Table of Contents

Lab Overview - HOL-1857-01-UEM - Workspace ONE UEM - Getting Started

Lab Guidance

NOTE - It will take more than 90 minutes to complete this lab. You should expect to only finish 2-3 of the modules during your time. The modules are independent of each other so you can start at the beginning of any module and proceed from there. You can use the Table of Contents to access any module of your choosing.

The Table of Contents can be accessed in the upper right-hand corner of the Lab Manual.

The introduction to AirWatch lab is designed to introduce you to many of the features of AirWatch Enterprise Mobility Management and Administration. Each Module can be taken independently or you can start at the beginning and work your way through each module in sequence. In most cases, a unique "sandbox" instance of AirWatch will be created just for you when you begin a Module. When the Module has ended, this sandbox will be deleted and the device that you are enrolling in the lab will be returned to the state that it was in prior to the lab. The approximate time it will take to go through all the modules is around 2.5 hours.

Lab Module List:

- **Module 1 - Introduction to Workspace ONE UEM** (30 minutes) (Basic) Introduction to AirWatch Admin Console and how to enroll a device to AirWatch EMM.
- **Module 2 - Basic Apple macOS Management** (45 minutes) (Basic) Familiarize yourself with basic features of Apple macOS with AirWatch EMM.
- **Module 3 - Basic Windows 10 Management** (30 minutes) (Basic) Enroll and explore EMM functionality with Windows 10 devices.
- **Module 4 - Workspace ONE UEM Console Roles** (30 minutes) (Basic) Customize permissions of your AirWatch console admin and enrollment user and validate those changes in the access level.
- **Module 5 - Branding the Workspace ONE UEM Console, SSP and SCL** (30 minutes) (Basic) Customize the look and feel of different AirWatch components to match organization's branding guidelines.

- **Lab Captains - All modules: Roger Deane, Shardul Navare, Justin Sheets.**

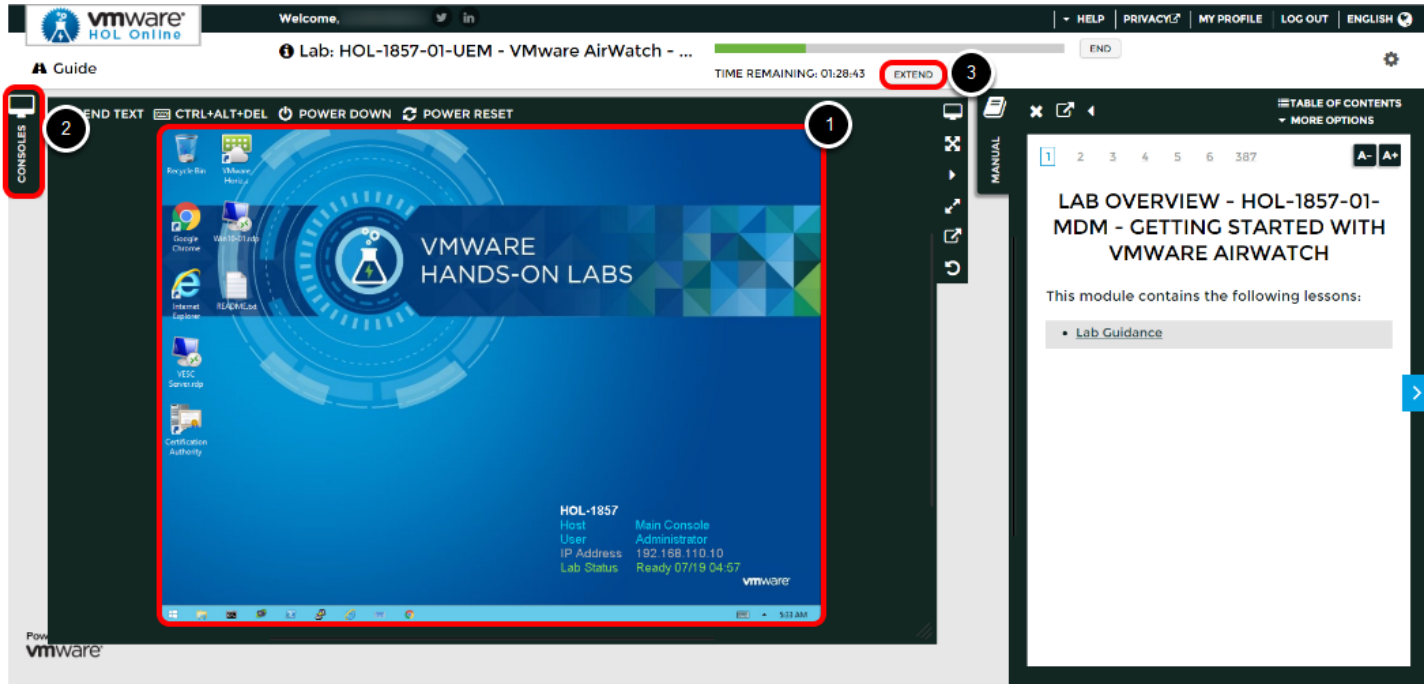
This lab manual can be downloaded from the Hands-on Labs Document site found here:

http://docs.hol.vmware.com

This lab may be available in other languages. To set your language preference and have a localized manual deployed with your lab, you may utilize this document to help guide you through the process:

http://docs.hol.vmware.com/announcements/nee-default-language.pdf

Location of the Main Console



1. The area in the RED box contains the Main Console. The Lab Manual is on the tab to the Right of the Main Console.
2. A particular lab may have additional consoles found on separate tabs in the upper left. You will be directed to open another specific console if needed.
3. Your lab starts with 90 minutes on the timer. The lab can not be saved. All your work must be done during the lab session. But you can click the **EXTEND** to increase your time. If you are at a VMware event, you can extend your lab time twice, for up to 30 minutes. Each click gives you an additional 15 minutes. Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.

Alternate Methods of Keyboard Data Entry

During this module, you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.

Click and Drag Lab Manual Content Into Console Active Window

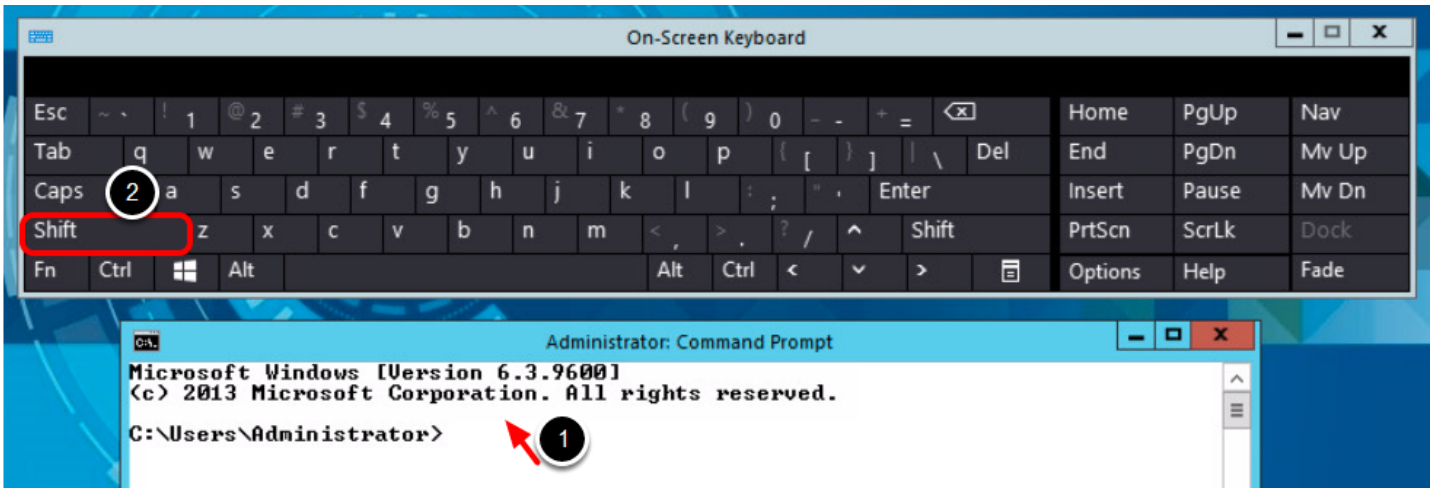
You can also click and drag text and Command Line Interface (CLI) commands directly from the Lab Manual into the active window in the Main Console.

Accessing the Online International Keyboard

You can also use the Online International Keyboard found in the Main Console.

1. Click on the Keyboard Icon found on the Windows Quick Launch Task Bar.

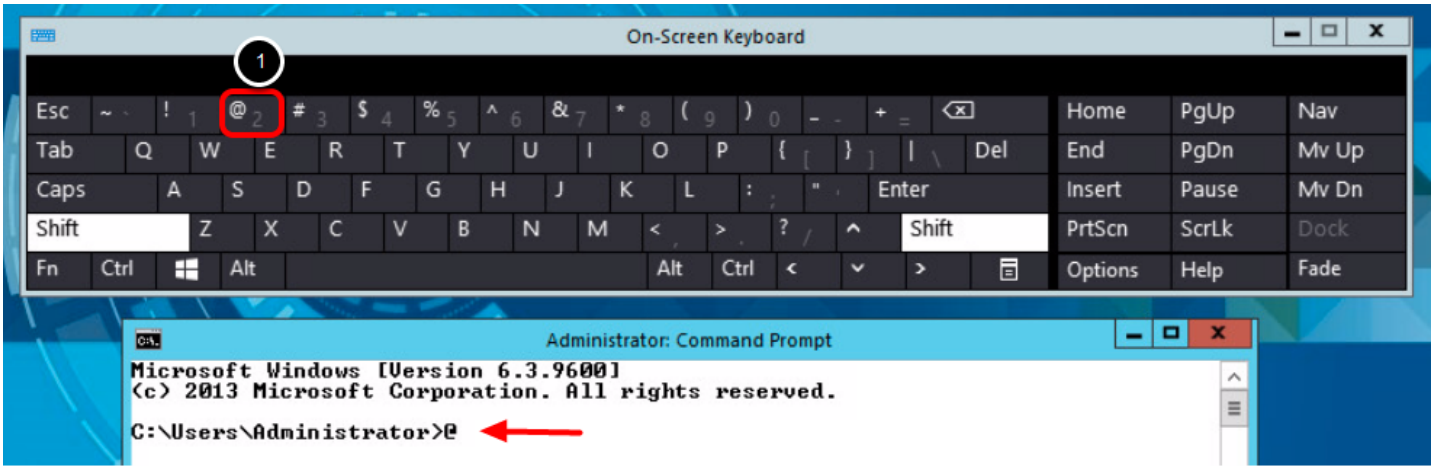
Click once in active console window



In this example, you will use the Online Keyboard to enter the "@" sign used in email addresses. The "@" sign is Shift-2 on US keyboard layouts.

1. Click once in the active console window.
2. Click on the **Shift** key.

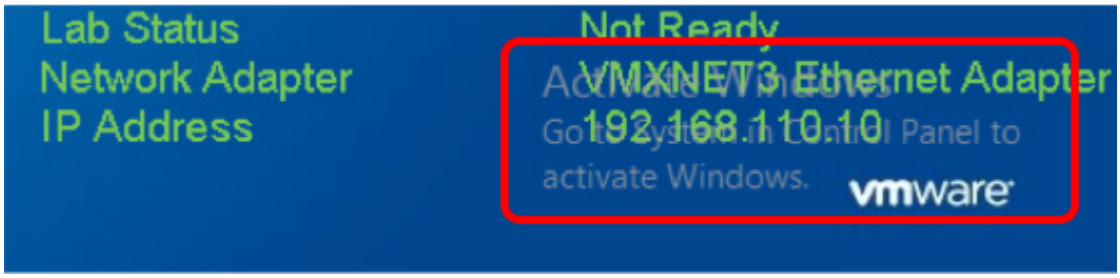
Click on the @ key



1. Click on the "@" **key**.

Notice the @ sign entered in the active console window.

Activation Prompt or Watermark



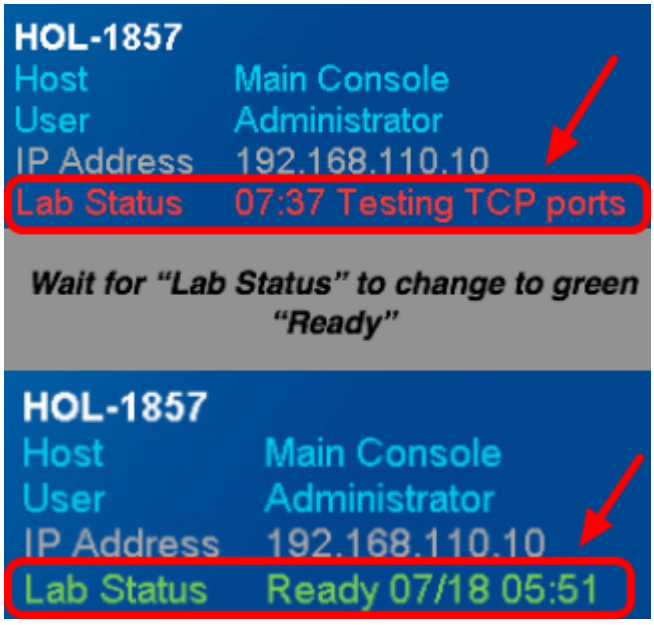
When you first start your lab, you may notice a watermark on the desktop indicating that Windows is not activated.

One of the major benefits of virtualization is that virtual machines can be moved and run on any platform. The Hands-on Labs utilizes this benefit and we are able to run the labs out of multiple datacenters. However, these datacenters may not have identical processors, which triggers a Microsoft activation check through the Internet.

Rest assured, VMware and the Hands-on Labs are in full compliance with Microsoft licensing requirements. The lab that you are using is a self-contained pod and does not have full access to the Internet, which is required for Windows to verify the activation. Without full access to the Internet, this automated process fails and you see this watermark.

This cosmetic issue has no effect on your lab.

Look at the lower right portion of the screen



Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes you lab has not changed to "Ready", please ask for assistance.

Module 1 - Introduction to Workspace ONE UEM (30 min)

Introduction

This lab module will focus on introducing the concepts of Enterprise Mobility Management (EMM) with AirWatch, using the AirWatch Console, and how to enroll an iOS device into AirWatch. By the end of this lab, you should have a better understanding of why Enterprise Mobility Management (EMM) is important and how AirWatch can manage your devices.

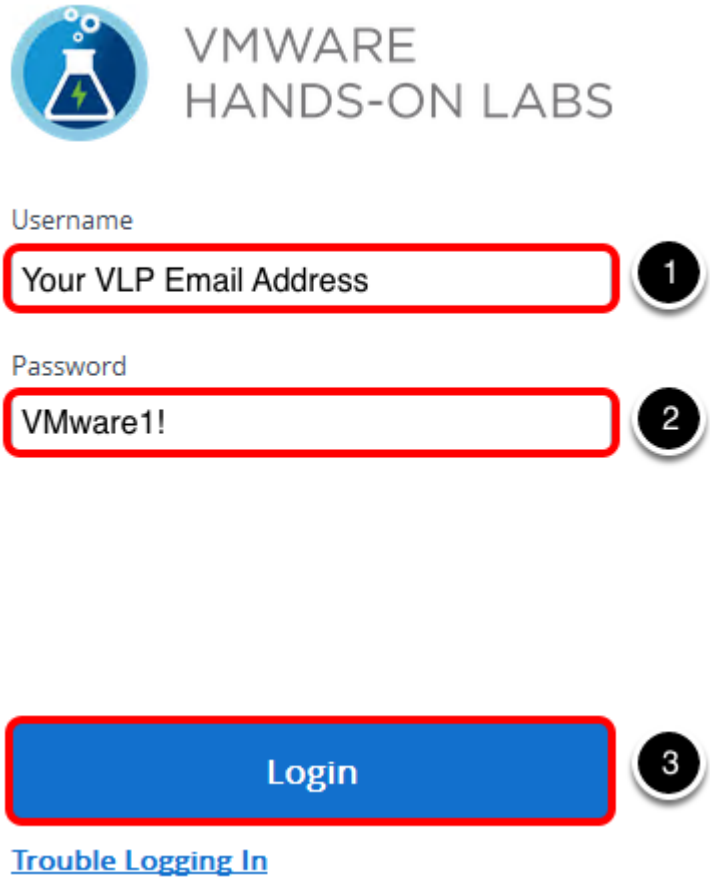
Login to the AirWatch Console

To perform most of the lab you will need to login to the AirWatch Management Console.

Launch Chrome Browser

Double-click the **Chrome** Browser on the lab desktop.

Authenticate to the AirWatch Administration Console



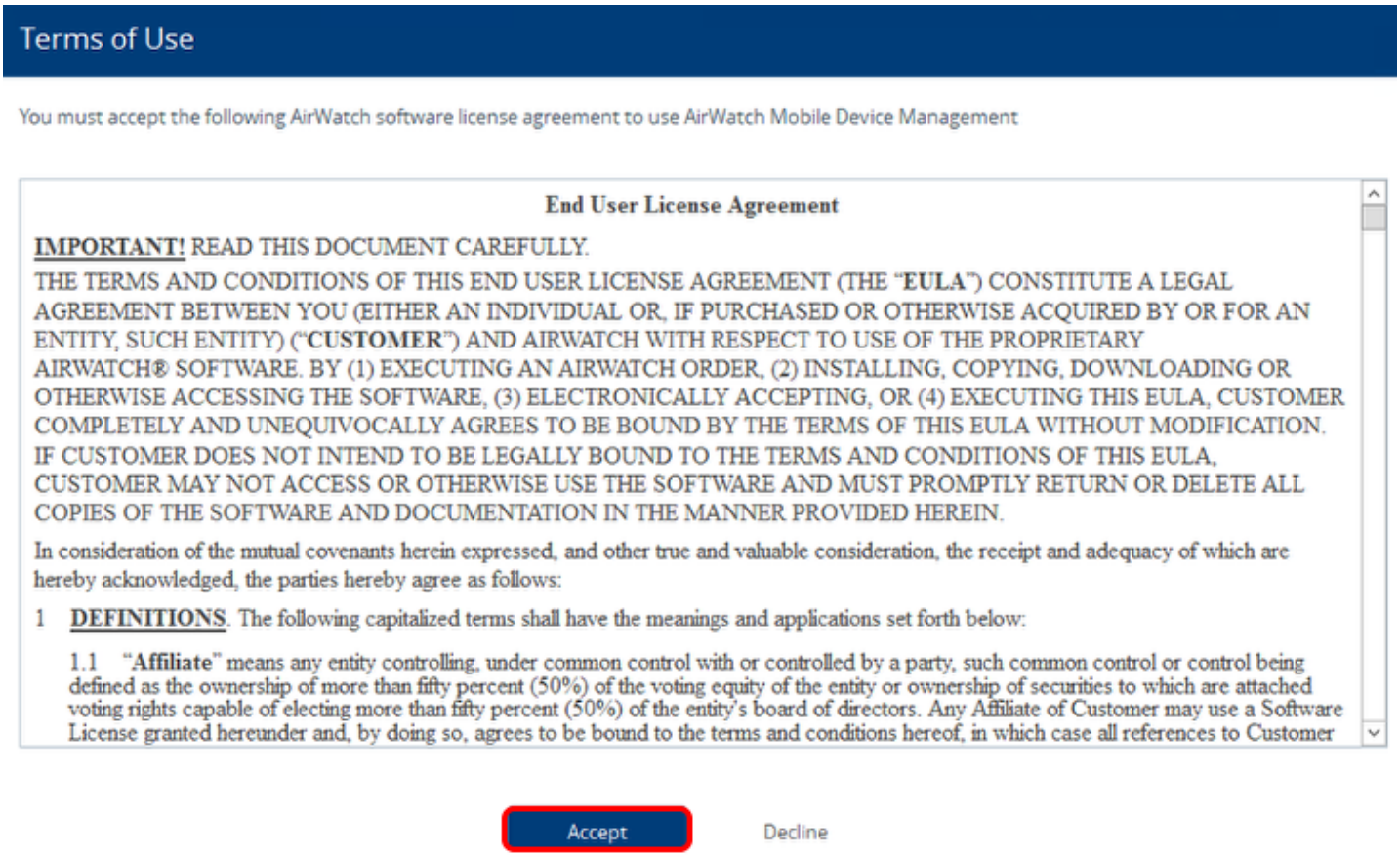
The default home page for the browser is **https://hol.awmdm.com**. Enter your AirWatch Admin Account information and click the **Login** button.

NOTE - If you see a Captcha, please be aware that it is case sensitive!

1. Enter your **Username**. This is you **email address** that you have associated with your **VMware Learning Platform (VLP) account**.
2. Enter **"VMware1!"** for the **Password** field.
3. Click the **Login** button.

NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the AirWatch Hands On Labs server.

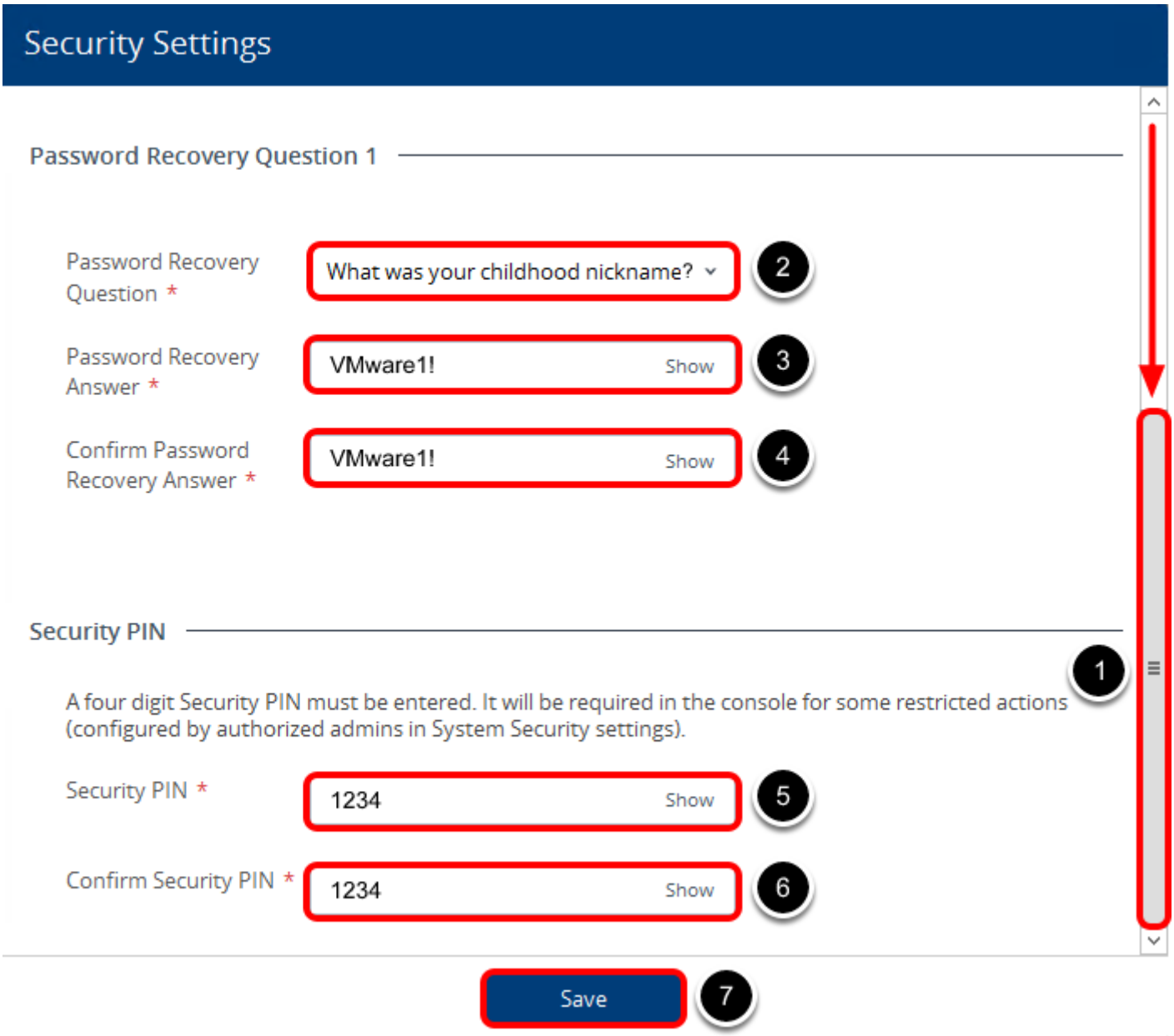
Accept the End User License Agreement



NOTE - The following steps of logging into the Administration Console will only need to be done during the initial login to the console.

You will be presented with the AirWatch Terms of Use. Click the **Accept** button.

Address the Initial Security Settings

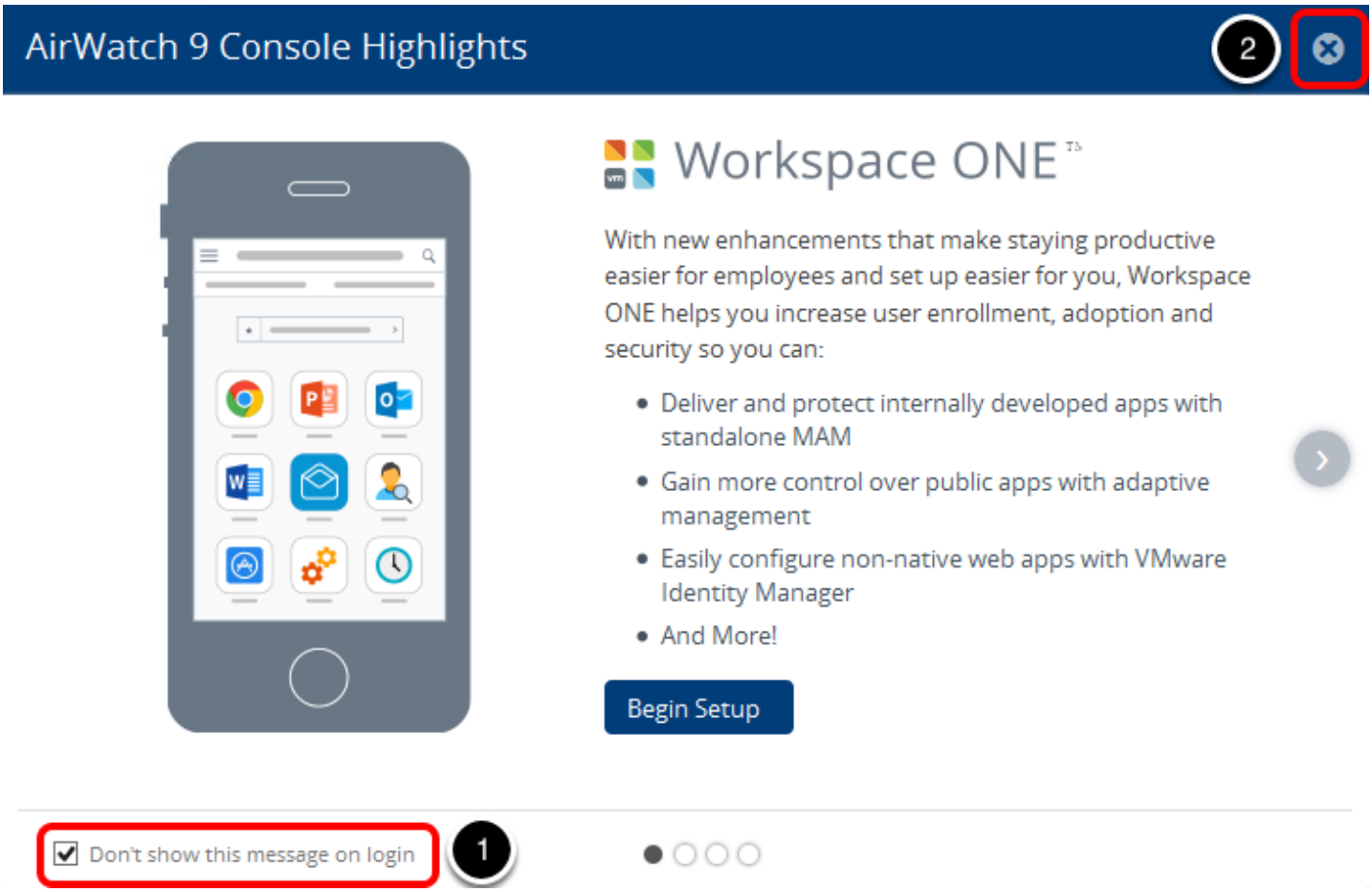


After accepting the Terms of Use, you will be presented with a **Security Settings** pop-up. The **Password Recovery Question** is in case you forget your admin password and the **Security PIN** is to protect certain administrative functionality in the console.

1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a **question** from the **Password Recovery Question** drop-down (default selected question is ok here).
3. Enter **"VMware1!"** in the **Password Recovery Answer** field.
4. Enter **"VMware1!"** in the **Confirm Password Recovery Answer** field.
5. Enter **"1234"** in the **Security PIN** field.
6. Enter **"1234"** in the **Confirm Security PIN** field.

7. Click the **Save** button when finished.

Close the Welcome Message



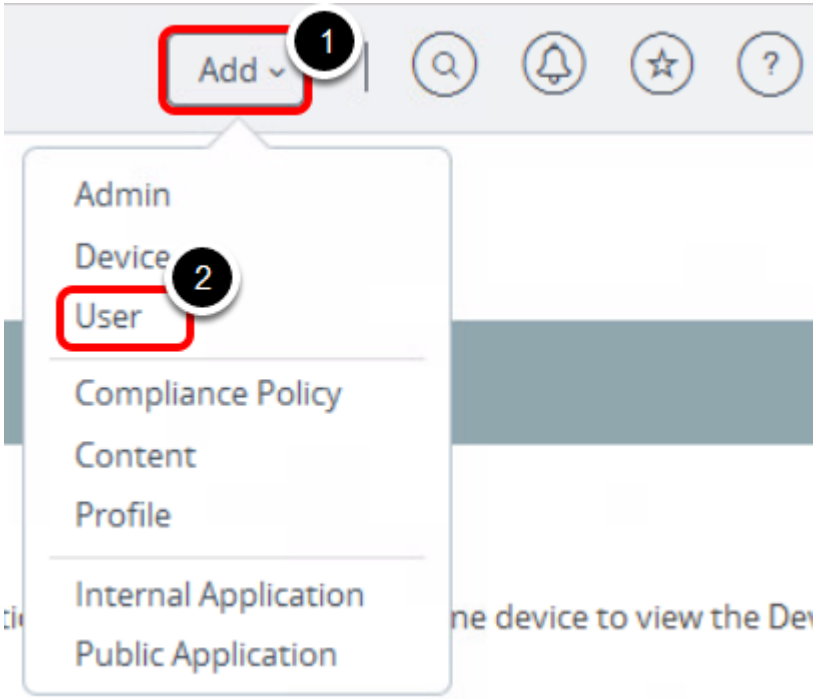
After completing the Security Settings, you will be presented with the AirWatch Console Welcome pop-up.

1. Click on the **Don't show this message again** check box.
2. Close the pop-up by clicking on the **X** in the upper-right corner.

Add A Basic User Account

Basic accounts are the accounts which are created locally in the AirWatch admin console, as opposed to the accounts which are imported from an active directory. In this section, we will create a Basic User account which we will use for enrollment in the following section.

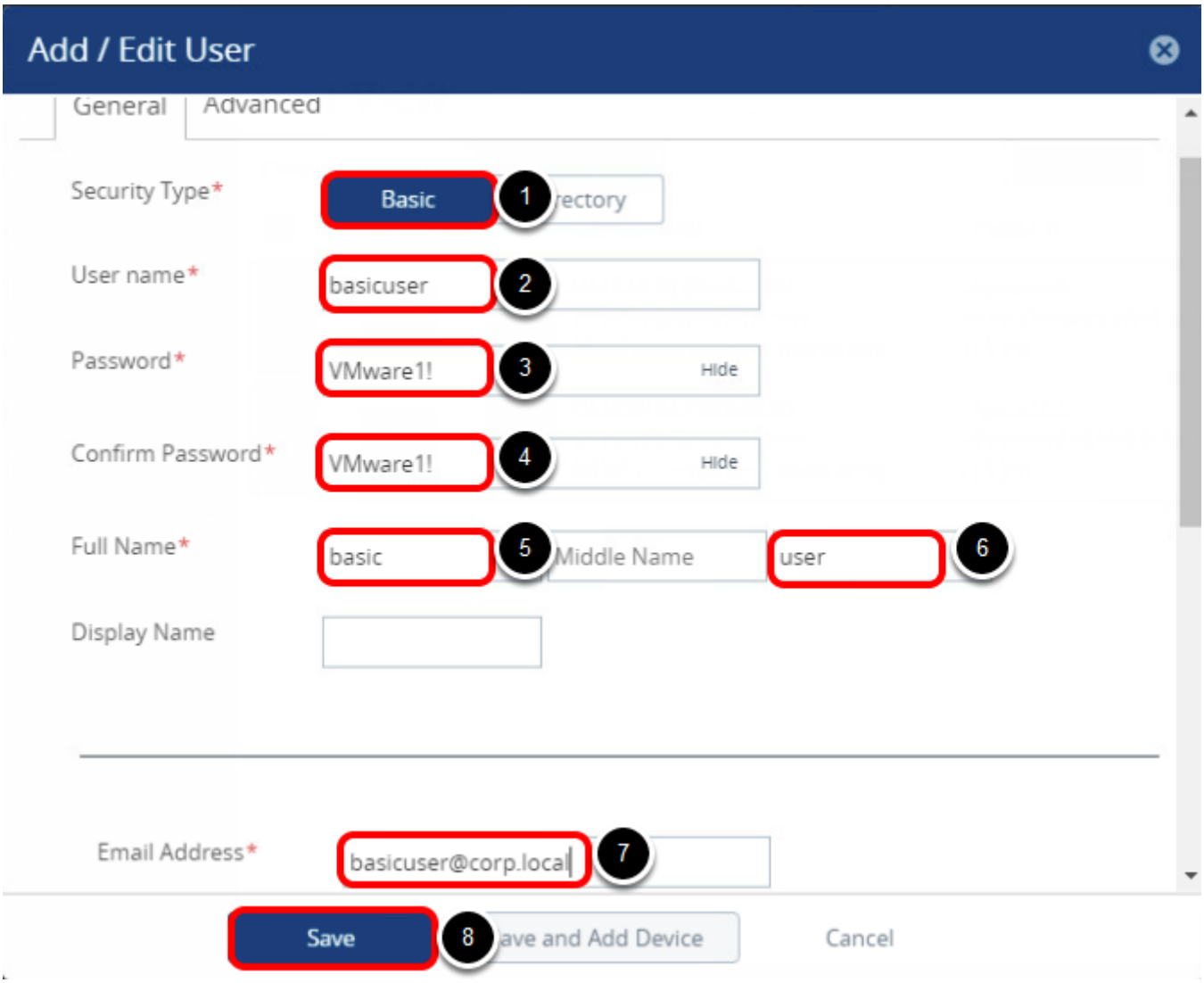
Click on Add / User



In the top right corner of the AirWatch console,

1. Click **Add**.
2. Click **User**.

Add User information



In the pop-up window,

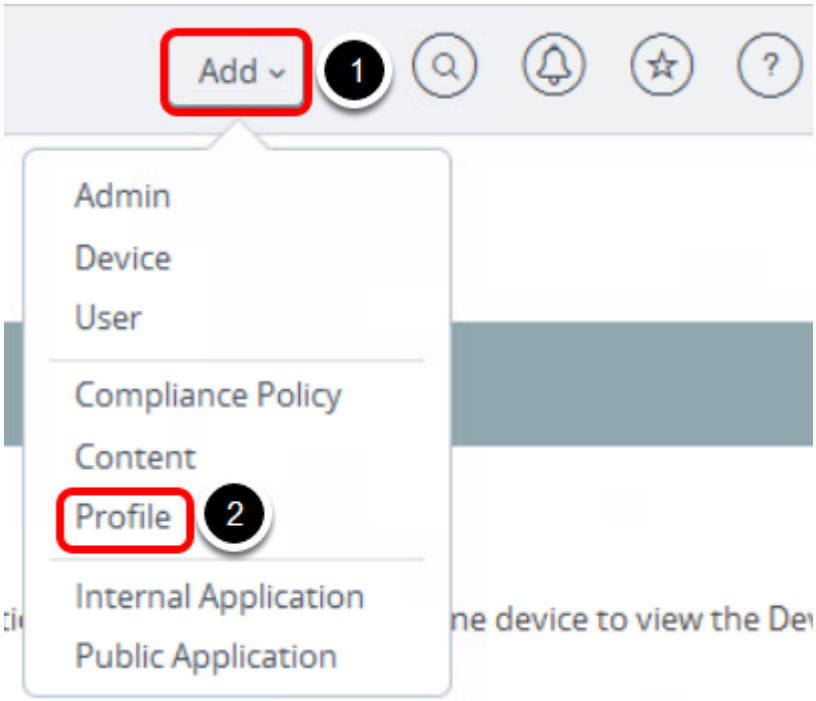
1. Ensure that security type is **Basic**
2. Enter the username as "**basicuser**"
3. Enter the password as "**VMware1!**"
4. Confirm the password as "**VMware1!**"
5. Enter the first name as **"basic**"
6. Enter the last name as **"user"**
7. Enter the e-mail address as "**basicuser@corp.local**"
   NOTE - Use the scroll bar if you don't see the option to enter email address
8. Click on **Save**

You should see a confirmation that user is created successfully. If the user is already created with the same username then you can use the existing user in the following section.

Create a Device Restriction Profile

In this section, we will create a restriction profile that will disable the camera on the device. We will set the profile for auto-deployment, so that the profile to disable the camera will install automatically when the device is enrolled.

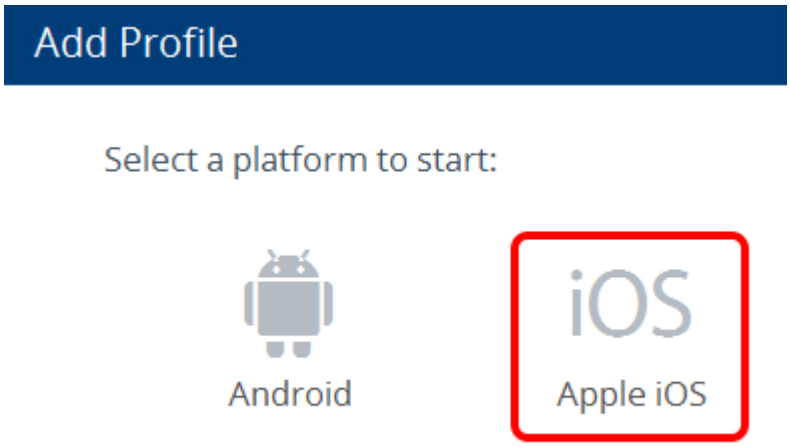
Add A Profile



In the top right corner of the AirWatch console,

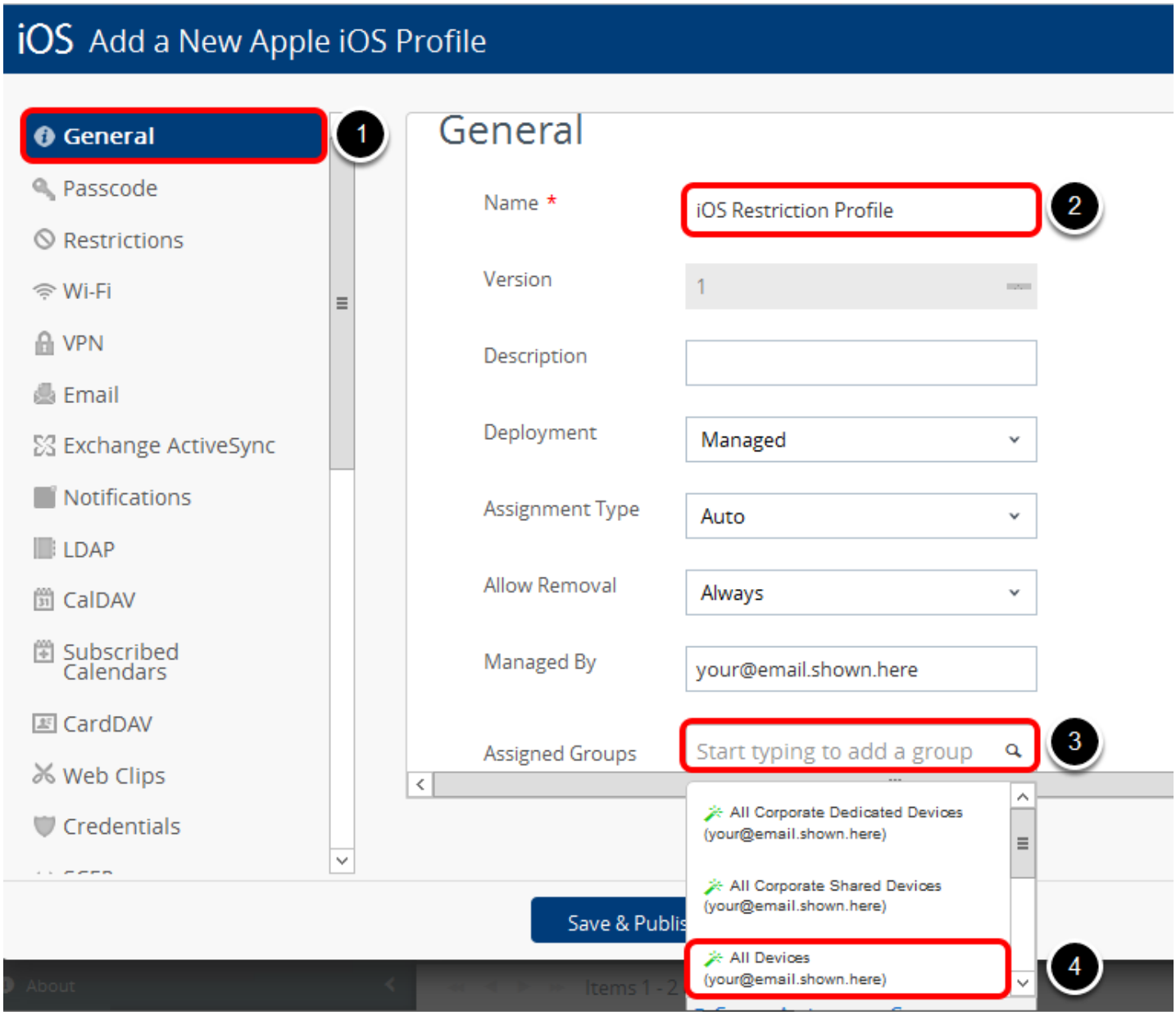
1. Click **Add**.
2. Click **Profile**.

Select Platform as Apple iOS



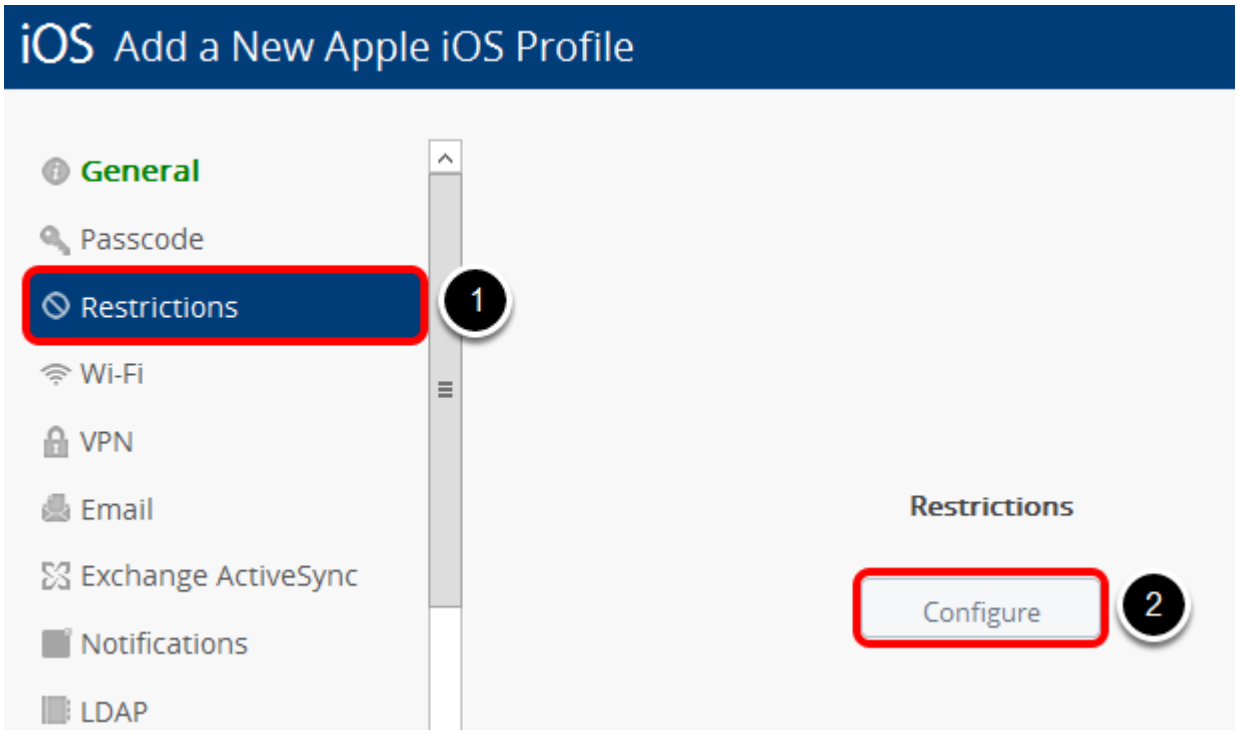
Click **Apple iOS**.

Configure General Payload



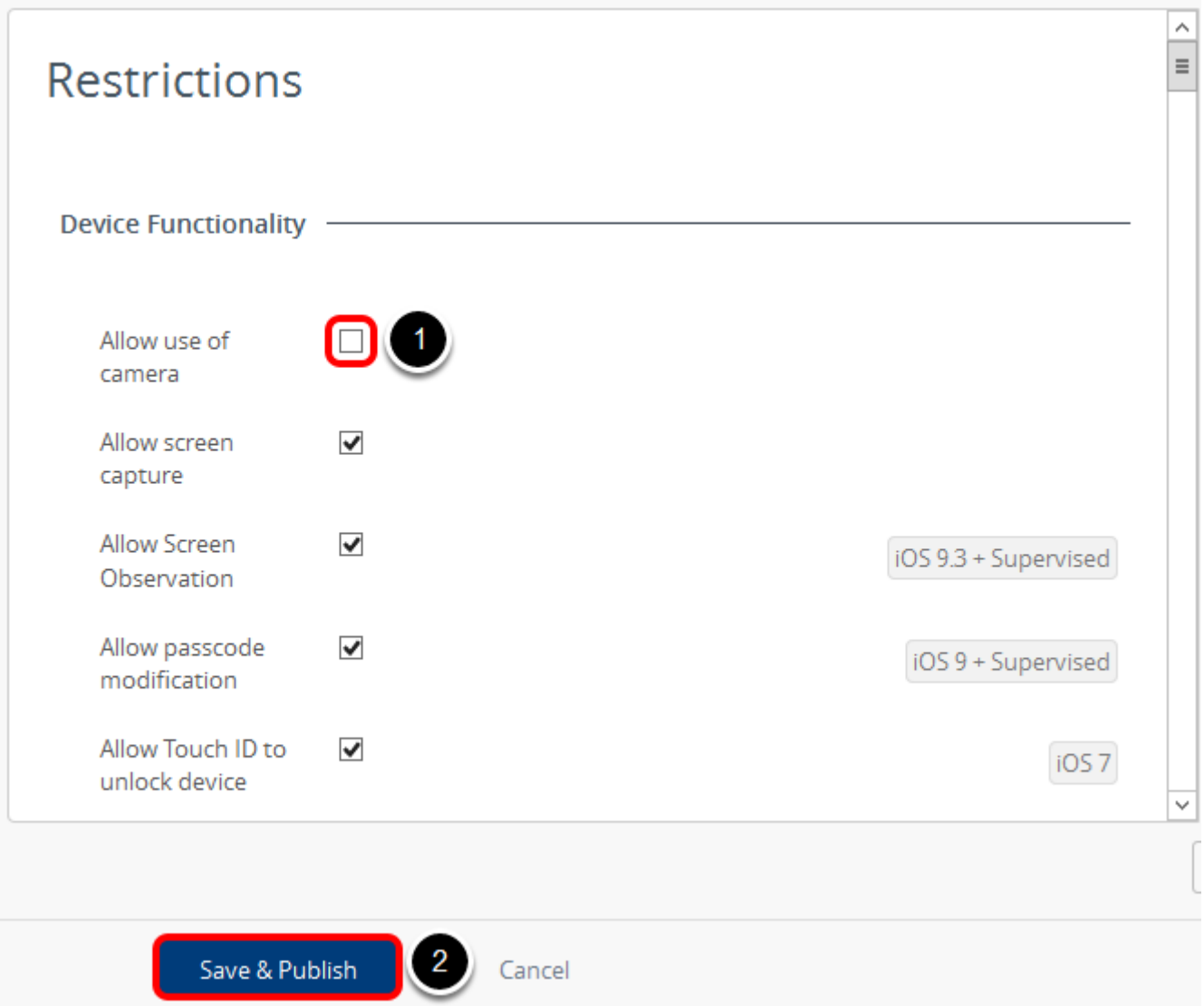
1. Select **General** if not selected already.
2. Enter "**iOS Restriction Profile**" for the **Name** field.
3. Click the **Assigned Groups** dropdown field to view all available assignment groups.
   NOTE - You may need to scroll down to find the Assigned Groups dropdown.
4. Select **"All Devices (your@email.shown.here)"** from the list.

Configure Restriction Payload



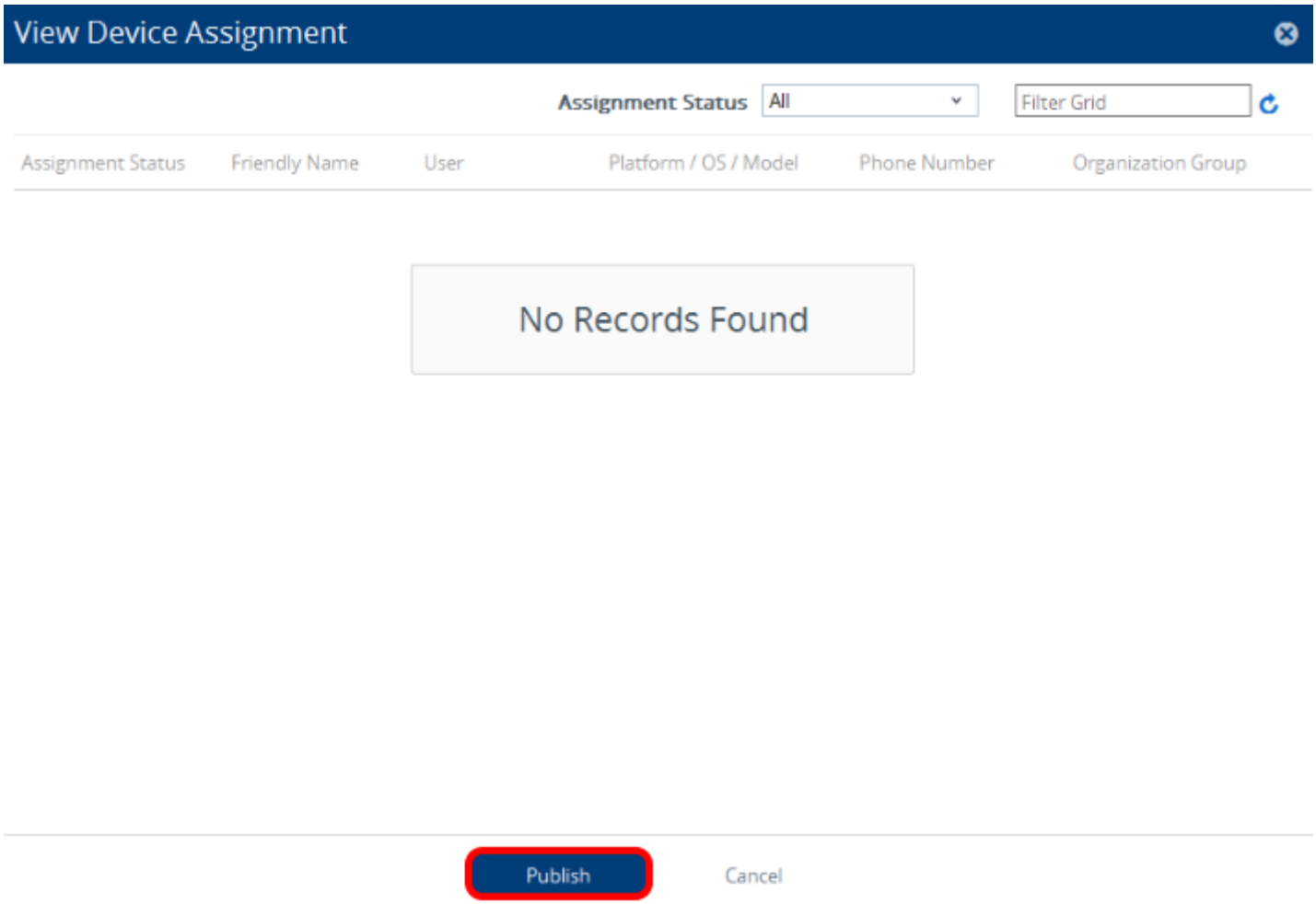
1. Click on the **Restrictions** payload in the left panel.
2. Click **Configure**.

Disable Allow use of camera



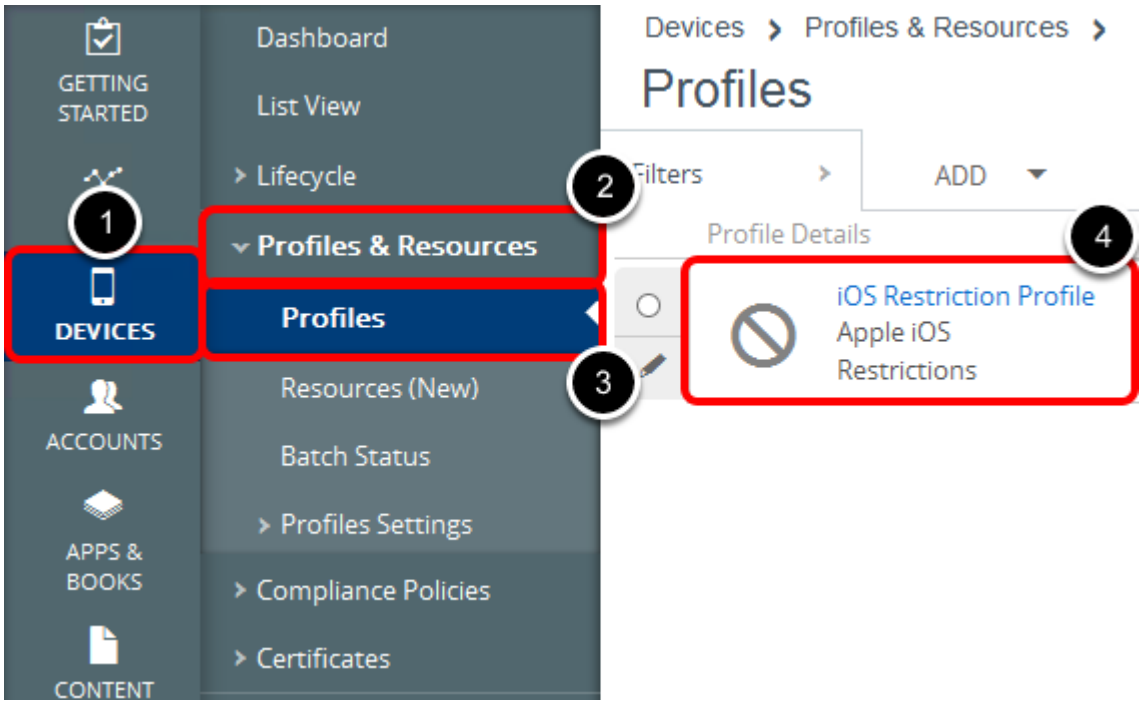
1. Uncheck the **Allow use of Camera** checkbox.
2. Click **Save & Publish**.

Publish the Profile



Click **Publish**.

Validate profile creation



1. Click **Devices**.
2. Expand **Profiles & Resources**.
3. Click **Profiles**.
4. Validate that you see **iOS Restriction Profile** in the Profiles List View.

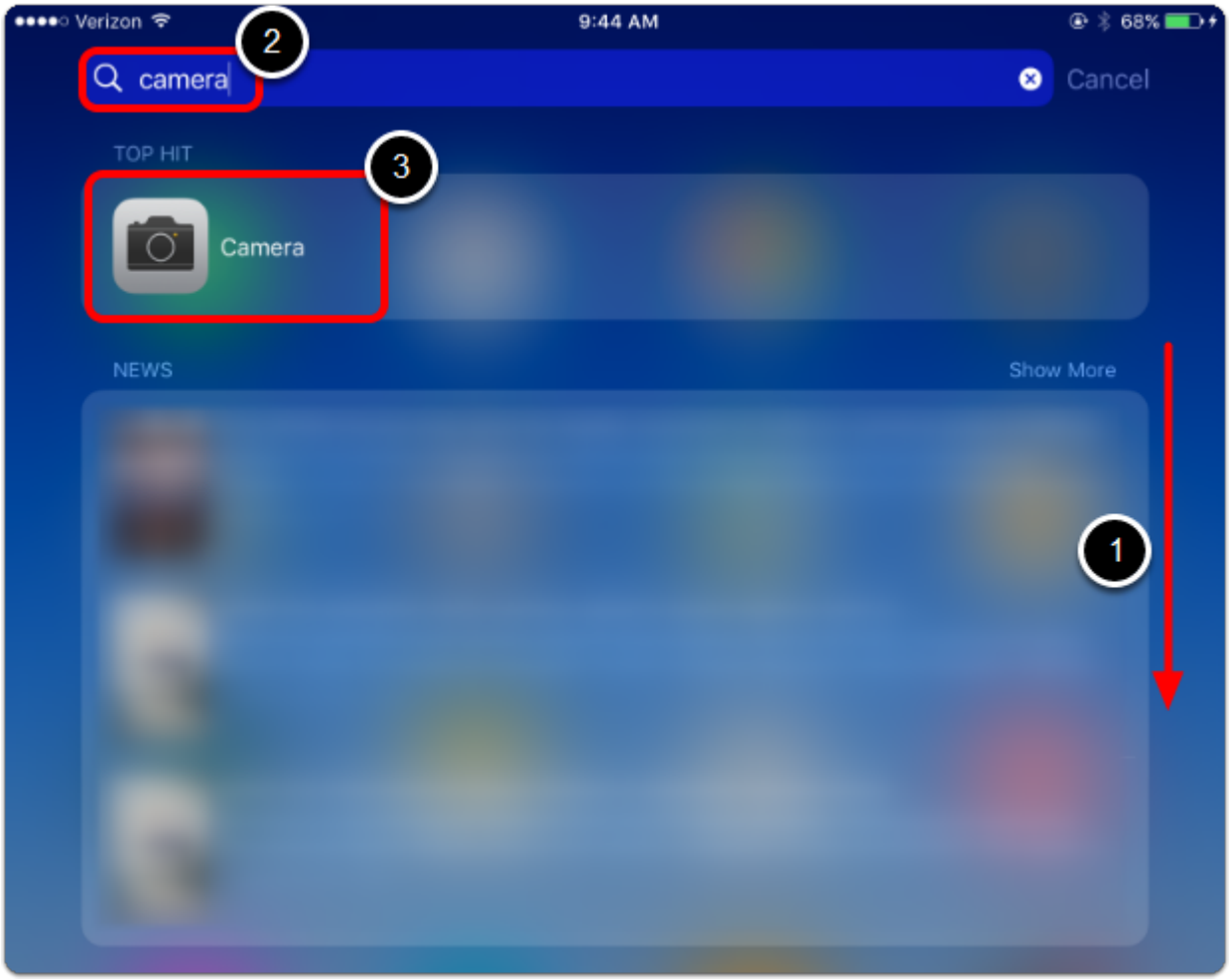
Validate Device Before Restriction Profile

Before enrolling your device, confirm that the Camera app is available on your iOS device.

Find the Camera App

Press the **Home** button on your device and find the **Camera** app. Take note of the location of the app, as we will confirm the removal of the app in a later step after enrollment.

Search for the Camera App (Optional)

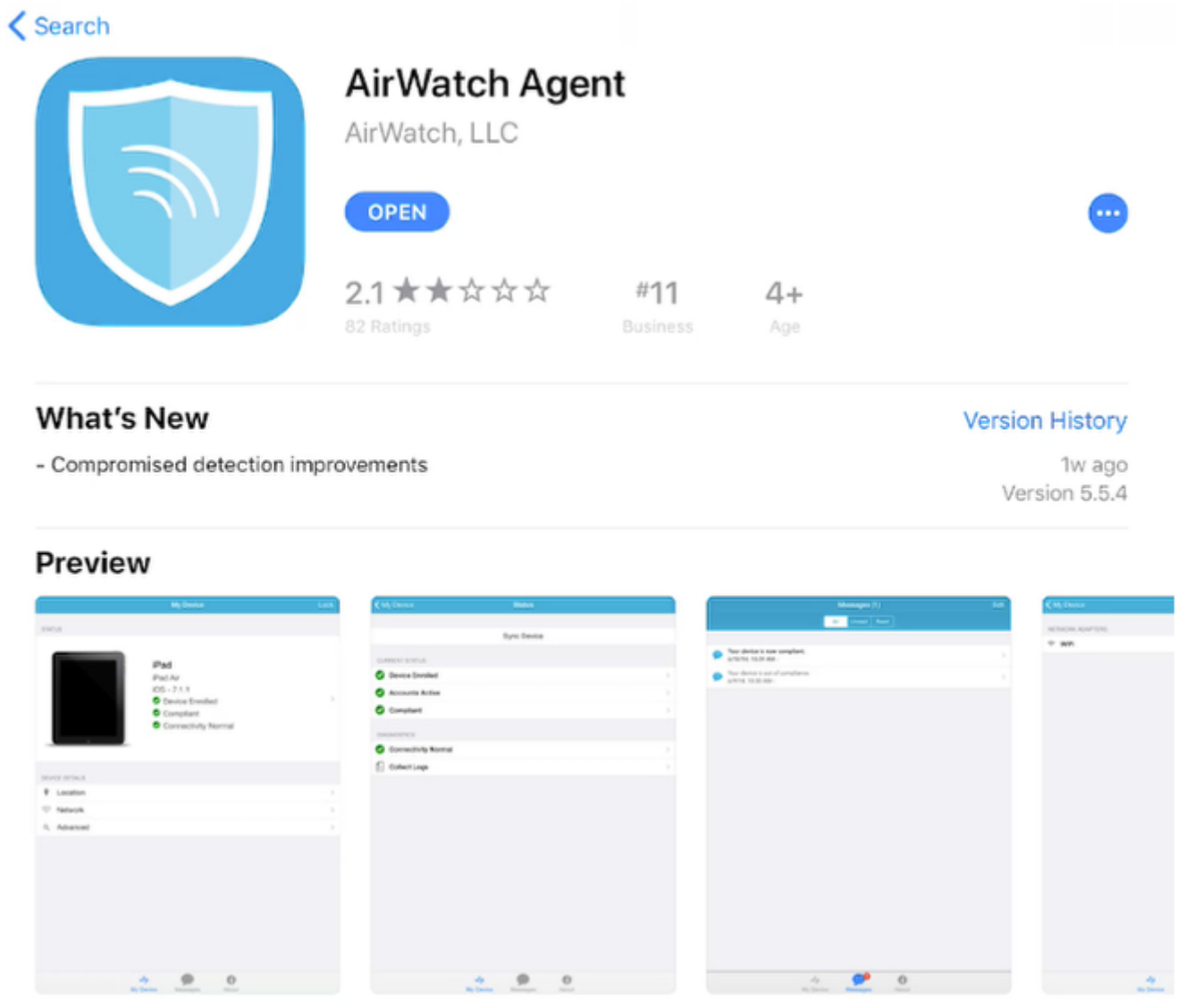


1. Swipe down to show the Search bar.
2. Enter **"camera"** in the Search bar.
3. Ensure the **Camera** app displays, confirming the app exists on the device.

iOS Device Enrollment using basicuser

In this section, we are going to enroll an iOS device to complete the steps on the device side.

Download/Install AirWatch MDM Agent Application from App Store - IF NEEDED



NOTE - Checked out devices will likely have the AirWatch MDM Agent already installed. You may skip this step if your device has the AirWatch MDM agent installed.

At this point, if using your own iOS device or if the device you are using does NOT have the AirWatch MDM Agent Application installed, then install the AirWatch Application.

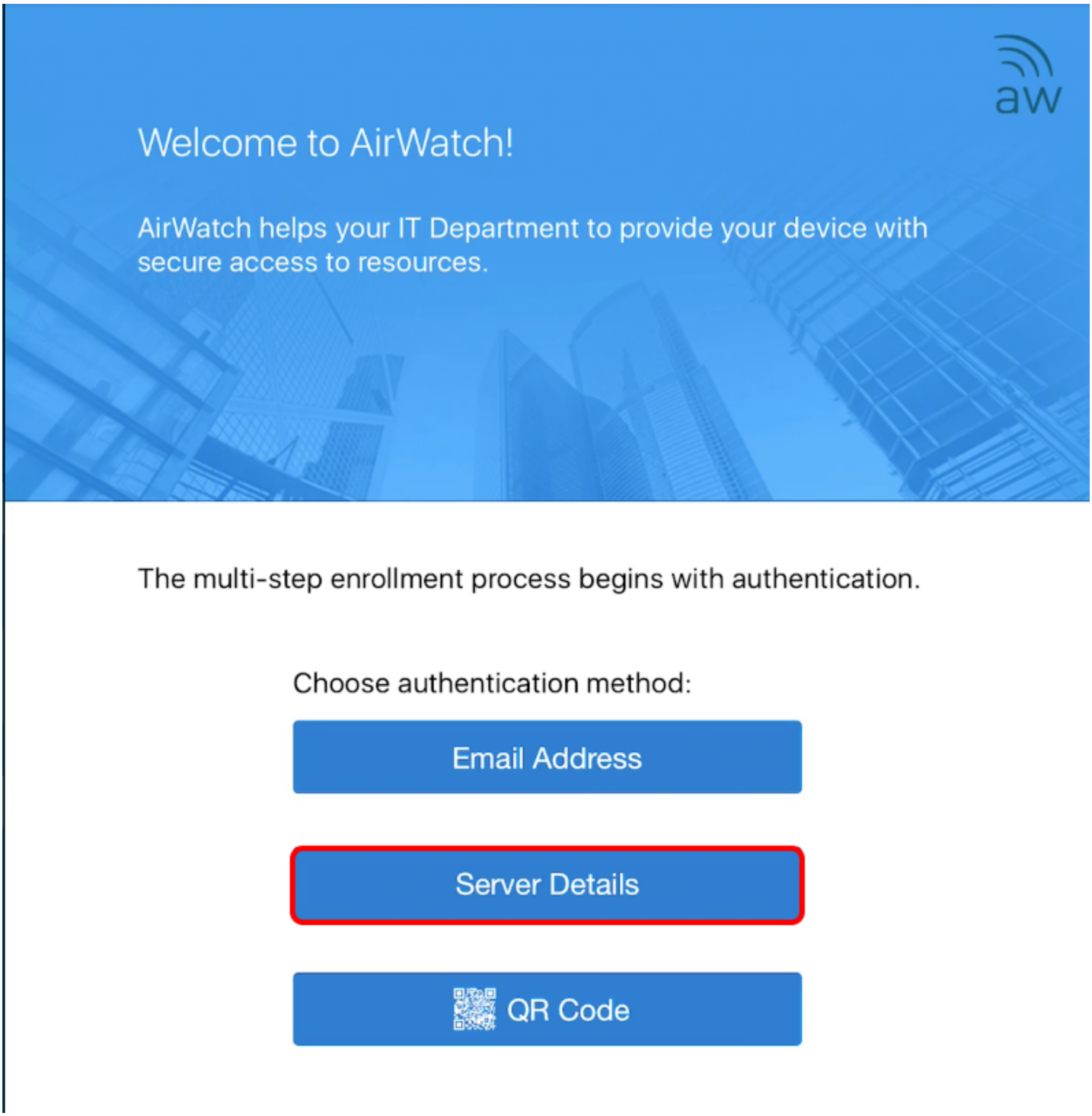
To Install the AirWatch MDM Agent application from the App Store, open the App Store application and download the free **AirWatch MDM Agent** application.

Launching the AirWatch MDM Agent

Launch the **AirWatch Agent** app on the device.

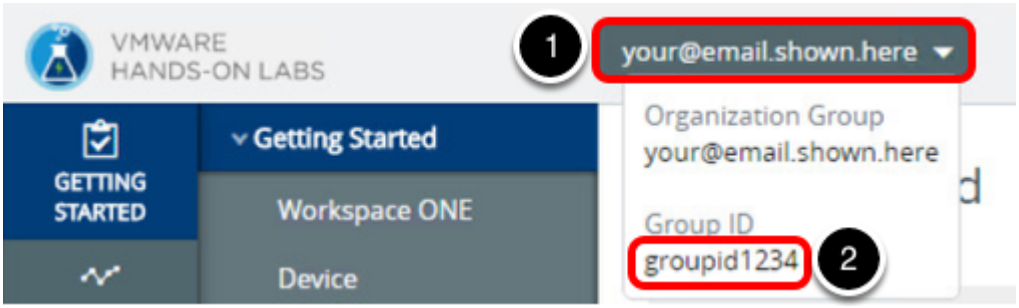
NOTE - If you have your own iOS device and would like to test you will need to download the agent first.

Choose the Enrollment Method



Click on the **Server Details** button.

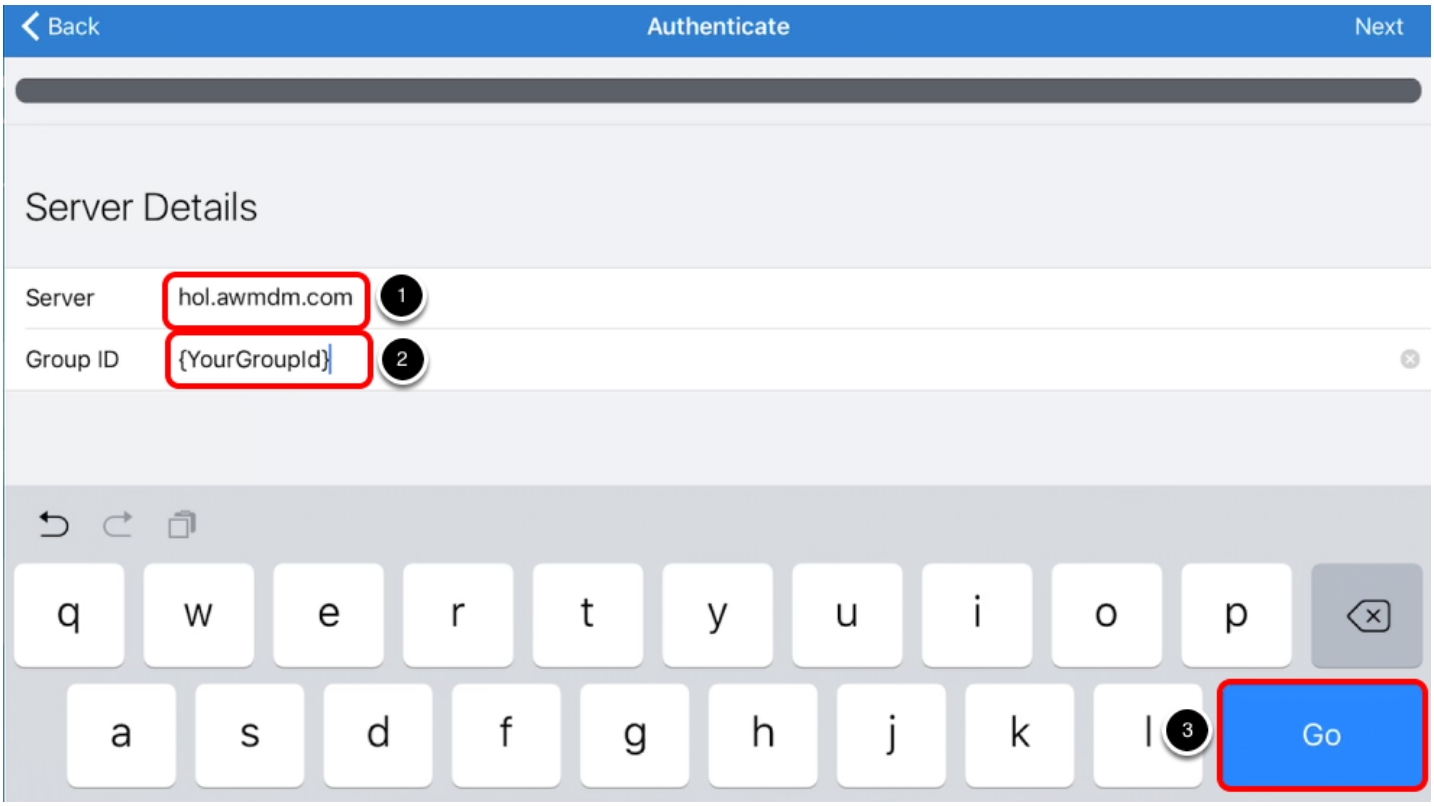
Find your Group ID from AirWatch Console



1. To find the Group ID, hover your mouse over the Organization Group tab at the top of the screen. Look for the email address you used to log in to the lab portal.
2. Your **Group ID** is displayed at the bottom of the Organization Group pop up.

NOTE - The Group ID is required when enrolling your device in the following steps.

Attach the AirWatch MDM Agent to the HOL Sandbox



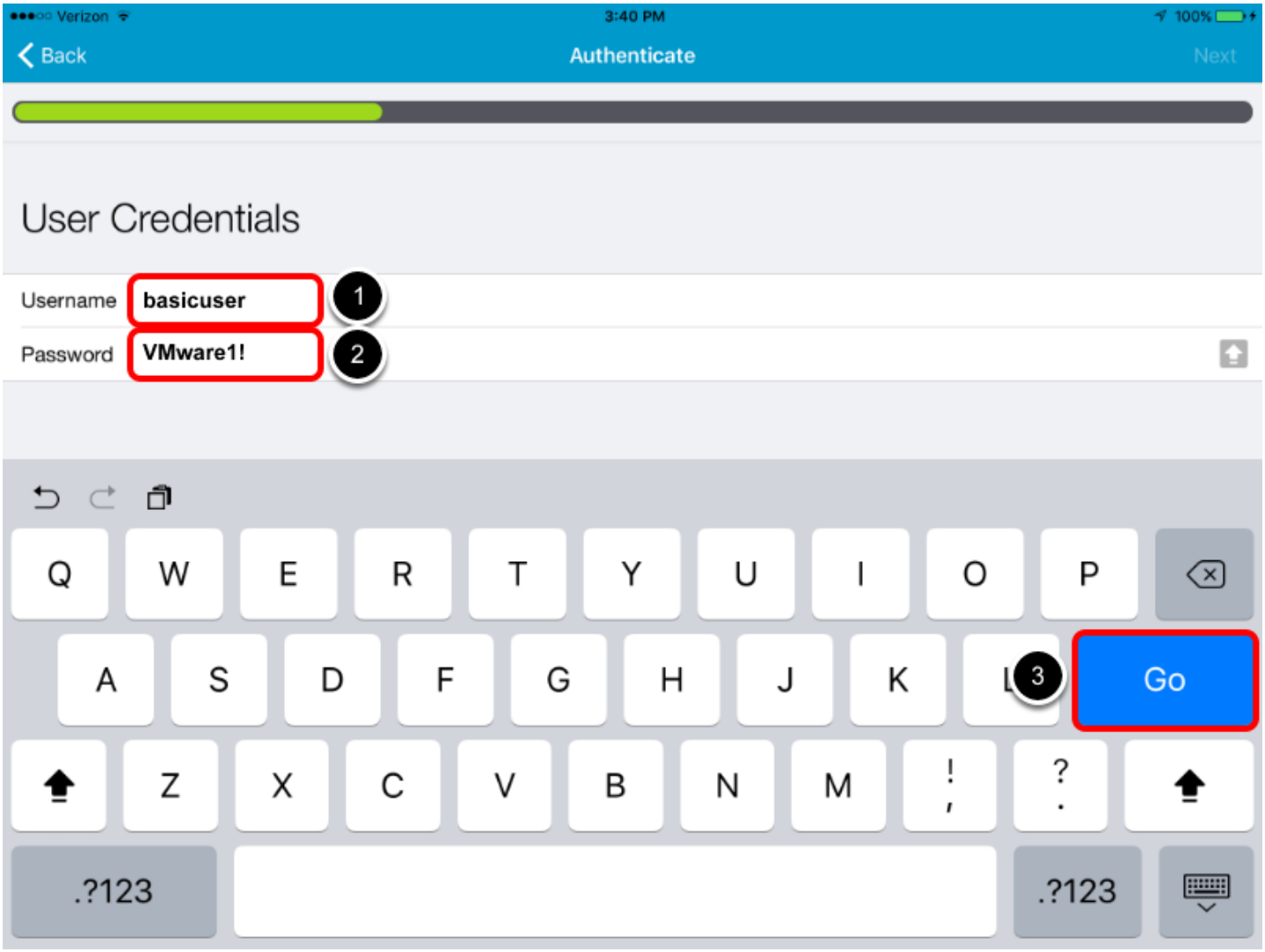
Once the Agent has launched you can enroll the device. To do so, follow the below steps.

1. Enter **"hol.awmdm.com"** for the **Server** field.

2. Enter your **Group ID** for your Organization Group for the **Group ID** field. Your Group ID was noted previously in the **Finding your Group ID** step.
3. Tap the **Go** button.

NOTE - If on an iPhone, you may have to close the keyboard by clicking Done in order to click the Continue button.

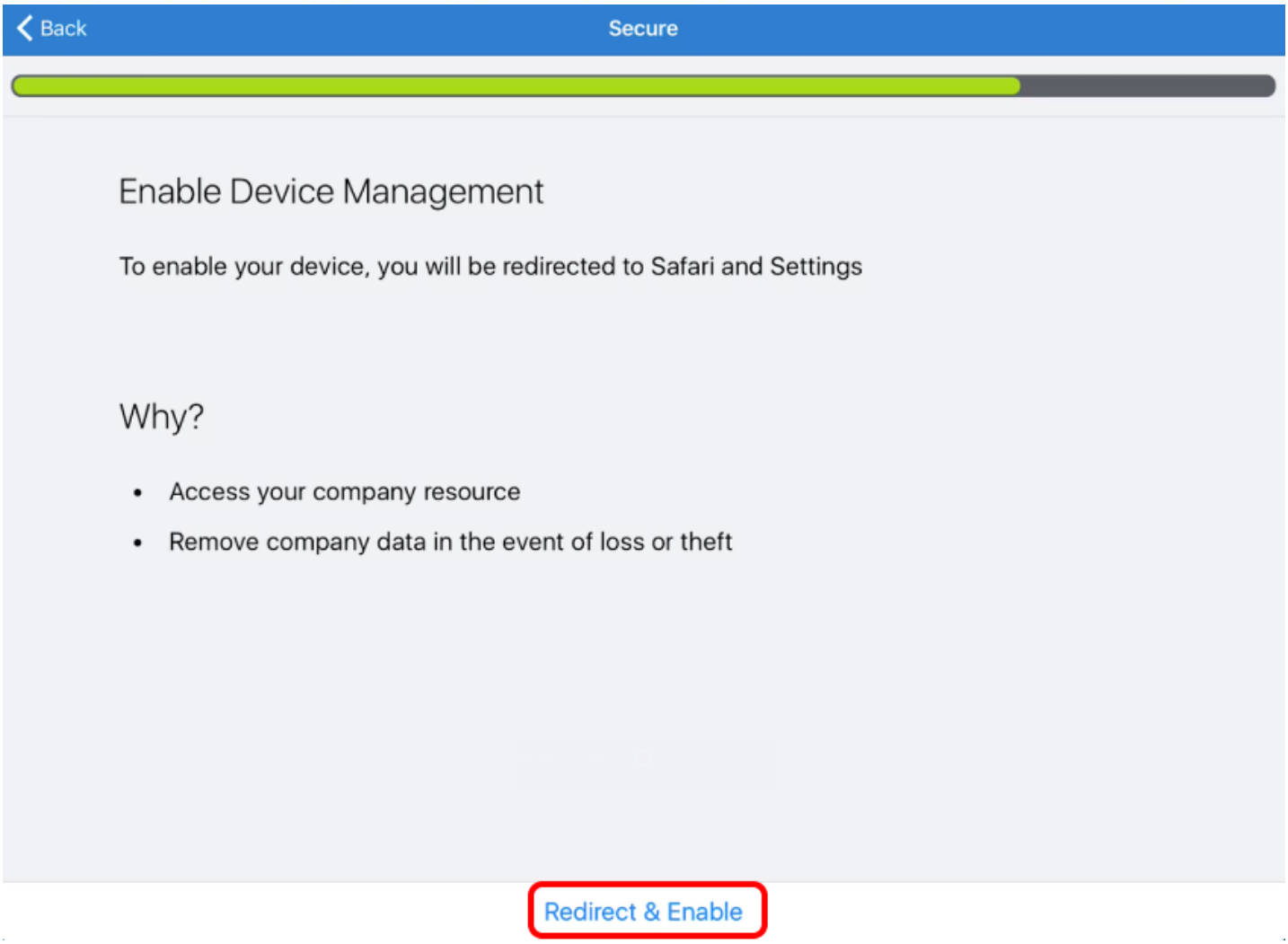
Authenticate the AirWatch MDM Agent



On this screen, enter the **Username** and **Password** for the basic user account.

1. Enter **"basicuser"** in the **Username** field.
2. Enter **"VMware1!"** in the **Password** field.
3. Tap the **Go** button.

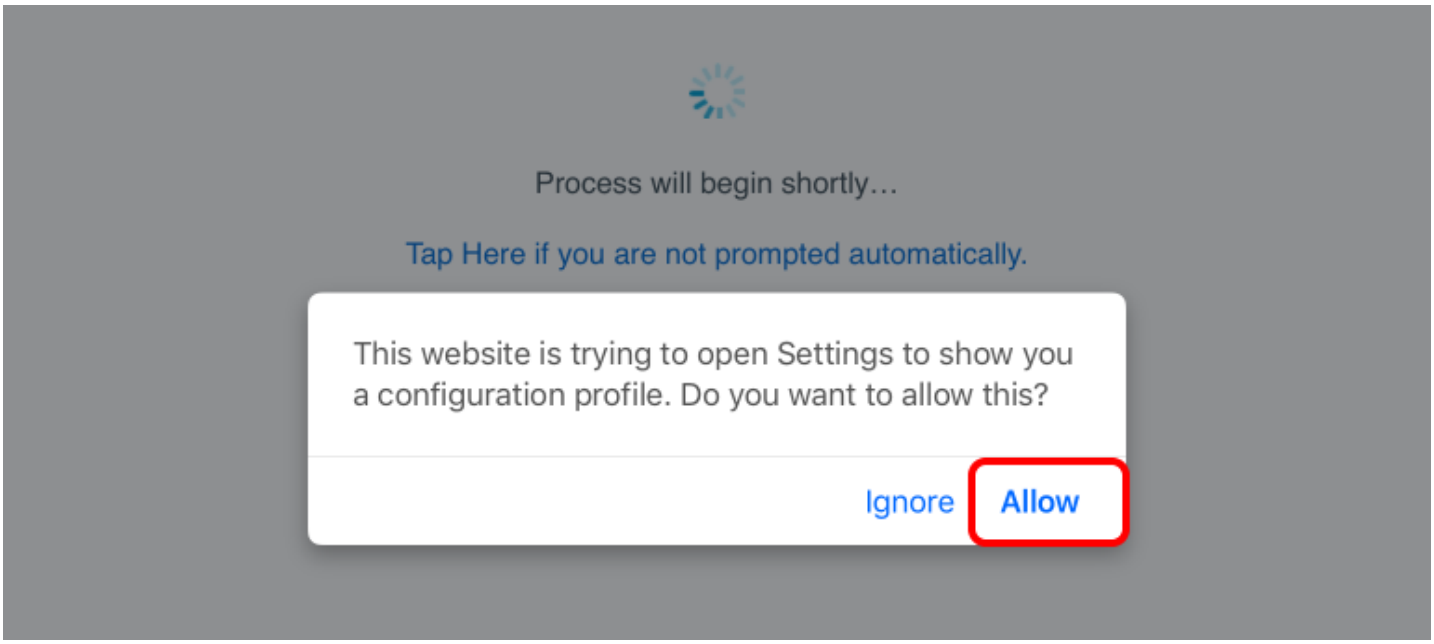
Redirect to Safari and Enable MDM Enrollment in Settings



The AirWatch Agent will now redirect you to Safari and start the process of enabling MDM in the device settings.

Tap on **Redirect & Enable** at the bottom of the screen.

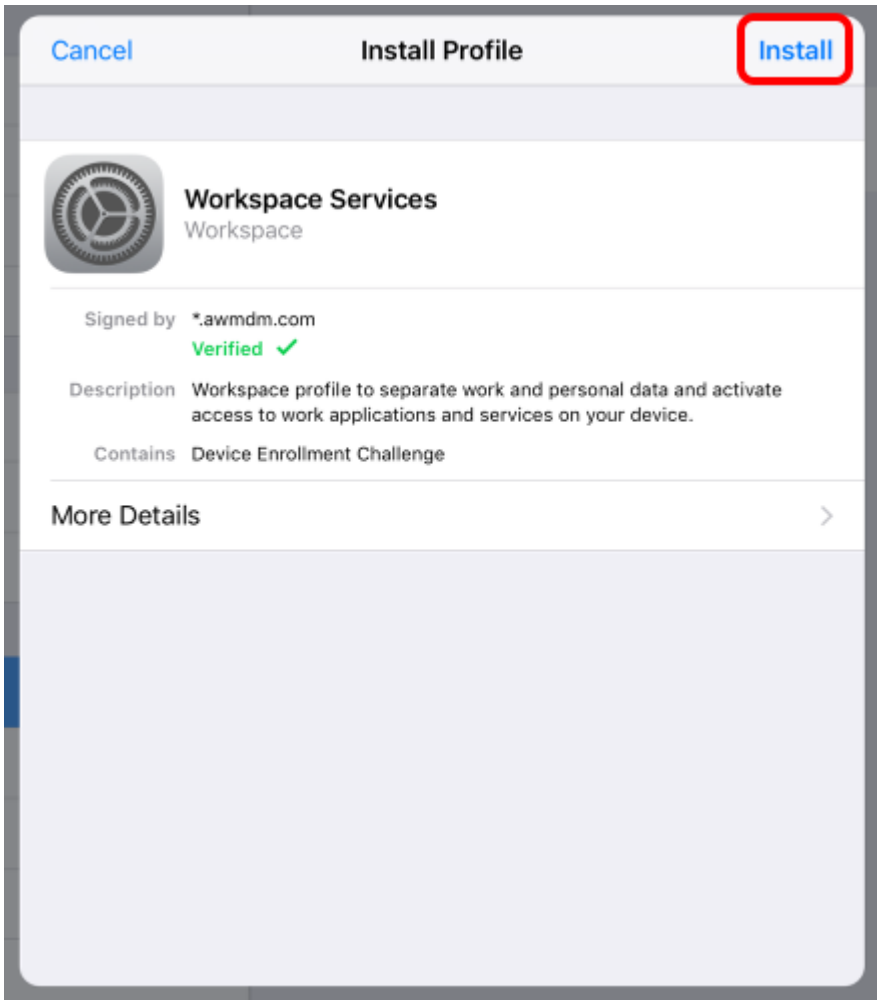
Allow Website to Open Settings (IF NEEDED)



If you prompted to allow the website to open Settings to show you a configuration profile, tap **Allow**.

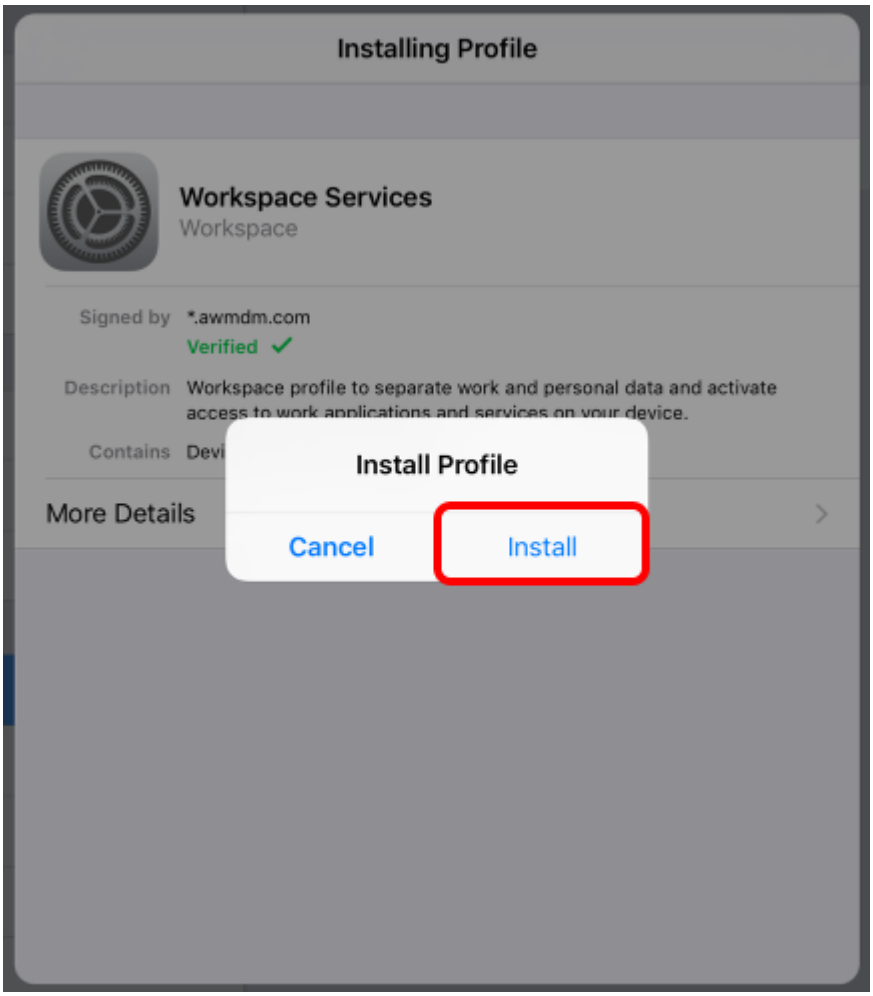
NOTE - If you do not see this prompt, ignore this and continue to the next step. This prompt will only occur for iOS Devices on iOS 10.3.3 or later

Install the MDM Profile



Tap **Install** in the upper right corner of the Install Profile dialog box.

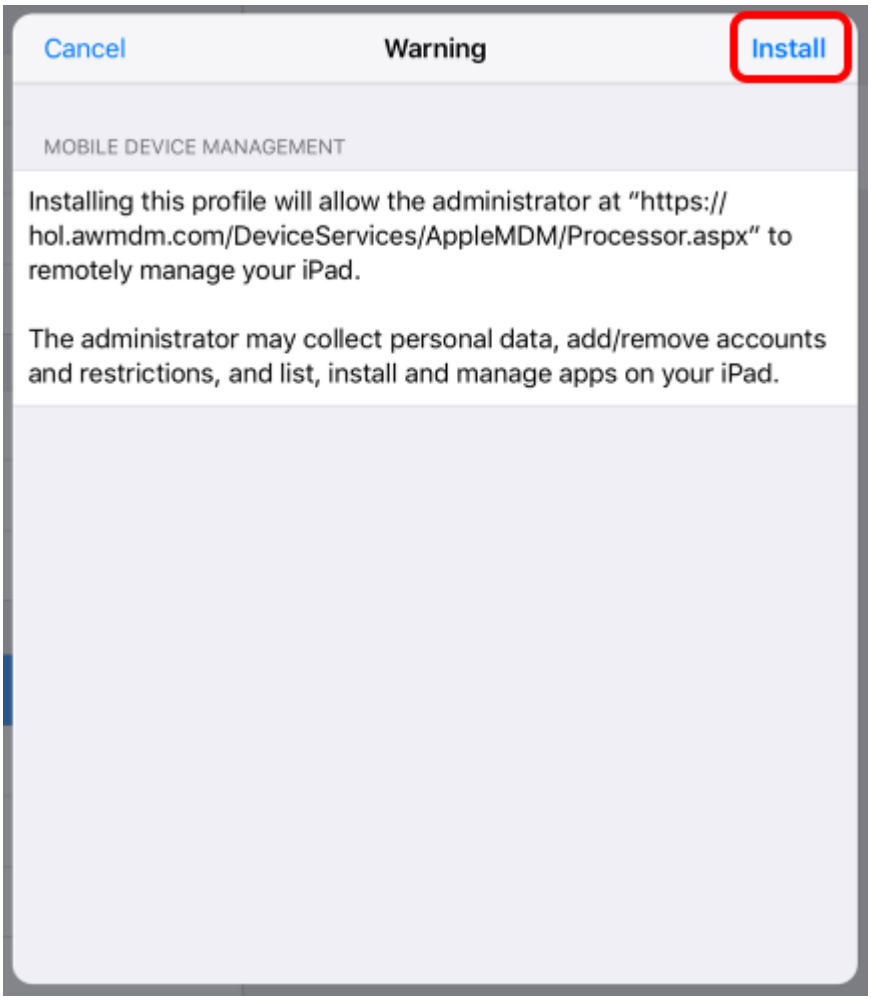
Install and Verify the AirWatch MDM Profile



Tap **Install** when prompted at the Install Profile dialog.

NOTE - If a PIN is requested, it is the current device PIN. Provided VMware devices should not have a PIN.

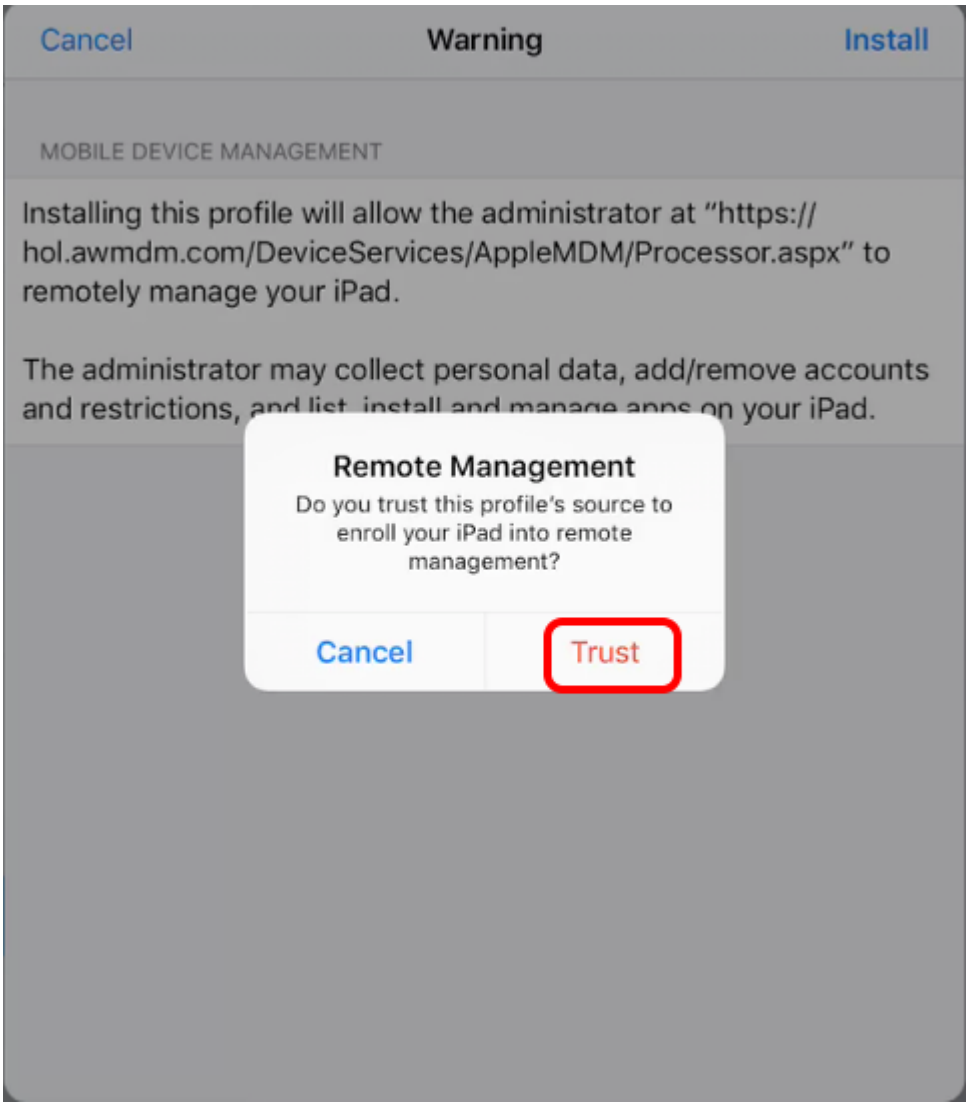
iOS MDM Profile Warning



You should now see the iOS Profile Installation warning explaining what this profile installation will allow on the iOS device.

Tap **Install** in the upper-right corner of the screen.

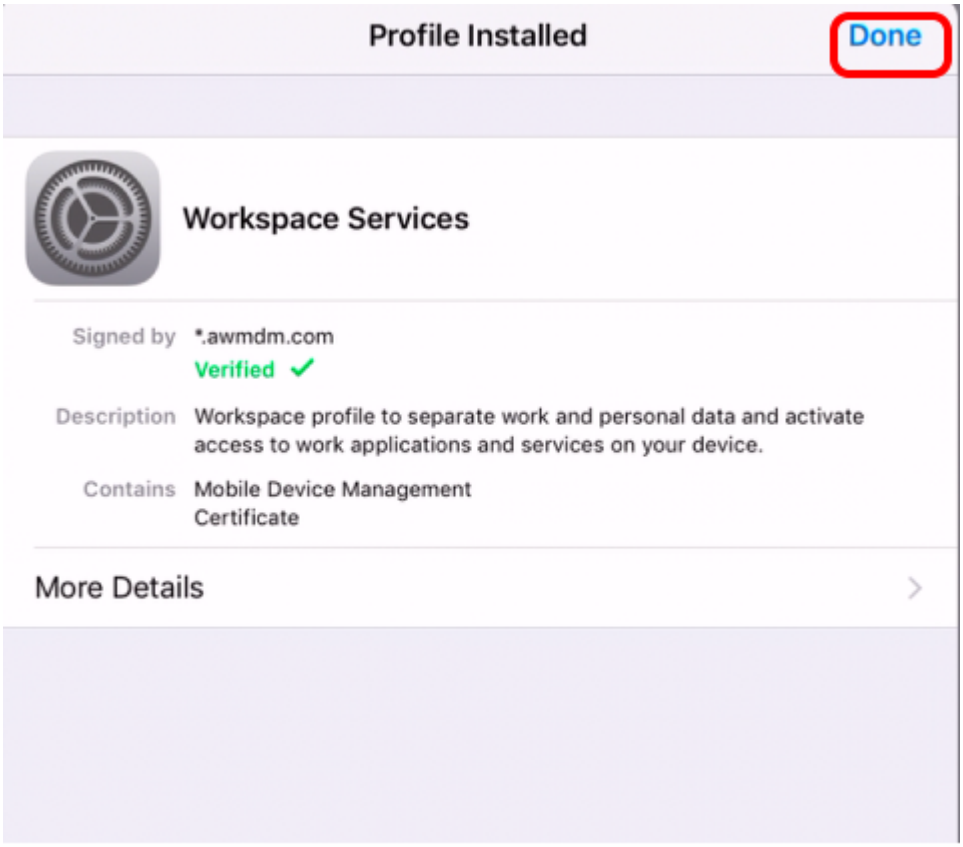
Trust the Remote Management Profile.



You should now see the iOS request to trust the source of the MDM profile.

Tap **Trust** when prompted at the Remote Management dialog.

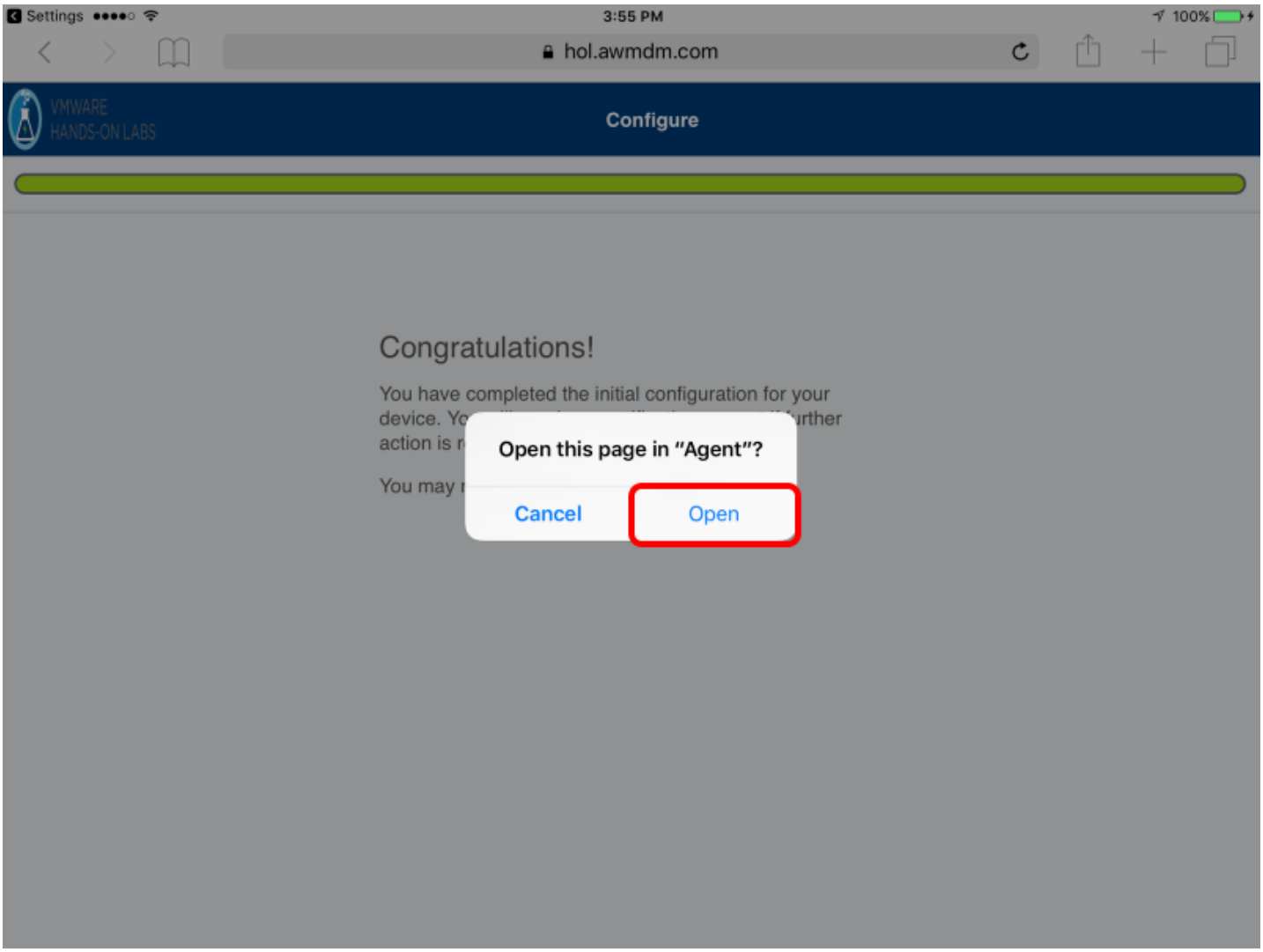
iOS Profile Installation Complete



You should now see the iOS Profile successfully installed.

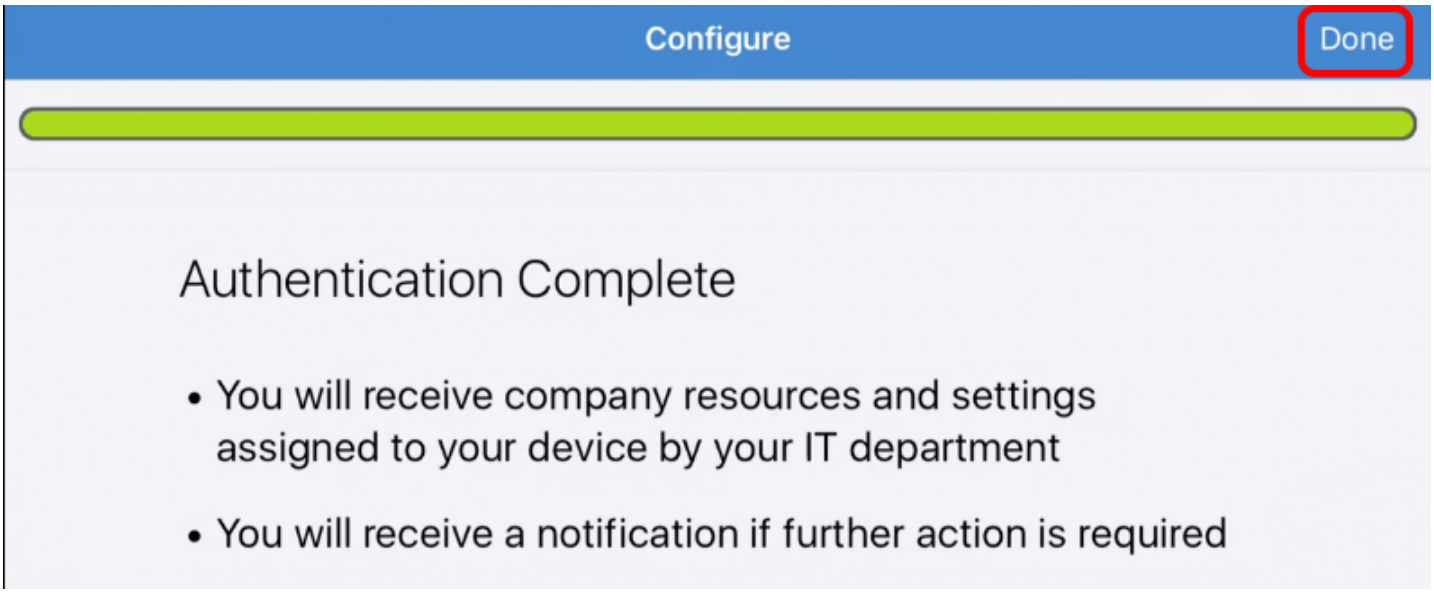
Tap **Done** in the upper right corner of the prompt.

AirWatch Enrollment Success



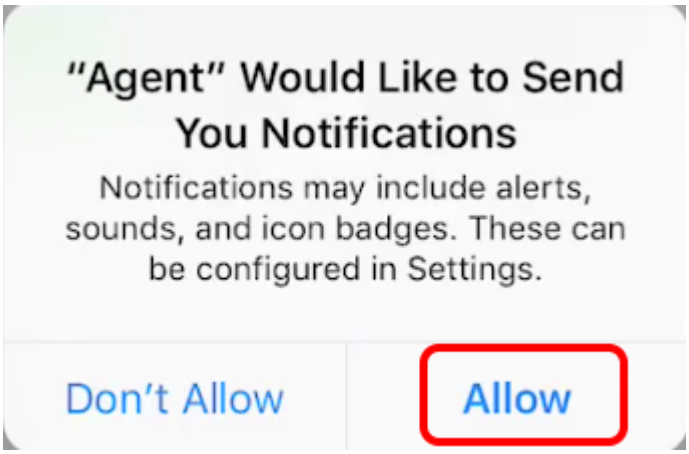
Your enrollment is now completed. Tap **Open** to navigate to the AirWatch Agent.

Accept the Authentication Complete Prompt



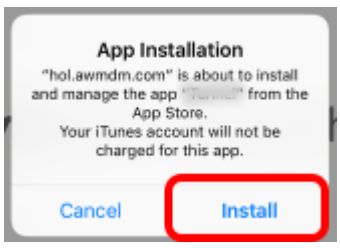
Click on **Done** to continue.

Accept Notification Prompt (IF NEEDED)



Tap **Allow** if you get a prompt for Notifications.

Accept the App Installation (IF NEEDED)



You may be prompted to install a series of applications depending on which Module you are taking. If prompted, tap **Install** to accept the application installation.

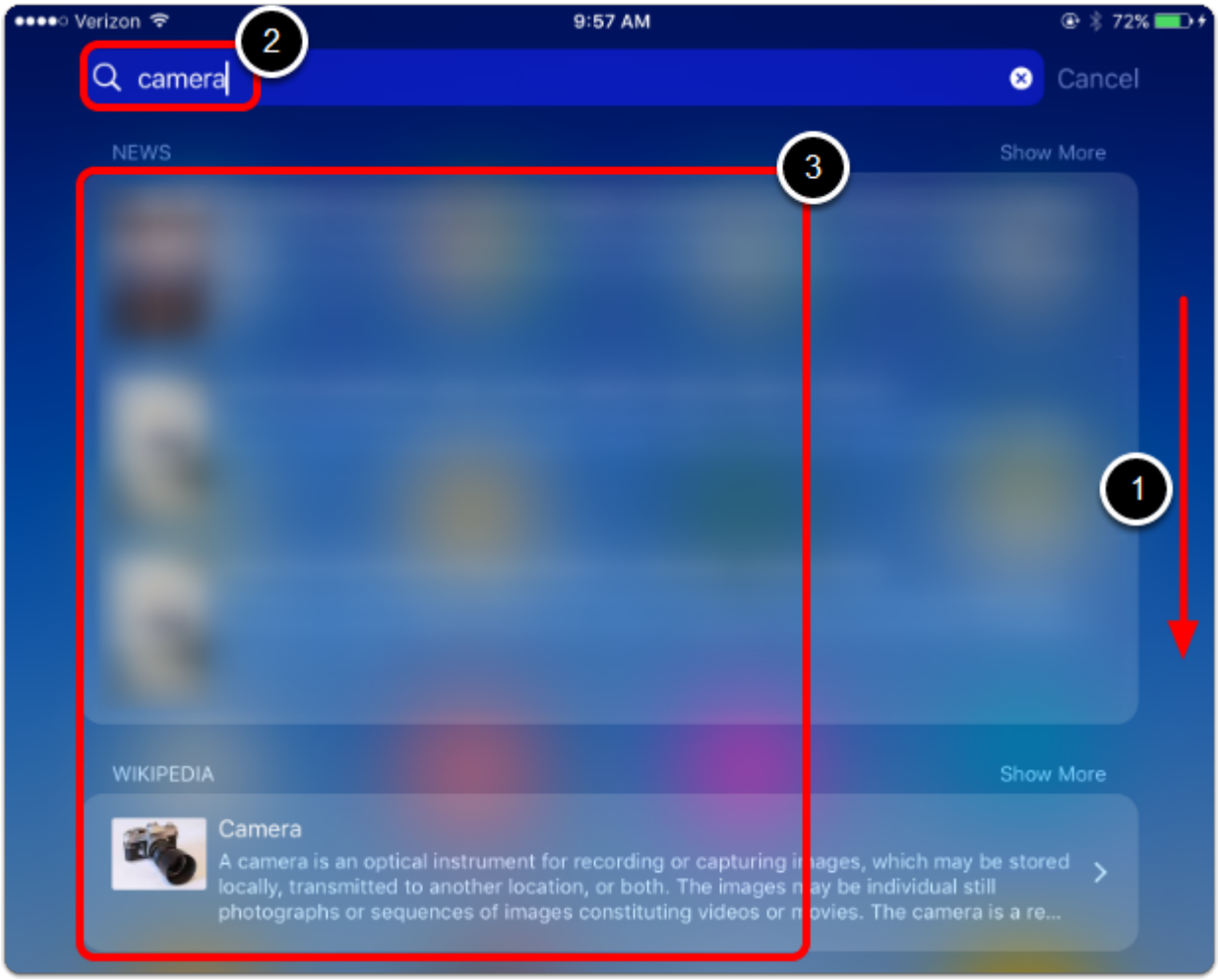
Validate the Restriction Profile

Now that the device is enrolled, the restriction profile we created will be installed on the device and the Camera app will be disabled. Continue to the next steps to verify that the Camera app is successfully disabled.

Return to the Camera App

If you located the Camera app on the device earlier, return to your device and navigate back to where the Camera app previously was. Notice that the Camera app is now disabled and is no longer displayed on the device.

Search for the Camera App (Optional)



1. Swipe down to show the Search bar.
2. Enter **"camera"** in the Search bar.
3. Notice that the Camera app is disabled and no longer displays in the search results.

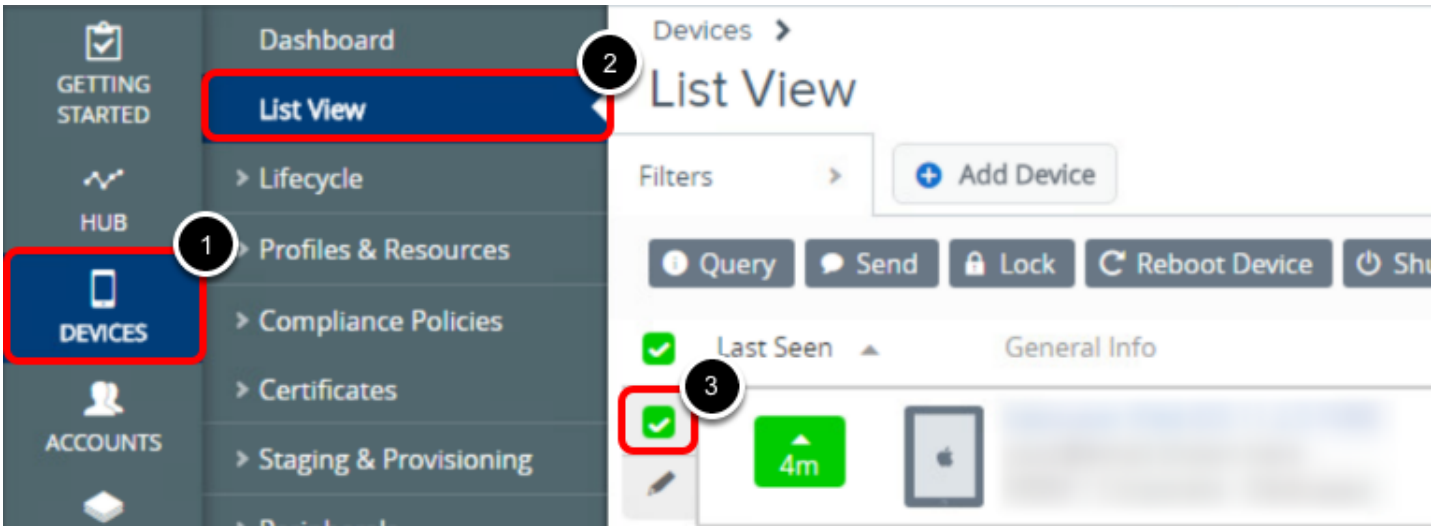
Un-enrolling Your Device

You are now going to un-enroll the iOS device from AirWatch.

NOTE - The term "Enterprise Wipe" does not mean reset or completely wipe your device. This only removes the MDM Profiles, Policies, and content which the AirWatch MDM Agent controls.

It will NOT remove the AirWatch MDM Agent application from the device as this was downloaded manually before AirWatch had control of the device.

