

VMware AirWatch: Configure & Manage

Lab Manual



VMware AirWatch: Configure & Manage

VMware Workspace ONE & AirWatch

Part Number AW-EDU-MANAGE

Lab Manual

Copyright © 2017 VMware, Inc. All rights reserved. This manual and its accompanying materials are protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

The training material is provided “as is,” and all express or implied conditions, representations, and warranties, including any implied warranty of merchantability, fitness for a particular purpose or noninfringement, are disclaimed, even if VMware, Inc., has been advised of the possibility of such claims. This training material is designed to support an instructor-led training course and is intended to be used for reference purposes in conjunction with the instructor-led training course. The training material is not a standalone training tool. Use of the training material for self-study without class attendance is not recommended.

These materials and the computer programs to which it relates are the property of, and embody trade secrets and confidential information proprietary to, VMware, Inc., and may not be reproduced, copied, disclosed, transferred, adapted or modified without the express written approval of VMware, Inc.

CONTENTS

<i>Lab 1</i> Welcome to VMware Labs	1
<i>Lab 2</i> Before You Begin	3
<i>Lab 3</i> VMware AirWatch Basics	5
<i>Lab 4</i> Mobile Device Management	19
<i>Lab 5</i> Mobile Email Management	91
<i>Lab 6</i> Mobile Application Management	105
<i>Lab 7</i> Mobile Content Management	125

Lab 1 Welcome to VMware Labs

Exercise Introduction

Thank you for your interest in learning more about VMware solutions. We have developed a series of lab exercises for you to learn more about the Workspace ONE platform. These labs are designed to lead you through the various components of the AirWatch products in a hands-on format. Please refer to the training decks, my.air-watch.com and the on-line help in the console for additional assistance.

If you have any questions or feedback, please send them to Eduoperations@vmware.com.

Sincerely,

VMware Education Services

Lab 2 Before You Begin

Lab Preparation

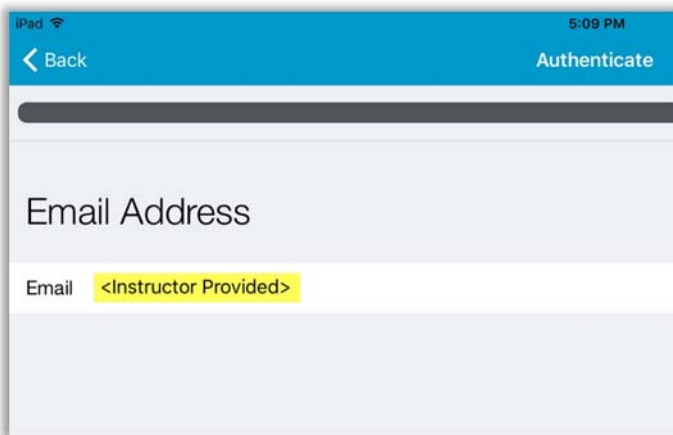
Please be sure that you have the following tools ready and available for the lab.

1. **Laptop:** either PC or Mac, used for accessing the AirWatch training environment.
2. **Mobile Device:** iOS or Android device used for lab exercises. This device should be running the most up-to-date version of its operating system; This is considered a best practice.
3. **App Store Login:** based on the platform of your mobile device, either an Apple ID or Google account, used for downloading public applications.
4. **Browser:** modern browser used throughout the duration of the training. We recommend the use of a modern browser such as Google Chrome, Firefox or Safari.
5. **Academic Success Kit:** contains the `Course_Materials` folder, which includes assets used for lab activities. Please ensure the Academic Success Kit is staged on your desktop for easy access.

Lab 3 VMware AirWatch Basics

Task 1: Enrolling with the AirWatch Agent

1. Navigate to <https://AWAgent.com> and download the AirWatch Agent to your device.
AWAgent.com automatically determines the platform of the device accessing the page and forwards the device to the appropriate public app store, which prevents confusion with direct app access. A valid Apple ID or Google Play account is required to install the AirWatch Agent.
2. Open the **Agent** app, accept any pop-up notifications, and select **Email Address**.
3. Enter the email address provided by the instructor.

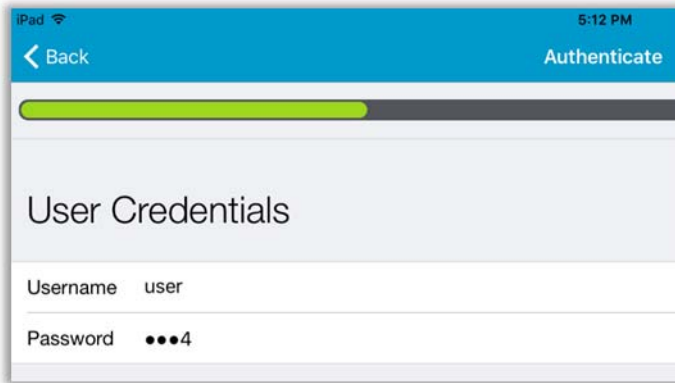


4. Click **Next** to proceed with the enrollment process.

AirWatch can be configured to use a process called Autodiscovery, which associates users with the proper AirWatch environment using an email address. The user could also enroll by entering the MDM Server URL/Group ID or by scanning a QR code to initiate enrollment.

5. Input the following user credentials:

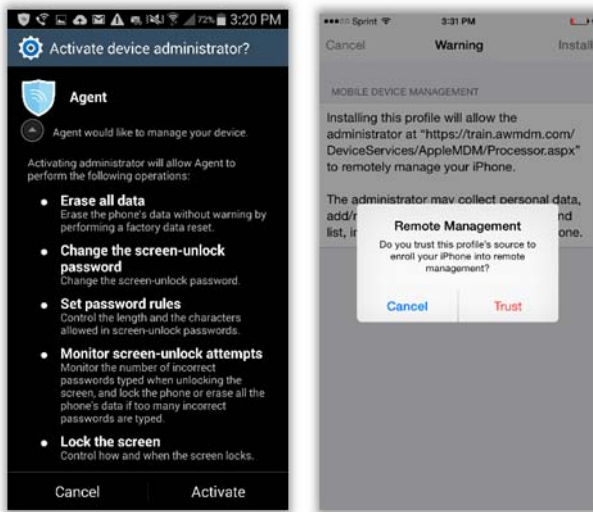
- **User:** user
- **Password:** AirWatch



AirWatch authenticates end users by enrolling them into virtual containers known as Organization Groups.

6. Accept the **Terms of Use** policy.
7. Click the option prompted to continue to with the enrollment process, such as **Redirect & Enable** for iOS.
8. Depending on the platform, you should install, activate and/or accept all prompts and Click **Done** to complete the enrollment.
 - **iOS:** Install a Digital Workspace (Enrollment Profile) and trust Remote Management.
 - **Android:** Some platforms require the user to enable AirWatch as a Device Administrator or to install and activate additional Manufacturer Service Applications.
9. Accept any prompts to install the following applications:
 - AirWatch Inbox
 - Content Locker

- Browser



Your device is now enrolled in AirWatch.

The AirWatch Catalog (Web Clip/Bookmark) will install silently.

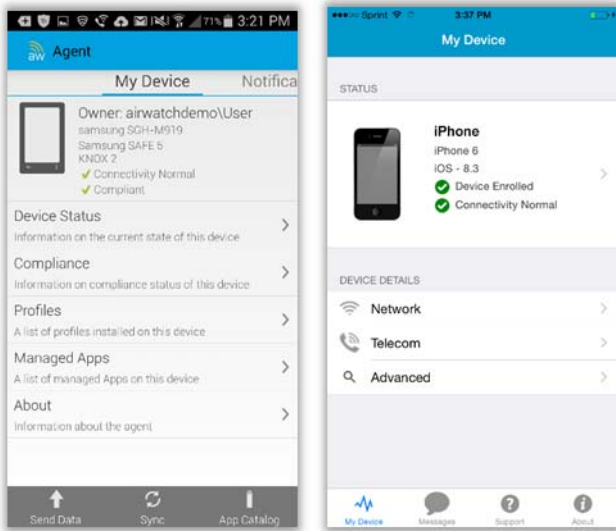
10. Open the **Agent** app.

The AirWatch Agent shows information about the device status, connectivity, compliance, and assignments.

The AirWatch Agent can also receive messages sent by administrators relating to the status, health, and compliance of the device.

Enrollment may be facilitated on iOS devices using the native browser rather than the AirWatch Agent. This flow negates the ability to perform certain management functions. For other

platforms, the native browser may be utilized to start enrollment, but the AirWatch Agent must be used for full MDM functionality.



11. Take a picture.

Specific device functions can be restricted according to administrator configurations.

12. Take a screen capture.

Disallowing device functions like screen capture allow organizations to better prevent data loss.

The specific functions that can be controlled on each device is subject to the device manufacturer.



Task 2: Using VMware Boxer

1. Open the **Boxer** app and accept any pop-up notifications.

If VMware Boxer requires installation, open the App Catalog, Click the option to install VMware Boxer. A prompt to install the application will appear, either in the middle of the screen or in the notification bar. For iOS, Click Install and enter your Apple ID credentials, if prompted. For Android, the prompt will take you into the AirWatch Agent. Tap on AirWatch Inbox, which will then direct you to the Google Play store for installation.

2. Provide the Boxer credentials:

- **Username:** student
- **Password:** AirWatch

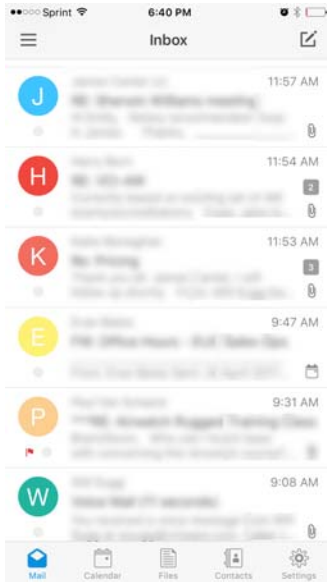
NOTE

student1/student1 may be used an alternate if access is blocked for maintenance.

3. Browse email, calendar and contacts.

- **iOS:** email, calendar and contacts are containerized in one application.

- **Android:** email, calendar and contacts arrive in separate applications.



4. Attempt to copy/paste information from an email to another app.

Data Loss Protection (DLP) settings allow control over what information can be moved to which locations and apps on a device.

LEARN MORE!

During the MEM training module, you will learn more how AirWatch can protect your email infrastructure. This is accomplished by either deploying the AirWatch Secure Email Gateway to act as a proxy for email requests or with direct integration leveraging PowerShell Cmdlets or Google Apps for Business API.

Task 3: Using the VMware Content Locker

1. Open the **Content** app.

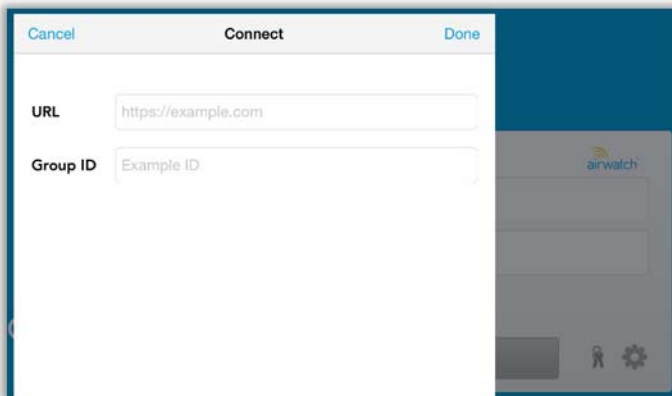


If a URL is presented upon login, verify the following details and Click **OK**:

- **URL:** <Instructor Provided>
- **Group ID:** intro

If prompted for credentials, enter the following:

- **User:** user
- **Password:** AirWatch



If VMware Content Locker requires installation, open the App Catalog, Click the option to install the VMware Content Locker. A prompt to install the application will appear, either in the middle of the screen or in the notification bar. For iOS, Click Install and enter your Apple ID credentials, if prompted. For Android, the prompt will take you into the AirWatch Agent. Tap on VMware Content Locker, which will then direct you to the Google Play store for installation.

Single sign-on has been enabled and leverages the AirWatch Software Development Kit (SDK), which is coded into the application. Credentials are not required, since the AirWatch Agent is used to authenticate the session.

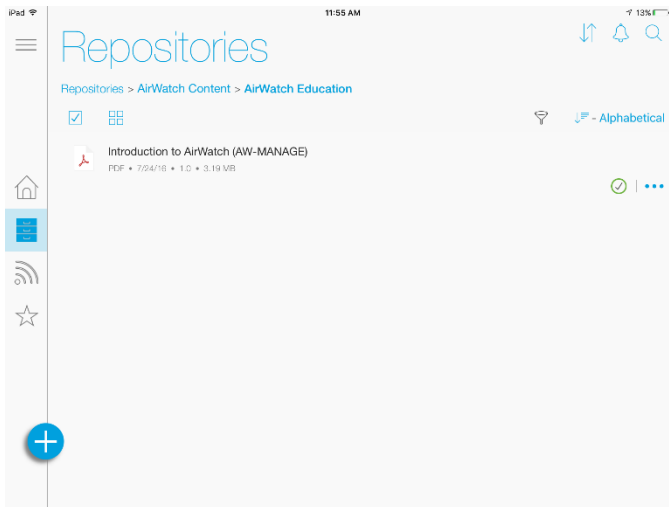
2. Accept any pop-up notifications and swipe through the tutorial screens and Click **Got it, Thanks** to view the **Repositories** page.
3. Click **AirWatch Content**, choose a document to download and then tap to view.



The AirWatch Admin can determine what content is pushed for automatic download or in an on-demand capacity. Additional settings, such as enabling downloads only when devices are connected to Wi-Fi or configuring an expiration date for content availability, can additionally be defined.

4. Click Back or “X” out of the document and select the file cabinet to go back to the main **Repositories** screen.
5. Click **AirWatch Content** and navigate to **AirWatch Education**.
6. Attempt to email the *Introduction to AirWatch* document. The steps below are for iOS; similar series of actions would be carried out on other platforms:
 - Click the **Checkmark** button from the top left of the navigation panel.

- Click the **Radio Button** next to the document and note the email icon on the left side is greyed out.
- Click the red “X” button to exit the option.



Application-level DLP settings allow control over content access to be flexibly organized throughout different levels of the organization group structure.

7. Tap on the document and review the available options.
8. Assign a document as a favorite by selecting the star button.



LEARN MORE!

During the MCM training module, you will learn about the differences between corporate and user content, how to create categories associated with content loaded into AirWatch, configuring content repositories (such as Google Drive or SharePoint) and enforcing application-level DLP settings.

Task 4: Using the VMware Browser

1. Open the Browser app and accept any pop-up notifications.



If VMware Browser requires installation, open the App Catalog, select the option to install the VMware Browser. A prompt to install the application will appear, either in the middle of the screen or in the notification bar. For iOS, Click Install and enter your Apple ID credentials, if prompted. For Android, the prompt will take you into the AirWatch Agent. Tap on VMware Browser, which will then direct you to the Google Play store for installation.

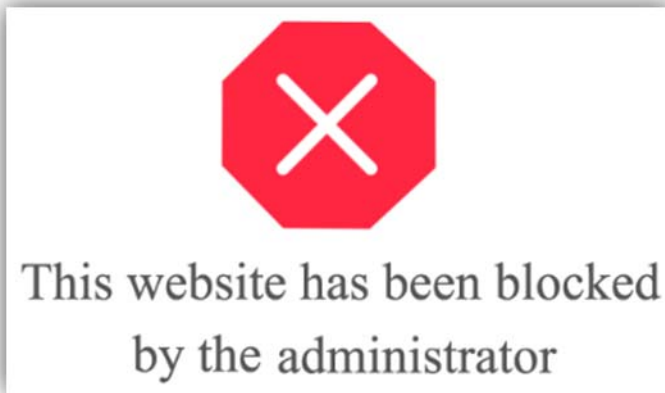
Single sign-on has been enabled and leverages the AirWatch Software Development Kit (SDK), which is coded into the application. Credentials are not required, since the AirWatch Agent is used to authenticate the session.

2. Navigate to `google.com`.

Users can access pre-approved sites that were deemed acceptable for work use.

3. Attempt to navigate to `twitter.com`.

Blacklisting allows organizations to prevent access to inappropriate sites.

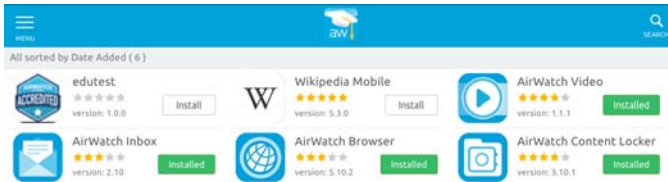


LEARN MORE!

If you are interested in learning more about the VMware Browser, refer to supporting documentation in the Resources section of the myAirWatch portal.

Task 5: Using the AirWatch Catalog

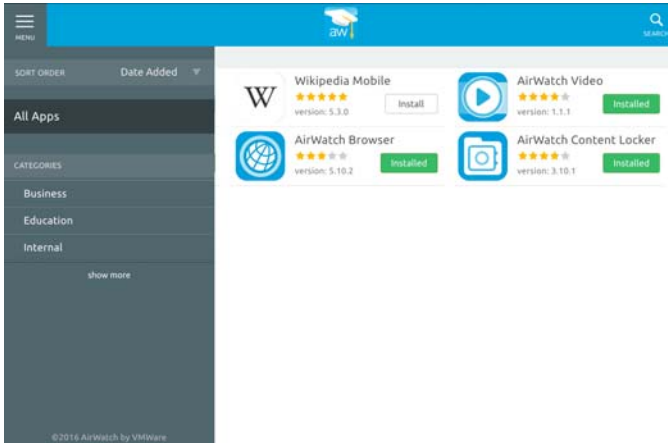
1. Open the App Catalog Web Clip/Bookmark.



For iOS and Android, the AirWatch Catalog is a shortcut to an AirWatch website. This site enables users to install, interact with and deploy approved applications. iOS refers to this shortcut as web clip, while Android refers to this shortcut as a bookmark.

No credentials are required for access. This setting could be enabled on your environment by an AirWatch Administrator.

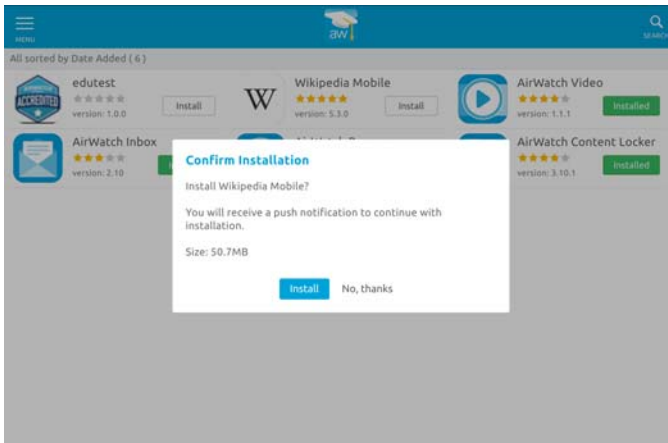
- From the menu, filter by the Business category.



- Select an application by tapping on the icon, scroll down to the bottom of the navigation pane on the right, provide an internal rating on an app, and then Click **Save**.

Administrators can promote selected applications to increase application adoption.

- From the menu, filter by **All Apps**.
- Select **Wikipedia** and then click **Install** to start the installation process for the application.



Though Wikipedia is a public application, it can be removed from your device remotely by the AirWatch Administrator.

AirWatch Administrators can promote selected applications to increase application adoption without bothering end users. Alternatively, they can make other applications push down automatically, as they did when you successfully enrolled your device.

LEARN MORE!

During the MAM training module, you will learn about how to enable and configure the AirWatch Catalog, how to push, load and assign public and internal applications, and how to enforce app compliance. If you are interested in learning more about AirWatch app development tools, refer to supporting documentation in the Resources section of the myAirWatch portal.

Lab 4 Mobile Device Management

AirWatch Fundamentals

Task 1: Logging in to the AirWatch Admin Console

1. From your computer, open a supported browser.
2. Navigate to the instructor-provided URL for the AirWatch Admin Console.
3. Enter the **username** and **password** provided by the instructor.

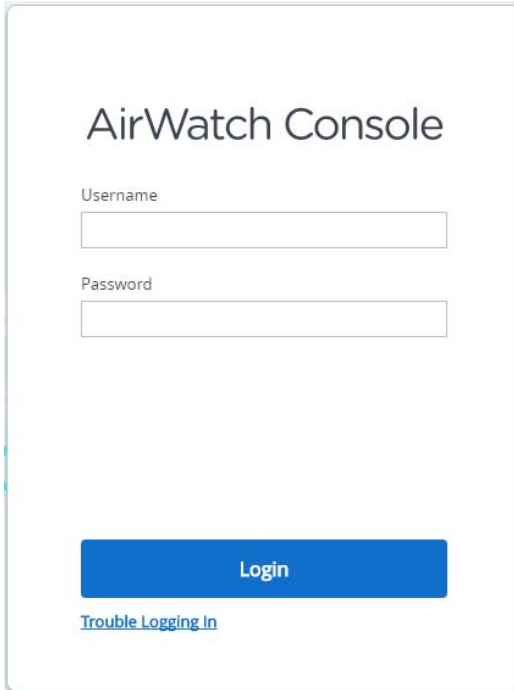
Username:

Password:

The password is case sensitive.

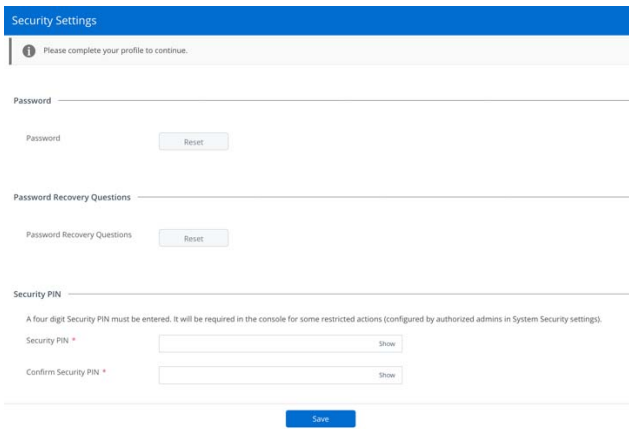
4. Click **Login**.

5. Read through and verify that you accept the AirWatch Terms of Use agreement.



The image shows the AirWatch Console login page. At the top, the text "AirWatch Console" is displayed in a large, dark font. Below this, there are two input fields: "Username" and "Password". Each field is a simple rectangular box with a thin border. Underneath the password field, there is a blue button with the word "Login" in white text. At the bottom left of the page, there is a link that says "Trouble Logging In" in blue text.

6. Define a four-digit Security PIN and a security question.



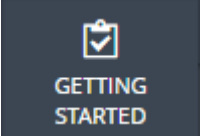
The image shows the "Security Settings" configuration screen. At the top, there is a blue header bar with the text "Security Settings". Below the header, there is a message: "Please complete your profile to continue." followed by a right-pointing arrow. The screen is divided into three sections, each with a horizontal line above it. The first section is "Password", which has a "Password" label and a "Reset" button. The second section is "Password Recovery Questions", which has a "Password Recovery Questions" label and a "Reset" button. The third section is "Security PIN", which has a "Security PIN" label and a "Show" button. Below this, there is a "Confirm Security PIN" label and another "Show" button. At the bottom center of the screen, there is a blue "Save" button.

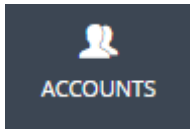
The Security PIN is a safeguard for all major MDM functions and serves as a second layer of security while preventing inadvertent commands. The Security Settings menu provides options for changing the passcode or creating passcode recovery questions.

Optionally, adjust the console actions which require the Security PIN by navigating to **Groups & Settings > All Settings > System > Security > Restricted Actions**.

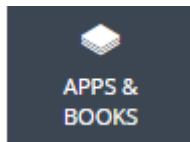
Task 2: Navigating the AirWatch Console

1. Select each Main Menu tab from the left side and review the options.

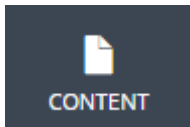
Button	Description
	Ensure that all aspects of a basic successful deployment are established. Getting Started is organized to reflect only those modules within an AirWatch Admin Console deployment that you are interested in. This produces an onboarding experience that is more tailored to your actual configuration.
	View and manage MDM information that drives decisions you must make and access a quick overview of your device fleet. View specific information such as the most blacklisted apps that violate compliance. Keep track of module licenses with the Admin Panel Dashboard and monitor all devices that are currently out of compliance. Select and run Industry Templates to streamline the onboarding process with industry-specific apps and policies for your iOS devices.
	Access an overview of common aspects of devices in your fleet, including compliance status, ownership type breakdown, last seen, platform type, and enrollment type. Swap views according to your own preferences including full Dashboard, list view, and detail view. Access additional tabs, including all current profiles, enrollment status, Notification, Wipe Protection settings, compliance policies, certificates, product provisioning, and printer management.



