# Revision Table

The following table displays revisions to this guide since the release of AirWatch v8.3.

<table>
<thead>
<tr>
<th>Date</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 2016</td>
<td>Initial upload.</td>
</tr>
</tbody>
</table>
# Table of Contents

## Chapter 1: Overview
- What's New ................................................................. 9
- Introduction to Mobile Device Management (MDM) .................. 10
- Before You Begin .......................................................... 10
- Supported Browsers ......................................................... 10
- Supported Devices ......................................................... 11

## Chapter 2: Getting Started with AirWatch
- Overview ............................................................................ 13
- Logging into the AirWatch Admin Console .......................... 13
- Setting Your Security PIN .................................................. 13
- Using the Getting Started Wizard ........................................ 14
- The AirWatch Admin Console at a Glance ......................... 15
- Using the Global Search .................................................... 17
- Viewing Notifications ....................................................... 18
- Using the Mobile Console ................................................. 18

## Chapter 3: Environment Setup
- Overview ............................................................................ 20
- Generating an APNs Certificate ......................................... 20
- Creating a Privacy Notification ........................................... 20
- Configuring Privacy Settings .............................................. 21
- Privacy Best Practices ....................................................... 23
- Setting Up Autodiscovery .................................................. 25
- Configuring Terms of Use ................................................ 26
- Configuring Console Branding .......................................... 28
- Configuring Restricted Actions .......................................... 29
- Integrating with Other Enterprise Systems ....................... 31

## Chapter 4: Organization Groups
- Overview ............................................................................ 34
- Creating Organization Groups ............................................ 35
### Chapter 5: User and Admin Accounts

- Overview .......................................................... 40
- Choosing User Authentication Types ........................ 41
- Creating Basic User Accounts ................................. 47
- Creating Directory-Based User Accounts ........................ 50
- Managing User Accounts ........................................ 53
- Using the Bulk Import Feature .................................. 55
- Creating an Admin Account ..................................... 57
- Managing Admin Accounts ...................................... 58

### Chapter 6: Role-Based Access

- Overview .......................................................... 59
- Default and Custom Roles ........................................ 60
- Creating and Managing User Roles ............................ 62
- Creating and Managing Administrator Roles .................. 63
- Comparing Admin Roles ........................................ 66
- Added Resources .................................................. 68

### Chapter 7: User Groups

- Overview .......................................................... 69
- Adding User Groups Without Directory Integration (Custom) ............................ 70
- Adding Directory-Based User Groups .......................... 70
- Editing User Groups Permissions ............................... 72
- Accessing User Details .......................................... 72
- Managing User Groups .......................................... 73
- Device Assignments .............................................. 75

### Chapter 8: Smart Groups

- Overview .......................................................... 78
- Creating a Smart Group ........................................... 79
- Assigning a Smart Group ......................................... 80
### Managing Smart Groups ................................................................. 82

#### Chapter 9: Assignment Groups ..................................................... 85

Overview ......................................................................................... 86
Using Assignment Groups ............................................................... 86

#### Chapter 10: Shared Devices ........................................................... 88

Overview ......................................................................................... 89
System Capabilities ........................................................................ 89
Supported Platforms ....................................................................... 89
Organizing Shared Devices ............................................................. 90
Provisioning Devices for Multi-User Device Staging ....................... 91
Using Shared Devices ..................................................................... 91

#### Chapter 11: Device Enrollment ...................................................... 92

Overview ......................................................................................... 93
Required Information ...................................................................... 93
The Enrollment Process ................................................................ 93
Additional Enrollment Workflows ............................................... 94
Performing Device Staging ............................................................ 94
Registering Devices ...................................................................... 96
Configuring Enrollment Options .................................................. 100
Customizing Enrollment Messages ............................................. 102
Blacklisting and Whitelisting Device Registration ....................... 103
Configuring Enrollment Restrictions .......................................... 104

#### Chapter 12: Device Profiles ......................................................... 106

Overview ......................................................................................... 107
Configuring General Profile Settings .......................................... 107
Managing Device Profiles ............................................................ 109
Editing Device Profiles ................................................................ 113
View Device Assignment ............................................................... 114
Compliance Profiles ..................................................................... 115
Geofences ...................................................................................... 115
Chapter 13: Compliance ................................................................. 119

Compliance Overview ................................................................. 120
Navigating Compliance Policies List View .................................. 121
Compliance Policies by Platform ............................................... 123
Adding a Compliance Policy ...................................................... 125

Chapter 14: Tags .......................................................................... 130

Overview .................................................................................... 131
Creating a New Tag ..................................................................... 131
Adding Tags ................................................................................. 132
Managing Tags ............................................................................ 133
Filtering Devices by Tag ............................................................. 133
Tags and Smart Groups ............................................................... 134

Chapter 15: Managing Devices ....................................................... 135

Overview .................................................................................... 136
Using the Device Dashboard ...................................................... 136
Using the Device List View ....................................................... 137
Using Device Details ................................................................. 141
Using Device Actions ................................................................. 144
Using the Enrollment Status Page ............................................. 150
Using Lifecycle Notifications ................................................... 152
Using Wipe Protection .............................................................. 153
Using AirWatch Hub ................................................................. 155

Chapter 16: Certificate Management .............................................. 160

Overview .................................................................................... 161
Managing Digital Certificates .................................................. 161
Certificate Integration Resources ............................................. 161

Chapter 17: Custom Attributes ...................................................... 163

Overview .................................................................................... 164
Creating Custom Attributes ................................................................. 164
Assigning Organization Groups Using Custom Attributes ....................... 165

Chapter 18: Self-Service Portal .............................................................. 166
Overview ............................................................................................... 167
Accessing the Self Service Portal on Devices ........................................... 167
Using the My Devices Page of the SSP ..................................................... 167
Performing Actions in the SSP ................................................................. 171
Self-Service Portal Actions Matrix .......................................................... 174
Customizing the Self Service Portal (SSP) ............................................... 175

Finding Additional Documentation ......................................................... 176
Chapter 1: Overview

What's New ........................................................................................................... 9
Introduction to Mobile Device Management (MDM) ........ 10
Before You Begin ................................................................................................. 10
Supported Browsers ............................................................................................. 10
Supported Devices ............................................................................................... 11
What's New

The Mobile Device Management Guide has been updated with the latest features and functionality from the most recent release of AirWatch, AirWatch v8.3. The list below includes these new features and the sections and pages on which they appear.

- Device Assignments (previously Network Range Assignments) has been enhanced with an ability to assign devices to an organization group based on custom attributes. See Device Assignments on page 75.

- Assigning a Smart Group is now easier due to the addition of a Groups link on the Assign page. See Assigning a Smart Group on page 80.

- Determining which Assignment Groups are actionable by admins has been made clearer in Managing Smart Groups on page 82.

- If no device hardware identifiers are included during the addition of a device, such as UDID, IMEI, and Serial Number, AirWatch will now attempt to match the device registration record to the enrollment automatically. You can also opt out of sending the device user an email upon a successful device registration. See Registering Devices on page 96.

- You are now able to select a contiguous block of devices, even across multiple pages, by shift-clicking in the Device List View, similar to how it works in the Windows and Mac desktop environments. See Using the Device List View on page 137.

- When you select a Revoke Token or Reset Token action for one or more devices in the Enrollment Status page, you can now choose to disable the Notify Users field which prevents the default email notification from being sent. See Using the Enrollment Status Page on page 150.

- The Event Log now captures server thread information when multi-threading is enabled at the server level. See Using Reports & Analytics on page 158.

- A new section containing information about certificate management including a list of external resources with instructions on integrating your specific certificate authority with AirWatch. See Certificate Management on page 160.

- Custom Attributes, including how to create them and use them to assign devices to organization groups, has been added to the MDM Guide. See Custom Attributes on page 163.
Introduction to Mobile Device Management (MDM)

Mobile devices are valuable enterprise tools. They allow employees to have immediate access to your company's internal content and resources. However, the diversity of mobile platforms, operating systems and versions can make managing a 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. MDM allows you to:

- 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.
- Remotely lock and wipe managed devices.

You can tailor your MDM environment to gain immediate access to device locations, current users, and content. You can also automate your MDM deployment to enforce security and compliance settings with rules and warnings that are unique to each user or organization group. Finally, you can restrict or enable content and features based on a device's geographic location.

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

Before You Begin

Before configuring your AirWatch MDM deployment, you should familiarize yourself with the following prerequisites.

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 Control Panel > 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, AirWatch recommends upgrading your browser to guarantee the performance of the AirWatch Admin Console. Comprehensive platform testing has been performed to ensure functionality using these web browsers. The AirWatch Admin Console may experience minor issues if you choose to run it in a non-certified browser.
Supported Devices

AirWatch supports the following devices and operating systems:

- Android 3.0+
- Apple iOS 5.0+
- Apple Mac OS X 10.9+
- BlackBerry 5+
- BlackBerry 10
- Chrome OS 39.0+
- QNX 6.5+
- Symbian OS ^3 and S60
- Tizen 2.3+
- Windows Desktop (8/8.1/RT/10)
- Windows 7 (Windows 7 or higher)
- Windows Phone (Windows Phone 8/ 8.1, Windows 10 Mobile)
- Windows Rugged (Mobile 5/6 and Windows CE 4/5/6)

Limited support may be available for other devices or operating systems. Please refer to each platform's specific User Guide, available on AirWatch Resources, or contact AirWatch Support for more information.
Chapter 2:
Getting Started with AirWatch

Overview .................................................................13
Logging into the AirWatch Admin Console ..................13
Setting Your Security PIN ........................................13
Using the Getting Started Wizard .............................14
The AirWatch Admin Console at a Glance ..................15
Using the Global Search ..........................................17
Viewing Notifications ..............................................18
Using the Mobile Console ........................................18
Overview

The AirWatch Admin Console allows you to view and manage every aspect of your Mobile Device Management (MDM) deployment. With this single, web-based resource, you can quickly and easily add new devices and users to your fleet, manage profiles, and configure system settings.

Logging into the AirWatch Admin Console

To log in to the AirWatch Admin Console, you must have the Environment URL and login credentials. Where you obtain this information depends on your type of deployment. For example:

- **SaaS Deployment** – Your Account Manager provides your Environment URL and username/password. The URL is not customizable, and generally follows the format of `awmdm.com`.
- **On-Premise** – The On-Premise URL is customizable and follows the format `awmdm.<MyCompany>.com`. Your Account Manager provides the initial setup credentials for your environment. Administrators 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 AirWatch Admin Console Environment URL, you can log in using the Username and Password provided by your AirWatch Administrator.

Setting Your Security PIN

When you first log in to the AirWatch Admin Console, you will be prompted to establish a Security PIN. The PIN acts as a safeguard against accidentally wiping a device or deleting important aspects of your environment, such as users and organization groups.

The Security PIN also works as a second layer of security. It presents an additional point of authentication by blocking actions made by unapproved users.

Enter and confirm your four-digit Security PIN on 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

1. Select the Account icon in the top-right corner of the admin console and visit the Security Settings page.
2. Select Manage Account Settings and then select Reset from the Security Settings menu to reset your PIN.
3. Log out of the console and complete the PIN creation prompt upon logging back in.
Using the Getting Started Wizard

The Getting Started Wizard serves as a checklist that helps you confirm that all aspects of a successful deployment are established. It is organized 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 section has its own set of steps. Steps that are shared among the three sections are tracked automatically so you never have to complete the same step twice.

- **Mobile Device Management** (MDM) – Establish the level of control you want 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 should install recommended apps and identify and install public apps to enrolled devices.

You can review your responses to any module at any time by selecting Review Section from each completed module. Additionally, you can 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 step in a module. Here you will answer questions and access the exact pages within the AirWatch Admin Console to configure settings for each feature. As you answer each question, the percentage counter progresses and displays how far along you are in completing the module. If you stop a module before completing it, select Continue to return to where you left off.

As each substep in the module is completed, a small check mark is placed in the header bar for 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 previous question or screen.
Manually Enable the Getting Started Wizard

For a new AirWatch implementation, you can access the Getting Started page from the main menu, which is above the Hub icon on the left side of the console screen. However, you can manually enable the Getting Started Wizard at any time. This will restart the walk-through.

To manually enable the Getting Started Wizard:

1. Select any Organization Group other than the top-level group. To learn more about organization groups, including how to create a new OG during this step, see Organization Groups.

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 to Groups & Settings > All Settings > System > Getting Started.

4. Select Enable for each of the fields on this page:
   a. Getting Started Device Status
   b. Getting Started Content Status
   c. Getting Started Application Status

5. Save changes to the page.

The AirWatch Admin Console at a Glance

Header Menu

- Organization Group – Select the Organization Group from the tab labeled Global that you want to apply changes to.
- Global Search – Search all aspects of your 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 on the Notifications button indicates the number of alerts requiring your attention.
- Add – Quickly add an admin, device, user, 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 Admin Console and return to the Login screen.
- Help – Launch the help portal to browse or search the available guides and feature documentation.
- Refresh – Execute a screen refresh (to see updated stats and info) without leaving the current view.


- **Available Sections** – Customize the sections you want to see. This button is accessible only on the Hub Overview.
- **Export** – Produce a .pdf version of the console screen with the Export button. The Export button is accessible only on the Hub Overview.
- **Home** – Use this icon to assign any screen in the AirWatch Admin Console as your home page. The next time you open the Admin Console, your selected screen displays as your home page.
- **Save** – Save the current page or view for quick access from your list of Saved pages.

**Main Menu**

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

- **Getting Started**
  
  Ensure 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 configuration.

- **Hub**
  
  View and manage MDM information that drives decisions you need to make, access a quick overview of specific information such as the most blacklisted apps that violate compliance, and Admin Panel Dashboard to keep track of module licenses or all devices that are currently out of compliance, and Industry Templates to streamline the onboarding process with industry-specific apps and policies for your iOS devices. Review the Using the Hub section for details. For more information about Industry Templates, see the VMware AirWatch iOS Platform Guide, available on AirWatch Resources.

- **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, Notification and Wipe Protection settings, compliance policies, certificates, product provisioning and printer management.

- **Accounts**
  
  Survey and manage users and administrators involved with your MDM deployment. Access and manage user groups, roles, batch status and settings associated with your users. 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 and 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 homscreen configuration and all other content-specific settings.
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.

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.

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.

Select the bottom-left arrow to collapse or close the Secondary Menu, which creates more space for device information. To expand or reopen the Secondary Menu, select the modified right arrow.

Using the Global Search

The AirWatch Admin Console Global Search box lets you search information across your entire deployment. Global Search uses a modular design with a tabbed interface, applying your search to a single tab at a time, producing faster results. Select another tab to apply the same parameters to a new search group.

After executing a global search, select the following tabs to view the results:

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

You can also perform a search for an organization group by selecting the organization group drop-down menu. The Search bar displays above the list.
Viewing Notifications

The Notifications button is located next to the Global Search bar. Notifications appear when APNs for MDM certificates will expire within 30 days. Notifications help you avoid the hassles involved with expired certificates and keep 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 indicating the number of unread alerts. Select the Notifications button to display the Notifications screen.

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

The View APNs for MDM settings link displays the System Settings page for the organization group (OG) that 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.

For information about Device Lifecycle Notifications, please see Lifecycle Notifications.

Using the Mobile Console

Overview

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

The Admin Console automatically invokes the correct version (Mobile vs. Full) depending upon the device you are using. Tablet devices run the full version in their default browsers. Mobile phones display the Mobile Console view. For either type of device, enter the default login URL https://<AirWatchEnvironment>/AirWatch. The Console displays in the optimal configuration.

Device List View

The Device List view features options for sorting (ascending and descending) by User, Friendly Name, and Last Seen. It also displays whether 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.

Details View

The Details view displays the Friendly Name, Model and OS info, Device Ownership, and Username. You can also see the user’s email, how many profiles are installed on the device, and any device security violations.

Tapping the gray buttons at the top of the Details view initiates administrative actions for the selected device, including Enterprise Wipe, Send Message, and Lock Device.
Chapter 3: Environment Setup

Overview ........................................................................................................... 20
Generating an APNs Certificate ................................................................. 20
Creating a Privacy Notification ................................................................. 20
Configuring Privacy Settings ................................................................. 21
Privacy Best Practices .................................................................................... 23
Setting Up Autodiscovery ........................................................................... 25
Configuring Terms of Use ........................................................................... 26
Configuring Console Branding .................................................................... 28
Configuring Restricted Actions ................................................................. 29
Integrating with Other Enterprise Systems ............................................... 31
Overview

As part of environment setup for your AirWatch deployment you can generate certificates for managing certain platforms, configure telecom and privacy settings, and more.

Generating an APNs Certificate

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

To generate an APNs Certificate, follow the 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 alerts you if your APNs for MDM certificates are close to expiring, so you can take action in time. See Notifications for details about this feature.

For more information, please see the Generating and Renewing an APNs Certificate for AirWatch KB article: https://support.air-watch.com/articles/93878197-Generating-and-Renewing-an-APNs-Certificate-for-AirWatch.

Creating a Privacy Notification

AirWatch strongly recommends that you inform your end users about how their data is collected and stored when they enroll into AirWatch. The AirWatch Admin Console allows you to create a customized privacy notification to inform your users about what data your company collects from their enrolled devices.

Work with your legal department to determine what message about data collection you should communicate to your end users.

To create a privacy notification, navigate to Groups and Settings > All Settings > Devices and Users > General > Message Templates.

1. Select Add to create a new template. If you have already created a privacy notification template, select it from the list of available templates to use or edit it.
2. Complete the **Add/Edit Message Template** settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the notification template.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the template you are creating.</td>
</tr>
<tr>
<td>Category</td>
<td>Select <strong>Enrollment</strong>.</td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>MDM Device Activation</strong>.</td>
</tr>
<tr>
<td>Select Language</td>
<td>Select the default language for your template. Use the Add button to add additional default languages for a multi-language delivery.</td>
</tr>
<tr>
<td>Default</td>
<td>Select this check box to make this template the default message template.</td>
</tr>
<tr>
<td>Message Type</td>
<td>Select one or more message types: <strong>Email</strong>, <strong>SMS</strong>, or <strong>Push</strong> message.</td>
</tr>
</tbody>
</table>

3. Create the notification content. The message types that you selected in the **Message Type** field above determine which messages appear for you to configure.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email</strong></td>
<td><strong>Email Content Formatting</strong> Choose whether your email notification will be delivered as <strong>Plain Text</strong> or <strong>HTML</strong>.</td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td>Enter the subject line for your email notification.</td>
</tr>
<tr>
<td><strong>Message Body</strong></td>
<td>Compose the email message to send to your users. The editing and formatting tools that appear in this field depend on which format you chose in the <strong>Email Content Formatting</strong> field. If you have enabled the Visual Privacy Notice, include the lookup value {PrivacyNotificationUrl} in the message body.</td>
</tr>
<tr>
<td><strong>SMS</strong></td>
<td><strong>Message Body</strong> Compose the SMS message to send to your users. If you have enabled the Visual Privacy Notice, include the lookup value {PrivacyNotificationUrl} in your message body.</td>
</tr>
<tr>
<td><strong>Push</strong></td>
<td><strong>Message Body</strong> Compose the Push notification to send to your users. If you have enabled the Visual Privacy Notice, include the lookup value {PrivacyNotificationUrl} in your message body.</td>
</tr>
</tbody>
</table>

4. Select **Save** to save your message template.

**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 align with 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.

**Important:** Each jurisdiction has its own regulations governing what data can be collected from end users. These should be thoroughly researched before configuring your privacy policies.

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, Applications, and Profiles.
   - **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.
3. Select one of the following options for the Commands that can be performed on devices.
   - **Allow** – Allow the command to be made on devices without user permission.
   - **Allow With User Permission** – Allow the command to be made on devices but only with the user's permission.
   - **Prevent** – Prevent the command from executing 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 Rugged devices, you should consider using the **Allow With User Permission** option. This requires the end user to consent to admin access on their device through a 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, Email Accounts, and Username.
   - 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.
   - 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. Select whether to **Enable** or **Disable** the **Do Not Disturb Mode** on the device. When Enabled, you may also select a grace period which delays the activation of the do not disturb mode by minutes, hours, or days.

6. Select to **Enable** or **Disable** the **User Friendly Privacy Notice** on the device.

   - When **Enabled**, you may choose **Yes** (display a privacy notice) or **No** (do not display a privacy notice) for each ownership level: **Employee Owned**, **Corporate - Dedicated**, **Corporate - Shared**, and **Unknown**.

   You must create a privacy notice before you assign ownership types to receive the notice. For more information, see Creating a Privacy Notification in the **VMware AirWatch BYOD Guide**, available through **AirWatch Resources**.

