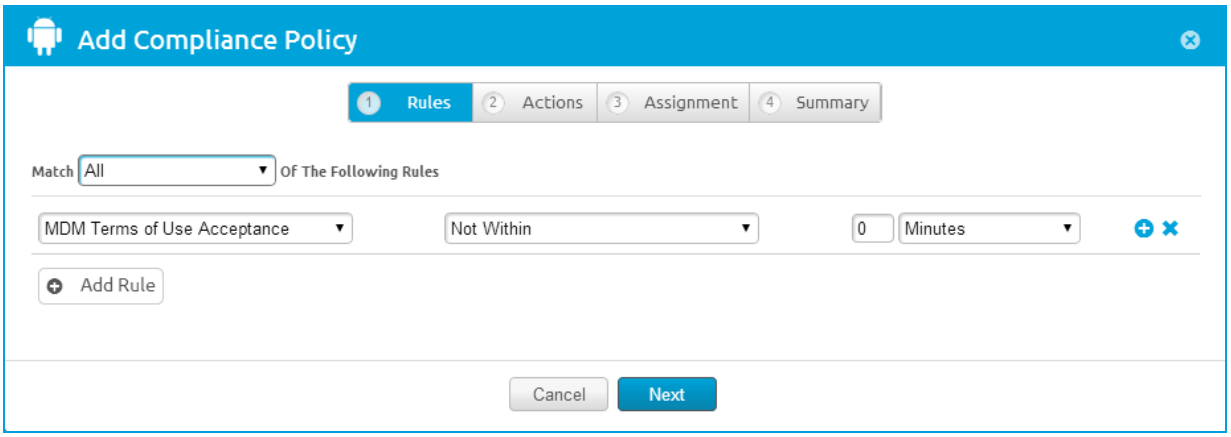


Note: Windows Mobile compliance is only supported on Motorola devices (compliance can only be enforced by the **Enterprise Reset** action).

Once a platform is selected, the **Rules** tab displays.

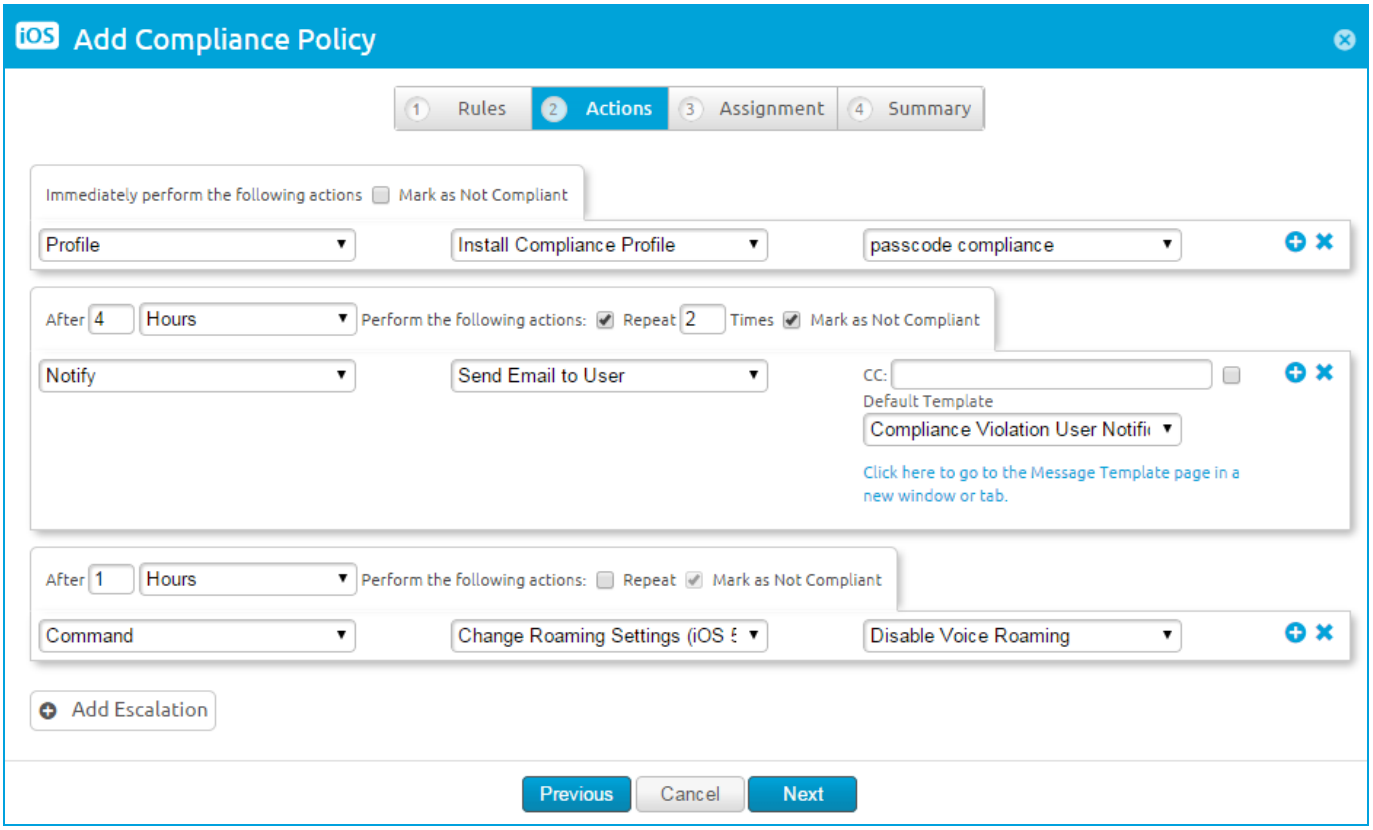
3. Configure the **Rules** tab by first selecting to match **Any** or **All** of the rules to detect conditions.

   Choose the rule from the drop-down field and set specific rule parameters.



- **Add Rule** – Select to add additional rules and parameters.
- **Previous** and **Next** – Select to go back to the previous step or advance to the next step, respectively.

4. Configure the **Actions** tab.



Specify **Actions** and **Escalations** that occur.

An **Escalation** is simply an automatic action taken if the prior **Action** does not cause the device user to take steps to make their device compliant. You may delay the escalation by minutes, hours or days. You may also opt to **Repeat** the escalation a selected number of times before the next scheduled action begins.

For email-related actions, there is a drop-down menu enabling you to select an email template. There is also a link that, when selected, displays the **Message Template** page in a new window, enabling you to customize your own message template. Enable this drop-down menu by deselecting the checkbox to the right of the **CC:** field.

The **Mark as Not Compliant** checkbox gives you the option of temporarily delaying the assignment of a noncompliant status to a device.

While *unchecked*, the **Mark as Not Compliant** checkbox enables you to perform an action on a device while temporarily preventing the device from being marked as not compliant. A compliant device has access to server resources a noncompliant device does not. Enabling a delay of noncompliant status enables you to proactively alert users about compliance risks (via email and text message alerts) while at the same time keeping the device able to access internal resources via the Mobile Access Gateway (MAG). The compliance engine accomplishes this by observing the following rules:

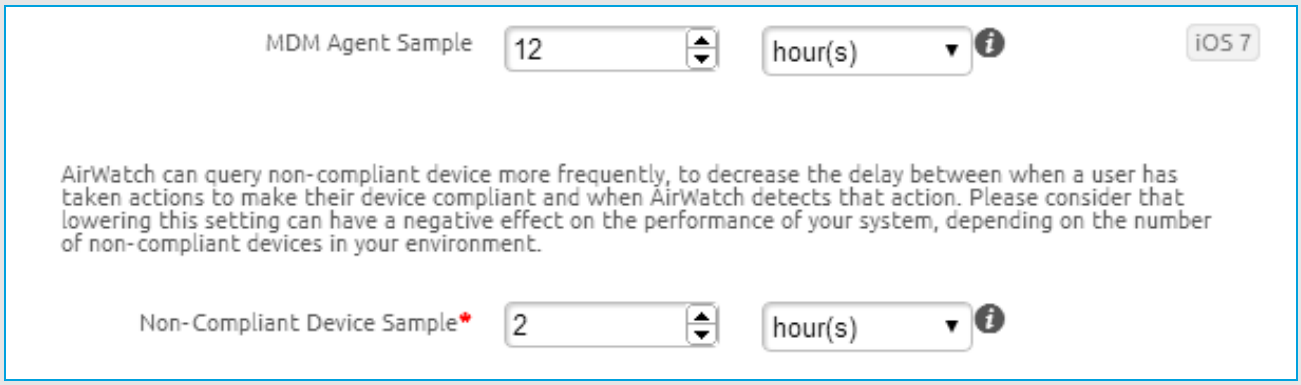
- The **Mark as Not Compliant** checkbox is enabled (checked) by default for each newly-added **Action**.
- If one action has the **Mark as Not Compliant** option enabled (checked), then all subsequent actions and escalations are also marked as not compliant (checked) and these subsequent checkboxes cannot be edited.
- If an action has the **Mark as Not Compliant** option disabled (not checked), then the next action/escalation has the option enabled by default (checked) but the checkbox can be edited.
- If an action or escalation has the **Mark as Not Compliant** option disabled (not checked) and the device does not pass the compliance rule, the device's compliance status will be officially 'compliant' and the action is executed.
- As the compliance rule progresses through the series of actions and escalations, the device's status will remain 'compliant' unless and until it encounters an action or escalation with the **Mark as Not Compliant** checkbox enabled (checked). Only then will the device be noncompliant.

Create an escalation by selecting the **Add Escalation** button. When adding escalations, it is a best practice to increase the security of actions with each additional escalation.

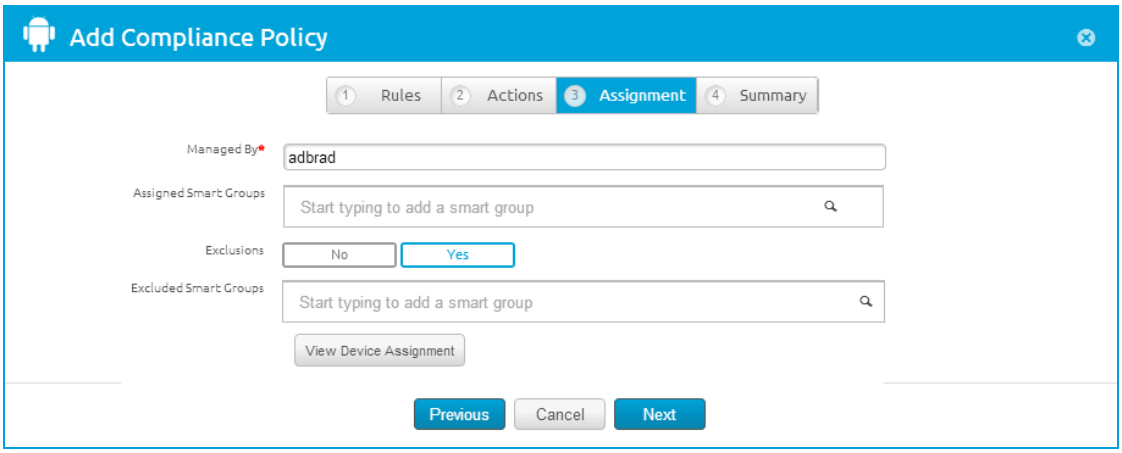
Select the options and type of actions to perform:

- **Application** – Block or remove a managed application.
  - You can enforce application compliance as well by establishing a whitelist, blacklist or required list of applications. For more information on establishing a robust and effective Mobile Application Management (MAM) plan, please see the **AirWatch MAM Guide**, available via AirWatch Resources.
- **Command** – Initiate a device check-in or execute an enterprise wipe.
- **Email** – Block the user from being able to use email.
  - The 'Block Email' action applies if you are using Mobile Email Management together with the Email Compliance Engine, which is accessed by navigating to **Email ▸ Compliance Policies ▸ Email Policies**. This lets you use Device Compliance policies such as blacklisted apps in conjunction with any Email Compliance Engine policies you configure. With this Action selected, email compliance is triggered with a single device policy update if the device falls out of compliance.
- **Notify** – Send an email, SMS or push notification to the device or administrator.
- **Profile** – Install, Remove or Block a specific Device Profile or a Device Profile type.

Tip: Query non-compliant iOS 7 and higher devices to decrease the delay between when a user has taken action to make their device compliant and when AirWatch detects that action. Set this sample by navigating to **Groups & Settings ▸ Settings ▸ Devices & Users ▸ Apple ▸ MDM Sample Schedule** and setting the **Non-Compliant Device Sample**.



5. Configure the **Assignment** tab by completing the following fields:



- **Managed By** – Select the Organization Group by which this compliance policy will be managed.
- **Assigned Smart Groups** – Select one or more Smart Groups to assign to this policy.