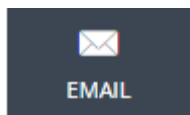
Survey and manage users and administrators involved with your MDM deployment. Access and manage user groups, roles, batch status and settings associated with your users. Also, access and manage admin groups, roles, system activity, and settings associated with your administrators.



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



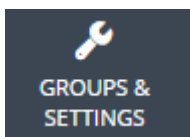
Access detailed overview of content usage including storage history trends, user and content status, engagement and user breakdown. Manage and upload content available to users and devices. Also, access batch import status, content categories, content repositories, user storage, VMware Content Locker home screen configuration, and all other content-specific settings.



Access detailed overview of email information related to your deployment. This includes email management status, managed devices, email policy violations, deployment type, and time last seen.



Access detailed overview of telecom-enabled devices including usage history, plan usage, and roaming data. View and manage telecom use and track roaming, including call, Short Message Service (SMS), and content settings.



Manage structures, types and statuses related to organization groups, smart groups, app groups, user groups, and Admin Groups. Configure entire system settings or access settings related to all Main Menu options.

The Main Menu enables you to navigate quickly to all available features within your deployment based on role-based permissions. These options generally include the Getting Started Wizard, Hub, Devices, Accounts, Apps & Books, Content, Email and Groups & Settings. Your access to these Main Menu options may vary depending on whether your role permissions have been changed. You will explore each Main Menu option later in this course.

2. At the bottom left-hand corner, Click the **gray disclosure arrow** to expand the submenu.

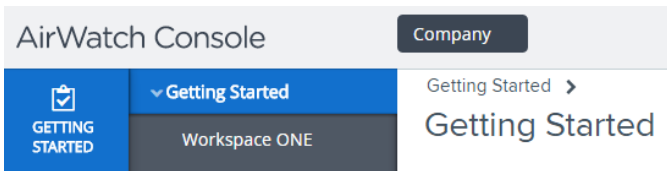


3. Click the **About** button to view the current version of AirWatch.

When navigating the submenu, some options may display an icon of a Hammer and Wrench. When this icon is selected, it will trigger a blue settings popup for available advanced settings tied to that submenu. If you need to go back to the **Main Menu**, close the popup.



4. From the top, locate the **Organization Group** menu. The information displayed on each page will be relevant for the Organization Group (OG) level displayed.

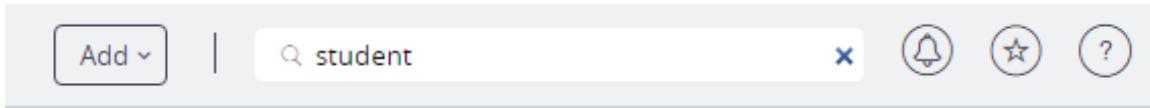


In a later lab activity, you will create a hierarchy under **Company**. This may include further defining your deployment with distinct categories, including geographies, divisions and business units.

In the training environment, your OG is a child of several parent OGs. These parent OGs are not visible to you since they are above your Company OG. As an AirWatch Administrator at your Company OG, your role-based permissions define what you can configure and manage within the AirWatch Admin Console. The AirWatch Administrator at the parent OG above yours has full governance over all settings, since they created your AirWatch Administrator account and defined your role-based permissions. As the AirWatch Administrator at your Company OG, you can similarly decide and define what access levels to grant to AirWatch

Administrators in child OGs. Understanding the relationship between parent and child OGs is a very important concept, and will be reinforced as you work through lab exercises.

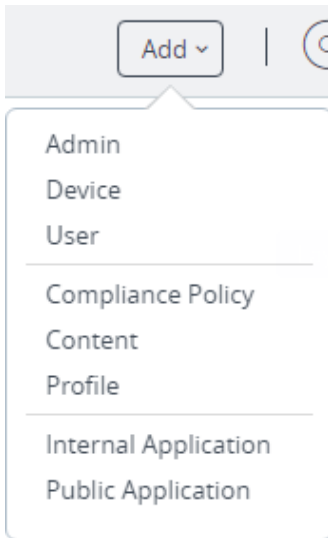
5. From the Header Menu, Click the **search icon** and enter **Student**.



The search provides results based on the Organization Group level for all aspects of your AirWatch deployment, including devices, users, content, applications, configuration settings, admins, pages and more.

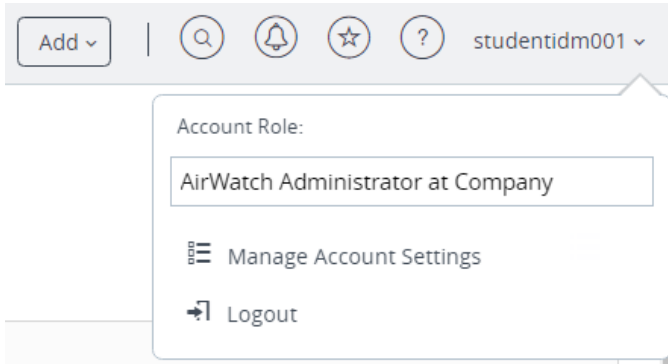
6. Click **Add** and review the options.

The **Add** button makes it easy to quickly add an admin, device, user, compliance policy, piece of content, profile, internal or public application, rather than forcing you to navigate to a specific page to add a new configuration via the Main Menu. The Add button will add the object or configuration to whichever Organization Group is currently being accessed.

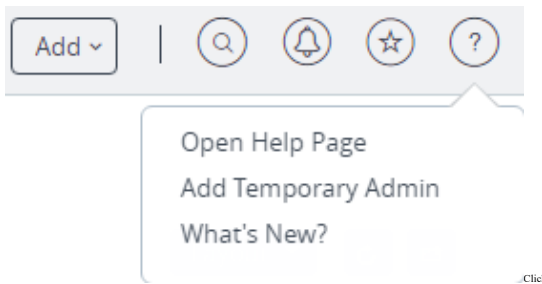


7. Click **Saved**. No saved menu pages appear. To tag a page as a favorite, Click the **Star** icon.
8. Click the **House** icon. This option will set the current menu page as the homepage; this page appears to the AirWatch Administrator as the first page when they log in to the AirWatch Admin Console.

9. Click **Account** (your username in the upper right). You will notice that you cannot change your Account Role, since only one role is defined. Other available options include **Manage Account Settings** and **Logout**.



10. Click **Manage Account Settings** to review the options for changing admin user metadata such as login history and other security settings.
11. Click **Help** and select **Open Help Page**.



Help will launch the online help portal, where you can browse and search available guides and feature documentation. The Help menu displays information based on where you are in the console (such as Apps & Books), but launches in a separate tab so that you can navigate back to the console without being forced to log out and back in.

There is another option under the Help icon that will create a Temporary Administrator. This option allows you to create a basic administrator account that is intended to be used for troubleshooting. This account will become inactive after a defined time threshold of 6 hours to 1 week.

Setting Up Your Environment

Task 3: Reviewing the Status of Your APNs Certificate

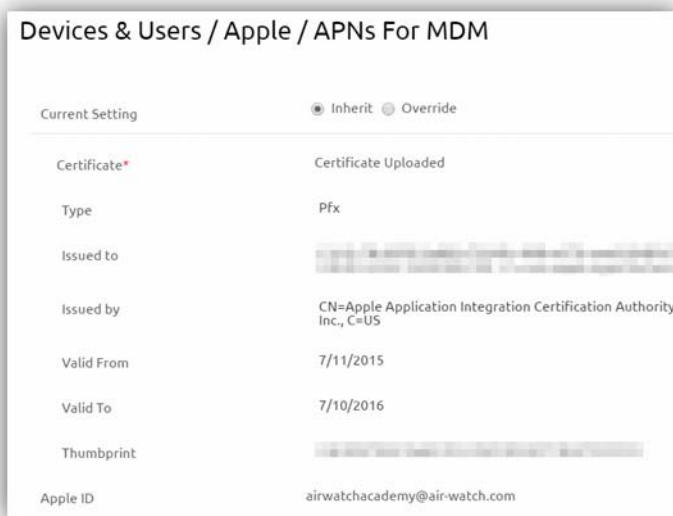
The Apple Push Notification service (APNs) is used to allow AirWatch to securely communicate with Apple devices over-the-air. Internet Explorer cannot be used to perform the APNs certificate lab. If you are using Internet Explorer, log out and log in using another browser. If installing another browser is not an option, omit this lab and proceed to the privacy settings lab.

1. From the Main Menu, navigate to **Devices > Devices Settings > Apple > APNs for MDM**.

NOTE

The APNs certificate can also be created using the Getting Started Wizard. Since there is already a APNs certificate loaded at a higher-level OG than you have permissions to modify, you must override the parent settings in the AirWatch Admin Console settings.

2. If a APNs certificate was not loaded, this is where you would go through the process of loading a new one. This is also the location where you would update an existing APNs certificate once your existing certificate expires. If you intend to use Apple devices within your deployment, you will need to ensure that this certificate is kept up-to-date. If it expires, all Apple devices will become unenrolled.



Task 4: Reviewing the Process to Add an Email Domain for AirWatch Autodiscovery

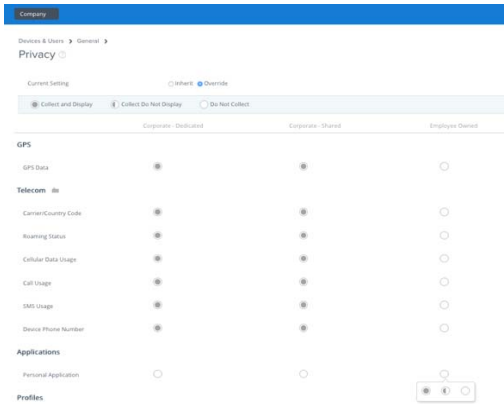
1. From the Main Menu, navigate to **Devices > Devices Settings > General > Enrollment > Authentication** tab.
2. Click **Add Email Domain** and enter **Business Email Domain** and **Confirmation Email Address**.
3. Exit out of the settings popup to ensure that your domain information is not tied to AirWatch Autodiscovery within the training environment.



Task 5: Defining Privacy Settings

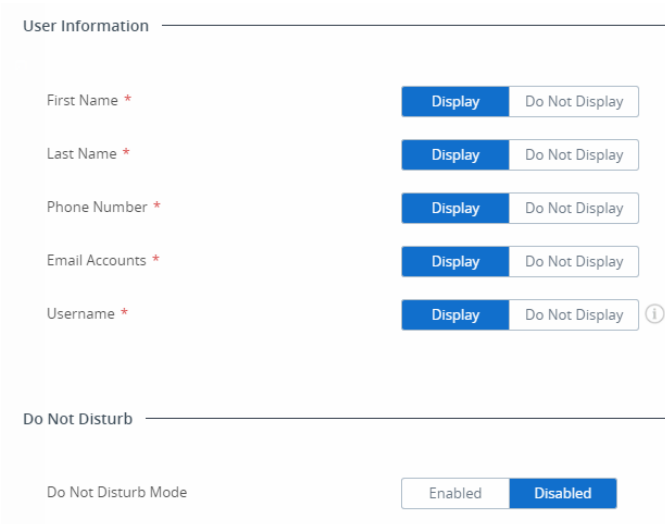
1. From the Main Menu, navigate to **Devices > Devices Settings > General > Privacy**.
2. Change the current setting to **Override**. This will allow you to change the Privacy settings at your Company OG.
3. Scroll down to **Personal Application** and change the setting to **Collect and Display** for Employee Owned devices. When you enroll your device, the AirWatch Admin Console has been set up to enroll it as an Employee Owned device, which will cause personal applications to show in device details within the Application tab. If you wish to prevent your personal

applications from being shown in the AirWatch Admin Console, set to **Do Not Collect** and Click **Save**.



The “Collect and Display” setting gathers user data and displays it in the AirWatch Admin Console. The “Collect Do Not Display” setting collects user data for use in reports and compliance, but is not displayed within the AirWatch Admin Console. The “Do Not Collect” setting prevents collection of user data from being shown in both the AirWatch Admin Console and in generated reports.

- Review all remaining privacy settings, including whether the AirWatch Administrator can remotely erase a device (factory wipe), remote control a device based on ownership, display user information and more.



Privacy settings are specific to your Company OG; child OGs could therefore be set up with different privacy settings. The concept of defining different settings at different OG levels is referred to as multitenancy. Privacy is one example of the many settings available in the AirWatch Admin Console, where the settings defined at the parent OG could be different from their child OGs.

Another key setting, Do Not Disturb (DND), provides a clean and automated way to halt profile, content and application changes on enrolled devices for a window of time defined directly within the AirWatch Admin Console. Integral MDM commands such as Full Wipe, Enterprise Wipe and Clear Passcode still function when the device is in DND mode. A device is put into DND from the device dashboard; this will be discussed in depth in a later lab activity.

Task 6: Defining a Terms of Use Policy

1. From the Main Menu, navigate to **Devices > Devices Settings > General > Enrollment > Terms of Use** tab.
2. Change the current setting to **Override**.
3. Select **Require Enrollment Terms of Use Acceptance** and then Click **Save**.

When an Enrollment Terms of Use policy is required, all devices will be required to accept the Enrollment Terms of Use during initial device enrollment. If a Terms of Use policy is not defined, a parent OG's Terms of Use would be enforced if one is defined.

Devices & Users > General > Enrollment

Authentication Terms of Use Grouping Restrictions Optional Prompt Customization

Current Setting Inherit Override

Require Enrollment Terms of Use Acceptance

Enrollment Terms Of Use

+ Add New Enrollment Terms Of Use

4. Click Add New Enrollment Terms of Use.
5. Enter a **Name** for the Terms of Use.
6. Review all options, such as enforcing the policy for specific platforms, ownership type, and enrollment.

NOTE

If you exclude the device you plan to enroll, the Terms of Use will not be shown during enrollment in a later lab activity.

NOTE

English is the default language. Use the **Select Language** list to change the default language.

7. Enter your Terms of Use in the text field provided and Click **Save**.

The editor provides an HTML entry tool to create a new Terms of Use or, alternately, copy and paste an existing Terms of Use. If you choose to use paste copied from external content, right-click the text box and choose Paste as plain text. This will prevent any HTML or formatting errors. For localized versions, previously-translated text must be entered.

The screenshot shows the 'Create New Terms of Use' form. The fields are as follows:

- Name: Enrollment Terms of Use Example
- Type: Enrollment
- Version: 1
- Platforms: Any Selected Platforms
- Device Ownership: Any Selected Ownership Types
- Enrollment Type: Any Selected Enrollment Types
- Notification: Send email to Users when Terms are updated
- Select Language: English (United States)

The rich text editor contains the text: "My legal team will love this!".

Buttons: Add, Save, Cancel

Task 7: Configuring Branding

The Branding settings page lets you configure settings related to the branding of the AirWatch Admin Console. Change branding to reflect company colors or visually delineate specific organization groups.

1. From the Main Menu, navigate to **Groups & Settings > All Settings > System > Branding**.

The Current Setting is set to **Inherit**, while the Child Permission is set to Inherit only. As an AirWatch Administrator, you can not only define which settings other administrators can access, but additionally whether they can change color values.

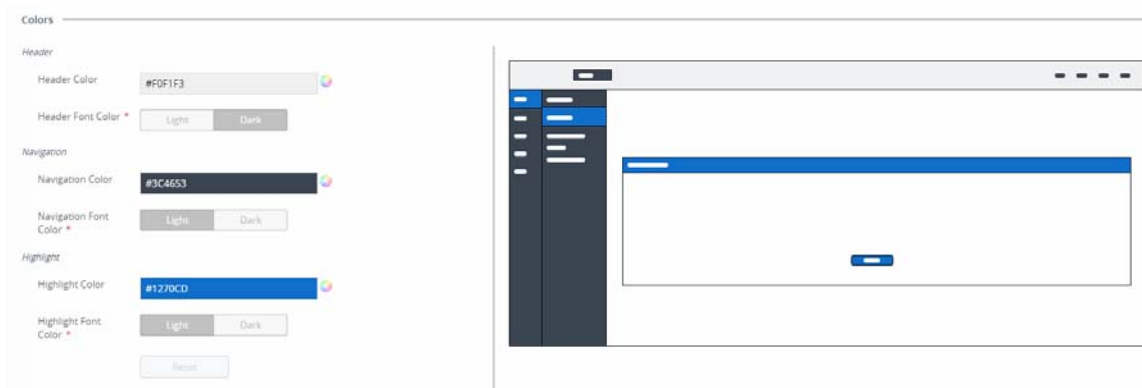
From the **Branding** tab, a full AirWatch Administrator would normally can change the following:

Setting	Description
Company Logo	The logo that appears in the upper left corner of the AirWatch Console.
Login Background Page	The image that displays on the login splash page. You can upload multiple images that will function as rotating slides.
Company Website URL	The URL that a user will be directed to after clicking the Primary Logo image.
Login Page Slide Delay (seconds)	The delay between image rotation on the login splash page.

In our environment, the current parent OG has disabled the settings available in the **Branding** tab.

2. Click **Override**.
3. Modify the colors assigned to the interface and Click **Save**.

All AirWatch websites will be branded with color assignments, including the AirWatch Admin Console, AirWatch Catalog, and AirWatch Self-Service Portal.

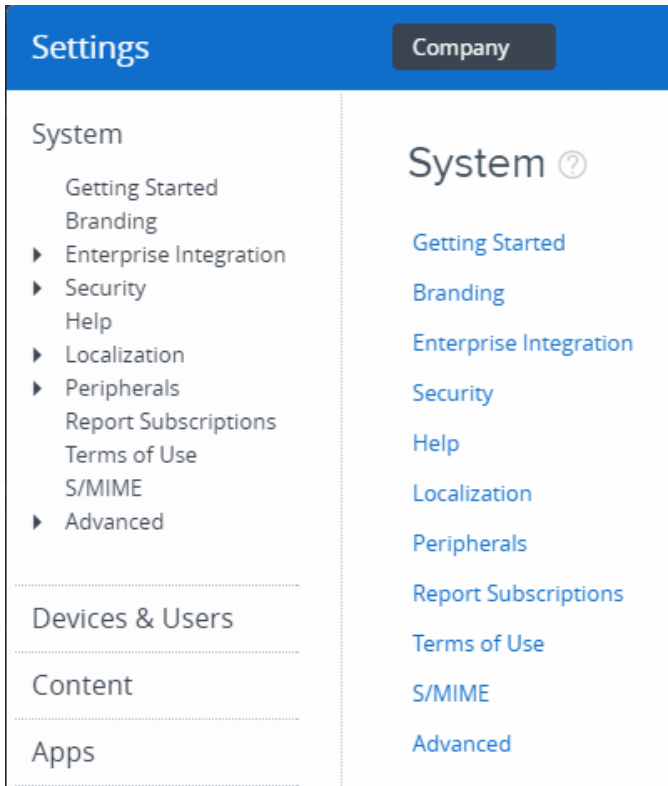


NOTE

The **Custom CSS** tab can be used to insert a cascading style sheet (CSS) of your own custom design that will override the console defaults.

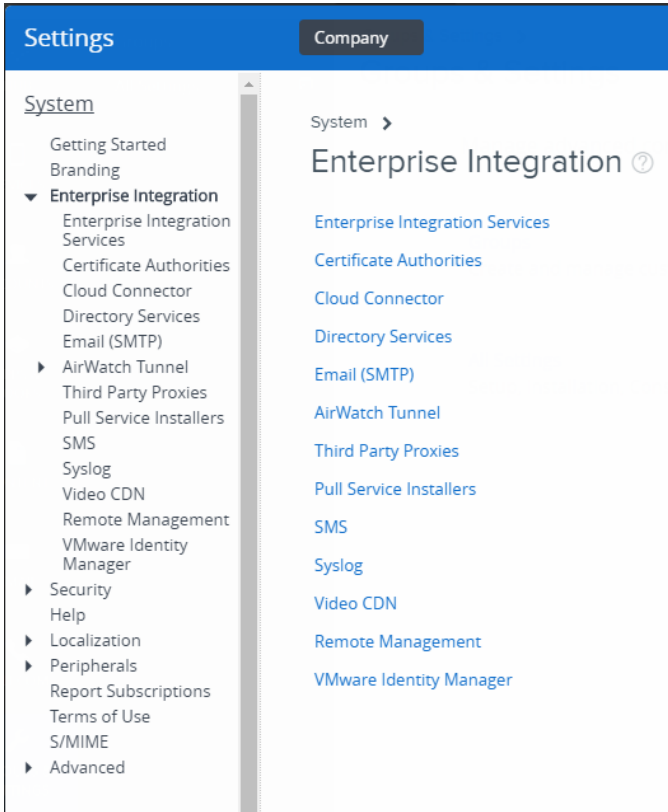
Task 8: Reviewing Core System Settings

1. From the Main Menu, navigate to **Groups & Settings > All Settings > System** and browse the core system options to understand their configuration settings.



2. From the **System** menu, Click **Getting Started**.
Use the **Getting Started** page to enable/disable the Getting Started Wizard.
3. From the System menu, Click Enterprise Integration.

Use the options under Enterprise Integration to facilitate AirWatch integration with your existing enterprise infrastructure, such as email management with SMTP, Directory Services and content management with repositories such as SharePoint and other network file shares.



4. From the **System** menu, Click **Security > Restricted Actions**.

Use the **Restricted Actions** page to send bulk messages to all devices, password protect actions performed in the AirWatch Admin Console using the Security PIN, and define if a note is required for tracking purposes.

5. From the **System** menu, Click **Localization**.

Use the **Localization** page to activate additional languages and edit language references.

6. From the **System** menu, Click **Terms of Use**.

Use the **Terms of Use** page to set up Application or Console Terms of Use policies.

Task 9: Defining Organization Groups

1. From the Main Menu, navigate to **Groups & Settings > Groups > Organization Groups > Organization Group Details**.
2. Change the **Organization Group Name** from **Company** to **Root**.

Changing Company to Root allows you to create child OGs for different companies or testing groups. The Group ID may have previously been defined based on your student number within the training environment and will not require adjustment.

3. Click **Save**. Refresh your browser to view the updated OG name.

Groups & Settings > Groups > Organization Groups > Organization Group Details

Organization Group Details Add Child Organization Group

Name * Root

Group ID idm001

Type * Customer

Country * United States

Locale * English (United States) [English (United States)]

Customer Industry * Unknown

Time Zone * (GMT-05:00) Eastern Time (US & Canada)

4. Select **Add Child Organization Group**.
5. Using the sample OG topology hierarchy, enter World Wide Enterprises in the **Name** field.
6. Define a unique **Group ID** and accept the default **Type**.

NOTE

For training purposes, define a Group ID which is easy to remember for future device enrollment. The Group ID is not case sensitive, but cannot contain spaces or special symbols. While the Group ID may be the same as your OG name, it may fail to save because another student within the training environment may have already defined this value. If this occurs, define a different Group ID.

7. Adjust **Country**, **Locale** and **Time Zone** settings based on your region.

Organization Group Details	Add Child Organization Group
Name *	<input type="text" value="World Wide Enterprises"/>
Group ID	<input type="text" value="wwe"/>
Type *	<input type="text" value="Container"/>
Country *	<input type="text" value="United States"/>
Locale *	<input type="text" value="English (United States) [English (United States)]"/>
Time Zone	<input type="text" value="(GMT-05:00) Eastern Time (US & Canada)"/>

NOTE

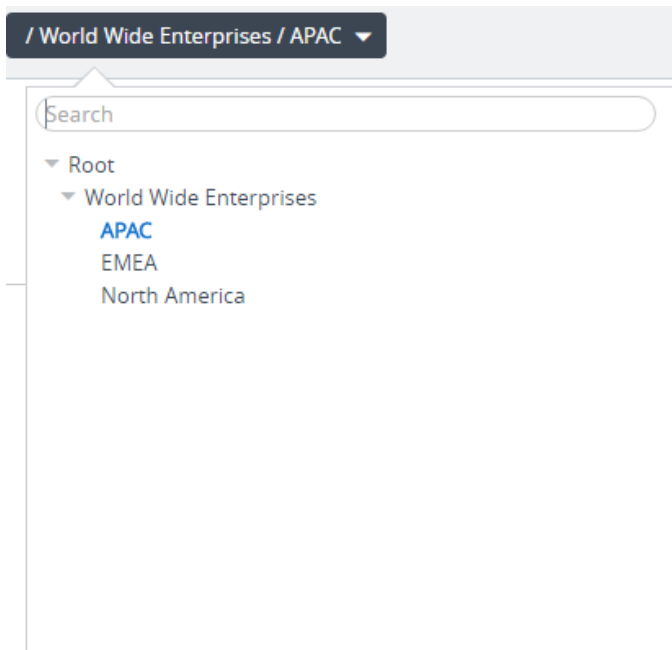
Changing OG Type, Country, Locale and Time Zone settings will only affect reporting metrics.