Enterprise Wipe (un-enroll) your iOS device



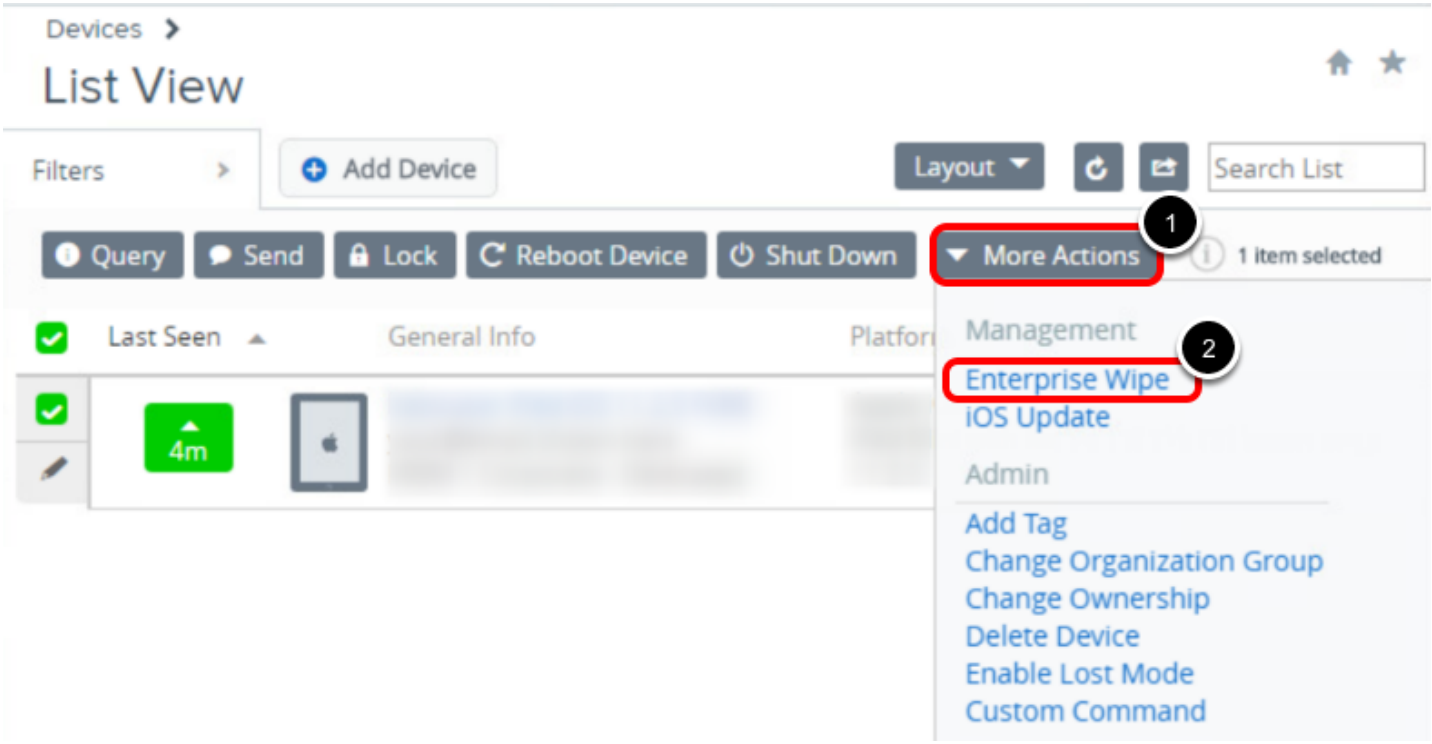
Enterprise Wipe will remove all the settings and content that were pushed to the device when it was enrolled. It will not affect anything that was on the device prior to enrollment.

To Enterprise Wipe your device you will first bring up the AirWatch Console in a web browser. You may need to re-authenticate with your credentials (VLP registered email address and "VMware1!" as the password).

1. Click **Devices** on the left column.
2. Click **List View**.
3. Click the **checkbox** next to the device you want to Enterprise Wipe.

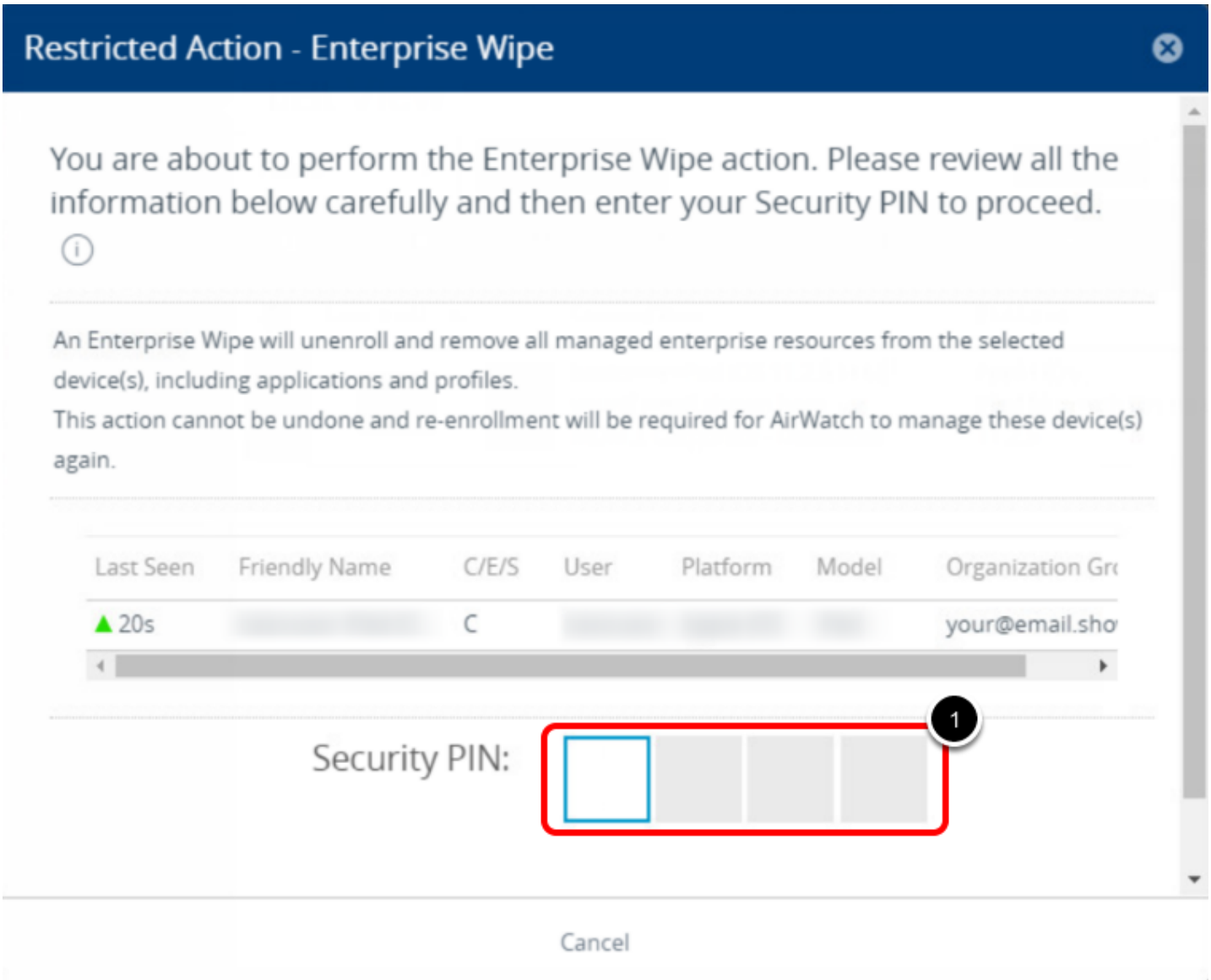
NOTE - Your Device Friendly Name will very likely be different than what is shown. It will, however, be in the same location as shown on image in this step.

Find the Enterprise Wipe Option



1. Click **More Actions**. ***NOTE - If you do not see this option, ensure you have a device selected by clicking the checkbox next to the device.***
2. Click **Enterprise Wipe** under **Management**.

Enter your security PIN



After selecting **Enterprise Wipe**, you will be prompted to enter your Security PIN which you set after your logged into the console (**"1234"**).

1. Enter **"1234"** for the **Security PIN**. You will not need to press enter or continue, the console will confirm your PIN showing "Successful" below the Security PIN input field to indicate that an Enterprise Wipe has been requested. ***NOTE:*** If **"1234"** does not work, then you provided a different Security PIN when you first logged into the AirWatch Console. Use the value you specified for your Security PIN.

NOTE - If the Enterprise Wipe does not immediately occur, follow the below steps to force a device sync:

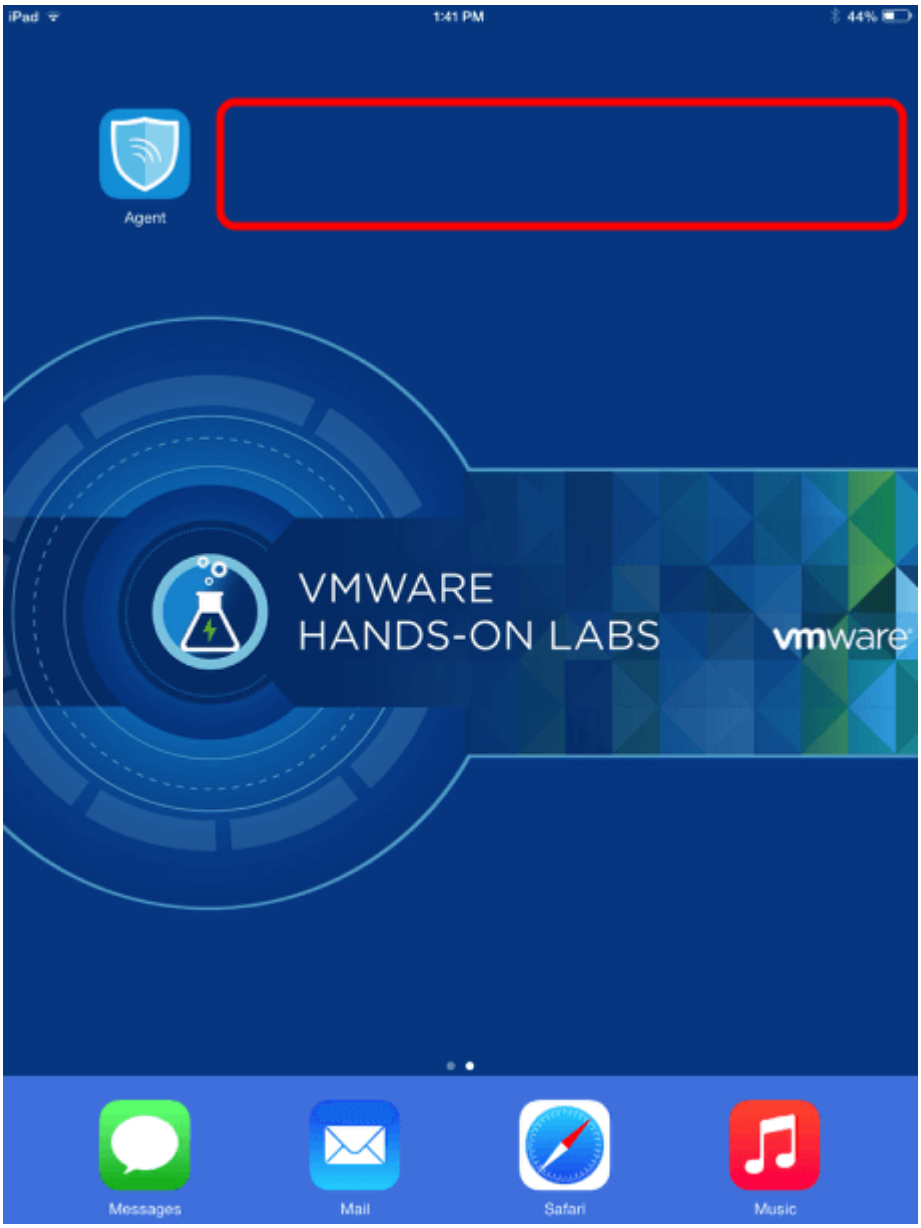
1. On your device, open the **AirWatch Agent** application.

2. Tap the **Device** section (under **Status**) in the middle of the screen.
3. Tap **Send Data** near the top of the screen. If this does not make the device check in and immediately un-enroll, continue to Step #4.
4. If the above doesn't make it immediately un-enroll, then tap **Connectivity [Status]** under Diagnostics.
5. Tap **Test Connectivity** at the top of the screen.

NOTE - Depending upon Internet connectivity of the device and responsiveness of the lab infrastructure, this could take a couple of minutes or more if there is excessive traffic occurring within the Hands On Lab environment.

Feel free to continue to the **"Force the Wipe"** step to manually uninstall the AirWatch services from the device if network connectivity is failing.

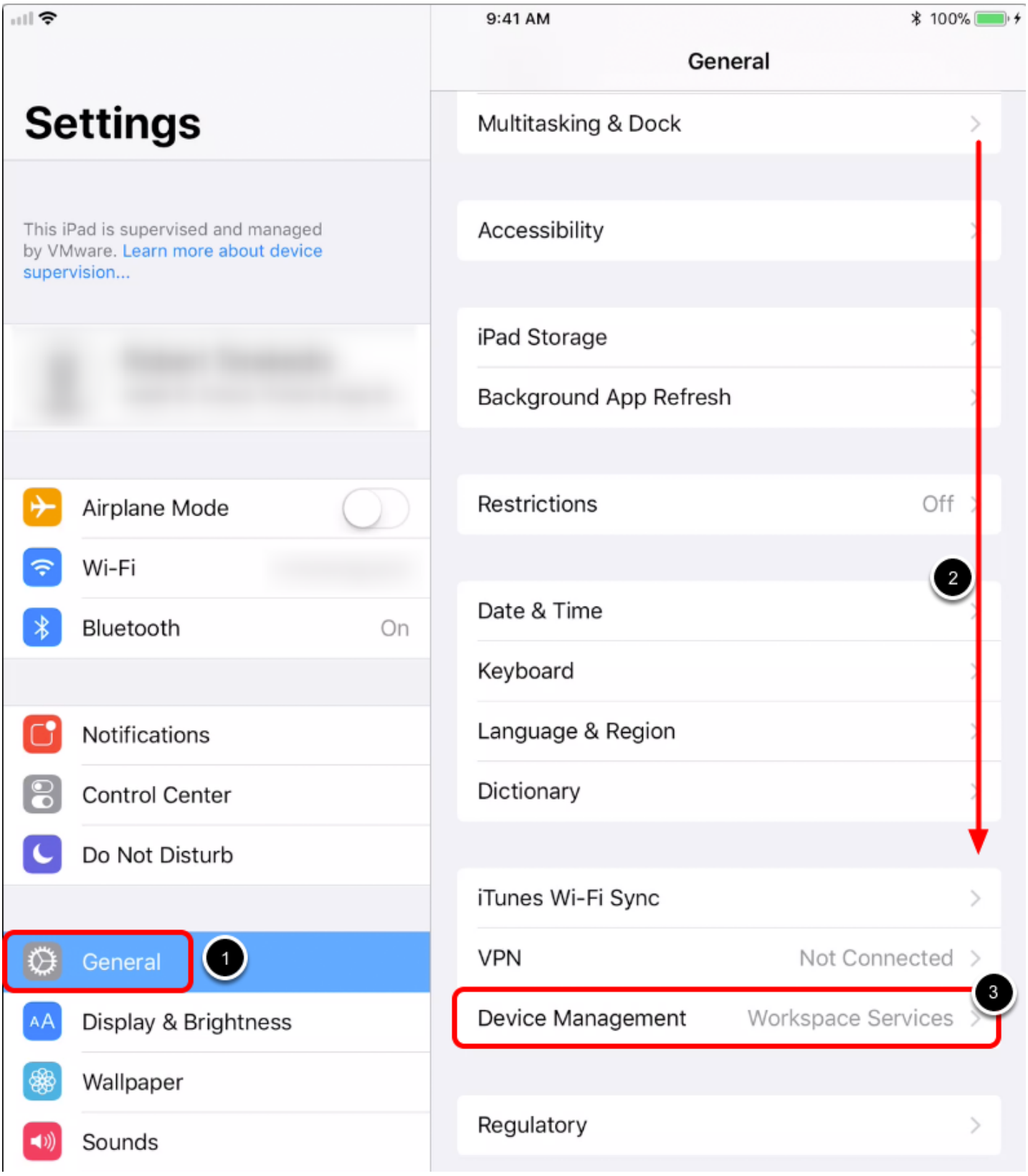
Verify the Un-Enrollment



Press the Home button on the device to go back to the home screen. The applications pushed through AirWatch should have been removed from the device.

NOTE - The applications and settings pushed through AirWatch management should have been removed. The Agent will still be on the device because that was downloaded manually from the App Store. Due to lab environment settings, it may take some time for the signal to traverse through the various networks out and back to your device. Continue on to the next step to force the wipe if the needed.

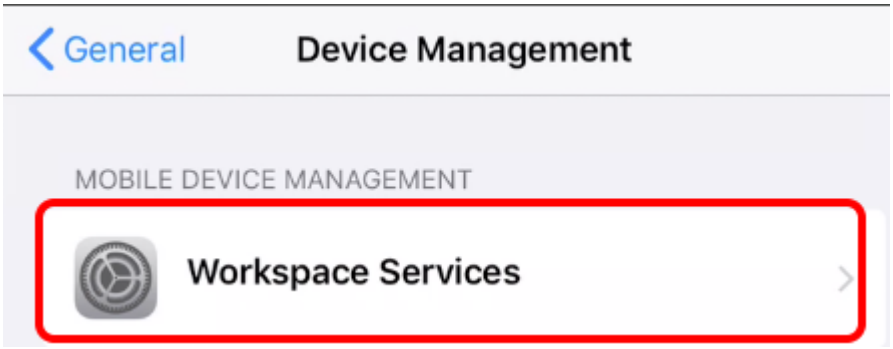
Force the Wipe - IF NECESSARY



If your device did not wipe, follow these instructions to ensure the wipe is forced immediately. Start by opening the iOS **Settings** app.

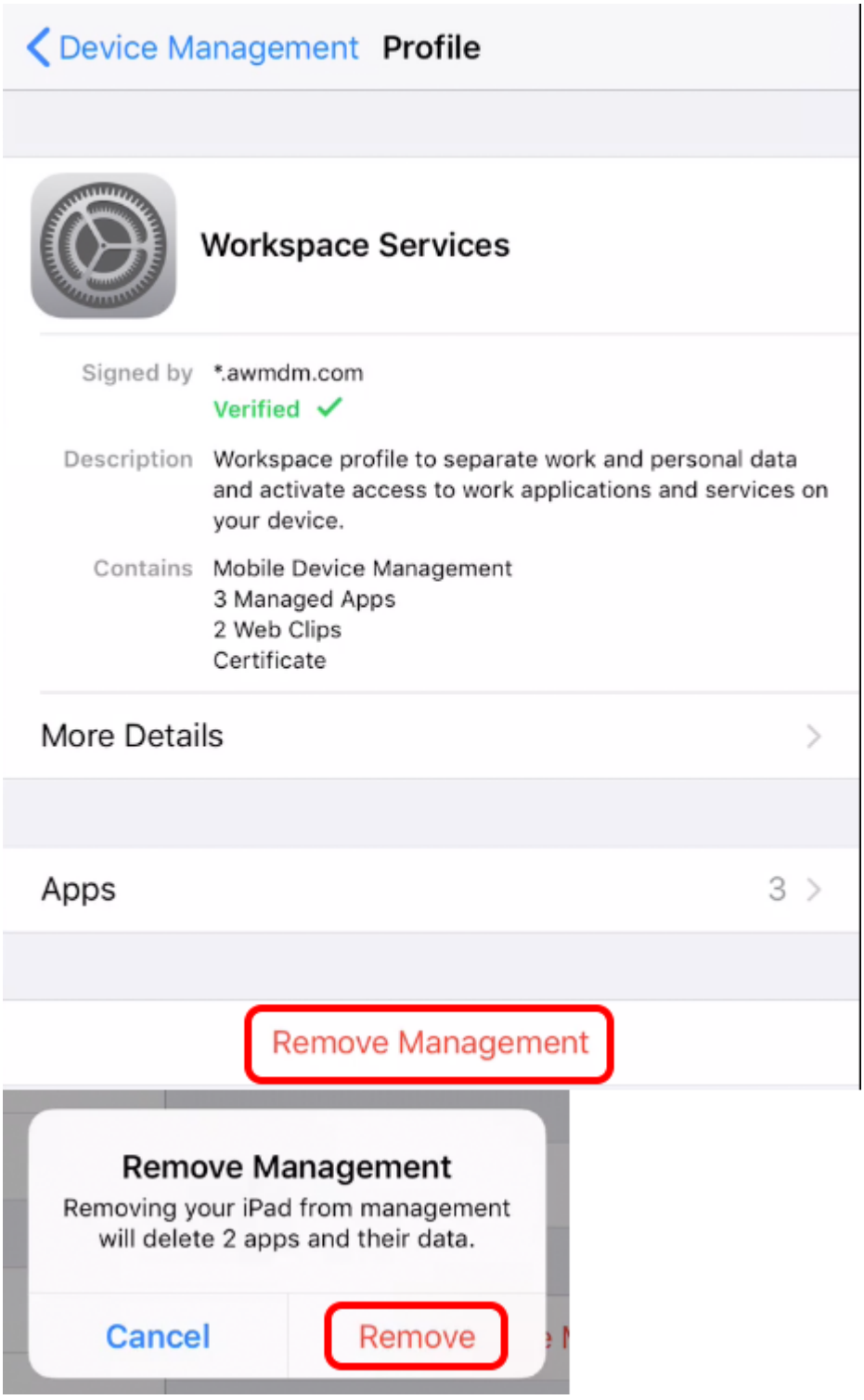
1. Tap **General** in the left column.
2. Scroll down to view the **Device Management** option.
3. Tap **Device Management** at the bottom of the list of General settings.

Force the Wipe - IF NECESSARY



Tap the **Workspace Services** profile that was pushed to the device.

Force the Wipe - IF NECESSARY



1. Tap **Remove Management** on the Workspace Services profile.
   NOTE - If prompted for a device PIN, enter it to continue. VMware provisioned devices should not have a device PIN enabled.
2. Tap **Remove** on the Remove Management prompt.

After removing the Workspace Services profile, the device will be un-enrolled. Feel free to return to the **"Verify the Un-Enrollment"** step to confirm the successful un-enrollment of the device.

Conclusion

Managing your devices with AirWatch empowers your administrators to ensure devices are operating and accessing corporate resources securely without violating user privacy. Now that you know how to enroll a device a push a profile, consider exploring the other lab topics available in this module to further expand your AirWatch knowledge.

This concludes the Introduction to AirWatch module.

Module 2 - Basic Apple macOS Management (45 min)

Introduction

In this lab module, we will explore some AirWatch administration features and concepts available for the macOS platform. This lab will give you a better understanding of how macOS devices are enrolled, what management options you have available, and how these options can improve and impact the user experience by configuring macOS and publishing applications.

Before you can start the lab, make sure you review the next page ensure you can successfully complete the lab.

Pre-Requisites

To successfully complete this Hands-On Lab, you'll need to ensure you have the following pre-requisites:

- An Apple device running macOS version 10.12.6 (Sierra) or later.

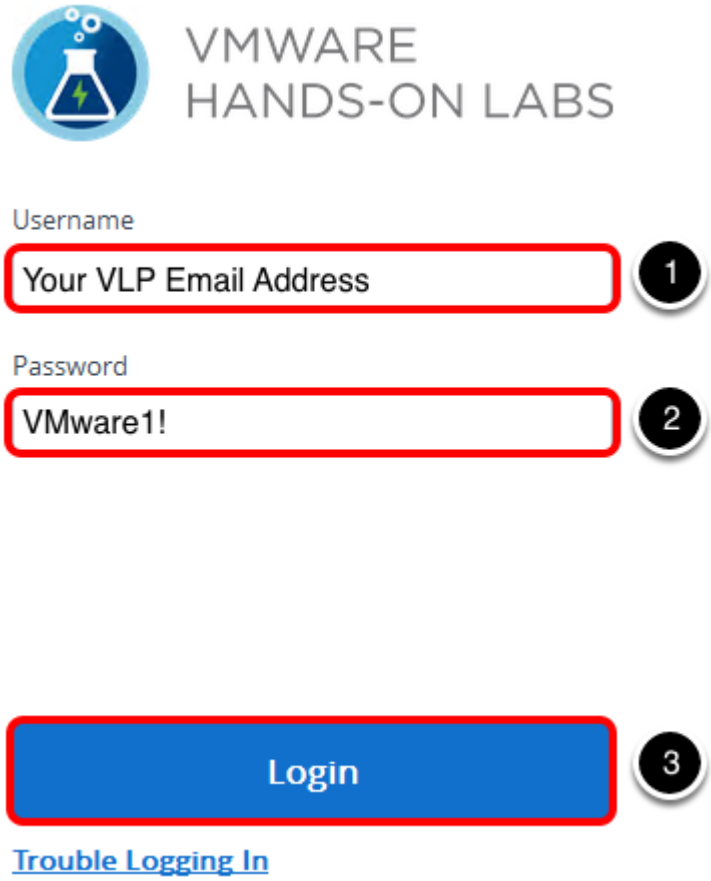
Login to the AirWatch Console

To perform most of the lab you will need to login to the AirWatch Management Console.

Launch Chrome Browser

Double-click the **Chrome** Browser on the lab desktop.

Authenticate to the AirWatch Administration Console



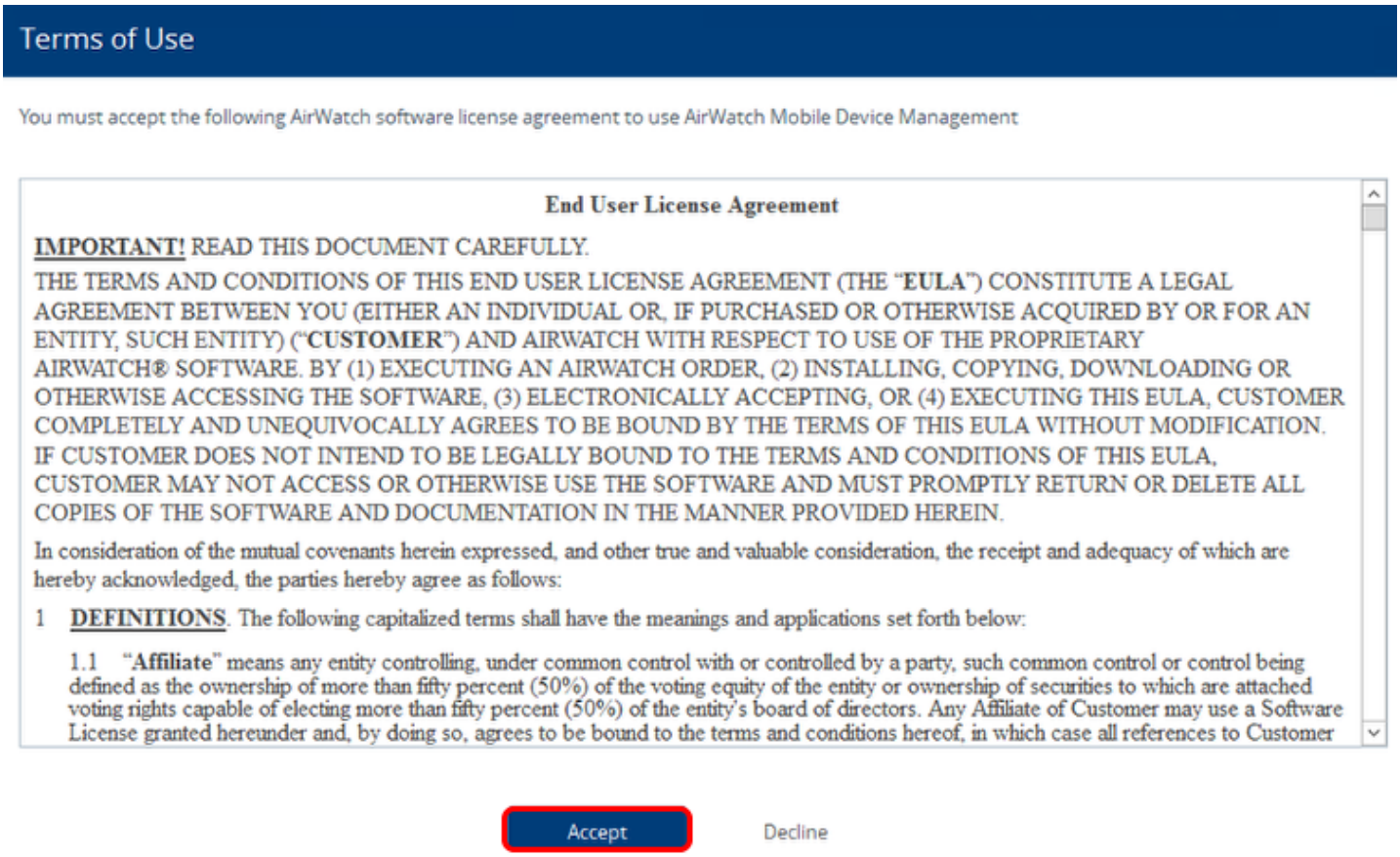
The default home page for the browser is **https://hol.awmdm.com**. Enter your AirWatch Admin Account information and click the **Login** button.

NOTE - If you see a Captcha, please be aware that it is case sensitive!

1. Enter your **Username**. This is you **email address** that you have associated with your **VMware Learning Platform (VLP) account**.
2. Enter **"VMware1!"** for the **Password** field.
3. Click the **Login** button.

NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the AirWatch Hands On Labs server.

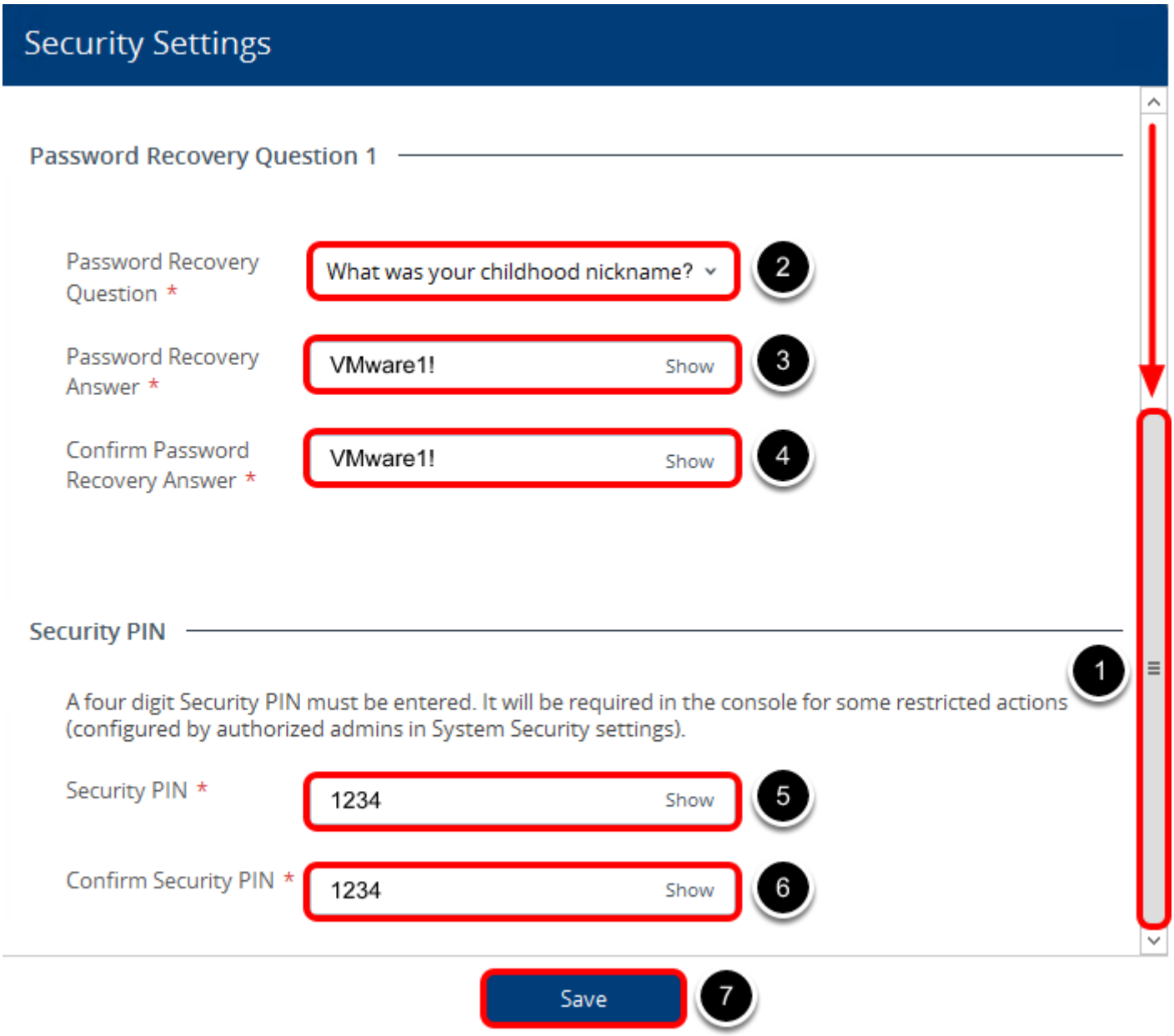
Accept the End User License Agreement



NOTE - The following steps of logging into the Administration Console will only need to be done during the initial login to the console.

You will be presented with the AirWatch Terms of Use. Click the **Accept** button.

Address the Initial Security Settings

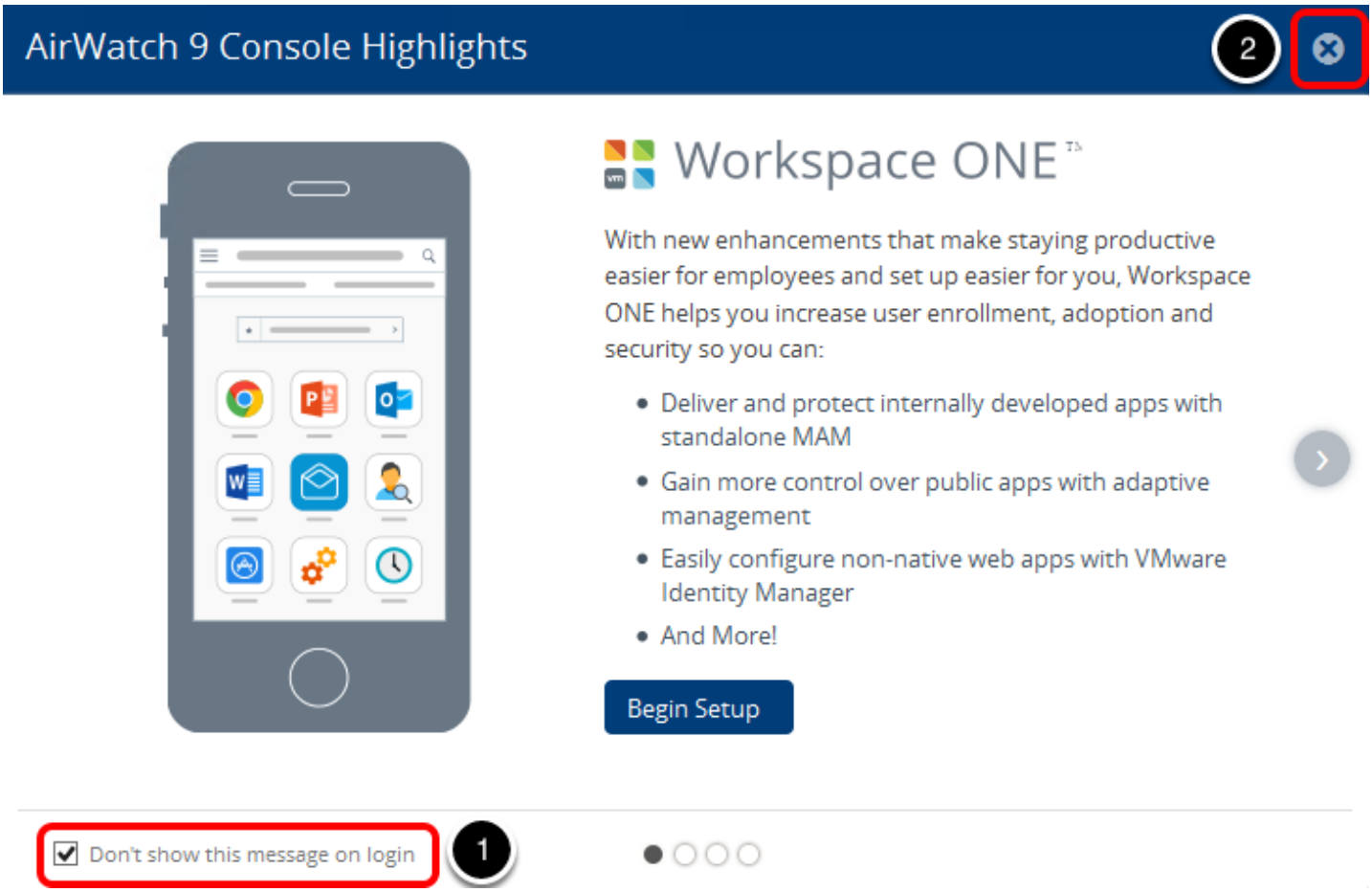


After accepting the Terms of Use, you will be presented with a **Security Settings** pop-up. The **Password Recovery Question** is in case you forget your admin password and the **Security PIN** is to protect certain administrative functionality in the console.

1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a **question** from the **Password Recovery Question** drop-down (default selected question is ok here).
3. Enter **"VMware1!"** in the **Password Recovery Answer** field.
4. Enter **"VMware1!"** in the **Confirm Password Recovery Answer** field.
5. Enter **"1234"** in the **Security PIN** field.
6. Enter **"1234"** in the **Confirm Security PIN** field.

7. Click the **Save** button when finished.

Close the Welcome Message



After completing the Security Settings, you will be presented with the AirWatch Console Welcome pop-up.

1. Click on the **Don't show this message again** check box.
2. Close the pop-up by clicking on the **X** in the upper-right corner.

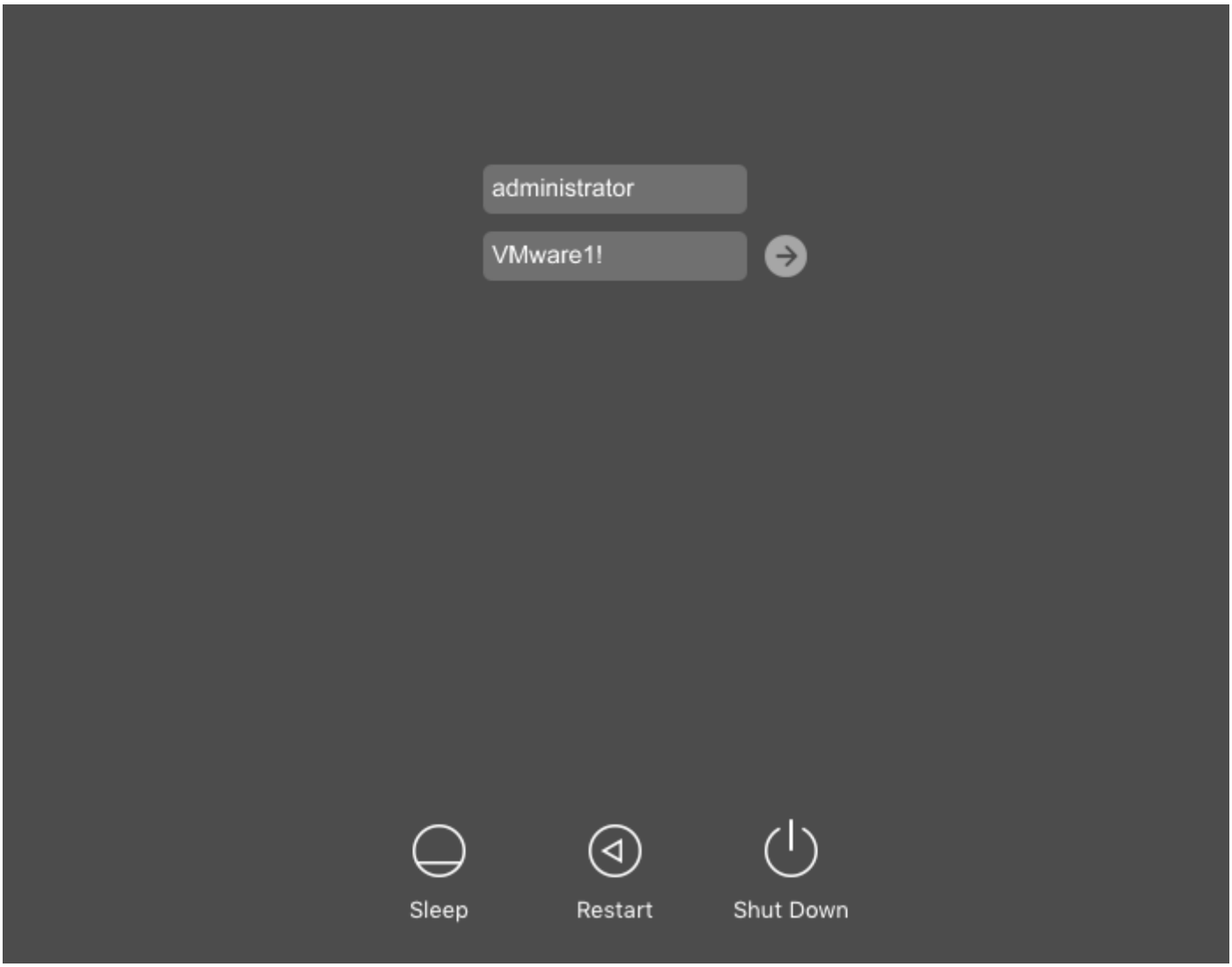
macOS Enrollment

In this section you will enroll a macOS device into AirWatch. Enrollment is the action that brings a device under management and control by AirWatch. There are a number of ways to enroll the various platforms (macOS included), but for this lab we cover just a basic enrollment scenario.

Download the AirWatch Agent

In this exercise, you will enroll using the AirWatch Agent to begin the staging process.

Login to the Mac - IF NEEDED

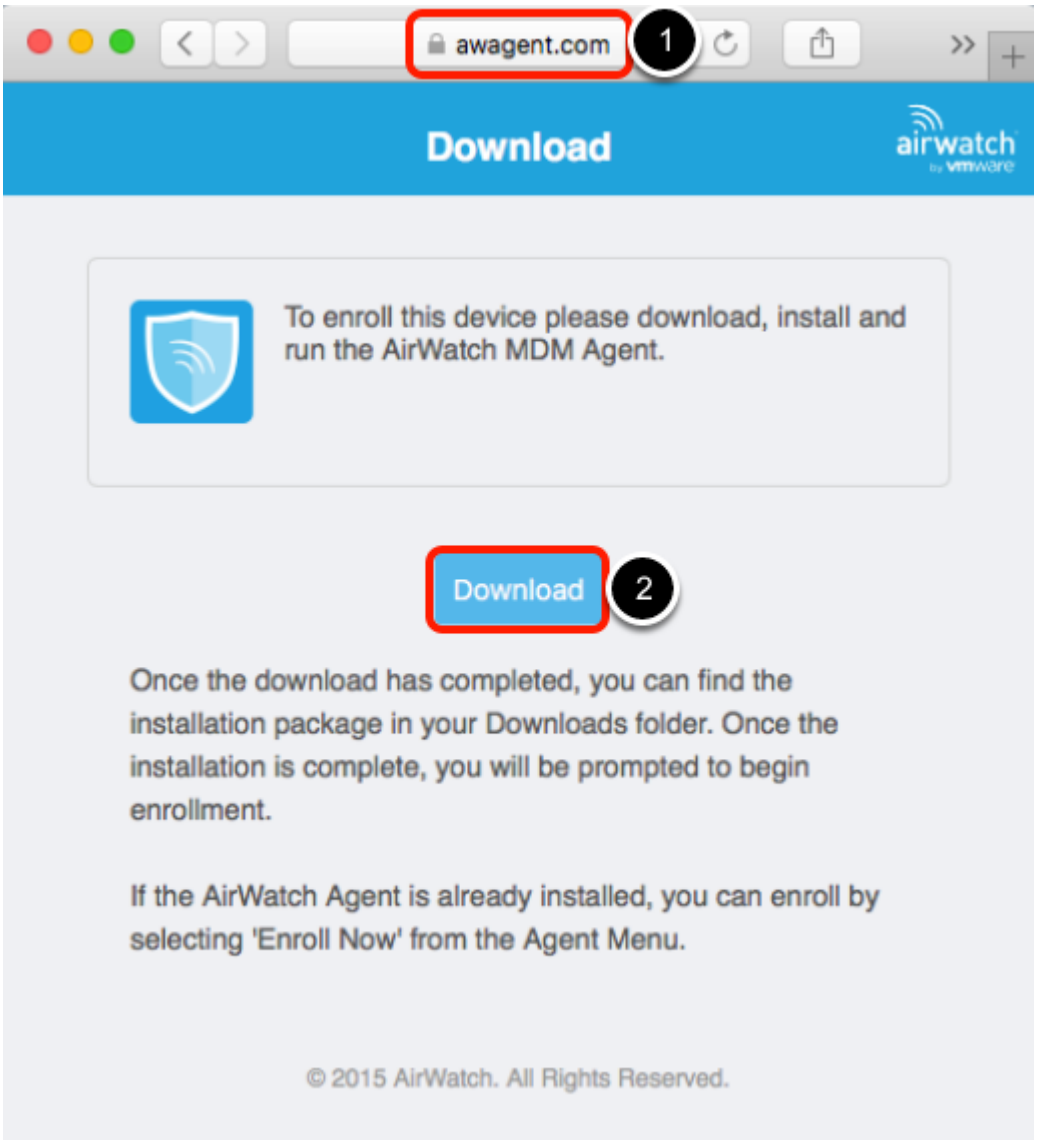


If you are prompted to login to the Mac, enter the username **"administrator"** and the password **"VMware1!"**.

Open the Safari Browser on the MacBook

Click on the Safari icon (blue compass) to open the Safari browser

Download the AirWatch Agent

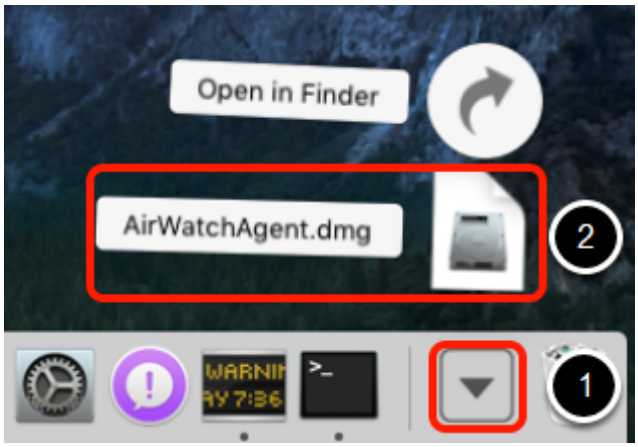


1. Type "**https://awagent.com**" in the URL field and hit enter.
2. Click on the button **Download** to download the MDM Agent. The download will be saved to your downloads folder by default.

Install the AirWatch Agent

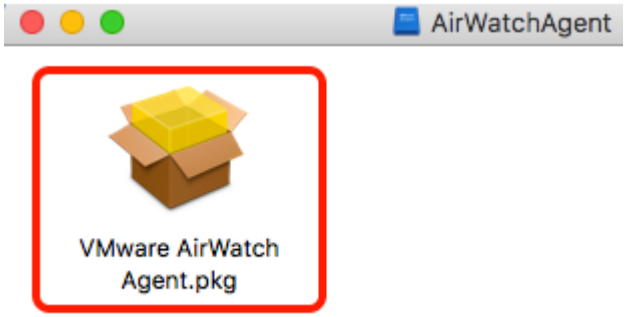
In these steps you'll install the AirWatch Agent on the macOS device so that you can later begin the Enrollment process.

Launch the AirWatch Agent Installer



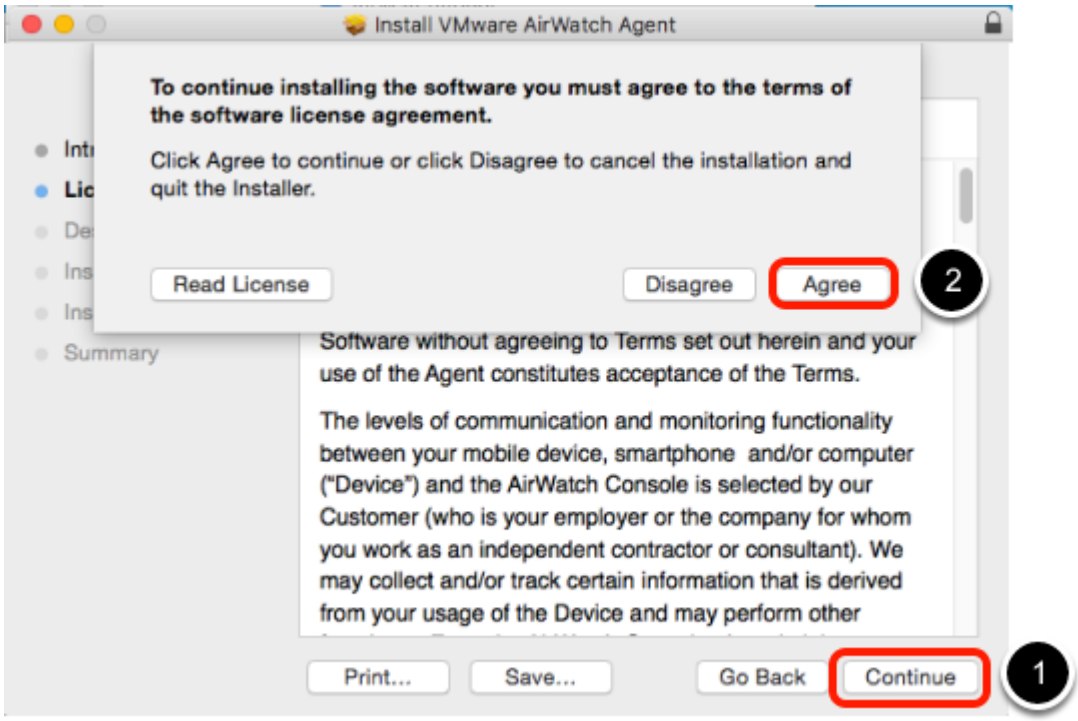
1. Click on the **Downloads** folder in the dock (next to the Trash Bin).
2. Click the **AirWatchAgent.dmg** file to begin the installer.

Launch the AirWatch Agent Installer Package



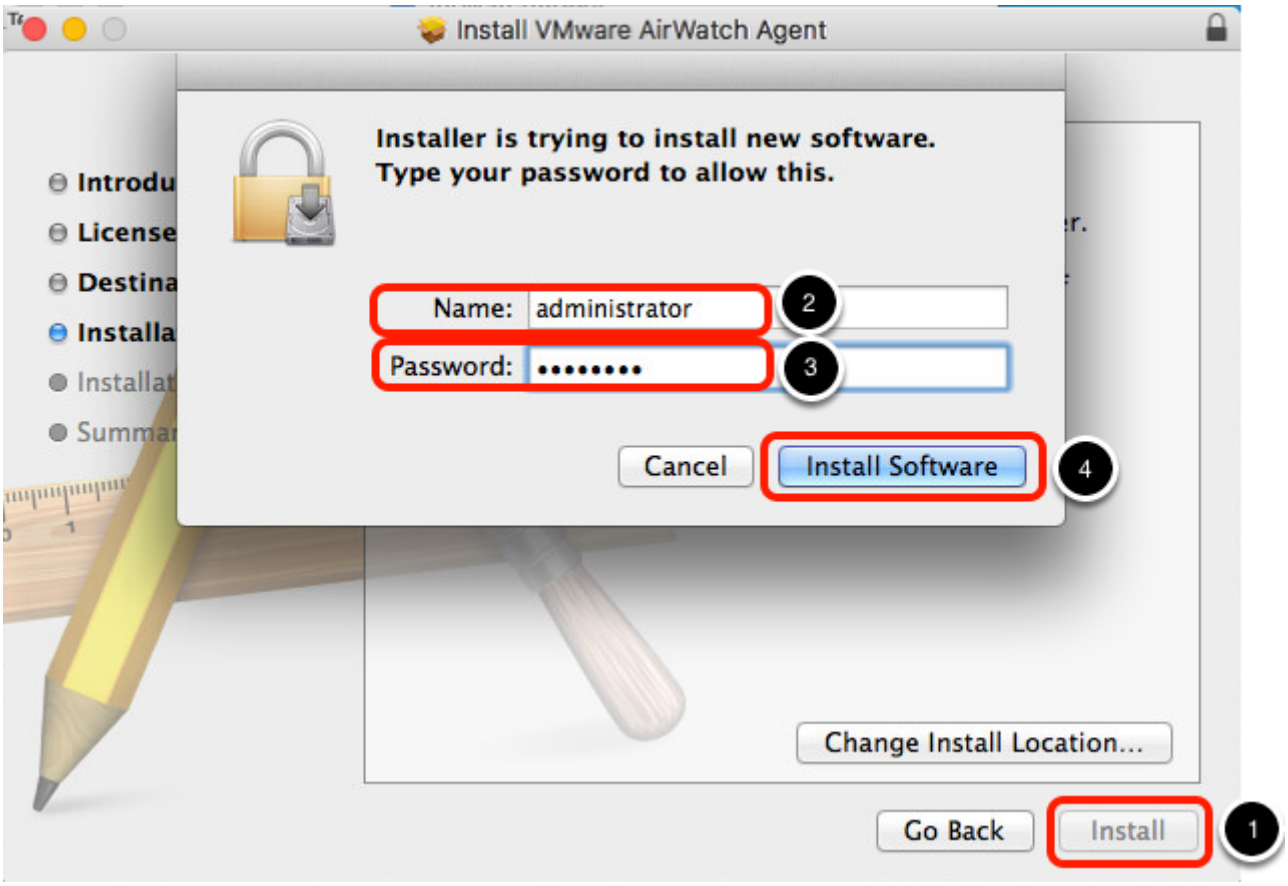
Double-click the **VMware AirWatch Agent.pkg** file to start the install.

Continue and Agree to Terms



1. In the Installer, click **Continue > Continue**
2. Click **Agree** (to the license terms)

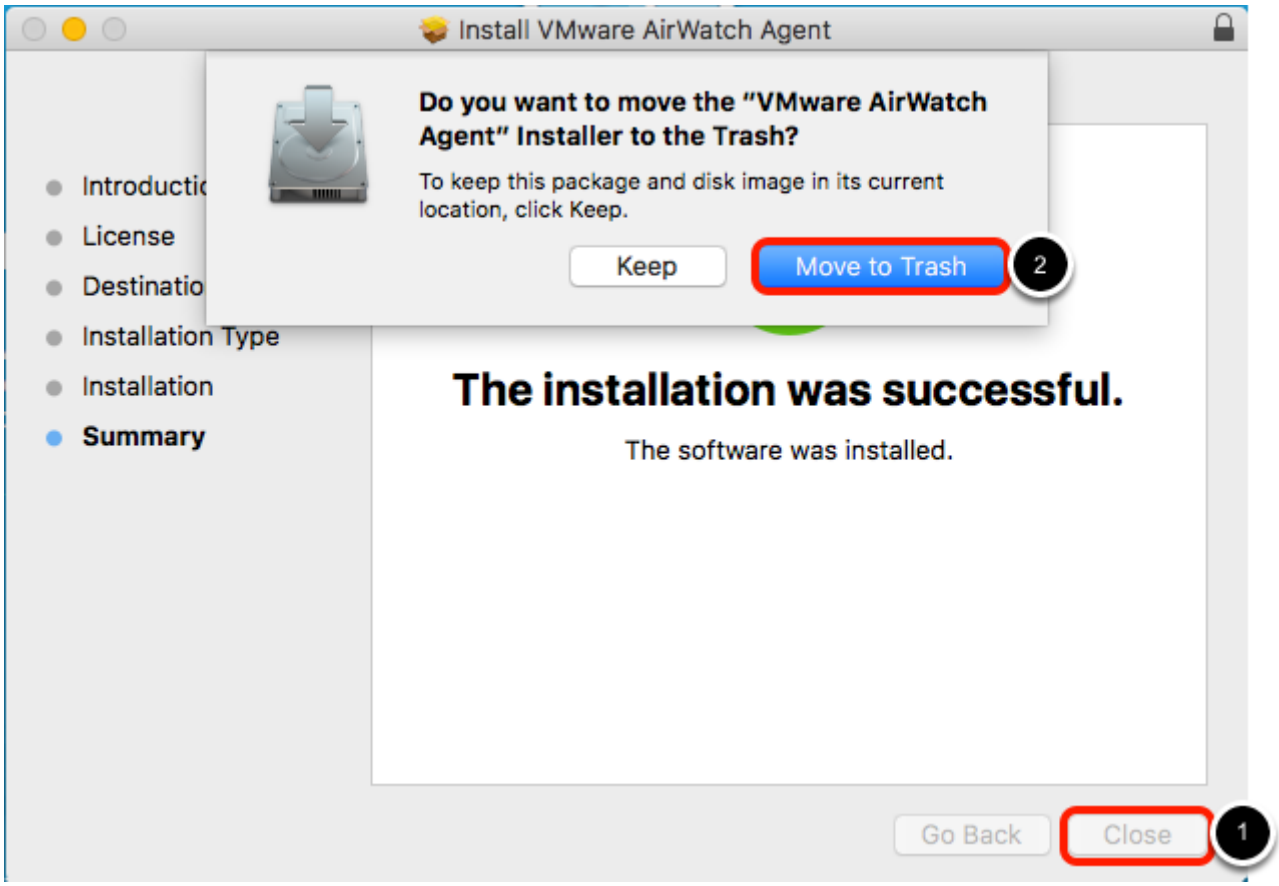
Provide Credentials for the Installer



1. Click **Install**.

   You will now be prompted to enter the computers administrator credentials.
2. Enter "**administrator**" in the Name field.
3. Enter "**VMware1!**" in the Password field.
4. Click the **Install Software** button.

Close and Move to Trash

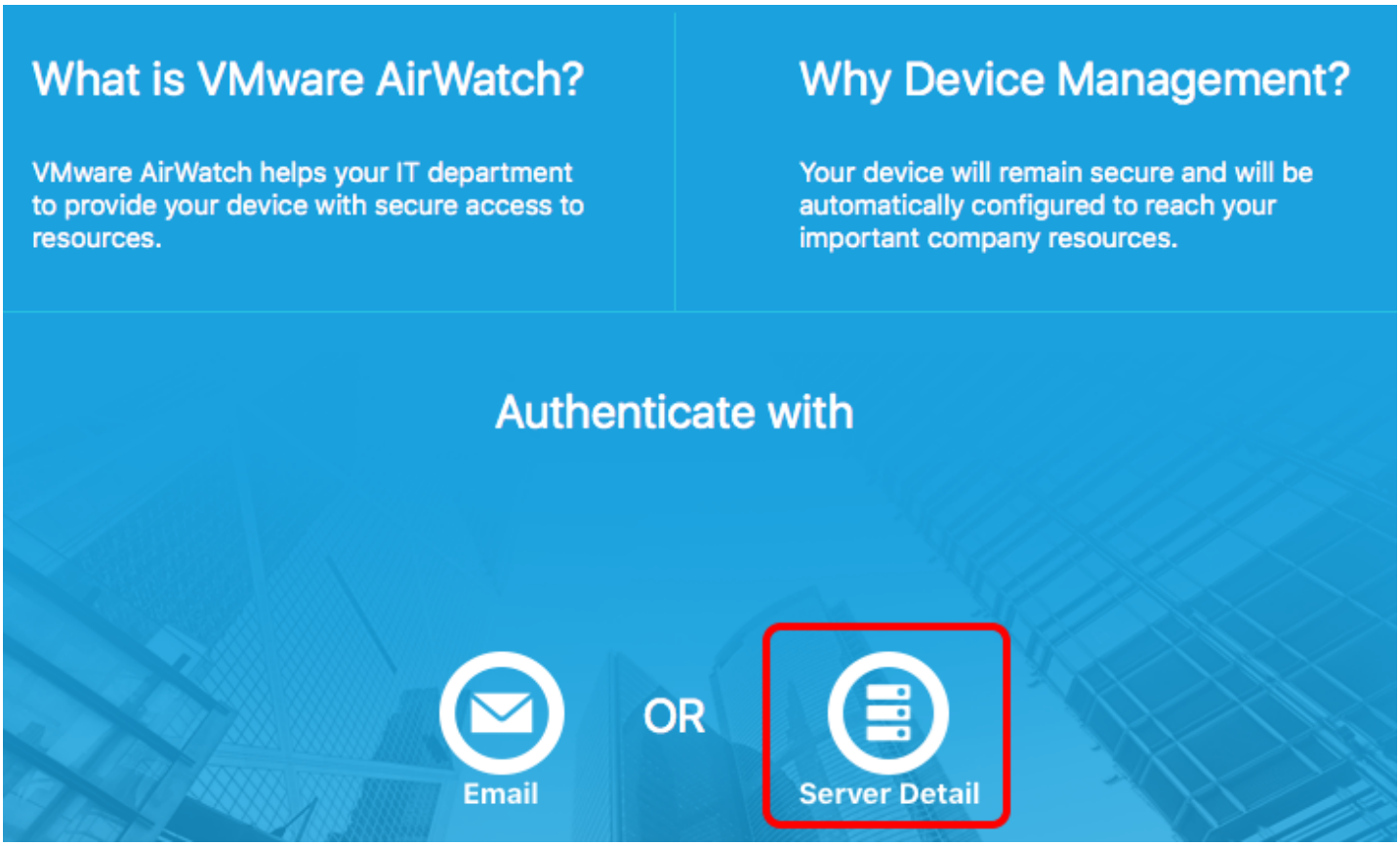


1. Click **Close** when the installer finishes.
2. Click **Move to Trash** to move the installer to the trash.

Enroll the macOS Device

In these next steps you'll enroll the macOS device, bringing it under control and management by AirWatch.

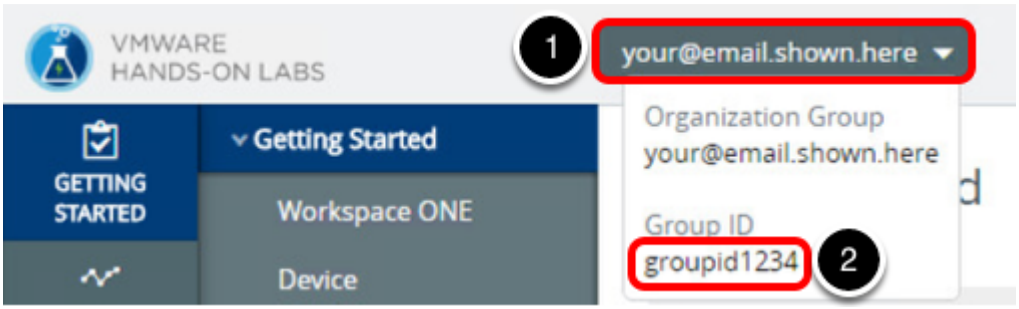
Begin macOS Enrollment Process



The Enrollment Wizard should start automatically. From within the Enrollment wizard window, click **Server Detail**.

NOTE - The Enrollment Wizard may take several minutes to launch. If you do not see the Enrollment Wizard immediately, please be patient and wait for it to appear.

Find your Group ID from AirWatch Console

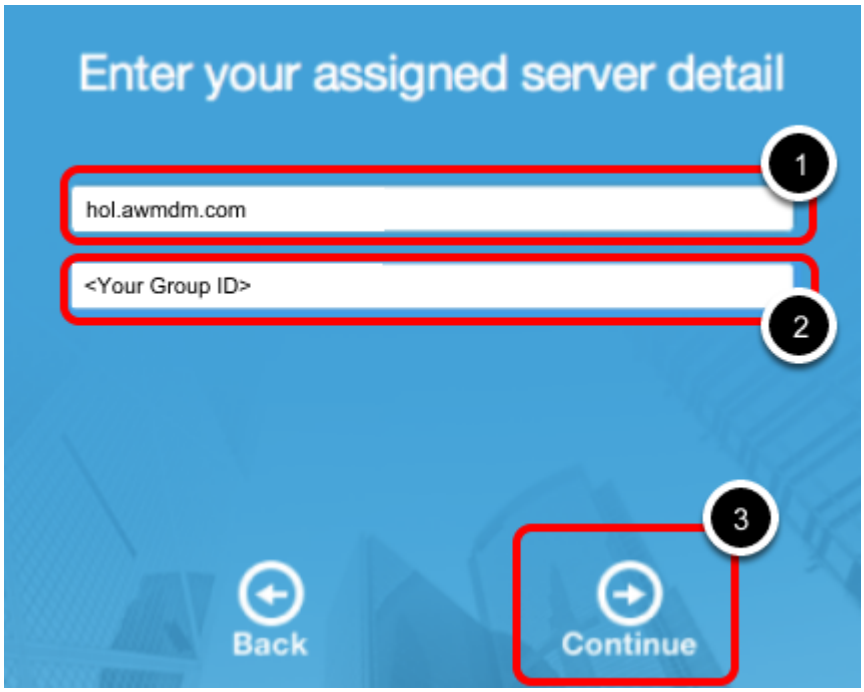


1. To find the Group ID, hover your mouse over the Organization Group tab at the top of the screen. Look for the email address you used to log in to the lab portal.

2. Your **Group ID** is displayed at the bottom of the Organization Group pop up.

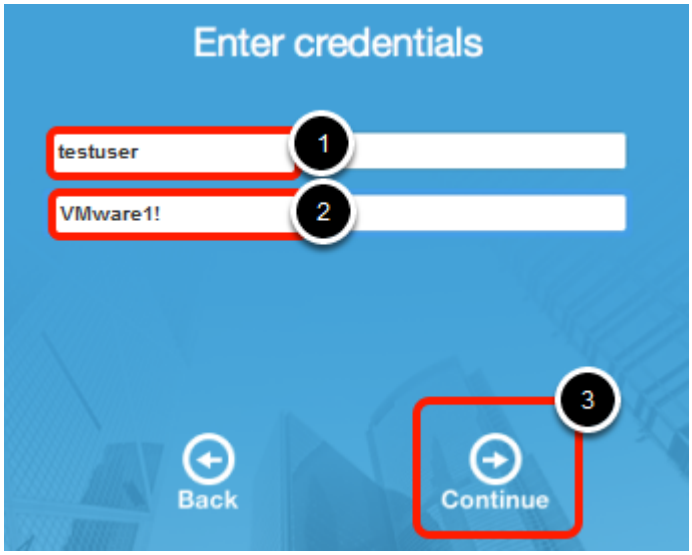
NOTE - The Group ID is required when enrolling your device in the following steps.

Enter Enrollment Server Details



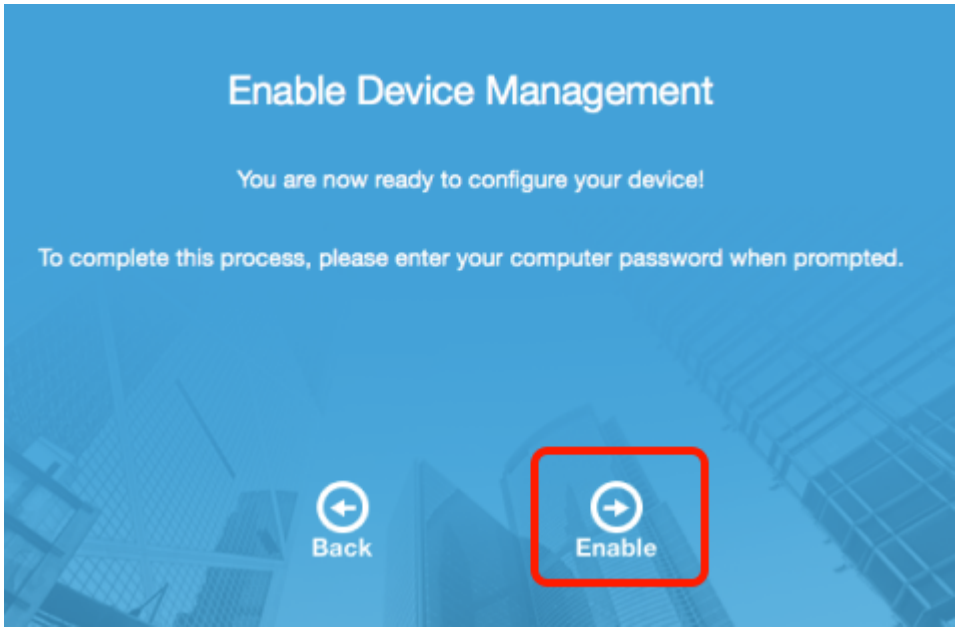
1. Enter your Hands-On Lab URL "**hol.awmdm.com**".
2. Enter your Group ID. This was described in the **"Finding your Group ID"** section.
3. Click on the **Continue** button.

Enter Enrollment Credentials



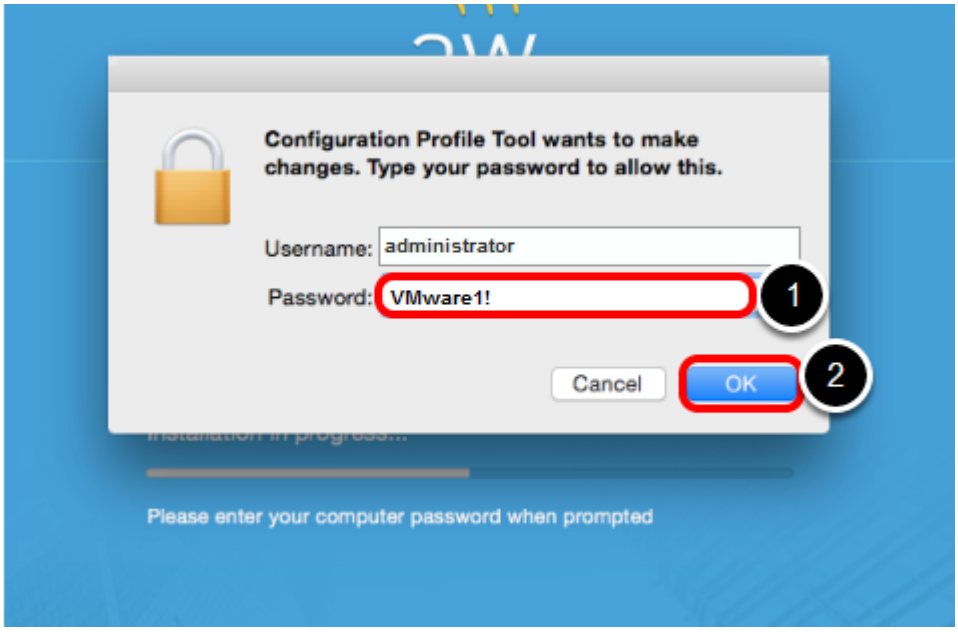
1. Enter the staging enrollment username "**testuser**" in username field.
2. Enter the enrollment user password "**VMware1!**" in the password field.
3. Click on the **Continue** button.

Enable Device Management



Click **Enable** to enable device management.

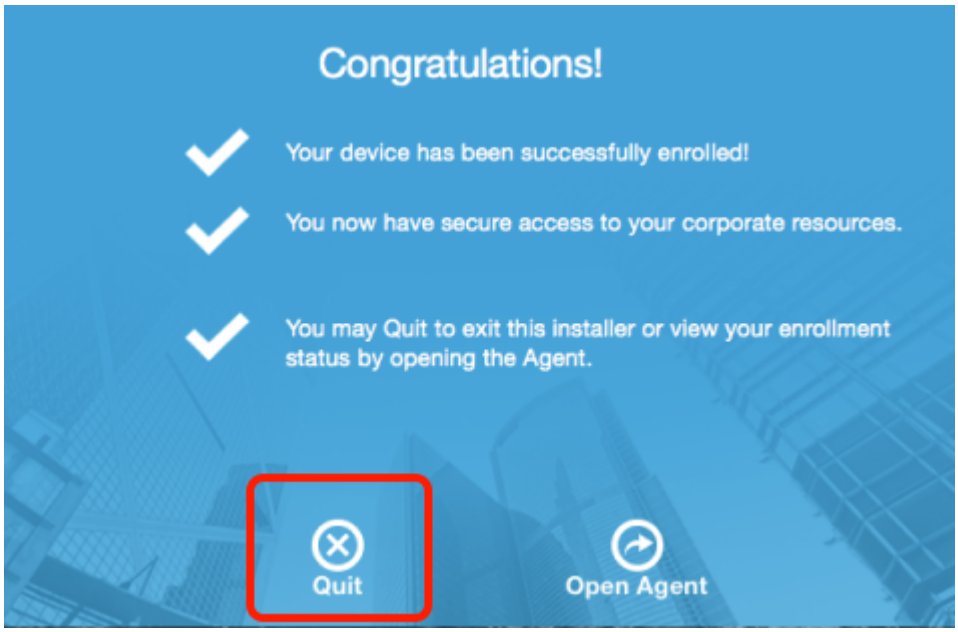
Enter Administrative Credentials for Profile Install



1. When prompted, enter the password "**VMware1!**" for your user account on the Mac.

2. Click on the **OK** button.

Quit the Enrollment Wizard



Click **Quit** when the installation completes.

Enable Location Services

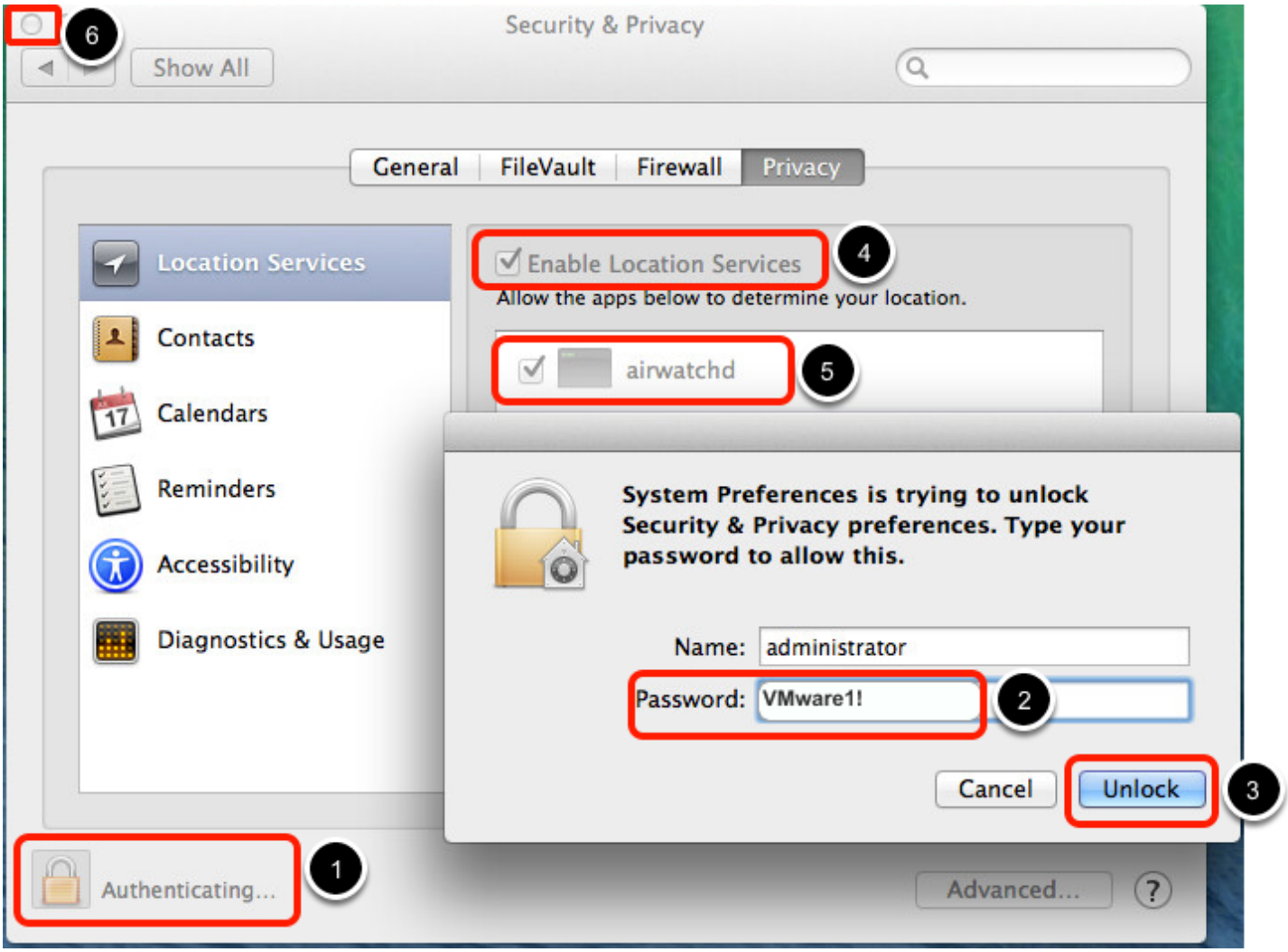
In these next few steps we'll enable location services on macOS so that the device can report its location to AirWatch.

Open Location Services

If the location services are not already enabled (under System Preferences > Security & Privacy), the AirWatch Agent should prompt you to enable them.

Click **OK** to allow the AirWatch Agent to display the Settings pane for Location Services

Enable Location Services

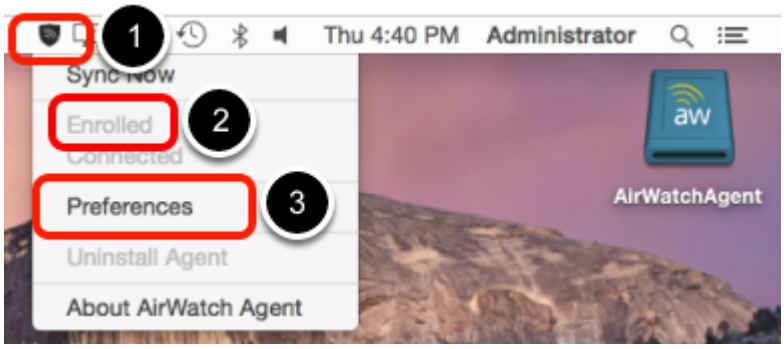


1. Click the lock to Unlock the preference pane.
2. Enter the password for the administrator account **"VMware1!"**
3. Click **Unlock.**
4. Check the box for **Enable Location Services.**
5. Check the box for **airwatchd** to grant the AirWatch Agent access to Location Services.
6. Click the red Close button.

Validate Mac Enrollment

Follow the next steps to see how to verify that the Mac has been successfully enrolled.

Validate Mac Enrollment



In top right corner,

1. Note the shield icon in the menu bar. Click the icon.
2. Note the menu shows your device as **Enrolled**.
3. Click **Preferences** and review the options available to you in the agent.

Key Takeaways

- Agent-based macOS enrollment is streamlined and intuitive.
- AirWatch supports a number of enrollment methods for macOS devices: web-based, agent-based, staged (pre-installed agent), enrollment on-behalf, and enrollment via the Apple Device Enrollment Program.
- Agent logs can be collected directly from the AirWatch Agent. This eases helpdesk troubleshooting by allowing end-user to quickly send diagnostic information to helpdesk and/or administrative users.

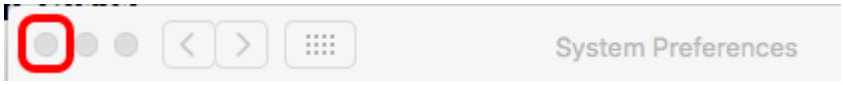
macOS Device and Application Management (MDM and MAM)

This chapter will explore the basics of modifying the macOS device behavior by using Profiles and how to easily distribute applications.

Configure macOS Profiles

Profiles are the mechanism by which AirWatch manages settings on a macOS device. macOS profile management is done in two ways: device level and enrollment-user level. You can set appropriate restrictions and apply appropriate settings regardless of the logged-on user. You can also apply settings specific to the logged-on user on the device.

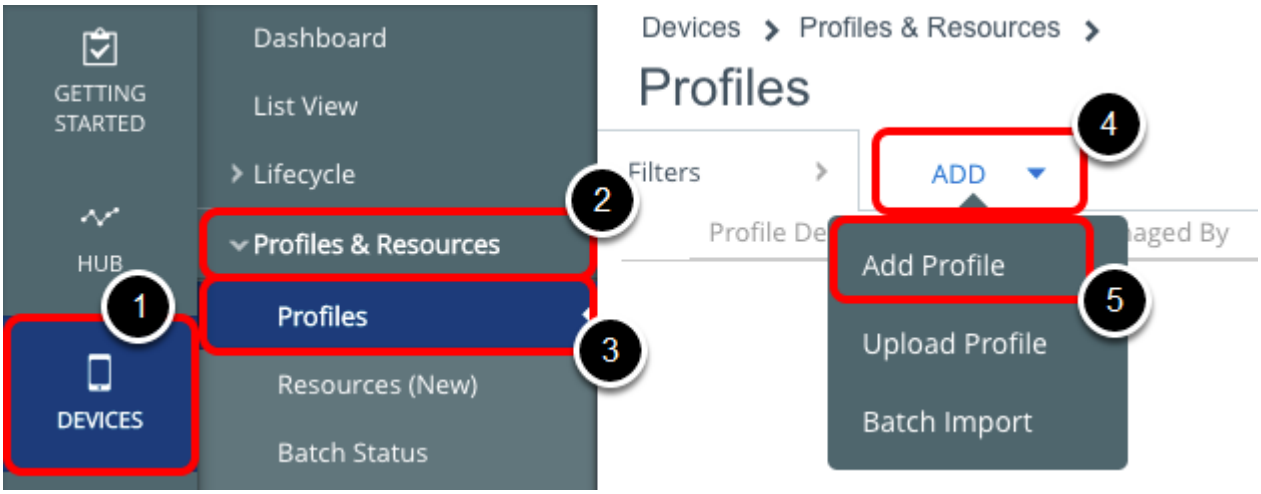
Close System Preferences if opened



In the following section, we are going to create a device profile which will change some system preferences in your Mac. However, in order to see those changes take place, please close any existing System Preference sessions if they are already open.

If System Preferences are opened, click on **X** to close.

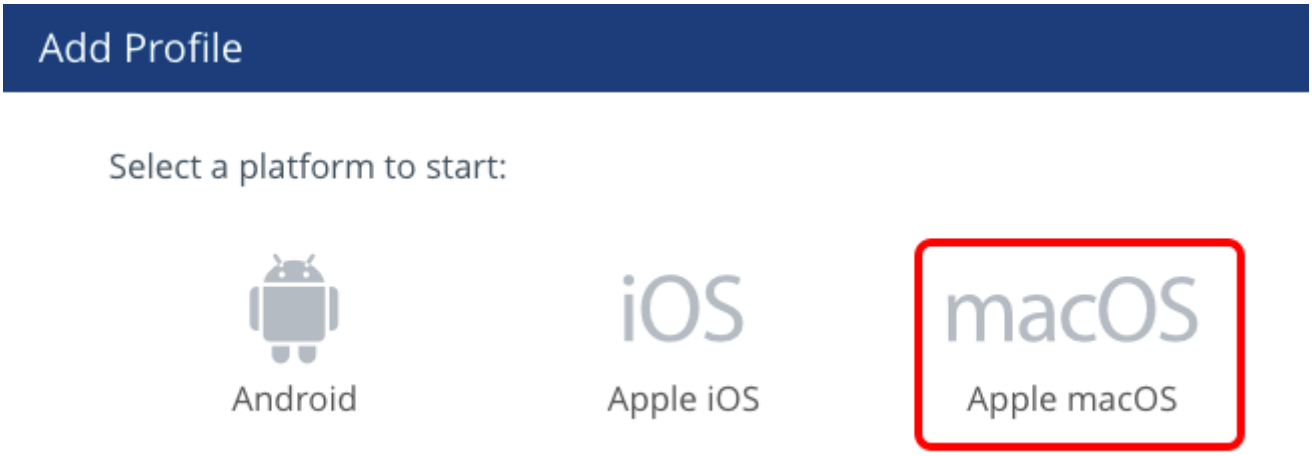
Add a macOS Device Profile



In the AirWatch console,

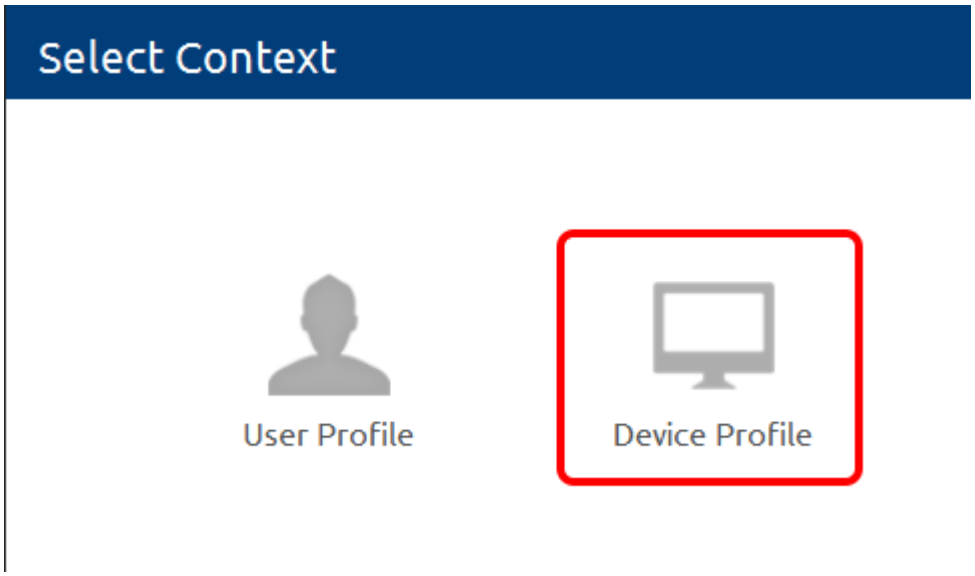
1. Click on **Devices.**
2. Click on **Profiles & Resources.**
3. Click on **Profiles.**
4. Click on **Add**
5. Click **Add Profile**.

Select Profile Platform



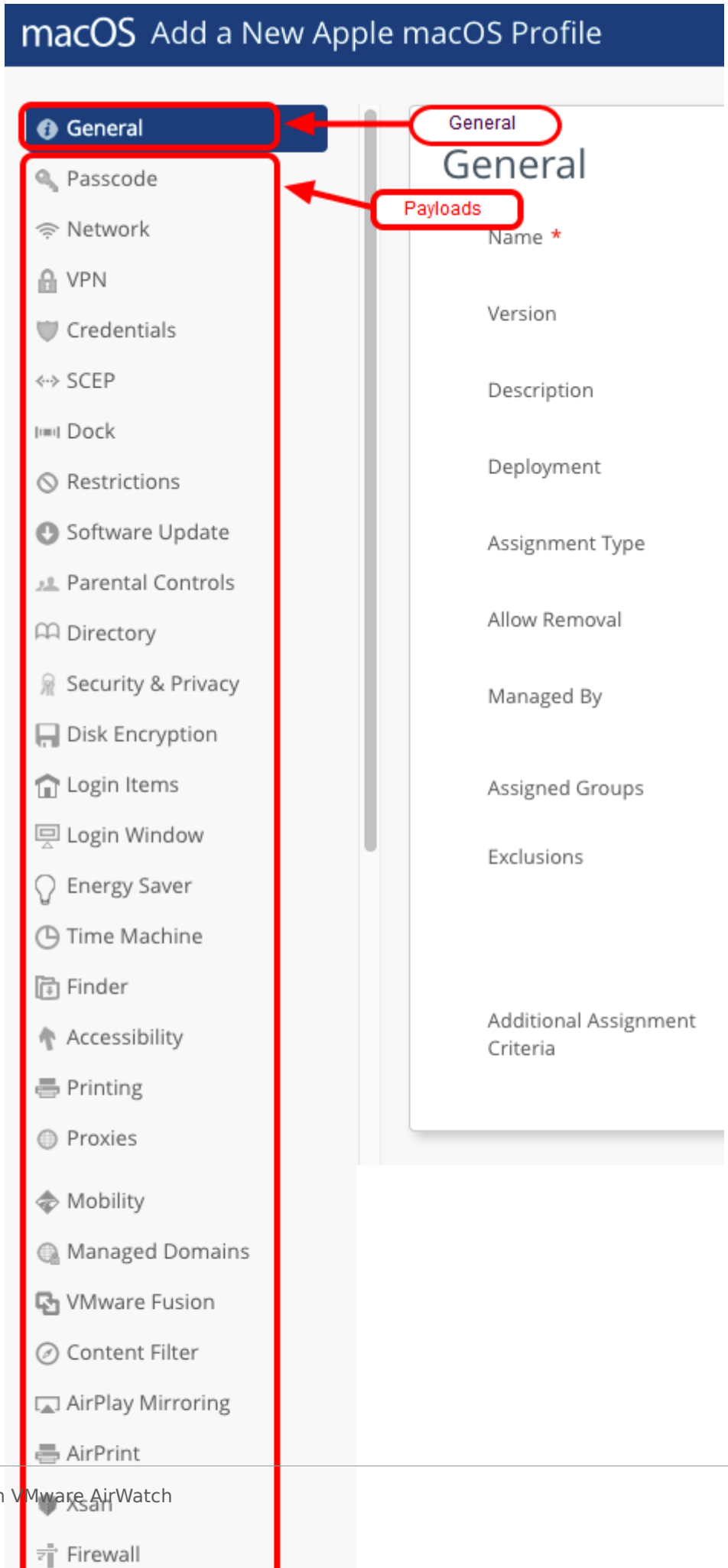
Click on the **macOS** icon.

Select the Profile Context



Click on the **Device Profile** icon.

macOS Profiles


macOS Add a New Apple macOS Profile
General
Passcode
Network
VPN
Credentials
SCEP
Dock
Restrictions
Software Update
Parental Controls
Directory
Security & Privacy
Disk Encryption
Login Items
Login Window
Energy Saver
Time Machine
Finder
Accessibility
Printing
Proxies
Mobility
Managed Domains
VMware Fusion
Content Filter
AirPlay Mirroring
AirPrint
Xsan
Firewall
General
Payloads
General
Name *
Version
Description
Deployment
Assignment Type
Allow Removal
Managed By
Assigned Groups
Exclusions
Additional Assignment Criteria

After clicking on the macOS icon, you will be presented with the **Add a New Apple macOS Profile**. All profiles are broken down into two basic sections, the **General** section and the **Payload** section.

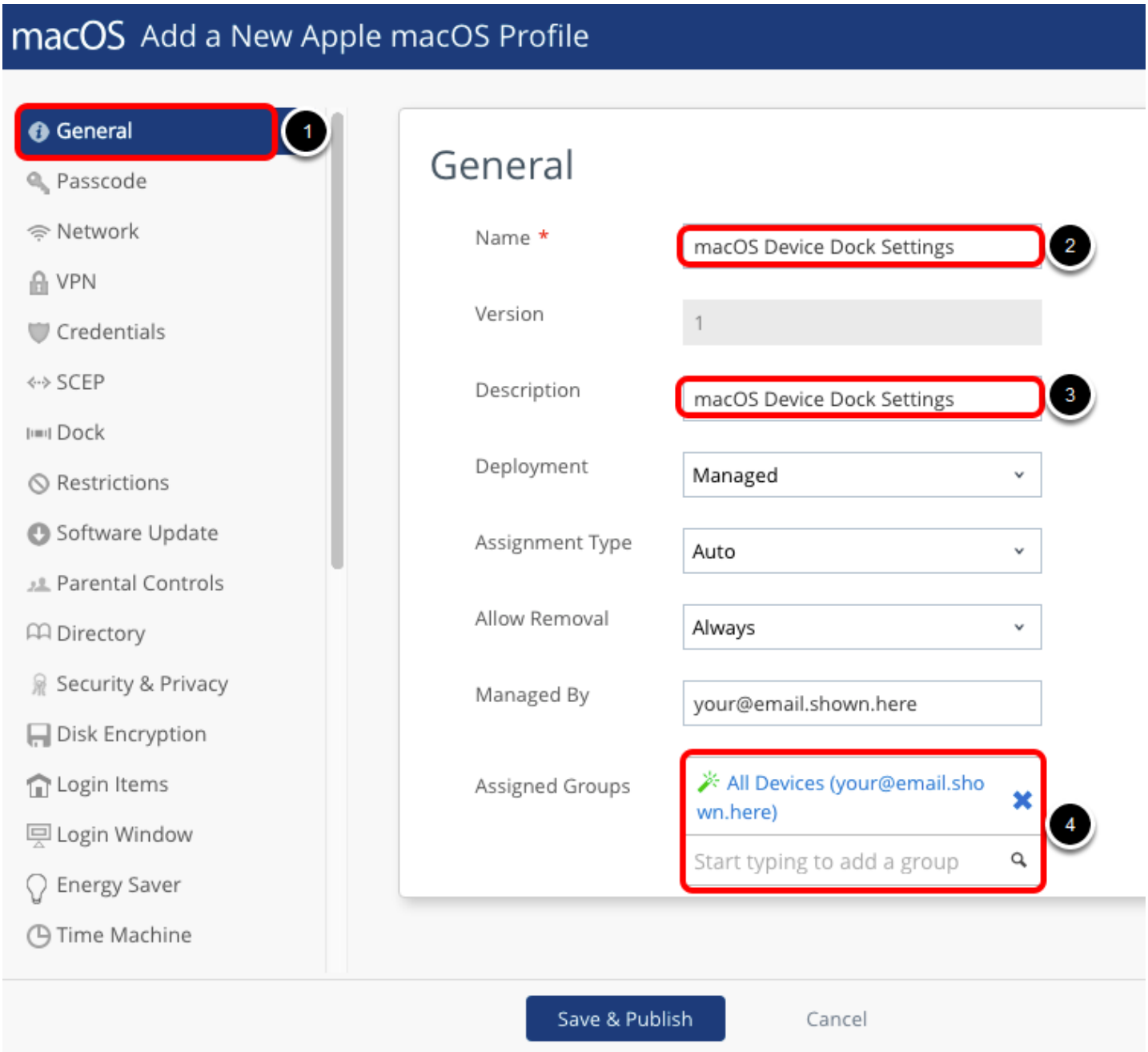
The **General** section has information about the Profile, its name and some filters on what device will get it.

The **Payload** sections define actions to be taken on the device.

Every Profile must have all *required* fields in the General section properly filled out and at least one payload configured.

NOTE - It is recommended a Profile contain only one payload.

Profile General Settings



Device Profiles are typically used to control settings that apply system-wide. Device profiles can include items such as VPN and Wifi configurations, Global HTTP Proxy, Disk Encryption, and/or Directory (LDAP) integration. In this case, we create a profile that modifies the dock for all users on the machine.

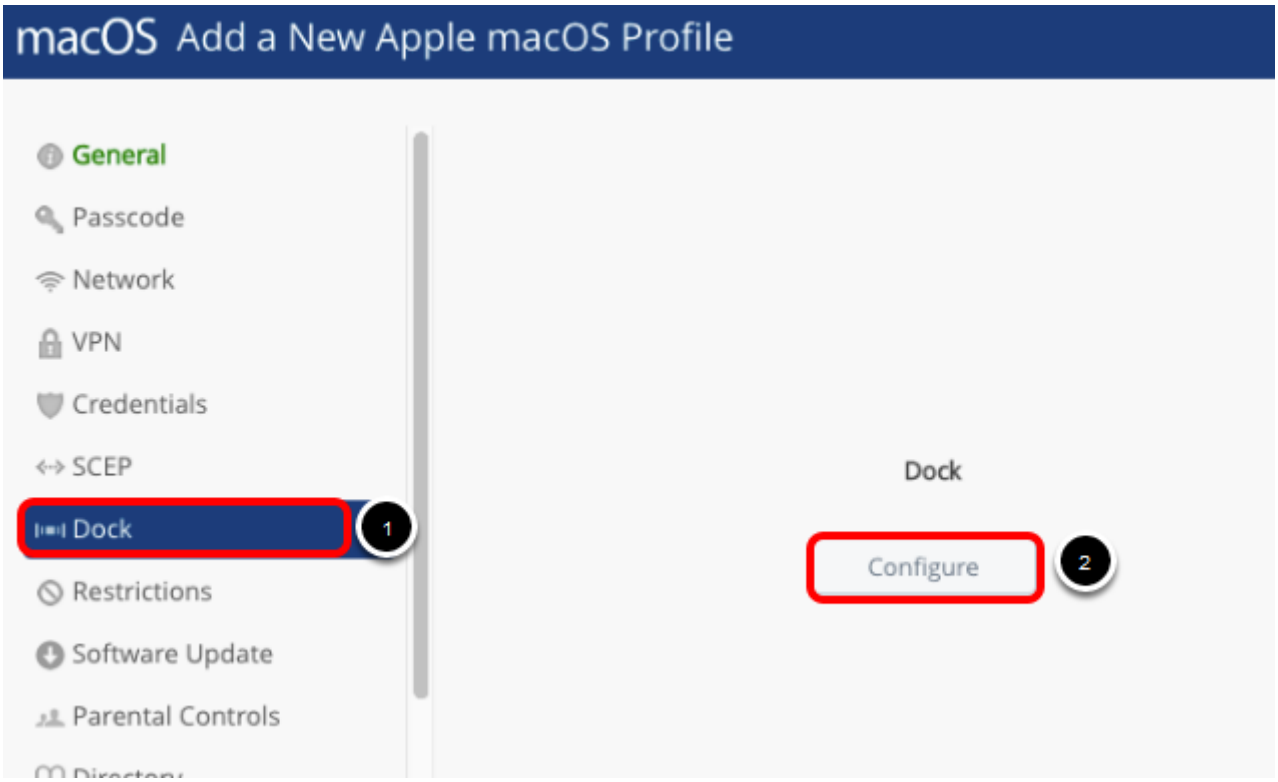
Configure the profile as follows:

1. Click on **General** if it is not already selected.
2. Give the profile a name such as **macOS** Device Dock Settings by entering the string in the Name field.

3. Copy the profile name in the the **Description** field.
4. Click in the **Assigned Groups** field. This will pop-up the list of created Assignment Groups. Start Typing All Devices and select the **All Devices (your@email.shown.here)** Assignment Group.
   NOTE - You may need to scroll down to view the Assigned Groups field.

NOTE - You do not need to click SAVE or SAVE AND PUBLISH at this point. This interface allows you to move around to different payload configuration screens before saving.

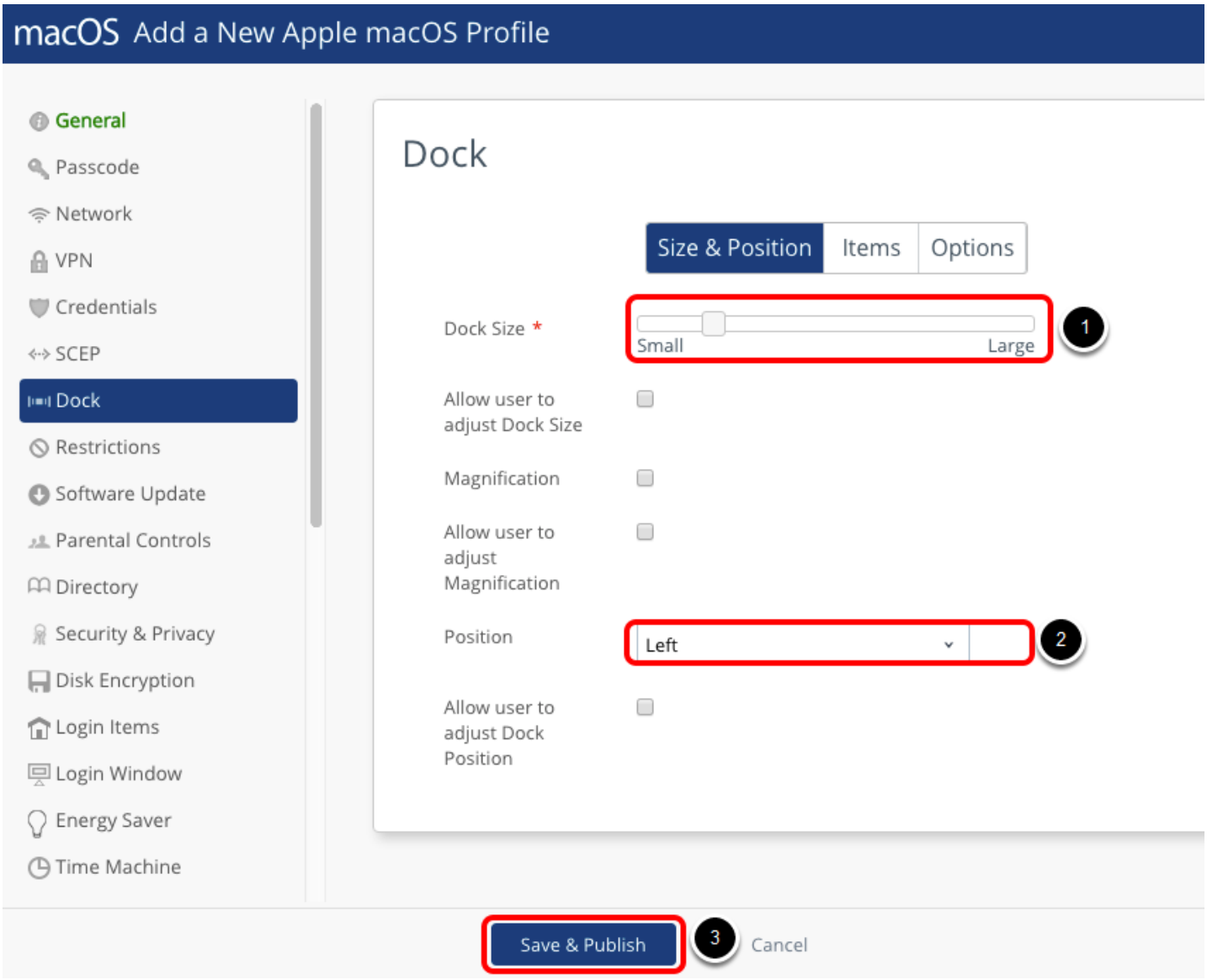
Select the Dock Payload



NOTE - When initially setting most payloads a Configure button will show to reduce the risk of accidentally setting a payload configuration.

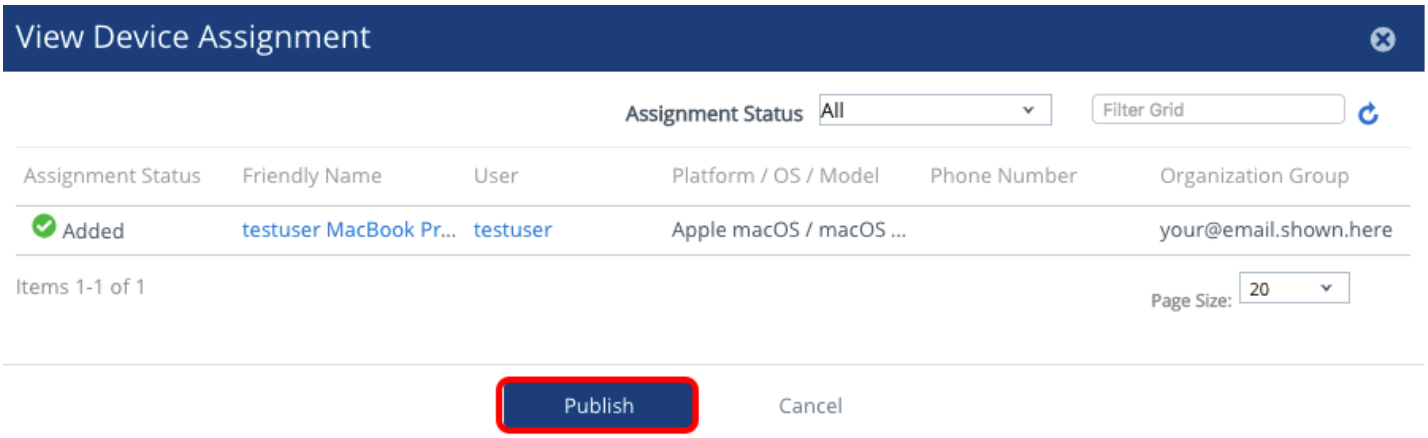
1. Click on **Dock.**
2. Click the **Configure** button.

Configure the Dock Payload



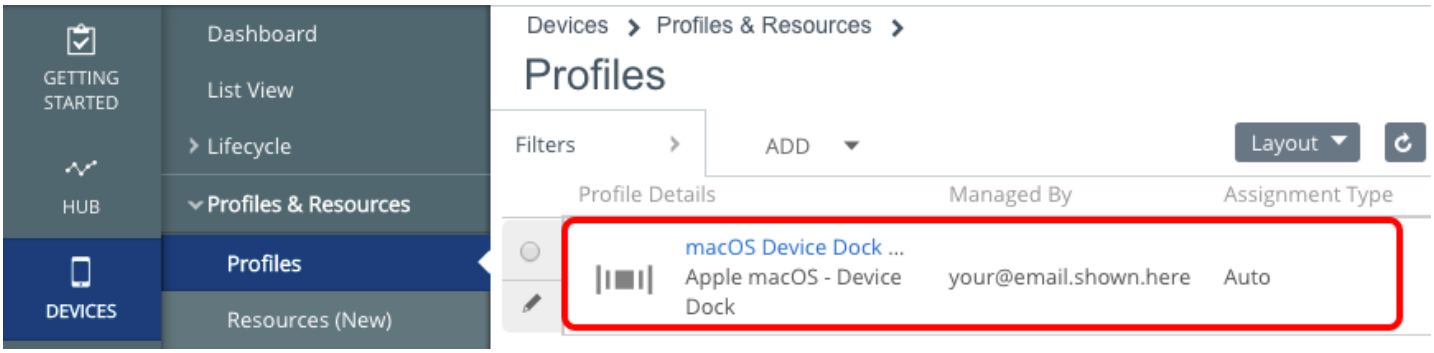
1. Reduce the dock size.
2. Change the position to **Left**.
3. Click **Save & Publish**.

Publish the Device Profile



Click on the **Publish** button.

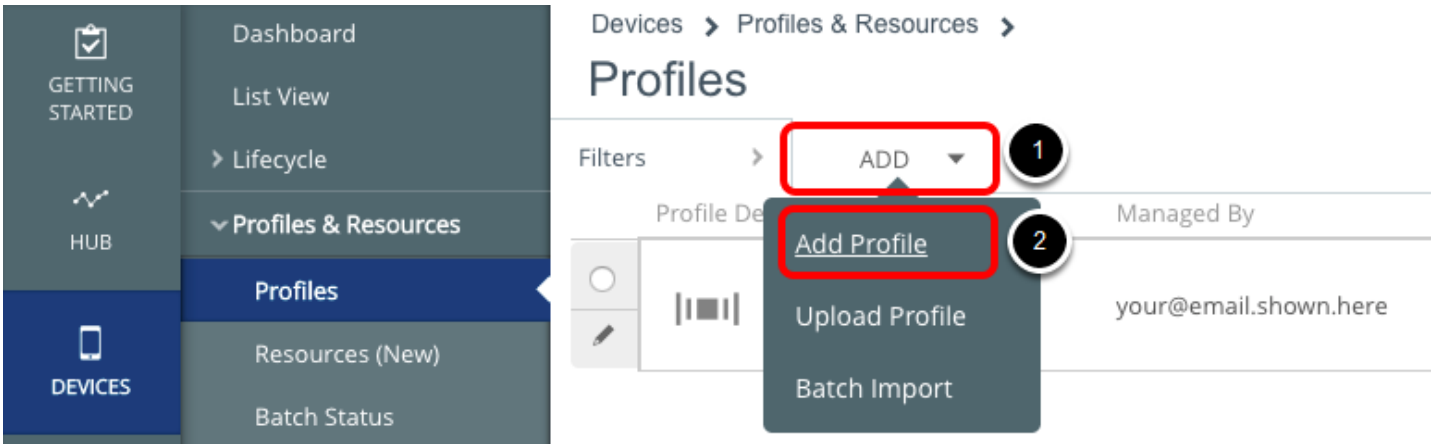
Verify the Device Profile Now Exists



You should now see your Device Profile within the list of the Profiles window.

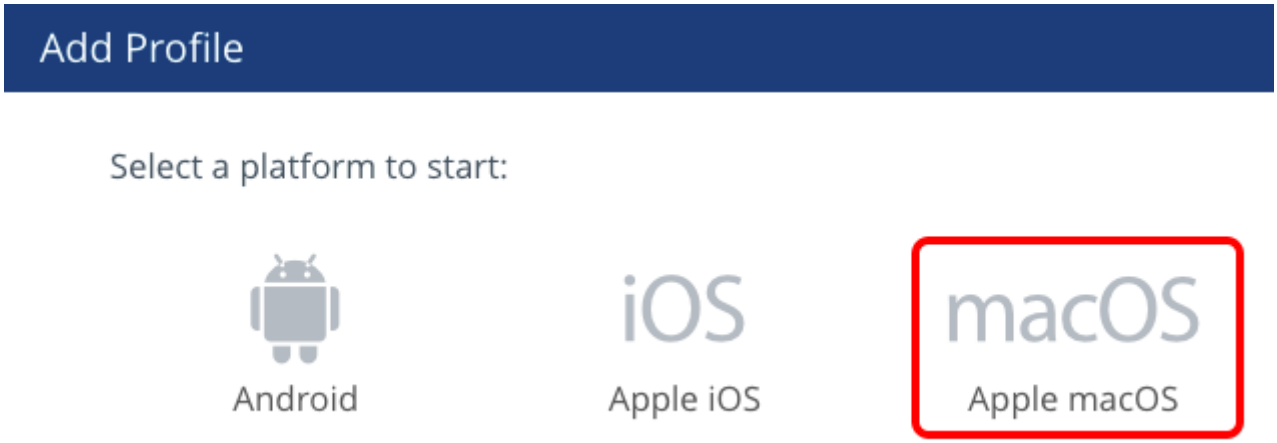
NOTE - If you need to edit the Profile, this is where you would come back to in order to do so.

Add an macOS User Profile



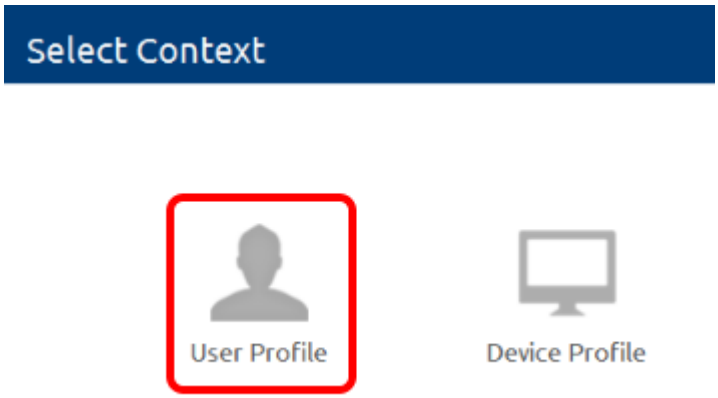
1. Click on **Add.**
2. Click on **Add Profile.**

Select Profile Platform



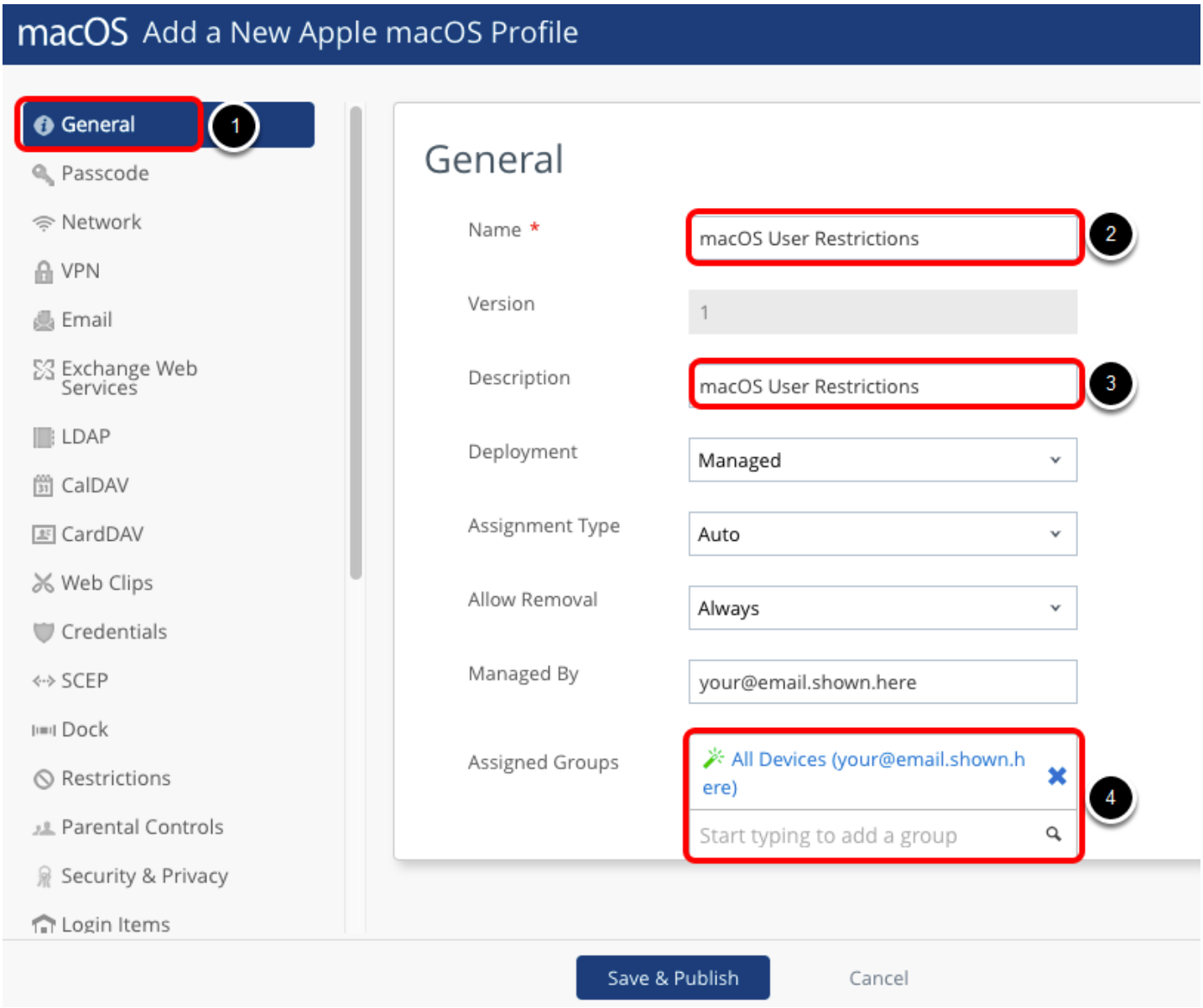
Click on the **macOS** icon.

Select the Profile Context



Click on the **User Profile** icon.

Profile General Settings



User Profiles are typically used to control settings that apply to the enrolled user. User profiles can include items such as Email configurations, web clips (URL shortcuts), credentials (certificates), and content filtering settings. In this case, we will create restrictions for system preferences panes for the enrolled user on this machine

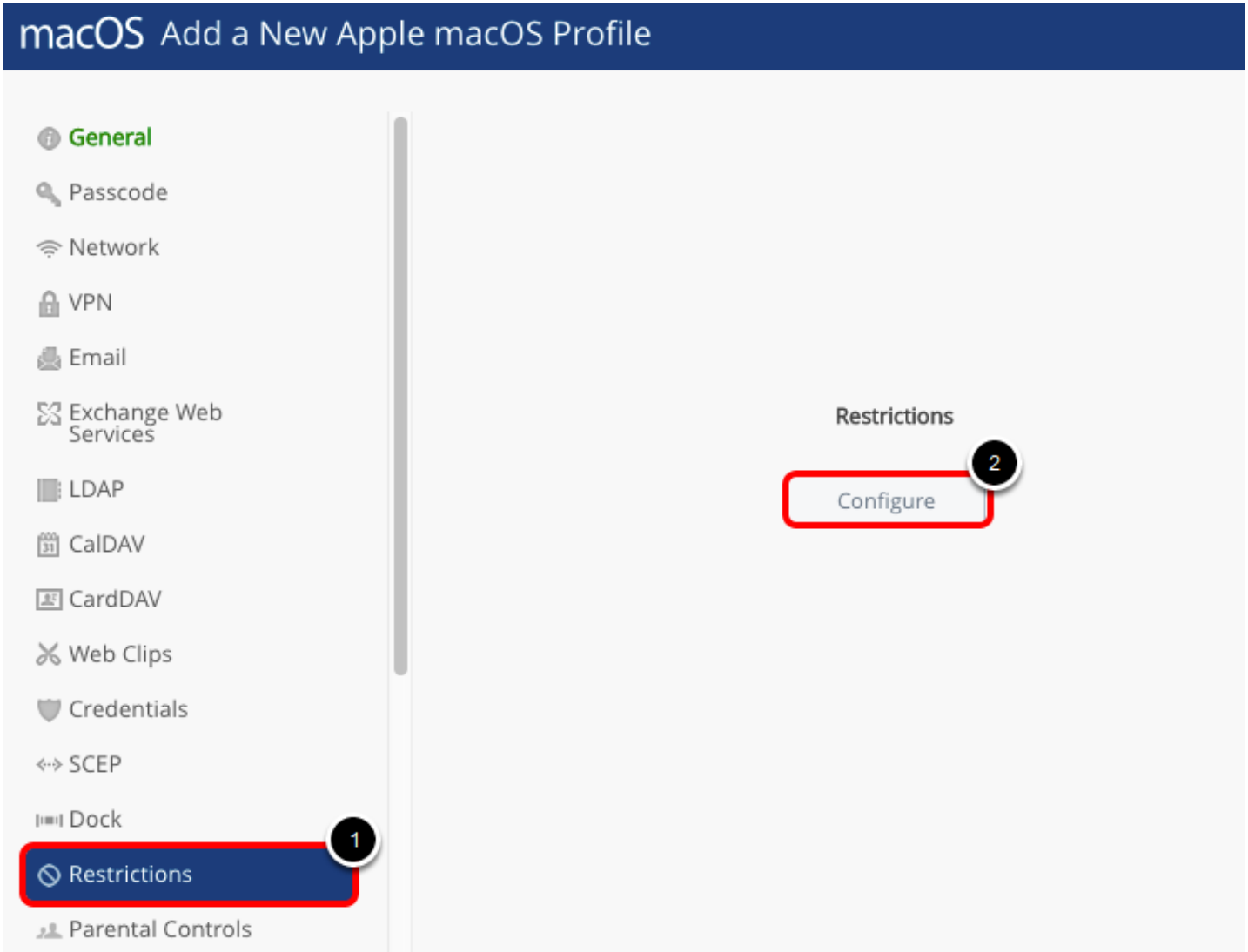
Configure the profile as follows:

1. Click on **General** if it is not already selected.
2. Give the profile a name such as **macOS** User Restrictions by entering the string in the Name field.
3. Copy the profile name in the the Description field.