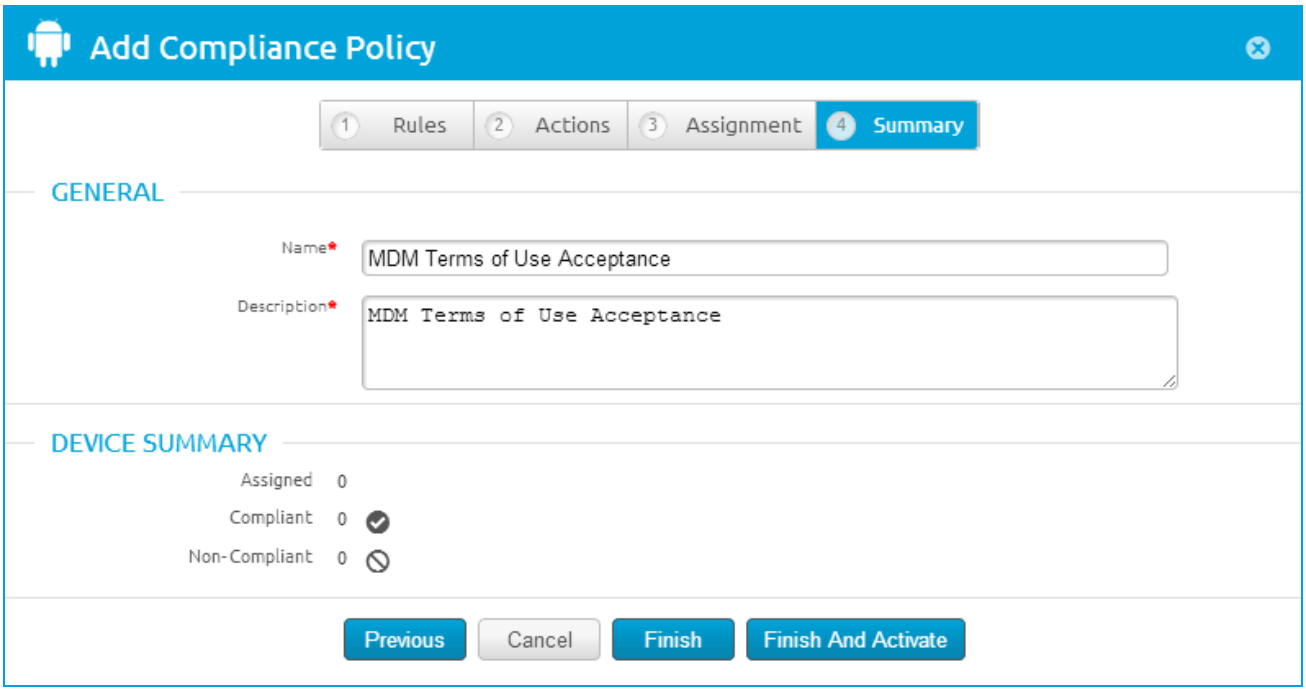
  For more information about Smart Groups please see the Mobile Device Management Guide available via AirWatch Resources.
- **Exclusions** – Decide if you want to exclude any Smart Groups by selecting **Yes** on the **Exclusions** field and select from the available listing of Smart Groups to exclude in the **Excluded Smart Groups** field. See Excluding Smart Groups in Compliance Policies for details.

  For more information about Smart Groups please see the Mobile Device Management Guide available via AirWatch Resources.
- You may optionally select the **View Device Assignment** button to see a listing of devices affected by this compliance policy assignment.

Note: While Platform is a criterion within a Smart Group, the Platform configured in the device profile or compliance policy will always take precedence over the Smart Group's platform. For instance, if a device profile is

created for the iOS platform, the profile will only be assigned to iOS devices even if the Smart Group includes Android devices.

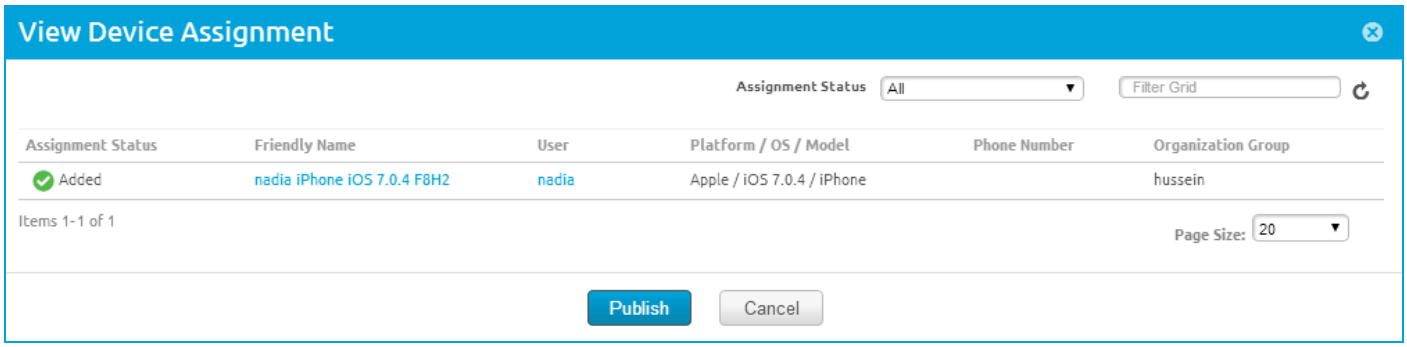
6. When finished determining the Assignment of this policy, select **Next**. The **Summary** tab displays.



- In this final step, provide a **Name** and a useful **Description** of the compliance policy.
- Complete the process by selecting one of the following:
  - **Finish** – Save your compliance policy without activating it to the assigned devices.
  - **Finish And Activate** – Save and apply the policy to all affected devices.

View Device Assignment

Selecting the **View Device Assignment** button on the **Assignment** tab while configuring a compliance policy displays the **View Device Assignment** screen and serves as a confirmation of affected (or unaffected) devices.



The **Assignment Status** column will display the following entries for the devices that appear in the listing:

- **Added** – The compliance policy has been added to the listed device.
- **Removed** – The compliance policy has been removed from the device.
- **Unchanged** – The device remains unaffected by the changes made to the compliance policy.

Select **Publish** to finalize the changes and, if necessary, re-publish any compliance policy.

Managing Devices

Overview

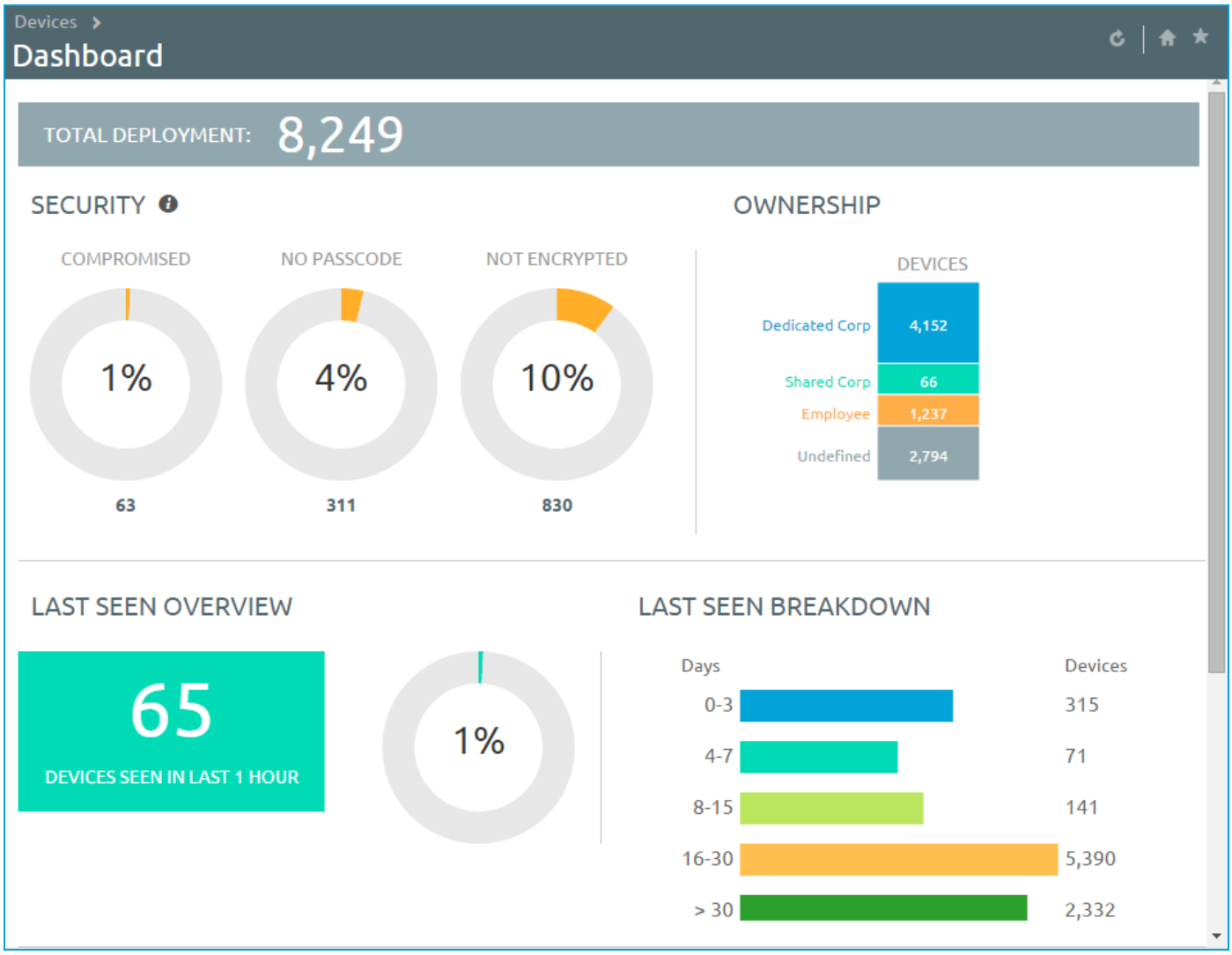
You can manage all of your deployment's devices from the AirWatch Dashboard, which is a searchable, customizable view you can use to filter and find specific devices based on various criteria. This simplifies performing actions and administrative functions on a particular set of devices. You may also generate **Reports** and examine the data flow within the AirWatch **Hub**. Additionally, you can easily identify devices with **Tags**. Lastly, you can set up the **Self-Service Portal** (SSP) to empower end users to manage their own devices and reduce the strain on Help Desk personnel.

In This Section

- Using the Device Dashboard – Covers stats and data about your devices available in the Device Dashboard.
- Using the Device List View – Details how to use the Devices List View to search for filter and perform remote actions on multiple devices.
- Using Device Actions – Presents a matrix summarizing the platform-specific remote actions an admin can invoke from the AirWatch Admin Console.
- Using the Device Details Page – Covers how to review and take action on a single device from the Device Details Page.
- Using Wipe Protection – Details how to set up wipe protection for your environment, which helps ensure large numbers of devices are not inadvertently wiped at once.
- Utilizing Reports – Explains where to create and generate ongoing reports with detailed information on all aspects of your deployment.
- Using the AirWatch Hub – Describes the data flow within AirWatch Hub and how to use the data.
- Using the Admin Panel – Review AirWatch software license information from a single screen.
- Using the Self-Service Portal – Details how end users can use the SSP to manage their own devices.
- Using the Mobile Console – Describes what you can see and do with the mobile version of the AirWatch Admin Console.
- Using Tags – Explains the concept behind device tags and how they are used to identify devices.

Using the Device Dashboard

As devices are enrolled, view and manage them from the AirWatch **Device Dashboard**. The **Device Dashboard** provides a high-level view of your entire fleet of mobile devices while allowing a quick and easy way to drill down to individual devices and take MDM actions. View graphical representations of relevant statistics, including important device information for your fleet, such as device ownership type, compliance statistics and platform breakdown.



Select any of the available data views from the **Device Dashboard** to quickly access each set of devices in the **List View**. From this **List View**, take administrative action, including send a message, lock devices, delete devices and change groups associated with the device.

Security

View security-related information related to your entire deployment, such as:

- **Compromised** – The number and percentage of compromised devices (i.e. jailbroken, rooted, etc.) in your deployment.
- **No Passcode** – The number and percentage of devices without a passcode configured for security.

- **No Encryption** – The number and percentage of devices that are not encrypted for security. This reported figure excludes Android SD Card encryption; only those Android devices lacking *disc encryption* will be reported in the donut graph.

If supported by the platform, you can configure a compliance policy to take action on these devices.

Ownership

View the total number of devices in each ownership category.

Last Seen Overview

View the number and percentage of devices that have recently communicated with the AirWatch MDM server. For example, if several hundred devices have not been seen in over 30 days, you can select the corresponding bar graph to pull of a List View of those devices, add additional filters if needed (e.g. Corporate Dedicated), and follow-up with the employees accordingly.

Platforms

View the total number of devices in each device platform category.

