Mobile Device Manager
v. 7.3
Admin Guide

Document Revision Date: Oct. 14, 2014
# Contents

- Introduction .................................................................................................................................................. 1
- System Requirements ............................................................................................................................... 1
- Getting Started with AirWatch ................................................................................................................. 2
- Environment Setup ................................................................................................................................... 6
- Privacy Best Practices ................................................................................................................................ 8
- Organization Groups ................................................................................................................................... 10
  - Creating Organization Groups ................................................................................................................. 12
- Smart Groups .............................................................................................................................................. 13
  - Creating a Smart Group .......................................................................................................................... 13
  - Assigning a Smart Group ......................................................................................................................... 14
  - Managing Smart Groups ......................................................................................................................... 15
- Device Users ................................................................................................................................................ 18
  - Choosing User Authentication Types ...................................................................................................... 18
  - Managing User Accounts ........................................................................................................................ 19
  - Accessing User Details ............................................................................................................................ 19
- Device Profiles ............................................................................................................................................. 20
  - Configuring General Profile Settings ....................................................................................................... 20
  - Managing Device Profiles ........................................................................................................................ 22
  - Editing Device Profiles ............................................................................................................................. 23
  - View Device Assignment ........................................................................................................................... 24
  - Geofences ............................................................................................................................................... 25
  - Defining Geofences ................................................................................................................................. 26
  - Applying a Geofence to a Profile ............................................................................................................. 26
  - Time Schedules ....................................................................................................................................... 28
  - Defining Time Schedules ......................................................................................................................... 28
  - Applying a Time Schedule to a Profile ..................................................................................................... 28
- Compliance ................................................................................................................................................. 30
  - Compliance Policies by Platform ............................................................................................................. 31
  - Adding a Compliance Policy .................................................................................................................... 33
  - Managing Devices ................................................................................................................................... 37
  - Using the Device Dashboard .................................................................................................................... 37
Using the Device List View ......................................................................................................................38
Using the Management Tabs ..................................................................................................................41
Using the Device Details Page.................................................................................................................42
Using Wipe Protection ............................................................................................................................43
Utilizing Reports ......................................................................................................................................46
Using AirWatch Hub ................................................................................................................................47
Introduction
Mobile devices are valuable enterprise tools, allowing immediate access to your internal content and resources. However, the diversity of mobile platforms, operating systems, and versions can make managing a uniform set of devices difficult. Mobile Device Management (MDM) solves this problem by enabling you to configure, secure, monitor, and manage all types of mobile devices in the enterprise.

Manage large-scale deployments of mobile devices from a single console. Quickly enroll devices in your enterprise environment, configure, and update device settings over-the-air, enforce security and compliance policies, secure mobile access to corporate resources, and remotely lock and wipe managed devices.

Tailor your MDM environment to gain immediate access to device locations, current users, and content. Automate your MDM deployment to enforce security and compliance settings 24/7 with rules and warnings unique to each user or Organization Group. Ensure that content and features are available and establish restrictions based on a device’s geographic location. This guide outlines how to effectively create, configure, and maintain your MDM deployment.

NOTE: Many of the configurations in this guide are geared towards iOS due to OEM limitations. If there are fewer notes relating to Android or other platforms, you can assume that this is because there are generally fewer, if any, pre-configurations for those platforms relative to iOS.

System Requirements
The following system requirements should be met before using AirWatch.

Supported Browsers
Comprehensive platform testing has been performed to ensure functionality using these web browsers. The AirWatch Admin Console may still function in non-certified browsers with minor issues.

- Internet Explorer 8+
- FireFox 3.x+
- Google Chrome 11+
- Safari 5.x

Supported Devices
AirWatch supports the following devices and operating systems:

- Android versions 2.3+
- BlackBerry versions 5+; BlackBerry 10
- iOS versions 4.0+; Mac OS X 10.7+
- Symbian OS ^3 and S60
- Windows Mobile 5/6 and Windows CE 4/5/6; Windows Phone 7 and 7.5 Mango; Windows Phone 8; Windows 8/8.1/RT; Win32
Getting Started with AirWatch

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

The AirWatch Admin Console is also a universal tool with customization benefits, including:

- **HTML5** – Allowing a clean and consistent user experience.
- **Global Access and Language Support** – Providing a location-friendly portal with language and localization support that can be accessed anywhere using a web browser.

Logging into the AirWatch Admin Console

Before logging into the AirWatch Admin Console, you must have the Environment URL and login credentials provided to you by your AirWatch administrator.

**NOTE:** Passwords are case-sensitive.

Setting Your Security PIN

Upon first logging into the AirWatch Admin Console, you must establish a Security Personal Identification Number (PIN). The Security PIN acts as a safeguard against accidental device wipes or deletion of major MDM-related aspects of your environment, including users and Organization Groups. The Security PIN also serves as a second layer of security, presenting an additional point of authentication blocking actions made by unapproved users if the Admin Console is left open and unattended.

Enter and confirm your four-digit security PIN when presented with the **Security Settings** page and save this PIN for future use. You may not bypass this page or proceed to any area within the Admin Console before creating this PIN.

