HOL-2451-09-DWS (NEW)

Getting Started with the Digital Workspace

vmware®

Table of contents

Module 2 - Introduction to Apple iOS Management (30 minutes) Beginner

Introduction [134]

This lab module will focus on introducing the concepts of Unified Endpoint Management (UEM) with Workspace ONE. This lab will walk you through how to enroll an iOS device and deploy device profiles to configure your iOS devices to leverage UEM functionality.

DO NOT Enroll Personal iOS Devices [135]

IMPORTANT: You SHOULD NOT enroll a personal device for the upcoming exercise!

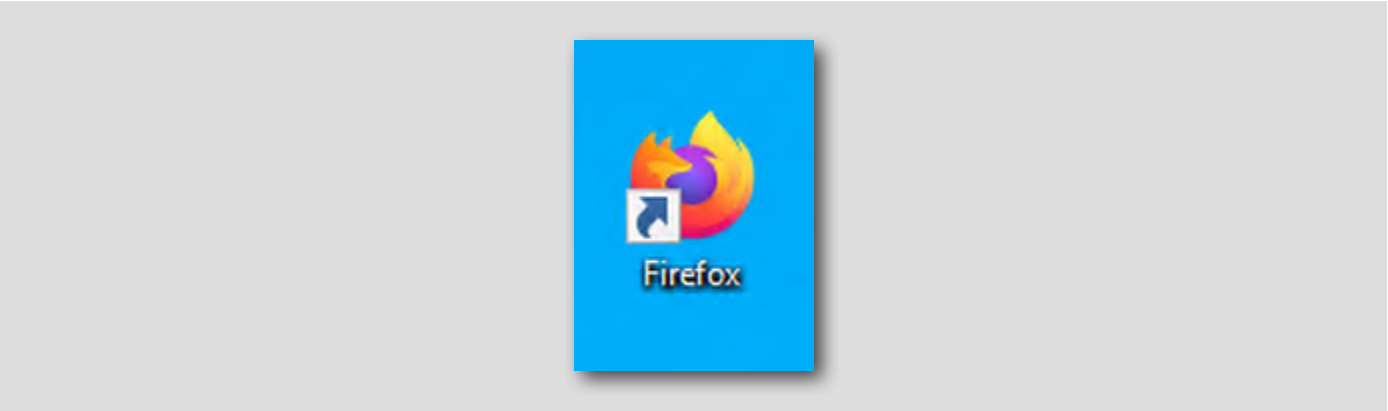
Personal devices may be enrolled into other UEM providers which can cause undesired conflicts and issues.

To complete this lab, we recommend you use a test device ONLY and avoid enrolling personal devices in the lab.

Login to the Workspace ONE UEM Console [136]

To perform most of the lab, you will log into the Workspace ONE UEM Admin Console.

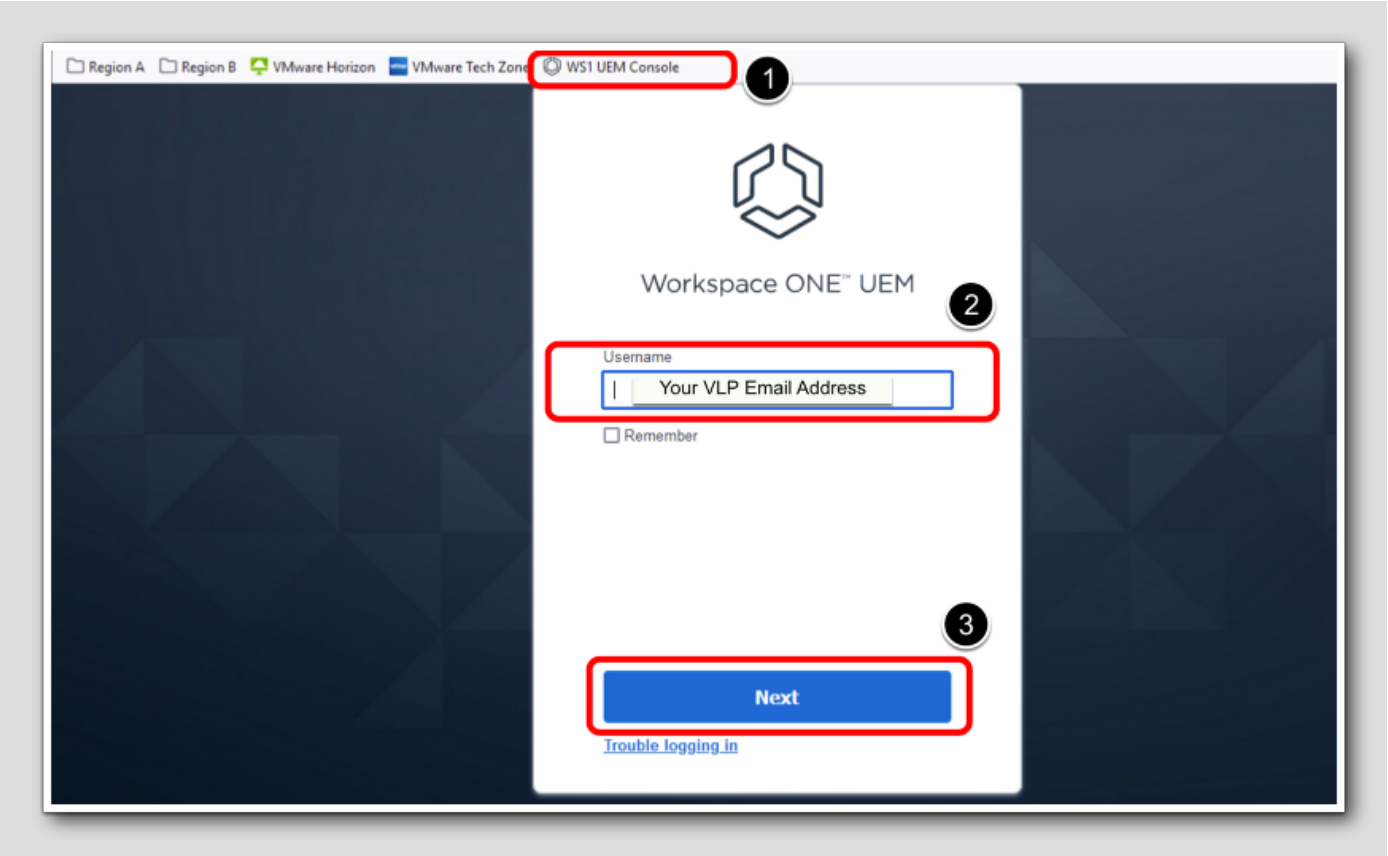
Launch Firefox Browser [137]



Double-click the **Firefox** shortcut located on the desktop of the virtual machine you are currently connected to.

Enter the Admin Username for the Workspace ONE UEM Admin Console

[138]

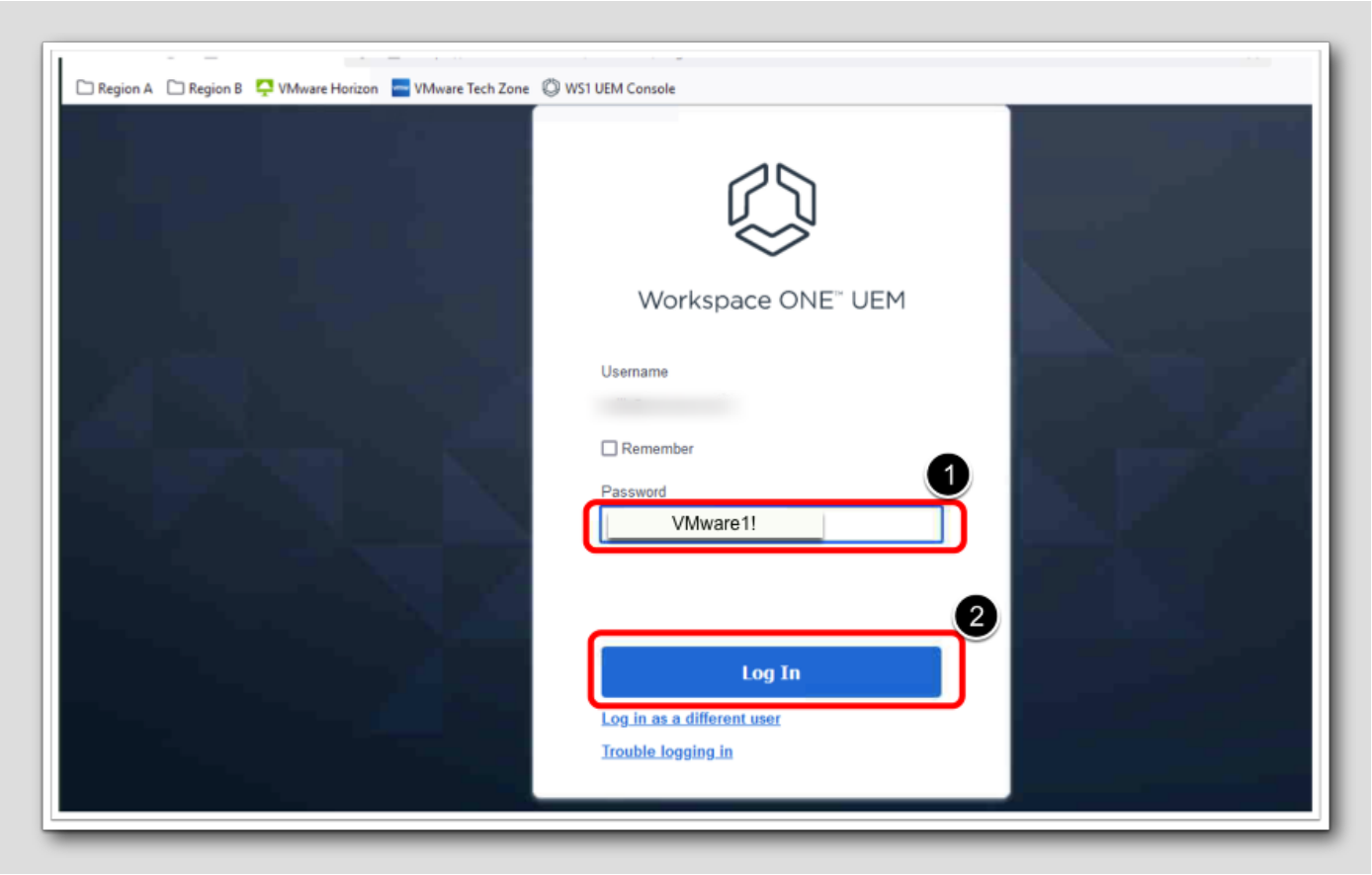


1. Select the **WS1 UEM Console** link from the Bookmark Toolbar
2. Enter your **Username**. This is the **email address** that you have associated with your **VMware Learning Platform (VLP)**account that you utilized to take Hands-on Labs.
3. Click **Next**, then advance to the next step of the lab manual to enter the password.

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

Authenticate to the Workspace ONE UEM Console

[139]



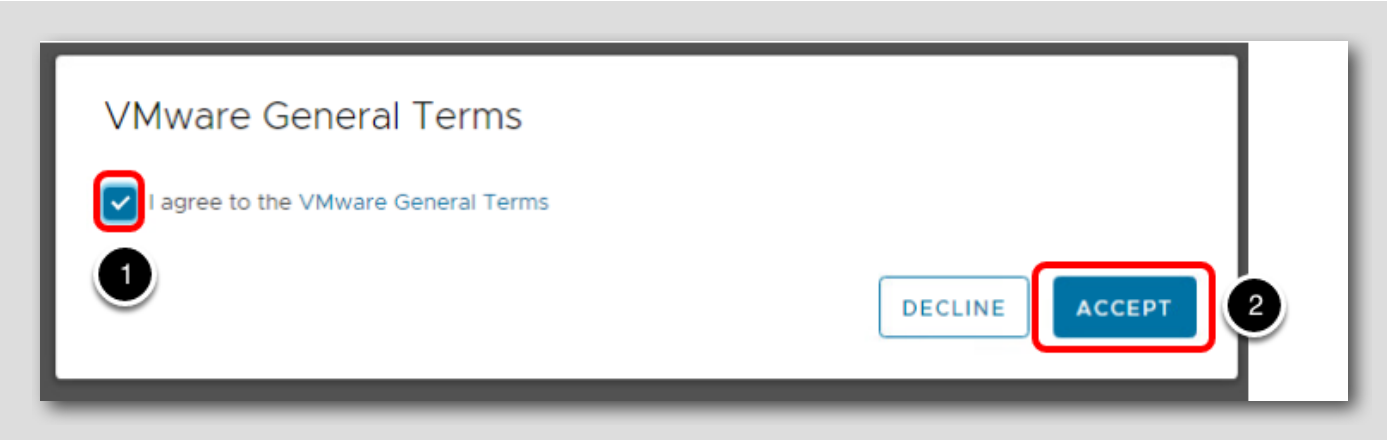
The password field will be displayed after entering your username.

1. Enter **VMware1!** for the Password field.
2. Click the Log In button.

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

Accept the VMware General Terms

[140]



You will be presented with the VMware General Terms.

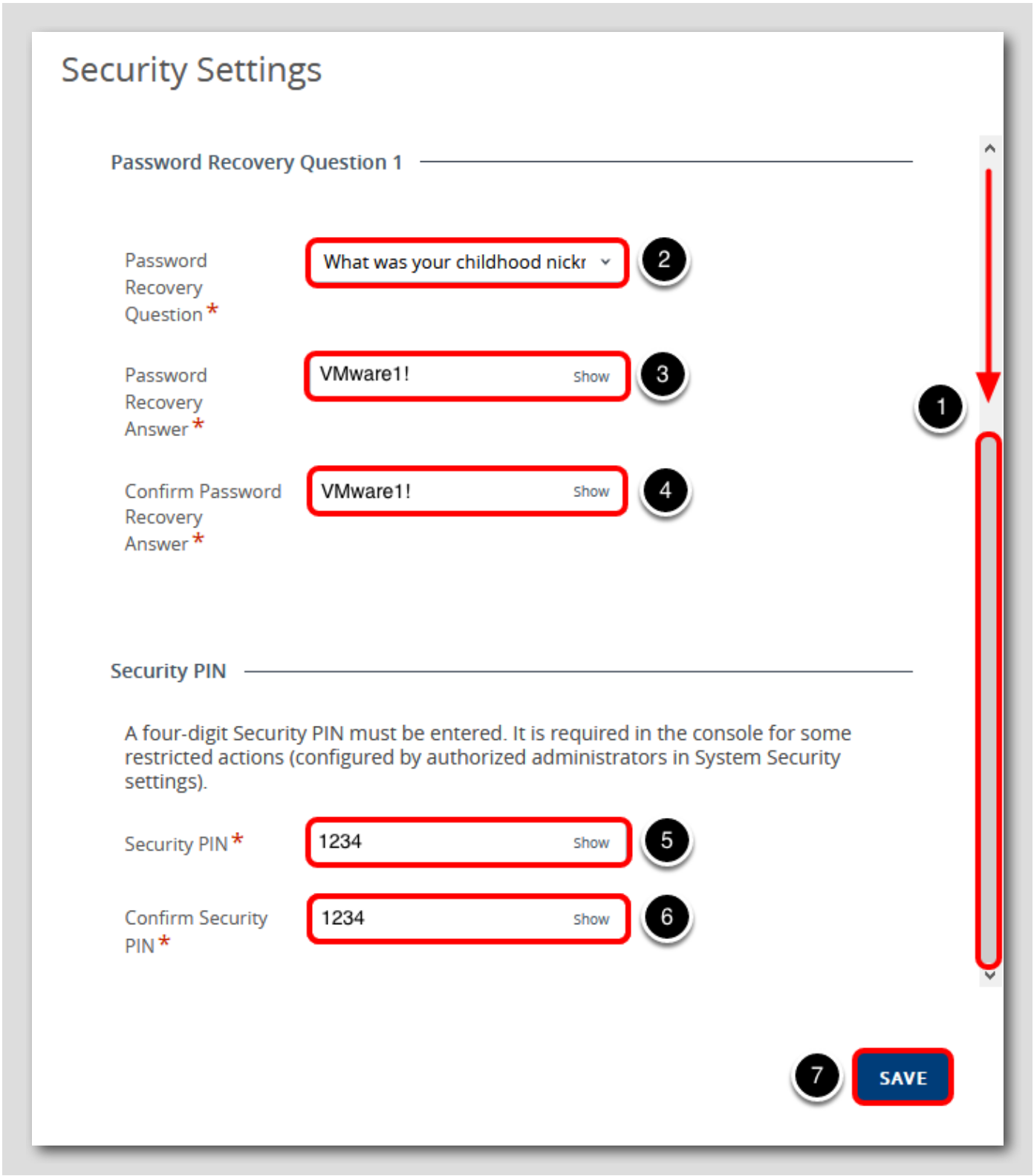
1. Select the box next to I Agree to the VMware General Terms.
2. Click the **Accept** button.

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

Address the Initial Security Settings

[141]

After accepting the Terms of Use, you will be presented with this **Security Settings** pop-up

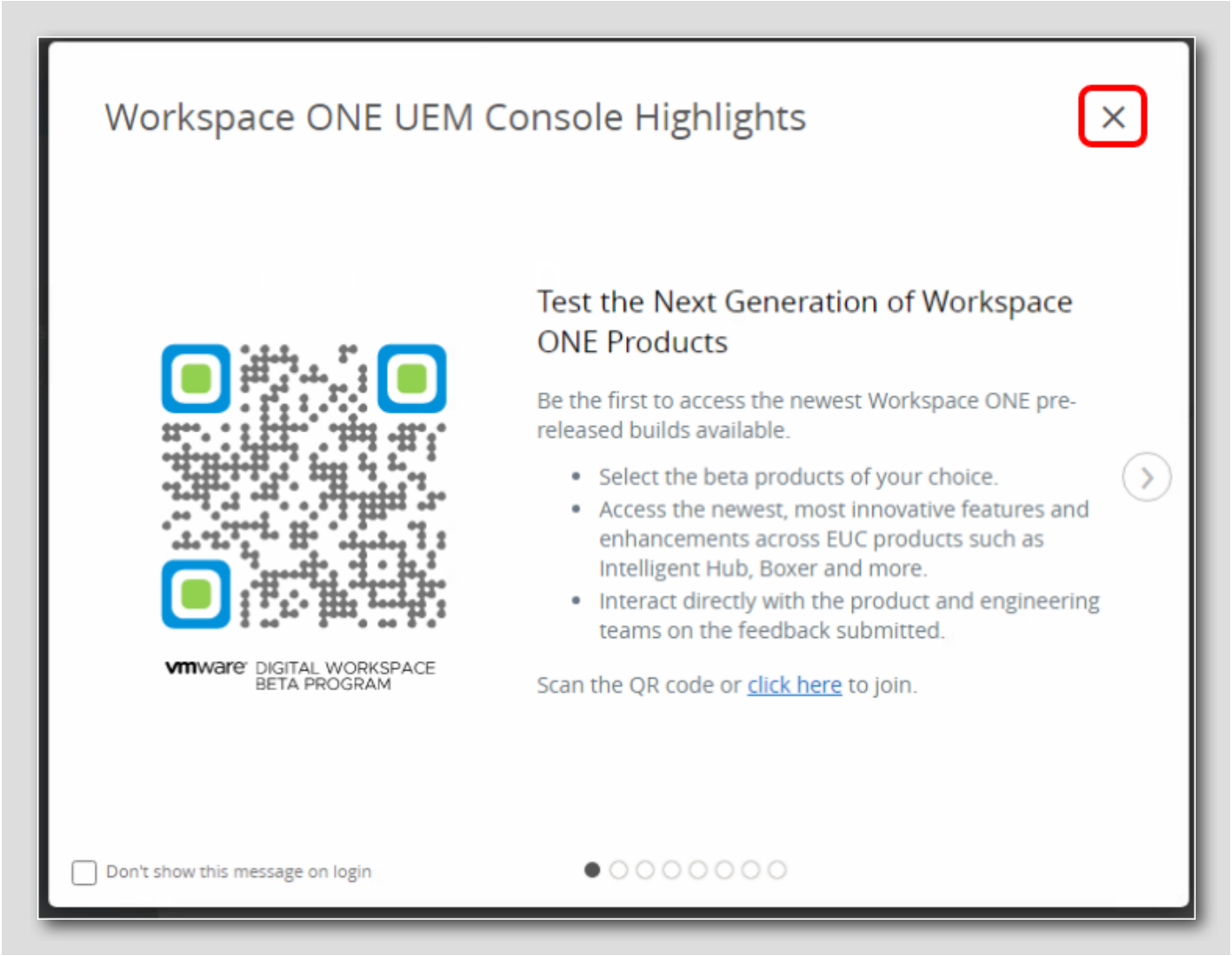

Security Settings
Password Recovery Question 1
Password Recovery Question *
What was your childhood nickr
2
Password Recovery Answer *
VMware1!
Show
3
1
Confirm Password Recovery Answer *
VMware1!
Show
4
Security PIN
A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).
Security PIN *
1234
Show
5
Confirm Security PIN *
1234
Show
6
7
SAVE

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.

Console Highlights

[142]



A popup window will appear after you complete your security questions.

Click the 'X' in the upper right corner to close the **Workspace ONE UEM Console Highlights** window.

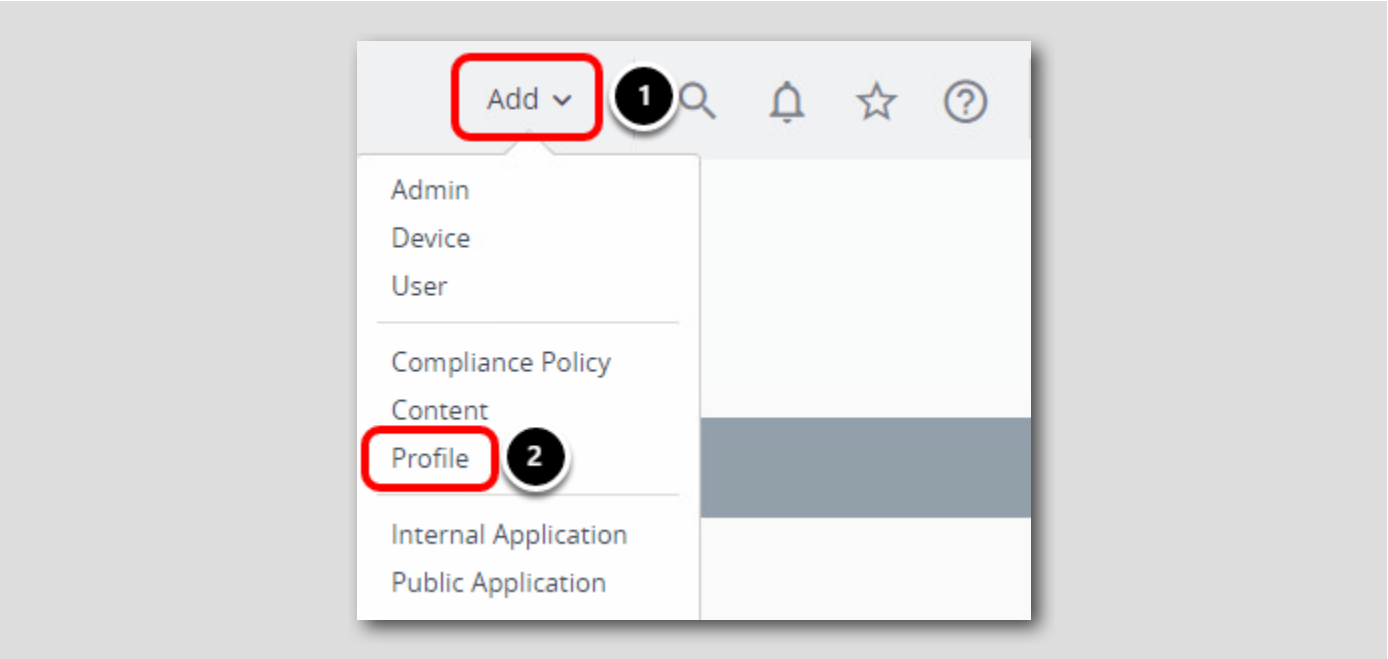
Create a Device Restriction Profile

[143]

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

Add A Profile

[144]

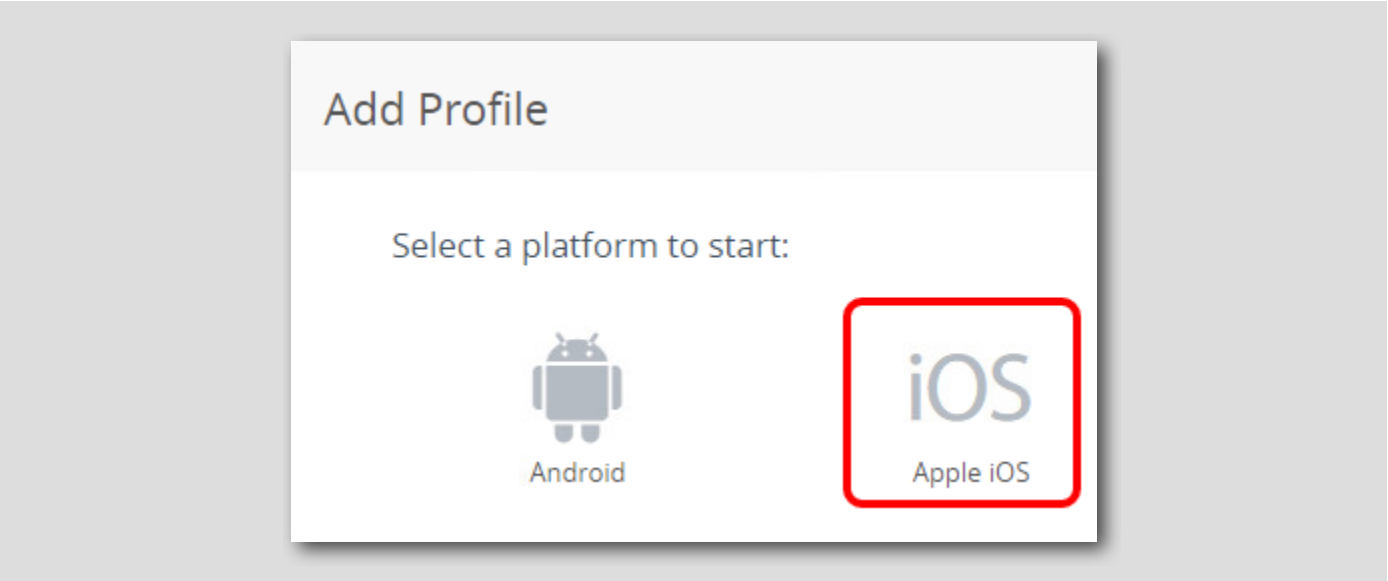


In the top right corner of the Workspace ONE UEM console,

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

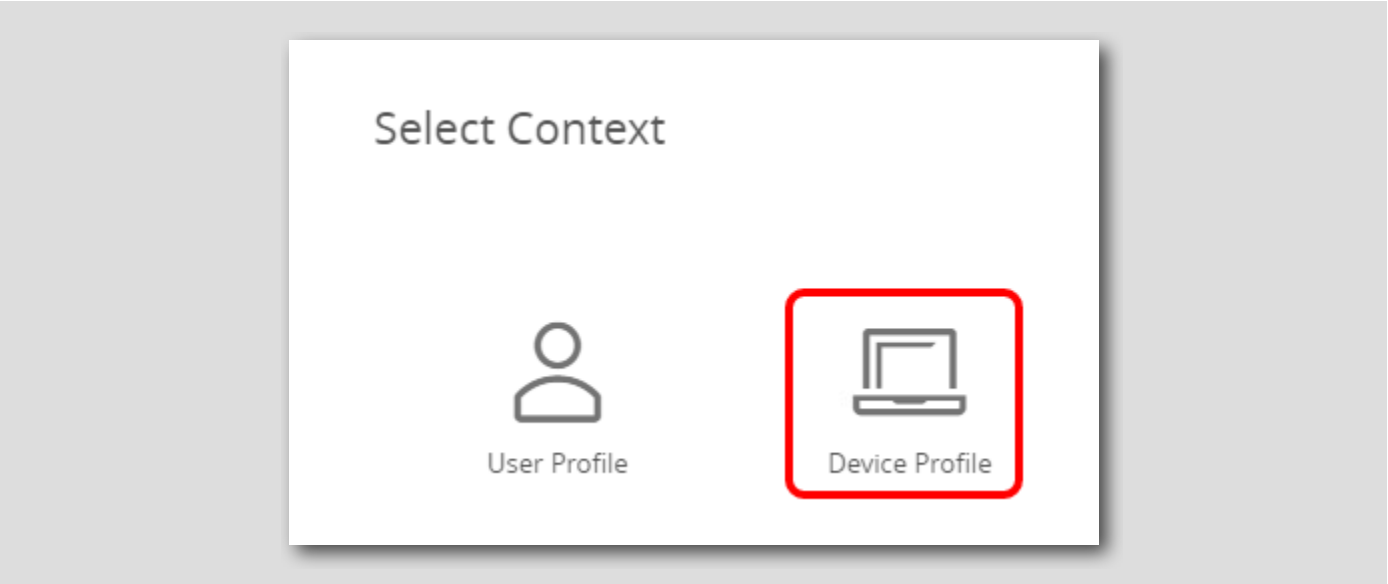
Select Platform

[145]



Select the Context

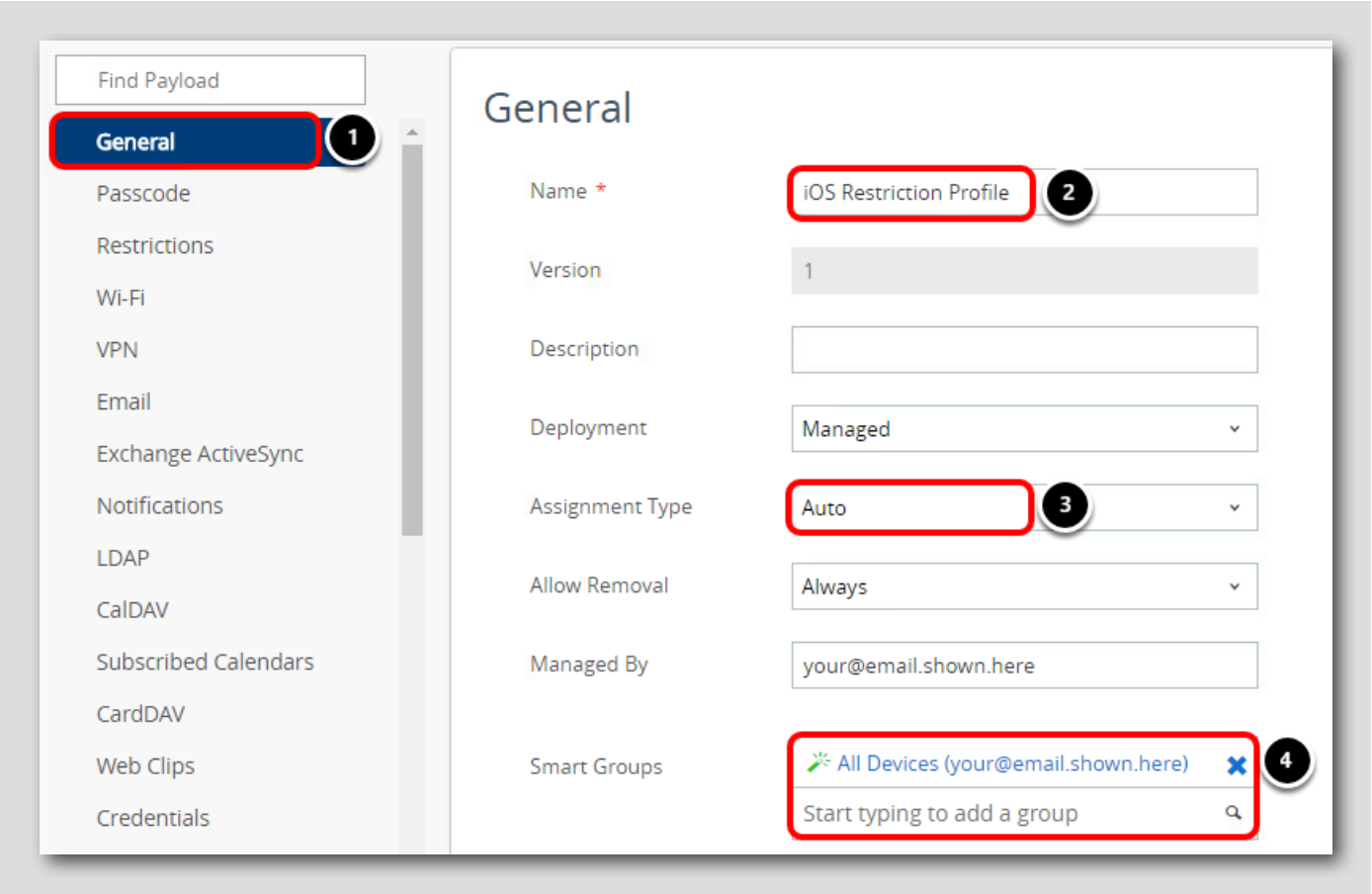
[146]



Click the **Device Profile** context option.

Configure General Payload

[147]



1. Select **General** if not selected already
2. Enter **`iOS Restriction Profile`** for the Name field
3. Ensure the Assignment Type is **Auto**
4. Click the Smart Groups dropdown field and select **All Devices (your@email.shown.here)**

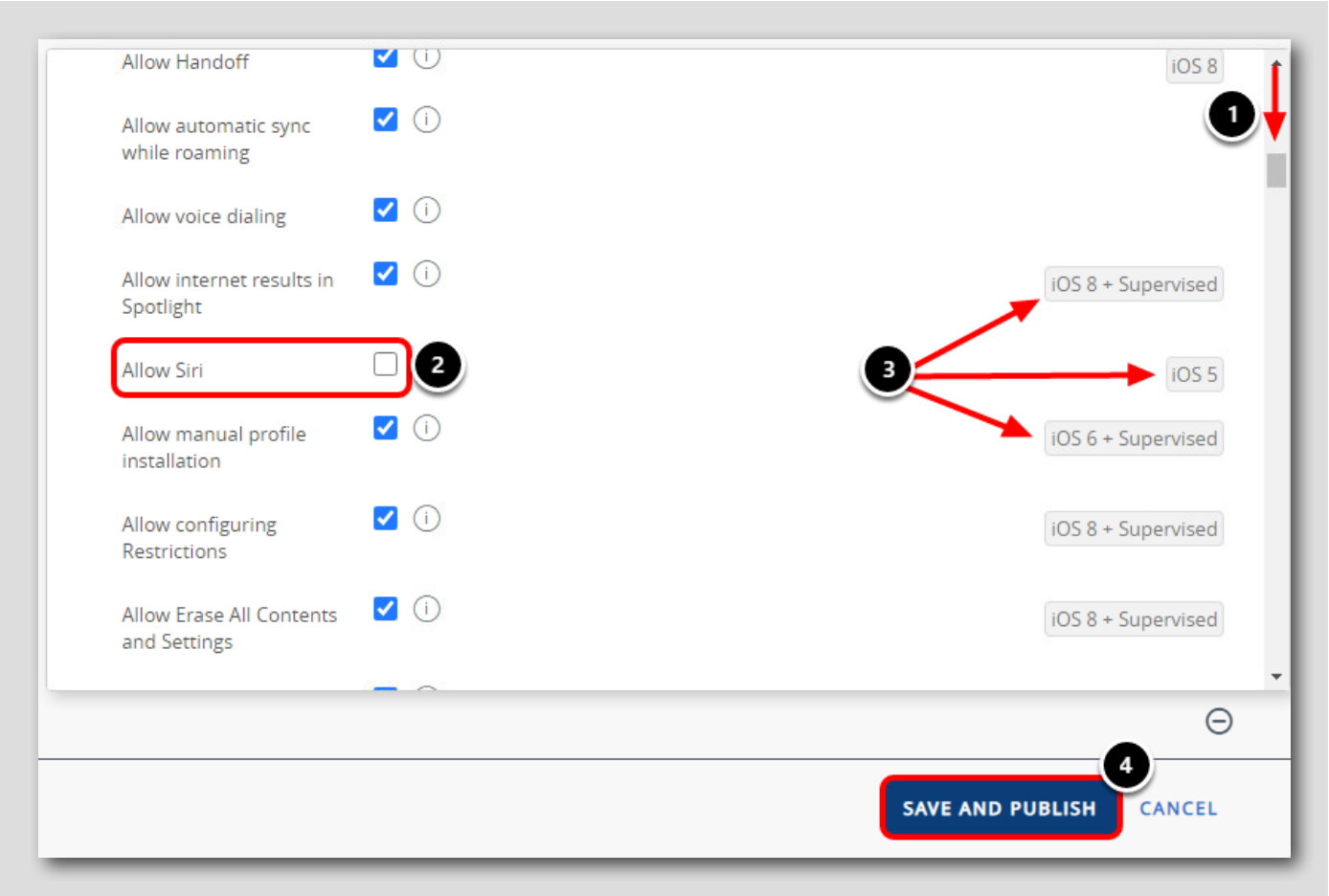
Configure Restriction Payload

[148]

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

Disable Siri

[149]

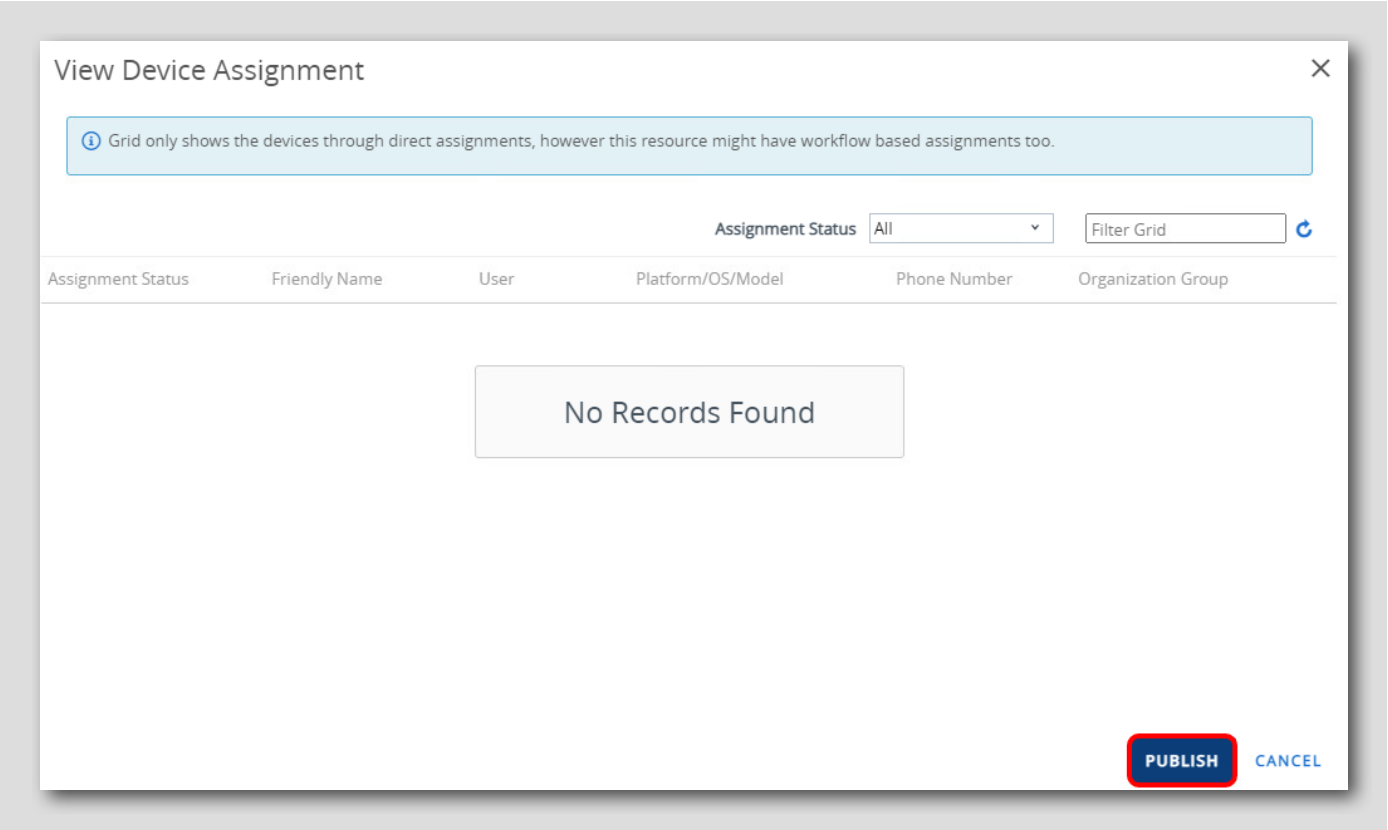


1. Scroll down approximately one page to find the **Allow Siri** option.
2. Uncheck the **Allow Siri** checkbox listed under the Device Functionality section. This will disable Siri on the device.
3. Take note of the **iOS version** and **Supervised** requirements for each restriction. The target device receiving this restriction must on the listed iOS version or higher (ie: iOS 5) and must be Supervised if the Supervised tag is also shown.
   For example: The Allow Siri restriction does not require the device to be Supervised, but the Allow Manual Profile Installation restriction does. Take note of these requirements and ensure your devices meet all of the requirements shown when publishing restriction profiles.
4. Click **Save & Publish**.

NOTE: Supervised devices give schools and business greater control over iOS device that they own. Supervising devices allows administrators additional device restrictions that are not possible with Bring Your Own Device (BYOD) scenarios to respect end user privacy.

Publish the Profile

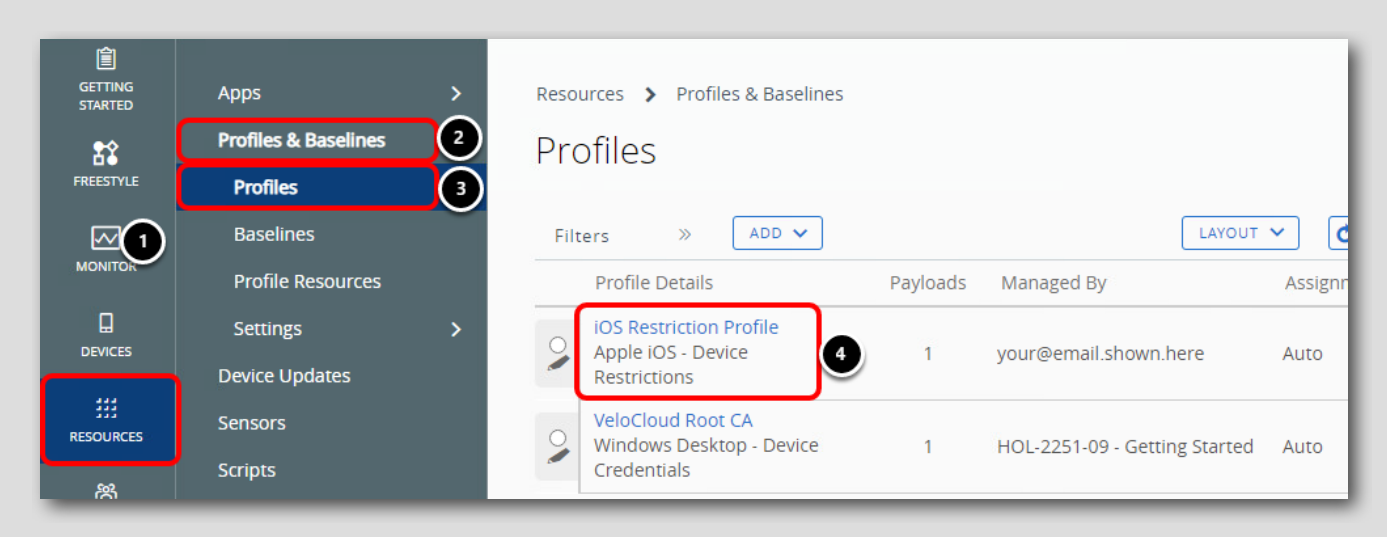
[150]



Click **Publish**.