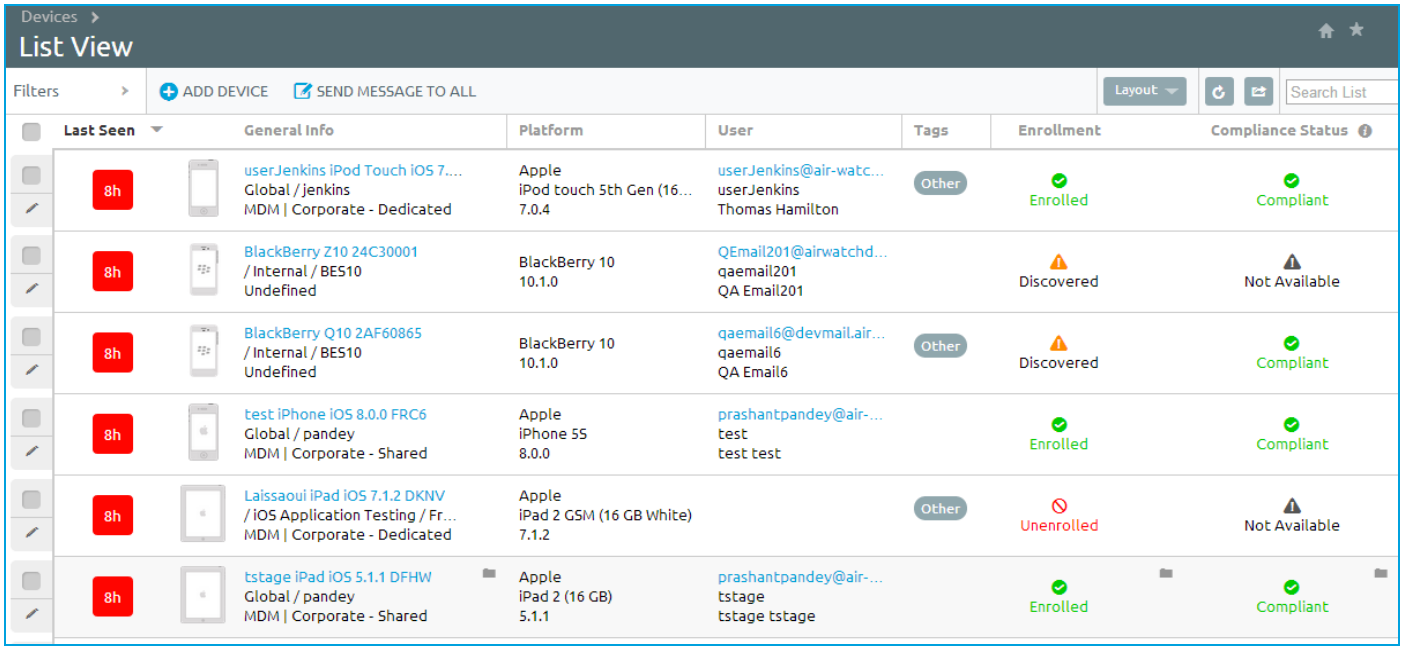
Enrollment

View the total number of devices in each enrollment category.

Using the Device List View

Switch to **Devices ▸ List View** at any time to sort and manage devices by filtering the available columns:

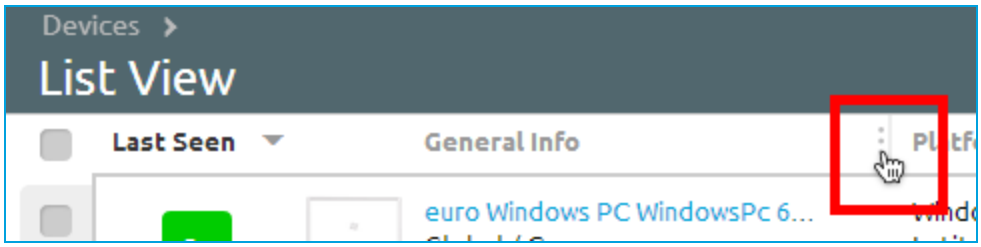
- Last Seen, Device Group, Notes, Wi-Fi MAC Address
- General Info (friendly name, first/last name, display name username, ownership, email, organization group, phone)
- Platform/OS/Model
- Home Carrier, Current Carrier
- Tags, Management, Enrollment
- Asset Number, Serial Number
- Compliance Status, Enrollment Status



Select a device **Friendly Name** at any time to open the device 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 take action on only those specific devices. Search all devices for a friendly name or user's name to isolate one device or user.

You may also rearrange the order of the columns as they are presented in the listing by dragging & dropping the column headings.

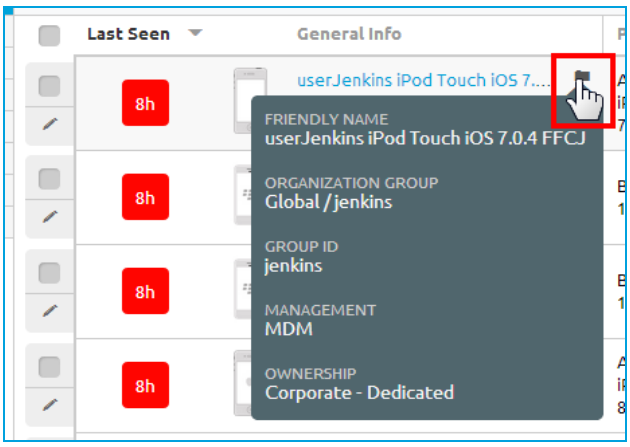


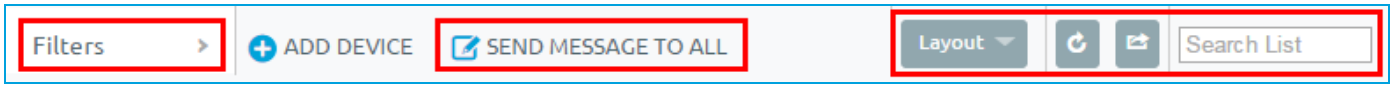
Once you have filtered the dashboard, you may export the data to a .csv file (comma-separated values) for review and analysis using Excel. Select the Export button  to utilize this feature.

Hover-Over Pop-up

Each device in the **General Info** column features a tooltip icon in the upper-right corner. When this icon is tapped (mobile touch device) or hovered-over with a mouse cursor (PC or Mac), it will display a Hover-Over Pop-up containing information such as the device's **Friendly Name**, **Organization Group**, **Group ID**, **Management** and **Ownership**.

Similar tooltip icons are found in the **Enrollment** and **Compliance Status** columns in the Device List view, featuring Hover-Over Pop-ups displaying **Enrollment Date** and **Compliance Violations** respectively.





Using Search

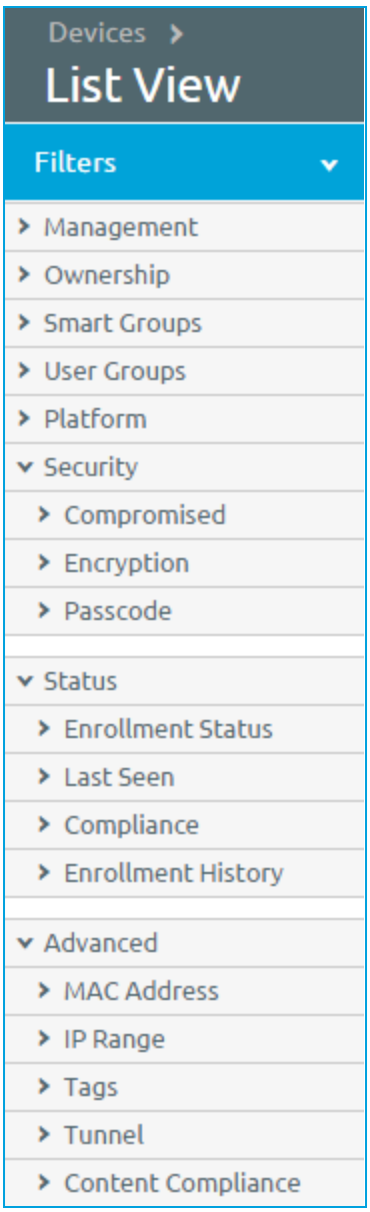
At times, you will need to search for a single device for quick access to its information and to take remote action on the device.

For example, search for a specific device, platform or user then navigate to **Devices ▸ List View** and select the **Search List** bar. This will initiate a search for all devices within the current Organization Group and all child groups.

Using Filters

You may also filter out entire categories of devices by utilizing the available filters:

- **Management**
- **Ownership**
- **Smart Groups**
- **User Groups**
- **Platform**
- **Security** (Compromised, Encryption, Passcode)
- **Status** (Enrollment Status, Last Seen, Compliance, Enrollment History)
- **Advanced** (MAC Address, IP Range, Tags, Tunnel, Content Compliance).



You can also search specific information across all fields associated with devices and users, allowing you to search for a user name ("John Doe") or a device type.

Using Bulk Actions

Once you have applied a filter to show a specific set of devices, you may perform bulk actions to multiple, selected devices by clicking the check box for those devices and selecting an action from the **Action** buttons.

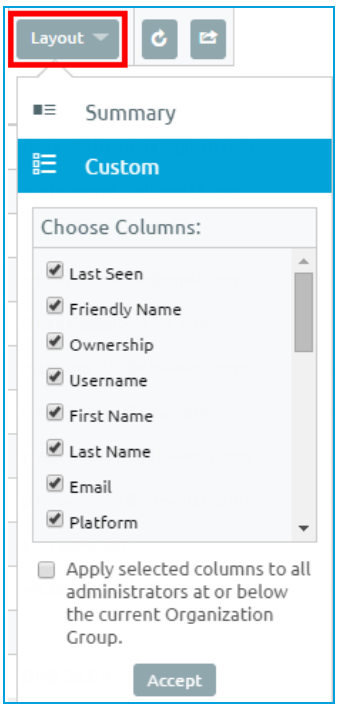
You can also select **Send Message to All** to send a message to all devices according to your current filters.

For example, if no filters are set, you will send a message to every device; but if you have filters applied for Android Compromised devices, then you will only send a message to those devices.

This action is only available if enabled in the system settings **(Groups & Settings ▸ All Settings ▸ System ▸ Security ▸ Restricted Actions)** and requires a PIN to perform.

Using Custom Layout

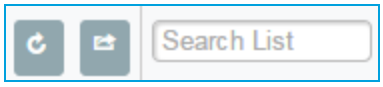
You may customize the visible columns in the **Device List** view by selecting the **Layout** button and choosing the **Custom** option. This displays the full listing of visible columns in the **Device List** view, which you may selectively choose to display or hide per your preferences.



There is also an option to apply your customized column view to all administrators at or below the current Organization Group. For instance, if you do not need to see the 'Asset Number' of a device, you can hide that column from a parent Organization Group and choose to hide it from the **Device List** views of all the child Organization Groups underneath.

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.

Using Refresh and Export

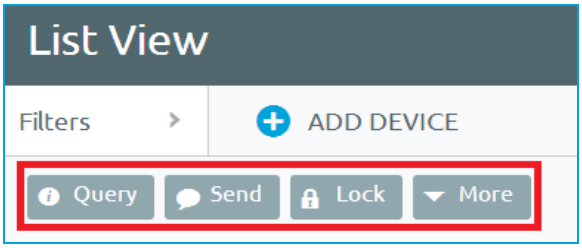


Select the **Refresh** button to re-send a query to the console to retrieve an up-to-date listing of devices. This can be useful in high-volume, high-activity environments.

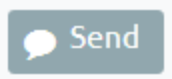
The **Export** button enables you to produce a full listing of filtered or unfiltered devices to a .csv file (comma-separated values) that you can view and analyze within Excel.

Using the Action Buttons

With the categorized devices displayed, you may take action on individual devices or initiate actions in bulk to multiple devices by selecting the check box next to each device and using the top Control Panel to execute the following actions:



Query – Query all selected devices for current device info, including last seen, OS, model and compliance status.



Send – Access Send Message menu and compose message to send to selected devices.

Lock – Lock all selected devices and force users to re-enter device security PIN.

More – View commands that you can perform on all selected devices. For example:

- **Management** – Query, lock or perform Enterprise Wipe on all selected devices.
- **Support** – Send a message to a device with instructions or communication to end user. Locate current GPS location of all selected devices.
- **Admin** – Change AirWatch Admin Console settings, including changing Organization Group, Ownership type or device 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 configuration for selected devices. Select Install Product to install a particular apps to selected devices.

See **Device Actions** for a full listing of platform-specific actions.

Note: The actions listed above will vary depending on factors such as device platform, AirWatch Admin Console settings and enrollment status.

Using Device Actions

The following matrix summarizes the platform-specific remote actions an admin can invoke from the AirWatch Admin Console. Enrolled devices have more actions available than their unenrolled counterparts.

