Introduction to the Enrollment Processes Guide

Overview

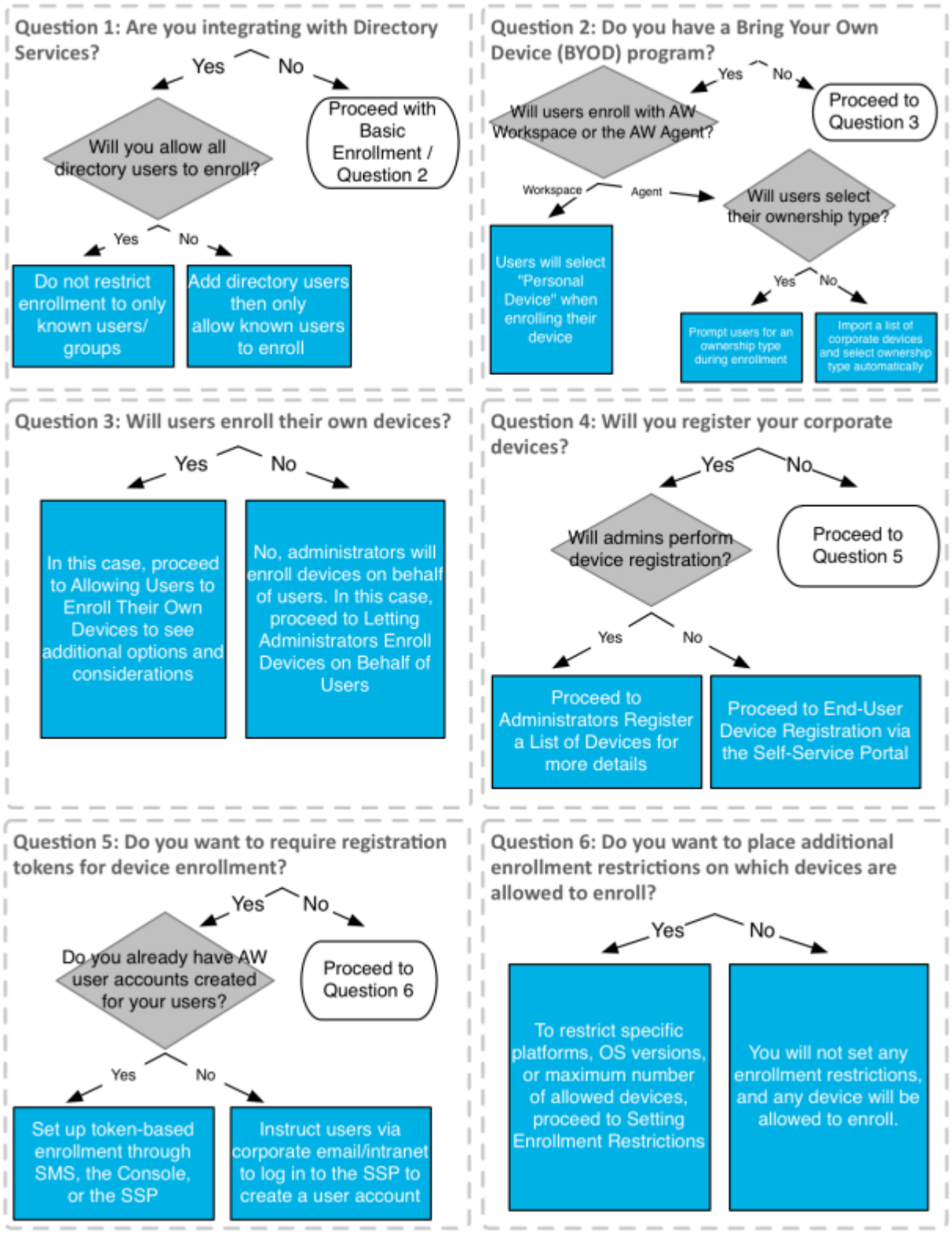
AirWatch provides multiple options for creating users and enrolling devices. This walkthrough outlines some of these combinations and walks you through choosing an appropriate method that best suits your organization's needs. It is not intended to be a comprehensive list of every enrollment option, but rather to help you think about which enrollment options you may want to consider.

Each section in this document corresponds to a specific question you answer, and within these sections you will find additional considerations along with question prompts to help you decide which enrollment options to use.

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.
- Q1: Are you integrating with directory services? – If your organization has a directory services infrastructure, you can leverage its existing users and groups in AirWatch.
- Q2: Do you have a Bring Your Own Device (BYOD) program? – If you support employee-owned devices as part of a BYOD program, then you will need to consider various enrollment options, including the AirWatch Workspace vs. the AirWatch MDM Agent.
- Q3: Will users enroll their own devices, or will administrators enroll devices on behalf of users? – AirWatch supports two methods for enrolling corporate devices. You can let users enroll their own devices, or administrators can enroll devices on users' behalf in a process called device staging.
- Q4: Will you register your corporate devices? – Registering corporate devices before they are provisioned and enrolled into AirWatch is an optional process. The main benefit of this is being able to restrict enrollment to registered devices only.
- Q5: Do you want to require registration tokens for device enrollment? – If you restrict enrollment to registered devices only, you also have the option of requiring a registration token to be used for enrollment.
- Q6: Do you want to place additional enrollment restrictions on which devices are allowed to enroll? – Applying additional enrollment restrictions is applicable to any deployment, regardless of directory services integration, BYOD support, device registration, or other setups.