   - New users will receive the privacy notice automatically if:
     - They enroll a new device and they are of an ownership type for which the privacy notice is enabled.
     - They currently use an enrolled device and their ownership is changed post-enrollment to a type that is assigned the web clip.

   - When you assign an ownership type to receive privacy notices, all current users in the selected ownership type will receive the configured privacy notification immediately in the form of a web clip.

   - When new users are added to an ownership type selected to receive privacy notices, they will receive a privacy notification email before they enroll their devices. If you inserted the privacy notice lookup value {PrivacyNotificationUrl} in your message template then the email will include a URL where they can read the privacy notice you created.

   - The privacy notice contents are automatically configured based on the organization group and device ownership of the device connecting. If your end user initiates the enrollment process through their web browser (for example, from the device activation email), the user will be prompted to select the device ownership of the device they intend to enroll. You should provide this information to your end users if they will be enrolling using a browser.

7. Click **Save** when finished.

For more information about leveraging a Bring Your Own Device solution, see the **VMware AirWatch BYOD and Privacy Guide**, available on **AirWatch Resources**.

### Privacy Best Practices

AirWatch recommends a few simple best practices for managing Privacy Settings.

#### 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 application 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 display user information such as first name and last name for both employee-owned and corporate-owned devices, as 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 if they are a part of a stipend program where you subsidize an end user's cellphone expenses. In this case, or for corporate-owned devices, consider the following about data you can collect:

- **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** – This status can be used to track which devices are in a ‘Roaming’ or ‘Not Roaming’ state. Compliance policies can be set up to disable voice and data usage while the device is roaming or you can also apply 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** – The 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 feature allows you to create compliance policies based on the percentage of data used and is helpful in preventing large carrier overage charges.

- **Cell Usage** – 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** – The short message service (SMS) 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. Monitoring SMS usage is 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 are reported to AirWatch.

If Do Not Collect is selected, only personal application information is not collected. All managed applications, whether public, internal or purchased, is 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 should explicitly mention these in your Terms of Use agreement.

**Important:** 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.

**Setting Up Autodiscovery**

AirWatch makes the enrollment process as simple as possible, leveraging an autodiscovery system to enroll devices to intended environments using end users' email addresses. Autodiscovery 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. AirWatch recommends that your domain is registered at your highest organization group.

Autodiscovery is configured automatically for new Software as a Service (SaaS) customers.

**Note:** To enable autodiscovery for on-premises environments, ensure your environment can communicate with the AirWatch Autodiscovery servers. For the latest on-premises requirements, refer to the *VMware AirWatch Installation Guide*, available on [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** to associate with this domain, enter a **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. Navigate to your email and verify your email address by clicking the confirmation link in the confirmation email.
4. Add more **Business Email Domains** as required, such as "us.example.com" or "eu.example.com."
   - Multiple email domains can be added in the same organization group level.
   - Consider adding alternative email domains within other organization groups to facilitate multi-tenancy.
5. Select **Save** to complete autodiscovery setup.

Instruct end users who enroll themselves to select the option to enroll using 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 are 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, 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 VMware AirWatch Enrollment Processes Guide, available on 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.

The Terms of Use displays during each device's enrollment. With the Terms of Use, you can:

- Set version numbers.
- Set platforms to receive the Terms of Use.
- Notify users by email with the Terms of Use updates.
- Create language specific copies of the Terms of Use.
- Create multiple Terms of Use agreements and assign them to organization groups based on ownership type or platform.
- Tailor each agreement to meet the liability requirements of specific groups.

**Creating Enrollment Terms of Use**

1. Ensure your current active organization group is correct 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. Enter a unique Name of the new Terms of Use agreement (TOU).
5. The Type of TOU is pre-populated as Enrollment.
6. Choose Any or Selected Platform from the Platform field to trigger Terms of Use depending on platform type. If you select Selected Platform option, then choose your desired platforms from the list that appears.
7. Choose Any to Selected Ownership Types from the Device Ownership field to trigger Terms of Use depending on ownership type. If you select Selected Ownership Types option, then choose your desired ownership from the list that appears.
8. Choose **Any** or **Selected Enrollment Types** from the Enrollment Types field to trigger terms of use depending on enrollment type. If you select **Selected Enrollment Types** option, then choose your desired enrollment from the list that appears.

9. Select the **Notification** field to send an email to users when the TOU is updated.

10. Optionally, for localization purposes, you may enter a Terms of Use agreement for each language applicable to your needs by making a choice in the **Select Language** field.

11. Enter your Terms of Use in the text field provided.
   This is where you can 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.

12. Select **Save**.
   You can enforce MDM Terms of Use acceptance by creating a compliance policy for **MDM Terms of Use Acceptance**. This does not apply to devices using AirWatch Container.

**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 is not 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 **VMware AirWatch Mobile Application Management Guide**, available on [AirWatch Resources](https://www.vmware.com/airwatch/).

**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.

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 Terms of Use row to see device information pertaining to that agreement. Optionally, access the drop-down menu for the row and select 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 Using 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, or Excel formats.

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

### Configuring Console Branding

The AirWatch Admin Console allows extensive customization options. These options allow you to 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. For more information, see Organization Groups.

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 an overall color theme from preset AirWatch colors, or upload your 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 unattended, AirWatch provides an additional safeguard against malicious actions that could be potentially destructive. You have the option to place those actions out of reach of unauthorized users.

Configure settings for restricted actions by navigating to Groups & Settings > All Settings > System > Security > Restricted Actions. Here you can require that certain actions require admins to enter a PIN 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

Here you can require that certain actions require admins to enter a PIN or a note of explanation.

For each action you choose to protect, select the appropriate Require PIN check box. This provides you with granular control over which actions you want to make more secure.

Note: Some actions always require a PIN and thus you cannot disable them.

You can set the maximum number of failed attempts the system should accept before automatically logging out the session. If you reach the set number of attempts, you need to re-login into the AirWatch Admin Console and set a new Security PIN.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Account Delete</td>
<td>Prevents the deletion of an admin user account in Accounts &gt; Administrators &gt; List View.</td>
</tr>
<tr>
<td>Regenerate ACC Certificate</td>
<td>Prevents the regeneration of the ACC certificate in Groups &amp; Settings &gt; All Settings &gt; System &gt; Enterprise Integration &gt; AirWatch Cloud Connector.</td>
</tr>
<tr>
<td>APNs Certificate Change</td>
<td>Prevents the disabling of APNs for MDM in Groups &amp; Settings &gt; All Settings &gt; Devices &amp; Users &gt; Apple &gt; APNs For MDM.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Application Delete/Deactivate/Retire</strong></td>
<td>Prevents the deletion, deactivation, or retirement of an application in Apps &amp; Books &gt; Applications &gt; List View.</td>
</tr>
<tr>
<td><strong>Content Delete/Deactivate</strong></td>
<td>Prevents the deletion or deactivation of a content file in Content &gt; List View.</td>
</tr>
<tr>
<td><strong>Data Encryption Toggle</strong></td>
<td>Prevents the Encryption of User Information setting in Groups &amp; Settings &gt; All Settings &gt; System &gt; Security &gt; Data Security.</td>
</tr>
<tr>
<td><strong>Device Delete</strong></td>
<td>Prevents the deletion of a device in Devices &gt; List View.</td>
</tr>
<tr>
<td><strong>Device Wipe</strong></td>
<td>Prevents any attempt to perform a device wipe from the Device List View or Device Details screens.</td>
</tr>
<tr>
<td><strong>Enterprise Reset</strong></td>
<td>Prevents any attempt to perform an enterprise reset on a device from the Devices Details page of a Windows Rugged, Rugged Android device, or QNX device.</td>
</tr>
<tr>
<td><strong>Enterprise Wipe</strong></td>
<td>Prevents any attempt to perform an enterprise wipe on a device from the Devices Details page of a device.</td>
</tr>
<tr>
<td><strong>Enterprise Wipe (Based on User Group Membership Toggle)</strong></td>
<td>Prevents any attempt to perform an enterprise wipe on a device when it is removed from a user group. This is an optional setting that you can configure under Groups &amp; Settings &gt; All Settings &gt; Devices &amp; Users &gt; General &gt; Enrollment on the Restrictions tab. If you Restrict Enrollment to Configured Groups on this tab, you then have the added option of performing an enterprise wipe a device when it is removed from a group. For more information, see the Configuring Enrollment Restrictions section.</td>
</tr>
<tr>
<td><strong>Organization Group Delete</strong></td>
<td>Prevents any attempt to delete the current organization group from Groups &amp; Settings &gt; Groups &gt; Organization Groups &gt; Organization Group Details.</td>
</tr>
<tr>
<td><strong>Profile Delete/Deactivate</strong></td>
<td>Prevents any attempt to delete or deactivate a profile from Devices &gt; Profiles &gt; List View.</td>
</tr>
<tr>
<td><strong>Provisioning Product Delete</strong></td>
<td>Prevents any attempt to delete a provisioning product from Devices &gt; Products &gt; List View.</td>
</tr>
<tr>
<td><strong>Revoke Certificate</strong></td>
<td>Prevents any attempt to revoke a certificate from Devices &gt; Certificates &gt; List View.</td>
</tr>
<tr>
<td><strong>Secure Channel Certificate Clear</strong></td>
<td>Protects from any attempt to clear an existing secure channel certificate from Groups &amp; Settings &gt; All Settings &gt; System &gt; Advanced &gt; Secure Channel Certificate.</td>
</tr>
<tr>
<td><strong>User Account Delete</strong></td>
<td>Prevents any attempt to delete a user account from Accounts &gt; Users &gt; List View.</td>
</tr>
<tr>
<td><strong>Delete Telecom Plan</strong></td>
<td>Prevents the deletion of a telecom plan in Telecom &gt; Plan List.</td>
</tr>
<tr>
<td><strong>Override Job Log Level</strong></td>
<td>Prevents attempts to override the currently-selected job log level from Groups &amp; Settings &gt; Admin &gt; Diagnostics &gt; Logging. Overriding the Job Log Level is useful when a device or group of devices is having an issue. In this case, the admin can override those devices' settings by forcing an elevated log level to Verbose, which logs the maximum level of console activity, making it ideal for troubleshooting.</td>
</tr>
<tr>
<td><strong>App Scan Vendor Reset/Toggle</strong></td>
<td>Prevents the resetting (and subsequent wiping) of your app scan integration settings. This action is performed in Groups &amp; Settings &gt; All Settings &gt; Apps &gt; Application Integration &gt; App Scan.</td>
</tr>
</tbody>
</table>
Required Notes for Action

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock Device</td>
<td>Require a note for any attempt to lock a device from the <strong>Device List View</strong> or <strong>Device Details</strong> pages.</td>
</tr>
<tr>
<td>Lock SSO</td>
<td>Require a note for any attempt to lock an SSO session from the <strong>Device List View</strong> or <strong>Device Details</strong> screens.</td>
</tr>
<tr>
<td>Device Wipe</td>
<td>Require a note for any attempt to perform a device wipe from the <strong>Device List View</strong> or <strong>Device Details</strong> screens.</td>
</tr>
<tr>
<td>Enterprise Reset</td>
<td>Require a note for any attempt to enterprise reset a device from the <strong>Devices Details</strong> page of a Windows Rugged or Rugged Android device.</td>
</tr>
<tr>
<td>Enterprise Wipe</td>
<td>Require a note for any attempt to perform an enterprise wipe from the <strong>Devices Details</strong> page of a device.</td>
</tr>
<tr>
<td>Override Job Log Level</td>
<td>Require a note prior to attempts to override the default job log level from <strong>Groups &amp; Settings</strong> &gt; <strong>Admin</strong> &gt; <strong>Diagnostics</strong> &gt; <strong>Logging</strong>.</td>
</tr>
</tbody>
</table>

Integrating with Other Enterprise Systems

Take advantage of advanced MDM functionality by integrating your AirWatch environment with existing enterprise infrastructures such as email management with SMTP, directory services, and content management repositories (such as SharePoint).

AirWatch can integrate with the following internal components:

- **Email Relay (SMTP)** – Provide 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 certificate management systems to be managed within the Console.
- **Lotus Domino Web Service (HTTPS)** – Access Lotus Domino content and features through your AW 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 settings, provision device profiles with 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 [VMware AirWatch Cloud Connector Guide](#), the [VMware AirWatch Tunnel Admin Guide](#), and the 'Syslog' section of the [Reports & Analytics Guide](#), available on [AirWatch Resources](#).
Chapter 4: Organization Groups

Overview .................................................................34
Creating Organization Groups .......................................35
Creating Organization Group Types .................................37
Comparing Organization Groups Using Settings Comparison 38
Overview

AirWatch identifies users and establishes permissions using organization groups. 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.

You can access organization groups by navigating to Groups & Settings > Groups > Organization Groups > List View or through the organization group drop-down list. 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.

The organization groups accommodate functional, geographic, and organization entities and enable 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 as shown in the image, profiles, features, applications and other MDM settings can be set at the 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 the settings that you want to change or keep. These settings can be altered or carried down at any level.
Before setting up your organization group hierarchy in the AirWatch Admin Console, first decide on the group structure. This will allow you to make the best use of settings, applications and resources. For example, review the following configuration options:

- **Delegated Administration** – You can delegate administration of sub-groups to lower level administrators by restricting their visibility to a lower organization group.
  
  - **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 setting, and branding.
  
  - **Overall company** establishes enrollment against the company Active 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** – 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.

You can add repositories and applications to child groups that inherit parent group settings. 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 [VMware AirWatch Mobile Content Management (MCM) Guide](https://www.vmware.com) and the [VMware AirWatch Mobile Application Management (MAM) Guide](https://www.vmware.com) respectively, each available on [AirWatch Resources](https://www.vmware.com).

**Creating Organization Groups**

You must create an organization group (OG) 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. The Group IDs are used during enrollment of group devices to the appropriate organization group.

See [Configure Enrollment Options](#) for details about Group IDs as used in organization groups.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organization Group Name</strong></td>
<td>Enter a name for the child organization group to be displayed within the AirWatch Admin Console. Use alphanumeric characters only. Do not use odd characters.</td>
</tr>
<tr>
<td><strong>Group ID</strong></td>
<td>Enter an identifier for the organization group for the end users to use during device log in. Ensure the end users who share devices receive the <strong>Group ID</strong> as it may be required for the device to log in depending on your Shared Device configuration.</td>
</tr>
<tr>
<td><strong>Organization Group Type</strong></td>
<td>Select the preconfigured organization group type that reflects the category for the child organization group.</td>
</tr>
<tr>
<td><strong>Country</strong></td>
<td>Select the country where the organization group is based.</td>
</tr>
<tr>
<td><strong>Locale</strong></td>
<td>Select the language classification for selected country.</td>
</tr>
<tr>
<td><strong>Time Zone</strong></td>
<td>Select the time zone for the organization group.</td>
</tr>
</tbody>
</table>
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.

![For more information about the different types of Organization Groups (e.g. Global, Partner, Customer, Container, etc.), refer to the following VMware AirWatch Knowledge Base article:](https://support.air-watch.com/articles/95342377-Types-of-Organization-Groups)

5. Add region information and select **Save**.

### Viewing and Assigning Organization Groups

Another method of viewing and managing organization groups is to navigate to **Groups & Settings > Groups > Assignment Groups**. For details on assigning multiple organization groups to profiles, public applications and compliance policies, see **Using Assignment Groups** in the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

### Creating Organization Group Types

You can create custom organization group types to categorize your organization groups (OG) with similar business purposes. For example, your OGs named Sales-Pacific, Sales-Midwest, and Sales-Atlantic can each have a customized organization group type of Revenue.

You can create as many OG types as you like. 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.

Take the following steps to create a new organization group type:

1. Navigate to **Groups & Settings > Groups > Organization Groups > Organization Group Types** and select the **Add Organization Group Type** button.
2. The Add/Edit Organization Group Type page displays.
3. Complete the Name and Description fields.
4. Select Save.

Comparing Organization Groups Using Settings Comparison

As an Administrator, you may find it useful to compare the settings of one organization group (OG) to another. Comparing the OG settings enables you to:

- Upload XML files containing the OG settings from different AirWatch software versions.
- Eliminate the possibility of a difference in configuration causing problems. 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 lets you compare the UAT settings with the production settings directly.
- Filter the comparison results, allowing you to display only the settings you are interested in comparing.
- Search for a single setting by name with the search function.

The Organization Group Compare feature is only available for on-premises customers.

![Admin/Settings Management/Settings Comparison](image_url)
Comparing OG Settings

1. Navigate to Groups & Settings > All Settings > Admin > Settings Management > Settings Comparison.

2. Select an OG in your environment from the left drop-down menu (labeled with the numeral 1). Alternatively, upload the XML settings file by selecting the Upload button and choosing an exported OG setting XML file.

3. Select the comparison OG 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. This check box displays only those settings that apply to one OG but not the other. Individual settings that are empty (or not specified) will display in the comparison listing as 'NULL'.

---

Copyright © 2016 VMware, Inc. All rights reserved. Proprietary & Confidential.
Chapter 5: User and Admin Accounts

Overview .......................................................... 41
Choosing User Authentication Types .................. 41
Creating Basic User Accounts .......................... 47
Creating Directory-Based User Accounts .......... 50
Managing User Accounts ................................. 53
Using the Bulk Import Feature ......................... 55
Creating an Admin Account ............................. 57
Managing Admin Accounts .............................. 58
Overview

AirWatch manages devices by keeping track of the users of each device. Therefore, you must create and integrate user accounts for devices to enroll into AirWatch. Likewise, Administrator accounts must be created and assigned so Admins can easily manage users and devices.

The AirWatch Admin Console allows you to establish a complete user and admin infrastructure. It provides configuration options for authentication, enterprise integration and ongoing maintenance.

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 number of login steps required by the end user of 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

The 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.
- Can be used for any deployment method.
- Requires no technical integration.
- 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.
Active Directory / LDAP Authentication

Active Directory (AD)/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.

1. Device connects to AirWatch MDM to enroll device, user enters their Directory Services username and password
   - Username and password are encrypted during transport
   - AirWatch does not store the user’s Directory Services password

2. AirWatch queries the client’s Directory Services via Secure LDAP protocol over the internet using a service account for authentication

3. The users credentials are validated against the corporate Directory Services

4. If the user credentials are valid, the AirWatch server allows the device to complete device enrollment
Active Directory / LDAP Authentication with AirWatch Cloud Connector

The 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 in the below image.

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.
- 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.

For information on how to integrate your AirWatch environment with these infrastructures, see the VMware AirWatch Cloud Connector Guide, available on AirWatch Resources.
Authentication Proxy

The 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.

1. Device connects to AirWatch MDM to enroll device, user enters their Directory Services username and password
   - Username and password are encrypted during transport
   - AirWatch does not store the user’s Directory Services password
2. AirWatch relays the username and password to a configured Authentication Proxy endpoint that requires authentication (e.g. Basic Authentication)
3. The user’s credentials are validated against the corporate Directory Services
4. If the user credentials are valid, the AirWatch server allows the device to complete device enrollment
SAML 2.0 Authentication

The 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, AirWatch recommends SAML 2.0 integration.

Pros

- Offers single sign on capabilities.
- Authentication with existing corporate credentials.
- 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 VMware AirWatch SAML Guide, available on AirWatch Resources.

Token-based Authentication

The 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.

---

### Enabling Security Types

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 selecting 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. If your authentication type is Basic, then you should create Basic User Accounts.

To add a Basic User account:
1. Navigate to Accounts > Users > List View and select Add and then Add User. The Add / Edit User page displays.