8. Click **Save**. Refresh your browser to view the updated OG name.
9. Select **Add Child Organization Group**.
10. Using the sample OG topology hierarchy, enter North America in the **Name** field, which is the first geographic region OG hierarchy.
11. Define a unique **Group ID** and accept the default **Type**.
12. Adjust **Country**, **Locale** and **Time Zone** settings based on your region.
13. Click **Save**. Refresh your browser to view the updated OG name.
14. Select your Company OG, and select **Add Child Organization Group** and follow the same procedures to build an OG for **EMEA** and **APAC**.

NOTE

Remember to navigate back to your Company OG to create each child OG for different geographical locations. The disclosure arrow to the left will expand or contract your OGs for each navigation.

15. Verify your environment displays the OG structure as shown in the illustration.

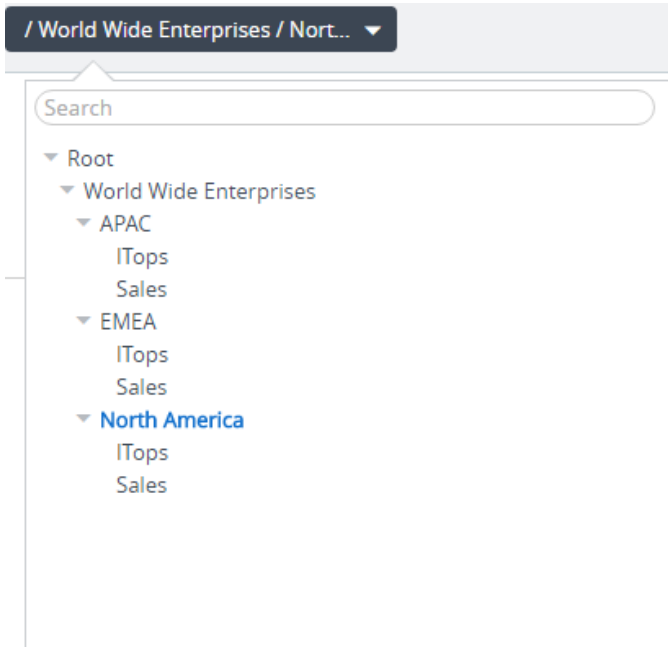


NOTE

The “Root” pictured here should be your email address. “World Wide Enterprises” represents the unique Organization Group you created in step 5.

16. At each geographic OG, create two child OGs called **Sales** and **ITops**.
17. Define a unique **Group ID** and accept the default **Type**.

18. Adjust **Country**, **Locale** and **Time Zone** settings based on your region Click **Save**.



If your OG structure does not mirror the displayed OG structure, and has a unique Group ID defined, select the incorrect OG and fix the issue or delete it. When you delete the OG, enter the Security PIN that you defined when you first logged in to the AirWatch Admin Console. Once this is complete, navigate back to your Company OG and create the correct child OGs.

NOTE

In some cases, there may be some dependencies that will not allow for deletion, where other associate settings must be deleted first, such as Assignment Groups with configurations tied to enrolled devices.

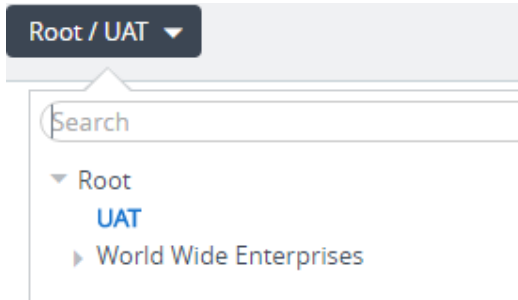
19. Navigate to any geographic OG and attempt to delete that OG. You will not be able to perform this action because all geographic OGs have child OGs. If you need to delete an OG with children, then you must delete all the children OGs prior to deleting the partner OG.



When an OG is deleted, all configurations and settings associated with it are erased as well. There is no option to restore this information; this is one reason why a Security PIN is required. Additionally, there are no options for moving or inserting OGs. For example, you could not

insert a new parent OG between your Company OG and your geographic OGs. For this reason, it is always important to ensure that you build out your OG structure to scale for growth.

20. Expand the OG hierarchy and select the **Root** OG.
21. Using the sample OG topology hierarchy, define the name of your testing OG: **UAT**.



A User Acceptance Testing (UAT) OG allows you to configure settings and enroll devices into a sandboxed OG, which is not affected by settings configured in your production Company OG. The UAT OG will not have a disclosure arrow next to it, since it has no child OGs.

22. Define a unique **Group ID** and accept the default **Type**.
23. Adjust **Country**, **Locale** and **Time Zone** settings based on your region.
24. Click **Save**. Refresh your browser to view the updated OG name.

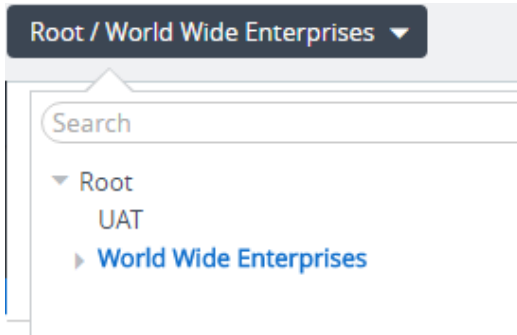
About Organization Groups

You can define Group IDs for every OG that you created, but do you plan to enroll devices into every OG? For example, would you enroll devices into the Company OG or rather into the business units or divisions below it? If a Group ID is not defined for an OG, no devices will be able to enroll into that OG. The OG name can be duplicated, as demonstrated with the multiple Sales and ITops OGs. If you plan to enroll a device into one of those OGs, a “unique” Group ID is required. When you start defining user accounts in the next lab activity, the placement of your users will dictate which OGs are available for enrollment.

Managing Users

Task 10: Adding a Basic User

1. Expand the OG hierarchy and select your Company OG.



2. From the Main Menu, navigate to **Accounts > Users > List View > Add > Add User**.

Create the user in the OG where you have a defined Group ID. Avoid creating the user in an OG where there is no Group ID defined.

There is also an option to perform a batch import of user data. If you wished to leverage this option, you could either perform a batch import or download the template for batch upload by selecting the **i** button.

- Complete all required fields (indicated with red asterisks) for a **Basic User**. For training purposes, make the username and password easy to remember. Be sure to use an active email address so that you will receive the activation email that is generated when **Save** is selected.

Add / Edit User

General Advanced

Security Type * Basic

Username *

Password * Show

Confirm Password * Show

Full Name *

Display Name

Email Address *

Email Username

Domain

Phone Number

Notice that the **Enrollment > Enrollment Organization Group** is defined as your Company OG. This means the user can enroll their device into any OG within your hierarchy, so long as they know the Group ID. If you change this setting to point to a lower Group ID, this will define into which OG(s) users are allowed to enroll.

For those using AirWatch Autodiscovery by with registered email domains, the **Enrollment Organization Group** field can funnel devices into a specific OG.

- Select **Enrollment > User Role** and note the built-in roles that are available. Leave the setting as Full Access. This role defines access permission in the AirWatch Self Service Portal, where users can manage their own devices. As an AirWatch Administrator, you can define what type of access users will have within their role. Custom roles can also be created to meet complex requirements.
- Click **Save** and verify you receive the user activation email, which includes enrollment instructions.

User activation emails can be customized by navigating to **Devices > Devices Settings > General > Message Templates**. If **Save and Add Device** was selected, then dependent device enrollment variables can be defined, such as friendly name and ownership type. When the device is enrolled, it will associate itself with these settings; these should be displayed in the device record. If token based enrollment was configured for this OG, a token would be sent to the user. Some user fields (such as username) cannot be changed.

LEARN MORE!

For training purposes, a directory user or user group will not be imported. If you are interested in learning more about directory services integration, view a recorded session, sign up for a live webinar or refer to supporting documentation in the Resources section of the myAirWatch portal.

Task 11: Reviewing User Management Options

1. Expand the OG hierarchy and select an OG under the location where the user was created.

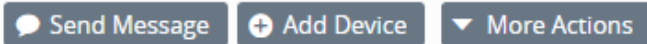
NOTE

The user is only visible at the OG where it was created/imported. This ensures AirWatch Administrators who are defined at lower OGs cannot alter user records defined at parent OGs.

2. Navigate back up to Company OG and select the check box next to your user to access common user functions.

NOTE

The **Add Device** button will associate a pending device record with the selected user; the pencil will allow for editing user fields; the unlock button is used to unlock an account which has failed to authenticate too many times.



3. Select **More** to review the menu options, which can be used to perform the following actions:
 - Add and remove user to/from User Group
 - Change Organization Group
 - Temporarily Activate/Deactivate user

- Delete the User Account

Management	Admin	Registration
Add To User Group	Deactivate	Add Device
Remove From User Group		Send Message
Change Organization Group		
Delete		

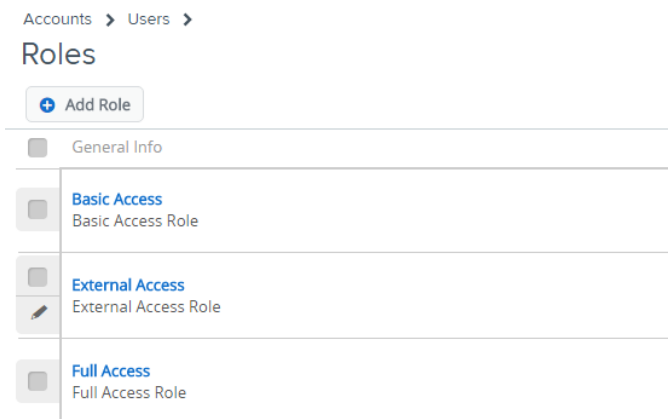
If you deactivate a user, they will not be able to enroll a device. Selecting **Change Organization Group** allows you to move a Basic user to another OG you are able to manage. You cannot delete a user if that user has a device enrolled. Should you wish to delete a user with an enrolled device, you would first have to deactivate the user account, which unenrolls the device. Once unenrolled, you may delete the account. Additional actions will be offered in the dropdown menu for users with enrolled devices, including the ability to view associated devices and verify their acceptance of any applicable Terms of Use policies.

4. Select the user to display the user record.

Task 12: Reviewing User Roles

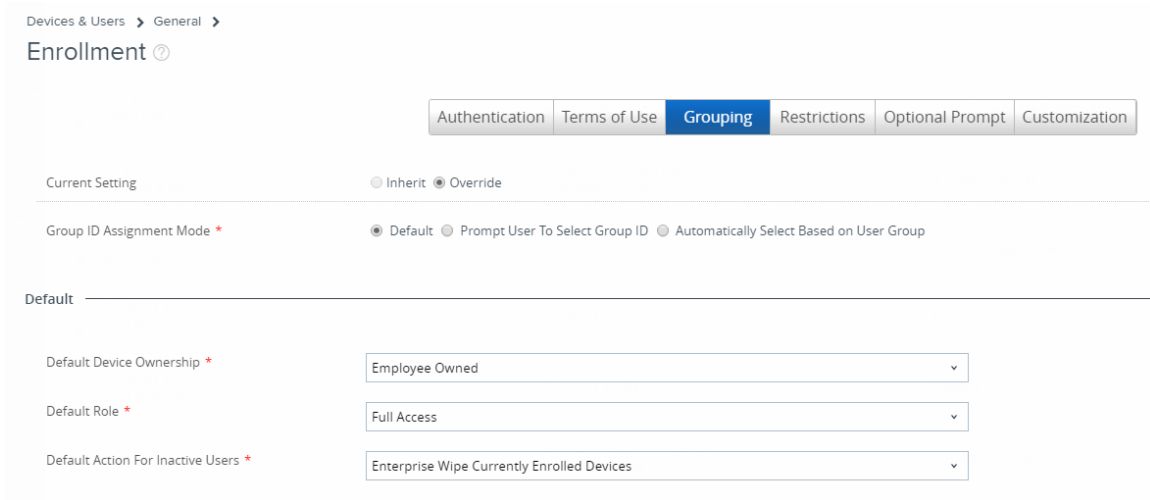
1. From the Main Menu, navigate to **Accounts > Users > Roles**.

All new or imported users can be defined within OG settings to have specific access to the AirWatch Self Service Portal. The Full, Basic and External Access roles cannot be changed since they are managed at the root OG (“Global”). If none of the roles match your deployment requirements, create a custom role by selecting “Add” and defining the required values.



Task 13: Reviewing Enrollment and Authentication Options

1. From the Main Menu, navigate to **Accounts > Users > Users Settings > Enrollment > Grouping** tab.



Devices & Users > General > Enrollment ⓘ

Authentication Terms of Use **Grouping** Restrictions Optional Prompt Customization

Current Setting Inherit Override

Group ID Assignment Mode * Default Prompt User To Select Group ID Automatically Select Based on User Group

Default

Default Device Ownership * Employee Owned

Default Role * Full Access

Default Action For Inactive Users * Enterprise Wipe Currently Enrolled Devices

The **DEFAULT** region displays the following fields:

- Default Device Ownership
- Default Role for AirWatch Self-Service Portal access
- Default Action for Inactive Users.

Other options are available should you choose not to leverage AirWatch Autodiscovery. These include options to change how the user is prompted to enter their Group ID (which may include a dropdown option for Group ID selection or filtering based on user group assignment) and defining user roles within user groups.

2. From the Main Menu, navigate to **Accounts > Users > Users Settings > Enrollment > Authentication** tab.

This tab enables to register your email domain with AirWatch Autodiscovery servers and additionally where you can define the authentication modes for users and enrollment.

Authentication Mode(s)	<input checked="" type="checkbox"/> Basic <input checked="" type="checkbox"/> Directory <input type="checkbox"/> Authentication Proxy
Devices Enrollment Mode	<input type="radio"/> Open Enrollment <input checked="" type="radio"/> Registered Devices Only
Require Registration Token	<input checked="" type="checkbox"/>
Registration Token Type	<input checked="" type="radio"/> Single-Factor <input type="radio"/> Two-Factor
Registration Token Length *	<input type="text" value="6"/> ⓘ
Token Expiration Time (hours) *	<input type="text" value="24"/>
Require Agent Enrollment for iOS	<input type="checkbox"/>
Require Agent Enrollment for macOS	<input type="checkbox"/>

If you selected **Override** as Current Setting, authentication modes and device enrollment methods could be modified here.

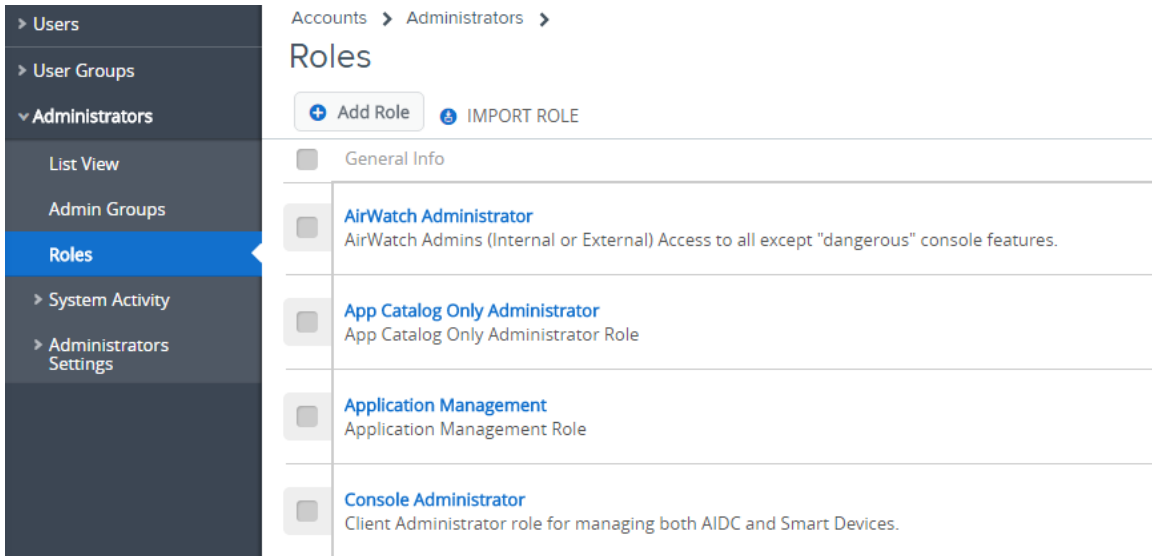
Regarding “Open Enrollment”: Users are able to enroll their devices, as long as they know their user credentials. This includes directory-based users who have not been imported into AirWatch. If you wish to limit enrollment to only import directory users and user groups, refer to the **Restrictions** tab on this page for details. If **Registered Devices Only** is selected, then the setting for token-based enrollment can be configured. There are also options to enforce enrollment using the AirWatch Agent rather than the native browser for iOS and Mac OS X.

Managing Administrators

Task 14: Adding a Custom Administrator Role

1. Expand the OG hierarchy and select your Company OG.

- From the Main Menu, navigate to **Accounts > Administrators > Roles**.



- Click Add Role.
- Define the following role fields:
 - Name:** Regional Admin - studentnumber
Example: Regional Admin - 001
 - Description:** Device Manager
- Expand **Device Management** using the disclosure arrow to display child categories.
- Click **Device Management** to display the Read and Write permissions in the right pane.

7. Click the radio button next to **Device Management** and choose **Edit**.

Name *

Description *

Categories

	Read	Edit	Category	Name	Description	
<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Bulk Management	Bulk Management	Perform bulk actions on devices from the device list view.	Details
<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Certificate Management	Certificate Management	View and manage certificates under device management.	Details
<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Compliance	Compliance	View and manage device compliance policies under device management.	Details
<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Custom Attributes	Custom Attributes	Custom Attributes	Details
<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Dashboard	Asset Tracking	Access to the asset tracking page under device management.	Details
<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>	Dashboard	View Dashboard	View the device dashboard page within device management.	Details
<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Device Details	Android File Manager	Remotely managed android files and folders from the device details page.	Details
					Remotely install and removed	

If required, settings for each permission can be toggled on or off for both read and edit functions.

8. Click **Save**. Note that the role is listed for your Company OG.

Task 15: Adding Administrator User and Assign Roles


1. From the Main Menu, navigate to **Accounts > Administrators > List View > Add > Add Admin**.

Accounts can also be imported using the Bulk Import button.

2. Click **Basic** for **User Type** to define a basic administrator role and complete all required fields (indicated with red asterisks).

Add / Edit Admin

Basic Details Roles API Notes

 Directory Admin Accounts can only be created from the Organization Group of the Directory Service.

User Type	<input type="radio"/> Basic <input checked="" type="radio"/> Directory
Username *	<input type="text" value="deviceadmin001"/>
Password *	<input type="password" value="....."/> Show
Confirm Password *	<input type="password" value="....."/> Show
Require password change at next login	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
First Name *	<input type="text" value="Device"/>
Middle Name	<input type="text"/>
Last Name *	<input type="text" value="Admin"/>
Email Address *	<input type="text" value="deviceadmin001@acme.com"/>
Time Zone *	<input type="text" value="(GMT-05:00) Eastern Time (US & Canada)"/> ▼
Locale *	<input type="text" value="English (United States) [English (United States)]"/> ▼

The password must be alphanumeric and minimum 6 character long. It could also be forced to change when the “new” AirWatch Administrator logs in. By default, no email is sent to the “new” AirWatch Administrator, though the Message Type field could be adjusted for this delivery.

3. Select the **Roles** tab.
4. From the **Organization Group** field, select a region within your OG hierarchy and define the Role as an **AirWatch Administrator**.
5. Click **Add Role** under the Organization Group you defined, and select a different region within your OG hierarchy. Define the Role as a **Regional Admin - XXX**.

The screenshot shows the 'Add / Edit Admin' interface with the 'Roles' tab selected. At the top, there are tabs for 'Basic', 'Details', 'Roles', 'API', and 'Notes'. Below the tabs is a '+ Add Role' button. The main area contains a table with two rows of roles. Each row has a checkbox, an 'Organization Group' field, and a 'Role' field. The first row has 'Root / World Wide Enterprises / North' and 'AirWatch Administrator'. The second row has 'Root / World Wide Enterprises / EMEA' and 'Device Admin - 001'.

6. Click **Save**.

NOTE

If saving the admin fails, ensure none of the checkboxes next the roles are selected, and the password is at least six characters in length and is a mixture of letters and numbers.

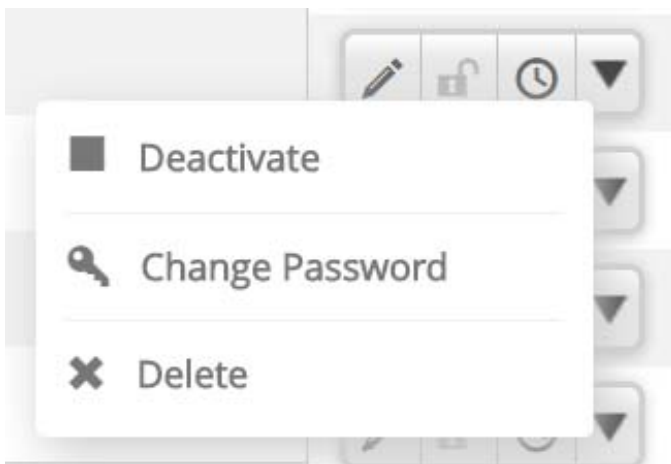
Reviewing Administrator User Management Options

Navigate to the Administrator Management page at **Accounts > Administrators > List View**. Use the actions menu to implement key management functions for ongoing maintenance and upkeep of admin accounts.



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

Click the down arrow for the admin account and review the available options.



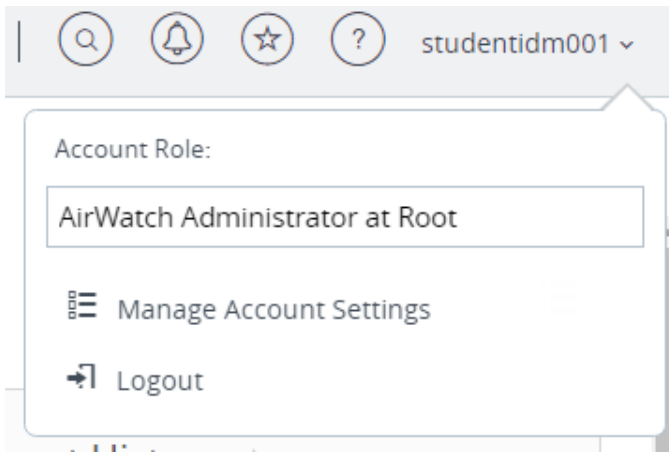
Passwords cannot be changed within AirWatch for directory-based accounts. Work with your directory administrator to manage passwords for these accounts.

Task 16: Logging in with a New Admin User and Test Role Permissions

1. Select your **username** from the Header Menu.

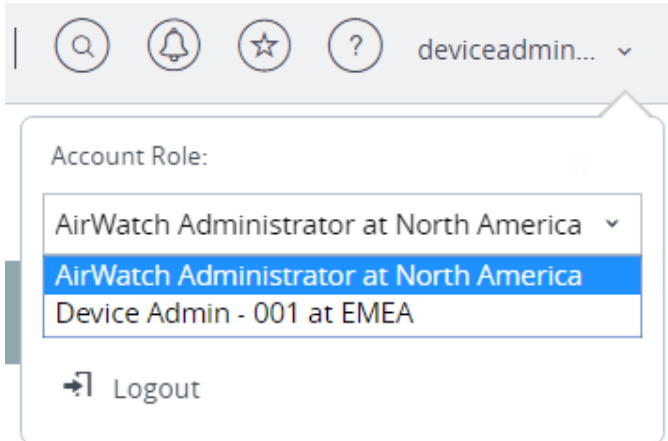
Note that the AirWatch Administrator account, with which you are currently logged in, has an AirWatch Administrator role at the Root OG.

- Note that the role is singular, and there is no drop-down arrow (as depicted in the included image) to select a different role.



- Click **Logout**.
- Log back in with the “new” AirWatch Administrator account you built.
The password is case sensitive.
- Click **Login**.
- Read and verify that you accept the AirWatch Terms of Use agreement.
- Define a four-digit Security PIN.
- Close the AirWatch Console Highlight page.

- Review the options in the navigation panel and then select **Account Role**.



The Account Role now displays two options. These are based on the roles that you defined for this AirWatch Administrator account.

- Toggle to the other role and note the differences between the roles you defined. For example, email access for managed devices (where email is being routed through an AirWatch-monitored email solution) is not visible in the Main Menu when the Device Manager role is enabled. The OG will also change based on assignment.

As an AirWatch Administrator, you have full control over the AirWatch Administrator accounts you build in AirWatch or import from directory services, as well as for their role-based permissions.

- Click **Logout**, then log in again using the AirWatch Administrator account that was previously assigned to you.

NOTE

You are logging in again with the AirWatch Administrator account that was previously assigned to you. This is because it has access to your Root OG with full role-based access.

Enrolling Devices

Task 17: Unenrolling Your Device

Your device should still be enrolled via the AirWatch Agent. This enrollment is based on the work previously accomplished during the “Introduction to AirWatch” lab activity.

1. Perform the following on your iOS or Android device to unenroll from full device management:

For iOS:

- Navigate to **Settings > General > Profiles**.
- Select the **Enrollment Profile**.
- Click the **Remove** button.