![Security Settings](image-url)
Resetting Your PIN
Once your PIN is set, revisit the Security Settings page to reset the PIN by selecting your username in the top right corner of the Admin Console. Select Reset from the Security Settings menu to reset your PIN, log out of the Admin Console and present the PIN creation prompt upon logging back in.

The Admin Console at a Glance
Now that you’re logged in and have established a security PIN, familiarize yourself with the key components of the AirWatch Admin Console.

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

- **Global Search** – Search all aspects of your MDM deployment within the Admin Console, including devices, users, content, applications, configuration settings admins, pages and more.
- **Getting Started** – Launch or continue the MDM setup guide with milestones and overall status. The red number badge hovering over the [Getting Started] button refers to the number of steps left to complete in the Getting Started Wizard.
- **Add** – Quickly add an admin, device, user, compliance policy, content, profile, internal application or public application.
- **Saved** – Access your favorite and most-utilized features within the Admin Console.
- **Account** – View your account information. Change roles that you are assigned to within the current environment. Customize preferences, including contact information, Admin Console settings and preferences and login history. Log out of the Admin Console and return to the Login screen.
- **Help** – Launch the online help portal to browse or search the available guides and feature documentation.
- **Home** – Returns you to your homepage within the Admin Console.
- **Save** – Saves the current page or view for quick access from your list of Saved pages.
Additionally, the **Main Menu** allows quick navigation all available features available to your role and Mobile Device Management (MDM) deployment. These options generally include:

**Hub** – View and manage MDM information that drives decisions you need to make. Gain a quick overview of specific information, such as the most blacklisted apps that violate compliance, or all devices that are currently out of compliance. See the [Using the Hub](#) section for more information.

**Devices** – Access the Device Dashboard for a detailed overview of common aspects of devices in your fleet, including compliance status and breakdown of ownership type, last seen, platform type, and enrollment type. Easily swap views according to your own preference, including full Dashboard, list view, or detail view. Drill down to additional tabs, including all current profiles, enrollment status, compliance policies, certificates, product provisioning, and printer management.

**Accounts** – Survey and manage Users and Administrators involved with your MDM deployment. Access and manage user groups, roles, batch status and settings associated with your users. Additionally, access and manage admin groups, roles, system activity, and settings associated with your administrators.

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

**Content** – Manage and upload content available to users and devices. Additionally, access batch import status, content categories, content repositories, user storage, Secure Content Locker home screen configuration, and all other content-specific settings.

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

**Telecom** – View and manage telecom usage and roaming tracking, including call, SMS, and content settings.

**Groups & Settings** – Manage structures, types and statuses related to Organization Groups, Smart Groups, App Groups, User Groups, and Admin Groups. Configure entire system settings or access settings related to all Main Menu options outlined above.
Using the Global Search
The Admin Console's **Global Search** box returns quick-access information from all aspects of your deployment, including:

- **Devices** – Shows device friendly name, device type and ownership type.
- **Users** – Shows display name, username and Organization Group.
- **Profiles** – Shows profile name and platform type.
- **Applications** – Shows information for internal, public and purchased apps, including app name and platform type.
- **Content** – Shows file name and version number.
- **Settings** – Shows section of Admin Console for settings related to search term.
- **Admins** – Shows any Admins related to the search term.
- **Pages** – Shows any pages in the Admin Console related to the search term.

For your convenience, these search results are displayed in order depending on the amount of results. For example, if you receive 75 results for Devices, 3 results for Users, 2 results for Internal Applications, and no results for the other categories, the results page would be ordered as Devices, Users, Internal Applications, Profiles, Content, and Settings.

You can perform the search for another Organization Group by selecting another group from the **Organization Group** drop-down menu.
Environment Setup

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

Generating an APNs Certificate

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

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

Configuring Privacy Settings

Configure Privacy Settings to define how device and user information is handled in the Admin Console. This is particularly useful in bring your own device (BYOD) deployments. The Admin Console enables you to review and adjust privacy policies according to device ownership. Configuring privacy settings by device ownership lets you easily adhere to data privacy laws in other countries or legally-defined restrictions. It also helps ensure certain IT checks and balances are in place, preventing overload of servers and systems.

To set up privacy settings:

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

   - **Collect and Display** – Collect user data and display it in the Admin Console.
   - **Collect Do Not Display** – Collect user data for use in reports but do not display it in the Admin Console.
   - **Do Not Collect** – Do not collect user data.
3. Select the Commands that can be performed on devices.

Consider disabling all remote commands for employee-owned devices – especially full wipe. This prevents inadvertent deletion or wiping of an end user's personal content. If you are going to allow remote control, file manager, or registry manager access for Android/WinMo devices, you should consider using the Allow With User Permission option. This requires the end user to consent to admin access on their device via message prompt before the action is performed. If you opt to allow use of any commands, explicitly mention these in your Terms of Use agreement.

4. For User Information, select whether to Display or Do Not Display in the Admin Console information for First Name, Last Name, Phone Number, and Email Accounts.
If a field is set to Do Not Display, then it displays as "Private" wherever it appears in the Admin Console. This means you are not be able to search for fields you set to Do Not Display.