Validate profile creation

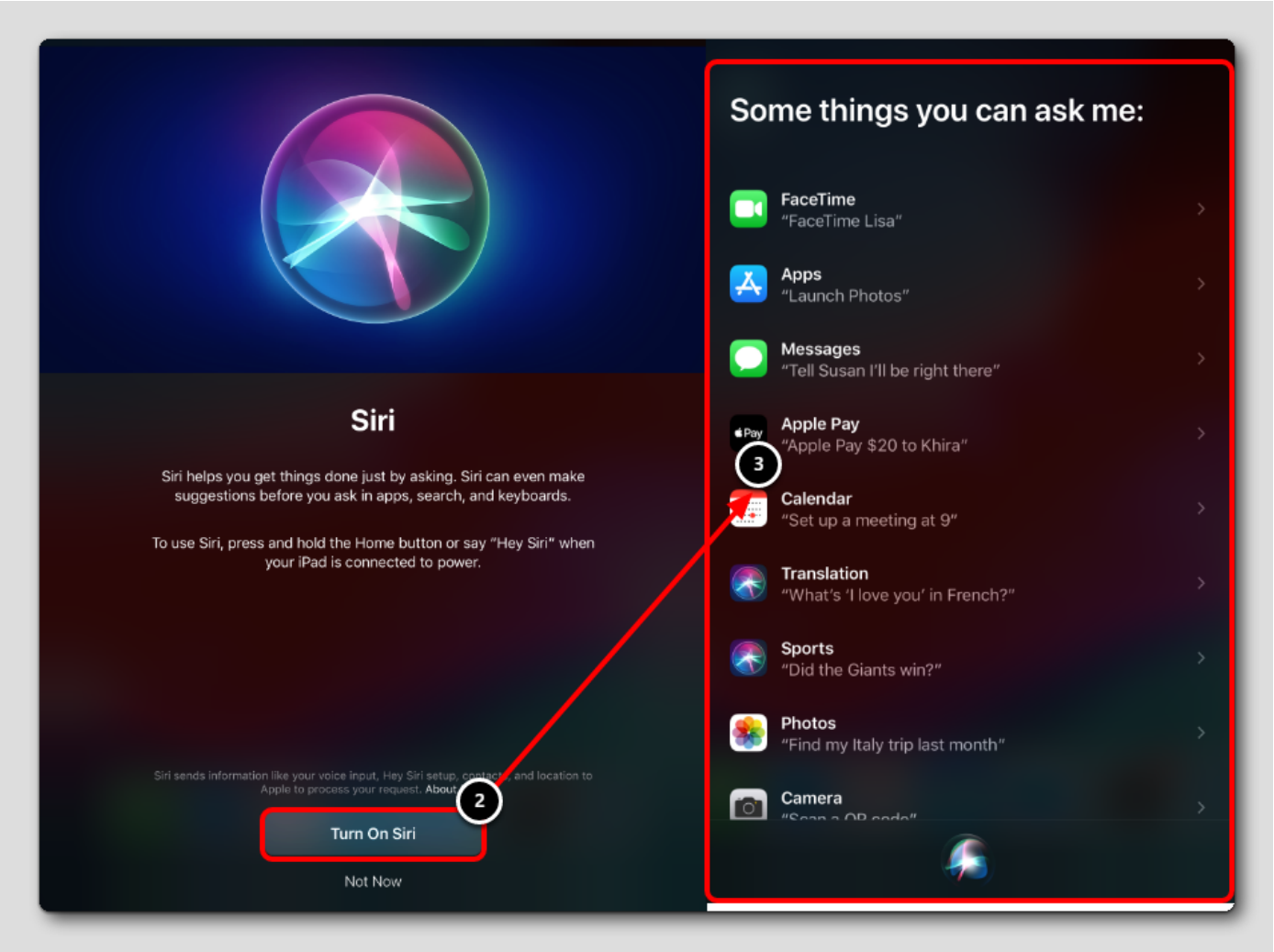
[151]



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

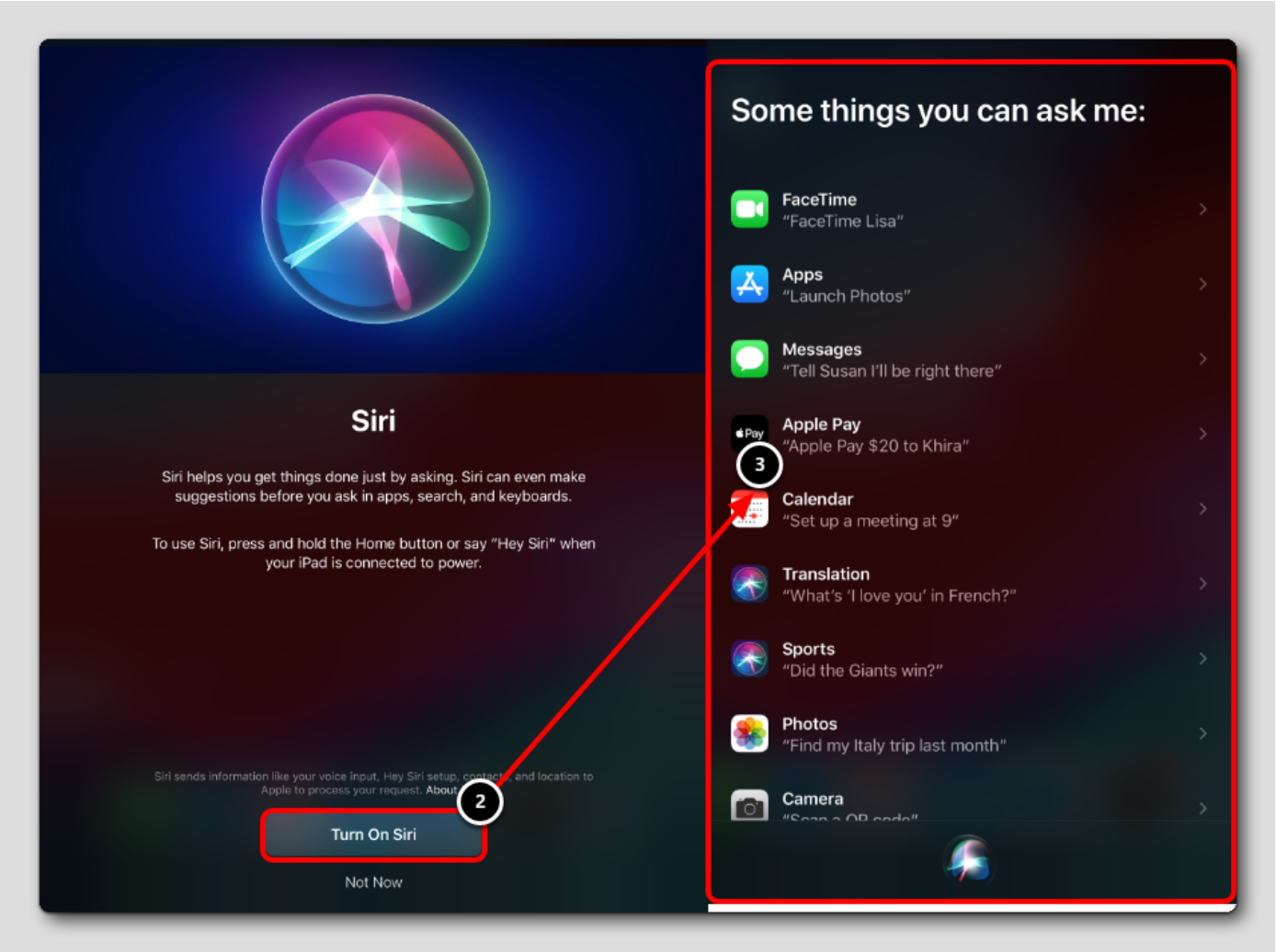
Validate Device Configuration Before Enrollment

[152]



Before enrolling your device, confirm that Siri is available for use on your iOS app so you can confirm that the iOS Restriction Profile properly disables Siri once the device is enrolled in an upcoming step.

1. Activate Siri on your device (holding the **Home** or **Side** button, depending on your device).
2. If Siri is disabled, tap **Turn On Siri**.
3. Ensure you see Siri is listening for input, confirming that Siri is enabled on the device.



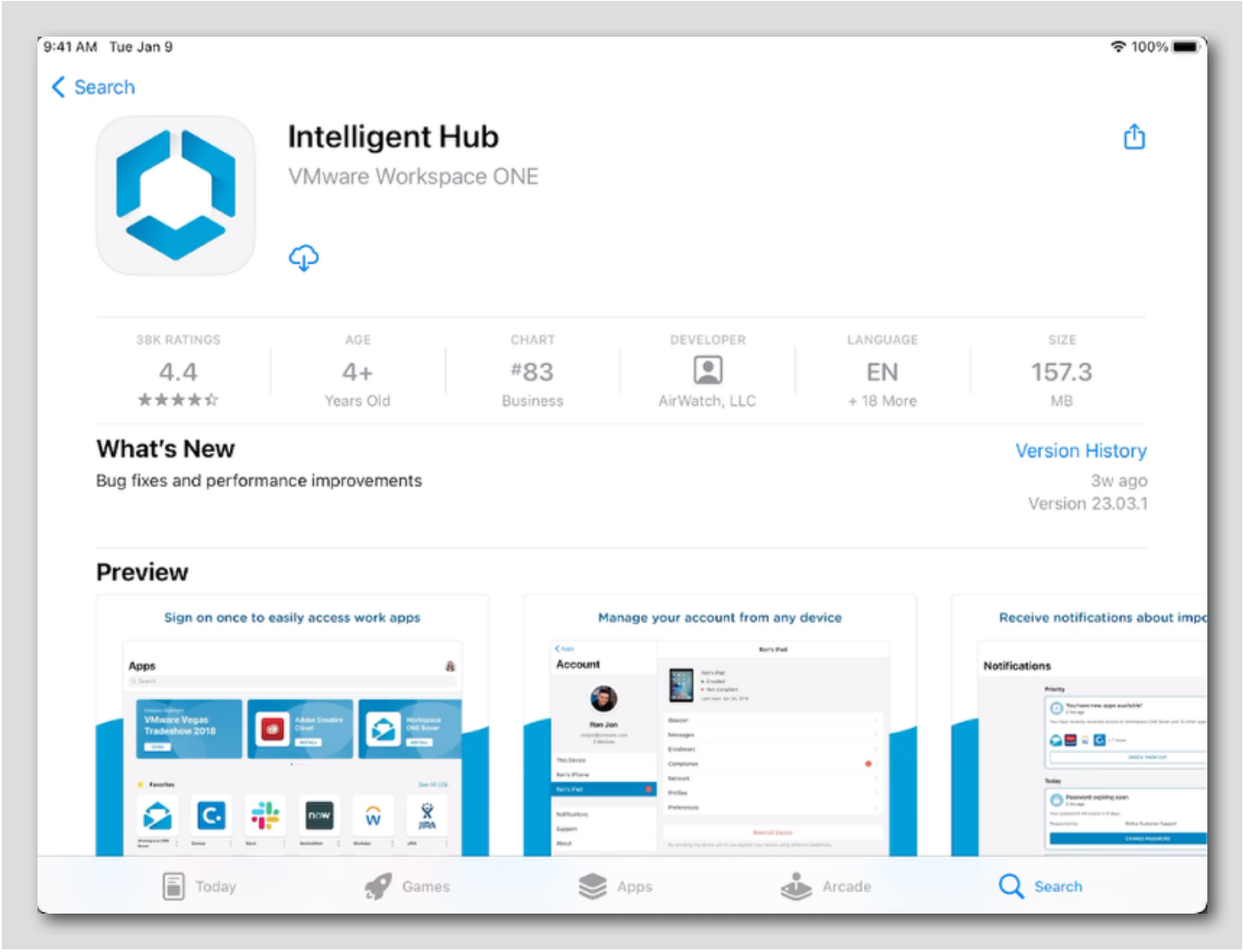
iOS Device Enrollment using testuser

[153]

In this section, we are going to enroll an iOS device. The upcoming steps will need to be completed from an iOS device.

Download and Install Workspace ONE Intelligent Hub from App Store (IF NEEDED)

[154]



NOTE: Checked out devices will likely have the Workspace ONE Intelligent Hub already installed. You may skip this step if your device has the Workspace ONE Intelligent Hub installed.

At this point, if you are using your own iOS device or if the device you are using does NOT have the Workspace ONE Intelligent Hub Application installed, then install the application from the App Store.

To Install the Workspace ONE Intelligent Hub application from the App Store, open the App Store application and download the free **Workspace ONE Intelligent Hub** application.

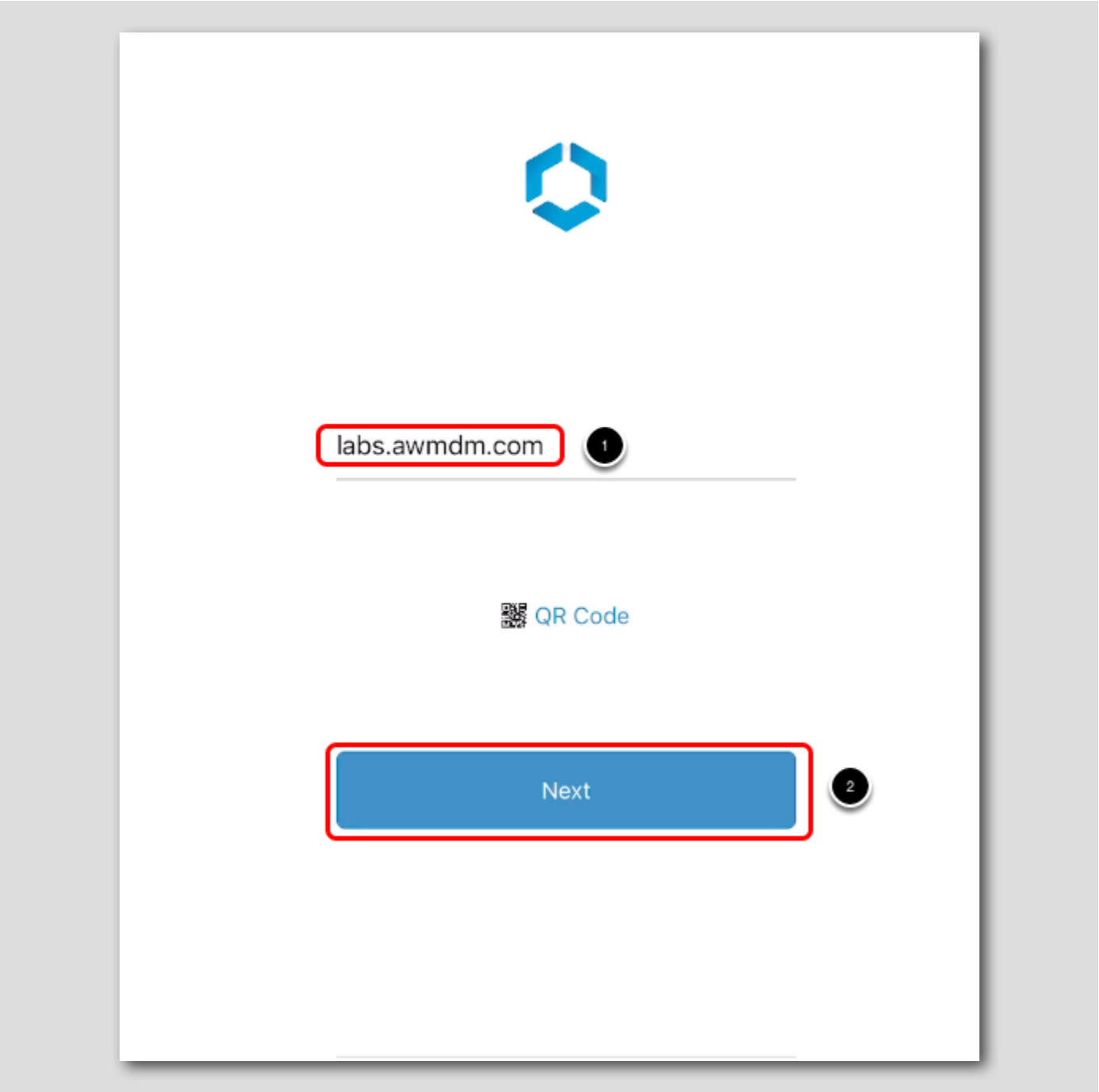
Launching the Workspace ONE Intelligent Hub

[155]

Launch the **Hub** app on the device.

NOTE: If you have your own iOS device and would like to test you will need to download the Workspace ONE Intelligent Hub app first.

Enter the Server URL [156]



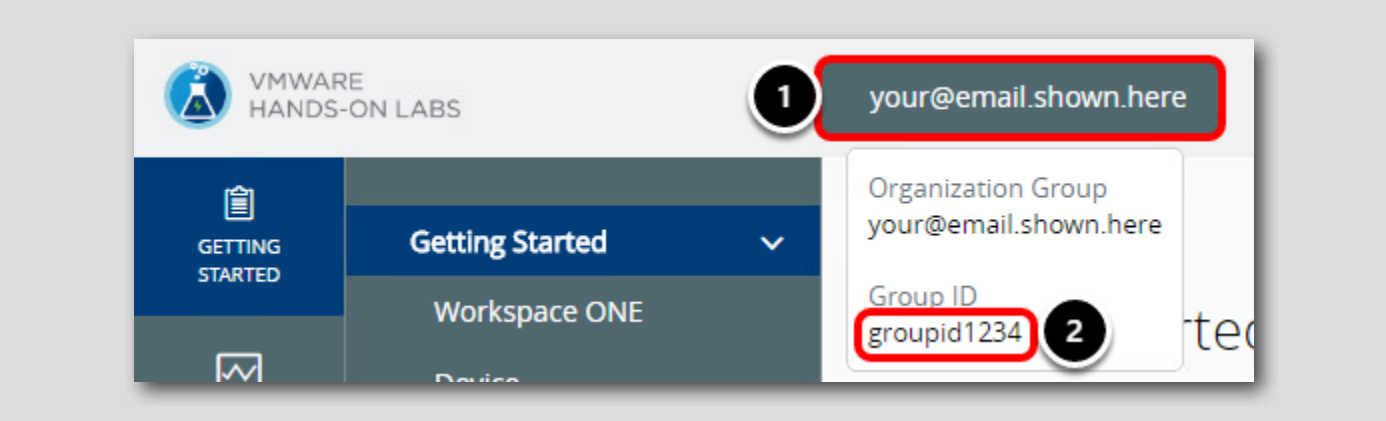
Once the Hub has launched you can enroll the device. To do so, follow the below steps.

1. Enter **`labs.awmdm.com`** for the **Server** field.
2. Tap the **Next** button.

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

Find your Group ID in the Workspace ONE UEM Console

[157]



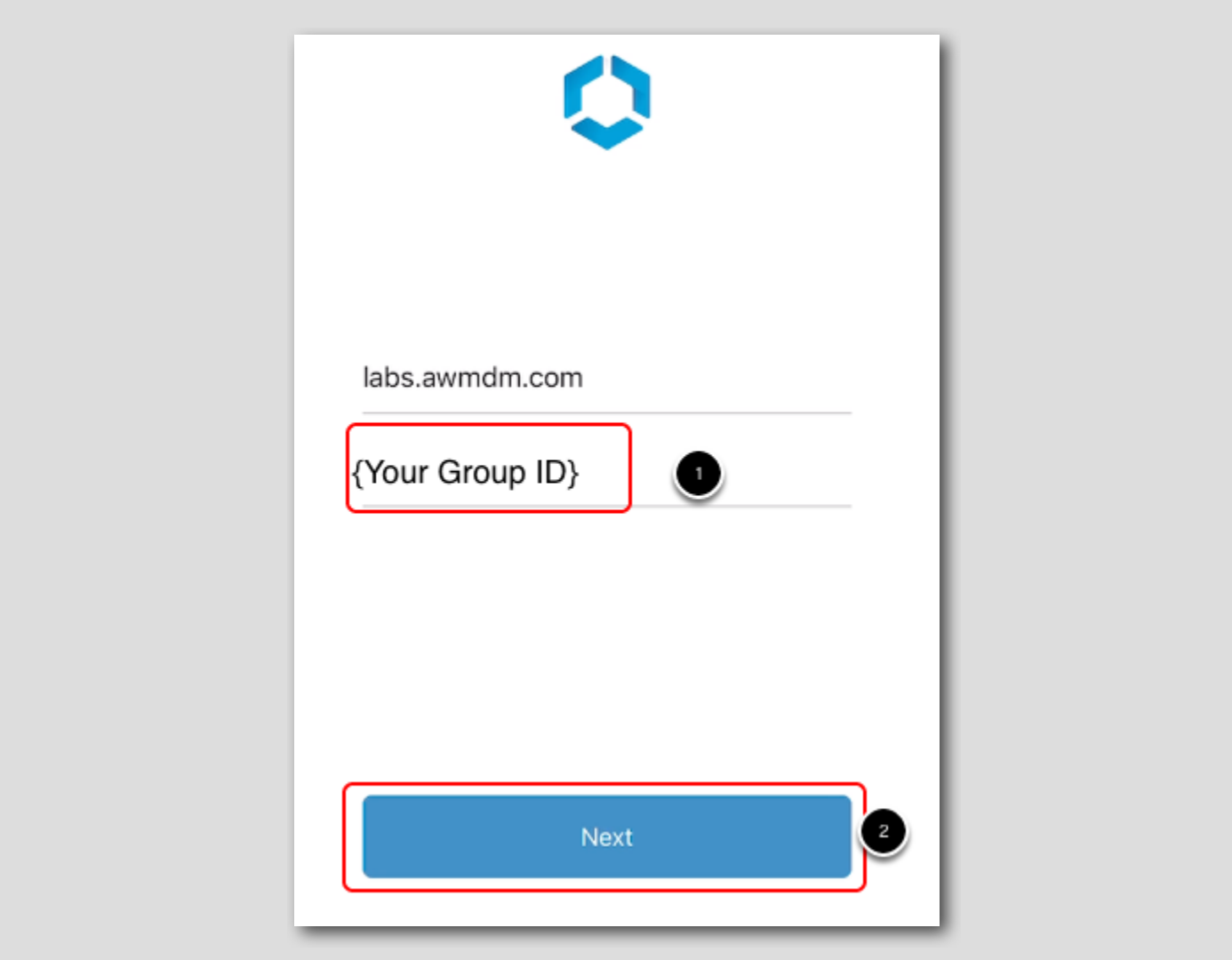
Return to the Workspace ONE UEM Console,

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 Workspace ONE Intelligent Hub to your Sandbox

[158]



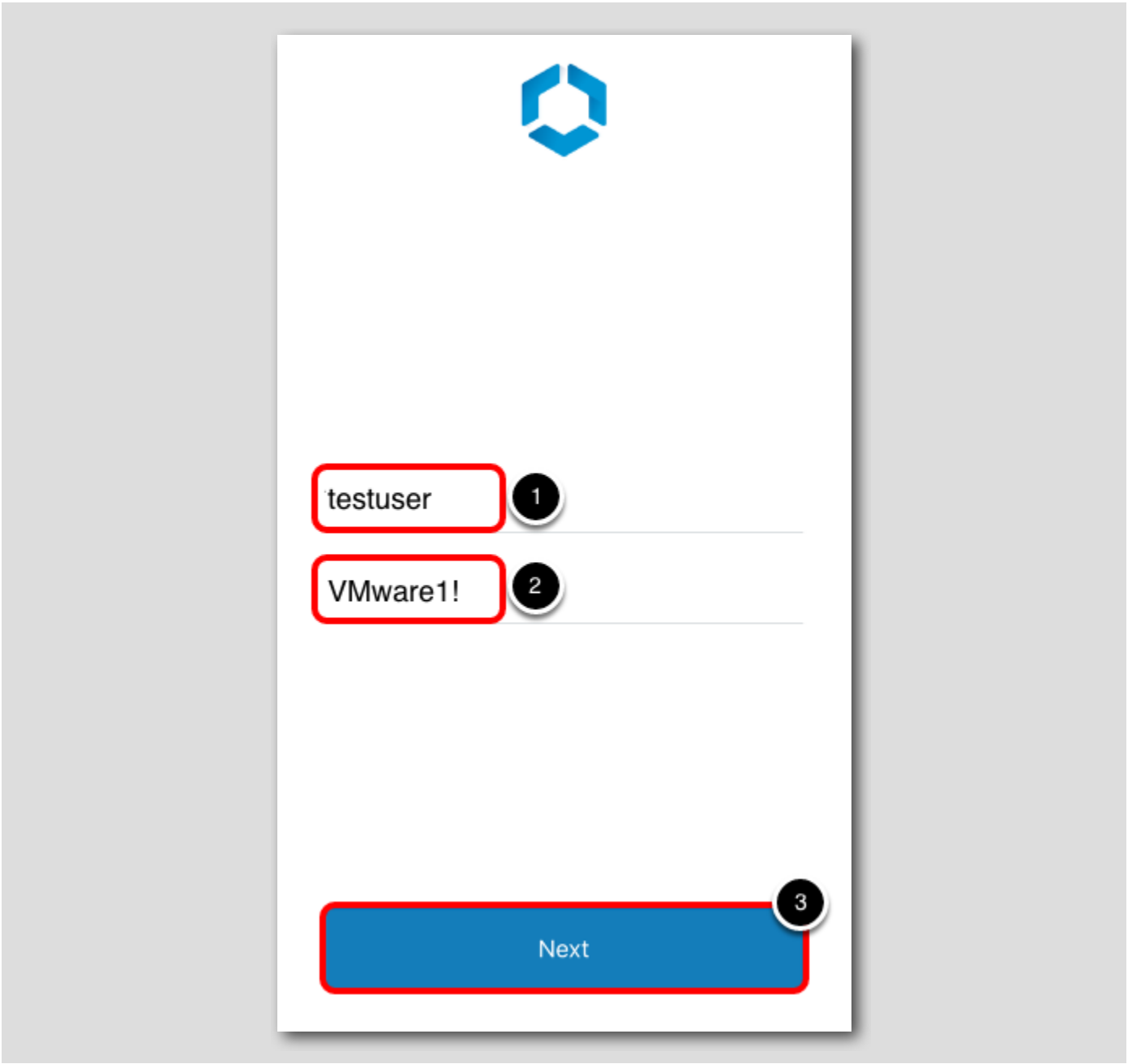
Return to the Workspace ONE Intelligent Hub application on your iOS Device,

1. 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.
2. Tap the **Next** button.

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

Enter User Credentials

[159]

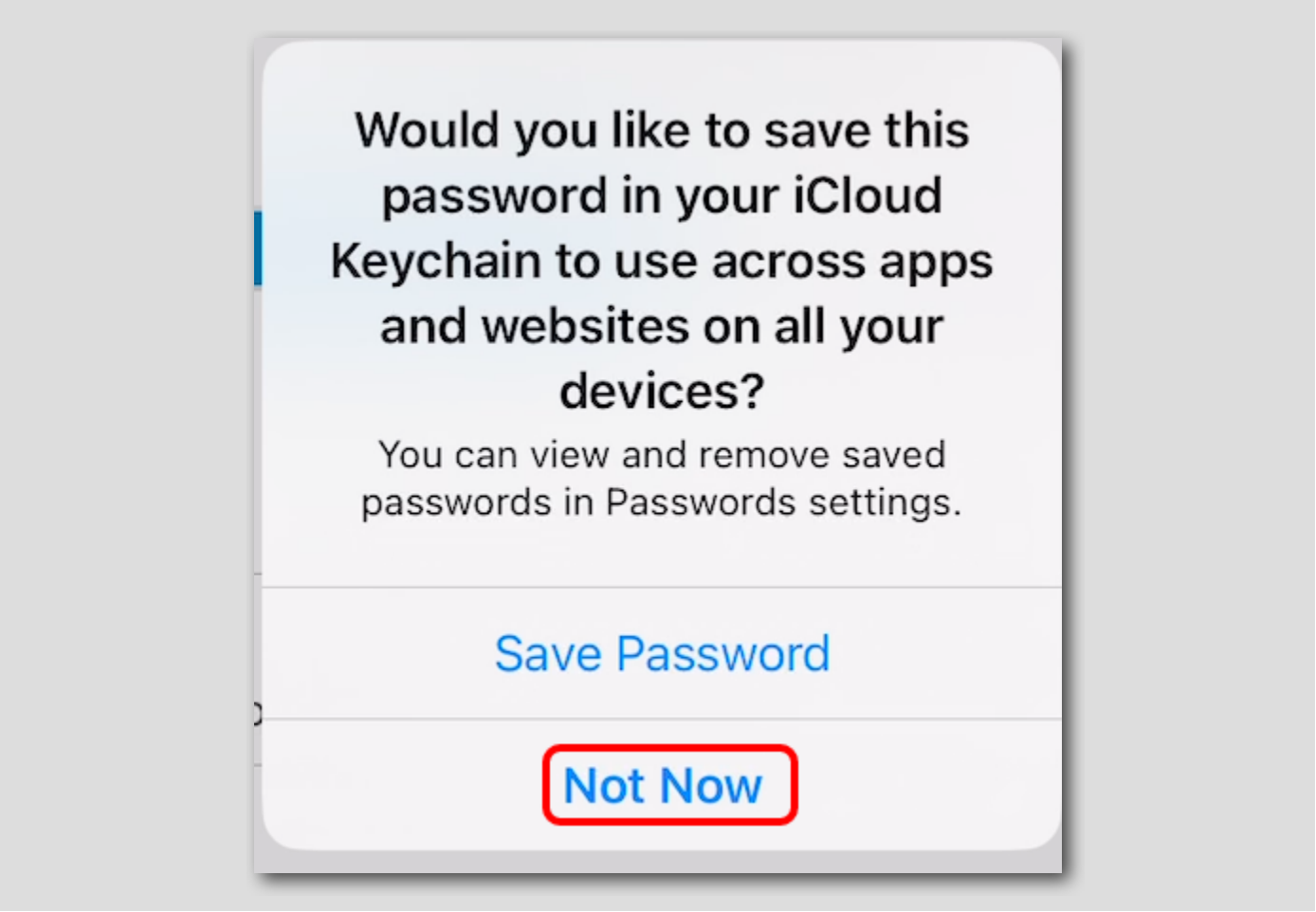


You will now provide user credentials to authenticate to Workspace ONE UEM.

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

Skip Password Save

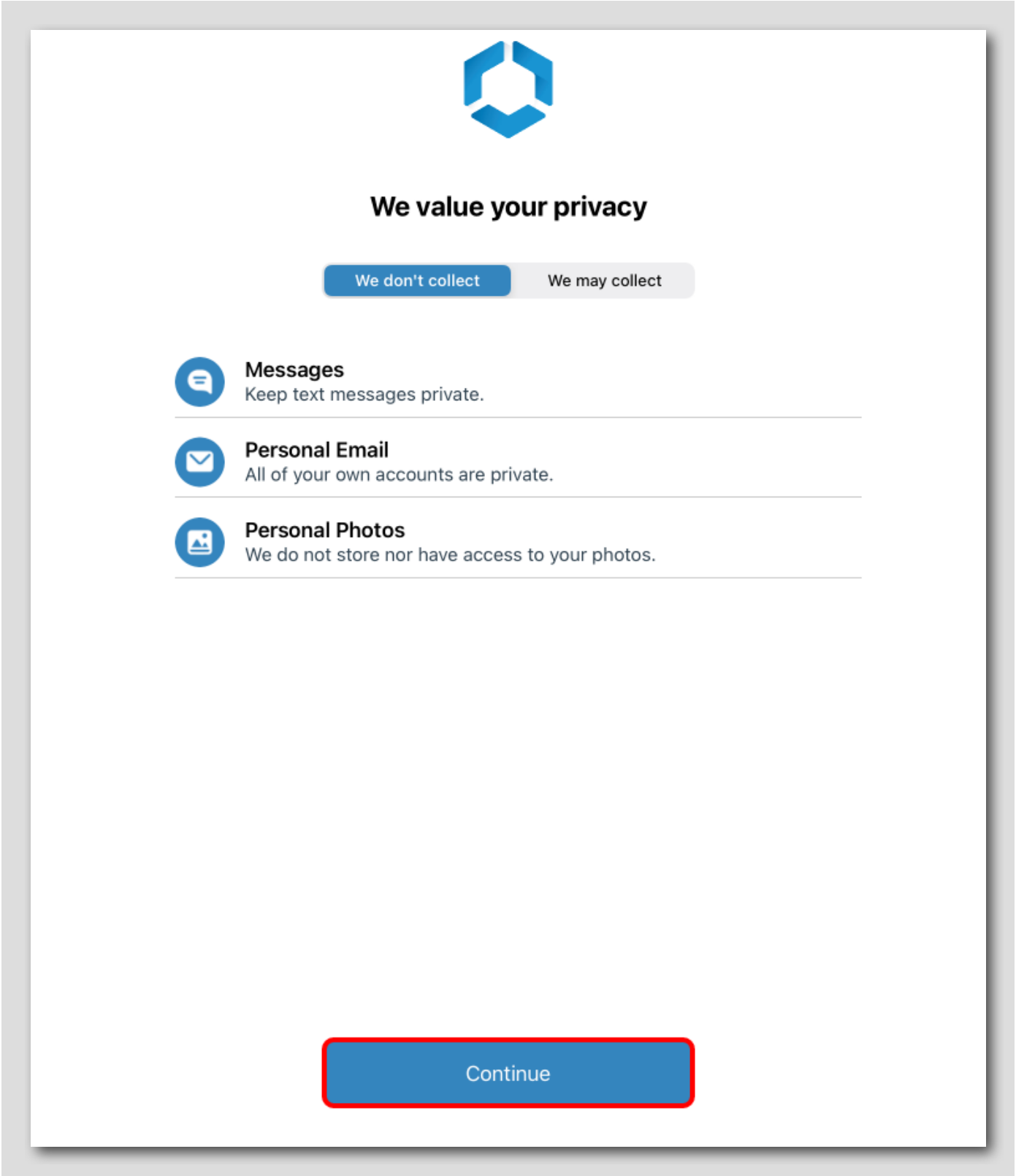
[160]



If prompted for password saving, click **Not Now**

Review privacy notice

[161]

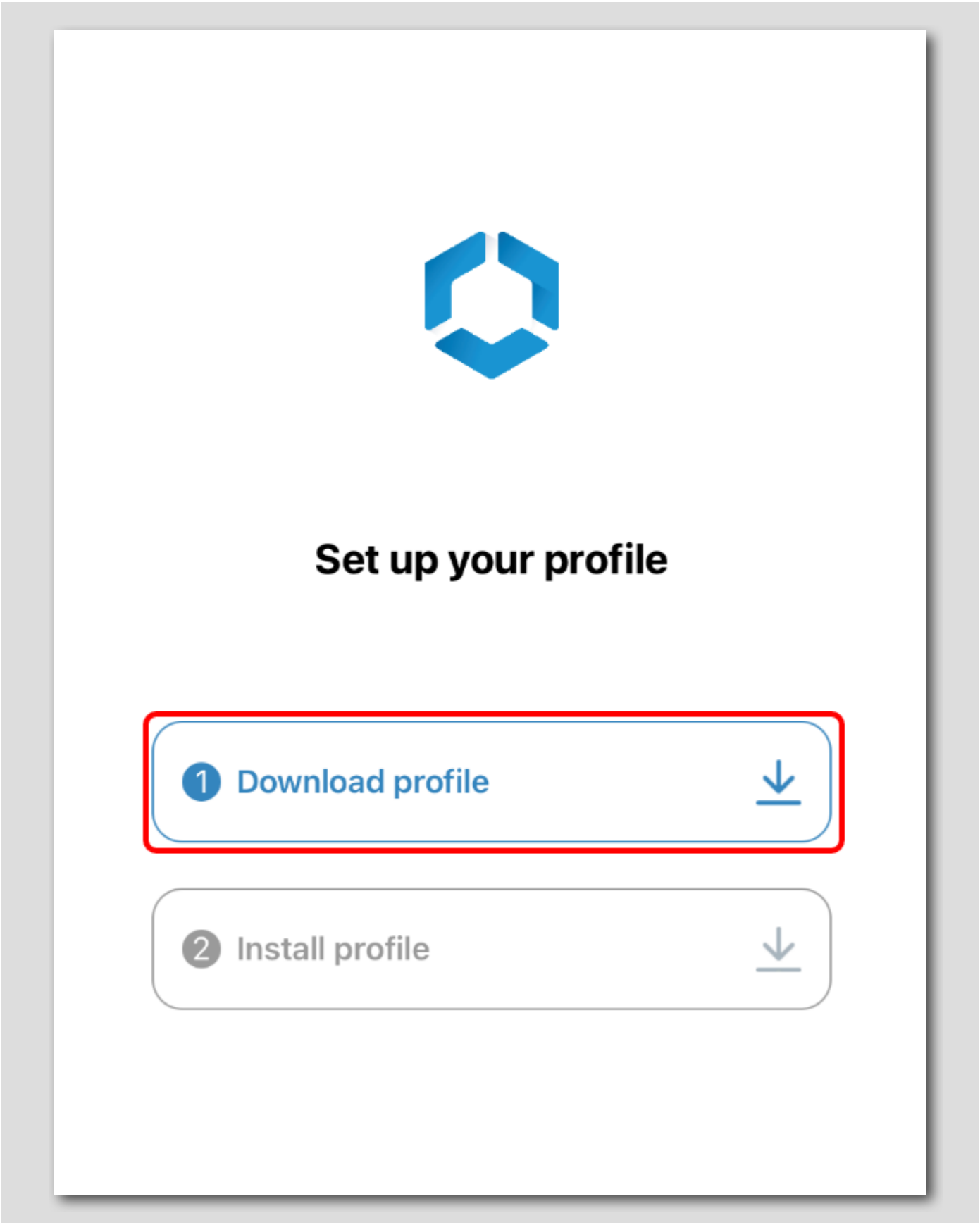

We value your privacy
We don't collect
We may collect
Messages
Keep text messages private.
Personal Email
All of your own accounts are private.
Personal Photos
We do not store nor have access to your photos.
Continue

The Workspace ONE Intelligent Hub will show a privacy message detailing what is collected and what is not collected from the device.

The next step is to download the configuration profile to enroll your device into Workspace ONE UEM.

Tap **Continue** to begin.

Setup device profile

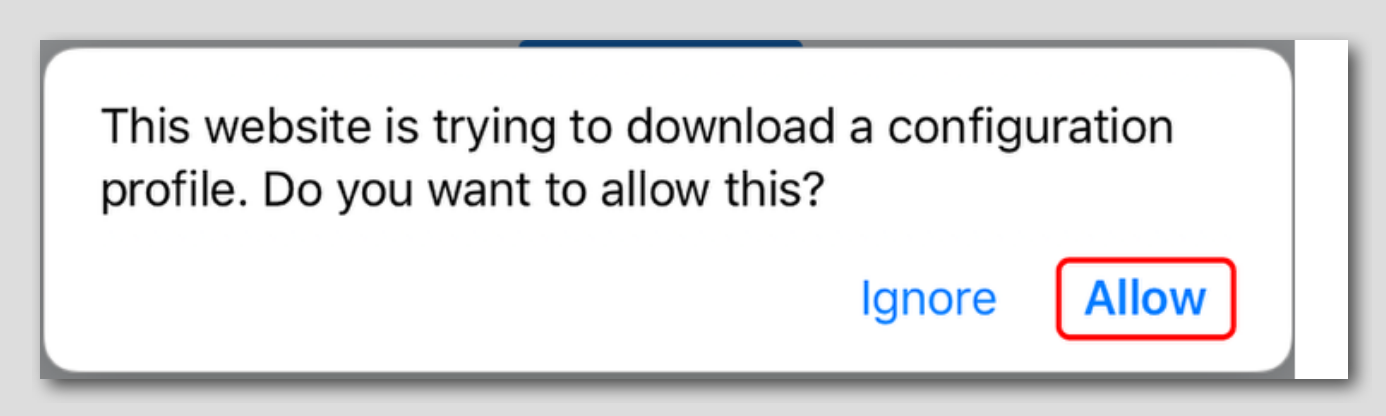

Set up your profile
1 Download profile
2 Install profile

The next step is to download the configuration profile to enroll your device into Workspace ONE UEM.

Tap **Download profile** to begin.

Allow Website to download a configuration profile

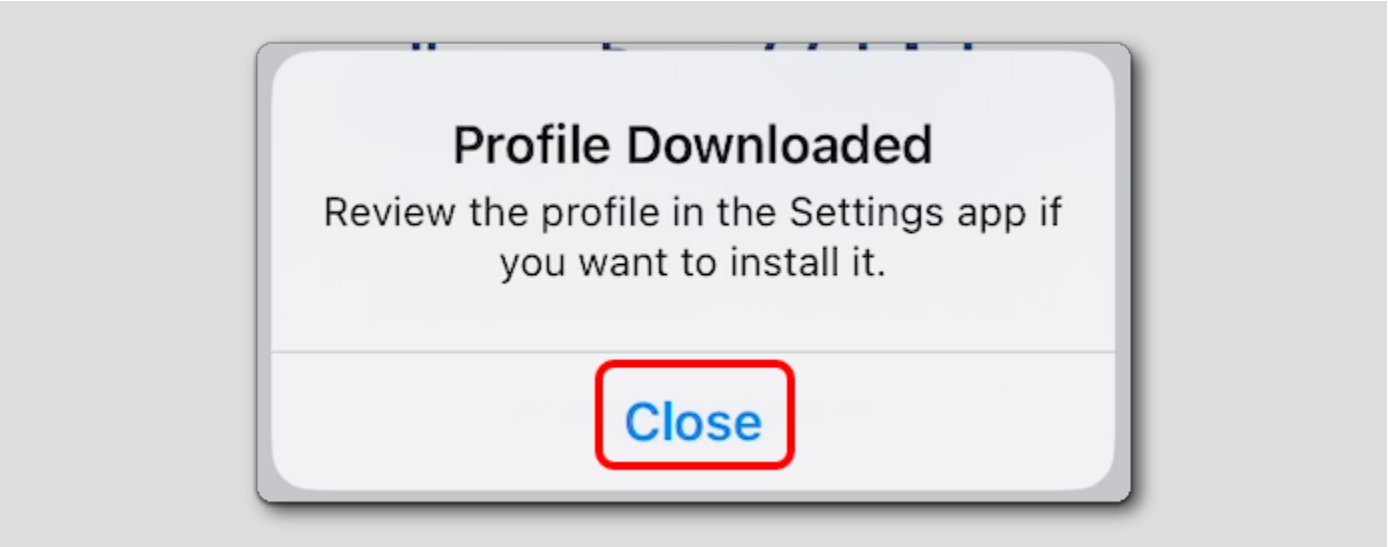
[163]



When prompted that the website is trying to download a configuration profile, tap **Allow**.

Close Profile Downloaded Notification

[164]



When the Profile Downloaded notification is displayed, click **Close**.

VMWARE
HANDS-ON LABS

Steps to download profile

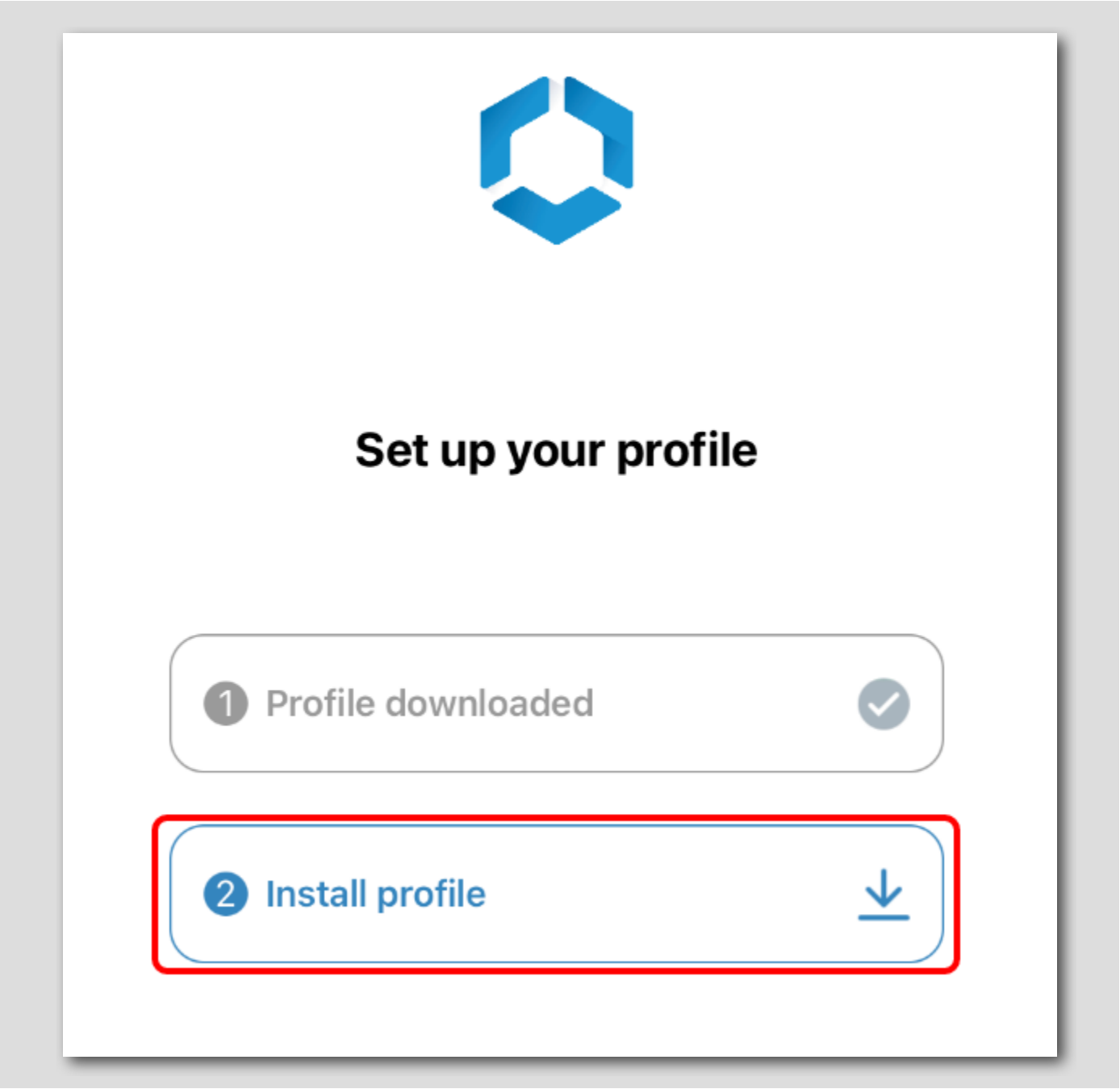
1. When prompted to download the profile, tap on **Allow**

2. After the download is complete, tap on

Now that the profile is downloaded, tap **Tap here when download finishes**. This will return you to the Intelligent Hub application where you will install the profile.