4. Click in the Assigned Groups field. This will pop-up the list of created Assignment Groups. Start Typing All Devices and select the **All Devices (your@email.shown.here)** Group.

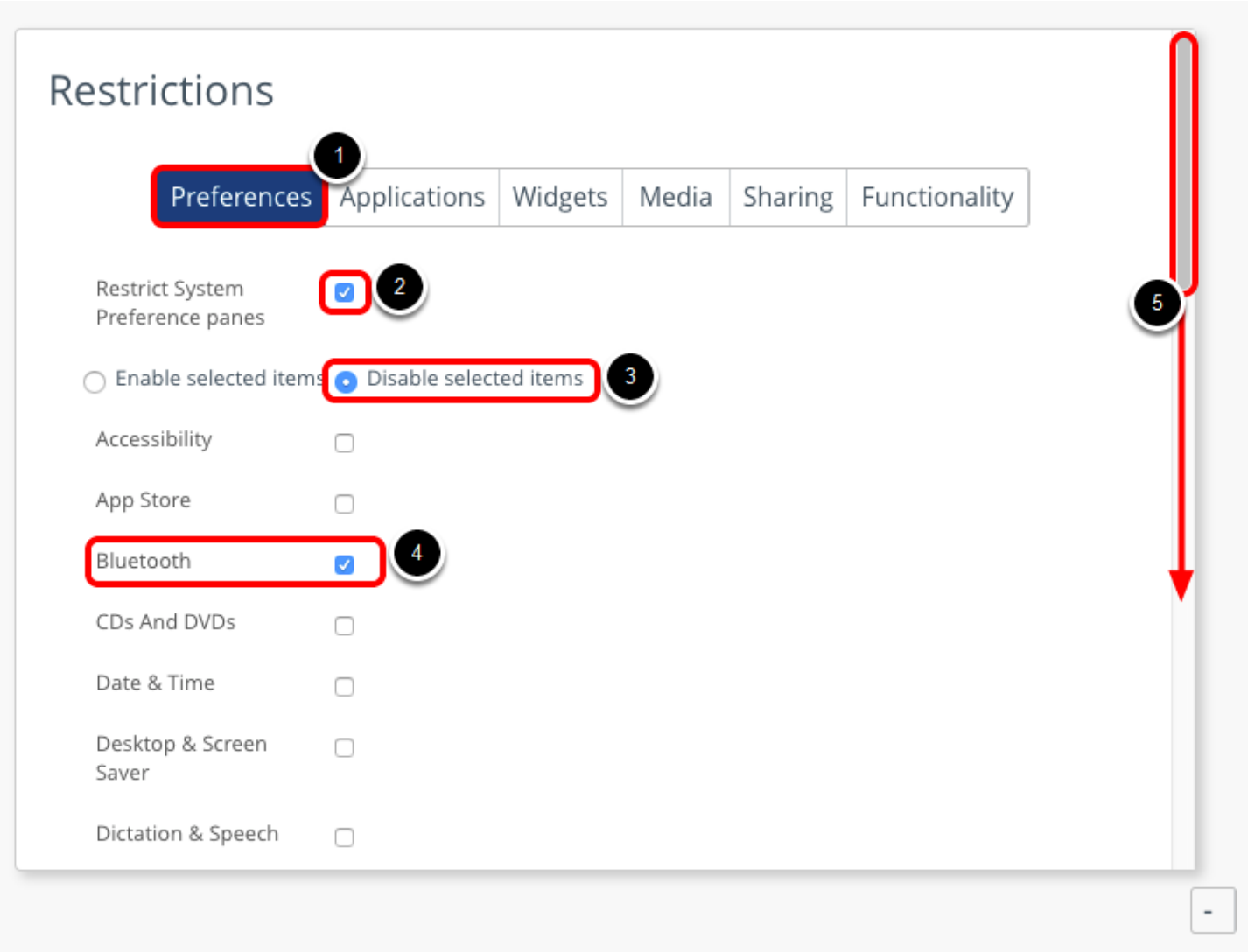
NOTE - You do not need to click SAVE or SAVE AND PUBLISH at this point. This interface allows you to move around to different payload configuration screens before saving.

Select the Restrictions Payload



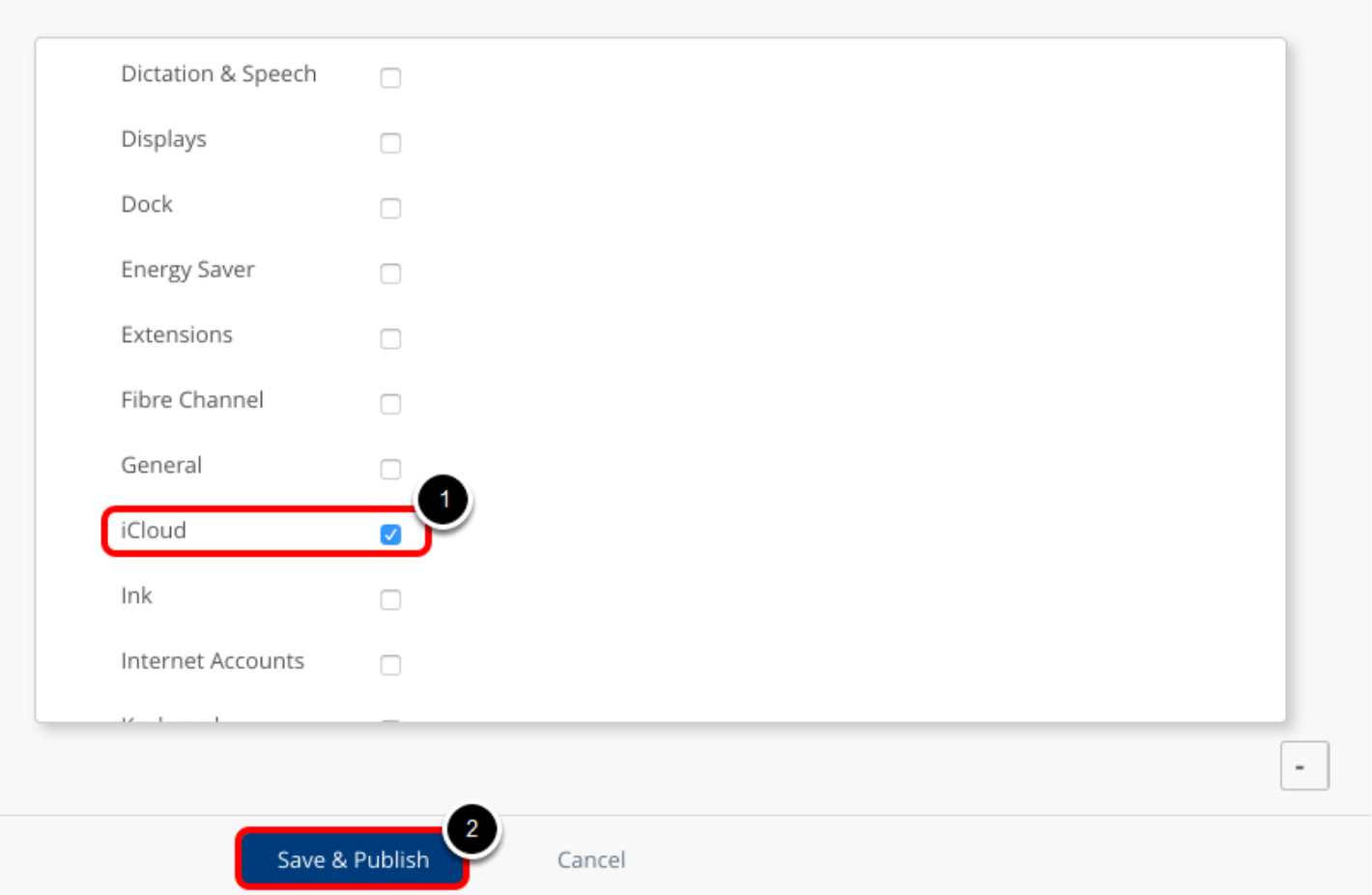
1. Click on **Restrictions**
2. Click on the **Configure** button

Configure the Restrictions Profile



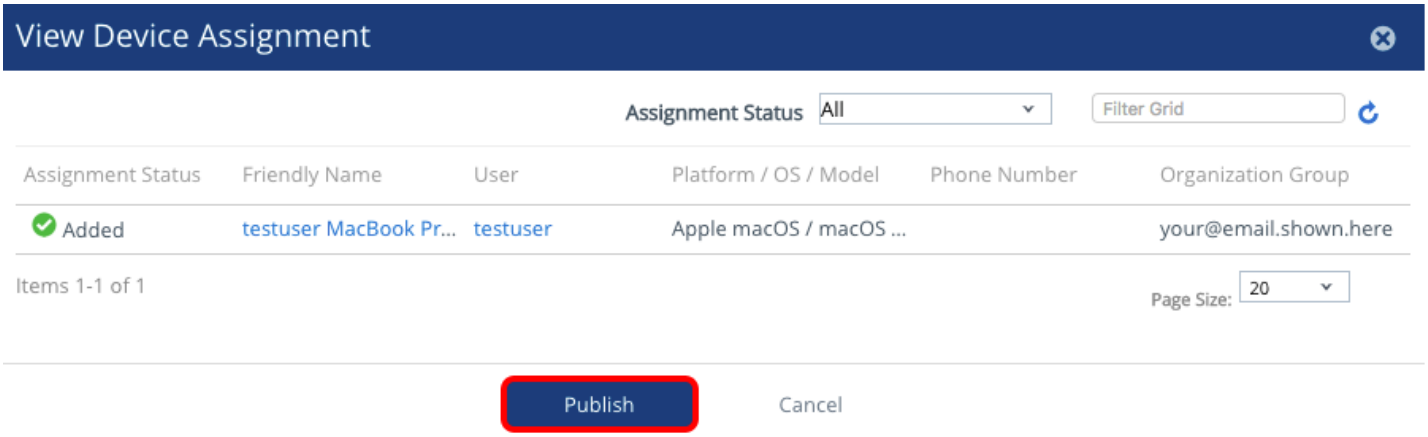
1. Click on the **Preferences** tab.
2. Select **Restrict System Preferences Panes**
3. Select **Disable selected items**
4. Select **Bluetooth**
5. Scroll the restrictions pane down to see more restrictions.

Finish Configuring the Restrictions Profile



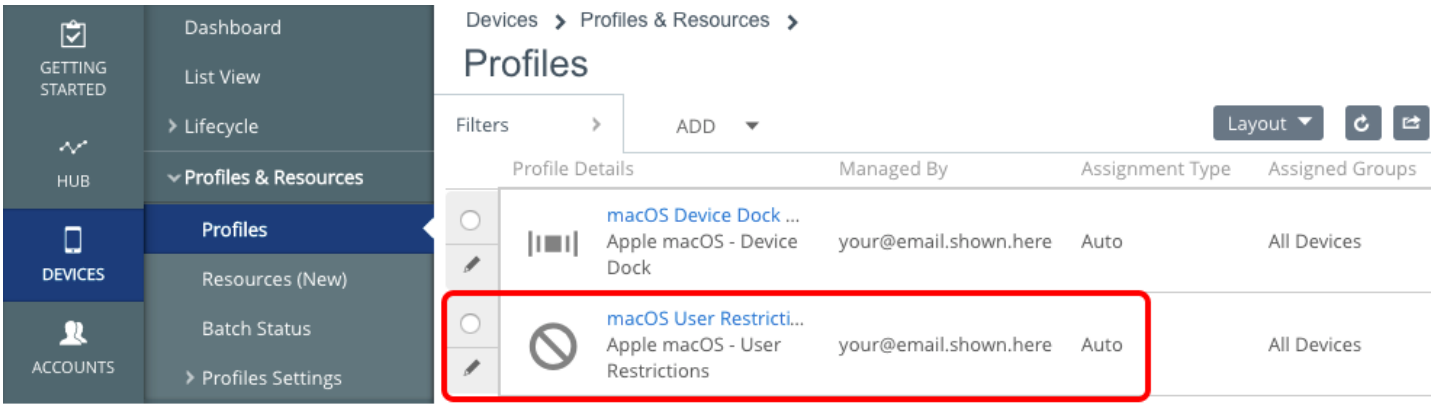
1. Select **iCloud.**
2. Click **Save & Publish.**

Publish the User Profile



Click on the **Publish** button.

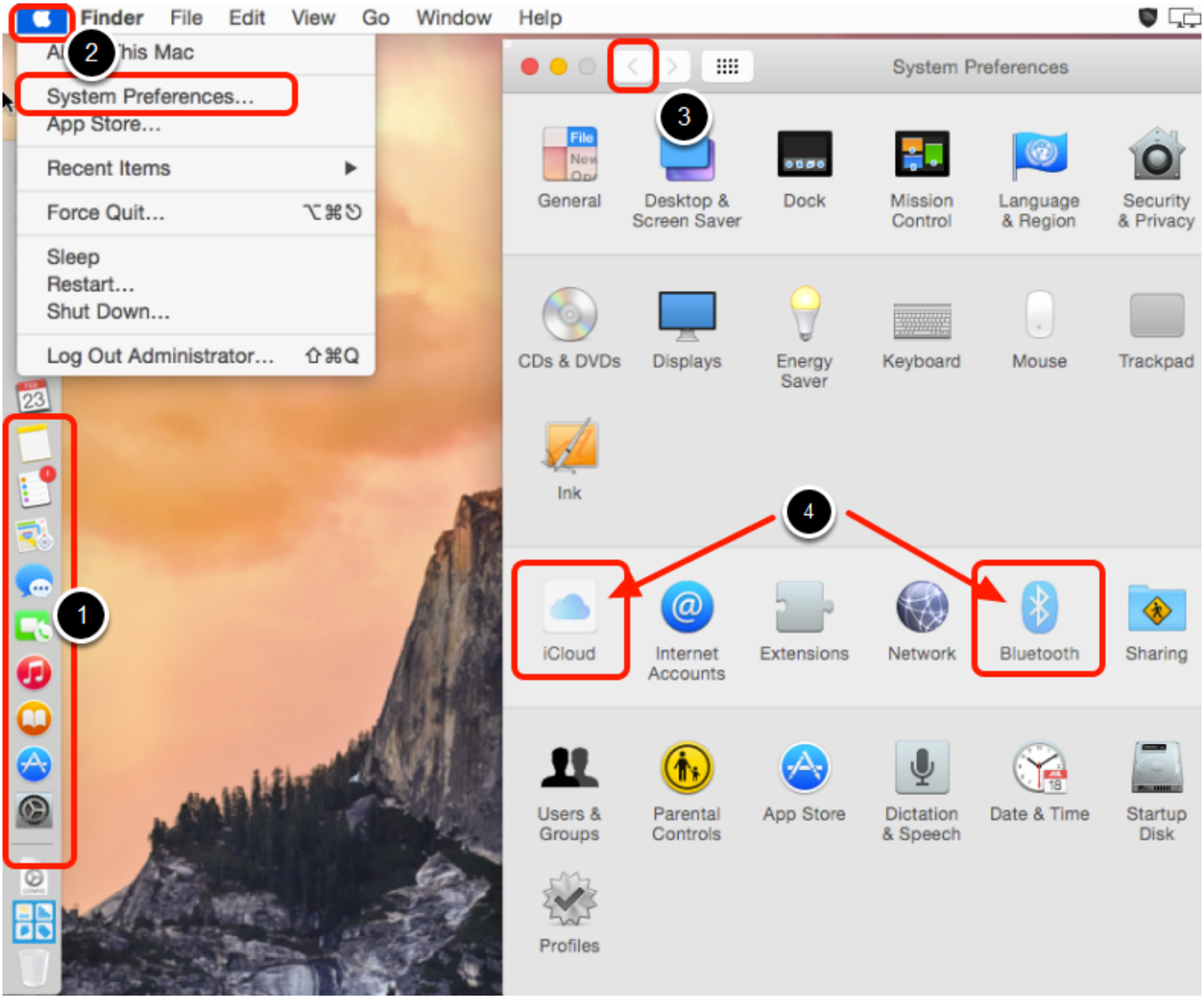
Verify the User Profile



You should now see your User Profile within the List of the Profiles window.

NOTE - If you need to edit the Profile, this is where you would come back to in order to do so.

Validate Applied Profiles



1. On your device, note that the dock has changed position and is now on the left side of the screen.
2. Click on the Apple icon in the top left corner, then click **System Preferences**.
3. If System Preferences shows you a specific subpanel, such as Time Machine, click the back button.
4. Note you are now unable to modify the settings for Bluetooth and iCloud as those icons are grayed-out.

Key Takeaways

- You can utilize a combination of Device-level and User-level profiles for flexibility in configuring your macOS devices.
- Profiles can be targeted against Assignment Groups for fine-grained control.

Configure App Catalog and Publish Internal Apps

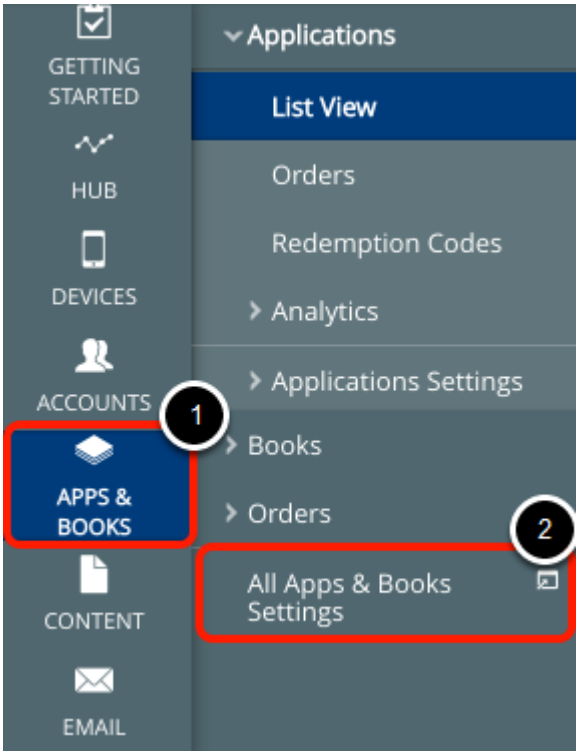
The Application catalog is a website in your AirWatch instance that provides a user and device specific list of managed applications available for installation. This provides a self-service method for end-users to select the software and applications they would like deployed to their device.

AirWatch also provides multiple methods to manage applications on a macOS device. Applications can be delivered as self-contained *.app files (what AirWatch labels an Internal Application). Applications can also be delivered as detailed manifests which allow step-by-step execution of multiple scripts and/or software packages. This second method, which AirWatch refers to as Product Provisioning, is outside the scope of this exercise.

In this exercise, you will enable the application catalog and deploy an Internal Application to your device.

NOTE - All AirWatch Management Console work should be done on the server in the VLP (VMware Learning Platform), not on the Mac.

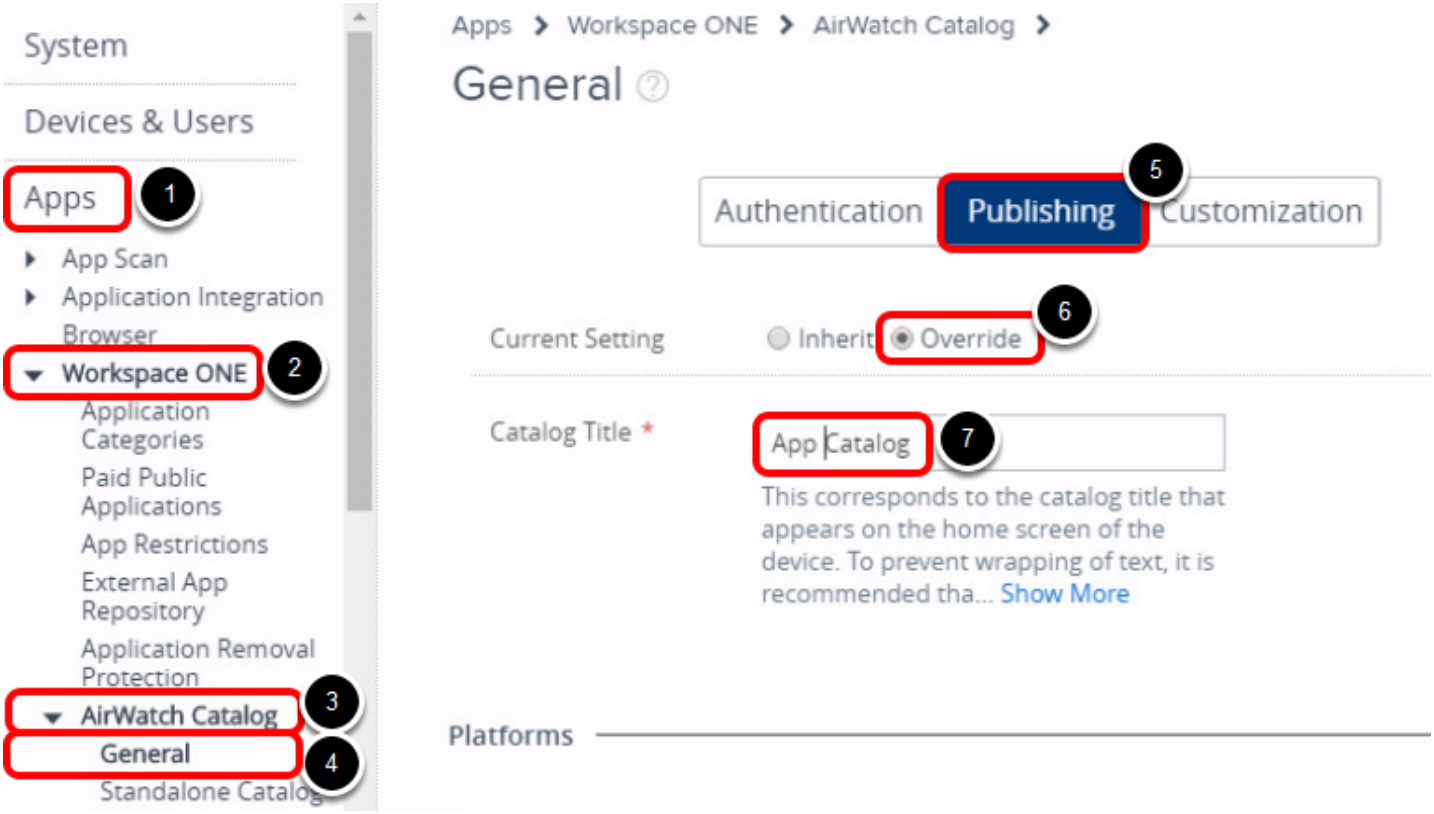
View All Settings



In the AirWatch Web Console

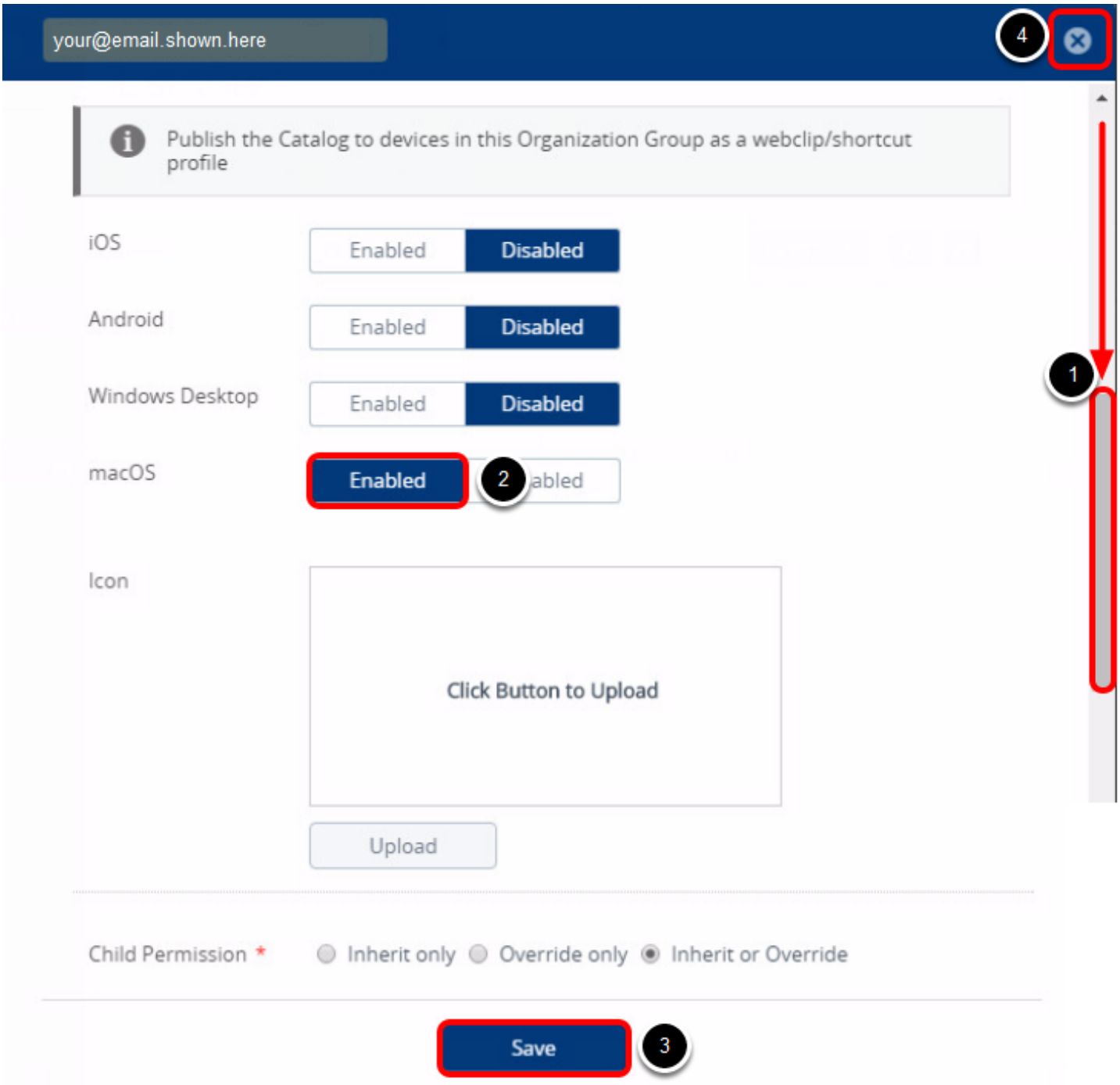
1. Click on **Apps & Books.**
2. Click on **All Apps & Books Settings.**

Enable the Application Catalog



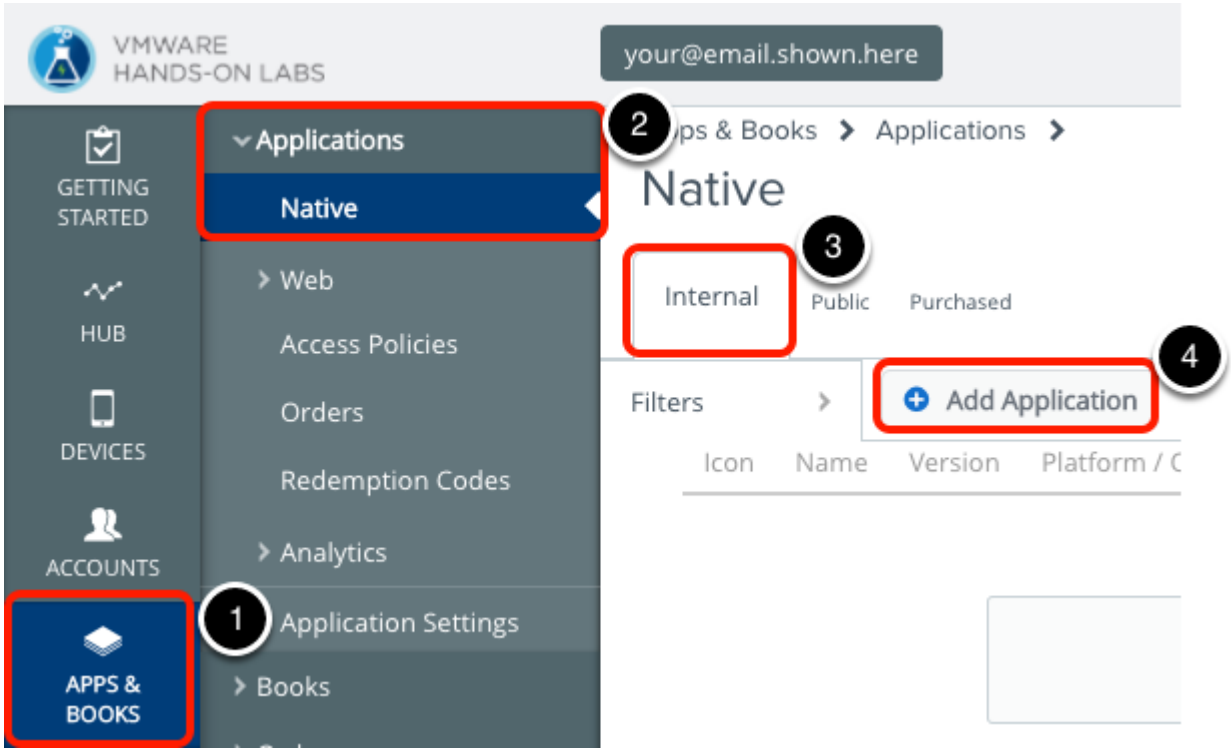
1. Click on **Apps**
2. Expand **Workspace ONE**
3. Expand **AirWatch Catalog**
4. Click on **General**.
5. Click on the **Publishing** tab
6. Click **Override**
7. Enter the Catalog title as **App Catalog**

Select Platform as macOS and Save



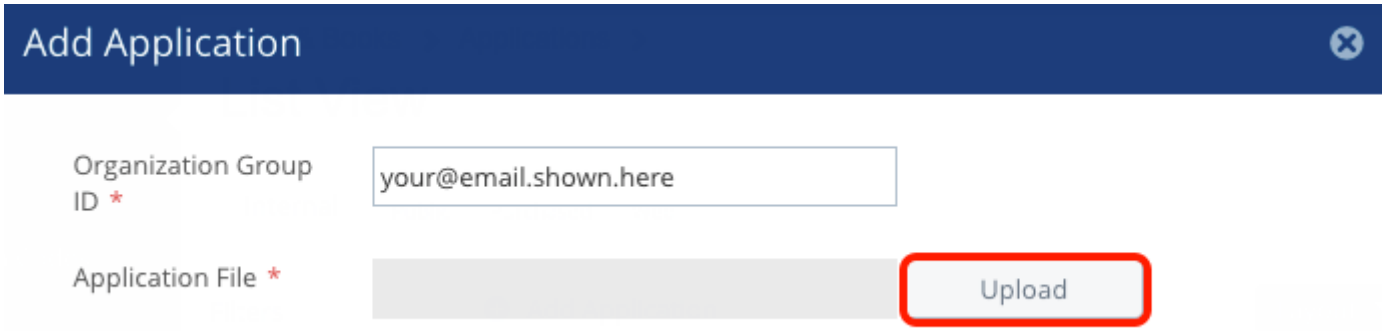
1. Scroll down until you see the platform macOS.
2. Select **Enabled** for **macOS**.
3. Click on **Save.**
4. Scroll to the top and click on **X** to exit the pop-up screen.

Add an Internal Application



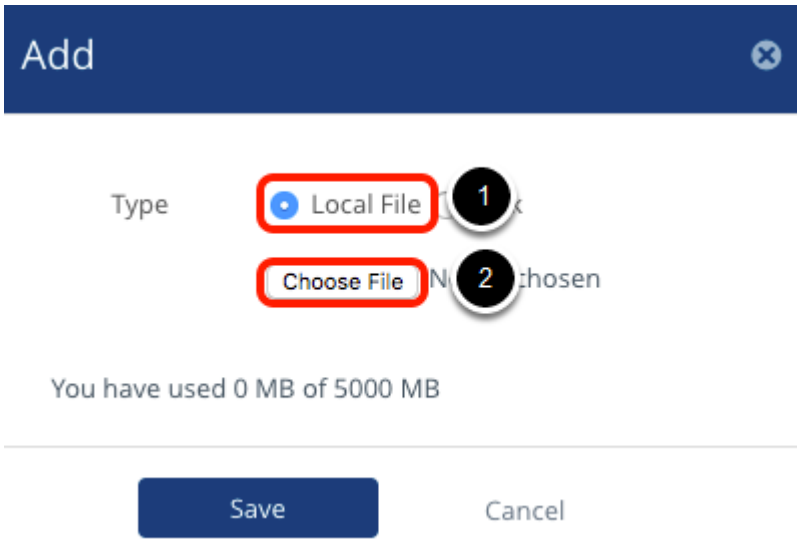
1. Click on **Apps & Books**
2. Expand **Applications** and click **Native**.
3. Click on the **Internal** tab
4. Click **Add Application**.

Select to Upload the Application



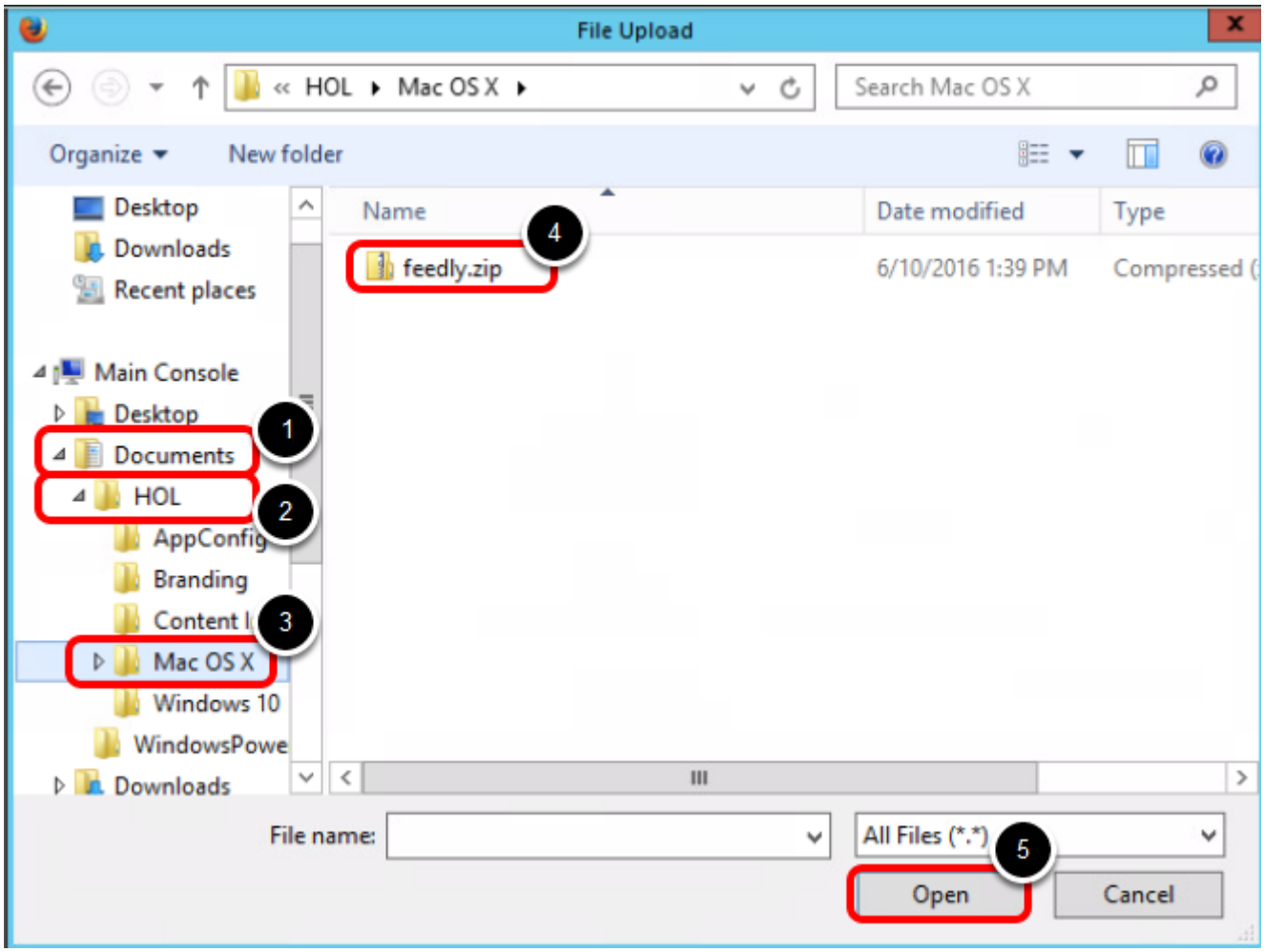
Click **Upload**

Choose the File to Upload



1. Ensure **Local File** is selected.
2. Click on the **Choose File** button.

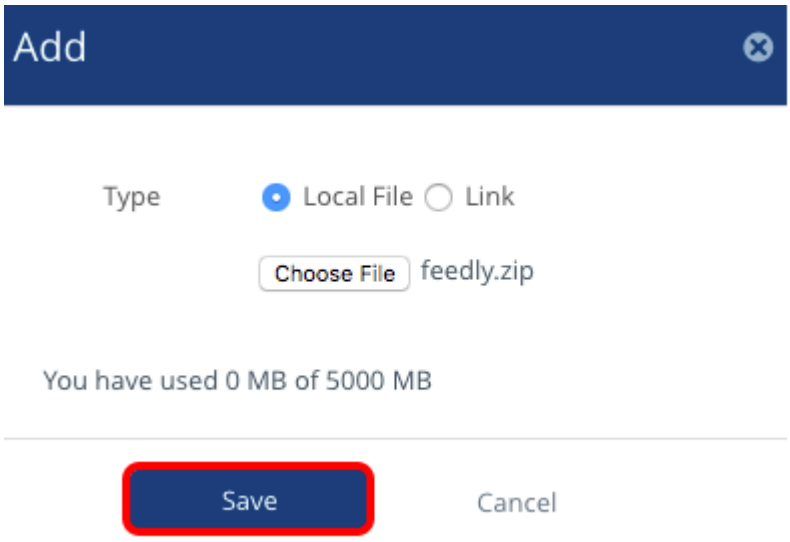
Selecting the App File



The **feedly.zip** file is located in the Documents folder.

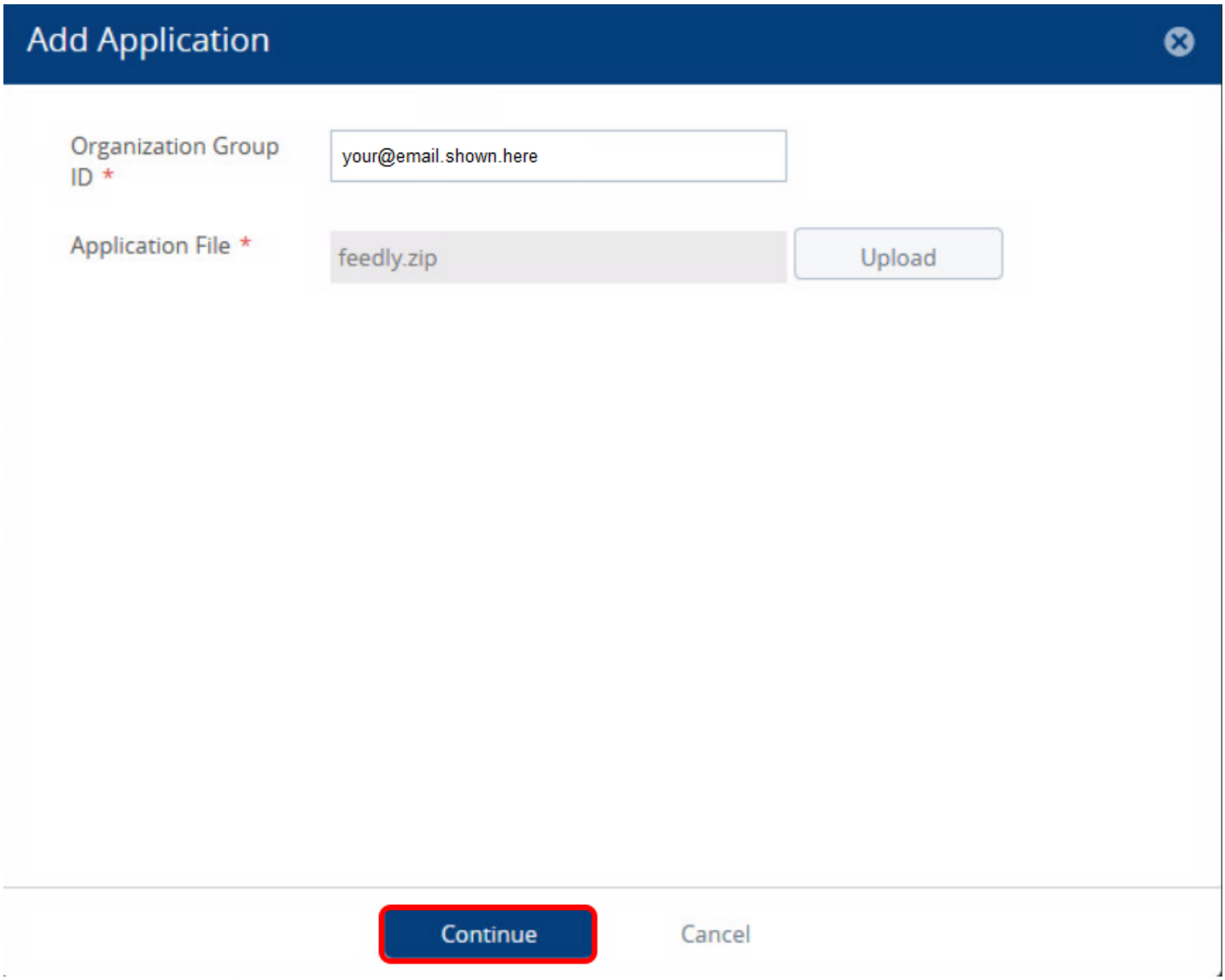
1. Click on **Documents** in the left pane
2. Click on folder **HOL**
3. Click on folder **Mac OS X**
4. Click on the **feedly.zip** file in the right pane
5. Click on the **Open** button

Saving the App File



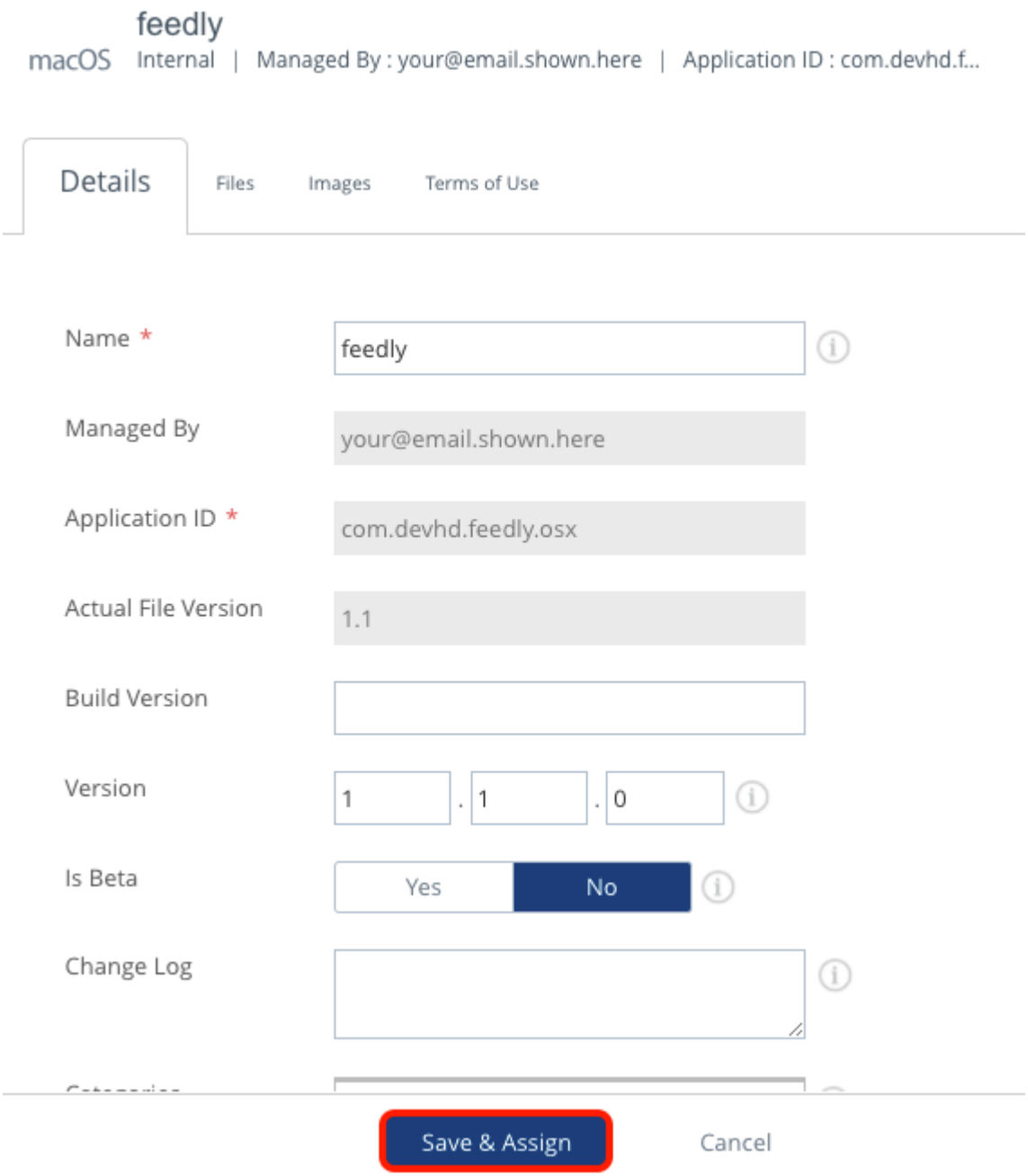
Click on the **Save** button.

Finish the Internal Application Installation



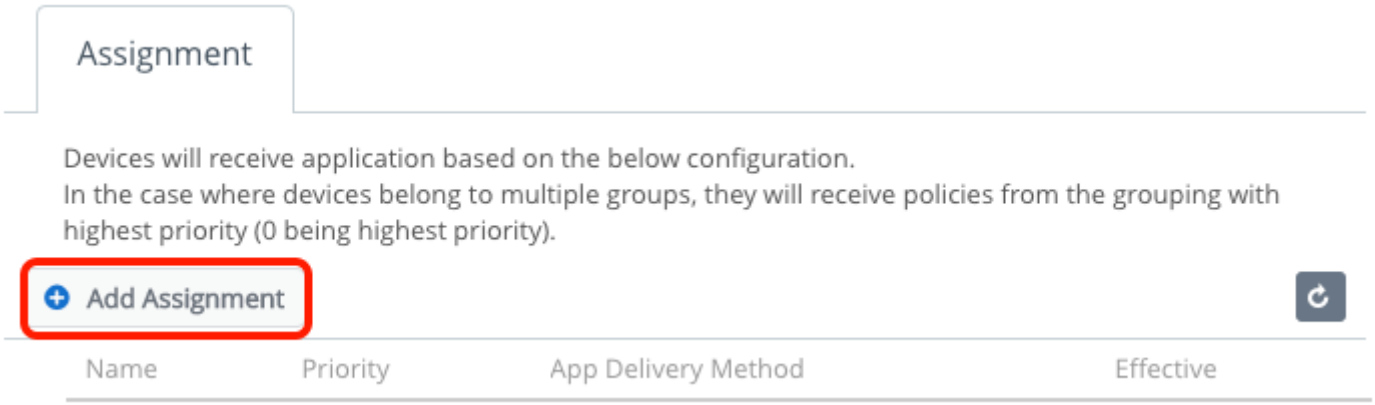
Click on the **Continue** button.

Accept Discovered Application Descriptor Information



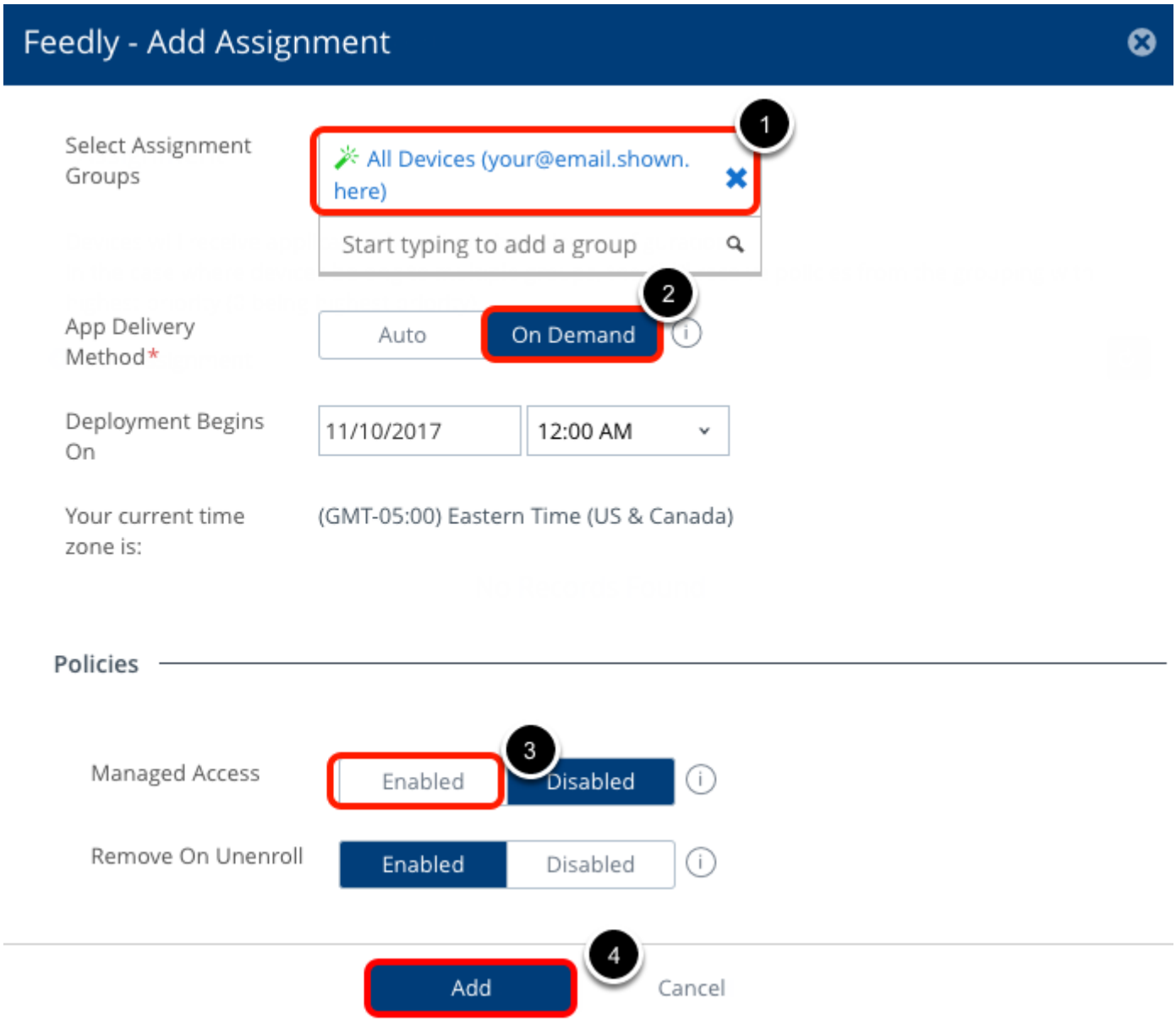
Click **Save & Assign** at the bottom of the app details page to begin the assignment of the app.

Add Application Assignment



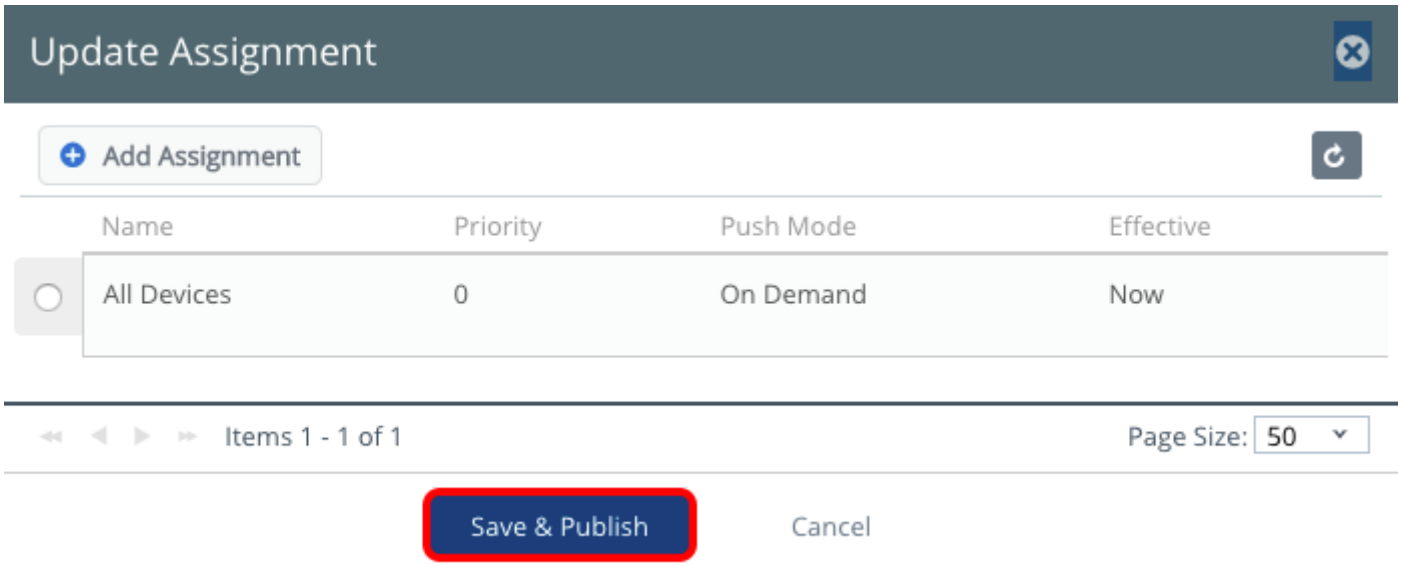
Click on the **Add Assignment** button.

Set Assignment Options



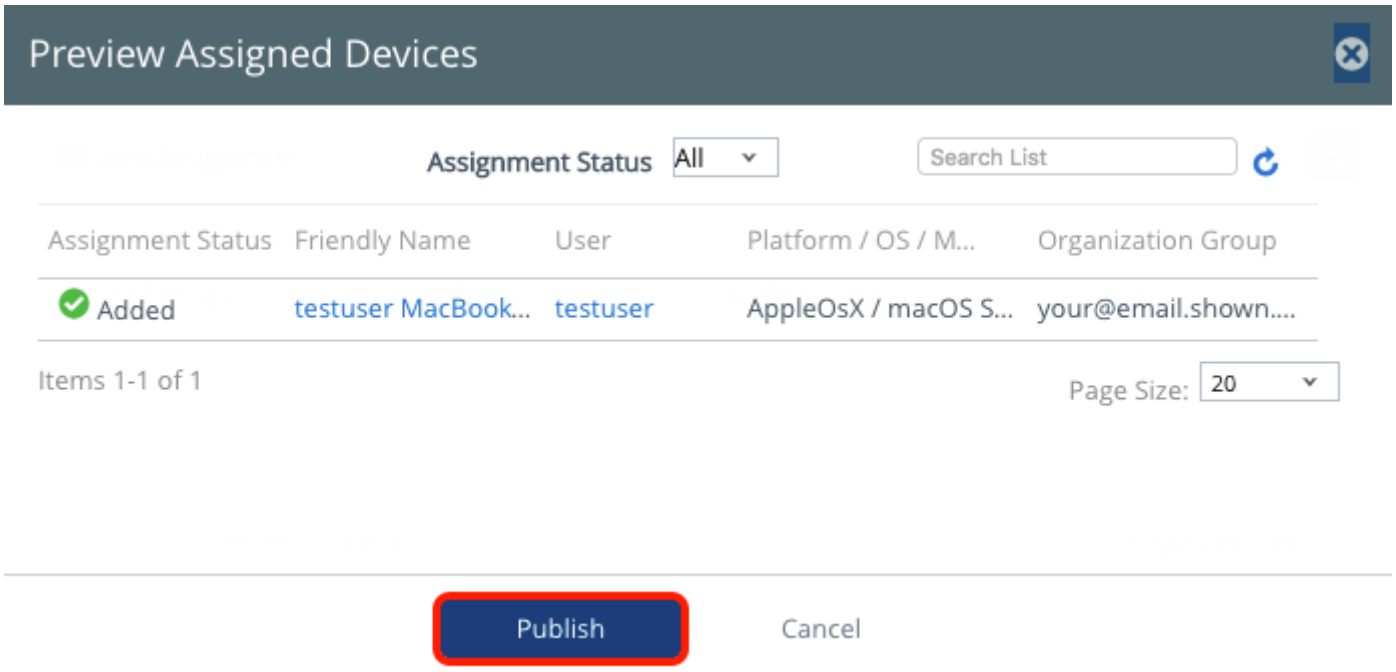
1. If you do not have the All Devices group assigned then click in the Select Assignment Groups field. This will pop up a list of created Assignment Groups. Click on the **All Devices** Group.
2. Ensure your Push Mode is set to **On Demand**.
3. Ensure Remove On Unenroll is set to **Enabled**.
4. Click **Add**.

Save the Assignment Rules



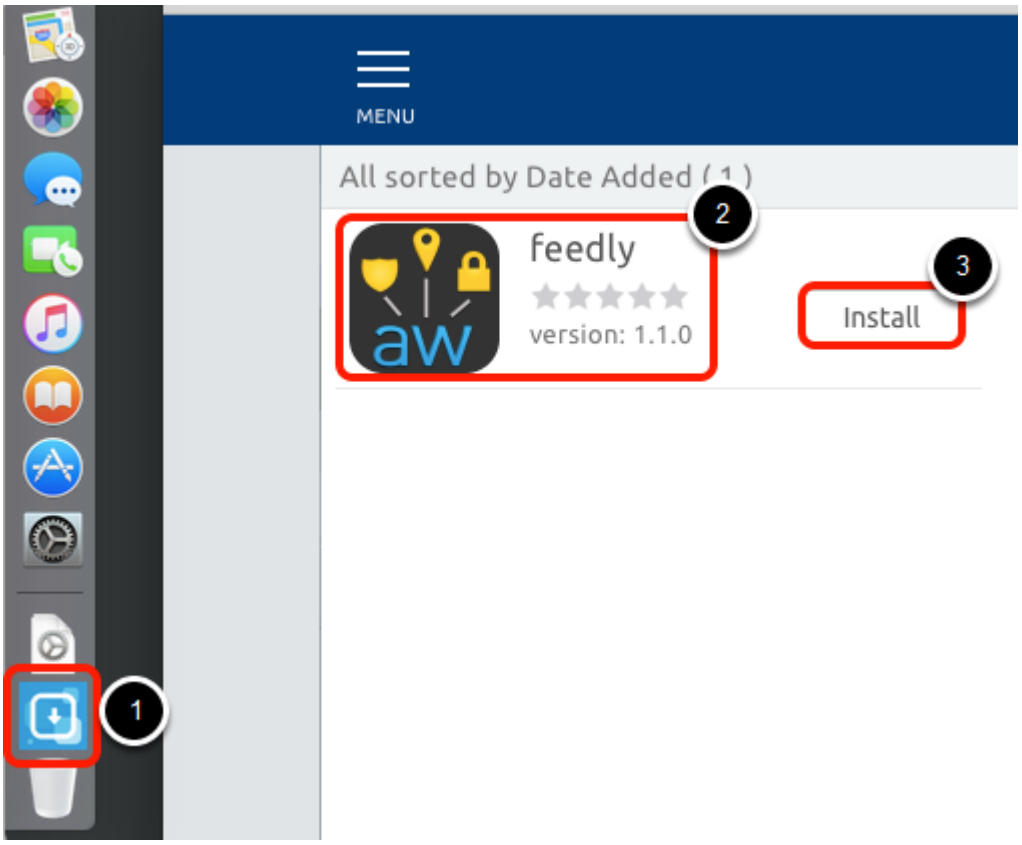
Review the Assignment rules and click **Save & Publish.**

Publish the Internal Application



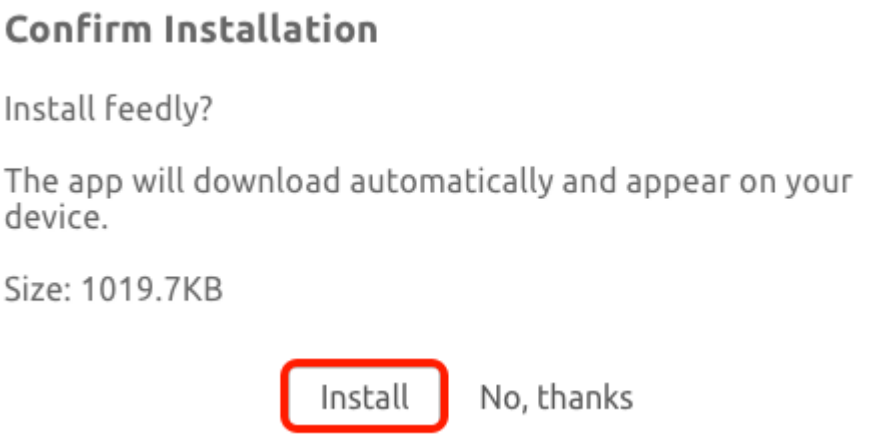
Click **Publish** to publish the internal application.

View the Published Application in the Application Catalog



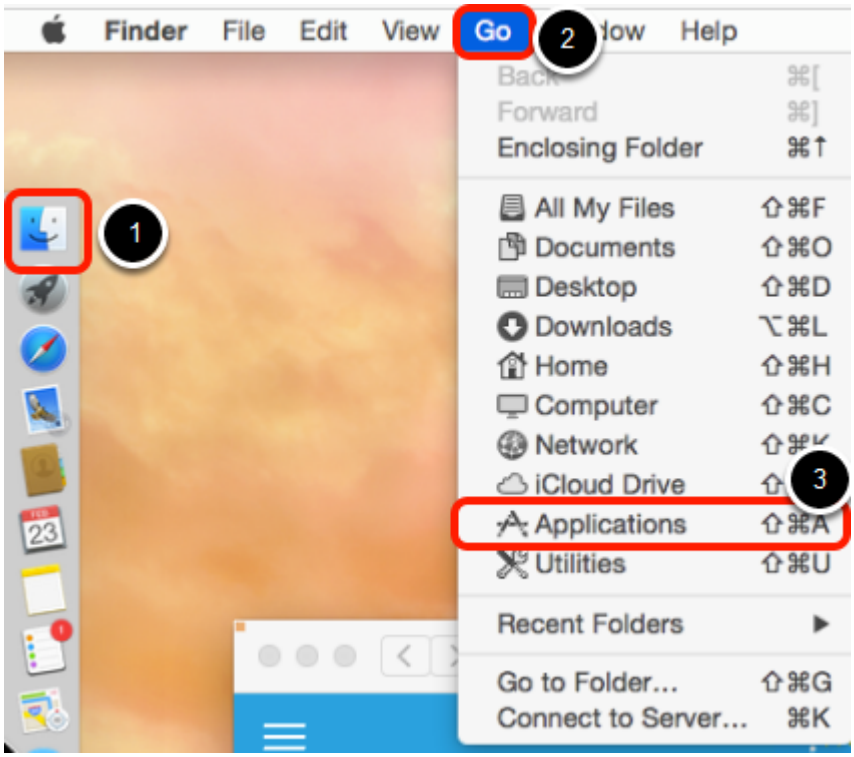
1. On your macOS test device, click on the App Catalog web clip that was added to the Dock when you enrolled.
2. Note that the Feedly app is listed as an internal app
3. Click the **Install** button for Feedly

Confirm Feedly Installation Request



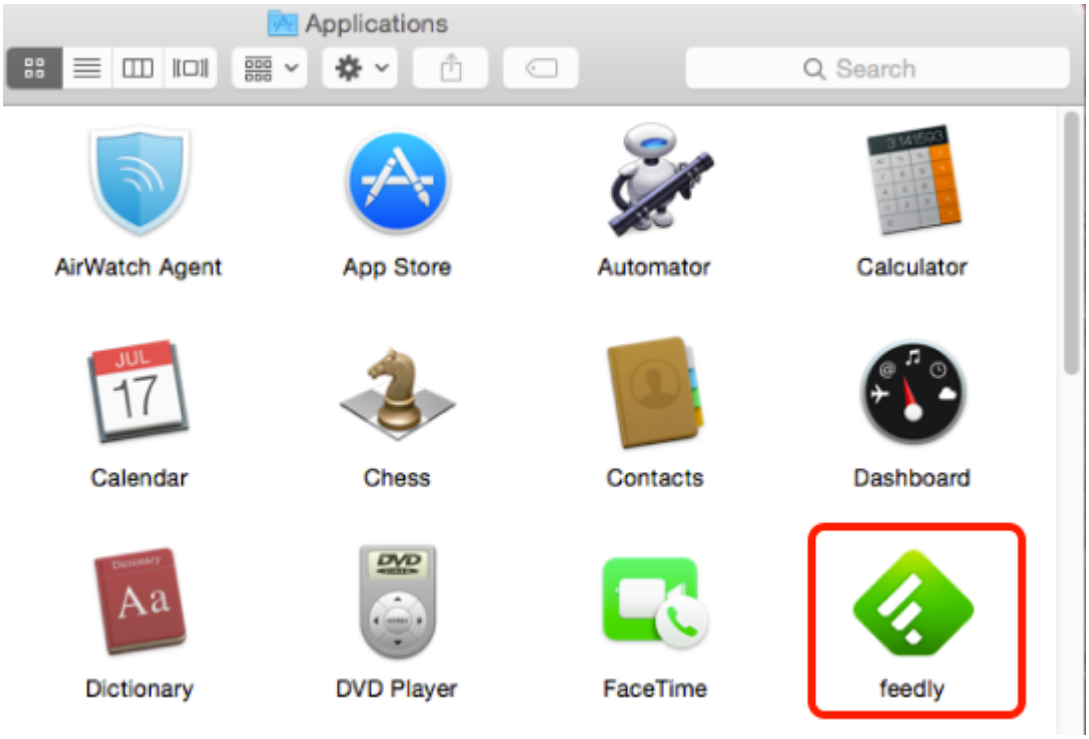
Click **Install** to confirm installation. Notice the AirWatch icon flashing in the menu bar. This indicates that the application is being downloaded and installed.

Open macOS Applications Folder



1. Click on Finder (Smiley Face) on the Dock
2. Click **Go** from the menu bar
3. Click **Applications**.

Validate Feedly Application Installation



There may be a slight delay while the AirWatch agent downloads and installs Feedly, but you can confirm the installation is complete when the Feedly icon appears in the Applications folder.

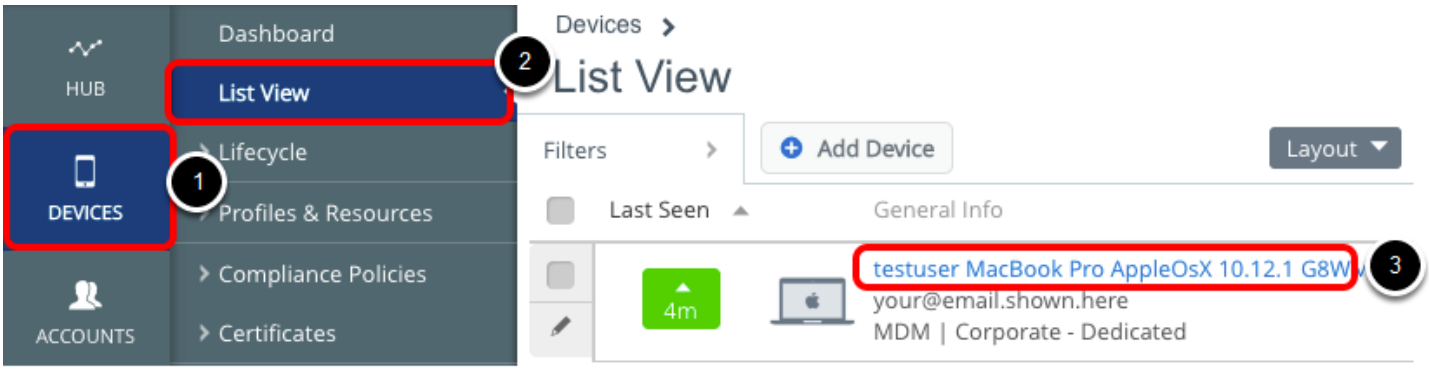
Key Takeaways

- AirWatch provides an Application Catalog to allow user and device specific self-service requests for application installation.
- macOS Applications can deployed as a single item (Internal Application) or a detailed manifest of scripts and packages (Products).

Configure Device Lock

Device lock for macOS devices causes the machine to reboot into a firmware-lock screen. This lock screen occurs at the firmware level prior to OS boot.

View macoS Device



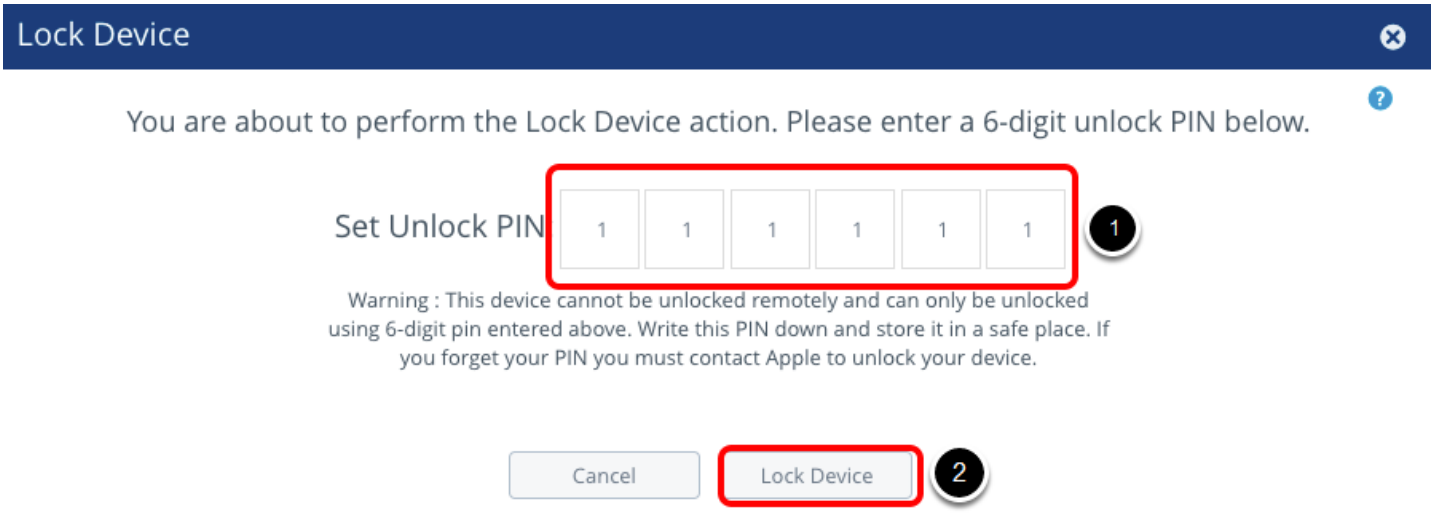
1. Click on **Devices.**
2. Click on **List View.**
3. Click on your enrolled macOS device.

NOTE - We are working with Mackbooks in this module, so please ensure that you are selecting your enrolled macOS device.

Lock Device

Click **Lock** in the top right corner of your device details view.

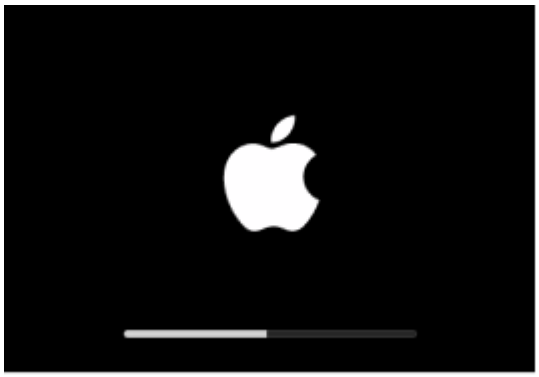
Enter Device Lock Code



1. Enter **111111** as the firmware lock code

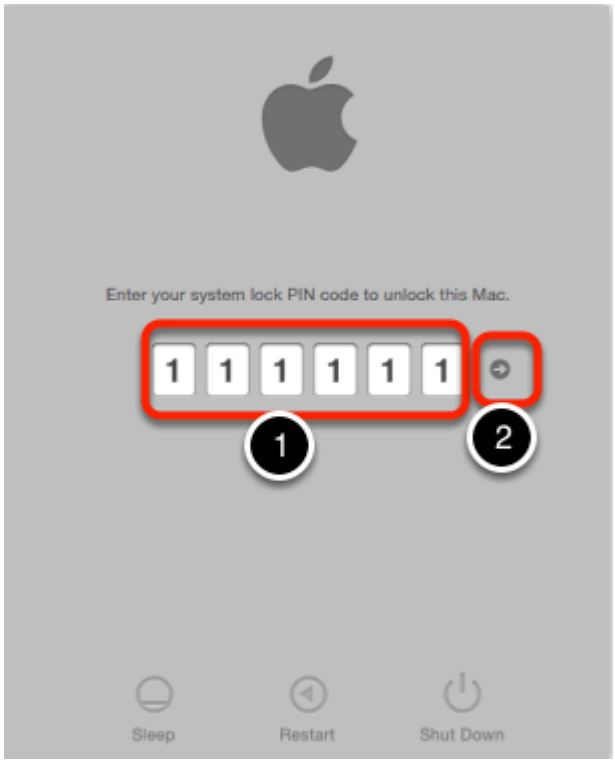
2. Click **Lock Device**

Device Reboot



1. The Device will reboot after a short delay and the firmware will be locked.

Unlock The Device



1. At the System Lock screen, enter the unlock code (**111111**)
2. Click the Arrow (**-->**) to boot the device.

Key Takeaways

- AirWatch supports a firmware-based device lock for macOS
- The device cannot be booted until the device lock code has been entered

Intro to Custom Attributes

Custom attributes enable administrators to extract particular values from a managed device and return it to the AirWatch Admin Console. This can be particularly useful for device configuration auditing and Product sequencing.

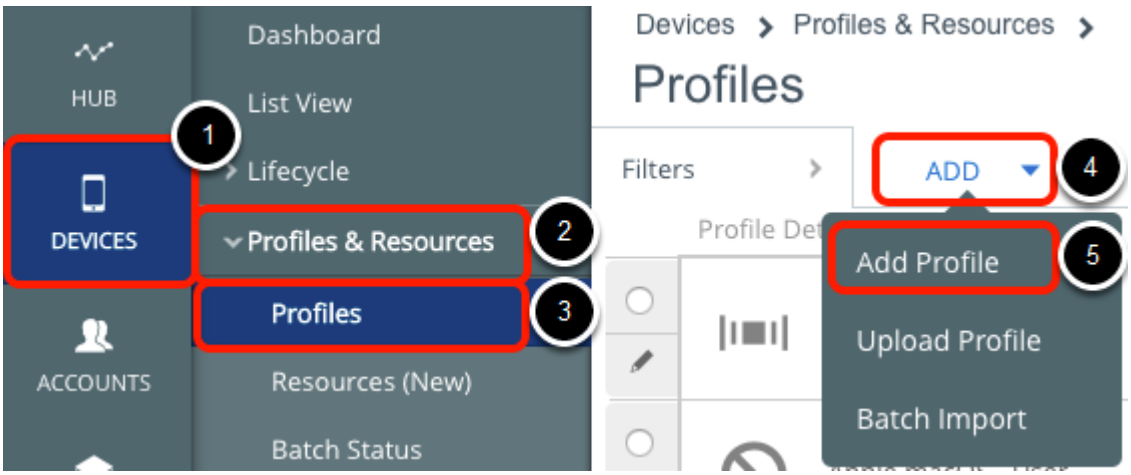
Custom Attributes

Custom Attributes are key-value pairs. These key value pairs are generated by scripting/commands which execute on the device and whose values are returned to the console via the AirWatch Agent. The scripts/commands are delivered to the device via a Custom Attributes payload in a profile. The profile also allows scheduling of the script/command to re-occur on a schedule or based on an event. Additionally, Custom Attribute payloads execute in the root context on the device, which allows you to gather information about the device without requiring the enrolled user to have Administrative permissions.

Custom Attribute Profiles

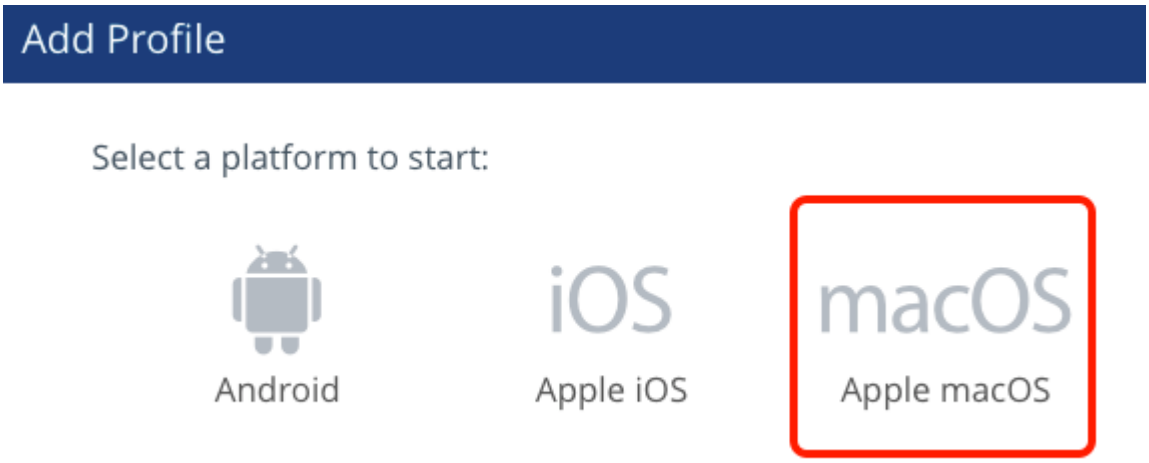
Previously, Custom Attributes were sent to the console by creating a shell script to write values to a specific Plist file monitored by the AirWatch Agent. With AirWatch 8.2 and above, this functionality is now included as a profile and adds additional features such as scheduling.

Create Custom Attribute Profile



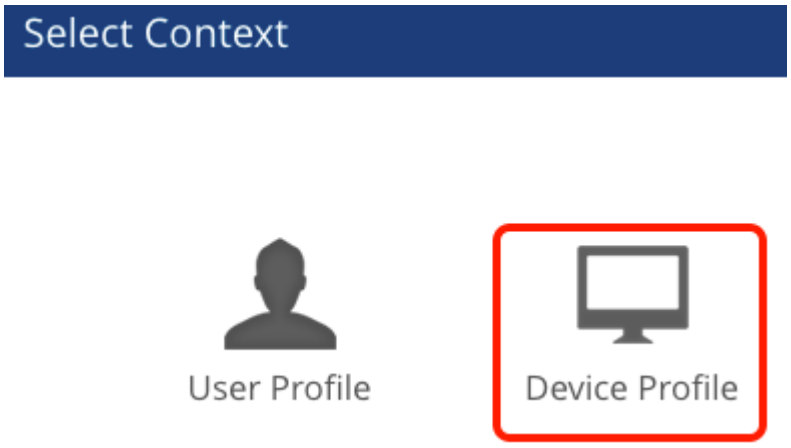
1. Click **Devices**
2. Expand **Profiles & Resources**
3. Click **Profiles**
4. Click **Add**
5. Click **Add Profile**

Select a Platform



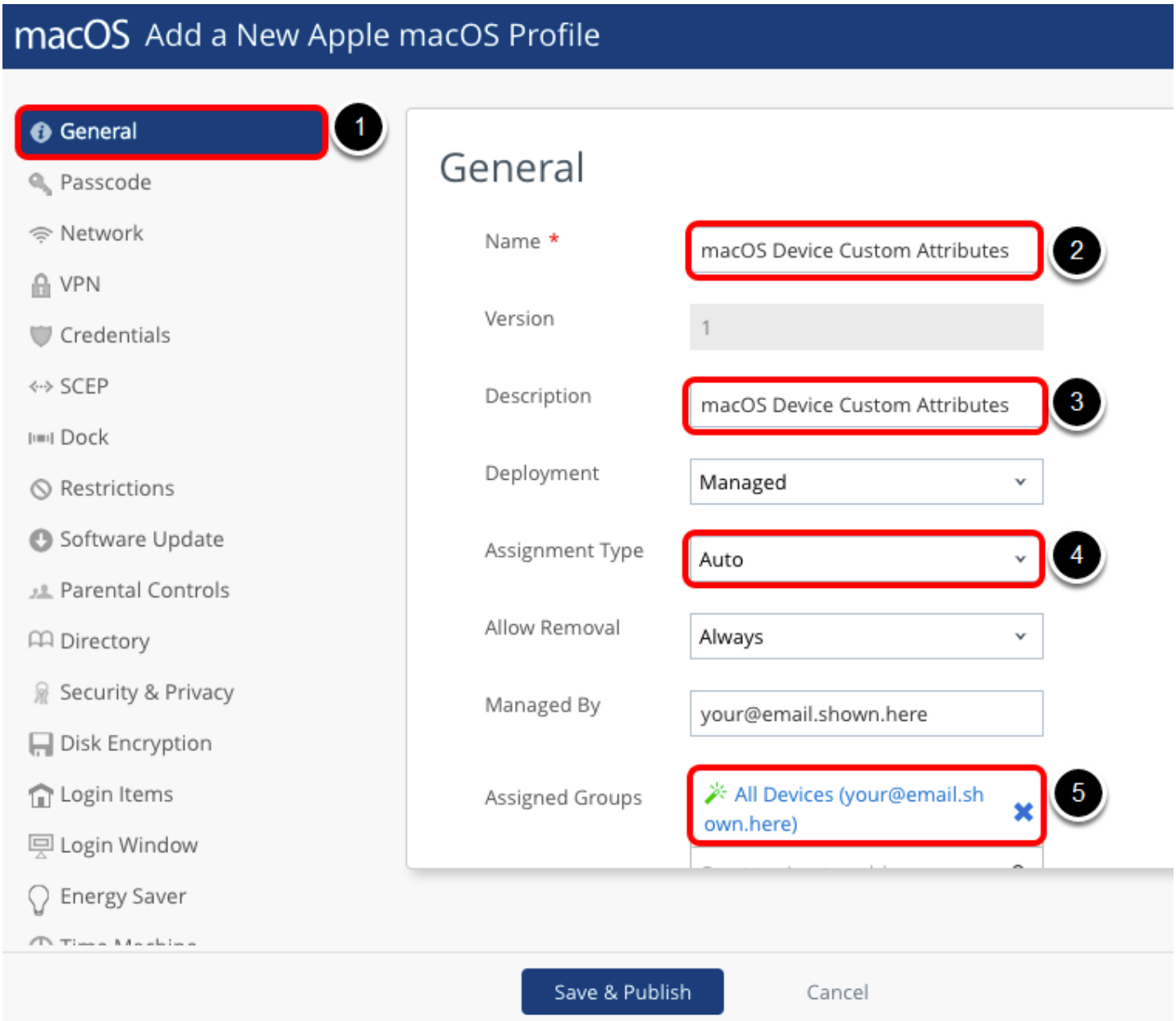
Click **macOS.**

Select Profile Context



Click **Device Profile**.

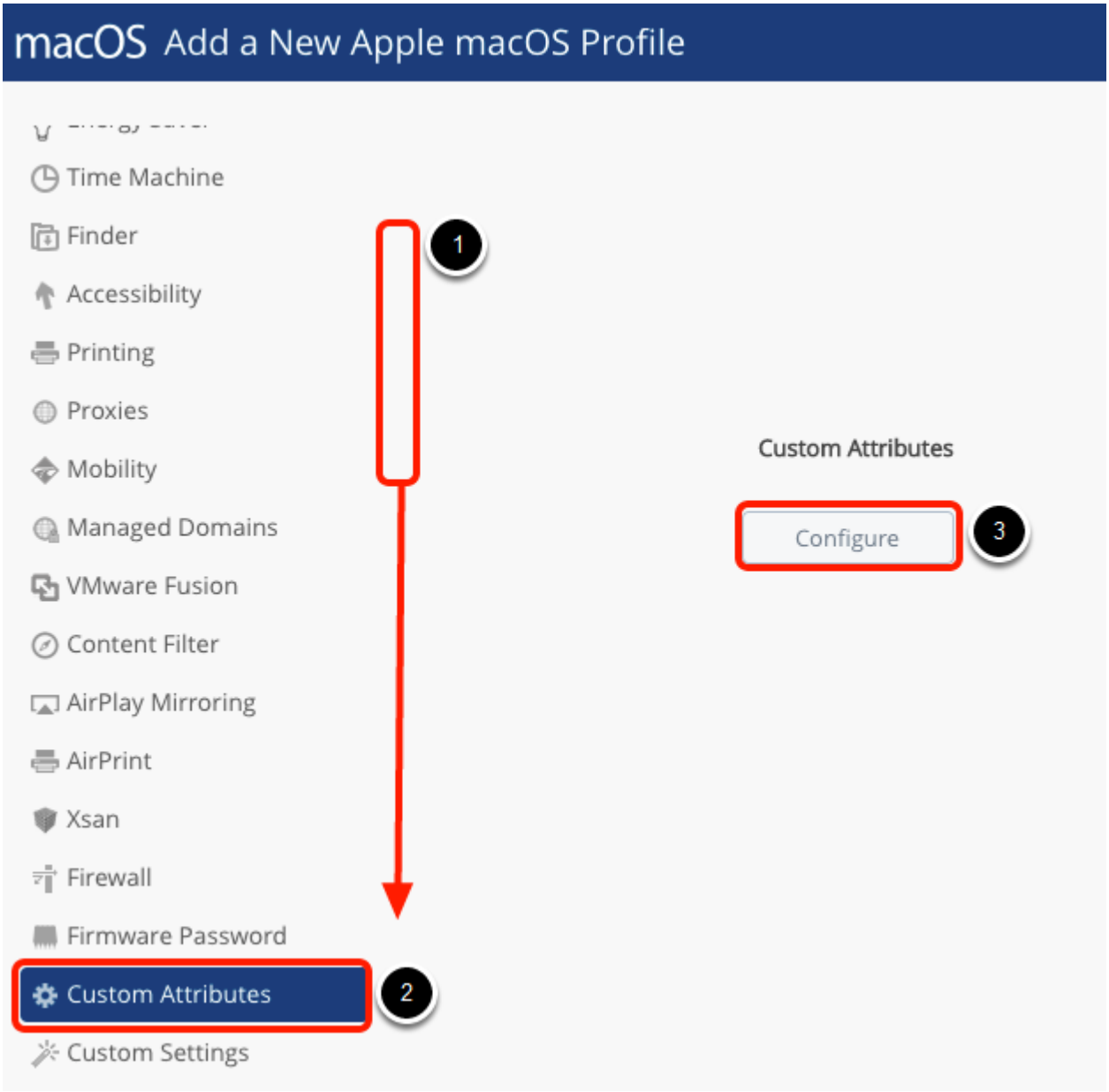
Configure General Profile Settings



1. Click on **General** if it is not already selected.
2. Give the profile a name such as **macOS Device Custom Attributes** by entering the string in the Name field.
3. Copy the profile name in the the **Description** field.
4. Ensure the Assignment Type is set to **Auto**
5. Click in the Assigned Groups field. This will pop-up the list of created Assignment Groups. Start Typing All Devices and select the **All Devices (your@email.shown.here)** Smart Group.
   NOTE - You may need to scroll down to find the Assigned Groups field.

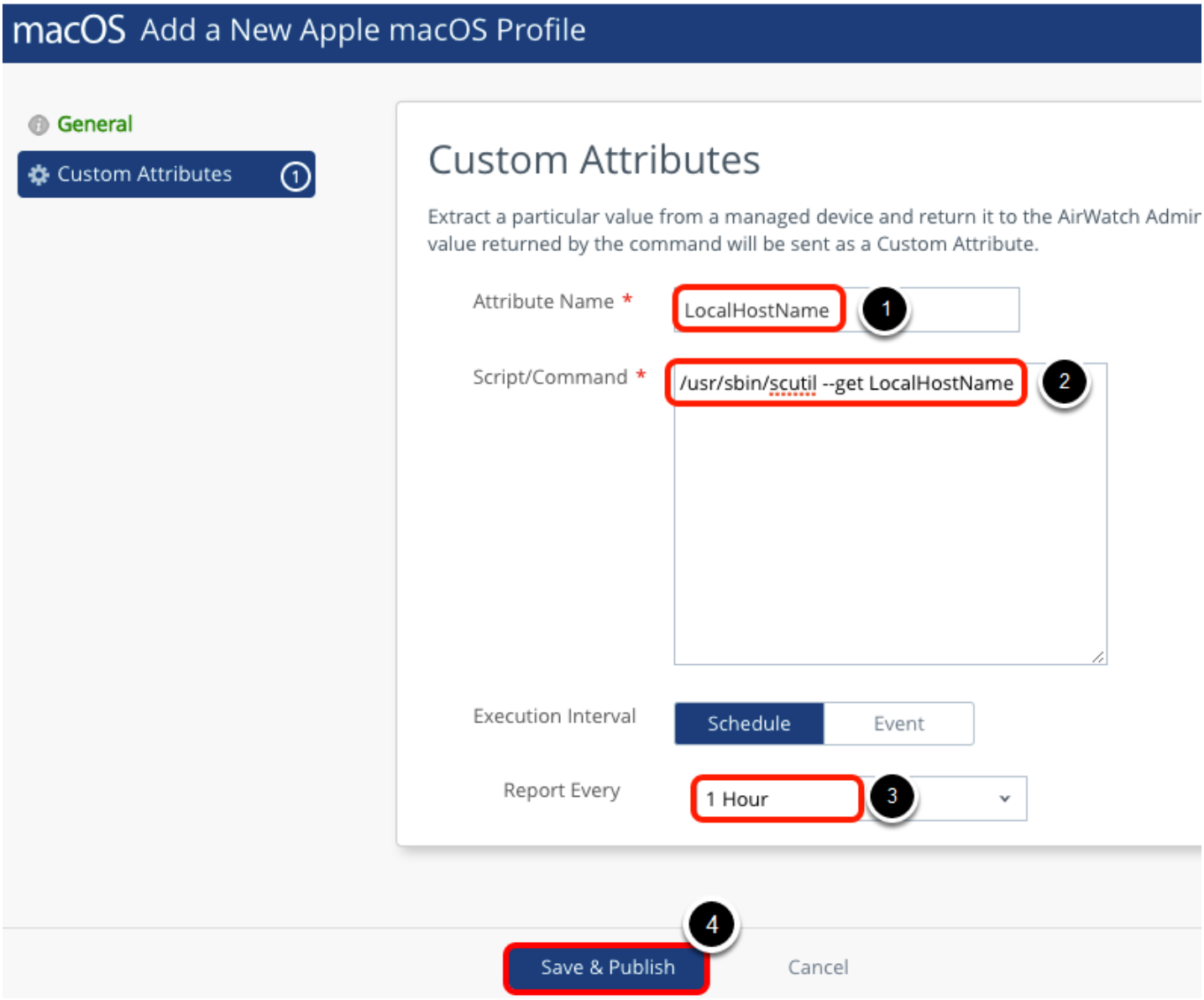
NOTE - You do not need to click SAVE or SAVE AND PUBLISH at this point. This interface allows you to move around to different payload configuration screens before saving.

Configure Custom Attributes Payload



1. Scroll down the list of Payload Types on the left side
2. Click **Custom Attributes**
3. Click **Configure**

Enter Local Host Name Custom Attribute Command



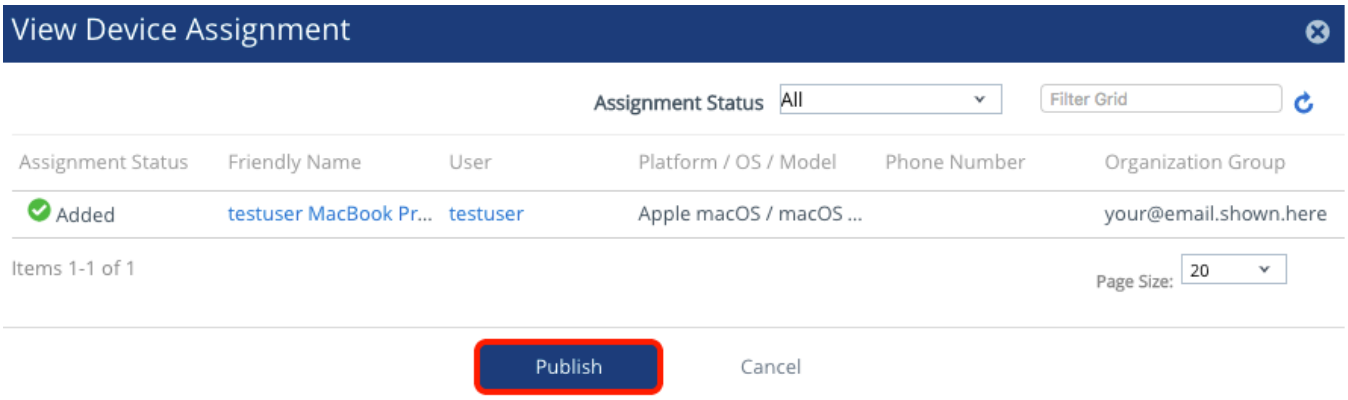
1. Enter **LocalHostName** as the Attribute Name
2. Enter the command shown below. Be sure to use the correct slash, two hyphens, and proper capitalization.
3. Select **1 Hour** as the Reporting
4. Click **Save & Publish.**

NOTE - Please refer the Lab Guidance section in the beginning for how to copy text from manual to use in VLP.

Custom Attribute Command:

```
/usr/sbin/scutil --get LocalHostName
```

Publish to Device Assignment

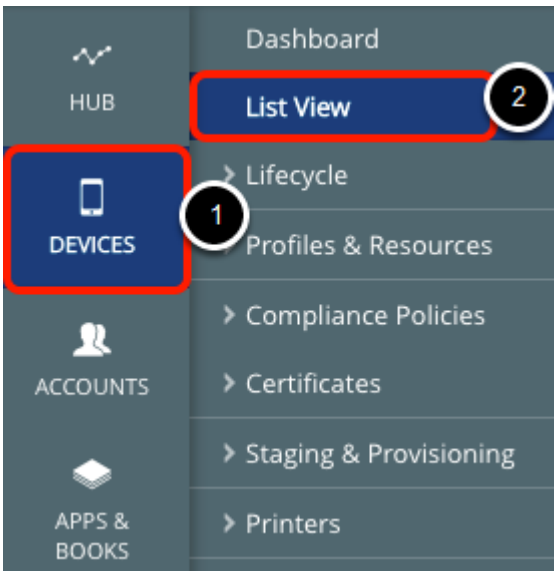


Click **Publish**.

Locating Custom Attributes

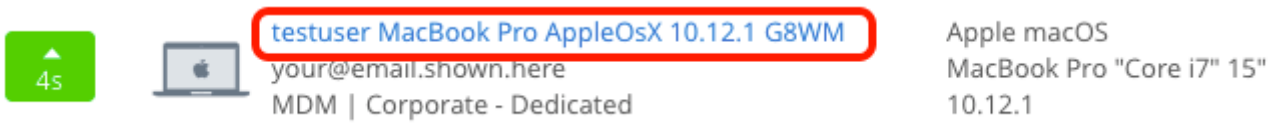
Once AirWatch delivers a Custom Attributes profile/payload to a device, the Agent will report the initial value of the Custom Attribute back to AirWatch and begin the Schedule or Event monitoring. Custom Attribute values that have been reported back to the console can be viewed in the device details.

Access Device List View



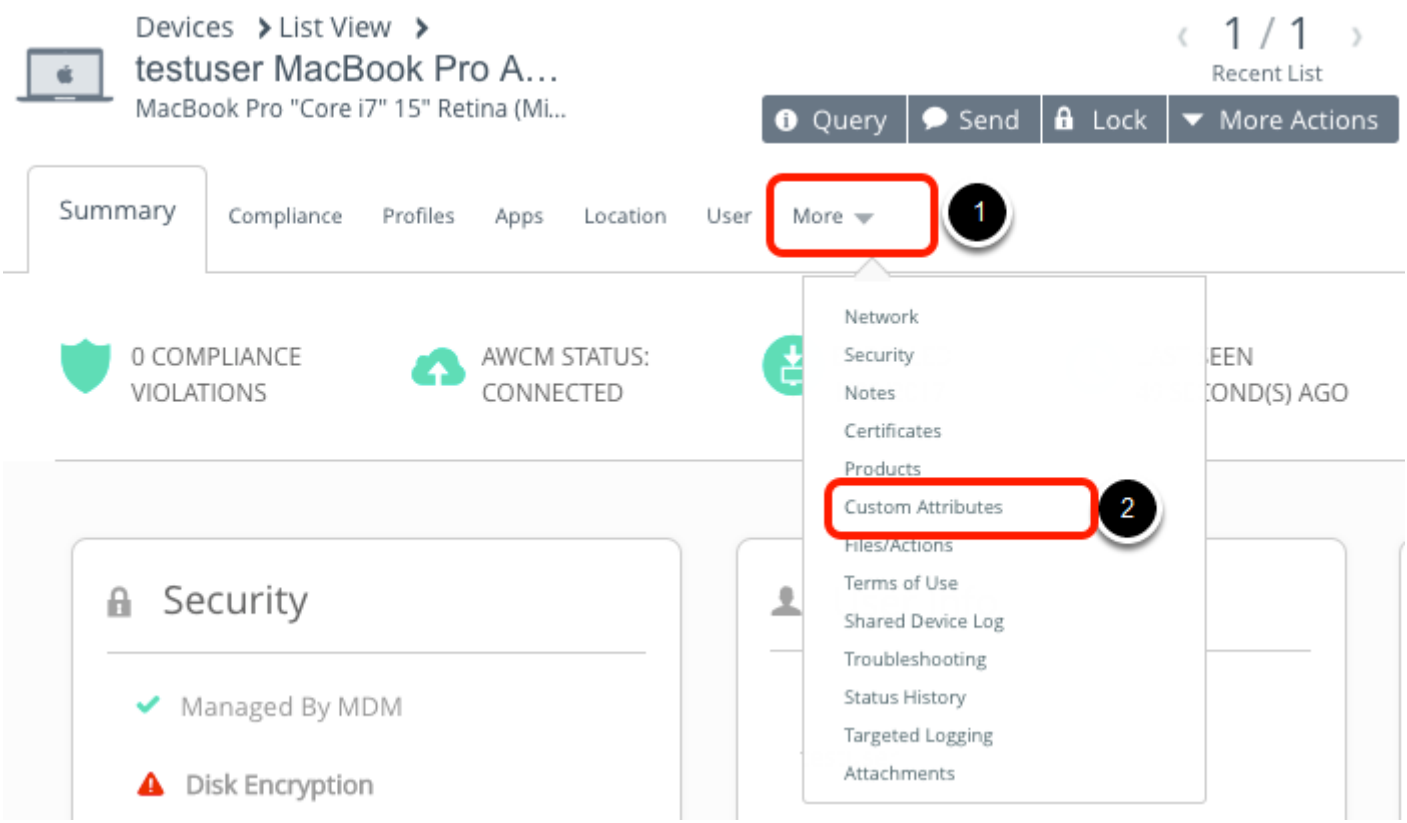
1. Click on **Devices**
2. Click on **List View**

Select Your Device



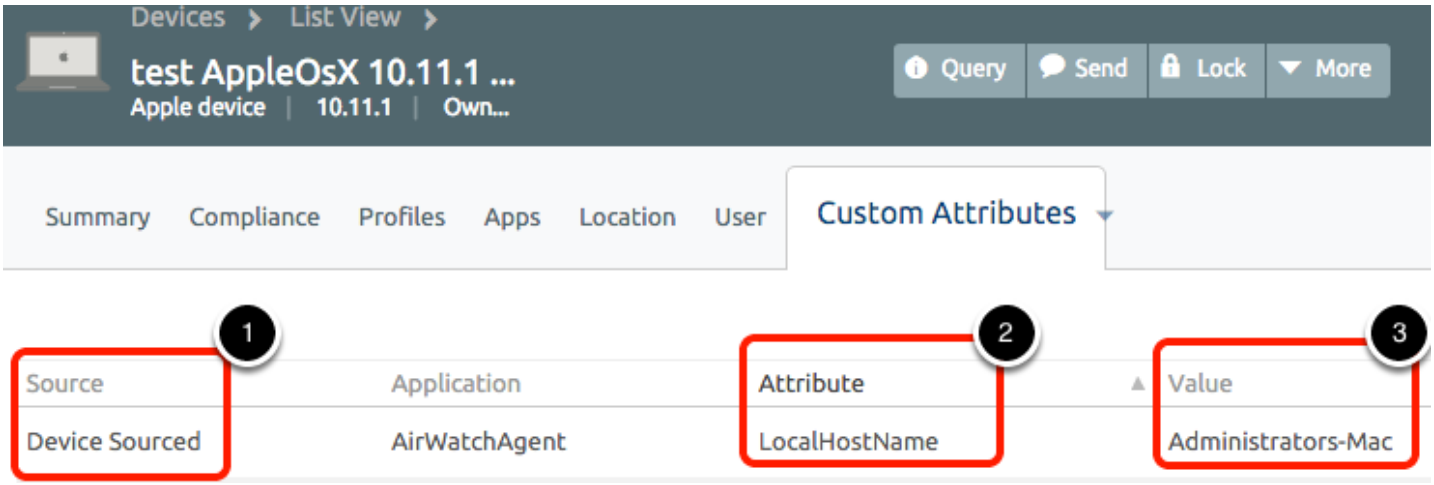
Click on your device

Access Custom Attributes



1. Click on **More.**
2. Click on **Custom Attributes.**

Review Custom Attributes

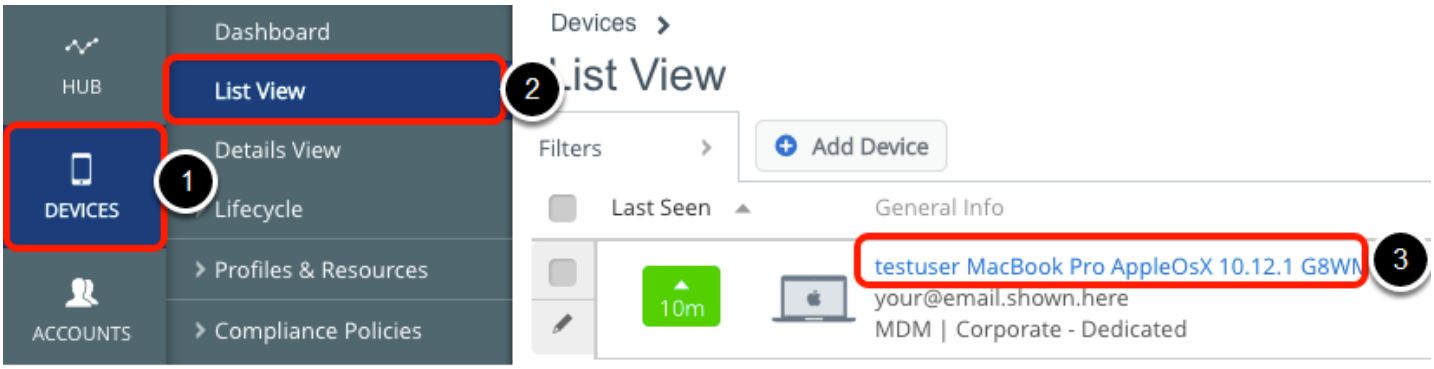


1. Notice that the Source of the Attributes is **Device Sourced**, meaning it was gathered at the device and sent to AirWatch.
2. Note the list of Attributes.
3. Note the value of each Attribute. These values were generated by the output of your command/script in the Custom Attributes payload.

Enterprise Wipe

An Enterprise Wipe removes corporate data that was added to the device while leaving personal data intact.

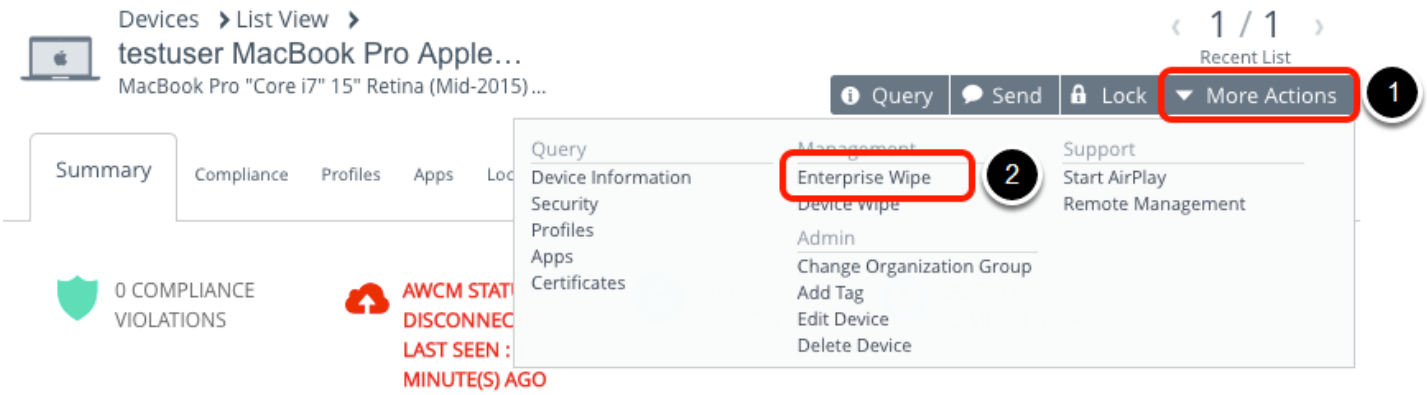
View Device List



From within the AirWatch console,

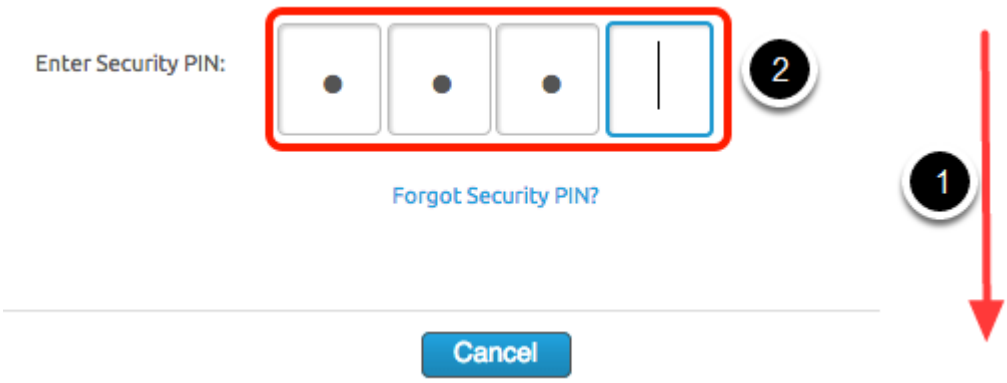
1. Click on **Devices**
2. Click on **List View**.
3. Click on your macOS device in the List View to view details.

Initiate Enterprise Wipe



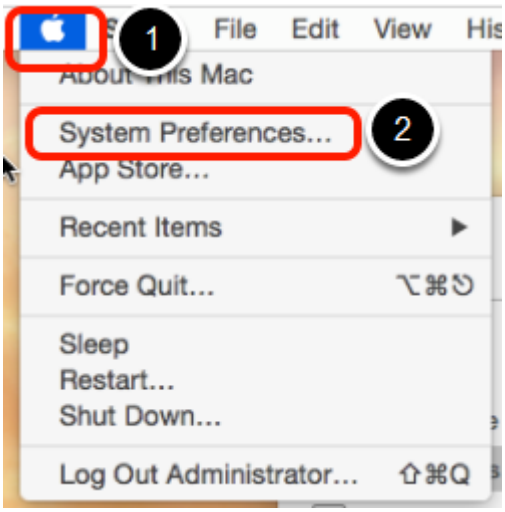
1. From the toolbar in the device details header, click **More Actions.**
2. Click **Enterprise Wipe** under the "Management" header in the menu that drops down.

Enter Security PIN to Confirm Wipe



1. Scroll down until you see the section to Enter Security PIN.
2. Enter your security PIN "**1234**" to initiate the Enterprise Wipe.

Access macOS System Preferences

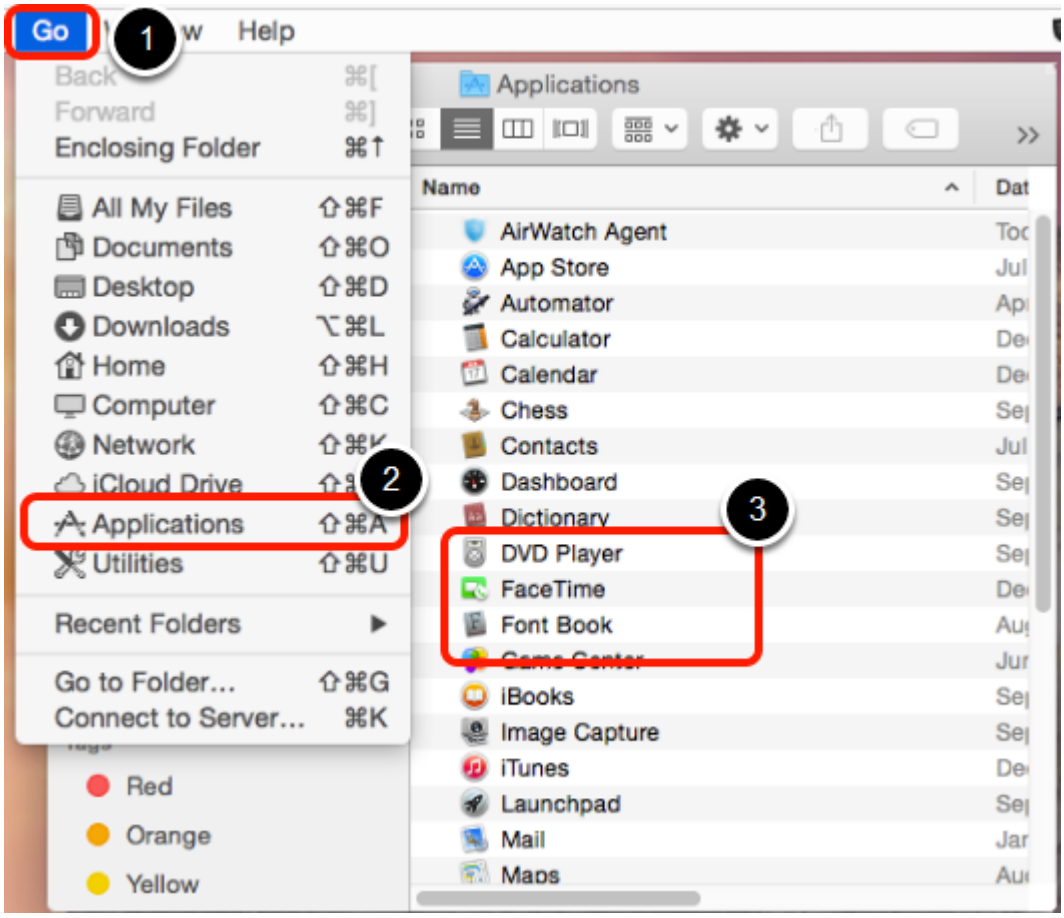


1. On your device, click on the Apple icon in the top left corner
2. Click **System Preferences**.

Verify Removal of System Preference Restrictions

1. Note you are now able to make modifications to iCloud and Bluetooth since the restriction you created earlier has been removed.

Verify Removal of Deployed Internal Application



1. Open Finder (Smiley Face) on the dock and click **Go.**
2. Click on **Applications**.
3. Confirm that **Feedly** has been removed from your device.

On your device, also note that the dock preferences have been removed and the dock has returned to its original position.

NOTE - Due to the limitations of the lab network, you may need to wait several minutes after un-enrolling before the Feedly application is removed and the dock is returned to the original position.

Conclusion

This lab covered basic macOS administration using AirWatch. You enrolled your macOS device, created profiles, deployed an application, locked the device, used Custom Attributes and then enterprise wiped the content and settings from the device.

For more information, please register for a free account at **https://my.air-watch.com** (My AirWatch) in order to access AirWatch Academy and our Resources page. There you will find courses and documentation that can help you with advanced topics in macOS management, such as:

- Device Enrollment Program
- Device Staging and Enroll-on-Behalf
- Application Volume Purchase Program
- Kiosk Mode
- Certificates and Identity/Directory Integration
- Mail Integration
- Product Provisioning
- ... and More!

This concludes the Basic Apple macOS Management module.

Module 3 - Basic Windows 10 Management (30 minutes)

Introduction

In this lab module, you will learn how to enroll a Windows 10 device into AirWatch and how to configure and deploy restriction profiles and applications to your enroll device.

Pre-Requisites

To successfully complete this Hands-On Lab, you'll need to ensure you have the following pre-requisites:

- A virtual machine or spare Windows device running Windows 10 (non Home edition) **with the latest updates installed**. **DO NOT access the Hands-On Lab from the same machine you will be managing.**
  NOTE - We have provided a Windows 10 VM for you which has all the pre-requisites setup for this lab. We recommend you using that by following the instructions in the manual for this lab.
- Administrative rights to the virtual machine or spare Windows device which you will be using to perform the Hands-On Lab.
- A Windows 10 Desktop app (*.msi), such as 7-Zip. A sample Windows 10 app has been provided in the lab machine for your use.

As a reminder, **DO NOT** access the Hands-On lab from the same machine you plan to enroll & manage as part of the HOL exercise. As part of the HOL, you will be rebooting this machine and will temporarily lose access to the lab documentation if you run the lab from the machine you enroll.

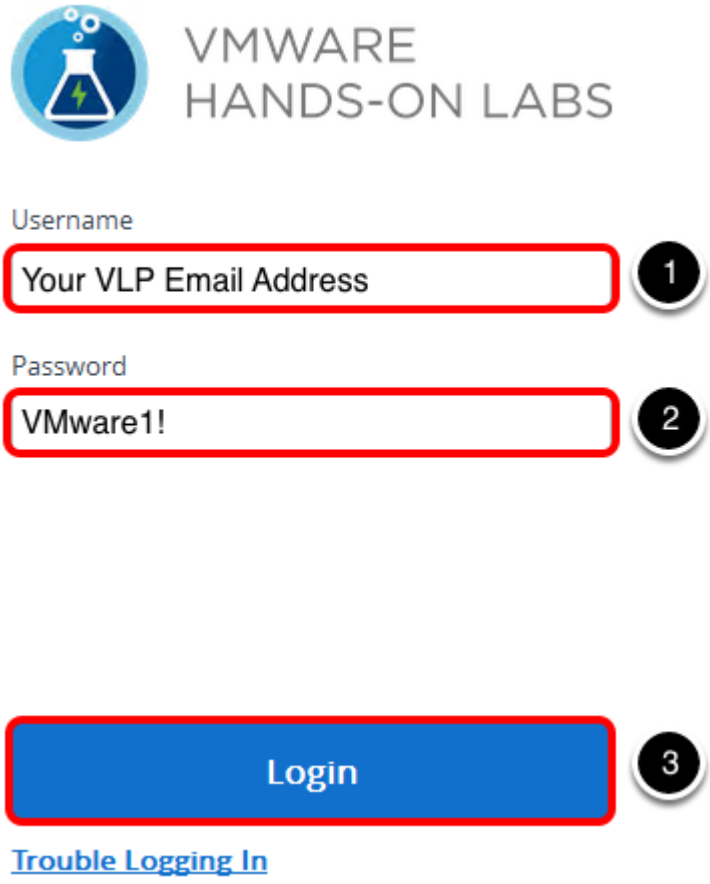
Login to the AirWatch Console

To perform most of the lab you will need to login to the AirWatch Management Console.