2. In the General tab, complete the following settings to add a basic user.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Type</td>
<td>Choose Basic to add an Active Directory user.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter a username with which the new user is identified.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password that the user can use to log in.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password.</td>
</tr>
<tr>
<td>Full Name</td>
<td>Complete the First Name, Middle Name, and Last Name of the user.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Enter a name to represent the user in the AirWatch Admin Console.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Enter or edit the user's email address.</td>
</tr>
<tr>
<td>Email Username</td>
<td>Enter or edit the user's email username.</td>
</tr>
<tr>
<td>Domain</td>
<td>Select the email domain from the drop-down field.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>Enter the user's phone number including plus sign, country code, and area code. This field is required if you intend to utilize SMS to send notifications, specified in the below Notification section.</td>
</tr>
<tr>
<td>Enrollment Organization Group</td>
<td>Choose the organization group into which the user can enroll by selecting from this drop-down field.</td>
</tr>
<tr>
<td>Allow user to enroll into additional Organization Groups</td>
<td>Choose whether or not to allow the user to enroll into more than one organization group. If you select Enabled, then complete the Additional Organization Groups drop-down field.</td>
</tr>
<tr>
<td>User Role</td>
<td>Select the role for the user you are adding from this drop-down field.</td>
</tr>
<tr>
<td>Message Type</td>
<td>Choose the type of message you may send to the user, Email, SMS, or None. Selecting SMS requires a valid entry in the Phone Number field above.</td>
</tr>
<tr>
<td>Message Template</td>
<td>Choose the template for either email or SMS messages by selecting one from this drop-down field. Optionally, select Message Preview to preview the template and select the Configure Message Template to create a new template.</td>
</tr>
</tbody>
</table>
3. You may optionally select the **Advanced** tab and complete the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advanced Info Section</strong></td>
<td></td>
</tr>
<tr>
<td>Email Password</td>
<td>Enter the email password of the user you are adding.</td>
</tr>
<tr>
<td>Confirm Email Password</td>
<td>Confirm the email password of the user you are adding.</td>
</tr>
<tr>
<td>Distinguished Name</td>
<td>For directory users recognized by AirWatch, this field is pre-populated with the distinguished name of the user. This is a string representing</td>
</tr>
<tr>
<td></td>
<td>the user name and all authorization codes associated with an Active Directory user. This field is not applicable to Basic Users.</td>
</tr>
<tr>
<td>Manager Distinguished Name</td>
<td>Enter the distinguished name of the user's manager. This field is optional.</td>
</tr>
<tr>
<td>Category</td>
<td>Choose the User Category for the user being added.</td>
</tr>
<tr>
<td>Department</td>
<td>Enter the user's department for your company's administrative purposes.</td>
</tr>
<tr>
<td>Employee ID</td>
<td>Enter the user's employee ID for your company’s administrative purposes.</td>
</tr>
<tr>
<td>Cost Center</td>
<td>Enter the user's cost center for your company's administrative purposes.</td>
</tr>
<tr>
<td>Custom Attribute 1-5 (for</td>
<td>Enter your previously-configured custom attributes, where applicable.</td>
</tr>
<tr>
<td>Directory users only)</td>
<td>You may define these custom attributes by navigating to <strong>Groups &amp; Settings &gt; All Settings &gt; Devices &amp; Users &gt; Advanced &gt; Custom Attributes</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Custom attributes can be configured only at Customer organization groups.</td>
</tr>
<tr>
<td><strong>Certificates Section</strong></td>
<td></td>
</tr>
<tr>
<td>Use S/MIME</td>
<td>Enable or Disable Secure/Multipurpose Internet Mail Extensions (S/MIME). If enabled, you must have an S/MIME-enabled profile and you must upload an S/MIME certificate by selecting <strong>Upload</strong>.</td>
</tr>
<tr>
<td>Separate Encryption Certificate</td>
<td>Enable or Disable encryption certificate. If enabled, you must upload an encryption certificate using <strong>Upload</strong>. Generally, the same S/MIME certificate is used for signing and encryption, unless a different certificate is expressly being used.</td>
</tr>
<tr>
<td>Old Encryption Certificate</td>
<td>Enable or disable a legacy version encryption certificate. If enabled, you must <strong>Upload</strong> an encryption certificate.</td>
</tr>
<tr>
<td><strong>Staging Section</strong></td>
<td></td>
</tr>
<tr>
<td>Enable Device Staging</td>
<td>Enable or disable the staging of devices. If enabled, you must choose between <strong>Single User Devices</strong> and <strong>Multi User Devices</strong>. If <strong>Single User Devices</strong>, you must select between <strong>Standard</strong>, where users themselves login after staging and <strong>Advanced</strong>, where a device is enrolled on behalf of another user. See <strong>Device Staging</strong> for more information.</td>
</tr>
</tbody>
</table>
4. Select *Save* to save only the new user or select *Save and Add Device* to save the new user and proceed to the *Add Device* page.

### Creating Directory-Based User Accounts

After you decide which [Authentication Type](#) you want to use, 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.

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. To import Active Directory users in bulk, see Using the Bulk Import Feature.

To add a Directory based user account:

1. Navigate to *Accounts* > *Users* > *List View* and select *Add* and then *Add User*. The *Add / Edit User* page displays.
2. In the *General* tab, complete the following settings to add a directory user.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Type</td>
<td>Choose <em>Directory</em> to add an Active Directory user.</td>
</tr>
<tr>
<td>Directory Name</td>
<td>This pre-populated field identifies the Active Directory name.</td>
</tr>
<tr>
<td>Domain</td>
<td>Choose the domain name from the drop-down field.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the user’s directory username and select <em>Check User</em>. If the system finds a match, the user’s information is automatically populated.</td>
</tr>
<tr>
<td>Full Name</td>
<td>In addition to automatically populating the matching user’s information, use <em>Edit Attributes</em> to allow any field that syncs a blank value from the directory to be edited. If a field syncs an actual (not empty) value from the directory, then that field needs to be edited in the directory itself and the change takes effect on the next directory sync. Complete any blank field returned from the directory in <em>Full Name</em> and select <em>Edit Attributes</em> to save the addition.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Enter the name that will display in the admin console.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Enter or edit the user’s email address.</td>
</tr>
<tr>
<td>Email Username</td>
<td>Enter or edit the user’s email username.</td>
</tr>
<tr>
<td>Domain</td>
<td>Select the email domain from the drop-down field.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>Enter the user’s phone number including plus sign, country code, and area code. This field is required if you intend to utilize SMS to send notifications.</td>
</tr>
</tbody>
</table>
### Setting Description

#### Enrollment

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrollment Organization Group</td>
<td>Select the organization group into which the user will enroll.</td>
</tr>
<tr>
<td>Allow user to enroll into additional Organization Groups</td>
<td>Choose whether or not to allow the user to enroll into more than one organization group. If you select Enabled, then complete the Additional Organization Groups.</td>
</tr>
<tr>
<td>User Role</td>
<td>Select the role for the user you are adding from this drop-down field.</td>
</tr>
</tbody>
</table>

#### Notification

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Type</td>
<td>Choose the type of message you may send to the user, Email, SMS, or None. Selecting SMS requires a valid entry in the Phone Number field above.</td>
</tr>
<tr>
<td>Message Template</td>
<td>Choose the template for either email or SMS messages from this drop-down field. Optionally, select the Message Preview to preview the template and select the Configure Message Templates link to create a new template.</td>
</tr>
</tbody>
</table>

3. You may optionally select the Advanced tab and complete the following settings.

#### Setting Description

##### Advanced Info Section

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Password</td>
<td>Enter the email password of the user you are adding.</td>
</tr>
<tr>
<td>Confirm Email Password</td>
<td>Confirm the email password of the user you are adding.</td>
</tr>
<tr>
<td>Distinguished Name</td>
<td>For directory users recognized by VMware AirWatch, this field is pre-populated with the distinguished name of the user. This is a string representing the user name and all authorization codes associated with an Active Directory user.</td>
</tr>
<tr>
<td>Manager Distinguished Name</td>
<td>Enter the distinguished name of the user's manager. This field is optional.</td>
</tr>
<tr>
<td>Category</td>
<td>Choose the user category for the user being added.</td>
</tr>
<tr>
<td>Department</td>
<td>Enter the user's department for your company's administrative purposes.</td>
</tr>
<tr>
<td>Employee ID</td>
<td>Enter the user's employee ID for your company’s administrative purposes.</td>
</tr>
<tr>
<td>Cost Center</td>
<td>Enter the user's cost center for your company's administrative purposes.</td>
</tr>
<tr>
<td>Custom Attribute 1-5 (for Directory users only)</td>
<td>Enter your previously-configured custom attributes, where applicable. You may define these custom attributes by navigating to Groups &amp; Settings &gt; All Settings &gt; Devices &amp; Users &gt; Advanced &gt; Custom Attributes.</td>
</tr>
</tbody>
</table>

**Note:** Custom attributes can be configured only at Customer organization groups.

##### Certificates Section
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use S/MIME</td>
<td>Enable or disable the use of Secure/Multipurpose Internet Mail Extensions (S/MIME). If enabled, you must have an S/MIME-enabled profile and you must upload an S/MIME certificate by selecting <strong>Upload</strong>.</td>
</tr>
<tr>
<td>Separate Encryption Certificate</td>
<td>Enable or disable the use of a separate encryption certificate. If enabled, you must upload an encryption certificate using <strong>Upload</strong>. Generally, the same S/MIME certificate is used for signing and encryption, unless a different certificate is expressly being used.</td>
</tr>
<tr>
<td>Old Encryption Certificate</td>
<td>Enable or disable a legacy version encryption certificate. If enabled, you must <strong>Upload</strong> an encryption certificate.</td>
</tr>
</tbody>
</table>

**Staging Section**

<table>
<thead>
<tr>
<th>Enable Device Staging</th>
<th>Enable or disable the staging of devices.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If enabled, you must choose between <strong>Single User Devices</strong> and <strong>Multi User Devices</strong>.</td>
</tr>
<tr>
<td></td>
<td>If <strong>Single User Devices</strong>, you must select between <strong>Standard</strong>, where users themselves login after staging and <strong>Advanced</strong>, where a device is enrolled on behalf of another user.</td>
</tr>
<tr>
<td></td>
<td>For more information about device staging, refer to the <strong>VMware AirWatch Mobile Device Management Guide</strong>, available on <strong>AirWatch Resources</strong>.</td>
</tr>
</tbody>
</table>

4. Select **Save** to save only the new user or select **Save and Add Device** to save the new user and proceed to the **Add Device** page.

For more information about adding directory users to AirWatch, refer to the **VMware AirWatch Directory Services Guide**, available on **AirWatch Resources**.
Managing User Accounts

The List View page, which you can find by navigating to Accounts > Users > List View, provides useful tools for common account maintenance and upkeep. Access the following options and functions from the main List View.

- **Filters** – View only the desired users by using the following filters:
  - Security Type
  - Enrollment Organization Group
  - Enrollment Status
  - User Group
  - User Role

- **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** – Enables you to fully customize the column layout.
  - **Summary** – View the List View with the default columns and view settings.
  - **Custom** – Select only the columns in the List View you want to see. You also have the option to apply selected columns to all administrators at or below the current organization group.

- **Sorting** – Most columns in the List View (in both Summary and Custom Layout) are sortable including Devices, User Groups, and Organization Group.
• **Export button ( )** – Save a .csv file (comma-separated values) of the entire List View that can be viewed and analyzed in Excel.

**Selecting Users and Performing Actions**

The List View features a check box and Edit icon located next to each user account. The Edit icon enables you to make basic changes to the user's account. Selecting a single check box causes three action 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** – Quickly and completely delete a user account if a member of your organization resigns or is fired.
  - **Activate** – Activate the account 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.

You can select multiple user accounts using the check box. Doing so modifies the available action buttons and applies the actions to the selected users and their respective devices.
Using the Bulk 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 users one at a time.

Create 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.

To 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 (i) 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.
   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. 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.
   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 page in the AirWatch Admin Console, and select Choose File to locate and upload the saved comma-separated values (.csv) file.
8. Select 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 (i) 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**.

8. 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 (i) 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. Select **Save**.
Creating an Admin Account

You 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. Each admin that will maintain and supervise the AirWatch Admin Console must have an individual account.

To add an admin account:

1. Navigate to Accounts > Administrators > List View, select Add and then Add Admin. The Add/Edit Admin page displays.

2. Under the Basic tab, for the User Type field, select either Basic or Directory.
   - If you select Basic, then fill in all required fields on the Basic tab, including username, password, First Name, and Last Name. You can also enable Two-Factor Authentication and select a Notification option including the use of a message template.
   - 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 then select the Organization Group followed by the Role you want to assign to the new admin. Add new roles by using Add Role.

5. Select the API tab to choose the Authentication type.

6. Select the Notes tab to enter additional Notes for the admin user.

7. Select Save to create the new admin account with the assigned role.

Creating a Temporary Admin Account

You may grant temporary 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, select Add. Select the Add Temporary Admin option.

2. Complete the following required fields:
   - Username
   - Password and Confirm Password
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.

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

6. 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. Use the actions menu to implement key management functions for ongoing maintenance and upkeep.

- **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.
Chapter 6: Role-Based Access

Overview ................................................................. 60
Default and Custom Roles ...................................... 60
Creating and Managing User Roles .......................... 62
Creating and Managing Administrator Roles ............ 63
Comparing Admin Roles ........................................... 66
Overview

The AirWatch Admin Console allows you to define access levels for individual users or groups based on the roles you created during the user enrollment process. For example, help desk administrators within your enterprise may have limited access within the console, while the IT Manager has a greater range of permissions.

To enable role-based access control, you must first set up the administrator and user roles within the AirWatch Admin Console. These roles are defined by specific resources, also known as permissions, which enable and disable access to various features within the AirWatch Admin Console. Roles can also be created for end-users who need access to the Self-Service Portal.

There are several default roles already provided by AirWatch from which you may select. These default roles are available with every AirWatch upgrade and help quickly assign roles to new users. If you require further customization, you have the option to create custom roles to further tailor the user privileges and permissions. Unlike default roles, custom roles require manual updates with every AirWatch upgrade.

Default and Custom Roles

There are several Default Roles provided by AirWatch. These default roles are available with every AirWatch upgrade, and help you 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 inherent advantages and disadvantages. 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 the Administrators and Users in your organization or MDM deployment, which is why Custom Roles were created.

Custom Roles allow you to customize as many unique roles as you require, 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 features.
Default End User Roles

The following roles are available by default to end users in the AirWatch Admin Console:

- **Full Access Role** – Provides full permission to perform all the tasks on the Self-Service Portal.
- **Basic Access Role** – Provides all permissions except MDM commands from the Self-Service Portal.

Editing a Default End User Role to Create a Custom User Role

If none of the available Default Roles provide the proper fit for user resources in your organization, then consider modifying an existing role and creating a custom user role by performing the following steps:

1. Ensure you are currently in the organization group you want the new role to be associated with.

2. Navigate to **Accounts > Users > Roles**.

3. Determine which role from the list best fits the role you want to create and edit that role by selecting the edit icon (edit) to the far right. The **Add/Edit Role** page displays.

4. Edit the **Name**, **Description**, and **Initial Landing Page** fields as necessary. Review each of the check boxes. These represent the various permissions, selecting and deselecting those options as necessary.

5. Select **Save** to save your changes, overwriting the role's prior settings in favor of the new settings.

Default Administrator Roles

The following roles are available by default to administrators in the AirWatch admin console:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Administrator</strong></td>
<td>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 <strong>Administration</strong> tab under <strong>System Configuration</strong>.</td>
</tr>
<tr>
<td><strong>AirWatch Administrator</strong></td>
<td>The AirWatch Administrator role allows comprehensive access to the AirWatch environment. However, this access excludes the <strong>Administration</strong> tab under <strong>System Configuration</strong>, because that tab manages top-level AirWatch Admin Console settings.</td>
</tr>
<tr>
<td><strong>Device Manager</strong></td>
<td>The Device Manager role grants users significant access to the AirWatch Admin Console. However, this role is not designed to configure most System Configurations (Active Directory (AD)/Lightweight Directory Access Protocol (LDAP), Simple Mail Transfer Protocol (SMTP), Agents, etc.). For these tasks, use a top-tier role like the AirWatch Administrator or System Administrator.</td>
</tr>
<tr>
<td><strong>Read Only</strong></td>
<td>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 an AirWatch environment. This role is not useful for system operators or administrators.</td>
</tr>
<tr>
<td><strong>Content Management</strong></td>
<td>The Content Management role only includes access to AirWatch Content Locker management. Use this role for specialized administrators responsible for uploading and managing a device fleet's content.</td>
</tr>
</tbody>
</table>

Note: The System Administrator role is not available for Software as a Service (SaaS) customers.
### Table: Role-Based Access

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Management</td>
<td>The Application Management role allows admins with this access to deploy and manage the device fleet's internal and public apps. Use this role for a application management administrator.</td>
</tr>
<tr>
<td>Help Desk</td>
<td>The Help Desk role provides the tools necessary for most Level 1 IT Help Desk functions. The primary tool available in this role is the AirWatch Administrators' ability to see and respond to device info with remote actions. However, this role also contains report viewing and device searching abilities.</td>
</tr>
<tr>
<td>Report Viewer</td>
<td>The Report Viewer role allows viewing of the data captured through Mobile Device Management (MDM). This role limits its users to generating, viewing, exporting, and subscribing to reports from the AirWatch Admin Console.</td>
</tr>
</tbody>
</table>

### Editing a Default Admin Role to Create a Custom Admin Role

If none of the available Default Roles provide the proper fit for admin resources in your organization, then consider modifying an existing default role into a custom admin role by performing the following steps:

1. Ensure you are currently in the organization group with which you want the new role to be associated.

2. Navigate to **Accounts > Administrators > Roles**.

3. Determine which role from the list best fits the role you want to create. Select the check box for that role.

4. Select **Copy** from the actions menu above the listing. The **Copy Role** page displays.

5. Edit specific settings of the copy in the resulting **Copy Role** page. Create a unique **Name** and **Description** for the customized role. See **Creating a New Administrator Role** for details.

6. Select **Save**.

### Creating and Managing User Roles

User roles enable you to customize initial landing pages, restrict access to the Self Service portal, and configure the actions that logged in users can perform for each type of user. 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.

#### Create a New User Role

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

1. Navigate to **Accounts > Users > Roles** and select **Add**. The **Add/Edit Role** page displays.

2. Enter a **Name**, **Description** and select the **Initial Landing Page** of the SSP for users with this new role.

   For existing user roles, the default **Initial Landing Page** is the **My Devices** page.

3. Select from a list of options the level of access and control end users of this assigned role should have in the SSP.

   - Click **Select None** to clear all check boxes on the page.

   - Select all the check boxes on the page by clicking **Select All**.
4. **Save** the changes to the role. The added user role now appears in the list on the Roles page. From the Roles page, you can view, edit, or delete roles.

**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 that the assigned end users should have in the SSP. These role settings are customizable by organization group.
3. Select **Save**.

**Assign or Edit the Role of an Existing User**

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

1. Select the appropriate organization group.
2. Navigate to Accounts > Users > List View
3. Search for the specific user from the list that you want to edit. Once you have identified the user, select the Edit icon under the check box. The **Add/Edit User** screen displays.
4. In the **General** tab, scroll down to the **Enrollment** section and select a **User Role** from this drop-down field to change the role for this specific user.
5. Select **Save**.

**Creating and Managing Administrator Roles**

To create a new administrator role, follow these steps.
1. Navigate to Accounts > Administrators > Roles and select Add Role in the AirWatch Admin Console.

![Create Role](image)

2. In the Create Role, 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 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.

You must 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 **Added Resources on page 68**.

**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 edits are disabled for at least one subcategory.
- All category settings have the read-only (edit disabled).
- The majority of category settings are read-only, but edits are enabled for at least one subcategory.

**Assign or Edit the Role of an Admin**

1. Navigate to **Accounts > Administrators > List View**, select **Add**, and then select **Add Admin**. The **Add/Edit Admin** page displays.
2. Select the **Roles** tab. Then select **Add Role**.
3. Enter the **Organization Group** and **Role** details for each role that is added.
4. Select **Save**.

**Importing and Exporting Administrator Roles**

**Exporting Roles**

Using an XML file, you can export an Administrator Role from one environment to another environment. To initiate this process, take the following steps:
1. Navigate to Accounts > Administrators > Roles.

2. Select the check box next to the administrator role that you want to export. Doing so displays actions buttons above the role listing.

3. Select Export and save the .xml file to a location on your device.
   The Export action is not available if you select more than one admin role.

**Importing Roles**
To import a role into a separate AirWatch environment, take the following steps:

1. Navigate to Accounts > Administrators > Roles and select Import Role.

2. In the Import Role page, select Browse... button and locate the previously-saved .xml file. Select the Upload button to upload the admin role to the Category listing for validation.

3. AirWatch performs a series of validation checks including an .xml file check, importing role permission check, duplicate role name check, and blank name and description check.

4. Select specific Categories in the left pane and check their resource settings to verify the imported role's specifications. You may also make adjustments to the resources and to the Name and Description of the imported role based on your needs.

5. Select Save to apply the imported role to the new environment.

**Versioning Issues**
There may be cases where an exported role is imported into an environment running an earlier version of AirWatch. This earlier version may not have the same resources and permissions that comprise the imported role.

In these cases, AirWatch notifies you with the following message:
*The status for some permissions were not found. Please review and correct the highlighted permissions before saving.*

Use the category listing page to deselect the highlighted permissions. This action allows you to save the role to the new environment.

**Comparing Admin Roles**

Compare two Admin Roles with the Compare Roles tool:

1. Navigate to Accounts > Administrators > Roles.

2. Choose any two listed roles, including roles that appear on different pages, and select those roles.

3. Select Compare. 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.
The **Compare** button does not display if you have fewer than two or more than two roles selected.

- By default, only differences between the two roles are displayed initially. This allows you to see only those categories and subcategories whose settings are different. Select the **Show All Permissions** check box to display all the permissions including those settings that are identical across the two selected roles.