To help you get started, refer to the flow chart below, which is broken down by each question you should answer.



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 bring your own device (BYOD) with AirWatch.
- Requirements – See a list of requirements you should fulfill before proceeding with this guide.
- Recommended Reading – See a list of guides you can reference to better understand various aspects of enrollment with AirWatch.
- Getting Started – See additional considerations you should know before you begin.

Supported Platforms

The procedures outlined in this document apply to all of AirWatch's supported device platforms unless specifically noted. You can locate a specific platform's enrollment instructions in the applicable platform guides.

Requirements

- To use directory-service based enrollment you will first need to integrate your directory service with AirWatch.

Recommended Reading

- AirWatch Mobile Device Management Guide – This guide provides a general overview of enrollment.
- AirWatch Directory Services Guide – This guide details how to integrate your directory service with AirWatch, which is required if you want users to use their directory service credentials during enrollment.
- AirWatch Workspace Guide – This guide highlights the AirWatch Workspace application, including how to enroll a device using the Workspace.
- AirWatch Integration with Apple Configurator – This guide details how AirWatch integrates with Apple Configurator. Administrators can use Apple Configurator to bulk enroll devices.
- AirWatch Shared Device Guide – This guide explains how to configure your environment to support the shared device feature, which lets multiple users share a single device. For enrollment purposes, administrators can stage a device for use by multiple users.

Getting Started

As mentioned in the introduction, this document is designed to get you thinking about which enrollment options you may want to consider for your deployment. Each section in this document corresponds to a specific question you answer, and within these sections you will find additional considerations along with question prompts to help you decide which enrollment options to use. It is helpful if you already have a list of questions or considerations you would like to address, such as who will enroll devices, whether you will support BYOD devices, or what types of device restrictions you would like to enforce.

Question One: Are you Integrating With Directory Services?

Overview

The first question you need to consider is whether or not you plan to integrate with existing Lightweight Directory Access Protocol (LDAP)-based directory services such as Active Directory (AD), Lotus Domino and Novell e-Directory. If your organization has a directory services infrastructure, you can leverage its existing users and groups in AirWatch.

If you do not have an existing directory services infrastructure or you choose not to integrate with it, you will need to perform Basic Enrollment by manually creating AirWatch user accounts.

Note: While AirWatch supports a mix of both Basic and Directory-based users, you typically will use one or the other for the initial mass enrollment of users and devices.

In This Section

- Pros and Cons – See the pros and cons of both the basic and directory service-based enrollment options.
- Enabling Basic Enrollment – See how to add basic users directly into the AirWatch Admin Console.
- Enabling Directory Service-Based Enrollment – See how to add existing users that are part of your directory service into AirWatch.

Pros and Cons

Basic Enrollment

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

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

Directory Service Enrollment

Directory service-based authentication is utilized to integrate user and admin accounts of AirWatch with existing corporate accounts.

- **Pros** – End users authenticate with existing corporate credentials. Ability to automatically detect and sync changes from the directory system into AirWatch. Secure method of integrating with your existing directory service. Standard integration practice. In SaaS deployments using the AirWatch Cloud Connector (ACC), it requires no

firewall changes and offers a secure configuration to other infrastructure, such as Microsoft ADCS, SCEP and SMTP servers.

- **Cons –** Requires an existing directory service infrastructure. For SaaS deployments, it requires additional configuration because the ACC must be installed behind the firewall or in a DMZ.

If you answered **Yes** to "Are you integrating with Directory Services?", or you want to see questions you will want to consider before integrating AirWatch with your directory services, proceed to Enabling Directory Service-Based Enrollment on page 8.

If you answered **No**, proceed to Enabling Basic Enrollment on page 7.

Enabling Basic Enrollment

Basic Enrollment refers to the process of manually creating user accounts and user groups in AirWatch for each of your organization's users. If your organization is not integrating AirWatch with a directory service, this is how you will create user accounts. You can easily do this by filling out and uploading .csv template files that contain all user information.

Creating Users and/or Devices in Bulk

To save the time and effort of uploading individual user account details, you can upload users in bulk through the batch import feature using the following step-by-step instructions:

1. Navigate to **Accounts ▶Users ▶Batch Status** and select **Batch Import**.
2. Enter the basic information including a **Batch Name** and **Batch Description** for reference in the AirWatch Admin Console.
3. Select the applicable batch type from the **Batch Type** drop-down menu.
4. Select the information icon () to access available templates. Then, choose the applicable template for your environment, click **Download Template and Example for this Batch Type** and save the .csv file somewhere accessible.
5. Open the .csv file, which has a number of columns corresponding to the fields that display on the Add / Edit User page. Columns with an asterisk are required and must be entered with data. The **GroupID** column corresponds to the **Enrollment Organization Group** field on the **Add / Edit User** page. This is the Organization Group in which the user will be enrolled if the **Group ID Assignment Mode** is set to **Default** in **Groups & Settings ▶All Settings ▶ Devices & Users ▶General ▶Enrollment** in the **Grouping** tab.