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

5. Click Save when finished.

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

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

- **GPS Data** – Information collected includes location data and a timestamp for when this information was sent to AirWatch.
  - For iOS devices, GPS data is reported automatically by opening any AirWatch application or internal applications with an AirWatch 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, but administrators can create compliance policies to ensure users keep this setting turned on.
- While GPS data is typically used for lost or stolen devices, it can also be used for any situation where knowing a device’s location is useful.
**User Information**
In general, you will display user information, such as first name and last name for both employee-owned and corporate-owned devices, since you need to know who you are managing. This information includes First Name, Last Name, Phone Number, and Email Address.

**Application Information**
In general, it is appropriate set the collection of application information to either Do Not Collect or Collect and Do Not Display for employee-owned devices. This is because public apps installed on a device, if viewed, can be considered personally identifiable information. For corporate-owned devices, all installed applications on the device will be reported to AirWatch. If Do Not Collect is selected, only personal application information will not be collected. All managed applications, whether public, internal, or purchased, will still be collected by AirWatch.

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

AirWatch identifies users and establishes permissions using Organization Groups, which you can view by navigating to Groups & Settings > Groups > Organization Groups > List View or via the Organization Group drop-down list. With Organization Groups, you can establish an MDM hierarchy identical to your organization's internal hierarchy. You may also choose to establish an Organization Group depending on features and content that will be accessed from sets of devices.

Organization groups allow you to:

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

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

- **Scalability** – Complete 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 drop-down list to the left, any profiles, features, applications, and other MDM settings can be set at the top World-Wide Enterprises level.

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

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

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

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

- **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 over-ridden at any level. Settings include device enrollment options, authentication methods, privacy settings, and branding.

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

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

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

- **Executive devices** cannot install applications and have access to the Wi-Fi sales network.
- **Sales devices** are allowed to install applications and have VPN access.

**Override vs Inherit Setting**

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

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

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

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

   See **Organization Groups** for details about Group IDs as used in Organization Groups.

5. Add region information and **Save**.
Smart Groups

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

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

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 or product, you must first create one.

Follow these steps to create a Smart Group:

1. Choose the applicable **Organization Group** to which your new Smart Group will apply and be managed from.
2. Navigate to **Groups & Settings > Groups > Smart Groups** and then select **Add Smart Group**.
3. Enter a **Name** for the Smart Group.
4. Configure the Smart Group type by choosing between **Select Criteria** and **Select Devices or Users**.
   - The **Select Criteria** option works best for groups with large numbers 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, Model, Operating System, and Enterprise OEM (Original Equipment Manufacturer) Version. You can also add and exclude specific devices and users in the Additions and Exclusions sections.

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

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

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

**NOTE:** It is not recommended to manually add more than 500 devices or users per smart group when Select Devices or Users is enabled. In such a scenario, consider enabling the Select Criteria option for the main bulk of devices that share a general criterion and if required, create a separate Select Devices or User smart group for those devices that fall outside the general criteria.

5. Click Save when finished.

### Assigning a Smart Group

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

Follow these steps to assign a Smart Group:

1. Complete the Assigned Smart Groups drop-down field as it appears during the process of adding or creating applications, books, device profiles, product provisions, or compliance policies.

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, profile, provision, or policy is being added, or to a child OG below it.
3. If no smart group matches the desired assignment criteria, then select the **Create New Smart Group** option. You can assign more than one Smart Group per profile, policy, application, book, or provision.

4. Select **Save** to include the assignment.

**Excluding Smart Groups in Profiles and Compliance Policies**

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

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

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

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

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

**Managing Smart Groups**

Manage your Smart Groups by Editing, Unassigning, and Deleting them with the Admin Console.

**Editing a Smart Group**

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

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

Take the following steps to edit a Smart Group:

1. Navigate to **Groups & Settings > Groups > Smart Groups**.
2. Select the **Edit** icon from the action menu to the right of the listed Smart Group that you wish to edit. The **Edit Smart Group** screen will display with its existing settings.
3. Make changes to either the **Criteria** or the **Devices and Users** (depending upon which type the Smart Group was saved with).
4. Select the **Next** button and the **View Smart Group Assignments** page displays, allowing you to review which profiles, apps, books, provisions and policies may be added or removed from the devices as a result.

5. Save your Smart Group edits by selecting the **Publish** button on the **View Smart Group Assignments** page. All profiles, apps, books, provisions, and policies tied to this smart group will now change its device assignment based on this edit.

**View Smart Group Assignments**

As a convenience, you can confirm the specific profiles, apps, books and compliance policies that are included in (as well as excluded from) the assigned Smart Group.

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

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

**Deleting a Smart Group**

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

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

**Unassigning a Smart Group**

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

1. Navigate to the edit screens (paths below) to unassign Smart Groups from applications, books, compliance policies, device profiles, or product provisions:
   - **Applications** – Navigate to **Apps & Books > Applications > List View** and select the **Public** or **Internal** tab.
   - **Books** – Navigate to **Apps & Books > Books > List View** and select the **Public** or **Internal** tab.
   - **Compliance Policy** – Navigate to **Devices > Compliance Policies > List View**.
   - **Device Profile** – Navigate to **Devices > Profiles > List View**.
   - **Product Provision** – Navigate to **Devices > Products > List View**.
2. Locate the content or setting from the listing and select the Edit icon from the actions menu.
3. Select the Assignment tab or locate the Assigned Smart Groups field.
4. Select Delete (X) next to the Smart Group you wish to unassign.