Launch Chrome Browser

Double-click the **Chrome** Browser on the lab desktop.

Authenticate to the AirWatch Administration Console



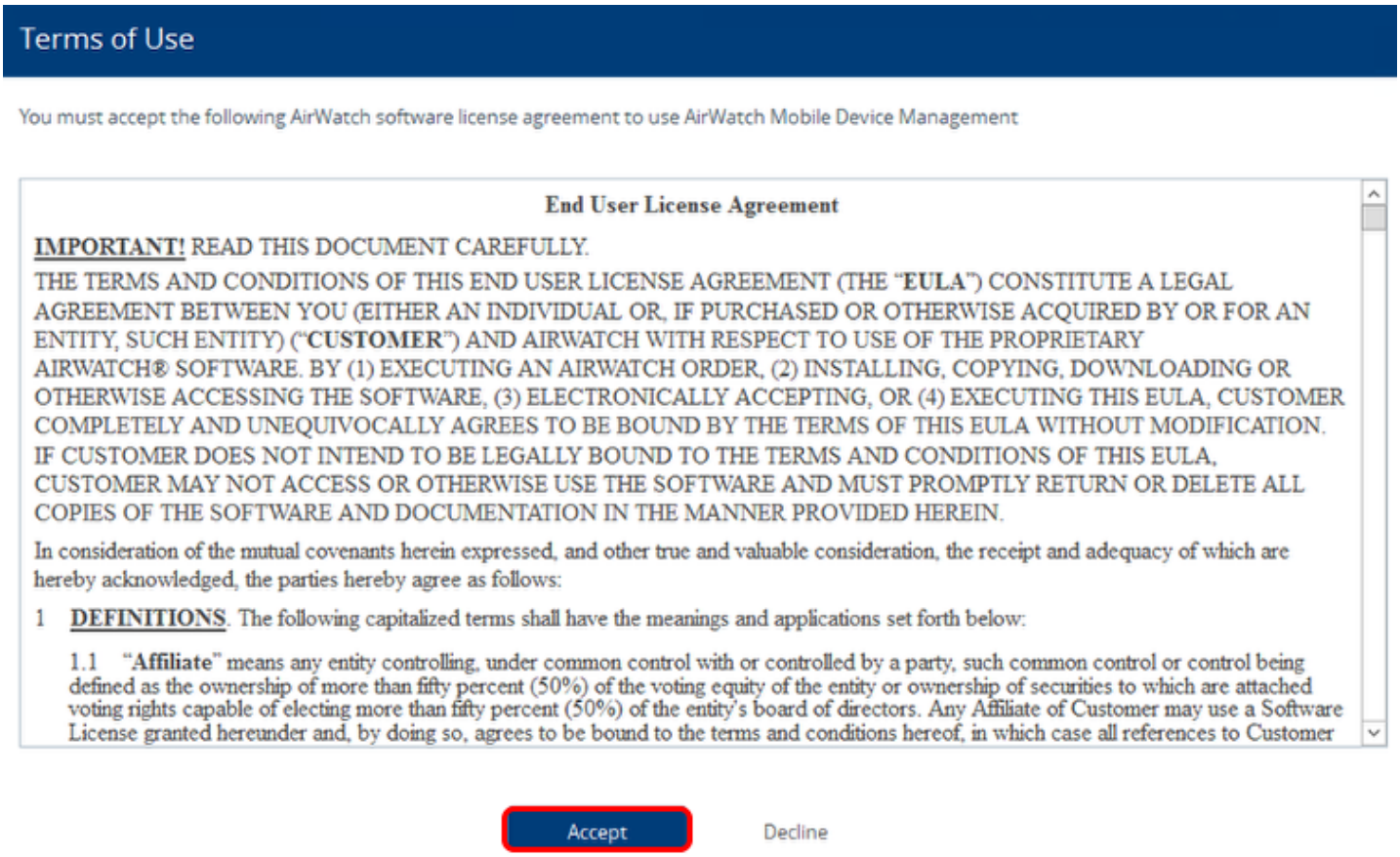
The default home page for the browser is **https://hol.awmdm.com**. Enter your AirWatch Admin Account information and click the **Login** button.

NOTE - If you see a Captcha, please be aware that it is case sensitive!

1. Enter your **Username**. This is you **email address** that you have associated with your **VMware Learning Platform (VLP) account**.
2. Enter **"VMware1!"** for the **Password** field.
3. Click the **Login** button.

NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the AirWatch Hands On Labs server.

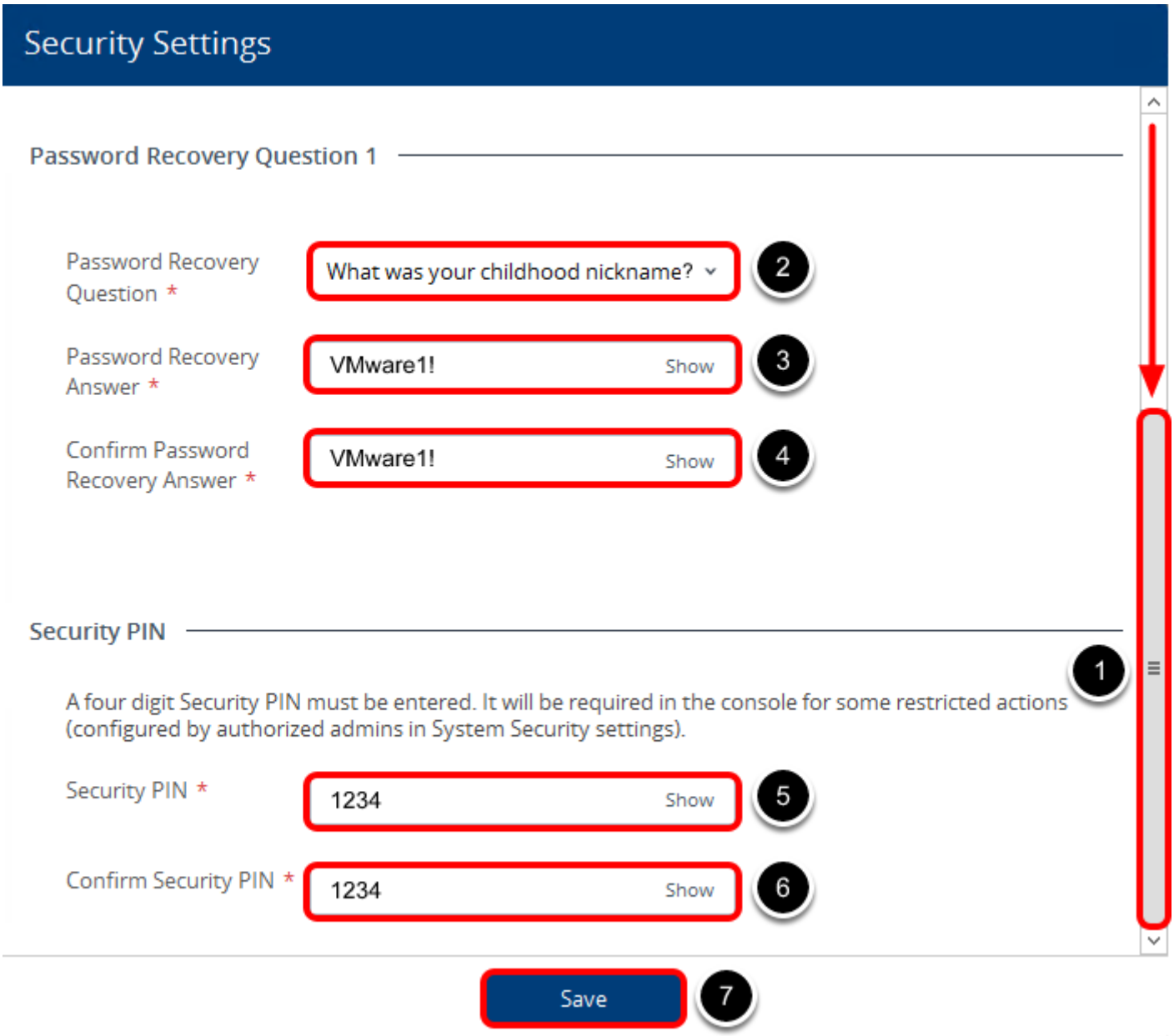
Accept the End User License Agreement



NOTE - The following steps of logging into the Administration Console will only need to be done during the initial login to the console.

You will be presented with the AirWatch Terms of Use. Click the **Accept** button.

Address the Initial Security Settings

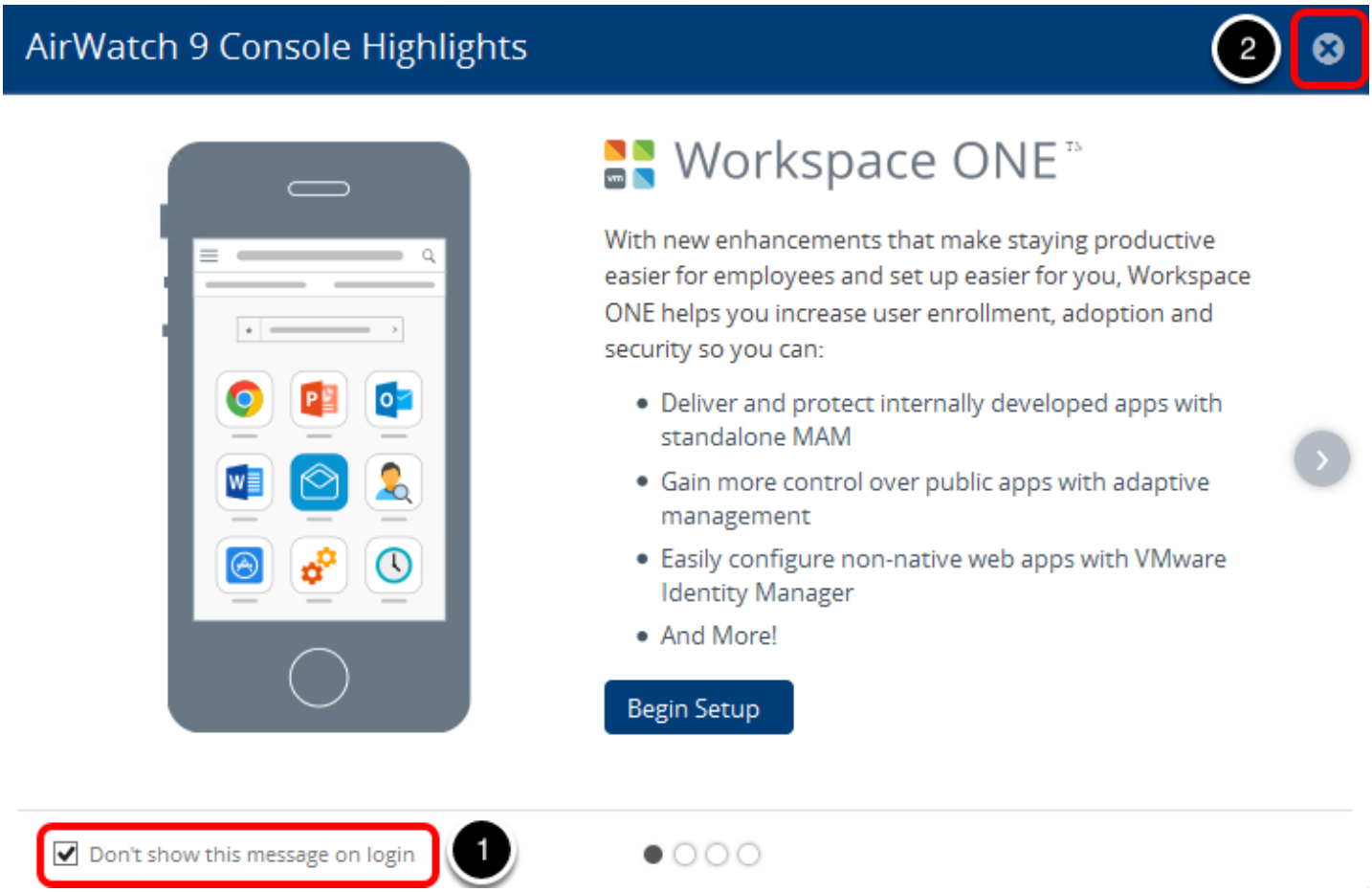


After accepting the Terms of Use, you will be presented with a **Security Settings** pop-up. The **Password Recovery Question** is in case you forget your admin password and the **Security PIN** is to protect certain administrative functionality in the console.

1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a **question** from the **Password Recovery Question** drop-down (default selected question is ok here).
3. Enter **"VMware1!"** in the **Password Recovery Answer** field.
4. Enter **"VMware1!"** in the **Confirm Password Recovery Answer** field.
5. Enter **"1234"** in the **Security PIN** field.
6. Enter **"1234"** in the **Confirm Security PIN** field.

7. Click the **Save** button when finished.

Close the Welcome Message



After completing the Security Settings, you will be presented with the AirWatch Console Welcome pop-up.

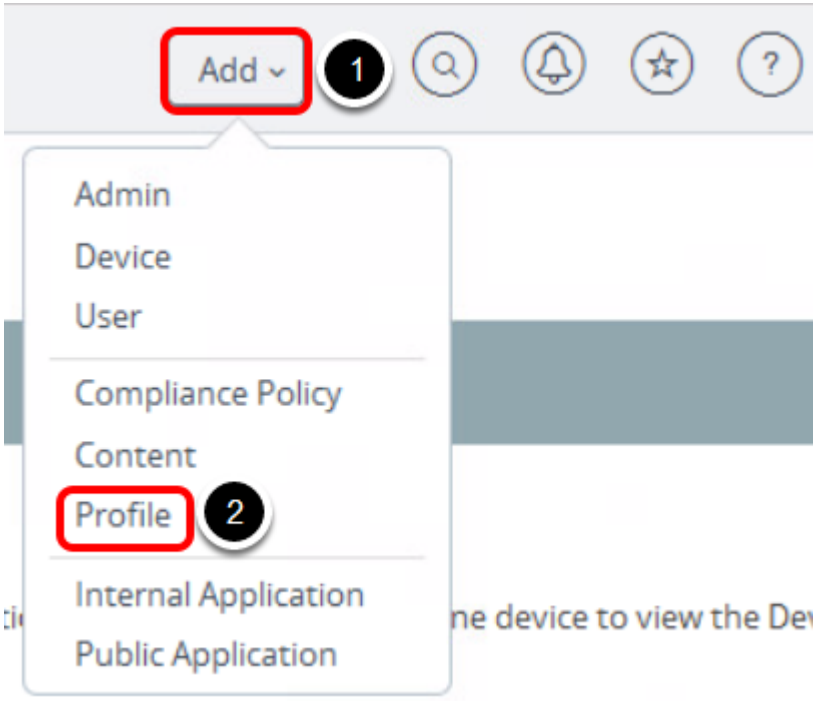
1. Click on the **Don't show this message again** check box.
2. Close the pop-up by clicking on the **X** in the upper-right corner.

Windows 10 Restriction Profile

Profiles allow you to modify how the enrolled devices behave. This section will walk you through how to configure and deploy a restriction profile that we can verify has applied to the device later in the module.

Continue to the next step.

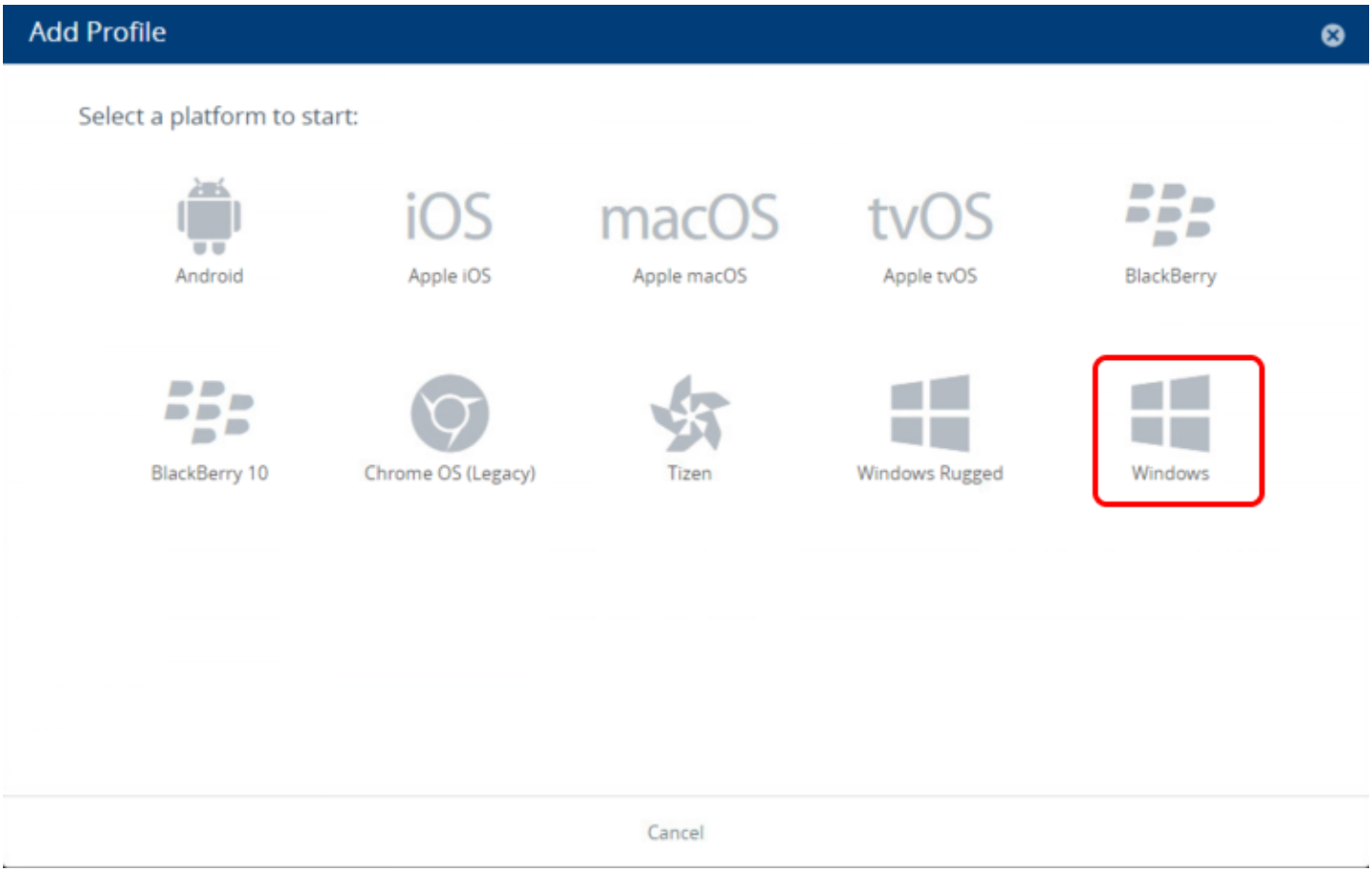
Create a Restriction Profile



In the top right corner of AirWatch console,

1. Click **Add.**
2. Click **Profile.**

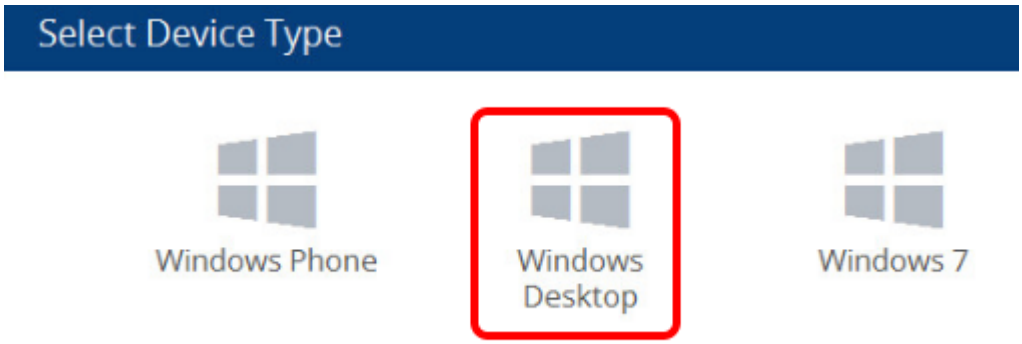
Add a Windows Profile



Click on the **Windows** icon.

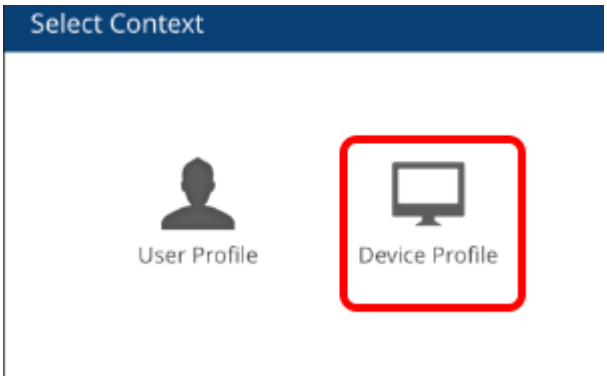
NOTE - Make sure that you are selecting Windows and NOT Windows Rugged.

Add a Windows Desktop Profile



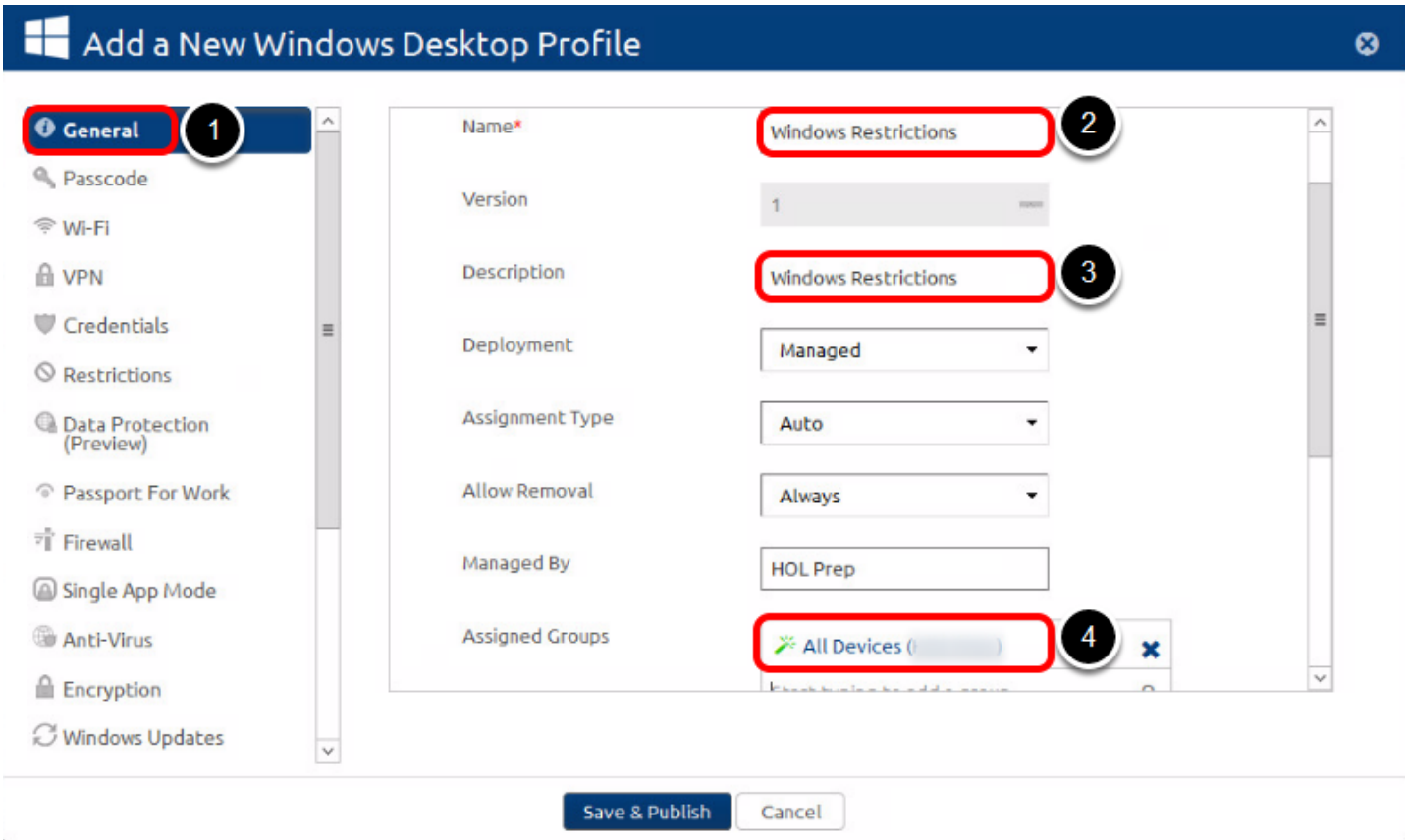
Click on **Windows Desktop**

Select Context - Device Profile



Click on **Device Profile.**

Define the General Settings

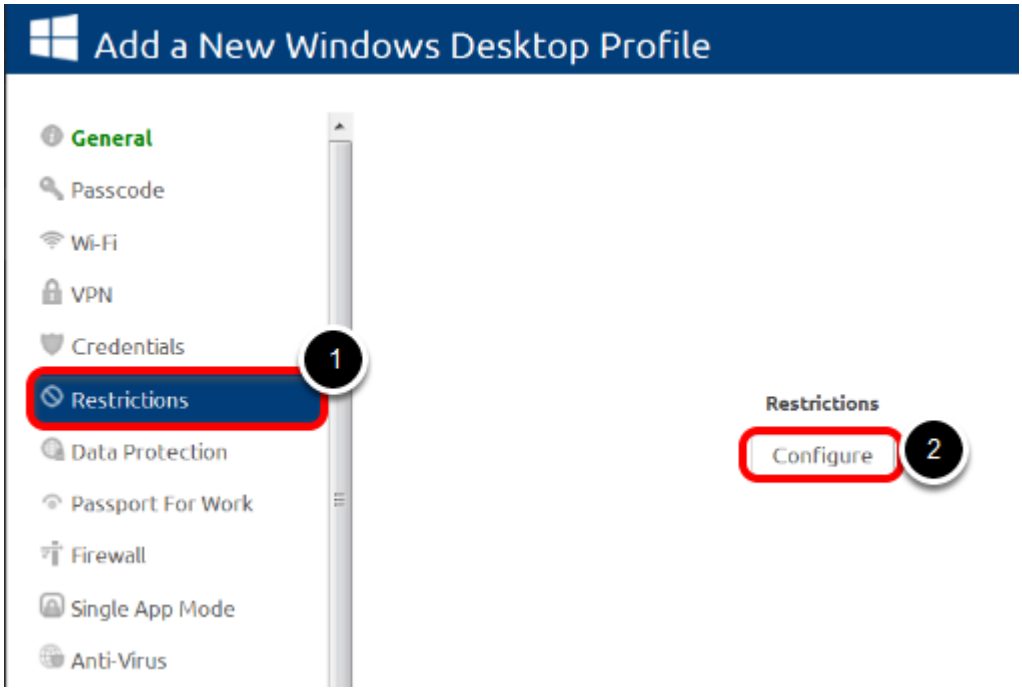


1. Click on **General** if it is not already selected.
2. Give the profile a name such as **"Windows Restrictions"** by entering the string the in the **Name** field.
3. Copy the profile name into the Description field.
4. Click in the **Assigned Groups** field. This will pop-up the list of created Assignment Groups. Click on the **All Devices** Assignment Group.
   NOTE - You may need to scroll down to view the Assigned Groups field.

NOTE - You do not need to click SAVE AND PUBLISH at this point. This interface allows you to move around to different payload configuration screens before saving.

Click to the NEXT STEP in the lab manual to continue configuration of the profile.

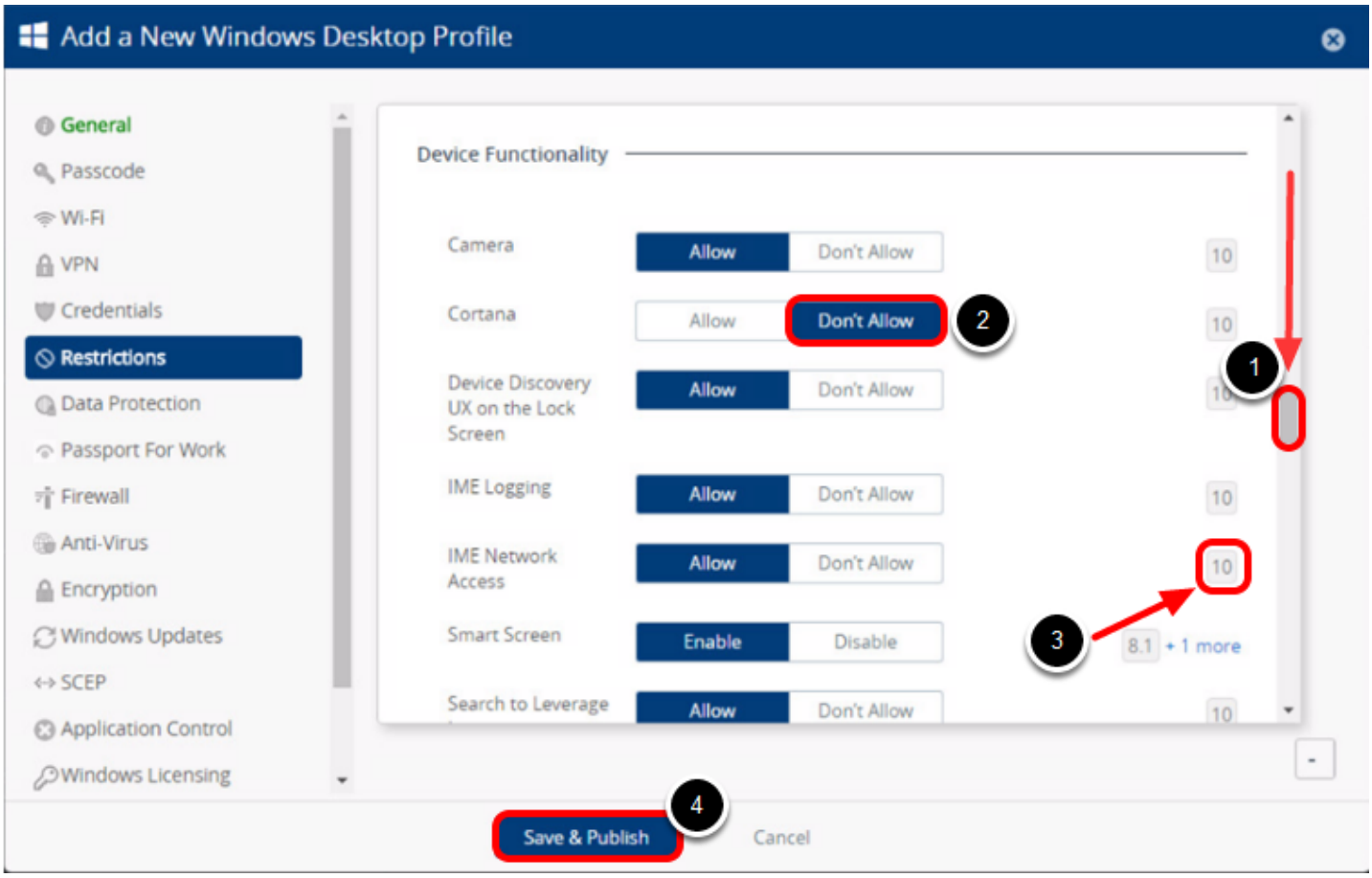
Select the Restrictions Payload



NOTE - When initially setting a payload, a "Configure" button will show to reduce the risk of accidentally setting a payload configuration.

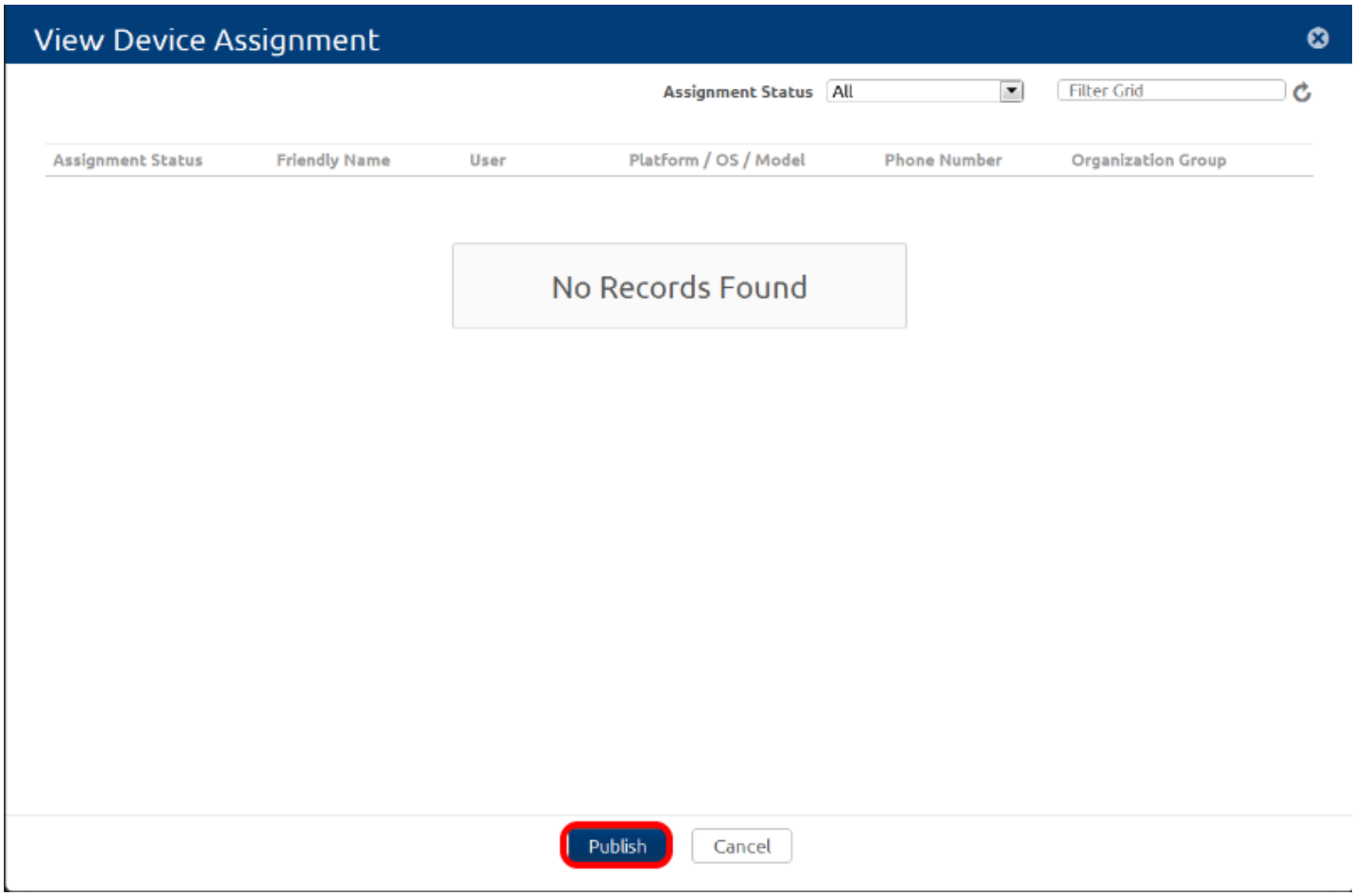
1. Click on the **Restrictions** payload in the Payload section on the left.
2. Click the **Configure** button to continue setting the Restrictions payload.

Adding a Restriction - Disable Cortana



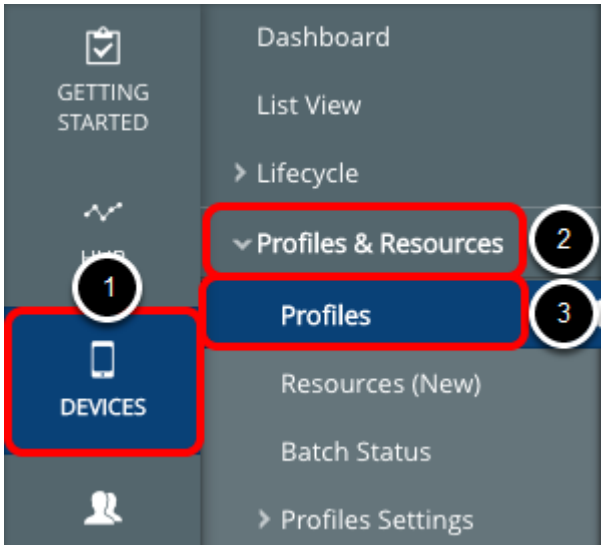
1. Using the scroll bar on the right, scroll down to the **Device Functionality** section.
2. Click on **Don't Allow** for **Cortana**
3. Notice the **10** on the right side of the Restrictions window. These are all the restrictions that AirWatch is able to apply to a Windows 10 computer.
4. Click **Save & Publish.**

Publish the Restrictions Profile



Click **Publish.**

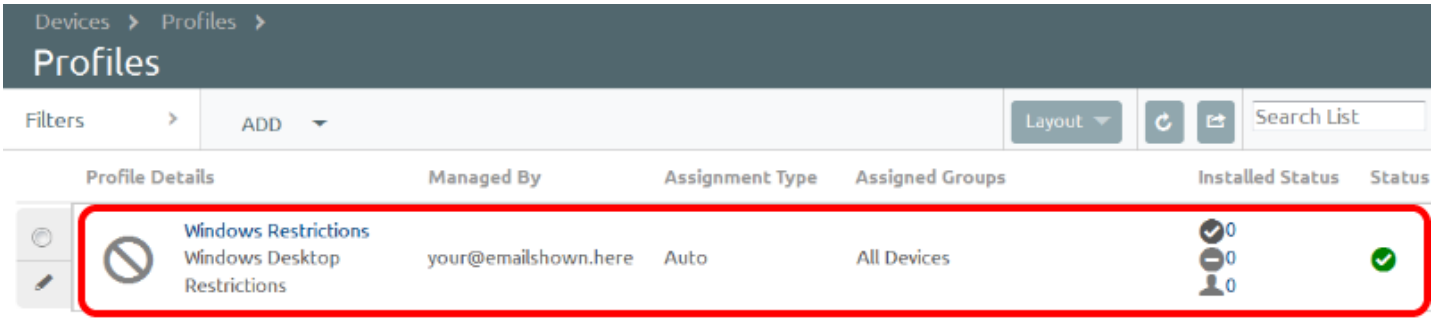
Navigate to Profiles List View



Now, from the left most column,

1. Click on **Devices.**
2. Click on **Profiles & Resources.**
3. Click on **Profiles.**

Verify the Restriction Profile Now Exists



You should now see your Restrictions Profile within the List View of the Devices Profiles window.

NOTE - If you need to edit the Restrictions Profile, this is where you would come back to in order to do so. To edit the profile, click the profile name then select "Add Version", make your changes and click "Save & Publish" to push the new settings to the assigned devices. Feel free to explore the options available and continue to the next step when you are prepared to end the Module.

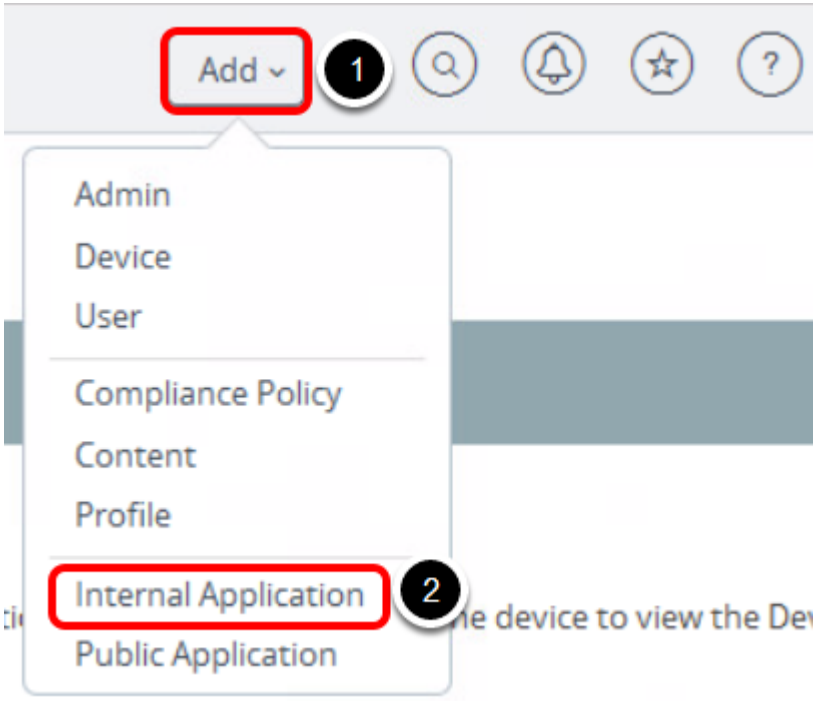
Windows 10 App Delivery

You can also distribute applications to Windows 10 devices, allowing for a seamless user experience. Continue to explore the process of creating and distributing an application to your Windows 10 device.

Create an Internal Application Profile

This exercise requires the 7-Zip installation program which is already downloaded and stored for you in the **Documents** folder.

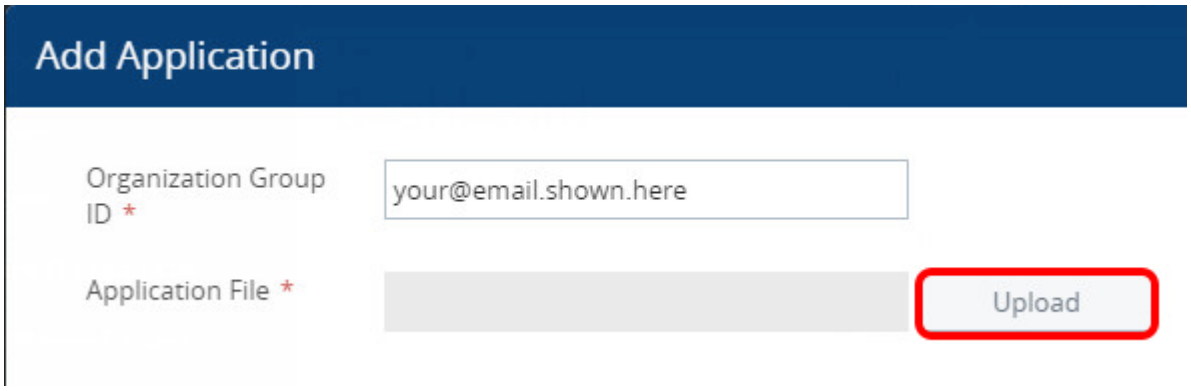
Add Internal Application



In the top-right corner of the AirWatch Console,

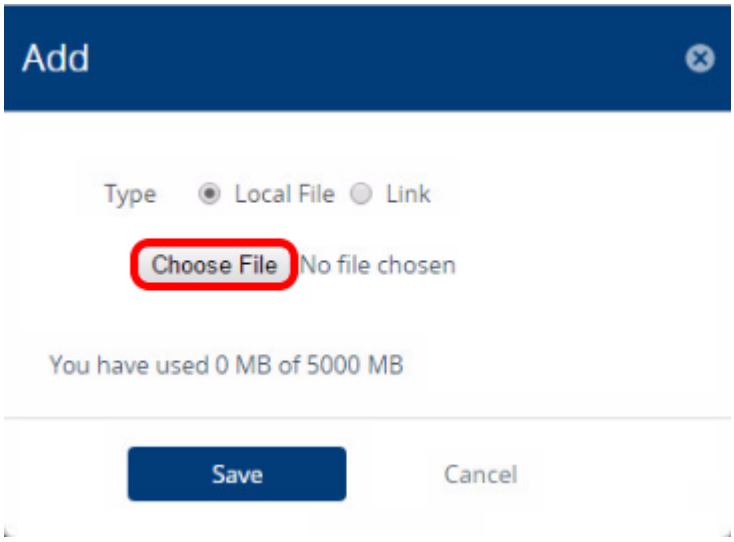
1. Click **Add.**
2. Click **Internal Application.**

Upload Application



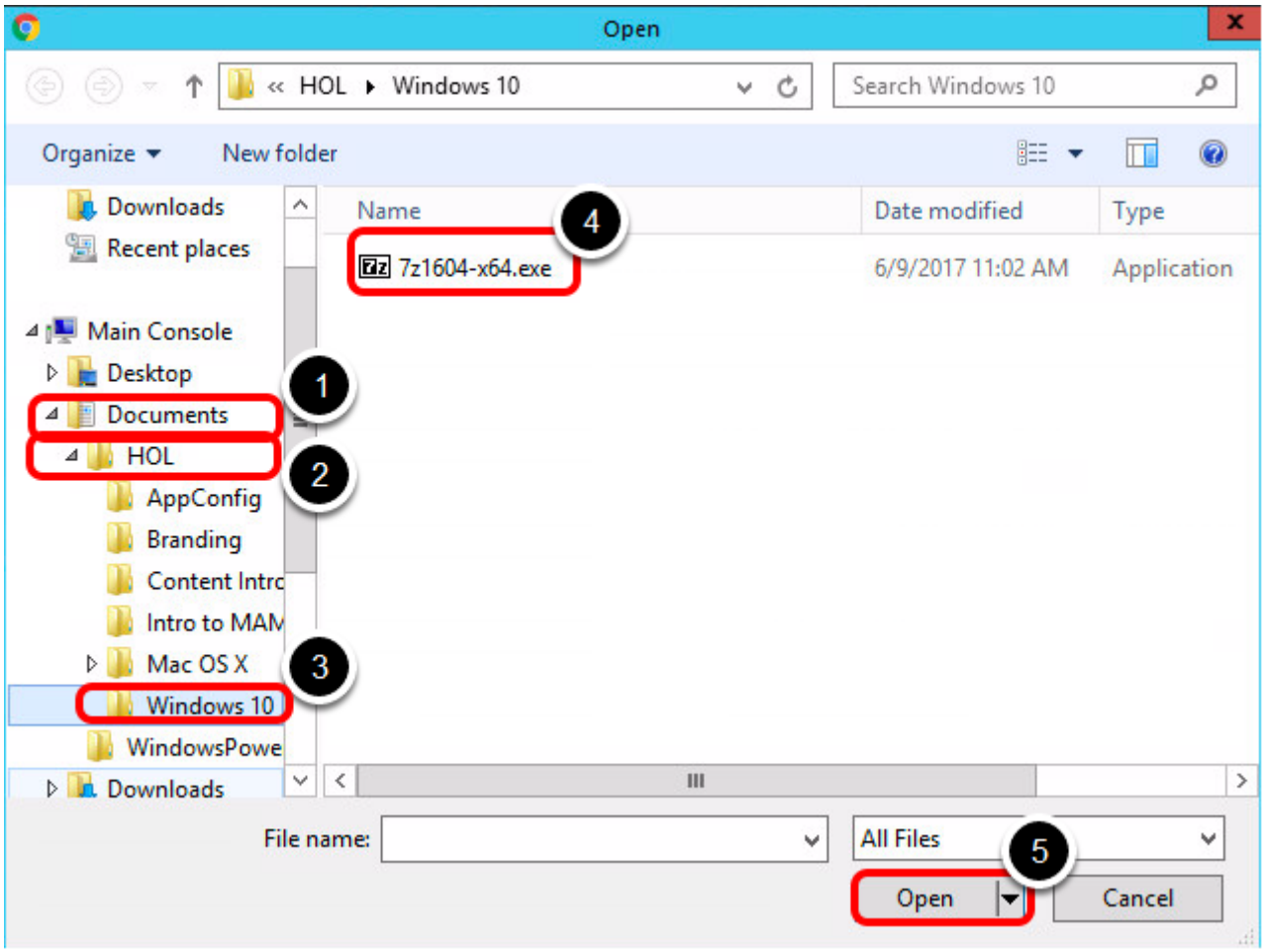
Click on **Upload.**

Find the Application MSI



Click on the **Choose File** button

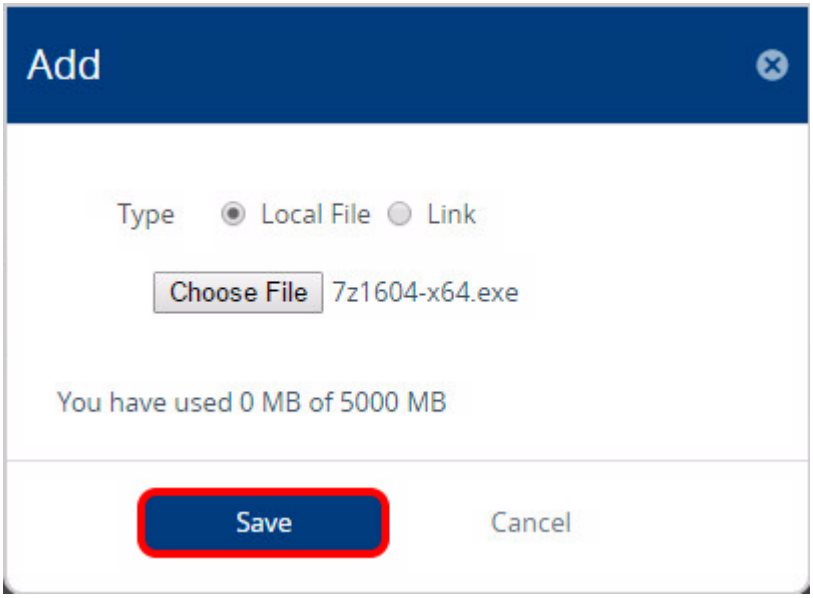
Upload the MSI File



The installation file for Google Chrome has already been downloaded to the server and placed in the **Documents** folder.

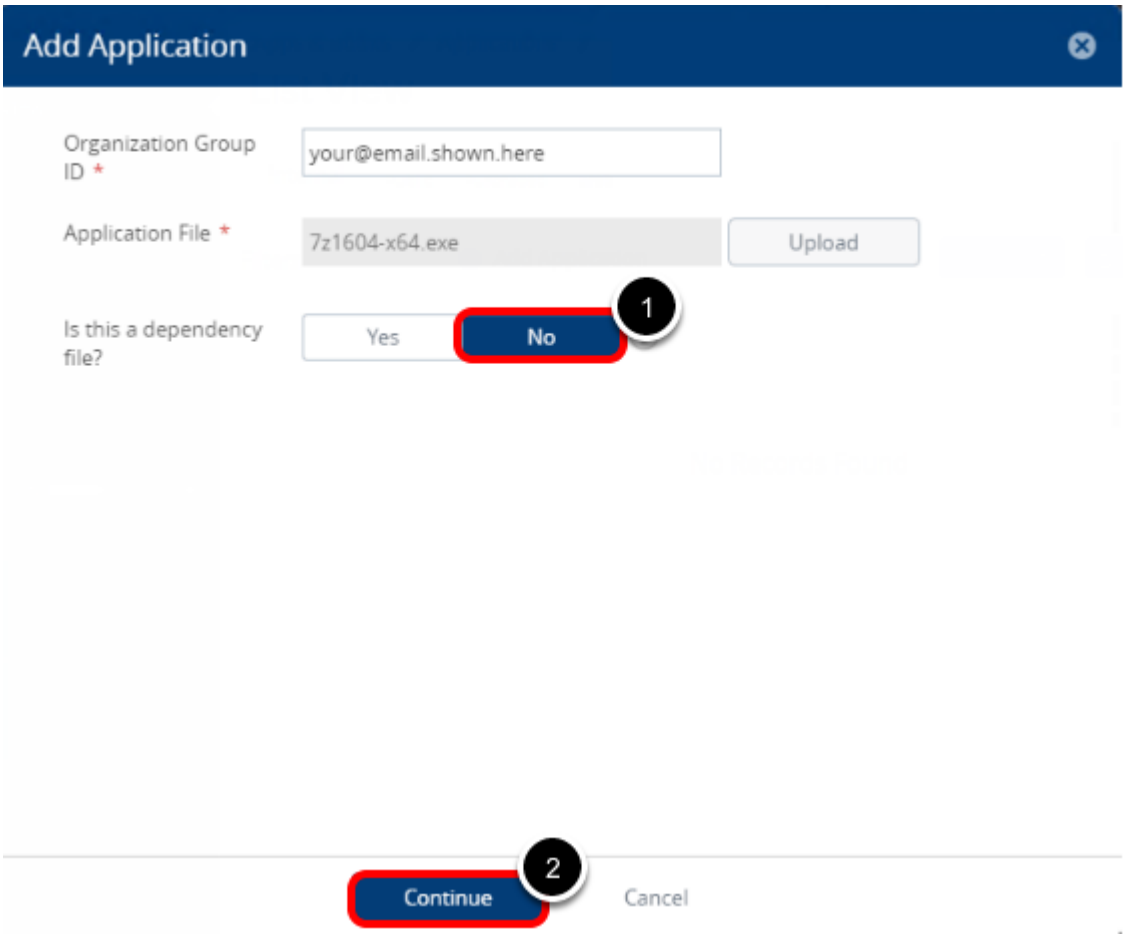
1. Click on **Documents.**
2. Expand **HOL.**
3. Click on Folder **Windows 10**.
4. Select **7z1604-x64.exe**
5. Click **Open.**

Saving the MSI File



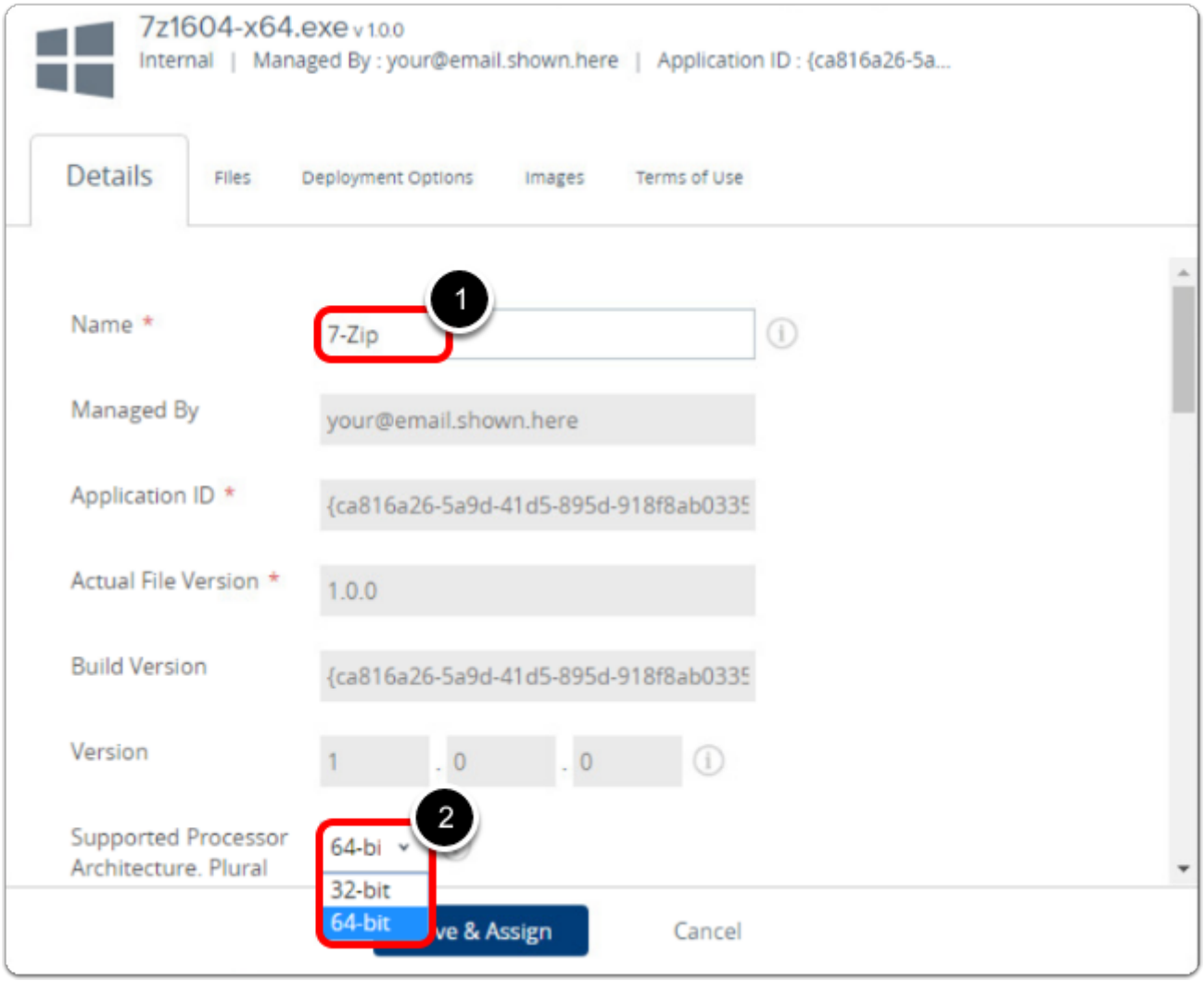
Click **Save.**

Continue to the App Settings



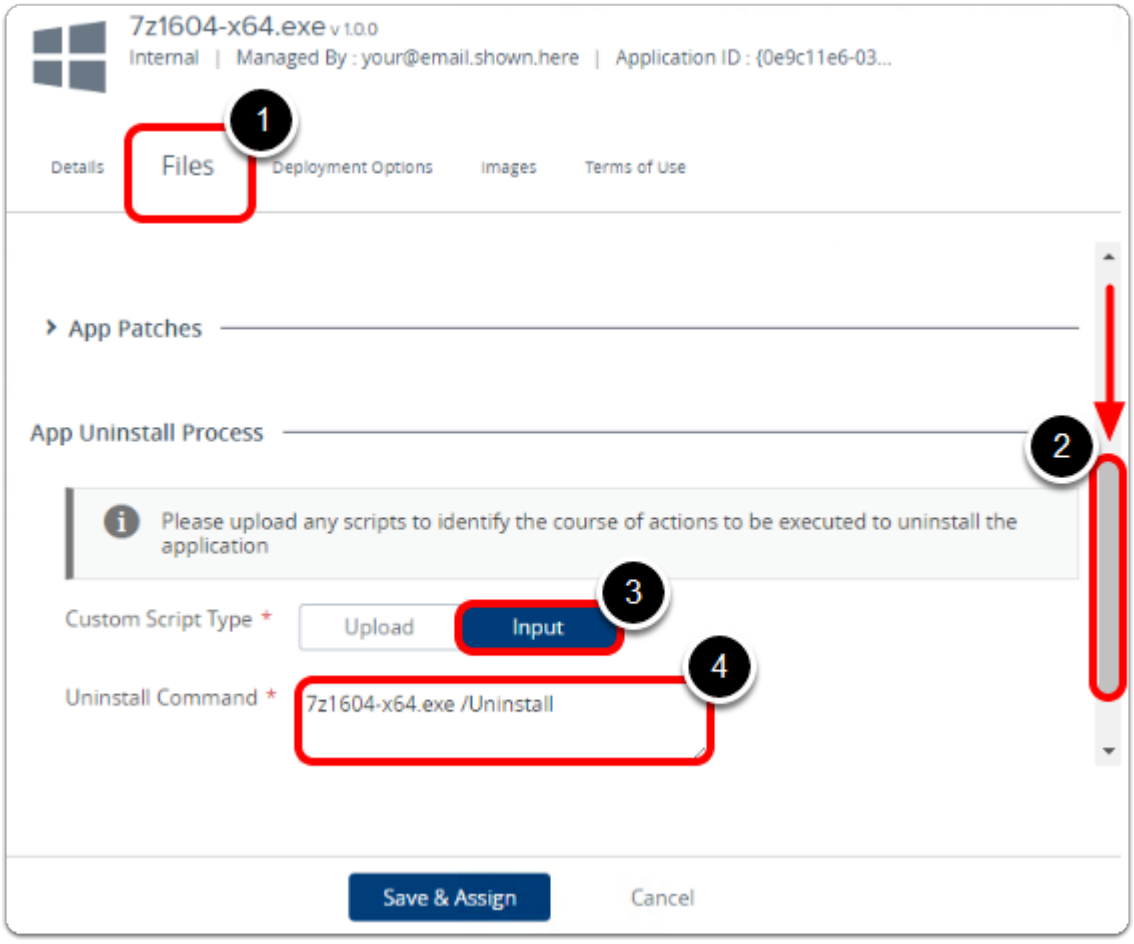
1. Click **No** for is this a dependency File
2. Click **Continue**

Configure App Details



1. Enter **"7-Zip"** for the **Name**.
2. Enter **"16.04"** for the **Actual File Version.**
3. Select **64-bit** for the **Supported Processor Architecture**.

Configure Application Files

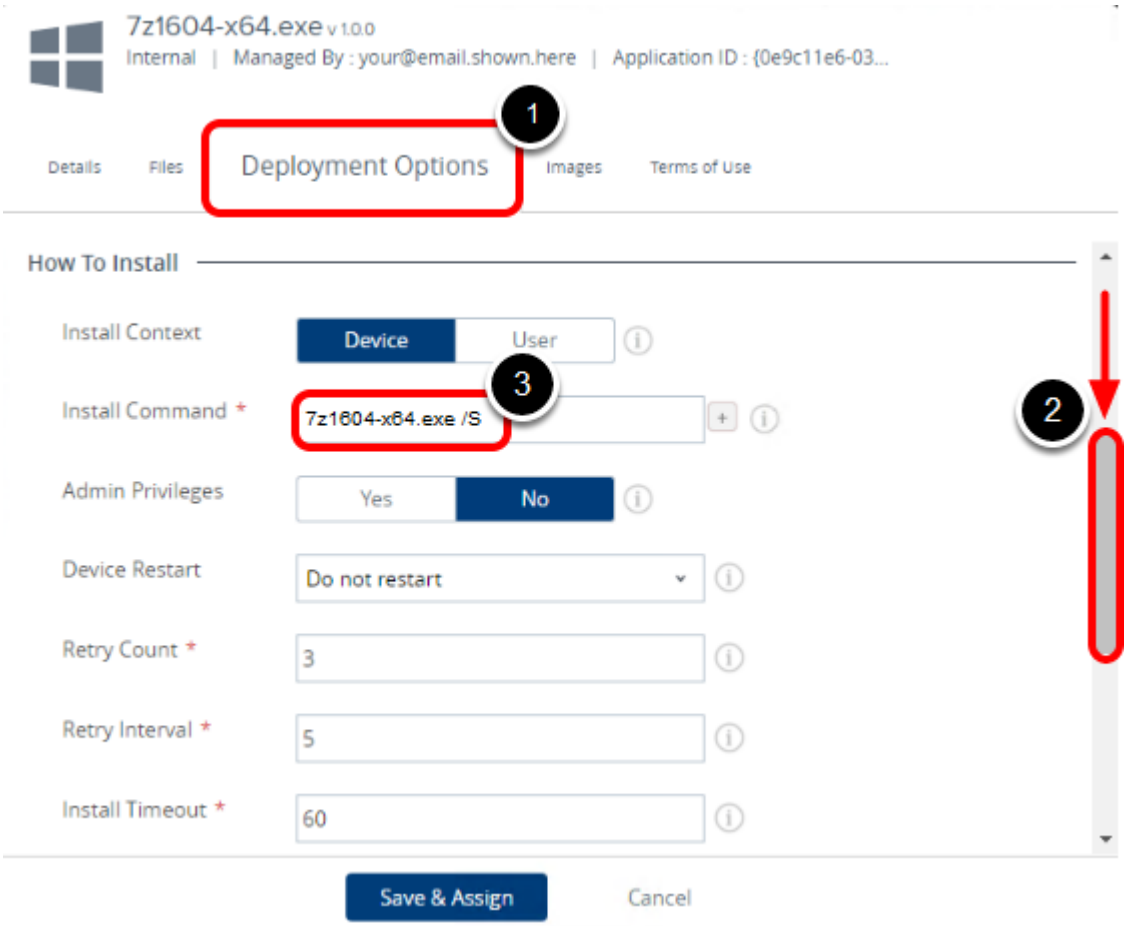


1. Click the **Files** tab.
2. Scroll down to find the **App Uninstall Process** section.
3. Select **Input** for the **Custom Script Type**.
4. Enter the following for **Uninstall Command**:

```
7z1604-x64.exe /Uninstall
```

NOTE - Please refer the Lab Guidance section in the beginning for how to copy text from manual to use in VLP.

Click on Deployment Options

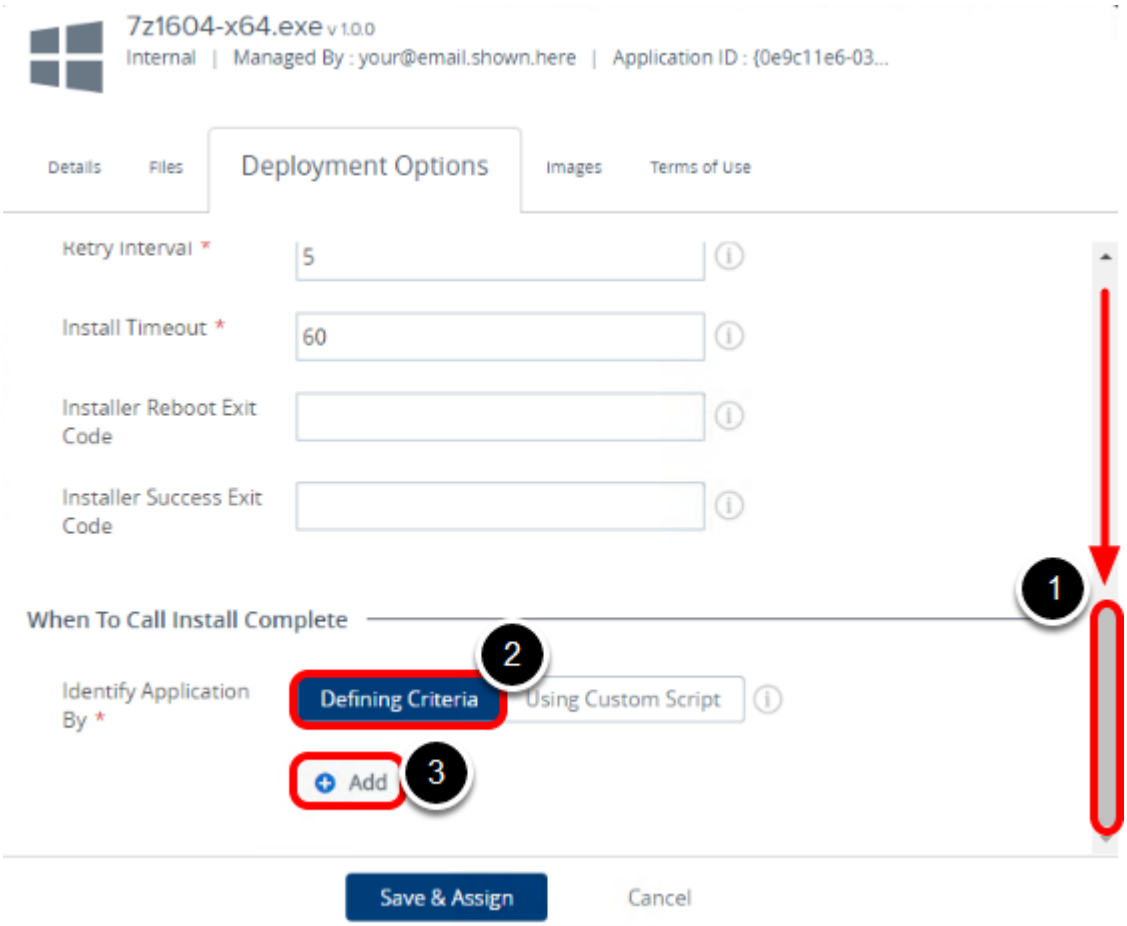


1. Click on **Deployment Options**
2. Scroll down until you see the option for **Install Command**
3. Type **Install Command** as:

```
7z1604-x64.exe /S
```

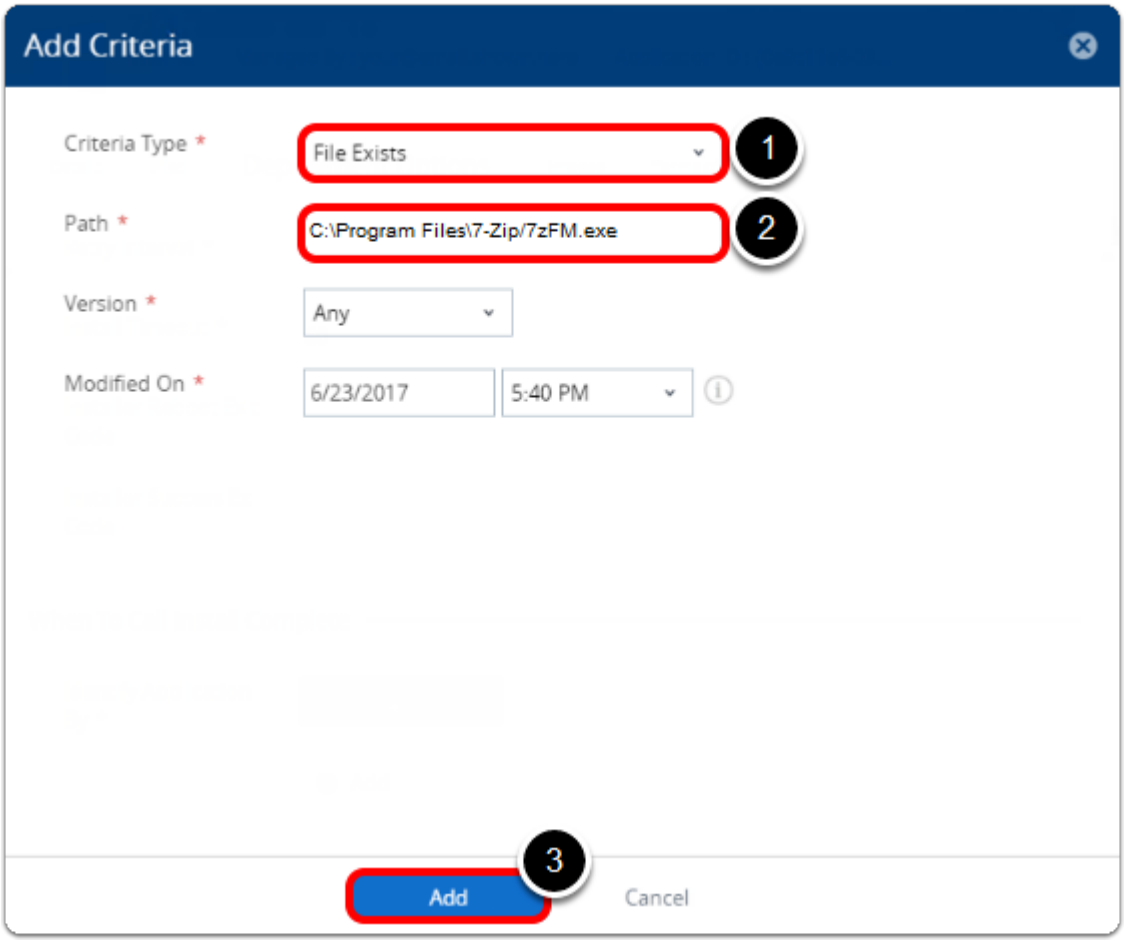
NOTE - Please refer the Lab Guidance section in the beginning for how to copy text from manual to use in VLP.

Add Identify Application Condition



1. Scroll down to find the **When To Call Install Complete** section.
2. Select **Defining Criteria** for the **Identity Application By** field.
3. Click **Add**.

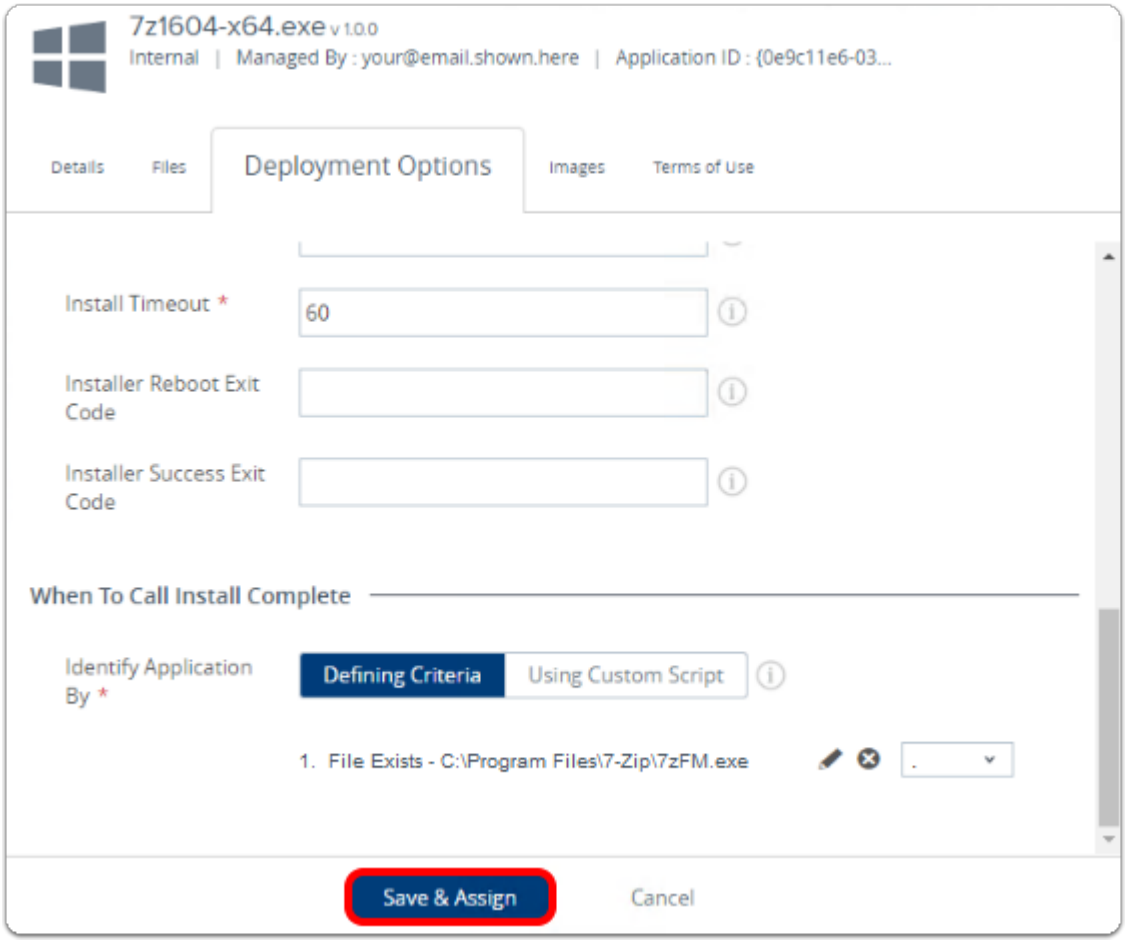
Configure the Install Complete Defining Criteria



1. Select **File Exists** for the **Criteria Type**.
2. Enter **"C:\Program Files\7-Zip\7zFM.exe"** for the **Path**.
3. Click **Add**.

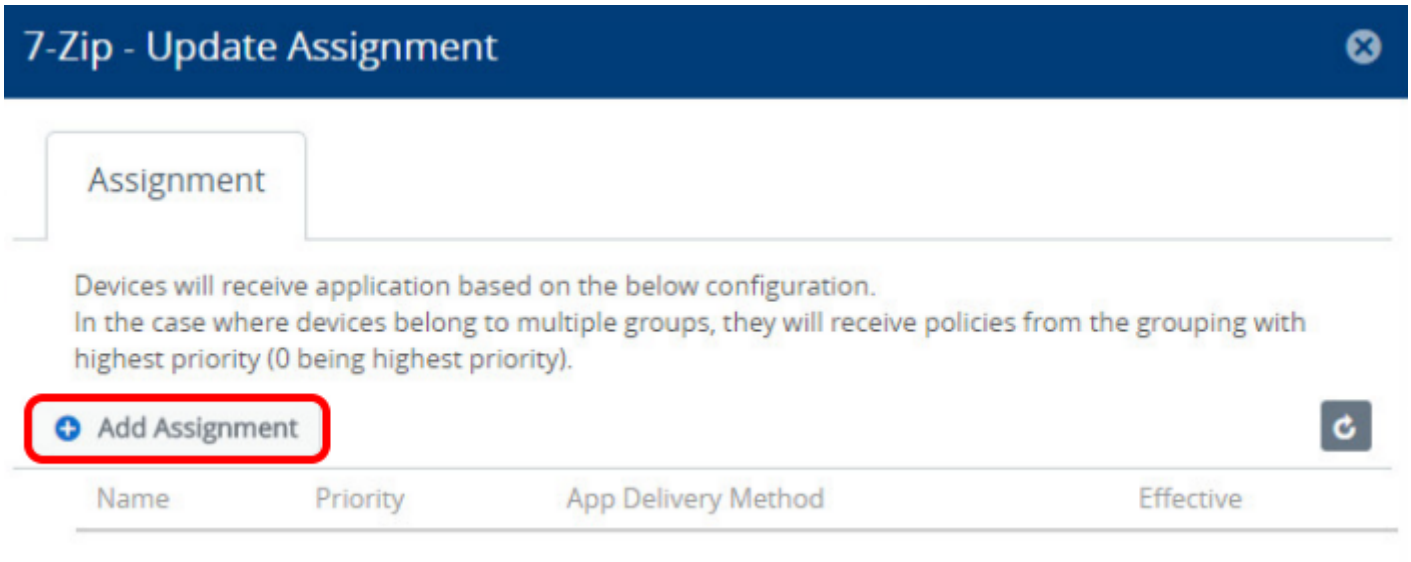
NOTE - Please refer the Lab Guidance section in the beginning for how to copy text from manual to use in VLP.

Save and Assign the Application



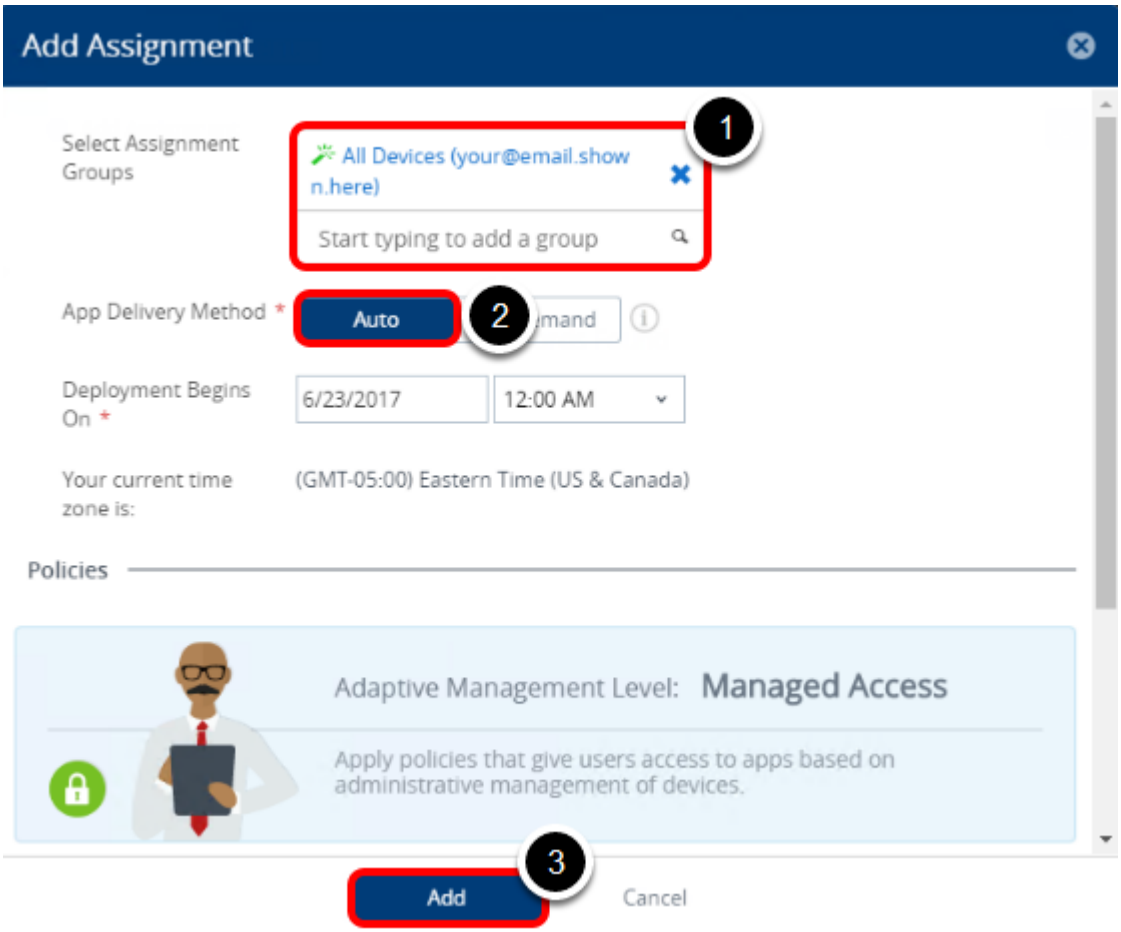
Click **Save & Assign**.

Add an Assignment



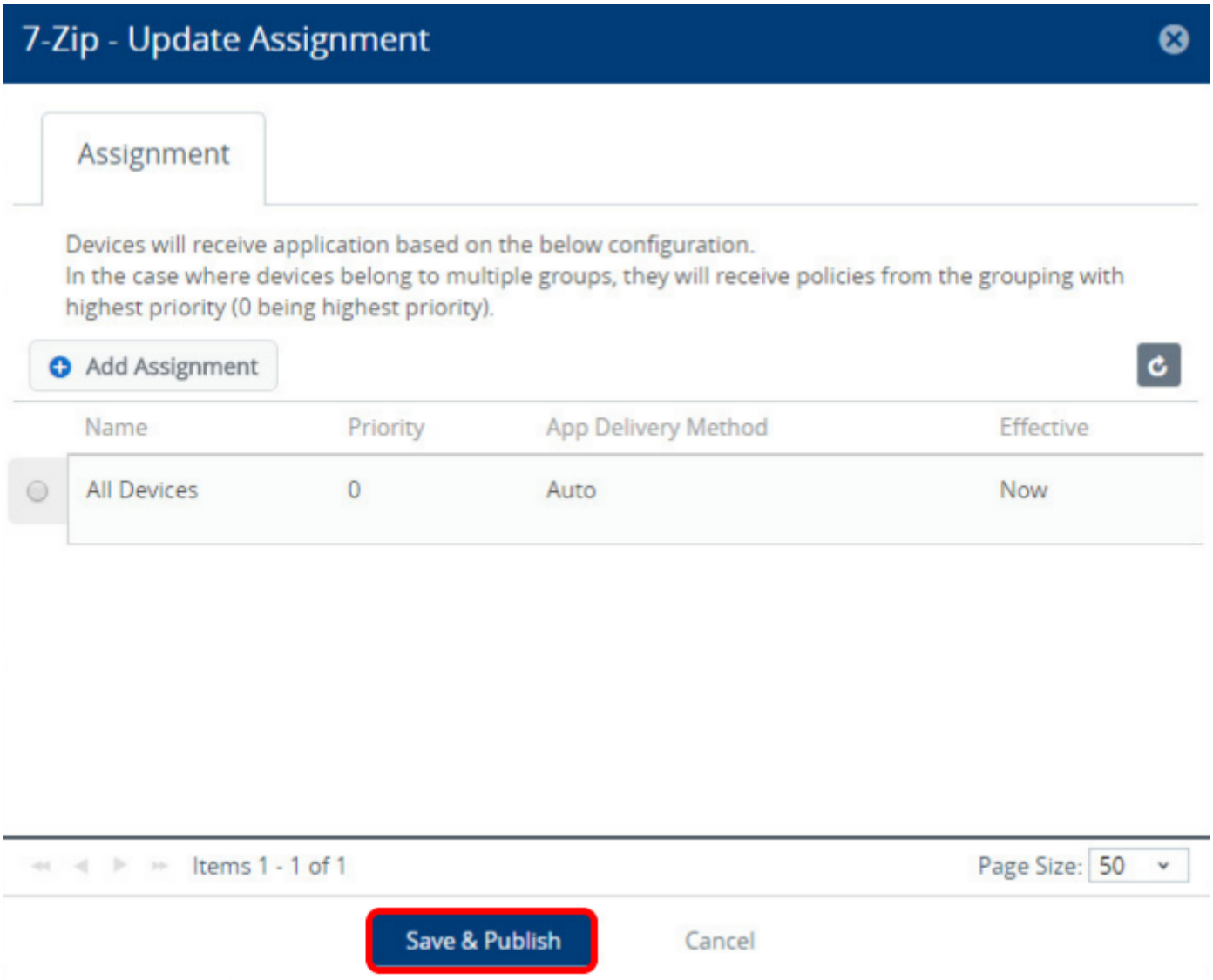
Click **Add Assignment.**

Add Assignment Group and Push Mode



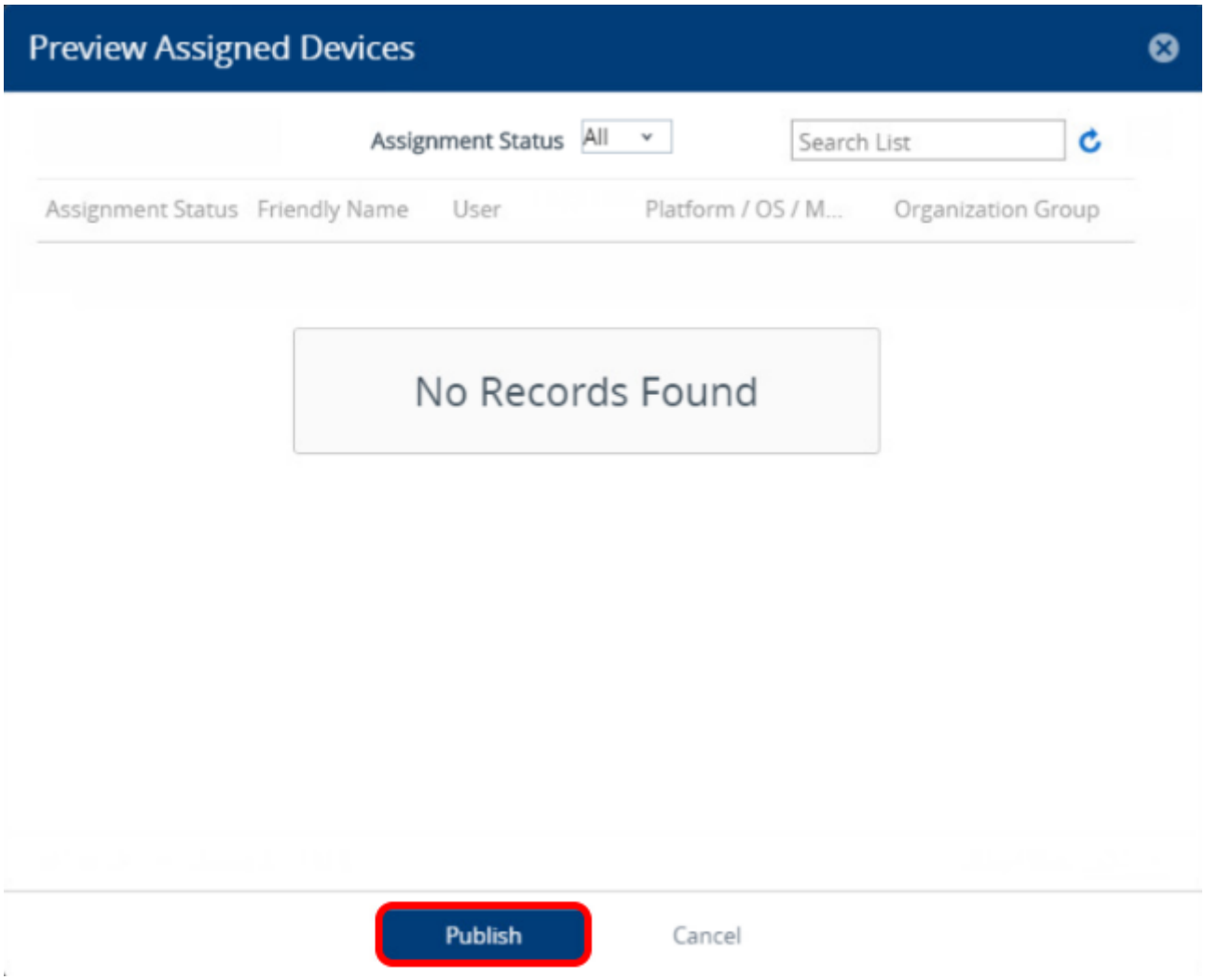
1. Click the **Select Assignment Groups** search box and select **All Devices (your@email.shown.here)**.
2. Select **Auto** for the **App Delivery Method.**
3. Click **Add.**

Save and Publish the Application



Click **Save & Publish**

Preview the Assigned Devices



Click **Publish**

Windows 10 Work Access Enrollment

Device enrollment establishes the initial communication with AirWatch to enable Enterprise Mobility Management (EMM). The enrollment methods for Windows Desktop focus on adding features and functionality depending on how devices are enrolled.

All Windows Desktop enrollments use the native enterprise management app to complete the enrollment process. Windows Auto-Discovery is an optional method of enrolling devices that only requires the end-user's email address to begin the enrollment process.

Enrollment can also require the enabling (console checkbox) of the AirWatch Protection Agent. This agent adds endpoint security to your Windows Desktop devices to ensure your data and devices remain secure wherever the device may go. The AirWatch Protection Agent for Windows Desktop co-opts the native Windows Desktop functionality such as BitLocker encryption, Windows Firewall, and Windows Automatic Updates to keep devices secure and up-to-date.

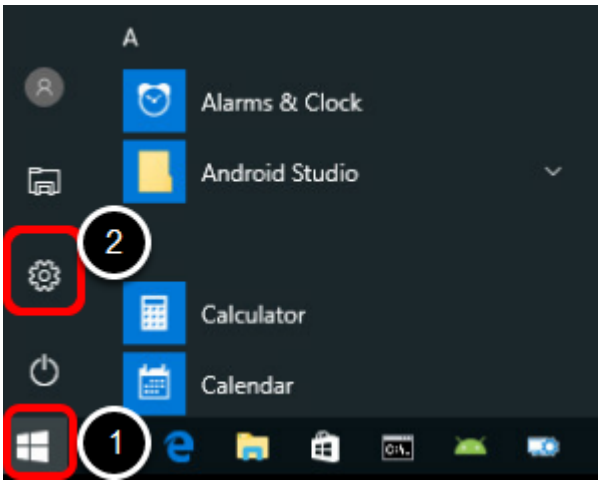
Work Access Enrollment

This section will guide you through how to enroll your Windows 10 device through work access enrollment.

Launch Windows 10 VM

From Main Console Desktop, launch RDP session for Windows 10 VM labeled **Win10-01.rdp**.

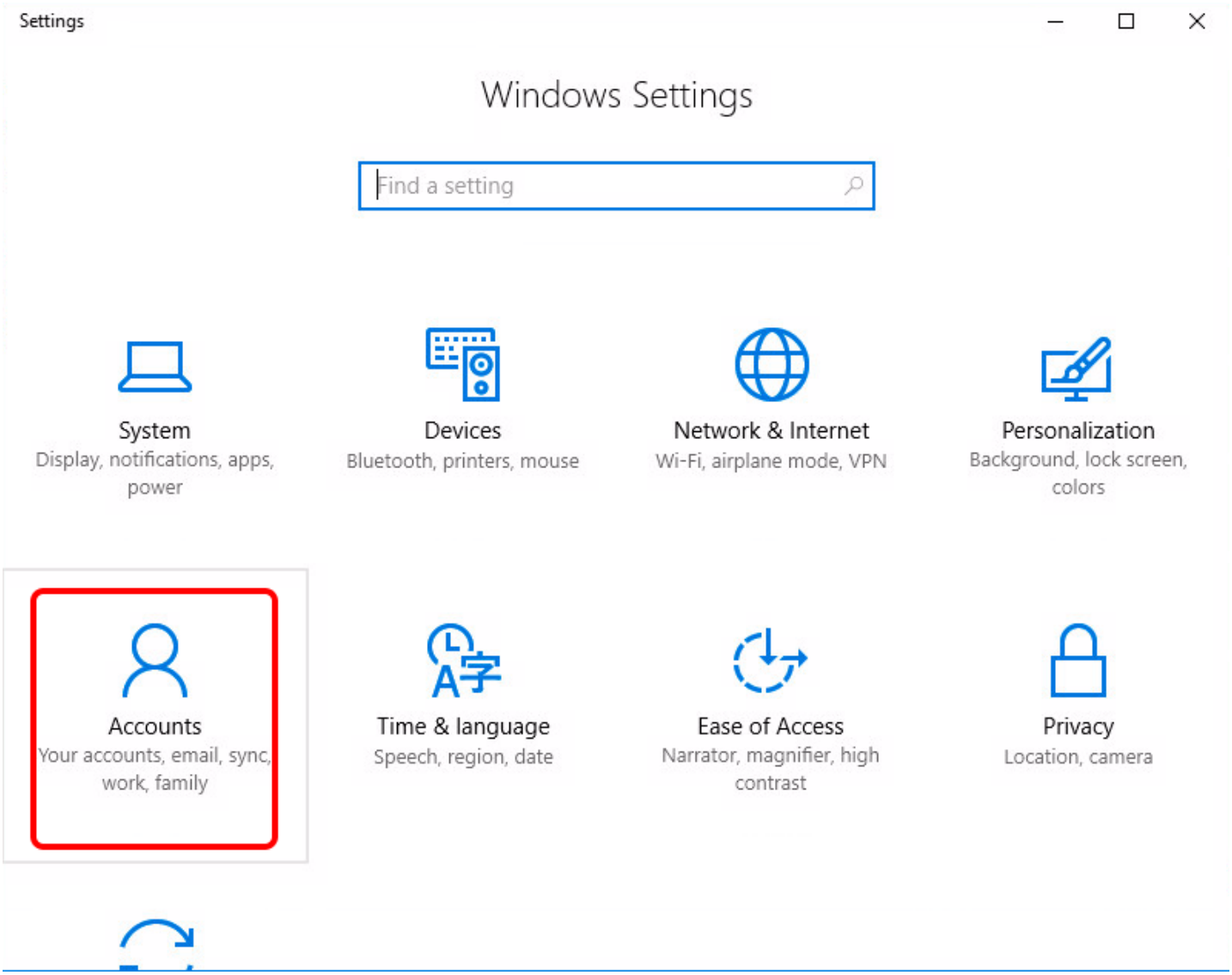
Launching Settings



On the Win 10 VM,

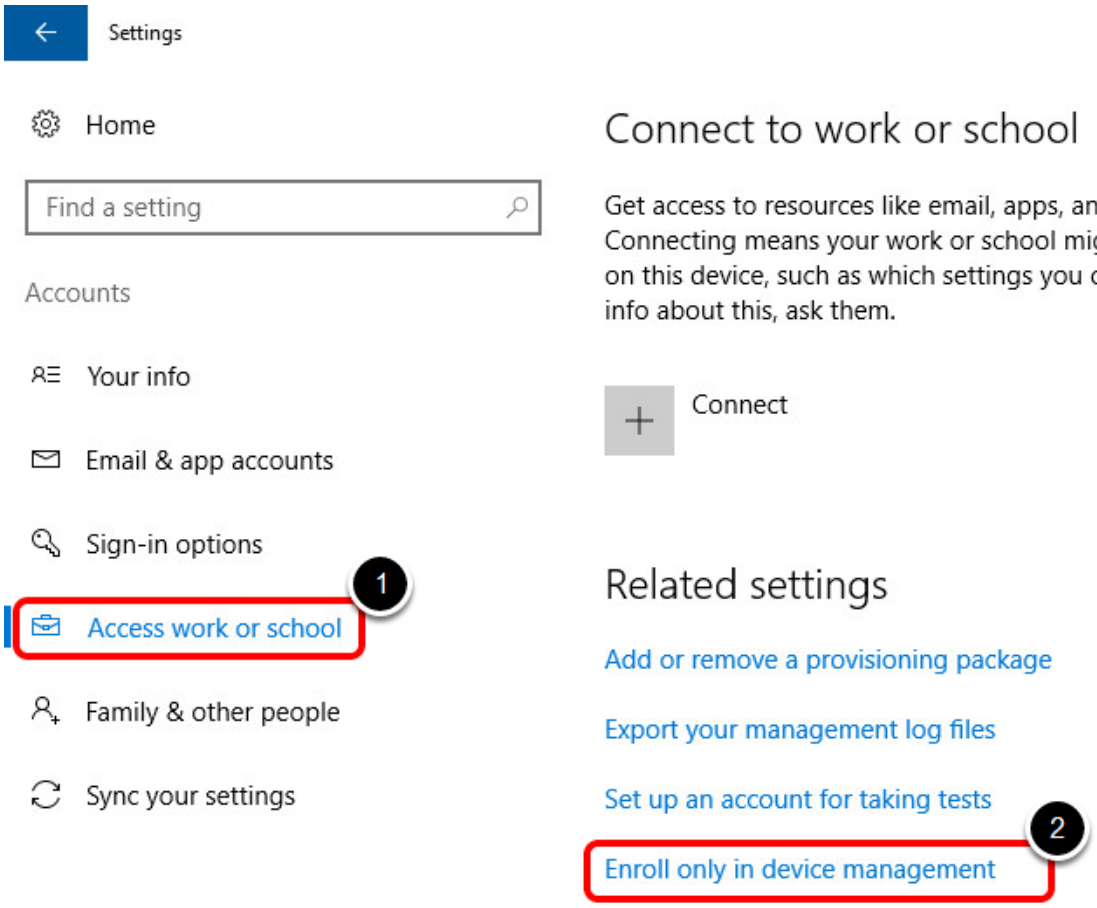
1. Click on **Start** logo
2. Click on **Settings** icon

Accessing Accounts



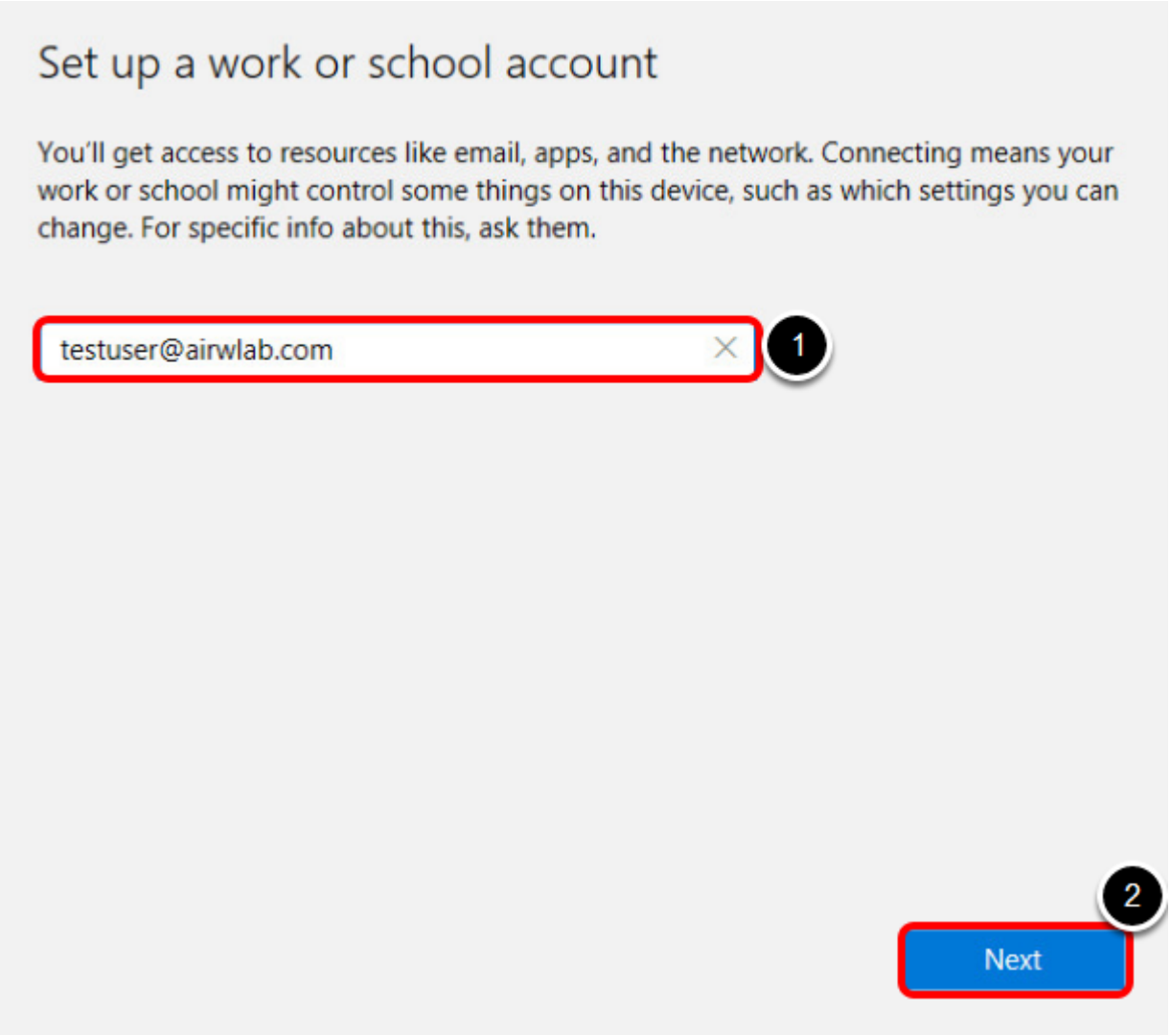
Click on the **Accounts** icon.

Access Work or School



1. Click on **Access work or school.**
2. Click on **Enroll only in device management.**

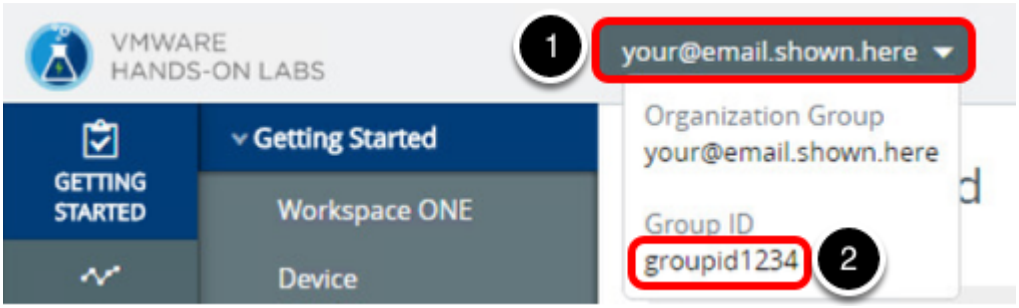
Connecting to Windows Auto Discovery Service



For the workshop we will be using a static email address. This is **NOT** your email address that you used to login to the lab environment. The reason for this is that there is a Windows Auto-Discovery Service (WADS) setup for this email domain which will point your device to the AirWatch Hands-On-Lab environment that was specifically created for this event. Normally, your user community would enter their corporate email address which would then point their device to your AirWatch environment. If you choose not to use a WADS server then the user would be forced to enter the enrollment URL manually.

1. Enter the email address "**testuser@airwlab.com**"
2. Click on the **Next** button.

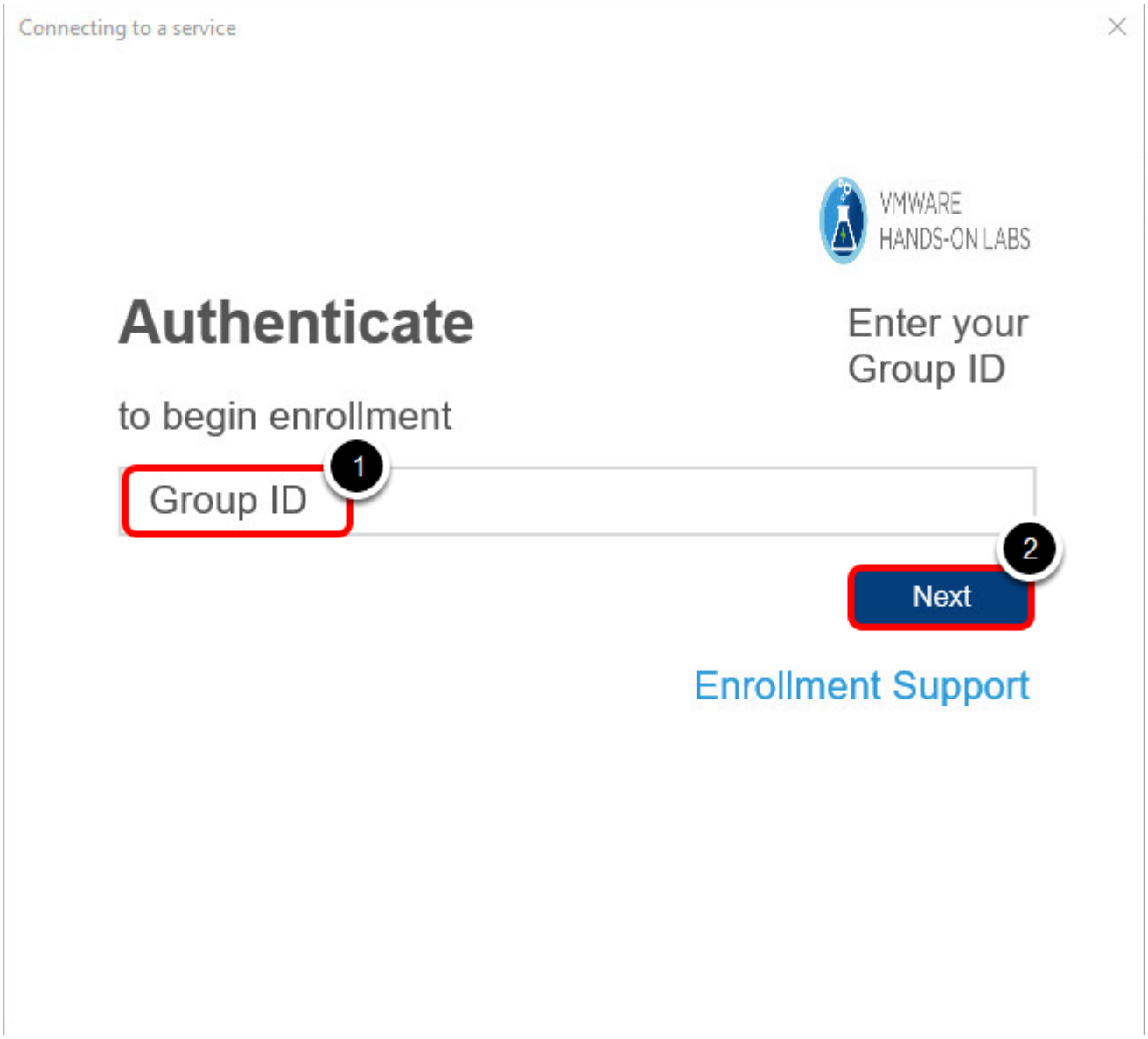
Find your Group ID from AirWatch Console



1. To find the Group ID, hover your mouse over the Organization Group tab at the top of the screen. Look for the email address you used to log in to the lab portal.
2. Your **Group ID** is displayed at the bottom of the Organization Group pop up.

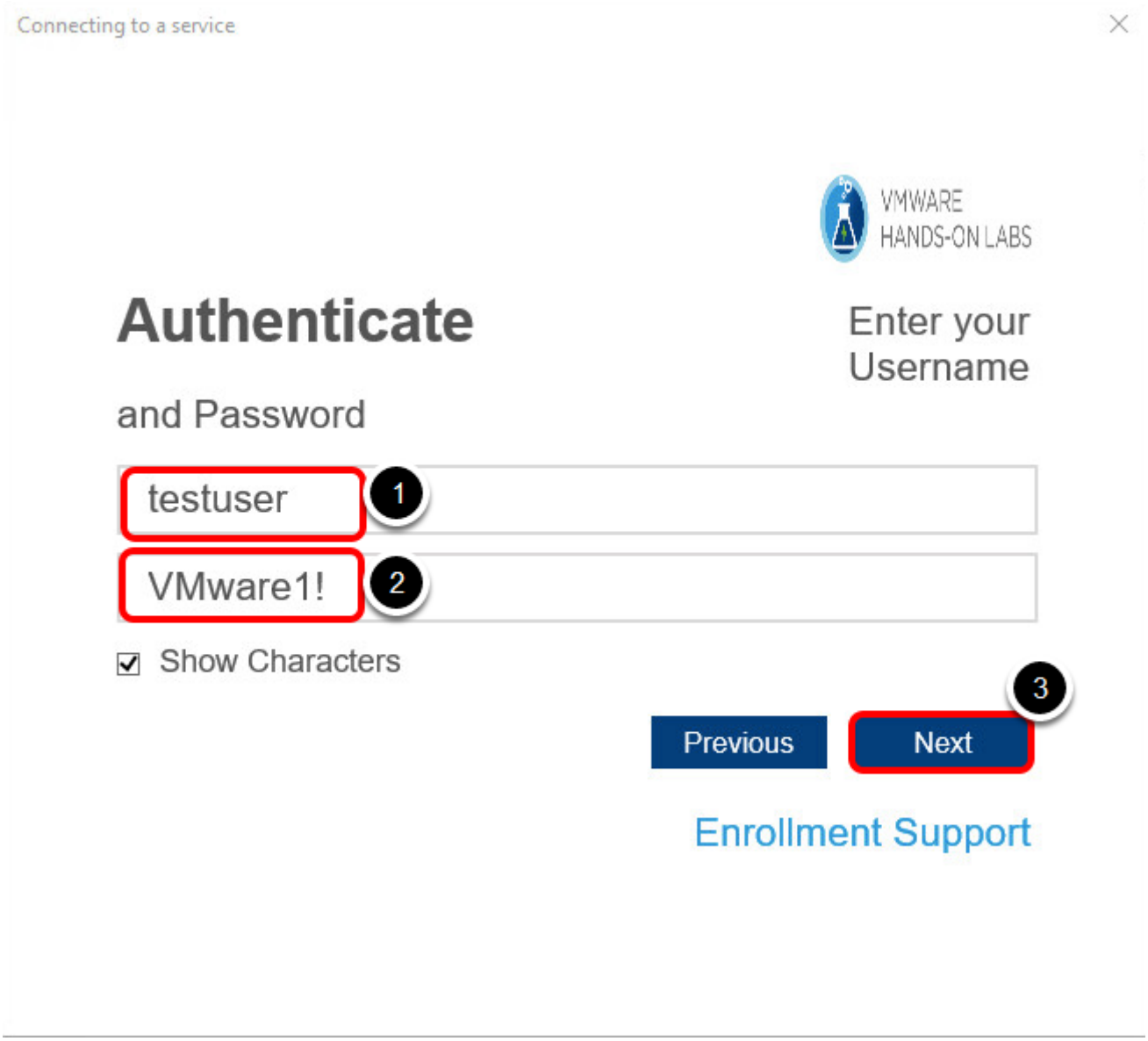
***NOTE* - The Group ID is required when enrolling your device in the following steps.**

Group ID



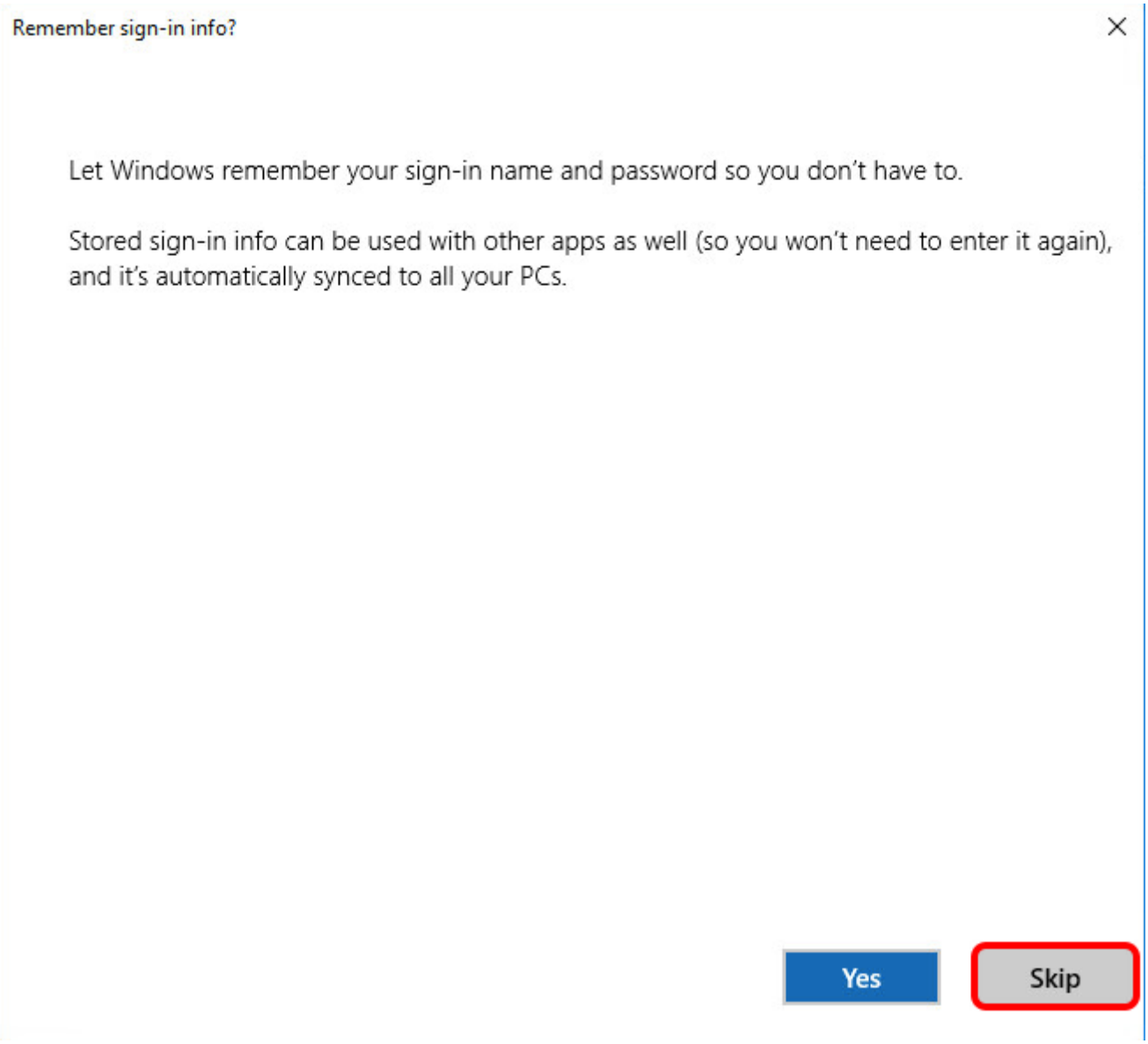
1. Enter the Group ID from the beginning of this section in the **Group ID** field.
2. Click **Next.**

Username and Password



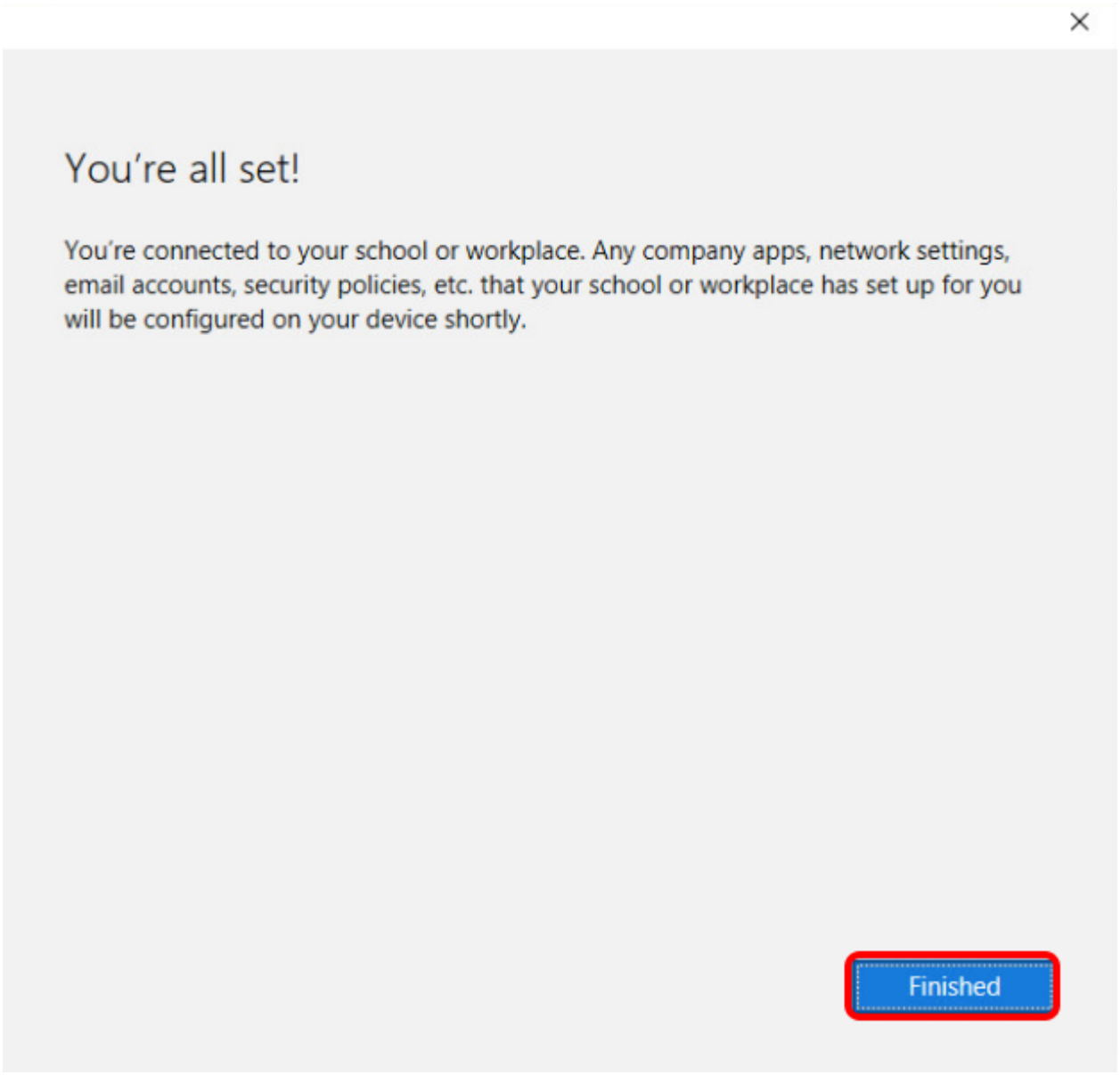
1. Enter the "**testuser**" in the **Username** field
2. Enter the "**VMware1!**" in the **Password** field
3. Click **Next.**

Remember Sign-In Info



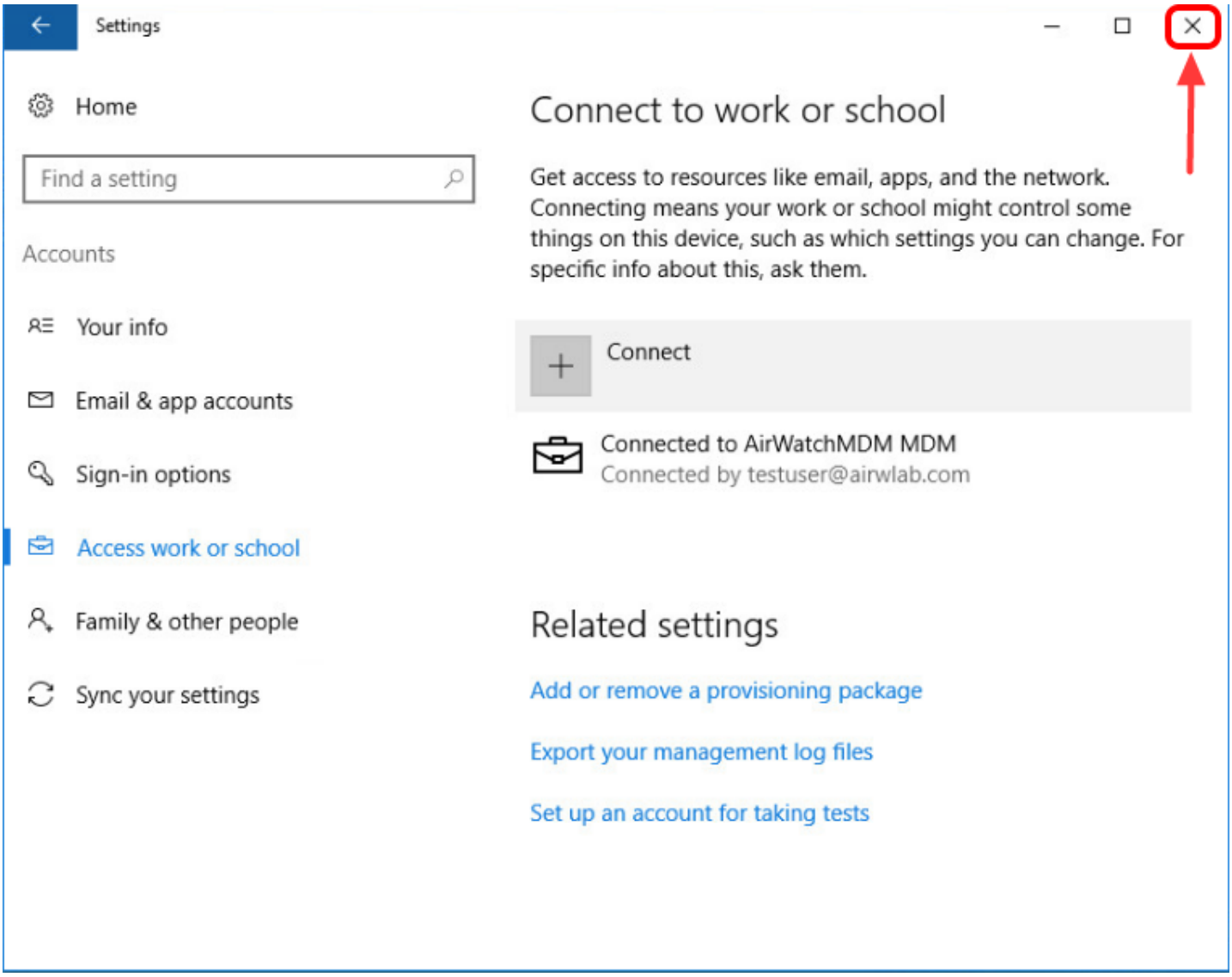
Click **Skip** to not remember sign-in info.