   Note: For directory-based enrollment, the **Security Type** for each user should be **Directory**.
6. Enter data for your organization's users, including device information if applicable and save the file.
7. Return to the Batch Import screen in the AirWatch Admin Console, select **Choose File** to locate and upload the saved comma-separated values (.csv) file.
8. Click **Save**.

Proceed to Question Two: Do You Have a Bring Your Own Device (BYOD) Program? on page 11.

Enabling Directory Service-Based Enrollment

Directory Service Enrollment refers to the process of integrating AirWatch with your organization's directory service infrastructure to automatically import users and, optionally, user groups such as security groups and distribution lists. When integrating with a directory service such as Active Directory (AD), you have a few options for how you will import your users.

- **Allow all directory users to enroll** – With this method, you allow all of your directory service users to enroll. In addition, you can set up your environment to auto discover users based on their email and create an AirWatch user account for them when they perform device enrollment.
- **Add users one by one** – After integrating with your directory service, you can add users one by one as you would if you were creating basic AirWatch user accounts. The only difference is you only need to enter their username and select **Check User** to auto populate remaining information from your directory service.
- **Batch upload a .csv file** – Using this option, you can import a list of directory services accounts in a .csv template file. This template file has very specific columns, some of which require data.
- **Integrate with user groups (Optional)** – With this method, you can use your existing user group memberships to assign profiles, apps, compliance policies, and so on. For more information, refer to the **AirWatch Directory Services Guide**.

Note: For information about how to integrate your AirWatch environment server with your directory service server and add users into the AirWatch Admin Console, refer to the **AirWatch Directory Services Integration Guide.** If you are considering integrating AirWatch with a SAML provider, refer to the **AirWatch SAML Integration Guide**.

Enrollment Considerations

With these options for adding users in mind, you will need to address the following considerations:

- **Consideration #1** – Will you allow all directory users to enroll or will you only allow certain directory users to enroll?
- **Consideration #2** – Will you automatically assign directory users to Organization Groups based on their directory service group assignment or allow them to select a Group ID from a list?

Consideration #1: Which Directory Users Can Enroll?

An important consideration to make when integrating your AirWatch environment with directory services is which users should be allowed to enroll. In answering this question, consider the following:

- Is the intent of your MDM deployment to manage devices for *all* of your organization's users at or below the base DN you configured? If so, the easiest way to achieve this is to allow all of your users to enroll by ensuring the Restrict Enrollment check boxes are *unchecked*.

  Note: You can choose to allow all of your users to enroll as part of your initial deployment rollout, and then after some period of time lock down enrollment to prevent unknown users from enrolling. As your organization adds new employees or members to existing user groups, these changes will be synced and merged with AirWatch and those users will be allowed to enroll.

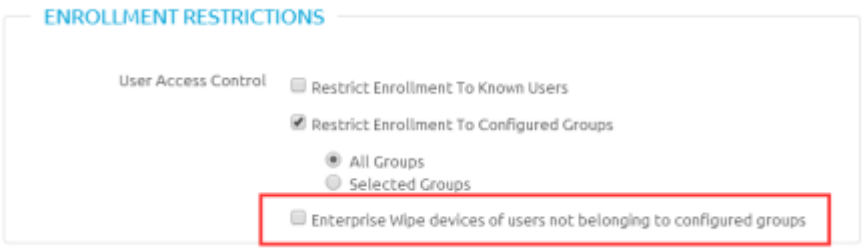
- Are there certain users or groups who should *not* be subject to MDM? If so, you will want to either add users one at a time or batch import a .csv file of only eligible users.

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.

Consideration #2: Where Will Users Be Assigned?

Another consideration to make when integrating your AirWatch environment with directory services is how you will assign directory users to Organization Groups upon device enrollment. In answering this question, consider the following:

- Have you created an Organization Group structure that logically maps to your directory service groups? You must do this before you can edit user group assignments.
- Are your users enrolling their own devices? If they are, the option to select a Group ID from a list is simple, but also subject to human error and can lead to incorrect group assignments.

You can automatically select a Group ID based on user group or allow users to select a Group ID from a list. These **Group ID Assignment Mode** options are available by navigating to **Devices ▶Settings ▶Devices & Users ▶General ▶ Enrollment** and selecting the **Grouping** tab:

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

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

Proceed to Question Two: Do You Have a Bring Your Own Device (BYOD) Program? on page 11

Question Two: Do You Have a Bring Your Own Device (BYOD) Program?

Overview

If you support employee-owned devices as part of a BYOD program, then you will need to consider certain enrollment options. A major challenge in managing users' personal devices is recognizing and distinguishing between employee-owned and corporate-owned devices and then limiting enrollment to only approved devices. For example, you can define device ownership types to facilitate more flexible device management and block specific device types to prevent unauthorized personal devices from having access to corporate content. Once enrolled, you can deploy corporate accounts, profiles, apps, and content based on the ownership type identified during enrollment.