- If you choose two roles that have identical permissions across the board, the console displays the following message at the top of the **Compare Roles** page:
  "There are no differences in permissions between the two roles."

- You may also select **Export** to create a .csv file (comma-separated values) that can be read by Excel. This .csv file contains the complete list of settings for Role 1 and Role 2, enabling you to fully analyze the differences between them.

**Using the Categories Column**

Selecting from the list of **Categories** on the left populates all the roles in that category on the right panel. Additionally, role subcategories can be viewed in the right panel by selecting the **Details** link to the far-right side. Collapse the role subcategory by selecting the **Hide** link.

There is an **All** category in the left panel that, when selected, displays all the parent categories on the **Compare Roles** page. When you enter a search parameter in the **Search Resources** bar, the right panel only displays matching category and resources listings. The search function is persistent. This means that as long as you have a parameter in the **Search Resources** bar, selecting the **All** category displays only the **matching** categories and resources even after you drill down into specific resources and make **Read** and **Edit** selections.
Added Resources

As part of AirWatch v8.3 release, below are the newly added resources in the AirWatch Admin Console.

<table>
<thead>
<tr>
<th>Main Category</th>
<th>Sub-Category</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>API &gt; REST</td>
<td>Compliance Policy</td>
<td><strong>Rest API Compliance Policy Delete</strong> – Enables access to all Delete APIs in Compliance Policy collection.</td>
</tr>
<tr>
<td>API &gt; REST</td>
<td>Compliance Policy</td>
<td><strong>Rest API Compliance Policy Execute</strong> – Enables access to all Execute APIs in Compliance Policy collection.</td>
</tr>
<tr>
<td>API &gt; REST</td>
<td>Compliance Policy</td>
<td><strong>Rest API Compliance Policy Write</strong> – Enables access to all Write APIs in Compliance Policy collection.</td>
</tr>
<tr>
<td>API &gt; REST</td>
<td>Compliance Policy</td>
<td><strong>Rest API Compliance Policy Read</strong> – Enables access to all READ only APIs Compliance Policy collection.</td>
</tr>
<tr>
<td>API &gt; REST</td>
<td>Users</td>
<td><strong>Rest API User Tokens Read</strong> – Enables access to Enrollment user tokens for APIs in Enrollment User collection.</td>
</tr>
<tr>
<td>Hub &gt; Overview</td>
<td>Overview</td>
<td><strong>ViewAppleTemplate</strong> – Enables read access to the Apple templates in the Hub.</td>
</tr>
<tr>
<td>Hub &gt; Overview</td>
<td>Overview</td>
<td><strong>EditAppleTemplate</strong> – Enables write access to the Apple templates in the Hub.</td>
</tr>
<tr>
<td>Hub &gt; Reports</td>
<td>General</td>
<td><strong>View All Reports</strong> – Gives permission to view All Reports.</td>
</tr>
<tr>
<td>Settings &gt; Apps</td>
<td>Catalog</td>
<td><strong>Paid Public Applications</strong> – To enable management of paid app store applications without volume purchasing.</td>
</tr>
<tr>
<td>Settings &gt; Email</td>
<td>Email Notification Service Settings</td>
<td><strong>Email Notification Service</strong> – Provides access to manage email notifications service settings.</td>
</tr>
<tr>
<td>Settings &gt; Content</td>
<td>Applications</td>
<td><strong>eSignature</strong> – Settings for eSignatures under Content. Navigate to Settings\Content\Advanced\eSignature.</td>
</tr>
<tr>
<td>Settings &gt; Devices &amp; Users</td>
<td>Windows Phone 8</td>
<td><strong>WindowsPhoneHealthAttestationEdit</strong> – Gives permission to view and edit data collected by Microsoft’s Health Attestation feature.</td>
</tr>
<tr>
<td>Settings &gt; System</td>
<td>Enterprise Integration</td>
<td><strong>Settings/HeaderBasedAuthentication</strong> – Gives permission to view and edit the settings for the authentication header protocol.</td>
</tr>
</tbody>
</table>
Chapter 7: User Groups

Overview ................................................................. 70
Adding User Groups Without Directory Integration (Custom) 70
Adding Directory-Based User Groups ......................... 70
Editing User Groups Permissions ............................. 72
Accessing User Details ............................................ 72
Managing User Groups ........................................... 73
Device Assignments .............................................. 75
Overview

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, user groups should be aligned with security groups and business roles within your organization.

AirWatch recommends 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. As an alternative to user groups, you can also manage content by assigning devices according to preconfigured network IP address ranges or custom attributes. For details, see the topic Device Assignments in the VMware AirWatch Mobile Device Management Guide, available on AirWatch Resources.

Adding User Groups Without Directory Integration (Custom)

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 modify 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 Bulk Import Feature for more about adding user groups in bulk.

To establish a custom user group without Active Directory integration:

1. Navigate to Accounts > User Groups > List View and select Add and then Add User Group.
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 through user group integration. Once you import your existing directory service groups into AirWatch 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 a 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.

The administrator must designate an existing organization group as the primary root location from which the administrator will manage devices and users. Directory services must be enabled at this root organization group. See the [VMware AirWatch Directory Services Guide](https://www.vmware.com/get/p/id/26958) 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 that AirWatch recognizes them as belonging to a configured group. You can use this group to restrict who can enroll. See [Using the Bulk Import Feature](https://docs.vmware.com/en/AirWatch/Guide/8.1/index.html#enrol) for more about adding directory user groups in bulk.

**To create a Directory-based User Group:**

1. Navigate to **Accounts > User Groups > List View** and select **Add** and then **Add User Group**.
   For adding admins, use the same steps 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 the search criteria to identify the name of 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** plus sign (+) 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. These can be configured from the Permission settings of the group after the group is saved.

As you configure **Custom Settings**, consider the following definitions:

   • **Management Permissions** – Allows all admins to manage the user group.

   • **Default Role** – Assigns a 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 the 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.

Send Email to User when Adding Missing Users – Sends a correspondence to the user if added to the user group.

7. Select Save.

Editing User Groups Permissions

Fine-tuning user group 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, you can 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. The User Details page is 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.
- All assigned, accepted and declined Terms of Use.
Encrypting User Personal Details

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.

1. Enable encryption, selecting which user data fields to encrypt.
2. Click Save to encrypt 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.

Managing User Groups

To manage user groups, navigate to Accounts > User Groups > List View. This page features useful tools for common user group maintenance and upkeep. Access the following options and functions from the main List View.

- Filters – View only the desired user groups by utilizing the following filters:
  - User Group Type
  - Sync Status
  - Merge Status

- Add
  - Add User Group – Perform a one-off addition of either a Directory-Based User Group or a Custom User Group.
  - Batch Import – Import new user groups in bulk by using a comma-separated values (.csv) file. Enter a unique name and description to organize multiple user groups at a time.

- Sorting and Resizing Columns – Columns in the List View that are sortable are Group Name, Last Sync On, Users, and Merge Status. Columns that can be resized are Group Name and Last Sync On.
• **Details View** – Select the link in the **Group Name** column to view basic user group information in the Details View, including group name, group type, external type, manager, number of users, and a link to the group mapping settings in **All Settings > Devices & Users > General > Enrollment** in the **Grouping** tab.

• **Export** – Save a .csv file (comma-separated values) of the entire unfiltered or filtered **List View** that can be viewed and analyzed in Excel.

**Adding Users to User Groups**

1. Navigate to **Accounts > Users > List View**.

2. Select one or more users in the listing by inserting a check mark in the check box to the left.

3. Select the **More** button and then select **Add To User Group**. The **Add Selected Users Into Custom User Group** page displays.

4. You may add users to an **Existing User Group** or create a **New User Group**.

5. Choose the **Group Name**.

6. Select **Save**.

7. Navigate to **Accounts > User Groups > List View**.
   
   a. At this point, the Active Directory (AD) synchronization (which is an automated, scheduled process) will copy these pending user group users to a temporary table where they can be reviewed, added or removed.

   b. If you do not want to wait for the automated AD sync, you may apply manual synchronization by selecting the user group to which you added users, then selecting the **Sync** button.

8. You may optionally select **More > View and Merge** to perform maintenance tasks such as review, add, and remove pending user group users.

9. Select **More > Add Missing Users** to combine the temporary table of pending user group users with the Active Directory user group users, making their addition official and complete.

**Selecting User Groups and Performing Actions**

The **List View** features a selection check box and **Edit** icon to the left of the user. Selecting the **Edit** icon enables you to make basic changes to the user group. Select one or more check boxes to see the action buttons for the listing.

You may select more than one user group by selecting as many checkboxes as you like. Doing so will modify the available action buttons and will also make the available actions apply to multiple groups and their respective users.

• **Sync** – Copy recently-added user group users to the temporary table, manually, ahead of the automatically scheduled Active Directory sync by AirWatch.

• **View Users** – Review the usernames of all the members of the selected user group.

• **More**
  
  o **View and Merge** – View, Add, and Remove users recently added to the temporary user group table. User group users that appear in this table await the automated AirWatch user group sync.
Add Missing Users – Combine the temporary user group table with the Active Directory table, making the addition of these new users in the user group official.

Delete – Delete a user group.

Viewing and Assigning User Groups

In addition to navigating to Accounts > User Groups > List View to view and manage user groups, another method is to navigate to Groups & Settings > Groups > Assignment Groups. For details on assigning multiple user groups to profiles, public applications, and compliance policies, see Using Assignment Groups in the VMware AirWatch Mobile Device Management Guide, available on AirWatch Resources.

Device Assignments

Device Assignments enable you to move devices across organization groups (OG) and usernames based on the network internet protocol (IP) address range or custom attributes. It is an alternative to organizing device content (e.g. profiles, apps, policies and products) by user groups.

When your device connects to Wi-Fi within a range of IP addresses that you define, the device then authenticates and automatically installs profiles, apps, policies, and product provisions specific to the OG that you associate with the IP address.

You can also define rules based on custom attributes. When a device with an assigned attribute enrolls (or when a device receives a product provision containing a qualifying custom attribute), the rule assigns the device to the configured organization group.

Instead of admins manually moving devices between OGs, device assignments direct the console to automatically change the device’s organization group (or username) when it connects to Wi-Fi of its own unique network range or custom attribute rule that you define.

A typical use case for device assignments is a user who regularly changes roles and requires specialized profiles and applications for each role.

You must choose between implementing User Groups for the purpose of moving devices and Device Assignments since AirWatch does not support both functions on the same device.

To configure the Device Assignment

Device assignments can only be configured at a child organization group. Configuring the Device Assignment is a two-step process:

1. Enable and configure Device Assignments
   a. Navigate to Groups & Settings > All Settings > Devices & Users > General > Advanced and then select Override or Inherit for the Current Setting according to your needs.
b. Select **Enabled** in the **Enable Device Assignment Rules** field.

c. Choose the management **Type**:

   - **Organization Group By IP Range** – Moves the device to a specified organization group when the device leaves one Wi-Fi network range and enters another, triggering the automatic push of profiles, apps, policies, and products.

   - **Organization Group By Custom Attribute** – Moves the device to an organization group based on custom attributes. Custom attributes enable administrators to extract particular values from a managed device and return it to the AirWatch Admin Console. You can also assign value to devices for use in functions such as rules-based product provisioning or device referencing in the AirWatch Admin Console with lookup values.

   - **Username By IP Range** – When a device exits one network range and enters another, the device, instead of moving from one OG to another, automatically changes usernames, and triggers the same push of profiles, apps, policies, and products. This option is for customers with a limited ability to create new organization groups, thus providing an alternate way to take advantage of the device assignment feature.

   **Important:** If you want to change the assignment **Type** on an existing device assignment configuration, you must first navigate to **Groups & Settings > Groups > Organization Groups > Network Ranges** and delete all existing defined ranges.

d. Choose the **Device Ownership** options. Only devices with the selected ownership types are assigned:

   - Corporate – Dedicated
   - Corporate – Shared
   - Employee Owned
   - Undefined

e. Select **Save** once all the options are set.
2. **Define Device Assignment Rule or Network Range**

Once the settings page refreshes, you may specify a device assignment by custom attribute rule, the directions to which are detailed in Assigning Organization Groups Using Custom Attributes, or you may specify a network range by taking the following steps:

a. Select the link **Click here to create a network range** or navigate to Groups & Settings > Groups > Organization Groups > Network Ranges.

b. To add a single internet protocol (IP) address range, select **Add Network Range**. In the Add/Edit Network Range page, complete the following fields and then select **Save**:
   - **Start IP Address** – Enter the top end of the network range.
   - **End IP Address** – Enter the bottom end of the network range.
   - **Organization Group Name** – Enter the organization group name to which devices will move when the above network range is entered. This field is only visible if the network assignment **Type** is 'Organization Group By IP Range.'
   - **Username** – Enter the username to whom devices will register when the above network range is entered. This field is only visible if the network assignment **Type** is 'Username by IP Range.'
   - **Description** – Optionally, add a helpful description of the network range.
   - Overlapping network ranges is not permissible and results in the message, "Save Failed, Network Range already exists."

c. If you have several network ranges to add, you can optionally select **Bulk Import** to save time. On the Bulk Import page, select the **Help** link to view and download the bulk import template. Complete this template, import it using the **Batch Import** page, and select **Save**.
Chapter 8: Smart Groups

Overview ................................................................. 79
Creating a Smart Group ........................................... 79
Assigning a Smart Group .......................................... 80
Managing Smart Groups ........................................... 82
Overview

Smart groups are customizable groups that determine which platforms, devices, and end users receive an assigned 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.

You can create smart groups when you upload content and define settings. However, their modular nature means you can also 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.

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 applies and from which it can be managed.
2. Navigate to Groups & Settings > Groups > Assignment Groups and then select Add Smart Group.
3. Enter a Name for the smart group.
4. Configure the smart group type. Choose 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.

While Platform is a criterion within a smart group, the platform configured in the device profile or compliance policy always takes precedence over the smart group’s platform. For instance, if a device profile is created for the iOS platform, the profile is only 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.

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.

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

- You will use the Select Devices or Users type 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.

5. Select Save when complete.

Assigning a Smart Group

Before smart groups take effect, you must first assign them to an application, book, compliance policy, device profile, video channel or product provision. There are two methods to assign a smart group:
• During the process of creating a device product (app, book, policy, profile, channel, or provision).
• During the process of managing the smart group itself.

Assigning While Creating a Device Product

Assign a smart group when you add or create an application, book, compliance policy, device profile, video channel, or product provision.

1. Complete the Assigned Groups drop-down field.

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 a 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.

Assigning While Managing the Smart Group

Take the following steps to assign a smart group during the process of managing the smart group.

1. Navigate to Groups & Settings > Groups > Assignment Groups to view the entire list of smart groups.

2. Select the smart group(s) you want to assign and select Assign. The Assign page displays.

Select the Groups link at the top of the Assign page to display the Groups page. On this page you will see the organization groups that manage the smart groups. Select the Close button to return to the Assign page.

3. On the Assign page, use the search box to view the list of eligible products and assign it to the selected smart groups.

4. Select Next to display the View Device Assignment page and confirm the assignment status.

5. Select Save & Publish.

Excluding Smart Groups in Profiles and Compliance Policies

In addition to apps, books, video channels and products, smart groups apply to device profiles and compliance policies. This flexibility lets you exclude selected smart groups from profiles and policies.

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 Exclusions field to display the Excluded Groups field.

2. In the Excluded Groups field, select those smart groups that you want to exclude from the assignment of this profile or policy.

If you select the same smart group in both the Assigned Groups and Excluded Groups fields, then the profile or policy fails to save.
3. Select **View Device Assignment** to preview the affected devices.

**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 > Assignment Groups** to view the entire list of smart groups. Admins will only see those groups they are able to manage based on their permissions settings.

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

Select a link in the **Devices** column to load up the **Devices > List View** with only those devices included in the smart group.

You can **Filter** your collection of groups by **Group Type** (Smart, Organization, User, or all) or by **Assigned** status (whether the group has been assigned, excluded, both, or neither).

You can also **Assign** a smart group directly from the listing. See **Assigning While Managing the Smart Group**.

**Editing a Smart Group**

Any edits that you apply to a smart group affects 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 want to exclude some of the executives, then simply edit the smart group by specifying **Exclusions**. This action removes not only the two internal apps but also the compliance policy and device profile from those excluded devices.

The **Console Event** logger keeps track of changes made to smart groups, including the author of changes, devices added, and devices removed. See **Console Event Logger** for detailed Information.

To edit a smart group:
1. Navigate to Groups & Settings > Groups > Assignment Groups.

2. Select the Edit icon located to the left of the listed smart group that you want to edit. You can also select the smart group name in the Group column. The Edit Smart Group page displays with its existing settings.

3. In the Edit Smart Group page, make changes to either the Criteria or the Devices and Users (depending upon which type the smart group was saved with) and then select Next.

4. In the View Smart Group Assignments page you can review which profiles, apps, books, provisions and policies may be added or removed from the devices as a result.

5. Select Publish to save your smart group edits. All profiles, apps, books, provisions and policies tied to this smart group update their device assignments based on this edit.

Viewing Smart Group Assignments

As a convenience, you can confirm the specific profiles, apps, books, channels, and compliance policies that are included in (as well as excluded from) the assigned smart group by taking the following steps:

1. Navigate to the smart group listing in Groups & Settings > Groups > Assignment Groups and locate a smart group that has been assigned to at least one device.

2. In the Assignments column, select the hyperlinked number to open the View Smart Groups Assignments page. This page displays only those categories that contain Assignments or Exclusions in the smart group.

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.

- **Refresh** – re-sends a query to retrieve an up-to-date listing of assignments and exclusions.

- **Export** – produces 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.

- **Search List** – locate a specific assignment or exclusion.
Reseaching Smart Group Events Using Console Event Logger
You can track the changes to smart groups (as well as when they were made and by whom) by utilizing the Console Event logger. To produce a list of smart group-related events:

1. Navigate to Hub > Reports & Analytics > Events > Console Events.
2. Select Smart Groups from the Module drop-down filter at the top of the Console Event listing.
3. Apply additional filters as you may require including Date Range, Severity, and Category.
4. Where applicable, select the hypertext link in the Event Data column which contains additional detail that may assist your research efforts.

Deleting a Smart Group

1. Navigate to Groups & Settings > Groups > Assignment Groups and locate the smart group you want to delete from the listing.
2. Select the check box to the left of the smart group name and select Delete from the actions menu that displays.
You can only delete one smart group at a time. Selecting more than one smart group causes the Delete button to be unavailable. You cannot delete a smart group if it is currently assigned.

Unassigning a Smart Group

You can unassign a smart group from an application, book, channel, policy, profile, or product.

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, Internal or Web 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 \( \square \) 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 that you want to unassign. This action does not delete the smart group.It simply removes the smart group assignment from the saved setting.
5. Follow the required steps to Save your changes.
Chapter 9: Assignment Groups

Overview .................................................................................................................. 86
Using Assignment Groups ................................................................. 86
Overview

**Assignment Groups** is an umbrella term used to categorize certain management grouping structures within AirWatch. **Organization Groups, Smart Groups**, and **User Groups** each have full feature sets and properties and are distinct from each other.

One element they have in common is the way they can be used to easily assign content to user devices. **Assignment Groups** enables an administrator to manage these three groups from a single location.

Using Assignment Groups

You can use the Assignment Groups page to simultaneously assign multiple organization groups, smart groups, and user groups to one or more device profiles, public applications, and compliance policies.

Navigate to **Groups & Settings > Groups > Assignment Groups**.

Viewing Assignment Groups

The Assignment Groups page contains a listing for three kinds of groups that have the function of assigning content to devices: **organization groups, smart groups**, and **user groups**.

Sorting by Columns

You can sort the listing of groups by individual columns by selecting the column header.

Selecting Links in the Listing

Four columns require special mention:

- The **Groups** column features a link for each **Smart Group**. The link opens the **Edit Smart Group** page for that smart group, enabling you to make changes.
If you select the Assignments column when it contains a number other than zero, the View Smart Group Assignments page displays, even for assigned organization groups and user groups. This function allows you to view and confirm assignments to profiles, public applications, and compliance policies.

If you select the Exclusions column when it contains a number other than zero, the View Smart Group Assignments page displays, even for excluded organization groups and user groups, allowing you to view and confirm exclusions from profiles, public applications, and compliance policies.

If you select the Devices column number, the Devices > List View page displays, containing the listing of all devices in the selected organization group, smart group, or user group.

Filtering Groups
You can filter groups by Group Type (Smart Groups, Organization Groups, and User Groups) and by how or whether they have been Assigned (Assignments, Exclusions, All, and None).

Managing Assignment Groups

Adding Smart Groups
You can add a new smart group by selecting Add Smart Group which displays the Create New Smart Group page.