For iOS, access **Settings > General**. Select **Device Management > MDM Profile > Remove Management**. Provide the device passcode if prompted to supply one.

For Android:

- Open the AirWatch Agent and tap the **Menu** button

For tablets, this button is represented by the three dots in the top right corner of the AirWatch MDM Agent.

- Click the **Unenroll** option. If applicable, accept the prompt to remove any service apps.

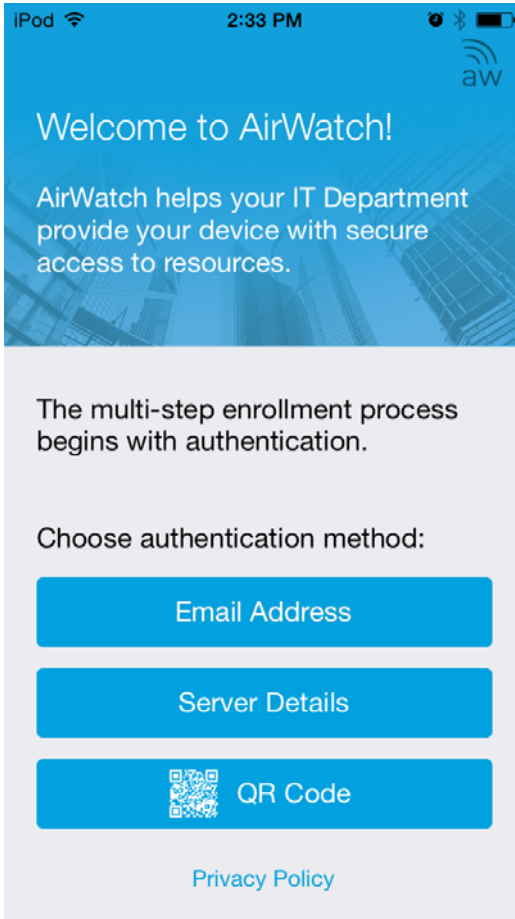
If device still appears as enrolled, delete the AirWatch Agent and re-install.

Task 18: Enrolling with the AirWatch Agent

1. Open the AirWatch Agent. If not installed, navigate to AWAgent.com to locate and download the AirWatch Agent to your device.

AWAgent.com determines the platform of the device and forwards the device to the platform-appropriate public app store, which prevents confusion with direct app access. A valid Apple ID or Google Play account is required to install the AirWatch Agent.

1. Open the **Agent** app and Click **Server Details**.



Enrollment cannot be completed using your email address, since the email domain was not registered with AirWatch Autodiscovery in the training environment.

2. Enter the **Server**, which is the URL of the AirWatch Admin Console, and the **Group ID**, which you defined for business unit under your geographic region, such as Sales or ITops.

NOTE

View the Group ID by placing your cursor over the OG hierarchy to display the OG name and Group ID. This feature may not be supported for all browsers.

3. Click **Next** to proceed with the enrollment process.
4. Input the user credentials you defined for the user.

NOTE

You defined the User Credentials in the lab. If you cannot remember the password, you can edit the user to change it. The password is case-sensitive.

5. Accept the **Terms of Use** policy you defined earlier.
6. Select the option prompted to continue with the enrollment process, such as **Redirect & Enable** for iOS.

NOTE

If the user will not authenticate, navigate to the user within the AirWatch Admin Console and change the password before trying again. Verify that the user is at an OG at the same level as the Group ID you defined or higher. In a previous lab, you were instructed to add the user at the Company OG. The user will be unable to be authenticated if it is in the OG below the Group ID that you defined. Verify the Enrollment OG is set as the Company OG so that the user can enroll into any OG within your hierarchy. If failure still occurs, exit and close the AirWatch Agent and restart the enrollment process. You should still verify that the Group ID supplied here is one that you defined.

7. Depending on the platform, you should install, activate, and accept all prompts. Click **Done** to complete the enrollment.
 - **iOS** requires the user to install an Enrollment Profile and accept Remote Management.
 - Some **Android** platforms require the user to allow AirWatch as a Device Administrator and to install and activate additional Manufacturer Service Applications.
8. Accept any prompts to install any other AirWatch applications for subsequent lab activities.

Task 19: Windows 10 Enrollment

1. Login to your Windows 10 Virtual Machine (VM)
 - **Username & Password** were provided by the instructor

Username:

Password:

2. Navigate to awagent.com on any browser within the VM

NOTE

Agent app can be downloaded from **Windows store** as well by searching “**AirWatch Agent**” in the Store.

3. Download and Install the **AirWatch Agent** app
4. Launch the Agent and Click the **Server Details** method

5. Enter the **Server**, which is the URL of the AirWatch Admin Console, and the **Group ID**, which you defined for business unit under your geographic region, such as Sales or ITops.
6. Input the **User Credentials** you defined for the user.

NOTE

You defined the User Credentials in the lab. If you cannot remember the password, you can edit the user to change it. The password is case-sensitive.

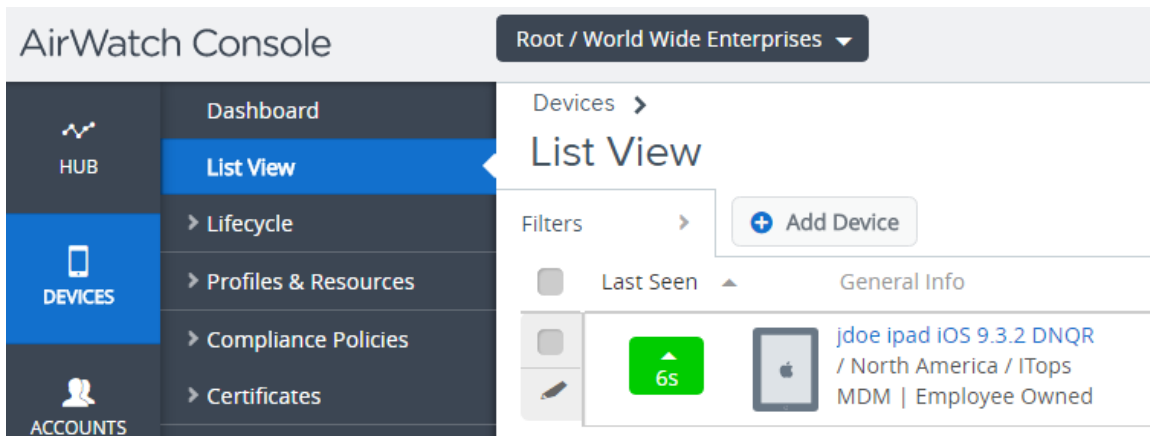
7. Click **Next**
8. Accept the **Terms of Use**
9. Click **Done**

NOTE

Only use the Windows 10 VM when explicitly directed to do so in the manual.

Task 20: Verifying Device Appears in the Device Dashboard

1. Expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate to **Devices > List View**.



3. Verify your device appears.

NOTE

If your device does not appear, verify you are at the Company OG. If the device is still does not appear, refer to the previous steps to unenroll and reenroll the device. Ensure the correct Server and Group ID have been entered.

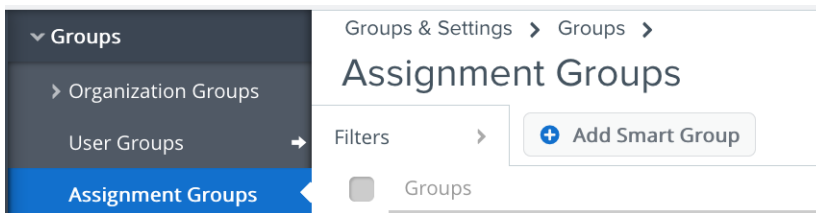
LEARN MORE!

If you are interested in learning more, view a recorded session, sign up for a live webinar or refer to supporting documentation in the Resources section of the myAirWatch portal.

Deploying Configuration Profiles

Task 21: Adding a Smart Group

1. Expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate to **Groups & Settings > Groups > Assignment Groups > Add Smart Group**.



3. Click **Add Smart Group**.

4. Enter All Devices in the **Smart Group** field.

Create New Smart Group

Choose Type:

Name:

Managed By: World Wide Enterprises

Organization Group All

- World Wide Enterprises
 - World Wide Enterprises / EMEA
 - World Wide Enterprises / North America
 - World Wide Enterprises / North America / ITops
 - World Wide Enterprises / North America / Sales

User Group Any

Ownership All

- Any
- Selected
 - Corporate
 - Employee
 - Shared
 - Unknown

Tags Any

Platform and Operating System Any

Model Any

Enterprise OEM Version Any

Devices in Smart Group

1 devices in group (1 total enrolled device(s))

Device Name	Username	Ownership	Platform/OS/Model
jdoe Ipad IOS 9.3.2 DNQR	jdoe	E	Apple IOS / 9.3.2 / I...

5. Accept the default options for **Select Criteria**.

NOTE

If **Select Devices or Users** was selected, the Smart Group could be assigned to specific users and/or devices for a very granular deployment.

6. Expand and review the criteria options shown on the left side. Filtering may be configured with specs for minimum OS, device models, ownership, tags, organization groups and more.
7. Verify your device appears in the **Devices in Smart Group** window. If not, verify you are at the Company OG and no filtered options are selected.
8. Click **Save**.

NOTE

The Smart Group will be tied to your Company OG for management with no assignments defined. Under devices, your device will be listed with a hyperlink option, since your device is in the scope of the filtered criteria of the Smart Group. When you define a profile, app, content, etc., you can assign these to a Smart Group, which will deploy to the devices you have filtered within the Smart Group criteria.

Task 22: Adding Profile Restrictions

1. At the Company OG, navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile**.
2. Select the platform you have enrolled.

Select a platform to start:



3. Define the following General properties:
 - **Name:** Camera Removal
 - **Assigned Smart Groups:** All Devices @ World Wide Enterprises
4. Hover over the other **General** options to review other options available for your deployment.

NOTE

Some options may require additional configuration, such as Allowing Removal, Device Exclusions or enabling a Geofencing zone/Time Schedule. Options may be different across

platforms. Refer to applicable platform guide in the myAirWatch portal via Resources for more details.

iOS Add a New Apple iOS Profile

General

- Passcode
- Restrictions
- Wi-Fi
- VPN
- Email
- Exchange ActiveSync
- Notifications
- LDAP
- CalDAV
- Subscribed Calendars
- CardDAV
- Web Clips
- Credentials
- SCEP
- Global HTTP Proxy
- Single App Mode
- Content Filter

General

Name *

Version

Description

Deployment

Assignment Type

Allow Removal

Managed By

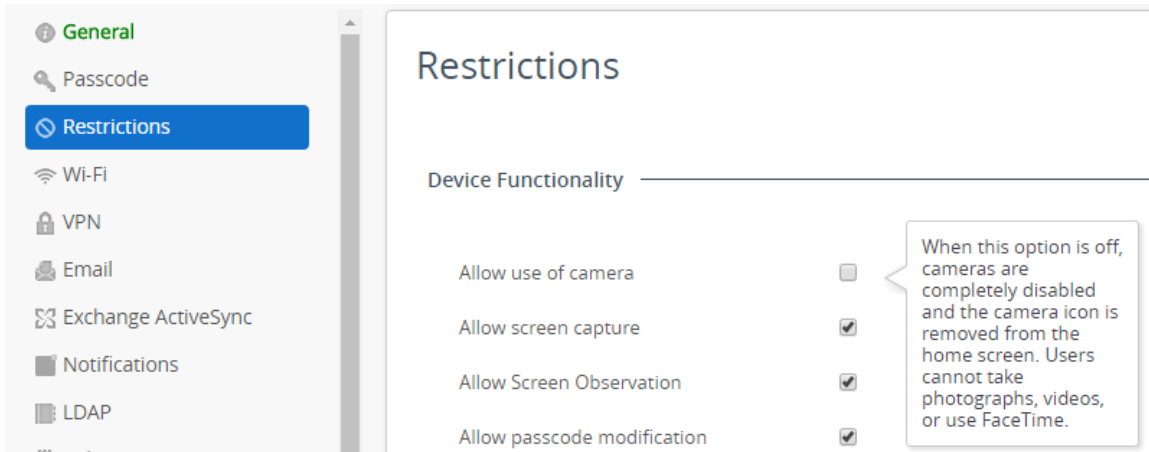
Assigned Groups

Exclusions

[View Device Assignment](#)

- From the left sidebar, select the **Restrictions** payload.
- Click **Configure**.

- De-select the option to **Allow use of camera**. Refer to the supported devices on the right side of the restriction to see if your enrolled device will be affected by this configuration.



If a payload option requires a minimum OS version, it is only available for select device types and/or requires special configuration. The specific requirements appear on the right side of the payload.

- Click **Save & Publish**.

Your device appears in the Smart Group.

- Click **Publish** to push the configuration to your device.

View Device Assignment			
Assignment Status	Friendly Name	User	Platform / OS / Model
✓ Added	jdooe iPad iOS 9.3.2 DNQR	jdooe	Apple iOS / iOS 9.3.2 / iPad

Items 1-1 of 1

NOTE

If other devices were part of this Smart Group assignment, they would also receive the configuration. If you Click **Cancel**, then you could add or remove Smart Groups to adjust you deployment plan.

- Go to your enrolled device and verify the camera has been removed. For supported Android devices, the Camera icon may still appear, but the functionality will be disabled.

11. To view the iOS configuration on the device, navigate to **Settings > General > Device Management > MDM Profile > Restrictions**.
12. You can view the Android configuration on the device by opening the AirWatch Agent, selecting profiles and viewing the configuration.

NOTE

If you made the profile removable in **General** settings, then the user would be able to remove the profile from the device.

Task 23: Adding a Wi-Fi Profile (Optional Based on Availability of a Wi-Fi Network)

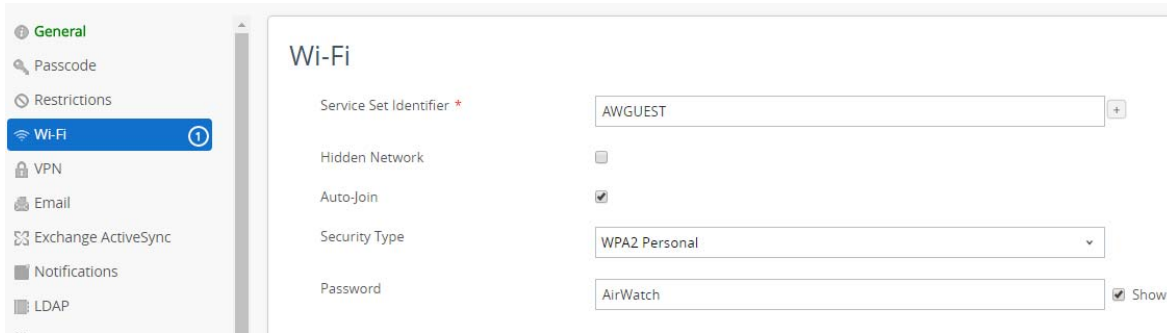
Create a Wi-Fi profile to connect devices to hidden, encrypted, or password-protected corporate networks. Wi-Fi profiles are useful for end users who travel to various office locations that have unique wireless networks or for automatically configuring devices to connect to the appropriate wireless network.

NOTE

You will need access to all the security information pertaining to the network in order to complete this task.

1. At the Company OG, navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile**.
2. Select the platform you have enrolled.
3. Define the following General properties:
 - **Name:** TBD by Network
 - **Assigned Groups:** All Devices (Company)
4. From the left sidebar, select the **Wi-Fi** payload, Click **Configure**.
5. Define the following:
 - **Service Set Identifier:** TBD by Network
 - **Security Type:** TBD by Network

- **Password:** TBD by Network



6. Click **Save & Publish** and verify your device appears in the **View Device** Assignment window.
7. Click **Publish** to push the configuration to your device.
8. Go to your enrolled device and verify that Wi-Fi configuration is available for connection without the password. If you are already connected to the same Wi-Fi network, the password will be removed when the device is unenrolled.

Task 24: Adding a Web Clip or Bookmark

Web Clips are web bookmarks that you can push to devices that display as icons on the device springboard or in your app catalog. You can even deploy the Self-Service Portal and app catalog as Web Clips.

1. At the Company OG, navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile**.
2. Select the platform you have enrolled.
3. Define the following **General** properties:
 - **Name:** myAirWatch
 - **Assigned Groups:** All Devices (Company)
4. From the left sidebar, select the **Web Clips** or **Bookmarks** payload.
5. Click **Configure**.
6. Define the following:
 - **Label:** myAirWatch
 - **URL:** `https://my.air-watch.com`
 - **Removable:** enabled

- **Icon:** Help_Desk.jpg
- **Precomposed Icon:** enabled
- **Full Screen:** enabled
- **Show in App Catalog / Container:** enabled

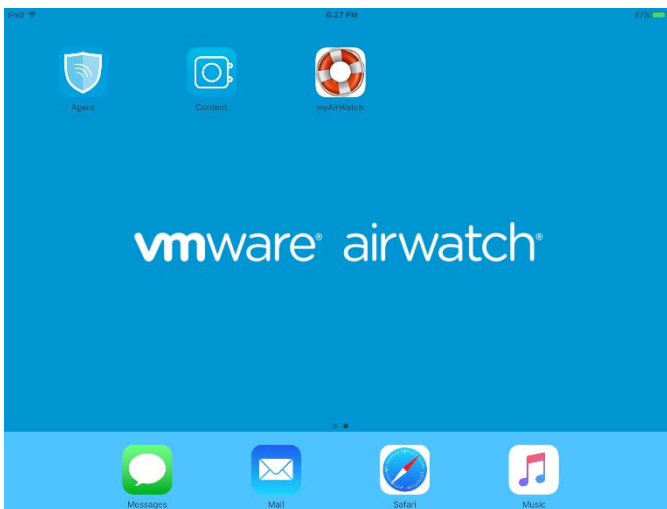
NOTE

Upload the Help_Desk.jpg from the Academic Success Kit. For Android, perform similar configurations, but ensure that **Add to Home screen** is enabled. This will push the bookmark to your device's home screen. If there is not room on the home screen of your device, then the bookmark will not be installed.

7. Click **Save & Publish** and verify your device appears in the **View Device Assignment** window.
8. Click **Publish** to push the configuration to your device.
9. Go to your enrolled device and verify the web clip or bookmark was successfully pushed down to the device.
10. Verify the web clip or bookmark displays `https://my.air-watch.com`.

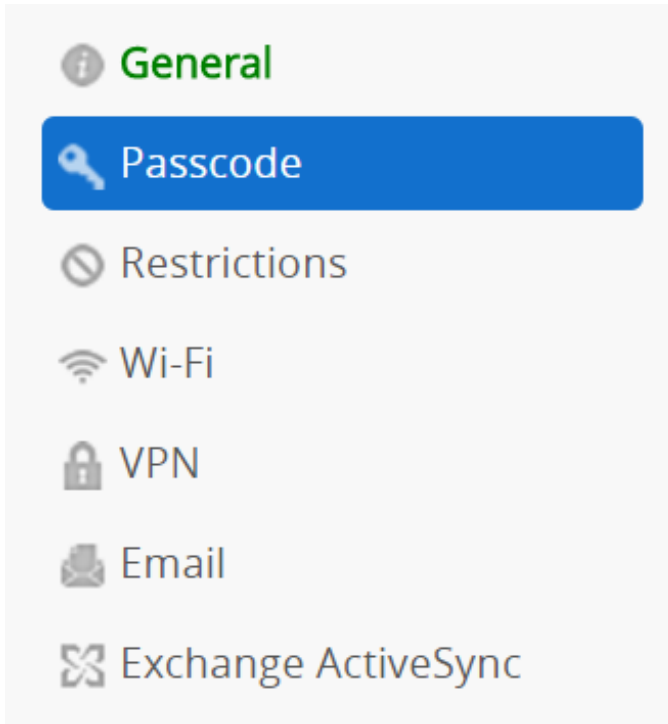
NOTE

Any profile created should include a single individual payload. For example, a Wi-Fi and Email configuration should not be paired together in the same profile, since removal of this profile will remove both configurations from the device. If they are created as separate profiles, then the Wi-Fi and Email configurations can be individually removed and troubleshot as needed.



Task 25: Reviewing Payload Capabilities

1. At the Company OG, navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile**.
2. Select the platform you have enrolled.
3. Review the other core payloads, such as Passcode, VPN, and Exchange ActiveSync.



4. Hover over each option to understand the functionality and requirements.
5. Exit the profile and create another profile. Select a different platform to compare functionality and options.
6. You will investigate email profile configuration in the MEM module using the Exchange ActiveSync payload.

Task 26: Reviewing Profile Management Options

1. Review the following options and actions:
 - Under Add, there are options to upload a profile or bulk import Wi-Fi profiles.
 - In the top right corner, perform a profile search, change the view, refresh the data or export the data in .csv.
 - Use the filtering toggles to filter profiles based on Status, Publishing State, Platform, Configuration Setting and Smart Group assignment.
 - On the left side, profiles can be disabled by selecting the radio button next to the profile name. Should a profile be disabled, the profile will be removed from all devices.

Devices > Profiles & Resources >

Profiles

Filters > ADD

Layout [refresh] [export] Search List

Profile Details	Managed By	Assignment Type	Assigned Groups	Installed Status	Status
<input type="radio"/> AirWatch Guest Wi-Fi Apple iOS Wi-Fi	World Wide Enterprises	Auto	All Devices	<input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 1 1	<input checked="" type="checkbox"/>
<input type="radio"/> Camera Removal Apple iOS Restrictions	World Wide Enterprises	Auto	All Devices	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 0 1	<input checked="" type="checkbox"/>
<input type="radio"/> myAirWatch Apple iOS Web Clips	World Wide Enterprises	Auto	All Devices	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 0 1	<input checked="" type="checkbox"/>

2. Select the number under **Installed** and then **Assigned** to view the different options. You should see your device listed with the option to remove or reinstall the profile. If zero is shown, this means that the profile is not yet installed or has a pending status.
3. Review the options in the buttons to the right, such as editing, copying, and viewing the devices which are being pushed the profile.
4. Click the down arrow to expand the menu and view the XML code for the profile, change your Smart Group assignments, or delete the profile.

Task 27: Defining Additional Assignment Options

1. At the Company OG, navigate to **Devices > Profiles & Resources > Profiles Settings > Areas**.
2. Select **Add > Geofencing Area**.
3. If the Terms of Use page appears, Click **Accept**. The Add/Edit Area page appears.
4. Define an **Address, Radius and Area Name**, and then Click **Click to Search**.
5. Click **Save**.

NOTE

0.5 miles is the smallest radius a profile can be deployed within a Geofencing radius.

6. Exit the Area page.
7. Navigate to **Devices > Profiles & Resources > Profiles Settings > Time Schedules**.
8. Click **Add Schedule**.
9. Define a **Schedule Name**, **Time Zone**, click **Add Schedule** to include today's day, and then Click **Save**.
10. Navigate to **Devices > Profiles & Resources > Profiles**.
11. Edit the **Camera Removal** profile, click **Add Version** to modify the profile, then enable **Geofencing** and **Time Scheduling**, and select the **Area** and/or **Schedule** you defined.
12. Click **Save & Publish** and verify you device appears in the **View Device Assignment** window.
13. Click **Publish** to push the configuration to your device.

NOTE

During the time the device is either reporting its location to AirWatch or is within the defined time schedule, access to the camera will remain disabled. Multiple factors, however, impact the pulling of device location data. This can range from not allowing the device to share location to the AirWatch Agent to the AirWatch Agent settings not being configured to pull location data and more. Geofencing profile functionality is currently only supported for iOS and Android devices; Time Scheduling is supported for most platforms.

