Disclaimer

While AirWatch strives to provide some level of direction for customers in terms of initially implementing a Bring Your Own Device (BYOD) program, it is up to your organization's legal, human resources and management teams to create a device management program that is right for your organization. The scenarios and issues in this document are provided as examples and are not meant to act as official guidance or recommendations regarding device management or liability.

References in this document to any specific service provider, manufacturer, company, product, service, setting, or software do not constitute an endorsement or recommendation by AirWatch. Under no circumstances shall AirWatch be liable to you or any other person for any damages, including without limitation, any direct, indirect, incidental, special or consequential damages, expenses, costs, profits, lost savings or earnings, lost or corrupted data or other liability arising out of or related in any way to information, guidance or suggestions provided in this document.

Introduction to BYOD

Overview

Your organization can use AirWatch to secure employee-owned devices that have access to corporate resources as part of a Bring Your Own Device (BYOD) program. While BYOD programs offer benefits such as maximized employee productivity, reduced overhead costs, management flexibility and a simplified IT infrastructure, they also pose challenges. For example, you will need to balance the need for maximum security against an end user's privacy expectations. You also must ensure end users completely understand your MDM Terms of Use agreement and what data you will and won't collect. AirWatch MDM provides your organization's employees the privacy they need while maintaining the level of protection your corporate assets require. By asking employees to bring their own device and enabling those devices with corporate content, your organization gains the following valuable resources:

- **Management flexibility** – Eliminate the need to select and manage a provider and plan.
- **Higher level of confidence** – Allow employees to use one device for both business and personal purposes.
- **Maximized employee performance** – Allow employees to work with the device with which they are most comfortable.
- **Cost savings** – Reduce overhead costs in managing a corporate plan.
- **Simplified IT infrastructure** – Reduce the strain on IT help desks to support additional devices.

In This Guide

- Before You Begin – This section covers topics and prerequisites you should familiarize yourself with so you can get the most out of using this guide.
- BYOD Privacy Settings – Privacy is one of the biggest concerns for both administrators and end users when it comes to implementing a BYOD program. This section outlines how to configure the types of data AirWatch collects and displays.
- Terms of Use – Ensuring end users understand the extent of your BYOD program is important, and this section outlines creating and enforcing your own BYOD terms of use agreements.
- BYOD Enrollment – BYOD devices can be enrolled multiple ways, which can have an affect on how they're managed. This section covers how to enroll BYOD devices.
- BYOD Devices (Using the Workspace) – If your BYOD users will be using only the AirWatch Workspace application, then how you manage them will differ from if they were to also use the AirWatch Agent. This section explains what is supported within the AirWatch Workspace.
- BYOD Devices (Using the Agent) – If your BYOD users will be downloading the AirWatch Agent onto their devices you will have more management capabilities you can perform. This section outlines some of the more important considerations.
- Self-Service Portal Permissions – The Self-Service Portal (SSP) empowers BYOD users to troubleshoot their own issues and take matters into their own hands. Configuring SSP settings lets you define roles and decide what actions users can perform.

Before You Begin

Overview

This section covers topics and prerequisites you should familiarize yourself with so you can get the most out of using this guide.

In This Section

- Supported Platforms – See a list of supported devices that can be enrolled into BYOD with AirWatch.
- Recommended Reading – See a list of guides you can reference to better your understanding of how to manage BYOD with AirWatch.
- Getting Started – See additional considerations you should know before you begin.

Supported Platforms

AirWatch supports the following platforms as part of a BYOD program:

- 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

However, at this time the AirWatch Workspace application is only available for Android Gingerbread 2.3+ and iOS 5.0+.

Recommended Reading

- Mobile Device Management Guide – Provides a general overview of the AirWatch solution.
- AirWatch Workspace Guide – Explains how to set up and use the AirWatch Workspace application.
- Mobile Application Management Guide – Gives details about how to deploy applications to your device fleet, including employee-owned devices.

Getting Started

Before reading this guide it is beneficial if you are aware of the AirWatch Workspace and its capabilities. AirWatch Workspace enables you to provide specific corporate resources to segments of BYOD users. For example, some users may only want access to corporate email, while others may only require access to a single enterprise app. With AirWatch Workspace, your BYOD users can enroll in AirWatch and securely access containerized business applications and resources without receiving the same AirWatch MDM profile corporate-owned devices receive. AirWatch Workspace addresses privacy concerns users have about MDM by only giving administrators the ability to control managed enterprise apps instead of the entire device. See the BYOD Enrollment section for more information about the differences between Workspace-based and Agent-based enrollment.

Note: For more information about configuring the AirWatch Workspace, refer to the **AirWatch Workspace Guide**.

BYOD Privacy Settings

Overview

One of the biggest concerns for many BYOD end users is the privacy of the personal content on their devices. Your organization must be able to assure employees their personal data cannot be threatened by any management actions and is not subject to corporate oversight. With AirWatch MDM, you can help ensure the privacy of personal data by creating privacy policies that do not collect personal data and customizing them based on device ownership type. In addition, you can define granular privacy settings to disable the collection of the personally identifiable information and disallow certain remote actions for employee-owned devices to ensure employee privacy.

Note: Certain jurisdictions and countries have their own rules, laws, and regulations of what can be collected from end users. These should be thoroughly researched before configuring your BYOD privacy policies.