Action	Android	Apple iOS	Apple OSX	Apple TV	Black-berry/10	Chrome-book	QNX	Symbian	Win Rugged	Win Legacy PC	Win-Mobile/ MDM	Win MDM
Add Tag	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AirWatch MDM Agent (Query)	✓	✓								✓ (*)		
App Remote View	✓	✓							✓			
Apps (Query)		✓	✓						✓	✓ (*)	✓	✓
BES Registration					✓ (10)							
Books (Query)		✓										
Certificates (Query)		✓	✓	✓					✓	✓ (*)	✓	✓
Change Device Passcode	✓										✓	
Change Organization Group	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Change Ownership	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Clear Activation Lock		✓										
Clear Passcode (Device)	✓	✓						✓	✓		✓	
Clear Passcode (Container)	✓											
Clear Passcode (Restrictions Setting)		✓										
Clear Passcode (SSO)	✓	✓										
Delete Device	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Device Information (Query)	✓	✓	✓	✓		✓			✓	✓ (*)	✓	✓
Device Wipe	✓	✓	✓	✓	✓			✓	✓		✓	
Edit Device	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓
Enroll	✓	✓	✓	✓							✓	✓
Enterprise Reset	✓								✓			
Enterprise Wipe	✓	✓	✓	✓	✓ (10)	✓	✓	✓	✓	✓	✓	✓
File Manager	✓						✓		✓			
Find Device	✓	✓									✓	
Location	✓	✓	✓		✓	✓		✓	✓			✓
Lock Device	✓	✓	✓		✓ (10)			✓		✓	✓	✓
Lock SSO	✓	✓										
Managed Settings		✓										
Mark Do Not Disturb	✓	✓										
Override Job Log Level	✓											
Profiles (Query)		✓	✓	✓		✓				✓ (*)		
Provision Now							✓		✓			
Query All	✓	✓	✓	✓		✓		✓		✓	✓	✓
Reboot Device	✓											
Registry Manager									✓			
Remote Control	✓					✓			✓			
Remote Management	✓						✓					
Remote View		✓										
Request Debug Log	✓											
Request Device Check-In		✓		✓		✓			✓			
Restart AirWatch Agent									✓			
Security (Query)		✓	✓	✓						✓ (*)	✓	✓
Send Message	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓

Start AirPlay		✓	✓									
Start AWCM	✓								✓			
Stop AWCM	✓								✓			
Sync Device	✓	✓		✓								
Task Manager									✓			
View Manifest									✓			
Warm Boot							✓		✓			

(*) This Windows PC device action is satisfied by executing a **Query All** command, which returns all the same information as if each individual Query command were executed separately.

(10) Applies only to BlackBerry 10 devices.

Add Tag – Assign a customizable Tag to a device, which can be used to identify a special device in your fleet.

AirWatch MDM Agent (Query) – Send a query command to the device's AirWatch MDM 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.

Note: AirWatch Content Locker must be installed on the device to execute **App Remote View**.

Apps (Query) – Send a query command to the device to return a list of installed apps.

BES Registration – Register your Blackberry device using this remote command and allow BES to manage the device instead of MDM. Applies only to Blackberry 10 devices.

Books (Query) – Send a query command to the device to return a list of installed books.

Certificates (Query) – Send a query command to the device to return a list of installed certificate authorities.

Change Device Passcode – Replace any existing device passcode used to access the selected device with a new passcode.

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.

Clear Activation Lock – Clear the Activation Lock on an iOS device. With the Activation Lock enabled, the user requires an Apple ID and password prior to taking the following actions: disabling Find My iPhone, factory wipe, and reactivate to use the device.

Clear Passcode (Container) – Clear the container-specific passcode. To be used in situations where the user has forgotten their device's container passcode.

Clear Passcode (Device) – Clear the device passcode. To be used in situations where the user has forgotten their device's passcode.

Clear Passcode (Restrictions Setting) – Clear the passcode that restricts device features such as app installation, Safari use, camera use and more.

Clear Passcode (SSO) – Clear the SSO passcode, for situations where the user has forgotten their single sign-on passcode.

Delete Device – Delete and unenroll a device from the 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 phone 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 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 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.

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 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** and **Phone Number** and **Note Description**.

Lock SSO – Lock the device user out of AirWatch Workspace and all participating apps.

Managed Settings – Enable or disable voice roaming, data roaming, and personal hotspots.

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.

Profiles (Query) – Send a query command to the device to return a list of installed device profiles.

Provision Now – Provision products to a device. Provisioning is the ability to create an ordered installation of files, actions, profiles and applications into a single product that can be pushed to devices.

Query All – Send a query command to the device to return a list of installed apps (including AirWatch MDM 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.

Registry Manager – Launch a Registry Manager within the AirWatch Console that enables you to remotely view a device's OS registry, add keys, conduct searches and add properties.

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.

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.

Remote View – Enable an active stream of the device's output to a destination of your choosing (including IP address, port, audio port, password and scan time), allowing you to see what the user sees as they operate the device.

Request Debug 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 troublehsoot and provide support.

Request Device Check-In – Request that the selected device check itself in to the AirWatch Console. This action updates the **Last Seen** column status.

Restart AirWatch Agent – Restart the AirWatch MDM Agent. To be used during troubleshooting for when the enrollment process or submodule installation process is interrupted.

Security (Query) – Send a query command to the device to return the list of active security measures (device manager, encryption, passcode, certificates, etc.).

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

Start AirPlay – Stream audiovisual content from the device to the AirWatch Console using Apple's proprietary wireless streaming protocol. You must provide the **MAC Address** (media access control) and **Scan Time** in seconds. Requires iOS 4.2 or greater.

Start/Stop AWCM – Start/Stop the AirWatch Cloud Messaging service for the selected device. 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 Admin Console, aligning its **Last Seen** status.

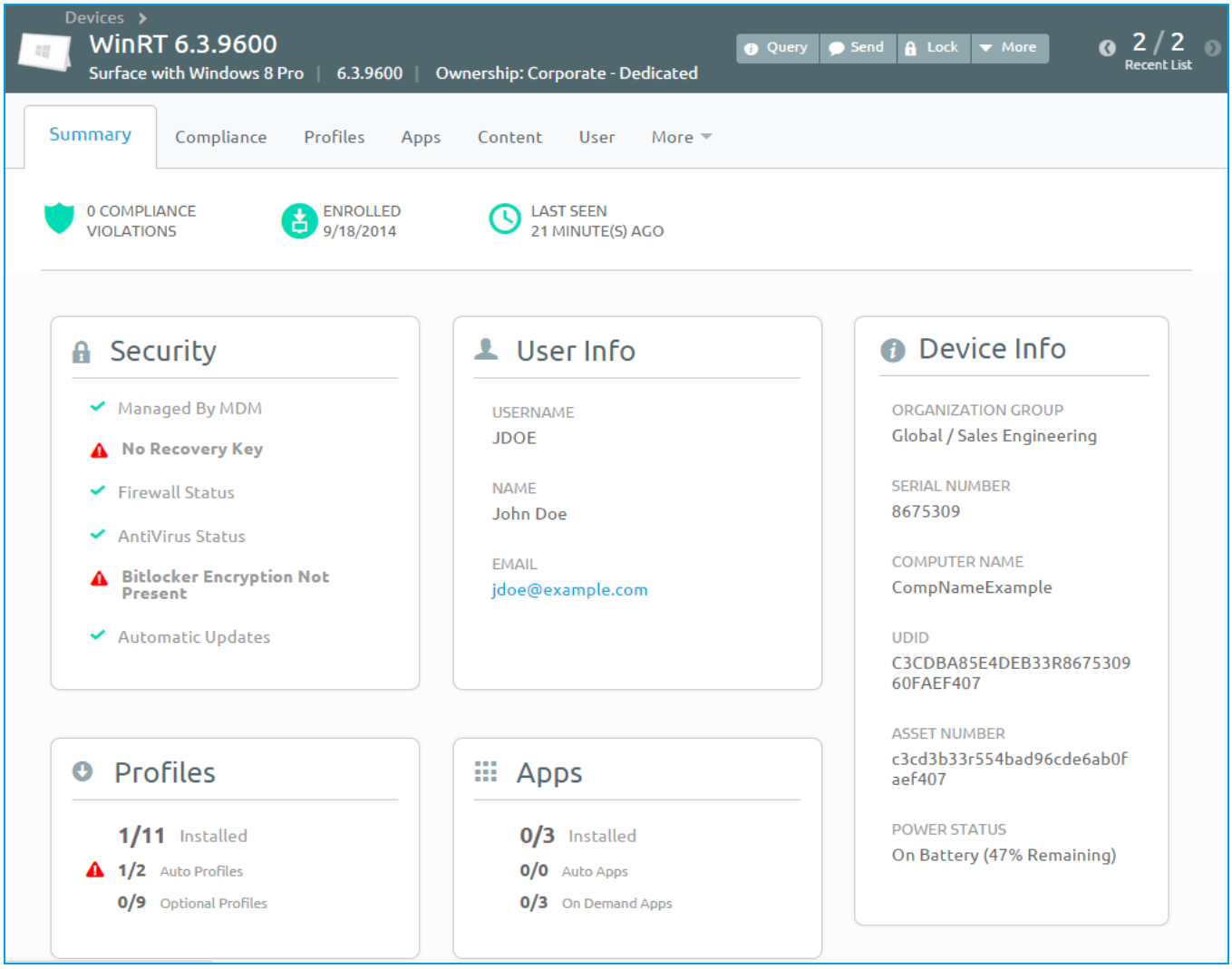
Task Manager – Launch a Task Manager within the AirWatch Console that enables you to remotely view a device's currently-running tasks, including task **Name**, **Process ID** and applicable **Actions** you may take.

View Manifest – View the device's **Package Manifest** in XML format from the AirWatch Admin Console. The manifest on Windows Rugged devices lists metadata for widgets and apps.

Warm Boot – Initiate a restart of the operating system without performaing a power-on self test (POST).

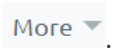
Using the Device Details Page

Use the **Device Details** page 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 **List View** page, from one of the available Dashboards or by using any of the available search tools with the AirWatch Admin Console.



The menu tabs you can use to access specific device information will vary depending on device platform. Some of the most common ones include:

- **Summary** – View general statistics such as enrollment status, compliance, last seen, platform/model/OS, Organization Group, contact information, serial number, power status, storage capacity, physical memory and virtual memory.
- **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 assigned and installed on a device.
- **Apps** – View all apps currently assigned and installed on the device.
- **Content** – View the status, type, name, version, priority, deployment, last update, date and time of views, acknowledged (reflecting whether required content has been acknowledged) of content on the device. This tab also provides 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 clicking **More** from the main **Device Details** tab 

. These additional menu tabs vary based on device platform. Some of the common ones include:

- **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.
- **Targeted Logging** – View the logs for the Console, Catalog, Device Services, Device Management and Self Service Portal. A link is provided enabling you to configure targeted logging.
- **Attachments** – Use this storage space on the server for screenshots, documents and links for troubleshooting and other purposes without taking up space on the device itself.

Using Wipe Protection

By configuring Wipe Protection settings, you can exert more control over how and when devices can be wiped to avoid mass wiping devices.

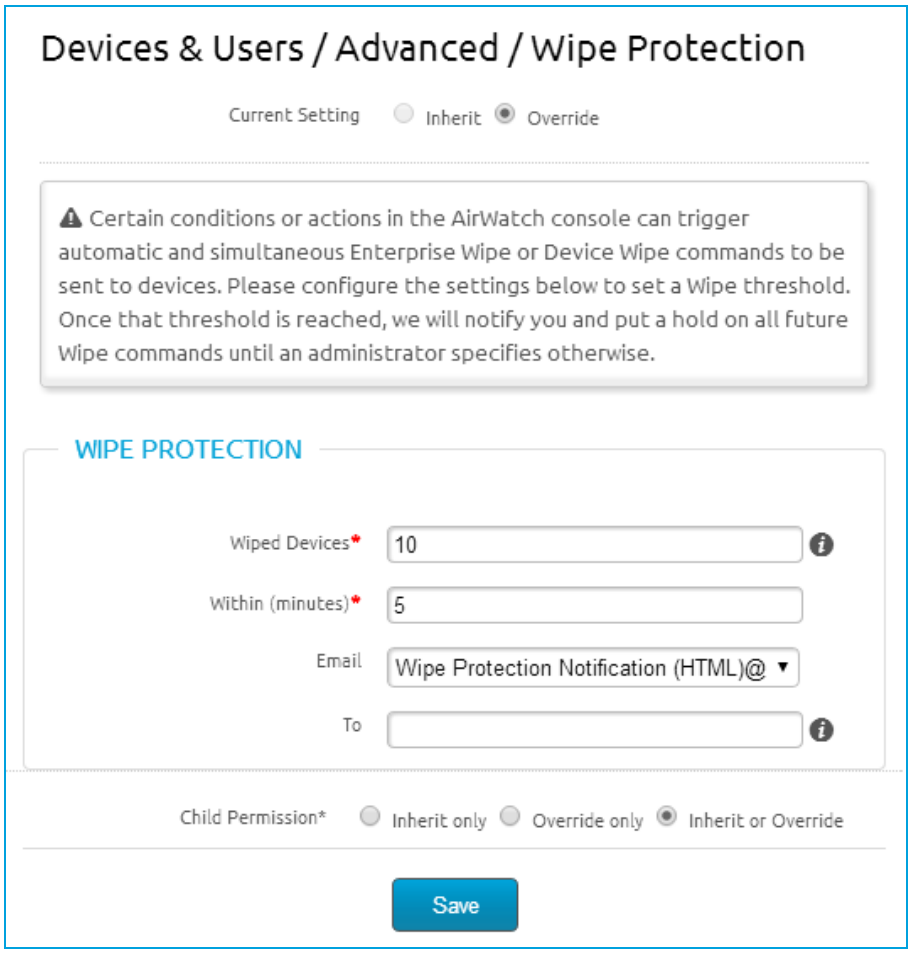
A device threshold is when a certain number of devices are automatically wiped or wiped as a result of an enterprise wipe or device wipe command, within a defined period of time.

Once this device threshold is exceeded, all subsequent wipe commands are put on hold and you and other administrators can optionally be notified. From that point you can review wipe logs to see when devices were wiped and for what reason. After reviewing the information you can accept or reject the on-hold wipe commands and unlock the system to reset the device threshold counter.

Configuring Wipe Protection Settings

Note: You can only configure these settings at the Global or Customer level Organization Group.