If you answered **Yes** to "Will you allow BYOD enrollment?", or you want to see questions you will want to consider before committing to a BYOD program, proceed to Configuring Bring Your Own Device (BYOD) Enrollment on page 12

If you answered **No**, proceed to Question Three: Will Users Enroll Their Own Devices, or Will Administrators Enroll Devices on Behalf of Users? on page 15

Configuring Bring Your Own Device (BYOD) Enrollment

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 identify employee-owned devices in your deployment and whether to enforce enrollment restrictions for employee-owned devices.

- **Consideration #1** – Will users with employee-owned devices enroll using the AirWatch Workspace or the AirWatch MDM Agent?
- **Consideration #2** – Will you allow users to select their own device ownership type during enrollment or will you import corporate-owned devices and automatically set the ownership as Employee Owned?
- **Consideration #3** – Will you set additional enrollment restrictions, such as maximum number of devices and supported platforms for employee-owned devices?

Consideration #1: Will BYOD Users Enroll With the AirWatch Workspace App or the AirWatch MDM Agent?

AirWatch Workspace enables you to provide specific 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. Refer to the **AirWatch BYOD Guide** 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**.

Consideration #2: How Will You Specify Ownership Type?

Every device enrolled into AirWatch has an assigned device ownership type: Corporate Dedicated, Corporate Shared or Employee Owned. Employees' personal devices would fall under the Employee Owned type and be subject to the specific privacy settings and restrictions you configure for that type. An important consideration to make when managing a BYOD program with AirWatch is how to ensure each and every device has the correct device ownership type. In answering this question, consider the following:

- Do you have access to a master list of corporate devices that you can bulk upload into the AirWatch Admin Console? If so, you may consider uploading this list and setting the default ownership type to Employee Owned.
- Have you considered the legal implications of allowing users to select an ownership type from a list? For example, the ramifications if a user enrolls a personal device, incorrectly selects corporate owned as the ownership type, violates a policy and subsequently has a device fully wiped.

For your BYOD program, you can configure AirWatch to apply a default ownership type during enrollment *or* allow users to choose the appropriate ownership type themselves.

Identify Corporate Devices and Specify Default Device Ownership

You can identify a set list of your organization's corporate devices, which can be 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 have identified as Corporate-Owned will automatically have their

ownership type configured based on what you selected (Corporate-Owned or Corporate-Shared) at the time you created the list. Then you can configure all employee-owned devices – which are *not* in the list – that enroll to automatically have their ownership type set as Employee-Owned.

Note: The procedure below explains how to import a list of pre-approved corporate devices and automatically apply the Corporate-Owned ownership type after enrollment, even if you have a restriction that automatically applies the Employee-Owned ownership type. Enrollment restrictions for open enrollment, on the other hand, explicitly allow or block enrollment for those devices matching specific parameters you identify, such as platform, model or operating system. For more information on enrollment restrictions, see the next consideration.

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

   You can also select **Whitelisted Devices** to enter up to 30 whitelisted devices at a time by IMEI, UDID or Serial Number. You would also 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. Select **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. Select **Save**.

From here, you can set the **Default Device Ownership** type to Employee Owned for all open enrollment using the following step-by-step instructions:

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

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

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

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

5. Select **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.

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

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

3. Select **Save**.

While simple, this approach assumes every user will correctly 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 now 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.

Consideration #3: Will You Apply Additional Enrollment Restrictions for Employee-Owned Devices?

Another consideration to make when managing a BYOD program with AirWatch is if you will apply additional enrollment restrictions for employee-owned devices. When answering this question, consider the following:

- Does your MDM deployment only support certain device platforms? If so, you can specify these platforms and only allow devices running on them to enroll.
- Will you limit the number of personal devices an employee is allowed to enroll? If so, you can specify the maximum number of devices a user is allowed to enroll.

You can set up additional enrollment restrictions to further control who can enroll and which device types are allowed. For example, you may choose to support only those Android devices that feature built-in enterprise management functionality. 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 these settings.

For more information about enrollment restrictions, see Question Six: Do You Want To Place Additional Enrollment Restrictions On Which Devices Are Allowed To Enroll? on page 27

Proceed to Question Three: Will Users Enroll Their Own Devices, or Will Administrators Enroll Devices on Behalf of Users? on page 15

Question Three: Will Users Enroll Their Own Devices, or Will Administrators Enroll Devices on Behalf of Users?

Overview

AirWatch supports two methods for enrolling corporate devices. You can let users enroll their own devices or administrators can enroll devices on users' behalf in a process called **device staging**. In this process, an administrator enrolls devices before assigning them and distributing them to end users. This method is particularly useful for administrators who need to set up devices that will be shared by multiple users across an organization (for example, in retail stores and schools).

In addition, device staging works well for newly provisioned devices, since it happens before an employee receives the device. Letting end users enroll their own devices makes the most sense if your end users already have corporate devices or if the total number of devices makes it impractical for administrators to perform device staging.