**NOTE:** This action will not delete the Smart Group; it simply removes the Smart Group from the saved setting.

5. Take the normal steps to Save your changes.
Device Users

AirWatch manages devices by keeping track of the users who use each device. Therefore, user accounts must also be created or integrated for devices to enroll into AirWatch. The Admin Console allows you to establish a complete user infrastructure by providing configuration options for user authentication types, 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 amount of login steps required by the end user on the device at enrollment. If you want the enrollment process to be as simple as possible for the end user, the administrator must do more work to set up the process. Likewise, a lighter workload for the administrator means there is more setup to do by the end user.

Token-based Authentication

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

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

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

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

**NOTE:** SMTP is included with SaaS deployments.
Managing User Accounts

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

- **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.
- **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.
- **Edit User** – Edit the user details for a specific user.
- **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. You may only move a user account if it has no devices associated to it yet.

**NOTE:** You may only move a user account if it has no devices associated to it yet.

Accessing User Details

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

- All associated user groups.
- All Devices associated with the user over time and a link to complete history of enrolled devices.
- All devices a user has checked-out in a Shared Device Environment and a link to complete check-in/check-out device history.
- All device- and user-specific event logs.
- Summary of all assigned, accepted, and declined Terms of Use.
Device Profiles
Profiles are the primary means by which you can manage devices. You can think of profiles as the settings and rules that, when combined with compliance policies, help you enforce corporate rules and procedures. They contain the settings, configurations, and restrictions that you want to enforce on devices. Create profiles for each platform type, and configure a payload, which are the individual settings you configure, such as those for passcodes, Wi-Fi, restrictions, or VPN, for each one. Create a profile by navigating to Devices > Profiles > List View, selecting Add, and choosing your appropriate platform.

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

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 General settings listed below apply to any profile:

1. Navigate to Devices > Profiles > List View, select Add, and choose your appropriate platform.
2. Configure General settings:
   - **Name** – Name of the profile to be displayed in the Admin Console.
   - **Version** – Read-only field that reports the current version of the profile as determined by the Add Version button.
   - **Description** – A brief description of the profile that indicates its purpose.
   - **Deployment** – Determines if the profile will be automatically removed upon unenrollment:
     - **Managed** – The profile is removed.
     - **Manual** – The profile remains installed until removed by the end user.
   - **Assignment Type** – Determines how the profile is deployed to devices:
     - **Auto** – The profile is deployed to all devices automatically.
     - **Optional** – The end user can optionally install the profile from the Self-Service Portal (SSP) or can be deployed to individual devices at the administrator's discretion.
     - **Interactive** – This is a unique assignment type in which the profile integrates with third-party systems to deploy a specific payload to a device. This option will only be available if enabled in Groups & Settings > All Settings > Devices & Users > Advanced > Profile Options.
     - **Compliance** – The profile is deployed when the end user violates a compliance policy applicable to the device.
   - **Allow Removal** – Determines if the profile can be removed by the device's end user:
     - **Always** – The end user can manually remove the profile at any time.
     - **With Authorization** – The end user can remove the profile with the authorization of the administrator.
     - **Never** – The end user cannot remove the profile from the device.
• **Managed By** – The Organization Group with administrative access to the profile.

• **Assigned Smart Group** – The Smart Group to which you want the device profile added. Includes an option to create a new Smart Group which can be configured with specs for minimum OS, device models, ownership categories, organization groups and more. See *Smart Groups* for more information.

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

• **Exclusions** – If Yes is selected, a new field **Excluded Smart Groups** displays, enabling you to select those Smart Groups you wish to exclude from the assignment of this device profile. See *Excluding Smart Groups in Profiles and Compliance Policies* for details.

• **View Device Assignment** – After you have made a selection in the **Assigned Smart Group** field, you may select this button to preview a list of all devices to which this profile will be assigned, taking the Smart Group assignments and exclusions into account.

• **Additional Assignment Criteria** – These check boxes enable additional restrictions for the profile:

  **NOTE:** Geofencing is available for Android and iOS only.

  o **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. See *Time Schedules* for more information.

• **Removal Date** – The date the profile will be removed from the device. Must be a future date formatted as M/D/YYYY

3. Select and configure your profile payload. Each payload contains unique settings and options depending on make, model, and OS of the device you’re configuring.

  **NOTE:** AirWatch recommends setting up one payload per profile to minimize multiple settings pushed down at once. Pushing multiple payloads at once makes troubleshooting difficult, requires pushing down all settings at once (rather than the one that needs updating), and is a less granular configuration.