Install device profile

[165]



The next step is to Install the configuration profile to enroll your device into Workspace ONE UEM.

Tap **Install profile** to begin.

Open the Settings App

[166]

Install profile

1. In the **Settings** app, locate and tap **Profile Downloaded** at the top.

2. Select **Install** to continue the process.

3. Tap **Trust** on the **Remote Management** pop up.

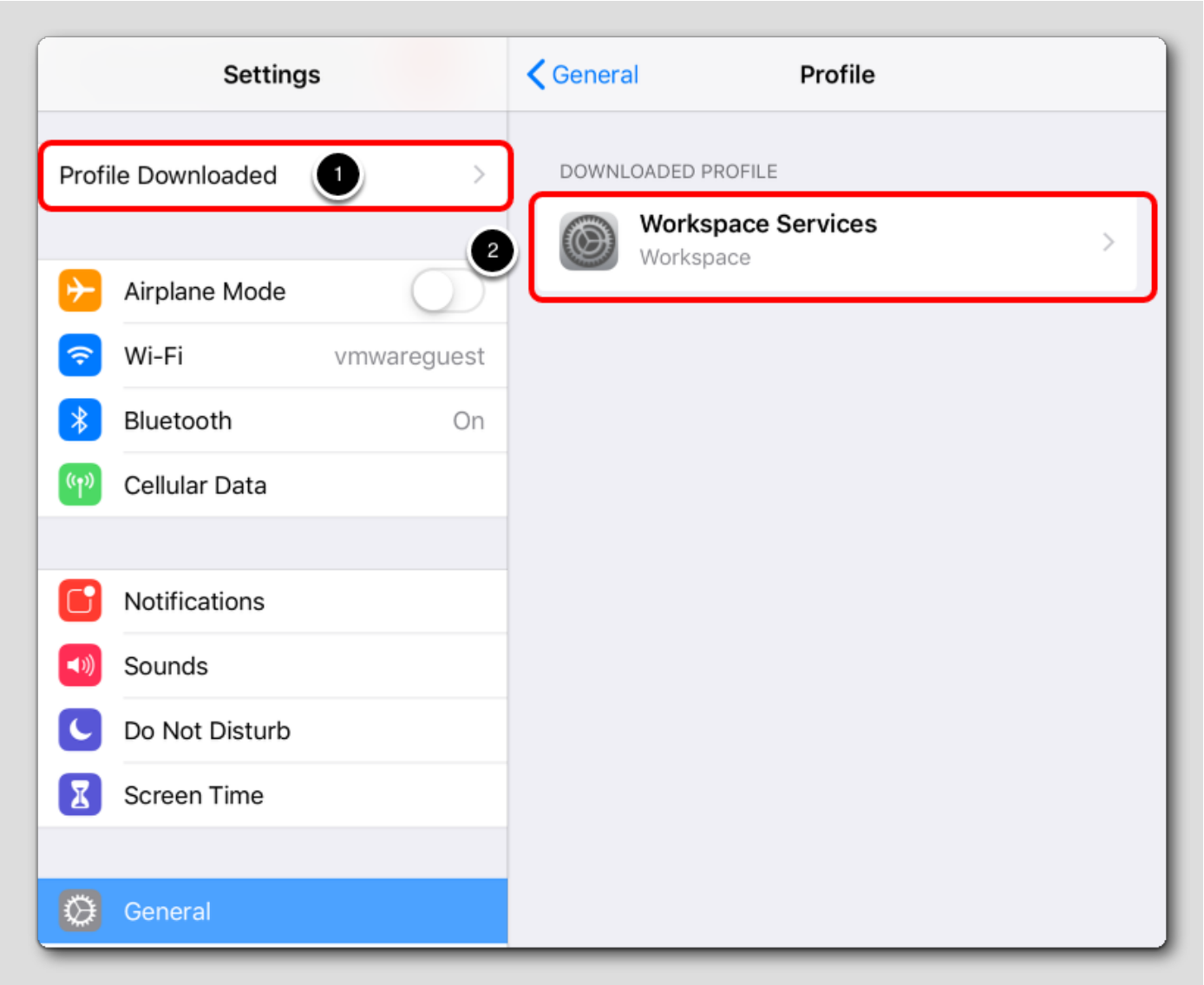
4. Once the profile is installed, return to **Hub** to complete your enrollment.

Open the Settings app

An instructional prompt will inform users how to finish their enrollment profile installation in the Settings app. Tap **Open the Settings app** to continue.

Open the Downloaded Profile

[167]

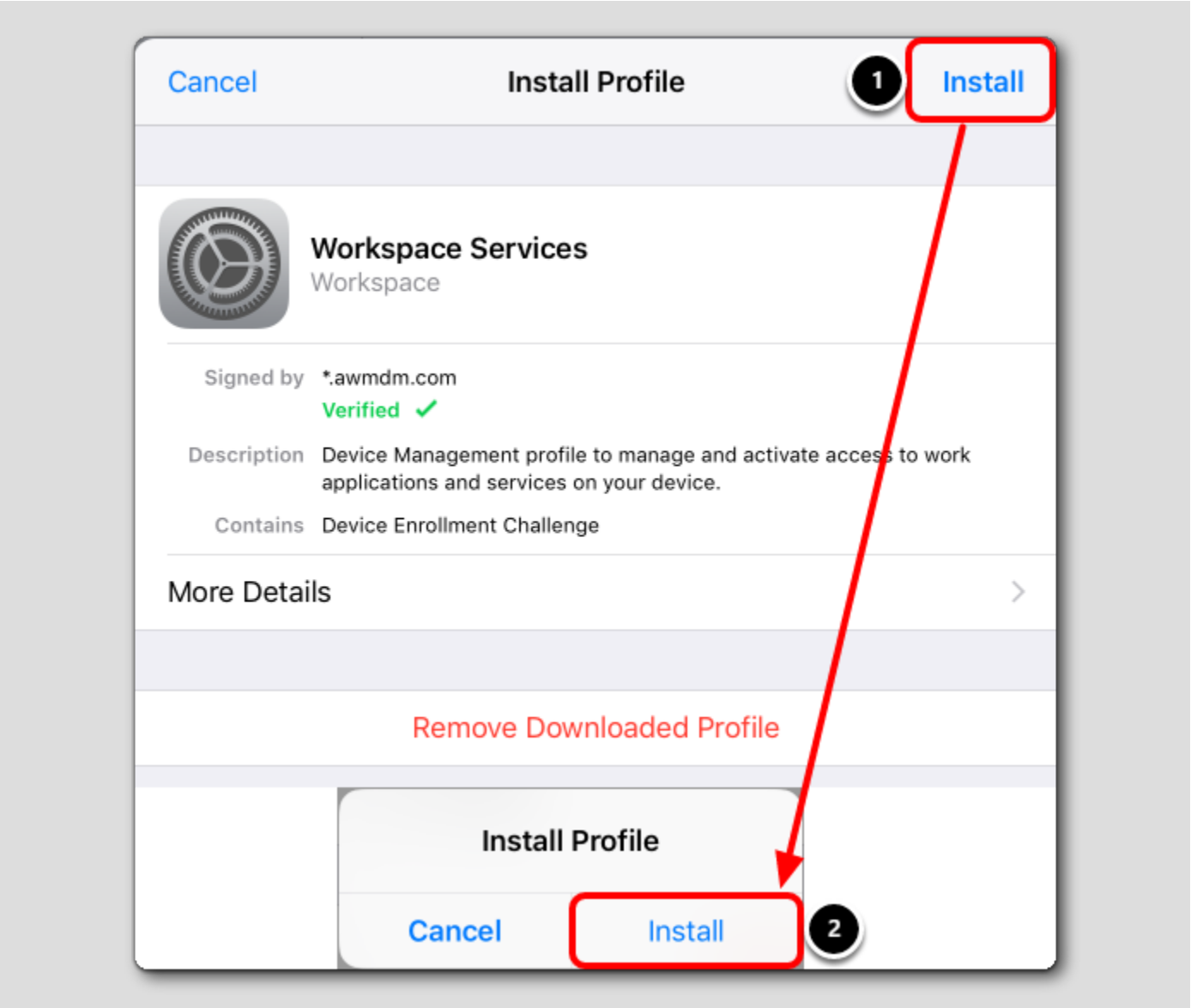


In the Settings app.

1. Tap **Profile Downloaded**.
2. Tap **Workspace Services** Profile

Install the Workspace ONE MDM Profile

[168]



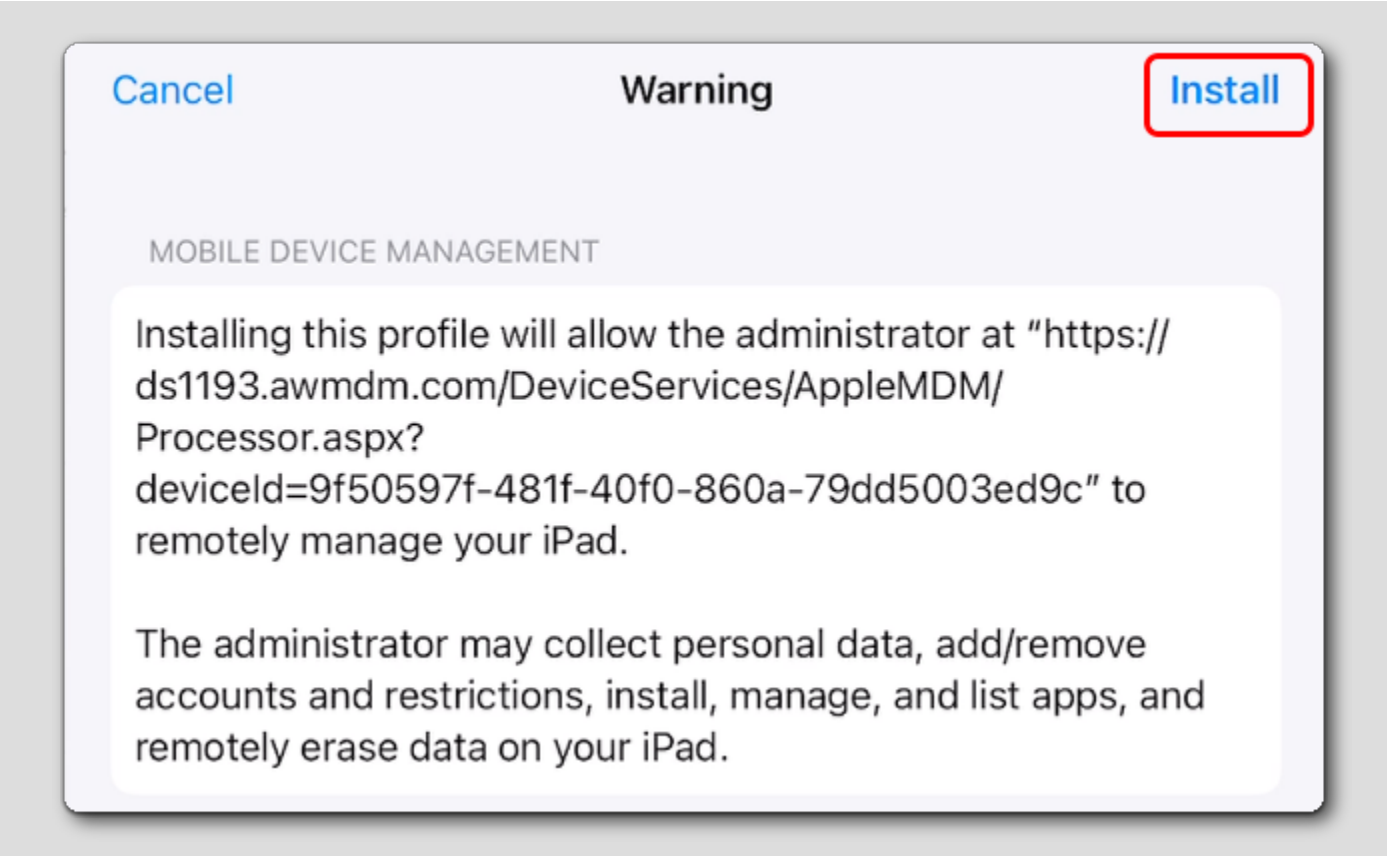
1. Tap **Install** in the upper right corner of the Install Profile dialog box.

   NOTE: If you have a passcode on your device, you will be prompted to input the passcode to continue.

2. Tap **Install** for the pop-up prompt to confirm.

iOS MDM Profile Warning

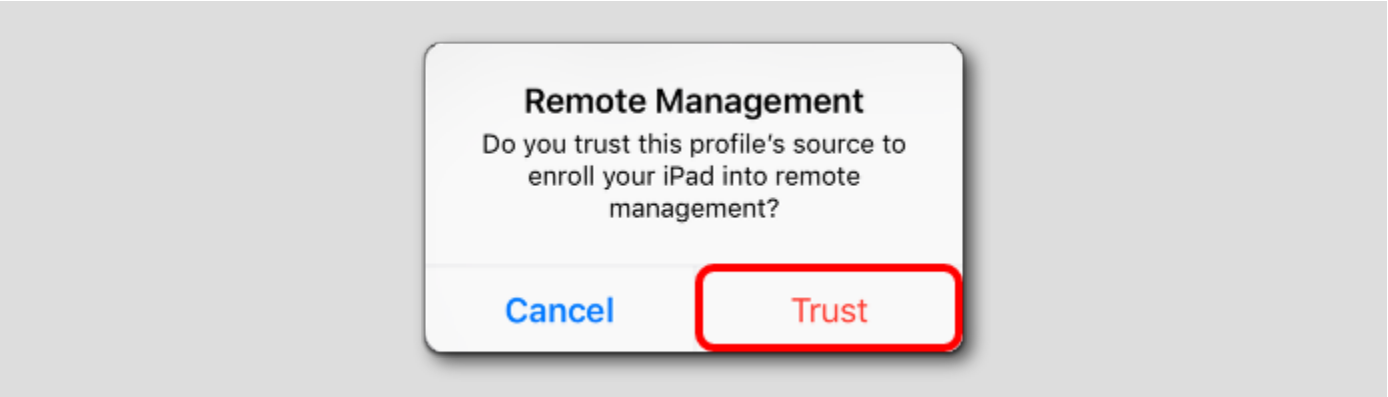
[169]



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. [170]

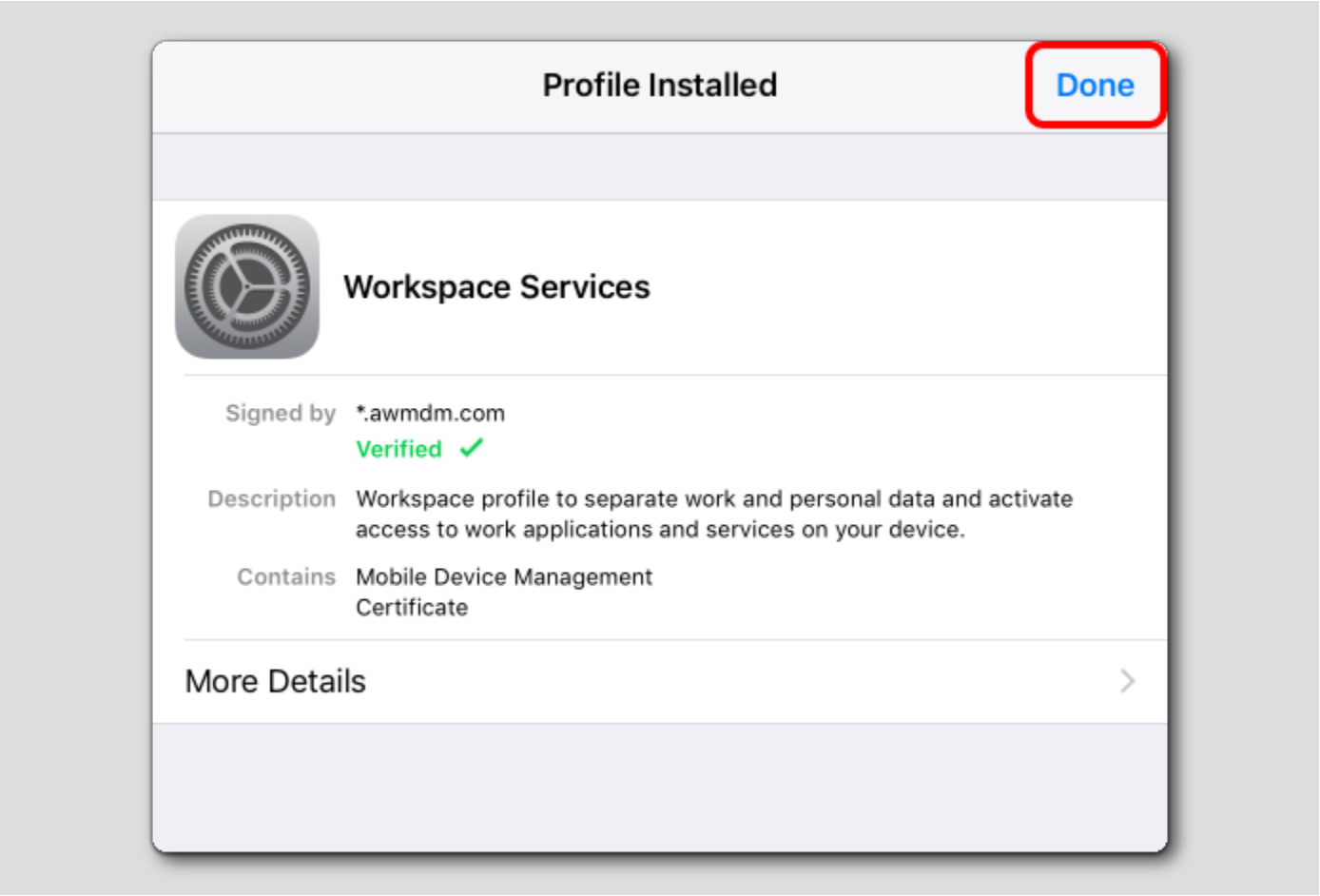


You should now see the iOS request to trust the source of the MDM profile.

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

iOS Profile Installation Complete

[171]



You should now see that the iOS Profile was successfully installed.

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

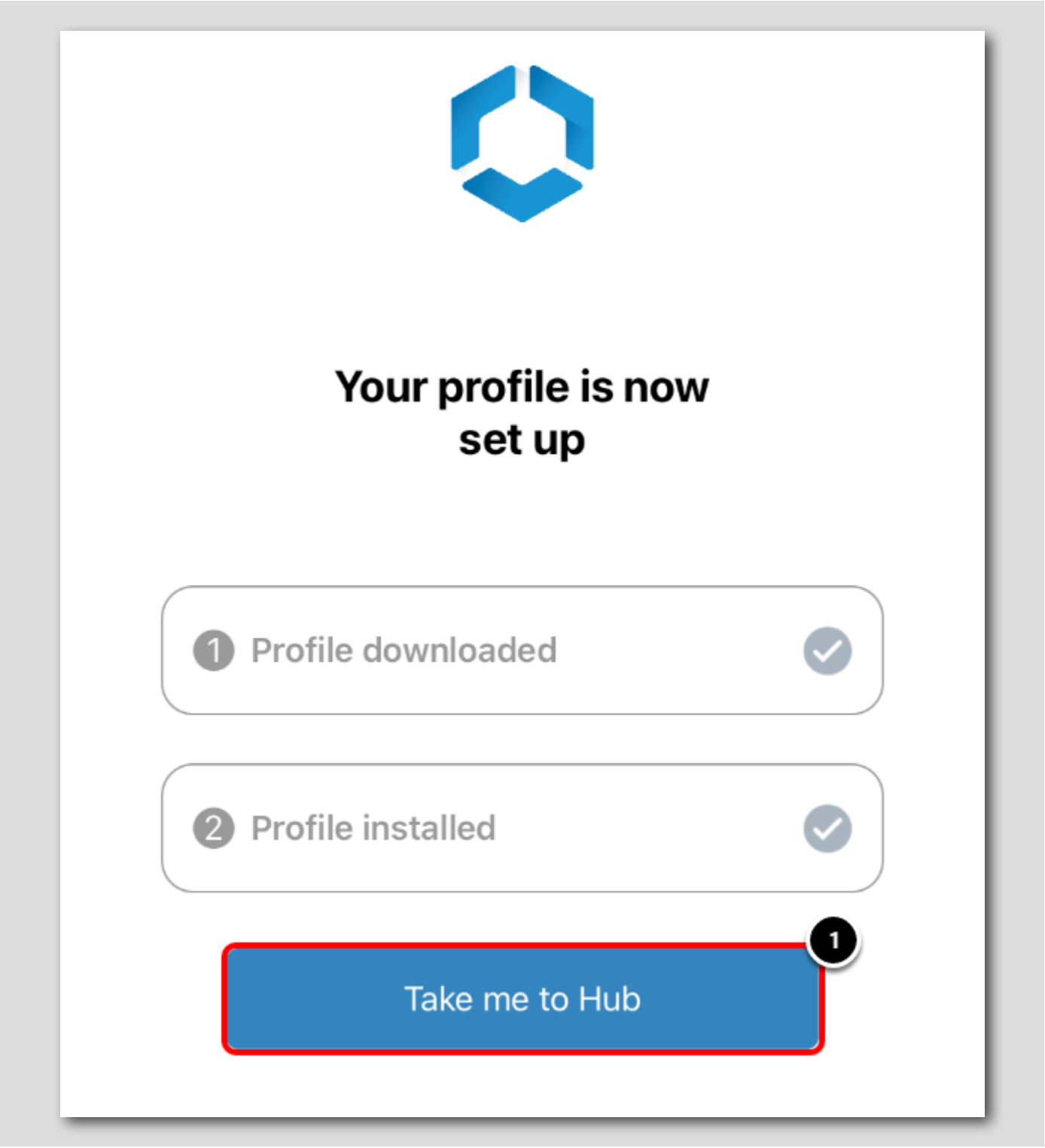
Navigate to Workspace ONE Intelligent Hub

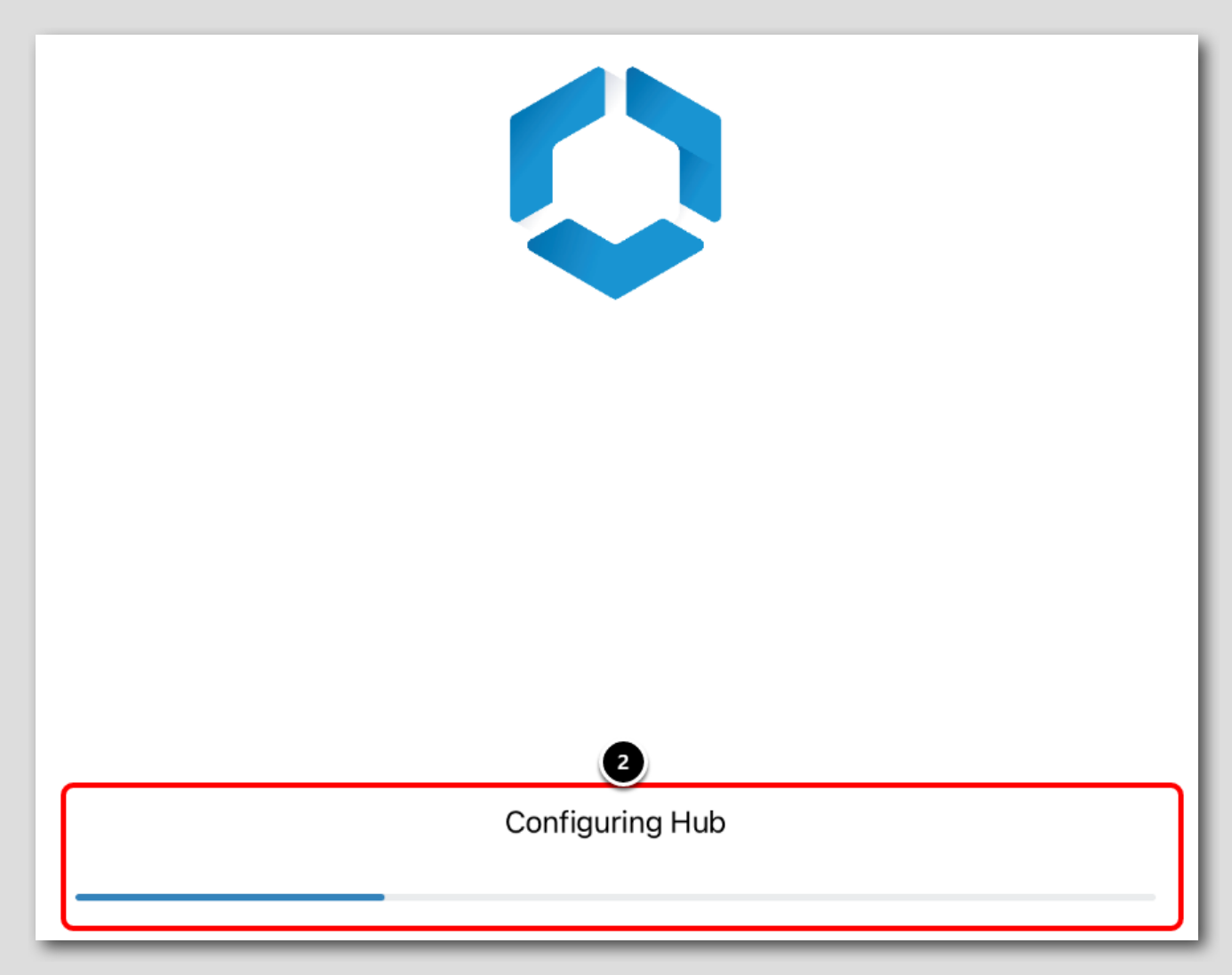
[172]

Your enrollment is now completed! Return to the **Workspace ONE Intelligent Hub** app.

Continue to Hub

[173]



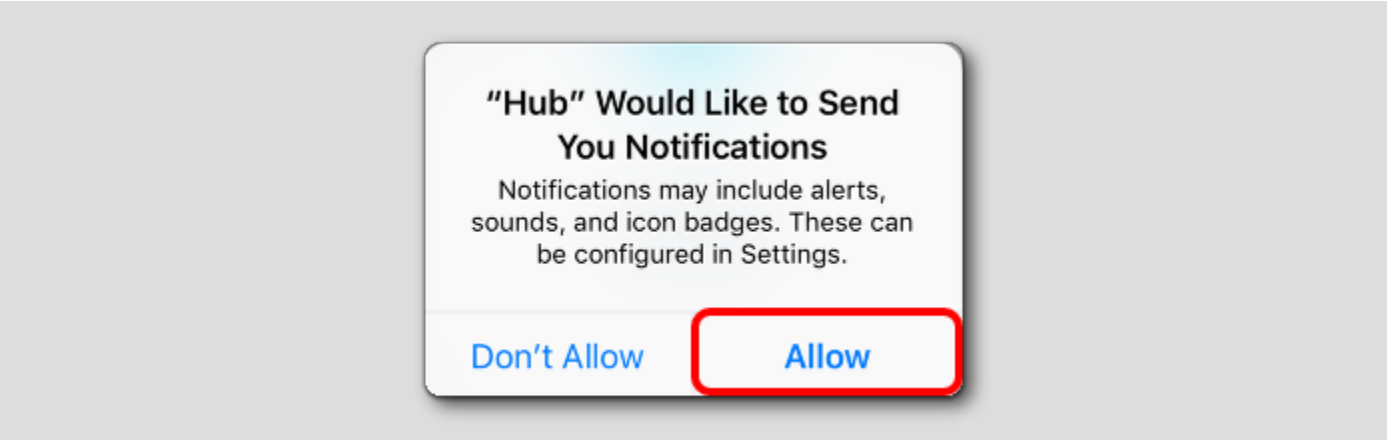


You will see that the profile is not successfully configured.

1. Tap **Take me to Hub** to continue.
2. A **Configuring Hub** loading bar will display, wait for this to complete and then continue to the next step.

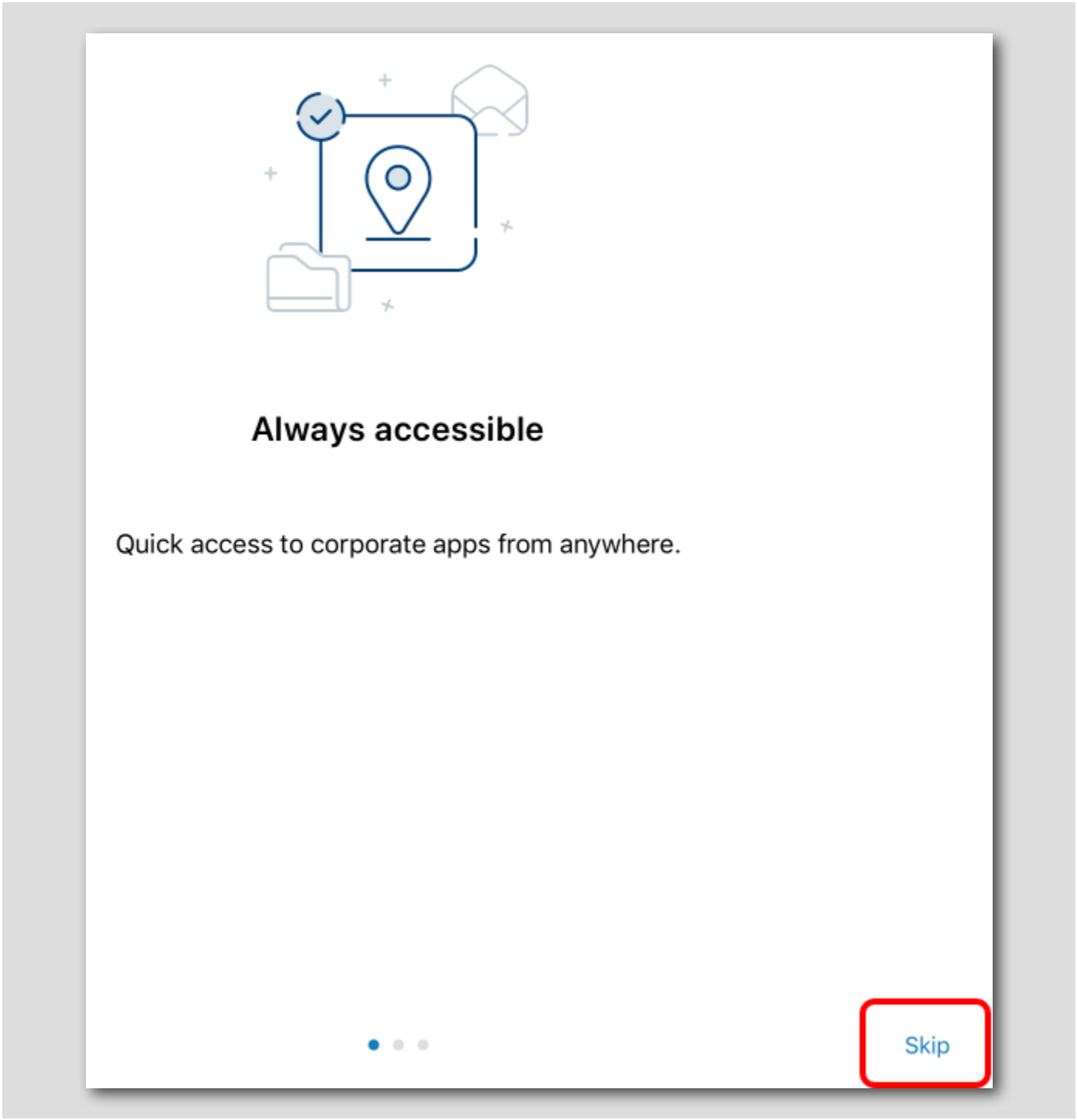
Accept Notifications for Hub (IF NEEDED)

[174]



Tap **Allow** if you get a prompt to allow notifications for the Hub app.

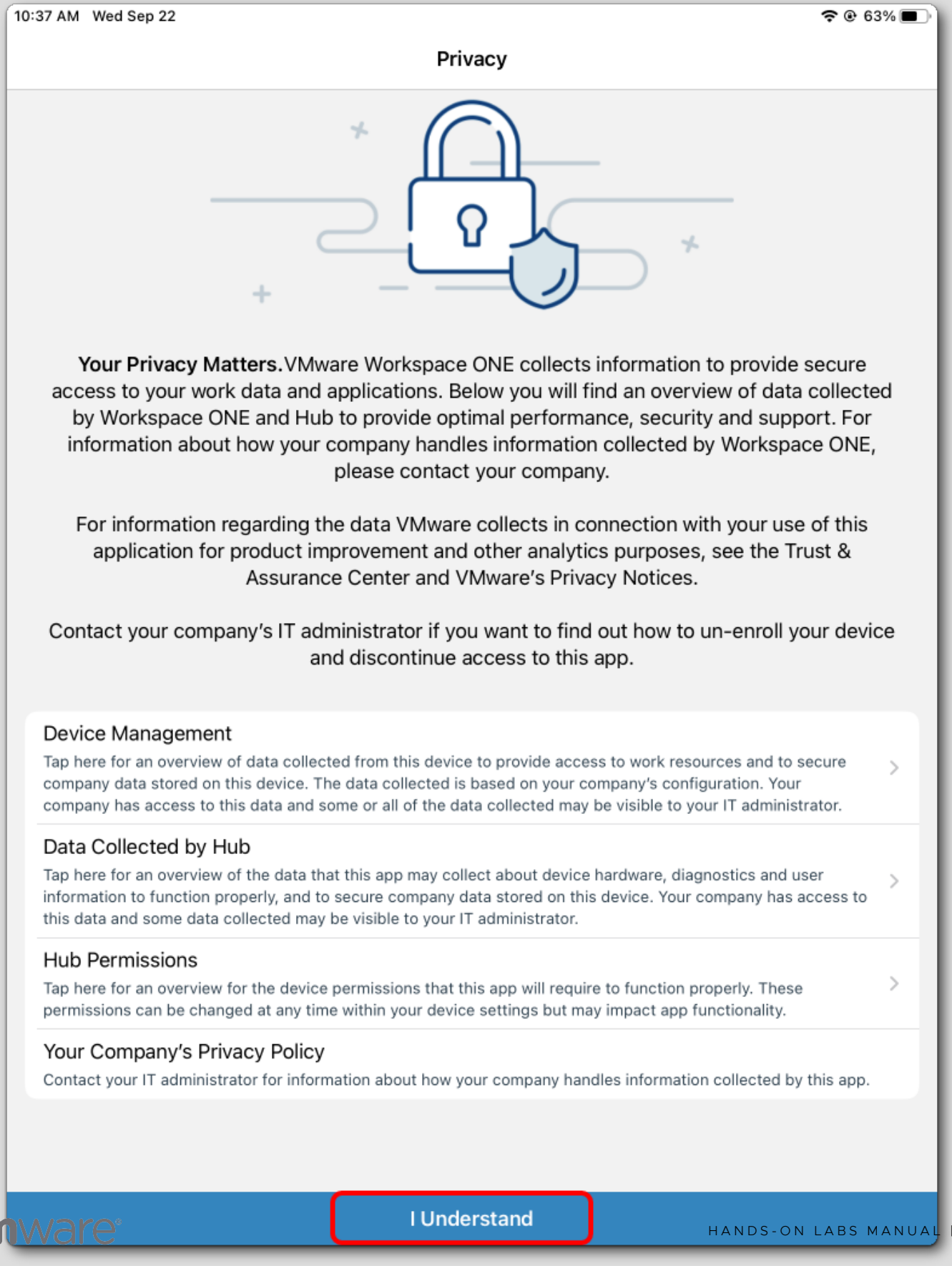
Skip the Introduction (IF PROMPTED) [175]



Click **Skip**.

Confirm the Privacy Policy

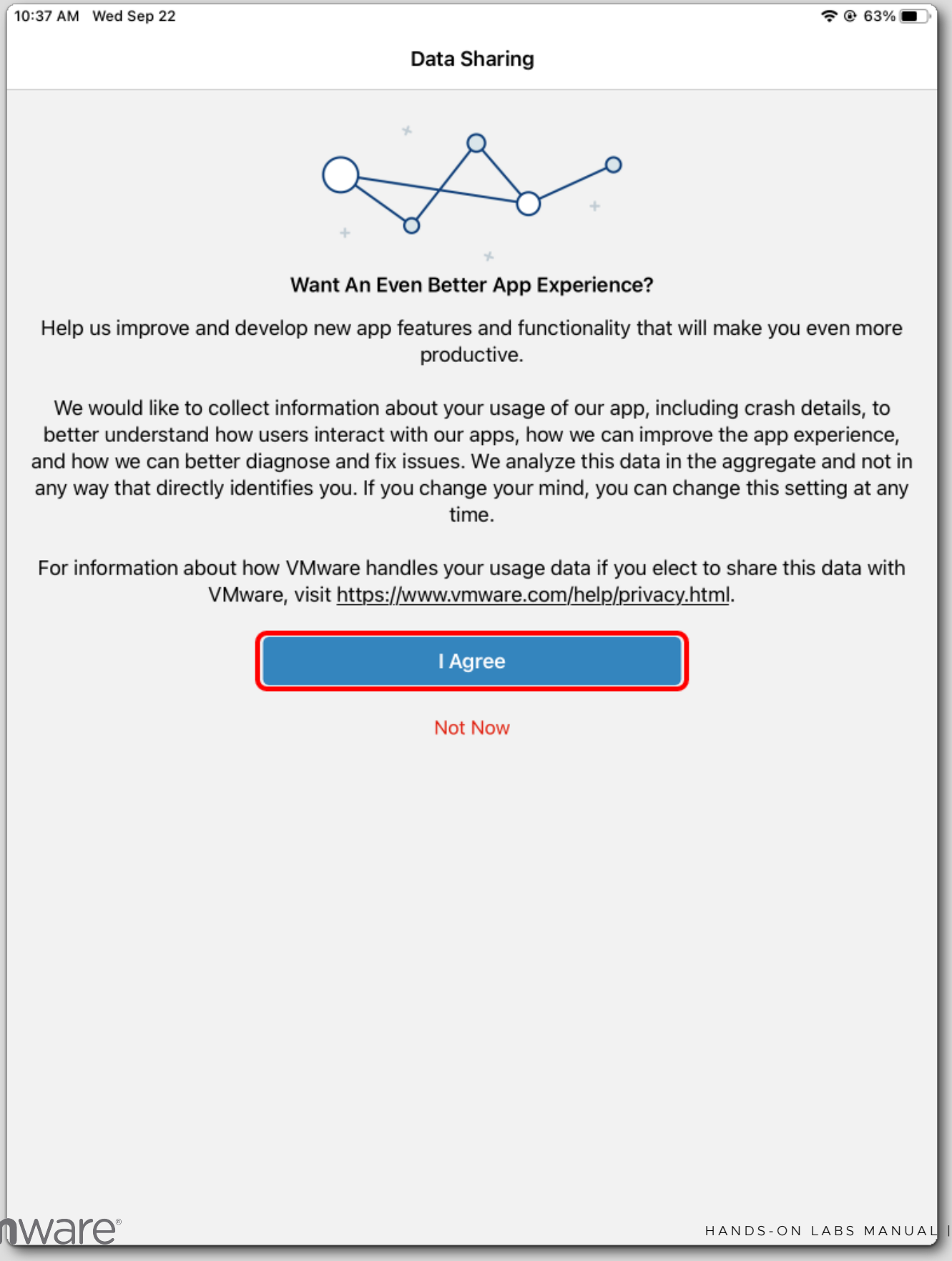
[176]


10:37 AM Wed Sep 22
63%
Privacy
Your Privacy Matters. VMware Workspace ONE collects information to provide secure access to your work data and applications. Below you will find an overview of data collected by Workspace ONE and Hub to provide optimal performance, security and support. For information about how your company handles information collected by Workspace ONE, please contact your company.
For information regarding the data VMware collects in connection with your use of this application for product improvement and other analytics purposes, see the Trust & Assurance Center and VMware's Privacy Notices.
Contact your company's IT administrator if you want to find out how to un-enroll your device and discontinue access to this app.
Device Management
Tap here for an overview of data collected from this device to provide access to work resources and to secure company data stored on this device. The data collected is based on your company's configuration. Your company has access to this data and some or all of the data collected may be visible to your IT administrator.
Data Collected by Hub
Tap here for an overview of the data that this app may collect about device hardware, diagnostics and user information to function properly, and to secure company data stored on this device. Your company has access to this data and some data collected may be visible to your IT administrator.
Hub Permissions
Tap here for an overview for the device permissions that this app will require to function properly. These permissions can be changed at any time within your device settings but may impact app functionality.
Your Company's Privacy Policy
Contact your IT administrator for information about how your company handles information collected by this app.
I Understand

Tap **I Understand** when shown the Privacy policy.

Accept the Data Sharing Policy

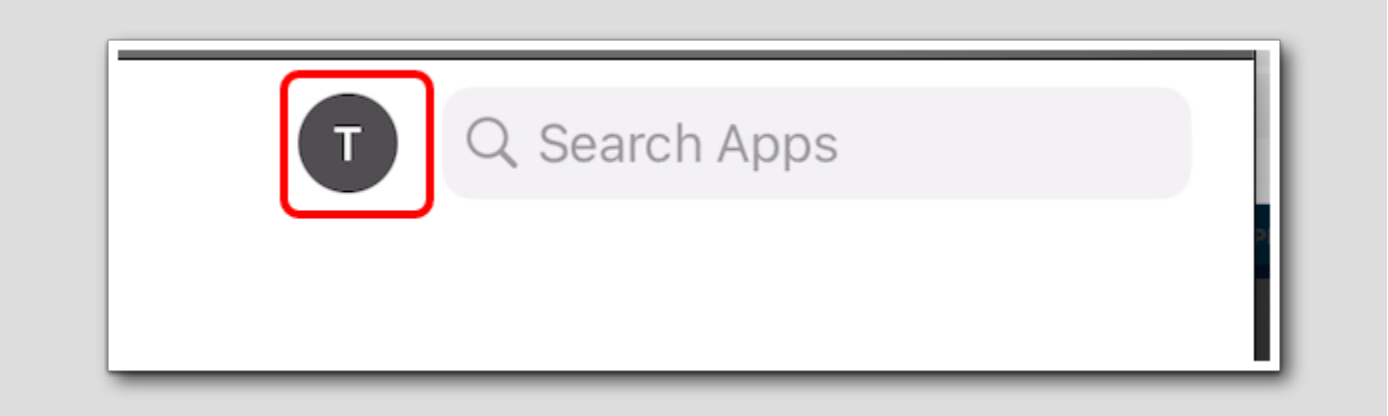
[177]

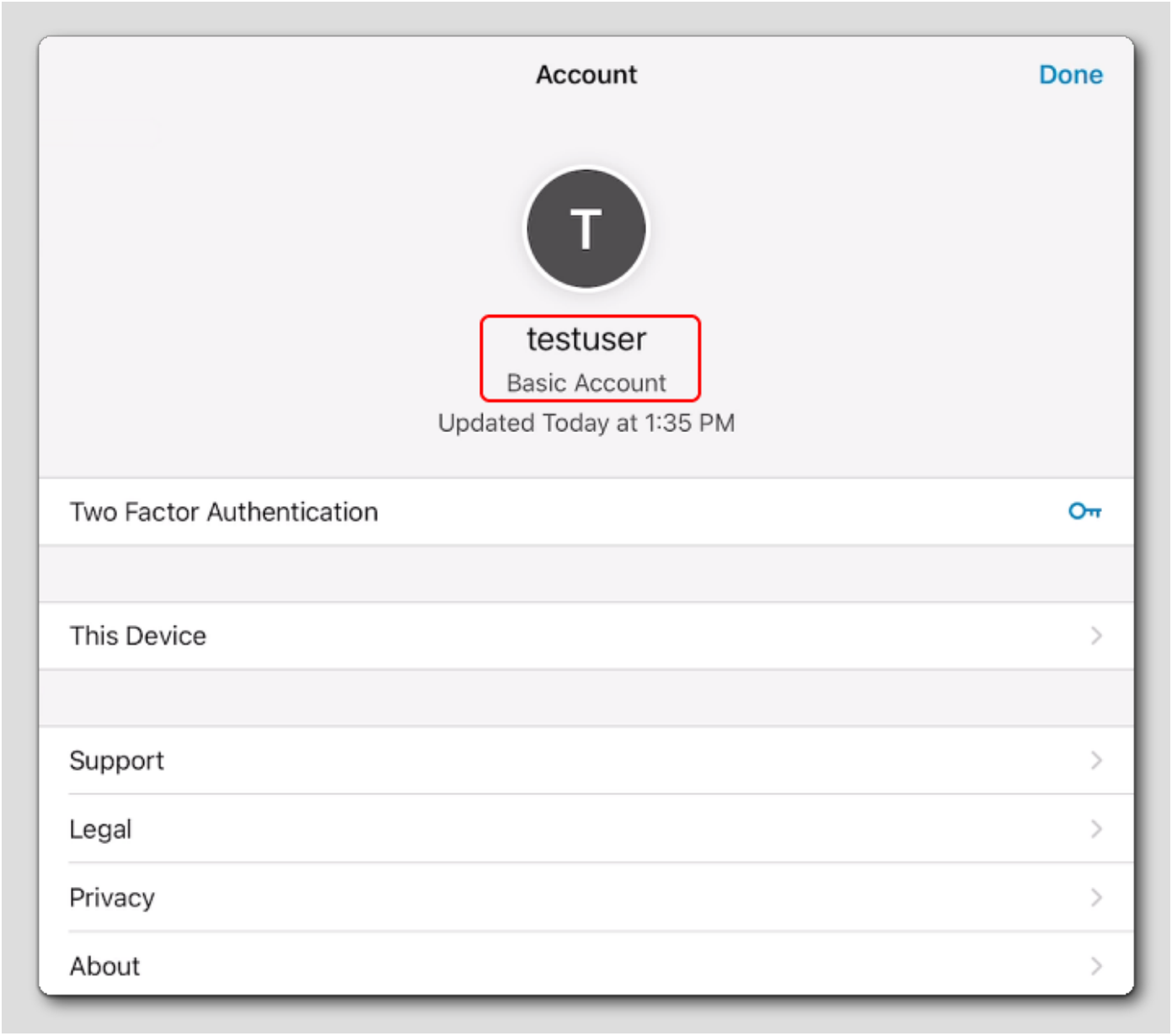

10:37 AM Wed Sep 22
63%
Data Sharing
Want An Even Better App Experience?
Help us improve and develop new app features and functionality that will make you even more productive.
We would like to collect information about your usage of our app, including crash details, to better understand how users interact with our apps, how we can improve the app experience, and how we can better diagnose and fix issues. We analyze this data in the aggregate and not in any way that directly identifies you. If you change your mind, you can change this setting at any time.
For information about how VMware handles your usage data if you elect to share this data with VMware, visit https://www.vmware.com/help/privacy.html.
I Agree
Not Now

Tap **I Agree** for the Data Sharing policy.