Complete Enrollment



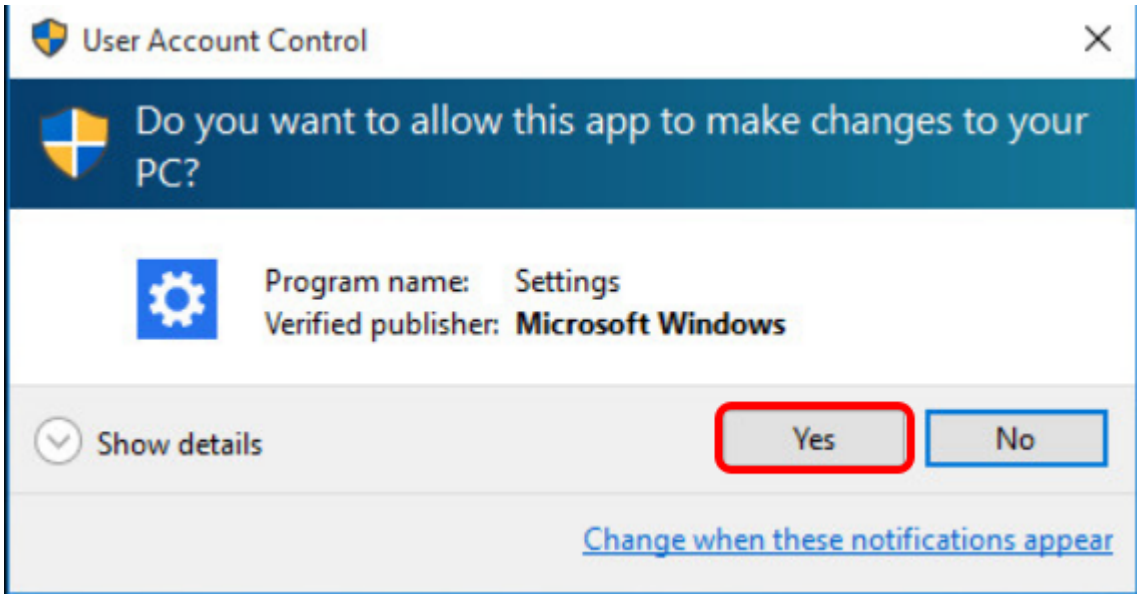
Click **Finished.**

Close Settings



Close the Settings page by clicking on the **X** in the upper right corner.

Allowing Application to Make Changes

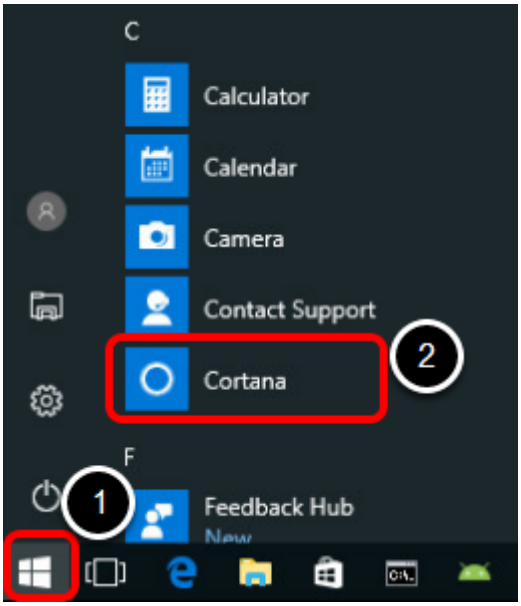


You may be prompted by User Account Control (UAC) to allow the app to make changes to your PC. If so, click **Yes**.

Confirm MDM Enrollment

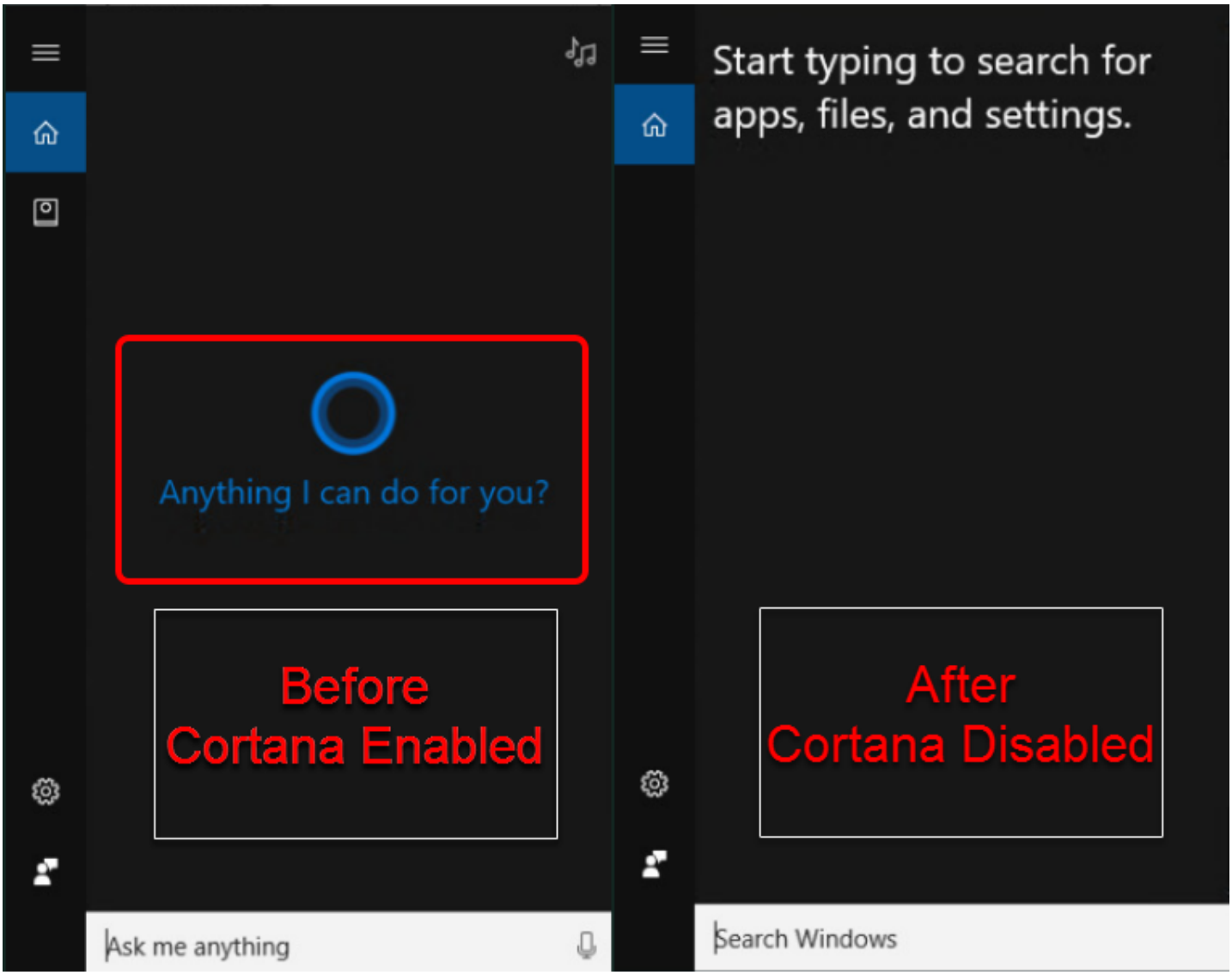
Once your Windows 10 device is enrolled, the restriction profile you created earlier will be installed on the device. Continue to confirm enrollment was successful and that the profile installed correctly by verifying that the restrictions took place on your device.

Selecting Cortana



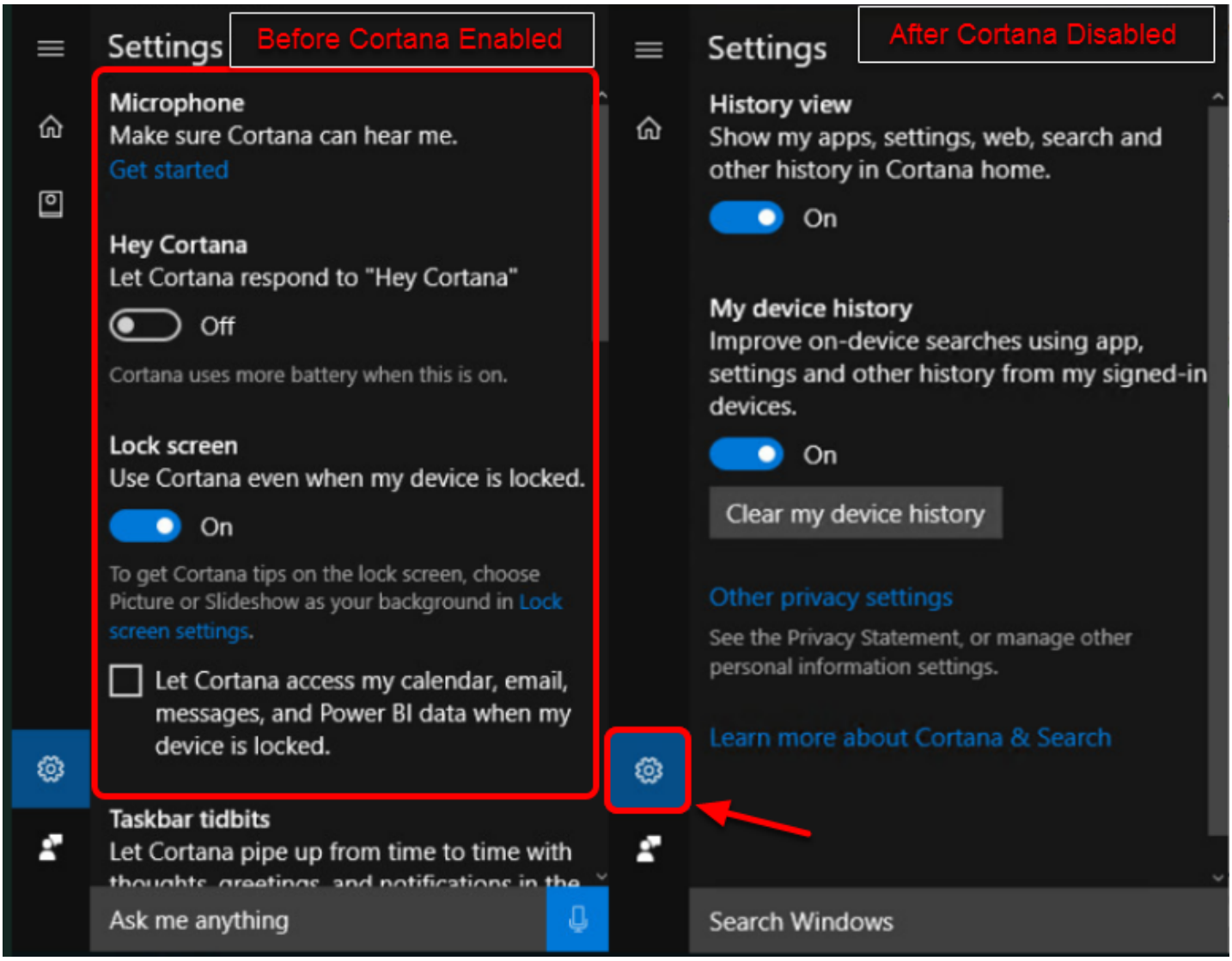
1. Click on **Start** logo.
2. Click on **Cortana** in the apps list.

Cortana Disabled



Notice now you are not greeted by Cortana, you only have basic search capabilities now that AirWatch has disabled Cortana.

Confirming Cortana is Disabled

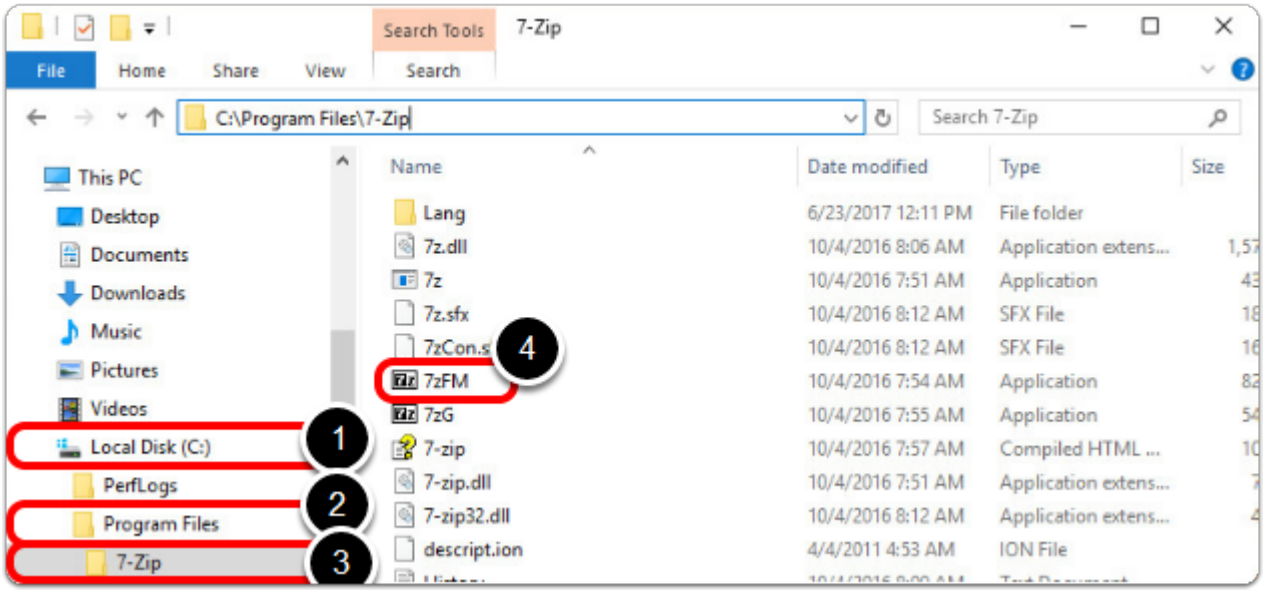


For further confirmation, click on the **Gear icon** and you will see that all of the Cortana settings which were present before have now disappeared. You should only see settings regarding searching and indexing.

Open Explorer

Click **Explorer** from the bottom toolbar.

Open 7-Zip



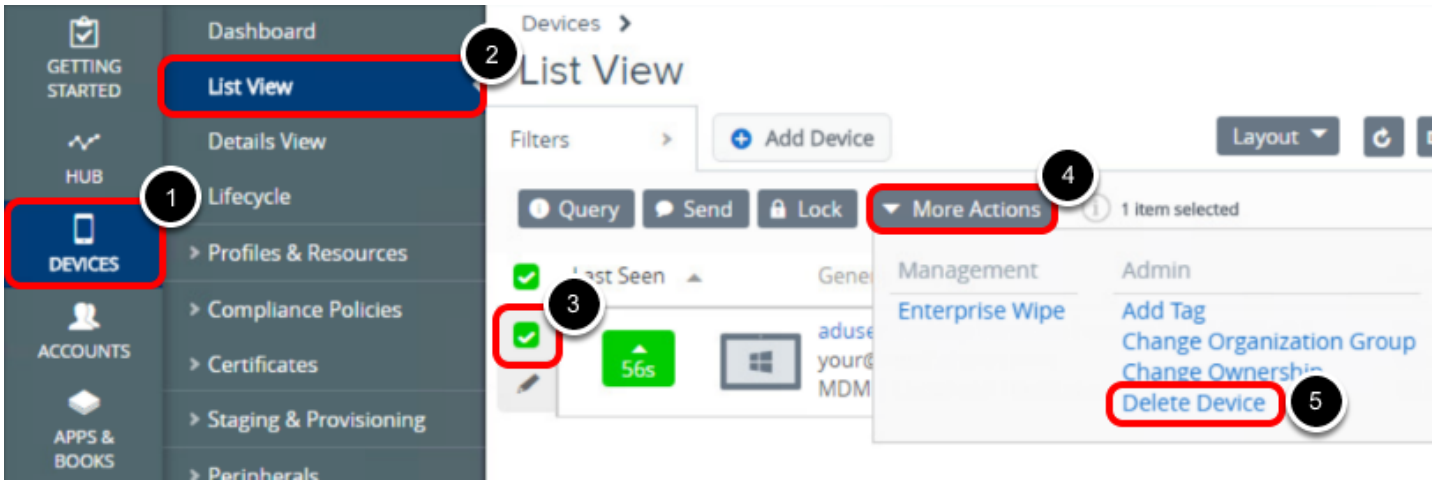
1. Click **Local Disk (C:)**.
2. Click **Program Files**.
3. Click **7-Zip**.
4. Double-click **7zFM.exe** to launch the **7-Zip File Manager**.

NOTE - If you do not see the 7-Zip Folder, your application may still be downloading. Due to lab scalability and network resources, this may take several minutes to finish.

Un-enrolling your Windows 10 Device

In this section, we are going to un-enroll our Windows 10 VM so that we can use it for other lab modules. We will delete the device record from the console, which will also un-enroll the device and remove all the apps and profiles that are pushed from AirWatch console, also known as managed content.

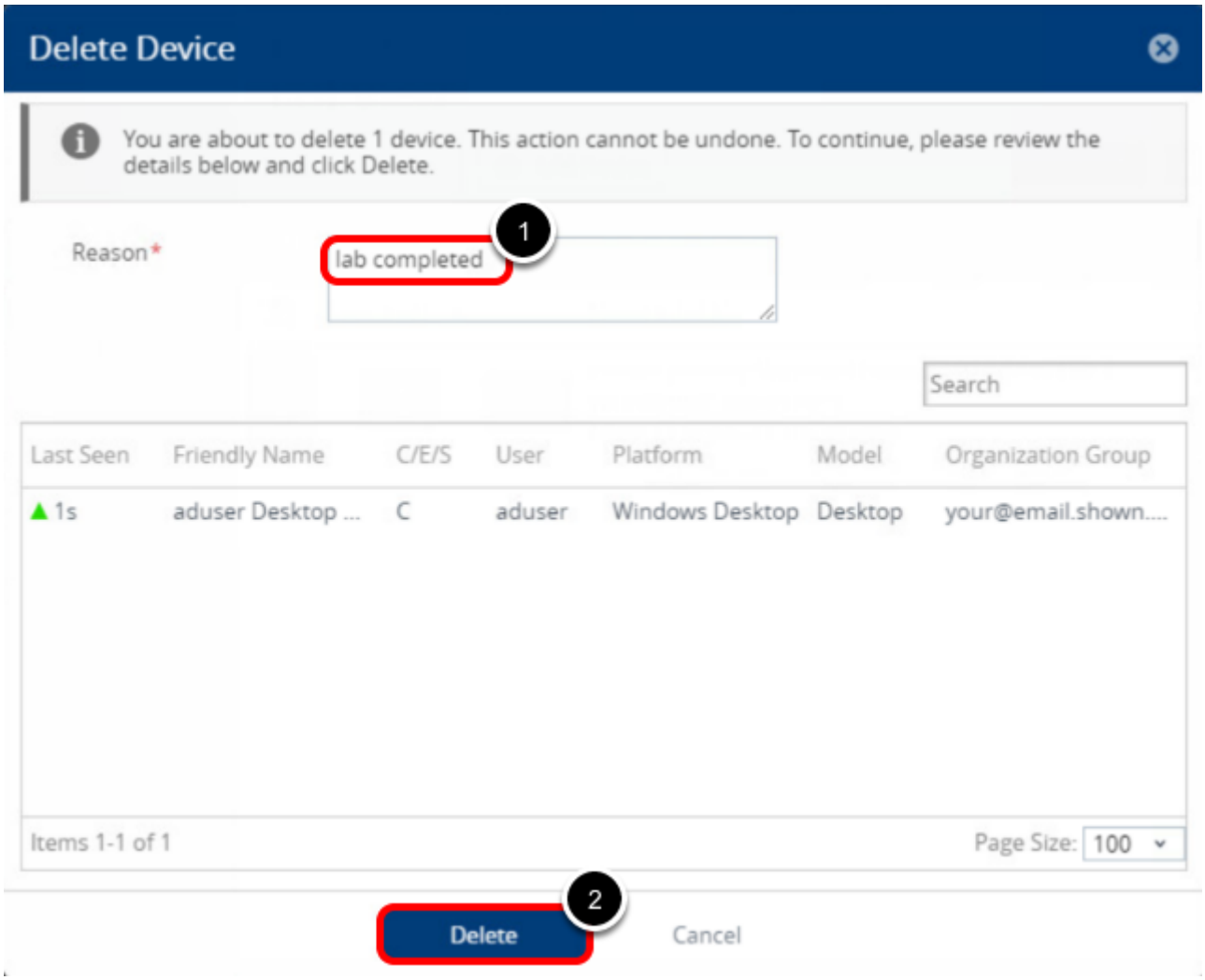
Delete Device from AirWatch Console



From the AirWatch Console,

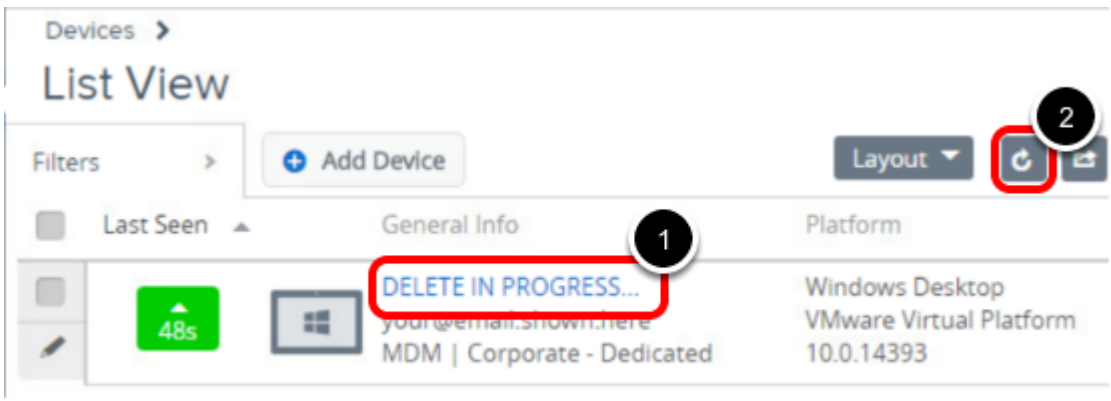
1. Click on **Devices**
2. Click on **List View**
3. Select the check box next to your device friendly name.
4. Click on **More Actions**
5. Click on **Delete Device**

Enter Reason and Delete



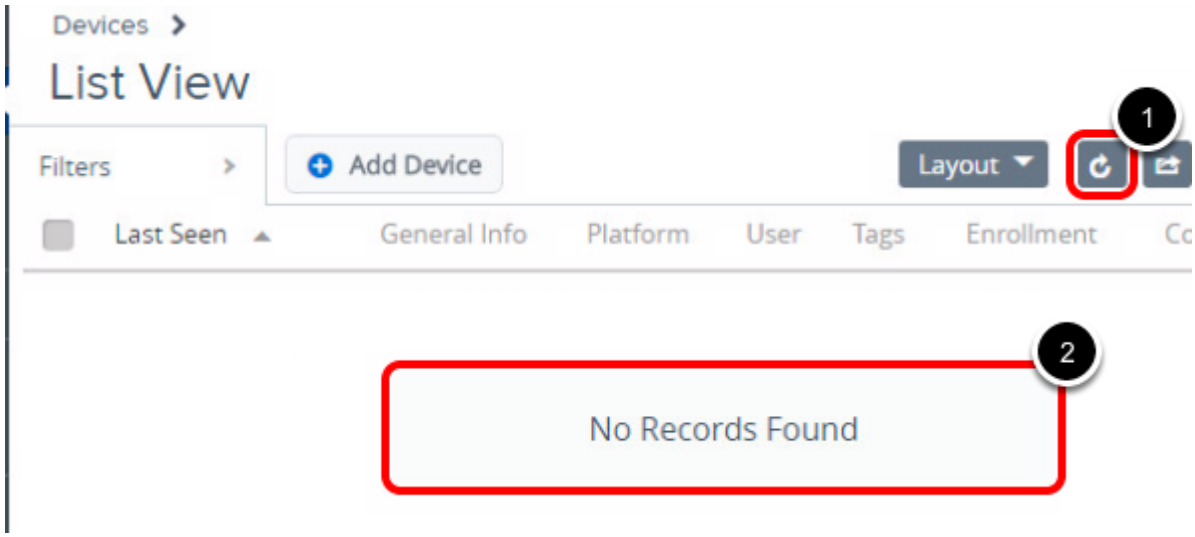
1. Enter the reason as "**lab completed**"
2. Click on **Delete**

Validate DELETE IN PROGRESS...



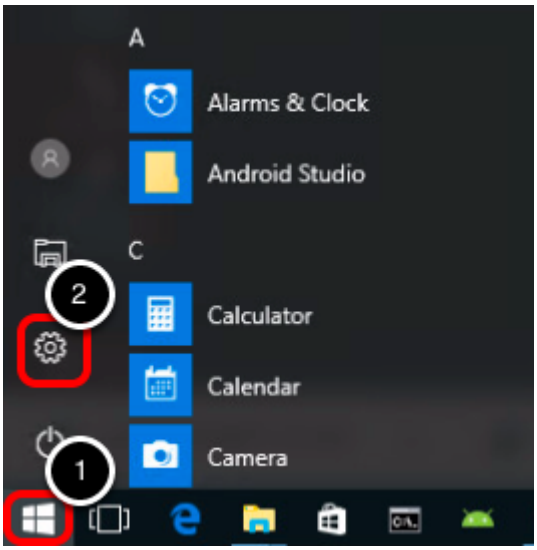
1. You may see device friendly name changing to **DELETE IN PROGRESS...**
2. Click on the **Refresh Icon** to validate if the device deletion is successful.

Ensure that device record is deleted



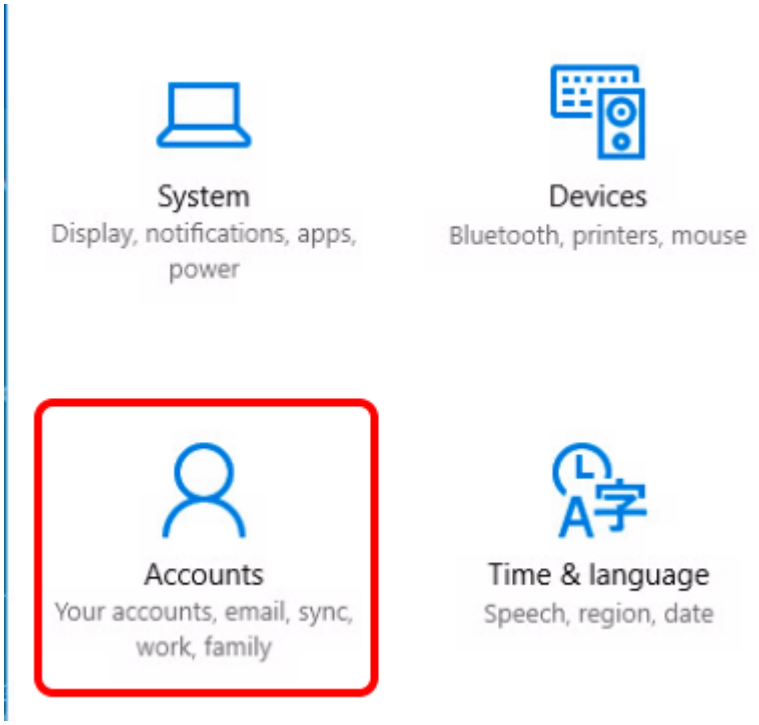
1. Use the **Refresh Button** if needed.
2. Ensure that the device record is now deleted from the AirWatch console and you see the message **No Records Found.**

Navigate to Windows 10 Settings



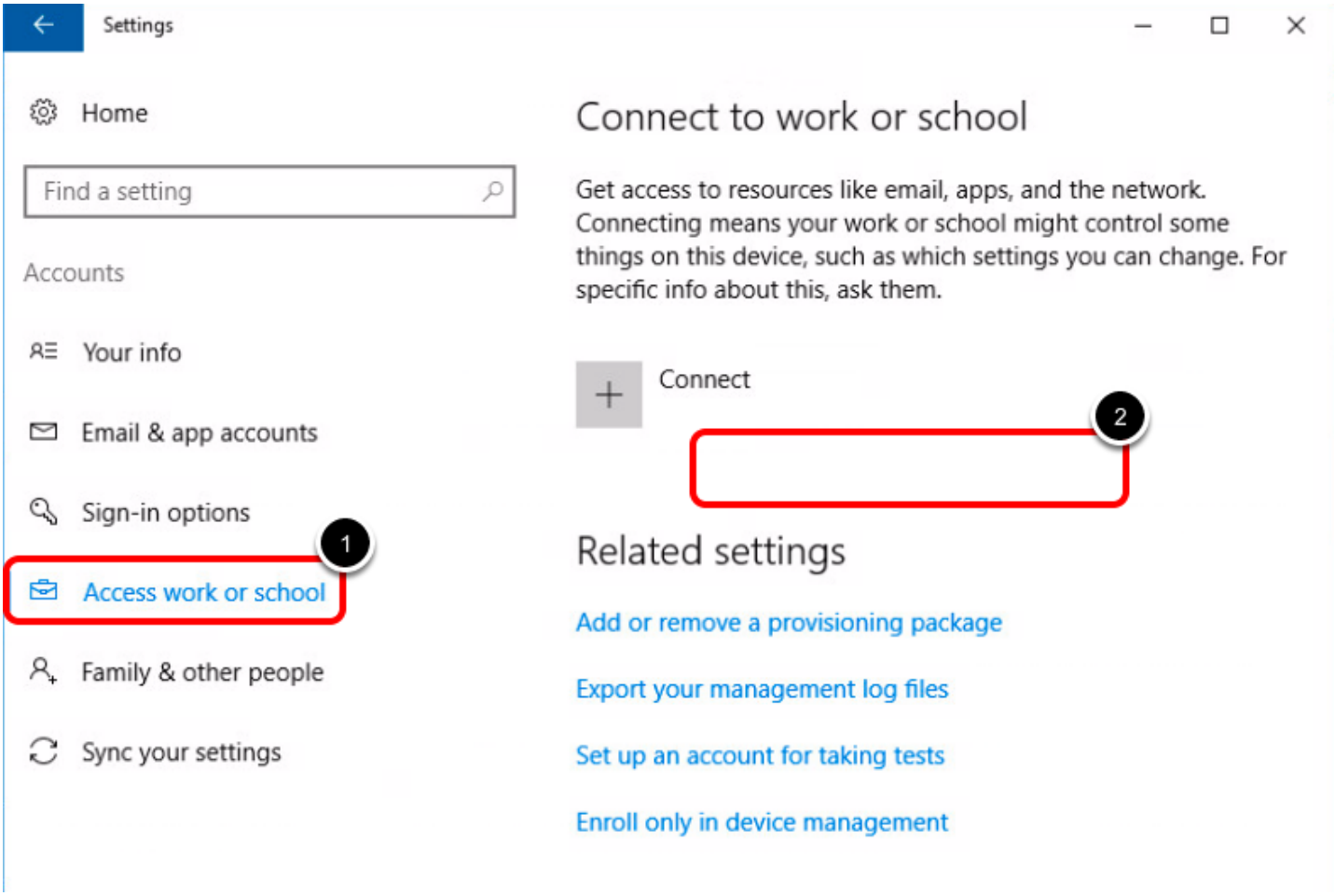
1. Click on the **Windows Icon**
2. Click on the gear icon to access **Windows 10 Settings**

Access Accounts Settings



From the Settings Menu, access **Accounts**

Validate That No Management Account Exists



1. Click on **Access work or school**
2. Validate that you DO NOT see any account connected to device management or other types.

Conclusion

In addition to managing mobile devices, AirWatch can also manage your Windows 10 applications as well. This quick look into Windows 10 management should provider a clearer picture on how you can manage your Windows 10 devices by configuring restrictions and profiles and deploying applications alongside your mobile workforce. For a deeper dive into Windows 10 Management, consider taking *HOL-1857-02-UEM - VMware AirWatch: Unified Endpoint Management for Windows 10*.

This concludes the Basic Windows 10 Management module.

Module 4 - Workspace ONE UEM Console Roles (30 minutes)

Introduction

In this lab module, you will learn how AirWatch Console Roles can be used to define how AirWatch administrators can interact with the AirWatch Console. This module will also review how to configure Self-Service options available for your end users. You will learn how to create and assign Roles to administrators and users alike and see how these changes impact the experience for both.

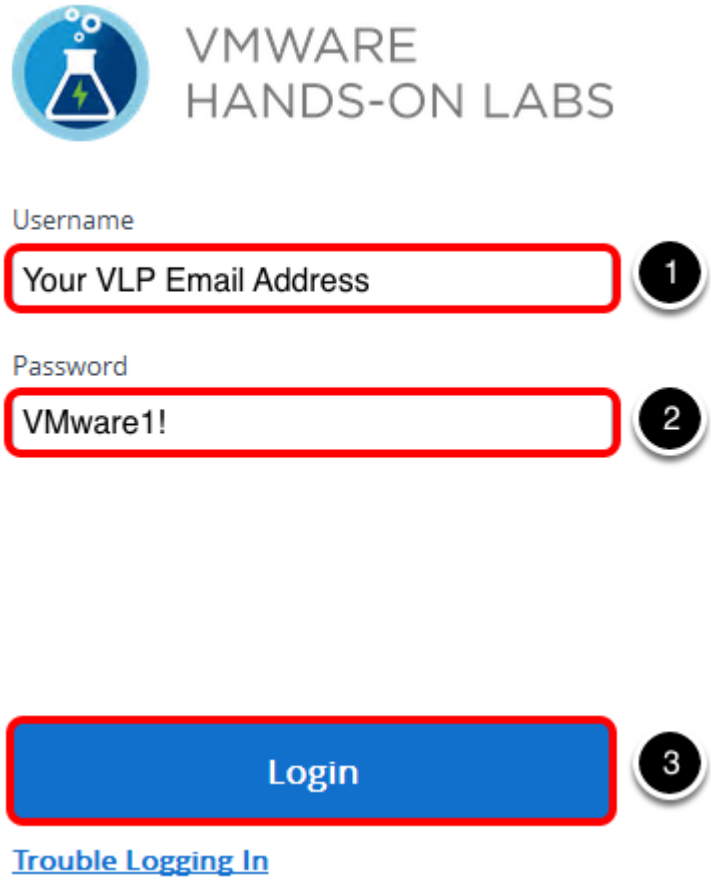
Login to the AirWatch Console

To perform most of the lab you will need to login to the AirWatch Management Console.

Launch Chrome Browser

Double-click the **Chrome** Browser on the lab desktop.

Authenticate to the AirWatch Administration Console



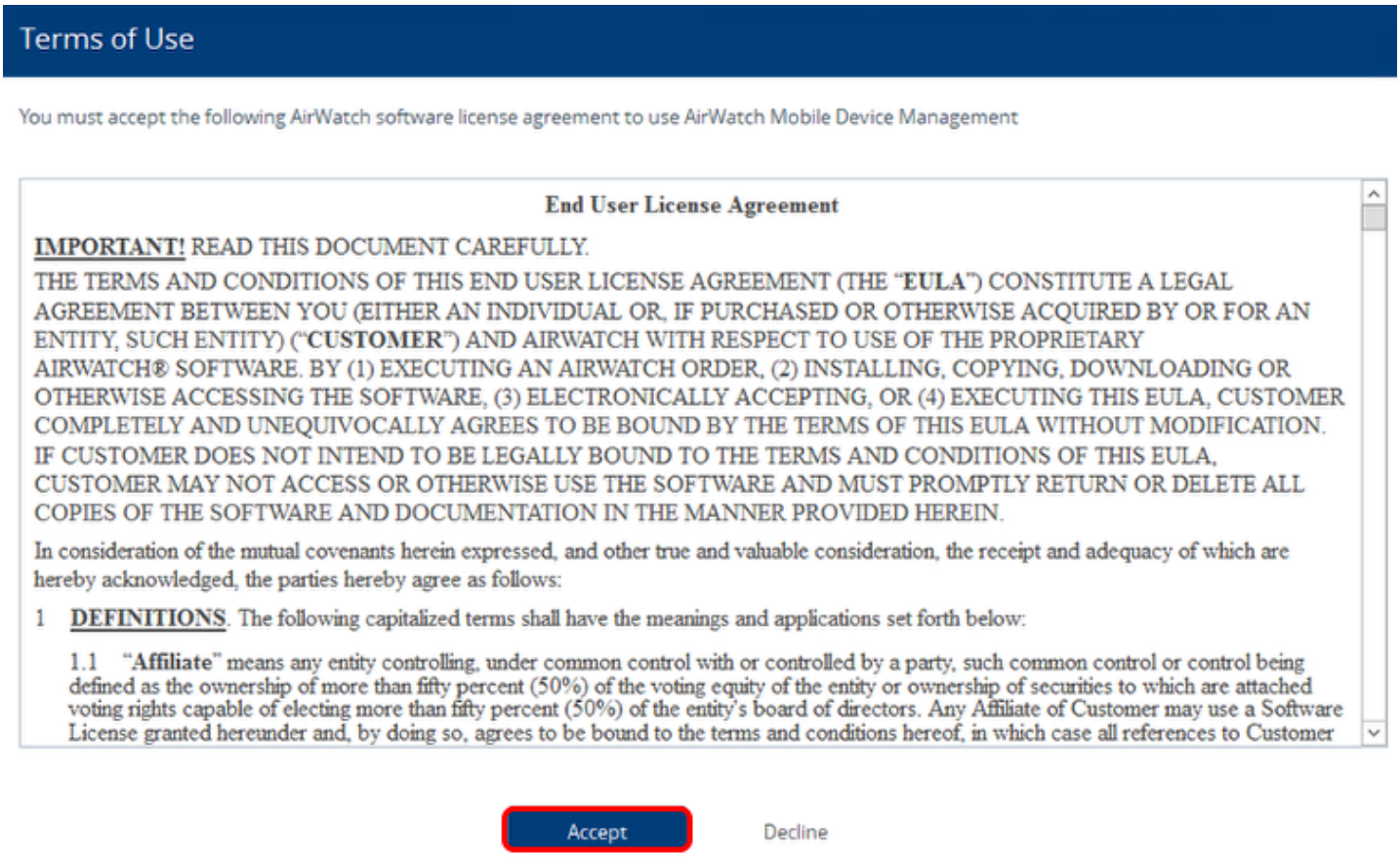
The default home page for the browser is **https://hol.awmdm.com**. Enter your AirWatch Admin Account information and click the **Login** button.

NOTE - If you see a Captcha, please be aware that it is case sensitive!

1. Enter your **Username**. This is you **email address** that you have associated with your **VMware Learning Platform (VLP) account**.
2. Enter **"VMware1!"** for the **Password** field.
3. Click the **Login** button.

NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the AirWatch Hands On Labs server.

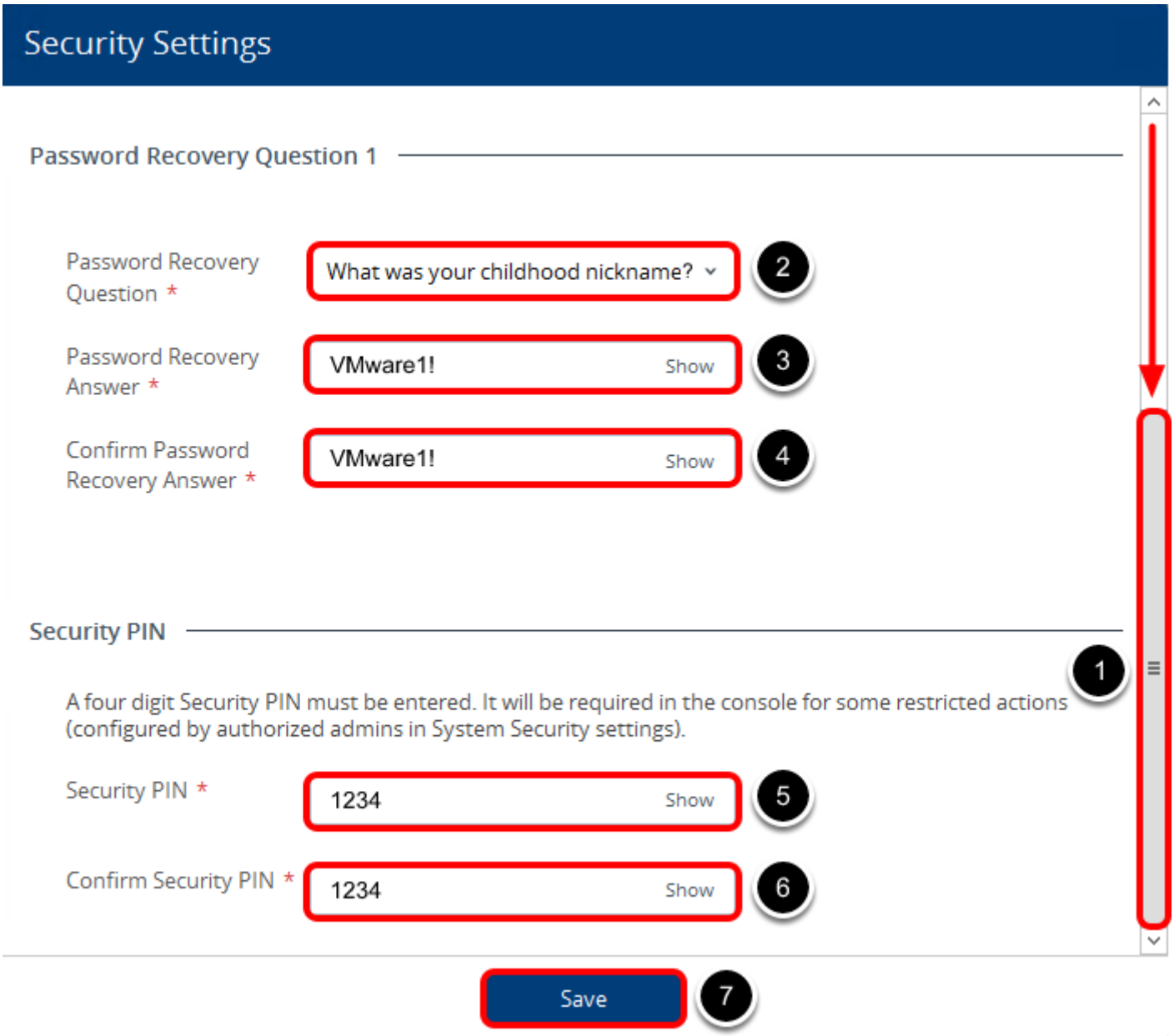
Accept the End User License Agreement



NOTE - The following steps of logging into the Administration Console will only need to be done during the initial login to the console.

You will be presented with the AirWatch Terms of Use. Click the **Accept** button.

Address the Initial Security Settings

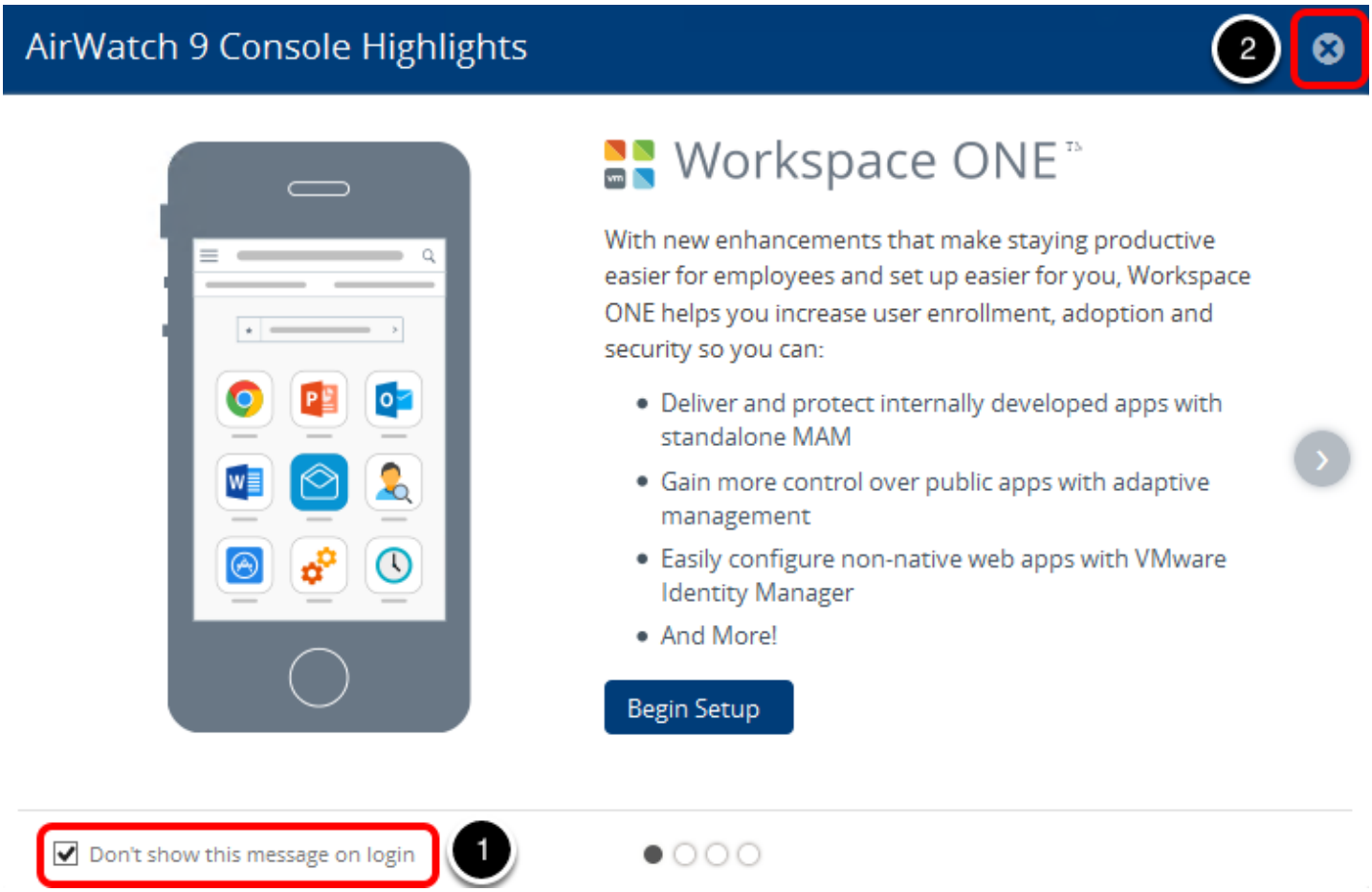


After accepting the Terms of Use, you will be presented with a **Security Settings** pop-up. The **Password Recovery Question** is in case you forget your admin password and the **Security PIN** is to protect certain administrative functionality in the console.

1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a **question** from the **Password Recovery Question** drop-down (default selected question is ok here).
3. Enter **"VMware1!"** in the **Password Recovery Answer** field.
4. Enter **"VMware1!"** in the **Confirm Password Recovery Answer** field.
5. Enter **"1234"** in the **Security PIN** field.
6. Enter **"1234"** in the **Confirm Security PIN** field.

7. Click the **Save** button when finished.

Close the Welcome Message



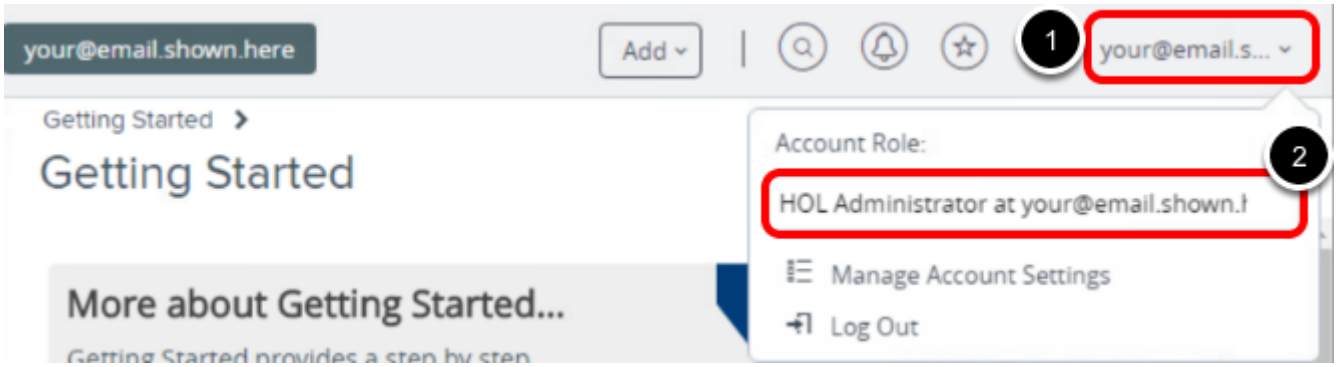
After completing the Security Settings, you will be presented with the AirWatch Console Welcome pop-up.

1. Click on the **Don't show this message again** check box.
2. Close the pop-up by clicking on the **X** in the upper-right corner.

Administrator Roles

AirWatch lets you control specific roles to be applied to different administrators for different administrative purposes. In this Hands-On-Lab (HOL), you'll learn how to configure roles for your administrators.

Check Your Current Admin Role

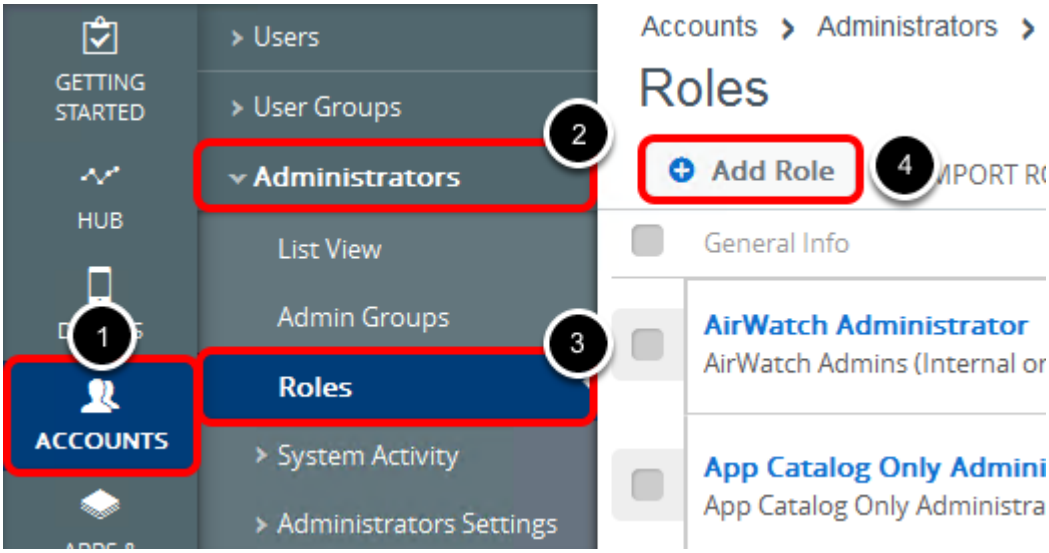


Check the current role of the logged in user:

1. Click **Account** button in the top-right corner of the Console. Your email address will be listed on the button.
2. Confirm that the current Role is **HOL Administrator** at your organization group.

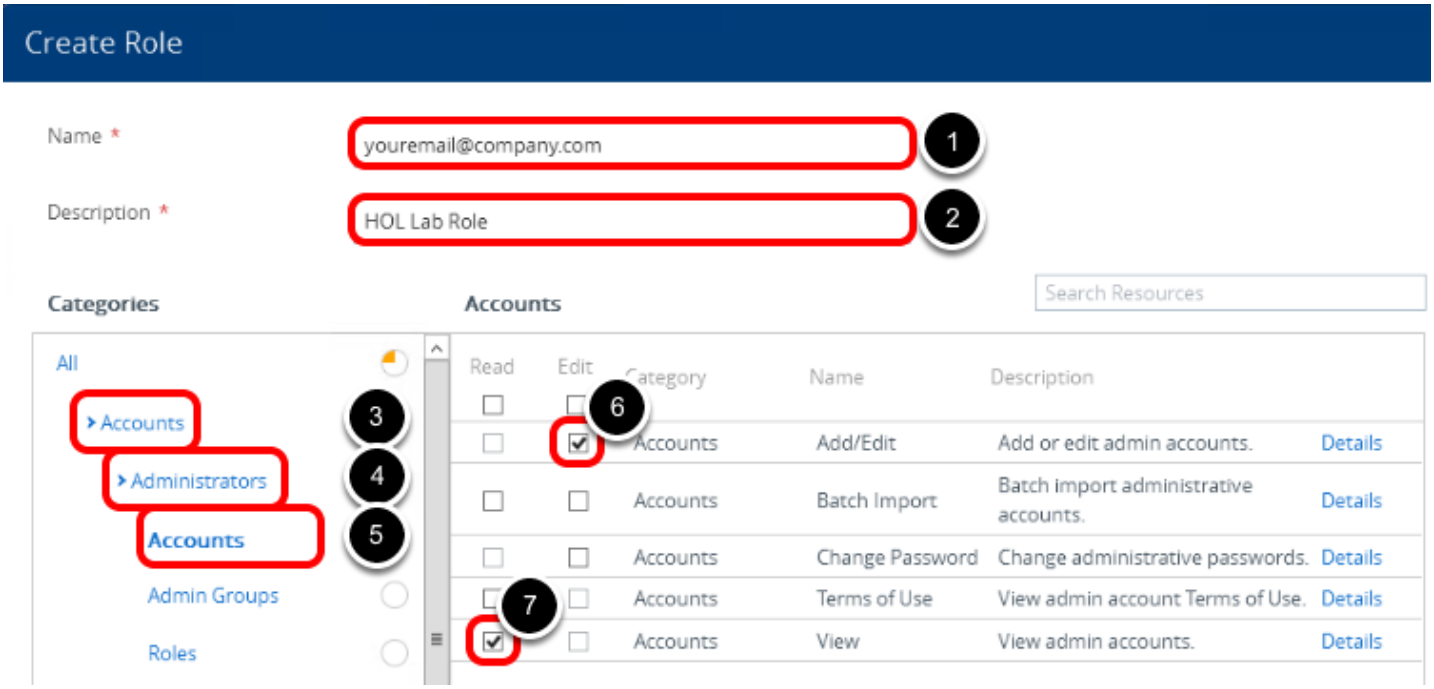
A good strategy when creating new roles is to assign the role to yourself. That allows you to use this dropdown menu to select different roles and actually see the effects of the role you are editing!

Creating a new role



1. Click **Accounts**.
2. Expand the **Administrators** dropdown.
3. Click **Roles** under **Administrators**.
4. Click **+ Add Role**.

Admin Accounts Permissions

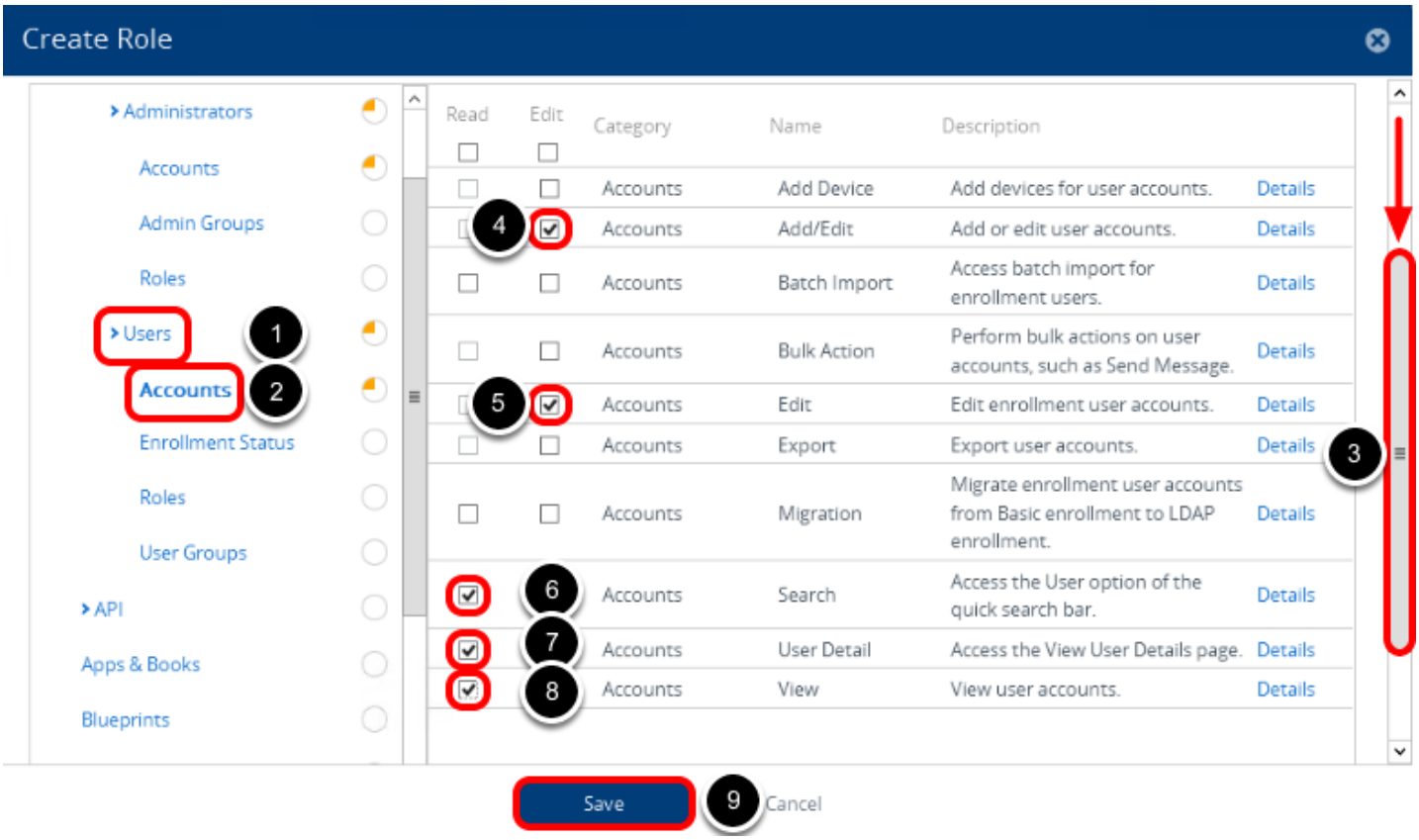


1. Enter a unique value (such as **your email address**) in the **Name** field.
2. Enter "**HOL Lab Role**" in the **Description** field.

   The Permissions categories are located on the left side. Each category applies to different Console functions.
   The Search Resources box located on the top right is used to look for specific permissions. By selecting a category, you can search solely within it.
3. Expand **Accounts** by clicking the **>** to the left.
4. Expand **Administrators** by clicking the **>** to the left.
5. Click **Accounts**.

   Here you will see all the permissions relevant to the Accounts section of the Console.
6. Check the **Edit** check box for the permission with the name **Add/Edit..**
7. Check the **Read** check box for the permission with the name **View**.

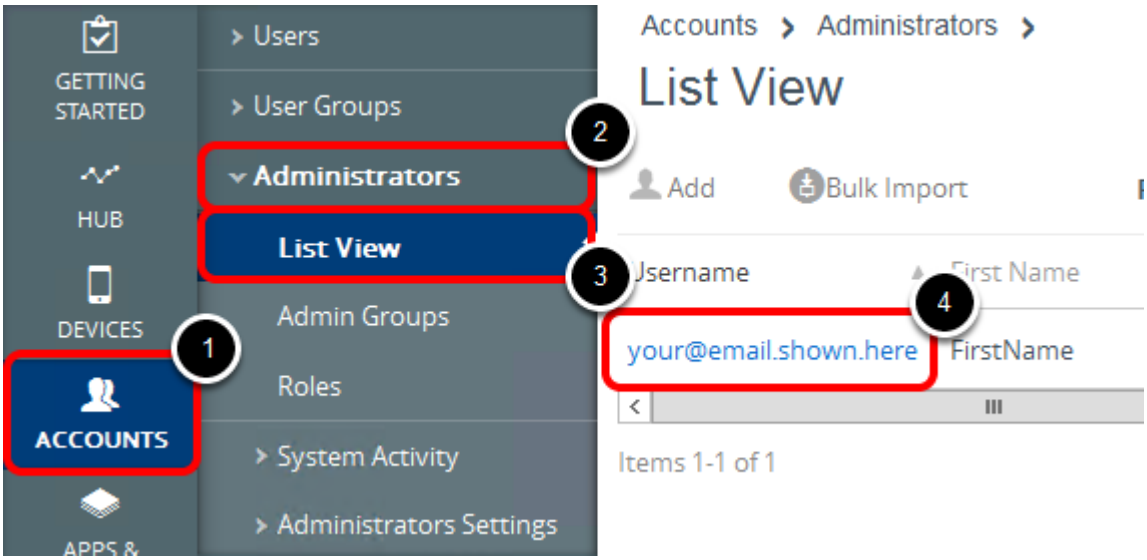
Users Permissions



1. Expand **Users** by clicking the **>** to the left.
2. Click **Accounts**.
3. You may need to scroll down to view the necessary permissions.
4. Check the **Edit** check box for the permission with the Name **Add/Edit**.
5. Check the **Edit** check box for the permission with the Name **Edit**.
6. Check the **Read** check box for the permission with the Name **Search**.
7. Check the **Read** check box for the permission with the Name **User Detail**.
8. Check the **Read** check box for the permission with the Name **View**.
9. Click **Save**.

We have now created a role that has restricted access to permissions within Account (Administrators & Users) and Devices.

Adding the New Role and Attaching It To Your Admin Account

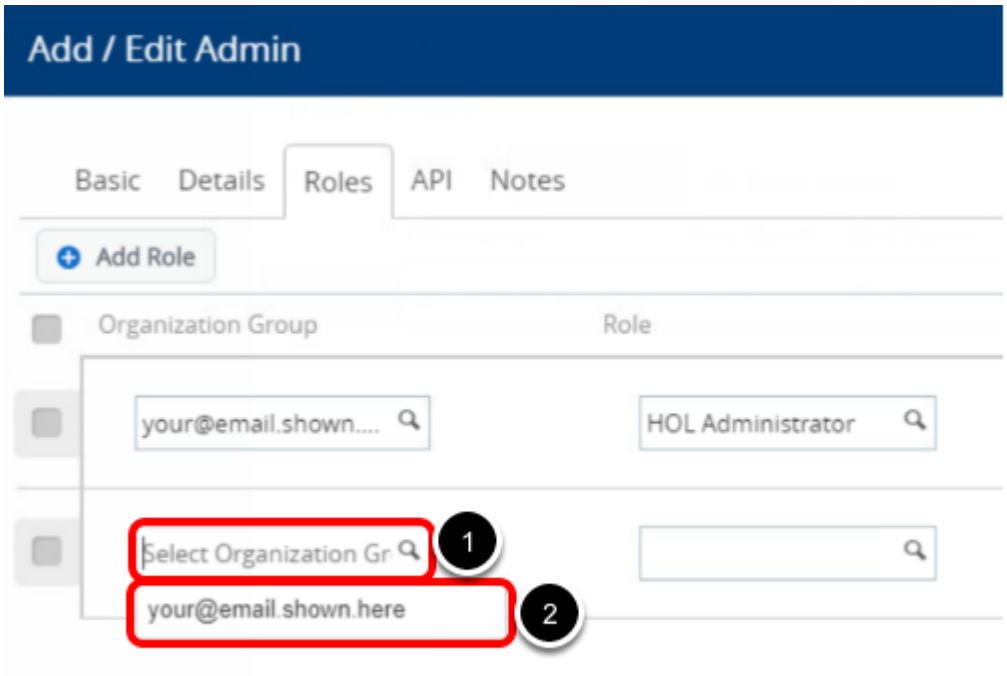


1. Click **Accounts**.
2. Expand **Administrators**.
3. Click **List View**.
4. Click the Administrator account, which will be your **email address**.

Add the Role

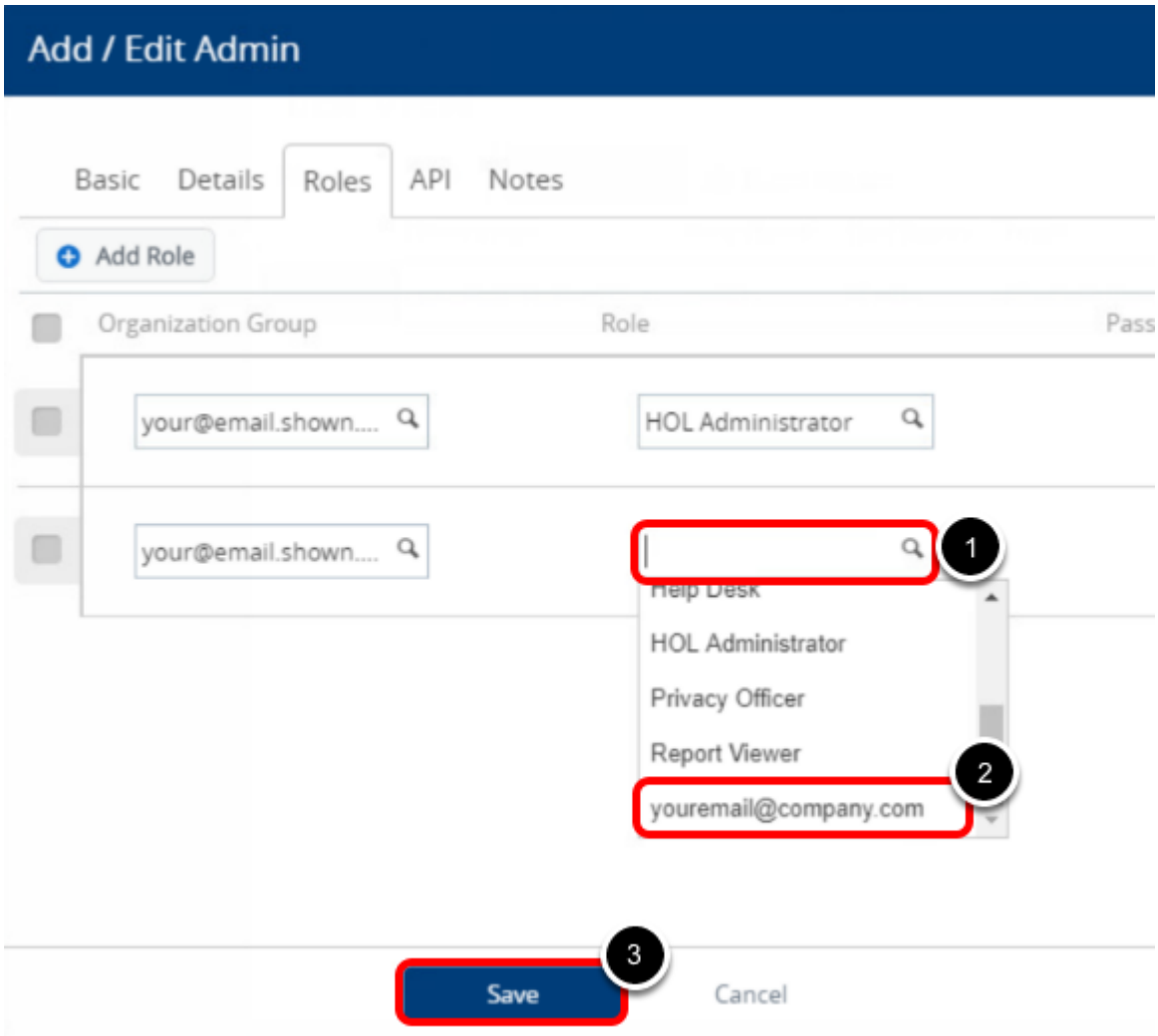
1. Click the **Roles** tab.
2. Click **+ Add Role**.

Selecting the Organization Group



1. Click the **Select Organization Group** search field to view your Organization Groups.
2. Click your Organization Group, which will be named after your **email address**.

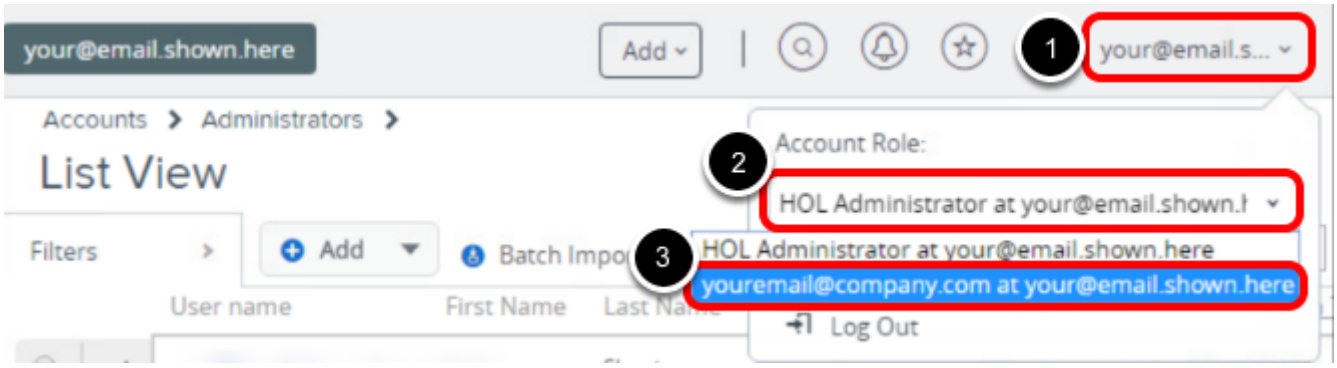
Selecting the New Role



1. Click the **Role** search box.
2. Click the Role that you created in the previous step. You can scroll through the list and click your **email address**, or begin typing to reduce the Roles shown.
3. Click **Save**.

NOTE - You may receive an email from AirWatch titled "AirWatch Administrator Personal Information Updated" noting this role change for your administrator account. Please feel free to ignore and delete this email notification, as it is not needed for the lab.

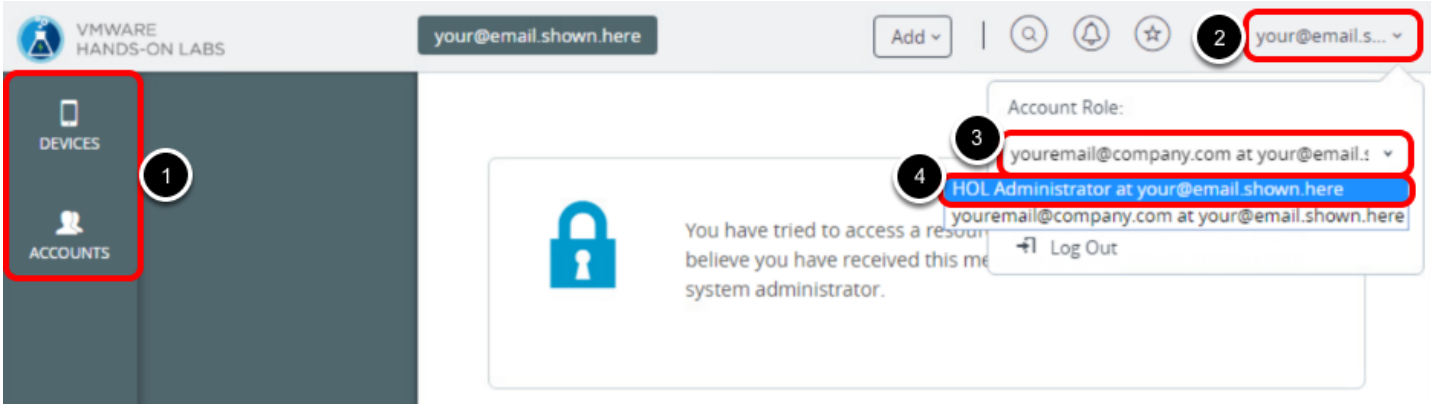
Toggling between Roles



1. Click **Account** button in the top-right corner of the Console. Your email address will be listed on the button.
2. Click your current **Account Role**.
3. Click the created Account Role, which will be named after your **email address**.

NOTE - If you are unable to change your role, you may need to refresh the page and try again.

View the Restricted Role



1. Notice how your screen options have changed and you only have access to a very limited number of actions in the console.

   This is a quick way to see how the Roles you have created with appear to any administrators you assign these roles to. Let's change our Account Role back to the **HOL Administrator** role by following the below steps:

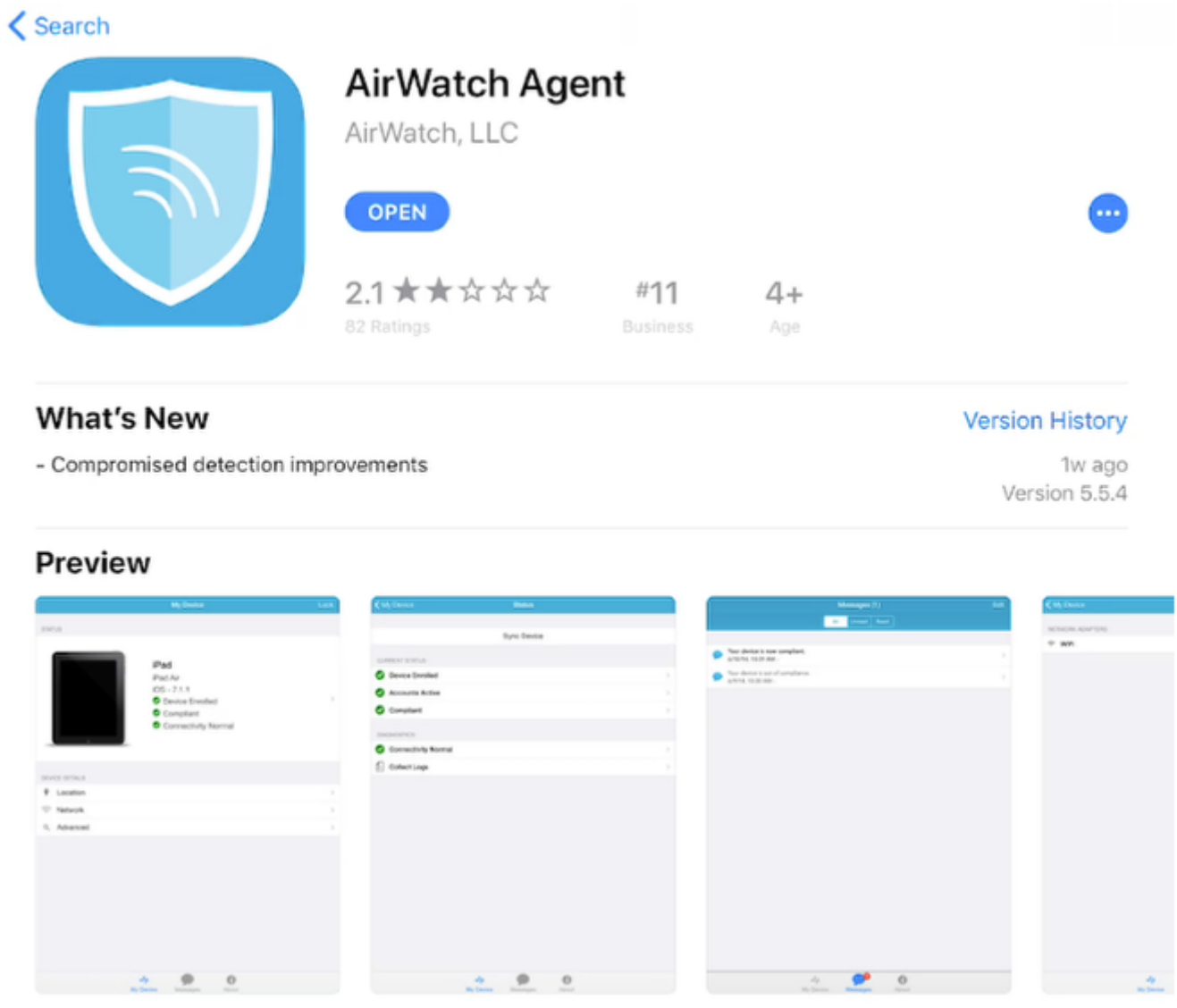
2. Click **Account** button in the top-right corner of the Console. Your email address will be listed on the button.
3. Click your current **Account Role**.
4. Click the default Account Role, which will be **HOL Administrator**.

NOTE - Ensure your Account Role has been changed back to HOL Administrator before continuing, as you will be unable to perform the rest of the lab module with the restricted admin role you created.

iOS Device Enrollment

In this section, we are going to enroll an iOS device to complete the steps on the device side.

Download/Install AirWatch MDM Agent Application from App Store - IF NEEDED



NOTE - Checked out devices will likely have the AirWatch MDM Agent already installed. You may skip this step if your device has the AirWatch MDM agent installed.

At this point, if using your own iOS device or if the device you are using does NOT have the AirWatch MDM Agent Application installed, then install the AirWatch Application.

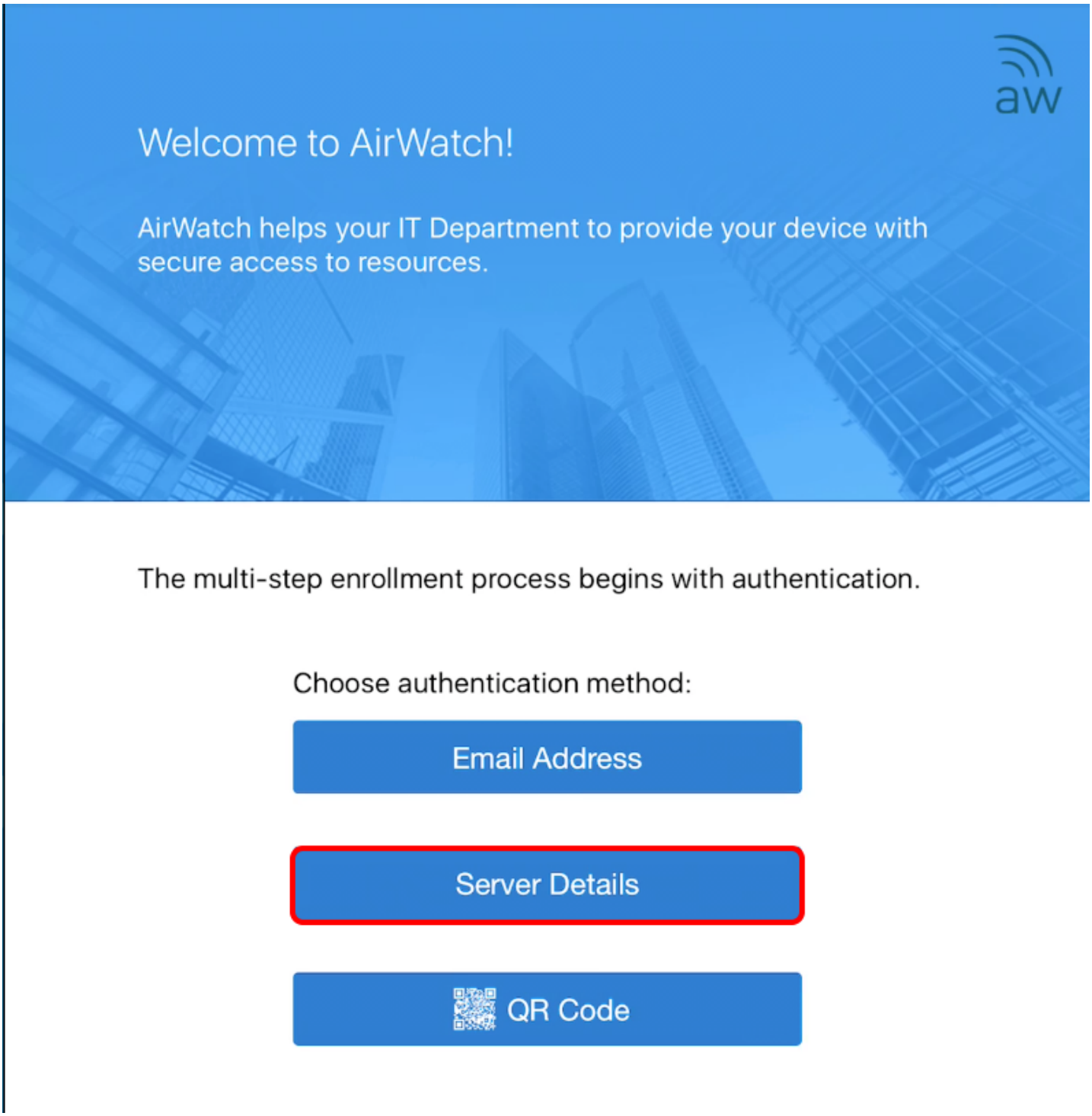
To Install the AirWatch MDM Agent application from the App Store, open the App Store application and download the free **AirWatch MDM Agent** application.

Launching the AirWatch MDM Agent

Launch the **AirWatch Agent** app on the device.

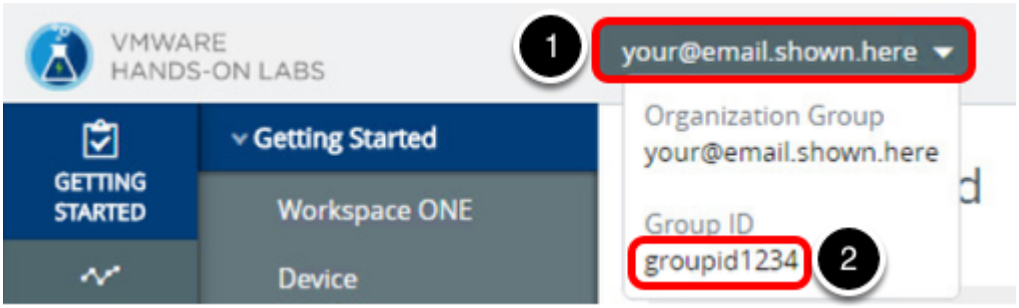
NOTE - If you have your own iOS device and would like to test you will need to download the agent first.

Choose the Enrollment Method



Click on the **Server Details** button.

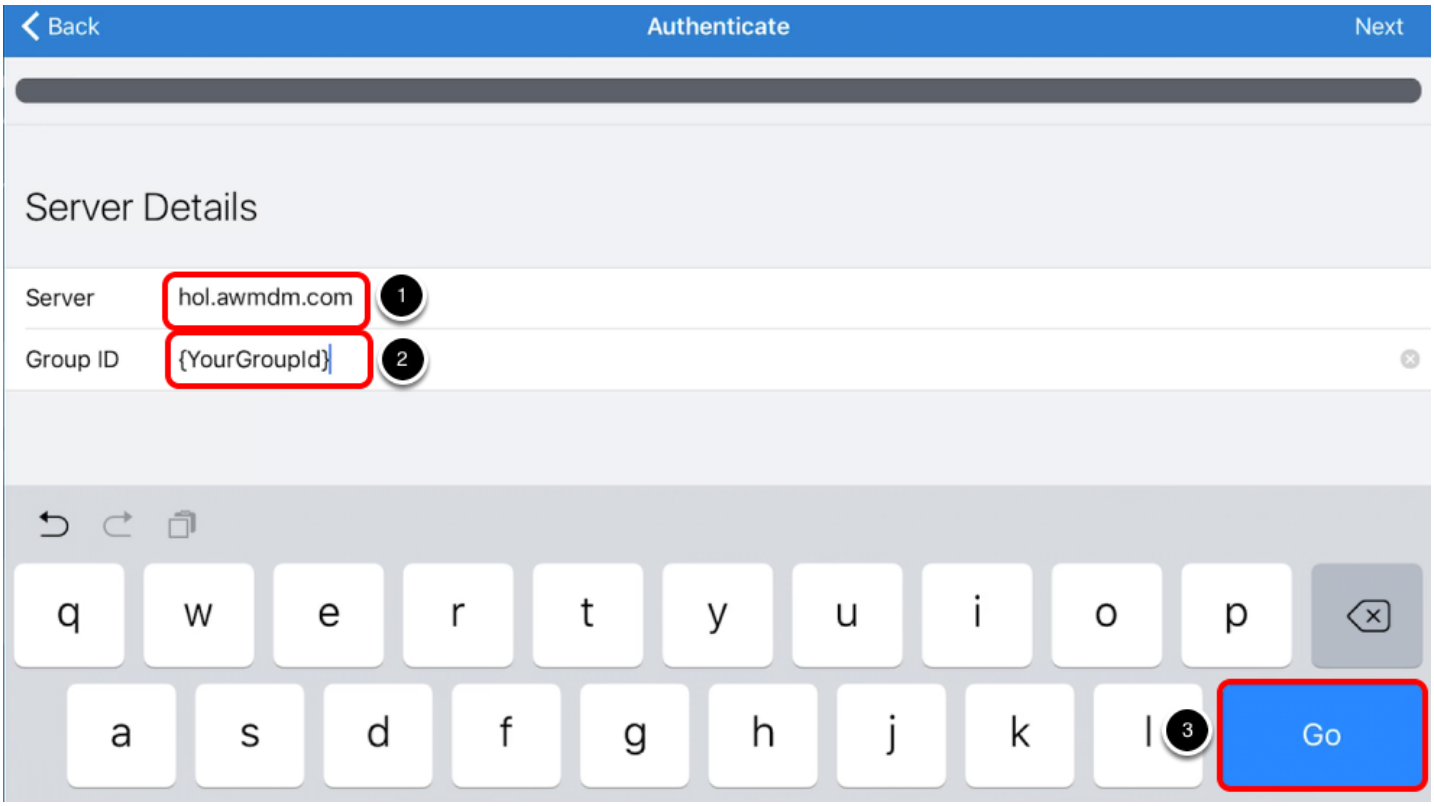
Find your Group ID from AirWatch Console



1. To find the Group ID, hover your mouse over the Organization Group tab at the top of the screen. Look for the email address you used to log in to the lab portal.
2. Your **Group ID** is displayed at the bottom of the Organization Group pop up.

NOTE - The Group ID is required when enrolling your device in the following steps.

Attach the AirWatch MDM Agent to the HOL Sandbox



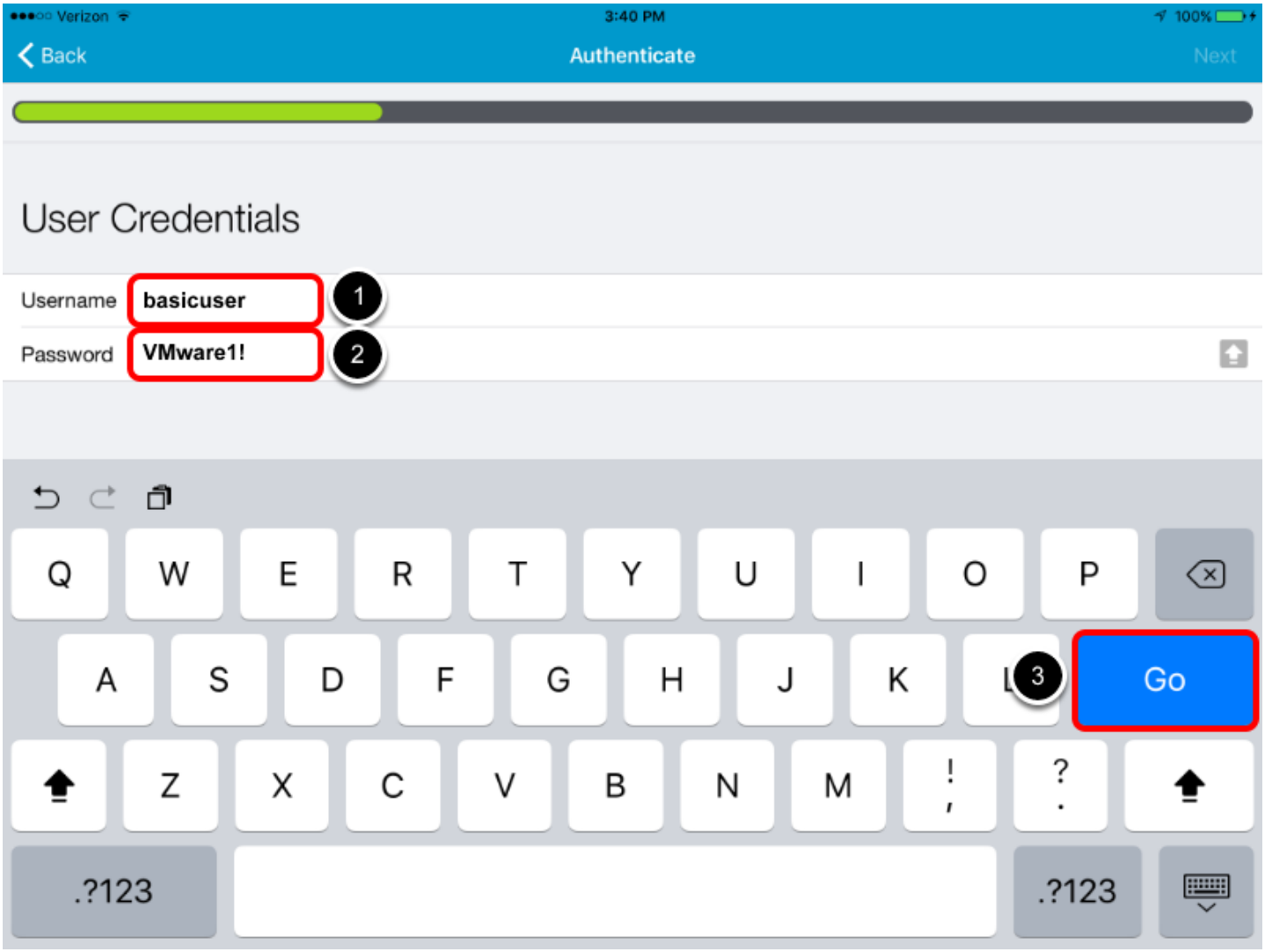
Once the Agent has launched you can enroll the device. To do so, follow the below steps.

1. Enter **"hol.awmdm.com"** for the **Server** field.

2. Enter your **Group ID** for your Organization Group for the **Group ID** field. Your Group ID was noted previously in the **Finding your Group ID** step.
3. Tap the **Go** button.

NOTE - If on an iPhone, you may have to close the keyboard by clicking Done in order to click the Continue button.

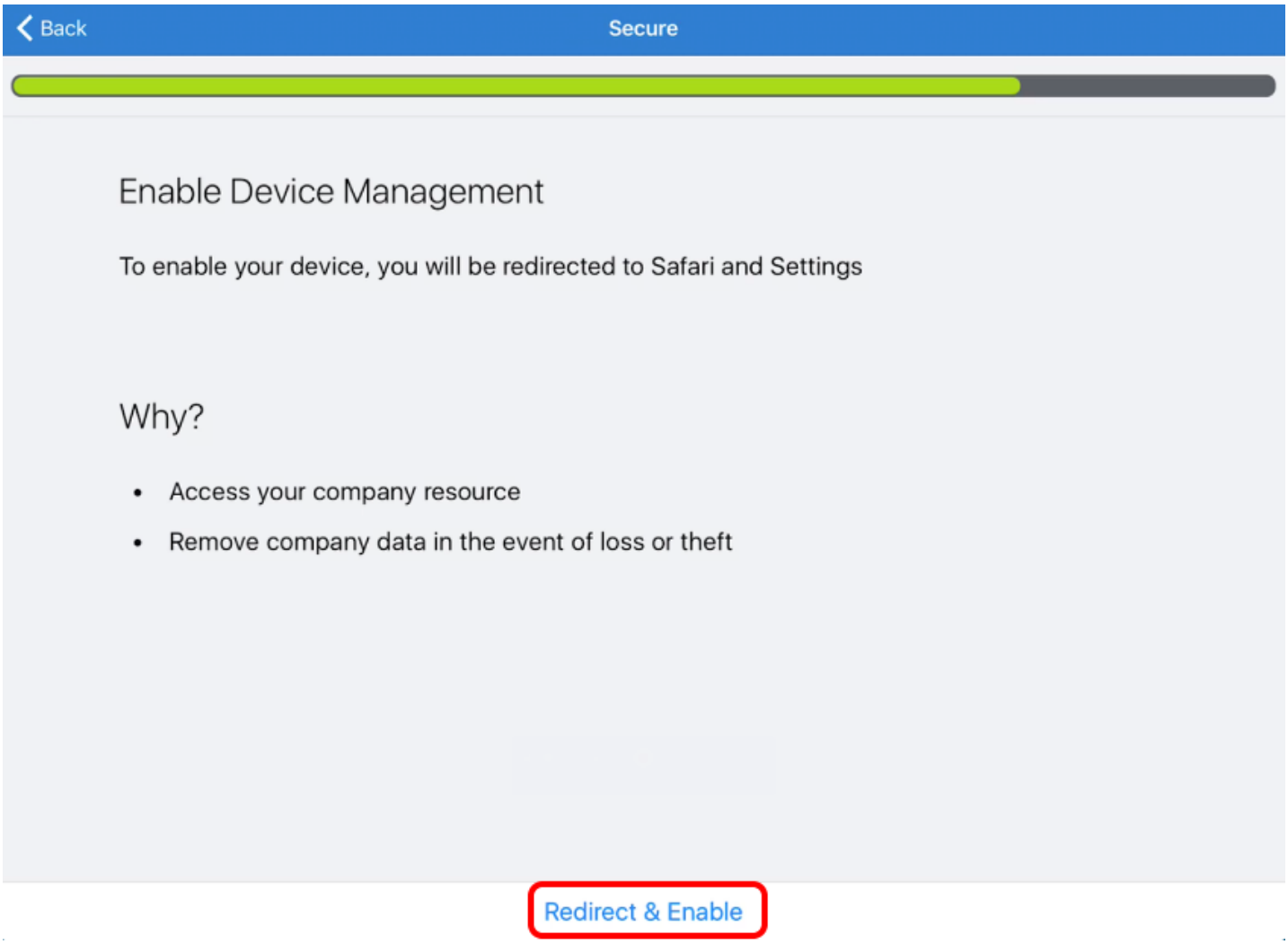
Authenticate the AirWatch MDM Agent



On this screen, enter the **Username** and **Password** for the basic user account.

1. Enter **"testuser"** in the **Username** field.
2. Enter **"VMware1!"** in the **Password** field.
3. Tap the **Go** button.

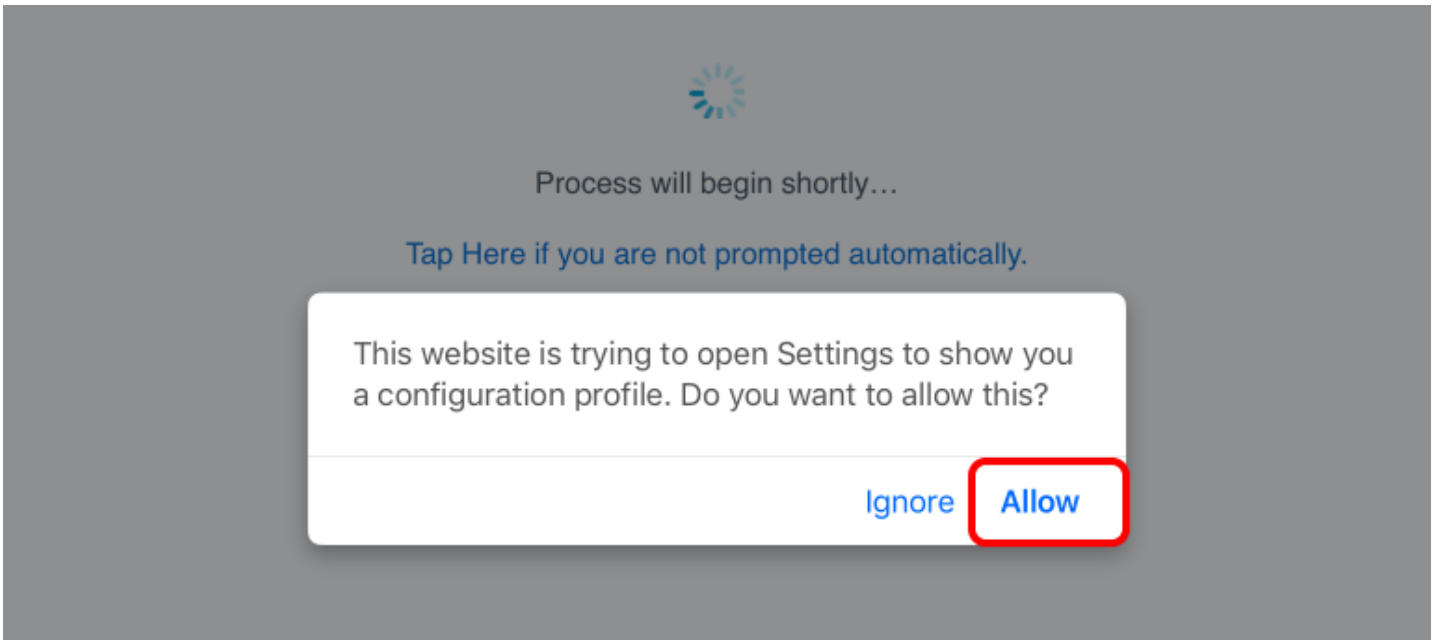
Redirect to Safari and Enable MDM Enrollment in Settings



The AirWatch Agent will now redirect you to Safari and start the process of enabling MDM in the device settings.

Tap on **Redirect & Enable** at the bottom of the screen.

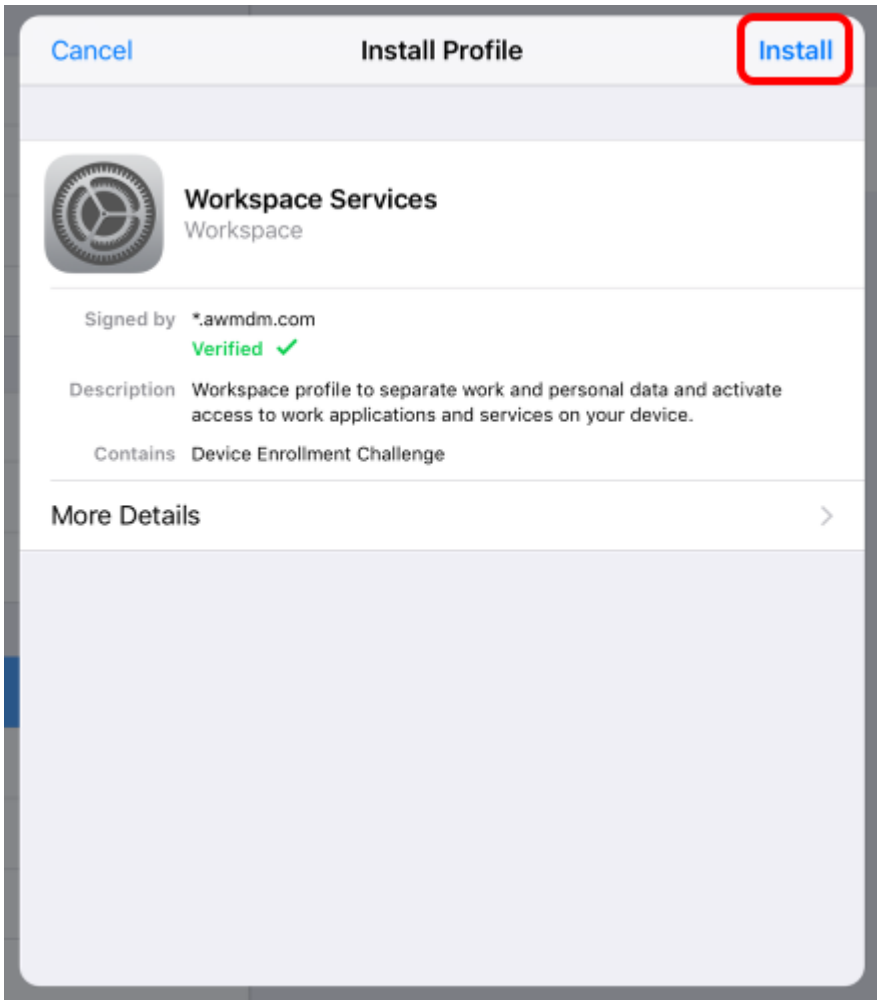
Allow Website to Open Settings (IF NEEDED)



If you prompted to allow the website to open Settings to show you a configuration profile, tap **Allow**.

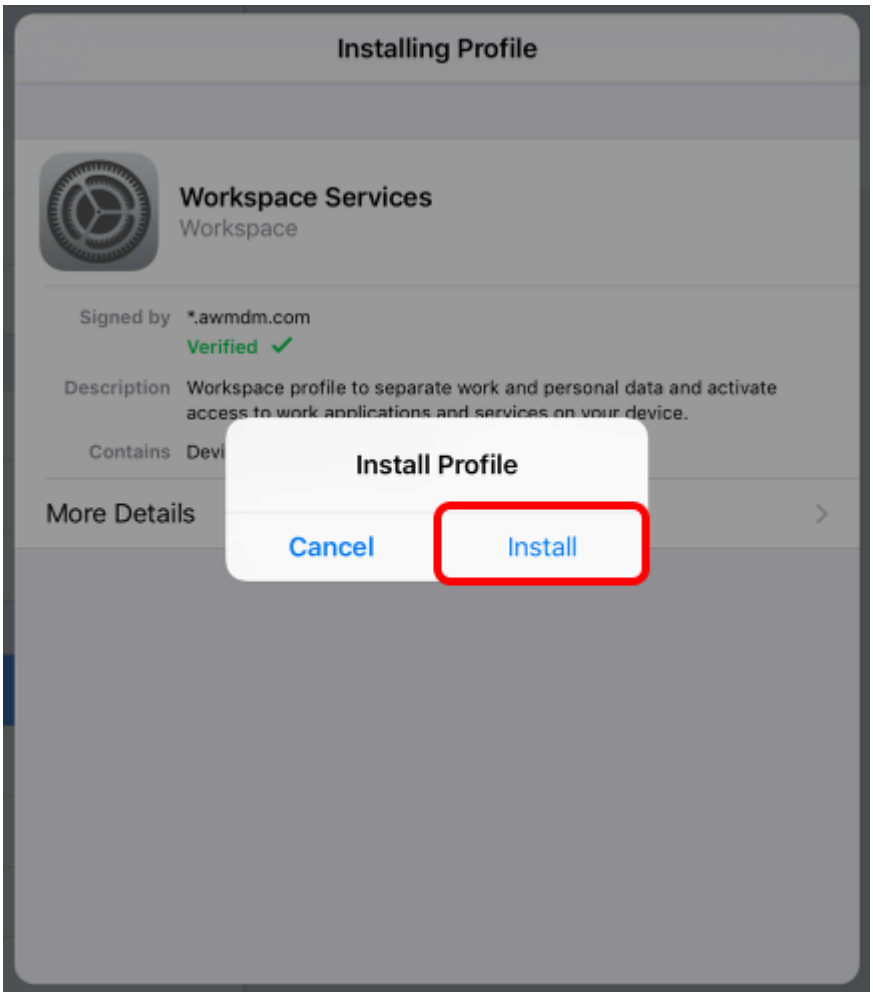
NOTE - If you do not see this prompt, ignore this and continue to the next step. This prompt will only occur for iOS Devices on iOS 10.3.3 or later

Install the MDM Profile



Tap **Install** in the upper right corner of the Install Profile dialog box.

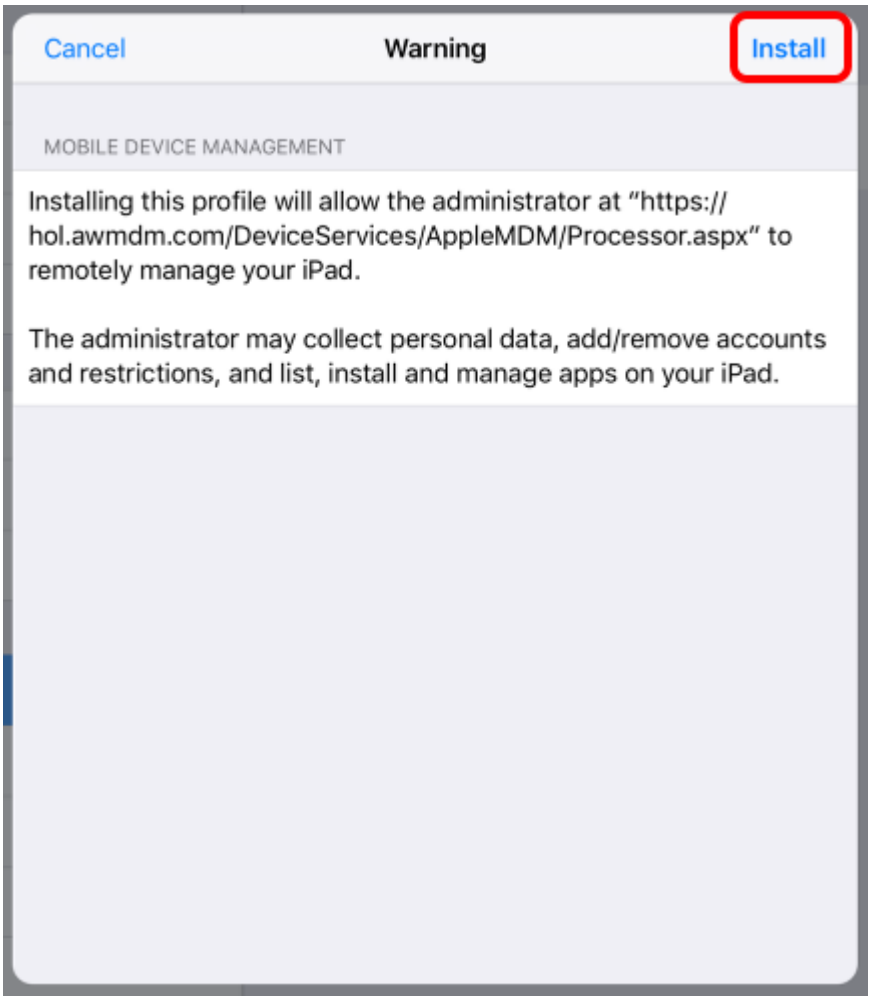
Install and Verify the AirWatch MDM Profile



Tap **Install** when prompted at the Install Profile dialog.

NOTE - If a PIN is requested, it is the current device PIN. Provided VMware devices should not have a PIN.

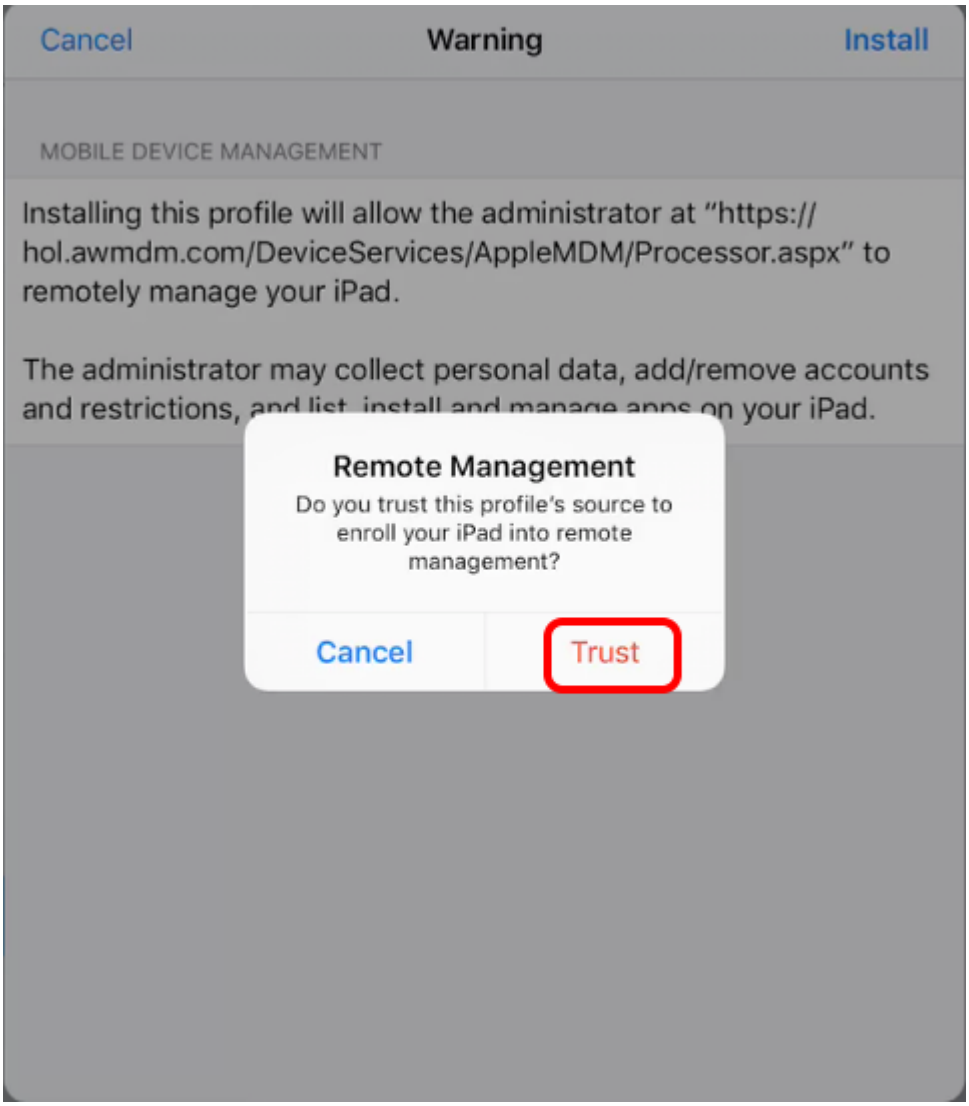
iOS MDM Profile Warning



You should now see the iOS Profile Installation warning explaining what this profile installation will allow on the iOS device.

Tap **Install** in the upper-right corner of the screen.