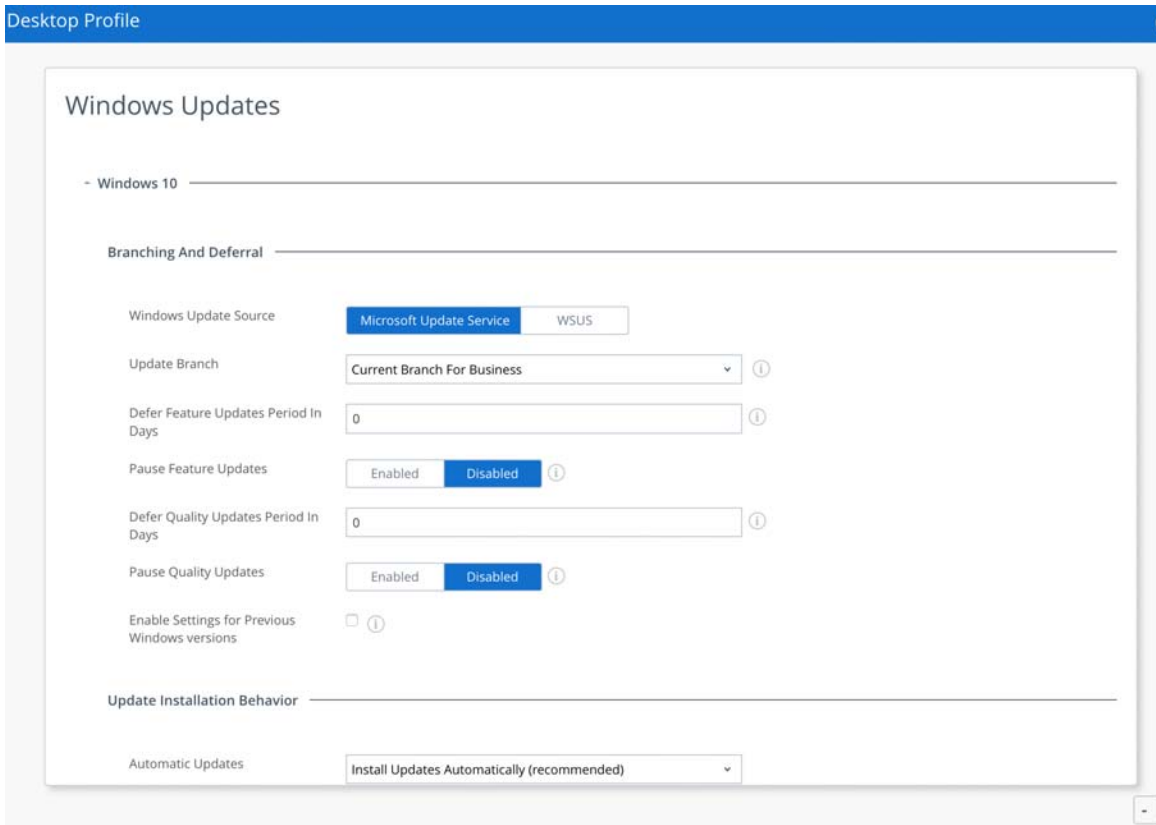
Task 28: Deploy a Windows 10 Update Profile

Create a Windows Updates profile to manage the Windows Updates settings for Windows Desktop devices. The profile ensures that all your devices are up-to-date, which improves device and network security.

1. Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**
2. Select **Windows** and then select **Windows Desktop**
3. Select **Device Profile**
4. Configure the **Profile General Settings**
5. Select the **Windows Updates Profile**
6. Configure the **Windows Updates Settings**:
 - a. Branching and deferral
 - b. Update Installation Behavior

- c. Update Policies
- d. Administrator Approved Updates
- e. Delivery Optimization

7. Click **Save & Publish**



Task 29: Deploy a Windows 10 App Control Profile

To allow or prevent installation of applications on devices, you can enable Application Control to whitelist and blacklist specific applications. While the compliance engine monitors devices for whitelisted and blacklisted apps, Application Control prevents users from even attempting to add or remove applications.

1. In the **Windows 10 VM**, Click on **Windows logo**
2. Enter **group policy**

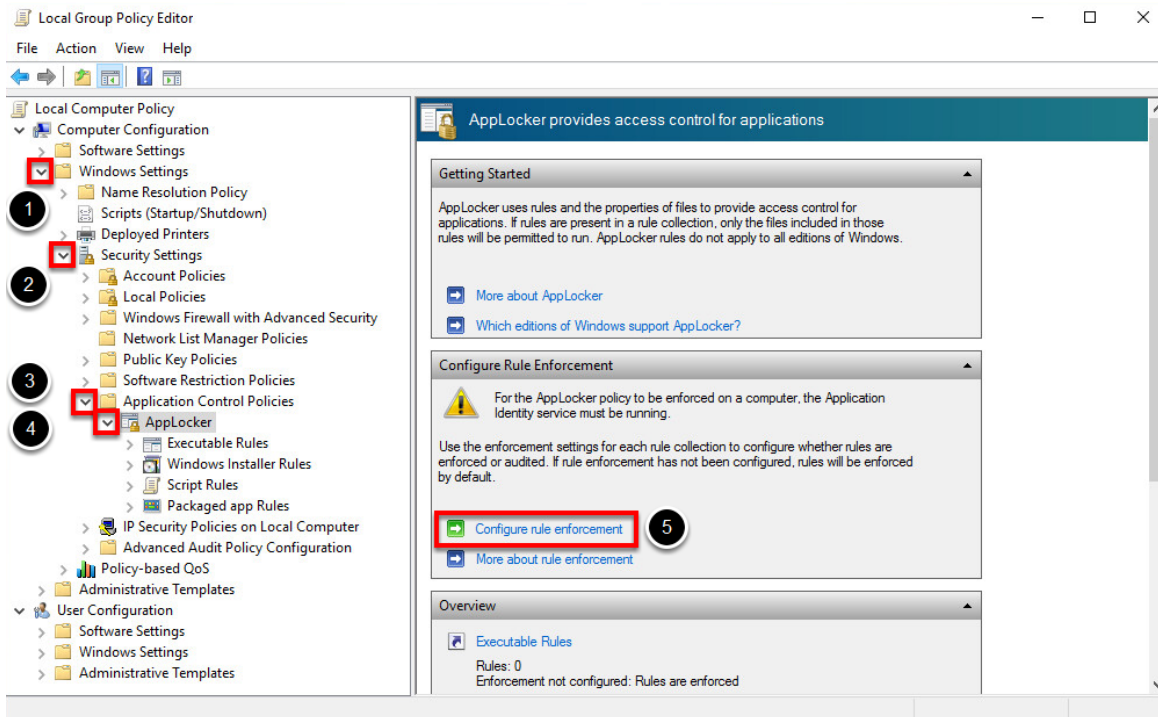
3. Click **Edit group policy**
4. Expand **Windows Settings**
5. Expand **Security Settings**
6. Expand **Application Control policies**
7. Expand **App locker**
8. Click **configure rule enforcement**

NOTE

In this example we will block the Xbox application (.appx).

CAUTION

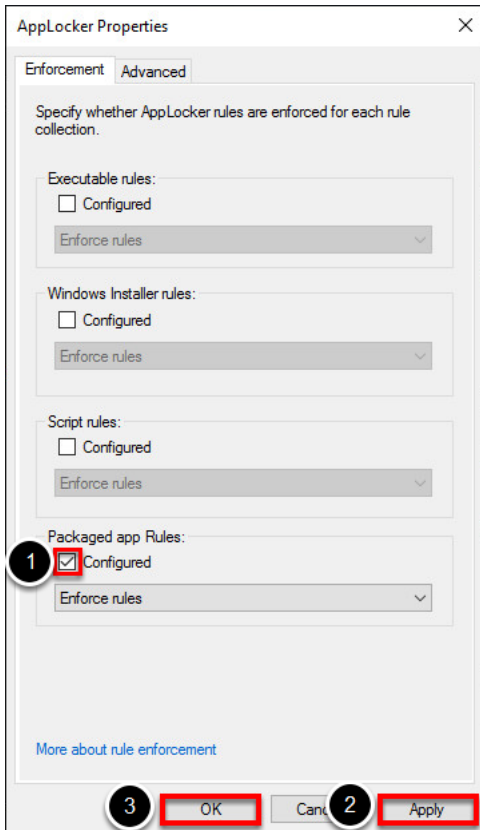
Failure to follow the steps as outlined will cause the VM to fail.

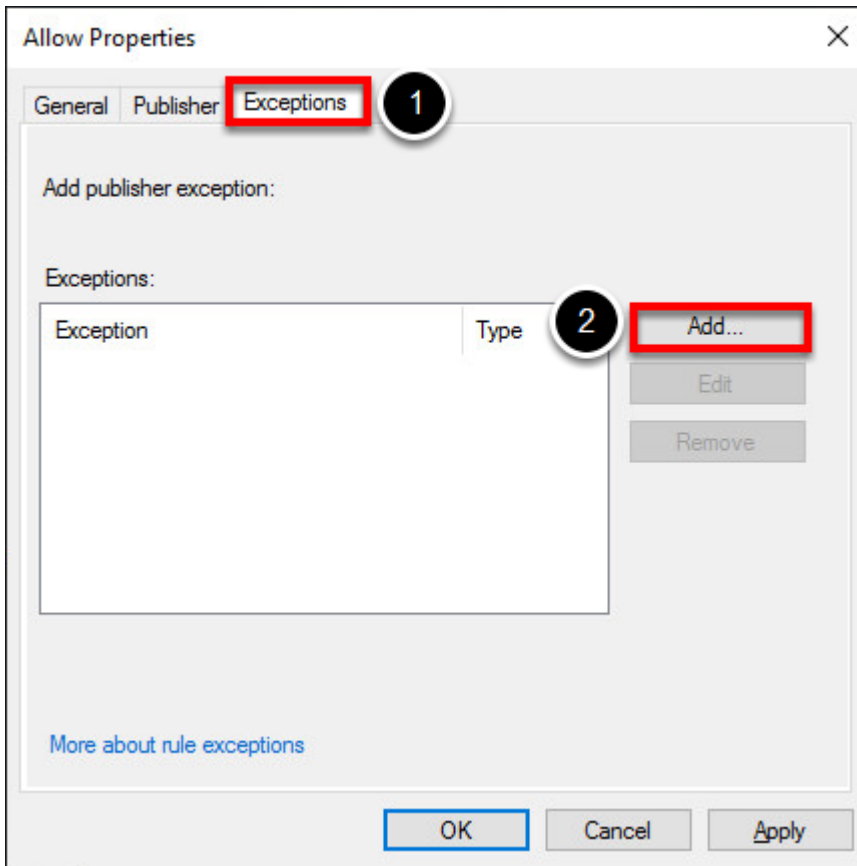


9. Check **Configured** under **Package app Rules**; Enforce rules option is default, if you want to test the rules before applying them, then you could run them in **Audit Mode** first.
10. Click **Apply**

11. Click **Ok**
12. Click **Packaged app Rules**, to start configuring the rules.
13. Right click in the white space to right of the window
14. Click **Create Default Rules**
15. Right click on the **Default Rule**
16. Click **Properties**
17. Click **Exceptions** tab

18. Click **Add**





19. Select **Use an installed packaged as a reference**
20. Click **Select**
21. Using the scroll bar, scroll to the bottom
22. Check the **Xbox** app with package name of the **Microsoft.XboxApp**
23. Click **OK**

NOTE

All the package's information is pre-populated. You can block the Xbox app based on the specific version, package name, or by the publisher. We want to block any version of the Xbox application.

24. Raise the lever from Package version to Package name

25. Click **OK**
26. Confirm the exception and click **Apply**
27. Click **OK**
28. Right click **AppLocker**
29. Click **Export Policy**
30. Select the **Downloads** directory
31. Enter **BlockXbox** in the **File Name** field
32. Click **Save**
33. Click **Ok**

NOTE

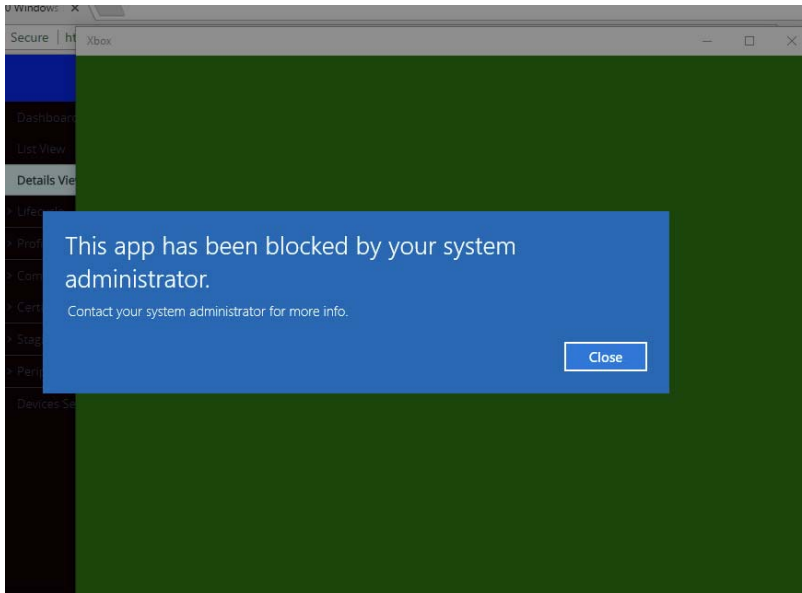
Now that you have exported the policy, we want to remove it from the test device (in this case the Windows 10 VM).

34. Right-click **AppLocker**
35. Click **Clear Policy**
36. Click **Yes** to delete the policy
37. Click **OK** to acknowledge the removal of policy
38. Close the **group policy editor** window
39. RETURN TO THE **AIRWATCH CONSOLE**
40. Ensure you are at company OG
41. Click **ADD** button at the top right corner of the console
42. Select **Profile > Windows > Windows Desktop**
43. In general tab, Enter "**Block Xbox**" into the Name field
44. Select your "All Devices" smart group for the Assigned Groups or the smart group/OG your device belongs to.
45. Select **Application Control** on the left-hand side panel
46. Click **Configure**
47. Check the **Import Sample Device Configuration** box
48. Click **Upload**
49. Click **Browse** and find the XML file created in the **Downloads** folder

50. Click on the **BlockXbox.xml** file
51. Click **Open**
52. Click **Save** once the XML has been uploaded
53. Click **Save & Publish**
54. Click **Publish** again upon ensuring the device shows up in the assigned devices list
55. Go back to **Windows 10 VM** and try to launch the **Xbox App**

NOTE

You should see the following error message:



Task 30: Configure Health Attestation Setting

The Health Attestation settings page allows you to configure the compromised status definitions for Windows Desktop devices

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Desktop > Windows Health Attestation**
2. Configure the **Health Attestation** settings
3. Click **Save**

Enforcing Mobile Security Policies

Task 31: Adding a Compliance Policy

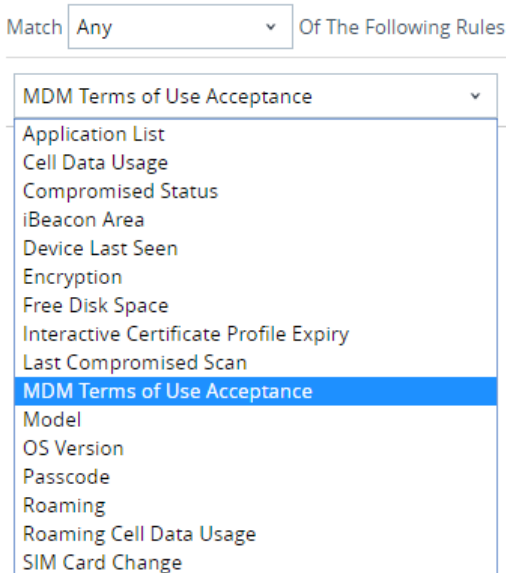
Adding a compliance policy is a process comprising four segments: Rules, Actions, Assignment, and Summary. Not all features and options presented in this guide are available for all platforms. The AirWatch Admin Console bases all available options on the initial platform choice, so the console never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

1. Expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate to **Devices > Compliance Policies > List View > Add**.
3. Select the **platform** you have enrolled.
4. Change Match field from **All** to **Any**.

NOTE

Using the **Any** setting, any rule that is violated within the list of rules that you create will trigger a compliance action. If **All** is selected, all conditions within the list of defined rules must be satisfied to trigger the compliance action.

5. Select the drop-down arrow next to the **MDM Terms of Use Acceptance** rule and review the available options.



NOTE

Different options may be available across different device platforms.

6. Change the **MDM Terms of Use Acceptance** rule to **Passcode**.
7. Click **Add Rule**, and choose **Compromised Status**.
8. Click **Add Rule**, and choose **Encryption**.

Match Any Of The Following Rules

Passcode	Is Not Present	+ x
Compromised Status	Is Compromised	+ x
Encryption	Is not encrypted	+ x

+ Add Rule

9. Click **Next** to define the actions.

NOTE

Based on these settings, if a device reports a missing passcode, jailbroken or rooted status, or is not encrypted, then the first rule will be triggered. Some data access may require the AirWatch Agent, such as Compromised Status.

10. Accept the default for sending an email to the user as the first action. Note that someone can be copied (CC) on the email and that the Default Template can be replaced with one that is created by the AirWatch Administrator.
11. On the far right side, Click the + button to add another action. Click **Send Push Notification to Device**.

NOTE

This action will be triggered simultaneously with the email generation. The AirWatch Agent must be installed in order for push notifications to be received by the device.

Immediately perform the following actions Mark as Not Compliant

Notify	Send Email to User	CC: <input type="text"/>	<input checked="" type="checkbox"/>	+ x
Notify	Send Email to User	Default Template		
	Send Email to User	CC: <input type="text"/>	<input checked="" type="checkbox"/>	+ x
	Send SMS to Device	Default Template		
	Send Push Notification to Device			
	Send Email to Administrator			

+ Add Escalation

12. Click **Add Escalation** and accept the default for **1 Day**.

NOTE

Setting the threshold to occur within too small of a time range (such as 1 minute) may not give the device enough time to check in to AirWatch with an updated status. For example, what would happen if you were to define an escalating action to occur after 1 hour, but the default scheduled device check-in is set for every 12 hours? The device data would therefore not be updated until the next scheduled check-in, which would cause it to be deemed as noncompliant, with any associated compliance actions summarily being executed. Should the user open the AirWatch Agent, beacon data will be sent to the AirWatch MDM Server and the database would be updated to the most current compliance status.

- Click **Notify**, and view the available options. When notify is changed, the actions tied to that function also changes.
- Change **Notify** to **Profile** and accept the default for **Block/Remove All Profiles**.

This action will remove all profiles managed by AirWatch, though options to remove a specific profile or install a compliance profile could be defined. A compliance profile is an optional profile type, which could be created to make the device more restrictive to use should the device become non-compliant.

- Click the + button to add another action. Change **Notify** to **Application** and change the action to **Block/Remove All Managed Apps**.

NOTE

This action will remove all applications managed by AirWatch and will not remove personal applications from the device. Specific managed applications could also be removed by entering the Application Identifier. The Application Identifier can be found for enrolled devices in the application section of the Device Dashboard.

- Click the + button to add another action. Change **Notify** to **Email** and change the action to **Block Email**.

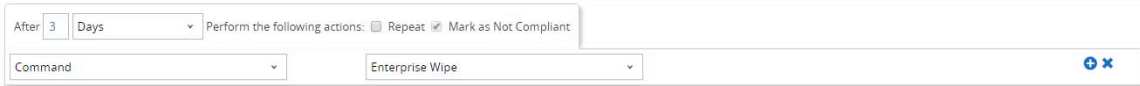
The screenshot shows a configuration window for actions. At the top, it says "After 1 Days" and "Perform the following actions: Repeat Mark as Not Compliant". Below this, there are three rows of actions, each with a dropdown menu for the trigger and a dropdown menu for the action:

Profile	Block/Remove All Profiles	+ x
Application	Block/Remove All Managed Apps	+ x
Email	Block Email	+ x

NOTE

If AirWatch is monitoring your email deployment, this compliance policy will tell the integration to block email. The email profile itself, though, will not be removed from the device configuration.

17. Click **Add Escalation** and review the different **After** hour/day options. Change the setting to **3 Days**.
18. Change **Notify** to **Command**, and change the action to **Enterprise Wipe**. Click **Next** to define the assignment.



The screenshot shows a configuration interface with the following elements:

- A dropdown menu set to '3 Days'.
- Text: 'Perform the following actions: Repeat Mark as Not Compliant'.
- A dropdown menu set to 'Command'.
- A dropdown menu set to 'Enterprise Wipe'.
- A blue plus icon and a red 'x' icon in the top right corner.

NOTE

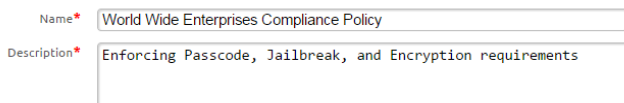
An enterprise wipe will remove all AirWatch functionality provisioned to the device. It will not, however, remove the AirWatch Agent, since you installed the AirWatch Agent prior to enrollment. Other commands will be offered depending on the type of device selected. The Full Wipe option is not offered; a Full Wipe can only be performed by an AirWatch Administrator. The Compliance Engine is built to automate policy management, and it would be foolhardy to entrust any automated system with the ability to wipe personal data without explicit administrator permission. In some cases, you may not want to enterprise wipe a device as the last action, and rather remove all the AirWatch functionality, so the device is still managed and email the administrator to follow-up.

19. For **Assignment**, define the following:
 - **Managed By:** Company OG
 - **Assigned Groups:** All Devices @ Company

NOTE

Additional Smart Groups or Exclusions could be defined. Use View Device Assignment to view impacted devices and accordingly adjust assigned Smart Groups.

20. Click **Next** to review the summary.
21. Under General, change the **Name** and **Description** to match the scope of the compliance policy.
22. Refer to the **Device Summary** to see how your device will be impacted by your compliance rule.



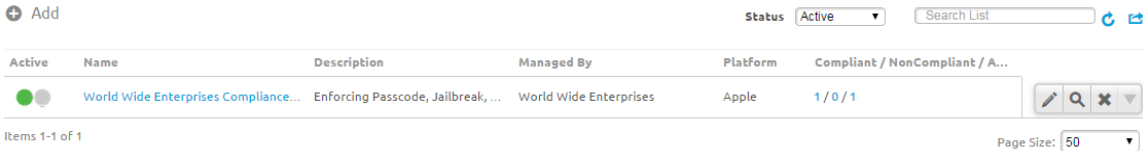
The screenshot shows a form with the following fields:

- Name***: World Wide Enterprises Compliance Policy
- Description***: Enforcing Passcode, Jailbreak, and Encryption requirements

NOTE

If your device is compliant, no actions will be triggered. If your device is noncompliant within 5 minutes, the first action in the list would be automatically performed.

23. Click **Finish and Activate**.
24. Once the compliance policy is saved, it can be changed from Active/Inactive or edited/deleted.
25. Under **Compliant / Noncompliant / Pending / Assigned**, hyperlinks to view impacted devices can be viewed. The **Magnifying Glass** icon will show similar data.



The screenshot shows a user interface for managing mobile devices. At the top left, there is a '+ Add' button. To the right, there is a 'Status' dropdown menu set to 'Active', a 'Search List' input field, and refresh/refresh icons. Below this is a table with the following columns: 'Active', 'Name', 'Description', 'Managed By', 'Platform', and 'Compliant / NonCompliant / A...'. A single row is visible with a green status indicator, the name 'World Wide Enterprises Compliance...', a description 'Enforcing Passcode, Jailbreak, ...', 'World Wide Enterprises' as the manager, 'Apple' as the platform, and '1 / 0 / 1' in the compliance column. To the right of the table are icons for edit, search, delete, and a dropdown arrow. At the bottom left, it says 'Items 1-1 of 1', and at the bottom right, there is a 'Page Size' dropdown menu set to '50'.

Active	Name	Description	Managed By	Platform	Compliant / NonCompliant / A...
<input checked="" type="checkbox"/>	World Wide Enterprises Compliance...	Enforcing Passcode, Jailbreak, ...	World Wide Enterprises	Apple	1 / 0 / 1

NOTE

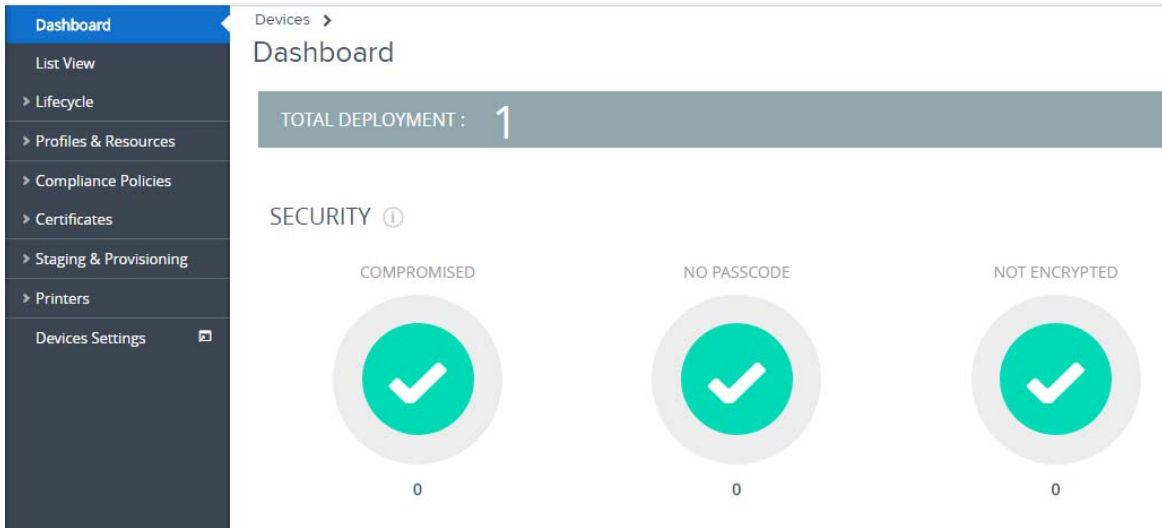
Since the compliance engine runs every 5 minutes against the database, the data shown may take up to 5 minutes to update.

Managing Your Devices

Task 32: Manage Your Device

1. Expand the OG hierarchy and select your Company OG.

- From the Main Menu, navigate to **Devices > Dashboard**.