In This Section

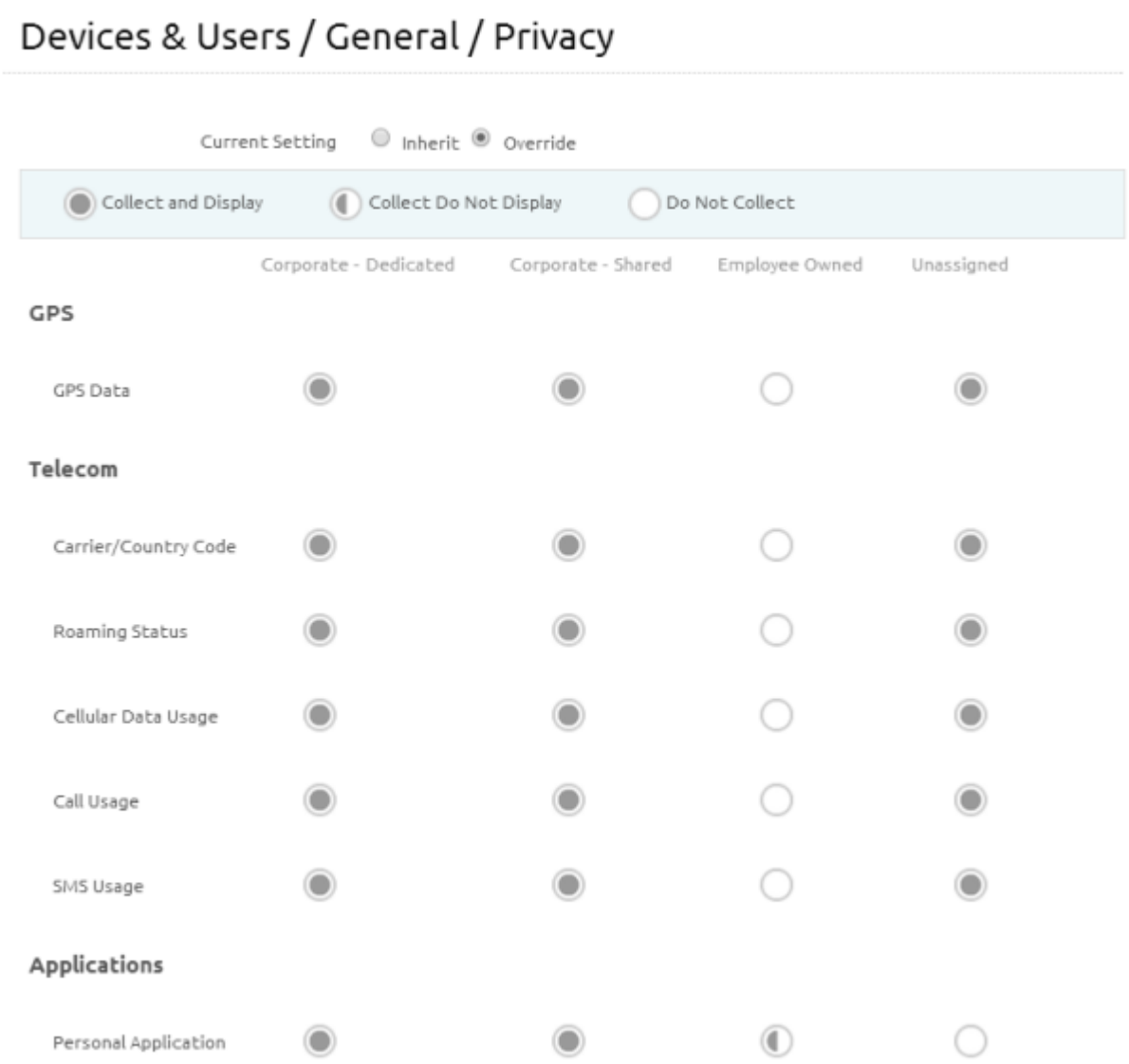
- Configuring Privacy Settings – Covers the various privacy options available in the AirWatch Admin Console.

Configuring Privacy Settings

Configure Privacy Settings to define how device and user information is 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. 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 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.

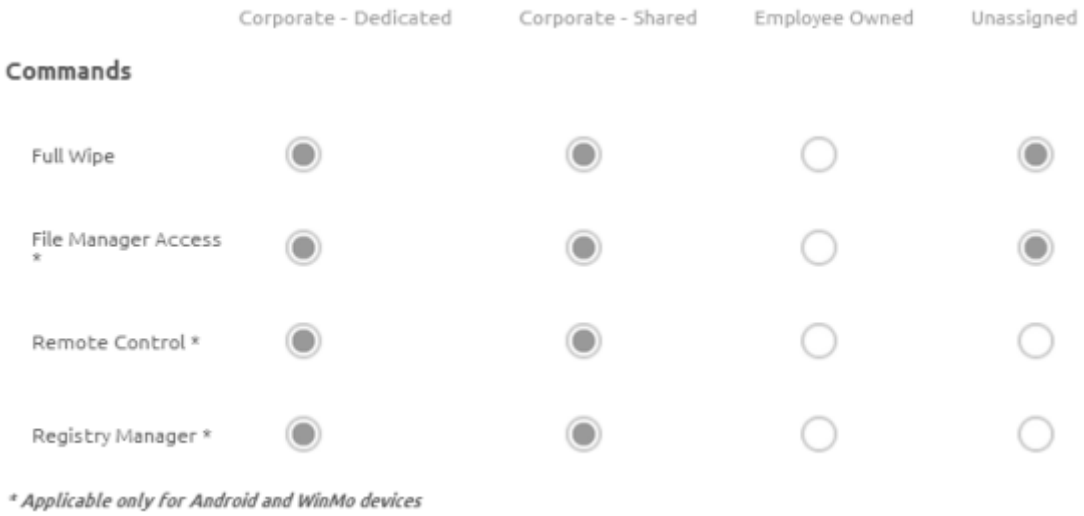


For more information on privacy within AirWatch, see recommended best practices.