Set a device threshold limit and amount of time in minutes by taking the following steps:



1. Navigate to **Groups & Settings** ▸ **All Settings** ▸ **Devices & Users** ▸ **Advanced** ▸ **Wipe Protection**.
2. Enter the number of **Wiped Devices** that will act as your threshold for triggering wipe protection.
3. Enter the value for **Within (minutes)** which is the set amount of time the wipes must occur in to trigger wipe protection.
4. Select a message template to email to administrators.

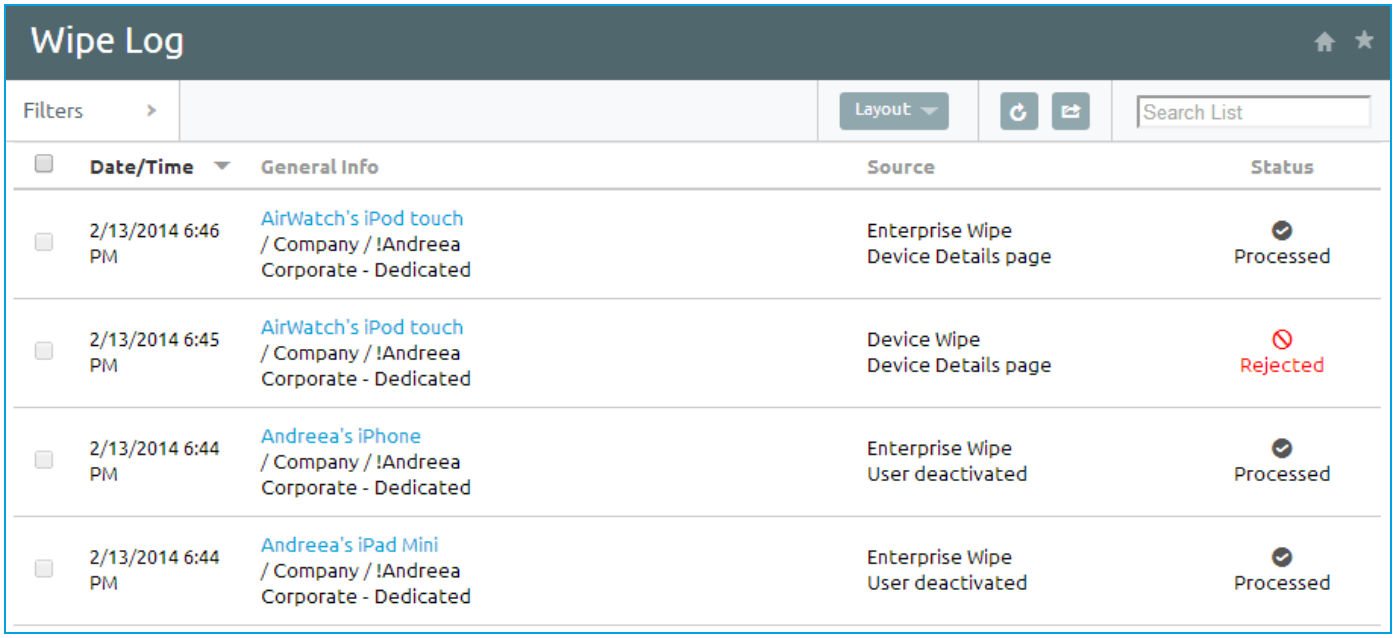
   Create a message template for wipe protection by navigating to **Devices & Users** ▸ **General** ▸ **Message Templates**, adding a new template and selecting **Device Lifecycle** as the **Category** and **Wipe Protection Notification** as the **Type**. You can use the following lookup values as part of your message template:

   - {EnterpriseWipeInterval} – The value of **Within (minutes)** on the settings page.
   - {WipeLogConsolePage} – A link to the Wipe Log page.

5. Enter the email addresses of administrators who should receive this notification message. You should only notify administrators who have access to the Wipe Log page.
6. Select **Save**.

Viewing Wipe Logs

If the device threshold limit is exceeded within the specified timeframe, then you can view the Wipe Log page to see when devices were wiped and for what reason. After reviewing the information you can accept or reject any on-hold wipe commands and unlock the system to reset the device threshold counter.



Note: If the system is locked then you will see a banner at the top of the page indicating this status.

1. Navigate to **Devices** ▸ **Lifecycle** ▸ **Wipe Log**. Access to this page is managed by the **Report Device Wipe Log** resource and is available by default for system admins, SaaS admins, and AirWatch admins. You can add it to any custom admin role using the **Roles** page.
2. View the list of devices and determine whether these are valid wipes. Devices pending action will have a status of On Hold.

   If they are, then select each device and then select **Approve wipe(s)** from the command list. The status will change to Approved.

   If they are not, then select each device and then select **Reject wipe(s)** from the command list. The status will change to Rejected.

   Note: Devices wiped before the threshold limit was reached will display as Processed.

   After you have taken action on each device, you must unlock the system to reset the device threshold counter to zero and allow wipe commands to go through until the threshold limit is exceeded.

3. Select **Unlock System** from the top of the page.

   You can only perform this action at a Global or Customer level Organization Group.

Utilizing Reports

AirWatch has extensive reporting capabilities that provide administrators with actionable, result-driven statistics about their device fleets. You can leverage these pre-defined reports or create custom reports based on specific devices, user groups, date ranges or file preferences. In addition, you can schedule any of these reports for automated distribution to a group of users and recipients on either a defined schedule or a recurring basis. These features are all centralized within the AirWatch Admin Console.

To access the Reports page, navigate to **Hub ▸ Reports & Analytics ▸ Reports ▸ List View**. From here, there are several key pieces of functionality that you can use to leverage AirWatch reporting capabilities:

Generating Custom Reports

You can create custom reports on the fly using the AirWatch Admin Console. To generate a custom report:

1. Navigate to the **Reports** page at **Hub ▸ Reports & Analytics ▸ Reports ▸ List View**.
2. Select a pre-defined report template from the list and then from the **Actions** bar click **View**.

Adding a Report to My Reports

Adding a report to My Reports allows you to essentially “bookmark” popular reports that you find particularly useful. To add a report to My Reports:

1. Navigate to the **Reports** page at **Hub ▸ Reports & Analytics ▸ Reports ▸ List View**.
2. Select a pre-defined report template from the list and then click the **Actions** icon on the right and then from the **Actions** bar click **Add to My Reports**.

From now on the report will be accessible from the **My Reports View** on the left side of the **Reports** page for quick access.

Creating Report Subscriptions

Report subscriptions can be used to send custom generated reports to specific recipients at a scheduled occurrence. To subscribe to a report:

1. Navigate to the **Reports** page at **Hub ▸ Reports & Analytics ▸ Reports ▸ List View**.
2. Select a pre-defined report template from the list and then from the **Actions** icon on the right, select the **Subscribe** button.
3. Complete the Report Subscriptions Form with all required information.
   - **General Information** – The name of the subscription, the email subject, etc.
   - **Report Parameters** – The parameters defining the scope and options of the report.

- **Distribution List** – The recipients who will receive the custom report whenever the subscription is executed.
- **Execution Schedule** – The time and schedule at which the custom report is generated.

4. Select **Save**.

Additional Reporting Tools

There are also several other additional tools that help you utilize AirWatch reporting capabilities:

- **Search Assistance Tools** – The **Report Category** drop-down menu and Search Box at the top of the reports page make finding particular reports very simple.
- **Report Samples Tool** – To view a sample output from a particular report, click the **Actions** icon on the right and then click the **Sample** button.
- **Report Export Tool** – To export a report in one of several formats, use the Export Bar on a custom generated report.

Note: For more information about reports, please see the **Reports and Analytics Guide**, available via AirWatch Resources.

Using AirWatch Hub

Utilize the AirWatch Hub as your central portal for fast access to critical information. Quickly identify important issues or devices and take action from a single location in the AirWatch Admin Console. Select any metric to open the **Device List View** for that specific set of devices, where you can perform actions such as sending a message to those devices.

The Hub provides both summary graphs and detailed views, covering:

- **Devices** – View exact number of devices in terms of:
  - Status breakdown of all devices in terms of registered, enrolled, enterprise wipe pending, device wipe pending and unenrolled.
  - Platform breakdown of devices enrolled in AirWatch.
  - Enrollment history over the past day, past week and past month.
- **Compliance** – View which devices are violating compliance policies according to:
  - All compliance policies currently violated by devices, including apps, security settings, geolocation and more.
  - Top violated policies, covering all types of compliance policies established.
  - Blacklisted Apps, including all blacklisted apps installed on devices, ranked by order of instances of violation.
  - Devices without required apps, included apps that should be installed on a device that are uninstalled or are not yet installed.
- **Profiles** – View which profiles are out of date according to:
  - Latest Profile Version, including devices with old versions of each profile.

- **Apps** – View which applications are associated with devices, including:
  - Latest Application Version, including devices with old versions of each application.
  - Most Installed Apps, ranked in order of number of devices that have the application currently installed.
- **Content** – View devices with content that is out of date, according to:
  - Latest Content Version, including each file that is out of date ranked by order of instance.
- **Telecom** – View devices sorted by telecom and data activity, according to:
  - Data Usage, including percentage of allotted or allowed data plans.
  - Device Roaming, including amount of time devices have been roaming sorted by day, week or month.
- **Email** – View devices that are currently unable to receive email, according to:
  - Devices Blocked from email, including devices blocked by default, blacklisted or unenrolled.
- **Certificates** – View which certificates are set to expire, according to:
  - Certificates expiring within one month, one to three months, three to six months, six to twelve months and greater than twelve months. Additionally, view certificates that have already expired.

The set of devices shown varies depending on the your current Organization Group, including all devices in child Organization Groups. Switch to lower Organization Groups and automatically update device results by using the Organization Group drop-down menu.

Toggle between views by selecting the **List View** icon and **Chart View** icon . Select any metric to open the Device List View for that specific set of devices, where you can perform actions such as sending a message to those devices.

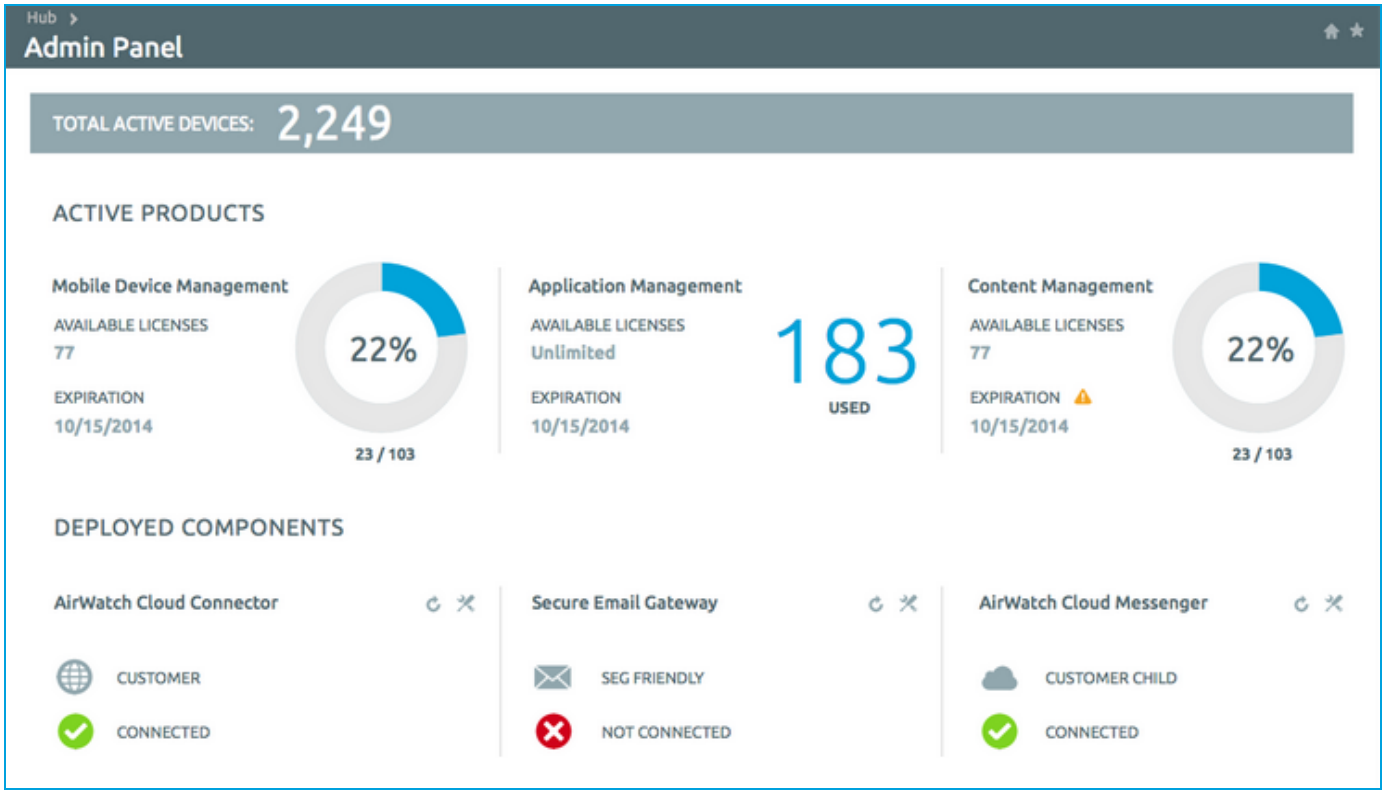
Customize the Hub by selecting the **Available Sections** icon . Next, insert or remove ticks from the checkboxes representing available sections (Devices, Compliance, Profiles, etc.) and select **Save** to craft the Hub's Overview to suit your needs.