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

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

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

- **Toggle Filters** (highlighted in red above) – Filter the list of device profiles by status, platform, smart group and others.
- **Edit** – Customize an existing profile. Tweak major or minor settings in a profile to maintain the most effective MDM settings.
- **Publish** – Deploy the profile to all assigned devices. Update a device's profile settings depending on the user’s (or device's) new role within your company.
- **View XML** – Display the XML code that AirWatch generates after profile creation. View and save the XML code to reuse or alter outside of the Admin Console.
- **Edit Assignment** – Change the Organization Group a profile is assigned to without re-publishing the profile to every assigned user. Reorganize your profiles to alternate Organization Groups to adapt to your organization’s restructuring.

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

- **Delete** – Delete a profile and remove it from all devices. Maintain your roster of profiles by removing unnecessary profiles. For example, delete an outdated profile for roles or teams that no longer exist or have been phased out.
- **Copy** – Duplicate an existing profile with a new profile name, which you can then edit for a new profile. Streamline the profile creation process by copying an existing profile and altering parts as needed.
- **View Devices** – View devices that are available for that profile and if the profile is currently installed. Survey which devices are in your fleet and manually push profiles if necessary. For example, provide remote support for an end-user who is requesting additional or necessary features.
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 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 configurations, or 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 weren’t already assigned to the profile.

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

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

**General Changes**

1. Navigate to Devices > Profiles > List View and select the Edit icon from the actions menu of the profile you wish to edit.
   
   **NOTE:** Only device profiles managed by that Organization Group or a child Organization Group below will be editable.

2. Make any changes you like in the General category.  
   See Configuring General Profile Settings for a detailed listing of General category field descriptions.

3. After completing General changes, you may select Save & Publish to apply the profile to any new devices you may have added or removed.  
   Devices already assigned with the profile will not receive the republished profile again.
   The View Device Assignment screen displays, confirming the list of currently-assigned devices.
Payload Changes
Optionally, you may continue to make Payload changes:

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

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

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

View Device Assignment
Selecting the Save & Publish button after configuring a profile displays the View Device Assignment screen and serves as a preview of affected (or unaffected) devices.
Depending upon which kind of change you make to the device profile, the Assignment Status column will reflect the following:

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

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

**Geofences**

AirWatch enables you to define geofences 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 one-mile radius could apply to your office, while a much larger geofence could apply approximately to an entire state. Once you have defined a geofence you can apply it to profiles, SDK applications, AirWatch apps such as the Secure Content Locker, and more.

**NOTE:** Geofencing is available for Android and iOS devices.

Enabling a Geofence is a two-step process:

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

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

<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>

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

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

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

To create a geofence:

1. Navigate to **Devices > Profiles > Settings > Geofencing** to access the **Geofencing Settings** page. Select **Add Area**.
2. Enter an **Address** and the initial **Radius** of the geofence. Additionally, you may double-click any area on the map to set the central location.
3. Select **Click to Search** to view on a map roughly where the geofence will be applied.

**NOTE:** Integration with Bing maps requires that "insecure content" be loaded on this page. If location search does not load as expected, you may need to allow "Show all Content" for your browser.

4. Enter the **Area Name** (how it appears in the Admin Console) and click **Save**.

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

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

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

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

**NOTE:** In the event that a user manually disables location services on their iOS device, AirWatch can no longer collect location updates and considers the device to be in the location where services were disabled.
Time Schedules
In addition to simply assigning applicable profiles, you have the ability to enhance device management further by controlling when each profile assigned to the device 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.

Defining Time Schedules
To create a time schedule:

1. Navigate to Devices > Profiles > 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 more days to the schedule.
8. Select Save.

Applying a Time Schedule to a Profile
Once you have defined a time schedule, you can apply it to a profile and combine it with other payloads to create more robust profiles.

For example, you can define time schedules for the normal work hours of different organization groups and add a Restrictions payload that denies access to the Game Center, multiplayer gaming, or YouTube content based on ratings and other settings.
Once activated, the employees of the Organization Group to whom the profile was applied will no longer have access to these functions during the specified times.

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

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

The Compliance Engine is AirWatch's automated tool to ensure all devices adhere to your policies. Your policies may include basic security settings such as requiring a passcode and having a minimum device lock period. You may also decide to set 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 out of compliance, the Compliance Engine begins to warn the user to fix compliance errors to prevent disciplinary action on the device. For example, if a user loads blacklisted games or social media apps onto their device, the Compliance Engine sends a message to notify the user that their device is out of compliance. If the errors are not corrected in the amount of time specified, the device loses access to certain content and applications.

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

Enforcing mobile security policies is as easy as:

- **Choosing your platform** – Determine on which platform you want to enforce compliance: Android, Apple iOS, Apple Mac, Windows Mobile, Windows PC, Windows Phone 8, or Windows 8/RT.
- **Building your policies** – Customize your policy to cover everything from application list, compromised status, encryption, 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.
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>Mac OS X</th>
<th>Windows Mobile</th>
<th>Windows PC (Win32)</th>
<th>Windows Phone 8</th>
<th>Windows 8/RT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application List</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>
</tr>
<tr>
<td>Cell Data Usage</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>
</tr>
<tr>
<td>Cell Voice Usage</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>
</tr>
<tr>
<td>Device Last Seen</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>
</tr>
<tr>
<td>Firewall Status</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>
</tr>
<tr>
<td>Interactive Certificate Profile Expiry</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>
</tr>
<tr>
<td>MDM Terms of Use Acceptance</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>
</tr>
<tr>
<td>OS Version</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>
</tr>
<tr>
<td>SIM Card Change</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>
</tr>
<tr>
<td>Windows Copy Genuine Validation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
Compliance Policies Detailed

- **Application List** – Detect specific, blacklisted apps that are installed on a device, or detect all apps that are not whitelisted.
  