Assigning Multiple Groups
With Assignment Groups, you can assign multiple groups to device profiles, public applications, and compliance policies. You can also assign multiple groups of each type (organization, smart, and user) at one time.

To assign groups:

1. Navigate to Groups & Settings > Groups > Assignment Groups.
2. Select one or more groups in the listing and select Assign above the column header.

3. The Assign page displays featuring the Organization Groups, Smart Groups, and User Groups you selected.
4. Assign them by initiating a search for a Profile, a Public Application, and Compliance Policy.
5. Select Next to display the View Device Assignment page which you can use to confirm the group(s) assignment.
6. Select Save & Publish to finalize the assignment.
Chapter 10: Shared Devices

Overview ................................................................. 89
System Capabilities .................................................... 89
Supported Platforms .................................................. 89
Organizing Shared Devices ......................................... 90
Provisioning Devices for Multi-User Device Staging .......... 91
Using Shared Devices ................................................ 91
Overview

Issuing a device to every employee in certain organizations can be expensive. AirWatch MDM lets you share a mobile device among end users in two ways: using a single fixed configuration for all end users, or using a unique configuration setting for individual end users. AirWatch’s Shared Device/Multi-User Device functionality ensures that 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 the 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 such as 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. This self-containment ensures that the device’s enrollment status is never affected, and that 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 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

The following devices support shared device/multi-user device functionality:

- Android 2.3+
- iOS devices with AirWatch Agent v4.2+
- Mac OS X devices with AirWatch Agent v2.1+
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. When you first organize groups within the AirWatch Admin Console, you should recreate your corporate hierarchy, because employee permissions, device restrictions, and corporate access are often based on users' defined roles within the hierarchy.

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 using the name of your organization. This group serves as your top-level organization group. Below this top-level group you can create subgroups 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, select Save.


4. Enter the following information for the first organization group underneath the top-level organization group.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Group Name</td>
<td>Enter a name for the child organization group to be displayed within the AirWatch Admin Console. Use alphanumeric characters only. Do not use odd characters.</td>
</tr>
<tr>
<td>Group ID</td>
<td>Enter an identifier for the organization group for the end users to use during device log in. Ensure the end users who share devices receive the Group ID as it may be required for the device to log in depending on your Shared Device configuration.</td>
</tr>
<tr>
<td>Organization Group Type</td>
<td>Select the preconfigured organization group type that reflects the category for the child organization group.</td>
</tr>
<tr>
<td>Country</td>
<td>Select the country where the organization group is based.</td>
</tr>
<tr>
<td>Locale</td>
<td>Select the language classification for selected country.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Select the time zone for the organization group.</td>
</tr>
</tbody>
</table>

5. Select Save.
Provisioning Devices for Multi-User Device Staging

Similar to single-user device staging, multi-user staging (a "shared device") allows an IT administrator to provision devices to be used by more than one user.

Staging Android devices requires you to use AirWatch Launcher for authentication, and to use a launcher profile configured at the child level organization group. For more information about shared Android devices, see the Shared Devices - Setting Up Check-In/Check-Out (Android) KB article: https://support.air-watch.com/articles/9505697-Shared-Devices-Setting-Up-Check-In-Check-Out-Android-

For more information about AirWatch Launcher, see the VMware AirWatch Launcher Guide or consult the Android Platform Guide for details about Android devices, available on AirWatch Resources.

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.
Chapter 11: Device Enrollment

Overview .......................................................... 93
Required Information ............................................. 93
The Enrollment Process ........................................... 93
Additional Enrollment Workflows ............................... 94
Performing Device Staging ....................................... 94
Registering Devices .................................................. 96
Configuring Enrollment Options ................................. 100
Customizing Enrollment Messages ............................... 102
Blacklisting and Whitelisting Device Registration .......... 103
Configuring Enrollment Restrictions ........................... 104
Overview

Use the organization groups, user groups and authentication established when you set up the environment in the AirWatch Admin Console to enable users to enroll their devices. Users will now have easy and secure access to content, features and applications from their mobile devices.

Required Information

To enroll an iOS or Android device, you will 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.
- **Group ID** – The Group ID determines what Mobile Device Management (MDM) resources and features the end user will have access to upon enrollment. You should provide your end users with this Group ID, if it is needed.

For a step-by-step walkthrough of all of the enrollment options, refer to the VMware AirWatch Enrollment Processes Guide, available on AirWatch Resources.

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 VMware AirWatch Enrollment Processes Guide, available on AirWatch Resources.
- To enroll with the AirWatch Container instead of the AirWatch Agent, refer to the VMware AirWatch Container Guide, available on AirWatch Resources.

In general, enrollment through the AirWatch Agent follows this workflow:

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.
   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, you will be prompted to enter your Environment URL, Group ID and Credentials. 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.

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, end users will need the credentials detailed in the Required Information section of this guide.

Examples of other enrollment workflows include:

- **Notification-Prompt Enrollment** – The end user receives a notification (email and SMS) with the Enrollment URL, and enters their Group ID and 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** – The administrator sends an AirWatch-generated token to the user along with the enrollment link URL. The 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. It can be secured by setting expiration times.

- **Dual-Factor Authentication** – The 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 it 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 for AirWatch version 8.0 and above.

- **End User Registration** – The 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 that includes the enrollment URL and login credentials.

- **Single-User Device Staging** – The 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, because it saves the end users the time and effort of enrolling their own devices. Using this method, the admin can also configure and enroll a device and mail it directly to a user who is off-site.

- **Multi-User Device Staging** – The 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 each user logs in with unique credentials.

For a step-by-step walkthrough of the various enrollment options, refer to the VMware AirWatch Enrollment Processes Guide, available on AirWatch Resources.

Performing Device Staging

Device staging is a simple process but this method can take too long if you have thousands of devices to pre-enroll. Device staging is most useful when you have a new, smaller 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, 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 currently only supports single user device staging.

### Single-User Device Staging

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

Single-User Device Staging of the AirWatch Admin Console allows a single administrator to outfit devices for other users on their behalf, which can be particularly useful for IT administrators provisioning a fleet of devices. 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. In the **Add / Edit User** page, select the **Advanced** tab.
   a. Scroll down to the **Staging** section.
   b. Select **Enable Device Staging**.
   c. Select the staging settings that will apply to this staging user.
3. **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 can enroll the device on behalf of another user.
4. Enroll the device using one of the two following methods:
   - Enroll using 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.
5. 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.
6. Complete enrollment for either Advanced or Standard staging:
   - If you are performing Advanced staging, you are prompted to enter the username of the end-user device owner who is going to use the device. Proceed with enrollment by installing the Mobile Device Management (MDM) profile and accepting all prompts and messages.
   - If you are performing Standard staging, then when the end user completes the enrollment, they will be prompted to enter their own credentials in the login window.

The device is now staged and ready for use by the new user.
Multi-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 Provisioning Devices for Multi-User Staging section in the VMware AirWatch Mobile Device Management Guide, available on AirWatch Resources.

Registering Devices

The devices involved in your Mobile Device Management (MDM) deployment should be registered through the AirWatch Admin Console. Registering devices provides additional detail when you review device information, and provides 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. It 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 an Individual Device

To register an individual device, follow one of three navigation paths and proceed to completing the Add Device page, detailed below:

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 displayed above the header in the listing.

   OR

2. Complete the New User Account Creation process (either Basic or Directory) and select Save and Add Device at the last step. This opens the Add Device page.

   OR

3. Navigate to Devices > Lifecycle > Enrollment Status, select Add and then select Register Device. The Add Device page displays with instructions on adding a device.

In the Add Device page, complete the following fields according to your needs:

Complete the User tab:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

User Section
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Text</td>
<td>Search for a user by entering a search parameter and selecting the <strong>Search User</strong> button.</td>
</tr>
<tr>
<td><strong>Device Section</strong></td>
<td></td>
</tr>
<tr>
<td>Expected Friendly Name</td>
<td>Enter the Friendly Name of the device. This field accepts <strong>Lookup Values</strong> which you can insert by selecting the plus sign.</td>
</tr>
<tr>
<td>Organization Group</td>
<td>Select the Organization Group to which the device belongs.</td>
</tr>
<tr>
<td>Ownership</td>
<td>Select the ownership level of the device.</td>
</tr>
<tr>
<td>Platform</td>
<td>Select the platform of the device.</td>
</tr>
<tr>
<td>Show advanced device information options</td>
<td>Select this check box to display advanced device information fields, detailed below.</td>
</tr>
<tr>
<td>Model</td>
<td>Select the device model. This drop-down field's options depend upon the <strong>Platform</strong> field selection.</td>
</tr>
<tr>
<td>OS</td>
<td>Select the device operating system. This drop-down field's options depend upon the <strong>Platform</strong> field selection.</td>
</tr>
<tr>
<td>UDID</td>
<td>Enter the device's unique device identifier.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Enter the serial number of the device.</td>
</tr>
<tr>
<td>IMEI</td>
<td>Enter the device's international mobile station equipment identity number.</td>
</tr>
<tr>
<td>SIM</td>
<td>Enter the subscriber identity module for the device.</td>
</tr>
<tr>
<td>Asset Number</td>
<td>Enter the device's asset number</td>
</tr>
<tr>
<td><strong>Messaging Section</strong></td>
<td></td>
</tr>
<tr>
<td>Message Type</td>
<td>The type of notification sent to the user once the device is added. Choose from <strong>None</strong>, <strong>Email</strong>, or <strong>SMS</strong>. The Email option requires a valid email address. You must also choose an Email Message Template. The SMS option requires a phone number including country code and area code. SMS charges may apply. You must also choose an SMS Message Template.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Required for the Email Message Type.</td>
</tr>
<tr>
<td>Email Message Template</td>
<td>Required for the Email Message Type. Choose a template from the drop-down listing. View the Email message with the <strong>Message Preview</strong> button.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>Required for the SMS Message Type.</td>
</tr>
<tr>
<td>SMS Message Template</td>
<td>Required for the SMS Message Type. Choose a template from the drop-down listing. View the SMS message with the <strong>Message Preview</strong> button.</td>
</tr>
</tbody>
</table>

Complete the **Custom Attributes** tab (optional):
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add button</td>
<td>Select this button to add a new custom Attribute and its corresponding Value. For more information about custom attributes, see the VMware AirWatch Product Provisioning and Staging Guide, available on AirWatch Resources.</td>
</tr>
<tr>
<td>Attributes</td>
<td>Select the custom attribute from the drop-down list.</td>
</tr>
<tr>
<td>Value</td>
<td>Select the value of the custom attribute from the drop-down list.</td>
</tr>
</tbody>
</table>

Complete the Tags tab (optional):

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add button</td>
<td>Select this button to add a Tag to the device. For information about device Tags, see the VMware AirWatch Mobile Device Management Guide, available on AirWatch Resources.</td>
</tr>
<tr>
<td>Tag</td>
<td>Select the Tag from the drop-down list of existing Tags.</td>
</tr>
</tbody>
</table>

Select Save to complete the device registration process.

**Missing Device Identifiers During Registration**

If no device identifier is specified during registration (such as UDID, IMEI, and Serial Number), AirWatch uses these attributes to automatically match an enrolled device to its registration record, in the following ranking:

1. User to whom the device is registered
2. Platform (if specified)
3. Model (if specified)
4. Ownership type (if specified)
5. Date of the oldest-matching registration record

**Register a List of Devices**

To register multiple devices, perform the following steps:

1. Navigate to Accounts > Users > List View or Devices > Lifecycle > Enrollment Status.
   a. Select Add and then Batch Import to open the Batch Import form.
2. Complete each of the required fields: Batch Name, Batch Description, and Batch Type.
3. Select the information icon (i) located next to the Batch File (.csv) field to access the User and Device Import help page featuring .csv templates and a description of each.
4. Select the appropriate Download Template and Example for this Batch Type and save the comma-separated values (.csv) file to somewhere accessible.
5. Locate the saved .csv file, open it, and enter all the relevant information for each of the devices that you want to import. The template is pre-populated with three sample entries demonstrating the type of information intended to
be placed in each column.

**Important**: Enter all data containing only numerical values in double quotation marks (for example, "123456") to avoid having the values truncated. Truncated data in the .csv file may result in devices being blacklisted by VMware AirWatch MDM.

- 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 info, make sure that **column AF (Store Advanced Device Info)** is set to **Yes**.

6. Save the completed template as a .csv file. In the AirWatch Admin Console, select **Choose File** from the **Batch Import** form, navigate to the path where you saved the completed .csv file and select it.

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

### End User Device Registration

You may prefer to have end users register their own device prior to enrolling into AirWatch. This may be preferable if you are unsure of the device details during setup, or if a bring your own device (BYOD) deployment is in effect and the end users opt-in various devices. In the case of end user device registration, you will need to notify your end users by:

- 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**.

- Creating user accounts that allow all of the end users to register their devices, and then sending User account activation messages to each user containing the registration instructions.

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](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 steps to register their device(s):

1. Navigate to the Self-Service Portal (SSP) URL: [https://<AirWatchEnvironment>/MyDevice](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 Enrollment Status page by navigating to Devices > Lifecycle > Enrollment Status.

Configuring Enrollment Options

Customize your enrollment workflow by incorporating advanced options available in the AirWatch Admin Console. Navigate to Devices > Device Settings > Devices & Users > General > Enrollment to access additional enrollment options.

The VMware AirWatch Enrollment Processes Guide, available on 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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ID Assignment Mode</td>
<td></td>
</tr>
<tr>
<td>Default</td>
<td>Select this option if users will be provided with Group IDs for enrollment. The Group ID used determines what organization group the user is assigned to.</td>
</tr>
<tr>
<td>Prompt User to Select Group ID</td>
<td>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.</td>
</tr>
<tr>
<td>Automatically Select Based on User Group</td>
<td>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.</td>
</tr>
</tbody>
</table>
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

On the Optional Prompt tab, you may decide to request additional device information, or to present optional messages regarding enrollment and MDM information to the end user. Choose one or more prompts from the provided list:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prompt for Device Ownership Type</td>
<td>Select to prompt the end user to select their device ownership type. Otherwise, configure a default device ownership type for the current organization group.</td>
</tr>
<tr>
<td>Display Welcome Message</td>
<td>Select to display a welcome message for your users early in the device enrollment process. You may configure both the header and the body of this welcome message by navigating to System &gt; Localization &gt; Localization Editor and selecting the labels 'EnrollmentWelcomeMessageHeader' and 'EnrollmentWelcomeMessageBody' respectively.</td>
</tr>
<tr>
<td>Display MDM Installation Message</td>
<td>Select to display a message for your users during the device enrollment process. You may configure both the header and the body of this MDM installation message by navigating to System &gt; Localization &gt; Localization Editor and selecting the labels 'EnrollmentMdmInstallationMessageHeader' and 'EnrollmentMdmInstallationMessageBody' respectively. If you choose to customize your own header and body messages using the Localization Editor, be sure to opt for 'Override' in the Current Setting field. Doing so will ensure that your customizations are used instead of the default messages.</td>
</tr>
<tr>
<td>Enable Enrollment Email Prompt</td>
<td>Enable to prompt the user to enter their email credentials during enrollment.</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Enable Device Asset Number Prompt</td>
<td>Enable to prompt the user to enter the device asset number during enrollment.</td>
</tr>
</tbody>
</table>
### Customization Options

You can 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. For iOS devices, you can 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 leading to additional resources.

### Customizing Enrollment Messages

You can customize the messages related to device enrollment and any future Mobile Device Management (MDM) prompts that are sent to a device. Customizing MDM messages reduces confusion among your users because they show 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** and 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 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. Select the **Default** check box if you would like the template to be the default template for the chosen **Category**.

6. Choose the **Message Type** for the template. The options are **Email**, **SMS**, and **Push** notification.

7. Compose your message(s) by entering text to the **Message Body** field(s).
   
   You have two methods with which to compose 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.

8. Save your template by selecting the **Save** button.

---

**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 can 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 does 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. Blacklisting a device unenrolls the device, removes all MDM profiles, and prevents enrollment until you remove the blacklist.

To blacklist or whitelist a device:

1. Navigate to **Devices > Lifecycle > Enrollment Status** and select **Add**.

2. Choose either **Blacklisted Devices** or **Whitelisted Devices** from the **Add** drop-down list.

3. In the form, enter the list of **Device Attributes** (up to 30 at a time) and select the corresponding device attribute type, such as IMEI, Serial Number, or UDID.

4. Confirm which organization group the devices are blacklisted from or whitelisted to:
   
   - If you chose to blacklist, then select the **Additional Information** check box to attribute a **Platform** type to the list of devices and block them by platform as well.
   
   - If you chose to whitelist, choose **Ownership** from the drop-down menu to allow devices only with the chosen ownership.

5. Select **Save** to confirm the settings.
Configuring Enrollment Restrictions

You can set up enrollment restrictions to control which users can enroll and which device types are allowed. 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 are users that already exist in the AirWatch Admin Console. Configured groups are users associated to directory service groups if you choose 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.

For information about integrating your directory services groups with AirWatch, refer to the VMware AirWatch Directory Services Guide document, available on AirWatch Resources.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrict Enrollment to Known Users</td>
<td>Enable to restrict enrollment only to users that already exist in the AirWatch Admin Console. This applies to directory users you manually added to the AirWatch Admin Console one by one or through batch import. It can also be used to lock down enrollment after an initial deployment that allowed anyone to enroll. This enables you to selectively allow users to enroll. Disable this option to allow all directory users who do not already exist in the Admin Console to enroll into AirWatch. AirWatch user accounts are automatically created during enrollment.</td>
</tr>
<tr>
<td>Restrict Enrollment to Configured Groups</td>
<td>Enable 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 services user groups. Disable this option 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). One option for integrating with user groups is to create an &quot;MDM Approved&quot; directory service group, import it to AirWatch, then add existing directory service user groups to the &quot;MDM Approved&quot; group as they become eligible for AirWatch MDM.</td>
</tr>
</tbody>
</table>

Note: For iOS devices enrolled through Apple's Device Enrollment Program (DEP), enrollment restrictions do not apply. This is because device information such as OS version, device model, etc. is only received after the device has been enrolled through DEP.

Policy Settings

Save your enrollment restrictions as a policy:

1. Navigate to Devices > Device Settings > Devices & Users > General > Enrollment.
2. Select the Restrictions tab and then select Add Policy located in the Policy Settings section. The Add/Edit
Enrollment Restriction Policy screen displays.

3. Add a new enrollment restriction policy:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrollment Restriction Policy Name</td>
<td>Enter a name for your enrollment restriction policy.</td>
</tr>
<tr>
<td>Organization Group</td>
<td>Choose an organization group from the drop-down field. This is the OG to which your new enrollment restriction policy will apply.</td>
</tr>
<tr>
<td>Policy Type</td>
<td>Select the type of enrollment restriction policy, which can be either Organization Group Default to apply to the selected organization group, or User Group Policy for specific User Groups through Group Assignment Settings on the Restrictions tab.</td>
</tr>
<tr>
<td>Allowed Ownership Types</td>
<td>Choose whether you will permit or prevent Corporate - Dedicated, Corporate - Shared, and Employee Owned devices.</td>
</tr>
<tr>
<td>Allowed Enrollment Types</td>
<td>Choose whether you will permit or prevent the enrollment of devices using MDM (AirWatch Agent) and AirWatch Container (for iOS/Android) apps.</td>
</tr>
<tr>
<td>Device Limit</td>
<td>Select Unlimited to allow users to enroll as many devices as they want. Leave this box unchecked to enter values for the Device Limit Per User section, to define the maximum number of devices per ownership type:</td>
</tr>
<tr>
<td></td>
<td>- Maximum Devices Per User</td>
</tr>
<tr>
<td></td>
<td>- Corporate Max Devices</td>
</tr>
<tr>
<td></td>
<td>- Shared Max Devices</td>
</tr>
<tr>
<td></td>
<td>- Employee Owned Max Devices</td>
</tr>
<tr>
<td>Allowed Device Types</td>
<td>Select the Limit enrollment to specific platforms, models or operating systems checkbox to add additional device-specific restrictions.</td>
</tr>
<tr>
<td></td>
<td>Determine what kind of device limitations you should have by selecting the Device Level Restrictions Mode. Your choices are:</td>
</tr>
<tr>
<td></td>
<td>- Only allow listed device types (Whitelist) – Select this option to explicitly allow only devices matching the parameters you enter and to block everything else.</td>
</tr>
<tr>
<td></td>
<td>- Block listed device types (Blacklist) – Select this option to explicitly block devices matching the parameters you enter and to allow everything else.</td>
</tr>
<tr>
<td></td>
<td>For either device-level restrictions mode, select Add Device Restriction to choose a Platform, Model, Manufacturer (specific to Android devices), Operating System, or Enterprise Version. You may also add a Device Limit per defined device restriction. You may add multiple device restrictions.</td>
</tr>
<tr>
<td></td>
<td>You can also block specific devices based on their IMEI, Serial Number or UDID by navigating to Devices &gt; Lifecycle &gt; 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.</td>
</tr>
</tbody>
</table>

4. 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.
Chapter 12: Device Profiles

Overview ................................................................. 107
Configuring General Profile Settings ...................... 107
Managing Device Profiles .......................................... 109
Editing Device Profiles ............................................. 113
View Device Assignment ........................................... 114
Compliance Profiles ................................................ 115
Geofences .............................................................. 115
Time Schedules ....................................................... 117
Overview

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 then configure a payload, which consists of the individual settings you configure (passcodes, Wi-Fi, restrictions or Virtual Private Networks (VPN)) for each platform type.