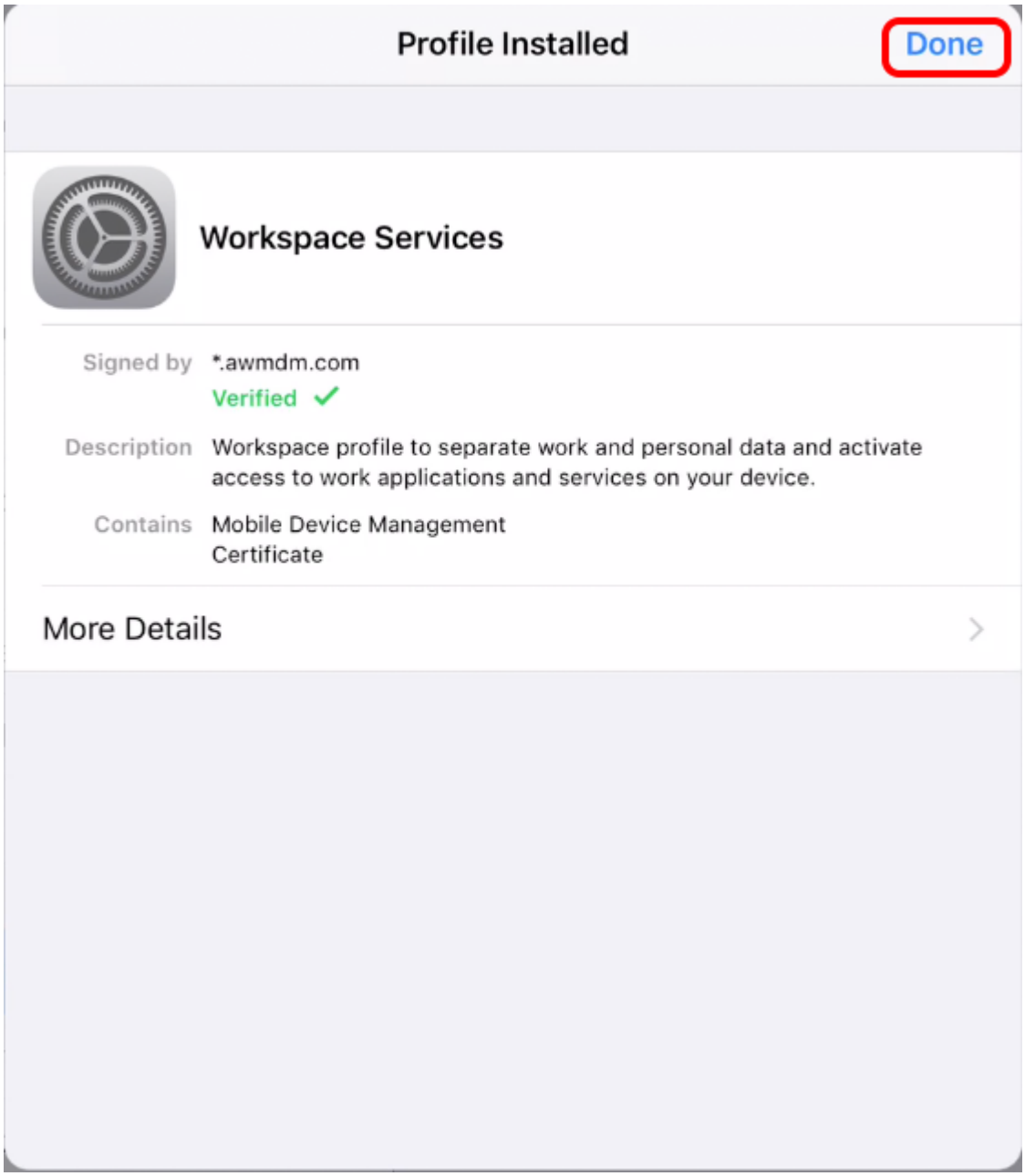
Trust the Remote Management Profile.



You should now see the iOS request to trust the source of the MDM profile.

Tap **Trust** when prompted at the Remote Management dialog.

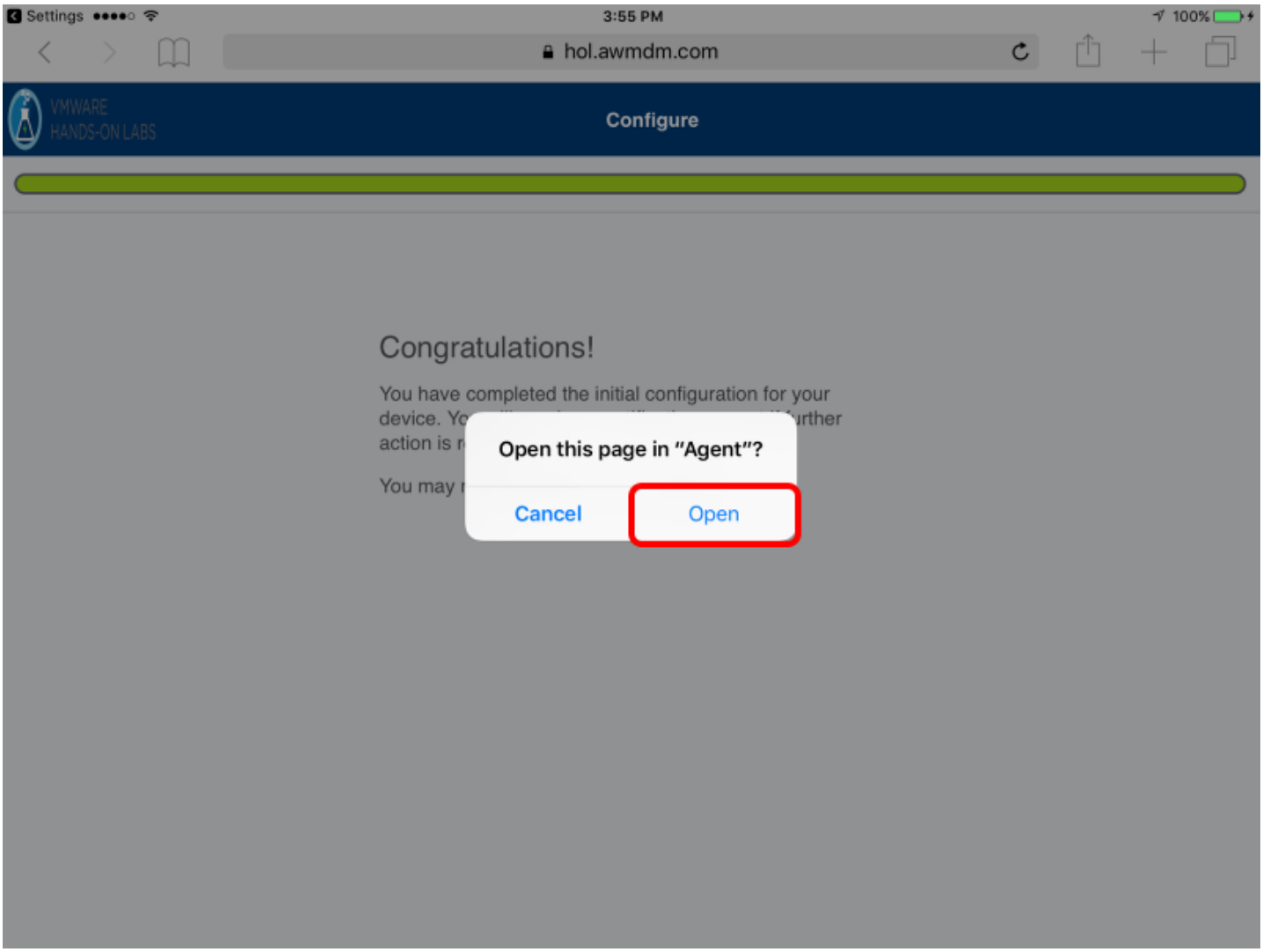
iOS Profile Installation Complete



You should now see the iOS Profile successfully installed.

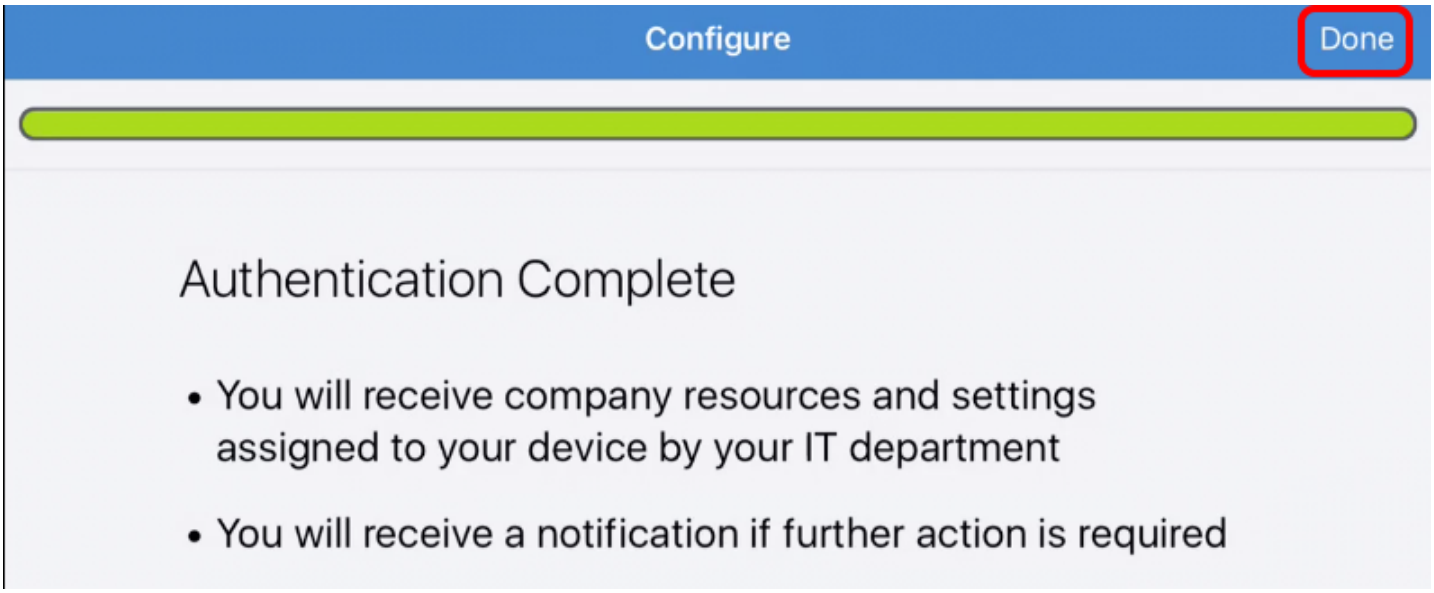
Tap **Done** in the upper right corner of the prompt.

AirWatch Enrollment Success



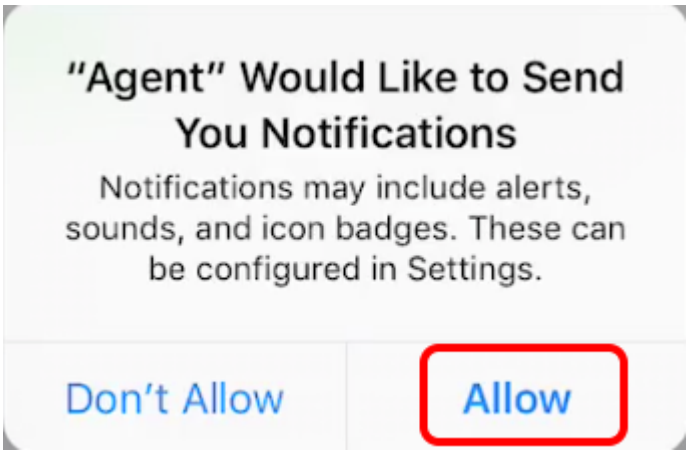
Your enrollment is now completed. Tap **Open** to navigate to the AirWatch Agent.

Accept the Authentication Complete Prompt



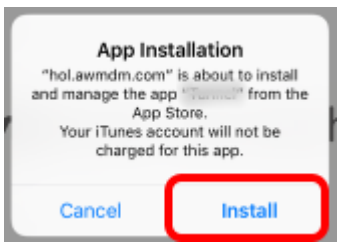
Click on **Done** to continue.

Accept Notification Prompt (IF NEEDED)



Tap **Allow** if you get a prompt for Notifications.

Accept the App Installation (IF NEEDED)

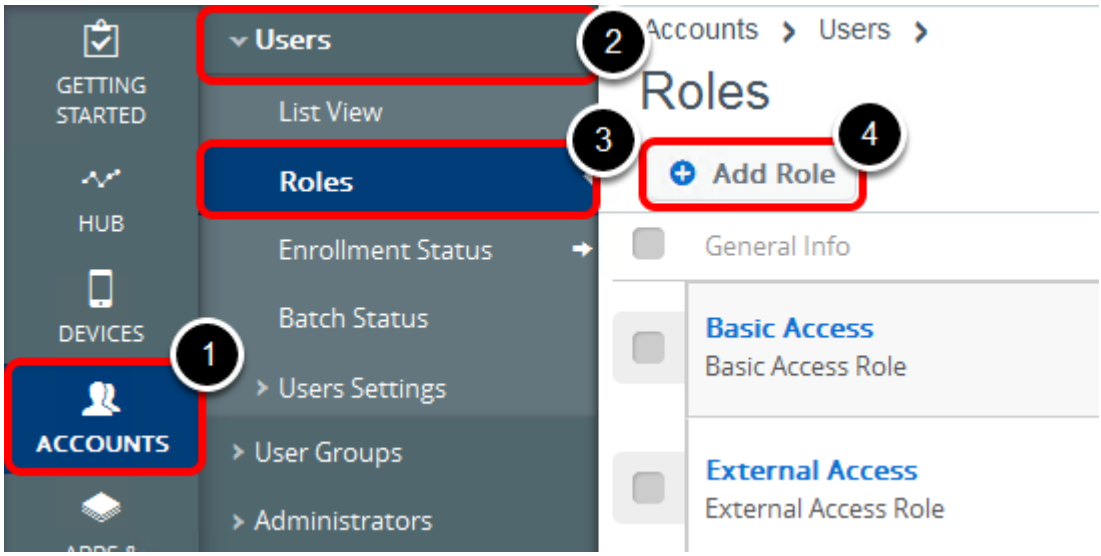


You may be prompted to install a series of applications depending on which Module you are taking. If prompted, tap **Install** to accept the application installation.

User Roles

Now that we have a device enrolled, we will look at how to configure User Roles to enable or prevent your users from performing specific actions in the Self Service Portal.

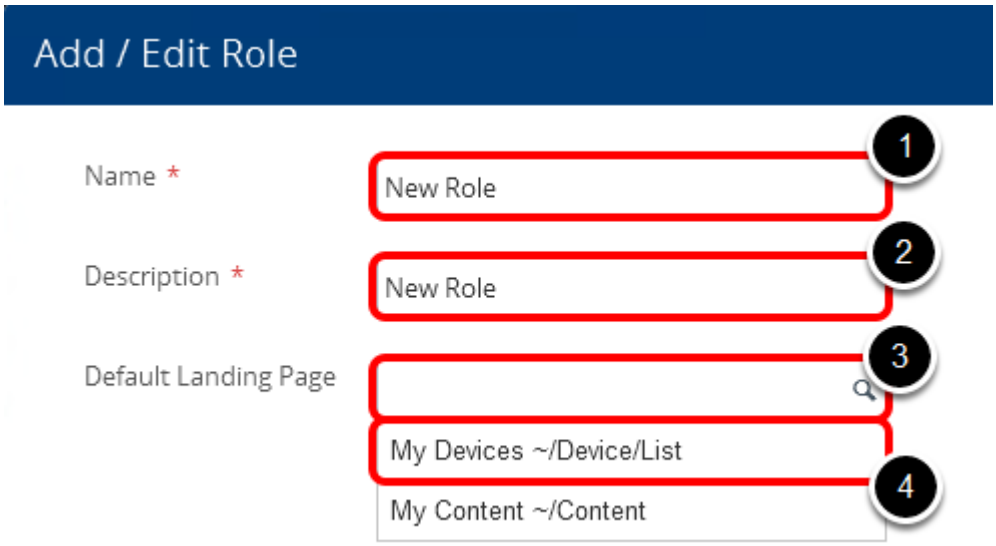
Adding a new Role



Return to the AirWatch Console and perform the following actions.

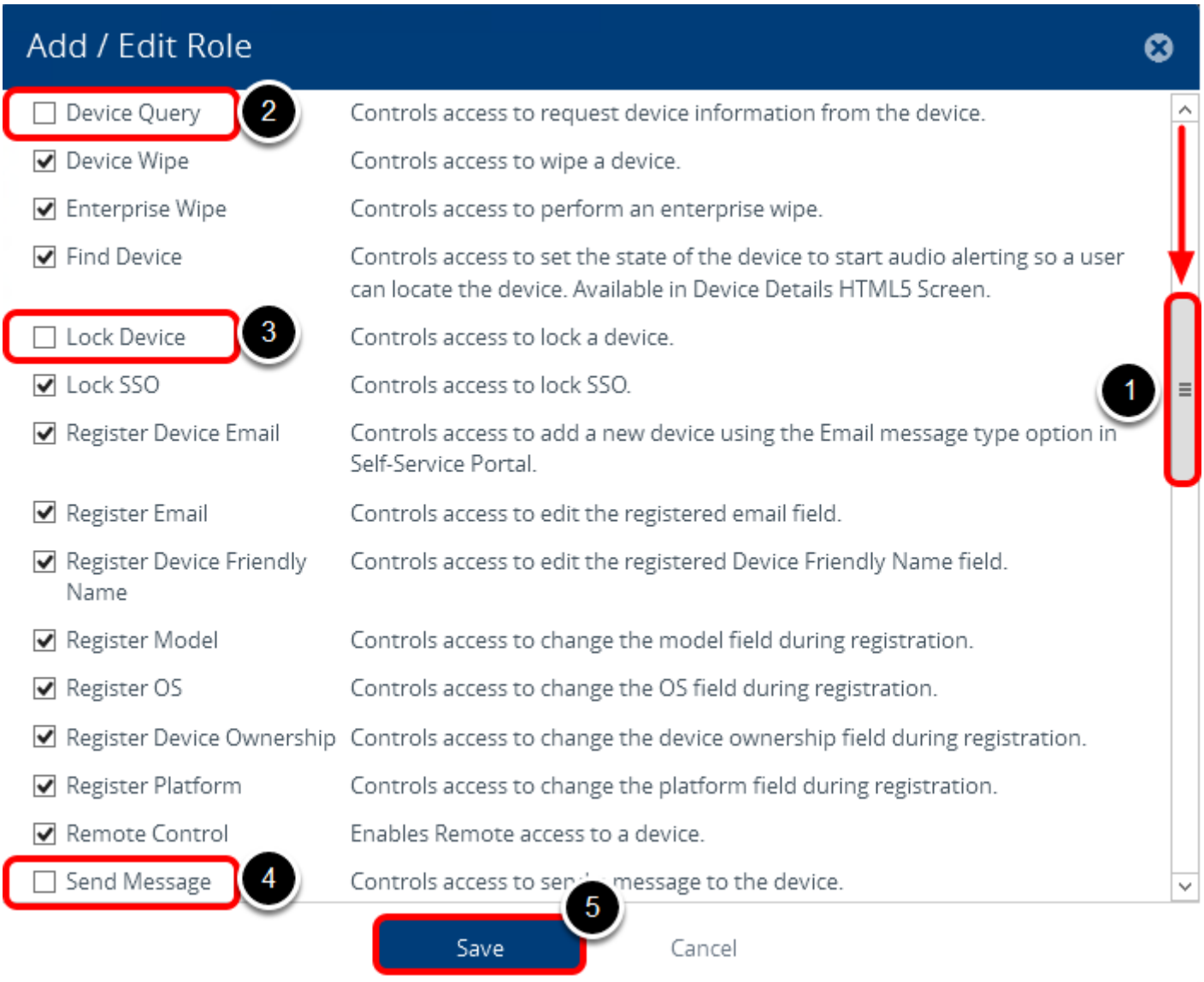
1. Click **Accounts**.
2. Expand **Users**.
3. Click **Roles**.
4. Click **+ Add Role**.

Define Role Details



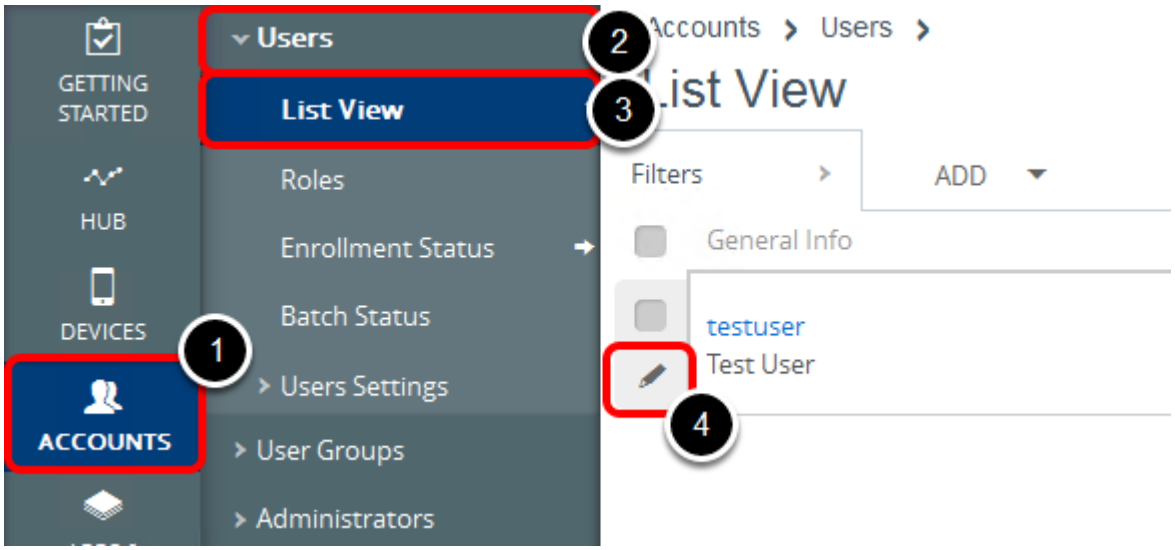
1. Enter "**New Role**" in the **Name** field.
2. Enter "**New Role**" in the **Description** field.
3. Click in the **Default Landing Page** field.
4. Select **My Devices ~/Device/List**.

Choosing Role Permissions



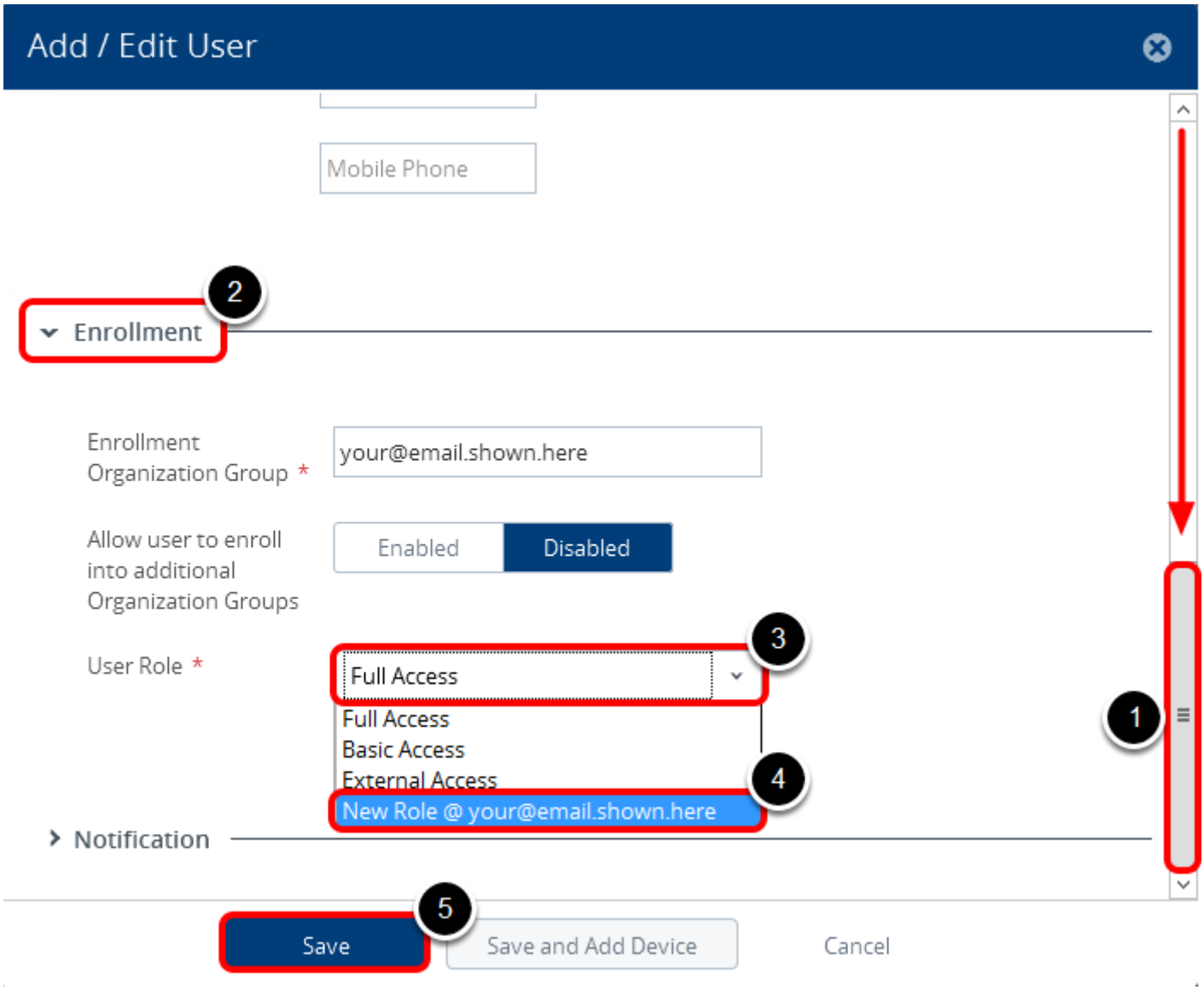
1. Scroll down to find the **Device Query**, **Lock Device**, and **Send message** permissions.
2. Un-check the box next to **Device Query**.
3. Un-check the box next to **Send Message**.
4. Un-check the box next to **Lock Device**.
5. Click **Save**.

Allocating Permissions



1. Click on **Accounts**.
2. Expand **Users**.
3. Click on **List View**.
4. Click on the **pencil icon** to edit the **testuser** account.

Assigning Role



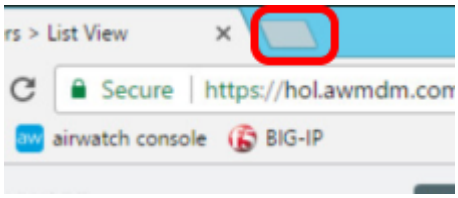
1. Scroll down until you see the **Enrollment** section.
2. Click **Enrollment** to expand the section.
3. Click on **User Role** dropdown to see a list of available User Roles.
4. Select the **New Role** role that you just created.
5. Click **Save**.

Your User's Role has now been changed.

Viewing Role changes in the Self Service Portal (SSP)

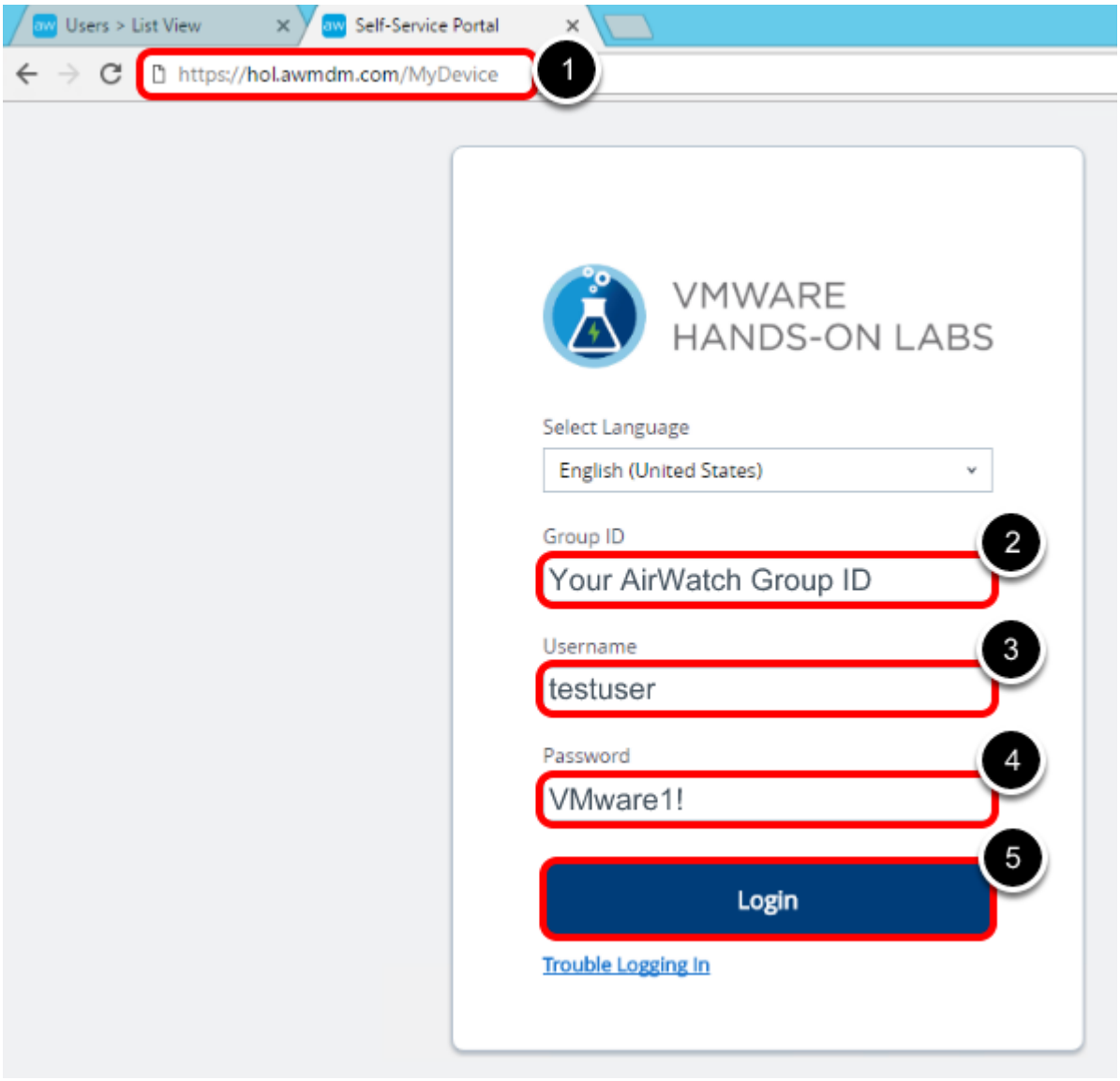
Now that we've assigned the new role to the user we will take a look at the effect this has on the user's ability to perform actions in the Self Service Portal.

Open a New Tab



Click on the tab button in the browser to open a new tab.

Log Into the Self Service Portal

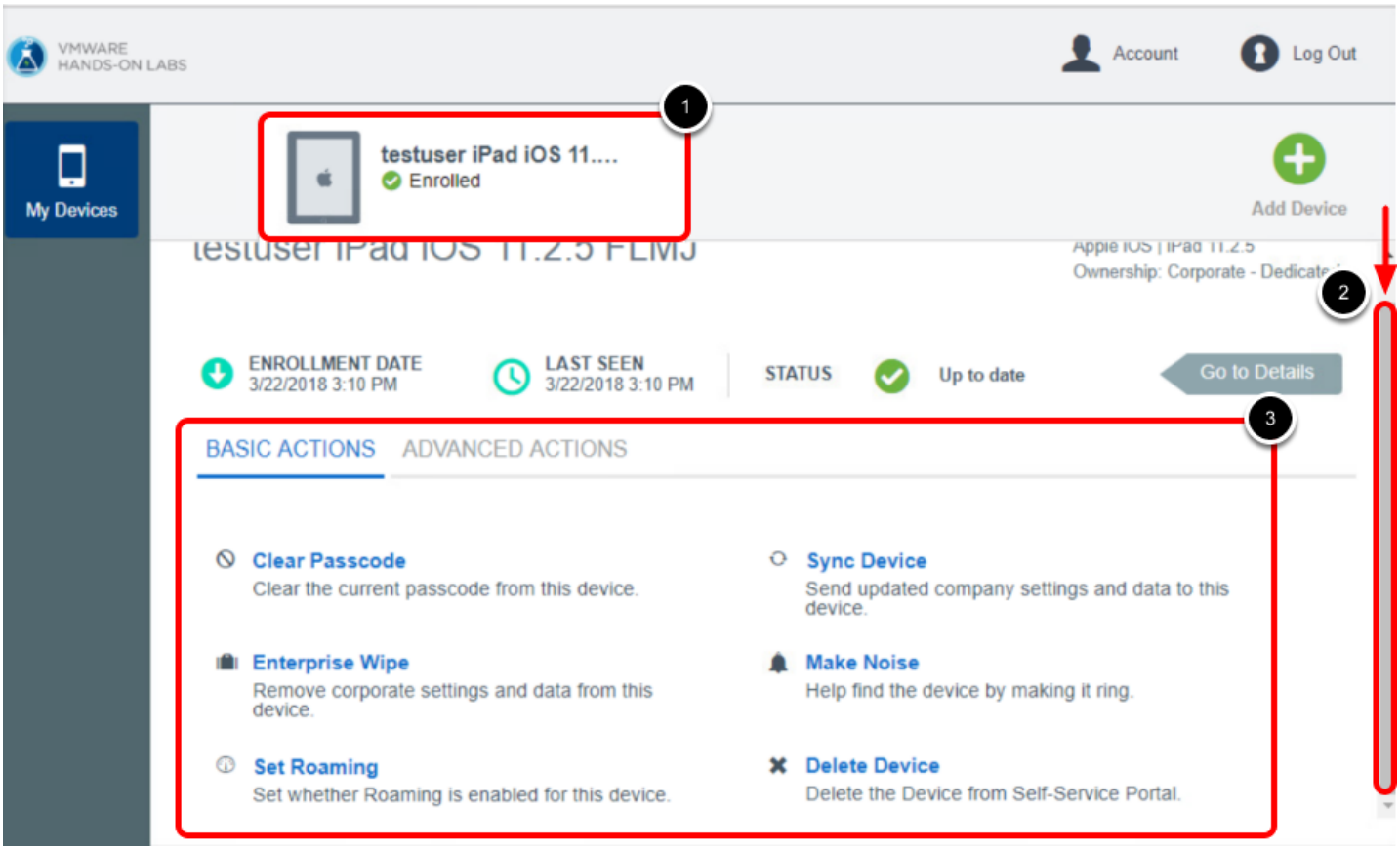


1. Navigate to **https://hol.awmdm.com/mydevice** in the new tab.
2. Enter your **Group ID** in the **Group ID** field. This should be your email username followed by 4 digits. You used this earlier when enrolling your device.
3. Enter **"testuser"** in the **Username** field.

4. Enter "**VMware1!**" in the **Password** field.
5. Click **Login**.

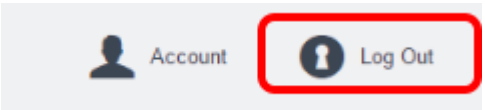
NOTE - If you see a Captcha, the input is case sensitive!

Role Changes in SSP



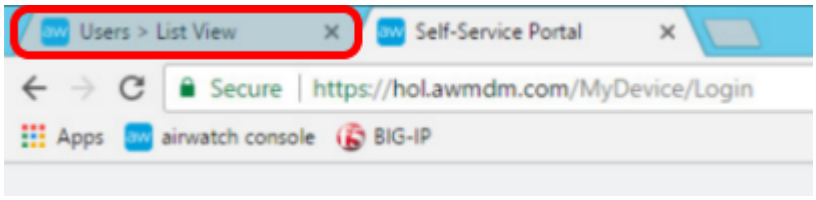
1. Ensure the device you enrolled is selected.
2. You may need to scroll down to see the full list of items under **Basic Actions**.
3. Here you see all of the options available in the Self Service Portal to a user with the New Role we created. Notice that **Lock Device**, **Device Query**, and **Send Message** do not show up in the **Basic Actions** screen. Normally these options would be available to your users, but the **New Role** we created specifically disabled this options for our **testuser** account.

Logout of the Self Service Portal



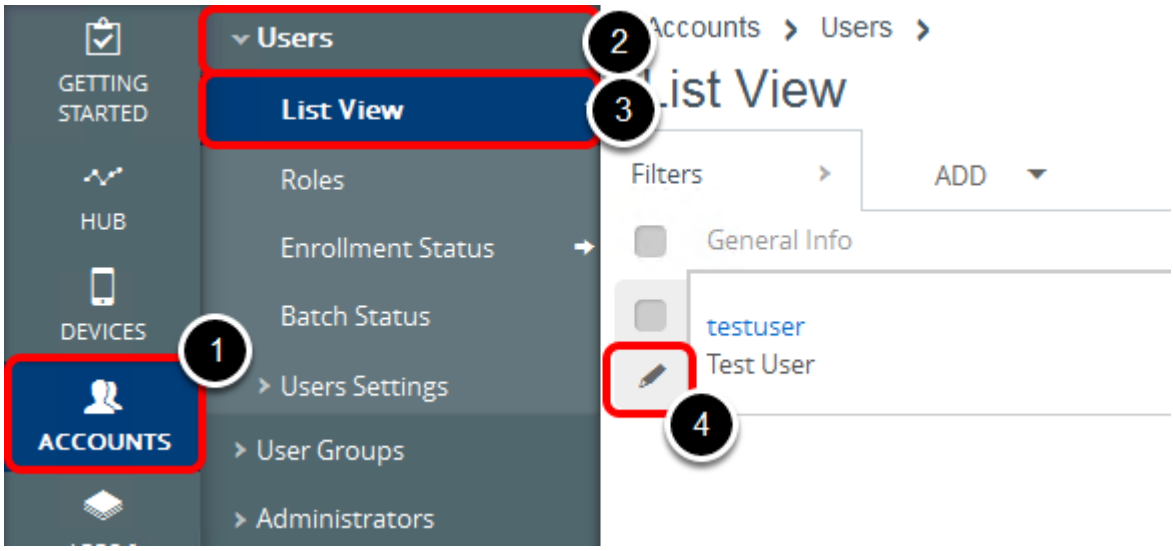
Click **Logout** in the top-right corner of the Self Service Portal.

Change to the AirWatch Console Tab



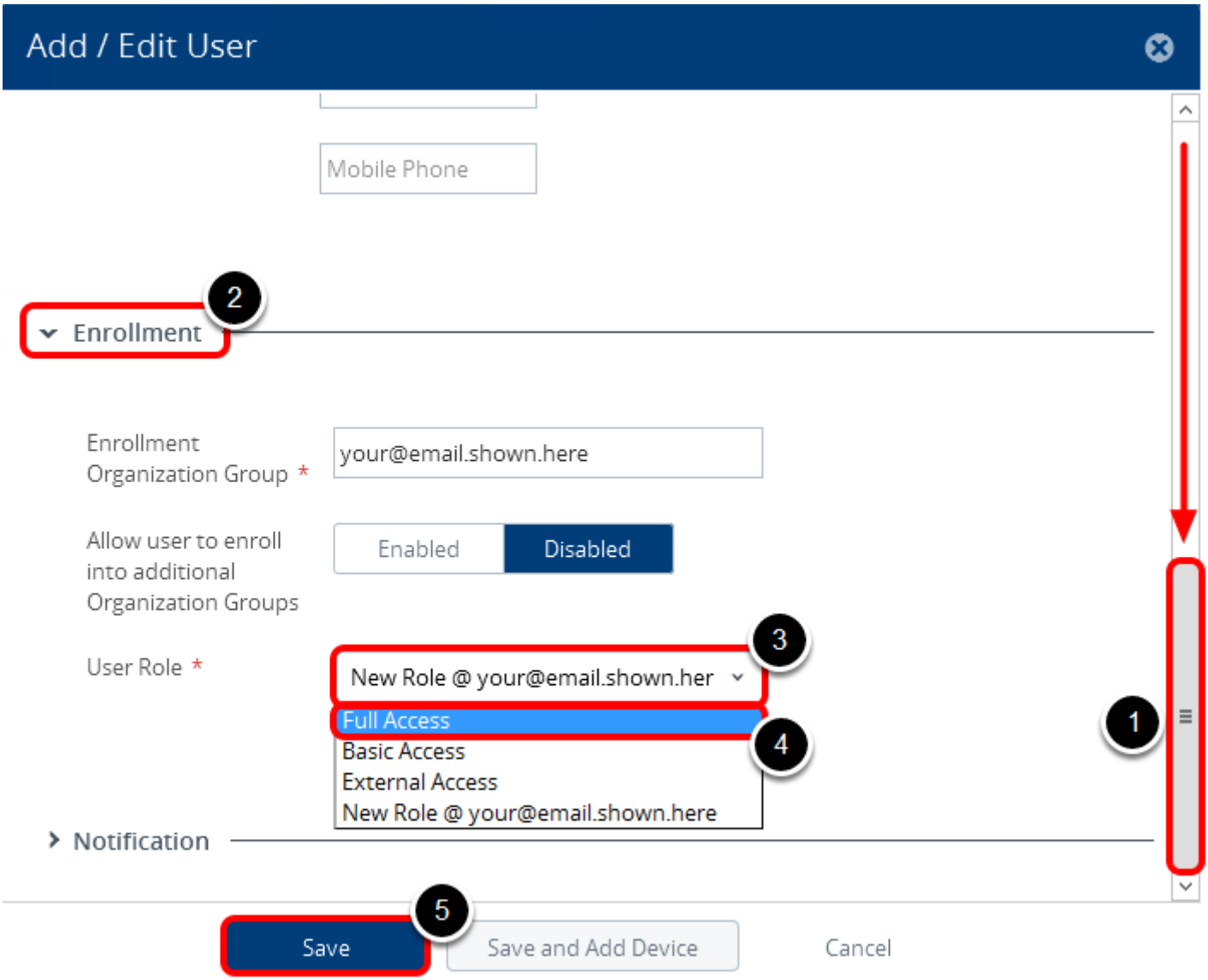
Click on the tab for the AirWatch Console.

Changing Users Role



1. Click on **Accounts**.
2. Expand **Users**.
3. Click on **List View**.
4. Click on the **pencil icon** to edit the **testuser** account.

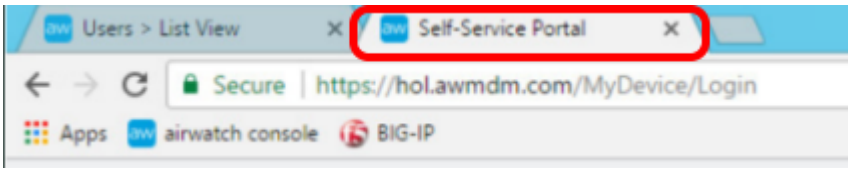
Change User Role Back To Full Access



1. Scroll down until you see the **Enrollment** section.
2. Click **Enrollment** to expand the section.
3. Click on **User Role** dropdown to see a list of available User Roles.
4. Select the **Full Access** role that the user initially had when they were first created.
5. Click **Save**.

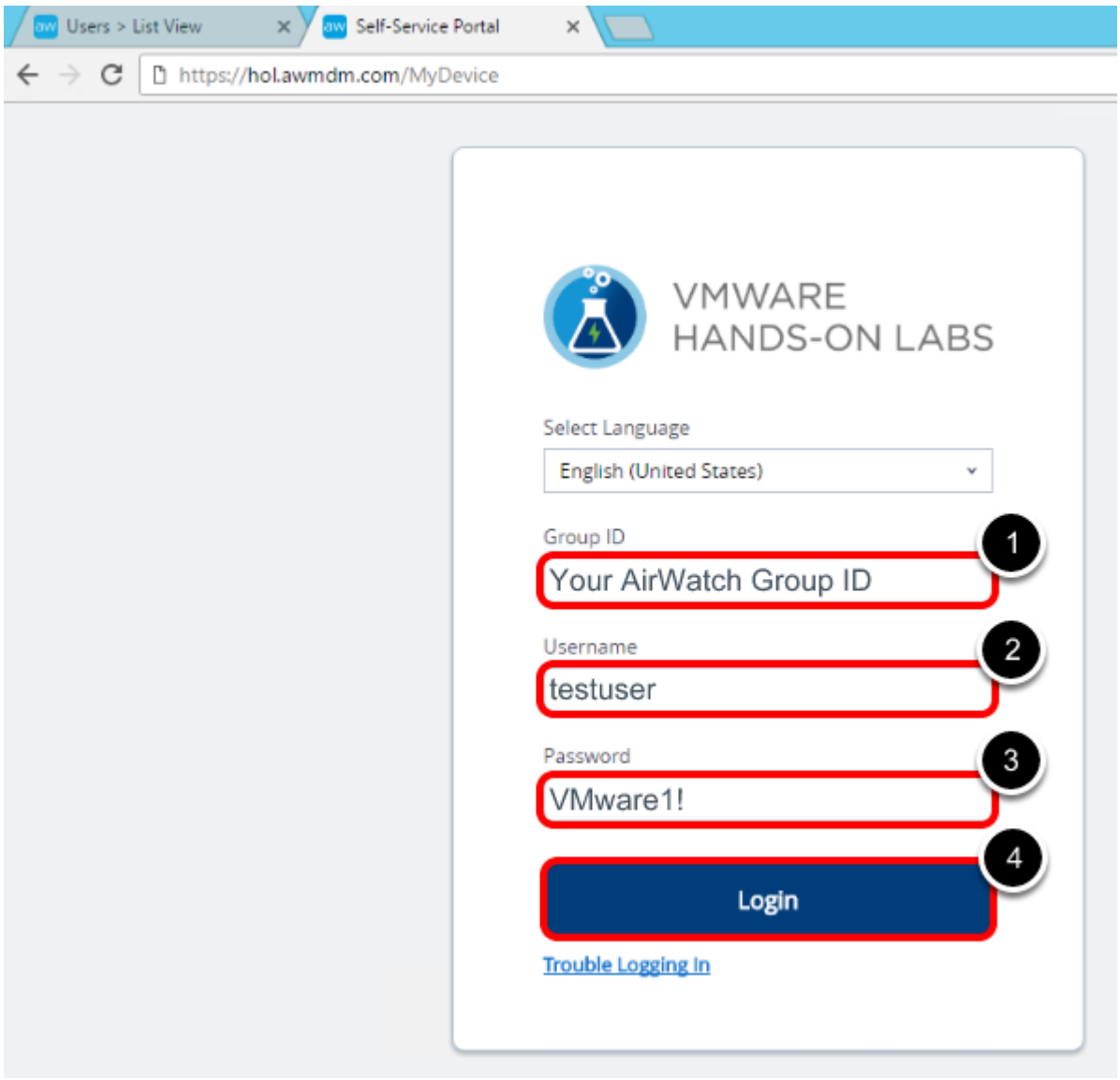
Your User's Role has now been changed.

Change to the SSP Tab



Click on the Browser tab for the **Self Service Portal**.

Log Into the Self Service Portal



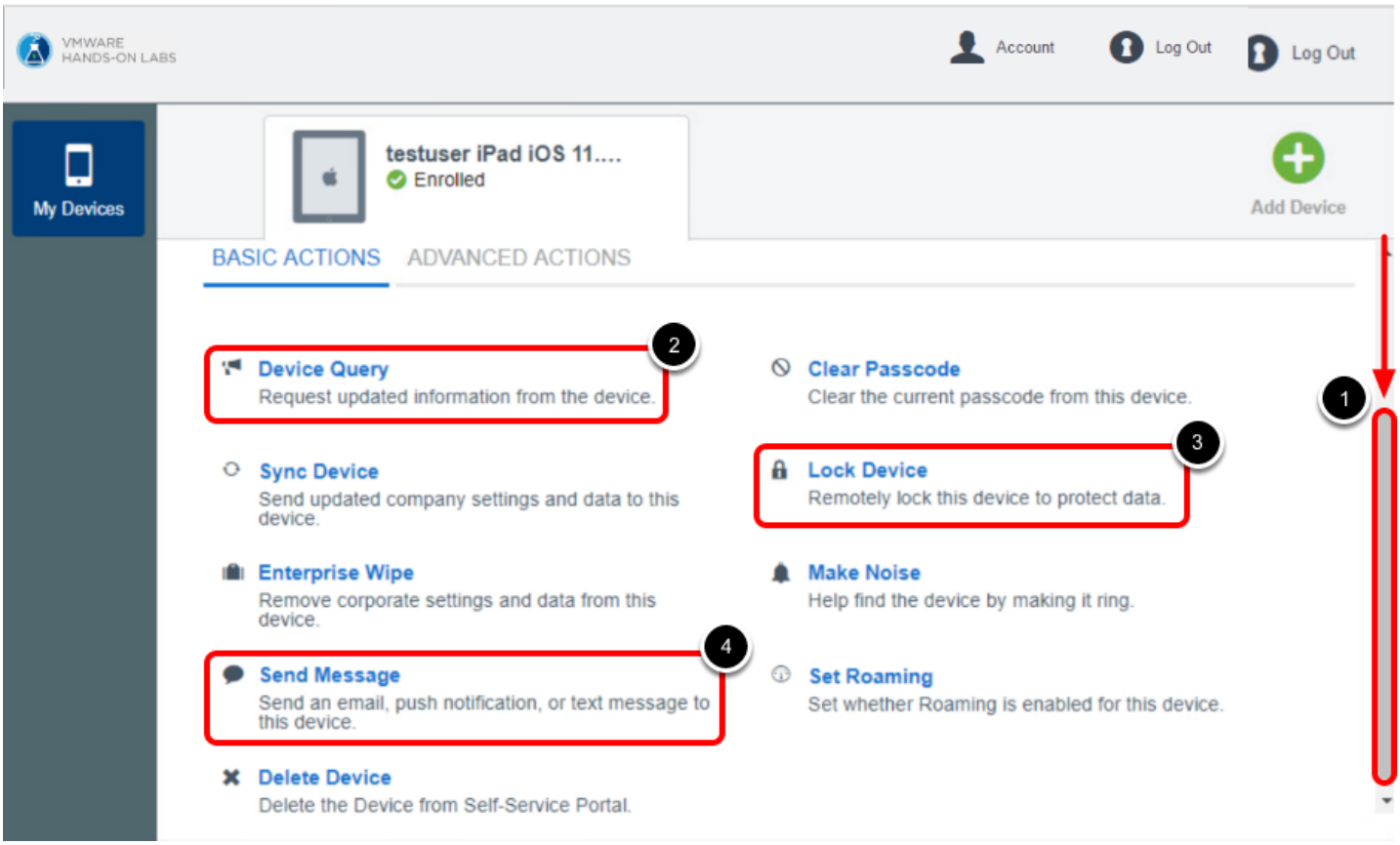
Login to the Self Service Portal again.

1. Enter your **Group ID** in the **Group ID** field. This should be your email username followed by 4 digits. You used this earlier when enrolling your device.
2. Enter **"testuser"** in the **Username** field.

3. Enter **"VMware1!"** in the **Password** field.
4. Click **Login**.

NOTE - If you see a Captcha, the input is case sensitive!

Full Access Roles



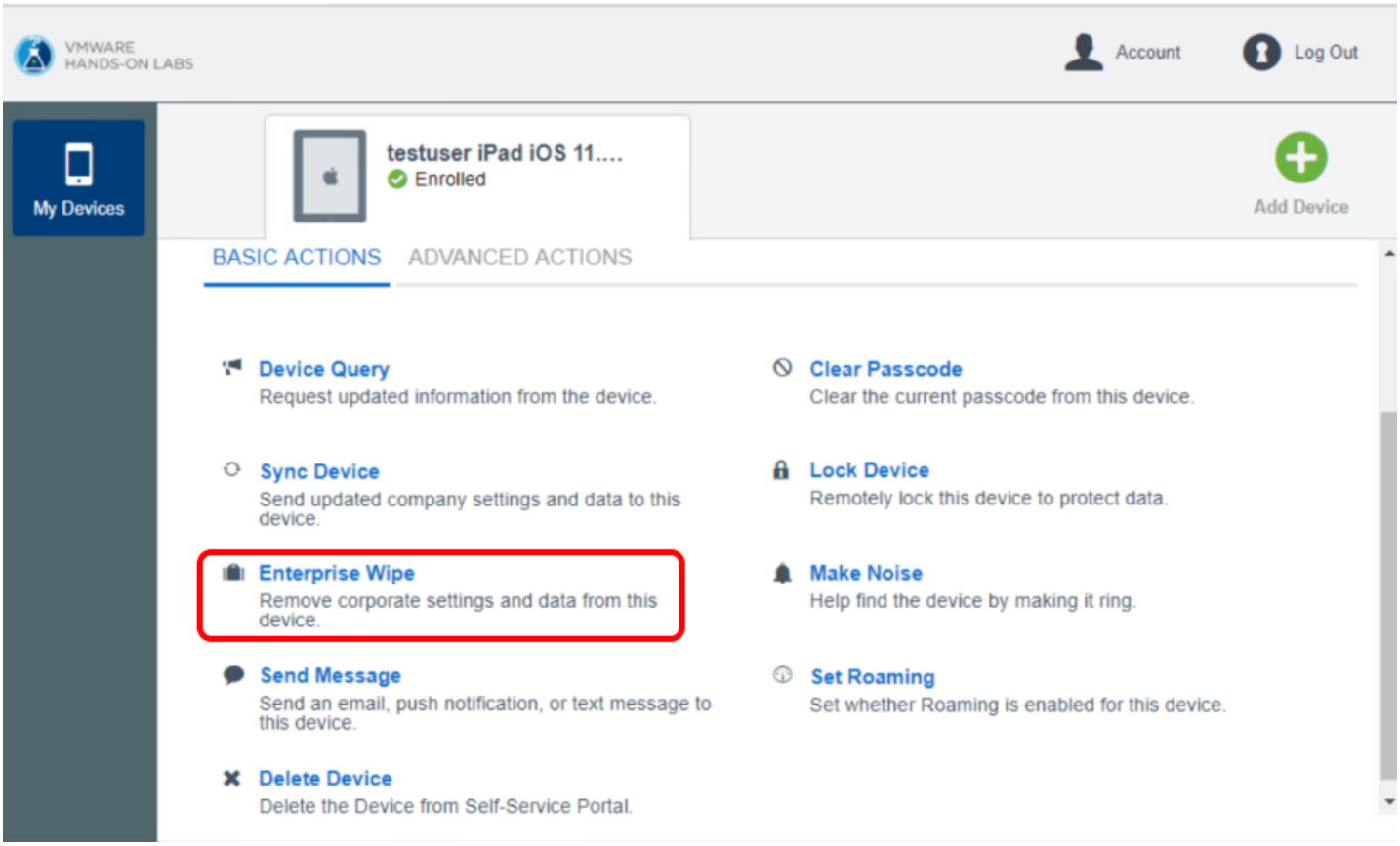
1. You may need to scroll down to view all of the available **Basic Actions**.
2. Notice you have access **Device Query**.
3. Notice you have access to **Lock Device**.
4. Notice you have access to **Send Message**.

Now that your User Role has been restored to Full Access, all of the default Basic Actions are available to your testuser account.

Enterprise Wipe Device From Self Service Portal

Since we've enabled our end users to Enterprise Wipe their devices from the Self Service Portal, we will now un-enroll our iOS device by performing an Enterprise Wipe as an end user.

Enterprise Wipe the Device

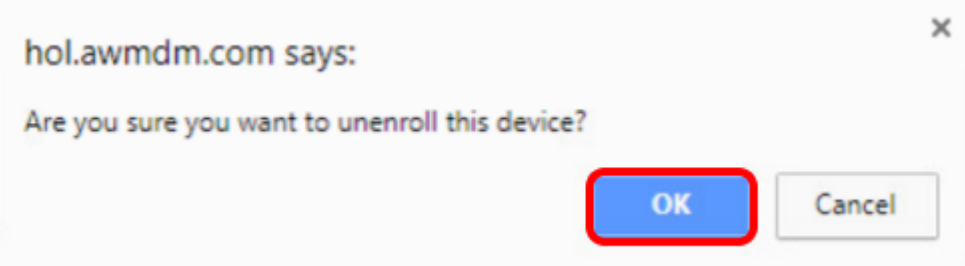


Next, we will Enterprise Wipe the enrolled device from the self service portal.

NOTE - Enterprise Wipe IS NOT a factory reset of the device, it will only remove the data that has been delivered to your device through AirWatch.

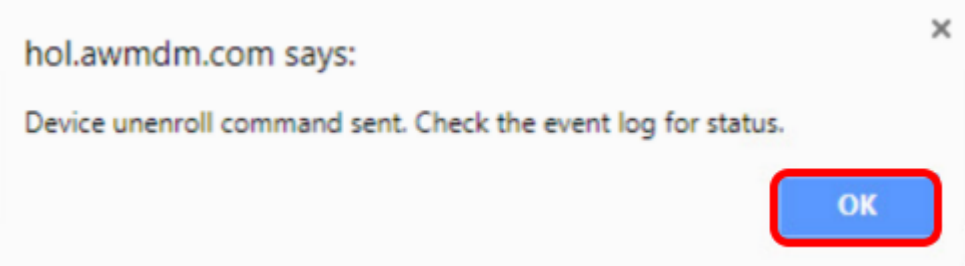
Click **Enterprise Wipe**.

Confirm Enterprise Wipe



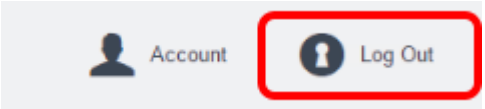
Confirm the Enterprise Wipe by clicking **OK**.

Accept the Pop-Up Message



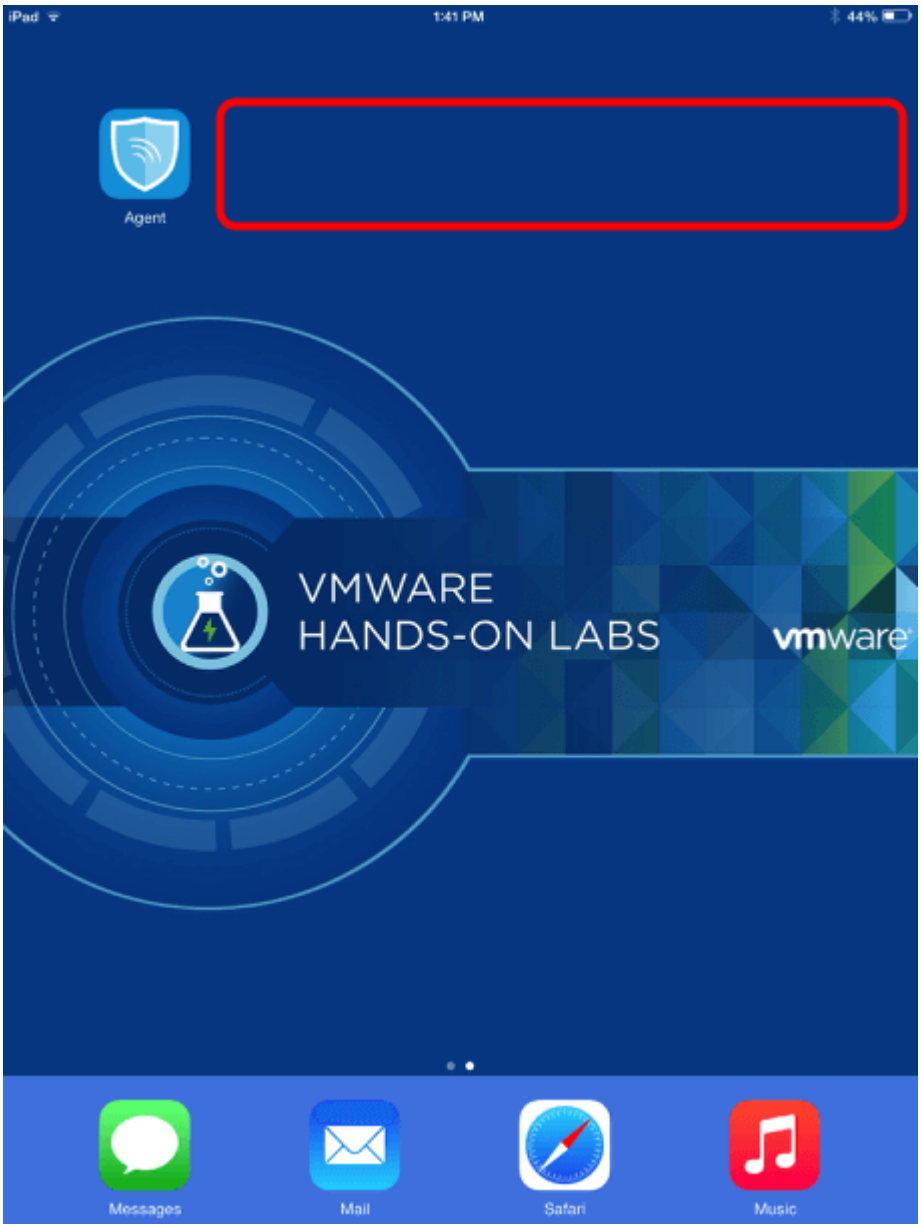
Click **OK** acknowledge that the Enterprise Wipe command was successfully sent.

Logout of the Self Service Portal



Click **Logout**.

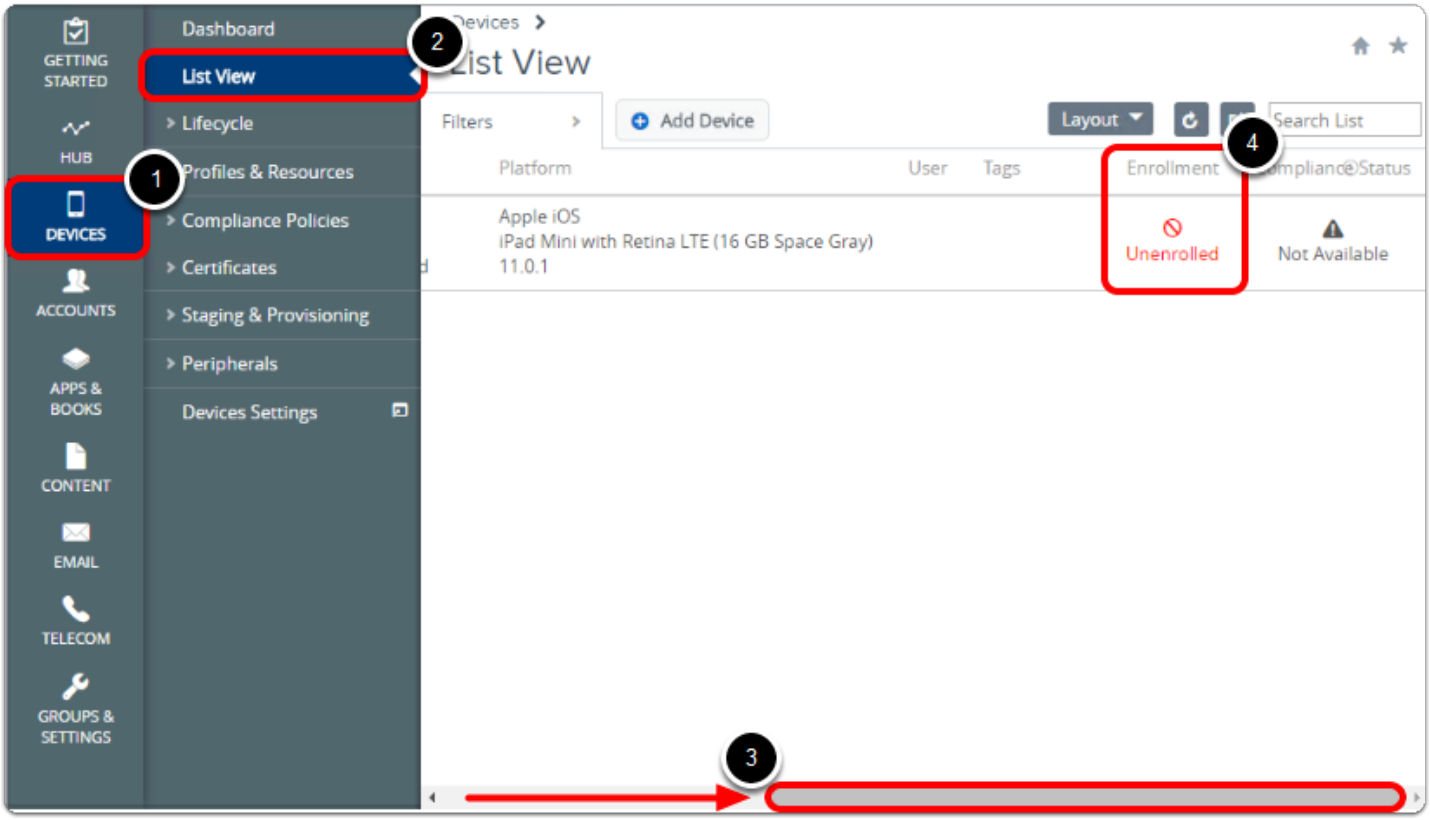
Verify the Device Un-Enrollment



Press the Home button on the device to go back to the home screen. The applications pushed through AirWatch should have been removed from the device.

NOTE - The App Catalog and any settings pushed through AirWatch management should have been removed. The Agent will still be on the device because that was downloaded manually from the App Store. Due to lab environment settings, it may take some time for the signal to traverse through the various networks out and back to your device.

Verify the Device Un-Enrollment in AirWatch Console



You can confirm that the device was un-enrolled through the AirWatch Console, as well.

1. Click Devices.
2. Click List View.
3. Find the device you enrolled, you may need to scroll to the right to view the Enrollment status.
4. Confirm the Enrollment status is showing as **Unenrolled**.

Conclusion

As seen, role based access allows you to configure what actions are available for both AirWatch administrators and users.

Administrator Roles define what functionality each admin had access to. This provides a more focused admin experience, ensuring your admins with limited permissions are only granted access to the items that they need for their day-to-day tasks. It also helps prevents unwanted changes by limiting what actions can be accessed by admins using certain roles.

User Roles define what actions users are allowed to take through the AirWatch Self Service Portal. Limiting these options can also help prevent your users from taking unwanted action, such as un-enrolling their own devices.

Experimenting with these roles and finding the right solution for your administrators and users is important to enable them with the appropriate access they need while ensuring they do not have access to unneeded actions. These roles can be easily removed, added, or changed when you need to adapt your use cases.

This concludes the AirWatch Console Roles module

Module 5 - Branding the Workspace ONE UEM Console, SSP and SCL (30 min)

Introduction

Branding allows you to provide a more familiar and personalized experience to both your AirWatch administrators and your end users. The AirWatch Console, Self Service Portal, and various applications can be branded to match your organization and provide a more cohesive experience from device enrollment to every day use. This module will explore how to enable and configure branding for the AirWatch Console, Self Service Portal, and the VMware Content Locker and VMware Browser apps.

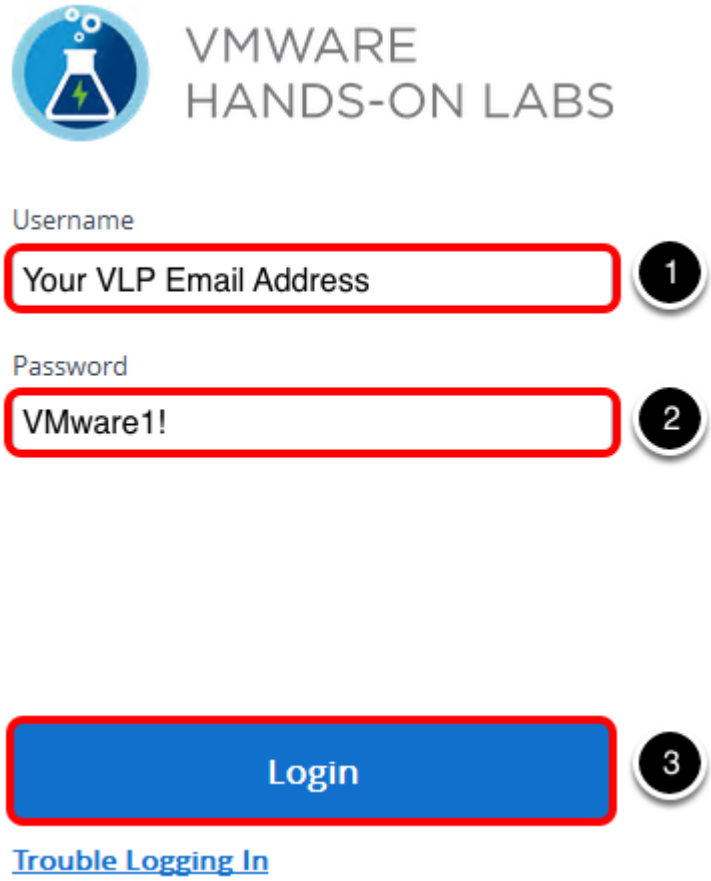
Login to the AirWatch Console

To perform most of the lab you will need to login to the AirWatch Management Console.

Launch Chrome Browser

Double-click the **Chrome** Browser on the lab desktop.

Authenticate to the AirWatch Administration Console



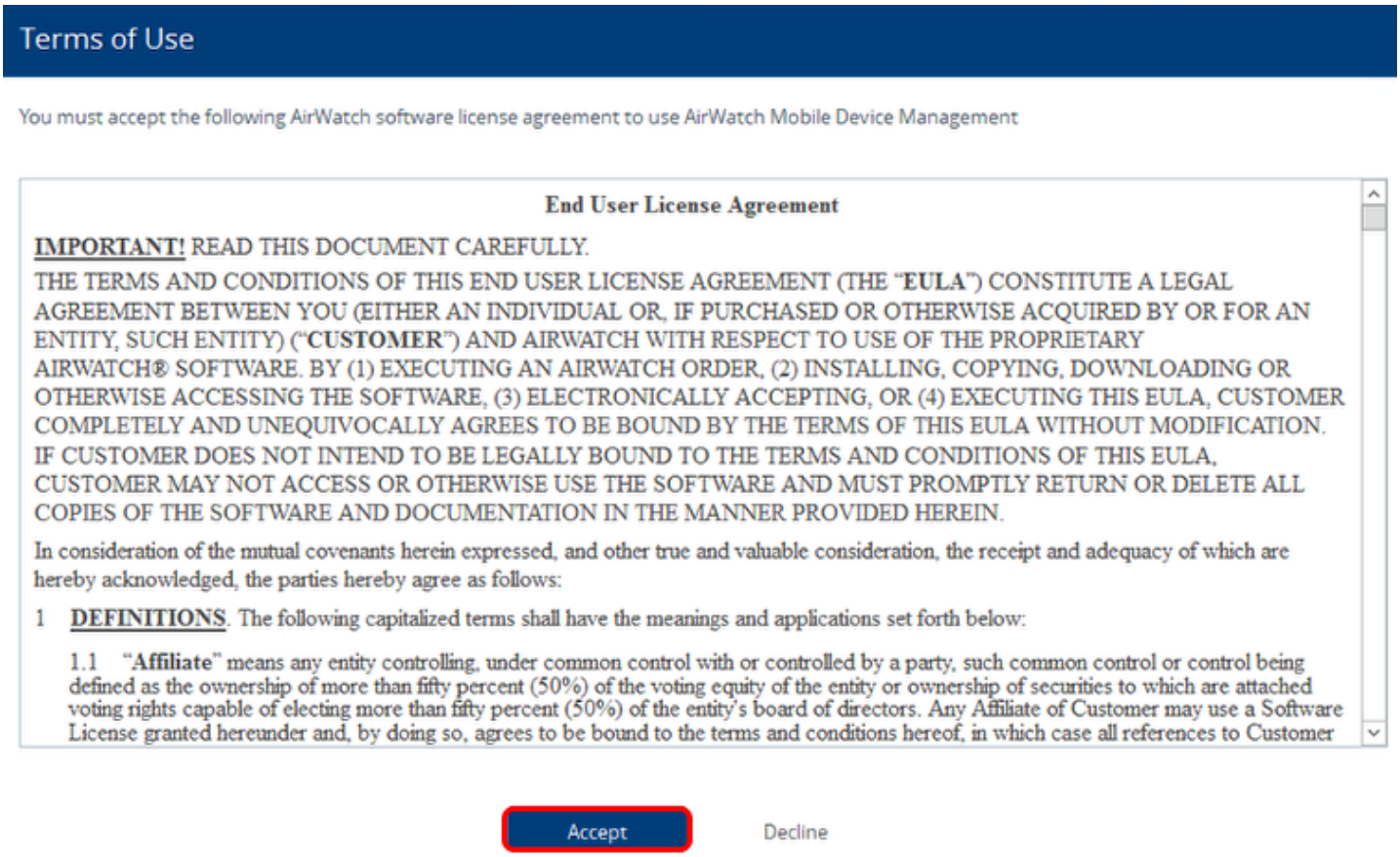
The default home page for the browser is **https://hol.awmdm.com**. Enter your AirWatch Admin Account information and click the **Login** button.

NOTE - If you see a Captcha, please be aware that it is case sensitive!

1. Enter your **Username**. This is you **email address** that you have associated with your **VMware Learning Platform (VLP) account**.
2. Enter **"VMware1!"** for the **Password** field.
3. Click the **Login** button.

NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the AirWatch Hands On Labs server.

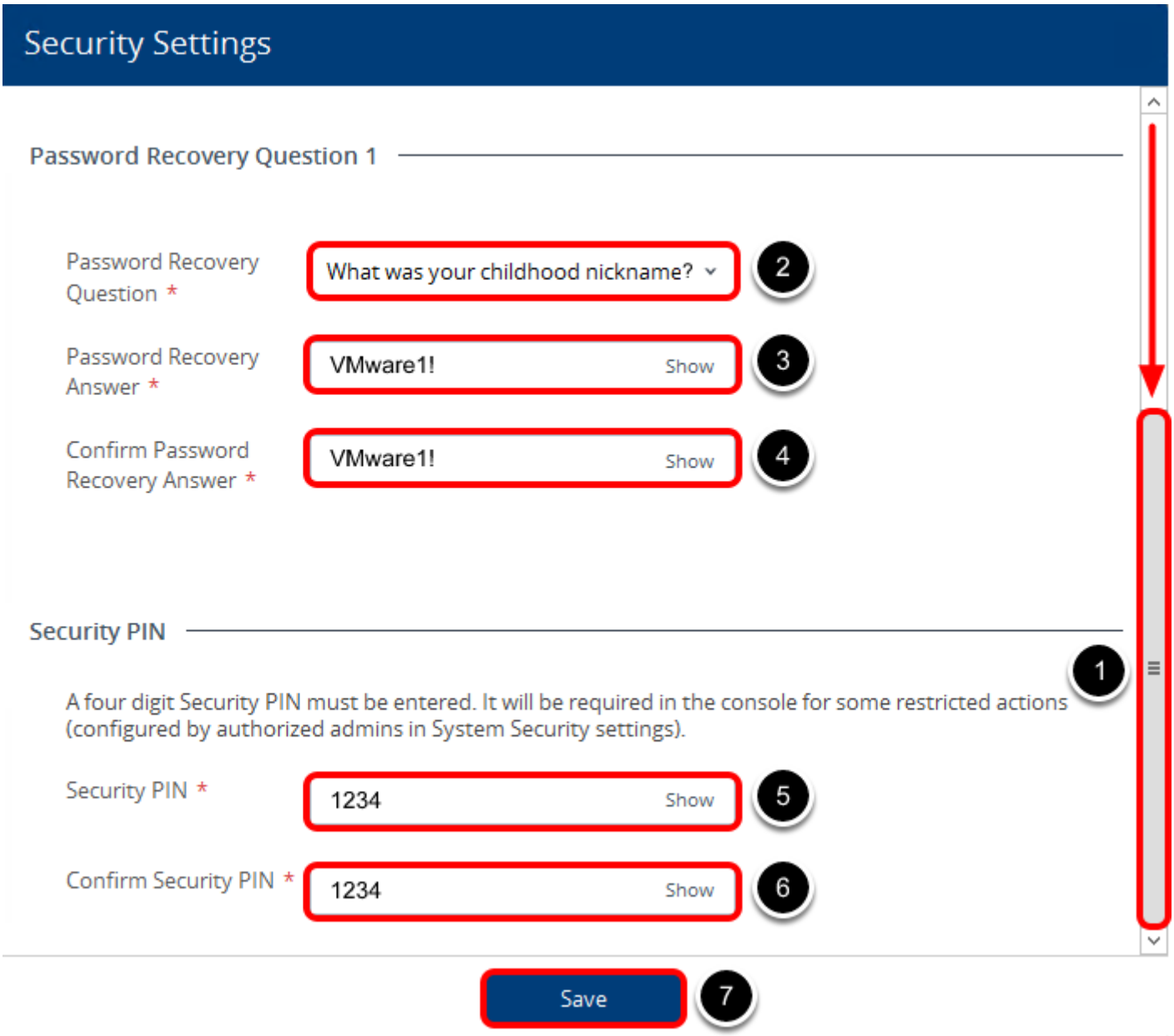
Accept the End User License Agreement



NOTE - The following steps of logging into the Administration Console will only need to be done during the initial login to the console.

You will be presented with the AirWatch Terms of Use. Click the **Accept** button.

Address the Initial Security Settings

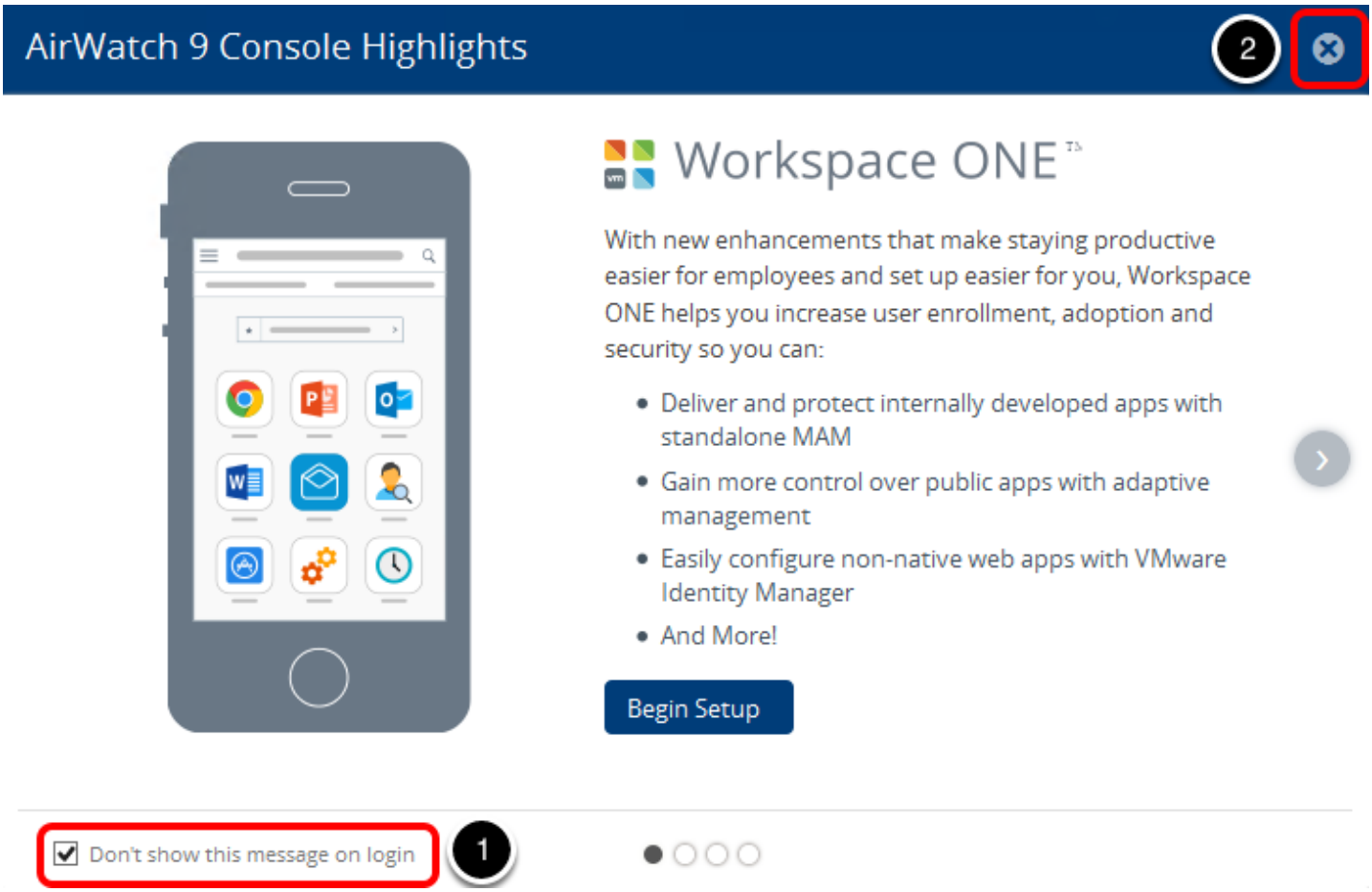


After accepting the Terms of Use, you will be presented with a **Security Settings** pop-up. The **Password Recovery Question** is in case you forget your admin password and the **Security PIN** is to protect certain administrative functionality in the console.

1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a **question** from the **Password Recovery Question** drop-down (default selected question is ok here).
3. Enter **"VMware1!"** in the **Password Recovery Answer** field.
4. Enter **"VMware1!"** in the **Confirm Password Recovery Answer** field.
5. Enter **"1234"** in the **Security PIN** field.
6. Enter **"1234"** in the **Confirm Security PIN** field.

7. Click the **Save** button when finished.

Close the Welcome Message



After completing the Security Settings, you will be presented with the AirWatch Console Welcome pop-up.

1. Click on the **Don't show this message again** check box.
2. Close the pop-up by clicking on the **X** in the upper-right corner.

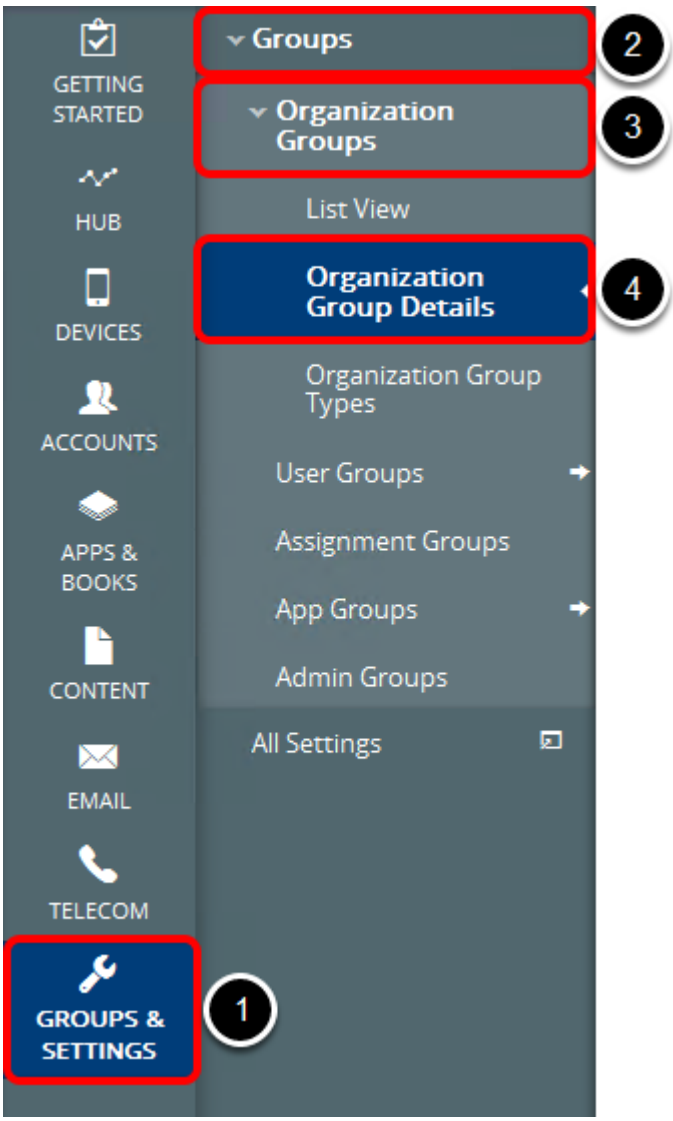
AirWatch Console & Self Service Portal Branding

This section will introduce you to Branding the AirWatch Web Console and Self Service Portal. Many customers alter the branding of their Web Console and Self Service Portal to match their corporate branding. In this section we will browse the available options for branding these two websites.

Create a Child Organization Group For Branding

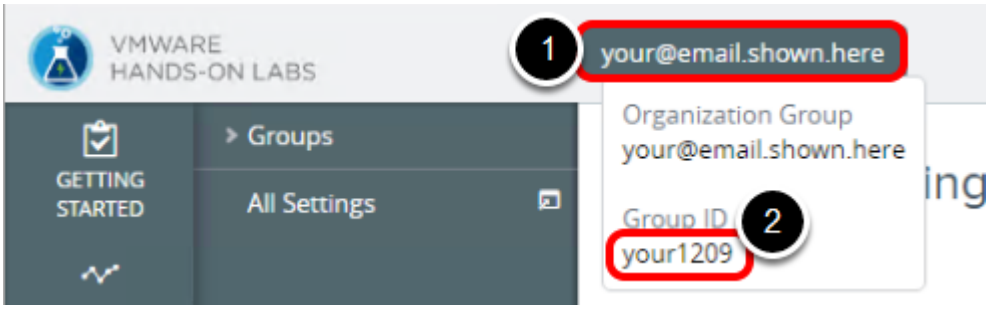
Because this lab will change the look and feel of the AirWatch Management Console you will create a child Organization Group under your main group to do this module.

Navigate to Organization Group Details



1. Click **Groups & Settings**.
2. Expand **Groups**.
3. Expand **Organization Groups**.
4. Click **Organization Group Details**.

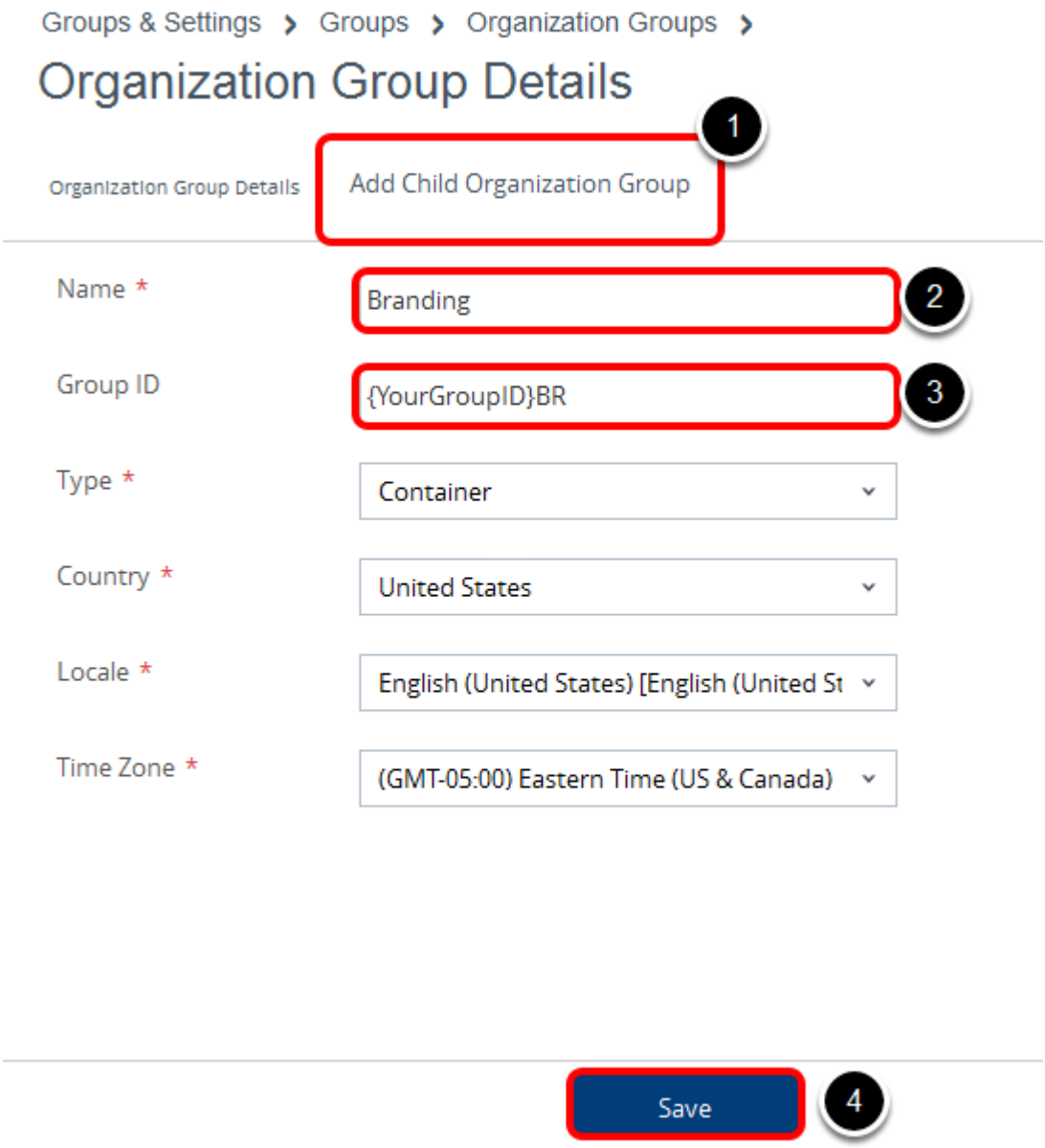
Finding your Group ID



First, make sure you know what your **Organization Group ID** is:

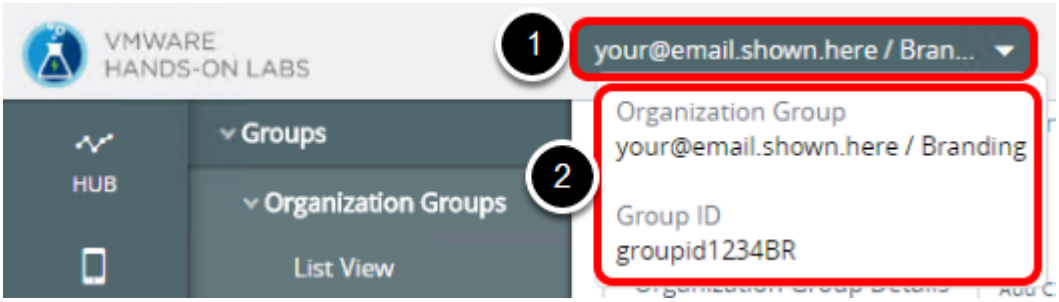
1. To find the Group ID, hover your mouse over the Organization Group tab at the top of the screen. Look for the email address you used to log in to the lab portal.
2. Your **Group ID** is displayed at the bottom of the Organization Group pop up. The **Group ID** is required in the following steps.

Add the Branding Child Organization Group



1. Click the **Add Child Organization Group** tab.
2. Enter **"Branding"** for the **Name** field.
3. For the Group ID field, enter your Group ID (from the previous step) with "BR" (short for "Branding") appended to the end.
   EXAMPLE - If your Group ID is **"groupid1234"**, then the Child Group ID you would use is **"groupid1234BR"**.
   NOTE - You will need this new Group ID for future steps, so be sure to note this Group ID.
4. Click **Save**.

Note Your Organization Group has Changed



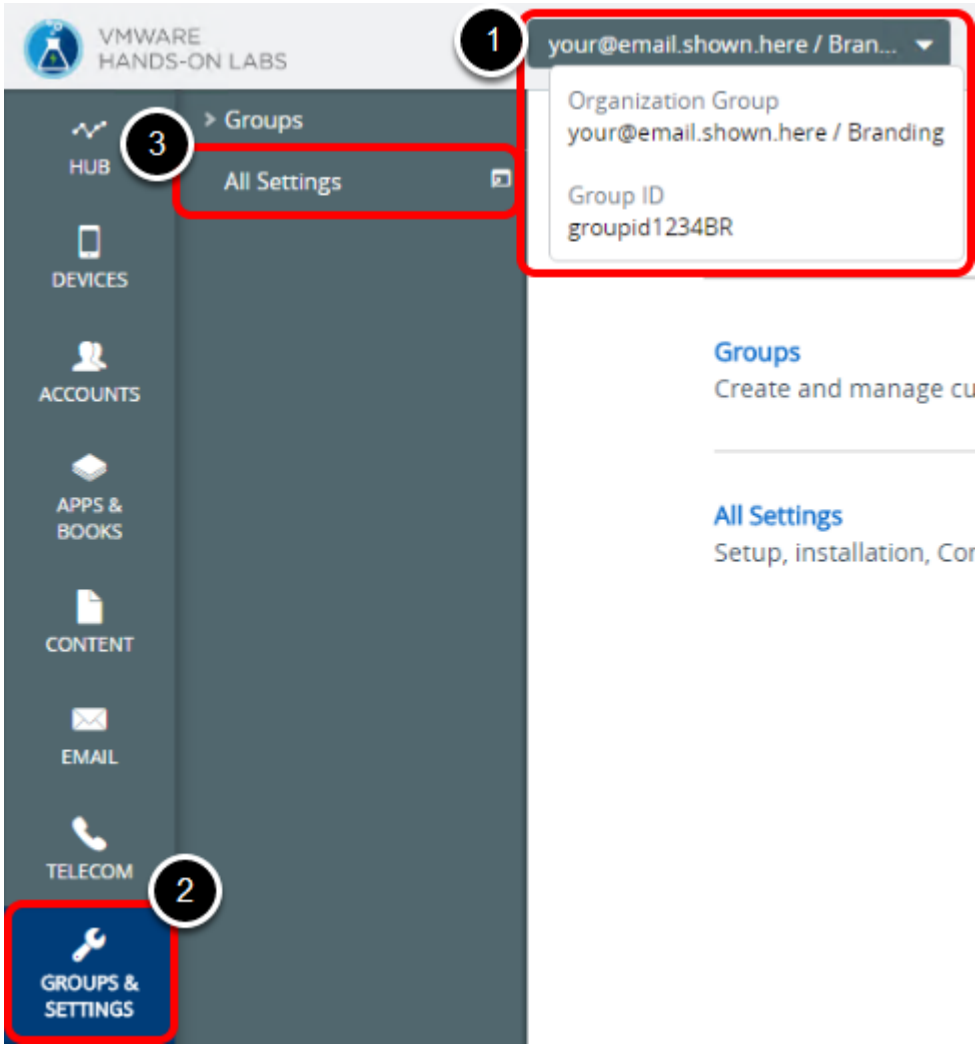
Once the save process completes, you will notice that your current Organization Group has been changed to the new **Branding** Organization Group you just created.

1. Hover your mouse over the **Organization Group** button.
   NOTE: The name on the button will be "{Parent Organization Group} / Branding".
2. Notice that the Organization Group and Group ID reflect the Branding group details you just created.

Company Logo

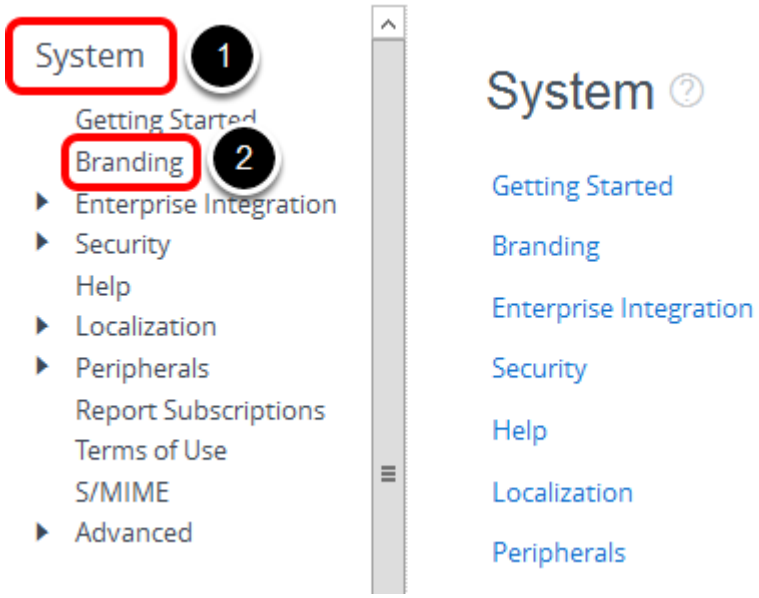
This step shows you how to change the Company Logo, which is seen at the AirWatch Console Login screen, the corner of the AirWatch Console screen, and the Self Service Portal.

Branding Settings



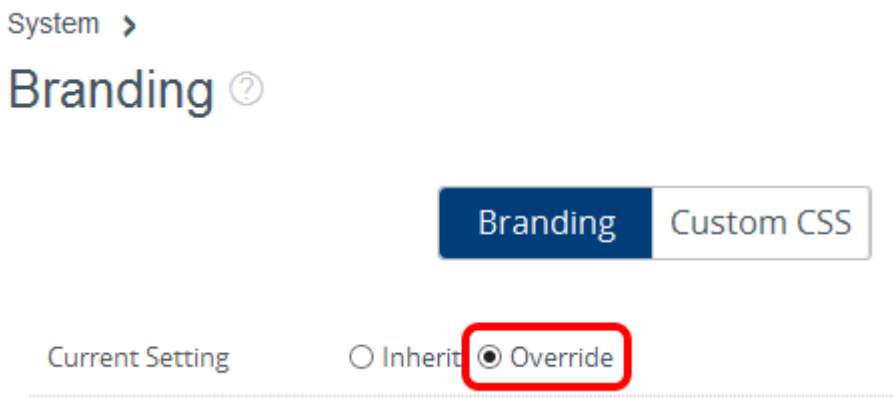
1. Confirm you are at the **Branding** Organization Group. Most tasks for this lab will be performed at this Organization Group level.
   NOTE: If you are not at the "Branding" Organization Group, switch by clicking the Organization Group button and selecting the "Branding" group in the dropdown menu.
2. Click **Groups & Settings**.
3. Click **All Settings**.

Branding Settings



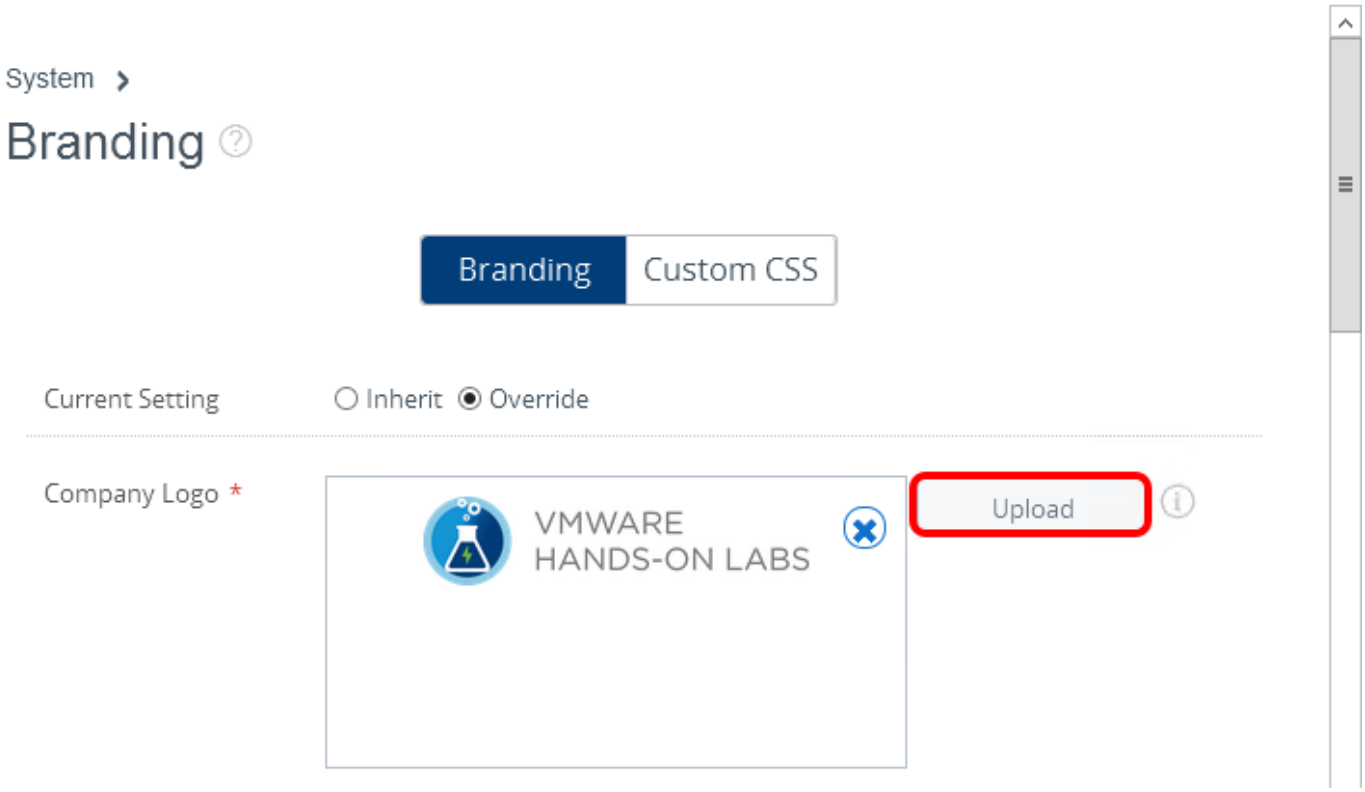
1. Click **System**.
2. Click **Branding**.

Override the Settings



Set the **Current Setting** to **Override**.

Configure the Primary Logo

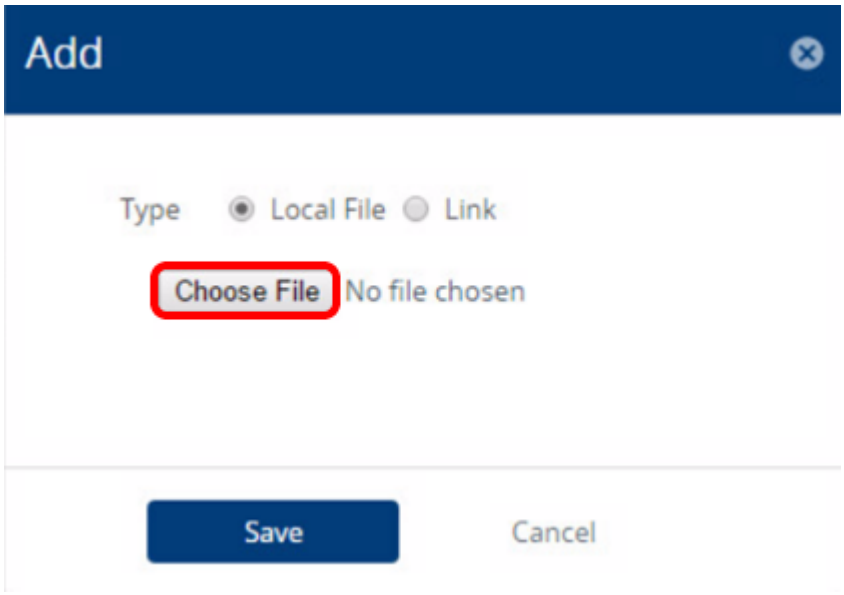


The Company Logo is the icon located at the AirWatch Console Login screen, as well as at the top left corner of your AirWatch Console.

NOTE - These branding updates will also be applied to the Self Service Portal.

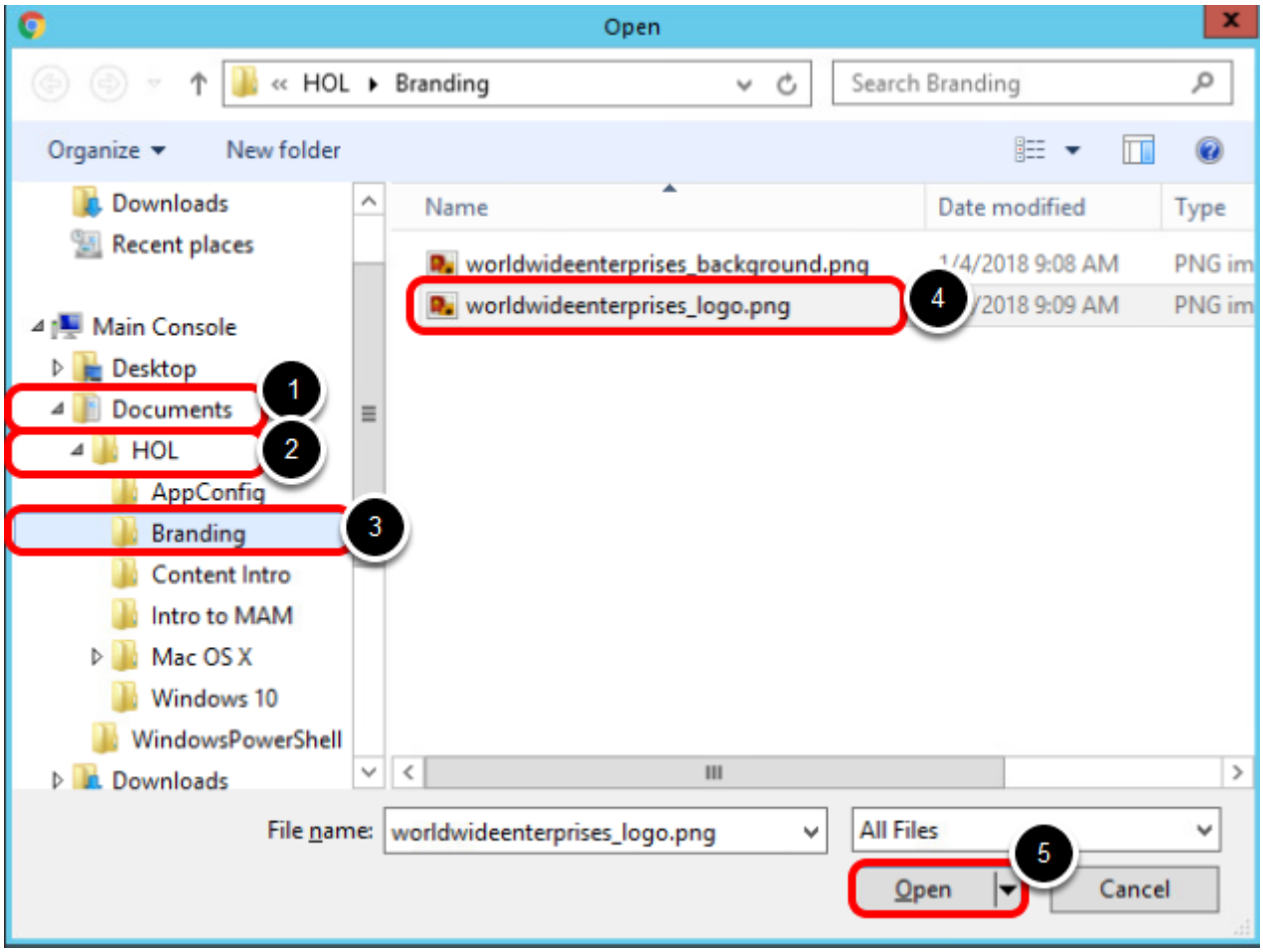
Click **Upload** by the Company Logo setting.

Uploading a File



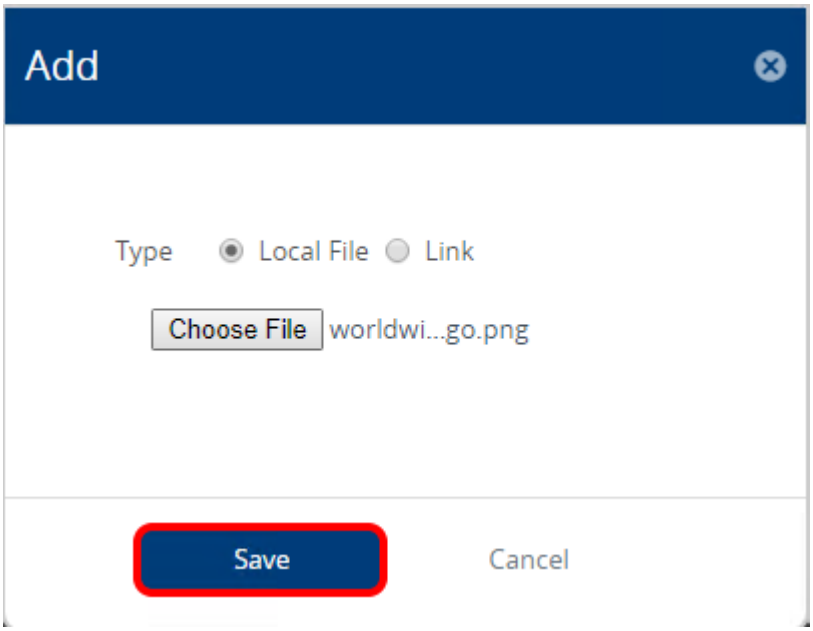
Click **Choose File**.

Selecting the World Wide Enterprises Logo



1. Click **Documents** in the left pane.
2. Click on the **HOL** folder.
3. Click on the **Branding** folder.
4. Click the **worldwideenterprises_logo.png** file.
5. Click **Open**.

Saving the World Wide Enterprises Corp Logo

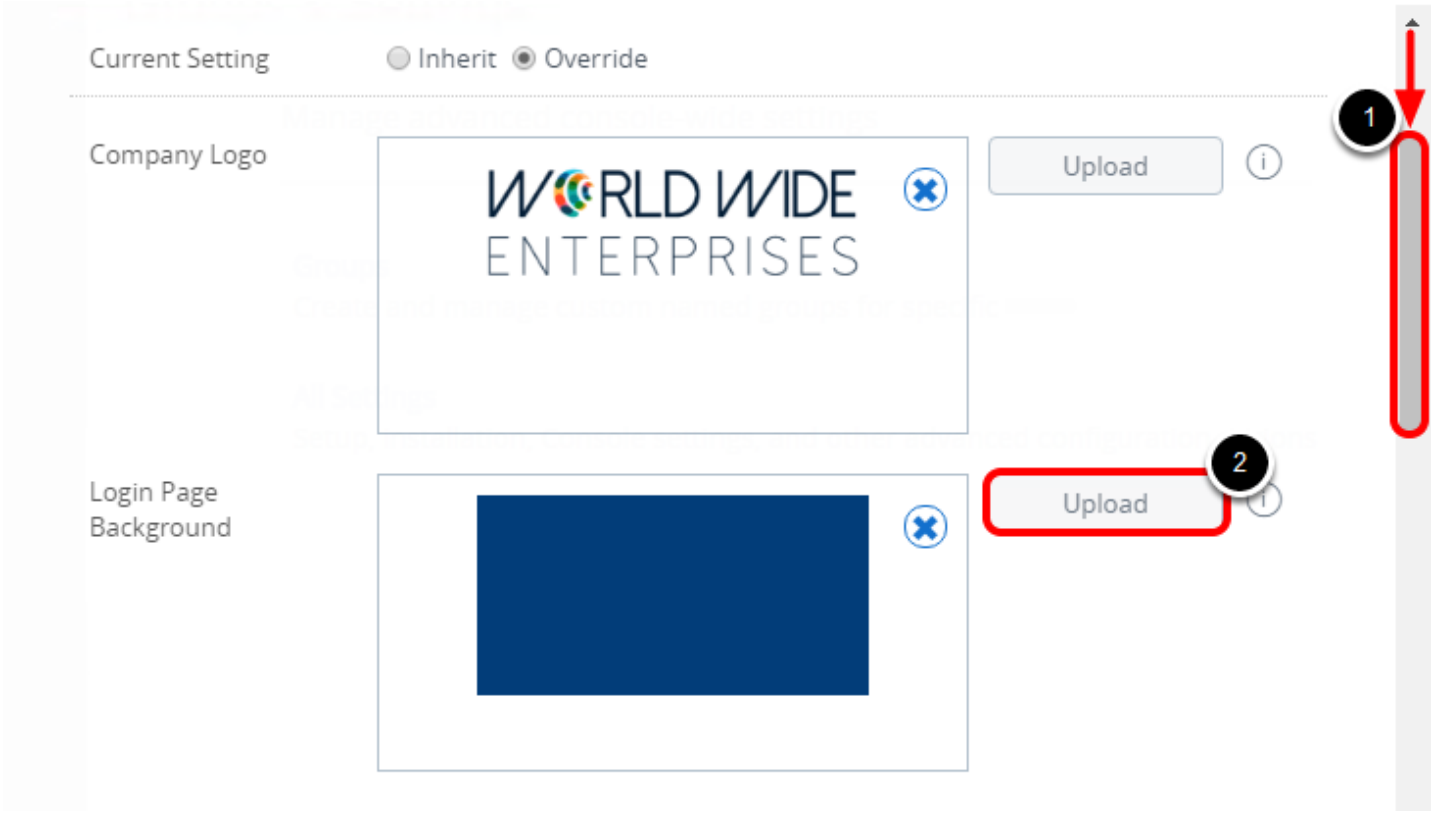


Click **Save**.

Login Page Background

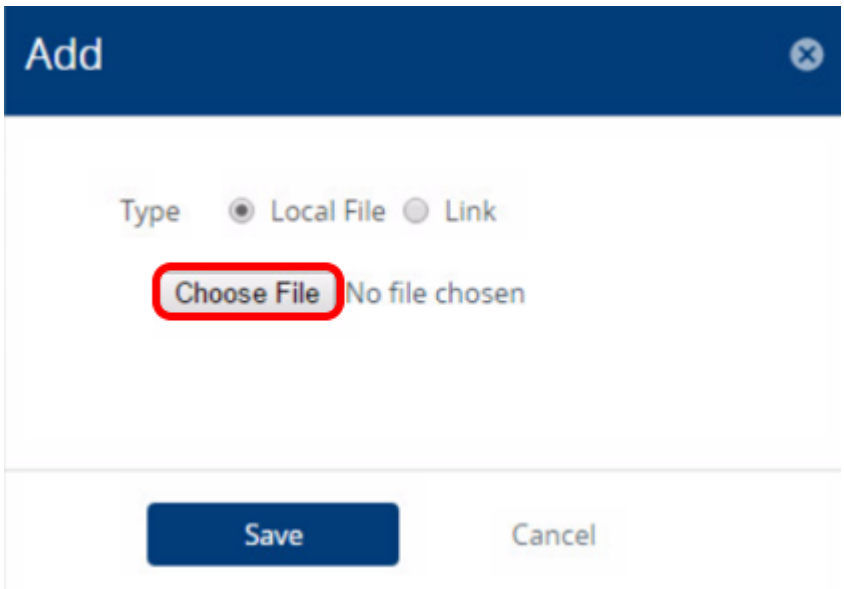
In this section you will change the Login Page Background, which is the image displayed at the AirWatch Console Login screen.

Uploading The Image



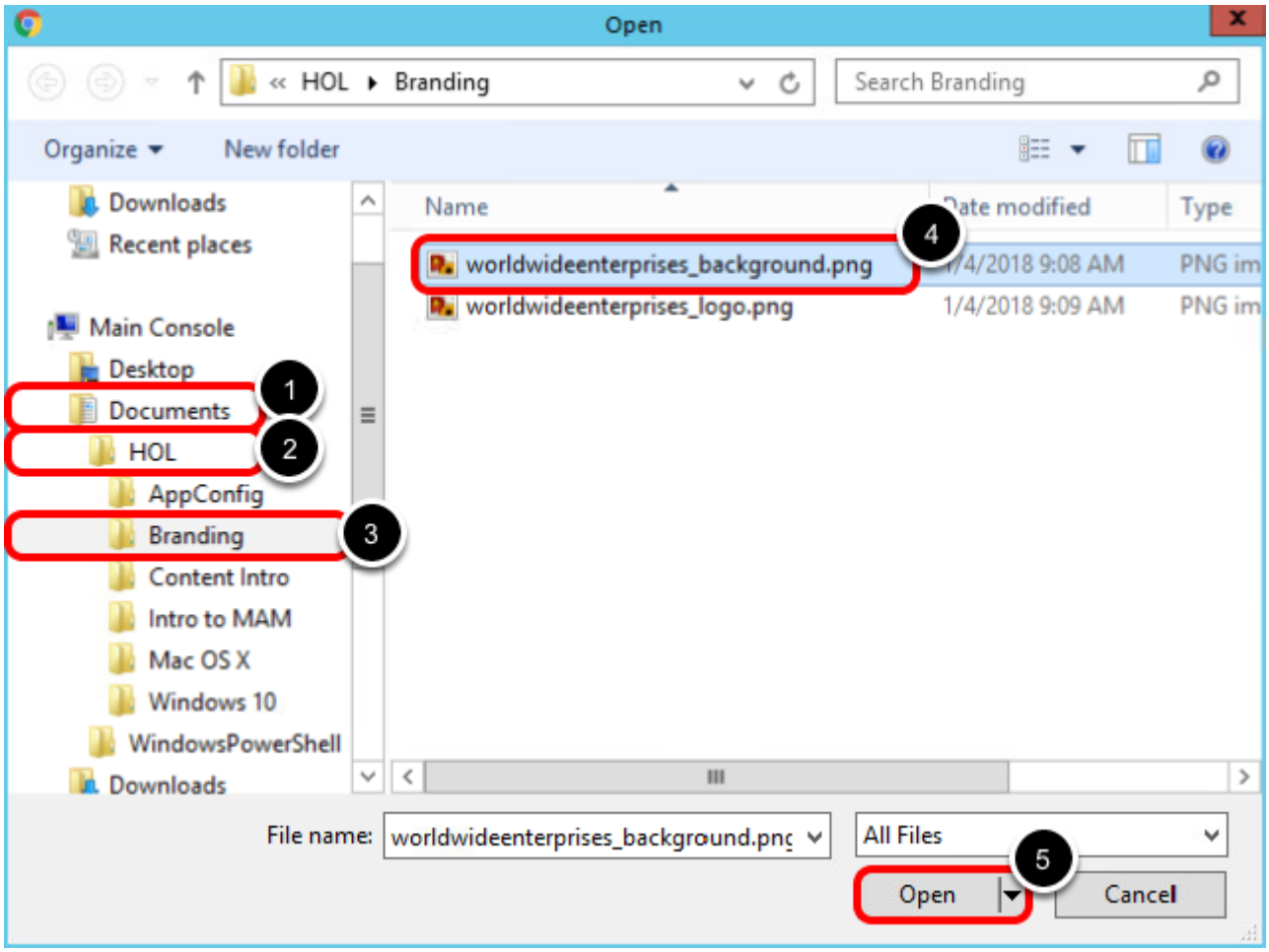
1. You may need to scroll down to find the **Login Page Background** area.
2. Click **Upload** for the Login Page Background area.