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

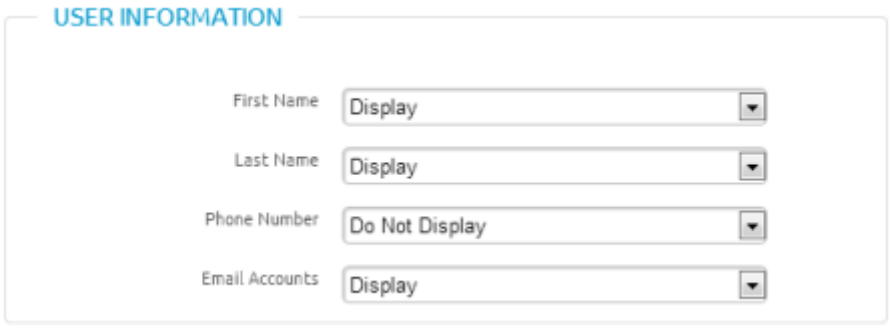
   Consider disabling all remote commands for employee-owned devices – especially full wipe. This prevents inadvertent deletion or wiping of an end user's personal content.

   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 AirWatch Admin Console information for **First Name, Last Name, Phone Number**, and **Email Accounts**.

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



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

5. Click **Save** when finished.

Terms of Use

Overview

For legal and liability reasons it is important to inform employees who use their own devices about the data that is captured and the actions that are allowed on them when enrolled in AirWatch MDM. You can do this by creating Terms of Use agreements in the AirWatch Admin Console, which users are prompted to read and accept before enabling MDM on their personal devices. By assigning Terms of Use agreements based on ownership type, you can create and distribute different agreements for corporate and BYOD users.

Creating your Terms of Use

Your organization's legal team should carefully consider how to tailor your Terms of Use for personal devices. A common practice is to reference a more extensive document hosted elsewhere, which details your legal agreements at length. However, a few items you might want to include in the Terms of Use agreement are:

- Highlight key MDM allowances (such as administrator permissions).
- Address user obligations in the event of a lost or stolen device.
- List the devices (platforms, operating systems, versions) you will allow to have access to corporate resources.
- Define the corporate resources (email and calendars, for example) that users can access via their personal devices.
- Acknowledge that the device will be enabled with proprietary corporate data and is subject to enterprise security policies regarding sensitive information. For example, you may want to include details such as a passcode profile you create that sets a maximum number of failed passcode attempts before a device is wiped.
- Detail any inappropriate behaviors that will not be tolerated per your normal business standards, such as using the device to harass others.
- Outline the reimbursement policies for telecom and other costs. For example, whether you have a stipend program for telecom usage, the cost of apps (personal vs. work-related), and roaming charges.

Note: One option is to take any Terms of Use employees sign for computer usage/access and tailor that to BYOD by mentioning specifically what information is collected.

Disseminating the Terms of Use

After your organization has written its Terms of Use agreement, consider giving it to end users in a one to two-page whitepaper form that omits legalese. This will not be the official Terms of Use end users agree to, but instead serve as a document they can read to better understand what using their own devices means. Ideally, end users should not be seeing the Terms of Use for employee-owned devices for the first time when they enroll their device. Consider being upfront about what end-user information you will collect and how your BYOD program will affect them.

In This Section

- Configuring Terms of Use – Details how to customize Terms of Use presented to users upon enrolling their device, logging into the AirWatch Admin Console and using applications.

Configuring Terms of Use

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

Creating Enrollment Terms of Use

The Terms of Use displays during each device's enrollment. Set Terms of Use version numbers, set platforms to receive the Terms of Use (all, multiple or one at a time), set to notify users by email if the Terms of Use is updated and create language-specific copies of the Terms of Use. You can create multiple Terms of Use agreements and assign them to Organization Groups based on ownership type or platform. This lets you tailor each agreement to meet the legal and liability requirements of specific groups, including users enrolled in your BYOD program.

1. Ensure your current active Organization Group is the one for which you would like to create terms of use.
2. Navigate to **Devices ▶Settings ▶Devices & Users ▶General ▶Enrollment** and select the **Terms of Use** tab.
3. Select **Add New Enrollment Terms of Use** to access the **Create New Terms of Use** text editor.
4. Set the Terms of Use to trigger depending on platform type by toggling the **Platforms** option from **Any** to **Selected Platform** and checking each desired platform.
5. Set the Terms of Use to trigger depending on ownership type by toggling the **Device Ownership** option from **Any** to **Selected Ownership Types** and checking each desired type of ownership.
6. 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. This is where you may want to mention any specific privacy settings and any applicable restrictions or compliance policies.
7. Select **Save**.

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

Creating Application or Console Terms of Use

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

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

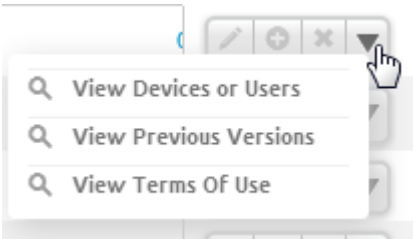
1. Navigate to **Groups & Settings ▶All Settings ▶System ▶Terms of Use**.
2. Select **Add Terms of Use** to access the **Create New Terms of Use** text editor.
3. Enter a **Name** for the Terms of Use and select the **Type**, which can be **Console**, **Enrollment** or **Application**.
4. Configure settings 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.