In This Section

- Allowing Users to Enroll Their Own Devices – See the enrollment options to consider if you will allow end users to enroll their own devices.
- Letting Administrators Enroll Devices on Behalf of Users – See the enrollment options to consider if you will have administrators enroll devices on end-users' behalf.

If you answered **Users will enroll their own devices**, or you want to see the different options for allowing users to enroll their own devices, proceed to Allowing Users to Enroll Their Own Devices on page 16

If you answered **Administrators will enroll devices on behalf of users**, or you want to see questions you will want to consider before utilizing device staging, proceed to Letting Administrators Enroll Devices on Behalf of Users on page 18

Allowing Users to Enroll Their Own Devices

An important consideration to make when deciding how devices will be enrolled is whether or not to allow users to enroll their own devices. In answering this question, consider the following:

- Do your end users already have assigned corporate devices? In this case, it may not be practical to collect each device and have it staged and instead have users enroll themselves.
- Will your end users be sharing devices or will they have their own dedicated devices? If end users are not sharing devices, then you can easily make it the responsibility of that device's single owner to enroll.
- Will you associate your organization's email domain with your AirWatch environment? This process, known as **auto discovery**, means end users will only need to enter their email address and credentials – the enrollment URL and Group ID are automatically entered.

The following enrollment workflows enable end users to enroll their own devices.

Standard Enrollment Process

In the Standard enrollment process, end users navigate to AWAgent.com, which automatically detects whether the AirWatch Agent is installed and redirects to the appropriate mobile app store if it is not. After launching the Agent, users enter their credentials – in addition to either an email address or URL/Group ID – and proceed with enrollment.

Note: AirWatch Workspace users will download the Workspace app from the app store.

Standard enrollment may require that end users know their appropriate Group ID and login credentials. If you have integrated with directory services, these credentials will be the same as the user's directory service credentials.

Single-Click Enrollment

In this workflow, which applies to web-based enrollment, an administrator sends an AirWatch-generated token to the user along with an enrollment link URL. The user only needs to select the provided link to authenticate and enroll the device. This is the easiest and fastest enrollment process for the end user and can be secured by setting expiration times.

Note: For more information, see Question Five: Do You Want To Require Registration Tokens For Device Enrollment? on page 24

Two-Factor Authentication

In this workflow, an administrator sends the same enrollment token generated by AirWatch, but the user must also enter their login credentials. This method is just as easy to execute as the Single-Click Enrollment but adds one additional level of security by requiring the user to enter their unique credentials.

Note: For more information, see Question Five: Do You Want To Require Registration Tokens For Device Enrollment? on page 24

End User Registration

In this workflow, an end user logs into the Self-Service Portal (SSP) and registers their own device. Once registration is complete, the system sends an email to the end user, including the enrollment URL and login credentials.

This workflow assumes administrators have not already performed device registration for a corporate device fleet. It also assumes you require corporate devices to be registered so administrators can track enrollment status and use a list of corporate devices in conjunction with a BYOD program.

Note: For more information, see Consideration: Who Will Register Devices? on page 22.

Proceed to Question Four: Will You Register Your Corporate Devices? on page 21

Letting Administrators Enroll Devices on Behalf of Users

Administrators can enroll devices on behalf of users in a process called **device staging**. You may do this to streamline the process of device registration, to enroll iOS devices that are shared by multiple users, or to provision a fleet of devices quickly with Apple Configurator. Note the following items you should consider when deciding how to perform device staging:

- **Consideration #1** – Does it make sense to perform device staging on your organization's corporate devices? Unless you are using Apple Configurator, administrators must stage devices one-by-one, so for particularly large deployments you will want to consider the time and staffing this will take. In addition, whereas administrators can easily stage new devices, if employees already have corporate-owned devices then they will need to be shipped in or collected on-site to have them staged.
- **Consideration #2** – Do you have an exclusively iOS deployment, or do you want to enforce the advanced security restrictions for iOS devices that Apple Configurator provides? If yes, then consider integrating your AirWatch environment with Apple Configurator. Note that certain limitations apply.

Consideration #1: Should You Utilize Device Staging?

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

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

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

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

Single-User Device Staging

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

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

   Single User Devices – Stages devices for a single user. Toggle the type of Single User device staging mode to either **Standard** or **Advanced**. Standard staging requires an end user to enter login information after staging, while Advanced means the staging user will enroll the device on behalf of another user.
3. Enroll the device using one of the two following methods:
   - Enroll via the AirWatch MDM Agent by entering a server URL and Group ID.
   - Open the device's Internet browser, navigate to the enrollment URL and enter the proper Group ID.

4. Enter your staging user's credentials during enrollment. If necessary, specify that you are staging for **Single User Devices**. You will only have to do this if Multi User device staging is also enabled for the staging user.
5. Complete enrollment for either Advanced or Standard staging:
    - If performing Advanced staging, you will be prompted to enter the username of the end-user device owner who will be using the device. Proceed with enrollment by installing the Mobile Device Management (MDM) profile and accepting all prompts and messages.
    - If performing Standard staging, then upon completing enrollment the end user will be prompted to enter their own credentials.