Confirm the Device Enrollment in the Hub App

[178]





Confirm that the Hub app shows the user account (**testuser**) that you enrolled with..

You have now successfully enrolled your iOS device with Workspace ONE UEM! Continue to the next step.

Validate Device After Restriction Profile

[179]

You will now validate that the restriction profile for disabling Siri on the device is applying as expected. You will confirm the restriction profile in two ways:

1. Inspecting the Mobile Device Management profile that was installed to the device in previous steps to confirm that the restriction is present.
2. Attempting to interact with Siri on the device.

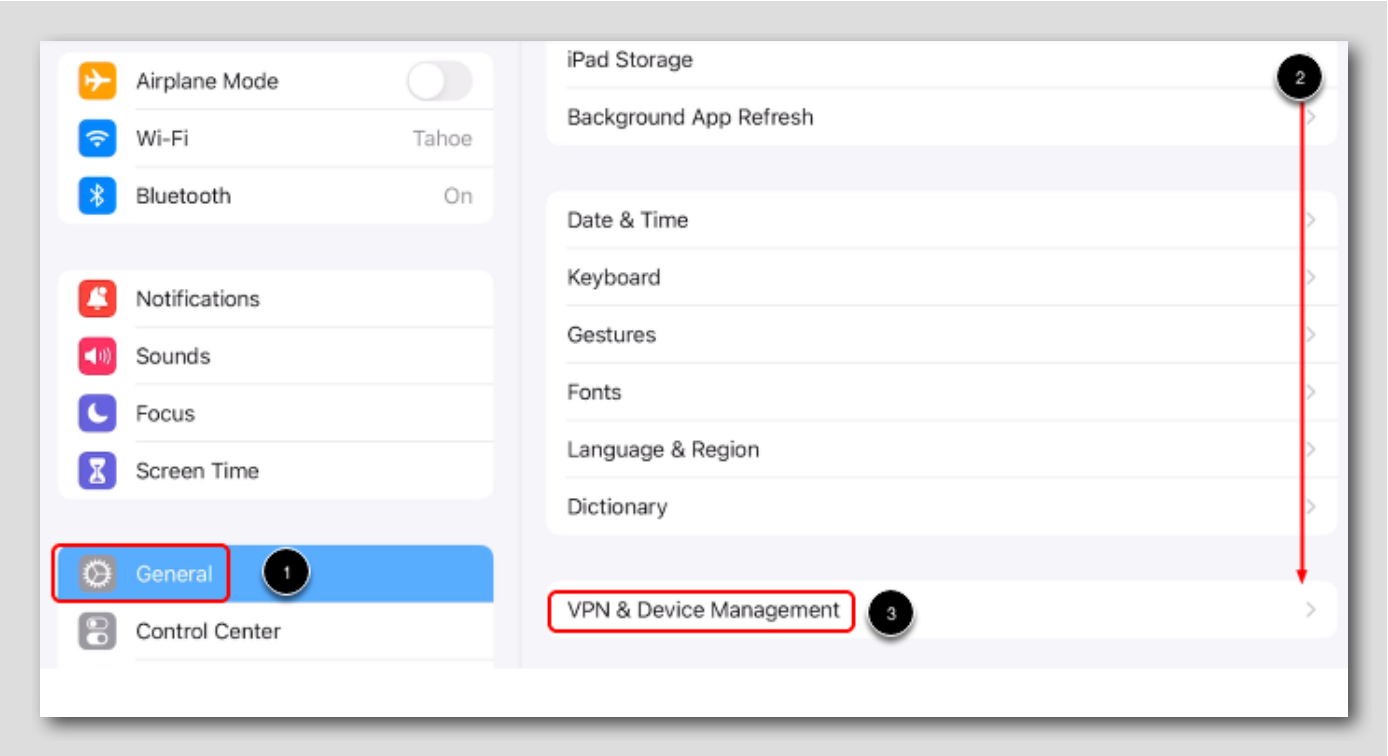
Validate the Restriction Profile in Settings

[180]

Tap the **Settings** app.

Navigate to Profiles & Device Management

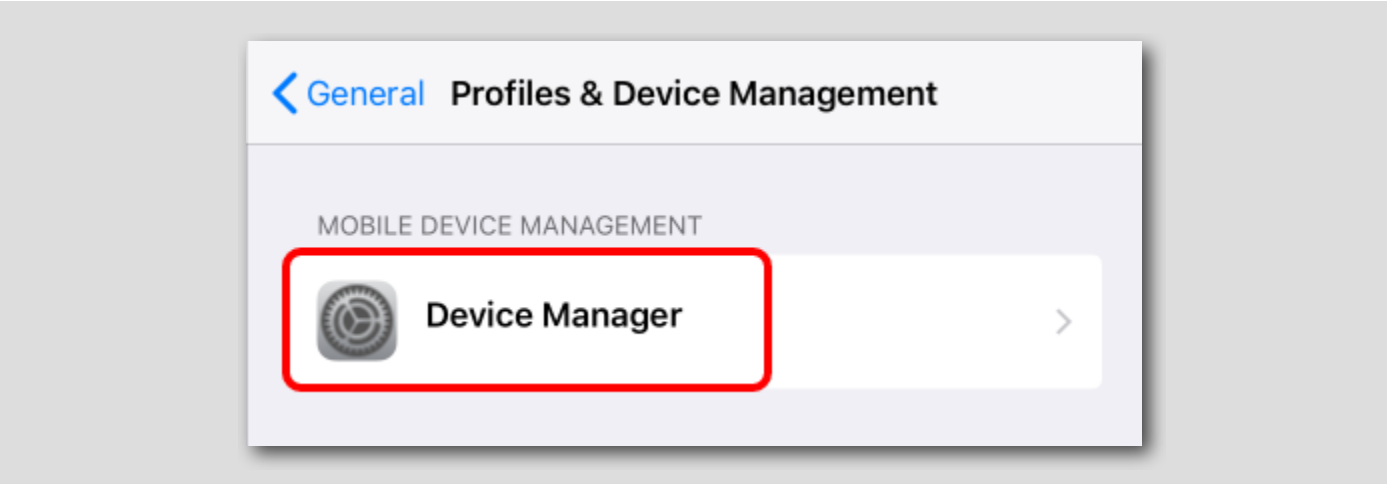
[181]



1. Tap **General**.
2. Scroll down to find the **VPN & Device Management** option.
3. Tap **VPN & Device Management**.

Open the Device Manager Profile

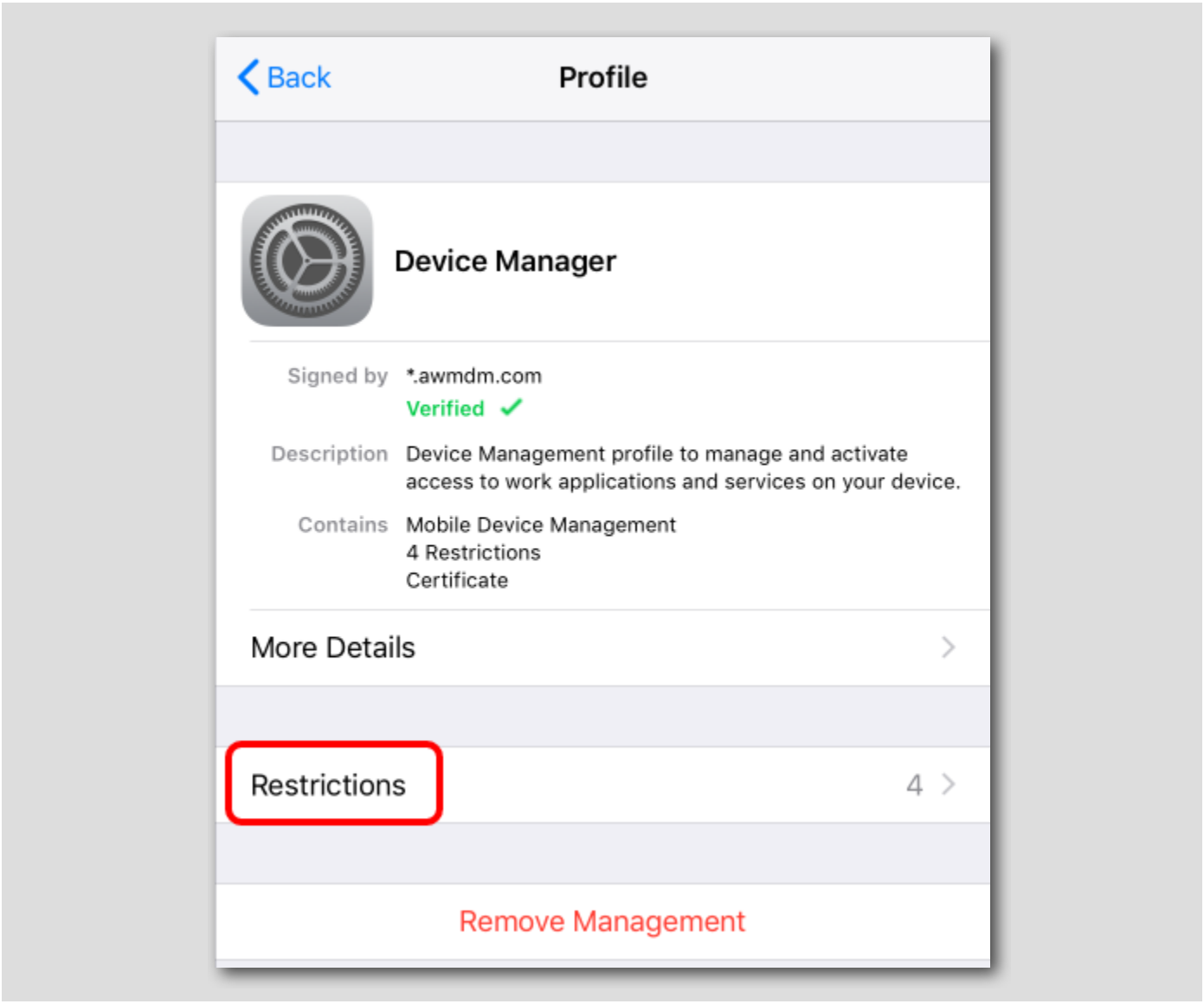
[182]



Tap the **Device Manager** profile under Mobile Device Management.

Inspect Restrictions

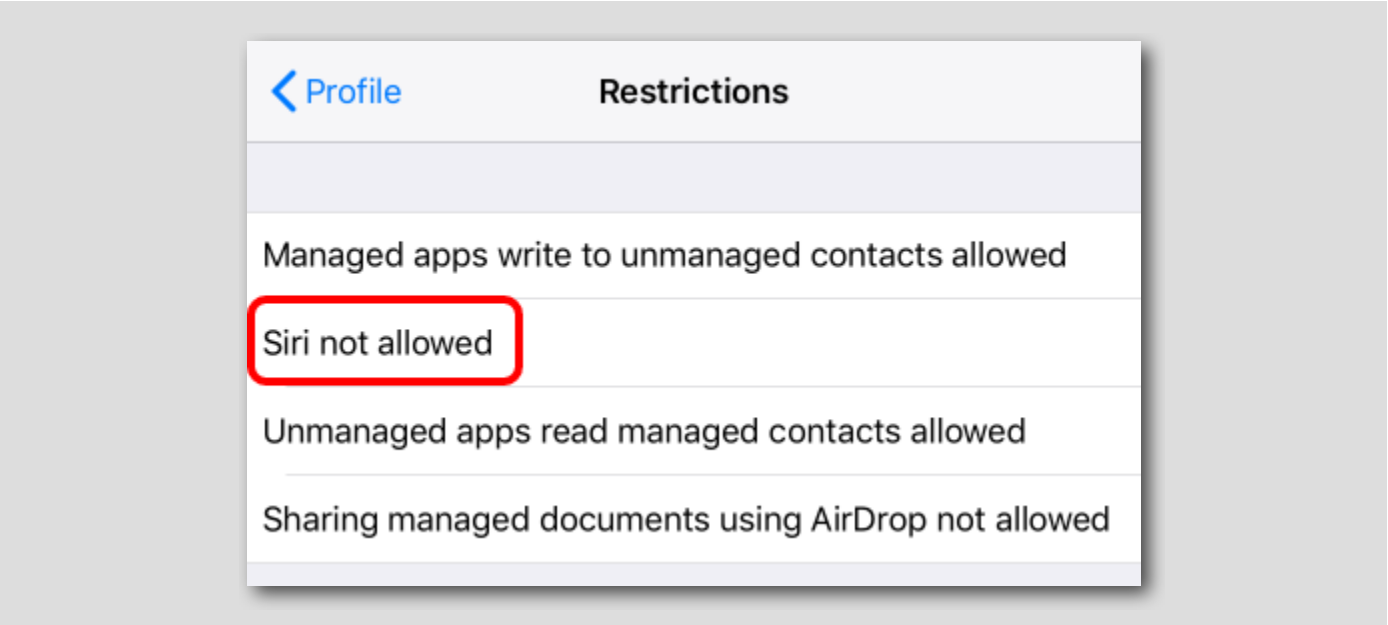
[183]



Tap Restrictions to inspect the restrictions associated with this profile.

Confirm Siri Not Allowed Restriction

[184]



Confirm that the **Siri not allowed** restriction is included in the list.

Validate Siri is Disabled on the Device

[185]

Attempt to activate Siri on your device again by holding the home button and notice that Siri no longer responds.

If you navigate to the **Settings** app, you will also notice that the **Siri & Search** settings are no longer available on the device.

Un-enrolling Your iOS Device

[186]

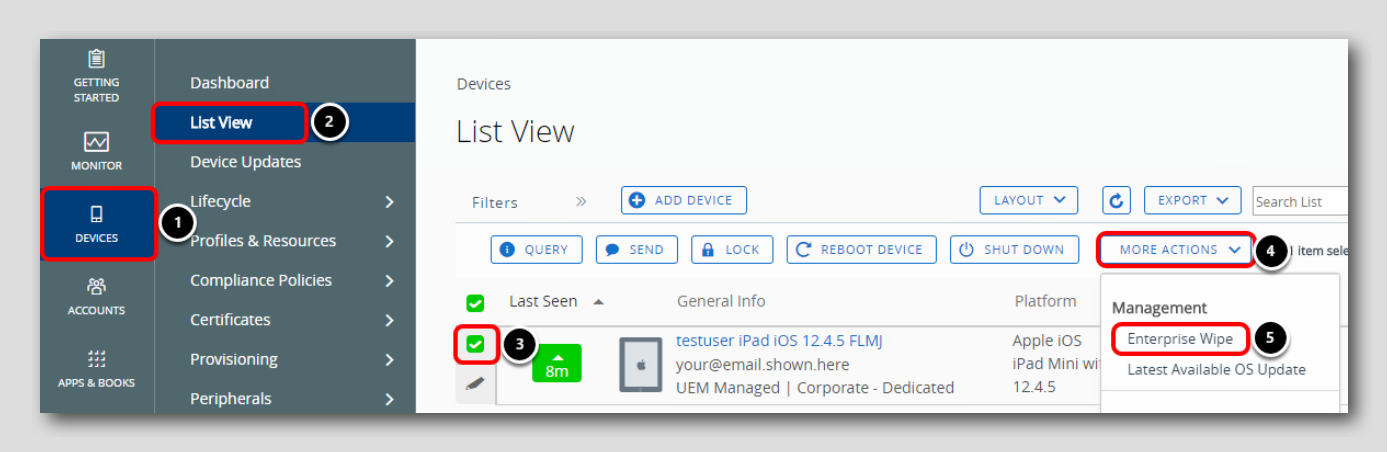
You are now going to un-enroll the iOS device from Workspace ONE UEM.

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 Workspace ONE Intelligent Hub controls.

It will NOT remove the Workspace ONE Intelligent Hub application from the device as this was downloaded manually before the user enrolled in to Workspace ONE UEM.

Enterprise Wipe (Un-Enroll) Your iOS Device

[187]

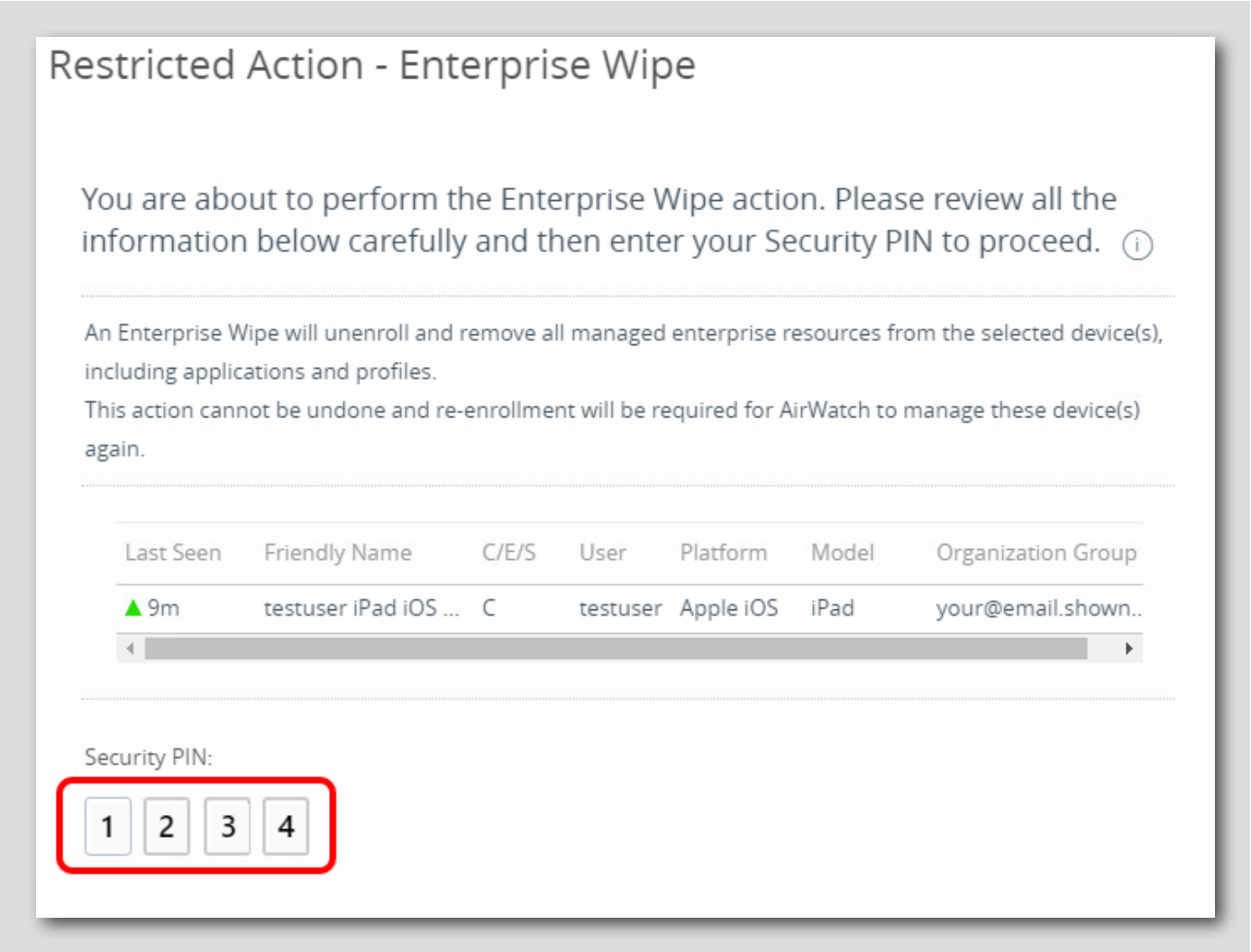


Enterprise Wiping will remove all the settings and content that were pushed to the device after it was enrolled. It will not affect anything that was on the device prior to enrollment.

Return to the Workspace ONE UEM Console,

1. Click **Devices**
2. Click **List View**
3. Click the **checkbox** next to the device you want to Enterprise Wipe
4. Click **More Actions**
5. Click **Enterprise Wipe**

Enter your security PIN [188]



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

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 Workspace ONE UEM 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:

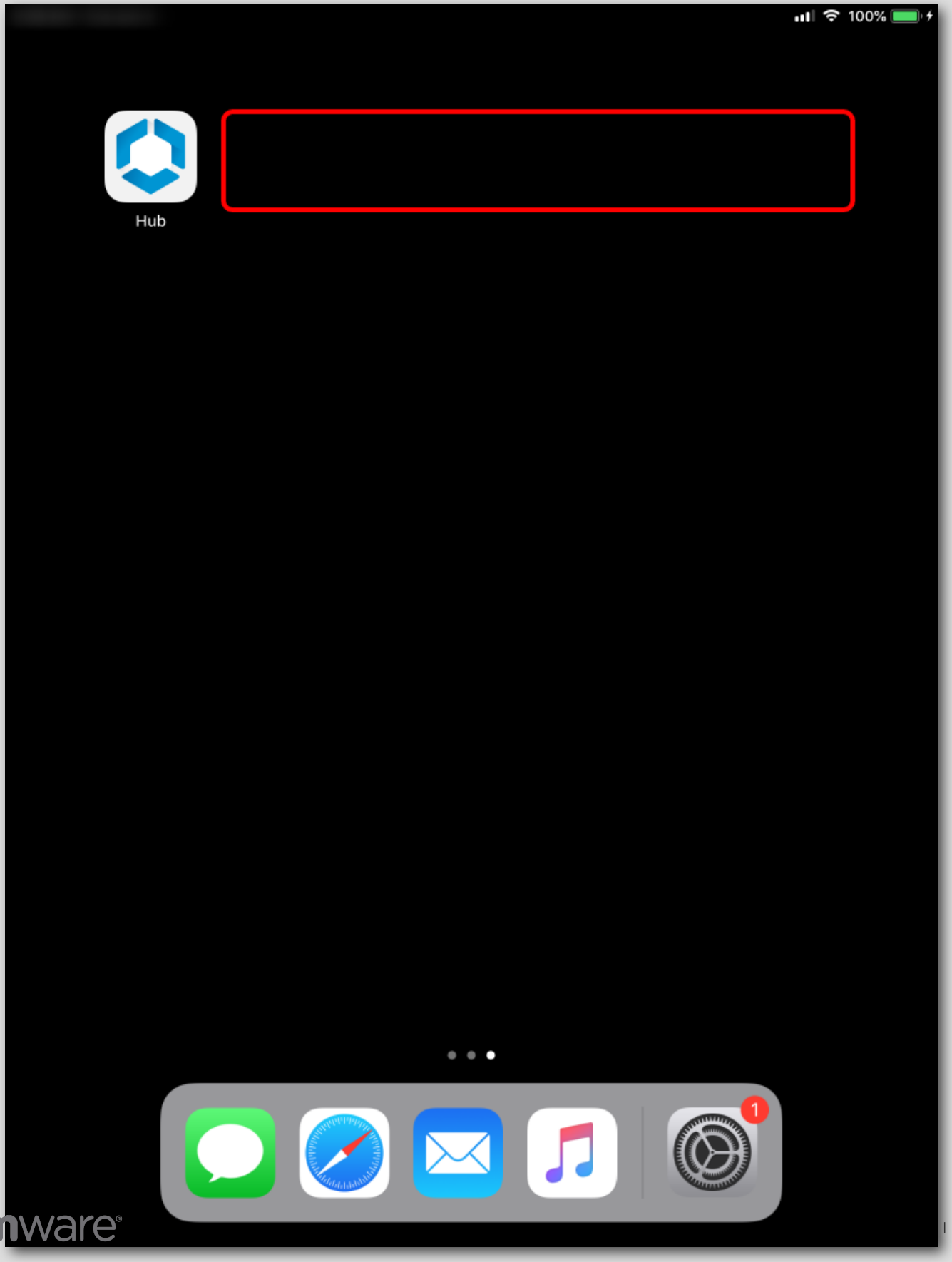
1. On your device, tap the **Workspace ONE Intelligent Hub** application
2. Tap **This Device**
3. Tap **Send Data** near the top of the screen. If this does not make the device check in and immediately un-enroll, continue to Step #4.
4. If the above doesn't make it immediately un-enroll, then tap **Connectivity [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 Workspace ONE UEM services from the device if network connectivity is failing.

Verify the Un-Enrollment

[189]

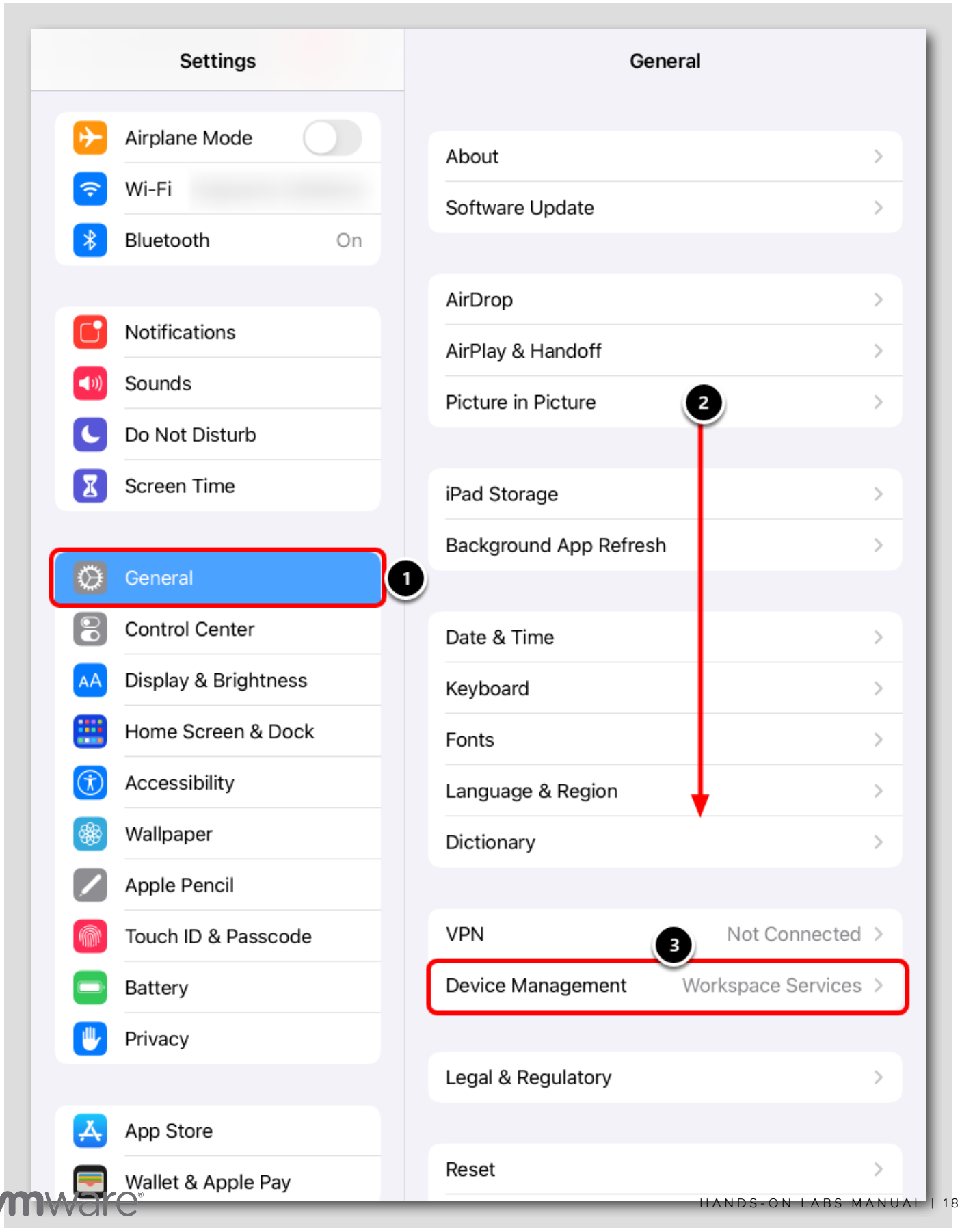

100%
Hub
1

Return to the device springboard. Notice that any applications pushed through Workspace ONE UEM have been removed from the device. In addition, navigating to Settings > General > Profiles will show that the Workspace Services profile has been removed from the device and any configurations pushed have been reverted.

NOTE: The Workspace ONE Intelligent Hub 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

[190]

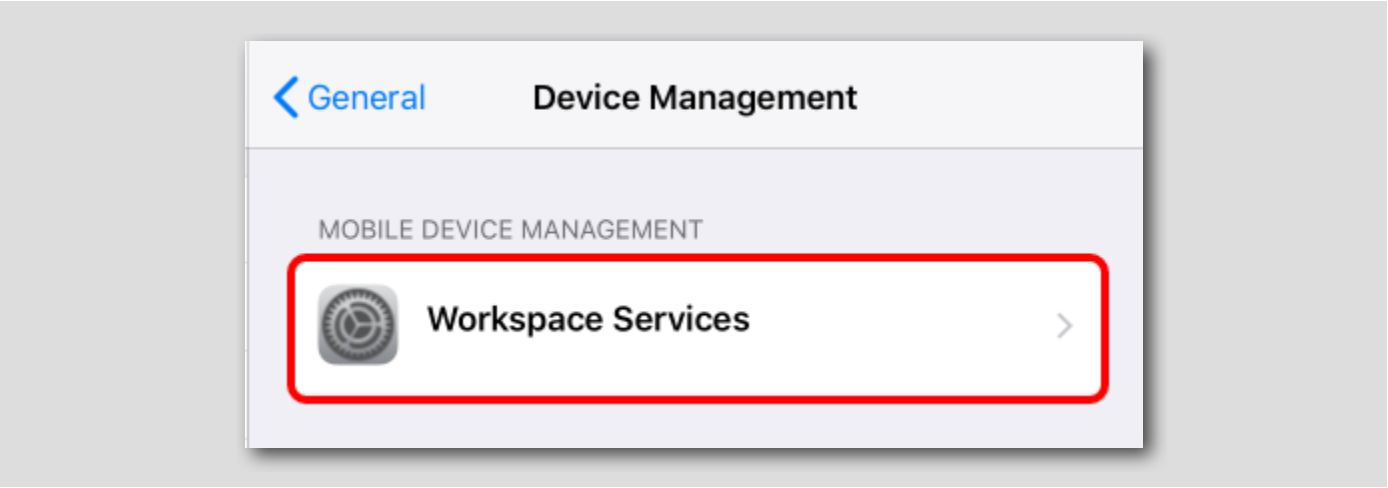

Settings
Airplane Mode
Wi-Fi
Bluetooth
On
Notifications
Sounds
Do Not Disturb
Screen Time
General
1
Control Center
Display & Brightness
Home Screen & Dock
Accessibility
Wallpaper
Apple Pencil
Touch ID & Passcode
Battery
Privacy
App Store
Wallet & Apple Pay
General
About
Software Update
AirDrop
AirPlay & Handoff
Picture in Picture
2
iPad Storage
Background App Refresh
Date & Time
Keyboard
Fonts
Language & Region
Dictionary
VPN
Not Connected
3
Device Management
Workspace Services
Legal & Regulatory
Reset

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

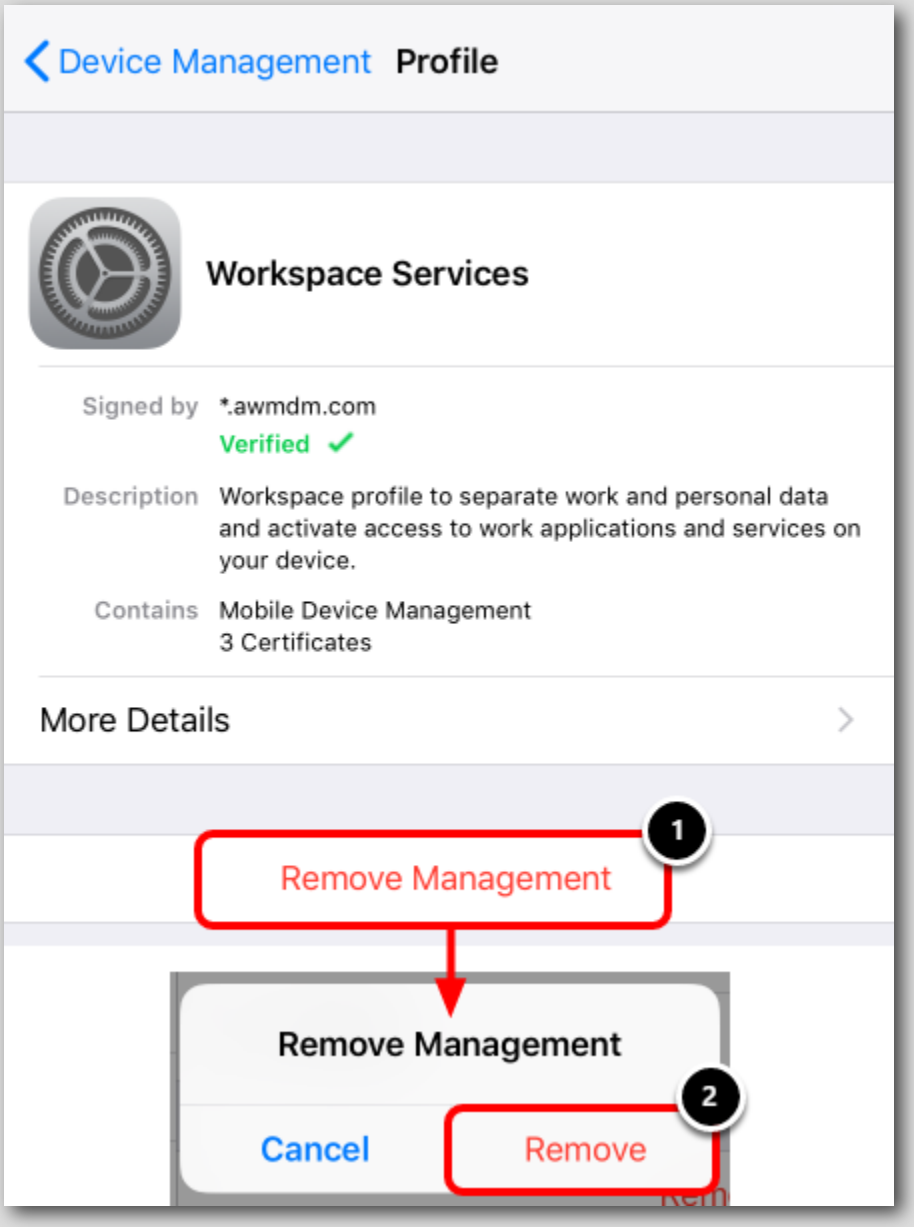
[191]



Tap the **Device Manager** profile that was pushed to the device.

Force the Wipe - IF NECESSARY

[192]



1. Tap **Remove Management** on the Workspace Services profile

   NOTE: If prompted for a device PIN, enter it to continue

2. Tap **Remove** on the Remove Management prompt

After removing the Device Manager 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.

Validate Device after Un-Enrolling

[193]

Once the device has unenrolled, the restrictions that you pushed to disable Siri will be removed but will not modify any other aspects of your device. Attempt to activate Siri again and confirm that Siri is now working.

Summary

[194]

Managing your devices with Workspace ONE UEM 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 and push a profile, consider exploring the other lab topics available in this module to further expand your Workspace ONE UEM knowledge.

This concludes the Introduction to Apple iOS Management module.

Note that this Hands-On Lab *does not* cover the full breadth and capabilities for managing iOS and tvOS with Workspace ONE. Please see VMware's TechZone for videos, blogs, and documentation that can help you with advanced topics in iOS/tvOS management, such as:

- Apple Business Manager and Automated Device Enrollment
- Device Staging and Enroll-on-Behalf
- Volume Purchased Application Deployment
- Kiosk Mode
- Certificates and Identity/Directory Integration
- Productivity Apps
- Check-In, Check-Out
- Unified App Catalog and Single Sign-On via Hub Services and VMware Access
- Apple Education Integration (e.g Apple School Manager
- … and More!

Level Up Your VMware End User Computing Knowledge with VMware Tech Zone

[195]

Interested in learning more about VMware End User Computing (EUC) but don't know where to start? Look no further than *https://techzone.vmware.com*, your fastest path to understanding, evaluating, and deploying VMware End User Computing products!

Tech Zone focuses on providing practical product guidance, curated activity paths, and technical content to take you from zero to hero! Our mission at Tech Zone is to provide you with the resources you need to keep leveling up your knowledge no matter where you are in your digital workspace journey.

Interested? Check us out at *https://techzone.vmware.com*!

Module 3 - Introduction to Apple macOS Management (45 minutes) Intermediate

Introduction

[197]

In this lab module, we will explore some Workspace ONE 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 to ensure you can successfully complete the lab.

Pre-Requisites

[198]

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

- An Apple device running macOS version 10.14.0 (Mojave) or later.

DO NOT Enroll Personal macOS Devices

[199]

IMPORTANT: You SHOULD NOT enroll a personal device for the upcoming exercise!

Personal devices may be enrolled into other UEM providers which can cause undesired conflicts and issues.

To complete this lab, we recommend you use a test device ONLY and avoid enrolling personal devices in the lab.

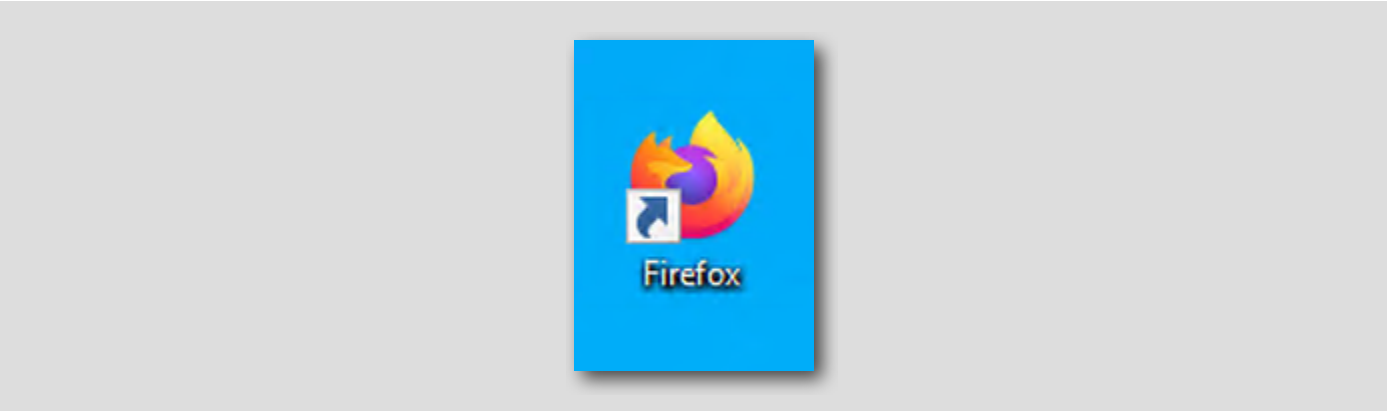
Login to the Workspace ONE UEM Console

[200]

To perform most of the lab, you will log into the Workspace ONE UEM Admin Console.

Launch Firefox Browser

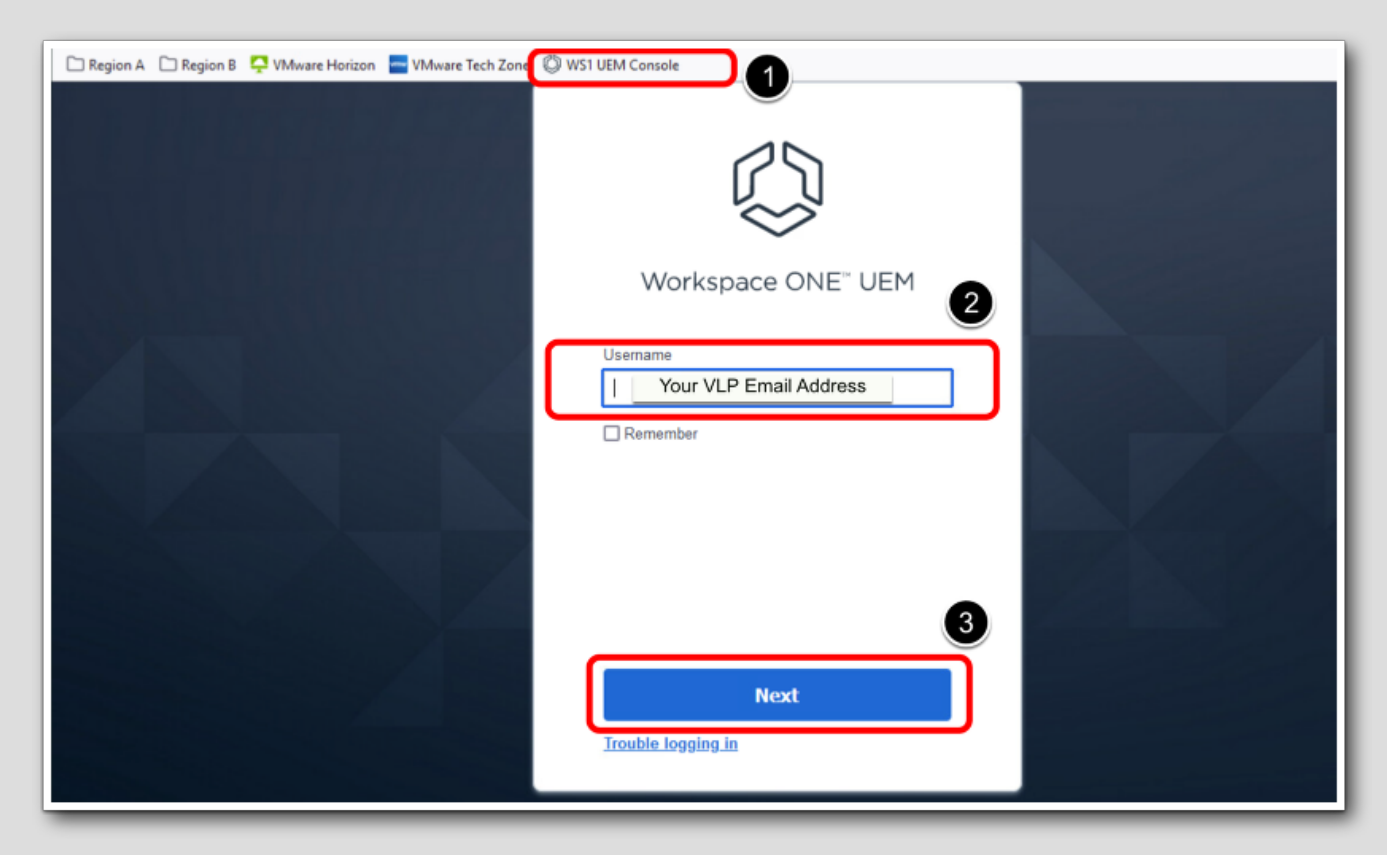
[201]



Double-click the **Firefox** shortcut located on the desktop of the virtual machine you are currently connected to.