View Terms of Use Acceptance

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

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



- **View Devices or Users** – Display a complete list of devices and their acceptance statuses. You can filter by Organization Group.
- **View Previous Versions** – View previous iterations of the agreement.
- **View Terms of Use** – View the Terms of Use agreement.

Tracking Terms of Use Acceptance via Reports

Track user acceptance for each Terms of Use by accessing the **Hub ▶Reports & Analytics ▶Reports ▶List View** page and generating the **Terms of Use Acceptance Detail** report. View details regarding specific Organization Groups and drill down to view AirWatch Admin Console acceptances or Device Enrollment acceptances. View the acceptances directly in the Admin Console or export the report in one of a variety of file types, including XML, CSV, PDF, MHTML, Excel, Word and TIFF.

Note: AirWatch does not provide suggested legal text, therefore we do not provide sample or default Terms of Use text.

BYOD Enrollment

Overview

A major challenge in managing employees' personal devices is recognizing and distinguishing employee-owned devices and limiting enrollment to only approved devices. AirWatch helps address end-user concerns about privacy and administrator concerns about security by providing two types of enrollment for BYOD users, which are outlined below.

Enrollment Considerations

AirWatch enables you to configure a variety of options that customize the end-user experience of enrolling a personal device. Before you begin, however, you need to consider how you plan to manage employee-owned devices. For example, are you:

- Allowing employee-owned devices to enroll through the AirWatch Workspace app or requiring them to enroll through the AirWatch MDM Agent?
- Allowing employees who enroll their own devices to select their Group ID and/or ownership type? Or will you manually add corporate-owned whitelisted devices, then automatically setting all other devices that enroll to employee-owned?
- Allowing or blocking certain platforms or operating systems based on your organization's security requirements?

The following sections detail these considerations and will help you determine the best enrollment configuration for your environment.

In This Section

- Workspace vs. Agent-based Enrollment – Compare the differences between Workspace vs. Agent-based enrollment.
- Configuring Device Ownership – Ensure that employee-owned devices receive the proper Ownership Type in the AirWatch Admin Console.
- Configuring Enrollment Restrictions – Restrict enrollment to specific devices based on various parameters.

Workspace vs. Agent-based Enrollment

BYOD users can enroll their devices via either the AirWatch Workspace app or the AirWatch MDM Agent app, both of which can be downloaded from the iOS or Android app stores. The differences between the two are outlined below:

- **Workspace-based enrollment** takes place when an end user enrolls through the AirWatch Workspace app, which means they do not receive an MDM profile on their device. You can think of this as a containerized approach, as opposed to true MDM. Those with supported platforms will still have access to email, content, and apps, but certain other settings, such as Wi-Fi and VPN profiles, and remote actions, such as full device wipes, are not supported with

this method. For more information about what security features and functionality are supported, see the Configuring BYOD Devices (Workspace) section and the **AirWatch Workspace Guide**.

- **Agent-based enrollment** follows the same enrollment process corporate-owned devices use with the AirWatch MDM Agent and lets you deploy corporate accounts, profiles, apps, and content based on the ownership type identified during enrollment. You can think of this as true MDM, since it installs an MDM profile on the device and allows you to perform more device management functions.

For deployments where you might want to fully manage some BYOD users while selectively managing others, these two enrollment methods can be combined to form a **hybrid approach**. Using a hybrid approach, you can manage some BYOD users under MDM (using the AirWatch Agent), which gives full access to internal resources, and others under the containerized method (using the AirWatch Workspace), which selectively gives access to content, apps, email, etc. on an individual basis.

Note: While you can install the AirWatch Workspace and AirWatch Agent together on the same device, the apps are mutually exclusive. The user will be prompted to unenroll from the one before enrolling into the other.

Enrollment Flow

With Workspace-based enrollment, the end user:

- Will download the **AirWatchWorkspace** app and launch it to perform enrollment using either their work email address (for auto discovery) or their credentials, server URL, and Group ID.
- Will access AirWatch apps, wrapped apps, and other internal apps, from the AirWatch Workspace application.

With Agent-based enrollment, the end user:

- Will download the **AirWatch MDM Agent** app (or navigate to **awmdm.com** for simplified enrollment) and launch it to perform enrollment using either a work email address (for auto discovery) or credentials, server URL, and Group ID.
- Will access AirWatch apps, deployed internal apps, etc. from the native device launch screens.

Configuring Device Ownership

Every device enrolled into AirWatch MDM, either via the Agent or the Workspace app, has an assigned device ownership type: corporate dedicated, corporate shared or employee-owned. Employees' personal devices fall under the employee-owned type and are subject to the specific privacy settings and restrictions you configure for that type.

For both Workspace-based and Agent-based enrollment, you have the following options:

- Upload a list of corporate devices and configure AirWatch to apply a default ownership type during enrollment. **(Recommended)**
- Allow users to choose the appropriate ownership type themselves.