  You can either specifically prohibit certain apps, such as social media or entertainment apps, or specifically permit only the apps you specify, such as internal applications for business use.

- **Antivirus Status** – Detect whether or not an antivirus program is running.

- **Cell Data/Message/Voice Usage** – Detect when end-user devices exceed a particular threshold of their assigned telecom plan. For this policy to take effect Telecom must be configured. See the *AirWatch Telecom Guide* for more information.

- **Compromised Status** – Select if the device is non-compliant when compromised.
  
  Prohibit the use of jailbroken devices that are enrolled with AirWatch. Jailbroken devices strip away integral security settings and may introduce malware in your network and provide access to your enterprise resources.
  
  Monitoring for compromised device status is especially important in BYOD environments where employees have various versions of devices and operating systems. For more information, refer to the *Detecting Compromised Devices* document available on the AirWatch Resources Portal.

- **Device Last Seen** – Select if the device is non-compliant when the device fails to check in within an allotted time window.

- **Encryption** – Select if the device is non-compliant when Encryption is not enabled.

- **Firewall Status** – Detect whether or not a firewall program is running.

- **Free Disk Space** – Detect the available storage space on the device.

- **Interactive Profile Expiry** – Select if the device is non-compliant when an installed profile expires within the specified length of time.

- **Last Compromised Scan** – Select if the device is non-compliant when AirWatch is unable to successfully query the device on schedule.

- **MDM Terms of Use Acceptance** – Select if the device is non-compliant when the current MDM Terms of Use have not be accepted by the end user within a specified length of time.

- **Model** – Select if the device is non-compliant based on a specific platform.

- **OS Version** – Select if the device should be marked as non-compliant when it is within a certain window of OS versions that you configure.

- **Passcode** – Select if the device is non-compliant when a passcode is not present.

- **SIM Card Change** – Select if the device is non-compliant when the SIM Card has been replaced.

- **Windows Automatic Update Status** – Detect whether or not Windows Automatic Update has been activated.

- **Windows Copy Genuine Validation** – Detect whether or not the copy of Windows currently running on the device is genuine.
**Adding a Compliance Policy**

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

1. Navigate to Devices > Compliance Policies > List View and select **Add**.
   The Add Compliance Policy screen appears.

2. Select a **Platform** on which to base your compliance policy.
   Choosing a Platform at the beginning means the available listing of rules, escalations, and actions will be Platform-specific.

   ![Add Compliance Policy](image)

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

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

3. Select **Any** or **All** rules in the **Match** field to detect conditions.

4. Choose the rule from the drop-down field and set specific rule parameters.
   Add more rules and parameters by selecting the **Add Rule** button.
   When finished building rules for this policy, select **Next** and the **Actions** tab displays.
5. Specify **Actions** and **Escalations** that occur.  
Select the type of action to perform: **Application**, **Command**, **Notify**, **Profile**, or **Email**.  

**NOTE:** For Mac OS X, you can only perform the following actions: **Enterprise Wipe**, **Send Email to User**, **Send Push Notification to Device**, **Send Email to Administrator**, **Block/Remove Profile**, **Block/Remove Profile Type**, and **Block/Remove All Profiles**.

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

**NOTE:** The **Block Email** action applies if you are using **Mobile Email Management and the Email Compliance Engine**, which is accessed by navigating to **Email > Compliance Policies > Email Policies**. This lets you use Device Compliance policies such as blacklisted apps in conjunction with any Email Compliance Engine policies you configure. With this action selected, email compliance is triggered with a single device policy update if the device falls out of compliance.

You can enforce application compliance as well by establishing a whitelist, blacklist or required list of applications. For more information on establishing a robust and effective Mobile Application Management (MAM) plan, please see the **AirWatch MAM Guide**, available via AirWatch Resources.

When finished building actions for this policy, select **Next** and the **Assignment** tab displays.
7. Select the Organization Group by which this compliance policy will be managed in the Managed By field.
8. Choose one or more Smart Groups by completing the Assigned Smart Groups field.
9. Decide if you want to exclude any Smart Groups by selecting Yes on the Exclusions field and select from the available listing of Smart Groups to exclude in the Excluded Smart Groups field. See Excluding Smart Groups in Compliance Policies for details.

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

10. You may optionally select the View Device Assignment button to see a listing of devices affected by this compliance policy assignment.
When finished determining the Assignment of this policy, select Next. The Summary tab displays.

11. In this final step, provide a Name and a useful Description of the compliance policy.
12. Complete the process by selecting **Finish**, which will save your compliance policy without activating it to the assigned devices or **Finish And Activate**, which will save and apply the policy to all affected devices.