Enter the Admin Username for the Workspace ONE UEM Admin Console

[202]

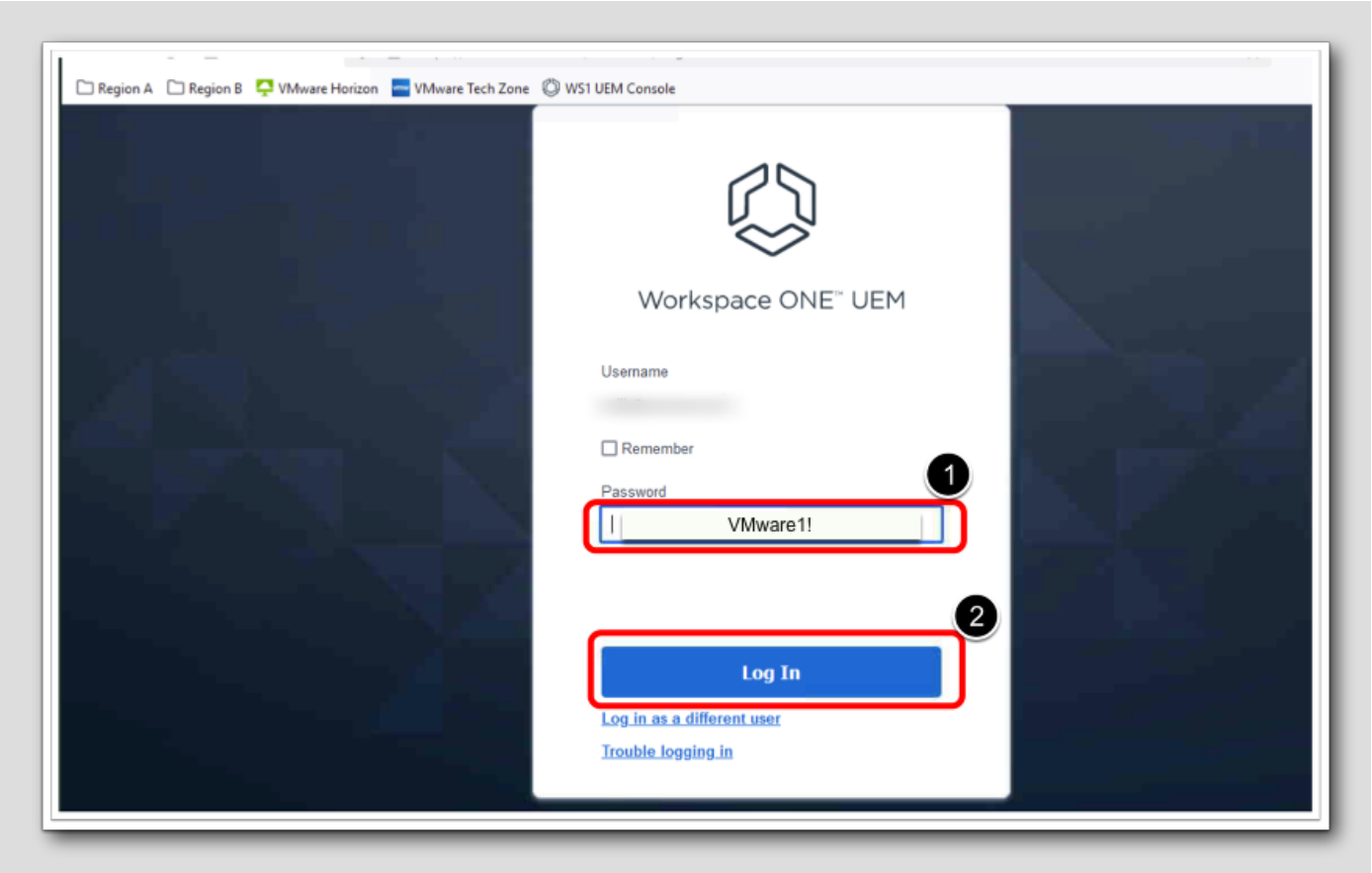


1. Select the **WS1 UEM Console** link from the Bookmark Toolbar
2. Enter your **Username**. This is the **email address** that you have associated with your **VMware Learning Platform (VLP)** account that you utilized to take Hands-on Labs.
3. Click **Next**, then advance to the next step of the lab manual to enter the password.

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

Authenticate to the Workspace ONE UEM Console

[203]



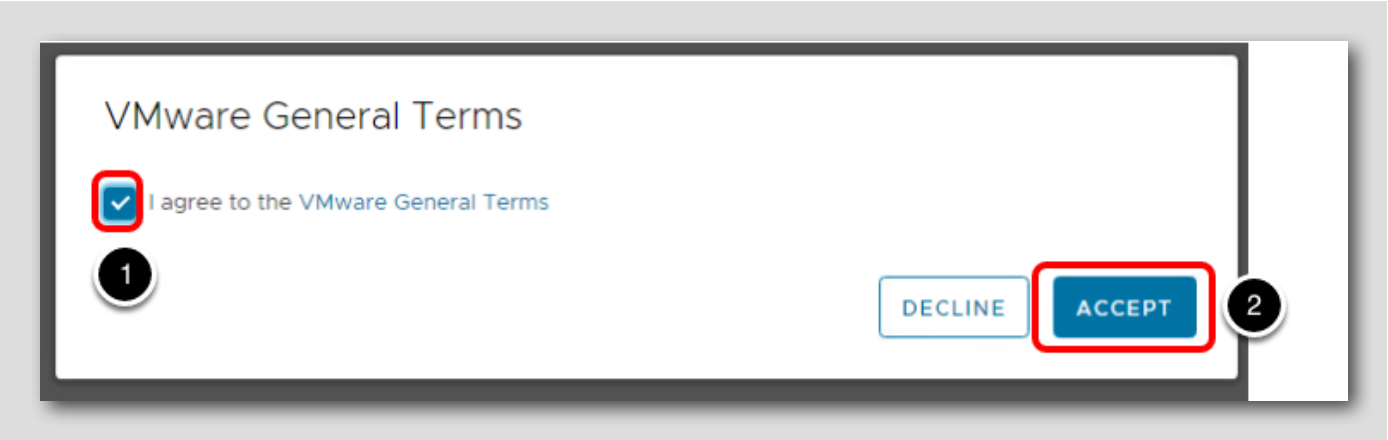
The password field will be displayed after entering your username.

1. Enter **VMware1!** for the Password field.
2. Click the Log In button.

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

Accept the VMware General Terms

[204]



You will be presented with the VMware General Terms.

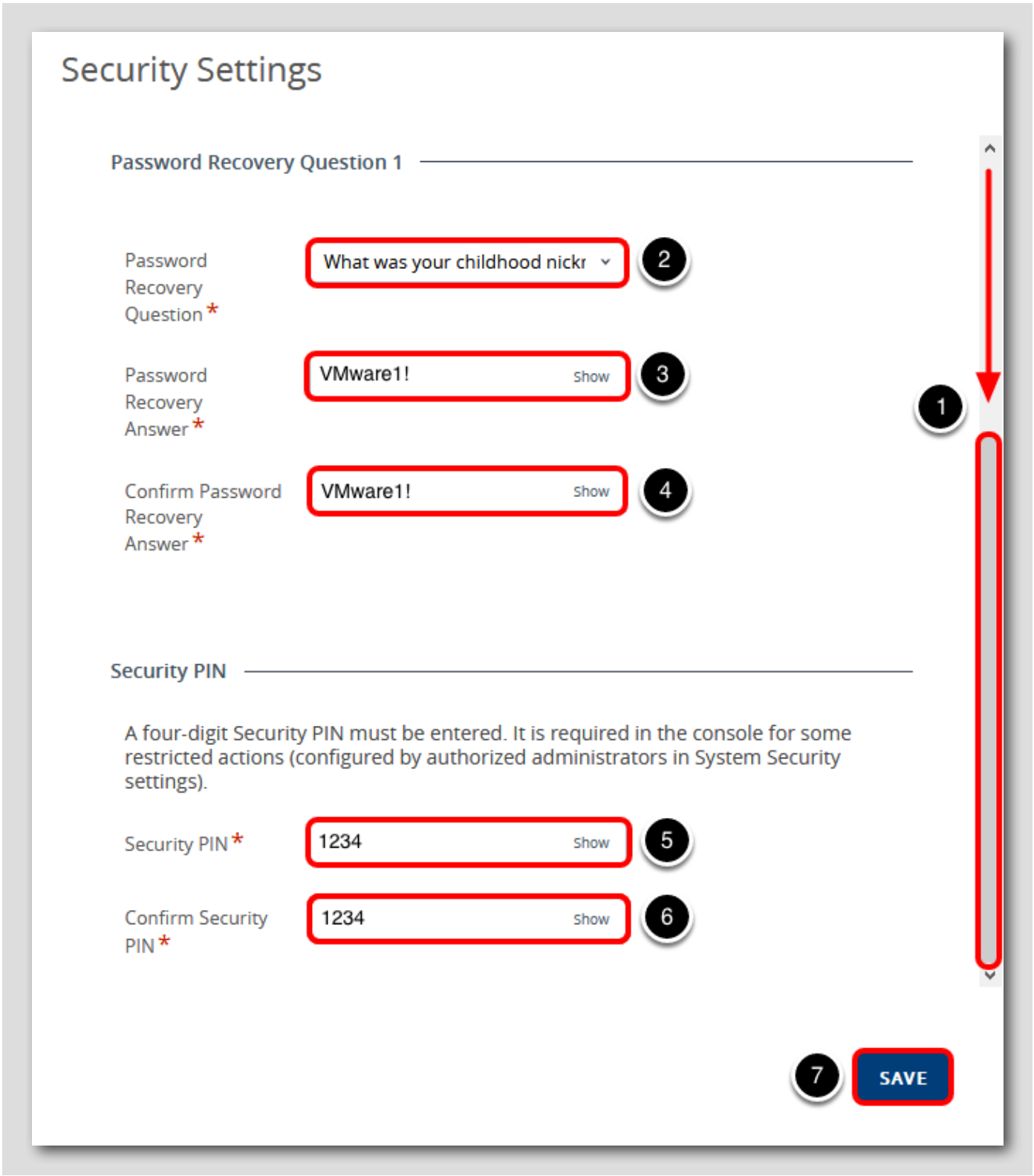
1. Select the box next to I Agree to the VMware General Terms.
2. Click the **Accept** button.

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

Address the Initial Security Settings

[205]

After accepting the Terms of Use, you will be presented with this **Security Settings** pop-up

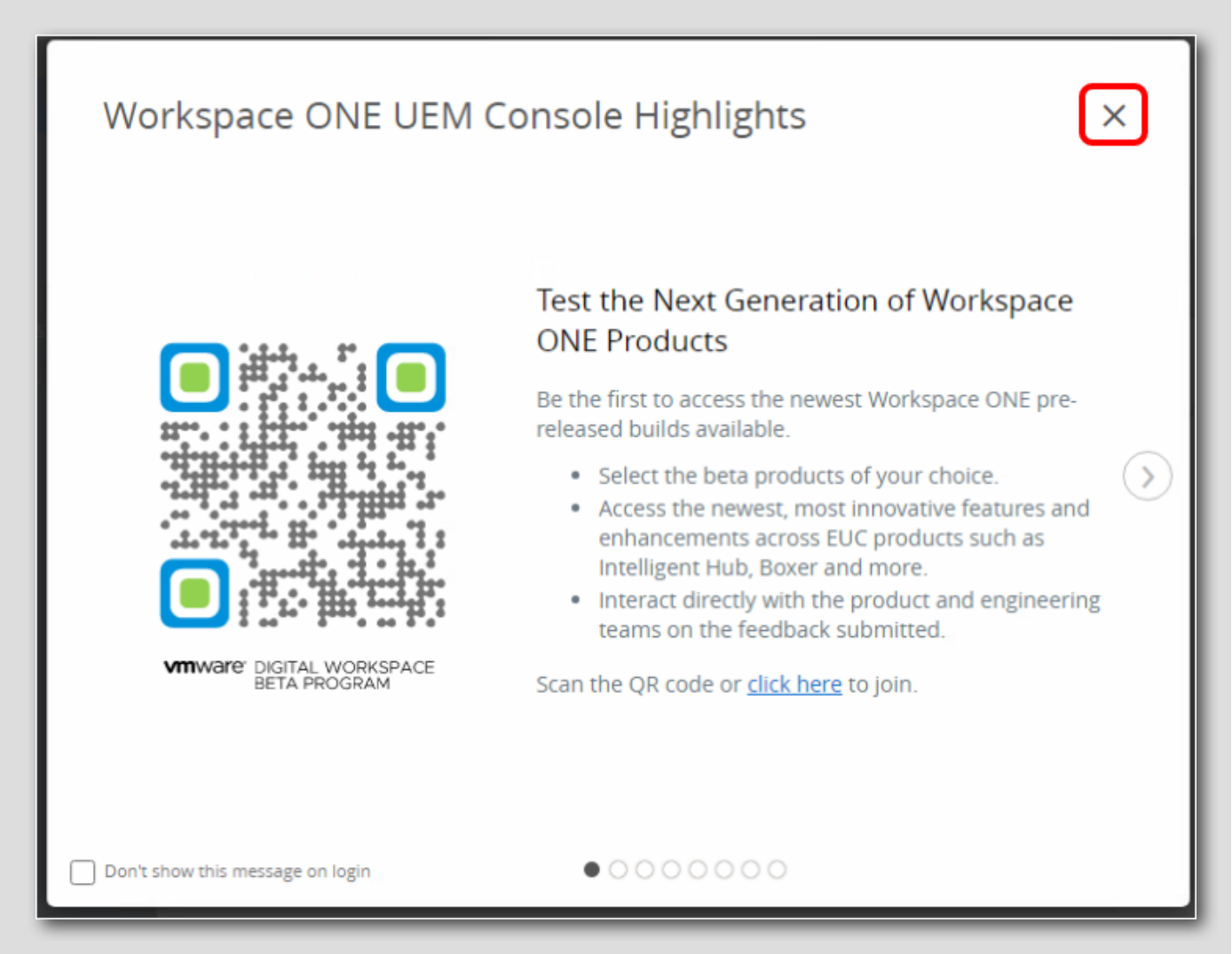

Security Settings
Password Recovery Question 1
Password Recovery Question *
What was your childhood nickr
2
Password Recovery Answer *
VMware1!
Show
3
1
Confirm Password Recovery Answer *
VMware1!
Show
4
Security PIN
A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).
Security PIN *
1234
Show
5
Confirm Security PIN *
1234
Show
6
7
SAVE

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.

Console Highlights

[206]



A popup window will appear after you complete your security questions.

Click the 'X' in the upper right corner to close the **Workspace ONE UEM Console Highlights** window.

Accessing Your Workspace ONE Access Tenant Details

[207]

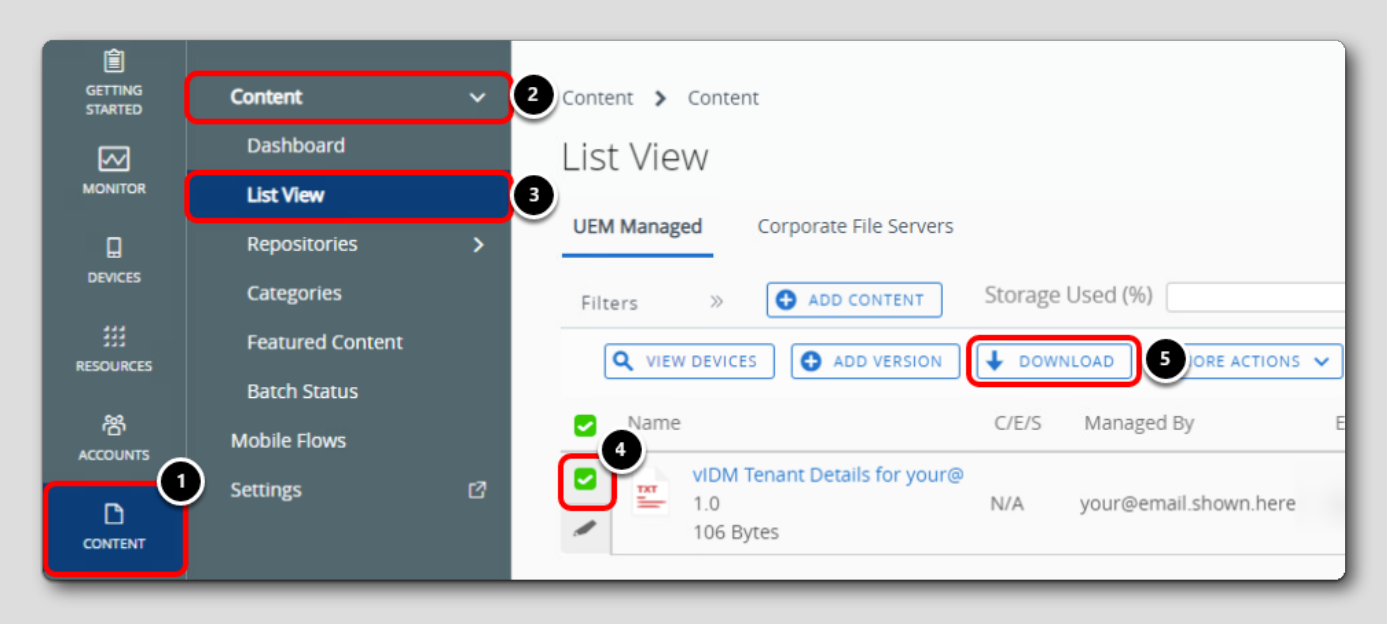
Workspace ONE Intelligent Hub end-user services are configured via the Hub Services admin console. Hub Services is co-located with Workspace ONE Access. Think of Hub Services as the server-side component and Intelligent Hub as the end-user client.

The following sections will guide you through accessing your Workspace ONE Access tenant, logging in, then accessing the Hub Services admin console.

Accessing Your Workspace ONE Access Tenant Details in the UEM Console

[208]

A temporary Workspace ONE Access tenant has been generated for you to use throughout this lab. The Workspace ONE Access tenant URL and login details were uploaded to the Content section in the Workspace ONE UEM Console at the start of the lab.

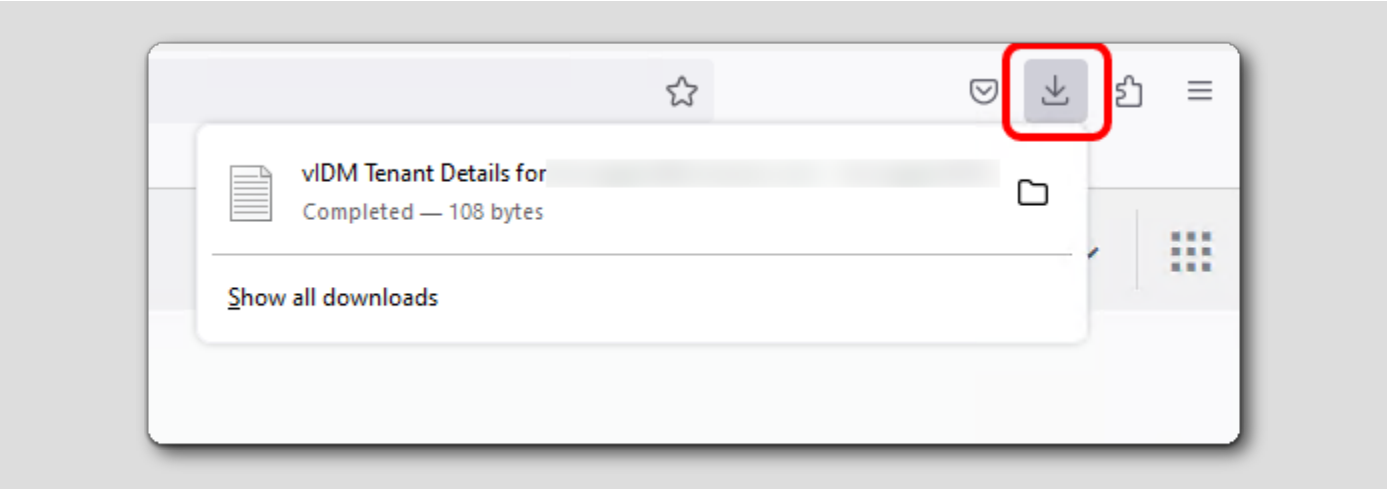


In the Workspace ONE UEM Console:

1. Click **Content** on the far left
2. Expand **Content** at the top
3. Click **List View**
4. Find the text file named **`vIDM Tenant Details for your@email.shown.here.txt`** and click the checkbox beside it to select the file
5. Click **Download**

Open the Downloaded Text File

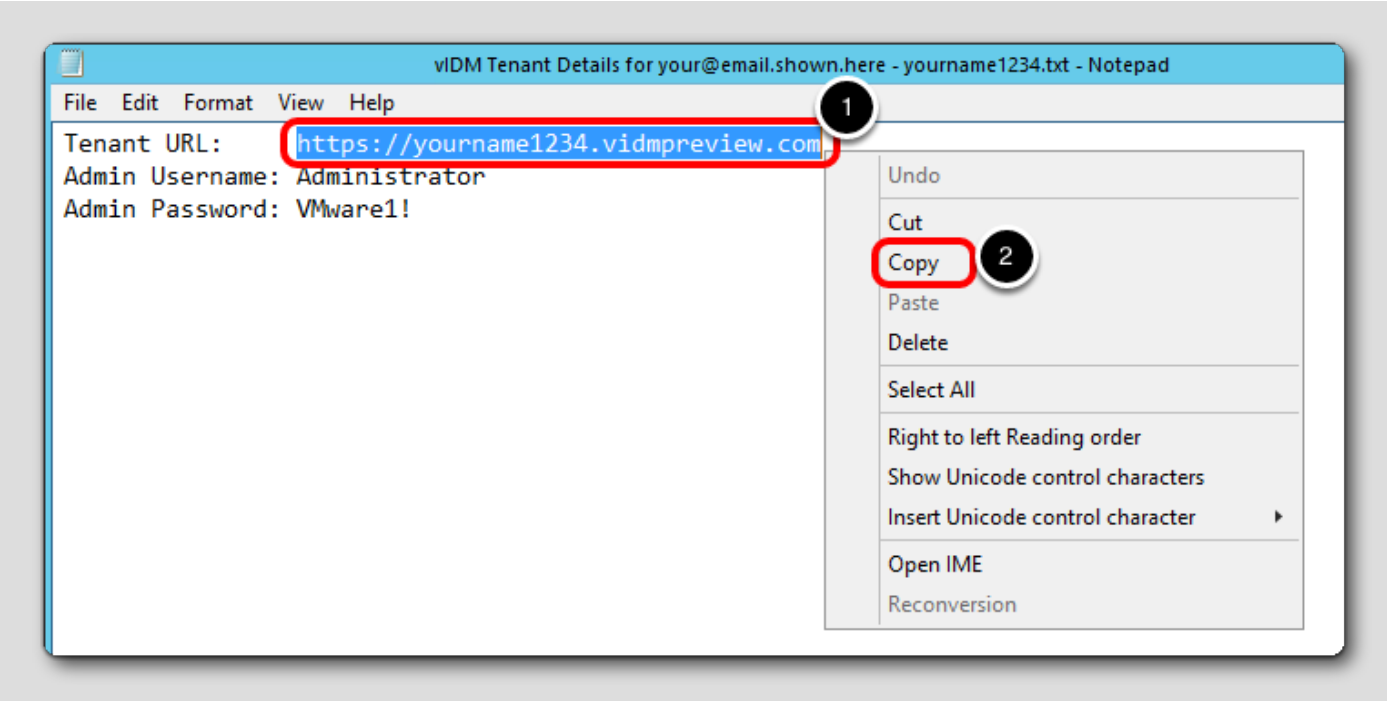
[209]



After the file downloads, click the **vIDM Tenant Details for your@email.shown.here.txt** file from the download bar to open it.

Copy the Tenant URL

[210]



1. Select the **Tenant URL** text and **right-click**
2. Click **Copy**

NOTE: Your tenant name will match your Group ID in the Workspace ONE UEM Console and will be entered in the UEM console in an upcoming step.

Activate Hub Services

[211]

The activation flow for Hub Services depends on whether you are a new customer or an existing customer.

New Customers to Workspace ONE

[212]

New cloud customers who purchased Workspace ONE after January 2019 have Hub Services activated automatically as part of the instance provisioning process. Workspace ONE UEM, Workspace ONE Access, and Hub Services consoles are connected together, and the Hub catalog is enabled for the Intelligent Hub app.

Existing Cloud Workspace ONE UEM Customers

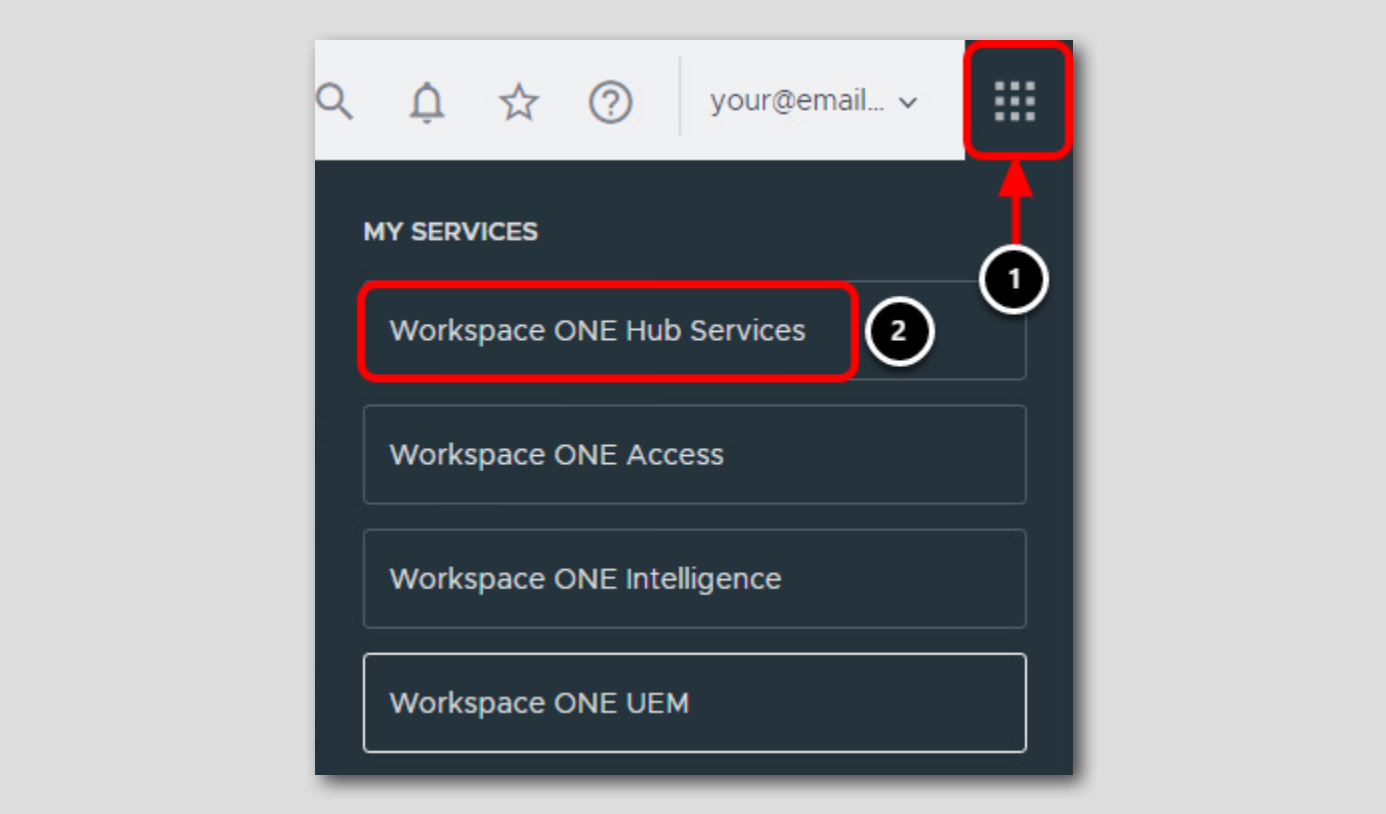
[213]

Existing customers can configure Workspace ONE Access tenant URL, tenant admin username and password to activate Hub Services. If you do not have a Workspace ONE Access tenant, you can request one from the Workspace ONE UEM administrator console itself, using the Request a Cloud Tenant button.

For this lab, we have already provided you a Workspace ONE Access tenant which we will use in the next step to active Hub Services.

Navigate to Workspace ONE Hub Services

[214]

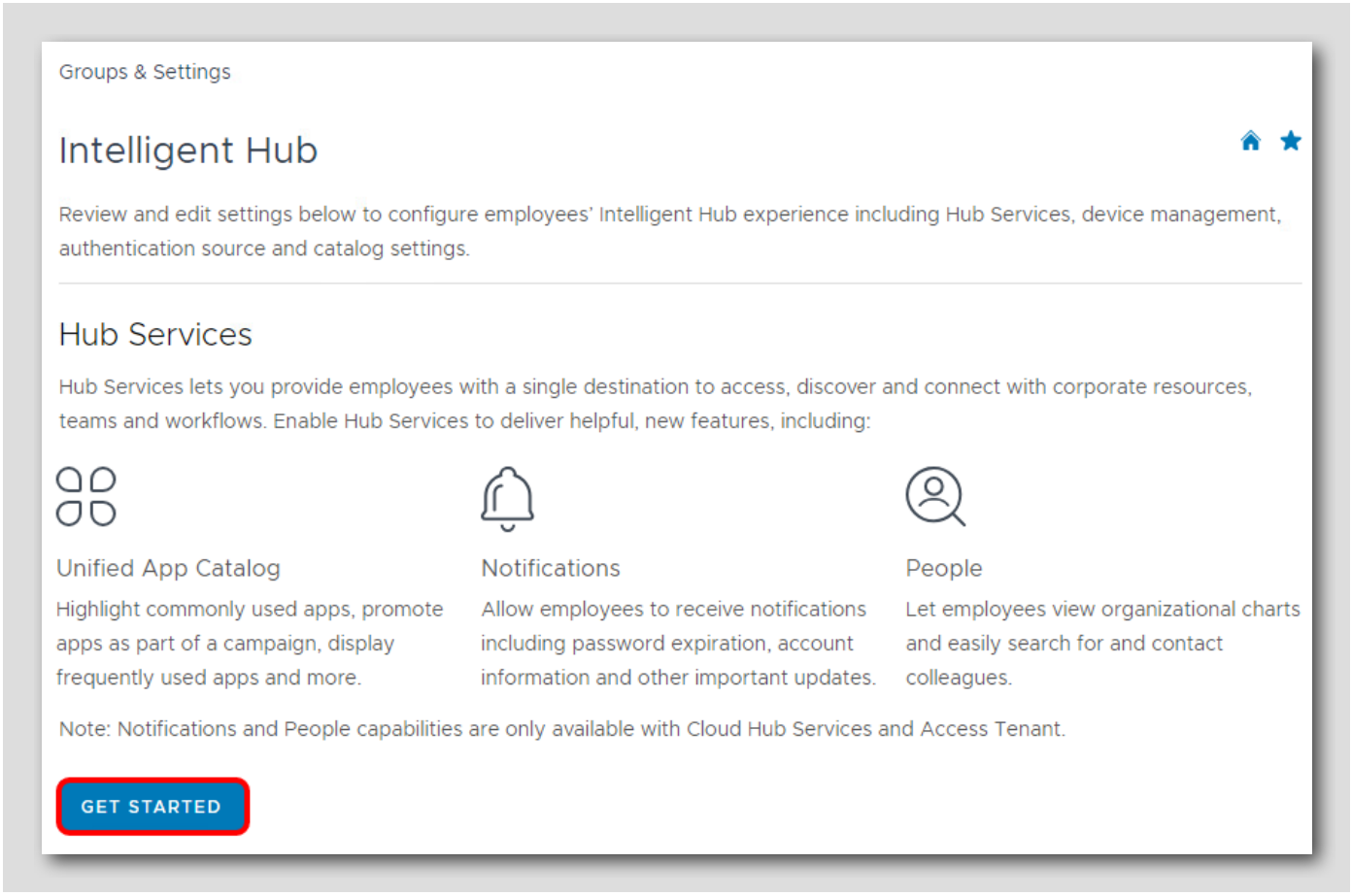


Return to the UEM console in the Firefox browser.

1. Click the **My Services** button
2. Click on **Workspace ONE Hub Services**

Get Started

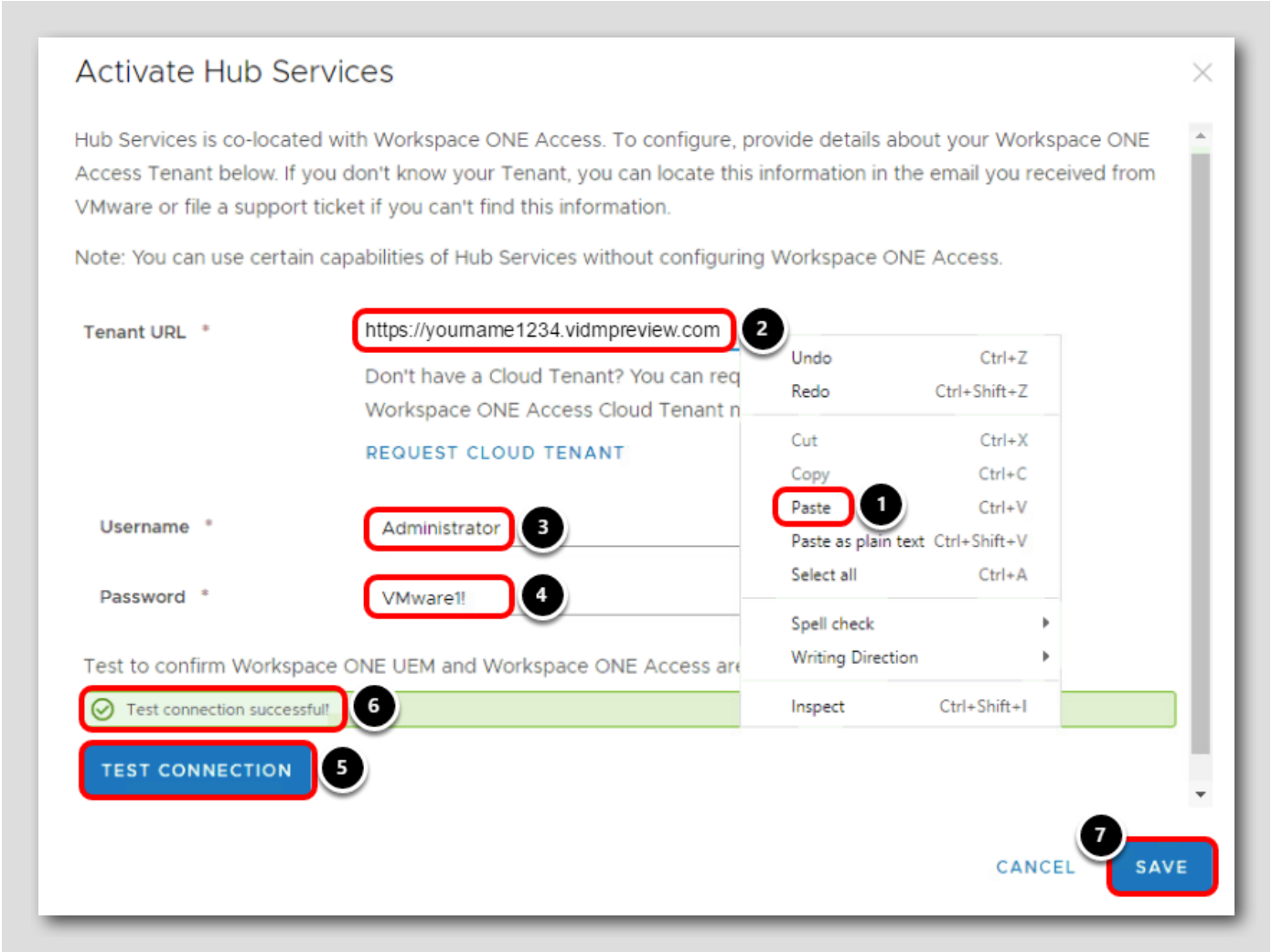
[215]



Click **Get Started** to begin the Hub Services activation process.

Activate Hub Services

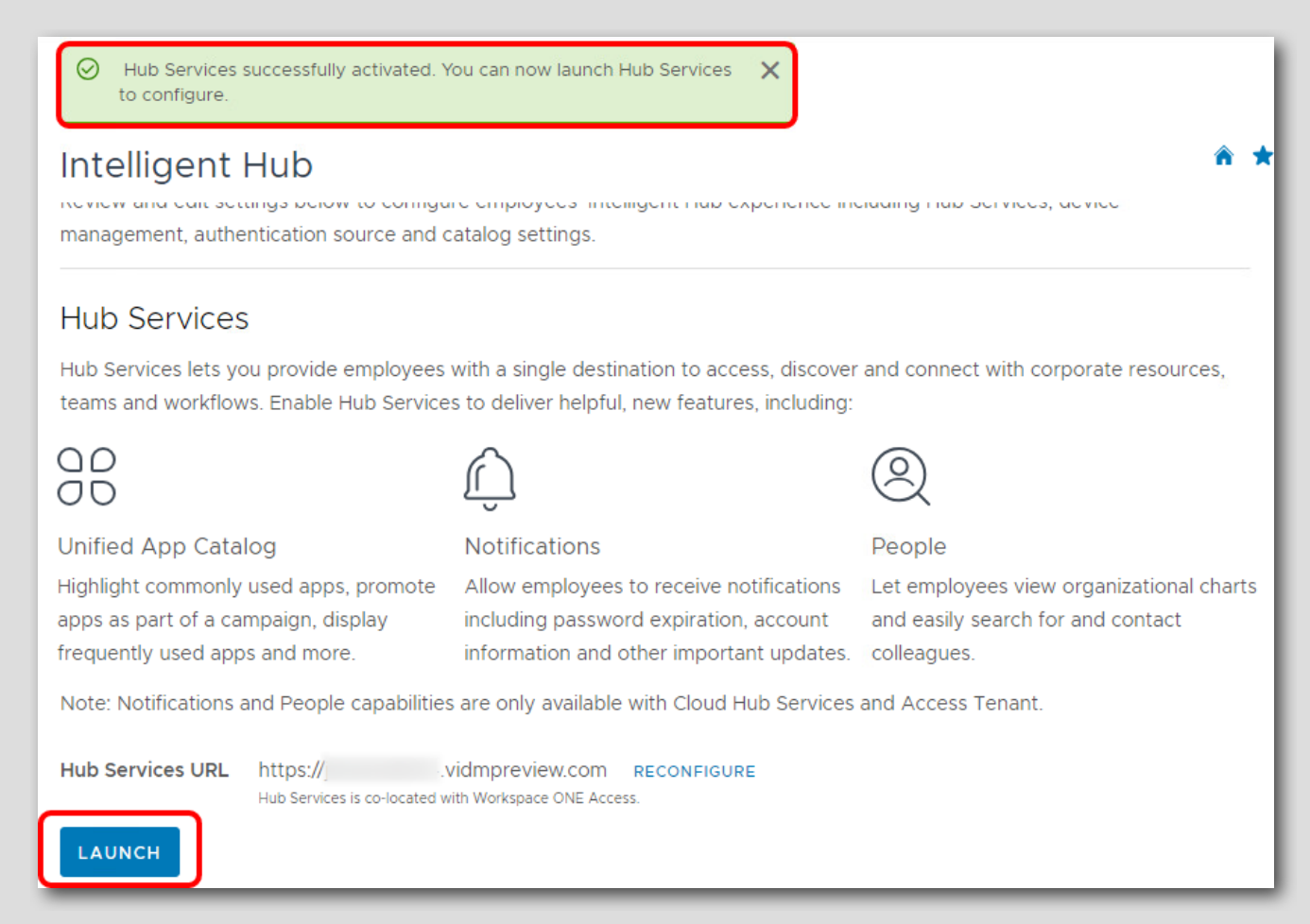
[216]



1. Right-click in the Tenant URL field and click **Paste**
2. Ensure that you have entered the URL from the notepad file you downloaded in the earlier step. If the clipboard is blank or carrying some other value, go back and copy the tenant URL from the notepad file you downloaded earlier.
3. Enter **`Administrator`** for the username
4. Enter **`VMware1!`** for the password
5. Click **Test Connection**
6. Ensure that the the success message **Test Connection Successful!** is displayed
7. Click **Save** to continue

Launch Hub Services

[217]



Ensure that the message confirming Hub Services has been successfully activated is displayed. You have now successfully Activated Hub Services for your tenant!

Activate macOS Hub App Catalog

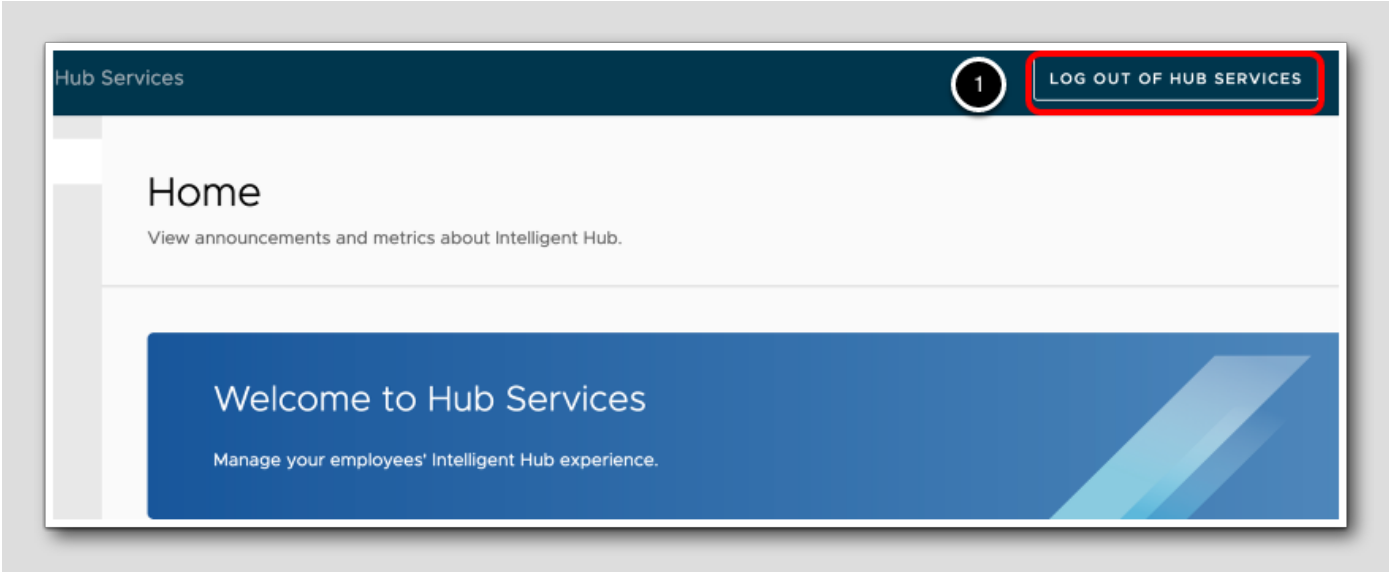
[218]

When you activate Hub Services with your Workspace ONE UEM tenant, the unified app catalog available in Hub Services will be used in the Intelligent Hub app on enrolled devices. One additional setting is needed to activate the modern unified app catalog with Hub Services - you will need to disable the legacy catalog for macOS.

In this section, you are going to activate the Hub App Catalog for macOS.