Upload a List of Corporate Devices and Specify Default Device Ownership

You can identify a set list of your organization's corporate devices, which is useful if you have a mix of corporate-owned devices that you give to certain employees *and* employee-owned devices that employees are allowed to enroll themselves. As devices are enrolled, those you identified as corporate-owned as part of a pre-approved list will

automatically have their ownership type configured based on the ownership type you selected for the list (either Corporate Owned or Corporate Shared). Then you can configure all other devices, which would only be end-user personal devices, to automatically have their ownership type set as Employee Owned.

1. Navigate to **Devices ▶Lifecycle ▶Enrollment Status** and select **Add**, then **Batch Import**.

   Alternatively, you can select **Whitelisted Devices** to enter up to 30 whitelisted devices at a time by IMEI, UDID or Serial Number. Additionally, select either **Corporate Owned** or **Corporate Shared** as the Ownership Type.

2. Enter a **Batch Name** and **Batch Description**, then select **Add Whitelisted Device** as the **Batch Type**.

3. Click **Choose File** to upload a file or select the Information icon to download a sample template. If saving a template, proceed to fill out the necessary information.

4. Click **Save**.

From here, you can either set the **Default Device Ownership** type to Employee Owned, or you can create a restriction that only allows Employee Owned as the ownership type during open enrollment. This ensures any device enrolling into this applicable Organization Group will be Employee Owned by default. However, this does not mean corporate devices will then display as Employee Owned, since those devices will be updated post-enrollment to reflect their Corporate Owned ownership type status.

To set the default ownership type as Employee Owned:

1. Navigate to **Devices ▶Settings ▶Devices & Users ▶General ▶Enrollment**. Click the **Grouping** tab.

2. Select **Employee Owned** as the **Default Device Ownership**.

3. Select the **Default Role** assigned to enrolled users, which will determine the level of access the user has to the Self-Service Portal.

4. Select the **Default Action** for **Inactive Users**, which determines what to do if the user is marked as inactive.

5. Click **Save**.

Prompt Users to Identify Ownership Type

If your organization has Organization Groups with multiple ownership types, such as a mix of corporate and employee-owned, you can prompt users to identify their ownership type during enrollment. You can always update the ownership type later, if necessary.

1. Navigate to **Devices ▶Settings ▶Devices & Users ▶General ▶Enrollment**. Click the **Optional Prompt** tab.

2. Select **Prompt for Device Ownership Type**. During enrollment, users will be prompted to select their ownership type.

3. Click **Save**.

While simple, this approach assumes every user will select the appropriate ownership type that applies to their device. If a user with a personal device chooses the Corporate-Owned ownership type, their device will be subject to a number of policies and profiles that normally would not affect an employee-owned device. This can have serious legal implications regarding user privacy. While you can always update the ownership type later, if necessary, it is safer and more secure to instead identify a list of corporate devices and then set the default ownership type to Employee Owned.

Configuring Enrollment Restrictions

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

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

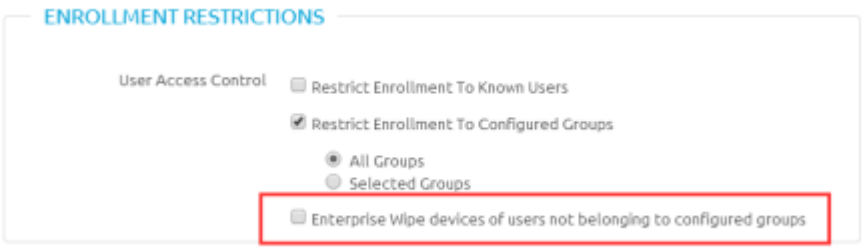
Enrollment Restrictions

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

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

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

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



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

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

Leave this option unchecked to allow all directory users to create new AirWatch user accounts during enrollment.

Policy Settings

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

   Note: You can also block specific devices based on their IMEI, Serial Number or UDID by navigating to **Devices ▶ Lifecycle ▶Enrollment Status** and selecting **Add**. This is an effective way to block a single device and prevent it from re-enrolling without affecting other users' devices. Preventing re-enrollment is also available as an option when performing an Enterprise Wipe.
7. 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.
8. Use the **Group Assignment Settings** section (scroll past the **Policy Settings** section) to assign customized policies to user groups. Set the rank of precedence and select a policy for each user group. This can be particularly useful if you are integrating with directory services.
9. Select **Save**.

BYOD Devices (Using the Workspace)

Overview

This section details configuring BYOD devices that are enrolled through the AirWatch Workspace. As described in BYOD Enrollment, Workspace-based enrollment does *not* install an MDM profile on the device and therefore limits the overall level of management you have. These settings and features are split into two types: automatic and configurable. Automatic items are enabled at all times and streamline the tracking and access features of the AirWatch Workspace. Configurable items provide specific options to custom-tailor your AirWatch Workspace deployment according to your organization's needs.

For more information on the features listed below please refer to the **AirWatch Workspace Guide**.

In This Section

- Automatic Features – See a list of features that require no prior setup or configuration.
- Configurable Features – See a list of features you can customize to meet your organization's needs.