**View Device Assignment**

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

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

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

Select **Publish** to finalize the changes and, if necessary, re-publish any compliance policy.
Managing Devices
You can manage all of your deployment’s devices from the AirWatch Dashboard. The Dashboard is a searchable, customizable view you can use to filter and find specific devices based on various criteria. This simplifies performing actions and administrative functions on a particular set of devices. In addition, 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, view and manage them from the Device Dashboard. The Device Dashboard provides a high-level view of your entire fleet of mobile devices while allowing a quick and easy way to drill down to individual devices and take MDM actions. View graphical representations of relevant statistics, including important device information for your fleet, such as device ownership type, compliance statistics, and telecom usage.

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

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

- **Compromised** – The number and percentage of compromised devices (i.e., jailbroken, rooted, etc.) in your deployment.
- **No Passcode** – The number and percentage of devices without a passcode configured for security.
- **No Encryption** – The number and percentage of devices that are not encrypted for security.

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

**Ownership**

View the total number of devices in each ownership category.

**Last Seen Overview**

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

**Platforms**

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

**Enrollment**

View the total number of devices in each enrollment category.

**Using the Device List View**

1. Switch to List View (Devices > List View) at any time to sort and manage devices by filtering the columns and fields available in the Device Dashboard, including:
   - Last Seen
   - General Info (friendly name, display name, ownership, organization group)
   - Platform/OS/Model
   - User
   - Tags
   - Enrollment Status
   - Compliance Status
2. Select a device **Friendly Name** at any time to open up the device details page for that device.

3. Sort columns and configure information filters to gain insight on device activity based on specific information you are curious about.
   
   For example, sort the **Compliance Status** column to view only devices that are currently out-of-compliance and take action or message only those specific devices.

4. Search all devices for a friendly name or user's name to isolate one device or user.
   
   You may also rearrange the order of the columns as they are presented in the listing by dragging and dropping the column headings.

Once you have sorted or filtered dashboard information, export, save, and send the data for review.
Hover-Over Pop-up

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

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

Using the Search List, Filters, and Bulk Messaging

At times, you will need to search for a single device for quick access to its information and take remote action on the device. For example, search for a specific device, platform or user.

Navigate to **Devices > List View > Search List** and search for all devices within the current Organization Group and all child groups.

You can also drill down to specific sets of devices by filtering device criteria, including by **Platform**, **Ownership Type**, **Passcode**, **Last Seen**, **Enrollment**, **Encryption**, and **Compromised** status.

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

Once you have applied a filter to show a specific set of devices, perform bulk actions to multiple, selected devices by clicking the check box for those devices and selecting an action from the **Management** tabs.
Using the Management Tabs
With the categorized devices displayed, take bulk action on specific devices by selecting the check box next to each device and using the top Control Panel to:

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

With the categorized devices displayed, take bulk action on specific devices by selecting the check box next to each device and using the top Control Panel to:

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

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

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

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

- **Management** – Query, lock or perform Enterprise Wipe on all selected devices.
- **Support** – Send a message to a device with instructions or communication to end user. Locate current GPS location of all selected devices.
- **Admin** – Change Admin Console settings, including changing Organization Group, Ownership type, or device group of selected devices or deleting devices from AirWatch MDM.
- **Advanced** – Perform a warm boot on devices to remotely reboot those devices.
  Select **Provision Now** to perform a number of configurations for selected devices.
  Select **Install Product** to install particular apps to selected devices.

You can perform additional remote actions to individual devices from the **Device Details** page.
Using the Device Details Page

Use the **Device Details** page to track detailed device information and quickly access user and device management actions. You can access the **Device Details** page by selecting a device’s **Friendly Name** from the **List View** page or from one of the available Dashboards, or by using any of the available search tools within the Admin Console.

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

- **Summary** – View general statistics such as enrollment status, compliance, last seen, platform/model/OS, Organization Group, contact information, serial number, power status, storage capacity, physical memory, and virtual memory.
- **Compliance** – Display the status, policy name, date of the previous and forthcoming compliance check, and the actions already taken on the device.
- **Profiles** – View all MDM profiles currently installed on a device.
- **Apps** – View all apps currently assigned and installed on a device.
- **Content (iOS and Android)** – View the status, type, name, priority, deployment, last update, and date and time of views, and provides a toolbar for administrative action (install or delete content).
- **Location** – View current location or location history of a device.
- **User** – Access details about the user of a device as well as the status of the other devices enrolled to this user.
The menu tabs below are accessed by clicking More from the main Device Details tab. Additional menu tabs vary, based on device platform. Some of the most common include:

- **Network** – View current network (Cellular, Wi-Fi, or Bluetooth) status of a device.
- **Security** – View current security status of a device based on security settings.
- **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 certificates by name and issuant. This tab also provides information about certificate expiration.
- **Provisioning** – View complete history and status of all packages provisioned to the device and any provisioning errors.
- **Terms of Use** – View a list of End User License Agreements (EULAs) which have been accepted during device enrollment.
- **Alerts** – View all alerts associated with the device.
- **Event Log** – View history of device in relation to MDM, including instances of debug, information and server check-ins.
- **Device Registration** – View all restrictions currently applied to a device. This tab also shows specific restrictions by Device, Apps, Ratings, and Passcode.
- **Status History** – View history of device in relation to enrollment status.