Log Out of Hub Services

[219]



1. Click **Log out of Hub Services**

Navigate to Catalog Settings

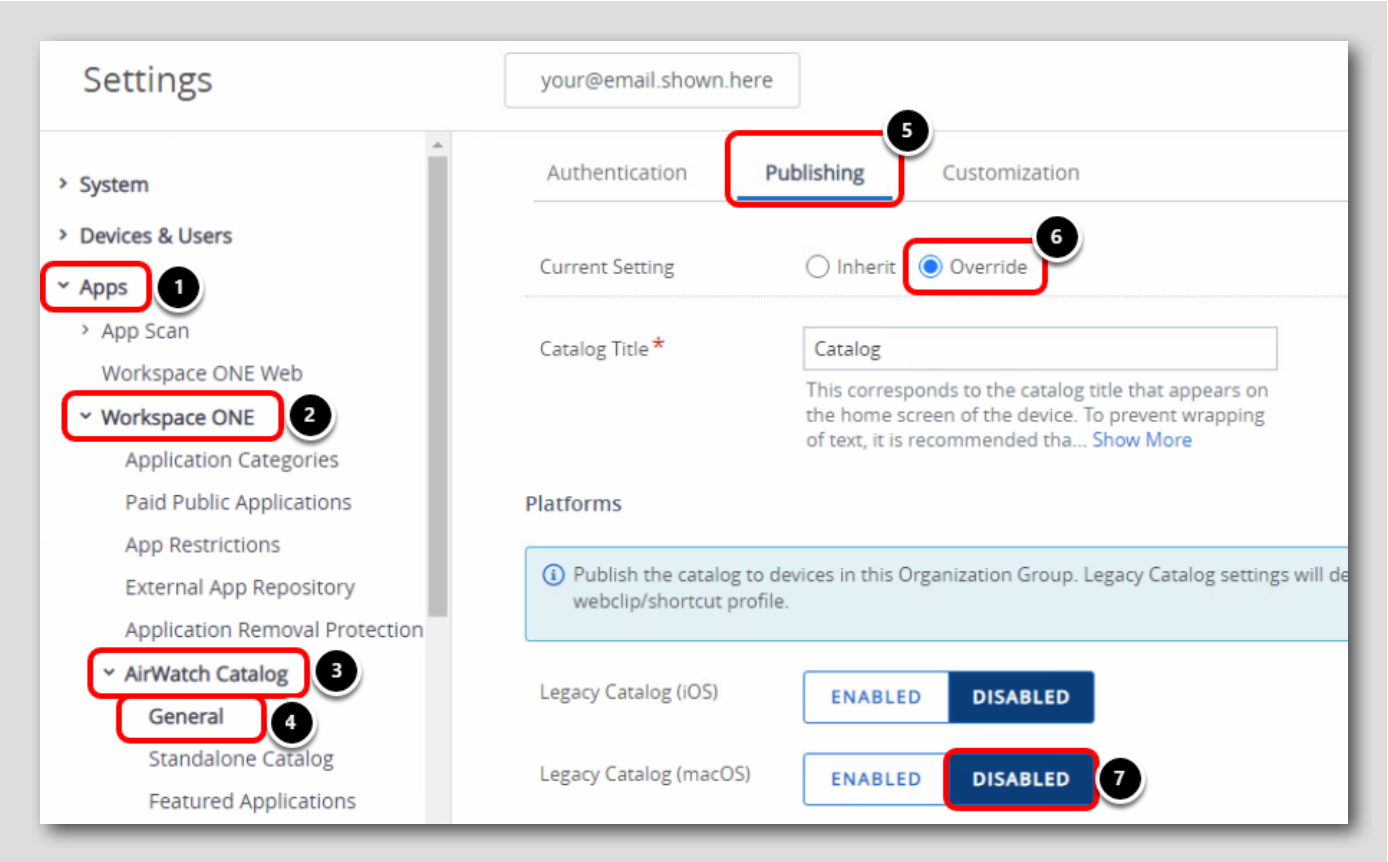
[220]

In the Workspace ONE UEM Console

1. Click **Groups & Settings**
2. Click **All Settings**

Override the Legacy Catalog Settings

[221]

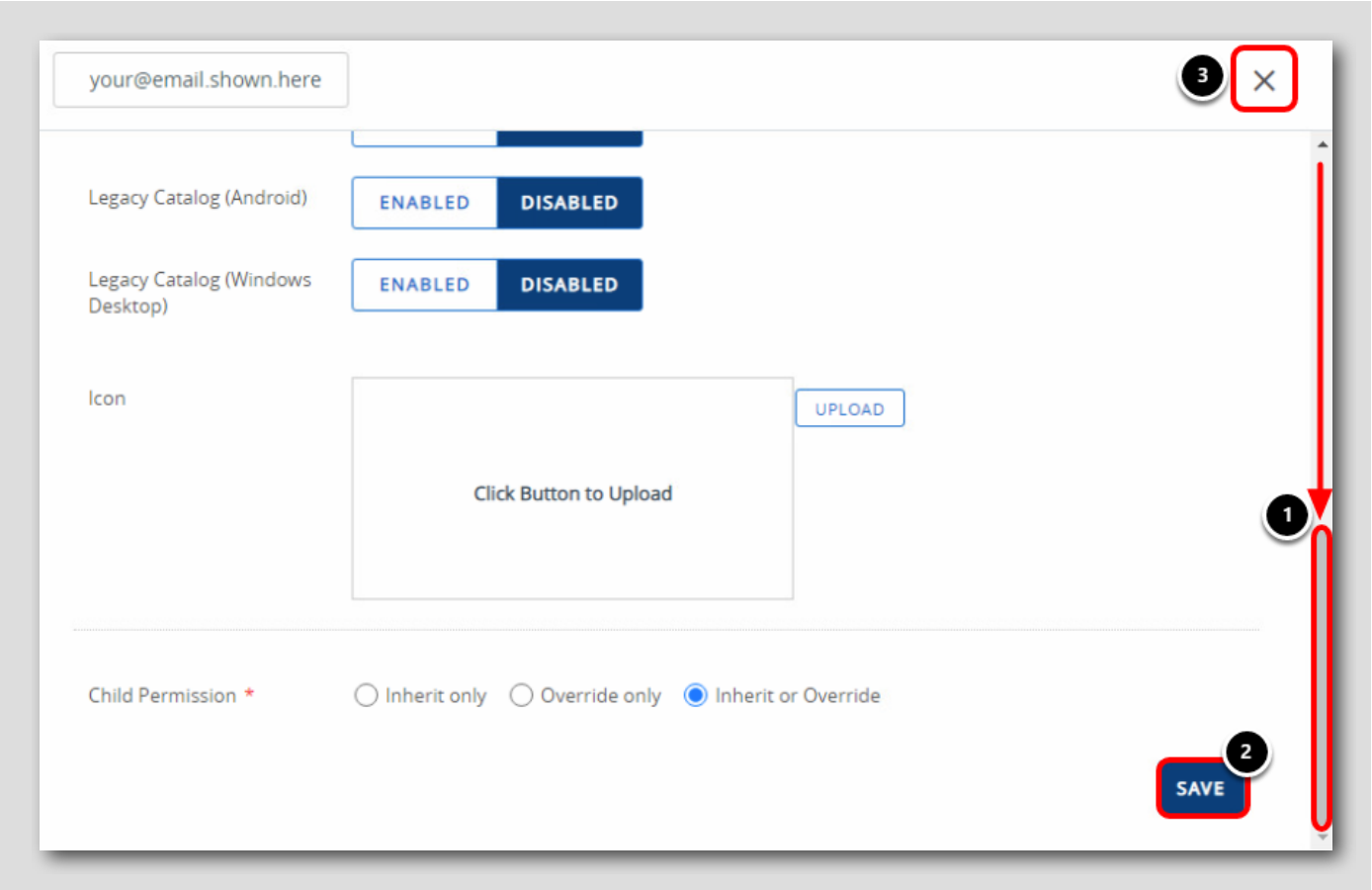


1. Click **Apps**
2. Click **Workspace ONE**
3. Click **AirWatch Catalog**
4. Click **General**
5. Click **Publishing**
6. Select **Override** for Current Setting
7. Select **Disabled** for Legacy Catalog (macOS)

This will disable the older web clip based Catalog for the macOS platform. Instead, users will receive the new Hub App Catalog which provides an updated app catalog with richer features, but also includes features such as notifications, people search, a custom home page, and more.

Save Changes

[222]



1. Scroll down to the bottom
2. Click **Save**
3. Click the **X** to close the Settings window

Create Profiles

[223]

This exercise explores how to modify the macOS device behavior using Profiles.

Profiles are the mechanism by which Workspace ONE UEM 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.

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.

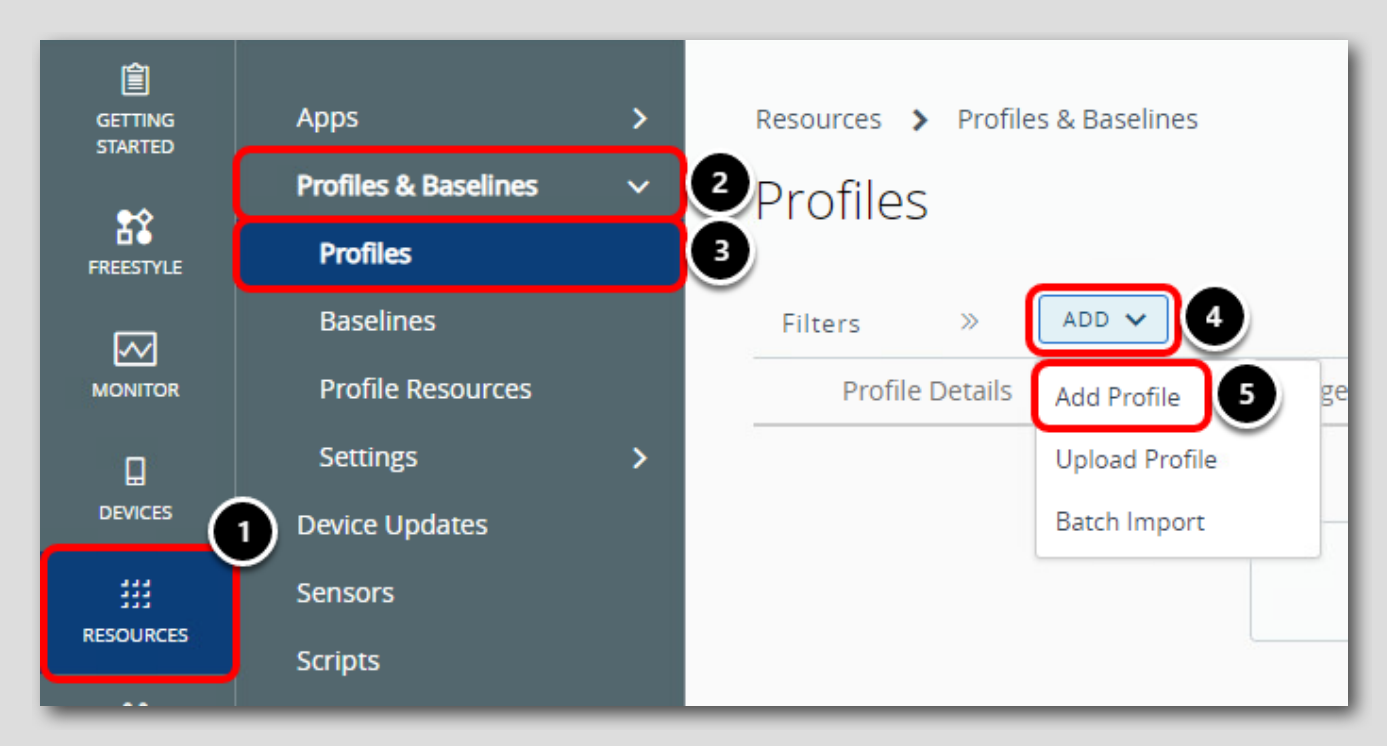
Every Profile must have all required fields in the General section properly filled out and at least one payload configured.

Device Profiles are typically used to control settings that apply system-wide. Device profiles can include items such as VPN and Wi-Fi configurations, Global HTTP Proxy, Disk Encryption, and/or Directory (LDAP) integration.

In this exercise, you will create a profile that disables various macOS System Preferences from being changed by the end user.

Add a macOS Profile

[224]

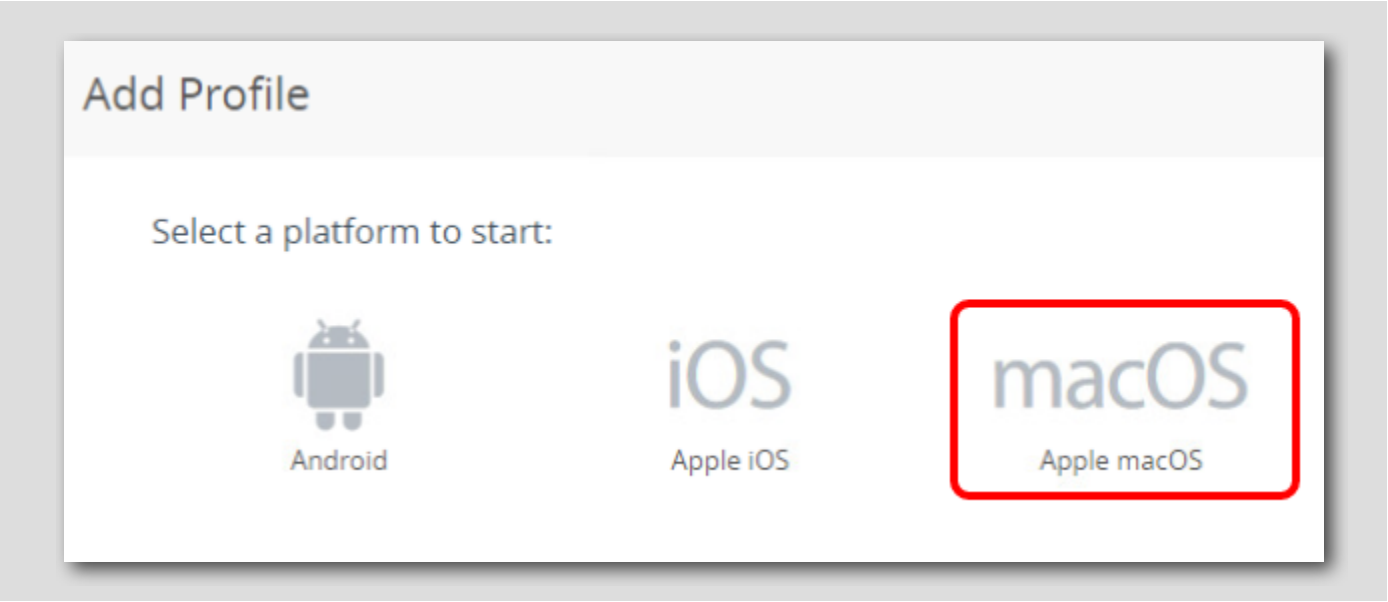


Return to the Workspace ONE UEM administration console in Google Chrome:

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

Select Profile Platform

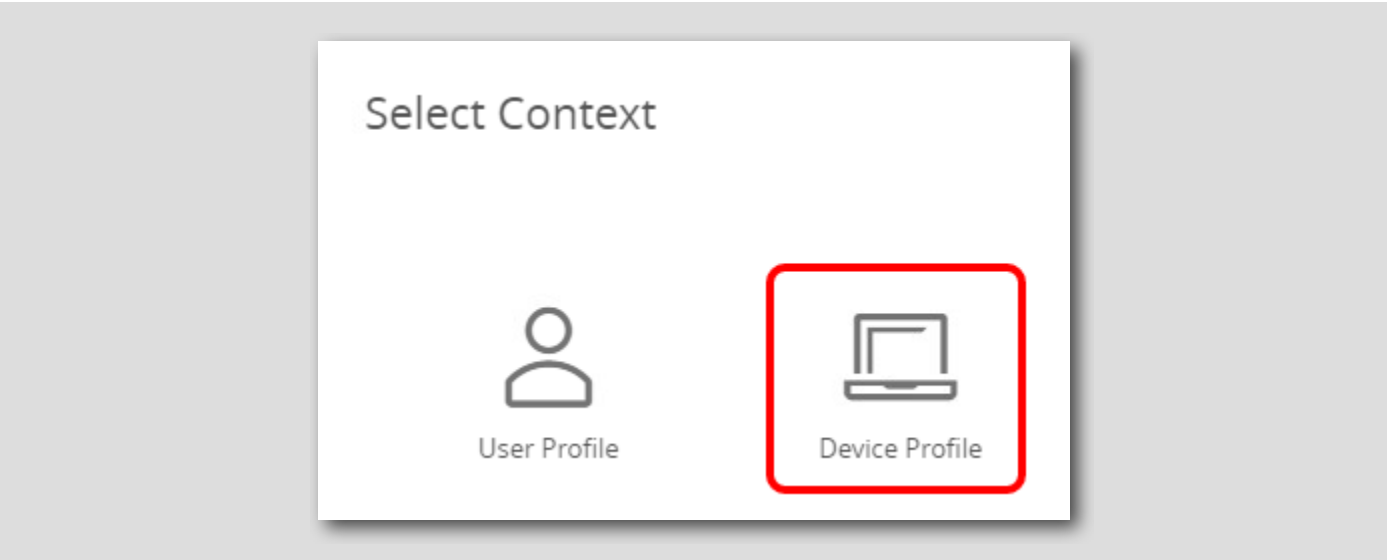
[225]



Click **macOS**.

Select the Profile Context

[226]

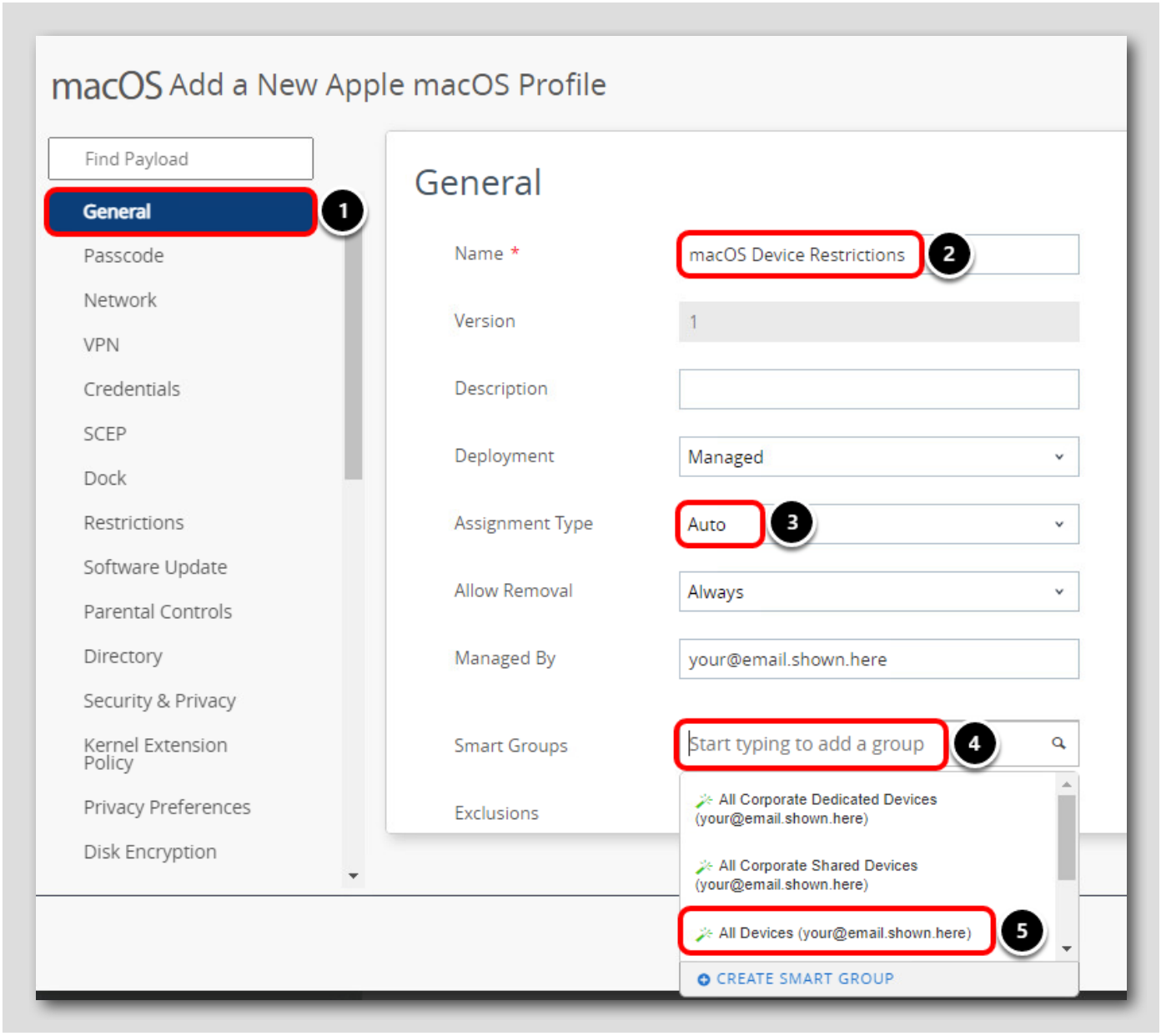


There are two contexts for Profiles: User and Device. User Profiles will apply the configuration to only the logged in user on the device. Device Profiles will apply the configuration to the entire device.

Click **Device Profile**.

Configure General Payload

[227]



Configure the device profile as follows:

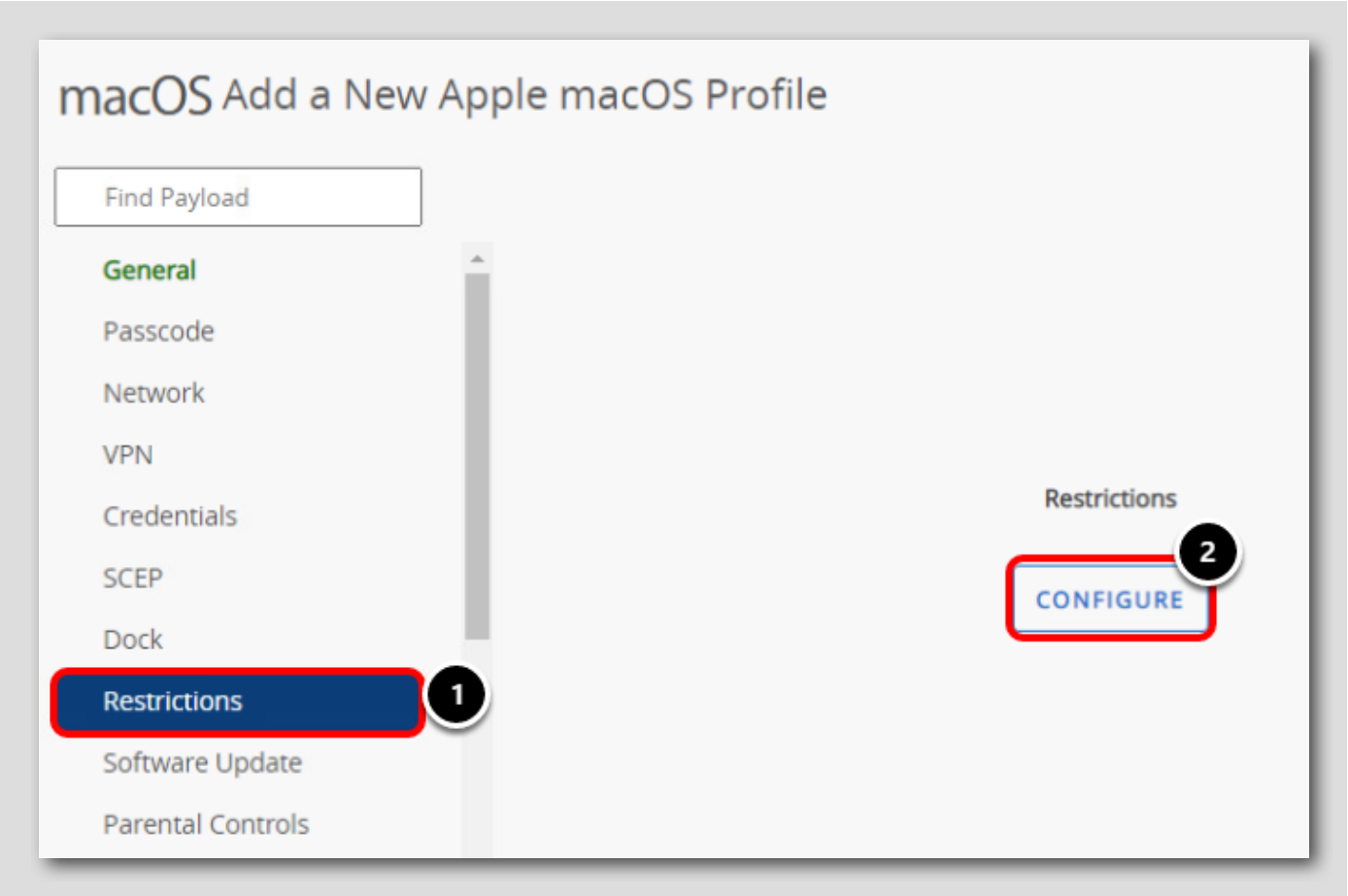
1. Select the **General** payload if not already selected
2. Enter **`macOS Device Restrictions`** for the profile name
3. Confirm **Auto** is selected for the Assignment Type
4. Scroll down to view the Smart Groups field and click in the search box
5. Select the **All Devices (your@email.shown.here)** group from the list

Each tab on the left is a "Payload". These represent different features or restrictions you can configure on the device with the selected platform and context of the Profile. You may have more than one Payload per Profile, but it is best practice to generally keep one Payload per Profile (excluding the General payload, which is required).

The configurations you have made with create a macOS device context profile that will be automatically assigned and applied to any macOS device that enrolls in your organization group.

Add the Restrictions Payload

[228]

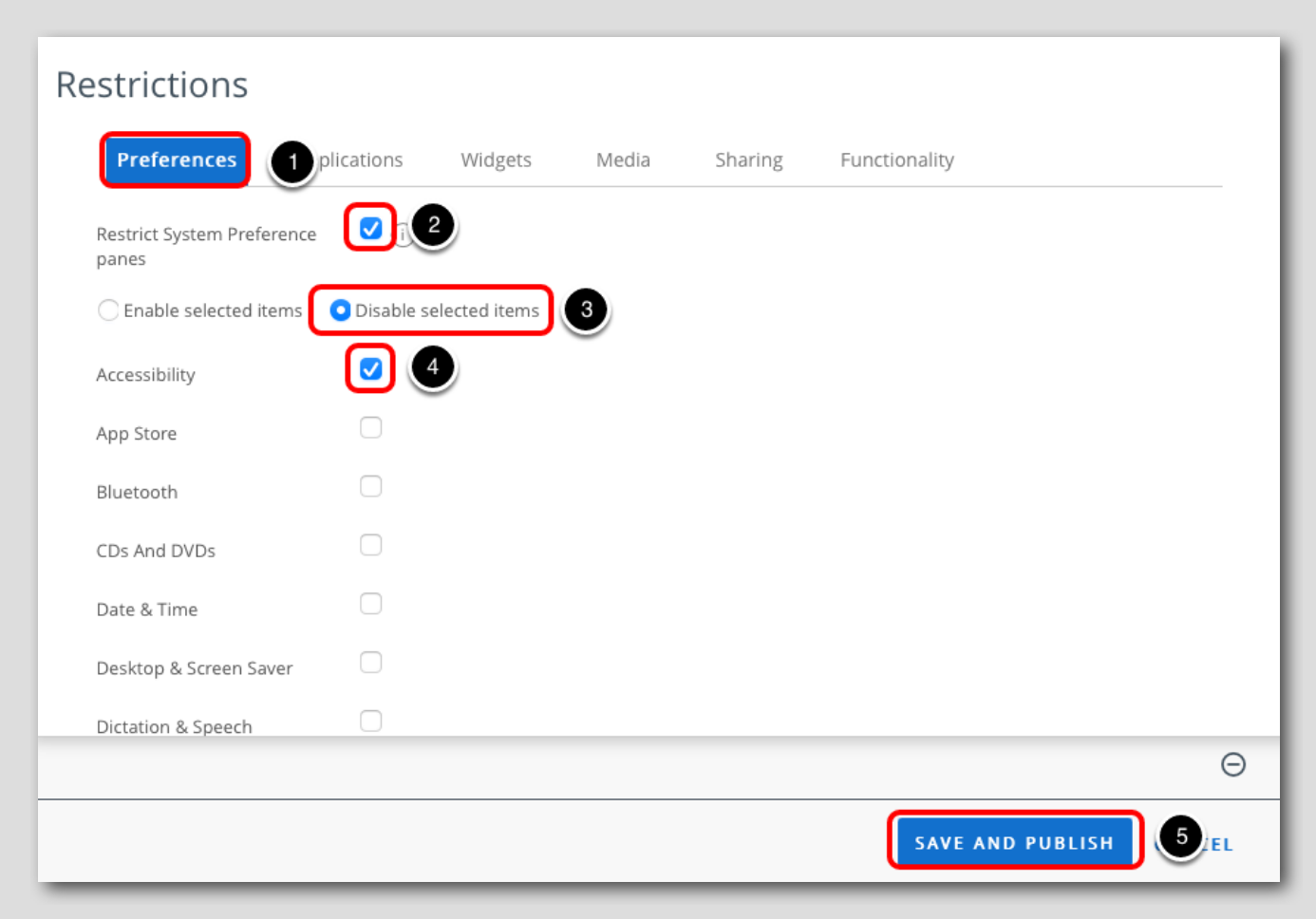


1. Click the **Restrictions** payload
2. Click **Configure**

Clicking Configure will add the Restrictions payload to the Profile and allow you to determine what restrictions will be applied to the macOS device with this Profile.

Configure the Restrictions Payload

[229]

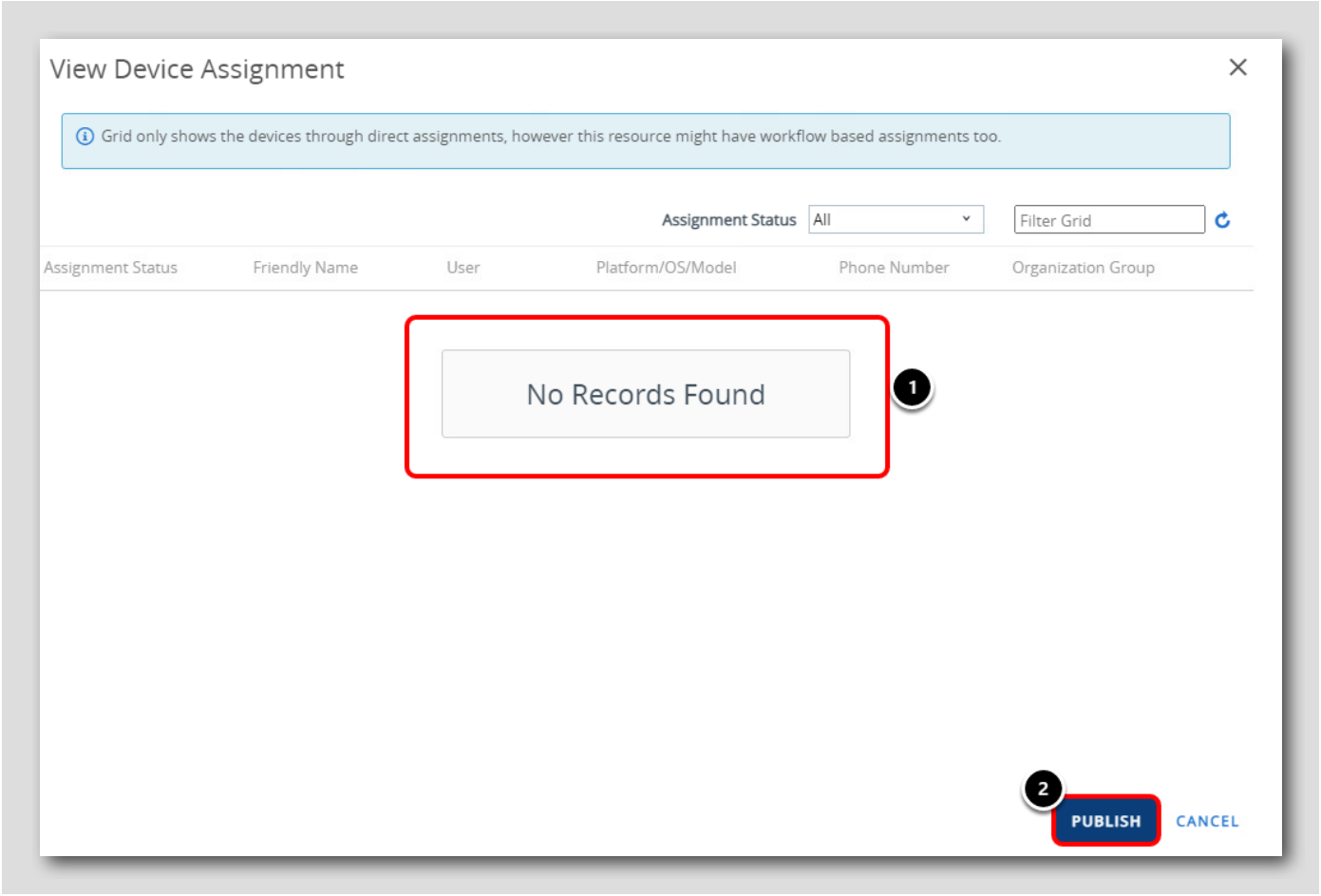


1. Click the **Preferences** tab
2. **Enable** the Restrict System Preference panes checkbox
3. Select **Disable Selected Items**
4. Enable the **Accessibility** checkbox
5. Click **Save & Publish**

This will prevent the end users from being able to access or change the Accessibility settings under System Preferences.

Preview and Publish Profile

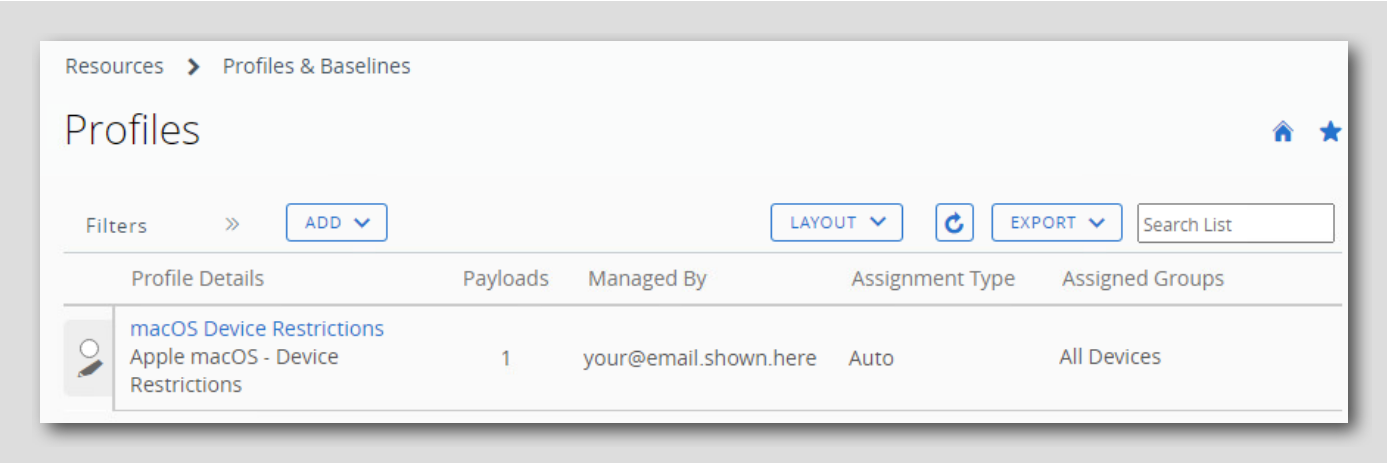
[230]



1. Normally, a list of devices that would receive this configuration would be displayed here. Since you have not enrolled a macOS device yet, no devices are displayed.
2. Click **Publish**.

Confirm the Profile was Created

[231]



The macOS Device Restrictions profile is now added to the list of Profiles in your organization group. You can see how many Payloads (excluding General) are configured, the assignment type, and assigned groups. If you need to edit the Profile, you would return to this view in order to make changes.

This Restrictions profile is now published and will be automatically assigned to any macOS device that enrolls in your organization group. You will confirm this Restrictions profile is applying on the device after enrolling a device in a later step.

Create Sensors

[232]

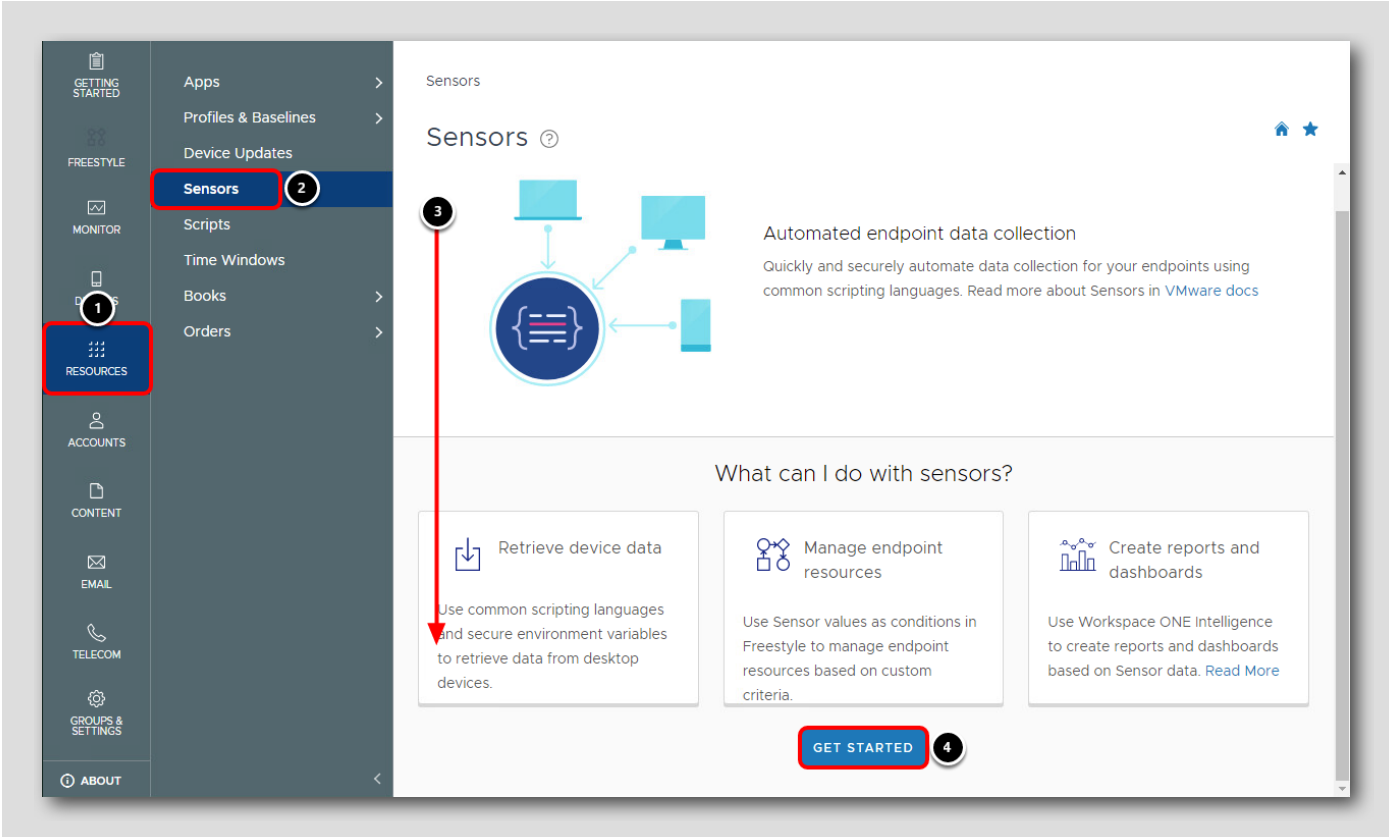
Sensors allow you to quickly and securely automate data collection from your endpoints with common scripting languages. macOS Sensors supports Bash, Python 3, and Zsh, and Windows Desktops support PowerShell.

This collected data can be used as conditions in the Freestyle Orchestrator feature to take action based on the condition and value of this data. You can learn more about Freestyle Orchestrator in *Module 1 - Introduction to Freestyle Orchestrator*. You can also use Workspace ONE Intelligence to create reports and dashboards based on your Sensor data.

In this section, you will create a Sensor for macOS which will query the type of processor that is used on the device.

Navigate to Sensors

[233]

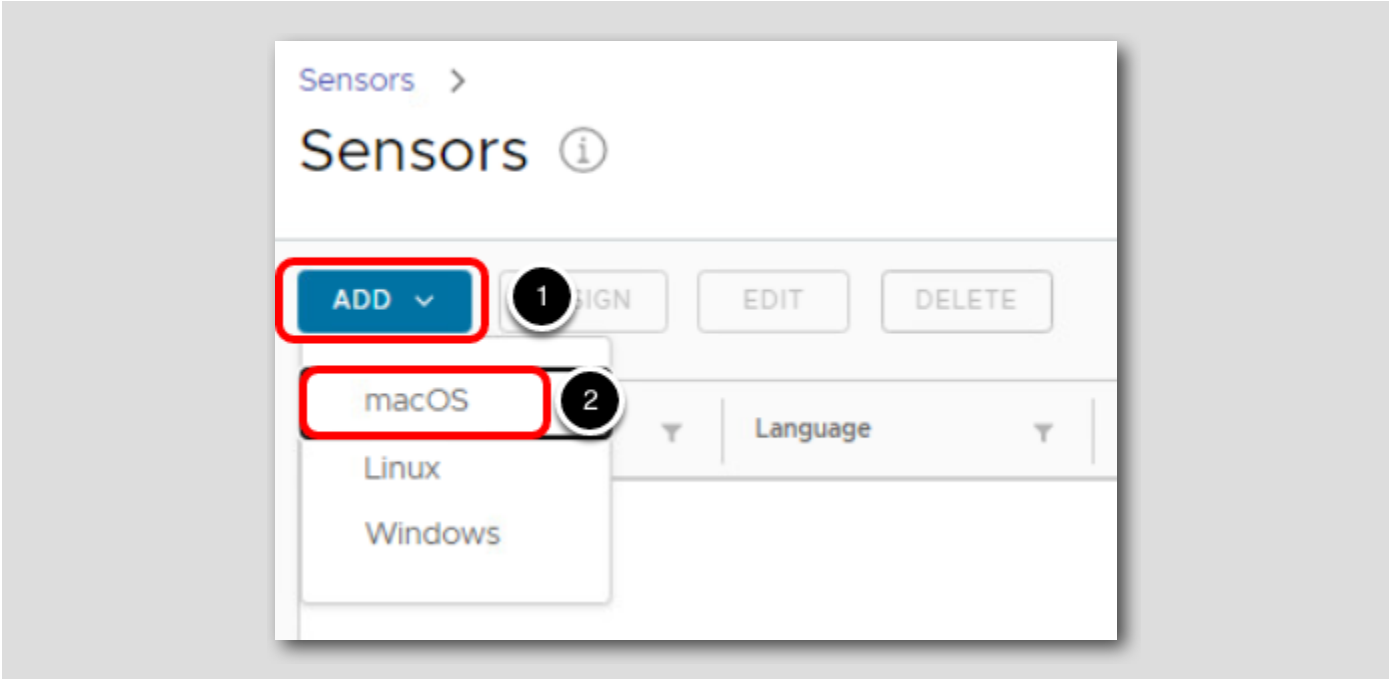


The first time you access the Sensors page, an overview will be presented with a link to the VMware docs articles for *macOS Sensors* and *Windows Desktop Sensors*. Refer to these links for additional documentation around Sensors.

1. Click **Resources**
2. Click **Sensors**
3. **Scroll down** to the bottom of the page
4. Click **Get Started**

Add a macOS Sensor

[234]



1. Click **Add**
2. Click **macOS**

Add General Information

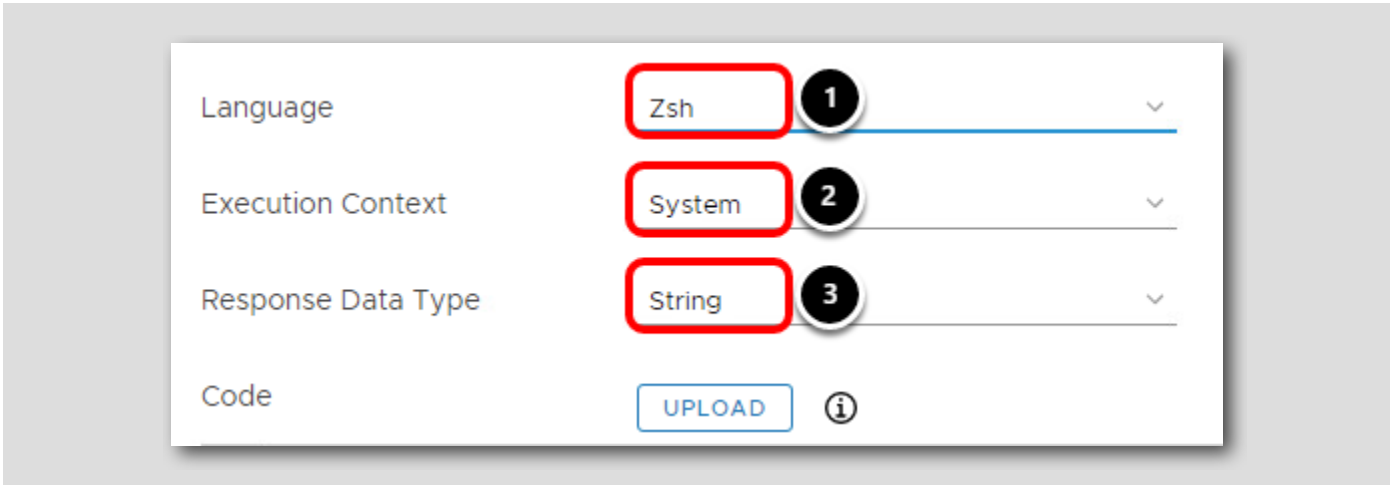
[235]

1. Enter **`macos_cpu_arch`** for the Name
2. Optionally enter **`Determine x64 (Intel) vs arm (M Series)`** for the description
3. Click **Next**

This sensor will be used to report if the device's CPU architecture is x64 (using the Intel chip) or arm (using the M series chip).