Automatic Features

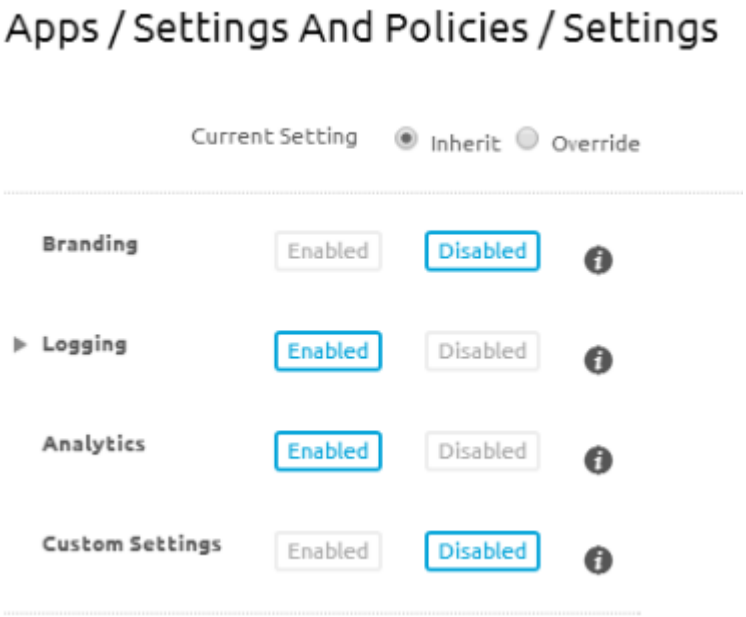
Automatic features require no additional setup or configuration and work as soon as you download and start using the AirWatch Workspace app.

Feature	Description
Secure	
Encryption	All corporate data within the Workspace is secured with FIPS 140-2 encryption. Encryption is supported at an application level only; all data within the app is encrypted, but full device encryption or SD card encryption cannot be enforced. This is because enterprise data is contained only in AirWatch apps. These apps do not allow enterprise data to be exported outside of the Workspace.
Apps	
App Tracking	AirWatch Workspace only tracks enterprise apps that are installed.
App Security	Application security and compliance is enforced for Workspace-enabled apps.
Asset Tracking	
Asset Tracking	Only device platform, model and OS are tracked.
Location	Location data is not tracked.
Support	

Feature	Description
Notifications	Push notifications from the AirWatch Admin Console to the Workspace.

Configurable Features

Configurable features can be controlled via **Settings and Policies** in the AirWatch Admin Console.



Feature	Description
Secure	
Passcode Policy	Containerized AirWatch apps within AirWatch Workspace leverage Single Sign On (SSO) to share the same SSO Passcode across applications. Configure SSO Passcode complexity in the AirWatch Admin Console. This SSO Passcode is set when the user initially enrolls using their username and password.
Compromised Detection	Compromised device detection is supported to control access to enterprise apps. A compromised device check occurs when an AirWatch is launched. If the app detects that a device is compromised, the app wipes its data and blocks access.
Clear SSO Passcode	Clears the current passcode used to sign in to apps and prompts the user to enter a new one.
SSO Passcode Lock	Signs the user out of all active Workspace-enabled apps and requires them to insert their SSO Passcode to access them the next time they launch an app.
Enterprise Wipe	Performs an enterprise wipe on a Workspace-enabled device, which clears all enterprise data within AirWatch Workspace, and revokes all access the next time a user opens an enterprise app.
Configure	
Terms of Use	Generate a fully customizable and enforceable Terms of Use policy.

Feature	Description
(TOU)	
AirWatch Inbox	Email configuration through AirWatch Workspace is supported using only the AirWatch Inbox. Workspace integration is currently only available for the Android and iOS platforms.
Wi-Fi	Use Wi-Fi to connect devices to corporate networks, even if they are hidden, encrypted, or password protected. Available on Android. (7.1 HF6+)
Apps	
Deploying Apps/App Catalog	Internal, public/purchased, and web apps can all be deployed to the AirWatch Workspace. Certain limitations may apply for apps that are not app wrapped or integrated with the AirWatch SDK.
Branding	Outfit AirWatch Workspace-related menu options, backgrounds, and text format according to your organization's brand and aesthetic.
Single Sign On (SSO)	Single sign-on allows a user to access all Workspace-enabled applications with a single SSO Passcode without having to enter login credentials for each app. SSO may also allow access to SharePoint and external file shares.

BYOD Devices (Using the Agent)

Overview

This section details configuring BYOD devices that are enrolled through the AirWatch Agent. As described in BYOD Enrollment, Agent-based enrollment installs an MDM profile on the device and lets you manage employee-owned devices with the same level of MDM functionality you use for corporate ones.

Comprehensive security is an integral part of MDM, and AirWatch lets you maintain a high level of security for both employee-owned and corporate devices. In addition to providing full administrative visibility over the security status of a device, AirWatch also continuously works in the background and proactively alerts you to any potential issues. With flexible management options, you can deploy one set of security policies and restrictions to employee-owned devices while simultaneously provisioning a greater level of restrictions to corporate-dedicated devices.

In This Section

- Creating Restrictions for BYOD – Deploy restrictions profiles meant specifically for employee-owned devices.
- Defining Compliance Policies for BYOD – Create compliance policies that will apply to BYOD users.
- Managing Access to Corporate Resources – Ensure BYOD users can access the applications and content necessary to perform work.
- Reclaiming Corporate Data upon Employee Departure – Remove traces of corporate content from the device when an employee leaves your organization.