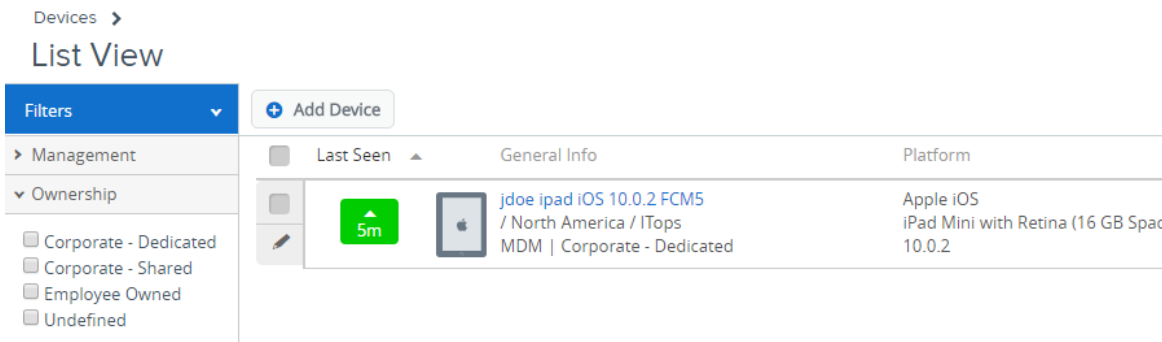


- All devices enrolled at this OG and below will be shown. Review the device details, such as security, ownership, last seen, platform and enrollment.

NOTE

Each option is hyperlinked to applicable devices, which are linked to the filtered view. If your device is compromised, has no passcode and/or is not encrypted, the device will only show as noncompliant if you have a compliance policy set to take action when any noncompliant status is detected.

- From the Main Menu, navigate to **Devices > List View**.
- Toggle the **Filters** button to adjust which devices are shown.



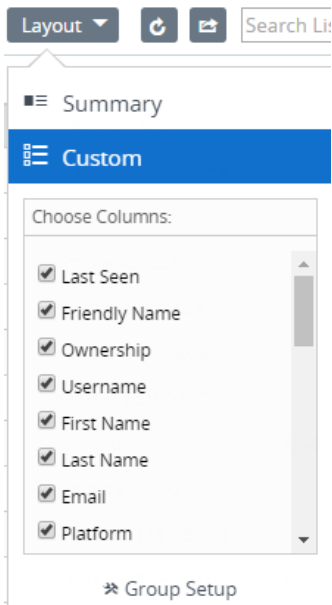
NOTE

Use **Add Device** to set up a pending device record for enrollment; this could be the issuance of an enrollment token. Use “Send Message to All” to send a message to all device within this OG, not just the ones shown in the filtered view.

- Review the different columns. **Last Seen** is when the device last checked in with AirWatch and device data was updated in the database. Under **General Info**, the Friendly Name of the device is shown.

The definition of the Friendly Name can be changed. To change the friendly name, navigate to **Devices > Devices Settings > General > Friendly Name**.

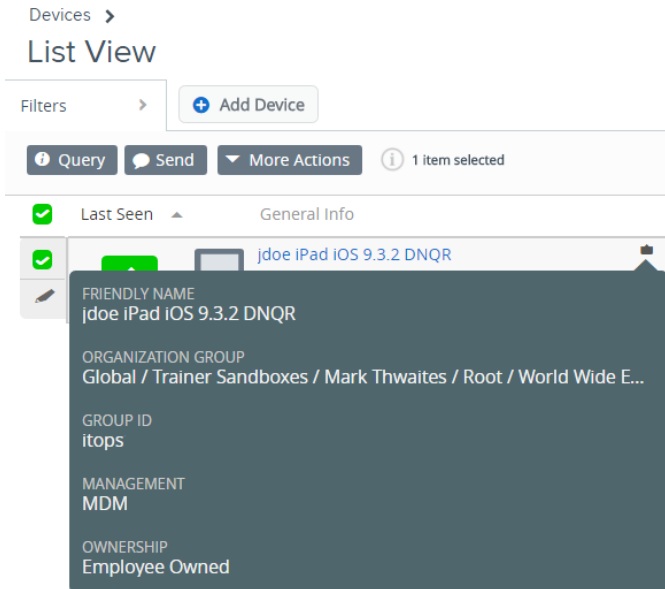
- Select the **Layout** button on the right side to change the view (e.g., include or exclude options). Additional options include manual refresh, data export and device search.



- Click the **Radio Button** next to the device to show bulk management options, including querying the device to check in, sending a message, locking the device and more. These actions can be executed on multiple devices at the same time by selecting all devices and then performing the necessary actions.

The edit button, represented by a pencil underneath the radio button, next to the device allows for editing device details.

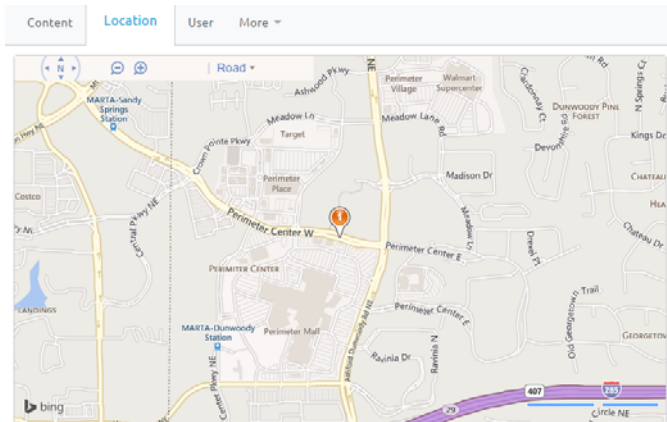
9. Hover to the right of the Friendly Name to view the **Folder Icon**, which shows additional details, most importantly the Group ID.



10. Select the **Friendly Name**, such as **jdoe iPad iOS 9.3.2 DNQR**. The Device detail page appears.
11. Select each tab and view the respective device details, such as a Summary, Compliance, Profiles, Apps, and Content.

Some tabs will allow for both the removal and re-pushing of configurations and functionality, such as profiles and applications.

12. Select the **Location** tab to view the location of the device.

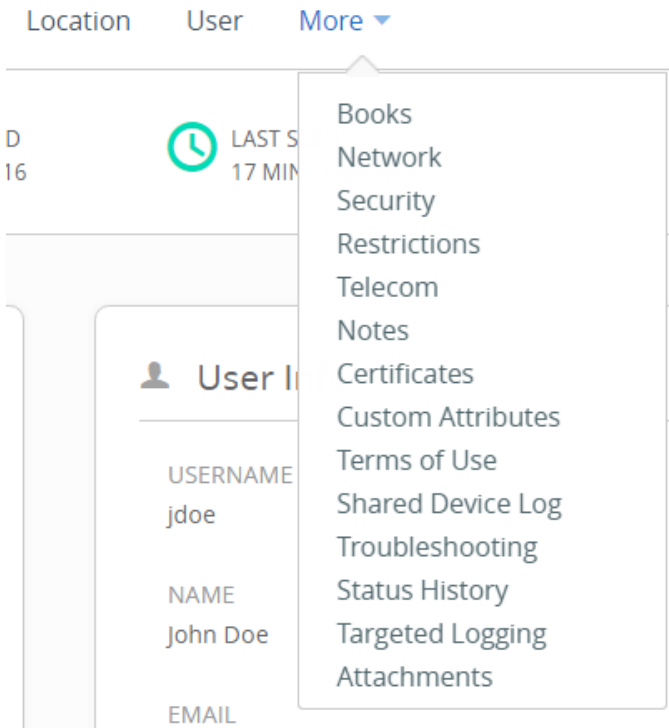


NOTE

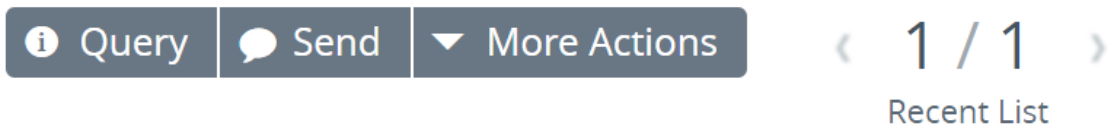
Multiple factors can impact whether the location appears in the console. Refer to the **Profiles** section within the console, where a geofencing zone was defined, for more details.

13. Select the **More** tab for additional options, such as Network, Notes, Terms of Use acceptance, Troubleshooting, Targeted Logging and attachments.

Some platforms may show additional options, such as Books for iOS.



14. From the top right corner, review the device commands that can be performed.
15. Use **Recent List** to toggle back and forth to next device viewable at this OG.



16. Click **Send**, and review the message types.
17. Click **Push Notification**.

NOTE

With iOS devices, the AirWatch Agent should be shown as the Application Name. If not, ensure that the AirWatch Agent is installed on the device, open it and ensure it states the device is enrolled.

18. Click **Send** to send the test message to your device. Verify your device receives the notification.

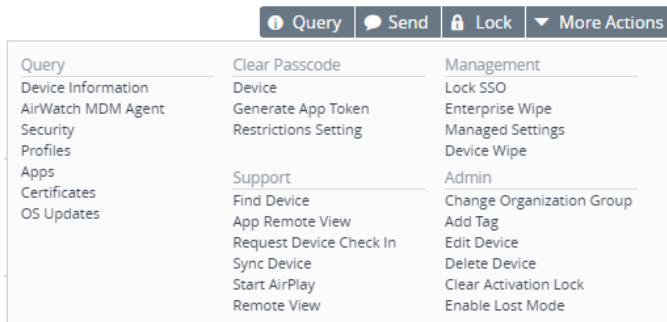
The screenshot shows a 'Send Message' form. At the top is a blue header with the text 'Send Message'. Below the header, there are three main sections. The first is 'Message Type *', which has a horizontal button menu with three options: 'Email', 'Push Notification' (which is highlighted in blue), and 'SMS'. The second section is 'Application Name *', which is a dropdown menu currently showing 'AirWatch Agent' and has a small circular information icon to its right. The third section is 'Message Body *', which is a large text input area containing the text 'Test Message' and a small plus icon to its right.

NOTE

The push notification message will be sent to the device through the supported messaging network (such as, APNs for iOS devices). If the AirWatch Agent is not configured to allow notifications, then no message will be received.

19. Click **More** and review the options. The following options are available:
 - **Query** the device to check in with updates to requested data.
 - **Clear** the Device Passcode.
 - **Erase** the device using an enterprise wipe (business data wipe) or full wipe (factory wipe).
 - **Find** a missing device using a chime/tone.
 - **Sync** the device to sync out of date profiles or apps that failed to install upon first push.
 - **Change** the Organization Group to a different OG within your hierarchy.
 - **Tag** to enable advanced filters within searches.

- **Delete** the device to enterprise wipe and remove the device record from AirWatch.



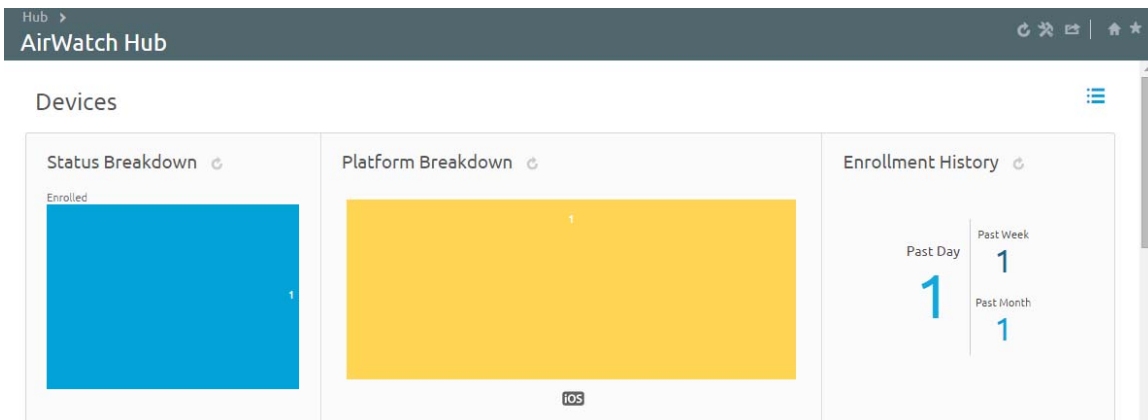
NOTE

The **Full Wipe** option may be hidden from your view since it is being restricted in the privacy settings. If you decide to enable this function, then you are liable should you perform this action on your device. Other options may additionally be available based on the platform.

Task 33: Using the AirWatch Hub

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

1. Expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate to **Hub**.
3. From the top right of screen, change the view from a Tabular View to Chart View and back.



4. Scroll down and review the options for Devices, Compliance, Profiles, Apps, Content, Email, and Certificates.

NOTE

The AirWatch Hub is your central portal for fast access to critical information. Each option is hyperlinked to respective devices, which are linked to the filtered view. Some actions may allow for a message to be sent to filtered devices.

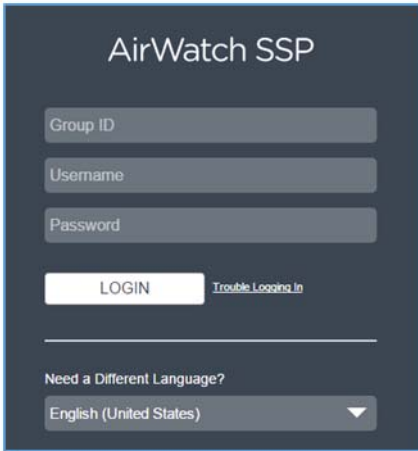
Task 34: Using the Self Service Portal (SSP)

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

1. On your computer, open a separate tab in your browser.
2. Navigate to: {instructor Provide}/MyDevice

NOTE

Replace “#” with the number of your training environment



3. Log in using the same credentials (Group ID, Username and Password) used to enroll your device into AirWatch.

NOTE

The SSP allows end users to monitor and manage their devices remotely from a central site. Available actions can range from simply viewing device information to performing remote actions on their devices. As an AirWatch Administrator, you can control what access end users have based on their user role, which is configured in their user account.

4. Under **Basic Actions**, perform the following actions on your enrolled device:
 - Make Noise
 - Send Message

NOTE

For Make Noise, the ringer will ring so long as the volume is not muted. In the AirWatch Admin Console, this is referred to as “Find Device.” The sound can be halted by opening the AirWatch Agent to disable it. When sending a message, choose to send out an email, as you can verify receipt in your email inbox. SMS is an available option, provided that you have

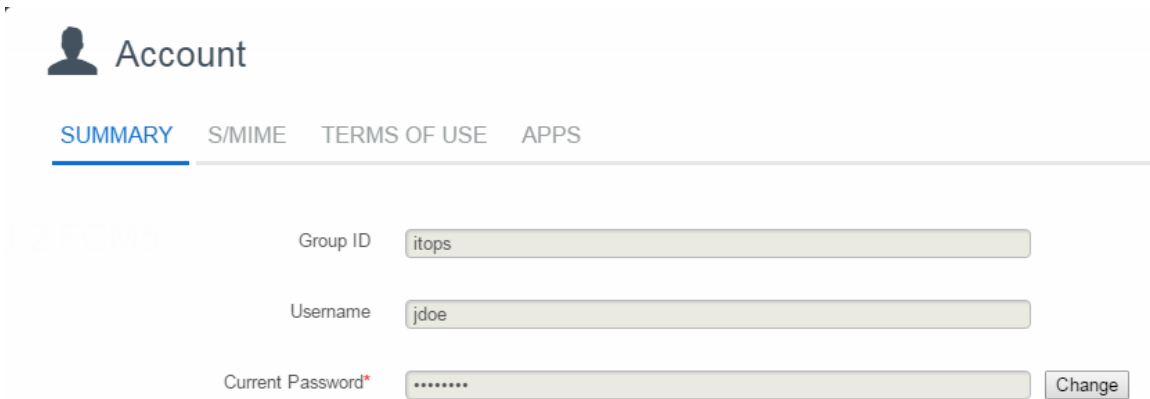
integrated with a third party vendor, such as CellTrust, to send SMS messages. SMS integration will have a separate fee structure.

The screenshot shows a mobile device management interface for an iPad. At the top, there is a header for the device: "jdoe ipad iOS 10.0.2 ..." with a green checkmark and the word "Enrolled" below it. Below this, the device name "jdoe ipad iOS 10.0.2 FCM5" is displayed. A status bar shows "ENROLLMENT DATE 10/24/2016 11:33 AM", "LAST SEEN 10/24/2016 11:42 AM", and "STATUS Up to date" with a green checkmark. A "Go to Details" button is located on the right. Below the status bar, there are two tabs: "BASIC ACTIONS" (selected) and "ADVANCED ACTIONS". Under "BASIC ACTIONS", there are several actions listed: "Device Query" (Request updated information from the device.), "Sync Device" (Send updated company settings and data to this device.), "Locate Device" (Find the most recent location of this device.), "Make Noise" (Help find the device by making it ring.), "Send Message" (Send an email, push notification, or text message to this device.), and "Delete Device" (Delete the Device from Self-Service Portal.). Under "ADVANCED ACTIONS", there are: "Clear Passcode" (Clear the current passcode from this device.), "Lock Device" (Remotely lock this device to protect data.), "Enterprise Wipe" (Remove corporate settings and data from this device.), "Device Wipe" (Erase all data and return device to factory settings.), and "Set Roaming" (Set whether Roaming is enabled for this device.).

5. Click **Go to Details** to see if your device is missing any required items, such as profiles, applications, or content.

This block shows a portion of the status bar and a button. The status bar displays "STATUS" followed by a green checkmark icon and the text "Up to date". To the right of this is a grey button with the text "Go to Details".

- In the top right corner, Click **Account** and review options, such as Summary, S/MIME, Terms of Use acceptance, and Apps.



Account

SUMMARY S/MIME TERMS OF USE APPS

Group ID

Username

Current Password*

NOTE

S/MIME requires additional steps for full configuration. For Apps, there is an option to create a unique token to access VMware Content Locker. This is an optional method for login, and is an alternative to using your enrollment credentials for access.

- Exit the Account window.
- The **Add Device** option is used in the same capacity as in the AirWatch Admin Console, where a pending device record could be created to send the user a token for enrollment.
- Underneath **My Devices**, there is an option for **My Content**. This option is covered fully in the Mobile Content Management training. This option is only available for customers who have purchased the editing and collaboration module for content management.
- Use the **Logout** button to exit the SSP.

Lab 5 Mobile Email Management

Prerequisites

The Mobile Email Management (MEM) lab requires the core configurations you performed during the completion of previous lab activities. Required configurations include setting up an OG hierarchy with a defined Group ID, a sample user and an enrolled device.

Choosing an Email Integration Model

Task 1: Configuring an Email Integration Model

1. Expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate to **Email > Email Settings**.
3. Review the current Mobile Email Management (MEM) configuration.

4. Select **Test Connection** to verify communication between AirWatch and the MEM solution. The settings can be exported, as an XML file, at the OG where the MEM solution is configured.

Mobile Email Management Configuration

← Advanced ✓ Test Connection ⇄ Export Settings

Status	Enabled
Friendly Name	MEM_dep01
Email Server Type	Microsoft Exchange
Deployment Type	Exchange 2010

SEG PROXY SETTINGS

i In order to complete Mobile Email Management configuration, download and install the [AirWatch](#). For help with configuration, refer to the [AirWatch Mobile Email Management Guide](#).

Secure Email Gateway URL [http://\[redacted\]/segconsole/management.ashx](http://[redacted]/segconsole/management.ashx)

NOTE

Within the training environment, the AirWatch Secure Email Gateway is deployed at a higher OG. Once a MEM solution is configured, no other MEM solution can be defined at a child OG. For the purposes of this lab, an MEM solution will not be configured; it has already been deployed at a higher OG to enable other lab exercises.

Deploying and Securing Mobile Email

Task 2: Associating User with the AirWatch Training Exchange Account

Your currently enrolled device is not tied to a user that has an email account associated with an AirWatch email server. To complete the following lab, your user will require editing so that they can be associated with an email account tied to an AirWatch training Exchange server. In most cases, such as when a user is created or imported from Directory Services, their email address, email username and domain will be tied to an existing email account.

1. Expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate to **Accounts > Users > List View**.
3. Select your user and select **Edit**.
4. Scroll down and change the following fields:

- **Email Address:** student@training.saas
- **Email Username:** student
- **Domain:** training

Email Address *	<input type="text" value="s@training.saas"/>
Email Username	<input type="text" value="student"/>
Domain	<input type="text" value="training"/>

5. Select **Save**.

NOTE

student1@training.saas/student1 may be used as an alternate if access is blocked for maintenance.

Task 3: Deploying Mobile Email

1. At the Company OG, navigate to **Devices > Profiles & Resources > Profiles > Add Profile**.
2. Select the platform you have enrolled.
3. Define the following General properties:
 - **Name:** Corporate Exchange
 - **Assigned Smart Groups:** All Devices @ World Wide Enterprises

The **All Devices @ World Wide Enterprises** Smart Group were previously defined during the MDM lab exercise.

4. From the left sidebar, select the **Exchange ActiveSync** payload and select **Configure**.

The screenshot shows the 'iOS Add a New Apple iOS Profile' configuration screen. The left sidebar lists various settings, with 'Exchange ActiveSync' selected and highlighted in blue. The main content area is titled 'Exchange ActiveSync' and contains the following fields:

- Mail Client:** Native Mail Client (dropdown menu)
- Account Name *:** Corporate Exchange (text input)
- Exchange ActiveSync Host *:** (empty text input)
- Use SSL:**
- Use S/MIME:**

Below these fields is a section titled 'Login Information' with the following fields:

- Domain:** {EmailDomain} (text input with a '+' icon)
- Username:** {EmailUserName} (text input with a '+' icon)
- Email Address:** {EmailAddress} (text input with a '+' icon)
- Password:** (empty text input with a '+' icon and a 'Show Characters' checkbox)
- Payload Certificate:** None (dropdown menu)

Below the 'Login Information' section is a section titled 'Settings And Security' with the following field:

- Past Days of Mail to Sync:** 1 Month (dropdown menu)

5. Configure the following fields to deploy the Native Mail Client to your device. Accept defaults, if not defined.
- **Mail Client:** Native Mail Client
 - **Account Name:** Corporate Exchange
 - **Exchange ActiveSync Host:** <Instructor Provided>
 - **Password:** AirWatch

The password field would normally be left blank, but the password is being “baked” into the payload to expedite configuration for training.

NOTE

If you previously configured the user account with student1 @training.saas/student1, the password is AirWatch.

- **Past Days of Mail to Sync:** 1 Month

NOTE

For Android, the default email configuration is for the AirWatch Mail Client (AirWatch Inbox). If your device is not supported, configure the same settings for the AirWatch Mail Client, though the AirWatch Inbox will require installation on the device to utilize the associated email account.

6. Select **Save & Publish**. Based on your defined Smart Group, your device appears.
7. Select **Publish** to push the configuration to your device.
8. Open your device’s native Mail, Contacts and Calendar applications and verify they have synced successfully. Sample content that should have seeded to the device includes one month of sample email and selected individual contacts and events.

If the AirWatch Email Client profile was configured, be sure to install the AirWatch Inbox from the appropriate app store. The AirWatch Inbox can also be required and pushed down to devices as a managed application from the AirWatch Admin Console. To push the application, refer to the Mobile Application Management module. Email passwords cannot be pushed within this configuration; enter “student” when prompted for authentication.

NOTE

If the AirWatch Inbox profile was configured, be sure to install the AirWatch Inbox from the appropriate app store. The AirWatch Inbox can also be required and pushed down to devices as a managed application from the AirWatch Admin Console. To push the application, refer to the Mobile Application Management module. Email passwords cannot be pushed within this configuration; enter “student” when prompted for authentication. If you previously configured the user account with sl@training.saas/student1, the password is student1.

Task 4: Reviewing Alternate Email Configurations

1. At the Company OG, navigate to **Devices > Profiles > List View > Add Profile**.
2. Select the alternate platform to your actively enrolled device to review the various other payload options that are available.
3. Define the following **General** properties:

- **Name:** Corporate Exchange
- **Assigned Smart Groups:** All Devices @ Company

4. From the left sidebar, select the **Exchange ActiveSync** payload and select **Configure**.

General

Name*	Corporate Exchange
Version	1
Description	
Deployment	Managed ▼
Assignment Type	Auto ▼
Allow Removal	Always ▼
Managed By	World Wide Enterprises
Assigned Smart Groups	All Devices @ World Wide Enterprises ✕ Start typing to add a smart group 🔍

5. Toggle the **Mail Client** to a different option and review the options. If necessary, exit the creation of the profile and create another one, to view all supported mail client options.

NOTE

The Email Settings payload is used for configuring IMAP/POP3 accounts and does not use ActiveSync.

- When AirWatch Mail Client (AirWatch Inbox) is selected, review the DLP settings to protect email for entering or leaving the device and how the **Calendar and Contacts** is defined.