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

Multi-User Device Staging

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

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

    Multi User Devices – Stages devices for use by multiple users.
3. Open a device's Internet browser, navigate to the enrollment URL and enter the proper **Group ID**.
4. Complete enrollment and install the Mobile Device Management (MDM) profile by following the prompts. Once you are done, the Login/Logout screen displays and prompts any users of the device to check out the device to access the applications, settings and content for their Organization Group, which is assigned based on the **Group Assignment Mode** settings you specify under **Devices ▶Settings ▶Devices & Users ▶General ▶Shared Device**.

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

Note: Refer to the **AirWatch Shared Device Guide** for more information about the different Group Assignment Modes.

Consideration #2: Should You Use Apple Configurator?

Apple Configurator enables IT administrators to effectively deploy and manage Apple iOS devices. It is especially useful for organizations such as retail stores, classrooms or hospitals that want to pre-enroll devices that will be shared by multiple end users. Using Configurator to enroll pre-registered dedicated devices meant for use by a single user is also supported by adding serial number/IMEI information to a user's registered device in the AirWatch Admin Console. A major benefit of Apple Configurator is that you can use a USB hub or iOS device cart to provision multiple devices in minutes.

Note: For more information about Apple Configurator, including information about integrating with Apple Configurator, refer to the **AirWatch Integration with Apple Configurator** document.

Supervised Mode

Administrators have the option of enabling Supervised Mode for devices enrolled via Apple Configurator, which enables additional enhanced security features. However, this does introduce several limitations on the device.

Benefits

- Elevated Restrictions over MDM
  - Prevent User from Removing Applications*.
  - Disable iMessage.
  - Disable Game Center and iBookstore.
  - Set iBookstore Content rating restrictions.

    *Removing applications can also be restricted locally on the device using restrictions under System Configuration.
- Enhanced security
  - Prevent installation of certificates or unmanaged configuration profiles.
  - Force all device network traffic through a global HTTP proxy.
- Kiosk Mode
  - Lock down devices to one app with single app mode and disable the home button.
- Customize Wallpaper and Text on Device

Limitations

- USB Access to supervised devices is restricted to the supervising Mac.
- Cannot move data from and to the device via iTunes.
  - Media such as photos and videos cannot be copied from the device to a PC or Mac. To transfer this type of data, AirWatch recommends using the AirWatch Content Locker to sync the content with the user's Personal Documents section. Alternatively, a file sharing application can be used to transfer the data over WLAN/WWAN to a server.
- Supervised mode prevents access to device-side logs via iPhone Configuration Utility (IPCU).
  - This makes it harder to troubleshoot any application or device issues, because the logs from the device can only be obtained if the device is connected to the supervising Mac. To remediate some of the challenges, AirWatch recommends utilizing the AirWatch SDK to send crash logs and logistics from the applications to the AirWatch Console.
- Devices cannot be factory reset on the field.
  - Once a device is factory reset, it will need to be brought back to the supervising Mac to restore it back into supervised mode. This may be an issue if the Mac is not in close proximity to the device.

In deciding whether or not to enable Supervised Mode, consider the following. While it enables additional features that enhance security on the device, the USB limitations need to be considered. The proximity of the device to the supervising Mac should play an important role in the decisions. Since the USB limitation prevents access to device-side logs, a device experiencing issues will need to be shipped back to a depot and re-staged to restore functionality. It is important to decide on device supervision in advance, because the process to supervise or "unsupervise" will require the extra step of shipping a device to an IT location or depot.

Proceed to Question Four: Will You Register Your Corporate Devices? on page 21

Question Four: Will You Register Your Corporate Devices?

Overview

Registering corporate devices before they are provisioned and enrolled into AirWatch is an optional process. The main benefit of this is being able to restrict enrollment to registered devices only. This enables an option to require a registration token for enrollment, which helps ensure the secure authorization of each corporate device that enrolls.

Another benefit it provides is being able to track enrollment statuses. This lets you know which of your users have enrolled and which still need to enroll. You can then notify those users who have not yet enrolled.

If you answered **Yes** to "Will you register your corporate devices?", or you want to see questions you will want to consider before registering corporate devices, proceed to Enabling Device Registration on page 22

If you answered **No**, proceed to Question Six: Do You Want To Place Additional Enrollment Restrictions On Which Devices Are Allowed To Enroll? on page 27

Enabling Device Registration

Device registration is the process of adding corporate devices to the AirWatch Admin Console before they are enrolled. When making the decision whether or not to register your organization's corporate devices, consider the following:

- **Consideration** – Who will register the devices? Administrators can register devices in bulk before provisioning them to end users, or end users can be instructed to register their devices using the Self-Service Portal.

Consideration: Who Will Register Devices?

An important consideration to make when registering devices is deciding who will perform the actual device registration. In answering this question, consider the following:

- What is the total number of devices in your deployment? In particularly large deployments of thousands of devices, you may want to add this information to a .csv file to be uploaded before devices are provisioned or pass on the act of device registration onto the end user.
- Do you support a BYOD program where employees can use their personal devices? If you choose to restrict enrollment to only registered devices, you will need to give employees instructions on how to register their devices.