Creating Restrictions for BYOD

AirWatch offers a number of restriction profiles through over-the-air profile provisioning and a range of related custom settings. This enables you to set very tight restrictions for corporate-dedicated devices while applying looser restrictions to employee-owned devices. For example, while some restrictions prohibit the use of certain features on the device, such as the iTunes store or YouTube, these restrictions are not typically deployed to employee-owned devices. Instead, you can create security profiles and restrictions that increase the level of device security without having a negative impact on functionality. AirWatch includes the following options, which are excellent examples of restriction policies for BYOD devices:

- **Encrypted backups –** Protect all backups with data encryption for BYOD devices with access to corporate content.
- **Force fraud warning in supported browsers –** Require users to acknowledge all warnings issued by the browser when it detects a suspicious site.
- **Disable moving emails –** Prohibit the exposure of sensitive corporate data by disabling the ability to forward a corporate email to a personal account or open it in third party applications.
- **Platform-specific restrictions –** Each platform, most notably Android and iOS, have their own list of restrictions you can enforce. You should evaluate these individually to determine whether or not they would be appropriate to your organization's deployment. For example, evaluating specific end user's job functions and their level of access to

sensitive information. Some, like iOS restrictions limited to supervised devices, do not apply, since employee-owned devices will not be enrolled with Apple Configurator.

You can create security profiles and restrictions by navigating to **Devices ▶Profiles ▶List View** and selecting **Add**, then the appropriate platform. If you create profiles for employee-owned devices specifically, be sure to select it as the **Ownership** type on the **General** tab. For more information about creating security profiles and restrictions, refer to the specific platform guides and the **AirWatch Mobile Device Management Guide**.

Defining Compliance Policies for BYOD

In addition to provisioning device restrictions, you can use compliance policies to monitor the security status of all devices in your fleet and respond to any policy violations. AirWatch contains a robust and highly customizable compliance policy engine to help you create and enforce custom policies for employee-owned devices. For example, you can define specific rules for employee-owned devices and then configure escalating actions that occur over time, such as restricting access to corporate content, if they do not comply. For additional information on creating compliance policies, refer to the **AirWatch Mobile Device Management Guide**.

The following options are prime examples of compliance policies for employee-owned devices:

- **Encryption Enforcement –** Require full device and SD card encryption.
- **Passcode Policies –** Require that a passcode should be present and enforced. For example, you could apply a passcode policy for any devices that have access to corporate content. This provides hardware-level encryption and protects information in the event of a lost or stolen device. Note that if you decide to set a maximum number of failed attempts before a device is wiped, then you may want to explicitly inform the user of this in your Terms of Use agreement.
- **Compromised Detection –** Detect devices that have been modified to remove security limitations imposed by manufacturers. Such devices are known as “jailbroken” or “rooted” devices and are deemed compromised by AirWatch. Because of the security vulnerabilities these devices can be exposed to, it is recommended they not be granted access to corporate content. As soon as devices are detected as compromised, AirWatch can automatically remove access to all corporate content enabled through MDM.
- **MDM Terms of Use Acceptance –** Ensure users accept your Terms of Use agreement by performing escalating actions that increasingly restrict access to corporate content the longer users go without accepting.

You can create compliance policies by navigating to **Devices ▶Compliance Policies ▶List View** and selecting **Add**. If you create policies for employee-owned devices specifically, be sure to select it as the **Ownership** type on the **Assignment** tab. For more information about creating compliance policies, refer to the specific platform guides and the **AirWatch Mobile Device Management Guide**.

Managing Access to Corporate Resources

Ensuring employee-owned devices are secure should not come at the cost of convenience to employees. With AirWatch MDM you can provide convenient access to email, VPN, Wi-Fi, apps and content.

Provide Access to Email, VPN and Wi-Fi

By creating configuration profiles you can configure employee-owned devices to access and automatically authenticate email, VPN and Wi-Fi settings while they are enrolled in AirWatch MDM. Since these are managed profiles on the

devices, you can remove access to these resources at any time. To add configuration profiles, navigate to **Devices ► Profiles List View** and select **Add**, then the platform. Configure a single payload, such as email, VPN or Wi-Fi per profile. Ensure **Ownership** is set to **Employee Owned** under the **General** tab if this profile should only apply to employee-owned devices.

For more information about creating configuration profiles, refer to the specific platform guides and the **AirWatch Mobile Device Management Guide**.

Email Containerization

For employee-owned devices, you can utilize the NitroDesk TouchDown email client for iOS and Android or the AirWatch Inbox to further secure access to corporate email. These containerized solutions allow you to require a passcode to access email while not forcing end users to have a passcode to access their devices. It also provides additional separation between their personal and work-related content. Refer to the specific platform guides, the **AirWatch Inbox Guide** and the **AirWatch Mobile Email Management Guide** for more information.

Enable Secure Access to Internal Apps

In addition to deploying your organization's internal apps to your device fleet, AirWatch can filter which device types receive certain apps. For example, your organization may have certain proprietary apps that do not belong on personal devices. By leveraging device ownership types in AirWatch, you can protect sensitive applications from employee-owned devices. To modify application assignments, navigate to **Apps & Books ►Applications ►List View**, select the **Internal** tab, then select an application from the list. Click the **Assignment** tab and select or create a Smart Group. When creating or editing Smart Groups, you can modify the **Ownership** to include or exclude Employee Owned devices.

For more information about managing application access, refer to the **AirWatch Mobile Application Management Guide**.