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

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.

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 steps and settings below apply to any profile:

1. Navigate to Devices > Profiles > List View > Add and select Add Profile.
2. Select the appropriate platform for the profile you want to deploy. Depending on the platform you select, the payload settings vary.
3. Complete the General tab by completing the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the profile to be displayed in the AirWatch Admin Console.</td>
</tr>
<tr>
<td>Version</td>
<td>Read-only field that reports the current version of the profile as determined by the Add Version.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the profile that indicates its purpose.</td>
</tr>
<tr>
<td>Deployment</td>
<td>Determines if the profile is automatically removed upon unenrollment (does not apply to Android for Work profiles).</td>
</tr>
<tr>
<td></td>
<td>• Managed – The profile is removed.</td>
</tr>
<tr>
<td></td>
<td>• Manual – The profile remains installed until removed by the end user.</td>
</tr>
</tbody>
</table>
## Setting | Description
--- | ---
**Assignment Type** | Determines how the profile is deployed to devices:
- **Auto** – The profile is deployed to all devices automatically.
- **Optional** – An end user can optionally install the profile from the Self-Service Portal (SSP), or it can be deployed to individual devices at the administrator's discretion.

End users can also install profiles representing Web applications, using a Web Clip or a Bookmark payload, from the App Catalog if you configure the payload to show in the App Catalog.
- **Interactive** – *(Does not apply to iOS or Android for Work)* 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 is only available if enabled in **Groups & Settings > All Settings > Devices & Users > Advanced > Profile Options**.
- **Compliance** – Compliance profiles are created and saved in the same manner as Auto and Optional device profiles, by navigating to **Devices > Profiles > List View** and then selecting **Add** and then **Add Profile**. However, compliance profiles are only applied in the **Actions** tab of the **Adding Compliance Policy** page to be used when an end user violates a compliance policy. Select **Install Compliance Profile** from the drop-down and then select the previously-saved compliance profile.

**Allow Removal** | 
- **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 an account **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 Groups** | Refers to 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. See the **VMware AirWatch Mobile Device Management Guide**, available on **AirWatch Resources**, for additional information.

While Platform is a criterion within a smart group, the platform configured in the device profile or compliance policy always takes precedence over the smart group's platform. For instance, if a device profile is created for the iOS platform, the profile is only assigned to iOS devices even if the smart group includes Android devices.

**Exclusions** | If **Yes** is selected, a new field **Excluded Smart Groups** displays which enables you to select those smart groups you want to exclude from the assignment of this device profile. See **Excluding Smart Groups in Profiles and Compliance Policies** for details.
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.

These check boxes enable additional restrictions for the profile.

- **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**.

  For more information on Time Schedules, please see [Time Schedules](#) and the Mobile Device Management (MDM) Guide, available on [AirWatch Resources](#).

The date when the profile will be removed from the device. Must be a future date formatted as MM/DD/YYYY.

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

   For step-by-step instructions on configuring a specific **Payload** for a particular platform, please refer to the applicable **Platform Guide**, available on [AirWatch Resources](#).

5. Select **Save & Publish**.

**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 organize and take actions on profiles.
Filters – View only the desired profiles by utilizing the following filters:

- Status
- Platform
- Smart Group

Add

- Add Profile – Perform a one-off addition of a new device profile.
- Upload Profile – Upload a signed profile on your device.
- Batch Import – Import new device profiles in bulk by using a comma-separated values (.csv) file. Enter a unique name and description to group and organize multiple profiles at a time.

Layout button enables you to fully customize the column layout of the listing.

- Summary – View the List View with the default columns and view settings.
- Custom – Select only the columns in the List View you want to see. You also have the option to apply selected columns to all administrators at or below the current organization group.
- **Export** button (-export-) - Save a .csv file (comma-separated values) of the entire **List View** that can be viewed and analyzed in Excel. If you have a filter applied to the **List View**, the exported listing will also abide by the filter.

- The **Installed Status** column displays the current status of a profile’s installation by displaying three icon indicators, each with a hypertext number link. Selecting this link displays the **View Devices** page, which is a listing of affected devices in the selected category:
  - **Installed (✓)** – This indicator displays the number of devices on which the profile is assigned and successfully installed.
  - **Not Installed (☐)** – This indicator displays the number of devices to which the profile is assigned but not installed.
  - **Assigned (👤)** – This indicator displays the total number of assigned profiles whether they are installed or not.

### Selecting a Profile and Performing Actions

The **List View** features a selection radio button and **Edit** icon, each to the left of the profile. Selecting the **Edit** icon (-edit-) enables you to make basic changes to the profile configuration. Selecting a single radio button causes the **Devices** button, the **XML** button, and **More** button to appear above the listing, enabling you to take the following actions:

- **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.

- **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.

### Manage (listed under the More button)

- **Copy** – Make a copy of an existing profile and tweak the configuration of the copy to quickly get started with device profiles.

- **Activate/Deactivate** – Toggle between making a device profile active and inactive.

- **Delete** – Delete a profile and remove it from all devices. Maintain your roster of profiles by removing unnecessary profiles.

### Hover-Over Pop-up

Each device profile in the **Profile Details** column features a tool tip 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 profile information such as **Profile Name**, the profile's effective **Platform**, and the included payload **Type(s)**.
A similar tooltip icon is found in the Assigned Groups column in the Profiles List view, featuring Hover-Over Pop-ups displaying Assigned Smart Groups and Deployment Type.

Profile Icons

In both the Summary and Custom views in the Profile Listing, each profile features an icon representing the payload Type.

- Single payload types feature a unique icon for that individual payload type.
- Profiles featuring multiple payloads of the same type feature a number badge in the upper-right corner of the icon.
- Profiles featuring multiple payloads of differing types feature a generic icon with a number badge.

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 number links to the right of the Installed Status column to open the View Devices screen.

💡 If your profile is not reaching intended devices, refer to the following VMware AirWatch Knowledge Base article for some troubleshooting tips: https://support.air-watch.com/articles/21743331-Troubleshooting-Profiles.
The **Command Status** column visible from the **View Devices** screen includes the following installation statuses as they relate to the selected device:

- **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 type is unmanaged.
- **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.

**Note:** The **Command Status** column is functional only for iOS devices.

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 by selecting the **Export** icon (🔗). Additionally, you can customize which columns in the **View Devices** page you want to be visible by selecting the **Available Columns** icon ( resizeMode ).

**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 ( ![Edit icon](image)) from the actions menu of the profile you want to edit.
   
   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.

   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 on [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.

<table>
<thead>
<tr>
<th>Assignment Status</th>
<th>Friendly Name</th>
<th>User</th>
<th>Platform / OS / Model</th>
<th>Phone Number</th>
<th>Organization Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changed</td>
<td>nedie</td>
<td>nedie</td>
<td>Apple / iOS 7.0.4 / iPhone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Updated</td>
<td>nedie</td>
<td>nedie</td>
<td>Apple / iOS 7.0.4 / iPhone</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

**Compliance Profiles**

Compliance profiles are created and saved in the same manner as Auto and Optional device profiles, by navigating to **Devices > Profiles > List View** and then selecting **Add** and then **Add Profile**. However, compliance profiles are only applied in the **Actions** tab of the **Adding Compliance Policy** page to be used when an end user violates a compliance policy. Select **Install Compliance Profile** from the drop-down and then select the previously-saved compliance 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, and AirWatch apps such as the AirWatch Content Locker, and more.

Geofencing is available for Android and iOS devices.

**Supported iOS Devices**

Geofencing for apps only works on iOS devices that have **Location Services** running. In order for location services to 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.

For Wi-Fi only devices, GPS data is reported when the device is on, unlocked, and the agent is open and being used. For cellular devices, GPS data will be reported when the device changes cell towers. AirWatch Browser and Content Locker will report GPS data when the end-user opens and uses them.

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

<table>
<thead>
<tr>
<th>Device</th>
<th>Wi-Fi</th>
<th>Cellular Network</th>
<th>Built-In GPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>iPad Wi-Fi + 3G/4G</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>iPad Wi-Fi</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPod Touch</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following requirements must all be met for the GPS location to be updated:
- The device must have the AirWatch MDM Agent running.
- Privacy settings need to allow GPS location data to be collected (Groups & Settings > All Settings > Devices & Users > General > Privacy).
- The Apple iOS Agent settings must enable “Collect Location Data” (Groups & Settings > All Settings > Devices & Users > Apple > Apple iOS > Agent Settings).
  AirWatch recommends that you set the Agent SDK settings to either Default SDK settings or any other SDK settings instead of "None."

Using iBeacons

iBeacon is specific to iOS and is used to manage location awareness. For more information, please see the VMware AirWatch iOS Platform Guide, available on AirWatch Resources.

💡 For more information about how AirWatch tracks GPS location, see the following VMware AirWatch Knowledge Base article: https://support.air-watch.com/articles/95795857-GPS-Tracking-Overview.

Enabling a Geofence is a two-step process:

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

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 > Areas to access the Area settings page. Select Add followed by Geofencing Area.
2. Enter an Address and the Radius of the geofence in kilometers or miles. 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 you want to apply the geofence.

**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 select 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 platform.

2. Select Install only on devices inside selected areas on the General tab. An Assigned Geofence Areas 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.

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.

3. In the **Assigned Schedules** box, enter one or more 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**.
Chapter 13: Compliance

Compliance Overview ................................................... 120
Navigating Compliance Policies List View ....................... 121
Compliance Policies by Platform .................................. 123
Adding a Compliance Policy ........................................... 125
Compliance Overview

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. For certain platforms, 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 determined to be out of compliance, the compliance engine warns users to address detected compliance errors to prevent disciplinary action on the device. For example, the compliance engine can trigger a message to notify the user that their device is out of compliance. If the errors are not corrected in the amount of time specified, the device loses access to certain content and functions that you define. The available compliance policies and actions vary by platform.

You may even automate the escalation process if corrections are not made; locking down the device and notifying 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.

There are two methods by which compliance is measured:

- **Real Time Compliance (RTC)** – Unscheduled samples received from the device are used to determine whether or not the device is compliant. The samples are requested on demand by the admin.

- **Engine Compliance** – The compliance of a device is primarily determined by the running of the compliance engine, a software algorithm that receives and measures scheduled samples. The time intervals for the running of the scheduler are defined in the console by the admin.

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.
Navigating Compliance Policies List View

The Compliance Policies List View enables you to see all the active and inactive compliance policies and their configurations. Devices are placed in a Pending compliance status during initial enrollment. Creating, saving, and assigning a policy to an enrolled device causes the device's compliance status to either be Compliant or NonCompliant. Similarly, changes to Smart Group assignments will only cause a device's compliance policy to be Pending when the device is new to the smart group. Devices already assigned to the smart group cannot see their compliance status change simply because the smart group expands (or contracts) its assignment.

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 digits in the column titled Compliant / NonCompliant / Pending / Assigned features hypertext links that, when selected, display the View Devices page for the specific status on the selected compliance policy.

For example, if you select the first hyperlink text digit of a compliance policy in the list view, the View Devices page displays featuring all the Compliant devices which have that policy assigned. The second digit displays the Noncompliant devices, the third digit is for devices whose compliance is Pending, and the fourth digit displays devices which have recently been Assigned the compliance policy.

The Assigned status is the sum of Compliant, NonCompliant, and Pending devices.

View Devices

The View Devices page is used to view the current compliance status for each device. Select the Status drop-down field to filter the listing among the four statuses with Assigned being the sum of Compliant, Non-Compliant, and Pending statuses.
There are three listed device statuses in the **Status** column:

- **Compliant** – The assigned compliance policy has determined that the device is compliant.
- **Non-Compliant** – The assigned compliance policy has determined that the device is non-compliant.
- **Pending** – The compliance policy is scheduled to be assigned to the newly-enrolled device.

You can also confirm the C/E/S (Ownership) of the device, the **Platform/OS/Model**, **Organization Group**, **Last Compliance Check**, **Next Compliance Check**, and **Actions Taken** which lists the actions that have been taken to address non-compliant devices.

You may also choose to re-evaluate the compliance for a specific device. Select **Re-Evaluate Compliance** to engage the compliance engine and re-report compliance status on the device.
Compliance Policies by Platform

The supported compliance policies by platform are as follows.

<table>
<thead>
<tr>
<th>Compliance Policy</th>
<th>Android</th>
<th>Apple iOS</th>
<th>Apple Mac OS X</th>
<th>Chrome OS</th>
<th>QNX</th>
<th>Windows Rugged</th>
<th>Windows 7</th>
<th>Windows Phone</th>
<th>Windows Desktop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application List</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antivirus Status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cell Data Usage</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cell Message Usage</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cell Voice Usage</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compromised Status</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Last Seen</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Device Manufacturer</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall Status</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Free Disk Space</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iBeacon</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interactive Certificate Profile Expiry</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Compromised Scan</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDM Terms of Use Acceptance</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Model</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS Version</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passcode</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roaming</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roaming Cell Data Usage</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIM Card Change</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Automatic Update Status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Copy Genuine Validation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
### Compliance Policies Descriptions

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application List</td>
<td>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.</td>
</tr>
<tr>
<td>Antivirus Status</td>
<td>Detect whether or not an antivirus program is running.</td>
</tr>
<tr>
<td>Cell Data/Message/Voice Usage</td>
<td>Detect when end users' devices exceed a particular threshold of their assigned telecom plan. For this policy to take effect Telecom must be configured. For more information, see the <a href="https://support.airwatch.com/articles/93879147-Compromised-Device-Overview">VMware AirWatch Telecom Guide</a>, available on <a href="https://support.airwatch.com/articles/25606467-Best-Practices-for-Compromised-Device-Detection">AirWatch Resources</a>.</td>
</tr>
<tr>
<td>Compromised Status</td>
<td>Detect if the device is compromised. Prohibit the use of jailbroken or rooted devices that are enrolled with AirWatch. Jailbroken and rooted 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.</td>
</tr>
<tr>
<td>Device Last Seen</td>
<td>Detect if the device fails to check in within an allotted time window.</td>
</tr>
<tr>
<td>Device Manufacturer</td>
<td>Detect the device manufacturer allowing you to identify certain Android devices. You can either specifically prohibit certain manufacturers or specifically permit only the manufacturers you specify.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Detect whether or not encryption is enabled on the device.</td>
</tr>
<tr>
<td>Firewall Status</td>
<td>Detect whether or not a firewall program is running.</td>
</tr>
<tr>
<td>Free Disk Space</td>
<td>Detect the available storage space on the device.</td>
</tr>
<tr>
<td>iBeacon Area</td>
<td>Detect whether your iOS device is within the area of an iBeacon Group. See &quot;Configuring iBeacon&quot; in the <a href="https://support.airwatch.com/articles/25606467-Best-Practices-for-Compromised-Device-Detection">VMware AirWatch Apple iOS Platform Guide</a>, available in <a href="https://support.airwatch.com/articles/25606467-Best-Practices-for-Compromised-Device-Detection">AirWatch Resources</a>.</td>
</tr>
<tr>
<td>Interactive Profile Expiry</td>
<td>Detect when an installed profile on the device expires within the specified length of time.</td>
</tr>
<tr>
<td>Last Compromised Scan</td>
<td>Detect if the device has not reported its compromised status within the specified schedule.</td>
</tr>
<tr>
<td>MDM Terms of Use Acceptance</td>
<td>Detect if the end user has not accepted the current MDM Terms of Use within a specified length of time.</td>
</tr>
<tr>
<td>Model</td>
<td>Detect the device model. You can either specifically prohibit certain models or specifically permit only the models you specify.</td>
</tr>
</tbody>
</table>
### Setting | Description
--- | ---
OS Version | Detect the device OS version. You can prohibit certain OS versions or permit only the operating systems and versions you specify.
Passcode | Detect whether a passcode is present on the device.
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 SIM card has been replaced.
Windows Automatic Update Status | Detect whether Windows Automatic Update has been activated.
Windows Copy Genuine Validation | Detect whether the copy of Windows currently running on the device is genuine.

For details about compliance policies, including how to create one, please see the VMware AirWatch Mobile Device Management Guide, available on AirWatch Resources.

### Adding a Compliance Policy

Adding a compliance policy is a process comprising four segments: Rules, Actions, Assignment, and Summary. Not all features and options presented in this guide are available for all platforms. The AirWatch Admin Console bases all available options on the initial platform choice, so the console never presents an option that your device cannot use.

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

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** page on which to base your compliance policy.
3. Configure the **Rules** tab by first selecting to match **Any** or **All** of the rules to detect conditions.

- **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.
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.

Select the options and types of actions to perform:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Mark as Not Compliant check box** | Enables you to perform actions on a device without marking it as non-compliant. The compliance engine accomplishes this by observing the following rules:  
  - The Mark as Not Compliant check box 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 this check box 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 check box enabled (checked). Only then will the device be non-compliant. |
| **Application**       | Block or remove a managed application.  
  You can enforce application compliance 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 VMware AirWatch MAM Guide, available on AirWatch Resources. |
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Initiate a device check-in or execute an enterprise wipe.</td>
</tr>
<tr>
<td>Email</td>
<td>Block the user from being able to use email.</td>
</tr>
<tr>
<td></td>
<td>The 'Block Email' action applies if you are using Mobile Email Management</td>
</tr>
<tr>
<td></td>
<td>together with the Email compliance engine, which is accessed by navigating</td>
</tr>
<tr>
<td></td>
<td>to Email &gt; Compliance Policies &gt; Email Policies. This lets you use Device</td>
</tr>
<tr>
<td></td>
<td>Compliance policies such as blacklisted apps in conjunction with any Email</td>
</tr>
<tr>
<td></td>
<td>compliance engine policies you configure. With this Action selected,</td>
</tr>
<tr>
<td></td>
<td>email compliance is triggered with a single device policy update if the</td>
</tr>
<tr>
<td></td>
<td>device falls out of compliance.</td>
</tr>
<tr>
<td>Notify</td>
<td>Send an email, SMS or push notification to the device or administrator.</td>
</tr>
<tr>
<td></td>
<td>Multiple emails may be inserted into the accompanying CC field provided</td>
</tr>
<tr>
<td></td>
<td>they are separated by commas.</td>
</tr>
<tr>
<td></td>
<td>For email-related Notify actions, there is a drop-down menu enabling you</td>
</tr>
<tr>
<td></td>
<td>to select an email template. There is also a link that, when selected,</td>
</tr>
<tr>
<td></td>
<td>displays the Message Template page in a new window, enabling you to</td>
</tr>
<tr>
<td></td>
<td>customize your own message template. Enable this drop-down menu by</td>
</tr>
<tr>
<td></td>
<td>deselected the check box to the right of the CC: field.</td>
</tr>
<tr>
<td>Profile</td>
<td>Install, Remove or Block a specific Device Profile, Device Profile type, or</td>
</tr>
<tr>
<td></td>
<td>Compliance Profile. Compliance profiles are created and saved in the same</td>
</tr>
<tr>
<td></td>
<td>manner as Auto and Optional device profiles, by navigating to Devices &gt;</td>
</tr>
<tr>
<td></td>
<td>Profiles &gt; List View and then selecting Add and then Add Profile. However,</td>
</tr>
<tr>
<td></td>
<td>compliance profiles are only applied in the Actions tab of the Adding</td>
</tr>
<tr>
<td></td>
<td>Compliance Policy page to be used when an end user violates a compliance</td>
</tr>
<tr>
<td></td>
<td>policy. Select Install Compliance Profile from the drop-down and then select</td>
</tr>
<tr>
<td></td>
<td>the previously-saved compliance profile.</td>
</tr>
<tr>
<td></td>
<td><strong>Escalations Only</strong></td>
</tr>
<tr>
<td>Add Escalation</td>
<td>Creates a new escalation. When adding escalations, it is a best practice</td>
</tr>
<tr>
<td>button</td>
<td>to increase the security of actions with each additional escalation.</td>
</tr>
<tr>
<td>After time</td>
<td>You may delay the escalation by minutes, hours or days.</td>
</tr>
<tr>
<td>Interval...</td>
<td></td>
</tr>
<tr>
<td>...Perform the</td>
<td>Repeat – Enable this check box to repeat the escalation a selected number</td>
</tr>
<tr>
<td>following actions</td>
<td>of times before the next scheduled action begins.</td>
</tr>
</tbody>
</table>

For Mac OS X, you can only perform the following actions:

- Device Wipe
- Enterprise Wipe
- Send Email to User
- Send Push Notification to Device
- Send Email to Administrator
- Block/Remove Profile
- Block/Remove Profile Type
- Block/Remove All Profiles

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed By</td>
<td>Select the organization group by which this compliance policy will be managed.</td>
</tr>
<tr>
<td>Assigned Smart Groups</td>
<td>Select one or more smart groups to assign to this policy.</td>
</tr>
<tr>
<td>Exclusions</td>
<td>Decide if you want to exclude any smart groups by selecting Yes in this field and select from the available listing of smart groups to exclude in the Excluded Smart Groups field that displays. See Excluding Smart Groups in Compliance Policies for details.</td>
</tr>
<tr>
<td>View Device Assignment button</td>
<td>Select this button to see a listing of devices affected by this compliance policy assignment.</td>
</tr>
</tbody>
</table>

While Platform is a criterion within a smart group, the platform configured in the device profile or compliance policy always takes precedence over the smart group’s platform. For instance, if a device profile is created for the iOS platform, the profile is only assigned to iOS devices even if the smart group includes Android devices.