Restrictions

Restrict Copy-Paste

Disable Attachments

Maximum Attachment Size (MB)

Open all links in Airwatch Browser

Content Locker Only Attachments

Restrict Attachments To Be Opened In
The Following Apps

Applications

✕

 + Add

Allow Printing

- Exit out of the profile.

Enforcing Email Access Control

Task 5: Reviewing Email Compliance Options

- At the Company OG, navigate to **Email > Compliance Policies**.

2. Review the General Email Policies, Managed Device Policies, and Email Security Policies options.

Email >

Compliance Policies

General Email Policies

Active	Policy
<input type="checkbox"/>	Sync Settings
<input checked="" type="checkbox"/>	Managed Device
<input type="checkbox"/>	User
<input type="checkbox"/>	EAS Device Type
<input type="checkbox"/>	Mail Client

Managed Device Policies

Active	Policy
<input checked="" type="checkbox"/>	Inactivity
<input checked="" type="checkbox"/>	Device Compromised
<input type="checkbox"/>	Encryption
<input type="checkbox"/>	Model
<input type="checkbox"/>	Operating System
<input type="checkbox"/>	Require ActiveSync Profile

Email Security Policies

Active	Policy
<input type="checkbox"/>	Email Security Classifications
<input checked="" type="checkbox"/>	Attachments (Managed devices)
<input type="checkbox"/>	Attachments (Unmanaged devices)
<input checked="" type="checkbox"/>	Hyperlink

If you were at the OG where the MEM solution was configured, you would see options to activate, deactivate and edit compliance policies. Since the MDM solution was defined at a lower OG, unmanaged devices cannot be configured to traffic email through the AirWatch Secure Email Gateway, inactive devices will not be able to sync after a defined number of days, and attachments will be forced to open into VMware Content Locker. The command to Run Compliance may be executed at a lower OG.

LEARN MORE!

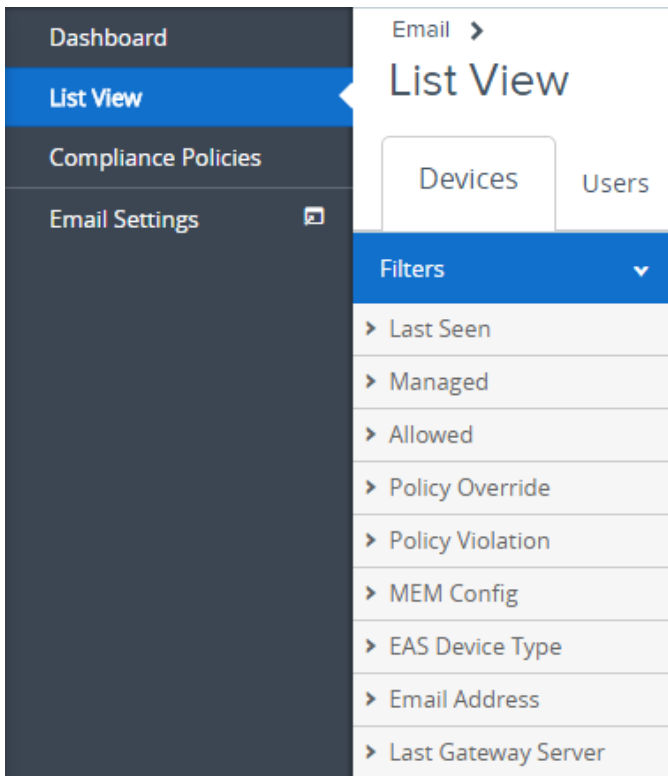
If you are interested in learning more about email compliance, view a recorded session, sign up for a live webinar or refer to supporting documentation in the Resources section of the myAirWatch portal.

Managing Mobile Email Access

Gaining Visibility into Mobile Email

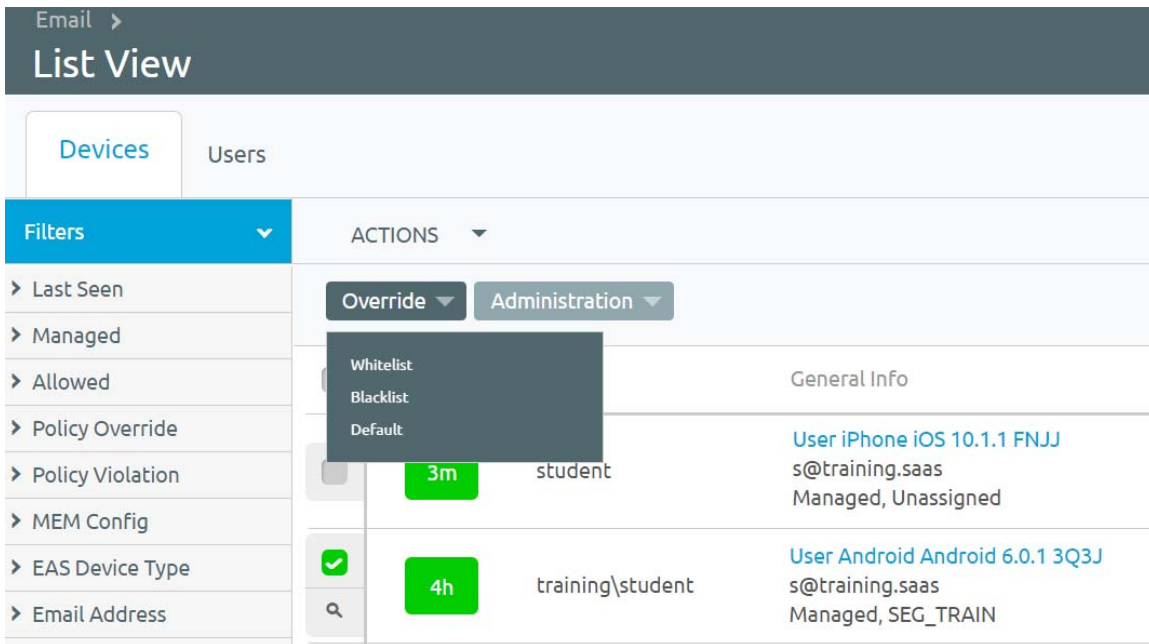
1. At the Company OG, navigate to **Email** and review the Email Management summary data.
2. At the Company OG, navigate to **Email > List View**.

3. Select the **Filters** arrow to adjust how devices and users are displayed under the **Devices** and **Users** tabs.



4. Select the radio button next to your device, select **Override**, choose **Blacklist**, and enter the provided code to blacklist the device.

- On the device, attempt to sync mail and observe that the sync fails. Try to send an email and note nothing is sent.



- Go back to the AirWatch Admin Console, select the radio button next to your device, select **Override**, choose **Default**, and enter the code to set the device back into its default state.
- On the device, attempt to sync mail and observe that the sync is restored and an email can be sent.
- Select the radio button next to your device and select **Administration**. The following options are available:
 - Enable/disable additional logging.

- Delete unmanaged devices.

The screenshot shows a web interface for mobile device management. At the top, there is a dark header with "Email >" and "List View". Below this, there are two tabs: "Devices" (selected) and "Users". A "Filters" dropdown menu is open on the left, listing options like "Last Seen", "Managed", "Allowed", "Policy Override", "Policy Violation", and "MFM Config". In the center, there is a table of devices. One device entry is highlighted, and a context menu is open over it. The context menu has three options: "Dx Mode On", "Dx Mode Off", and "Delete Unmanaged Device". The device entry shows a "Last Requested" status of "5m" (5 minutes ago) and a user named "training\student". To the right of the device entry, there is a "General Info" section with the text "User Android Android 6.0.1 3Q3Js@training.saas Managed, SEG_TRAIN".

Filters	ACTIONS	General Info
<ul style="list-style-type: none">> Last Seen> Managed> Allowed> Policy Override> Policy Violation> MFM Config	<ul style="list-style-type: none">OverrideAdministration	
<input type="checkbox"/>	Last Requested: 5m	User Android Android 6.0.1 3Q3Js@training.saas Managed, SEG_TRAIN

Lab 6 Mobile Application Management

Prerequisites

The Mobile Application Management (MAM) lab requires the core configurations you performed during the completion of previous lab work. Required configurations include an OG hierarchy set up with a defined Group ID, a test user and an enrolled device.

Managing Public Applications

Task 1: Adding a Public Application

1. Go back into the AirWatch Admin Console where you have your device enrolled, expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate **Apps & Books > Applications > List View > Public** tab.
3. From the Main Menu, navigate **Apps & Books > Applications > Native > Public** tab
4. Select **Add Application**.
5. Select the platform for your enrolled device, select **Search App Store** as Source option, and enter **Salesforce1** as the name of the application to search for.

NOTE

If Salesforce is installed on your device, please un-install it.

Add Application ✕

Managed By *

Platform *

Source *


Name *

6. Select **Next** and select the **Salesforce1** application from the provided search results.

If you are unable to locate the app you seek, either scroll through the results or alter your search terms. You can additionally verify that you are searching the correct app store by verifying that you are searching in the correct country.

Search ✕

Country



Salesforce1
com.salesforce.chatter
Free
Category: Business
Current Version: 11.0.2
★★★★★

Salesforce1 is a brand new way to experience Salesforce from any device and brings all your Chatter, CRM, custom apps, and business processes together in a unified, modern experience for any Salesforce user. With the power of the Salesforce1 Platform, you can now customize and build any app and instantly deploy that functionality through the Salesforce1 app.

7. Review the **Details** tab options, including adding comments, reimbursement information, ratings and categories.
8. Click on save and assign

9. **Update assignment** page pops up, click on **add assignment**

Managed Access Enabled Disabled ⓘ

App Tunneling Enabled Disabled ⓘ

Send Application Configuration Enabled Disabled ⓘ

ⓘ

Application Configuration

Configuration Key	Value Type	Configuration Value
<input type="text" value="AppServiceHosts"/>	<input type="text" value="String"/> ▾	<input type="text" value="vmwareairwatch-dev-ed.my.s"/> ✕

10. In the select Assignment Groups field type in the **All Devices@company** smart group created during MDM lab exercise
11. From the Deployments region, perform the following:
 - a. Set App Delivery Method to **Automatic: system push**.
 - b. Set **Application Configuration** to **Enabled**.
 - c. Input the following application configurations:

Configuration Key	Value Type	Configuration Value
AppServiceHost	String	Customer Salesforce URL Example: vmwareairwatch-dev-ed.my.salesforce.com

12. Click on **Add** button

NOTE

The update Assignment page will come back up and notice that the smart group now shows up with the priority 0 and rest of the configured settings like the push mode as Auto

13. Select **Save & Publish**.
14. Based on your defined Smart Group, your device will be shown. Select **Publish** to push the configuration to your device.
15. On your device, verify that you receive a prompt to install the application from the app store. The application will prompt differently on both devices. If the app has never been previously installed, iOS will prompt for your Apple ID; Android will similarly require a Google Play account to be configured on the device to install the application.

NOTE

If the app was pushed in an **On Demand** capacity, the application would be installed either through the AirWatch Catalog or the Workspace ONE application.

Task 2: Managing Public Applications

1. Expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate **Apps & Books > Applications > Native > Public** tab.
3. View all the managed apps on the Applications page.



4. Scroll down and find the app you recommended. Note that personal feedback about the app is shown under the OG where the app is managed.
5. Under the Install Status column, click/hover verify whether your app is installed or not-installed. It should show assigned.

NOTE

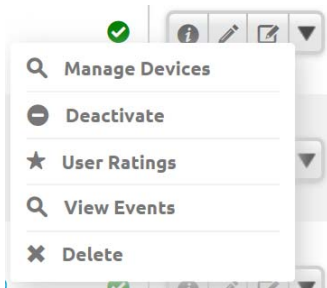
Clicking/Hovering over View link should show the number of devices app is assigned to, installed and not installed. If the app is not assigned to any device, then the link reads "Assign" and clicking on it opens up the update assignment dialog box.

NOTE

Applications may require a check-in (query) to show an updated status, if the application is installed on the device, but does not show an updated status dashboard.

6. Review the available options to the far right:

- **Query:** Get the latest app sample from the device to see the apps installed on it.
- **Send/Send to all:** Send a notification to the device as email or push notification, a supported SDK app should be installed on device to receive the push notification. Any VMware Workspace ONE apps will serve the purpose.
- **Install:** Send a command to install the app on the device
- **Remove/Remove from All:** Send a command to remove the app from the device
- **More:** Should allow for managing the Icon image, SDK settings and Terms of use for the app
- **More button** (on the right side of the screen): Should pop up a menu with following features
- **Deactivate:** This will push the app into a deactivated status and remove it from the devices however the app remains on the console maintaining its state for re-activation.
- **Send app configuration:** Add and send down the app configuration if applicable
- **User ratings:** View app ratings and user-provided feedback
- **Events:** Display events for apps and export activity as a .CSV.
- **Delete:** Remove the app from the admin console.



Managing Enterprise Applications

Task 3: Adding an Internal Application

1. Expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate **Apps & Books > Applications > Native > Internal** tab.
3. Select **Add Application**, select **Upload** and browse and select the **Android_MDM_Info.apk** from the Academic Success Kit.

NOTE

A similar flow could be done for other platforms if you have a signed application that has been internally developed by your organization, such as an .ipa for iOS. If you do not have an Android device enrolled, you will be able to load the app by completing this lab module, but it will not push down to your device since the app was built for Android platform.

4. Select **Continue** when upload is complete.

Add Application

Organization Group ID *


Application File *

5. From the **Details** tab, update the Name of the app to **MDM Info** and review the additional fields.

NOTE

Depending on the app developer this info could be coded into the app, so it automatically populates.

Internal | Managed By : World Wide Enterprises | Application ID : com.samsung.sidi.mdm



Details | Files | Images | Terms of Use | More ▾

Name * ⓘ

Managed By

Application ID *

Actual File Version

6. Select the **Files** tab and review the options. For other platforms, different options may be available.
7. Select the **Images** tab and review the options, such as loading application images to represent the apps in the AirWatch Catalog.
8. Select the **Terms of Use** tab to add an Application terms of use. If one has not been created, the Manage Terms option could be selected to create one.
9. Select the More tab to review **SDK** for either enable SDK capabilities with a define SDK profile.

NOTE

Developer files may be required. A SDK would be selected to turn on SDK functionality.

10. Select **Save & Assign**, and then select **Add Assignment**.
11. Select the **Smart Group** tab and choose the **All Devices @ Company** Smart Group you defined during the MDM lab exercise.
12. Change the **App Delivery method** to **Auto** and select **Add**.

Add Assignment

Select Assignment Groups ✕

✱ All Devices (World Wide Enterprises)

Start typing to add a group 🔍

Push Mode *

Auto

On Demand

i

Deployment Begins On *

11/29/2016

12:00 AM ▼

Your current time zone is: (GMT-05:00) Eastern Time (US & Canada)

13. Review the rest of the configuration settings
14. Click on **Add** button

NOTE

Note: The update Assignment page will come back up and notice that the smart group now shows up with the priority 0 and rest of the configured settings like the push mode Auto

15. Select **Save & Publish**.

16. Based on your defined Smart Group, your device will be shown. Select Publish to push the configuration to your device.
17. On your Android device, verify the application is installed. For most vendors this will happen silently with no prompt. If you provided an application file for another platform, the flow for installation may be different. For example, iOS it will prompt to install, but no Apple ID is required since it's not tied to the Apple Store.

NOTE

If the app was pushed in an **On Demand** capacity, the application would be installed either through the AirWatch Catalog or the Workspace ONE application.

Task 4: Managing Internal Applications

1. Expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate **Apps & Books > Applications > Native > Internal** tab.
3. View all the managed apps on the Applications page.
4. Under the Install Status column, verify if your app is installed or not-installed by clicking the **View** option. It should show assigned.

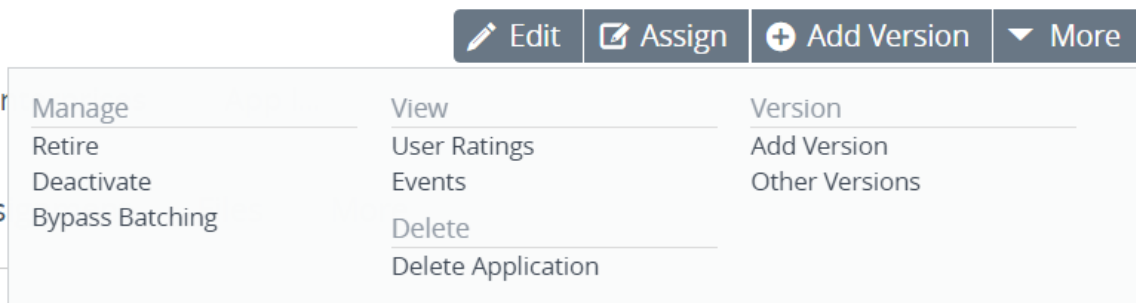
NOTE

Applications may require a check-in (query) in order to show an up-to-date status. This is necessary in the event that the application is installed on the device, but is not reflected as such on the status dashboard.

Icon	Name	Version	Platform / OS / Model	Renewal Date	Install Status	Status	Wrap Status
	MDM Info World Wide Enterprises ☆☆☆☆☆	1.0.0	Android / All / Android	Not Applicable	View		Not Applicable

5. Click on the app to see the further management options. It should pop up tabs like Summary, Details, Devices, Assignment and More.
6. Click on the name of the app, to see further management options and to review the following options
 - **Files Tab:** Shows the application file
 - **More Tab:** Review the images, Terms of Use, SDK and App Wrapping options Further options available on right hand side of the screen
 - **Edit**

- **Assign**
- **More Button:** Pops up a menu with following options
- **Add Version:** Update your internal application with a new version.
- **Retire:** Retire a version of the app and pushes an older app version out to the device and updates the AirWatch Catalog.
- **Deactivate:** Deactivates all versions of the app, removes the app from the device and AirWatch Catalog.
- **User Ratings:** View and delete user ratings and comments about applications.
- **Events:** Show device and console events for apps and export events as a .csv file.
- **Other Versions:** Show previous versions added to the admin console.



Task 5: Reviewing VPP and AirWatch SDK Settings

1. Expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate **Apps & Books > Applications > Native > Purchased** tab.

NOTE

Once integrated, this is where purchased applications are found.

3. From the Main Menu, navigate to **Devices and Users > Apple > VPP Managed Distribution**.
4. Review the setting to integrate directly with Apple by uploading an Apple VPP token to manage VPP licenses codes in bulk.

IMPORTANT

If you have an active VPP token for your company, **do not** upload it into the training environment.

5. From the Main Menu, navigate **Apps & Books > Applications Settings > Default Policy**. The **Security Policies** page appears.
6. Review the defined SDK settings for the OG.
7. Navigate to **Settings** and review additional SDK settings for the OG.
8. Navigate to **Profiles**, and review the options to create unique SDK profiles, which could be enabled for individual iOS and Android internal applications.

Building the AirWatch Catalog

Task 6: Configuring and Launching the AirWatch Catalog

1. Expand the OG hierarchy and select your **Company OG**.
2. From the Main Menu, navigate **Apps & Books > All Apps & books Settings > Workspace ONE > AirWatch Catalog**.
3. Review the **Authentication** options for AirWatch Catalog authentication, which are disabled by default.
4. Select the **Publishing** tab and define the following settings:
 - **Catalog Title:** World Wide Apps

- **Platforms:** Enable all and Full Screen mode for iOS

Apps > Catalog >

General ?

Authentication Publishing Customization

✓ Saved Successfully

Current Setting Inherit Override

Catalog Title *

Platforms

i Publish the Catalog to devices in this Organization Group as a webclip/shortcut profile

iOS	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled
Full Screen	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled
Android	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled
Windows Desktop	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled
macOS	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Disabled

NOTE

A default icon for the AirWatch Catalog is loaded in the database, but a custom one could be loaded.

5. Select **Save**.
6. Select the **Customization** tab and review the options, such as branding logo, default filter, sorting and pinned categories.
7. Verify the AirWatch Catalog is pushed to your device.

NOTE

If you have an Android device, there must be an open space on your device's home screen to accommodate the AirWatch Catalog. The AirWatch Catalog may also be opened from the

AirWatch Agent. There may also be the MDM Info app you deployed earlier, if it's supported for your device.



8. Browse the **AirWatch Catalog** on your device and perform the following:
9. Change filter options.
10. Select an application and view its description and provide an internal feedback.
11. Install or re-install any missing applications.

To view the internal feedback, go back to the AirWatch Admin Console, select the application and choose the option to view User Feedback.

NOTE

The Workspace ONE app combines all the apps that are integrated with the App Catalog. When Workspace ONE is fully integrated and deployed, you could disable the App Catalog and use

the Workspace ONE app as your Unified Catalog for all apps & services tied to AirWatch and the VMware Identity Management solution.

Enforcing Application Security

Task 7: Adding an Application Group

1. Expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate to **Groups & Settings > Groups > App Groups**.
3. Select **Add Group**.
4. Select **Blacklist** and choose the platform you have enrolled.

NOTE

An Application Group for white-listed and/or required apps may also be configured separately.

5. Select the type as **Blacklisted Apps**.
6. Select **Add Application** and search and select the following applications:
 - Pandora Radio
 - Facebook
 - Dropbox

Use the magnifying glass icon to search and select the application to blacklist.



List Assignment

Type* Blacklist Platform* Apple Name* Blacklisted Apps

Add Application

Application Name*	Application ID*
Pandora - Free Music	com.pandora
Facebook	com.facebook.Facebo
Dropbox	com.getdropbox.Drop

7. Select **Next** and Review the options, under the **Assignment** tab and select **Finish**.

The screenshot shows the 'Assignment' tab in the AirWatch Admin Console. At the top, there are two tabs: 'List' (with a '1' icon) and 'Assignment' (with a '2' icon and highlighted in blue). Below the tabs, there are several configuration fields:

- Description:** An empty text input field.
- Device Ownership:** A dropdown menu with 'Any' selected.
- Model:** A dropdown menu with 'Any' selected.
- Operating System:** A dropdown menu with 'Any' selected.
- Managed By*:** A text input field containing 'World Wide Enterprises'.
- Organization Group*:** A dropdown menu with 'World Wide Enterprises' selected and a blue 'x' icon to the right. Below the dropdown is a text input field with the placeholder 'Start typing to add a new group'.
- User Group:** A text input field with the placeholder 'Start typing to add a new group'.

At this point, you have identified **Pandora Radio**, **Facebook** and **Dropbox** as blacklisted apps. You have not yet defined what actions will be taken if a device reports that any of these applications are installed. If you do not pull Personal Application data, you will be unable to monitor which applications are installed onto devices within your deployment. Refer to Privacy settings in the AirWatch Admin Console to determine if Personal Application data is pulled based on device ownership.

8. Review the options to sort and search Apps Groups based on Platform or Type. You can also edit, delete or deactivate the App Group.



Task 8: Adding an Application Compliance Policy

1. Expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate to **Devices > Compliance Policies > List View > Add**.

3. Select the platform you have enrolled.
4. Change the **MDM Terms of Use Acceptance** rule to **Application List**.
5. Change **Contains** to **Contains Blacklisted Apps(s)**.

Match Of The Following Rules

<input type="text" value="Application List"/>	<input type="text" value="Contains Blacklisted App(s)"/>
---	--

[+ Add Rule](#)

6. Select **Next** to define the actions.
7. Change **Send Email to User** to **Send Push Notification to Device**.

Immediately perform the following actions Mark as Not Compliant

<input type="text" value="Notify"/>	<input type="text" value="Send Push Notification to Device"/>
-------------------------------------	---

[+ Add Escalation](#)

NOTE

Additional actions and escalation may be defined. An email is not being sent for this lab, since you changed your email address during the MEM lab.

8. Select **Next** to define the assignment.
9. For Assignment, define the following:
 - **Managed By:** Company OG

- **Assigned Groups:** All Devices @ (OG)

Managed By *

Assigned Groups

Exclusions

NOTE

Additional Smart Groups or Exclusions could be defined. Use View Device Assignment to view impacted devices to adjust assigned Smart Groups.

10. Select **Next** to review the summary.
11. Under General, change the **Name** and **Description** to match the scope for the compliance policy.

General

Name *

Description *

12. Refer to the **Device Summary** info to see how your device will be impacted by the compliance rule.
If your device is compliant, no actions will be triggered. If your device is noncompliant, the first compliance action would trigger within 5 minutes of detection.
13. Select **Finish and Activate**.

Task 9: Reviewing Platform-Specific Application Restrictions

1. Expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate to **Apps & Books > All Apps & Books Settings > Catalog > App Restrictions**.