Reclaiming Corporate Data upon Employee Departure

An essential aspect of your BYOD program is removing corporate content when an employee leaves or when a device is lost or stolen. With AirWatch you can easily perform an Enterprise Wipe on devices to remove all corporate content and access while leaving personal files and settings untouched. This command also un-enrolls the device from AirWatch and strips it of all content enabled through MDM. This includes email accounts, VPN settings, Wi-Fi profiles, and enterprise apps. Consider the following when an employee-owned device should no longer be a part of your BYOD program:

- To perform an Enterprise Wipe to ensure a device is fully unenrolled and no longer has access to content and settings enabled through MDM:
    1. Select the appropriate Organization Group, then navigate to **Devices ►List View** and search for and select a device from the list. The device details view displays, with a list of actions you can perform under the **More** drop-down in the top right.
    2. Select **Enterprise Wipe** . A confirmation screen displays asking you to confirm the action. Select **Prevent Re-Enrollment** if you wish to prevent this device from enrolling again. Enter a Security PIN if applicable and then select **Enterprise Wipe** to complete the action.
- AirWatch lets you decide how an Enterprise Wipe applies to public and purchased VPP applications that sit in a gray area between corporate and employee-owned devices. To require that an application be removed:
    1. Navigate to **Apps & Books ►Applications ►List View**, select whether to view Public, Internal, or Purchased apps, and click the app name from the list. The application screen displays. Click **Edit**.

2. For public apps, select the **Deployment** tab, if it displays. Check the **Remove on Unenroll** check box.

   For purchased VPP apps, check the **Remove on Unenroll** check box under the **Deployment** section.

   Note: Even if you opt to remove an app purchased through Apple's Volume Purchase Program, you cannot reclaim any redeemed licenses for that app if you used redemption codes for iOS 6 and earlier devices. This is because when installed, the app is associated to the user's App Store account. On the other hand, license codes used for iOS 7 and later devices can be redeemed. Refer to the **AirWatch Mobile Application Management Guide** for more details.

- While Enterprise Wipes may be appropriate for employee-owned devices, you may want to eliminate the chance of issuing a full device wipe on personal devices. To disable this command as an option for employee-owned devices:

  1. Navigate to **Devices ▶Settings ▶Devices & Users ▶General ▶Privacy**.
  2. Scroll down to the **Commands** section and under the **Employee Owned** column set **Full Wipe** to **Prevent**. Click **Save**.

Self-Service Portal (SSP) Permissions

Overview

The AirWatch Self-Service Portal (SSP) is a useful tool for end users that can help reduce the overall "hidden cost" of managing a BYOD deployment. By empowering and educating users on how to perform basic device management tasks, your organization may be able to reduce the overall amount of help desk tickets end users raise for support issues. By training your end users on how they can use the SSP, you give them the ability to investigate their own issues and fix problems themselves.

In This Section

- Performing Remote Actions – See the various remote actions you can perform on managed devices as an administrator.
- Viewing Tabs – See the various tabs users can utilize to view information about their devices.
- Defining User Roles – See how to define the user roles that determine who has access to the Self-Service Portal.

Performing Remote Actions

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

Note: For information on deploying, accessing and using the SSP, refer to the appropriate platform guides.

Here are some examples of information you can let end users view and actions you can allow them to perform:

The **Remote Actions** menu, if enabled, allows users to perform the following remote actions over-the-air to their selected devices:

- **Device Query –** Manually requests the device to send a comprehensive set of MDM information to the AirWatch Server.
- **Lock Device –** Locks the selected device so that an unauthorized user cannot access it. This feature is useful if the device is lost or stolen. If using AirWatch Workspace, it signs the end user out of Workspace-enabled apps and requires them to enter their PIN the next time they access them.
- **Clear Passcode –** Clears the passcode on the selected device and will prompt for a new passcode. This is useful if you forget your device passcode and are locked out of your device. If using AirWatch Workspace, it clears the PIN used to sign in to Workspace-enabled apps.
- **Device Wipe –** Wipes all data from the selected device, including all data, Email, profiles and MDM capabilities and returns the device to factory default settings. If using AirWatch Workspace, this remote command is not available.

- **Enterprise Wipe –** Wipes all corporate data from the selected device and removes the device from AirWatch MDM. All of the enterprise data contained on the device is removed, including MDM profiles, policies and internal applications. The device will return to the state it was in prior to the installation of AirWatch MDM.
- **Send Message –** Sends a message via email, phone notification or SMS to the device.
- **Find Device –** Plays an audible tone on the device in the event it is nearby but hard to locate.

Viewing Tabs

The following SSP **Tabs** let users view information about all devices enrolled under their user accounts:

- **Security** – This tab shows the following general security information about a particular device enrolled under your user account.
- **Compliance** – This tab shows the compliance status of the device, including the name and level of all compliance policies that apply to the device. It is important for end users to take note of these policies to ensure devices remain compliant and operate as intended.
- **Profiles** – This tab shows all of the MDM profiles that have been sent to the devices enrolled under your user account and the status of each profile.
- **Apps** – This tab displays all applications that have been installed on the selected device and provides basic application information.
- **Event Log** – This tab contains a comprehensive log of all interactions between the AirWatch Admin Console and the device.
- **Support** – This tab contains detailed device information and contact information for your organization's support representatives.

Defining User Roles

By defining user roles on the **User Roles** page you can set who has access to the Self Service Portal (SSP) and what actions users who are logged in can perform. You can create multiple roles for different Organization Groups or change the user role for a specific user at any time.

Define a User Role

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

1. Navigate to **Accounts ▶Users ▶Roles** and click **Add**. Enter a **Name** and **Description** for the new role.
2. Select from a list of options the level of access and control end users of this assigned role should have in the SSP.
3. Click **Save** when you are finished.

Configure a Default Role

By configuring a default role you set the permissions and privileges users will automatically receive upon enrollment.

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

Set a Role for a Specific User

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

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