Uploading a File



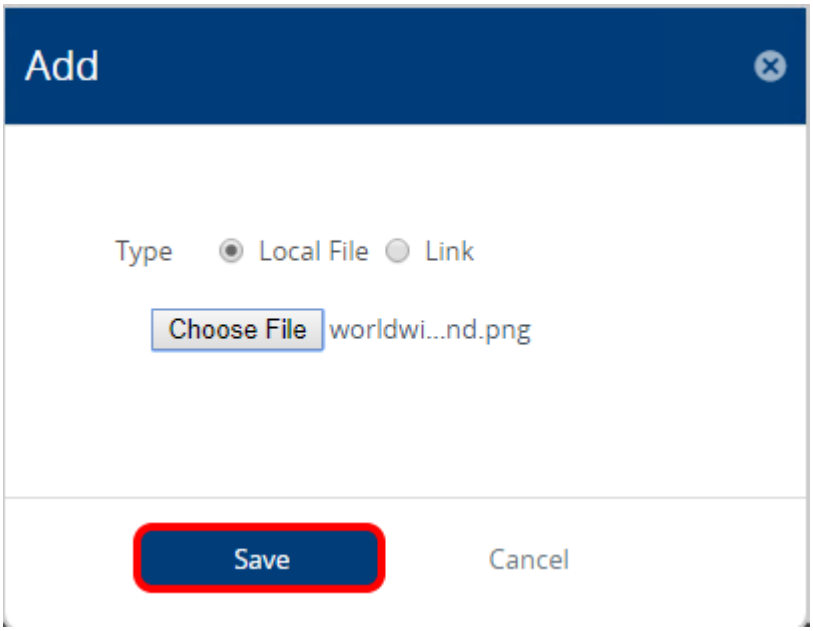
Click **Choose File**.

Selecting the World Wide Enterprises Background



1. Click **Documents** in the left pane.
2. Click on the **HOL** folder.
3. Click on the **Branding** folder.
4. Click the **worldwideenterprises_background.png** file.
5. Click **Open**.

Saving the World Wide Enterprises Background

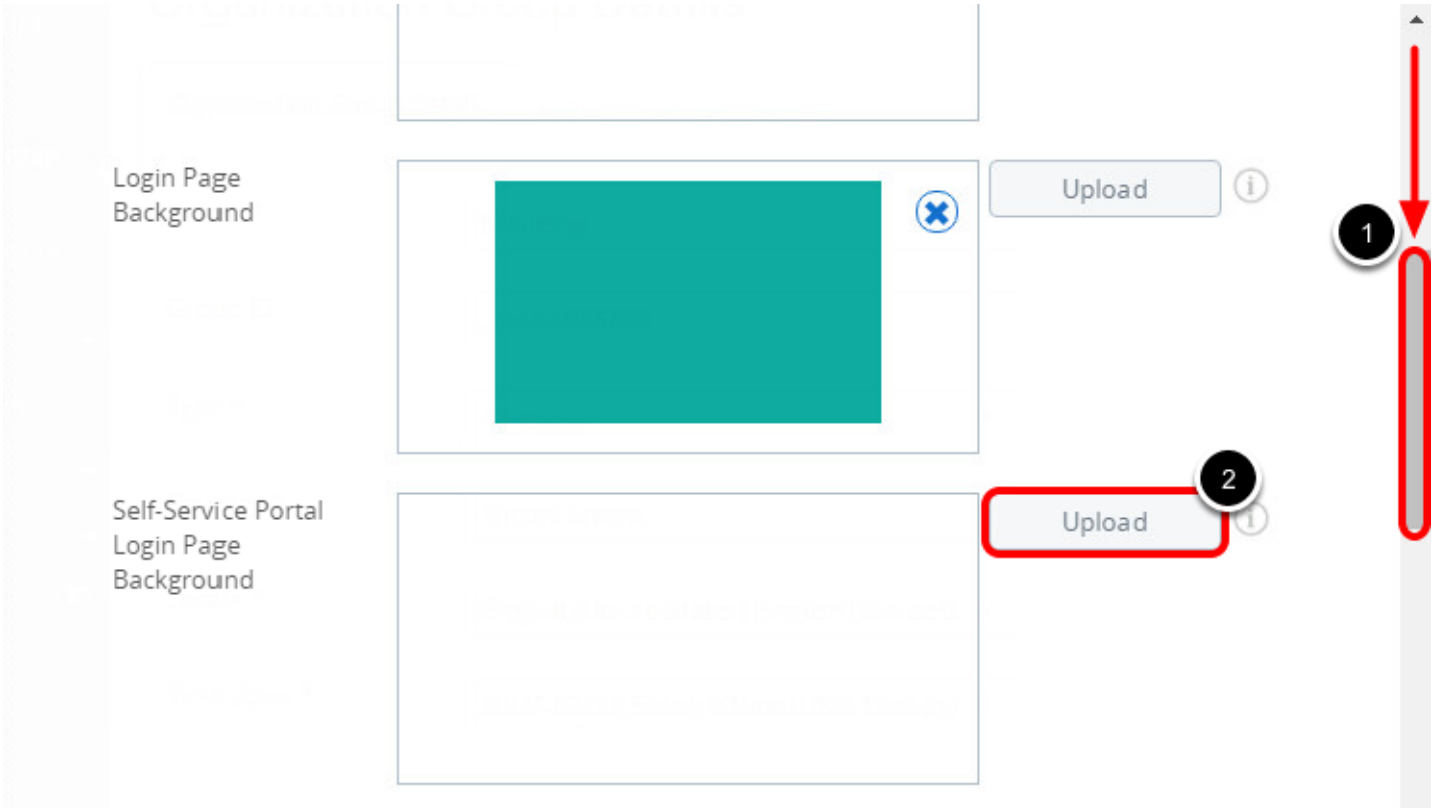


Click **Save**.

Self Service Login Page Background

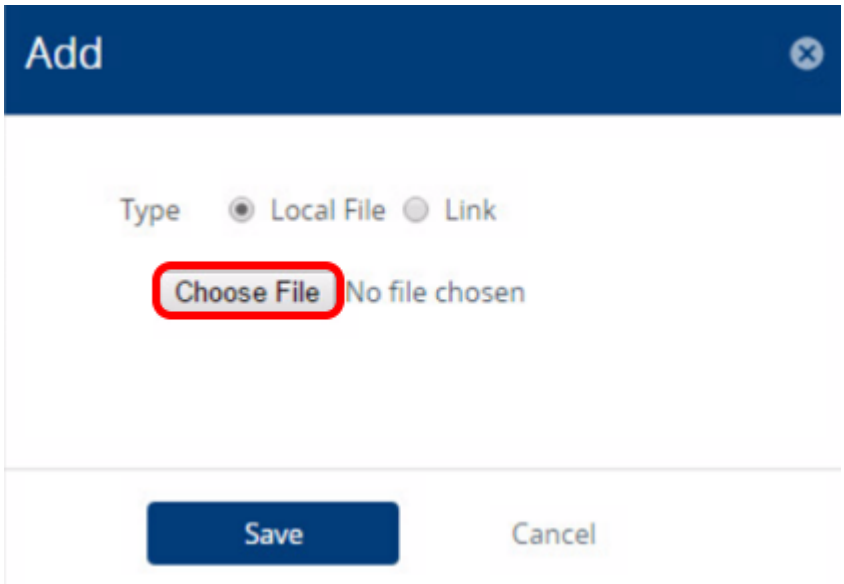
In this section, you will change the Self Service Login Page Background so that the Self Service Portal login background matches the AirWatch Console login background.

Uploading the Image



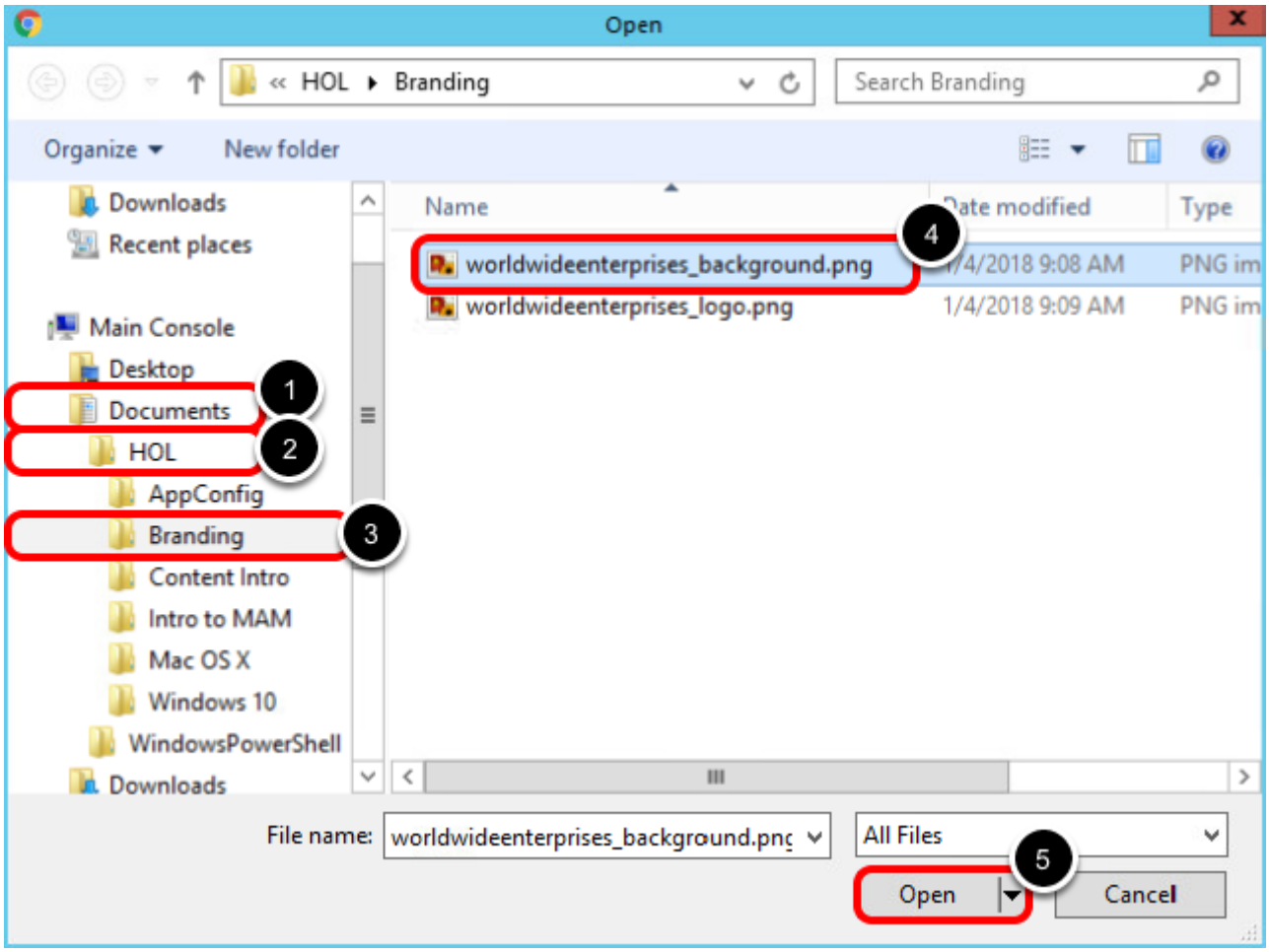
1. You may need to scroll down to find the **Self-Service Portal Login Page Background** area.
2. Click **Upload** for the Self-Service Portal Login Page Background.

Uploading a File



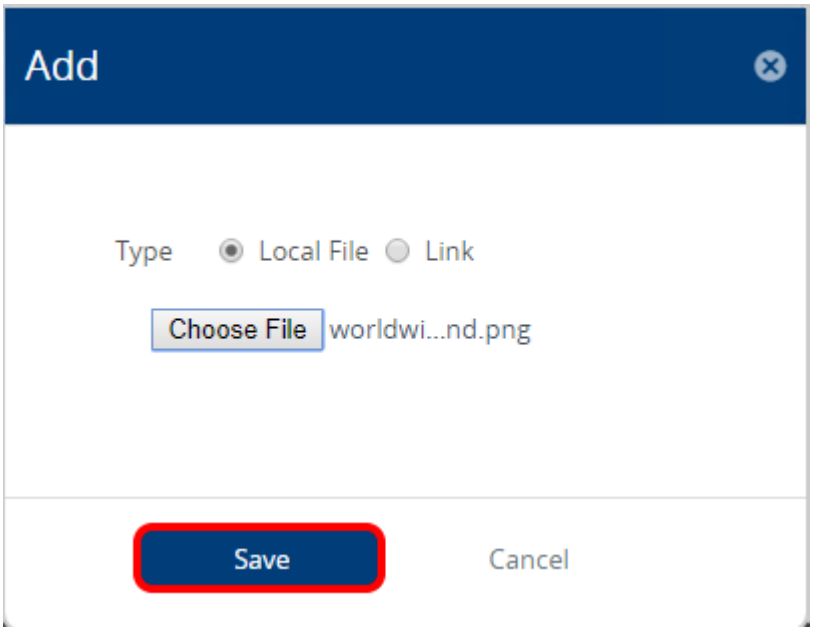
Click **Choose File**.

Selecting the World Wide Enterprises Background



1. Click **Documents** in the left pane.
2. Click on the **HOL** folder.
3. Click on the **Branding** folder.
4. Click the **worldwideenterprises_background.png** file.
5. Click **Open**.

Saving the World Wide Enterprises Background

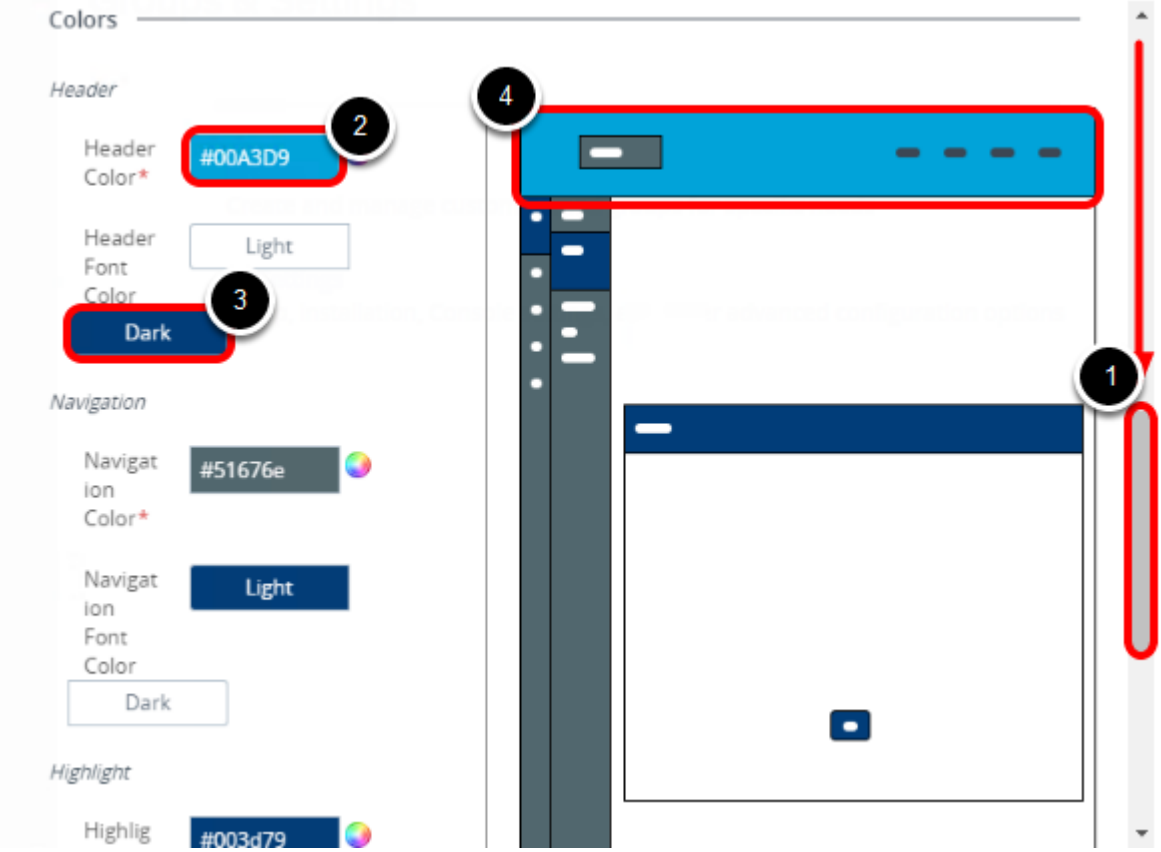


Click **Save**.

Colors

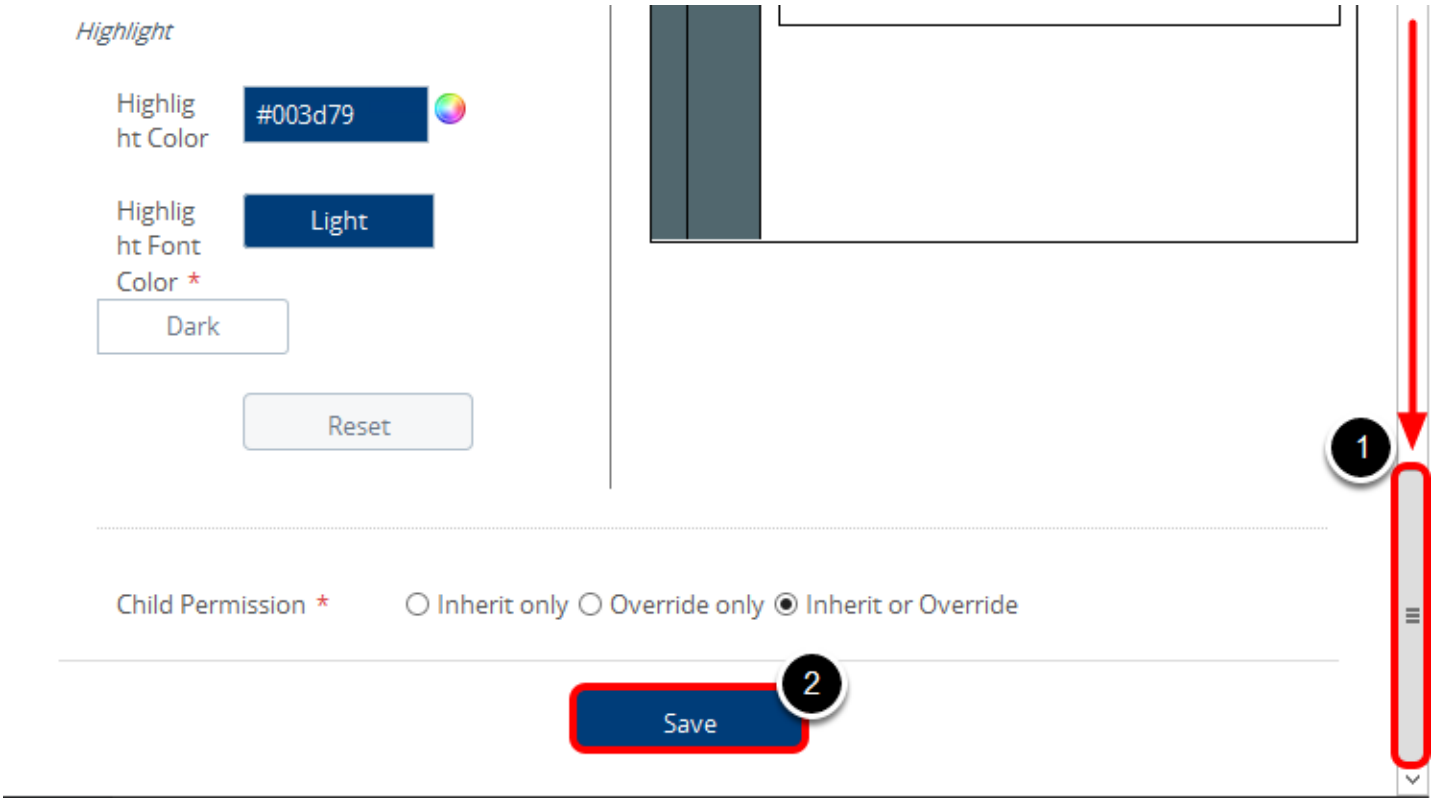
In this section you will change the Color theme of the AirWatch Console.

Changing the Header Color



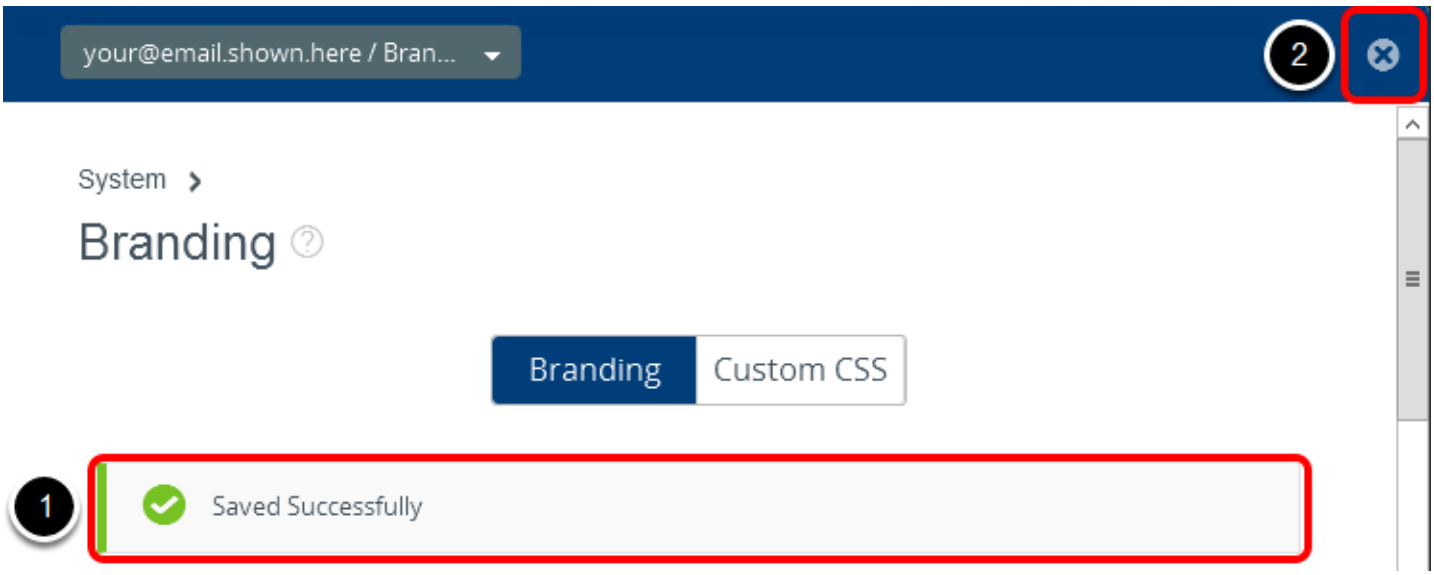
1. Scroll down in the Branding settings to find the **Colors** section.
2. Under the Header section, enter **"#00AED9"** for the **Header Color** field.
3. You can also toggle the **Font Color** between **Light** and **Dark** to better fit your theme. Change the **Header Font Color** to **Dark**.
4. Notice that the live preview updates instantly as you change any of the Color settings.

Apply Your Changes



1. Scroll down to view the Save button.
2. Click **Save**.

Close the Branding Settings Screen

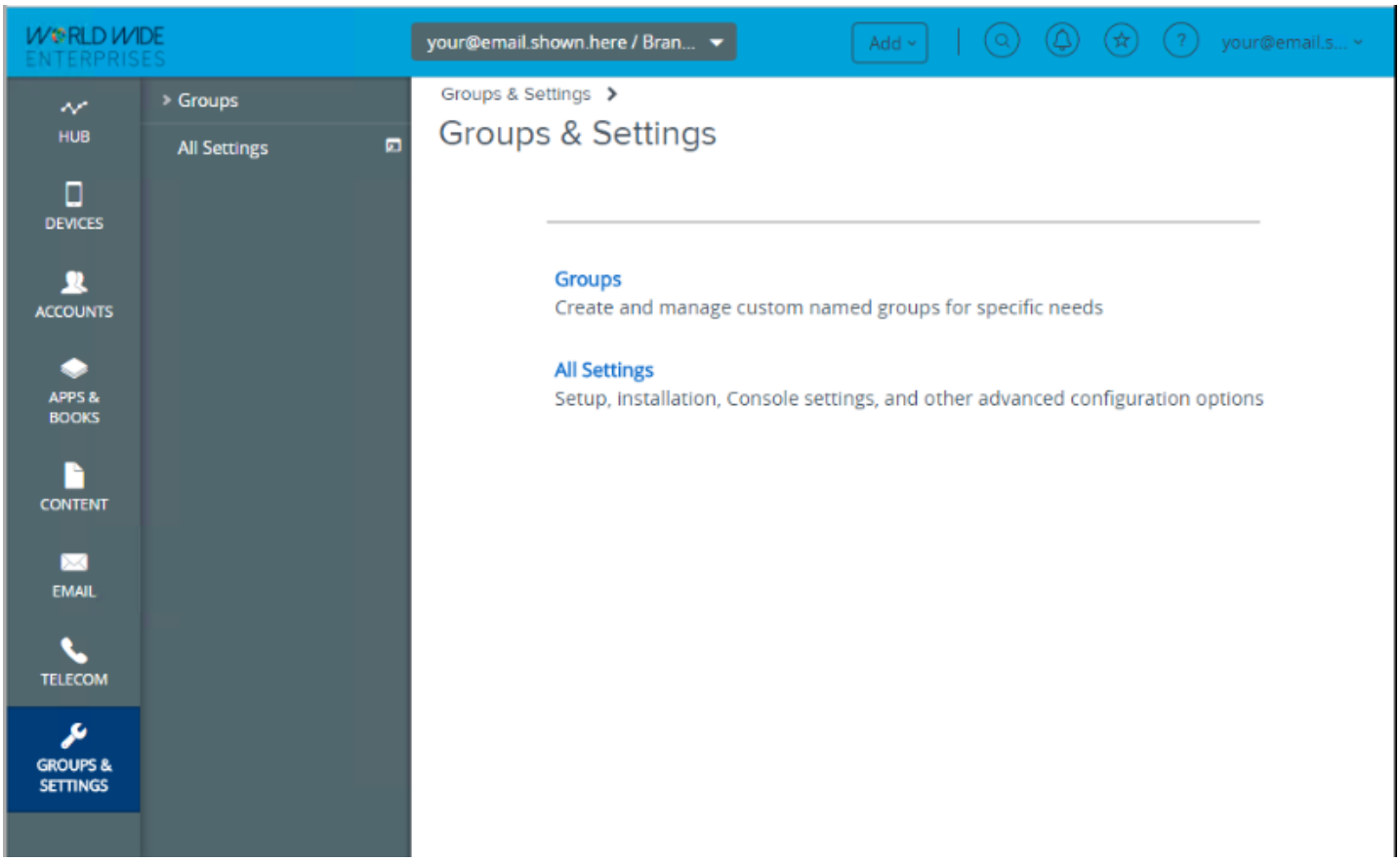


1. Notice the Saved Successfully message prompt, confirming your changes.
2. Close the **Close (X)** button.

Confirm the Console Branding Changes

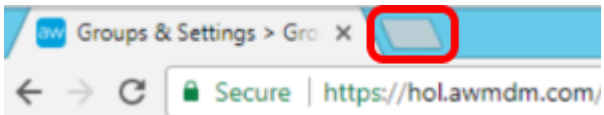
Now that the Branding changes have been configured and saved, we can test these changes within the AirWatch Console and the Self Service Portal.

View the Console Changes



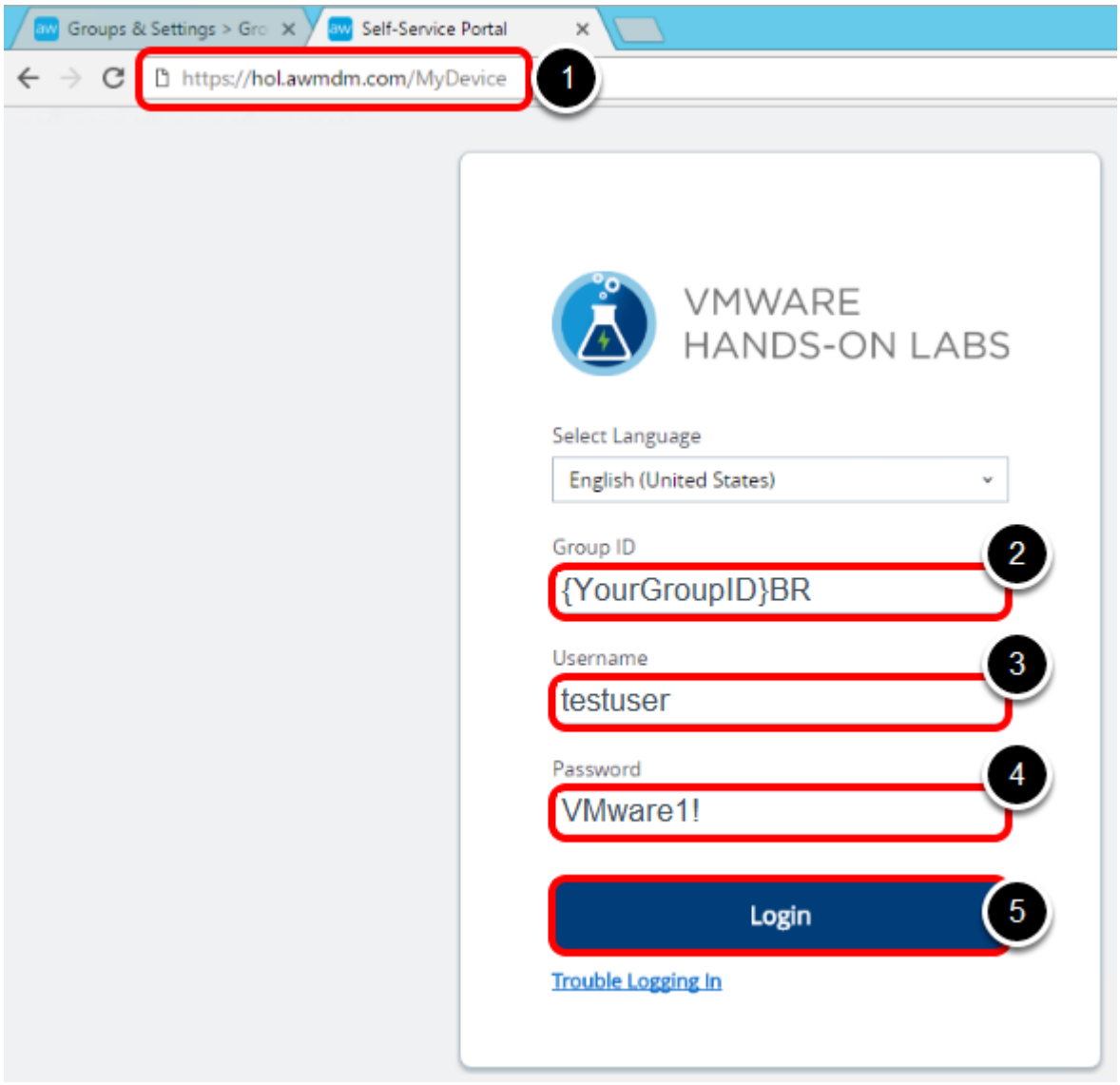
Notice that the **Company Logo**, and **Header Color** changes have been applied to the AirWatch Console.

Open a new Browser Tab



In your browser, click the **new tab button** to open a new tab.

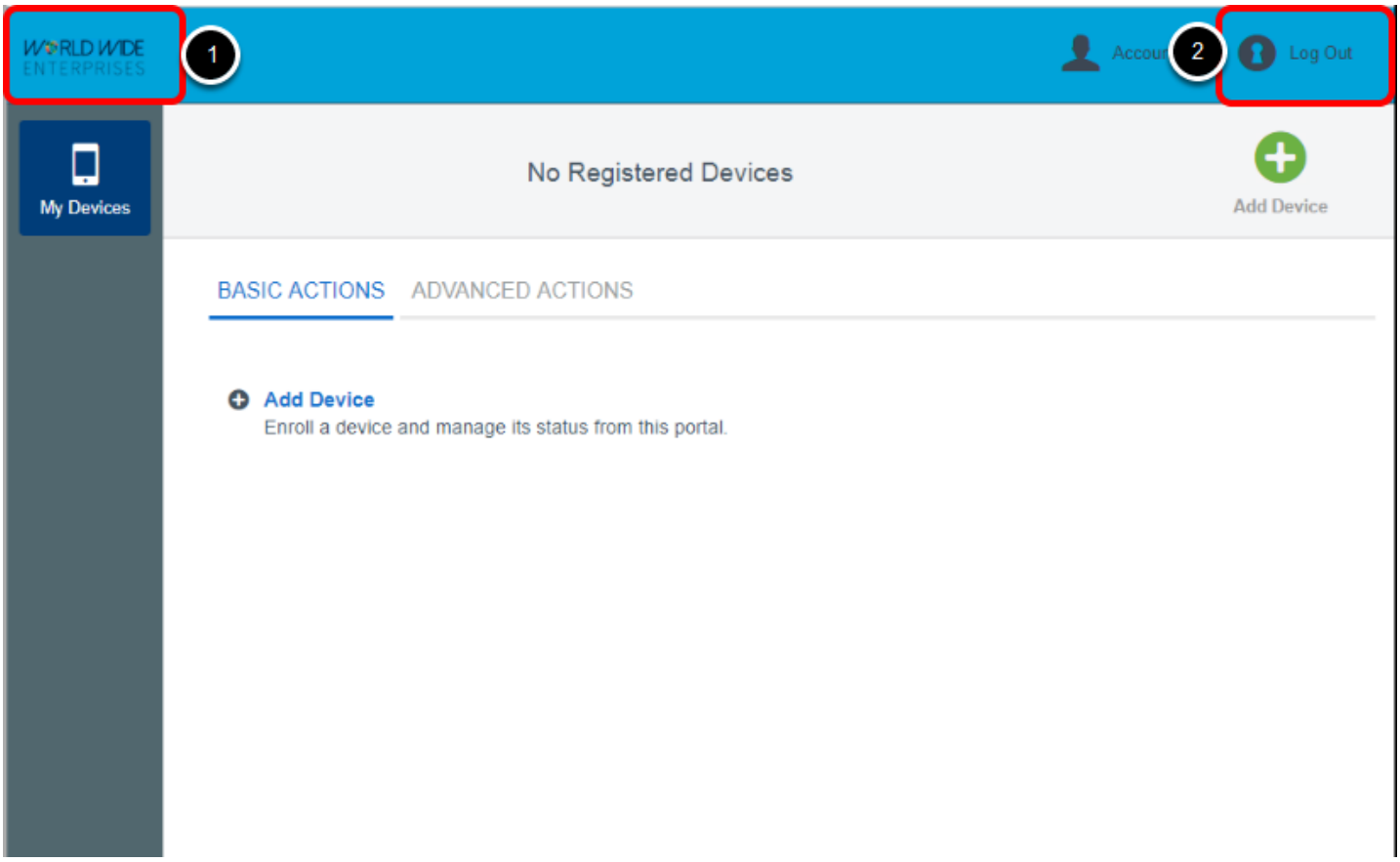
Navigate to the Self Service Portal and Login



1. Navigate to **https://hol.awmdm.com/MyDevice**
2. Enter your **Group ID** for the **Group ID** field.
   IMPORTANT - Remember to use your Branding Organization Group ID, ending in 'BR'. If you forgot this value, please refer to the previous step "Note Your Organization Group Has Changed" *to find the value.*
3. Enter **"testuser"** in the **Username** field.
4. Enter **"VMware1!"** in the **Password** field.
5. Click **Login**.

NOTE - If you see a Captcha here, please note that it is case sensitive!

Confirm the Self Service Portal Branding Changes



1. Confirm that the **Company Logo, Header Color and Navigation Color** changes have been applied to the Self Service Portal.
2. Click **Logout**.

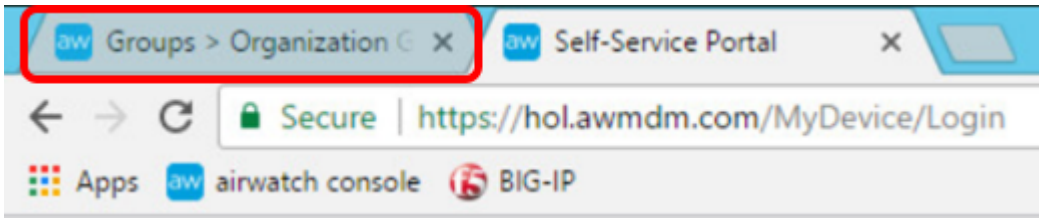
View the Self-Service Portal Branding Changes

Upon logging out and returning to the Self-Service Portal login page, notice that the Company Logo and Self-Service Login page, notice that the **Company Logo** and **Self-Service Login Page Background** settings have been applied.

Why didn't our branding changes display when we first navigated to the Self Service Portal at https://hol.awmdm.com/MyDevice? This is because our branding configurations were made at a child organization group and the Self Service Portal uses the branding configurations at the global organization group by default.

Alternatively, you can specify the group ID in the URL for the Self Service Portal, which would pull the branding configurations for the group ID you specify. To do so, you would navigate to https://hol.awmdm.com/MyDevice/Login?ac={groupID}, where {groupId} would be replaced with the Group ID retrieved from the AirWatch Console as did we in previous steps to login to the Self Service Portal. Using this direct link would also prevent your end users from having to enter the Group ID field during login, which may provide a better login experience.

Return to the AirWatch Console



Return to the **AirWatch Console** by clicking the first tab.

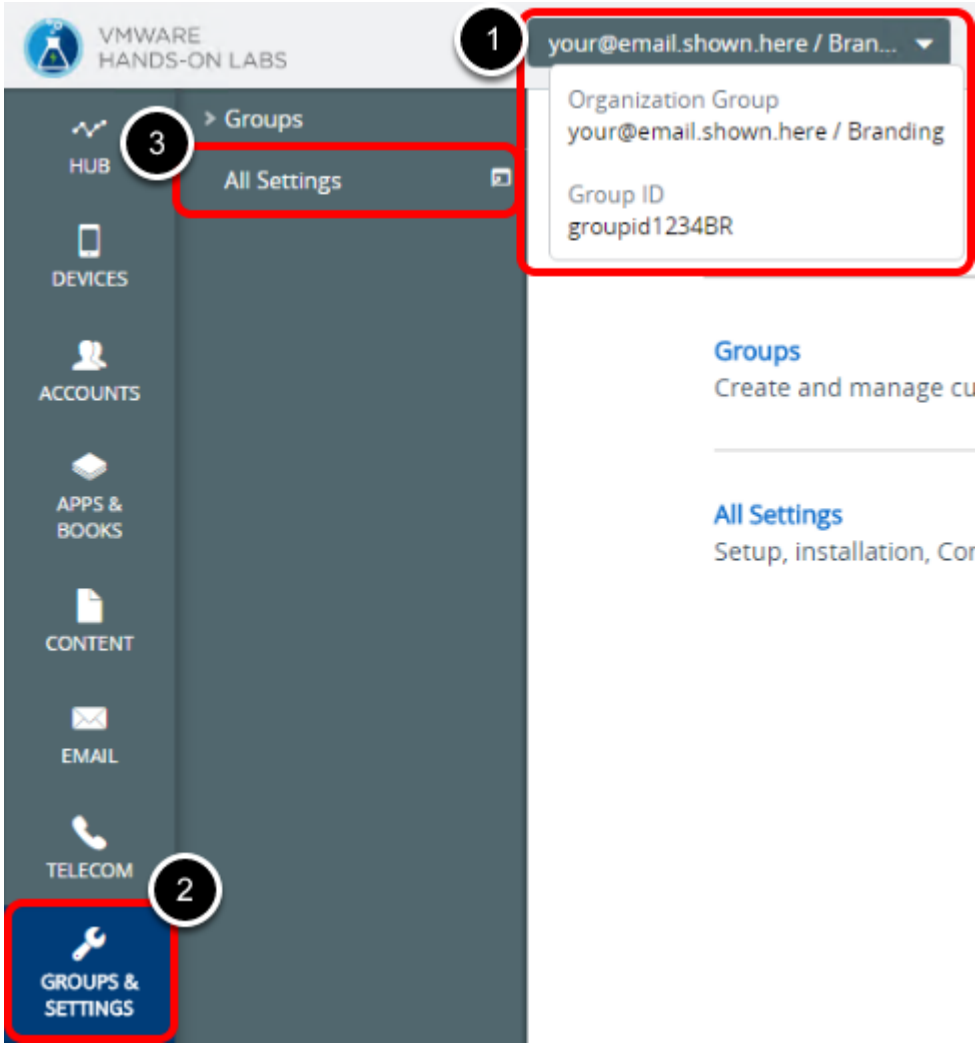
Content Locker & Browser Branding (iOS)

This section will show you how to brand your VMware Content Locker and AirWatch Browser application. We will browse the available options for branding an AirWatch SDK enabled application, create a Branding profile and attach the SDK profile to AirWatch applications.

Creating SDK Branding Profiles

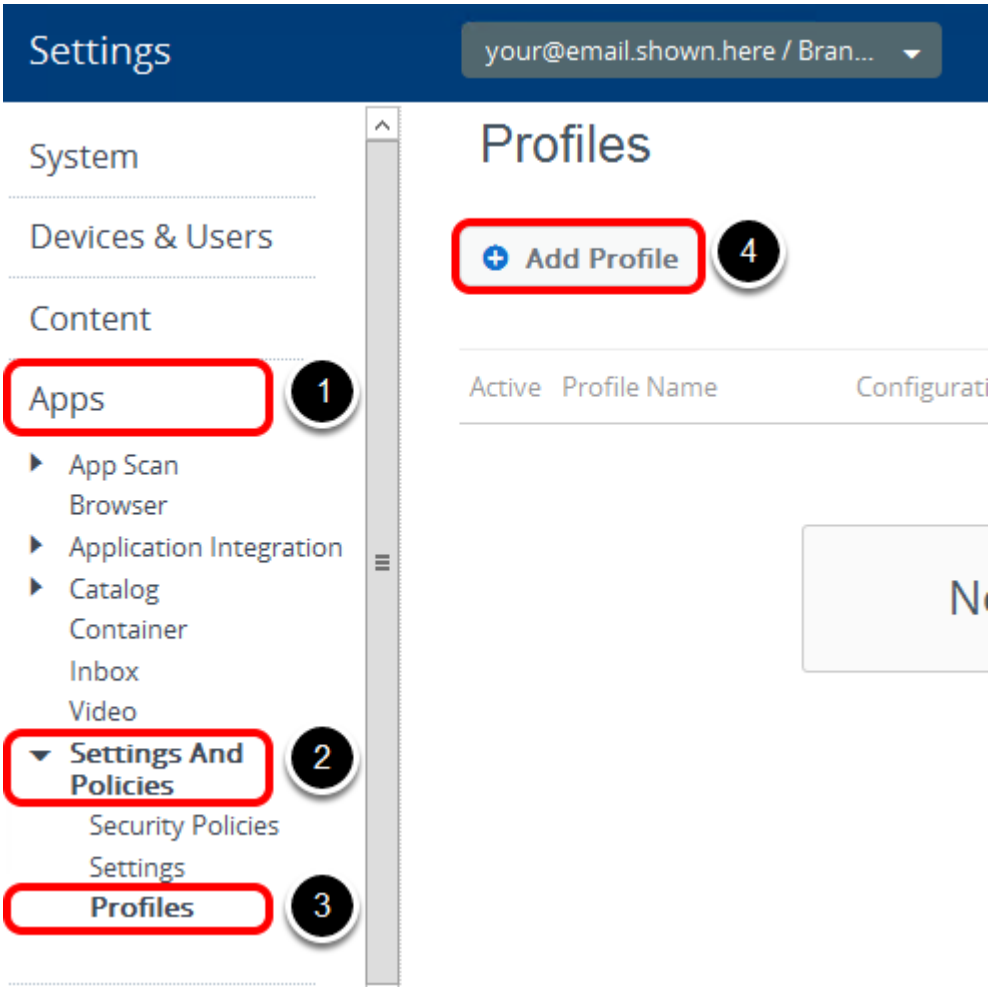
In this step we will create a new SDK Profile with a Branding Payload.

Branding Settings



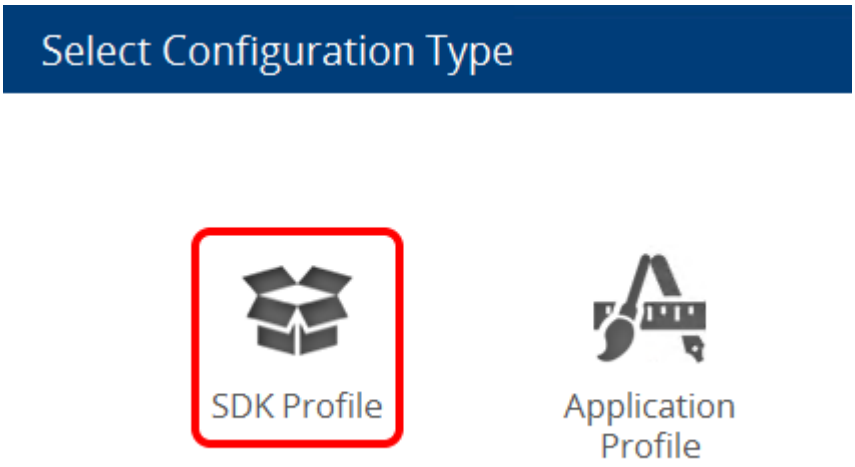
1. Confirm you are at the **Branding** Organization Group. If you are not, switch to the Branding Organization Group before progress by clicking the **Organization Group** button and selecting the **Branding** Organization Group.
2. Click **Groups & Settings**.
3. Click **All Settings**.

Adding a New Profile



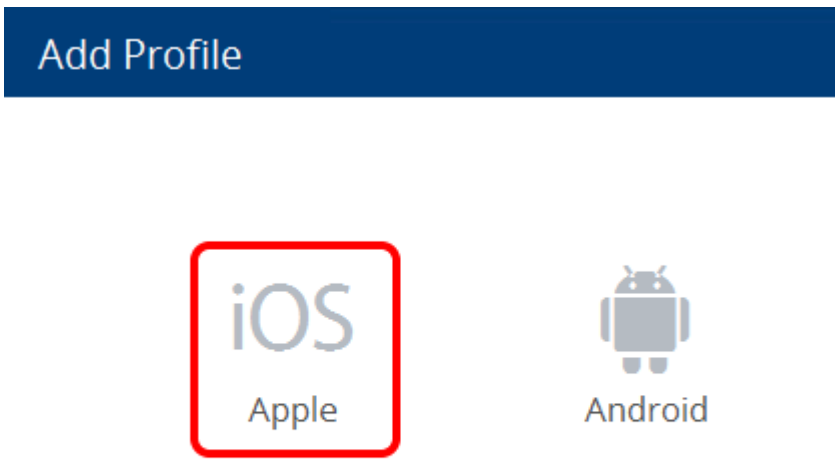
1. Click **Apps**.
2. Expand **Settings And Policies**.
3. Click **Profiles**.
4. Click **+ Add Profile**.

Select Configuration Type



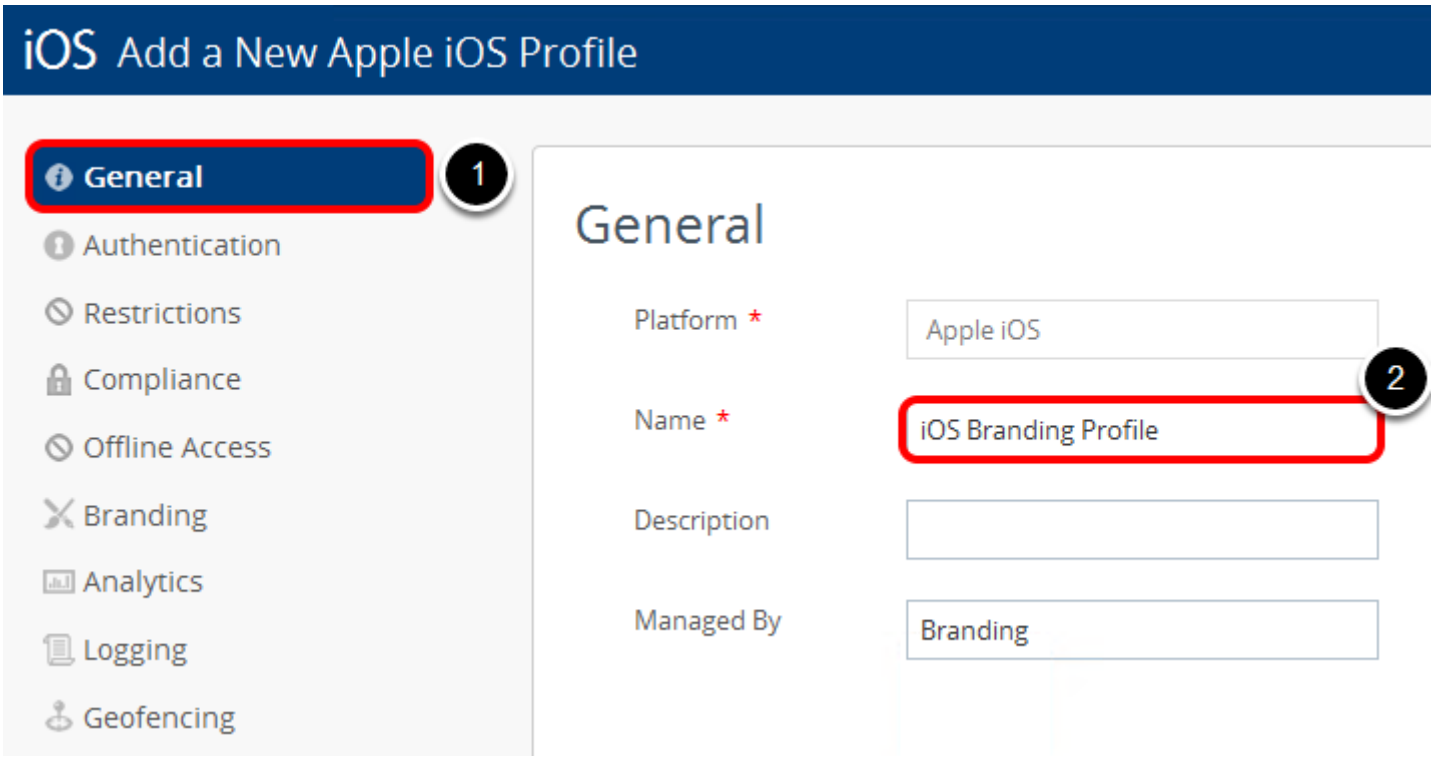
Click **SDK Profile**.

Select Profile Type



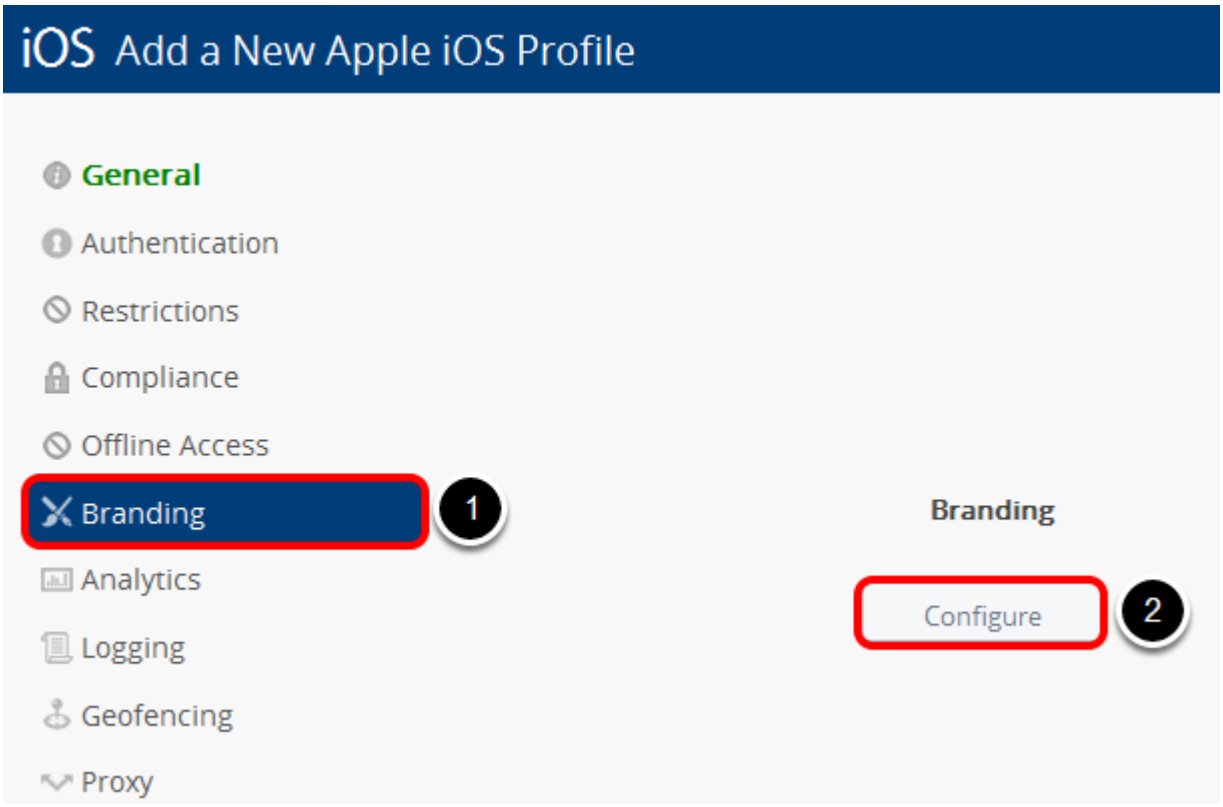
Click **Apple iOS**.

General - Naming the Profile



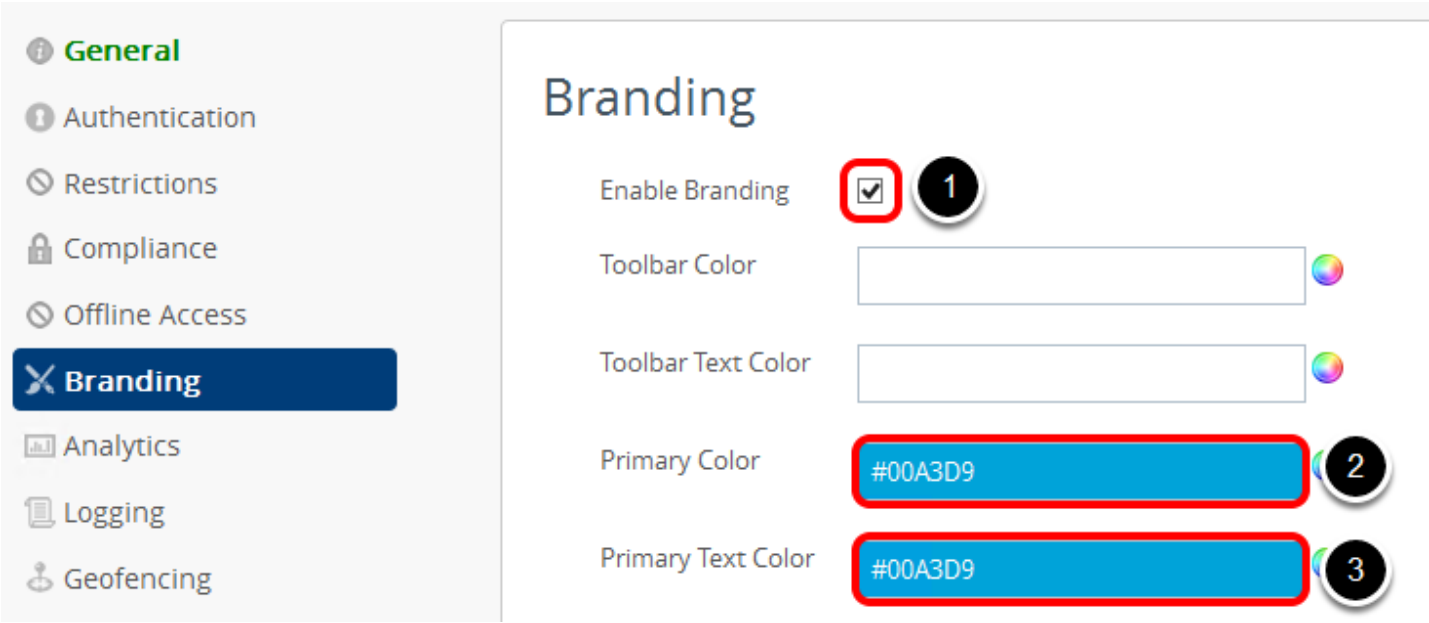
1. Click the **General** payload if is not already selected.
2. Enter **"iOS Branding Profile"** in the **Name** field.

Configure the Branding Payload



1. Click **Branding** in the payload section (left column)
2. Click **Configure**.

Configuring Branding Colors

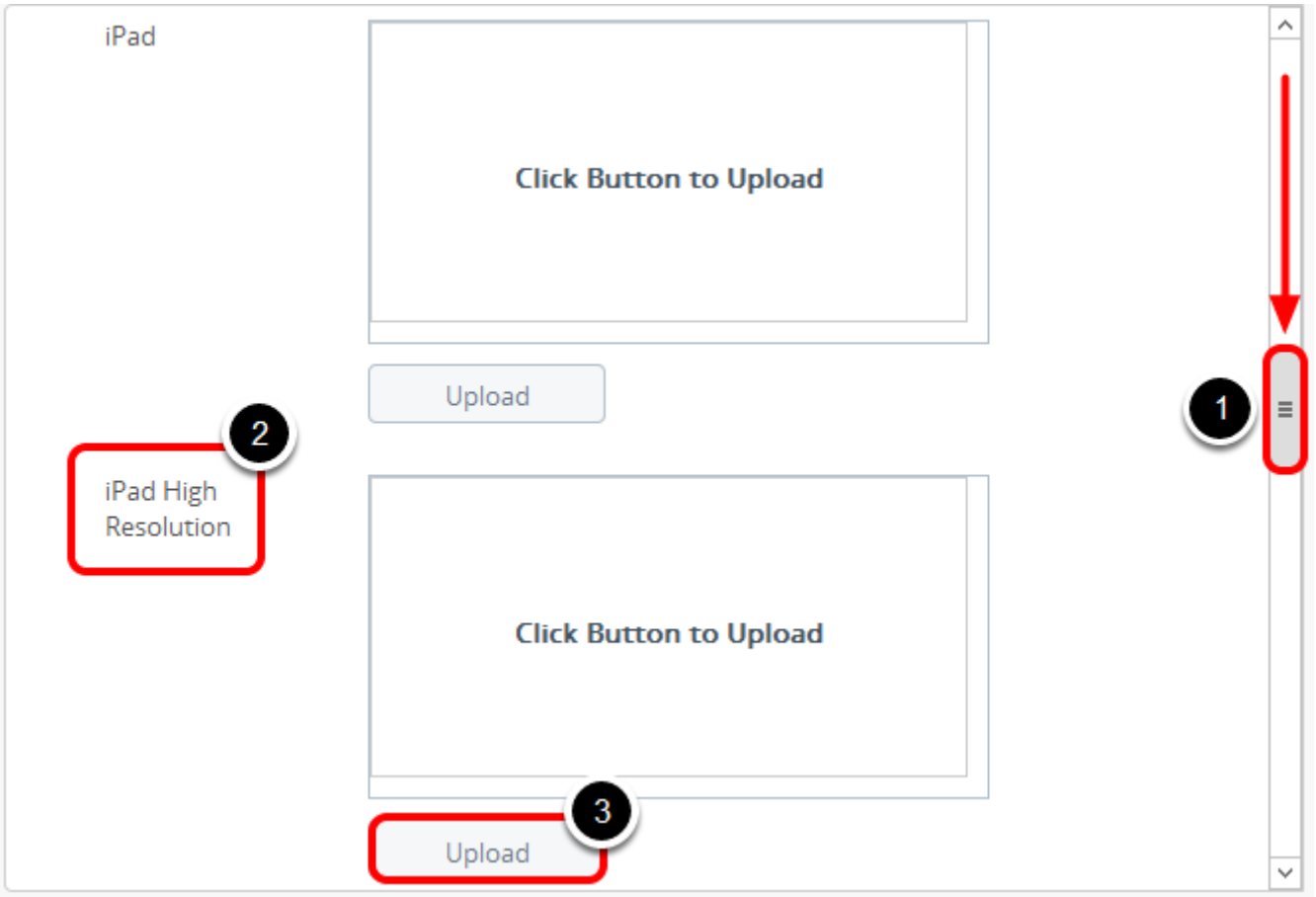


1. Check the **Enable Branding** checkbox.

2. Enter **"#00a3d9"** for the **Primary Color** field.
3. Enter **"#00a3d9"** for the **Primary Text Color** field.

The First Section of the payload is for branding general colors. Color values can be entered for each selection.

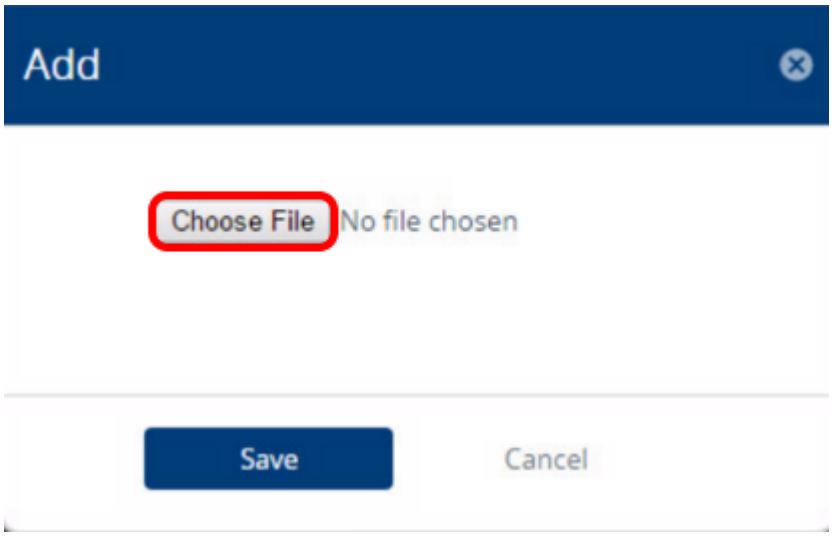
Company Logo



This section allows you to customize the branding for your company logo.

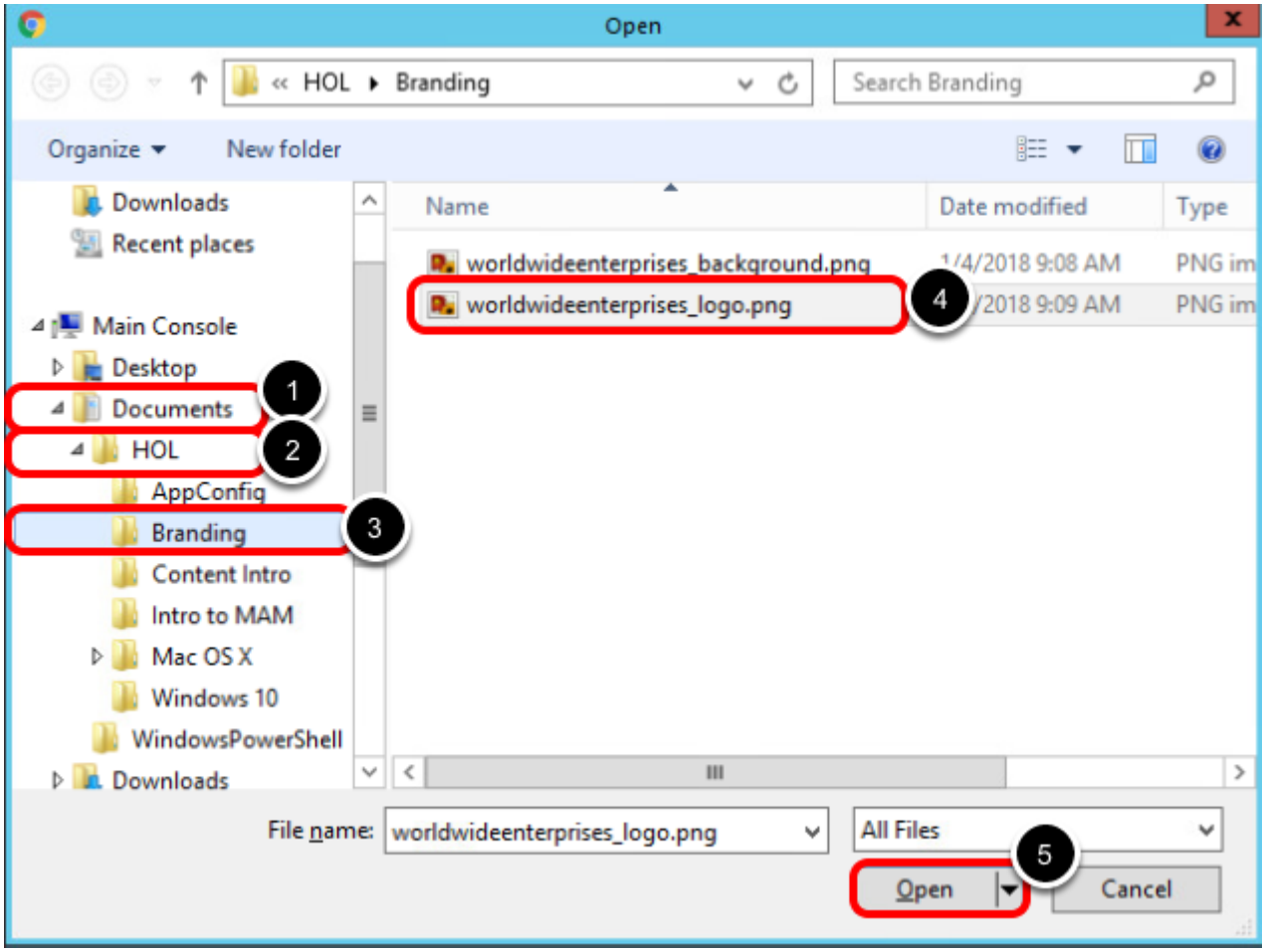
1. Scroll down until you see the Background Image section.
2. For VMware provisioned devices, select **Upload** under the **iPad High Resolution**. If you are using your own device, select **Upload** under the device type that matches your testing device.
3. Click on the **Upload** button.

Browse for the Logo File



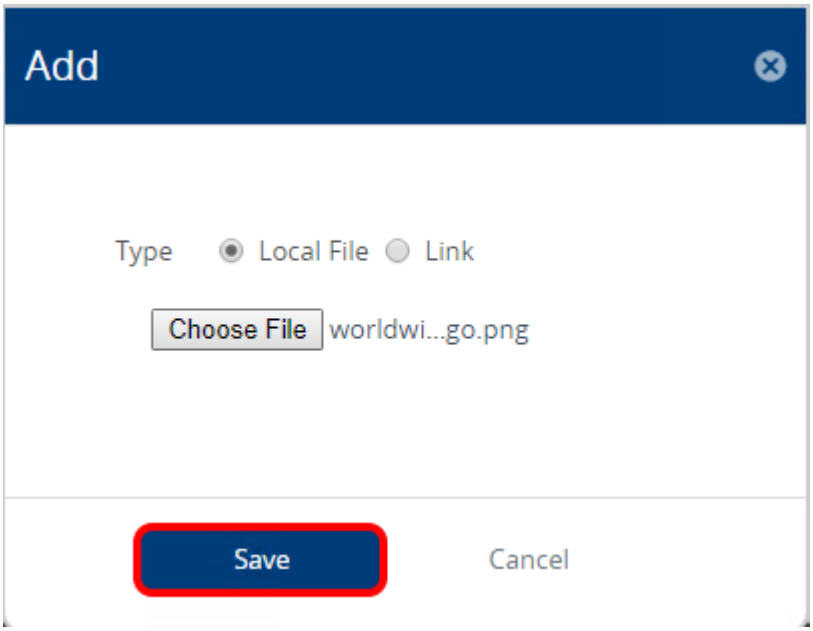
Click **Choose File**.

Select the Logo File



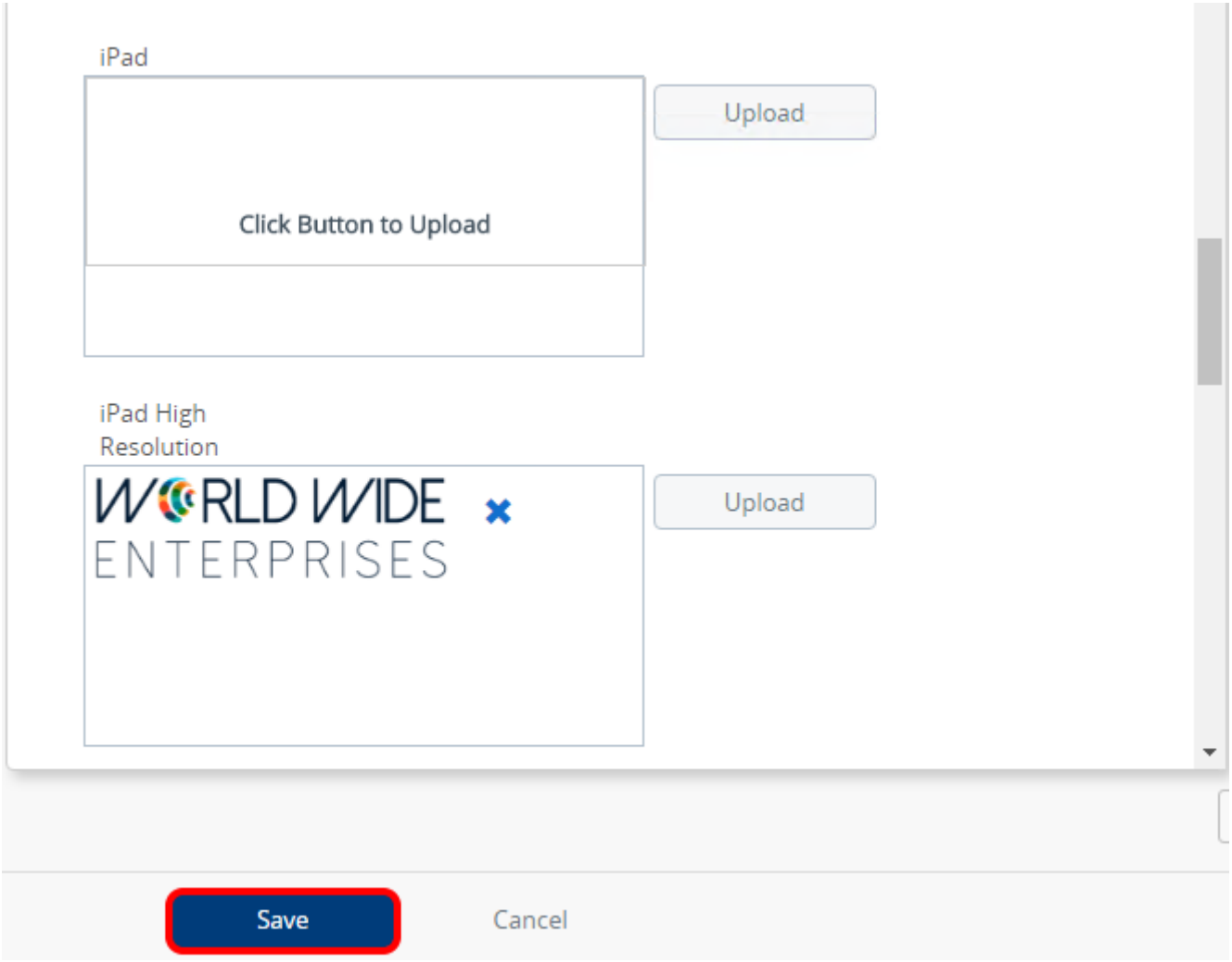
1. Click **Documents** in the left pane.
2. Click on the **HOL** folder.
3. Click on the **Branding** folder.
4. Click the **worldwideenterprises_logo.png** file.
5. Click **Open**.

Save the Logo File



Click **Save**.

Save the iOS SDK Profile

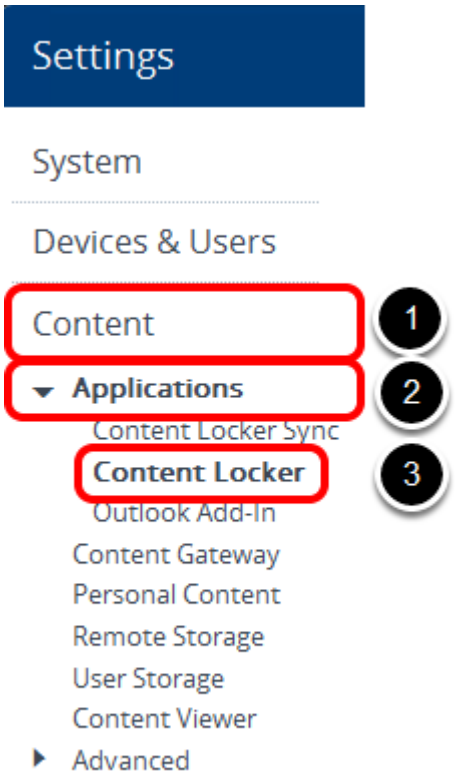


Click **Save**.

Edit the VMware Content Locker Settings

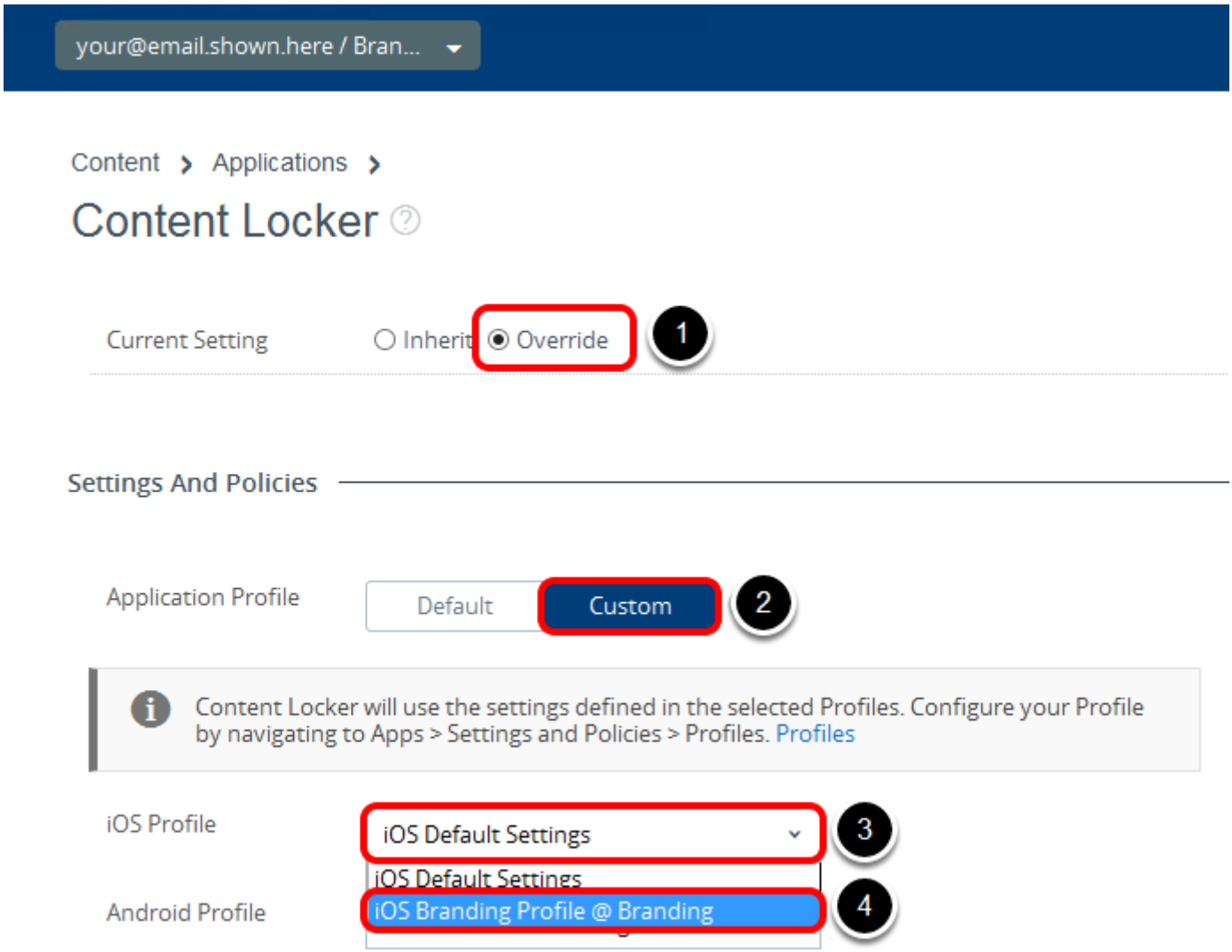
In this step we will set the previously created branding profile as the active SDK profile for the AirWatch VMware Content Locker.

Content Locker Settings



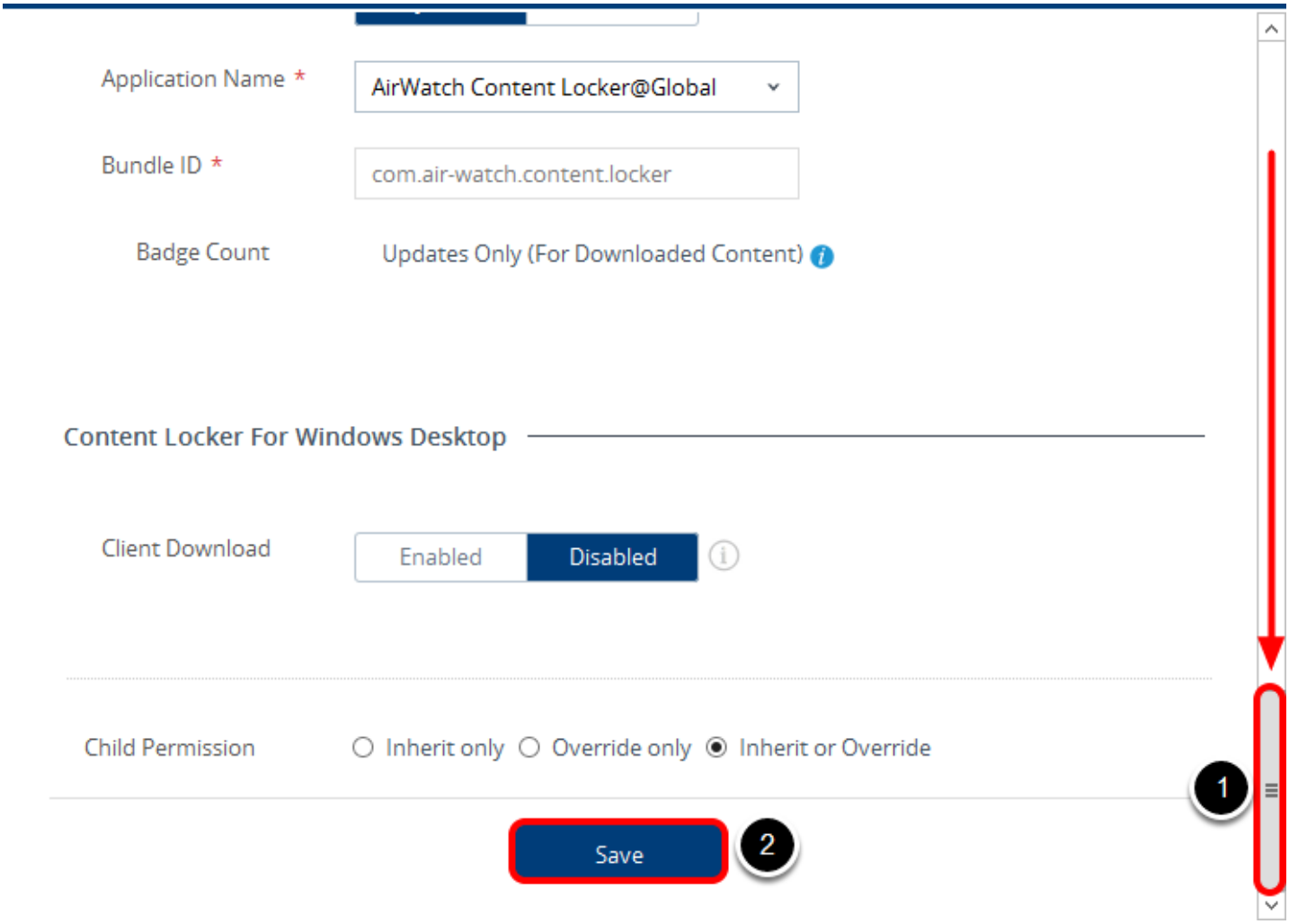
1. Click on **Content** in the navigation panel on the left.
2. Click on **Applications**.
3. Click on **Content Locker**.

Content Locker Settings Configuration



1. Select **Override** for the **Current Setting** field.
2. Select **Custom** for the **Application Profile** selection.
3. Click the **iOS Profile** dropdown menu to see your available Profiles.
4. Click **iOS Branding Profile @ Branding**. This is the Branding profile you just configured previously.

Save Settings

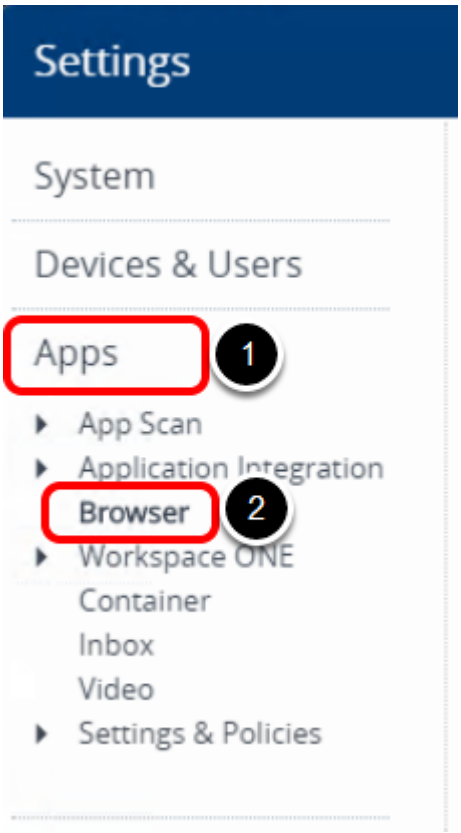


1. Scroll down to the bottom of the page.
2. Click **Save**.

Edit the AirWatch Browser Settings

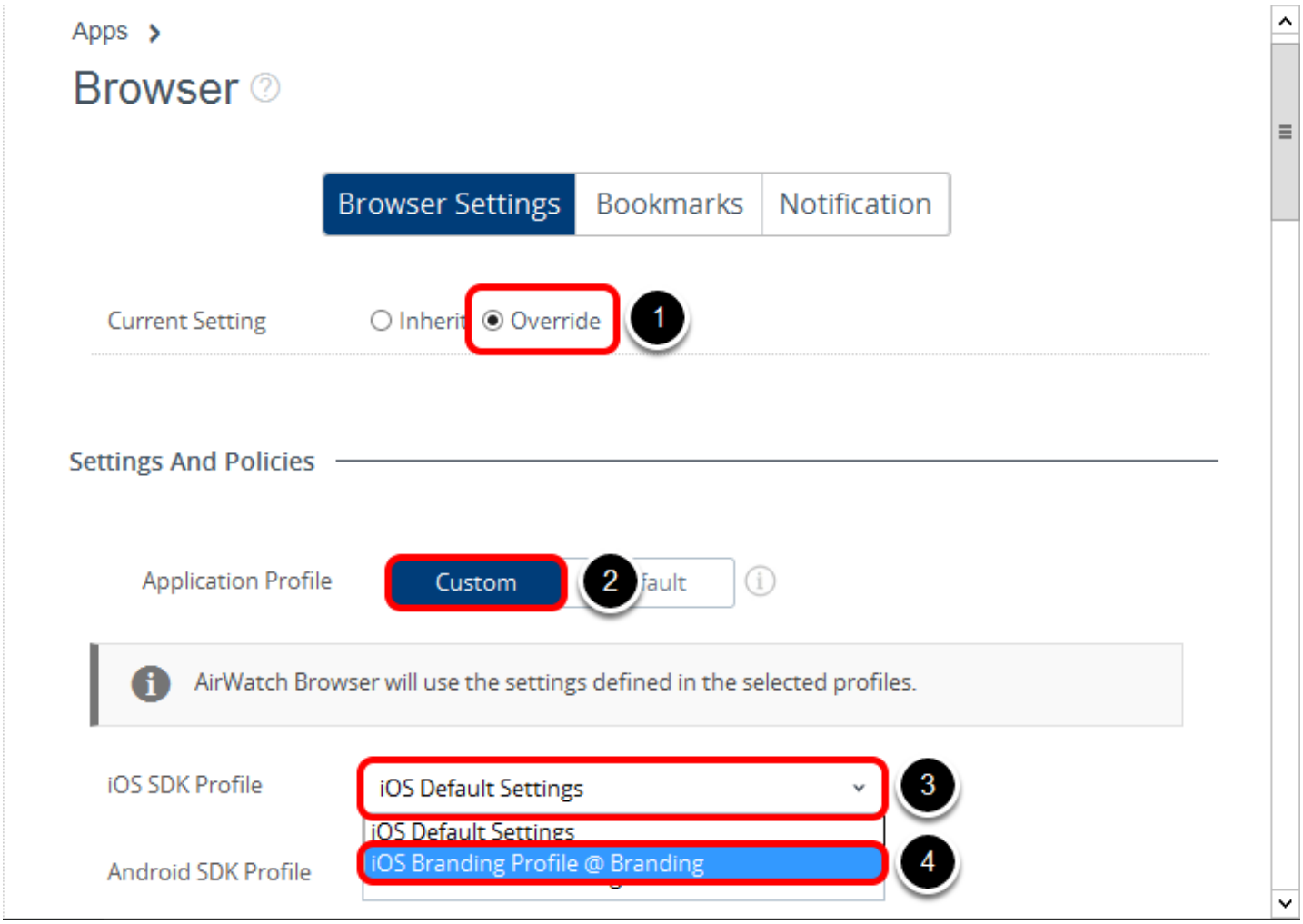
In this step we will set the previously created branding profile as the active SDK profile for the AirWatch Browser.

AirWatch Browser Settings



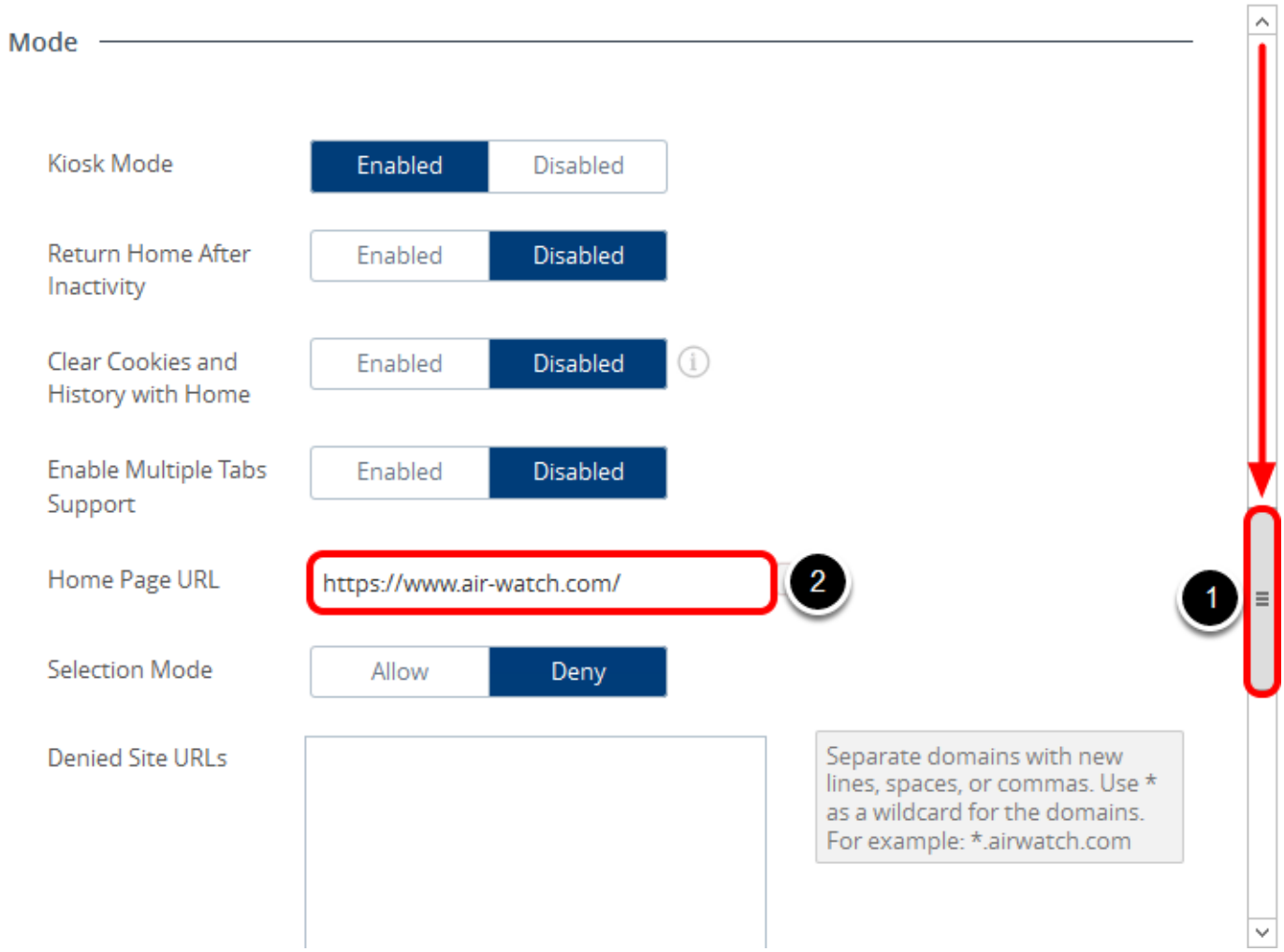
1. Click **Apps**.
2. Click **Browser**.

AirWatch Browser Configuration



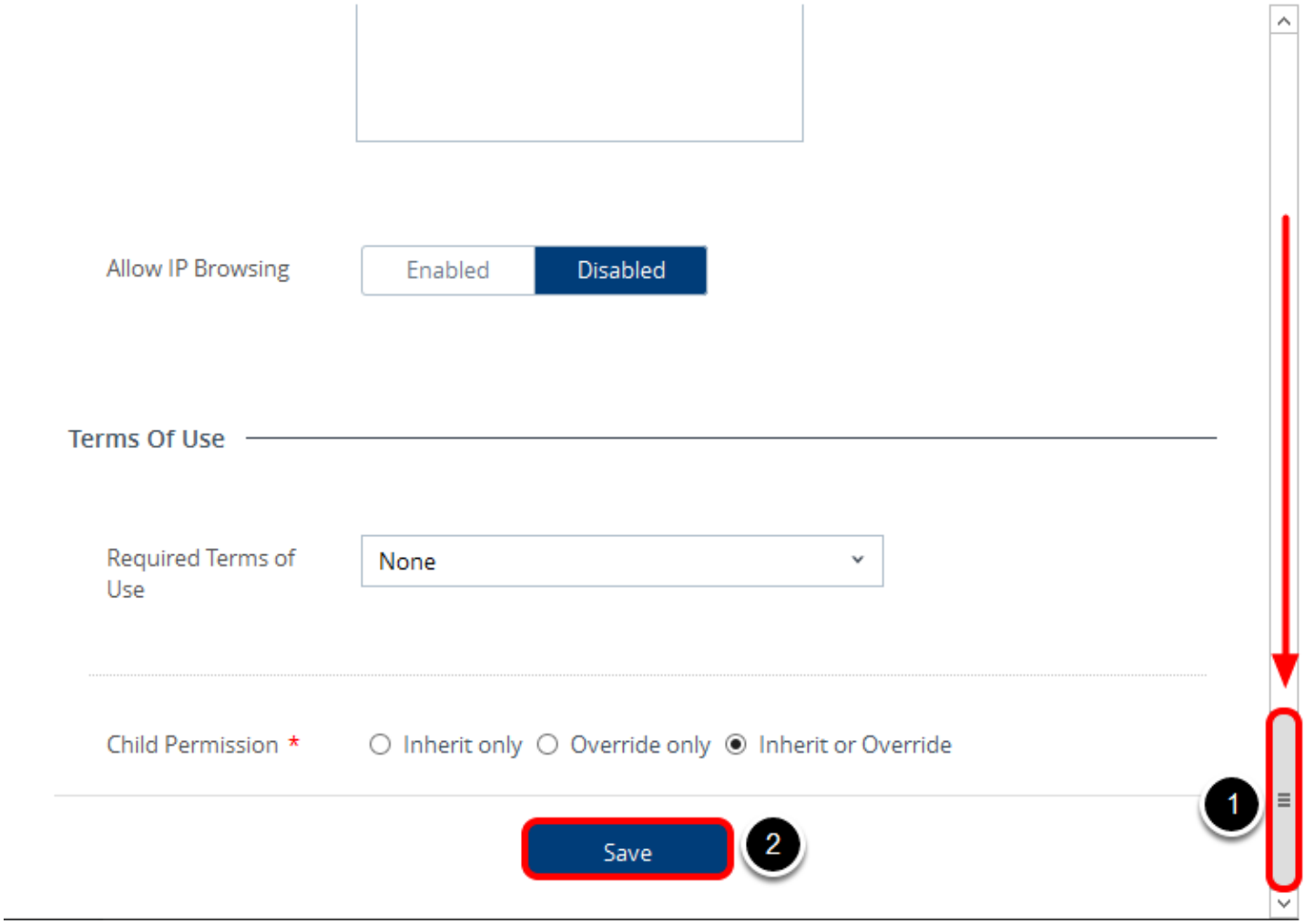
1. Select **Override** for **Current Setting**.
2. Select **Custom** for **Application Profile.**
3. Click the **iOS SDK Profile** dropdown to see your available Profiles.
4. Click **"iOS Branding Profile @ Branding"**. This is the Branding profile you just configured previously.

Add a Home Page URL



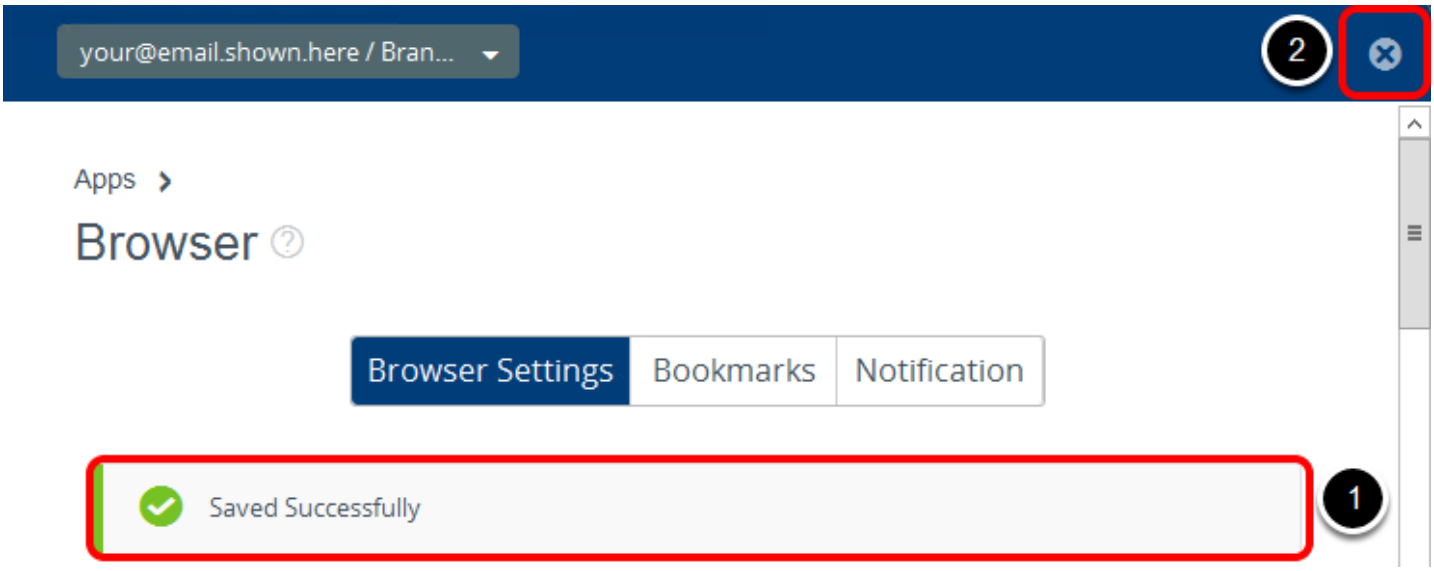
1. Scroll down to find the **Mode** section and the **Home Page URL** field.
2. Enter **"https://www.air-watch.com/"** in the **Home Page URL** field.

Save Settings



1. Scroll down to the bottom of the page.
2. Click **Save**.

Close the Settings Page

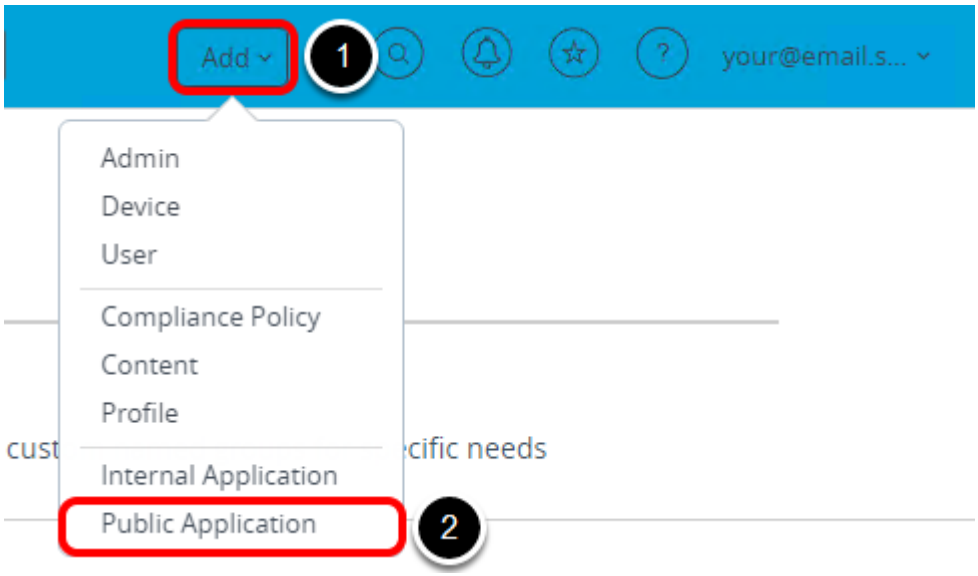


1. Confirm the save was successful with the **Saved Successfully** confirmation.
2. Click the **X** icon in the upper right corner of the Settings page to close Settings.

Publish the VMware Content Locker

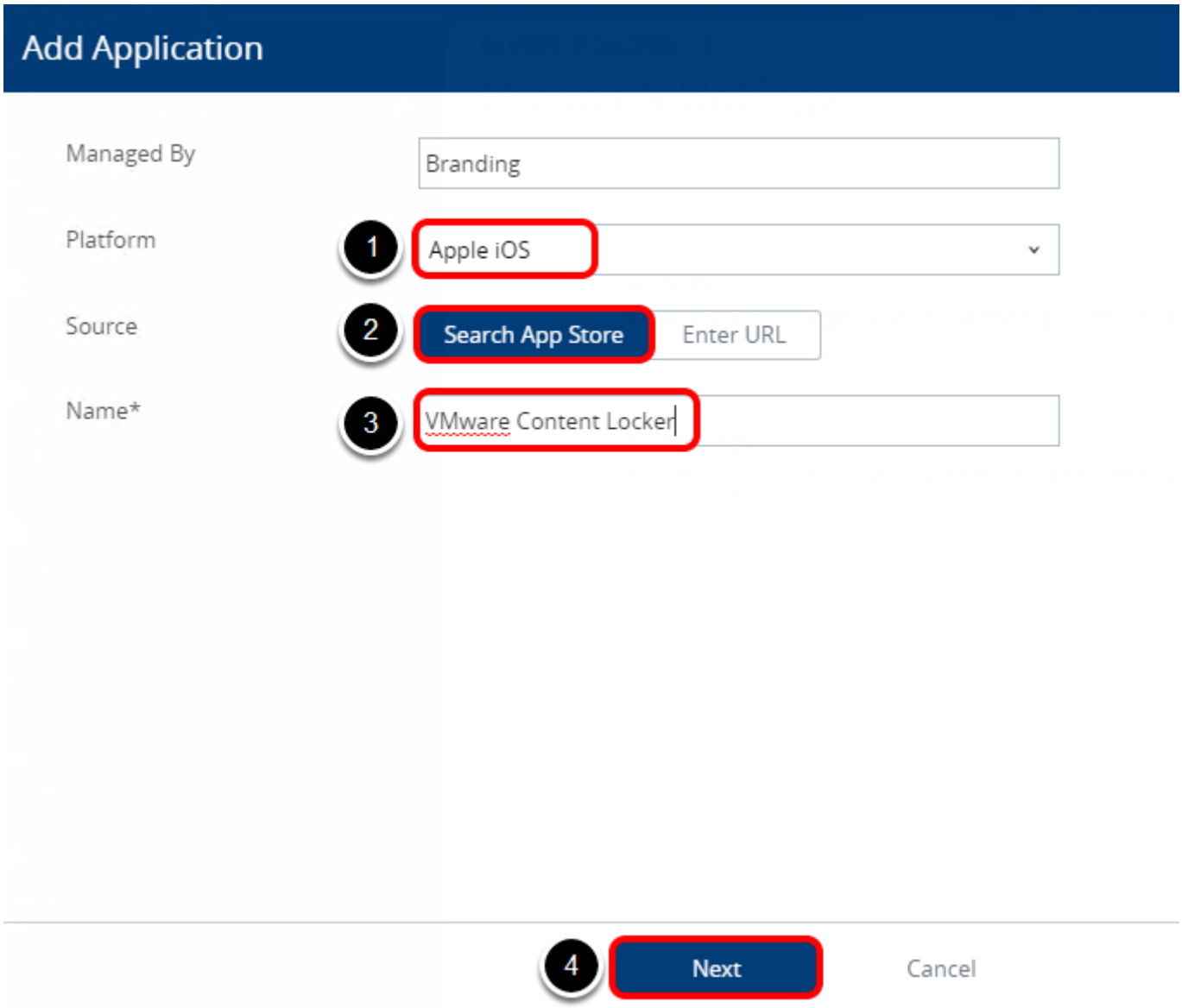
In this step, we will publish the VMware Content Locker to registered devices in order to test the Branding updates.

Add a New Public Application



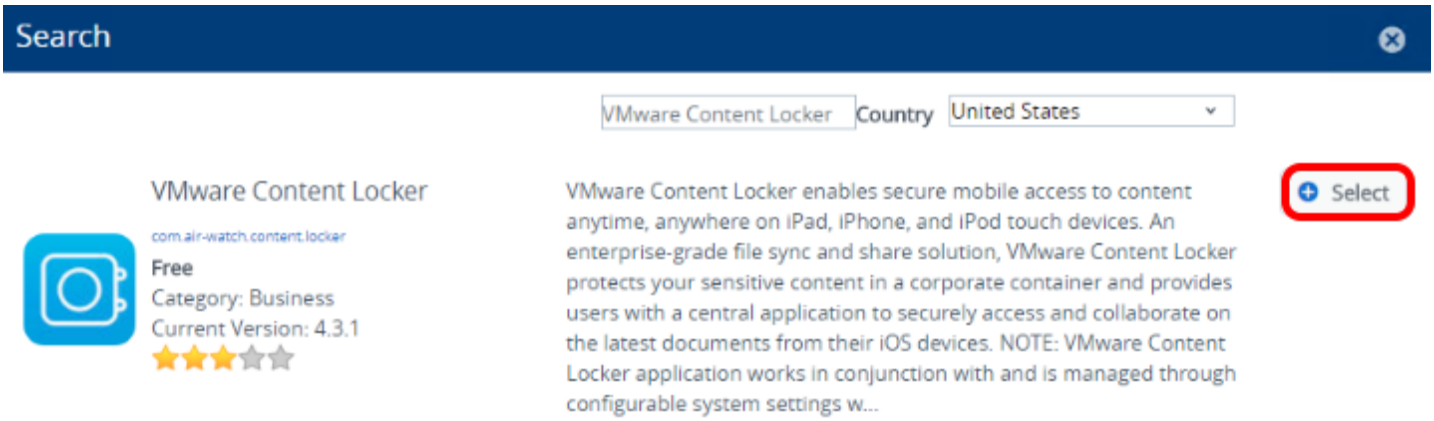
1. In the top-right corner, click the **Add** button.
2. Click **Public Application**.

Search for the VMware Content Locker Application



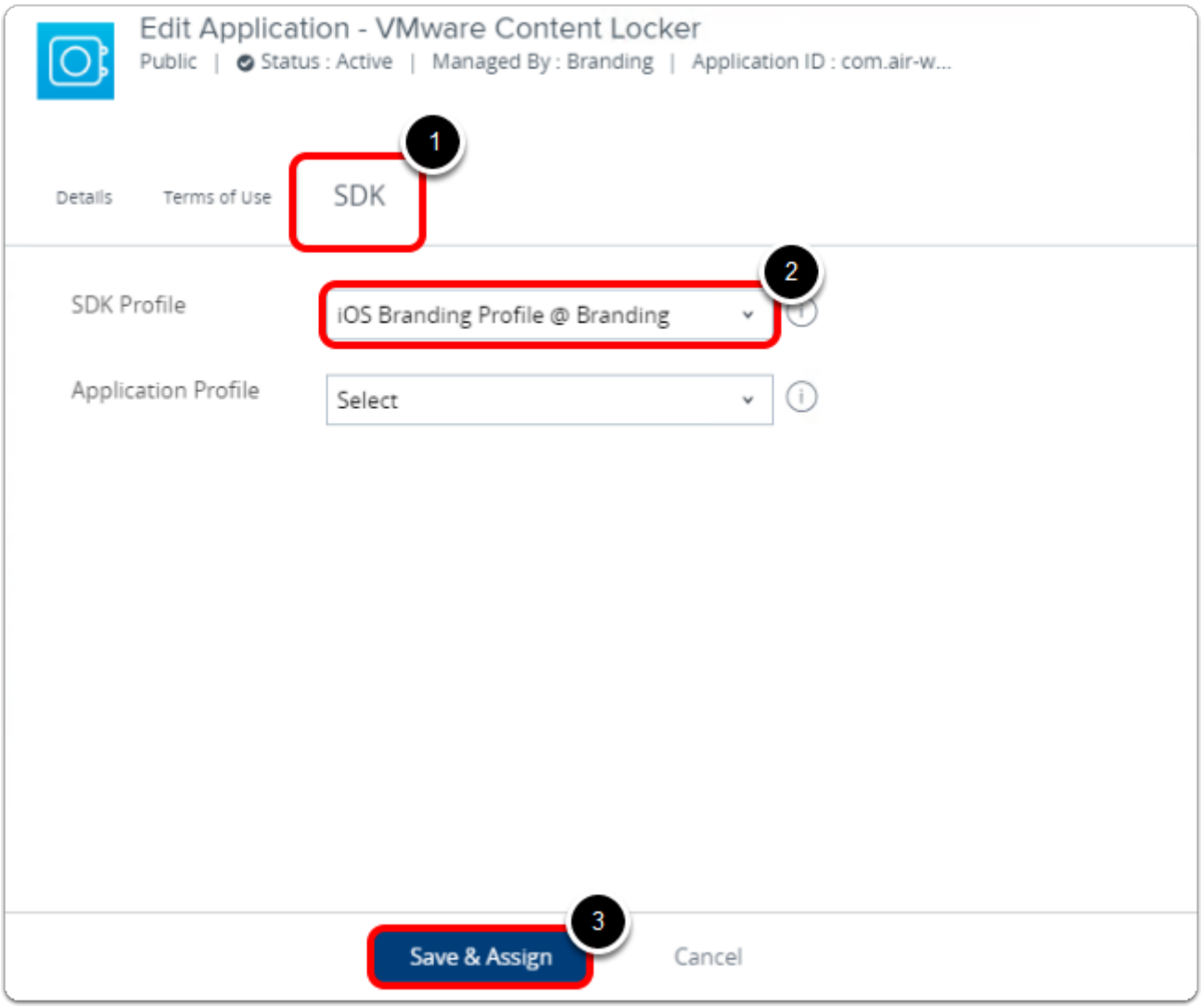
1. Select **Apple iOS** for the **Platform**.
2. Select **Search App Store** for the **Source**.
3. Enter **"VMware Content Locker"** for the **Name**.
4. Click **Next**.

Select the VMware Content Locker Application



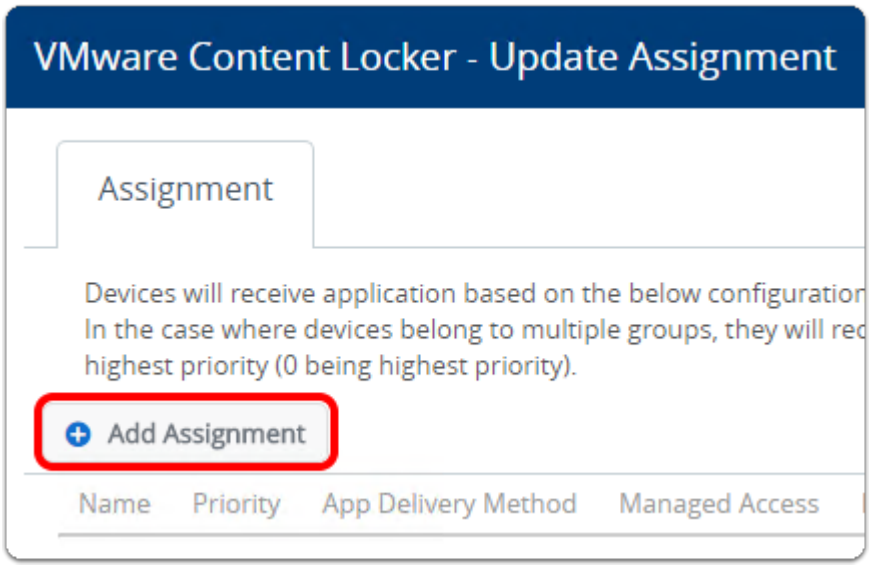
Click **Select** for the VMware Content Locker application.

Assign Branding Profile to VMware Content Locker



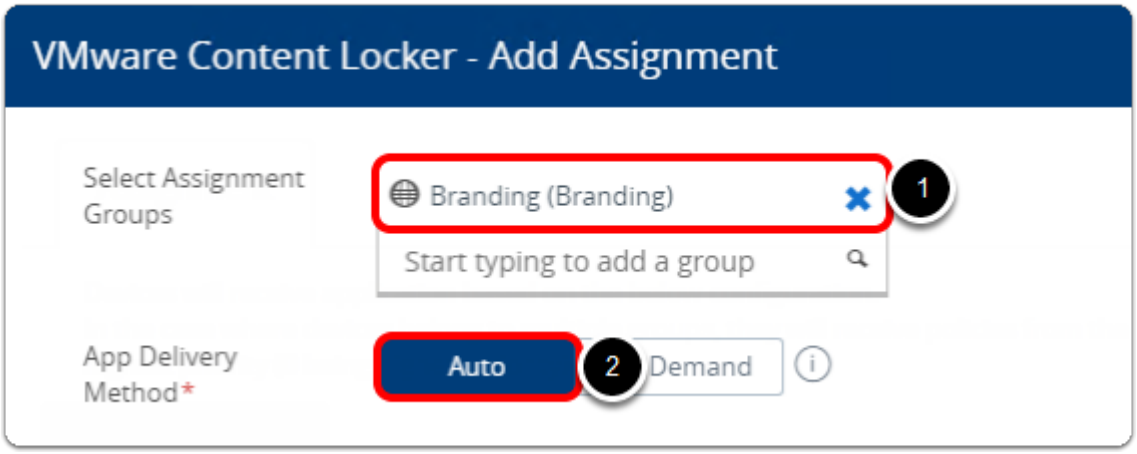
1. Click the **SDK** tab.
2. Select **iOS Branding Profile** for the **SDK Profile**.
3. Click **Save & Assign**.

Add Assignment to VMware Content Locker



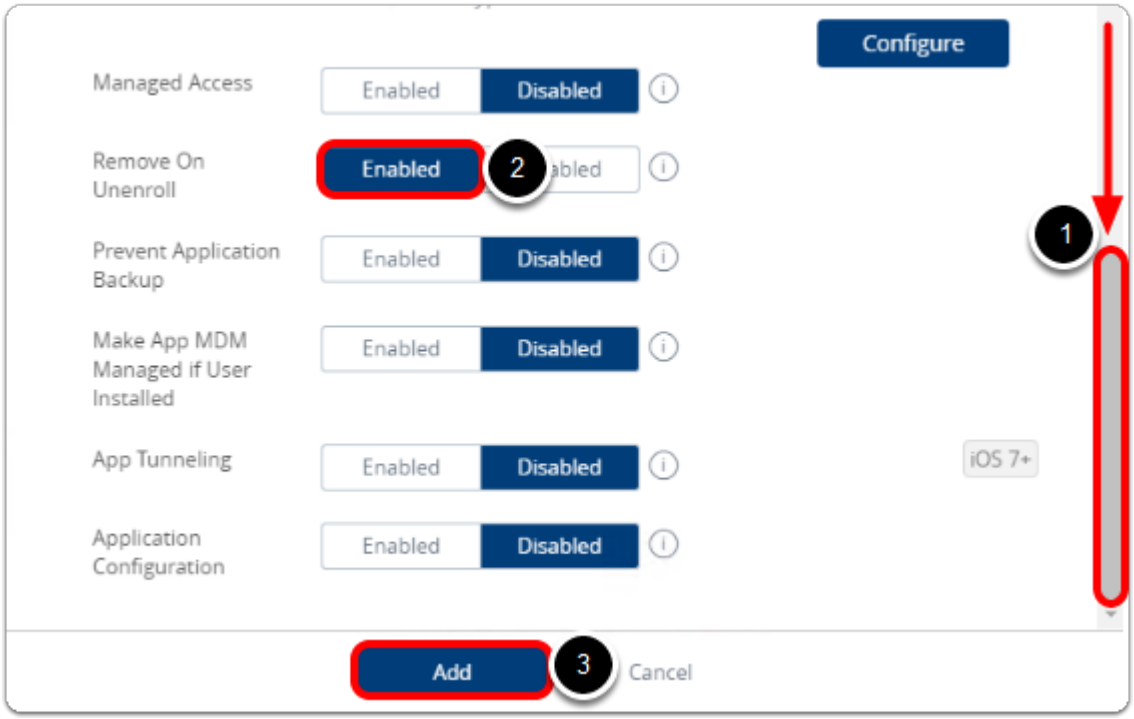
Click **+ Add Assignment**.