Lastly, you can export Hub data to .PDF by selecting the **Export** icon . This is useful for providing daily, weekly, or monthly reports of the current state of your mobile device deployment.

Using the Admin Panel Dashboard

The **Admin Panel** provides an at-a-glance overview of module license information and deployed AirWatch components. Access the **Admin Panel** by navigating to **Hub ▸ Admin Panel**.

Note: The Admin Panel can only be accessed from a Customer Organization Group.



The **Admin Panel** contains a summary of AirWatch licenses condensed into two separate sections, **Active Products** and **Deployed Components**.

Active Products

Active Products features three panels that report MDM, App Management and Content Management licenses available as well as expiration dates. The donut chart displays a comparison of the quantity of licenses used as a percentage of the quantity of licenses purchased. In the case of an unlimited or site license arrangement, the donut chart will be replaced with a simple count of licenses used.

These panels include the following SKUs (stock keeping unit) and their expiration information:

- App Catalog
- App Wrapping
- Browser
- Chat
- Content Locker Collaborate
- Content Locker View
- Inbox
- Mobile Device Management
- Telecom
- Video
- Workspace

Note: When a module listed in **Active Products** contains multiple licenses that expire at different times, then the **Expiration** label will reflect the nearest expiration date.

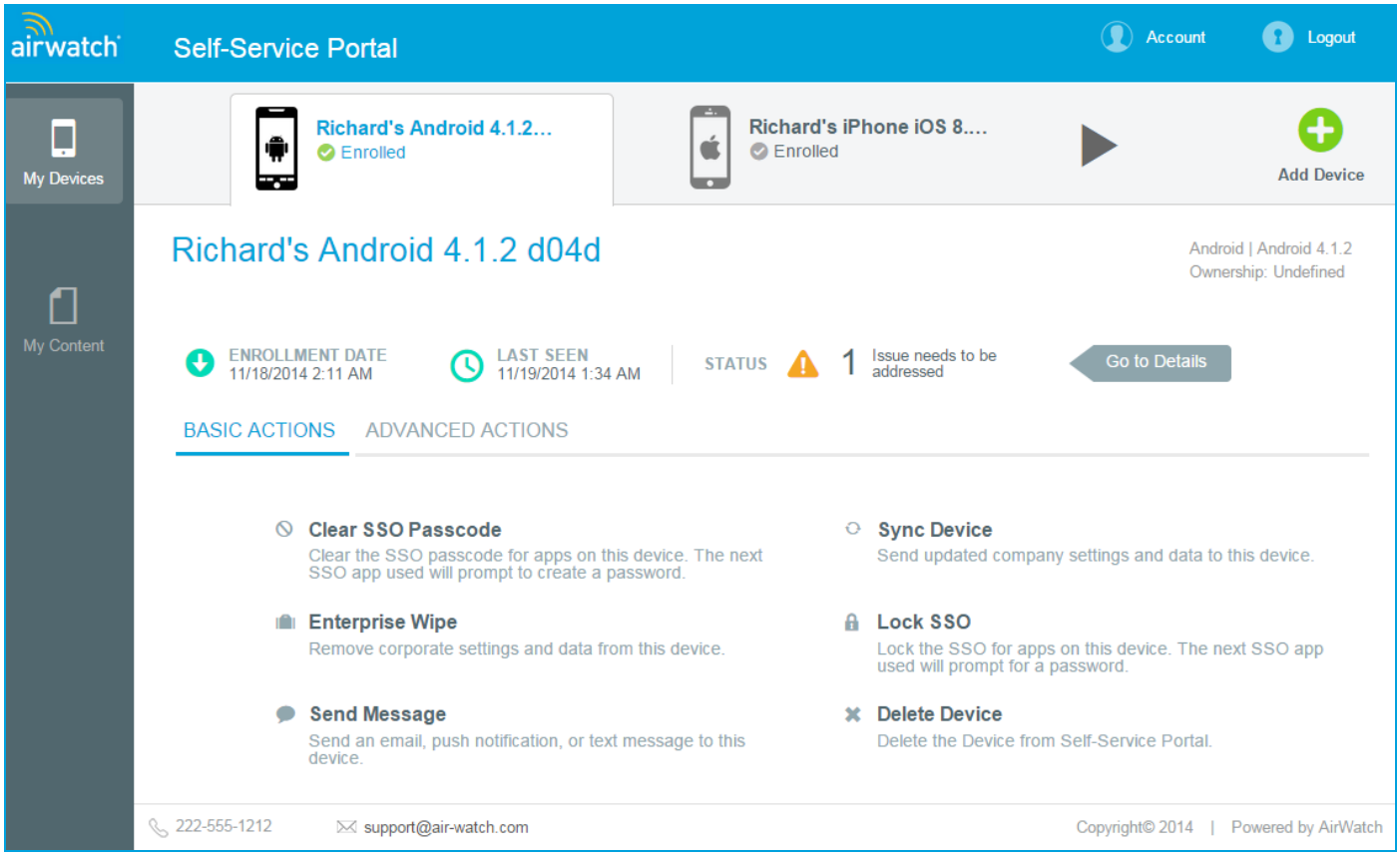
Deployed Components

Deployed Components features a panel for every enabled component at the customer organization group, each reporting the connectivity status of the following components:

- AirWatch **Cloud Connector**
- **Secure Email Gateway**
- AirWatch **Mobile Access Gateway**
- **Enterprise Integration Service** (not shown).

Self-Service Portal

The **AirWatch Self-Service Portal** (SSP) is a useful online tool used to remotely monitor and manage smart devices and can help reduce the overall "hidden cost" of managing a device fleet. By empowering and educating device users on how to perform basic device management tasks, investigate issues and fix problems, your organization may be able to reduce the number of help desk tickets and support issues.



In This Section

- Accessing the Self Service Portal – Learn how to access the SSP directly from your mobile device.
- Using the 'My Devices' Page in the SSP – See how you can choose a language, login, select devices, add a new device and view your device's information.
- Performing Actions in the SSP – Learn how easy it is to perform remote actions using the Self Service Portal.
- Self Service Portal Actions Matrix – See at-a-glance which basic and advanced actions apply to all the major platforms.
- Customizing the SSP – See how you can customize the color scheme and title of the SSP and also how you can choose a default authentication method for logging into the SSP.

Accessing the Self Service Portal on Devices

Access the Self-Service Portal (SSP) from a workstation or device by navigating to **https://<AirWatchEnvironment>/MyDevice**. However, in many cases it is helpful to deploy SSP access as a Web Clip or Bookmark to managed devices. This gives users the ability to easily monitor and track their device status within AirWatch without worrying about a URL. Giving users the ability to perform such actions can simplify the administrative experience by reducing end user support requests.

Configuring a Web Clip or Bookmark

Deploying an SSP Web Clip or Bookmark is optional and allows users to access the SSP from their devices in addition to their computer's web browser. It is only available for platforms that support a Web Clip or Bookmark profile. For more information on Web Clips and Bookmarks, consult the appropriate Platform Guide.

Customizing the SSP URL

To make things even easier for your end-users, you may customize the URL before making a Web Clip or Bookmark such that it includes the email domain, group ID and username, making it unnecessary for end-users to retain and recall these pieces of information.

Accomplish this by appending the Self Service Portal URL in the following manner:

1. Add a "**/?**" (minus the quotes) to the end of the URL, such as **https://<AirWatchEnvironment>/MyDevice/?**
2. Add the following parameters and their values after the question mark (**?**) separated by an ampersand (**&**):
    a. **ed** – indicates the email domain. If email authentication is not configured, this parameter will be ignored.
    b. **ac** – indicates the group ID.
    c. **un** – indicates the username.

Example: **https://<AirWatchEnvironment>/MyDevice/?ed=gmail.com&ac=groupid&un=username**

Using the My Devices Page of the SSP

The **My Devices** page of the Self Service Portal provides access to detailed information about devices and enables users to perform a wide range of actions.

Choosing a Language

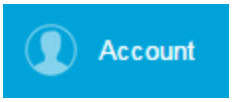
The Self Service Portal automatically matches the browser's default language, however, you may opt to override this default setting by choosing from the **Select Language** drop-down field directly from the login screen.

Logging into the SSP

Log in using the same credentials (**Group ID**, **username** and **password**) used to originally enroll in AirWatch. Optionally, if Email Domain registration is configured, you can log in using your corporate email address.

Changing the Password

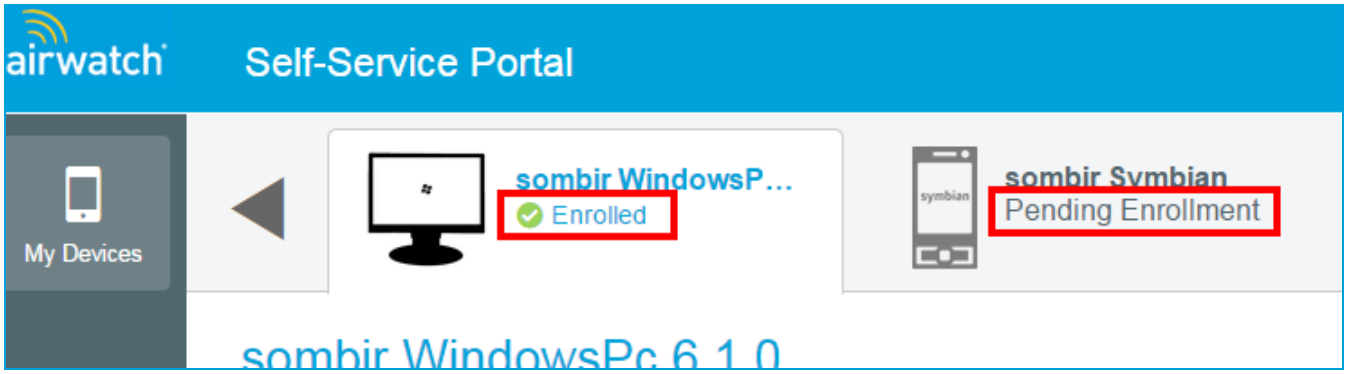
You may use the **User Account** page to change the password associated with your AirWatch account. This password will be used for device enrollment and logging into the SSP.



Change your password by selecting the **Account** button located at the top-right of the Self Service Portal screen. The **User Account** page displays allowing you to select the **Change** button next to the **Password** field.

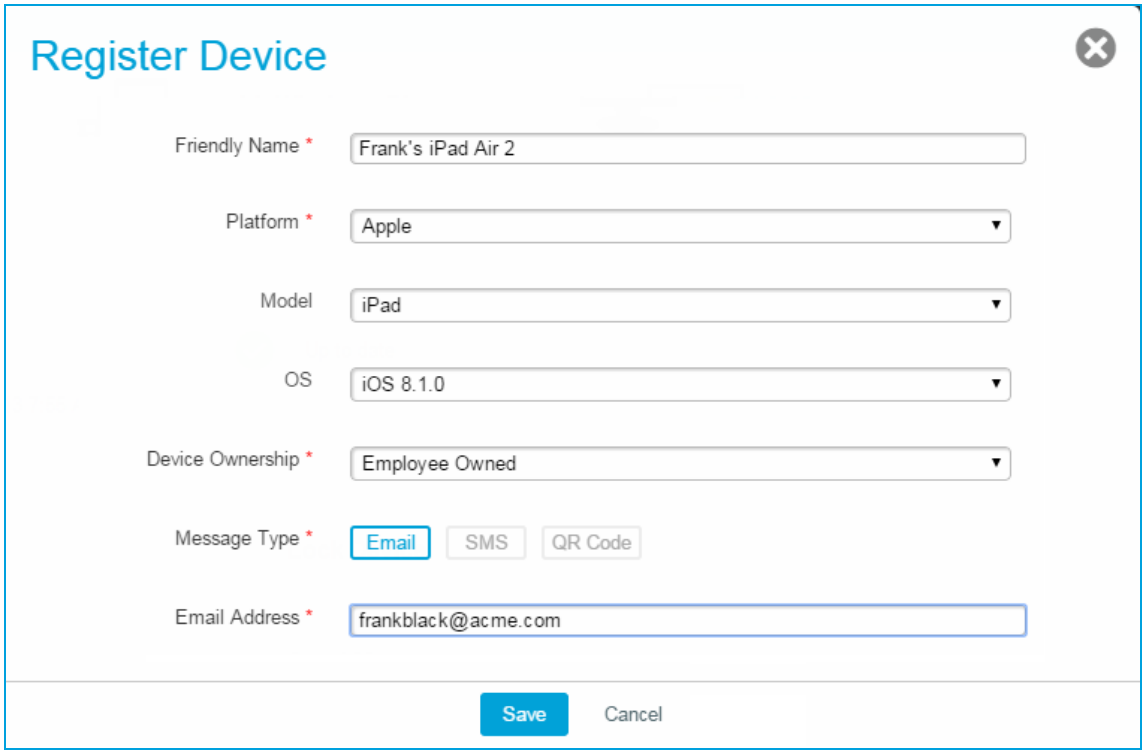
Selecting a Device in the SSP

After logging in to the SSP, the **My Devices** page displays all the devices associated with the account. Each enrolled device appears in its own tab across the top of the **Self Service Portal** screen. Select the tab representing the device you want to view and manage.