Administrators Register a List of Devices

1. Navigate to **Accounts ▶Users ▶List View**, select **Add** and then **Batch Import** to open the Batch Import Form.
2. Enter the basic information including a **Batch Name** and **Batch Description** for reference in the AirWatch Admin Console.
3. Select the information icon () to access available templates. Then, under Users And/Or Devices, select **Download Template and Example for this Batch Type** and save the .csv file.
4. Open the .csv file and enter all relevant information for each device in the template. Three sample users have been added to the top of the template for reference to the type of information to put into each column. To register a device, make sure that **column X (User Only Registration)** is set to **No**. To register an additional device to the same user account, make sure that all information in columns **A through W** is the same. The remaining columns are used to register each additional device. To store advanced registration information, make sure that **column AF (Store Advanced Device Info)** is set to **Yes**.
5. Save the completed template as a .csv file, return to the AirWatch Admin Console, select **Choose File** from the Batch Import Form and select the completed template.
6. Select **Save** to complete registration for all listed users and corresponding devices.

End-User Device Registration via the SSP

You may choose to have end users register their own devices before enrolling into AirWatch if you are supporting BYOD in your deployment and yet still require devices to be registered before they can enroll. You can also require users with corporate owned devices to register their devices if you want to track enrollment or utilize registration tokens. In either case, you will need to notify your end users of the process they will need to follow.

Note: The following instructions assume the end user has AirWatch credentials, either from directory services integration using their existing directory service credentials or from an AirWatch User Account that has already been activated. If you opted for an open enrollment with directory services without manually adding directory users, you will not have any user accounts already created for end users. In this case, if you want end users to be able to register

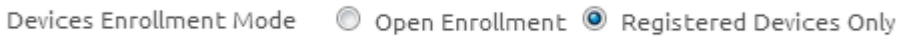
devices you will need to send an email or intranet notification to each user group outside of AirWatch with the registration instructions.

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

   If you enabled registration tokens for enrollment authentication, they will be sent to the user via the selected message type at this time.

Restrict Enrollment to Registered Devices Only

At this point, regardless of whether administrators or end users have registered devices, you can restrict enrollment to only registered devices. To do this, navigate to **Devices ▶Settings ▶Devices & Users ▶General ▶Enrollment** and select **Registered Devices Only.**



Selecting this setting also enables the option to require registration tokens for enrollment.

Tracking Enrollment Status

Once devices are registered, you can track enrollment statuses by either navigating to the **Device Dashboard** page and selecting the **Enrollment** chart, which lets you filter based on enrollment status, or accessing the **AirWatch Hub**, which lists devices recently enrolled.

Proceed to Question Five: Do You Want To Require Registration Tokens For Device Enrollment? on page 24

Question Five: Do You Want To Require Registration Tokens For Device Enrollment?

Overview

If you restrict enrollment to registered devices only, you also have the option of requiring a registration token to be used for enrollment. This increases security by confirming that a particular user is authorized to enroll. You can send an email or SMS message with the enrollment token attached to users with AirWatch accounts.

If you answered **Yes** to "Do you want to require registration tokens for device enrollment?", or want to see questions you should consider before requiring registration tokens, proceed to Enabling Registration Tokens on page 25.

If you answered **No**, proceed to Question Six: Do You Want To Place Additional Enrollment Restrictions On Which Devices Are Allowed To Enroll? on page 27.

Enabling Registration Tokens

Token-Based Enrollment adds extra layers of security and authentication to the enrollment process. A token is generated by creating a Messaging Template that includes the Enrollment Token variable. In addition to providing a simple enrollment process, it also ensures only authorized users can enroll into your environment. Registration tokens are sent through AirWatch messages to existing AirWatch user accounts. In considering whether or not to utilize registration tokens, consider the following:

- Do you already have AirWatch user accounts created to send the token messages to? If not, you will want to send users instructions via corporate email or intranet announcement to log in to the Self-Service Portal (SSP), which will create a user account for them. You can then send messages with tokens directly to the newly-created user accounts.

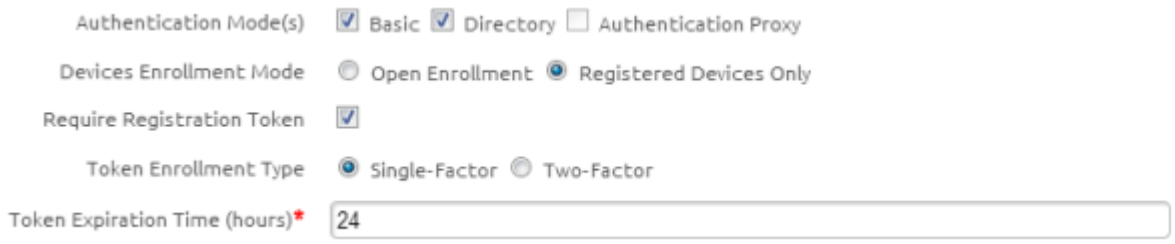
Preparing Token-Based Enrollment

Use the following step-by-step instructions to set up token-based enrollment.