Configure VMware Content Locker Assignment Settings



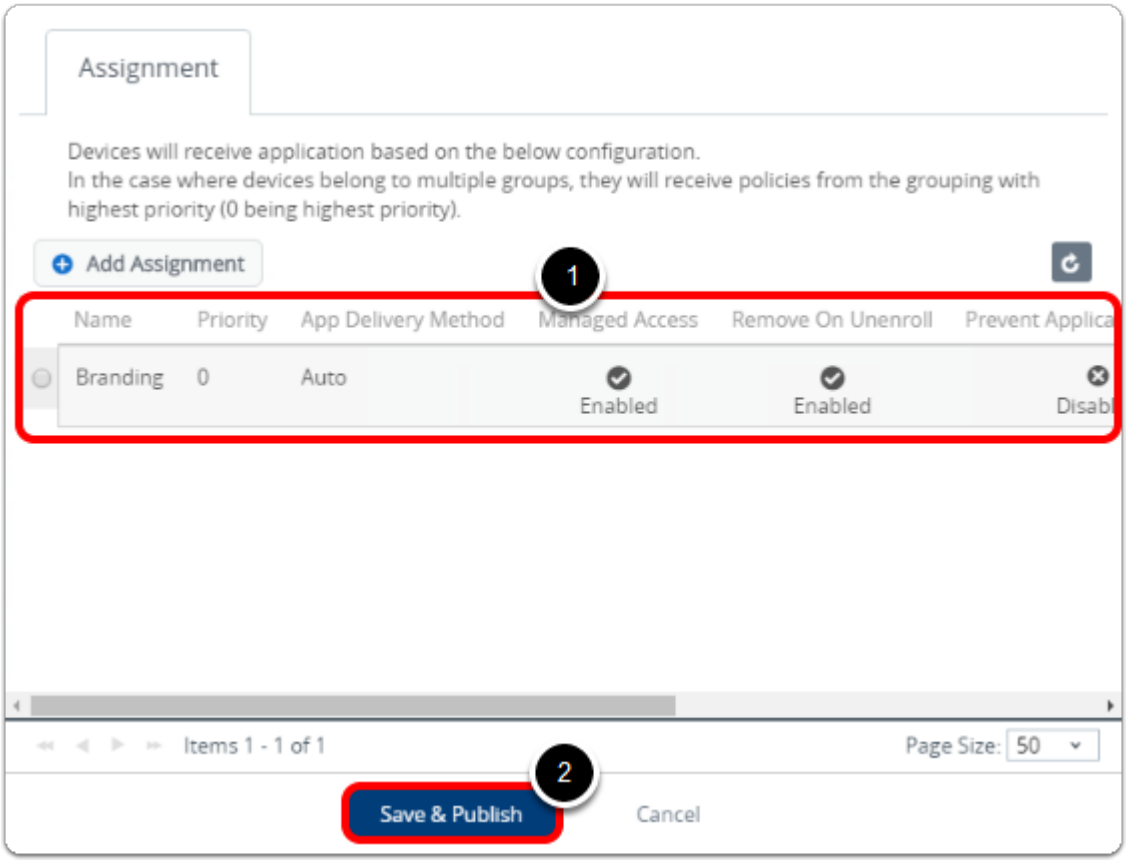
1. Select **Branding** for the **Select Assignment Groups** field.
2. Select **Auto** for the **App Delivery Method**.

Configure Policies for VMware Content Locker



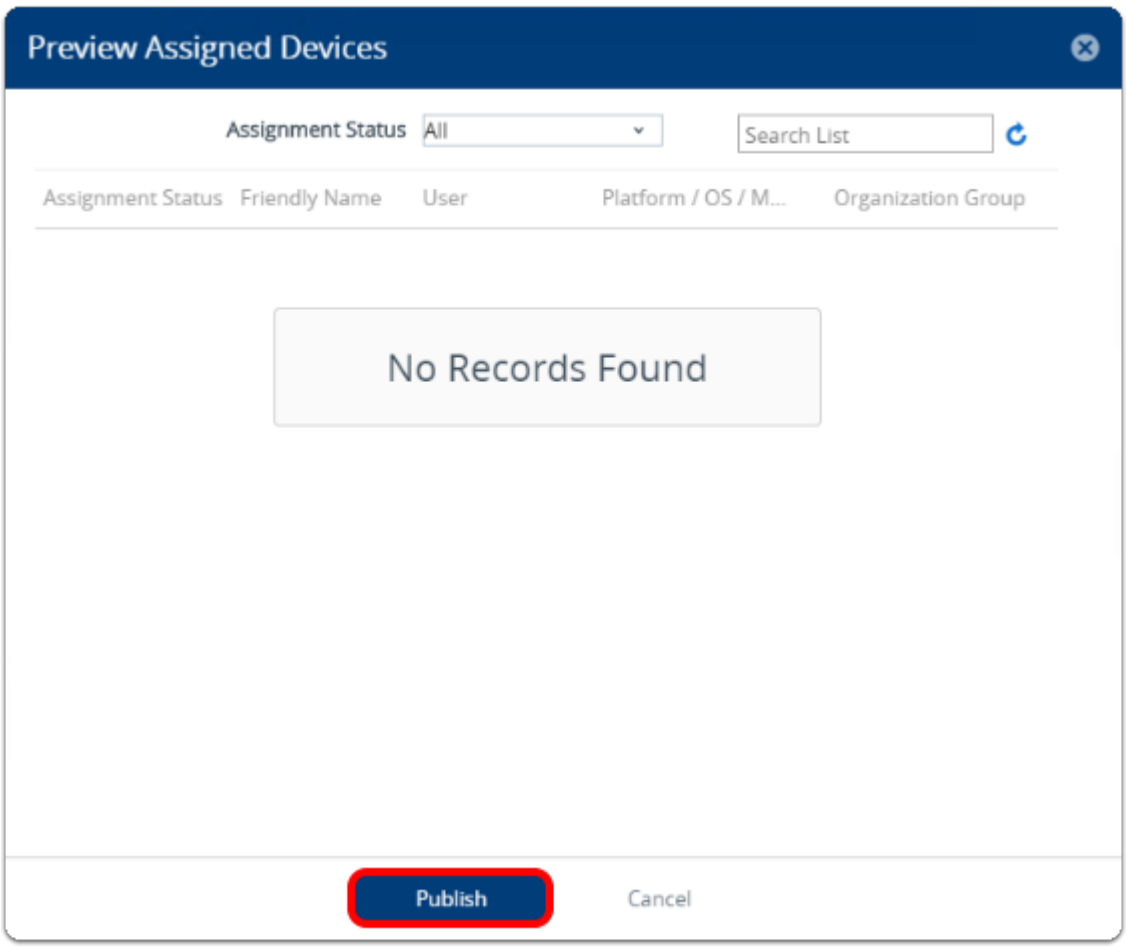
1. Scroll down to find the Policies section.
2. Set **Remove on Unenroll** to **Enabled**.
3. Click **Add**.

Save and Publish VMware Content Locker



1. Confirm that the Assignment you created for the Branding organization group is displayed.
2. Click **Save & Publish**.

Preview Assigned Devices and Publish VMware Content Locker

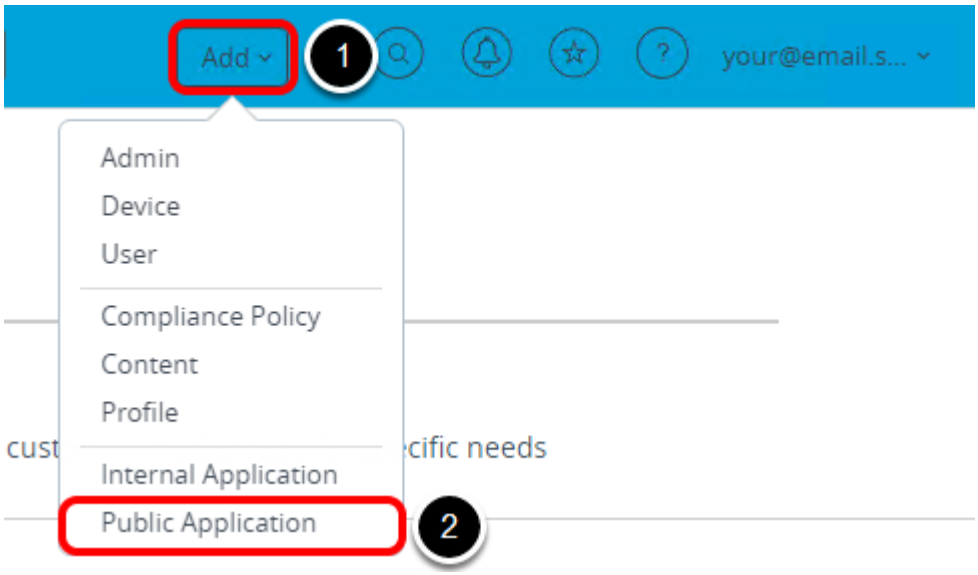


Click **Publish**.

Publish the VMware Browser Application

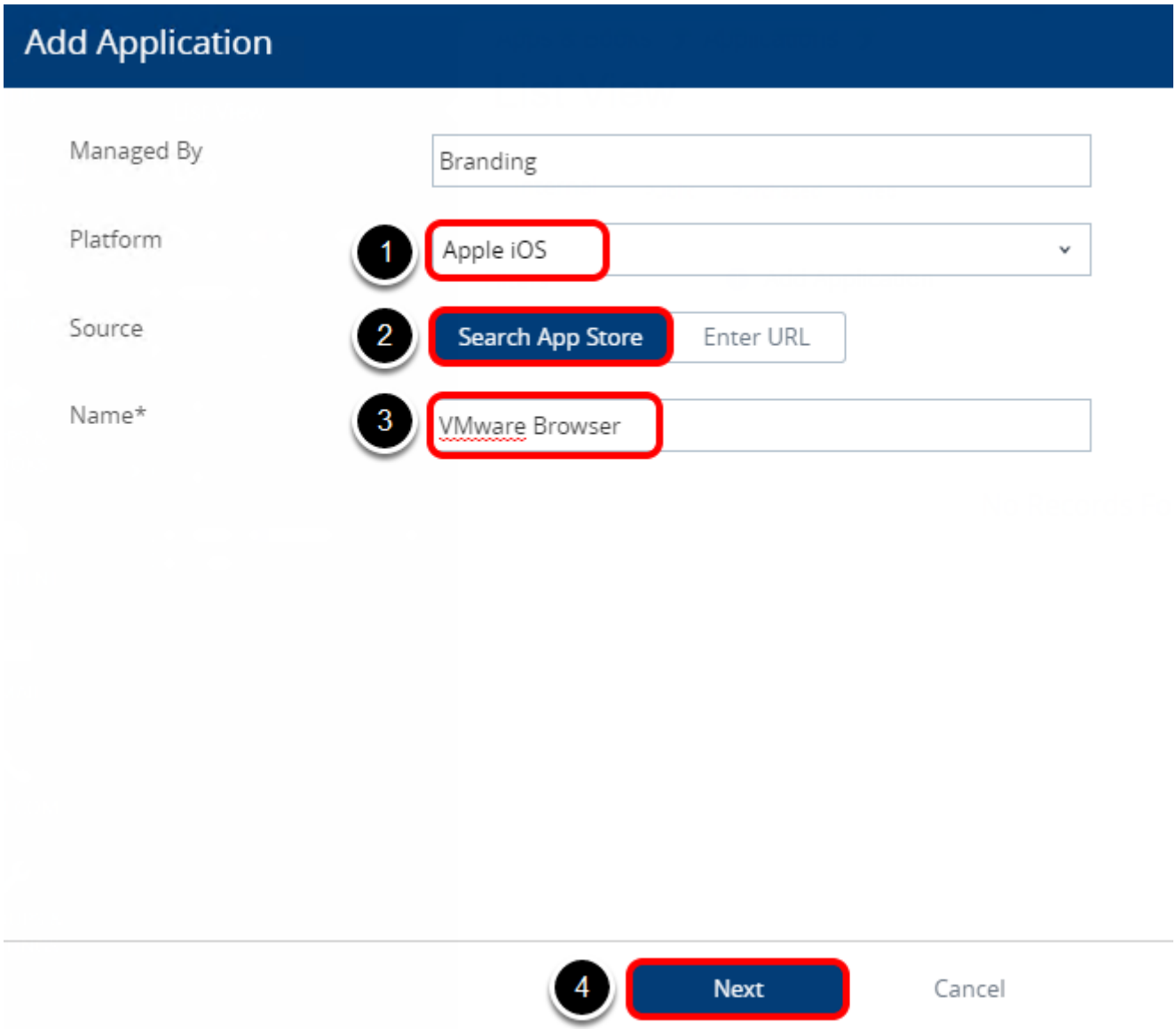
In this step, we will publish the VMware Browser application to registered devices to test the Branding changes.

Add a New Public Application



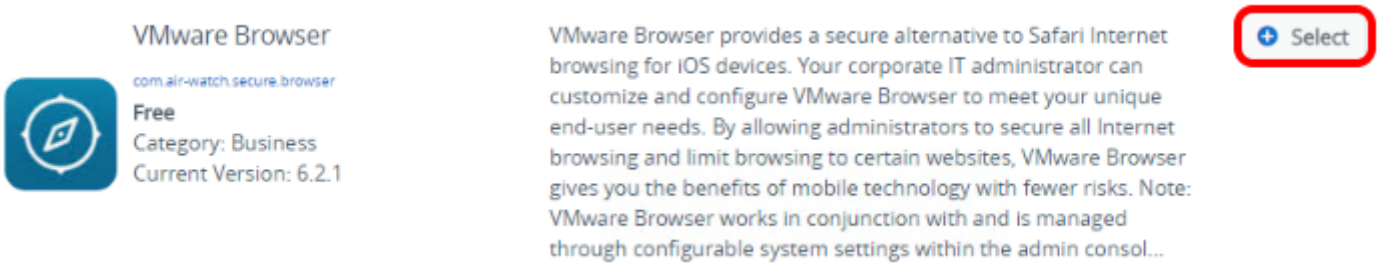
1. In the top-right corner, click the **Add** button.
2. Click **Public Application**.

Search for the VMware Browser Application



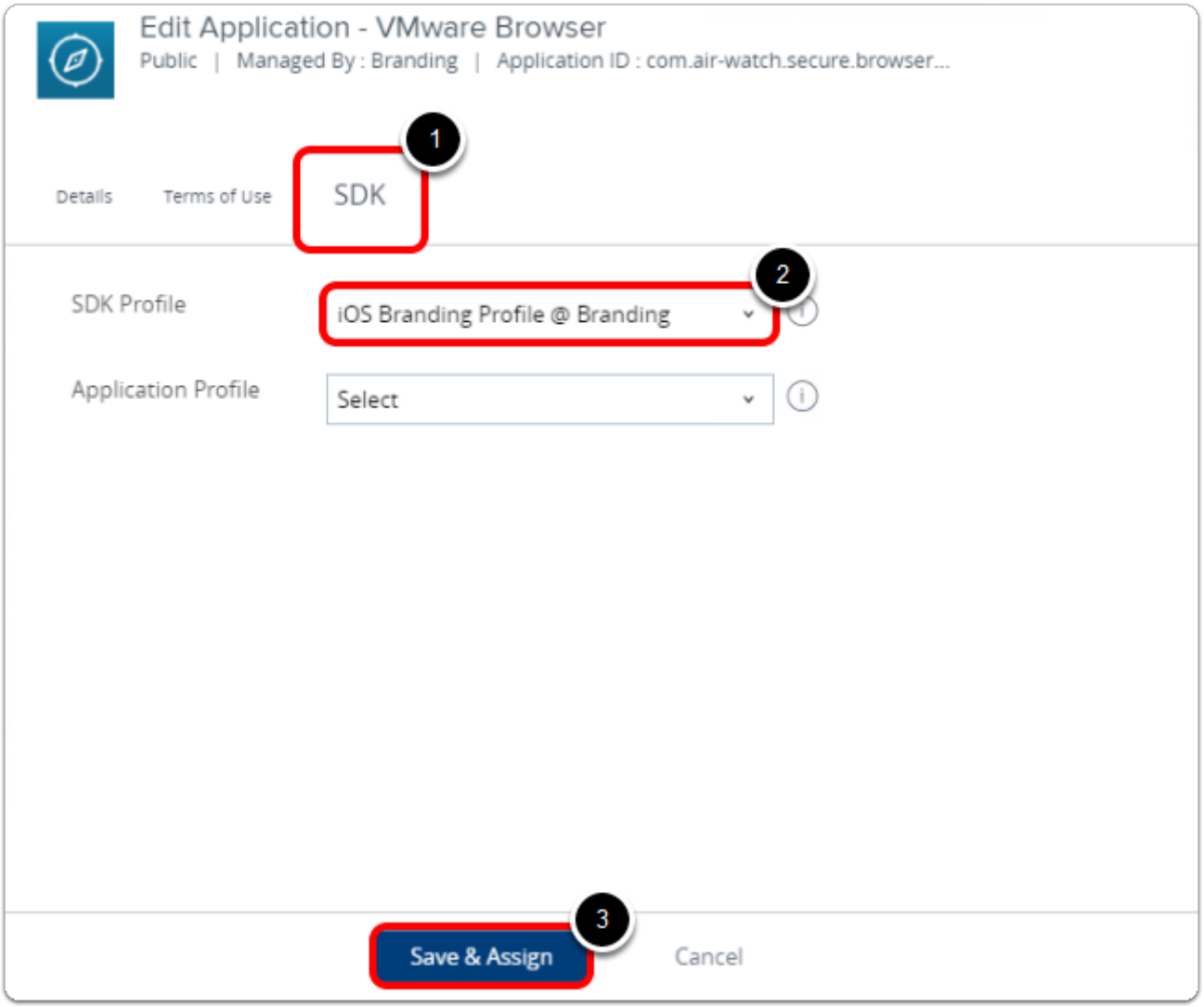
1. Select **Apple iOS** for the **Platform**.
2. Select **Search App Store** for the **Source**.
3. Enter **"VMware Browser"** for the **Name**.
4. Click **Next**.

Select the VMware Browser Application



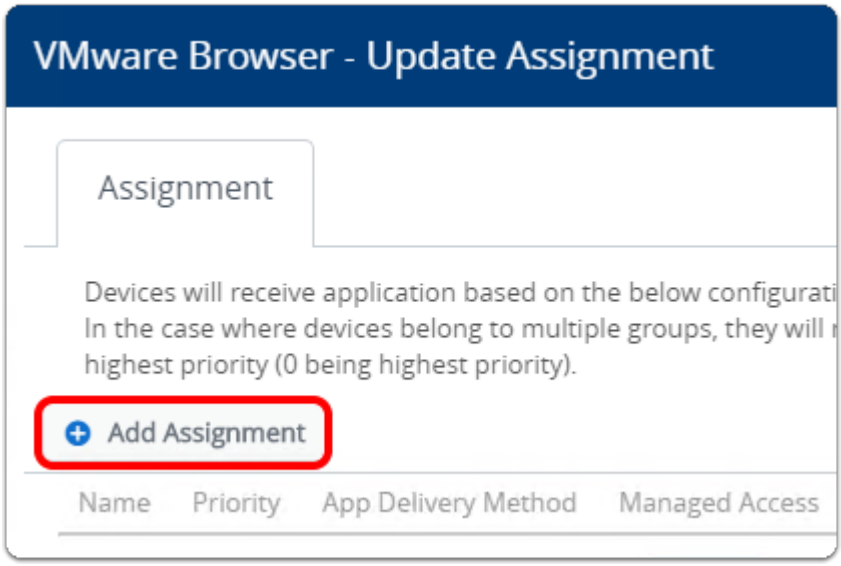
Click **Select** for the VMware Browser application.

Assign Branding Profile to VMware Browser



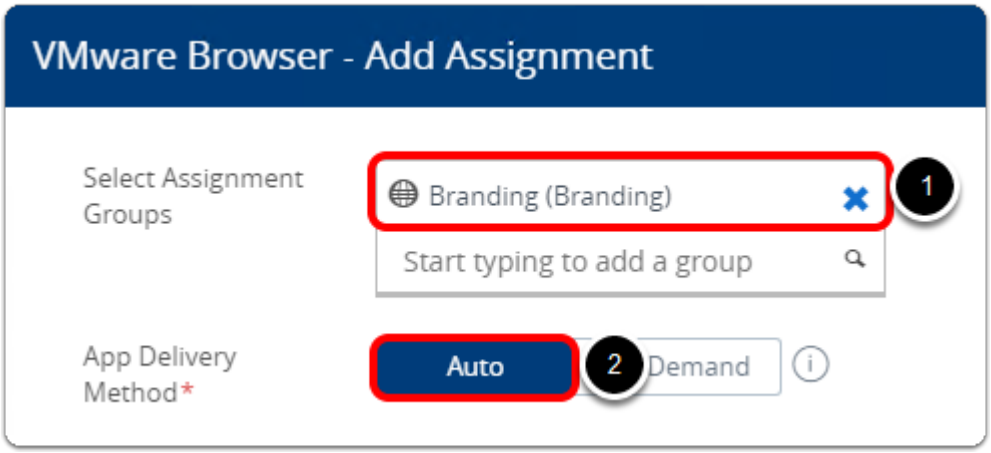
1. Click the **SDK** tab.
2. Select **iOS Branding Profile** for the **SDK Profile**.
3. Click **Save & Assign**.

Add Assignment to VMware Browser



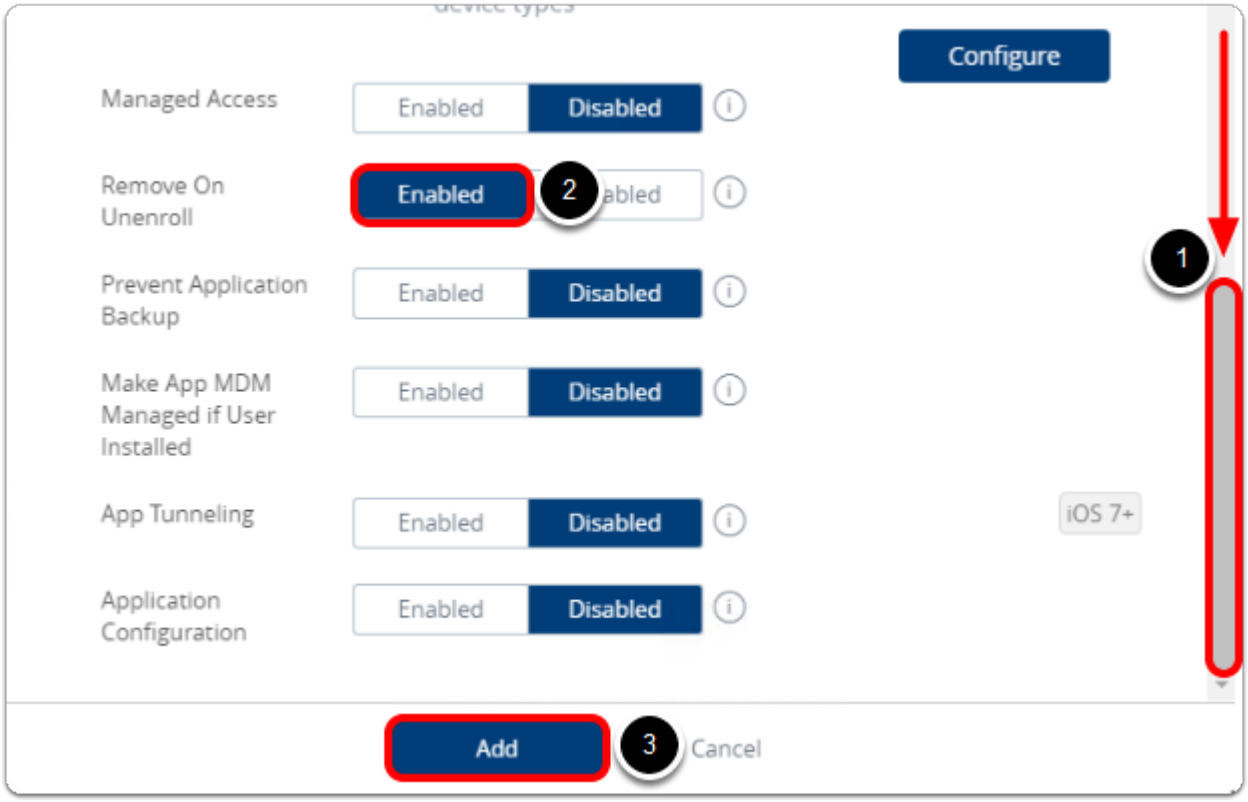
Click **+ Add Assignment**.

Configure VMware Browser Assignment Settings



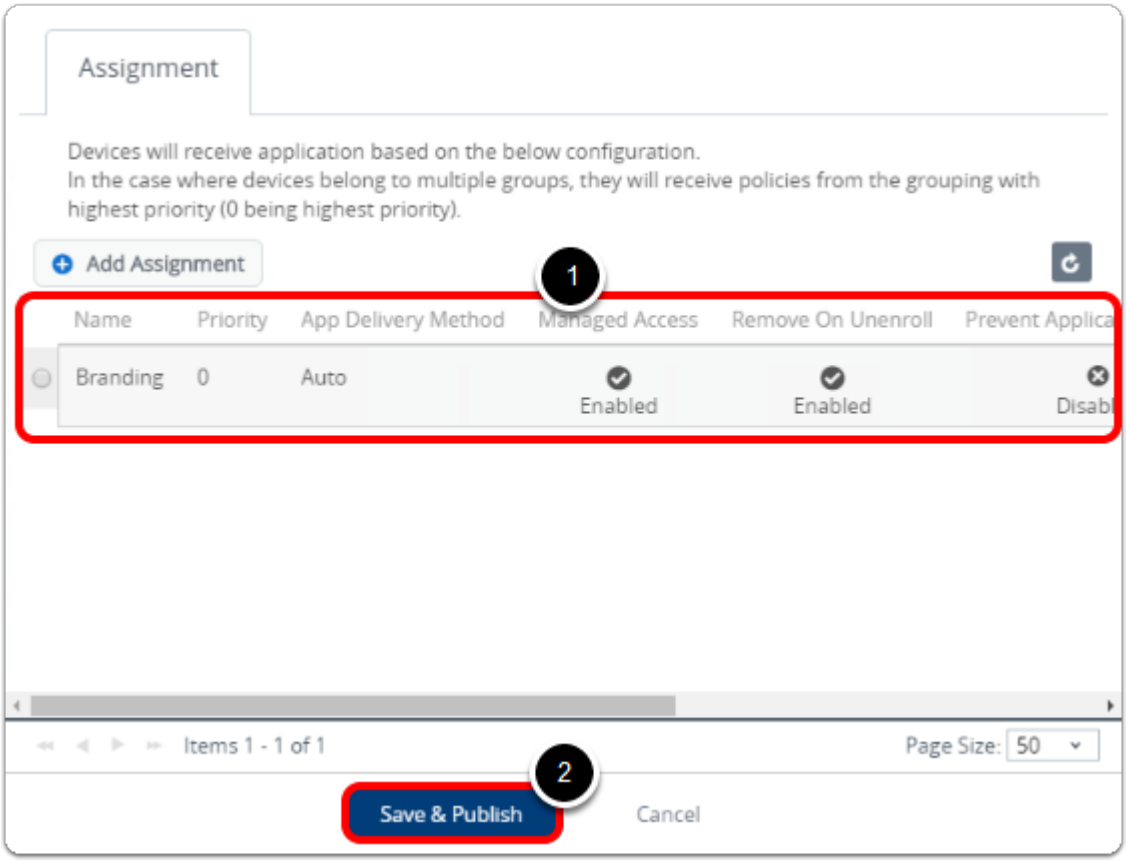
1. Select **Branding** for the **Select Assignment Groups** field.
2. Select **Auto** for the **App Delivery Method**.

Configure Policies for VMware Browser



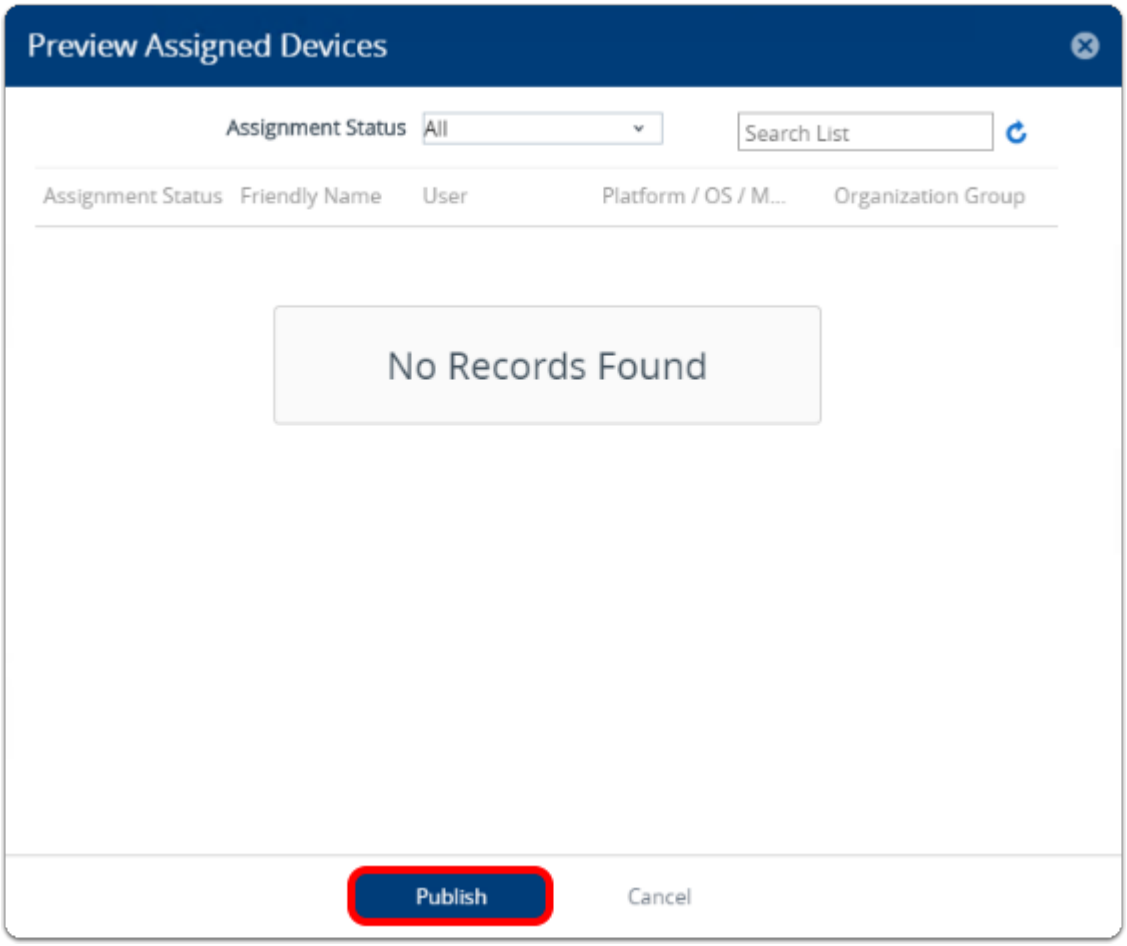
1. Scroll down to find the Policies section.
2. Set **Remove on Unenroll** to **Enabled**.
3. Click **Add**.

Save and Publish VMware Browser



1. Confirm that the Assignment you created for the Branding organization group is displayed.
2. Click **Save & Publish**.

Preview Assigned Devices and Publish VMware Browser

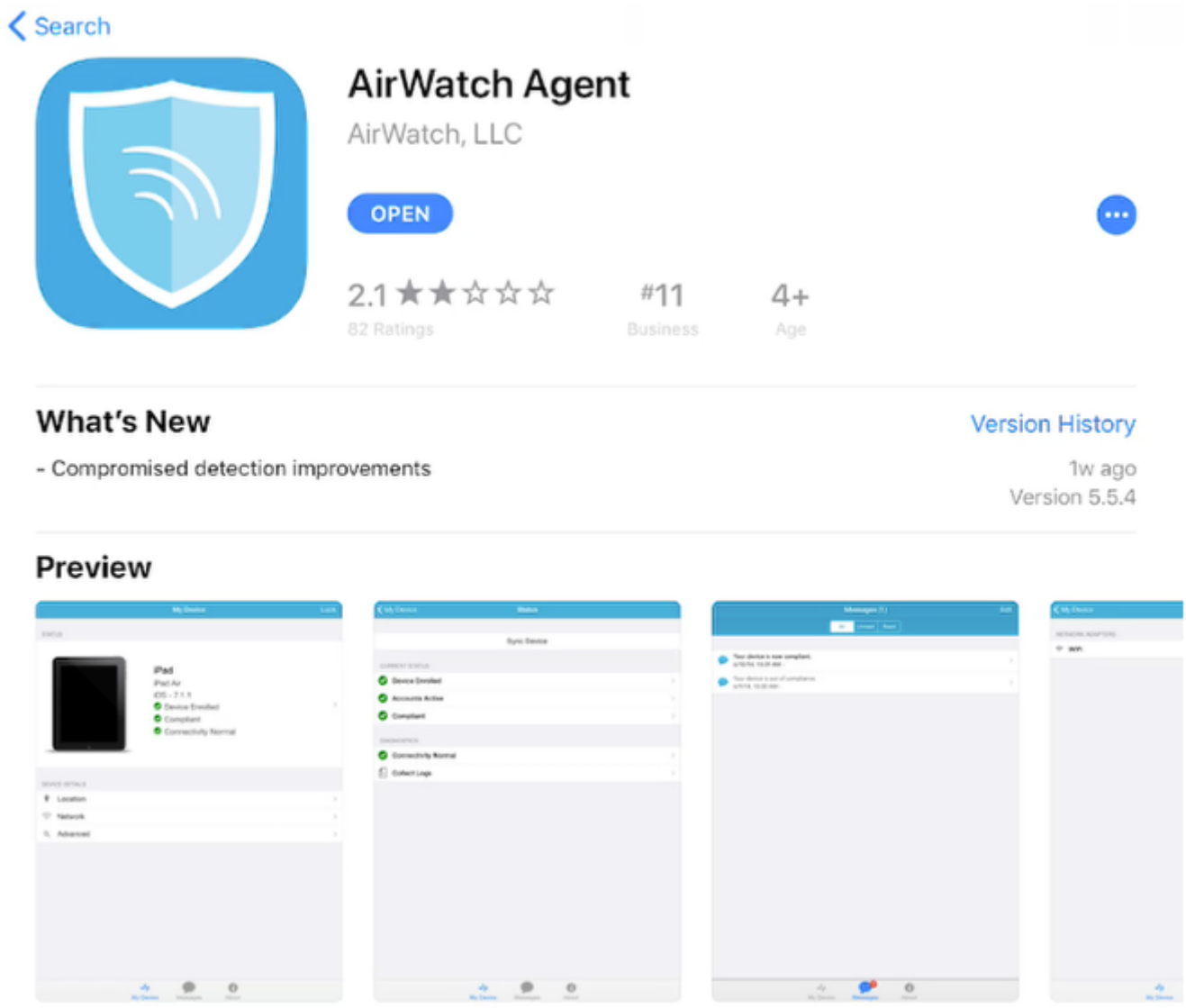


Click **Publish**.

iOS Device Enrollment (into Branding Group)

You are now going to enroll your iOS device for use with this module.

Download/Install AirWatch MDM Agent Application from App Store - IF NEEDED

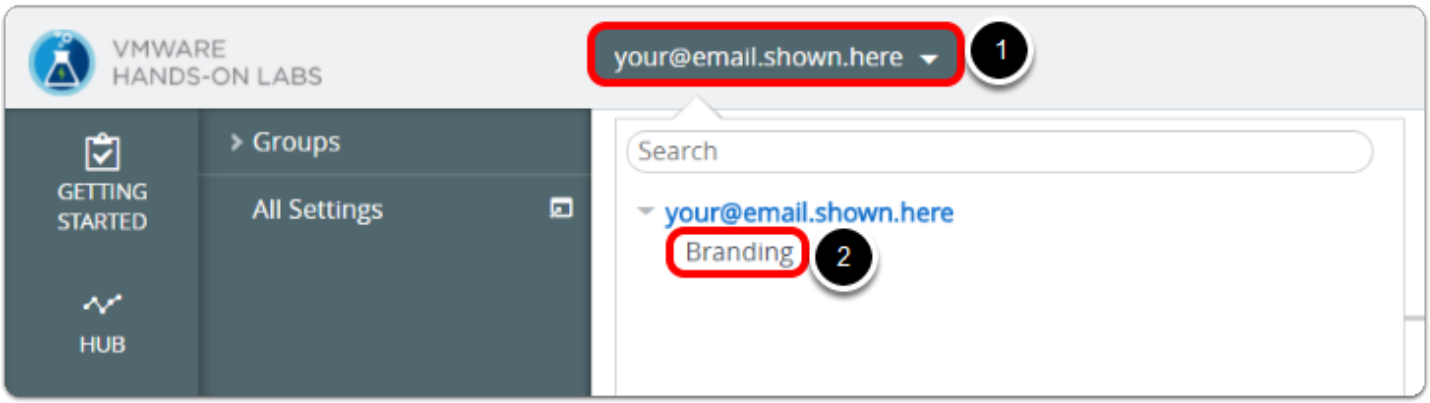


NOTE - Checked out devices will likely have the AirWatch MDM Agent already installed. You may skip this step if your device has the AirWatch MDM agent installed.

At this point, if using your own iOS device or if the device you are using does NOT have the AirWatch MDM Agent Application installed, then install the AirWatch Application.

To Install the AirWatch MDM Agent application from the App Store, open the App Store application and download the free **AirWatch MDM Agent** application.

Switch to the Branding Group (IF NEEDED)



If your organization group is not showing as **your@email.shown.here / Branding**, follow the below steps to switch to the Branding organization group that you created earlier.

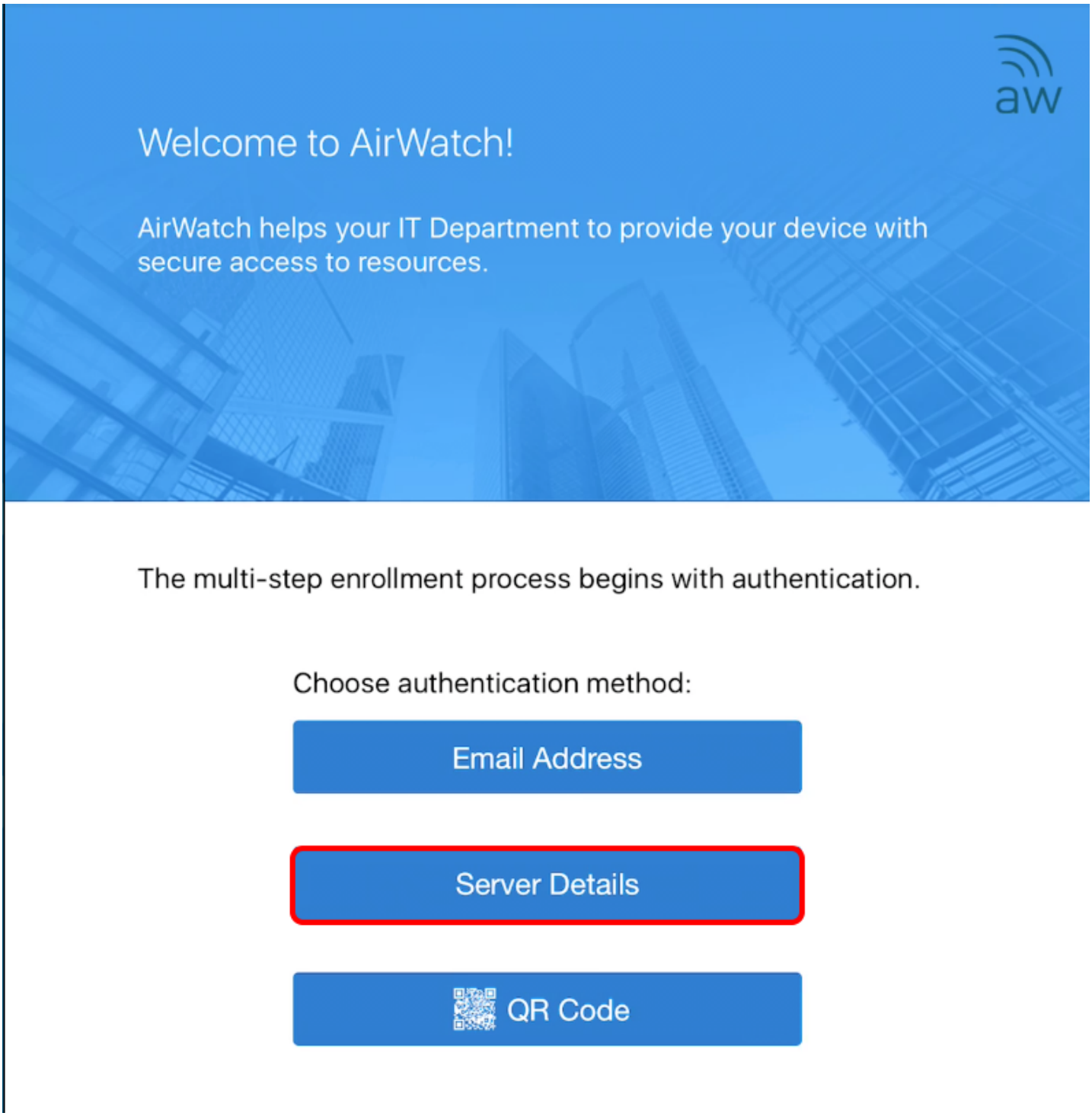
1. Click the **Organization Group** dropdown labeled **your@email.shown.here**.
2. Click the **Branding** organization group under your@email.shown.here.

Launching the AirWatch MDM Agent

Launch the **AirWatch Agent** app on the device.

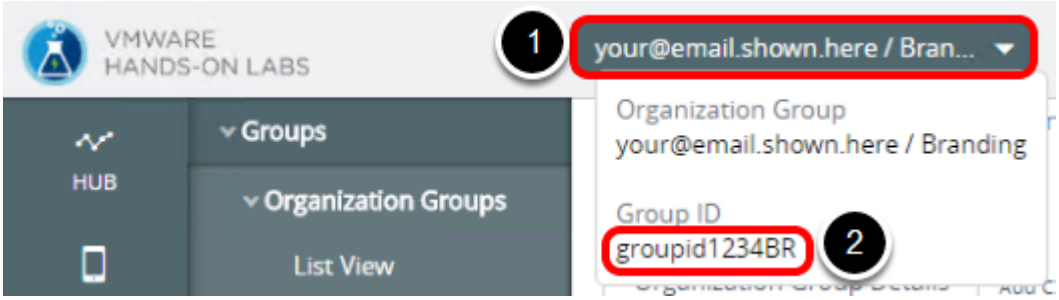
NOTE - If you have your own iOS device and would like to test you will need to download the agent first.

Choose the Enrollment Method



Click on the **Server Details** button.

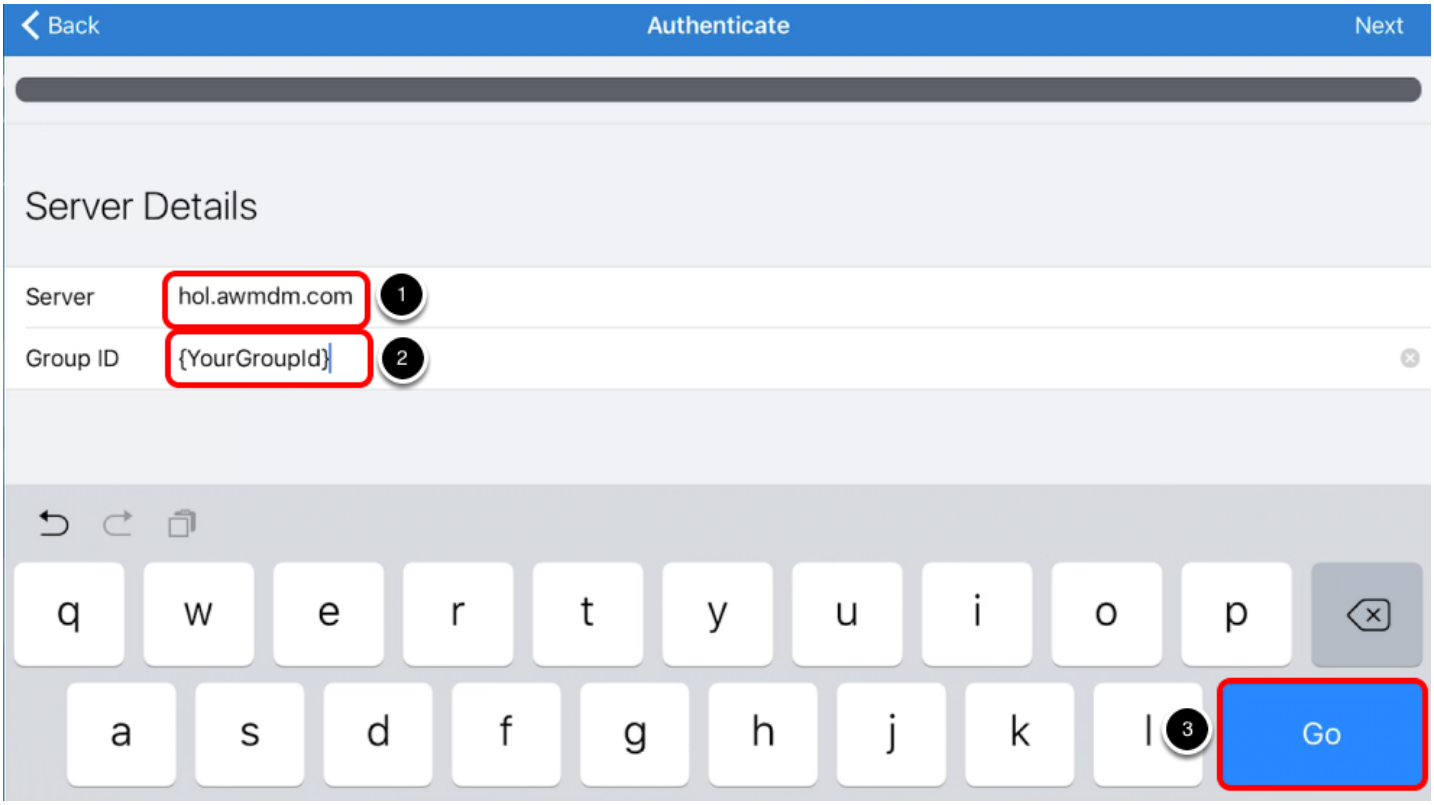
Finding your Group ID



The first step is to make sure you know what your **Organization Group ID** is.

1. To find the Group ID, hover your mouse over the Organization Group tab at the top of the screen. Look for the email address you used to log in to the lab portal.
2. Your **Group ID** is displayed at the bottom of the Organization Group pop up. The **Group ID** is required when enrolling your device in the following steps.

Attach the AirWatch MDM Agent to the HOL Sandbox



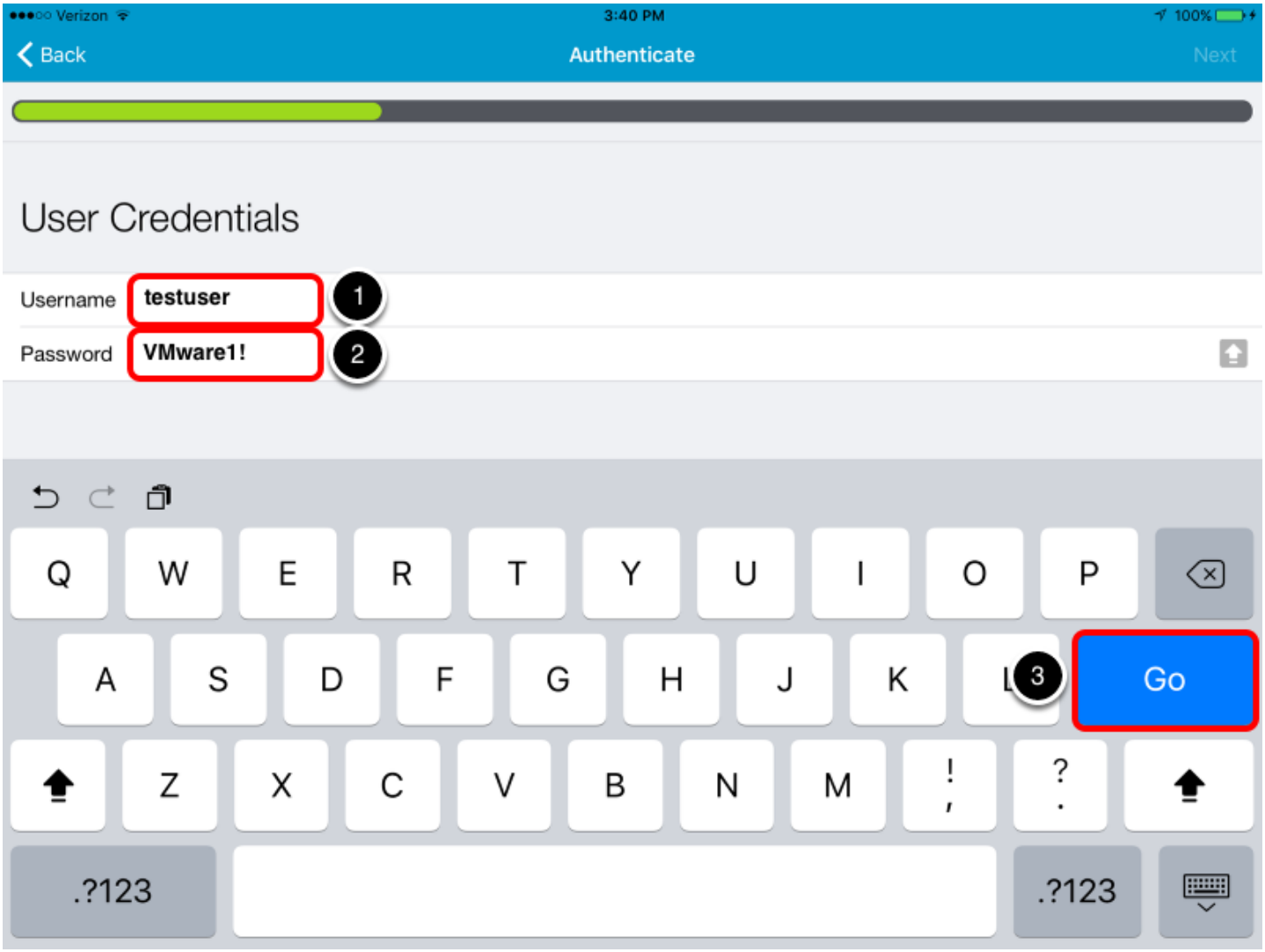
Once the Agent has launched you can enroll the device. To do so, follow the below steps.

1. Enter **"hol.awmdm.com"** for the **Server** field.

2. Enter your **Group ID** for your Organization Group for the **Group ID** field. Your Group ID was noted previously in the **Finding your Group ID** step.
3. Tap the **Go** button.

NOTE - If on an iPhone, you may have to close the keyboard by clicking Done in order to click the Continue button.

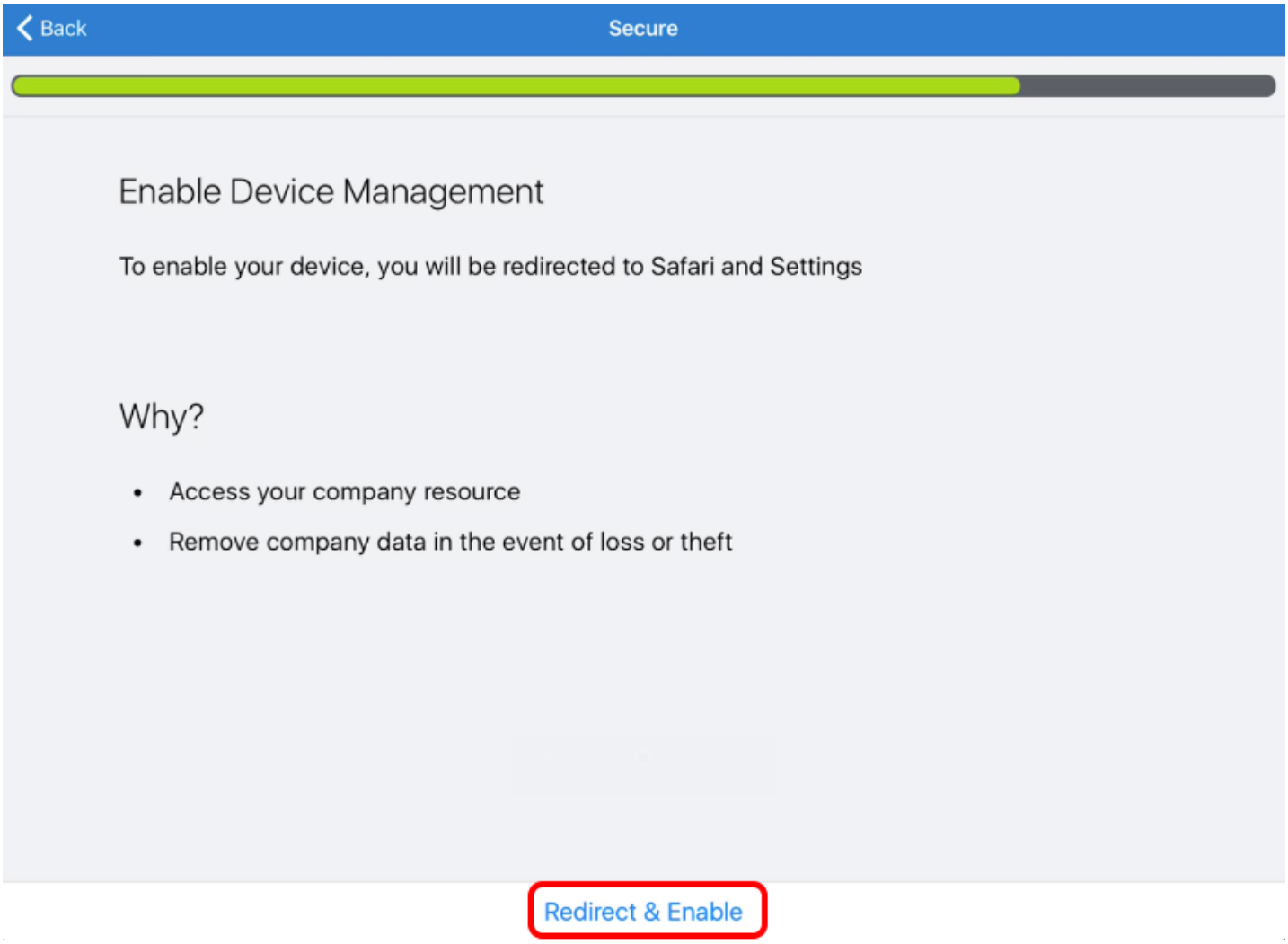
Authenticate the AirWatch MDM Agent



On this screen, enter the **Username** and **Password** for the basic user account.

1. Enter **"testuser"** in the **Username** field.
2. Enter **"VMware1!"** in the **Password** field.
3. Tap the **Go** button.

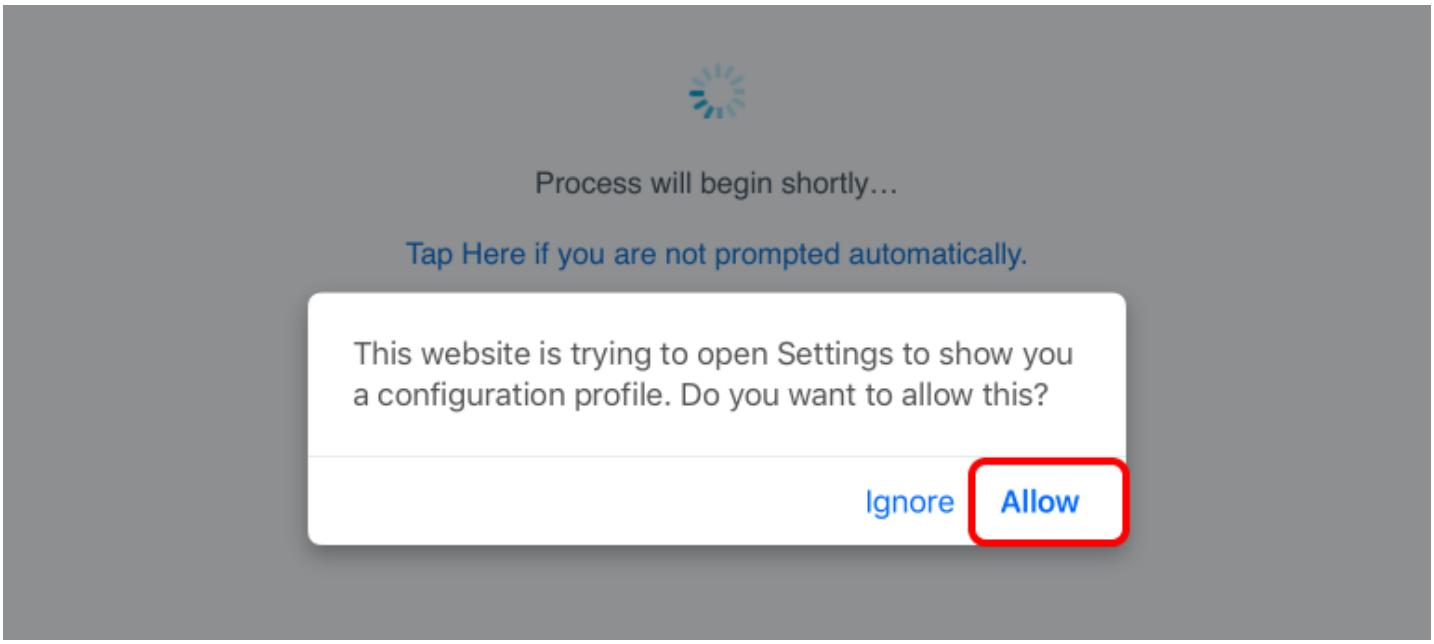
Redirect to Safari and Enable MDM Enrollment in Settings



The AirWatch Agent will now redirect you to Safari and start the process of enabling MDM in the device settings.

Tap on **Redirect & Enable** at the bottom of the screen.

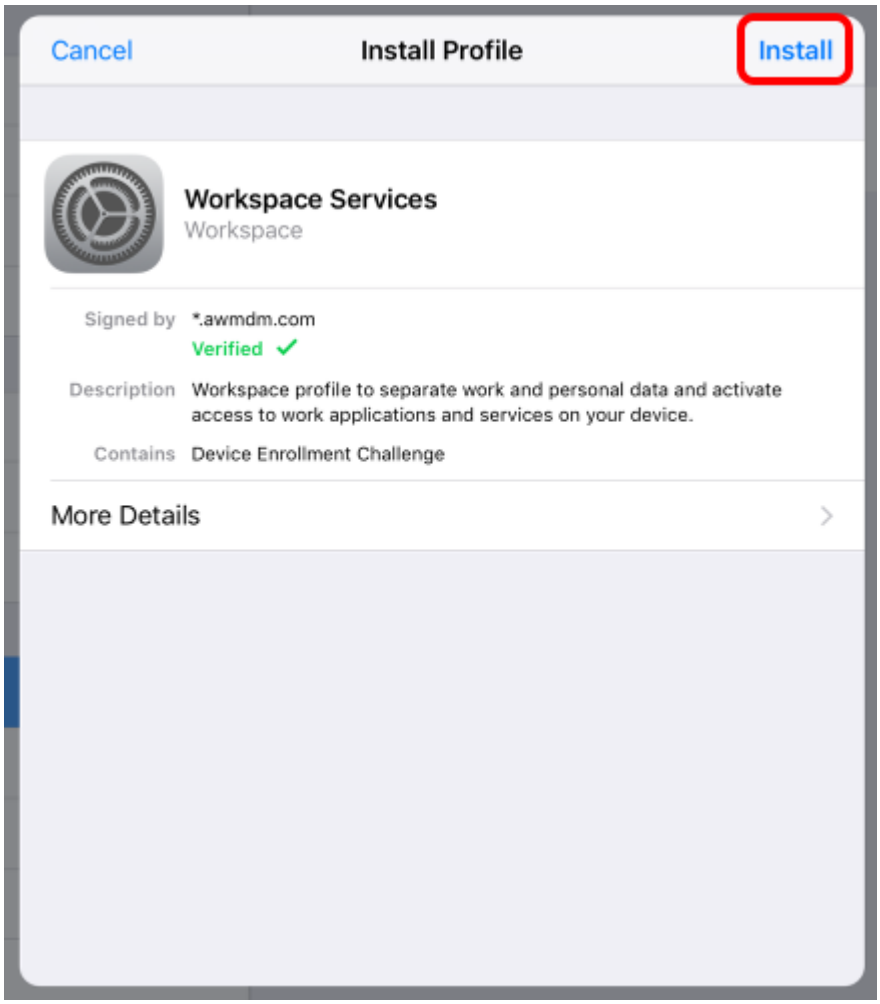
Allow Website to Open Settings (IF NEEDED)



If you prompted to allow the website to open Settings to show you a configuration profile, tap **Allow**.

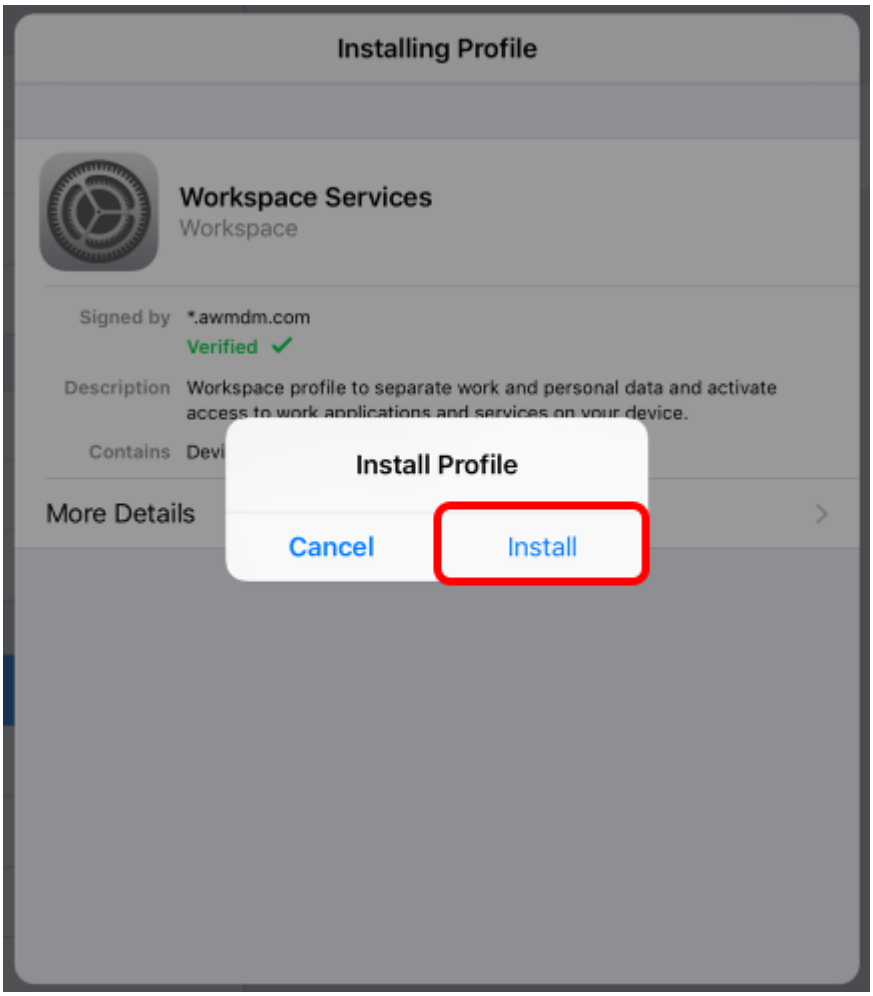
NOTE - If you do not see this prompt, ignore this and continue to the next step. This prompt will only occur for iOS Devices on iOS 10.3.3 or later

Install the MDM Profile



Tap **Install** in the upper right corner of the Install Profile dialog box.

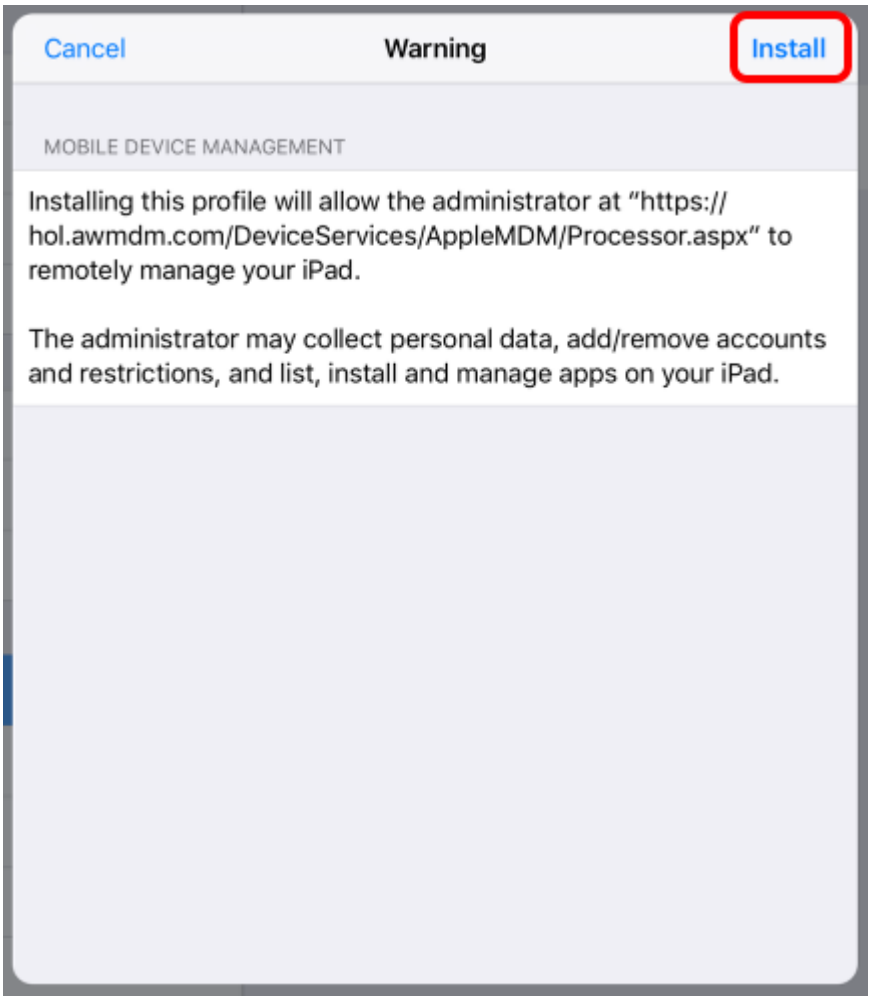
Install and Verify the AirWatch MDM Profile



Tap **Install** when prompted at the Install Profile dialog.

NOTE - If a PIN is requested, it is the current device PIN. Provided VMware devices should not have a PIN.

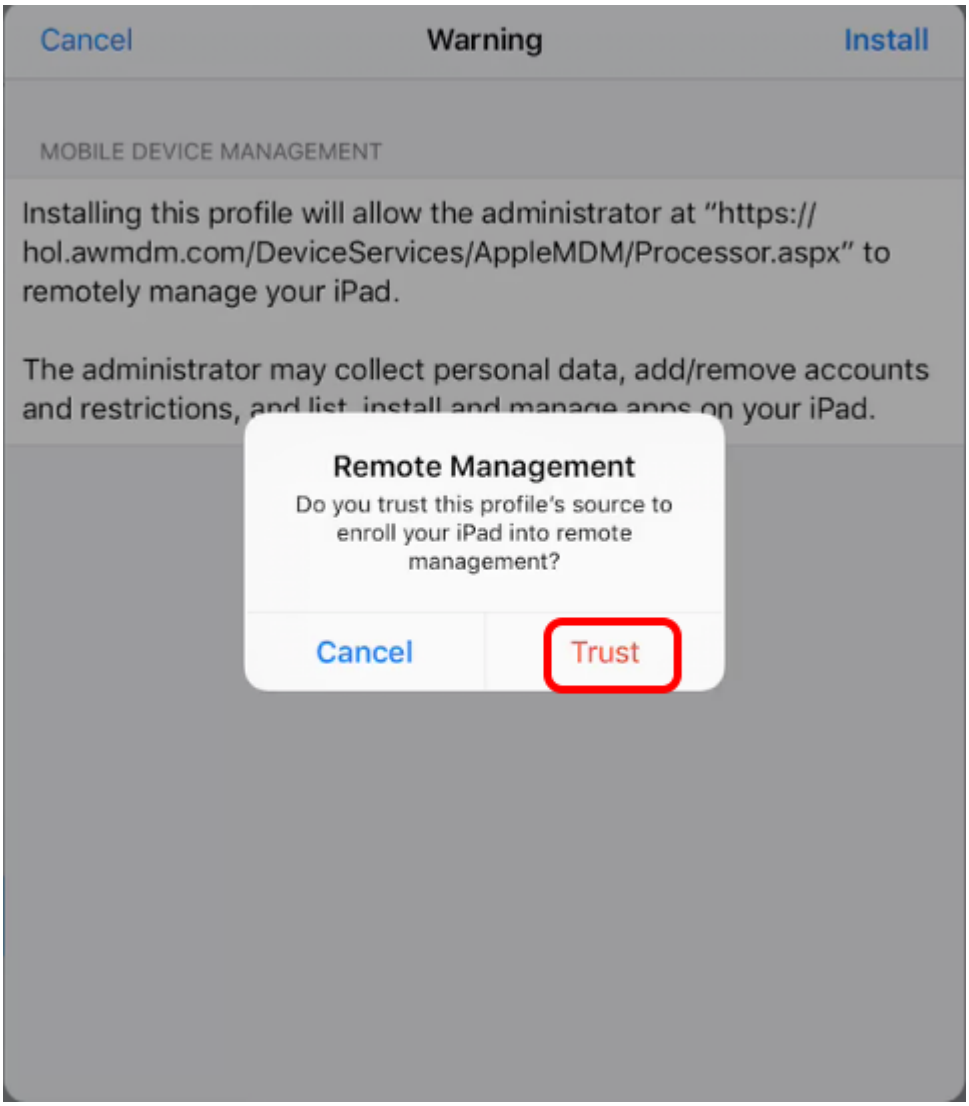
iOS MDM Profile Warning



You should now see the iOS Profile Installation warning explaining what this profile installation will allow on the iOS device.

Tap **Install** in the upper-right corner of the screen.

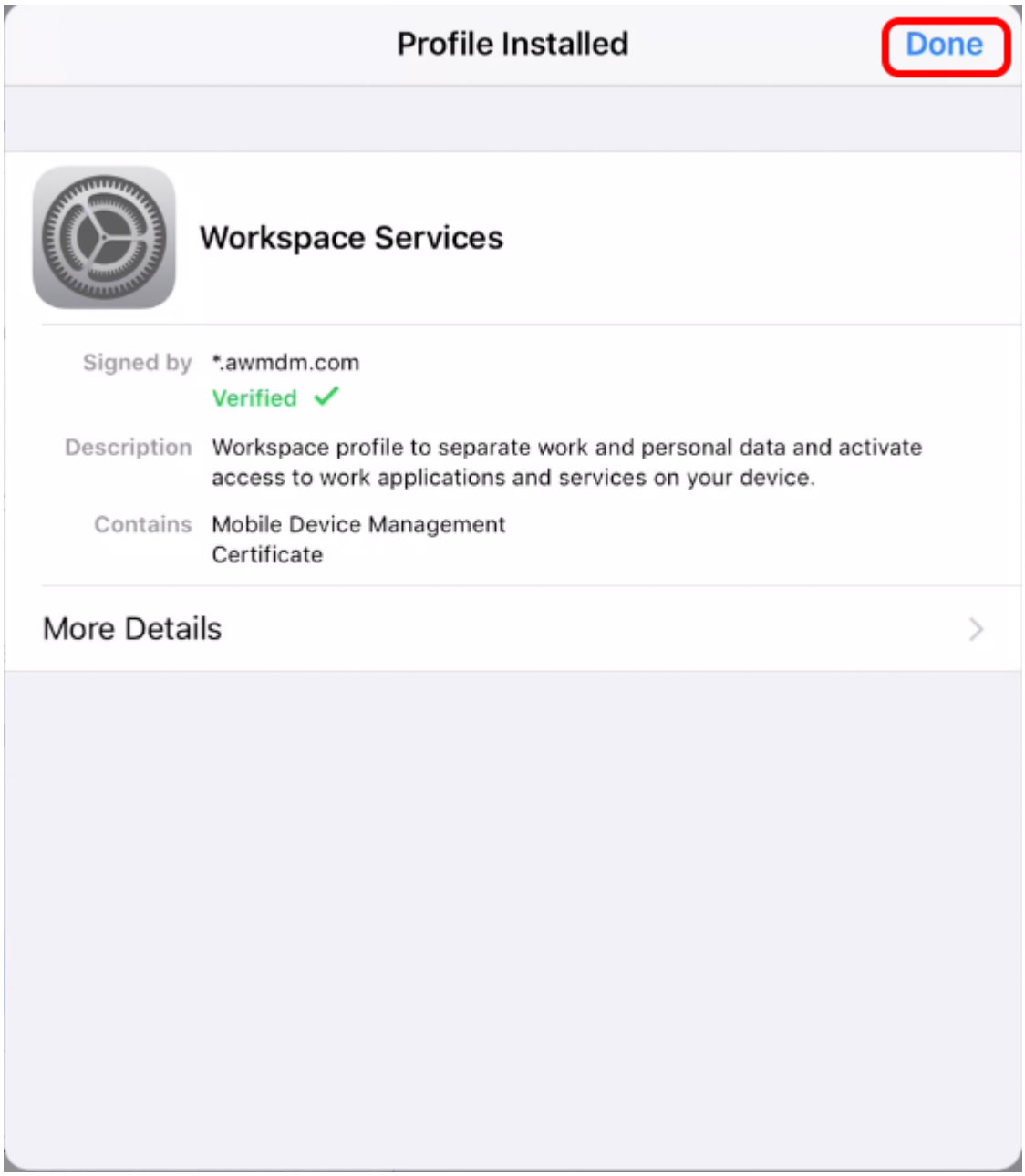
Trust the Remote Management Profile.



You should now see the iOS request to trust the source of the MDM profile.

Tap **Trust** when prompted at the Remote Management dialog.

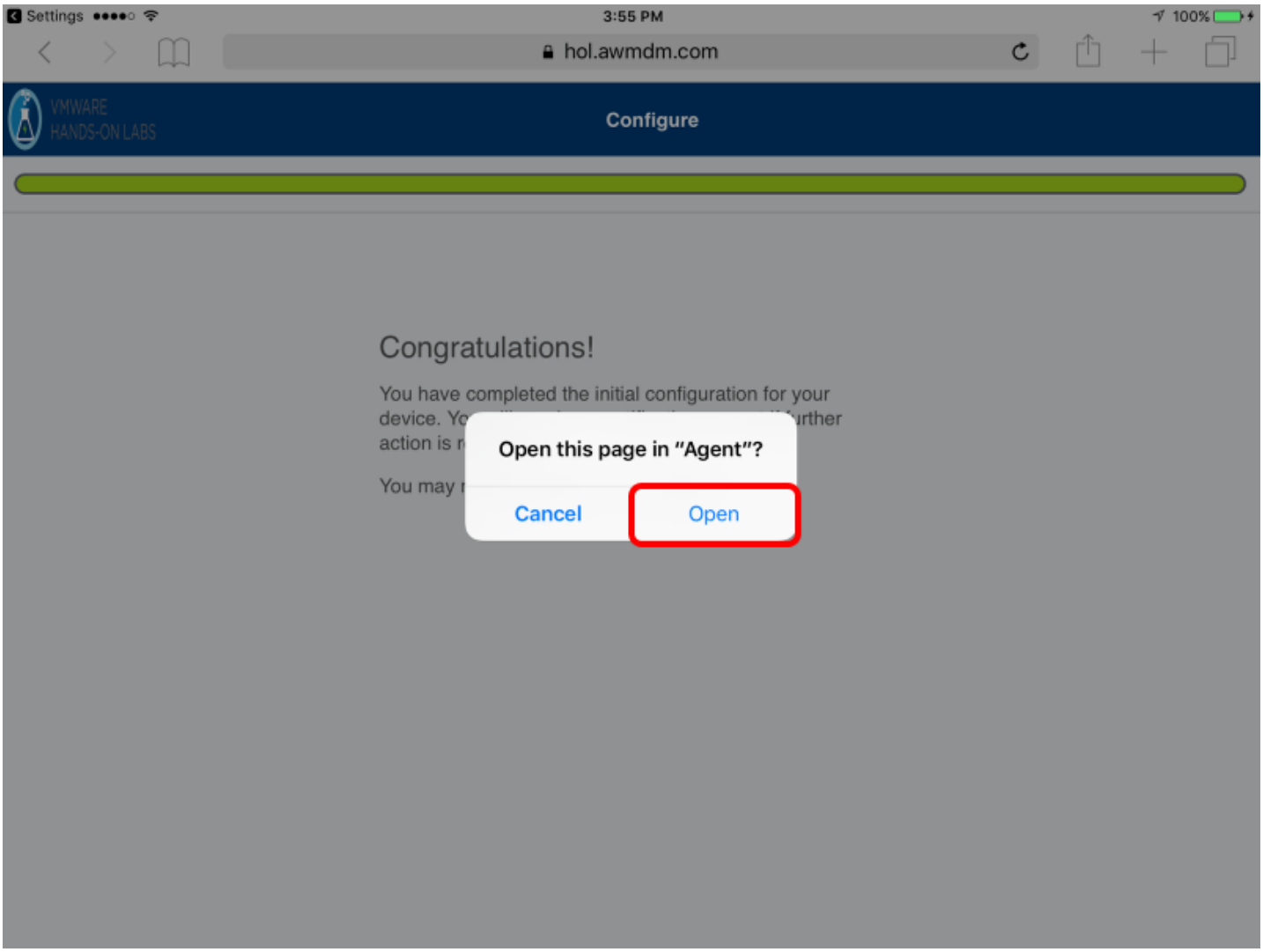
iOS Profile Installation Complete



You should now see the iOS Profile successfully installed.

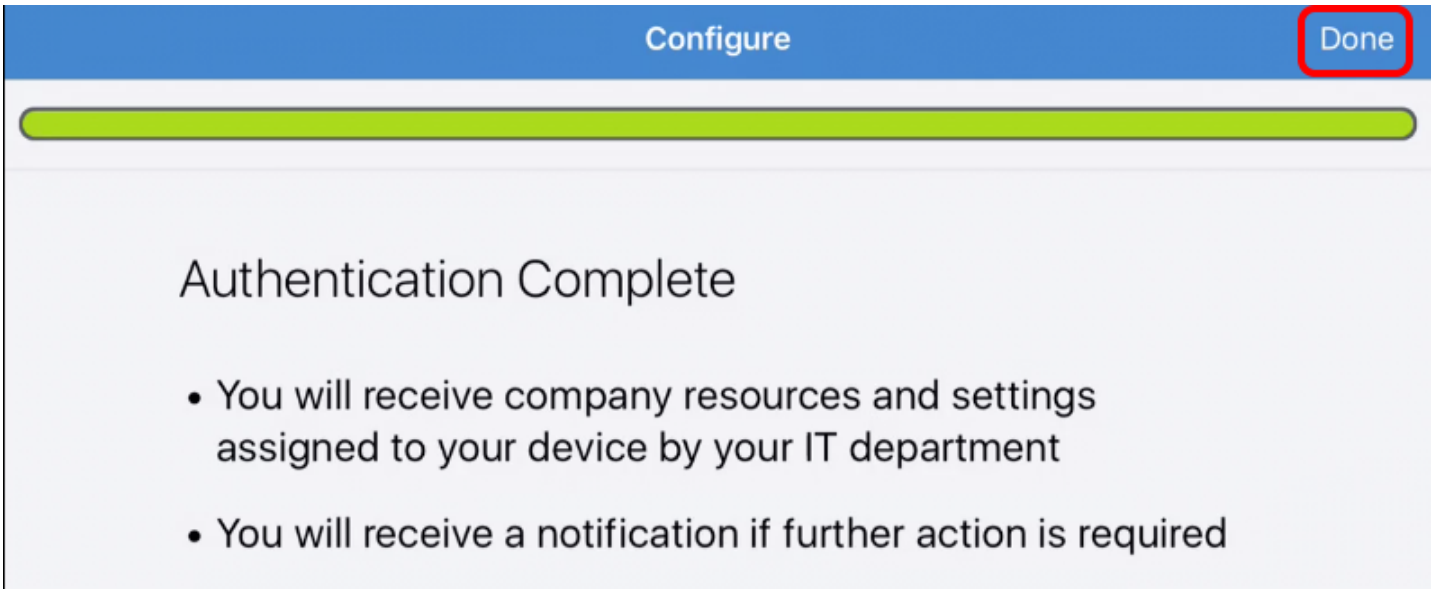
Tap **Done** in the upper right corner of the prompt.

AirWatch Enrollment Success



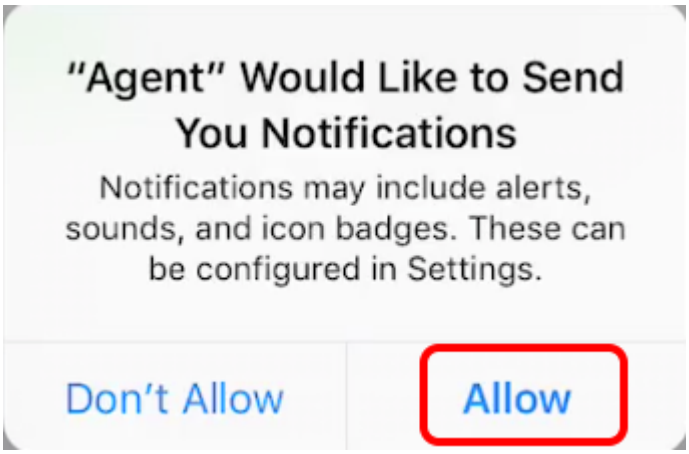
Your enrollment is now completed. Tap **Open** to navigate to the AirWatch Agent.

Accept the Authentication Complete Prompt



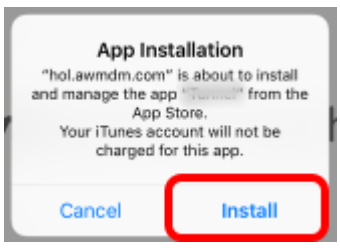
Click on **Done** to continue.

Accept Notification Prompt (IF NEEDED)



Tap **Allow** if you get a prompt for Notifications.

Accept the App Installation (IF NEEDED)



You may be prompted to install a series of applications depending on which Module you are taking. If prompted, tap **Install** to accept the application installation.

Confirm Application Branding

We will now inspect the applications on our enrolled iOS Device to confirm the Branding settings.

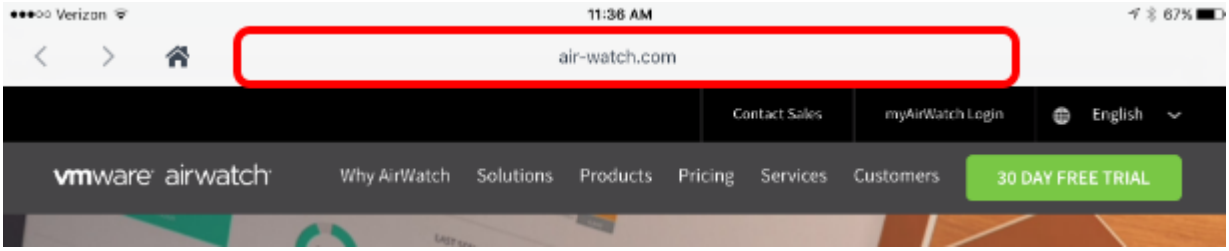
Confirm the Browser Branding Changes

Next, let us view the changes to the Browser.

Open the VMware Browser Application

Tap the **Browser** application.

View the VMware Browser Branding

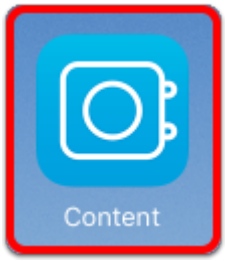


Notice that the Browser is in Kiosk mode, as we did not change this configuration in the Browser settings. The Home Page is also set to **https://www.air-watch.com** as per our branding update.

Confirm the Content Locker Branding

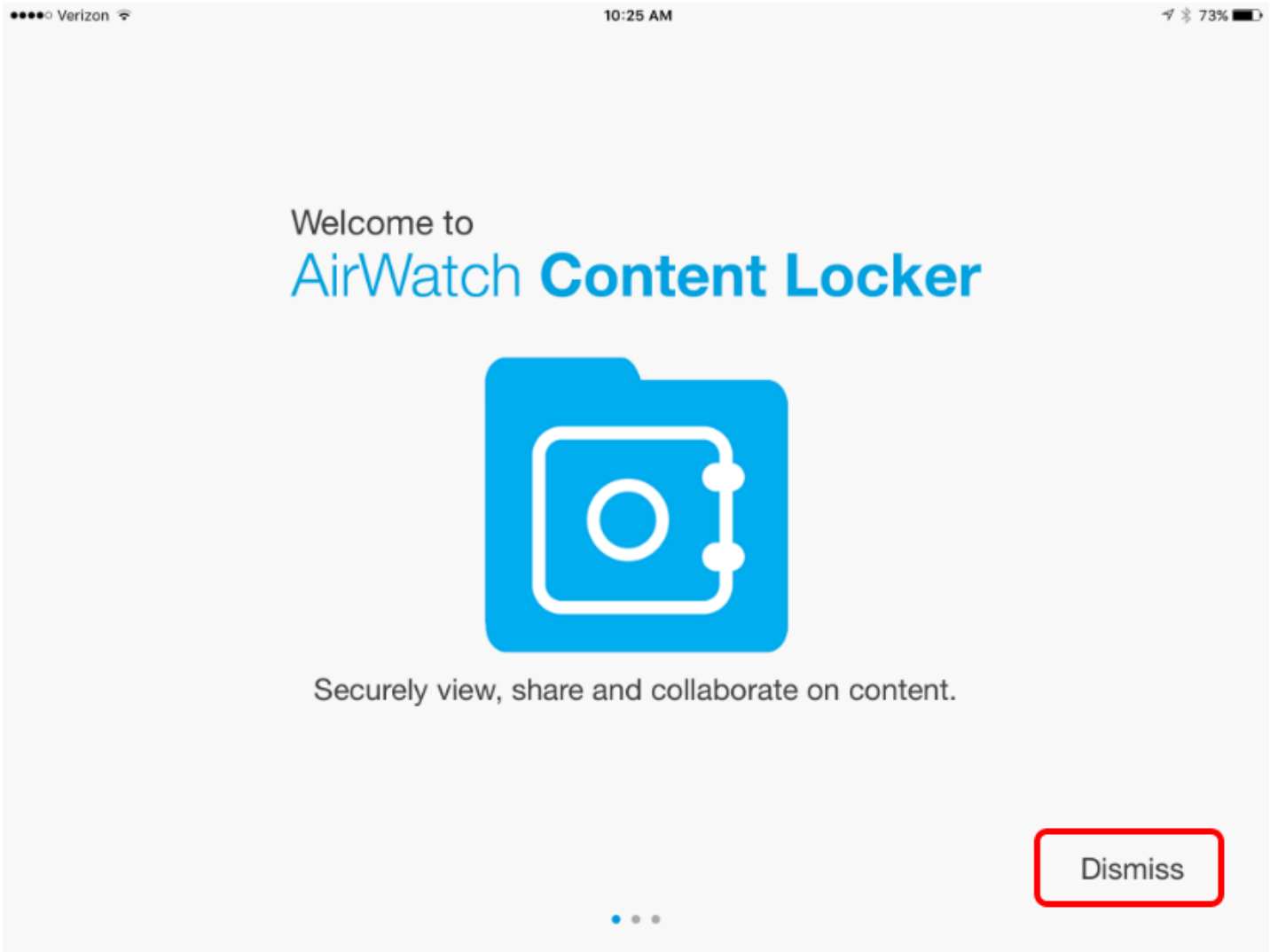
Lastly, let us view the Content Locker Branding changes.

Open the Content Locker Application



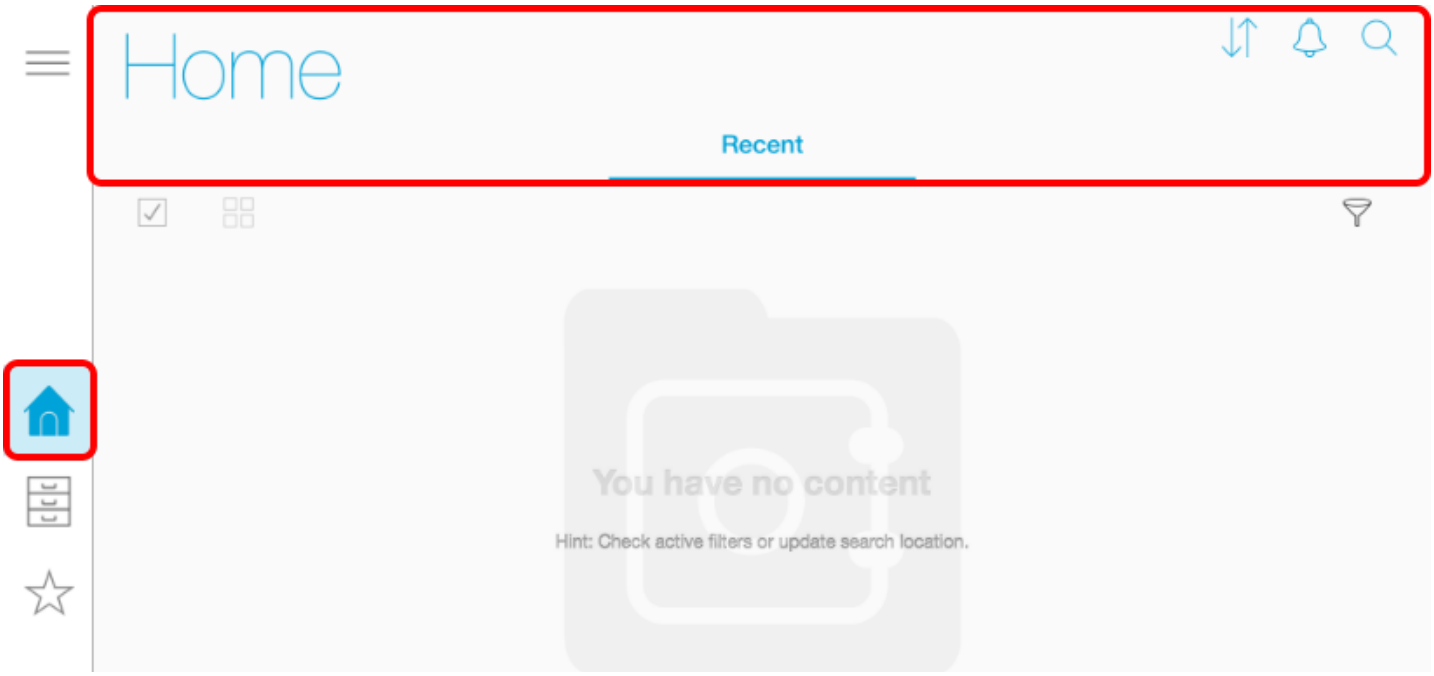
Tab the **Content Locker** app.

Dismiss Tutorial Prompts (Optional)



If prompted with the Tutorial, tap **Dismiss** to continue.

View the VMware Content Locker Branding



Notice that the Primary Color and Primary Text Color we set previously are applying to the assets here.

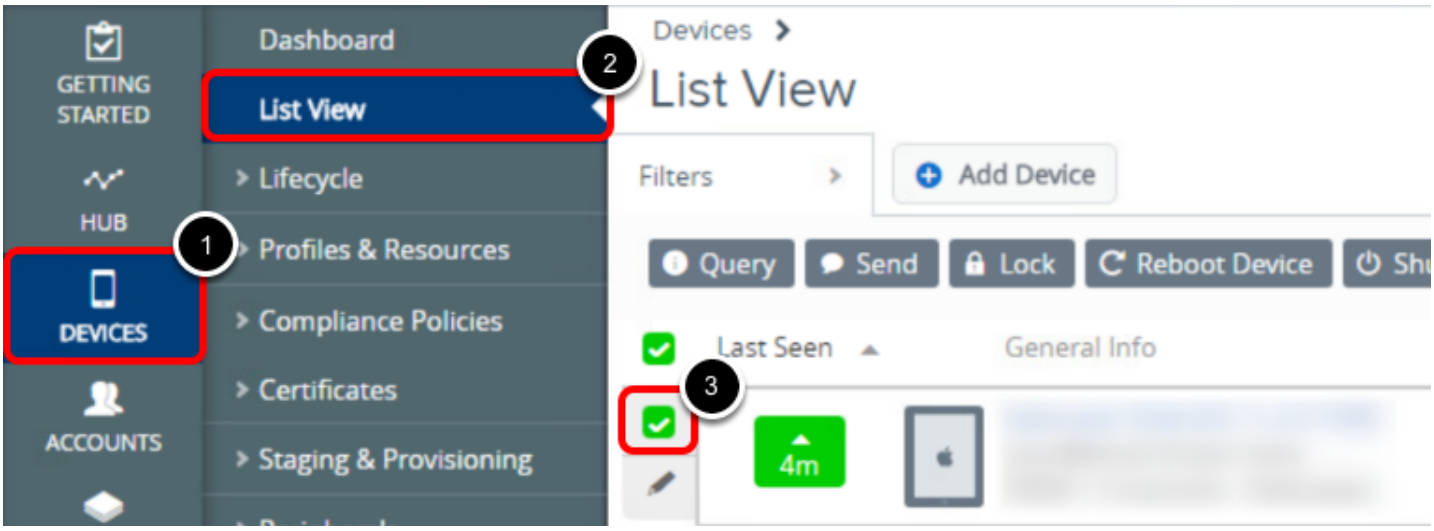
Un-enrolling Your Device

You are now going to un-enroll the iOS device from AirWatch.

NOTE - The term "Enterprise Wipe" does not mean reset or completely wipe your device. This only removes the MDM Profiles, Policies, and content which the AirWatch MDM Agent controls.

It will NOT remove the AirWatch MDM Agent application from the device as this was downloaded manually before AirWatch had control of the device.

Enterprise Wipe (un-enroll) your iOS device



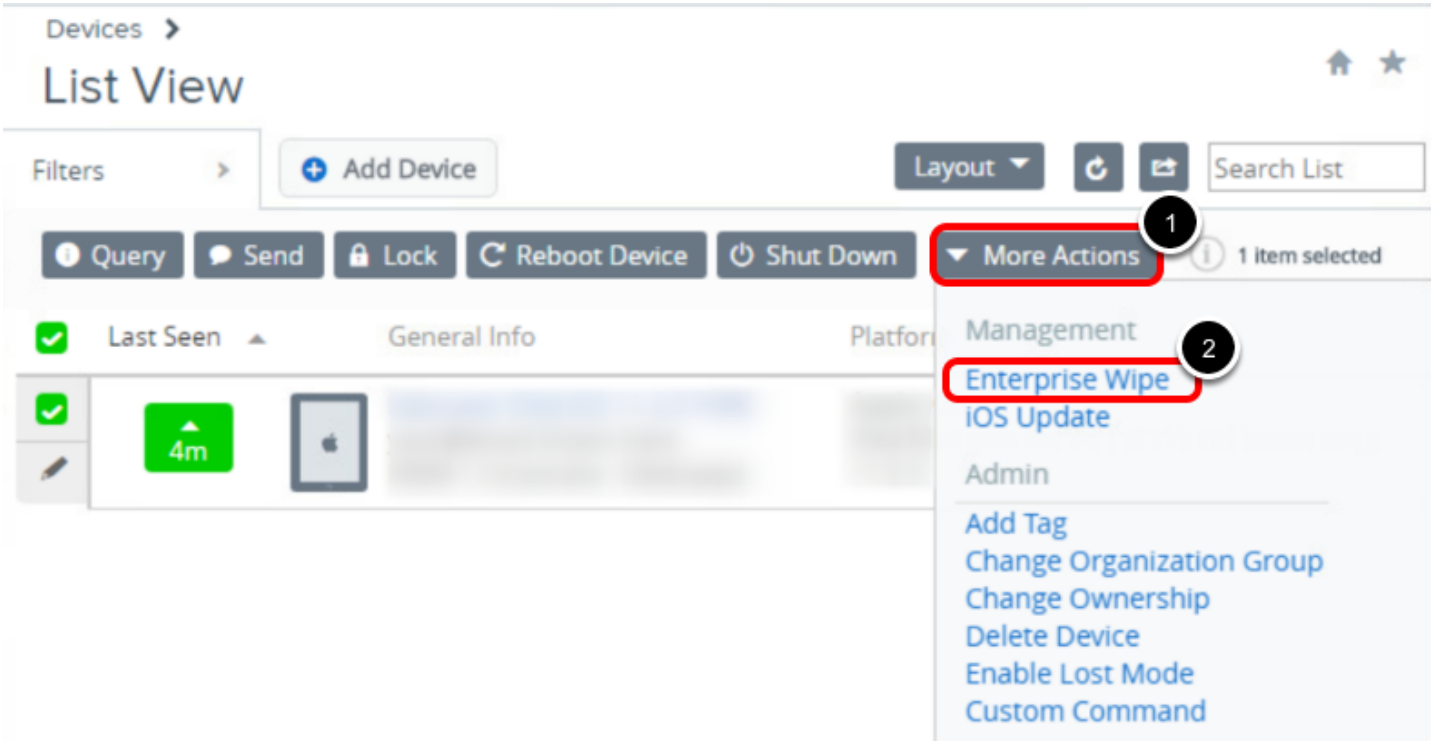
Enterprise Wipe will remove all the settings and content that were pushed to the device when it was enrolled. It will not affect anything that was on the device prior to enrollment.

To Enterprise Wipe your device you will first bring up the AirWatch Console in a web browser. You may need to re-authenticate with your credentials (VLP registered email address and "VMware1!" as the password).

1. Click **Devices** on the left column.
2. Click **List View**.
3. Click the **checkbox** next to the device you want to Enterprise Wipe.

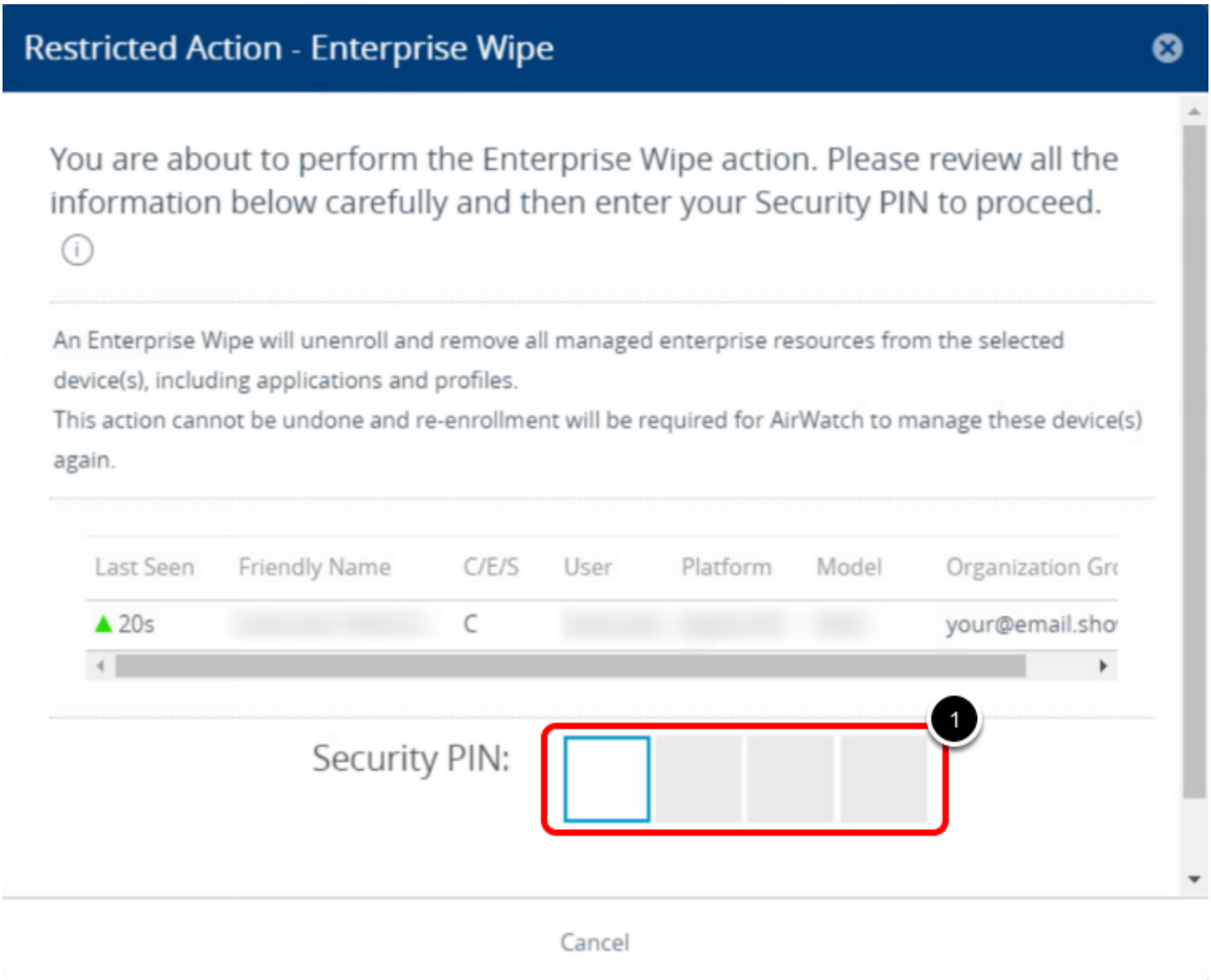
NOTE - Your Device Friendly Name will very likely be different than what is shown. It will, however, be in the same location as shown on image in this step.

Find the Enterprise Wipe Option



1. Click **More Actions**. ***NOTE - If you do not see this option, ensure you have a device selected by clicking the checkbox next to the device.***
2. Click **Enterprise Wipe** under **Management**.

Enter your security PIN



After selecting **Enterprise Wipe**, you will be prompted to enter your Security PIN which you set after your logged into the console (**"1234"**).

1. Enter **"1234"** for the **Security PIN**. You will not need to press enter or continue, the console will confirm your PIN showing "Successful" below the Security PIN input field to indicate that an Enterprise Wipe has been requested. ***NOTE:*** If **"1234"** does not work, then you provided a different Security PIN when you first logged into the AirWatch Console. Use the value you specified for your Security PIN.

NOTE - If the Enterprise Wipe does not immediately occur, follow the below steps to force a device sync:

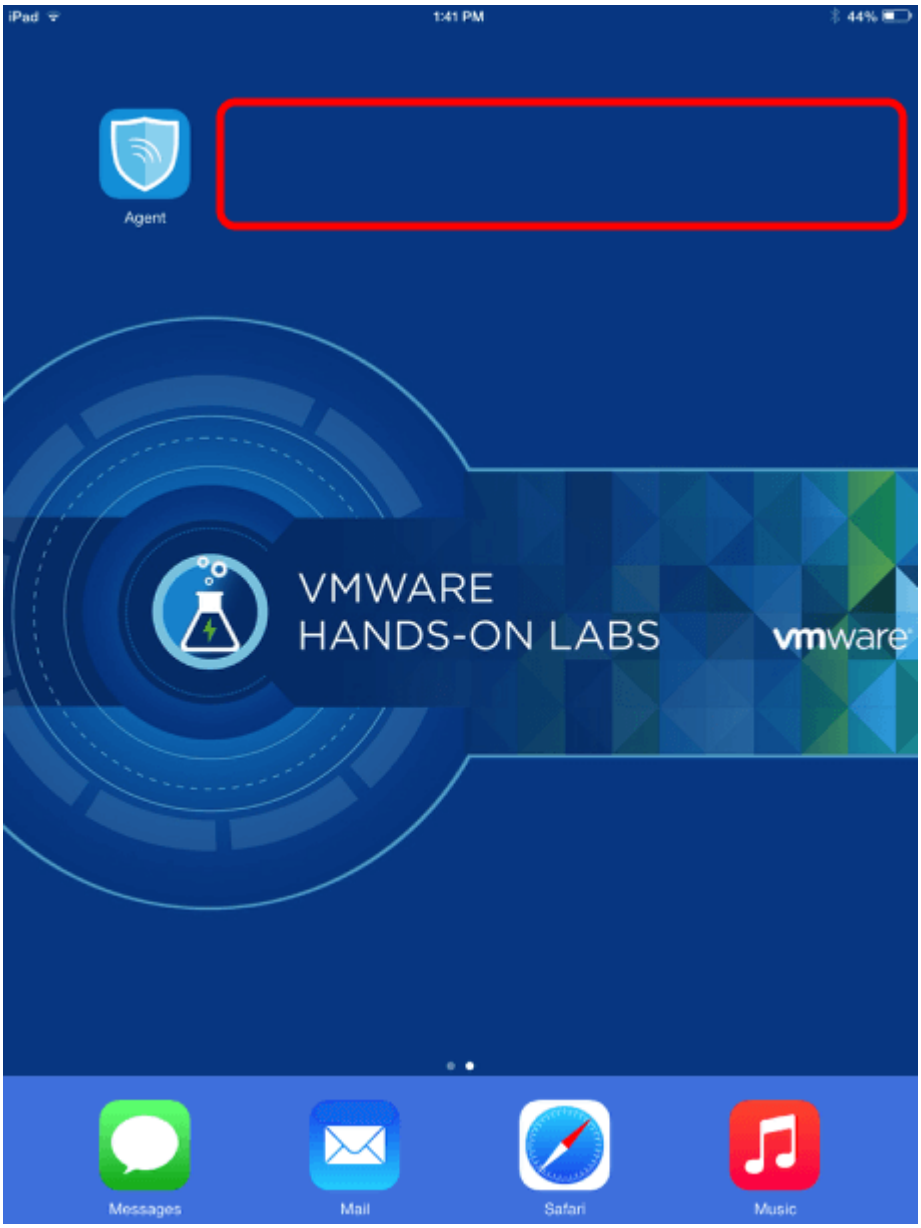
1. On your device, open the **AirWatch Agent** application.

2. Tap the **Device** section (under **Status**) in the middle of the screen.
3. Tap **Send Data** near the top of the screen. If this does not make the device check in and immediately un-enroll, continue to Step #4.
4. If the above doesn't make it immediately un-enroll, then tap **Connectivity [Status]** under Diagnostics.
5. Tap **Test Connectivity** at the top of the screen.

NOTE - Depending upon Internet connectivity of the device and responsiveness of the lab infrastructure, this could take a couple of minutes or more if there is excessive traffic occurring within the Hands On Lab environment.

Feel free to continue to the **"Force the Wipe"** step to manually uninstall the AirWatch services from the device if network connectivity is failing.

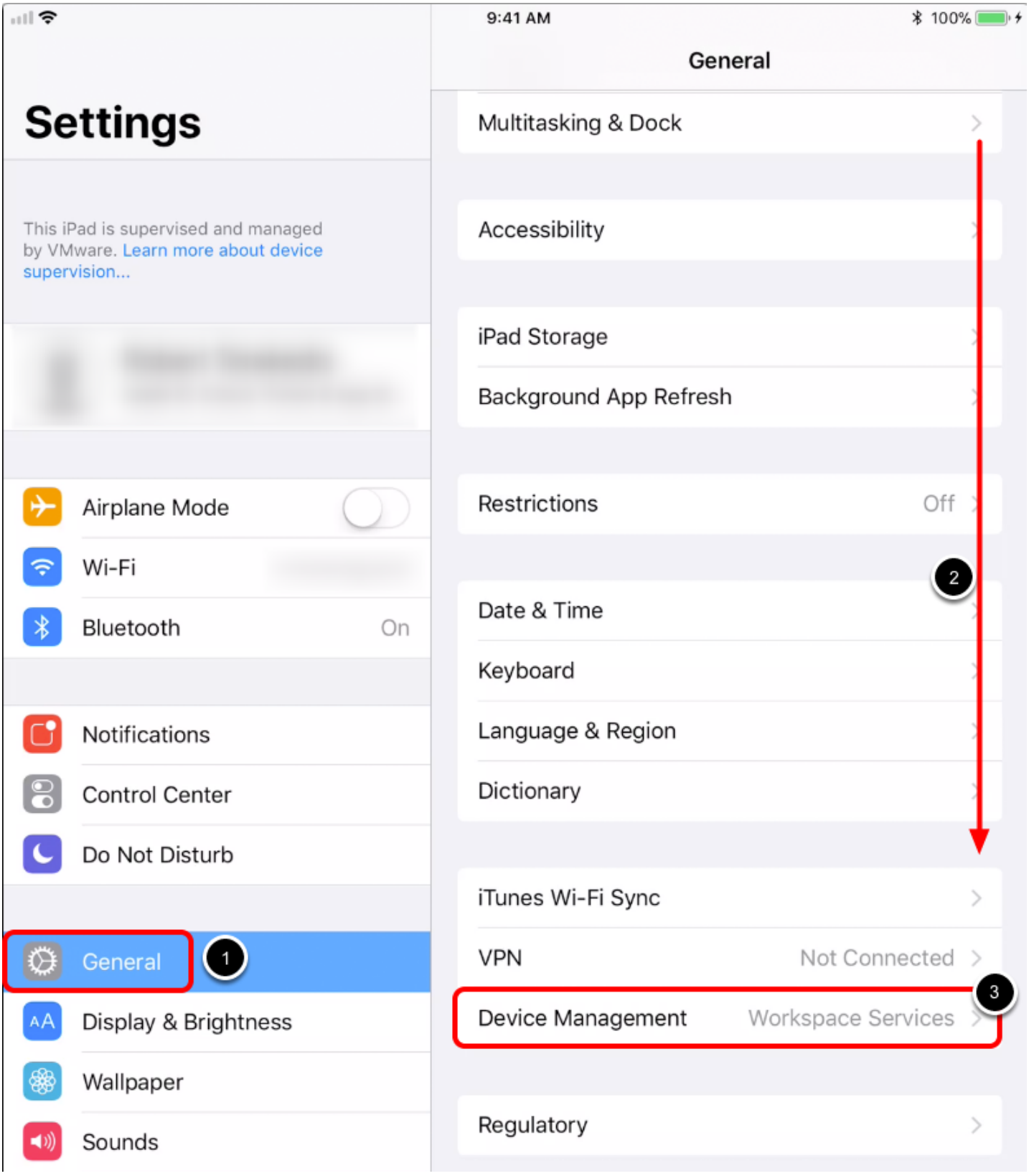
Verify the Un-Enrollment



Press the Home button on the device to go back to the home screen. The applications pushed through AirWatch should have been removed from the device.

NOTE - The applications and settings pushed through AirWatch management should have been removed. The Agent will still be on the device because that was downloaded manually from the App Store. Due to lab environment settings, it may take some time for the signal to traverse through the various networks out and back to your device. Continue on to the next step to force the wipe if the needed.

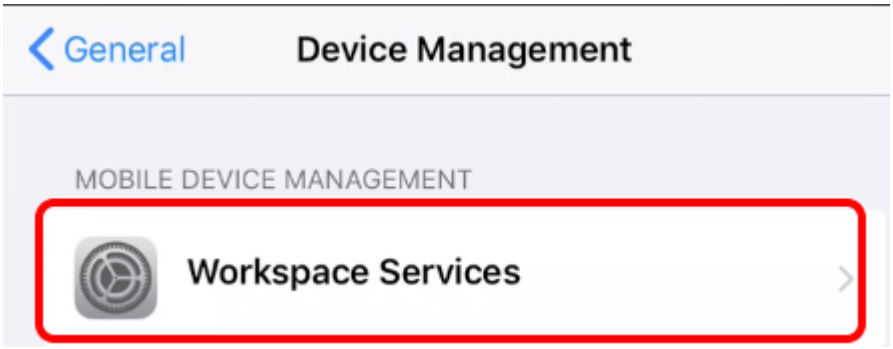
Force the Wipe - IF NECESSARY



If your device did not wipe, follow these instructions to ensure the wipe is forced immediately. Start by opening the iOS **Settings** app.

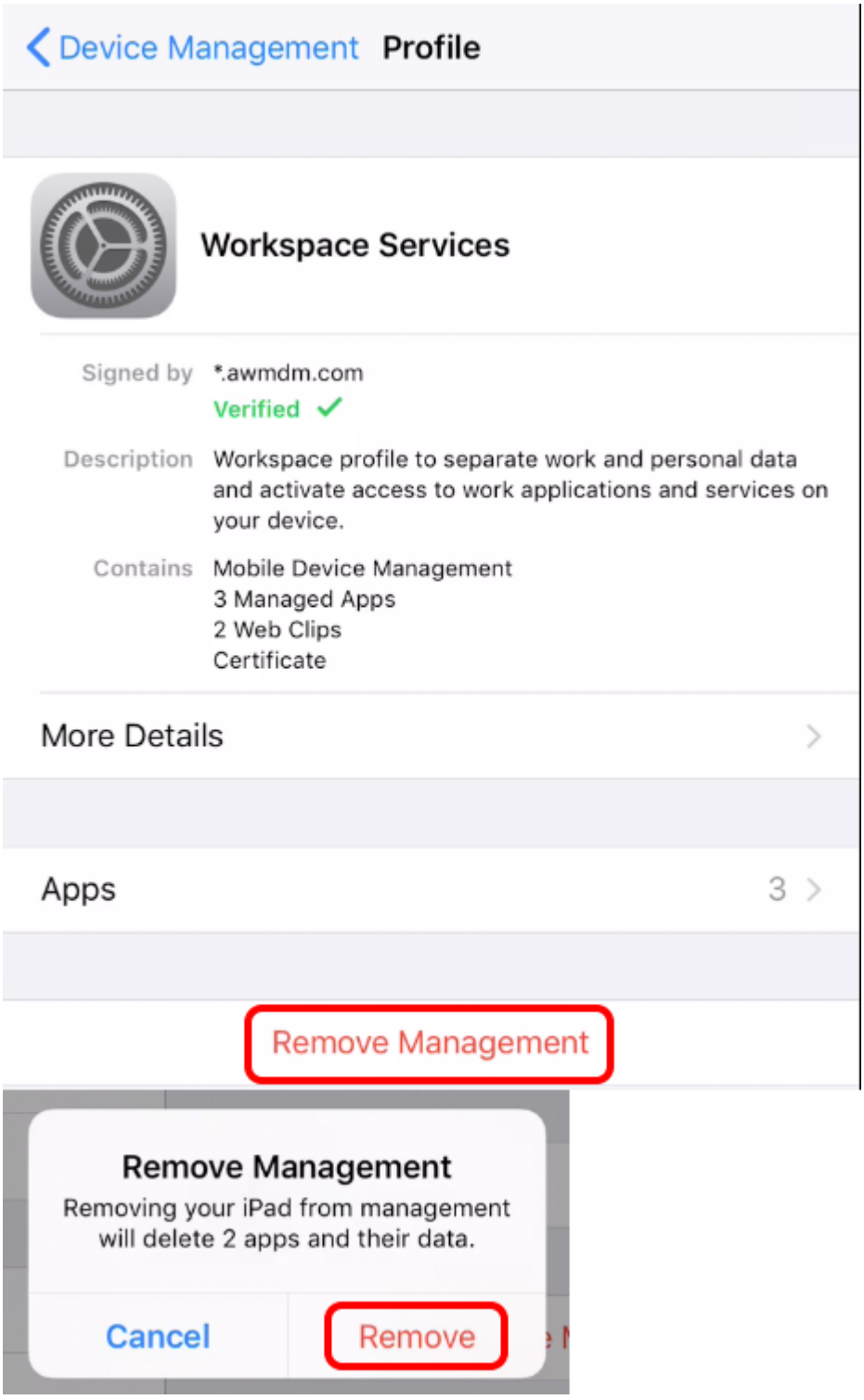
1. Tap **General** in the left column.
2. Scroll down to view the **Device Management** option.
3. Tap **Device Management** at the bottom of the list of General settings.

Force the Wipe - IF NECESSARY



Tap the **Workspace Services** profile that was pushed to the device.

Force the Wipe - IF NECESSARY



1. Tap **Remove Management** on the Workspace Services profile.
   NOTE - If prompted for a device PIN, enter it to continue. VMware provisioned devices should not have a device PIN enabled.
2. Tap **Remove** on the Remove Management prompt.

After removing the Workspace Services profile, the device will be un-enrolled. Feel free to return to the **"Verify the Un-Enrollment"** step to confirm the successful un-enrollment of the device.

Conclusion

Branding your AirWatch Console, Self Service Portal, and applications you distribute to devices can help unify the look and feel of your environment to match your company brand. This allows a more personal experience for your administrators and users from start to finish and can be a powerful tool to assist in user adoption. Explore ideas around how you can leverage your brand within AirWatch for your administrators and users.

This concludes the Branding the AirWatch Console, SSP and SCL module.

Conclusion

Thank you for participating in the VMware Hands-on Labs. Be sure to visit http://hol.vmware.com/ to continue your lab experience online.

Lab SKU: HOL-1857-01-UEM

Version: 20180430-190404