6. After you determine the Assignment of this policy, select Next. The Summary tab displays.
• Provide a **Name** and a useful **Description** of the compliance policy.

• Select one of the following:
  
  o **Finish** – Save your compliance policy without activating it to the assigned devices.
  
  o **Finish And Activate** – Save and apply the policy to all affected devices.

**View Device Assignment**

Select **View Device Assignment** on the **Assignment** tab while configuring a compliance policy to display the **View Device Assignment** page. This page serves as a confirmation of affected (or unaffected) devices.

The **Assignment Status** column displays 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.
Chapter 14: Tags

Overview ................................................................. 131
Creating a New Tag ................................................. 131
Adding Tags .............................................................. 132
Managing Tags .......................................................... 133
Filtering Devices by Tag ............................................. 133
Tags and Smart Groups ............................................. 134
Overview

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, if a device has a defective battery or a broken bezel or screen, you can use tags to identify these devices from the AirWatch Admin Console. Another use is to identify 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, instead of device identification purposes, tags represent classes taught in an educational setting. For more information, please see the VMware AirWatch Teacher Tools Guide document, available on AirWatch Resources.

Creating a New Tag

Create a new tag in the Device List View:

1. Navigate to Devices > List View.
2. Select a device using the check box to the left of the device listing.
3. Select More and choose Add Tag from the drop-down menu. The Tag Assignment page appears (shown above).
4. Select NEW TAG.
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 and then select Add.
3. In the Add Tag page, enter the Name of the tag.
4. Select the Type of tag you would like to add, General or Device.
5. Select Save.

Adding Tags

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

Adding 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 either of the two ways to display the Send and More buttons:
   - Select the device from the listing to display the Details View.
   - Select the check box next to the device.
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 Save to apply the tag(s) to the device.

Adding Tags to Multiple Devices (Bulk Add Tags)

1. Navigate to Devices > List View.
2. Select the check box of each device you would like to tag.
3. Select More and then select Add Tag. The Tag Assignment page 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 Save to apply the tag(s) to the devices.
Managing Tags

The following sections describe the steps you need to 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. Only the tags that are part of a child organization group and the organization group currently selected are editable.
2. Make your changes to the Name and Type fields per your preferences.
3. Select Save.

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 page, where you can find all the tags currently assigned to the device.
3. Select X next to each tag you want to remove.

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

Delete a Tag

To delete an existing tag, take the following steps:

1. Navigate to Groups & Settings > All Settings > Devices & Users > Advanced > Tags.
2. Select X next to the tag you want to delete.

Filtering Devices by Tag

You can use the filter feature in the Device List View to show only devices with specific tags.

1. Navigate to Devices > List View, select Filters to display the Filters column s 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 want to display from the list of tags. Devices with unchecked tags will be filtered out of the resulting list. The Device List View immediately refreshes itself as soon as the first tag is selected.
Tags and Smart Groups

The tag feature has been integrated with smart groups, meaning 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.

Yet another example in the Teacher Tools application, where each tag represents an individual class and corresponding curriculum. 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. This prevents the device from functioning outside the museum.

For more information about the Teacher Tools application, please see the VMware AirWatch Teacher Tools Guide, available on AirWatch Resources.
Chapter 15: Managing Devices

Overview .......................................................... 136
Using the Device Dashboard ................................ 136
Using the Device List View .................................. 137
Using Device Details ........................................... 141
Using Device Actions .......................................... 144
Using the Enrollment Status Page ....................... 150
Using Lifecycle Notifications .............................. 152
Using Wipe Protection ....................................... 153
Using AirWatch Hub .......................................... 155
Overview

You can manage all of your deployment’s devices from the VMware AirWatch Dashboard. The Dashboard is a searchable, customizable view that you can use to filter and find specific devices. This makes it easier to perform administrative functions on a particular set of devices. You may also generate Reports and examine the data flow within the VMware 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.

Using the Device Dashboard

As devices are enrolled, you can view and manage them from the VMware AirWatch Device Dashboard. The Device Dashboard provides a high-level view of your entire fleet of mobile devices, and allows you to quickly drill down to individual devices and take MDM actions. You can view graphical representations of relevant device information for your fleet, such as device ownership type, compliance statistics and platform and OS breakdowns.

Select any of the available data views from the Device Dashboard to quickly access each set of devices in the List View. From the List View, you can take administrative action: send messages, lock devices, delete devices, and change groups associated with the device.

- **Security** – View the top causes of security issues in your device fleet. Selecting any of the doughnut charts displays a filtered Device List view comprised of devices affected by the selected security issue.

- **Ownership** – View the total number of devices in each ownership category. Selecting any of the bar graph segments displays a filtered Device List view comprised of devices affected by the selected ownership type.

- **Last Seen Overview/Last Seen Breakdown** – 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 display a filtered **Device List** view of only those devices, add additional filters if needed (e.g. Corporate Dedicated), and follow-up with the users accordingly.

- **Platforms** – View the total number of devices in each device platform category. Selecting any of the bar graphs displays a filtered **Device List** view comprised of devices under the selected platform.

- **Enrollment** – View the total number of devices in each enrollment category. Selecting any of the bar graph segments displays a filtered **Device List** view comprised of devices with the selected enrollment status.

- **Operating System Breakdown** – View devices in your fleet based on operating system. There are separate charts for Apple iOS, Android, Windows Phone and Windows Rugged. Selecting any of the bar graphs displays a filtered **Device List** view comprised of devices running the selected OS version.

### Using the Device List View

Select **Devices > List View** to see a full listing of all the devices in the currently-selected organization group.

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

Sort by columns and configure information filters to review device activity based on specific information. For example, sort by the **Compliance Status** column to view only devices that are currently out-of-compliance and take action on only those specific devices. Search all devices for a friendly name or user's name to isolate one device or user.

### Hover-Over Pop-up

Each device in the **General Info** column features a tool tip 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 tool tip 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.

Managing Devices in the List View

Using Filters
You can filter out entire categories of devices by using the available filters:

- Management
- Ownership
- Smart Groups
- User Groups
- Device Software (Platform, OS Version)
- 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 for specific information across all user and device fields, allowing you to search for a user name ("John Doe") or a device type.

Adding Devices
To add a new device from the List View:

1. Select the user to whom the device is assigned.

2. Specify information about the device, including Friendly Name, Ownership, Platform, and Tags.

Using Bulk Actions
Once you apply a filter to display a subset of devices, you can perform bulk actions to multiple devices by clicking the check box for those devices and selecting an action from the Action buttons.
In addition to selecting individual check boxes, you may select the entire set of filtered devices by selecting the global check box located atop the check box column.

You may also select a contiguous block of devices, even across multiple pages, by selecting the check box next to the device at the beginning of the block, holding down the shift key, then selecting the check box next to the device at the end of the block. This is similar to the block-selection in the Windows and Mac desktop environments and it allows you to apply bulk actions to the selected devices.

These actions are only available if Bulk Actions are enabled in the system settings (Groups & Settings > All Settings > System > Security > Restricted Actions). Bulk Actions require a PIN to perform.

With devices selected in the List View, the number of devices selected is displayed next to the action buttons. This number includes filtered devices that are selected as well.

Global Check Box

To make selecting large numbers of devices easy, the Global Check box, located to the left of the Last Seen column header, can be used to select or deselect all devices in the listing. If your List View contains a filtered listing of devices, the Global Check box can be used to select or deselect all filtered devices.

When the Global Check box features a green minus sign (⁻), it means at least one but not all devices are selected. Select this icon again and it changes to a check mark sign (✔), indicating that all devices in the listing (either filtered or unfiltered) have been selected. Select it a third time and it changes again to an empty check box (□), indicating that no devices in the listing are currently selected.

Queued Bulk Action Warning

Since bulk actions take time to process, if you initiate a new bulk action while the VMware AirWatch Admin Console is processing an existing bulk action, you will see a warning message:

Your previous bulk actions requested are still being processed. This request will be executed once the previous actions are complete. Do you want to continue with the current request?

Select Yes to add the new bulk action to the queue. Select No to cancel the new bulk action.

Bulk Management Limit

To ensure smooth operations when managing a large device fleet, you may set a maximum number of devices that can receive a bulk action command.

You may change Bulk Management Limits by navigating to Groups & Settings > All Settings > Devices & Users > Advanced > Bulk Management.

When a bulk management limit is in place and multiple devices are selected, a link appears next to the 'number of items selected' message which reads: Some actions disabled due to bulk limits.

Restricted Action Warning on All Devices Selected

When you initiate an action with all devices in your fleet selected, a warning message is displayed:
This warning is an acknowledgment of the diverse nature of a large device fleet featuring a multitude of different manufacturers, operating systems, and capabilities. It is unrelated to the **Bulk Management Limit** and any warnings it may generate. If you have a **Bulk Management Limit** in place, then you will not see this **Restricted Action Warning** message.

### Using Custom Layout

Select the **Layout** button and choose the **Custom** option to display the full listing of visible columns in the **Device List** view, in which you may selectively choose to display or hide Device List columns 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. Any kind of filtered Device List, no matter how many layers of filters are applied, will be reflected in the exported listing.

### 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.

To execute a search, navigate to **Devices > List View**, select the **Search List** bar and enter a username, device friendly name, or any other identifying element. This will initiate a search across all devices, using your search parameter, within the current organization group and all child groups.

### Using the Action Buttons

With the categorized devices displayed, you may take action on individual devices or initiate actions in bulk to multiple devices. To do this, select the check box next to each device and use 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 all selected devices and force users to re-enter device security PIN.

View commands that you can perform on all selected devices. See Device Actions for a full listing of platform-specific actions.

Using Device Details

Use the Device Details page to track detailed device information, and to quickly access user and device management actions. You can access Device Details 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 main page features several major sections:

- **Notification Badges** – Displays the Compromised State, Compliance Violations, Enrollment Date, and time Last Seen for the selected device.

- **Security** – Displays security settings such as which management software is being utilized, passcode status, and data protections.

- **User Info** – Displays basic user information including full name and email.

- **Device Info** – Displays device details such as organization group, location, smart groups, serial number, UDID, asset number, power status, storage capacity, physical memory, and warranty information.
- **Profiles** – Displays all profiles; installed (active), assigned (inactive), and unmanaged (sideloaded).
- **Apps** – Displays all installed apps, both automatic apps and on-demand apps.
- **Content** – Displays any installed content such as user-added documents.
- **Certifications** – Displays all installed certificates, including those near their expiration date.

**Dashboard**

The dashboard shows you basic device information: (from left to right) the device type, device model, OS version number, ownership type, device action button cluster, and Recent List indicator.

Selecting the arrow buttons in the Recent List indicator will change the selected device in the Device Details view based on its position in the filtered List View.

**Device Action Button Cluster**

Use the device action button cluster found on the Device Details dashboard to perform common device actions such as Query, Send [Message], Lock, and other actions accessed through the More button.

Available Device Actions vary by platform, device manufacturer and model, and enrollment status, as well as the specific configuration of your AirWatch Admin Console. See Device Actions for a full listing of remote actions an admin can invoke using the Admin Console.

**Menu Tabs**

You can use the Menu Tabs to access specific device information, which will vary depending on the chosen device's platform. Some of the most common tabs include:

<table>
<thead>
<tr>
<th>Menu Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Menu Tab | Description
--- | ---
**Compliance** | Display the status, policy name, date of the previous and forthcoming compliance check and the actions already taken on the device. The **Compliance** tab includes advanced troubleshooting and convenience features:
- Non-Compliant devices, as well as devices in Pending Compliance status, have troubleshooting functions available. You may re-evaluate compliance on a per-device basis ( ) or get detailed information about the compliance status on the device ( ).
- Users with Read-Only privileges can view the specific compliance policy directly from the **Compliance** tab while those with Admin access are able to make edits to the compliance policy.
**Profiles** | View all profiles currently assigned, installed, and unmanaged 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.
**More** | These additional menu tabs vary based on device platform. Some of the common ones include:
- **Network** – View current network information (Cellular, Wi-Fi, Bluetooth, IMEI) 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.
### Menu Tab | Description
--- | ---
More, cont. |  
- **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.
- **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 (All Settings > Admin > Diagnostics > Logging).
- **Troubleshooting** – View Event Log and Commands logging information. This page features export and search functions, enabling you to perform targets searches and analysis.
  - **Event Log** – View detailed debug information and server check-ins. Includes a Filter enabling you to filter by Event Group Type, Date Range, Severity, Module and Category.
    In the Event Log listing, the Event Data column may display hypertext links that, when selected, open a separate screen with even more detail surrounding the specific event. This information enables you to perform advanced troubleshooting such as determining why a profile fails to install.
  - **Commands** – View detailed listing of pending, queued, and completed commands sent to the device. Includes a Filter enabling you to filter commands by Category, Status, and specific Command.
- **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 Device Actions

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

#### Device Actions Matrix

<table>
<thead>
<tr>
<th>Action</th>
<th>Android</th>
<th>Apple iOS</th>
<th>Mac OS X</th>
<th>Apple TV</th>
<th>BlackBerry/10</th>
<th>Chrome OS</th>
<th>QNX</th>
<th>Symbian</th>
<th>Windows Rugged</th>
<th>Windows 7</th>
<th>Windows Phone</th>
<th>Windows Desktop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Tag</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>AirWatch MDM Agent (Query)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓ (*)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>App Remote View</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Apps (Query)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓ (10)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>BES Registration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓ (10)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Books (Query)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Action</td>
<td>Android</td>
<td>Apple iOS</td>
<td>Mac OS X</td>
<td>Apple TV</td>
<td>Blackberry/10</td>
<td>Chrome OS</td>
<td>QNX</td>
<td>Symbian</td>
<td>Windows Rugged</td>
<td>Windows 7</td>
<td>Windows Phone</td>
<td>Windows Desktop</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------</td>
<td>-----------</td>
<td>----------</td>
<td>----------</td>
<td>---------------</td>
<td>-----------</td>
<td>-----</td>
<td>---------</td>
<td>----------------</td>
<td>-----------</td>
<td>--------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Certificates (Query)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Change Device Passcode</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Change Organization Group</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Change Ownership</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Clear Activation Lock</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Clear Passcode (Device)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Clear Passcode (Container)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Clear Passcode (Restrictions Setting)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Clear Passcode (SSO)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Delete Device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Device Information (Query)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Device Wipe</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Edit Device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Enroll</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Enterprise Reset</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Enterprise Wipe</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>File Manager</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Find Device</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Location</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lock Device</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lock SSO</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Managed Settings</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mark Do Not Disturb</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Override Job Log Level</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Profiles (Query)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Provision Now</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Query All</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Action</td>
<td>Android</td>
<td>Apple iOS</td>
<td>Mac OS X</td>
<td>Apple TV</td>
<td>Blackberry/10</td>
<td>Chrome OS</td>
<td>QNX</td>
<td>Symbian</td>
<td>Windows Rugged</td>
<td>Windows 7</td>
<td>Windows Phone</td>
<td>Windows Desktop</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------</td>
<td>-----------</td>
<td>----------</td>
<td>----------</td>
<td>---------------</td>
<td>-----------</td>
<td>-----</td>
<td>---------</td>
<td>----------------</td>
<td>-----------</td>
<td>--------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Reboot Device</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registry Manager</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Control</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Management</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote View</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rename Device</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request Debug Log</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request Device Check-In</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restart AirWatch Agent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security (Query)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send Message</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start AirPlay</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start AWCM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stop AWCM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sync Device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task Manager</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Manifest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warm Boot</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(*) This Windows 7 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.

### Device Action Descriptions

- **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.

- **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 VMware AirWatch enrollment.

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

• **File Manager** – Launch a File Manager within the VMware AirWatch Admin Console that enables you to remotely view a device's content, add folders, conduct searches and upload files.
- **Find Device** – Send a text message to the applicable VMware AirWatch application together with an audible sound (with options to repeat the sound a configurable number of times and the length of the gap, in seconds, between sounds). This audible sound should help the user locate a misplaced device.

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

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

- **Lock SSO** – Lock the device user out of VMware AirWatch 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.

  For more information about using Do Not Disturb Mode, see the following VMware AirWatch Knowledge Base article: [https://support.air-watch.com/articles/23999487-Using-Do-Not-Disturb-Mode](https://support.air-watch.com/articles/23999487-Using-Do-Not-Disturb-Mode).

- **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 VMware 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 VMware 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.

- **Rename Device** – Change the device friendly name within the AirWatch Admin Console.
- **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 troubleshoot and provide support.

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

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

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

- **Task Manager** – Launch a Task Manager within the VMware 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 VMware 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 performing a power-on self test (POST).
Using the Enrollment Status Page

Use the **Enrollment Status** page to assess and track enrollment status information, import and register devices in bulk, whitelist and blacklist devices, and revoke and reset device tokens. Select **Devices > Lifecycle > Enrollment Status** to see a full list of all devices by enrollment status in the currently-selected organization group.

Sort by columns and configure information filters to review device activity based on specific information. For example, sort by the **Token Status** column to view only devices whose registration is currently not applicable 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.

**Using Filters**

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

- **Enrollment Status**
- **Platform**
- **User**
- **Ownership**
- **Token Status**
- **Token Type**
- **Source**
- **First Seen**

**Adding Devices**

You can add a single device to be enrolled or batch import devices in bulk. For details, see [Adding a Device](#).

**Whitelisting and Blacklisting Devices**

You can restrict enrollment to only those devices you have identified or whitelisted. 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 device from the blacklist. To learn how to whitelist or blacklist devices, see [Blacklisting and Whitelisting Devices](#).
**Using the Action Buttons**

Take action on individual devices or multiple devices by selecting the check box next to each device and using the action buttons to execute the following:

- **Resend Message** – Resend the original message sent to a user, including Self-Service Portal URL, Group ID and login credentials.

- **More**
  - **Change Organization Group** – Move the selected device(s) to the organization group of your choosing.
  - **Change Ownership** – Change the type of ownership for the selected device(s).
  - **Delete** – Permanently delete the registration information for selected devices. This forces the user to re-register in order to enroll. Where applicable, you must first revoke the token prior to deleting a device registration.
  - **Reset Token** – Reset a token’s status if it has been revoked or is expired.
  - **Revoke Token** – Force the registration token status of selected devices to expire, essentially blocking access for unwanted users or devices.

When you select an action for one or more devices, a confirmation screen displays allowing you to Save or Cancel the action. For the **Reset Token** and **Revoke Token** actions, you can choose to disable the **Notify Users** field which prevents the default email notification from being sent.

**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.

In addition to selecting individual check boxes, you may select the entire set of filtered devices by selecting the global check box located atop the check box column.

For example, you may resend the enrollment message to every Android device in your fleet by applying the Platform filter, selecting the Global check box, then selecting the **Resend Message** button.

**Using Details View**

Select a device's Friendly Name in the **General Info** column at any time to open the **Details View** for that device.

From the **Details View**, you can resend the enrollment message by selecting the **Resend Message** button. You can also edit a device's registration info by selecting the **Edit Registration** button and completing the **Advanced Device Information** section.

The **Details View** displays a series of tabs, each containing relevant enrollment information about the device:

- **Summary** – View the registration date, time elapsed since the device was first seen, basic device and user info.

- **User** – View detailed user info.