Enable Tokens and Create a Default Message

1. Enable token-based enrollment by selecting the appropriate Organization Group and navigating to **Devices ▶ Settings ▶Devices & Users ▶General ▶Enrollment** and ensure the **Authentication** tab is selected.

   Scroll down past the **Getting Started** section and select **Registered Devices Only** as the **Devices Enrollment Mode**. A checkbox labeled **Require Registration Token** will appear in which you should insert a check mark. This will restrict enrollment to only registered devices.



2. Select a **Token Enrollment Type**.
   - **Single-Factor** – The token is all that is needed to enroll.
   - **Two-Factor** – A token and login with user credentials are required to enroll.
3. Set the **Token Expiration Time** (in hours). This is the amount of time an end user will have to select a link and enroll. Once it expires, you must send another link.
4. Prepare the default message, which will include the enrollment token, to send to users.
   a. Navigate to **Groups & Settings ▶All Settings ▶Devices & Users ▶General ▶Message Templates**.
   b. **Add** a new message template. For Category, select **Enrollment**. For Type, select **Device Activation**. Also select the appropriate **Message Type**.
   c. Enter a generic enrollment message that includes the enrollment link in the message body. Use the following look-up values to include an enrollment token:

{EnrollmentURL}?AC={EnrollmentToken}

Note: You can create Device Activation enrollment messages for each platform and assign them by navigating to **Groups & Settings ▶All Settings ▶Devices & Users ▶General ▶Enrollment** and selecting the **Customization** tab.

Generate a Token via the AirWatch Admin Console

1. Navigate to **Accounts ▶Users ▶List View** and select **Edit User** for a user. (This process also works with creating new users.) The Add / Edit User page displays.
2. Scroll down and select a **Message Type**: **Email** for directory users and **SMS** for basic user accounts.
3. Select the **Message Template** you previously created and select **Save** to send the token to the user via the selected message type.

Note: The token is not accessible via the AirWatch Admin Console for security.

Generate a Token via the Self-Service Portal (SSP)

1. Log in to the Self-Service Portal. This can be from a device or a computer if you are using single sign on or smartcards for authentication. (Directory users can log in using their directory service credentials.)
2. Select **Register Device**.
3. Enter the device information (friendly name and platform) and any other details by completing the fields in the Registration Form. Ensure the email address and phone number are present and accurate as they may not automatically populate.
4. Select **Save** to send the enrollment token to the user via the selected message type.

Note: The token will not be shown on this page and will only appear in the message that is sent.

Perform Enrollment with a Registration Token

1. Open the SMS or email message on the device and select the link that contains the enrollment token.

   If an enrollment page prompts for a Group ID or token, enter the token directly.
2. Enter a username or password if two-factor authentication is used.
3. Continue with enrollment as usual. Once complete, the device will be associated with the user for which the token was created.

Once the MDM profile is installed on the device, the token is considered "used" and cannot be used to enroll other devices. If enrollment was not completed, the token can still be used on another device. If the token expires based on the time limit you entered, you will need to generate another enrollment token.

Question Six: Do You Want To Place Additional Enrollment Restrictions On Which Devices Are Allowed To Enroll?

Overview

Applying additional enrollment restrictions is applicable to any deployment, regardless of directory services integration, BYOD support, device registration, or other setups. You can set up additional enrollment restrictions to control who can enroll and which device types are allowed.

If you answered **Yes** to "Do you want to place additional enrollment restrictions on which devices are allowed to enroll?" or want to know more about these optional enrollment restrictions, proceed to Setting Enrollment Restrictions on page 28

Setting Enrollment Restrictions

Before you implement enrollment restrictions, you should consider what types of restrictions you will want to enforce. Consider the following questions:

Consideration #1 – Will you restrict specific platforms, OS versions, or maximum number of allowed devices? If so, you can apply additional enrollment restrictions.

Consideration #2 – Do you want to restrict which devices are allowed to enroll to a set list of corporate devices? If so, you can upload a list to register multiple devices at once or create a "whitelist" of corporate devices.

Consideration #1 – Will You Restrict Specific Platforms, OS Versions or Maximum Number of Allowed Devices?

Enrollment restrictions let you fine-tune the enrollment parameters you want to apply to your deployment. When making the decision of which enrollment restrictions you may use, consider the following:

- Do you want to support only those devices that feature built-in enterprise management – such as Samsung SAFE/KNOX, HTC Sense, LG Enterprise, and Motorola devices? If so, you can require that Android devices have a supported enterprise version as an enrollment restriction.
- Do you want to limit the maximum devices that a user is allowed to enroll? If so, you can set this amount, including distinguishing between corporate owned and employee owned devices.
- Are there certain platforms you will not support in your deployment? If so, you can create a list of blocked device platforms that will prevent them from enrolling.

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.

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**.

Consideration #2: Will You Restrict Enrollment to a Set List of Corporate Devices?

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

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