The device status is listed under the name of the device on the tab.

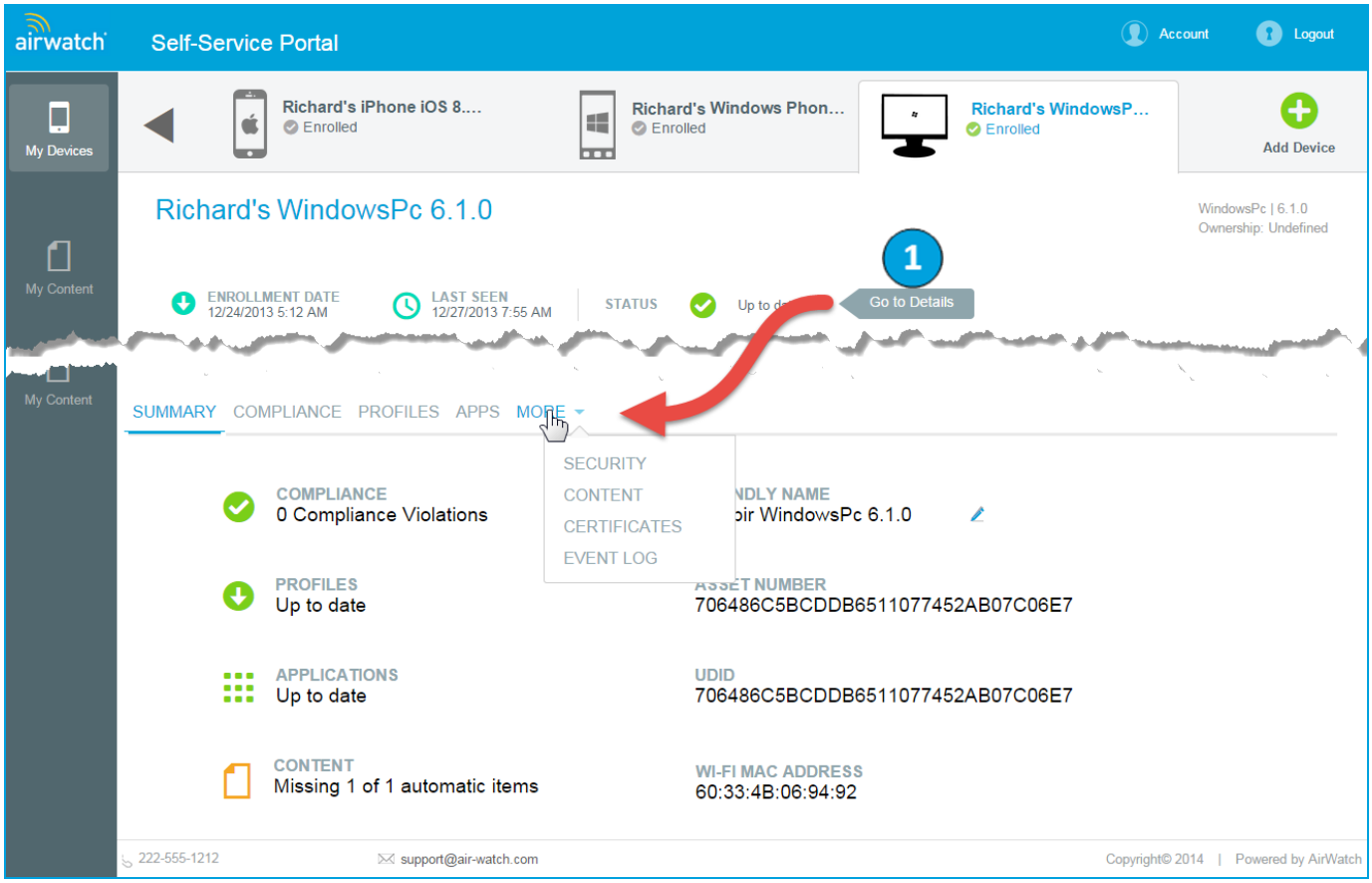
Adding a Device in the SSP



1. Select **Add Device** on the **My Devices** page.
2. Complete the required fields: **Friendly Name**, **Platform**, **Device Ownership**, **Message Type** and **Email Address**.
3. Select **Save** to add the new device to the SSP account.

Note: The status of a newly-added device will be set to "Pending Enrollment" until it is fully enrolled.

Viewing Device Information

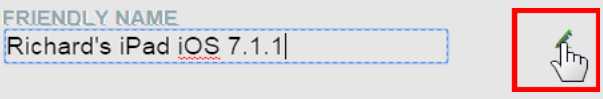


Upon logging in to the SSP, by default, the first device appears in the main viewer displaying basic information such as **Enrollment Date**, the **Last Seen** date and the device's **Status**.

The **Go to Details** button, when selected, displays the following tabs containing information about the selected device under the selected user account:

1. **Go to Details** button:
   - **Summary** – Displays summarized information for Compliance, Profiles, Apps, Content, Friendly Name, Asset Number, UDID number, and Wi-Fi MAC Address.

     Note: A device's friendly name can be edited directly from the **Summary** tab view by selecting the edit icon to the right of the **Friendly Name** field.

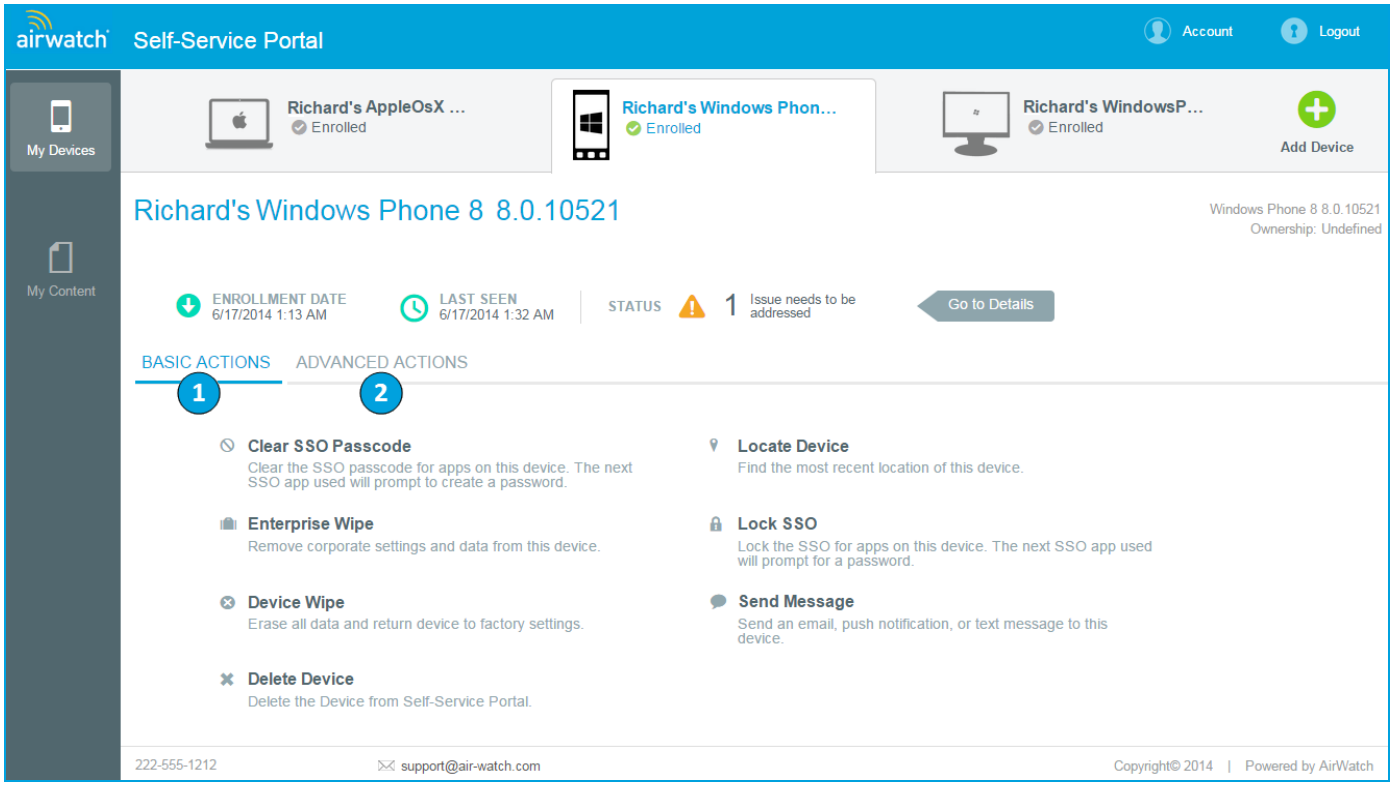
     

   - **Compliance** – Shows the compliance status of the device, including the name and level of all compliance policies that apply to the device.

- **Profiles** – Shows all of the MDM profiles (including automatic profiles) that have been sent to the devices enrolled under your user account and the status of each profile.
- **Apps** – Displays all applications installed on the selected device and provides basic app information.
- **Security** – Shows general security information about a device enrolled under the user account.
- **Content** – Displays the list of content currently installed on your device, providing options to install and uninstall individual files.
- **Certificates** – Shows each certificate installed on the device.
- **Event Log** – Contains a comprehensive log of all interactions between the AirWatch Admin Console and the device.

Note: The viewable tabs and available actions you can perform may vary based on device platform. See the applicable **AirWatch Platform Guide**, available in AirWatch Resources.

Performing Actions in the SSP



AirWatch gives you as an administrator several remote actions and options to perform on managed devices. However, when devices are employee-owned, those employees may want to access similar management tools for their own use. The AirWatch SSP provides a means for employees to utilize some key MDM tools without any IT involvement. If you enable it, end users can launch the SSP in a web browser and access key MDM support tools. You can also enable or disable the displays of information and the ability to perform remote actions from the SSP.

The selected device's available actions, which vary based on platform, are split between **Basic Actions** and **Advanced Actions** on the main access page:

Note: Action permissions are determined by the administrator, therefore device users may not be able to perform all listed actions. See the applicable **AirWatch Platform Guide**.

1. **Basic Actions**
   - **BES Registration** – Select this to register the device with BES 10.
   - **Change Passcode** – Set a new passcode for the selected device.
   - **Clear SSO Passcode** – Clears the single-sign on passcode on the selected device and will prompt for a new passcode. This is useful if users forget their device passcode and are locked out of their device.
   - **Clear Passcode** – Clears the passcode on the selected device and will prompt for a new passcode. This is useful if users forget their device passcode and are locked out of their device.
   - **Delete Device** – Removes the device from the Self Service Portal.
   - **Delete Registration** – Deletes any pending enrollment record from the Self Service Portal.
   - **Device Query** – Manually requests the device to send a comprehensive set of MDM information to the AirWatch Server.
   - **Device Wipe** – Wipes all data from the selected device, including all data, email, profiles and MDM capabilities and returns the device to factory default settings.
   - **Download Agent** – Download and install the AirWatch Agent for this device.
   - **Enterprise Wipe** – Wipes all corporate data from the selected device and removes the device from AirWatch MDM. All of the enterprise data contained on the device is removed, including MDM profiles, policies and internal applications. The device will return to the state it was in prior to the installation of AirWatch MDM.
   - **Locate Device** – Activates the GPS feature to locate a lost or stolen device.
   - **Lock Device/Screen** – Locks the selected device so that an unauthorized user cannot access it, which is useful if the device is lost or stolen. In such a case, end-users may also want to use the GPS feature to locate the device.
   - **Lock SSO** – Lock the single sign-on passcode for apps on this device. The next SSO app opened will prompt for a passcode.
   - **Make Noise** – Help find a device by remotely causing it to ring.
   - **Resend Enrollment Message** – Sends another copy of the initial enrollment email, SMS or QR code to the device intended to register.
   - **Send Message** – Sends an Email, SMS (text) or Push Notification over-the-air to the selected device.
   - **Sync Device** – Outfit devices with the latest company policies, content and apps.
   - **View Enrollment Message** – See the actual email, SMS or QR code that comprised the initial enrollment message.

Note: Registration and Enrollment actions will only display in the SSP when the enrollment of a selected device is still pending.

2. **Advanced Actions**
   - **Generate App Token** – Generate a token that the device can use to access secure applications.
   - **Manage Email** – Manage devices connected to an email account.
   - **Review Terms of Use** – Review past terms of use for this account.
   - **Revoke Token** – Revokes the token for a selected application.
   - **Upload S/MIME Certificate** – Upload an S/MIME Certificate for a corporate email account.

Self-Service Portal Actions Matrix

The table below shows which basic and advanced SSP actions are supported by the various major platforms.