**Using Wipe Protection**

By configuring Wipe Protection settings, you can exert more control over how and when devices can be wiped. Using this feature, you can avoid mass wiping devices. Begin by setting a device threshold limit and amount of time in minutes.

When the threshold you specify is exceeded in the set amount of time, all subsequent wipe commands are put on hold and you and other administrators can optionally be notified. From here you can view wipe logs to see when devices were wiped and for what reason. After reviewing the information you can accept or reject the on-hold wipe commands and unlock the system to reset the device threshold counter.

**Configuring Wipe Protection Settings**

Set a device threshold limit and amount of time in minutes. When the threshold you specify is exceeded in the set amount of time, all subsequent wipe commands are put on hold and you and other administrators can optionally be notified.

**NOTE:** You can only configure these settings at the Global or Customer level Organization Group.
1. Navigate to Groups & Settings > All Settings > Devices & Users > Advanced > Wipe Protection.
2. Enter the number of Wiped Devices that will act as your threshold for triggering wipe protection.
3. Enter the value for Within (minutes) which is the set amount of time the wipes must occur in to trigger wipe protection.
4. Select a message template to email to administrators.
   Create a message template for wipe protection by navigating to Devices & Users > General > Message Templates, adding a new template and selecting Device Lifecycle as the Category and Wipe Protection Notification as the Type.
   You can use the following lookup values as part of your message template:
   - {EnterpriseWipeInterval} – The value of Within (minutes) on the settings page.
   - {WipeLogConsolePage} – A link to the Wipe Log page.
5. Enter the email addresses of administrators who should receive this notification message.
   You should only notify administrators who have access to the Wipe Log page.
6. Select Save.

**Viewing Log Wipes**
If the device threshold limit is exceeded within the specified timeframe, then you can view the Wipe Log page to see when devices were wiped and for what reason. After reviewing the information you can accept or reject any on-hold wipe commands and unlock the system to reset the device threshold counter.
NOTE: If the system is locked then you will see a banner at the top of the page indicating this status.

1. Navigate to Devices > Lifecycle > Wipe Log.
   Access to this page is managed by the Report Device Wipe Log resource and is available by default for system admins, SaaS admins, and AirWatch admins. You can add it to any custom admin role using the Roles page.

2. View the list of devices and determine whether these are valid wipes.
   Devices pending action will have a status of On Hold.
   If they are, then select each device and then select Approve wipe(s) from the command list. The status will change to Approved.
   If they are not, then select each device and then select Reject wipe(s) from the command list. The status will change to Rejected.

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

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

3. Select Unlock System from the top of the page.
   You can only perform this action at a Global or Customer level Organization Group.
Utilizing Reports

AirWatch has extensive reporting capabilities that provide administrators with actionable, result-driven statistics about their device fleets. IT administrators can leverage these pre-defined reports or create custom reports based on specific devices, User Groups, date ranges, or file preferences. The administrator can also 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 Admin Console.

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

Generating Custom Reports
Administrators can create custom reports on the fly using the Admin Console. To generate a custom report:

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

Adding a Report to My Reports
Adding a report to My Reports allows administrators to essentially “bookmark” popular reports that they 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, click the Actions icon on the right, and then click the Add to My Reports button in the Actions bar.
   From now on the report will be readily accessible from the My Reports view on the left side of the Reports page.

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 click the Subscribe button from Actions icon on the right.
3. Complete the Report Subscriptions Form with all required information.
   - General Information – The name of the subscription, the email subject, etc.
   - Report Parameters – The parameters defining the scope and options of the report.
   - Distribution List – The recipients who will receive the custom report whenever the subscription is executed.
   - Execution Schedule – The time and schedule at which the custom report is generated.
4. Select Save.

Additional Reporting Tools
There are also several other additional tools that help administrators 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.

**Using AirWatch Hub**

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

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

• **Devices** – View exact number of devices in terms of:
  - Status breakdown of all devices in terms of registered, enrolled, enterprise wipe pending, device wipe pending, and unenrolled.
  - Platform breakdown of devices enrolled in AirWatch.
  - Enrollment history over the past day, past week, and past month.

• **Compliance** – View which devices are violating compliance policies according to:
  - All compliance policies currently violated by devices, including apps, security settings, geolocation, and more.
- Top violated policies, covering all types of compliance policies established.
- Blacklisted Apps, including all blacklisted apps installed on devices, ranked by order of instances of violation.
- Devices without required apps, included apps that should be installed on a device that are uninstalled or are not yet installed.

- **Profiles** – View which profiles are out of date according to:
  - Latest Profile Version, including devices with old versions of each profile.

- **Apps** – View which applications are associated with devices, including:
  - Latest Application Version, including devices with old versions of each application.
  - Most Installed Apps, ranked in order of number of devices that have the application currently installed.

- **Content** – View devices with content that is out of date, according to:
  - Latest Content Version, including each file that is out of date ranked by order of instance.

- **Email** – View devices that are currently unable to receive email, according to:
  - Devices Blocked from E-mail, 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. Also view certificates that have already expired.

Toggle between views by selecting the list icon and graph 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.

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