- **Message** – View the outgoing Device Activation email message including credential information and QR code. There is a resource available, called "User Registration Message," that allows the AirWatch administrator to hide the **Message** tab after the device has successfully enrolled. For more information about Admin roles and how to manage them, see the [VMware AirWatch Mobile Device Management Guide](https://www.vmware.com/products/aewd/airwatch/mobiledevicemanagementguide.html), available on [AirWatch Resources](https://www.vmware.com/products/aewd/airwatch/resources.html).
• **Custom Attributes** – View the Custom Attributes associated with the device. For more information about custom attributes, see the [VMware AirWatch Product Provisioning and Staging Guide](#), available on [AirWatch Resources](#).

• **Tags** – View the [Tags](#) currently associated with the device. For more information about Tags, see the [VMware AirWatch Mobile Device Management Guide](#), available on [AirWatch Resources](#).

### Using Custom Layout

Select the **Layout** button and choose the **Custom** option to display the full listing of visible columns in the **Enrollment Status** view, in which you may selectively choose to display or hide columns 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 **Enrollment Status** 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 Lifecycle Notifications

Lifecycle Notifications enable you to deliver 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 > Settings > Notifications** and entering the following fields for the following sections:

• **Device Enrolled Successfully** – Send an email notification when a device enrolls successfully.

• **Device Unenrolled** – Send an email notification when a device unenrolls.

• **Device Blocked by Enrollment Restriction** – Send an email notification if a device is blocked by an enrollment restriction, which can be configured by navigating to **Groups & Settings > All Settings > Devices & Users > General > Enrollment** and choosing the **Restrictions** tab.
### Setting | Description
--- | ---
Send Email To | • None – Send no confirmation email upon a successful device block, enrollment, or unenrollment.
• User – Send a confirmation email to the device user informing them of the successful device block, enrollment, or 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 block, enrollment, or unenrollment.
  ○ To – Send the same confirmation email to a single email address or multiple, comma-separated email addresses.

### Using Wipe Protection
By configuring Wipe Protection settings, you can exert more control over how and when devices can be wiped to avoid mass device wiping. To prevent this, set a wipe threshold.

A wipe 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 wipe threshold is exceeded, all future wipe commands are temporarily put on hold. You and other administrators can optionally be notified when this occurs.

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 wipe threshold counter.

### Configuring Wipe Protection Settings
Set a wipe threshold limit and amount of time in minutes during which the wipes must occur to trigger the wipe hold. You can only configure these settings at the Global or Customer level organization group.

1. Navigate to Devices > Lifecycle > Settings > Wipe Protection.
2. Configure the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wiped Devices</td>
<td>Enter the number of Wiped Devices that acts as your threshold for triggering wipe protection.</td>
</tr>
<tr>
<td>Within (minutes)</td>
<td>Enter the value for Within (minutes) which is the amount of time the wipes must occur in order to trigger wipe protection.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **Email** | 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. |
| **To** | 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. |

3. Select **Save**.

**Viewing Wipe Logs**

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 wipe threshold counter, or the time after which the number of devices wiped (device or enterprise) has exceeded a previously-defined number of devices or amount of time.

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. You may optionally **Filter** the Wipe Log by the following parameters:
   - Date Range
   - Wipe Type
   - Status
   - Source
   - Ownership

3. View the list of devices and determine whether these are valid wipes. Devices pending action will have a status of On Hold. Devices wiped before the threshold limit was reached will display as Processed.

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

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

   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.

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

   You can only perform this action at a Global or Customer level organization group.
Using AirWatch Hub

The VMware AirWatch Hub is your central portal for fast access to critical information. You can quickly identify important issues or devices and take action from a single location in the VMware 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 summary graphs and detailed views covering:

- **Devices** – View exact number of devices in terms of:
  - Status breakdown of all devices including 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 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.

You can export Hub data in .pdf format 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**. 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**

The **Active Products** section features three panels that report MDM, App Management, and Content Management licenses available as well as expiration dates. The doughnut 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 doughnut chart is 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**

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

- AirWatch **Cloud Connector**
- AirWatch **Secure Email Gateway**
- AirWatch **Tunnel**
Using Industry Templates for iOS

An Industry Template is a collection of mobile apps and device profiles that you can push to your devices, greatly expediting the deployment process. You can choose templates in support of industries such as healthcare and retail and you may edit these templates to better fit your needs.

For details about Industry Templates, please see the VMware AirWatch iOS Platform Guide, available on AirWatch Resources.

Using Reports & Analytics

AirWatch has extensive reporting and event logging 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. You can utilize several key pieces of functionality to leverage AirWatch reporting capabilities:

Generating Reports

You can create reports using the AirWatch Admin Console. To generate 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 bar click View.

Adding a Report to My Reports

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.
3. On the Actions bar click Add to My Reports.

Added reports 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 several 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.

Viewing Events

AirWatch keeps a running log of events that occur on the AirWatch Admin Portal. These logs can help you perform advanced troubleshooting tasks, such as determining the history of changes made to a smart group, researching when a specific user was added to a user group, producing a list of all devices blocked by an enrollment restriction, or capturing and viewing thread information when multi-threading has been enabled from the AirWatch server.

To access the Events page, navigate to Hub > Reports & Analytics > Events and select between Device Events and Console Events. The Device Events report logs events affecting devices, and the Console Events report logs events that are impactful to the administration of the device fleet.

Both menu items feature drop-down filters enabling you to filter events by Date Range, Severity, Category, and Module, in addition to a Search List function. The Event Data column in each menu item may display hypertext links. These links open a separate screen containing more detail about the specific event.

For more information about reports, please see the VMware AirWatch Reports and Analytics Guide, available on AirWatch Resources.
Chapter 16: Certificate Management

Overview ................................................................. 161
Managing Digital Certificates ................................. 161
Certificate Integration Resources ............................... 161
Overview

As the mobility of sensitive corporate content becomes the norm, the probability of unauthorized access and malicious threats increases. Even if you protect your corporate email, Wi-Fi, and virtual private network (VPN) using strong passwords, your infrastructure remains vulnerable to brute force, dictionary attacks, and even employee error. For much greater protection, consider implementing digital certificates for securing your corporate assets. Certificates offer a level of stability, security, and authentication with which passwords can’t compete. Mobile Certificate Management by VMware AirWatch solves this problem by ensuring security throughout a device’s lifecycle.

Managing Digital Certificates

Once issued, AirWatch enables you to manage deployed digital certificates using the Certificate List View in the AirWatch Admin Console. From here, administrators can view and sort certificates by device, authority, user, profile, issued date, org group, serial number, certificate thumbprint, renewal date, revoke reason, revoke date, expires in days, and status. Navigate to Devices > Certificates > List View.

The Certificate List View not only provides a summary of deployed certificates, it also provides the ability to immediately renew or revoke certificates individually or in bulk. Easily locate and revoke all digital certificates from a deactivated user/device or even renew/rotate all Wi-Fi authentication certs well in advance of a compliance driven expiration date.

Certificate Integration Resources

A comprehensive list of certificate management documentation is listed below, which you can find on AirWatch Resources.

- **AirWatch Certificate EOBO with ADCS via DCOM** – Explains the installation and setup of the Enrollment Agent Signing Certificate for direct integration with AirWatch using ADCS over the DCOM protocol. This setup allows AirWatch to take advantage of Microsoft’s Certificate Enroll On Behalf Of Others function.

- **AirWatch Integration with Microsoft ADCS via DCOM** – Explains the installation and setup of the Microsoft certificate authority for direct CA integration with AirWatch over the DCOM protocol. This will allow AirWatch to take advantage of digital certificates by automating the issuing, renewal, and revocation process to mobile devices.
• AirWatch Integration with Microsoft NDES via SCEP – Explains the installation and setup of the Microsoft certificate authority for direct CA integration with AirWatch over the NDES/SCEP/MSECP protocol.
• AirWatch Integration with SCEP – Provides details about using SCEP to allow you to leverage certificates as part of your AirWatch deployment.
• AirWatch Integration with RSA PKI – Explains how to integrate with RSA PKI services to issue certificates for your AirWatch MDM solution.
• AirWatch Integration with OpenTrust CMS Mobile 2.0 – Explains how to integrate with OpenTrust CMS Mobile services to issue certificates for your AirWatch MDM solution.
• AirWatch Integration with SecureAuth PKI – Explains how to integrate with SecureAuth PKI services to issue certificates for your AirWatch MDM solution.
• AirWatch Integration with Symantec MPKI – Explains how to integrate with Symantec's MPKI services to issue certificates for your AirWatch MDM solution.
• AirWatch Integration with GlobalSign – Explains how to integrate with GlobalSign's services to issue certificates for your AirWatch MDM solution.
• AirWatch Integration with JCCH – Explains how to integrate with JCCH's services to issue certificates for your AirWatch MDM solution.
• AirWatch Certificate Authentication for EAS with ADCS – Explains all of the necessary configurations to establish trust between your directory services, certificate authority, and an email server other than CAS.
• AirWatch Certificate Authentication for EAS with NDES-MSECP – Explains the configurations required for the Microsoft Exchange Client Access Server (CAS) and AirWatch in order to allow a device to connect to Microsoft Exchange ActiveSync (EAS) using a certificate for authentication.
• AirWatch Certificate Authentication for Cisco AnyConnect – Explains how to set up your Cisco ASA Firewall with AirWatch to automatically deploy and configure AnyConnect VPN with External CA Authentication.
• AirWatch Certificate Authentication for Cisco IPSec VPN – Explains how to set up your Cisco ASA Firewall and AirWatch to automatically deploy and configure IPSec VPN with External CA Authentication.
• AirWatch Certificate Authentication for EAS with SEG – Discusses how to configure your infrastructure for Kerberos Delegation to enable EAS certificate authentication with the Secure Email Gateway.
• AirWatch Certificate Authentication for EAS with SEG and TMG – Discusses two configurations – TMG to EAS server and TMG to SEG to EAS server and defines the configurations required in order to setup certificate authentication on a TMG to proxy requests to backend EAS or SEG servers.
• Securing Mobile Devices with Certificates Overview – Provides a business level introduction to the benefits of digital certificates. Learn more about why, in the mobile landscape, digital certificates do more than act as a security safeguard for internal content.
• Selecting Microsoft CA Deployment Models Overview – Provides you with an overview of the different Microsoft CA Deployment Model and helps you in selecting the right deployment model for your enterprise.
Chapter 17: Custom Attributes

Overview ................................................................. 164
Creating Custom Attributes ................................. 164
Assigning Organization Groups Using Custom Attributes ..... 165
Overview

Custom attributes enable administrators to extract particular values from a managed device and return it to the AirWatch Admin Console. You can also assign value to devices for use in functions such as rules-based product provisioning or device referencing in the AirWatch Admin Console with lookup values. These attributes allow you to take advantage of the rules generator when creating products using Product Provisioning. For more information on Product Provisioning see the following guides available on AirWatch Resources:

- Product Provisioning for Android Devices Guide
- Product Provisioning for Mac OS X Devices Guide
- Product Provisioning for QNX Devices Guides
- Product Provisioning for Windows 7 Devices Guide
- Product Provisioning for Windows Desktop Devices Guide
- Product Provisioning for Windows Rugged Devices Guide

Note: Custom attributes (and the rules generator) are only configurable and usable at Customer-level organization groups.

Custom Attributes Database

Custom attributes are stored either as XML files on the device or in the custom attribute database on the AirWatch Admin Console server. When using the database, Custom attributes are sent as samples to AirWatch periodically for asset tracking of key/value pairs. If a record in the device database is configured with 'Create Attribute' = TRUE, then the Name and Value will automatically be retrieved by the AirWatch Agent and sent with the custom attributes sample. The key/value pair will show in the Device Details page for the device in the Custom Attributes tab.

Creating Custom Attributes

1. Navigate to Devices > Custom Attributes > List View.
2. Select Add and then select Add Attribute.
3. Enter an Attribute Name.
4. Enter the optional Description of what the attribute identifies.
5. Enter the name of the Application that will gather the attribute.
6. Select Collect Value for Rule Generator to make the values of the attribute available in the drop-down menu of the rule generator.
7. Select Use in Rule Generator if you want to use the attribute in the rule generator.
8. Select Persist to prevent the removal of the custom attribute from the AirWatch Admin Console unless an Admin or an API call explicitly removes it. Otherwise, the attribute is removed as normal.
If you delete a custom attribute that reported from a device to the AirWatch Admin Console, a persisted custom attribute still remains in the AirWatch Admin Console.

Custom attribute persistence is only available to Android and Window Rugged devices.

9. Select **Use as Lookup Value** to use the custom attribute as a lookup value anywhere in the AirWatch Admin Console.
   For example, you could use custom attributes as part of a device friendly name to simplify device naming.

10. Select the **Values** tab.

11. Select **Add Value** to add values to the custom attribute and then select **Save**.

### Assigning Organization Groups Using Custom Attributes

Configure rules that control how devices are assigned to organization groups following enrollment.

You can only create one custom attribute assignment rule for each organization group you run.

To create assignment rules, follow the directions below:

1. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Advanced**.
2. Set **Enable Device Assignment Rules** to **Enabled**.
3. Set the **Type** to **Organization Group by Custom Attribute**.
4. Select **Save**.
5. Navigate to **Devices > Custom Attributes > List View > Add > Add Attribute** and create a custom attribute if you have not already done so. See [Creating Custom Attributes](#) for more information.
6. Navigate to **Devices > Custom Attributes > Custom Attributes Assignment Rules > Add Rule**.
7. Select the **Organization Group** to which the rule assigns devices.
8. Select **Add Rule** to configure the logic of the rule:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute/Application</td>
<td>This is the custom attribute with corresponding values for determining device assignment.</td>
</tr>
<tr>
<td>Operator</td>
<td>This operator compares the <strong>Attribute</strong> to the <strong>Value</strong> to determine if the device qualifies for the product. When using more than one Operator in a rule, you must include a <strong>Logical Operator</strong> between each <strong>Operator</strong>.</td>
</tr>
<tr>
<td>Value</td>
<td>This is the value of the custom attribute. All values from all applicable devices are listed here for the <strong>Attribute</strong> selected for the rule.</td>
</tr>
<tr>
<td>Add Logical Operator</td>
<td>Select to display a drop-down menu of logical operators such as AND, OR, NOT, and parentheses. Allows for more complex rules.</td>
</tr>
</tbody>
</table>

9. Select **Save** after configuring the logic of the rule.

When a device with an assigned attribute enrolls, the rule assigns the device to the configured organization group.
Chapter 18: 
Self-Service Portal

Overview ........................................................................................................167
Accessing the Self Service Portal on Devices .................................167
Using the My Devices Page of the SSP ..............................................167
Performing Actions in the SSP ..............................................................171
Self-Service Portal Actions Matrix ......................................................174
Customizing the Self Service Portal (SSP) ........................................175
Overview

The **AirWatch Self-Service Portal (SSP)** is a useful online tool used to remotely monitor and manage devices. It can help reduce the 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.

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. An SSP Web Clip or Bookmark 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, available on [AirWatch Resources](https://airwatch.com/resources).

Customizing the SSP URL

To make things even easier for your end-users, you can 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/?](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](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.

The viewable tabs and available actions may vary based on device platform. See the applicable [VMware AirWatch Platform Guide](https://airwatch.com/resources), available in [AirWatch Resources](https://airwatch.com/resources).
Choosing a Language

The Self-Service Portal automatically matches the browser's default language. However, you can 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. You may be required to enter a randomly-generated Captcha code.

Changing the Password

You may use the 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 Current 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 page. 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. Those statuses include Discovered, Enrolled, Pending Enrollment, Unenrolled, and Enterprise Wipe Pending.
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 as applicable.

3. Select Save to add the new device to the SSP account.

Note: The status of a newly-added device sets 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:

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

**Note:** The Device Summary User role resource controls the visibility of the Summary tab in the SSP. If specific pieces of information are restricted from a user role's view by way of a disabled resource such as Device Apps, Device Compliance, or Device Profiles, then corresponding information normally appearing on the Summary tab is also hidden.

Visit Defining User Roles and Creating Admin Roles for detailed instructions on limiting resources for user and admin roles.

- **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. This tab also shows the status of each profile.
- **Apps** – Displays all applications installed on the selected device and provides basic app information.
Performing Actions in the SSP

AirWatch gives administrators several remote actions and options for 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 and action permissions are determined by your administrator. Allowed actions are split between Basic Actions and Advanced Actions on the main access page.

Action permissions are determined by the administrator, therefore device users may not be able to perform all listed actions. See the applicable VMware AirWatch Platform Guide, available on AirWatch Resources.
## Basic Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BES Registration</td>
<td>Select this to register the device with BES 10.</td>
</tr>
<tr>
<td>Change Passcode</td>
<td>Set a new passcode for the selected device.</td>
</tr>
<tr>
<td>Clear SSO Passcode</td>
<td>Clears the single sign on passcode on the selected device and the next SSO app used will prompt for a new passcode. This is useful if users forget their device passcode and are locked out of their device.</td>
</tr>
<tr>
<td>Clear Passcode</td>
<td>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.</td>
</tr>
<tr>
<td>Delete Device</td>
<td>Removes the device from the Self Service Portal.</td>
</tr>
<tr>
<td>Delete Registration</td>
<td>Deletes any pending enrollment record from the Self Service Portal.</td>
</tr>
<tr>
<td>Device Query</td>
<td>Requests the device to send a comprehensive set of MDM information to the AirWatch Server.</td>
</tr>
<tr>
<td>Device Wipe</td>
<td>Wipes all data from the selected device, including all data, email, profiles and MDM capabilities and returns the device to factory default settings.</td>
</tr>
<tr>
<td>Download Agent</td>
<td>Download and install the AirWatch Agent for this device.</td>
</tr>
<tr>
<td>Enterprise Wipe</td>
<td>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.</td>
</tr>
<tr>
<td>Locate Device</td>
<td>Activates the GPS feature to locate a lost or stolen device. This action is hidden when privacy settings are restrictive.</td>
</tr>
<tr>
<td>Lock Device/Screen</td>
<td>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.</td>
</tr>
<tr>
<td>Lock SSO</td>
<td>Lock the single sign on passcode for apps on this device. The next SSO app opened will prompt for a passcode.</td>
</tr>
<tr>
<td>Make Noise</td>
<td>Helps find a device by remotely causing it to ring.</td>
</tr>
<tr>
<td>Resend Enrollment Message</td>
<td>Sends another copy of the initial enrollment email, SMS or QR code to the device intended to register.</td>
</tr>
<tr>
<td>Send Message</td>
<td>Sends a message using email, phone notification or SMS to the device.</td>
</tr>
<tr>
<td>Set Roaming</td>
<td>Set whether roaming is enabled for this device.</td>
</tr>
<tr>
<td>Sync Device</td>
<td>Outfit devices with the latest company policies, content, and apps.</td>
</tr>
<tr>
<td>View Enrollment Message</td>
<td>See the actual email, SMS or QR code that comprised the initial enrollment message.</td>
</tr>
</tbody>
</table>
**Note:** Registration and Enrollment actions will only display in the SSP when the enrollment of a selected device is still pending.

2. **Advanced Actions**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate App Token</td>
<td>Generate a token that the device can use to access secure applications.</td>
</tr>
<tr>
<td>Manage Email</td>
<td>Manage devices connected to an email account.</td>
</tr>
<tr>
<td>Review Terms of Use</td>
<td>Review past terms of use for this account.</td>
</tr>
<tr>
<td>Revoke Token</td>
<td>Revokes the token for a selected application.</td>
</tr>
</tbody>
</table>
# Self-Service Portal Actions Matrix

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

<table>
<thead>
<tr>
<th>Action</th>
<th>Android</th>
<th>iOS</th>
<th>Win Phone 8</th>
<th>Mac OS X</th>
<th>Win Mobile</th>
<th>Win PC</th>
<th>Win 8/RT</th>
<th>QNX</th>
<th>Black Berry</th>
<th>Symbian</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Actions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BES Registration</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Passcode</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear (SSO) Passcode</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete Device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Delete Registration</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Device Query</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Device Wipe</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Download Agent</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Wipe</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Locate Device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lock Device/Screen</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lock SSO</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Make Noise</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resend Enrollment Message</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send Message</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Set Roaming</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sync Device</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Enrollment Message</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Advanced Actions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Generate App Token</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Manage Email</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review Terms of Use</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revoke Token</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upload S/MIME Certificate</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Customizing the Self Service Portal (SSP)

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-premises 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.
Finding Additional Documentation

While reading through this documentation you may encounter references to documents that are not included here. You can access this additional documentation through the AirWatch Resources page (https://resources.air-watch.com) on myAirWatch.

**Note:** AirWatch recommends you always pull the document from AirWatch Resources each time you need to reference it.

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

1. Navigate to [http://my.air-watch.com](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, Airwatch recommends you always 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.