Enter the Sensor Details

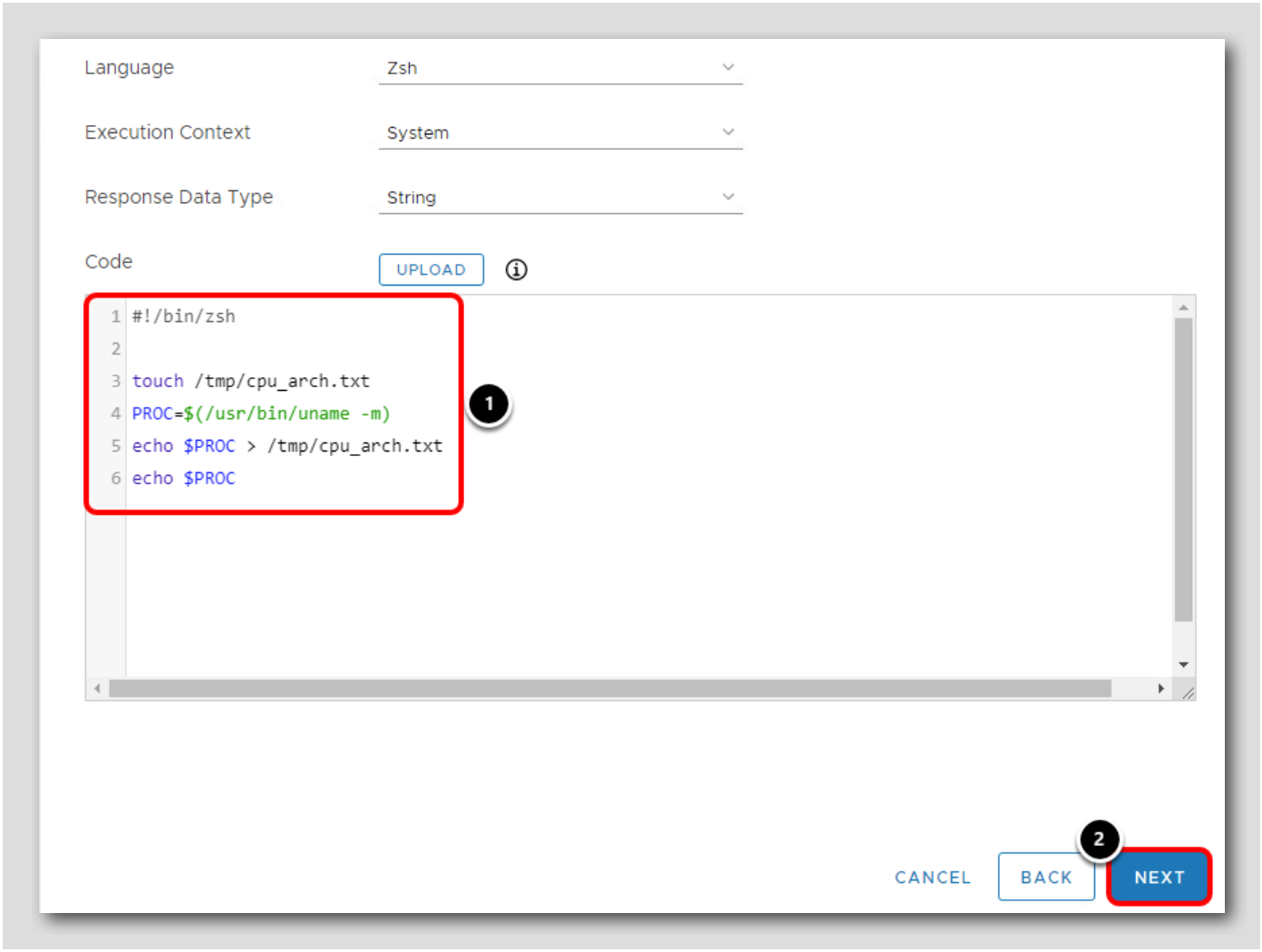
[236]



1. Select **Zsh** for the Language
2. Select **System** for the Execution Context
3. Select **String** for the Response Data Type

Copy and Paste the Sensor Code

[237]



This Sensor is setup to use the Zsh language and is targeting the System (Device-wide) execution context rather than the Current User context setting which will run against the currently logged in user of the device. The Response Data Type indicates what will be returned from the script: A String (text), Integer (number), Boolean (true/false), or Date Time.

In this case, the Sensor will read the CPU architecture, which will either be "x64" or "M1", so it is returning the value as a String.

1. Click and drag to highlight the below code block, starting from **`#!/bin/zsh`** to **`echo $PROC`**, and drag and drop it the **Code** section to paste the necessary sensor code.
2. Click **Next**.

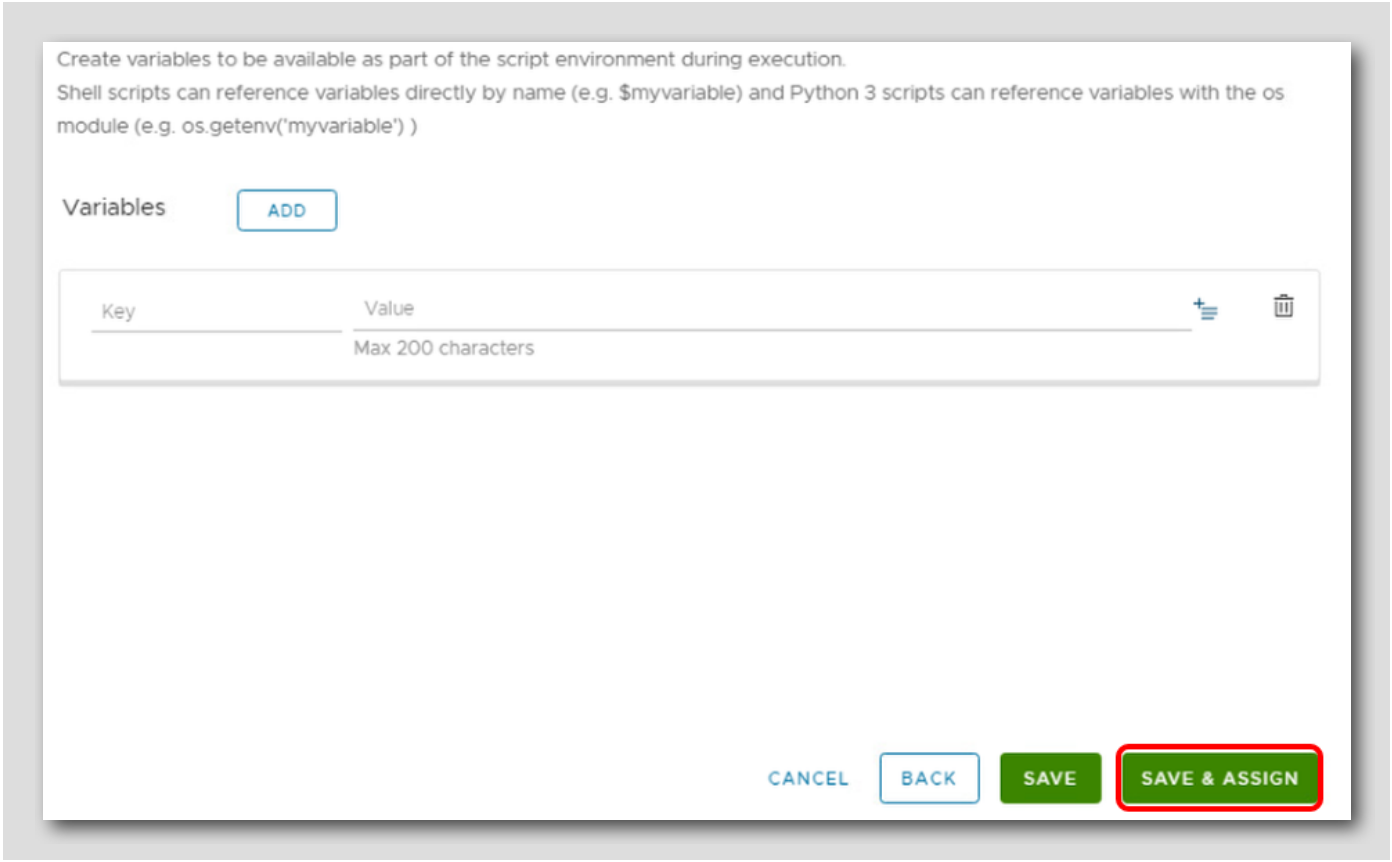
Note: We manually entered the code in this exercise but you can also upload a file containing the code instead.

```
#!/bin/zsh

touch /tmp/cpu_arch.txt
PROC=$(/usr/bin/uname -m)
echo $PROC > /tmp/cpu_arch.txt
echo $PROC
```

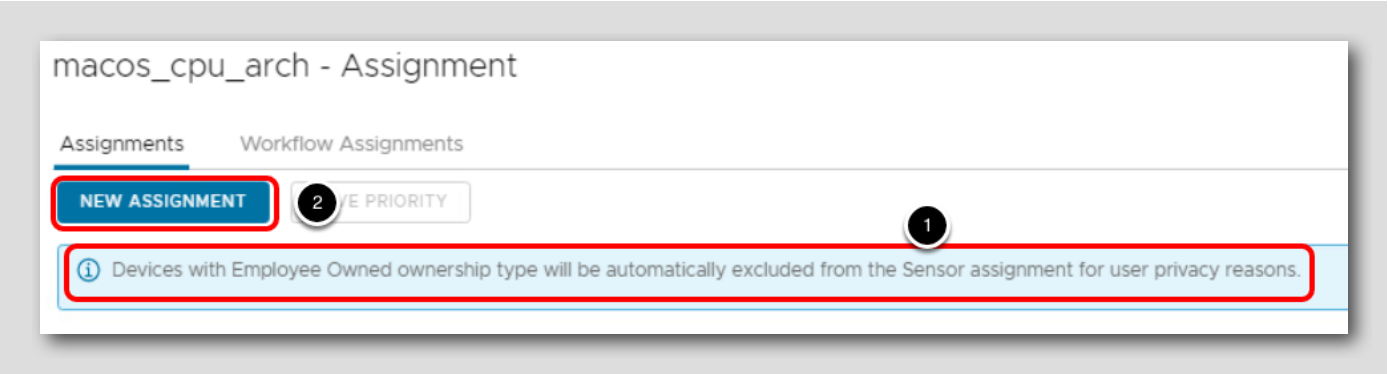
Save & Assign the Sensor

[238]



You can optionally create variables to use with this script, but it is not needed for this use case. Click **Save & Assign** to proceed.

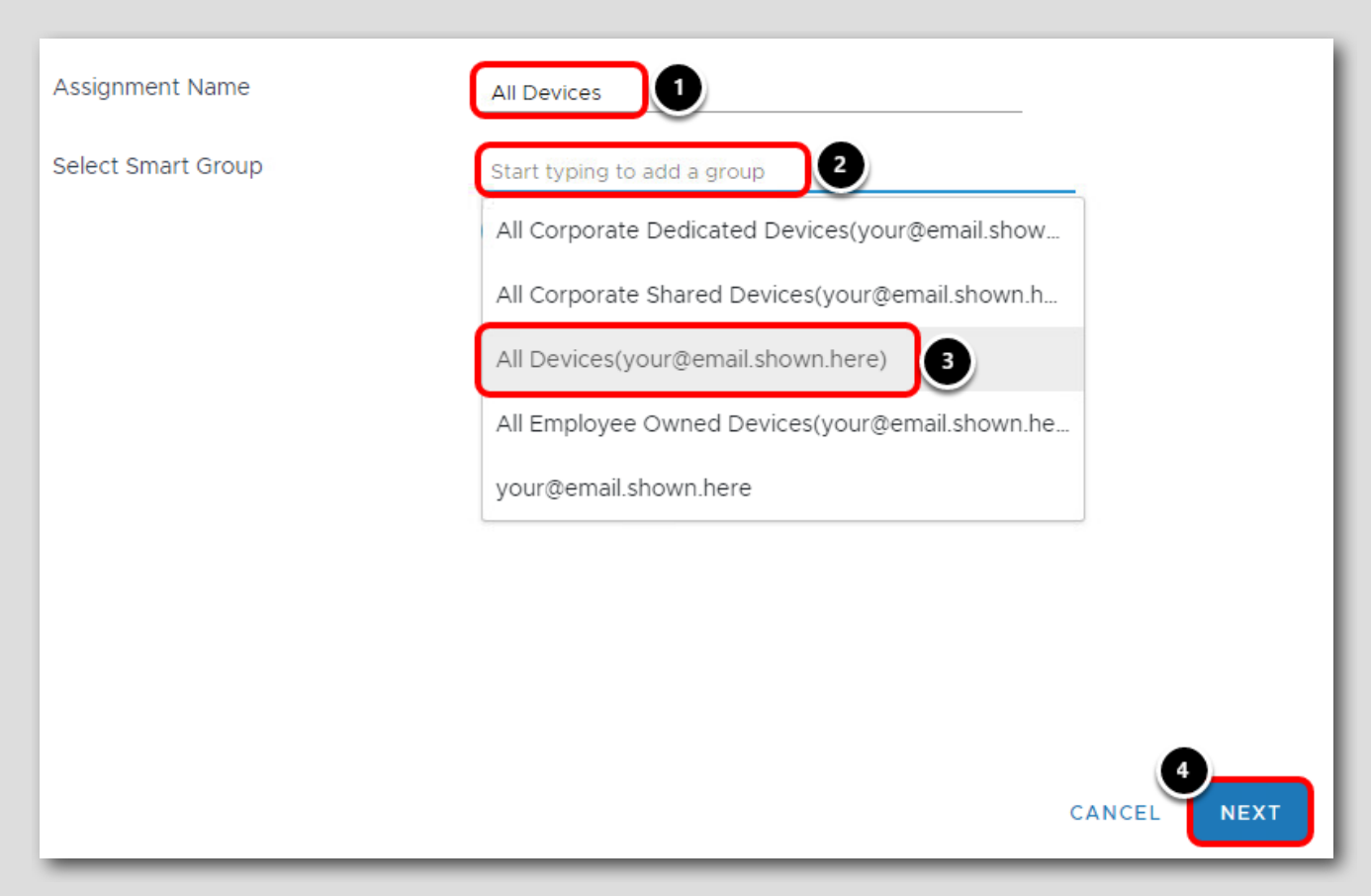
Assign a macOS Sensor



1. Notice the warning stating that Employee Owned devices will be automatically excluded from Sensor assignments due to privacy reasons, as Sensors can query sensitive details from the device.
2. Click **New Assignment**.

Assign to All Devices

[240]

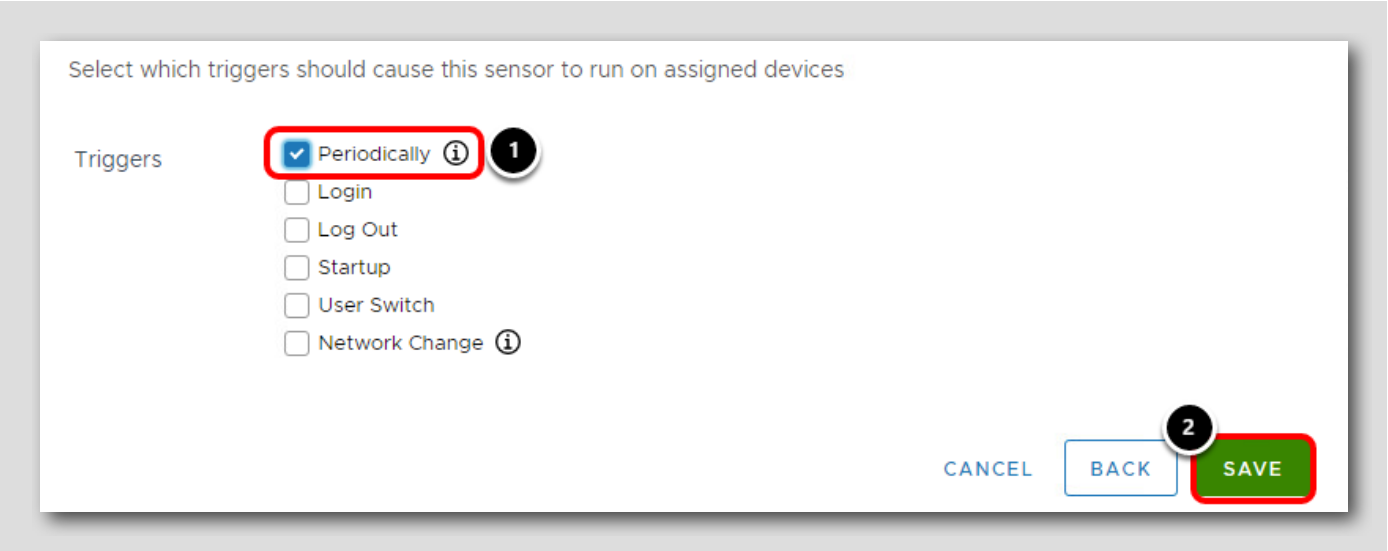


1. Enter **`All Devices`** for the Assignment Name
2. Click the **Select Smart Group** field
3. Select the **All Devices (your@email.shown.here)** group
4. Click **Next**

For ease, you will deploy this sensor to all non-Employee Owned devices that enroll into your organization. In a real deployment, you could target specific Smart Groups that you wish to deploy this Sensor to.

Configure Deployment Triggers

[241]

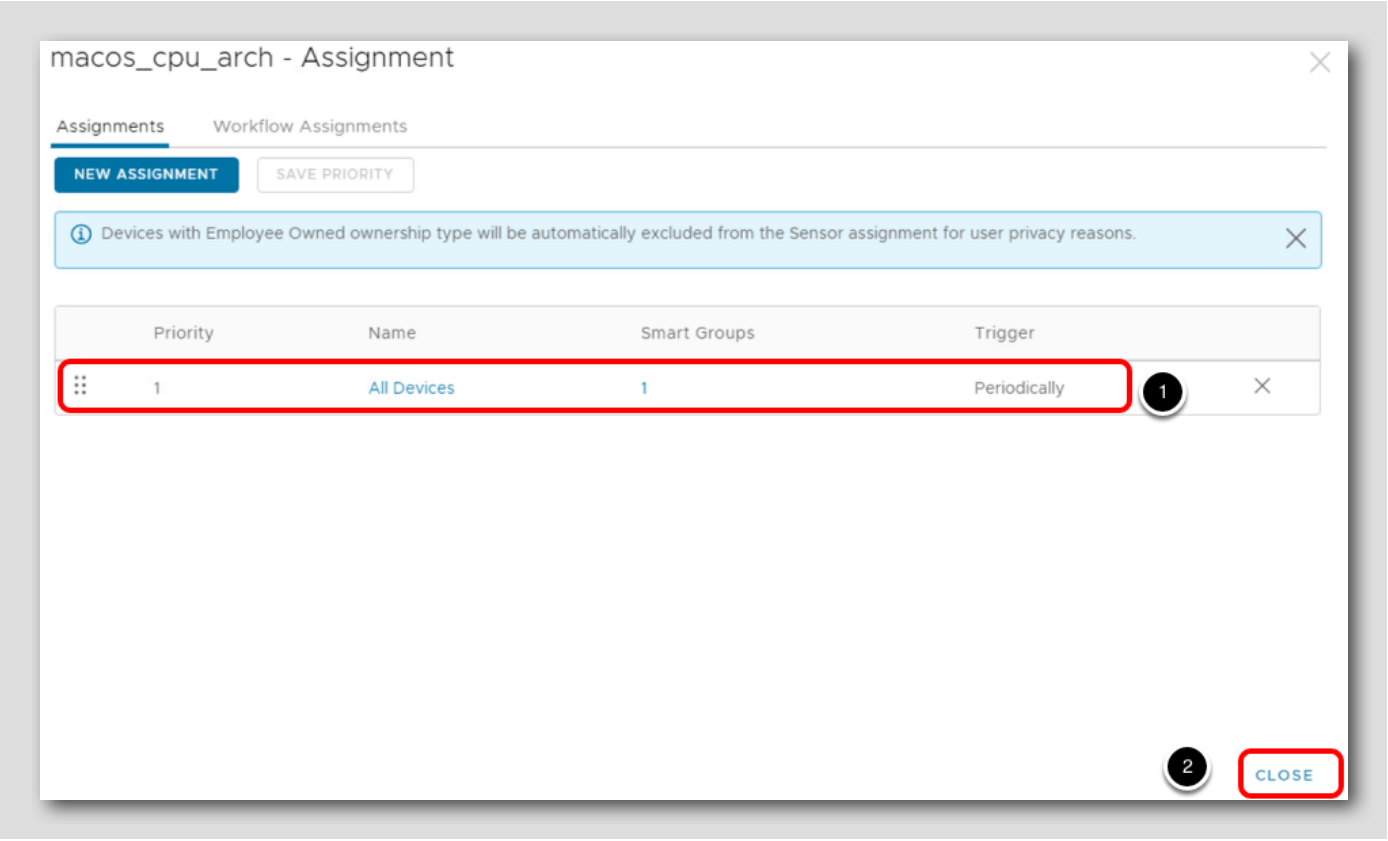


1. Select **Periodically** for the Triggers
2. Click **Save**

You can select more than one trigger, so consider what would fit your user case best when creating Sensors in your organization.

Confirm Sensor Creation

[242]



1. Your All Devices sensor is now created. If more than one Assignment was created, they would all show up here and you could use the left handlebar to re-arrange the Priority between them as necessary.
2. Click **Close** to return to the Resources page.

You have now successfully created and assigned a macOS Sensor which will report back if the device's CPU architecture is "x64" (Intel) or "arm" (M1). Once you enroll a device in later steps, you will view this sensor and confirm the value.

Sensors are powerful options for securely automating data collection for your endpoints. Consider what other use cases you could accomplish with sensors, and check our the *macOS Sensors examples* in the documentation for ideas.

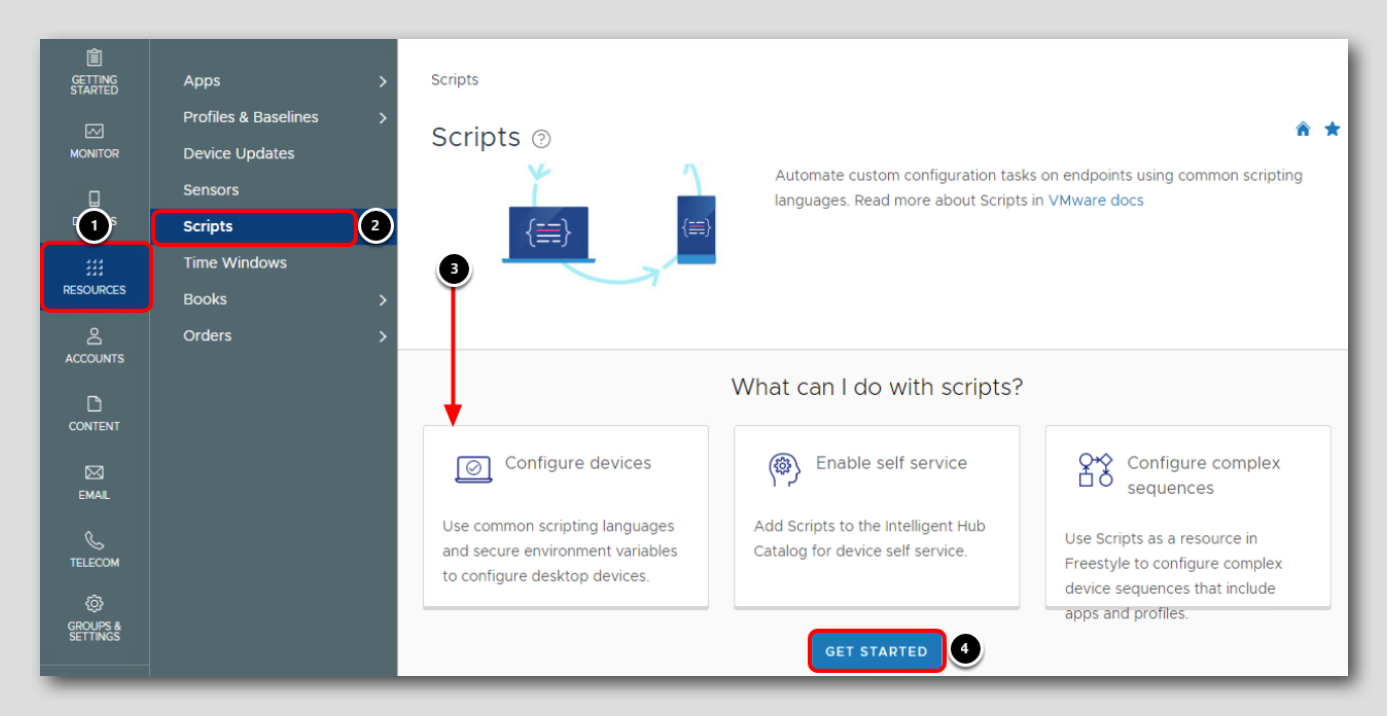
Create Scripts

[243]

Scripts allow you to automate custom configuration tasks on your devices with common scripting languages, including PowerShell, Bash, Python 3, and Zsh. These scripts can be deployed automatically, on demand through Intelligent Hub for self service, or in Freestyle Orchestrator to power complex sequences.

Navigate to Scripts

[244]

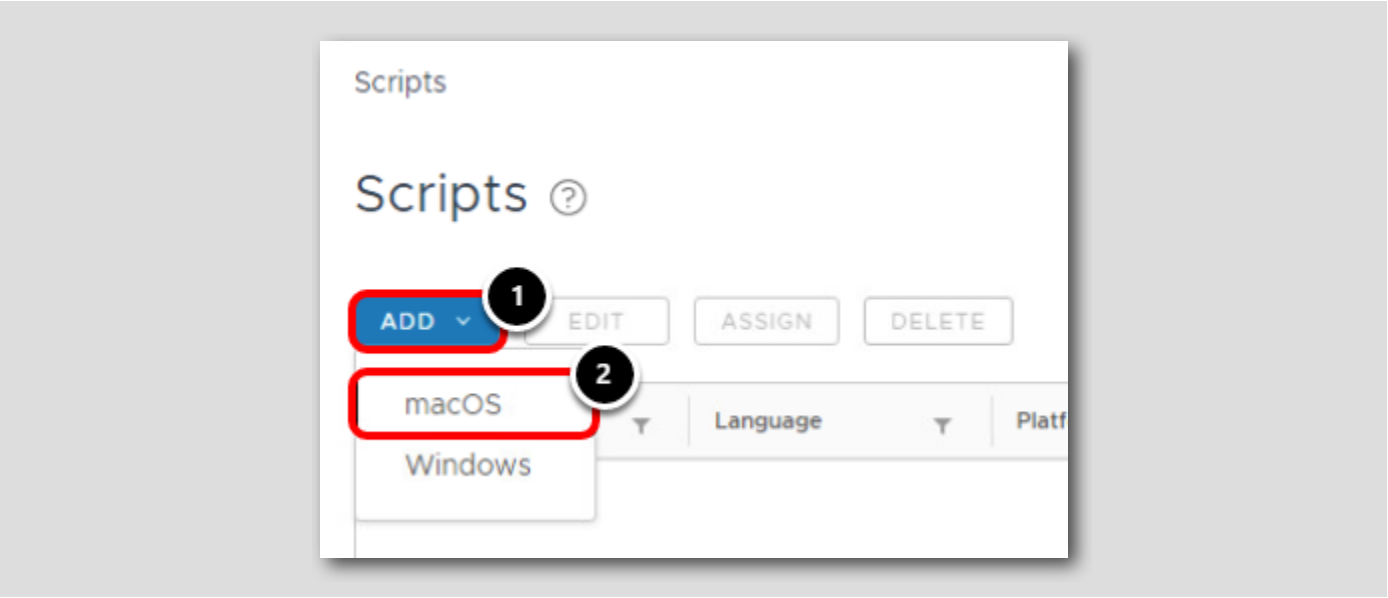


The first time you access the Scripts page, an overview will be presented with a link to the VMware docs articles for *macOS Scripts* and *Windows Desktop scripts*. Refer to these links if you desire more documentation around Scripts.

1. Click **Resources**
2. Click **Scripts**
3. **Scroll down** to the bottom of the page
4. Click **Get Started**

Add a macOS Script

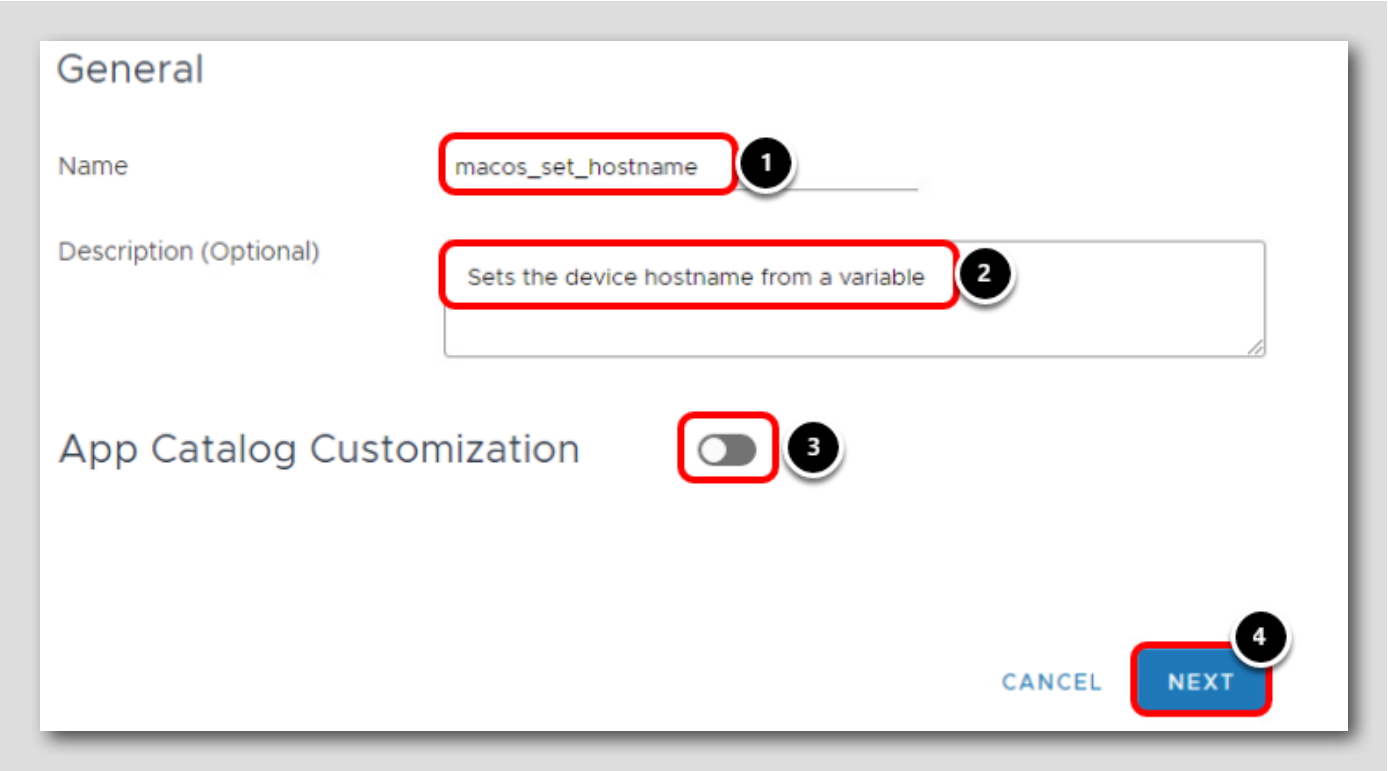
[245]



1. Click **Add**
2. Click **macOS**

Add General Information

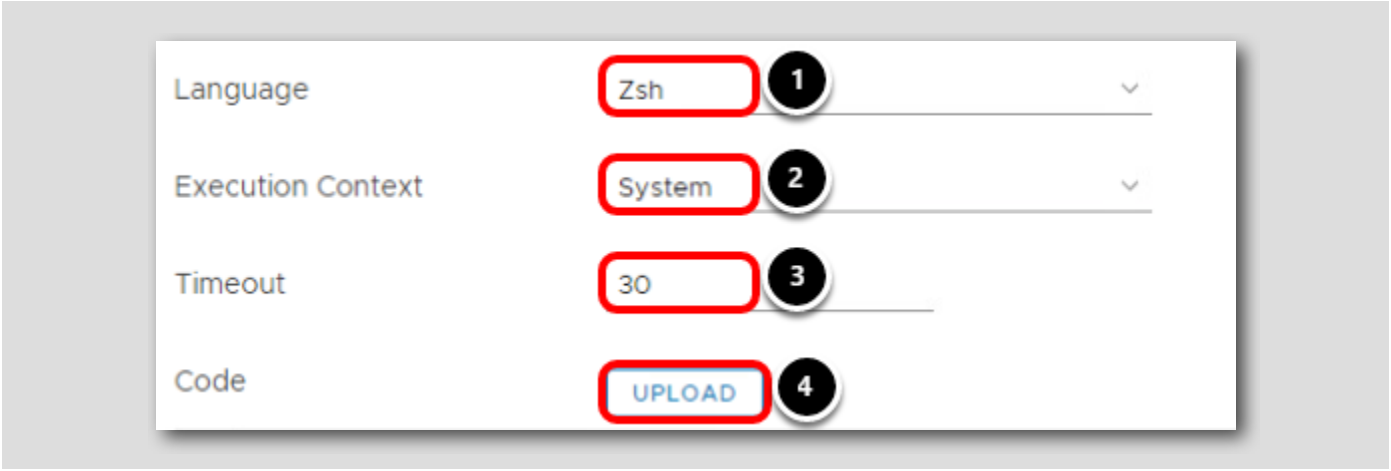
[246]



1. Enter **`macos_set_hostname`** for the Name.
2. Optionally enter **`Sets the device hostname from a variable`** for the description.
3. Leave the **App Catalog Customization disabled**. If you wish to configure how the script is displayed to users in Intelligent Hub, such as its display name and icon, you can configure those settings by enabling App Catalog Customization. You will provision this script through a Freestyle Orchestrator workflow, so we will not be focused on providing this script to users in Intelligent Hub for self service.
4. Click **Next**.

Enter the Script Details

[247]

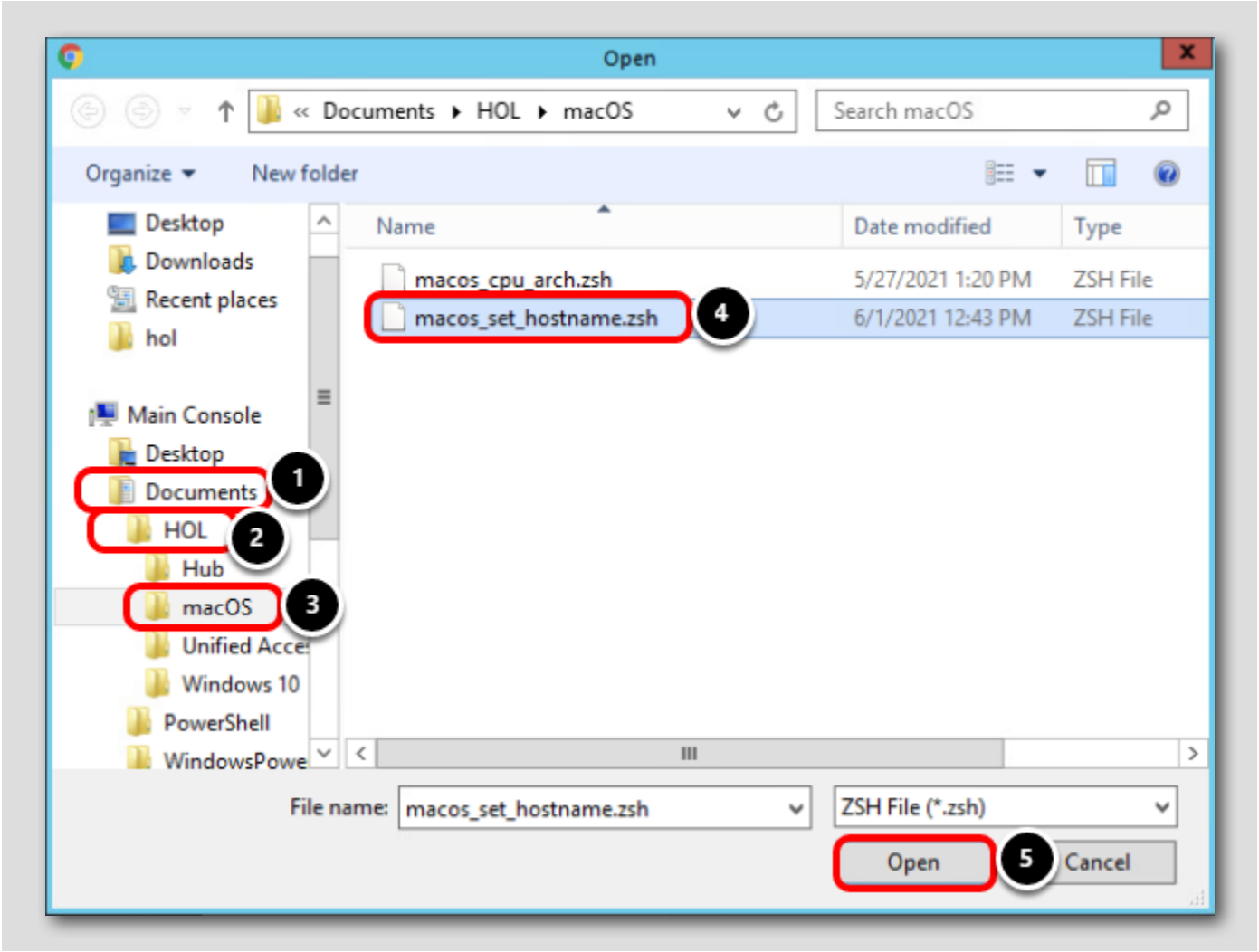


1. Select Zsh for the language
2. Select System for the Execution Context
3. Enter **`30`** as the Timeout value
4. Click Upload to select a file containing the code you wish to use for this Script. Optionally, you could enter the code in the Code window below this section.

We will explain each of these settings in an upcoming step.

Upload the macos_set_hostname.zsh File

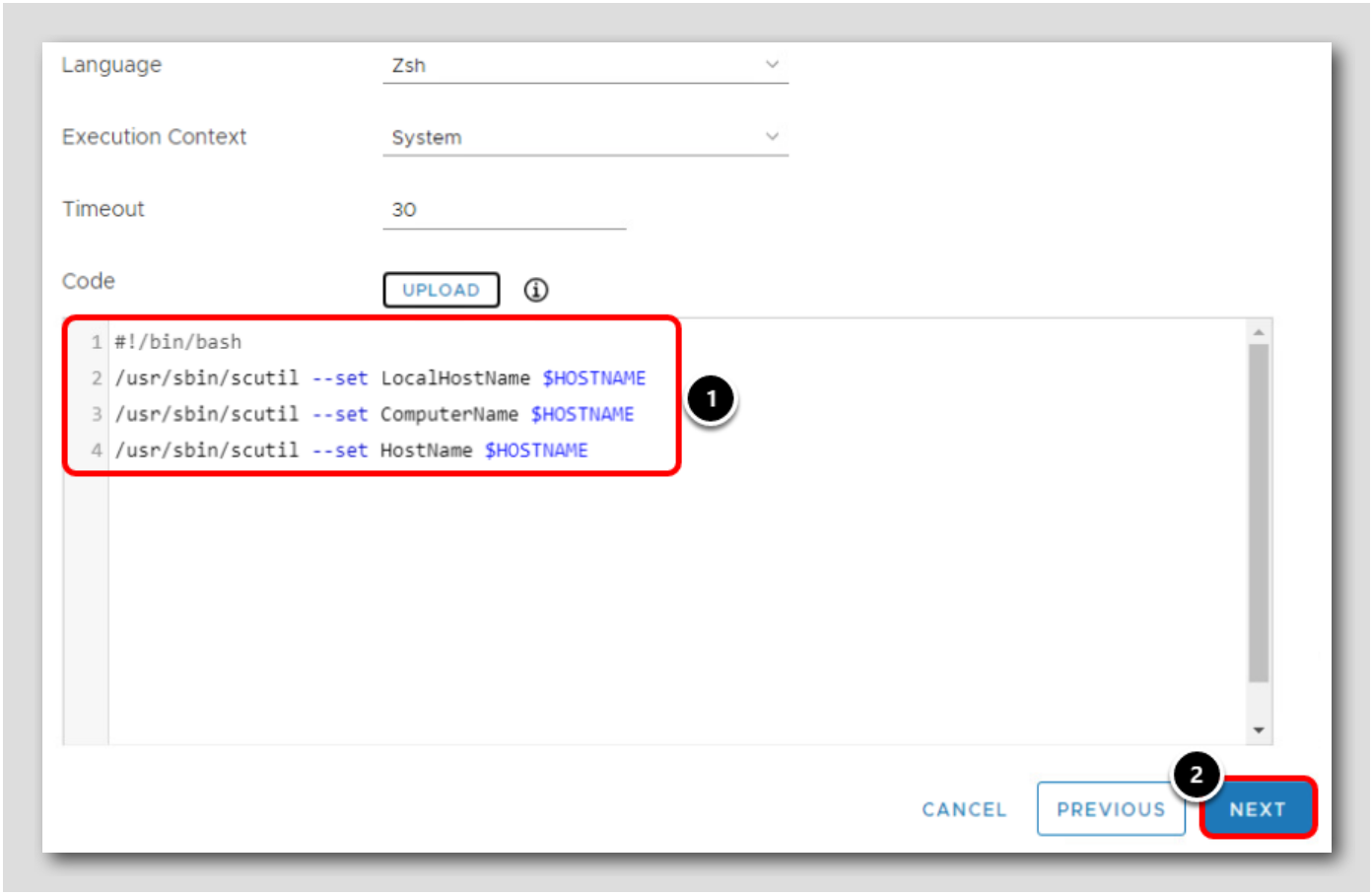
[248]



1. Click **Documents**
2. Click **HOL**
3. Click **macOS**
4. Select **macos_set_hostname.zsh**
5. Click **Open**

Confirm Script Details

[249]

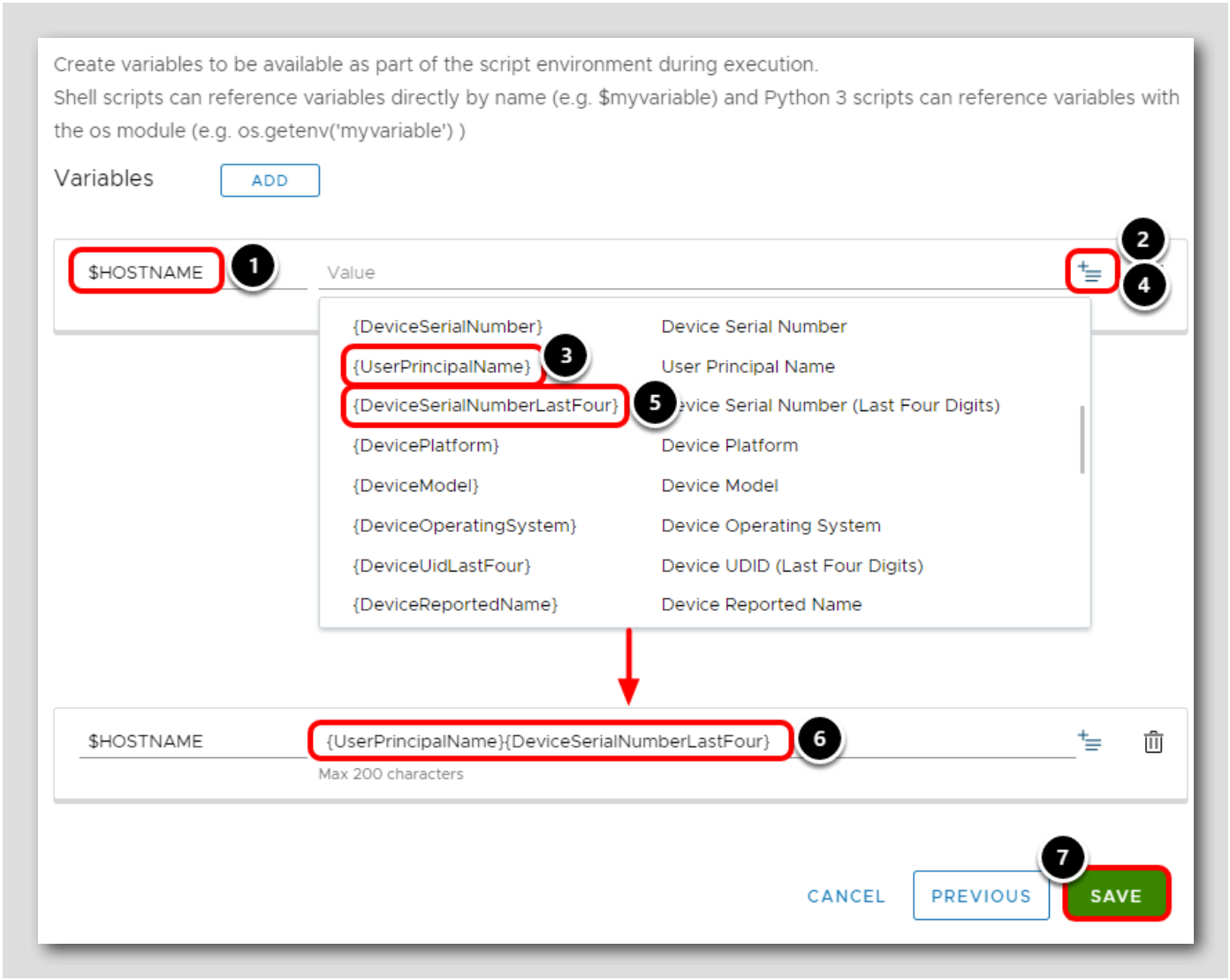


1. Confirm that the script uploaded. Alternatively, you can choose to type the code directly into the window.
2. Click **Next**.

You will create a value for the **$HOSTNAME** variable in the next step.