Action	Android	iOS	Win Phone 8	Mac OS X	Win Mobile	Win32	Win 8/RT	QNX	Black Berry	Sym-bian
Basic Actions										
BES Registration									✓	
Change Passcode	✓									
Clear (SSO) Passcode	✓	✓	✓				✓			
Delete Device	✓		✓	✓	✓	✓	✓		✓	✓
Delete Registration	✓	✓			✓	✓	✓			
Device Query	✓	✓		✓		✓	✓	✓		✓
Device Wipe	✓	✓	✓	✓	✓				✓	✓
Download Agent				✓		✓		✓		
Enterprise Wipe	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Locate Device	✓	✓	✓		✓				✓	✓
Lock Device/Screen	✓	✓		✓	✓	✓		✓	✓	✓
Lock SSO		✓	✓							
Make Noise	✓									
Resend Enrollment Message	✓	✓			✓	✓	✓			
Send Message	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sync Device	✓	✓								
View Enrollment Message	✓	✓			✓	✓	✓			
Advanced Actions										
Generate App Token	✓	✓	✓	✓	✓	✓	✓		✓	
Manage Email					✓	✓	✓			
Review Terms of Use	✓	✓	✓	✓	✓	✓	✓		✓	
Revoke Token	✓	✓	✓	✓	✓	✓	✓		✓	
Upload S/MIME Certificate	✓	✓	✓	✓	✓	✓	✓		✓	

Customizing the Self Service Portal

Custom-Branding the SSP

You may alter the logo, the color scheme and the title of the portal by Configuring Console Branding.

Configuring the Default Login Page for the SSP

You can set the default authentication method displayed on the Self-Service Portal depending on your organization's and users' needs.

Note: This setting is only accessible at the Global level for On-Premise customers.

Configure this setting by navigating to **Groups & Settings** ▸ **All Settings** ▸ **Installation** ▸ **Advanced** ▸ **Other** and set the **SSP Authentication Type** to:

- **Email** – Prompts users for only their email address if you have set up auto discovery.
- **Legacy** – Prompts users for their Group ID and credentials (username/password).
- **Dedicated** – Prompts users for only their credentials (username/password). This option defaults a single Group ID for single-customer environments.

Tags

Tags allow you to easily identify a specific device without requiring a device profile, smart group or compliance policy and without requiring the creation of a note.

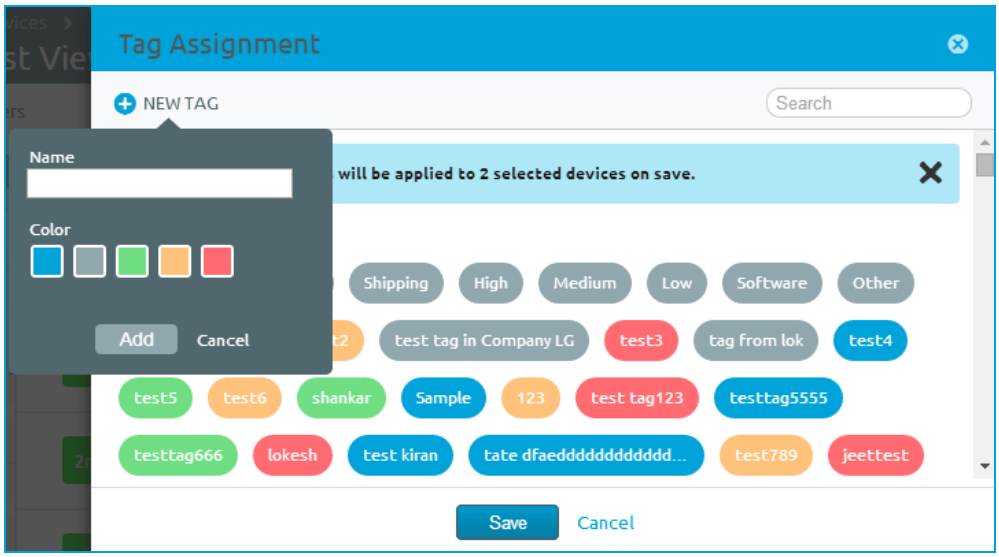
For example, one use for Tags is when a device has a defective battery or a broken bezel or screen, and you want to be able to identify these devices from the AirWatch Admin Console. Another use is in identifying hardware variants in a more visible way rather than relying on the model number or description to tell devices apart. For instance, two PCs may have the same model number but their CPUs may be slightly different or the amount of memory may have been customized. Tagging enhanced hardware enables easy identification of these devices.

Another specific use of Tags is in the **Teacher Tools** application, where Tags represent classes taught in an educational setting. For more information, please see the **Teacher Tools Guide** document, available via AirWatch Resources.

In This Section

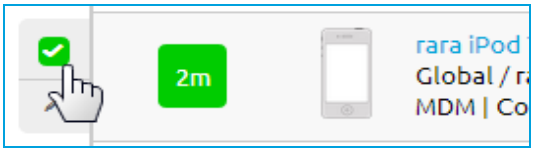
- Creating a New Tag – Learn how to create a new Tag.
- Adding Tags – See how you can add Tags to a single device or multiple devices simultaneously.
- Managing Tags – Find out how to edit an existing Tag, remove a Tag from a device and permanently delete a Tag.
- Filtering Devices by Tags – Learn how to produce a list of devices filtered by Tag.
- Tags and Smart Groups – Discover how tagging devices can make Smart Groups even more useful.

Creating a New Tag



The easiest way to create a new Tag is to create one while adding them in the **Device List View**:

1. Navigate to **Devices** ▸ **List View**.
2. Select a device by inserting a check mark to the left of the device listing.



3. Select the **More** button and choose **Add Tag** from the drop-down menu. The **Tag Assignment** screen appears (shown above).
4. Select the **NEW TAG** button.
5. Enter the **Name** of the new Tag and select a **Color**.
6. Select **Add** to save the Tag.

Alternatively, you may go through **Groups & Settings** to create a new Tag:

1. Navigate to **Groups & Settings** ▸ **All Settings** ▸ **Devices & Users** ▸ **Advanced** ▸ **Tags**.
2. Select the **Organization Group** to which you would like the Tag to belong.
3. Select the **Add** button. The **Add Tag** screen displays.
4. Enter the **Name** of the Tag.
5. Select the **Type** of Tag you would like to add, **General** or **Device**.
6. Select the **Save** button.

Adding Tags

Once you have created a new Tag, you must then tag devices to make use of them.

To Add Tags to a Single Device:

1. Navigate to **Devices** ▸ **List View** and select the device you would like to tag. You may select a single device in two ways:
   - Select the device from the listing to display the **Details View**.
   - Place a check mark in the device's check box.

     Selecting a device in either of these two ways displays the **Send** and **More** buttons.
2. Select the **More** button and then select **Add Tag**. The **Tag Assignment** screen displays with a listing of Tags available to apply to your selected device.
3. Select each of the Tags you would like to assign to the device. You may select more than one Tag.
4. Select the **Save** button to apply the Tag(s) to the device.

To Add Tags to Multiple Devices (Bulk Add Tags):

1. Navigate to **Devices** ▸ **List View**.
2. Place a check mark in the check box of each device you would like to tag.
3. Select the **More** button and then select **Add Tag**. The **Tag Assignment** screen displays with a listing of Tags available to apply to your selected devices.
4. Select the Tags you would like to assign to *all* of the selected devices. You may select more than one Tag.
5. Select the **Save** button to apply the Tag(s) to the devices.

Managing Tags

The following sections describe the steps you take to edit an existing Tag, remove a Tag from a device and delete a Tag.

Editing a Tag

To edit an existing Tag, take the following steps:

1. Navigate to **Groups & Settings** ▸ **All Settings** ▸ **Devices & Users** ▸ **Advanced** ▸ **Tags** and either select the edit button  or click the name of the Tag which you would like to edit.

   Note: Only Tags that are part of a child Organization Group and the OG currently selected will be editable.

2. Make your changes to the **Name** and **Type** fields per your preferences.
3. Select the **Save** button.

Removing a Tag

To remove a Tag from a device, take the following steps:

1. Navigate to that device's **Details View**.
2. Select the **Summary** tab and scroll to the bottom of the **Device Info** screen, where you will find all the Tags currently assigned to the device.
3. Select delete (**X**) next to each Tag you wish to remove.

Note: Removing a Tag from a device (or 'untagging' a device) is not the same thing as deleting a tag.

Deleting a Tag

To delete an existing Tag, take the following steps:

Navigate to **Groups & Settings** ▸ **All Settings** ▸ **Devices & Users** ▸ **Advanced** ▸ **Tags** and select the delete (**X**) button of the Tag you would like to delete.

Note: Only Tags that are part of a child Organization Group can be deleted.

Filtering Devices by Tag

You can use the filter feature in the **Device List View** to show only devices with specific Tags by taking the following steps:

1. Navigate to **Devices** ▸ **List View**, select the **Filters** button and the **Filters** column displays to the left of the device list.
2. Select **Advanced** from the list of Filter Categories.
3. Select **Tags**, which is a subcategory of **Advanced** (shown to the right)
4. Select the check boxes of each of the device Tags that you wish to display from the list of tags. Devices with unchecked tags will be filtered out of the resulting list. The **Device List View** will immediately refresh itself as soon as the first tag is selected.

Tags and Smart Groups

The Tag feature has been integrated with Smart Groups such that a Smart Group can be defined by tagged devices.

For instance, if you have tagged all the devices in your fleet that have cosmetic damage (cracked screens, cracked bezels, etc.) then you can make a Smart Group out of these devices and exclude them from the pool of devices you temporarily assign to site visitors.

Another example is tagging low-performing devices (those with less powerful processors or less memory capacity), creating a Smart Group of these tagged devices and excluding these devices from being used in mission-critical field assignments.

Related to the Teacher Tools application, where each Tag represents an individual class and corresponding curriculum, a good example is how a Smart Group can be made from the art history tag (class), then tied to a device profile with a geofence that can be applied when the class goes on a museum field trip, preventing the device from functioning outside the museum.

Note: For more information about the **Teacher Tools** application, please see the **Teacher Tools Guide**, available via AirWatch Resources.

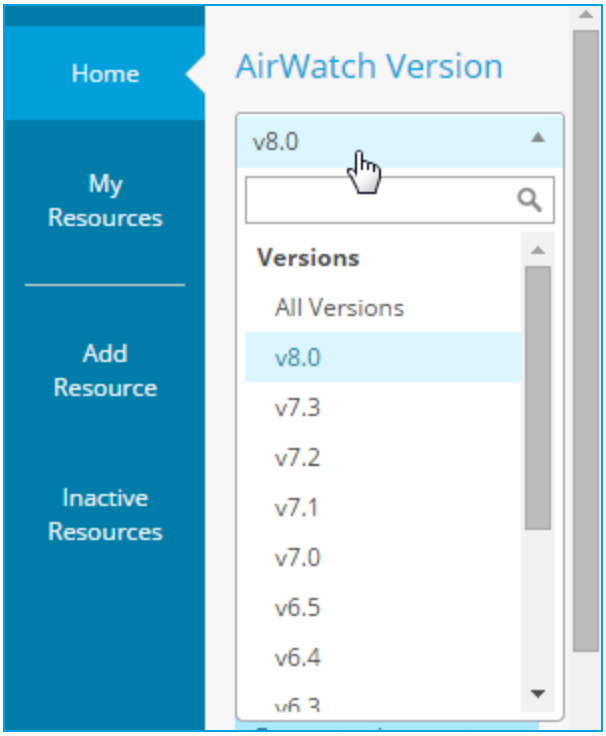
Finding Additional Documentation

While reading through this documentation you may encounter topics that reference other documents that are not included here. You may also be looking for separate documentation that is not a part of this resource. You can access this additional documentation through the AirWatch Resources page (https://resources.air-watch.com) on myAirWatch.

Note: It is always recommended you pull the document from AirWatch Resources each time you need to reference it.

To search for and access additional documentation via the AirWatch Resources page, perform the following step-by-step instructions:

1. Navigate to http://my.air-watch.com and log in using your AirWatch ID credentials.
2. Select **AirWatch Resources** from the navigation bar or home screen. The AirWatch Resources page displays with a list of recent documentation and a list of Resources Categories on the left.
3. Select your AirWatch Version from the drop-down list in the search parameters to filter a displayed list of documents. Once selected, you will only see documentation that pertains to your particular version of AirWatch.



4. Access documentation using the following methods:
   - Select a resource category on the left to view all documents belonging to that category. For example, selecting **Documentation** filters your search to include the entire technical documentation set. Selecting **Platform** filters your search to only include platform guides.
   - Search for a particular resource using the search box in the top-right by entering keywords or document names.
   - Add a document to your favorites and it will be added to **My Resources**. Access documents you have favorited by selecting **myAirWatch** from the navigation bar and then selected My Resources from the toolbar.

- Download a PDF of a document by selecting the button. Note, however, that documentation is frequently updated with the latest bug fixes and feature enhancements. Therefore, it is always recommended you pull the document from AirWatch Resources each time you need to reference it.

Having trouble finding a document? Make sure a specific **AirWatch Version** is selected. **All Versions** will typically return many results. Make sure you select **Documentation** from the category list, at a minimum. If you know which category you want to search (e.g., **Platform**, **Install & Architecture**, **Email Management**) then selecting that will also further narrow your search and provide better results. Filtering by **PDF** as a **File Type** will also narrow your search even further to only include technical documentation manuals.