3. Hover over the **i** button to review how the “Restricted Mode for Public iOS Applications” may be used. If deployed, the iOS App Store will be removed. The App Store can be triggered to open, however, when a public application listed within the AirWatch Catalog is selected for installation.
4. At the Company OG, navigate to **Devices > Profiles & Resources > Profiles > Add Profile**.
5. Select **Android**.
6. Define the following General properties:
 - **Name:** Blacklisted Applications
 - **Assigned Groups:** All Devices @ Company

General

Name *	<input type="text" value="Blacklisted Applications"/>
Version	<input type="text" value="1"/>
Description	<input type="text"/>
Profile Scope	<input type="text" value="Production"/>
Assignment Type	<input type="text" value="Auto"/>
Allow Removal	<input type="text" value="Always"/>
Managed By	<input type="text" value="World Wide Enterprises"/>
Assigned Groups	<input type="text" value="World Wide Enterprises (World Wide Enterprises)"/> <input type="button" value="✕"/>
	<input type="text" value="Start typing to add a group"/>
Exclusions	<input checked="" type="radio"/> No <input type="radio"/> Yes

7. From the left navigation, select the **Application Control** payload.
8. Select **Configure** and review the Prevent Installation of Blacklisted Apps option.

Only supported Android devices can disable or block the removal of applications you defined in the app group.

Application Control

Prevent Installation of Blacklisted Apps

SAFE v2

This will enforce the automatic removal and/or prevent the installation of the blacklisted apps defined in: [Application Groups](#)

9. Review the options for **Required** and **Whitelisted** apps.
10. Exit the profile configuration.

NOTE

Select platforms, such as variants of Android, Windows Phone 8.1/10, Windows Desktop (10), iOS 9.3+ with supervision, support similar application control for 8.3FP2/3+ by deploying Restrictions and the Application Control profile payloads. The “Carrot and Stick” method of setting up an application compliance rule may be used in conjunction with “Restricted Mode for Public iOS Applications” to enforce compliance for other devices and non-supervised iOS devices.

Task 10: Managing Applications

1. Expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate to **Devices > List View**.
3. Select the **Friendly Name** to view specific device details in the record.

Devices >

List View

Filters

- > Management
- ▼ Ownership
 - Corporate - Dedicated
 - Corporate - Shared
 - Employee Owned
 - Undefined

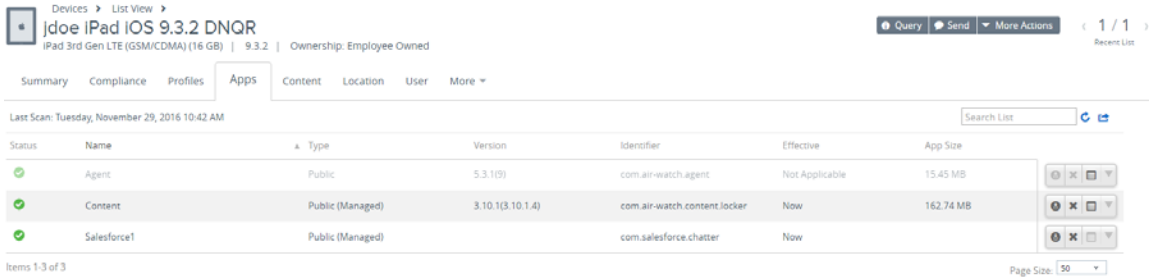
+ Add Device

Last Seen	General Info	Platform
5m	jdoe ipad iOS 10.0.2 FCM5 / North America / ITops MDM Corporate - Dedicated	Apple iOS iPad Mini with Retina (16 GB Space) 10.0.2

4. Select the **Apps** tab and view the application status for your device.
5. Review the options to remove or re-push “managed” applications.

NOTE

If personal applications are not shown, then Privacy settings are configured to suppress this information. The AirWatch Agent cannot be removed or re-pushed since it was installed prior to enrollment; this is an example of a behavior that can only be performed on “managed” applications.



Status	Name	Type	Version	Identifier	Effective	App Size
✓	Agent	Public	5.3.1(9)	com.air-watch.agent	Not Applicable	15.45 MB
✓	Content	Public (Managed)	3.10.1(3.10.1.4)	com.air-watch.content.locker	Now	162.74 MB
✓	Salesforce1	Public (Managed)		com.salesforce.chatter	Now	

Task 11: Unenrolling Your iOS Device

At this point, we are going to un-enroll your iOS device since you will start working on Active Directory integration where a user will be created and then used to enroll when VMware Identity Manager once its fully integrated with AirWatch.

NOTE

Other non-iOS device types can be left enrolled so they can be used for lab activities, which commence after the VMware Identity Manager/Workspace ONE labs are completed activities. If you did not bring an iOS device, all 1 VMware Identity Manager/Workspace ONE labs can be completed, but native SSO app integration will not work.

Your device should still be enrolled via the AirWatch Agent. This enrollment is based on the work previously accomplished during the “Mobile Device Management” lab activity.

1. Perform the following on your iOS device to unenroll from full device management:

For iOS:

- a. Navigate to Settings > General > Profiles.
- b. Select the Enrollment Profile.
- c. Select the Remove button.

For iOS 8.0+:

- d. Navigate to Settings > General.
- e. Select Device Management > MDM Profile > Remove Management.

f. Provide the device passcode if prompted to supply one.

NOTE

Leave the AirWatch Agent installed on the device for re-enrollment

Lab 7 Mobile Content Management

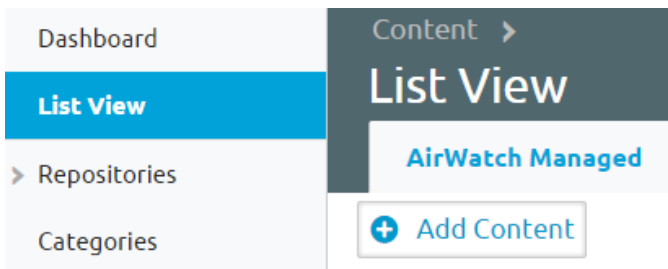
Requirements

The Mobile Content Management (MCM) lab requires the core configurations you performed during the completion of previous lab activities. Required configurations include a custom OG hierarchy with a defined Group ID, a test user and an enrolled device.

Deploying Content from Admin Console

Task 1: Adding Content Categories

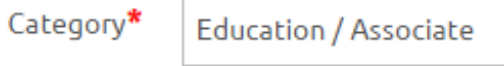
1. Expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate **Content > Content Locker > List View**.
3. Select **Add Content**.



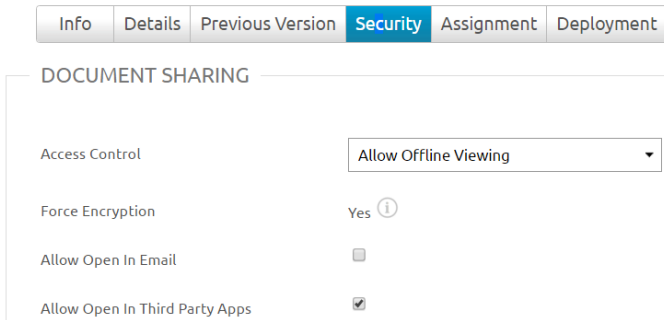
4. Browse the Academic Success Kit and select the `AirWatch_Enrollment.pptx`.

Files may also be dragged and dropped directly into List View dashboard without selecting **Add Content**.

5. Review the **Info** options and associate the content with the Education / Associate.



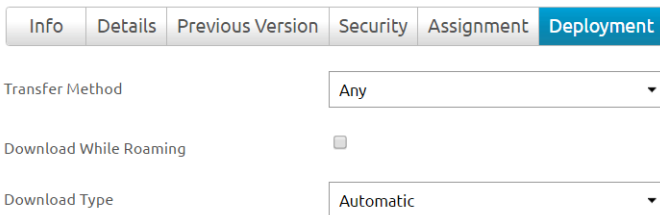
6. Select the **Details** tab, and review the Author, Notes, Subject, and Keyword fields.
7. Select the Security tab, select Allow Open in Third Party Apps.



8. Review the data loss prevention (DLP) settings.

Some DLP settings are dependent on the AirWatch SDK. Some examples of this are evident when using specific platforms. For example, AirPrint can only be managed for iOS devices, while Allow Editing can be managed for both Android and iOS devices.

9. Select the **Assignment** tab, and review the options, such as pushing content to specific device ownership, OGs, and User Groups.
10. Select the **Deployment** tab, and review the options.

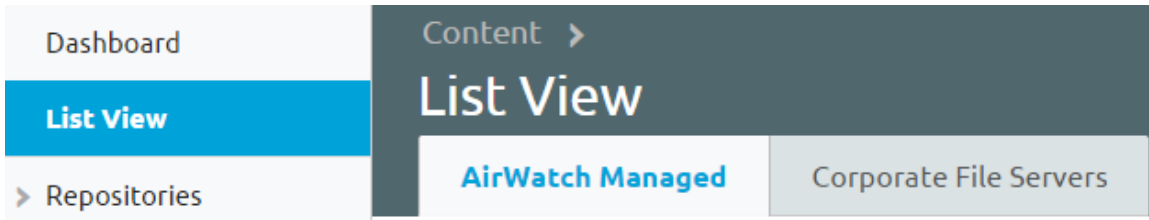


11. Change **Download Type** option from **On Demand** to **Automatic**, and then select **Save**.

Task 2: Managing Content

1. Expand the OG hierarchy and select your Company OG.

- From the Main Menu, navigate **Content > Content Locker > List View**.
- View all the managed content under the **AirWatch Managed** tab.



NOTE

Content tied to corporate file servers can be viewed by selecting the **Corporate File Servers** tab.

- Scroll down and find the content you uploaded.
Change the view by selecting the filter option in the top right corner, next to the house and star icons.
- Review each column, including the version, expiration and installation/assignment status.
- Select the install/assignment status hyperlink, to review options to install or delete the content from VMware Content Locker.

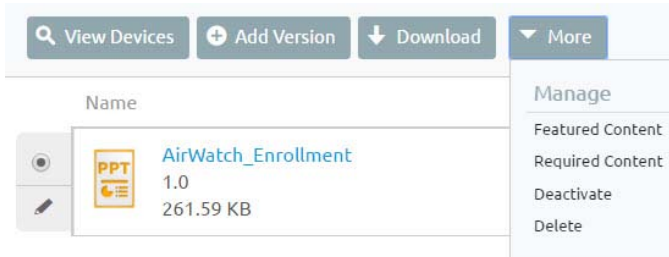
NOTE

Like other settings, content that you have uploaded to the console includes a hyperlink to ease access for management. Role-based access may prevent you from seeing this link for content which you did not upload. As with applications, newly-updated content may have been downloaded to a device and will not show an update on the dashboard until the device has checked in with the console.

Name	C/E/S	Managed By	Effective Date	Download Type	Modified By	Installed Status	Status
 AirWatch_Enrollment 1.0 261.59 KB	N/A	Company	3/29/2016	Automatic	Administrator	<input checked="" type="radio"/> 0 <input type="radio"/> 1	<input checked="" type="radio"/>

- Select the radio button next to the piece of content and review the following options:
 - View Devices:** View which devices are associated with the content.
 - Add Version:** Update your uploaded content with a new version.
 - Download:** Download content to your computer for auditing purposes.
 - Featured Content:** Add content to Feature Content section in VMware Content Locker.

- **Required Content:** Mark as required content which has to be viewed.
- **Deactivate:** Remove from devices but not removed from Console so it can be reactivated.
- **Delete:** Delete content from AirWatch Admin Console and device via VMware Content Locker.



Selecting the pencil icon or the name of the document allows you to change settings.

Task 3: Reviewing Onboarding (Required Content) and File Types Settings

1. Expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate **Content > Settings > Advanced > File Types**.
3. Review the options to Whitelist and Blacklist content file types for corporate and personal content.

Content / Advanced / File Types

Current Setting Inherit Override

Allowed File Types * ⓘ

Whitelist doc, docx, key, numbers, pages, pdf, ppt, html, png, jpg, jpeg, ePub, mov, mp4, mcsv, ibooks, dwg, zip, wav, wave, rar

Apply Restrictions to Personal Content

4. Expand the OG hierarchy and select your Company OG.

- From the Main Menu, navigate to **Content > Settings > Advanced > Onboarding**.

Content / Advanced / Onboarding

Current Setting Inherit Override

Onboarding	<input checked="" type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="i"/>
Administrative Unlock Code*	<input type="text" value="1234"/>
Entrance Message	<input type="button" value="Enable"/> <input checked="" type="button" value="Disable"/> <input type="button" value="i"/>
Exit Message	<input type="button" value="Enable"/> <input checked="" type="button" value="Disable"/> <input type="button" value="i"/>

- Hover over the **i** button to review the option to lock a supervised iOS device into only showing required content for onboarding purposes.
- Select **Enable** and review additional configuration options.
- Do not save the configuration.

Integrating with Content Repositories

Task 4: Configuring and Managing a Content Repository

To configure the following content repository, a Google Drive or OneDrive account is required. If you do not have an account, a free account can be created through Google or Microsoft.

- Expand the OG hierarchy and select your Company OG.
- From the Main Menu, navigate **Content > Content Locker > Repositories > Admin Repositories**.

List View	Admin Repositories		
▼ Repositories	<input type="button" value="+ Add"/>		
Admin Repositories	<table><thead><tr><th>Type</th><th>Name</th></tr></thead></table>	Type	Name
Type	Name		

- Select **Add**.

4. Review the different repository types, and then define the following settings:

- **Name:** Google Drive or OneDrive
- **Type:** Google Drive or OneDrive
- **OG:** Company OG
- **Allow Inheritance:** Enabled
- **Allow Write:** Disabled

Name*	Google Drive
Type	Google Drive
Organization Group*	World Wide Enterprises
Allow Inheritance	<input checked="" type="checkbox"/>
Allow Write	<input type="checkbox"/>

5. Select **Continue**.

6. Accept the default options for **Security** and **Assignment** tabs.

All configuration tabs provide the same options for uploading content.

7. For the Deployment tab, verify **Download Type** is set to **On Demand**.

Transfer Method	Any
Download While Roaming	<input type="checkbox"/>
Download Type	On Demand

It is not recommended to set a content repository to automatically download all content, since there could be a considerable amount of content loaded.

8. Select **Save**.
9. View the content repository in the Admin Repositories dashboard.
10. On the right side, review the options to edit or delete the content repository.

Type	Name	Link	Organization Group	Authentication Type	Access via MAG/Content Gateway	Allow Children	Enable Sync
	Google Drive	https://www.googl...	Company	None	No	Yes	Yes

The content in the repository may be viewed by the AirWatch Administrator in **Content > List View > Corporate File Server** tab so long as authentication credentials were defined during the initial association with the content repository.

Accessing Content from Devices

Task 5: Using VMware Content Locker

1. Open the **Content** app.

NOTE

If VMware Content Locker requires installation, open the **World Wide Apps** shortcut in the AirWatch Catalog. Select the option to install the VMware Content Locker. A prompt to install the application will appear, either in the middle of the screen or in the notification bar. For iOS, select **Install** and, if prompted, enter your Apple ID credentials. For Android, the prompt will take you into the AirWatch Agent. Once in the AirWatch Agent, select the VMware Content Locker. This will take you to the Google Play store for installation.

Single sign-on access has been enabled to leverage the AirWatch Software Development Kit (SDK), which has functionality coded directly into the application. As a result, the credentials are not required since the AirWatch Agent is used to authenticate the session.

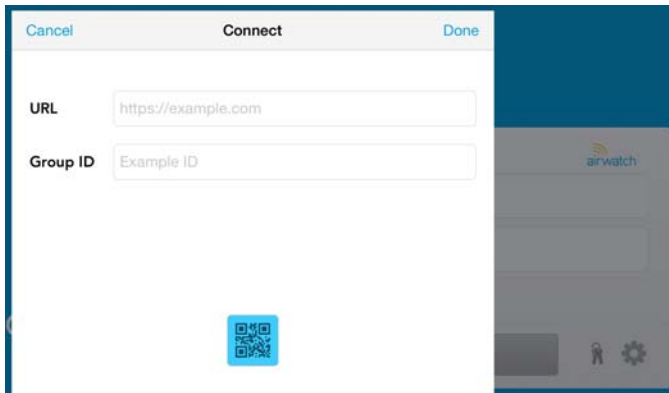
If a URL is presented upon login, verify the following details and select okay:

- **URL:** <Same URL as AirWatch Admin Console, such as `mdm.server.com`>
- **Group ID:** <Group ID you defined for enrollment during MDM lab>

If prompted for credentials, enter the following:

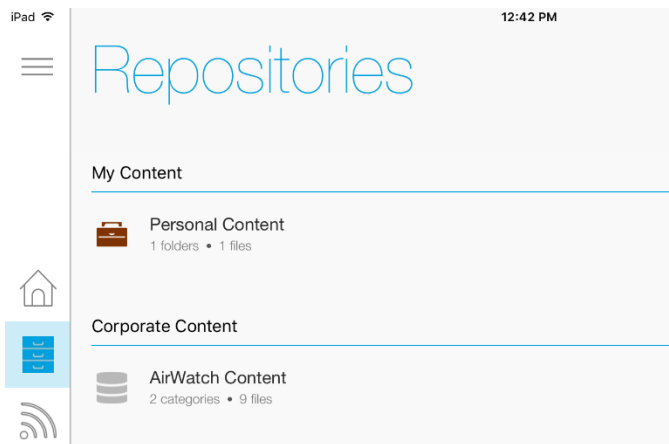
- **User:** <username you defined during MDM lab>

- **Password:** <password you defined during MDM lab>



If you forgot the Group ID, username or password, you can refer to these settings within the AirWatch Admin Console. If required, refer to the MDM lab exercise to locate and changes these settings.

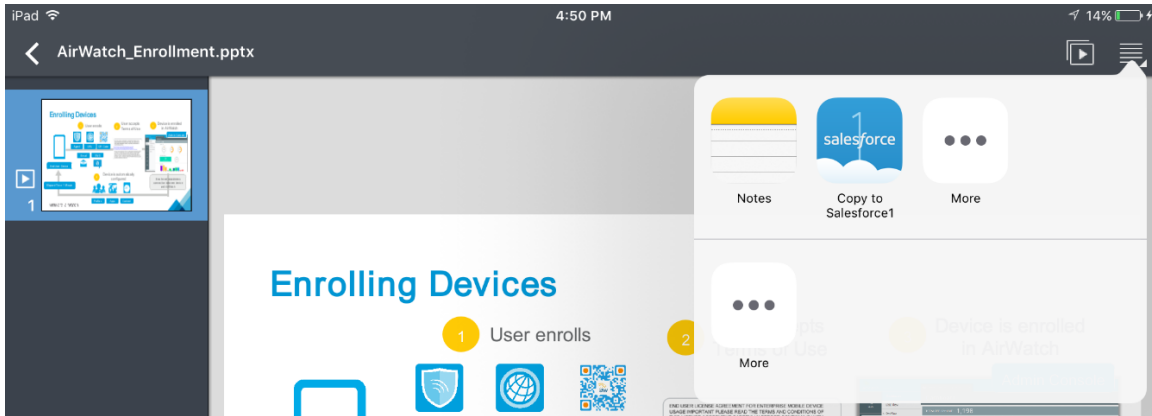
2. Accept any pop-up notifications and swipe through the tutorial screens and select **Got it, Thanks.** to view the **Repositories** page.



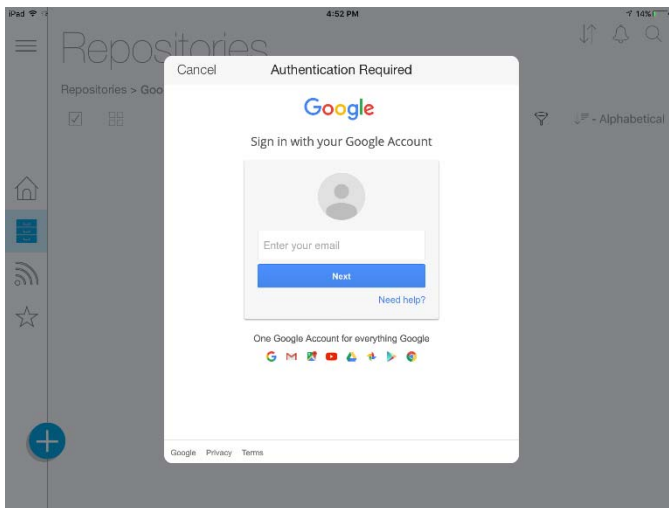
3. Select **AirWatch Content**, navigate to the appropriate category to select a document to download and then **tap** to view

The AirWatch Admin can determine what content is pushed for automatic download or in an on-demand capacity. Additional settings, such as enabling downloads only when devices are connected to Wi-Fi or configuring an expiration date for content availability, can additionally be defined.

4. Select **AirWatch Content** and navigate to **Education > Associate**.
5. Open the AirWatch_Enrollment document and select the **Open Into** button from the top right of the navigation panel. If you have an application which supports the Open Into option for this file type, an application will be prompted.

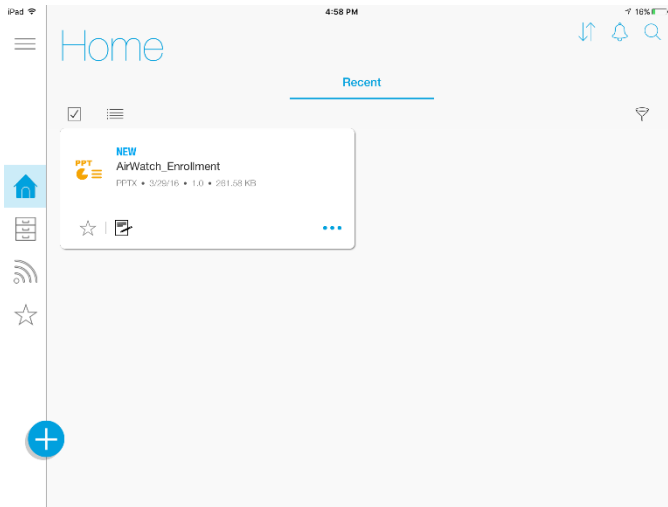


6. Navigate back to **Repositories**, and select the **Google Drive** or **OneDrive** repository.



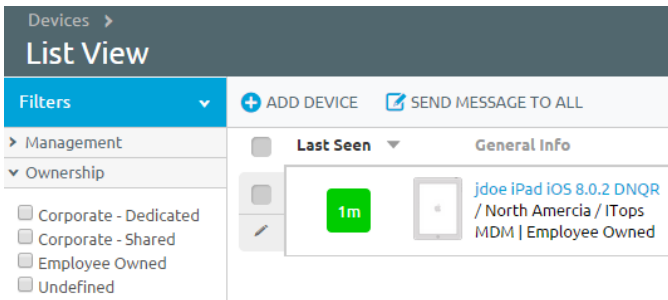
7. When prompted, enter your credentials, select **Allow** for Content Locker to connect to your account and view your cloud content.
8. Navigate back to **Repositories**, and note the Download transfer status. Alerts and search are available from the home screen.

9. Select the **Menu** icon to view storage and other settings, such as Home, Feed and Favorites. The gear icon provides access to Account, Preferences, About, and Help details.



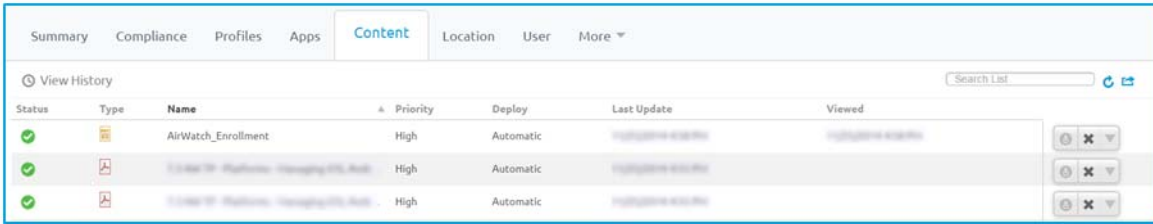
Task 6: Managing Content

1. Expand the OG hierarchy and select your Company OG.
2. From the Main Menu, navigate to **Devices > List View**.
3. Select the Friendly Name to view specific device details in the record.



4. Select the **Content** tab and view the content status for your device.

5. Review the options to remove or re-push the content.



The screenshot shows the 'Content' tab in the AirWatch Admin Console. It displays a 'View History' table with the following columns: Status, Type, Name, Priority, Deploy, Last Update, and Viewed. There are three rows of content items, all with a status of 'Success' (green checkmark) and a priority of 'High'. The first row is 'AirWatch_Enrollment'. The second and third rows are 'iCloud W/ Platform: Managing iOS App'. Each row has a 'Viewed' column with a date and time, and a 'More' dropdown menu with options for 'Refresh', 'Remove', and 'Push'.

Status	Type	Name	Priority	Deploy	Last Update	Viewed
Success	Profile	AirWatch_Enrollment	High	Automatic	11/11/2016 10:10:10 AM	11/11/2016 10:10:10 AM
Success	App	iCloud W/ Platform: Managing iOS App	High	Automatic	11/11/2016 10:10:10 AM	11/11/2016 10:10:10 AM
Success	App	iCloud W/ Platform: Managing iOS App	High	Automatic	11/11/2016 10:10:10 AM	11/11/2016 10:10:10 AM

The date the content was viewed is available once the device syncs with the AirWatch Admin Console. Additional content details may be viewed via the Content dashboard.

End