Set a Value for the Hostname Variable

[250]



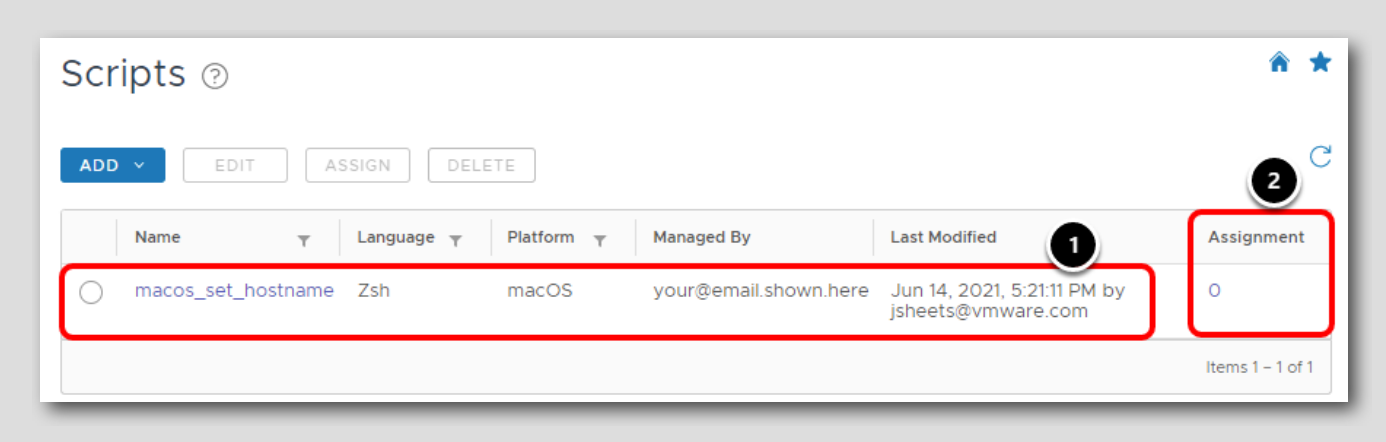
The value of the $HOSTNAME variable can be statically set, or dynamically set by using lookup values. Lookup values retrieve the value from the device at runtime to allow for dynamic values. For example, the **{UserPrincipalName}** lookup value will substitute the actual user principal name of the enrolled user on the device.

1. Enter **$HOSTNAME** for the key
2. Click the **Lookup button** to see a list of options
3. Select **{UserPrincipalName}** from the list
4. Click the **Lookup button** again
5. Select **{DeviceSerialNumberLastFour}** from the list
6. Confirm your value is **{UserPrincipalName}{DeviceSerialNumberLastFour}**. You can also optionally type this value in instead.
7. Click **Save**

This will cause the **$HOSTNAME** variable to dynamically pull the UPN and Last 4 Device Serial Numbers to create the record. So if our UPN was **testuser** and our last four serial numbers were **1234**, the new **$HOSTNAME** value retrieved from the device would be **testuser1234**.

Confirm Script was Created

[251]



1. Confirm that the script was created successfully.

Deploy a 3rd Party macOS Application (Internal Applications)

[252]

VMware integrates with the *Open-Sourced "munki" project* for third-party application management on enrolled macOS devices. Administrators can manage third-party (non-AppStore) software using the *internal apps* view in Workspace ONE UEM. The integration allows administrators to consume a global CDN for software delivery, without requiring the administrators to fully understand munki's inner workings and configuration.

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

Note: Workspace ONE UEM also provides a second facility for delivering software/configurations and running scripts/commands on a macOS device. This method, known as Product Provisioning, is outside the scope of this exercise. For more information, refer to *Deploying Third-Party macOS Applications: VMware Workspace ONE Operational Tutorial* on VMware TechZone.

Recommended Methods to Deliver Software [253]

Administrators can deliver software to macOS using multiple methods. As a quick reference, VMware recommends using the following methods to deliver software to macOS devices:

- Mac App Store Applications: VMware recommends delivering any application that may be available on the Mac App Store be delivered as a Volume-Purchased app from Apple Business Manager. Apps should be assigned via device-based licenses and set to auto-update if the application is not business-critical.
- Non-Store Applications: As much as possible, 3rd-Party applications which are not available through the app store should be delivered as an Internal Application (leveraging the underlying munki integration).

Enable macOS Software Management [254]

NOTE: The steps in this section have already been completed for you in the Hands-On Lab. You DO NOT need to Enable Software Management as it has already been completed on your behalf.

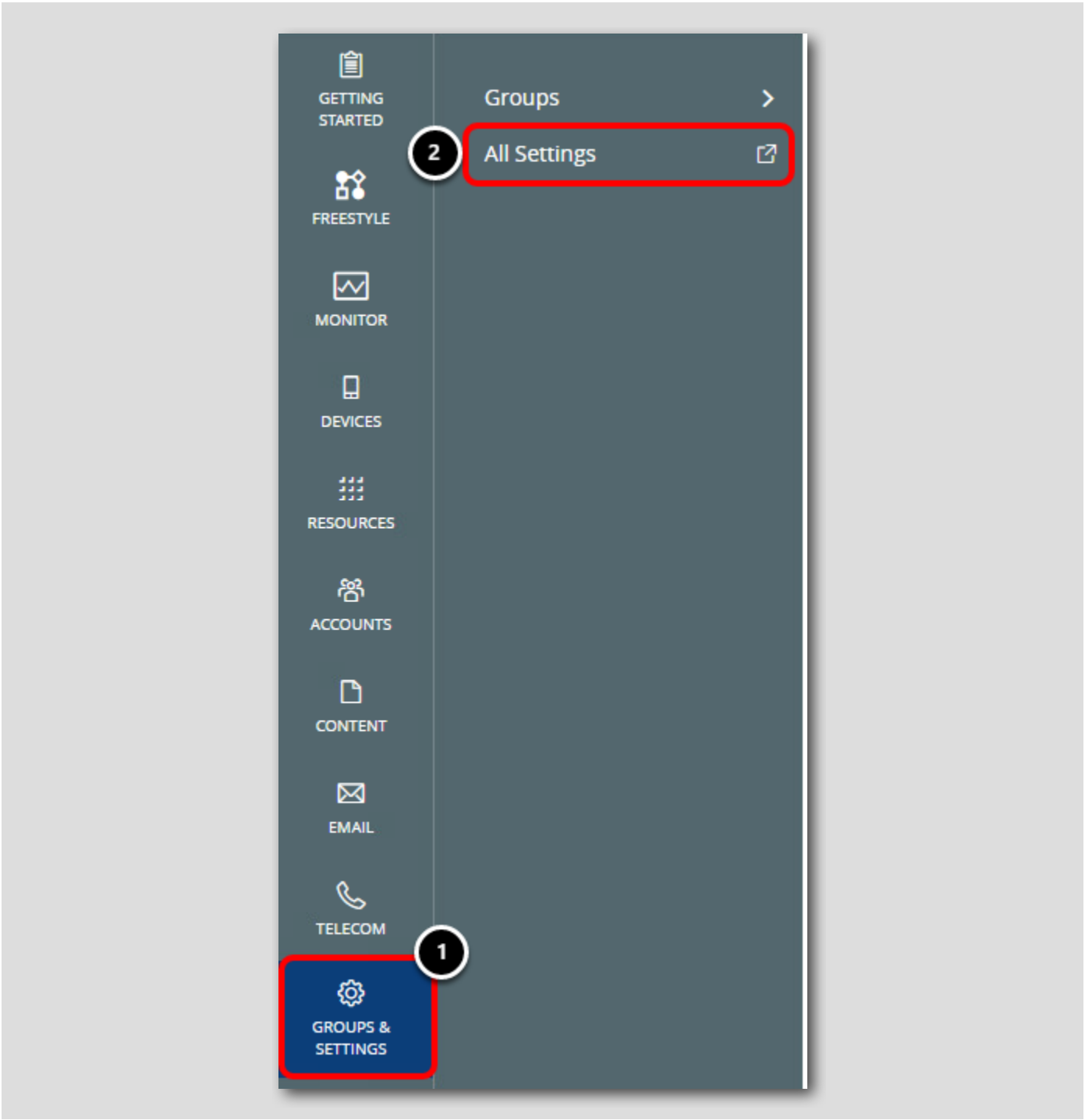
Prior to deploying a macOS Application, VMware Workspace ONE UEM administrators must enable their environments for Software Management. The following items are pre-requisites for macOS Software Management:

1. For On-Premise Installations, "File Storage" must be enabled (Settings > Installation > File Path).
2. "Software Management" must be enabled (Settings > Devices & Users > Apple > Apple macOS > Software Management)
3. VMware AirWatch Agent for macOS version 3.0 (or newer). Note the best experience is provided via macOS Intelligent Hub.

Continue to the next step.

Access All Settings (REFERENCE ONLY)

[255]

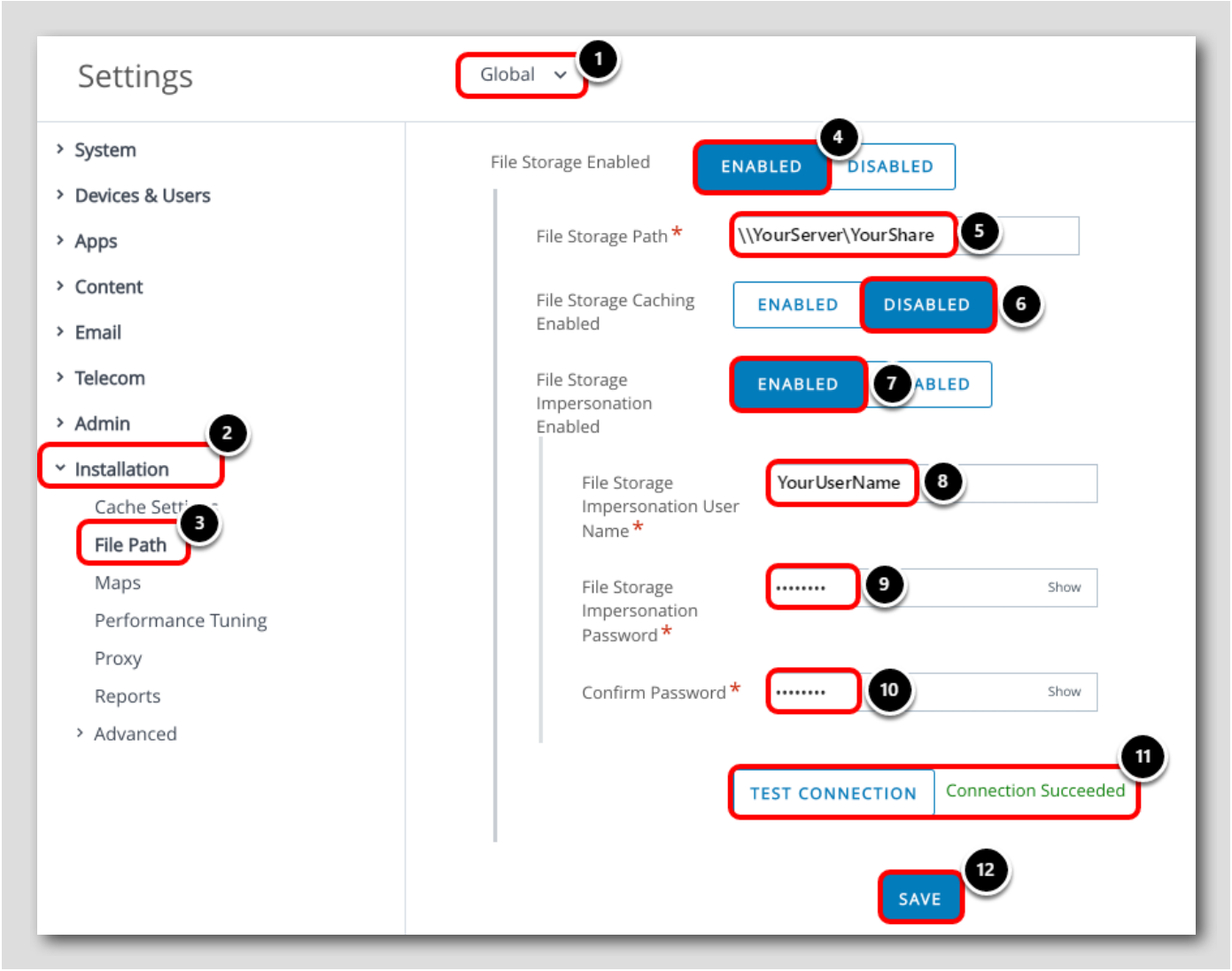


NOTE: The steps in this section have already been completed for you in the Hands-On Lab. You DO NOT need to Enable Software Management as it has already been completed on your behalf.

1. Click **Groups & Settings**
2. Click **All Settings**

Enable File Storage (REFERENCE ONLY)

[256]

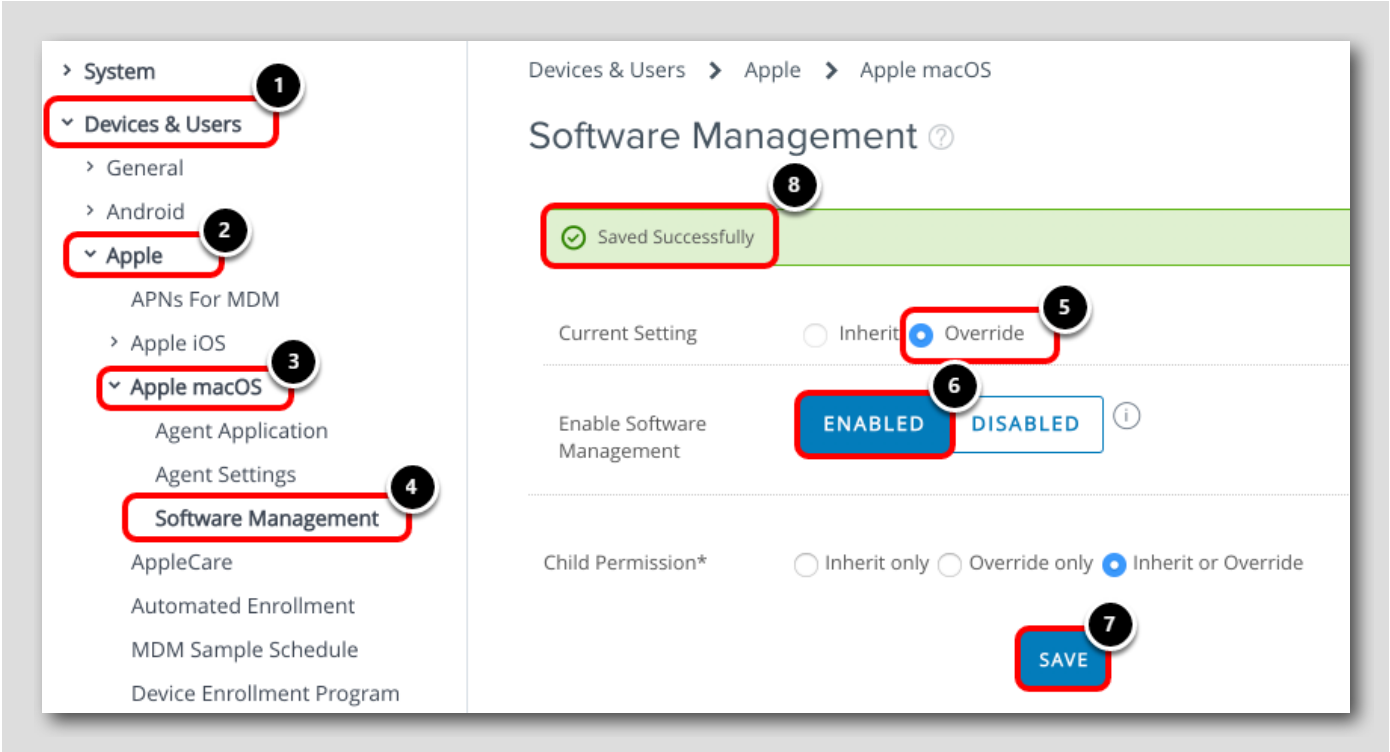


NOTE: The steps in this section have already been completed for you in the Hands-On Lab. You DO NOT need to Enable Software Management as it has already been completed on your behalf.

1. Ensure you are at the **Global** Organization Group unless your particular setup requires configuring at child Organization Groups.
2. Expand **Installation**
3. Click **File Path**
4. Scroll the file paths screen and click **Enabled** for *File Storage Enabled*
5. Enter the path of a file share accessible from your Device Services and Console servers.
6. Click **Disabled** for *File Storage Caching Enabled* unless you have planned and sized your Device Services server accordingly.
7. Click **Enabled** for *File Storage Impersonation Enabled*
8. Enter the username credentials to impersonate in order to access the file storage path
9. Enter the password for the impersonation user
10. Confirm the password for the impersonation user
11. Click **Test Connection** and ensure you see *Connection Succeeded*
12. Click **Save**

Enable Software Management (REFERENCE ONLY)

[257]



NOTE: The steps in this section have already been completed for you in the Hands-On Lab. You DO NOT need to Enable Software Management as it has already been completed on your behalf.

1. Expand **Devices & Users**
2. Expand **Apple**
3. Expand **Apple macOS**
4. Click **Software Management**
5. Click **Override**
6. Click **Enabled** for *Enable Software Management*
7. Click **Save**
8. Ensure settings are *Saved Successfully*

Prepare macOS Applications for Deployment

[258]

NOTE: These steps are optional as the necessary application files are included for you in the Hands-on Lab. If you wish to see how to extract the necessary files for app deployment on macOS, continue with these steps. If not, *CLICK HERE* to continue to uploading the app files.

NOTE: These steps require a macOS device.

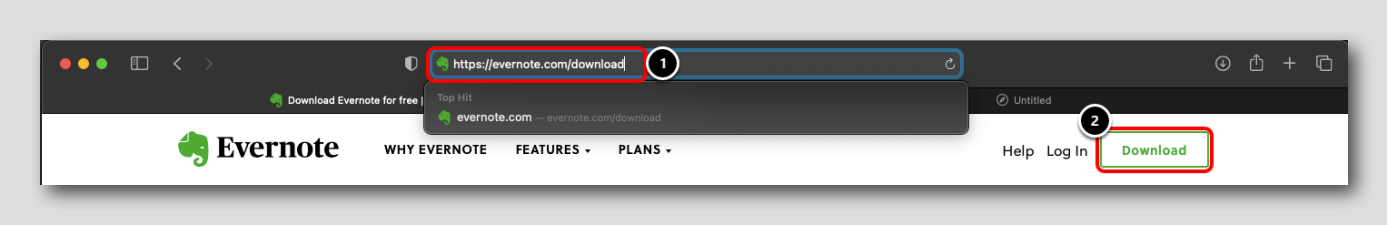
In this section, you will download the Workspace ONE Admin Assistant tool and use it to prepare another 3rd-Party application for deployment.

Download Evernote

[259]

NOTE: These steps are optional as the necessary application files are included for you in the Hands-on Lab. If you wish to see how to extract the necessary files for app deployment on macOS, continue with these steps. If not, *CLICK HERE* to continue to uploading the app files.

NOTE: These steps require a macOS device.



On a macOS device, open Safari or a web browser of your choice.

1. Enter **`https://evernote.com/download`** in the URL bar. Press **ENTER**.
2. Click **Download**.

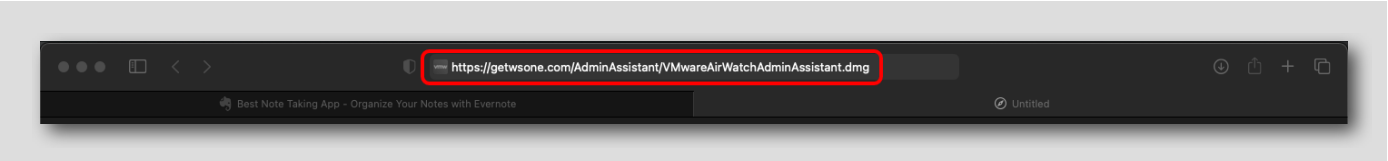
The DMG file for Evernote will download to the Downloads folder.

Download the Workspace ONE Admin Assistant Tool

[260]

NOTE: These steps are optional as the necessary application files are included for you in the Hands-on Lab. If you wish to see how to extract the necessary files for app deployment on macOS, continue with these steps. If not, *CLICK HERE* to continue to uploading the app files.

NOTE: These steps require a macOS device.



In the same tab as you downloaded Skitch, paste the link in Safari to download the **Workspace ONE Admin Assistant** tool and press **ENTER** on the keyboard: **`https://getwsone.com/AdminAssistant/VMwareAirWatchAdminAssistant.dmg`**

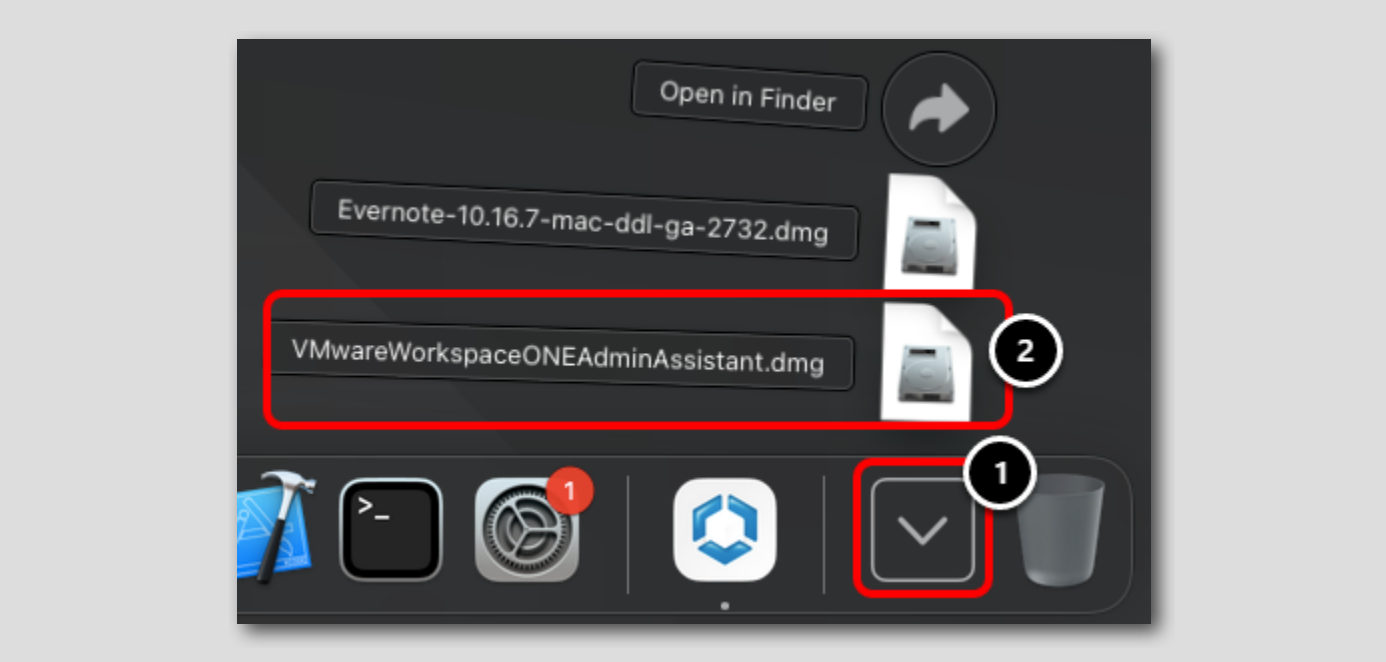
The DMG file will download to the Downloads folder.

Begin Installing Workspace ONE Admin Assistant Tool

[261]

NOTE: These steps are optional as the necessary application files are included for you in the Hands-on Lab. If you wish to see how to extract the necessary files for app deployment on macOS, continue with these steps. If not, *CLICK HERE* to continue to uploading the app files.

NOTE: These steps require a macOS device.



On the dock, perform the following:

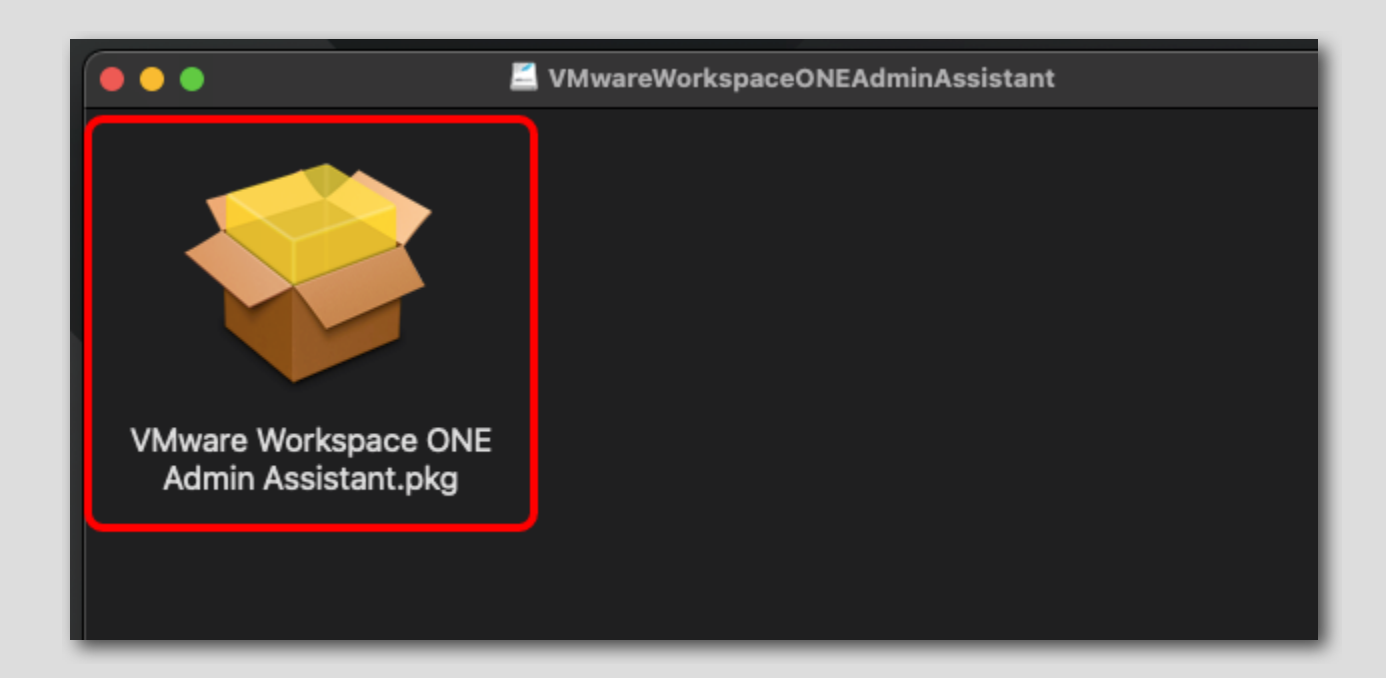
1. Click the **Downloads** folder.
2. Click **VMwareWorkspaceONEAdminAssistant.dmg**.

Launch Installer Package

[262]

NOTE: These steps are optional as the necessary application files are included for you in the Hands-on Lab. If you wish to see how to extract the necessary files for app deployment on macOS, continue with these steps. If not, *CLICK HERE* to continue to uploading the app files.

NOTE: These steps require a macOS device.



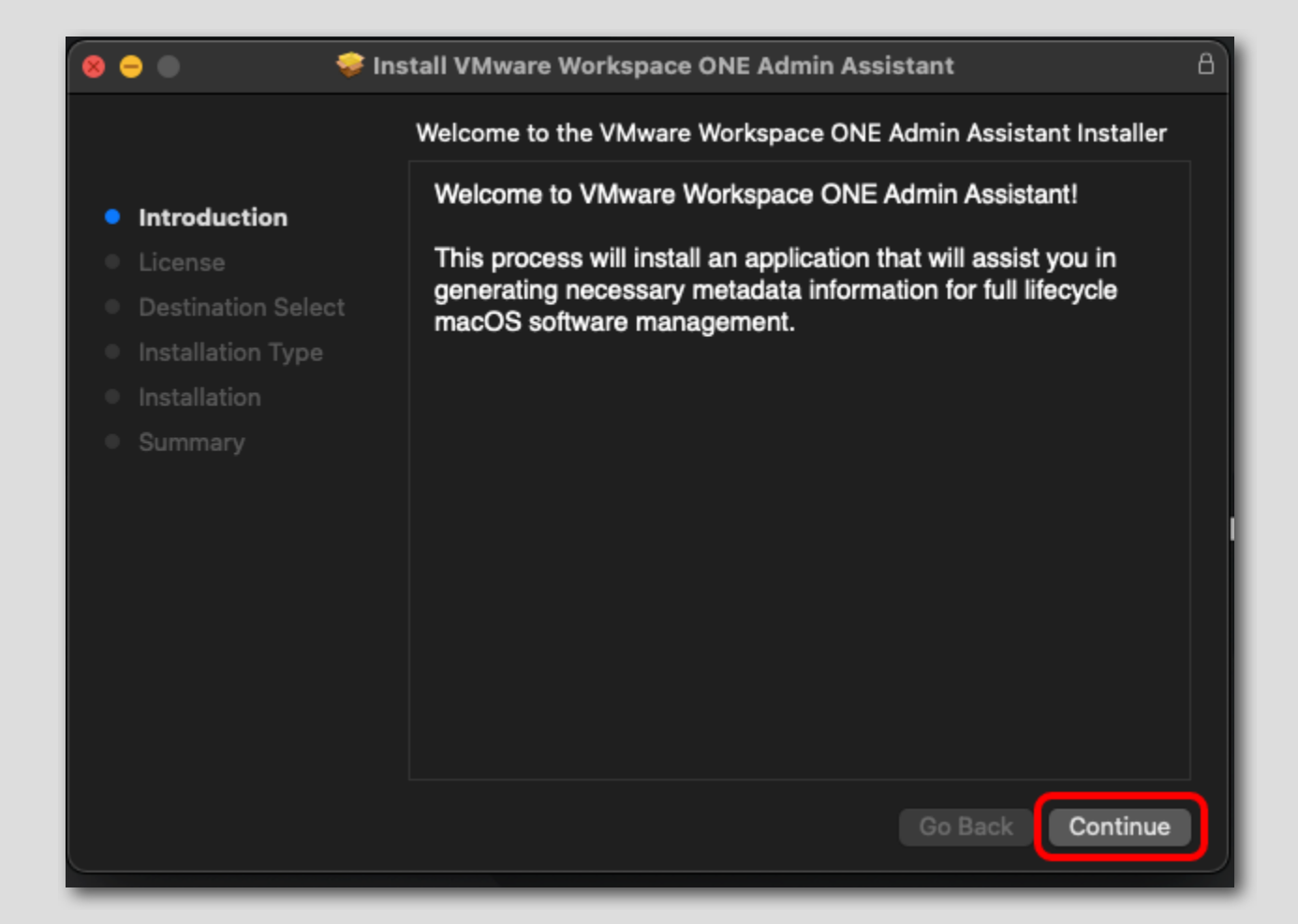
Double-click the **VMware Workspace ONE Admin Assistant.pkg** file

Continue Installer

[263]

NOTE: These steps are optional as the necessary application files are included for you in the Hands-on Lab. If you wish to see how to extract the necessary files for app deployment on macOS, continue with these steps. If not, *CLICK HERE* to continue to uploading the app files.

NOTE: These steps require a macOS device.



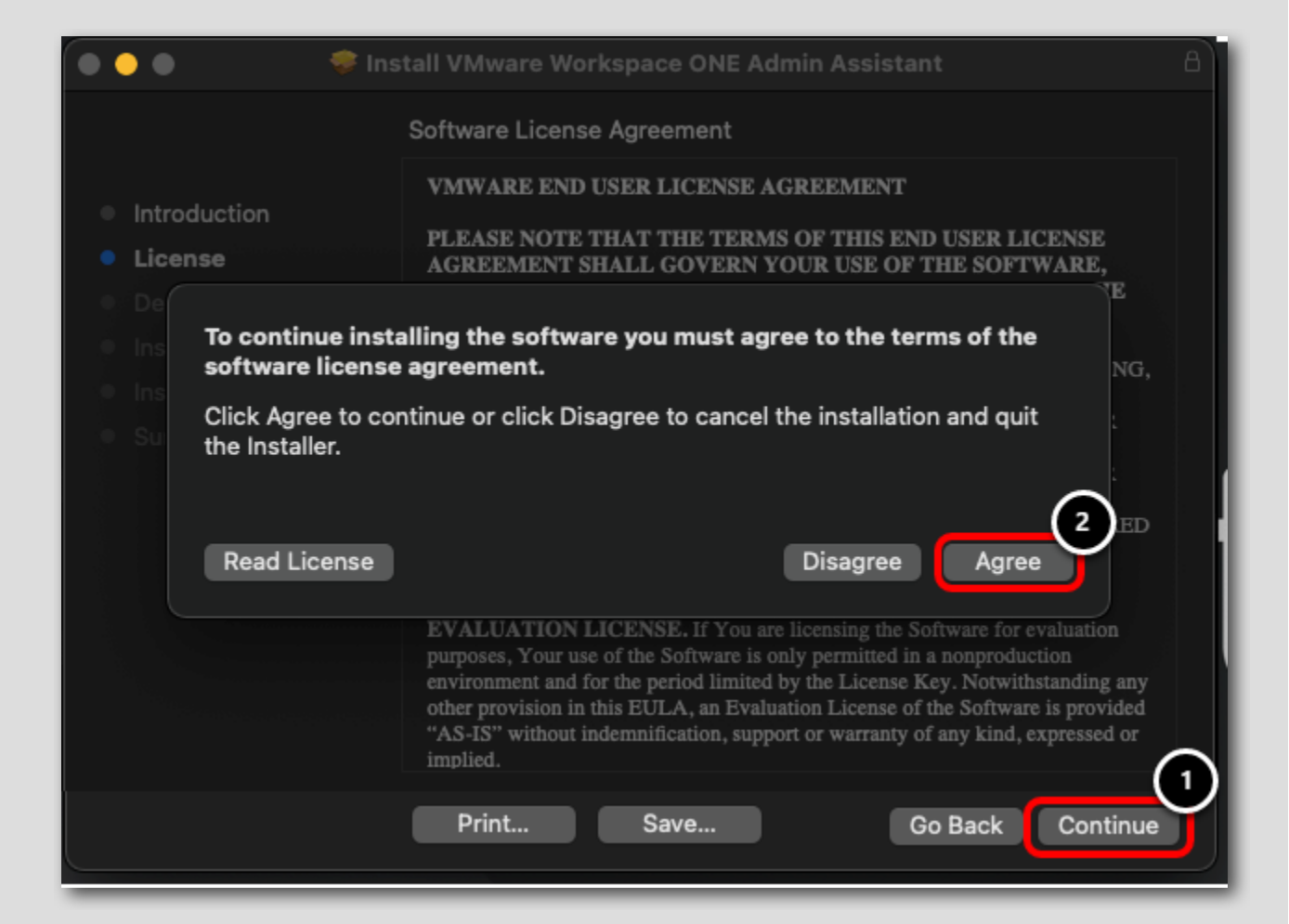
Click **Continue**

Review and Continue Installer

[264]

NOTE: These steps are optional as the necessary application files are included for you in the Hands-on Lab. If you wish to see how to extract the necessary files for app deployment on macOS, continue with these steps. If not, *CLICK HERE* to continue to uploading the app files.

NOTE: These steps require a macOS device.



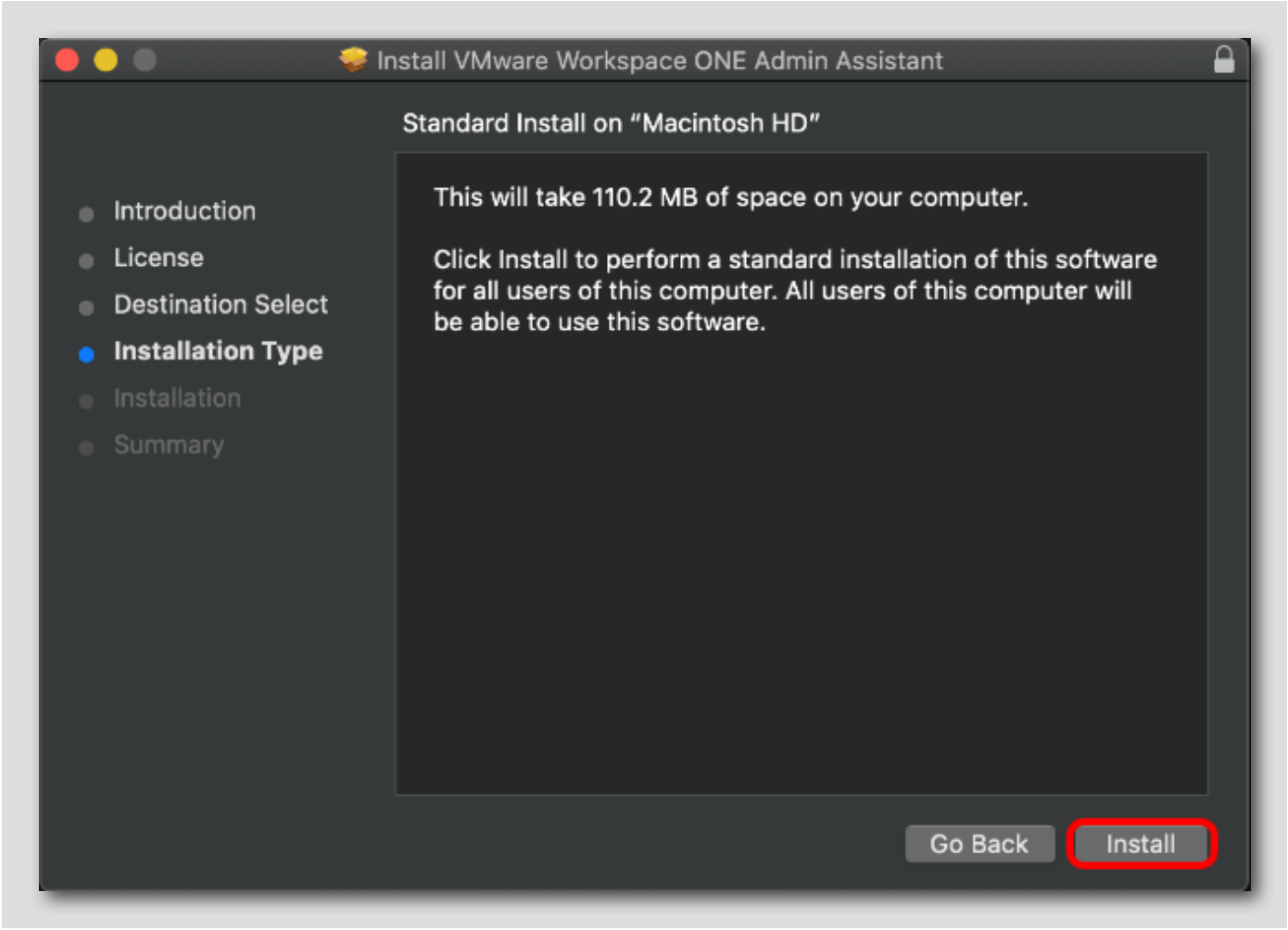
1. Review the License Agreement and click **Continue**
2. Click **Agree**.

Install the Admin Assistant Tool

[265]

NOTE: These steps are optional as the necessary application files are included for you in the Hands-on Lab. If you wish to see how to extract the necessary files for app deployment on macOS, continue with these steps. If not, *CLICK HERE* to continue to uploading the app files.

NOTE: These steps require a macOS device.



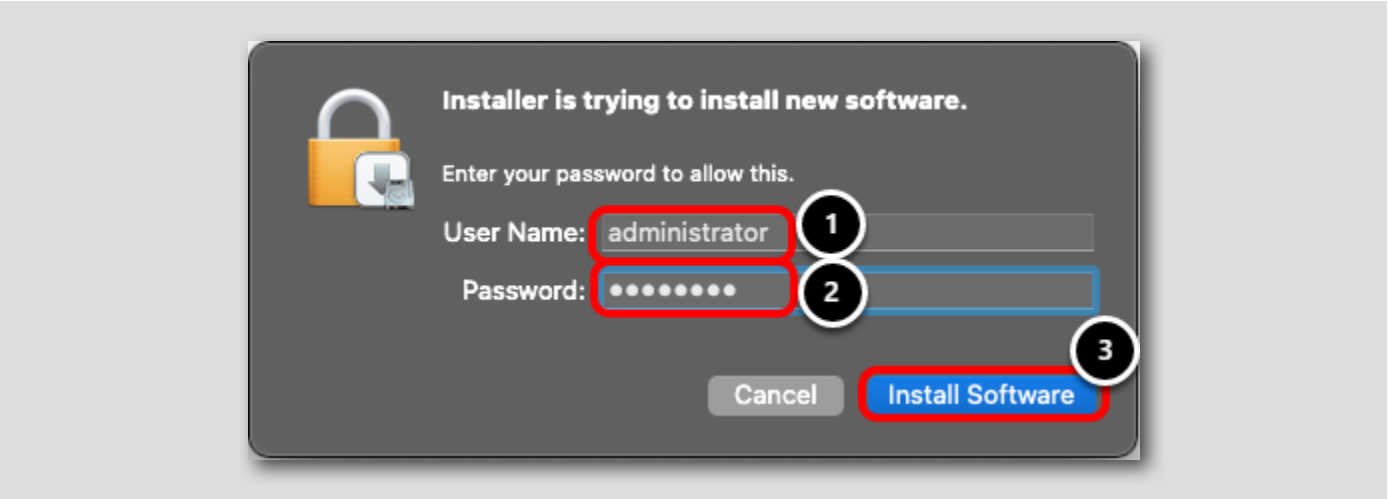
Click **Install**.

Enter Admin Credentials

[266]

NOTE: These steps are optional as the necessary application files are included for you in the Hands-on Lab. If you wish to see how to extract the necessary files for app deployment on macOS, continue with these steps. If not, *CLICK HERE* to continue to uploading the app files.

NOTE: These steps require a macOS device.



If prompted for administrative credentials, enter the credentials required to install.

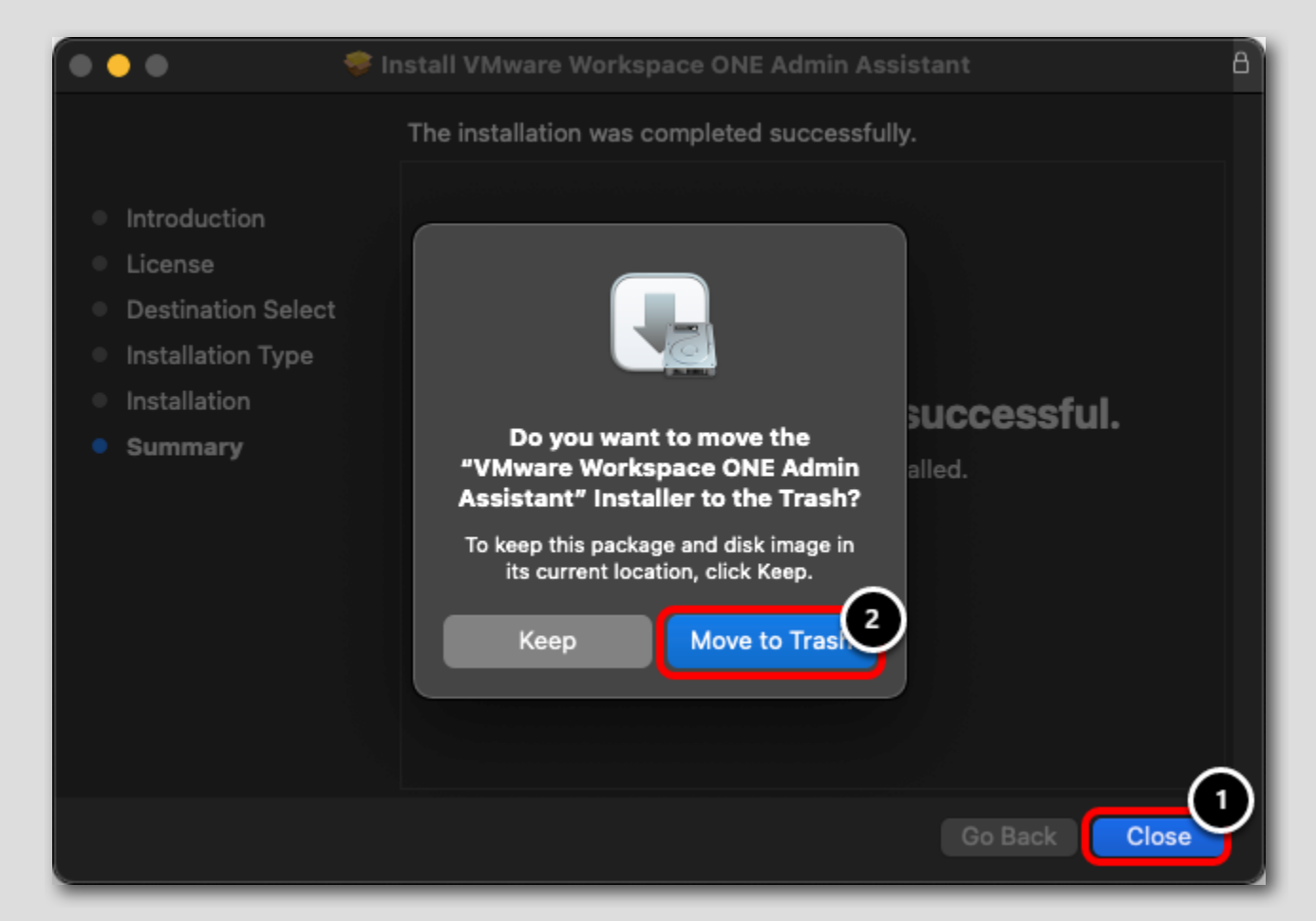
1. Enter the username for the device
2. Enter the password for the device
3. Click **Install Software**

Close the Installer

[267]

NOTE: These steps are optional as the necessary application files are included for you in the Hands-on Lab. If you wish to see how to extract the necessary files for app deployment on macOS, continue with these steps. If not, *CLICK HERE* to continue to uploading the app files.

NOTE: These steps require a macOS device.



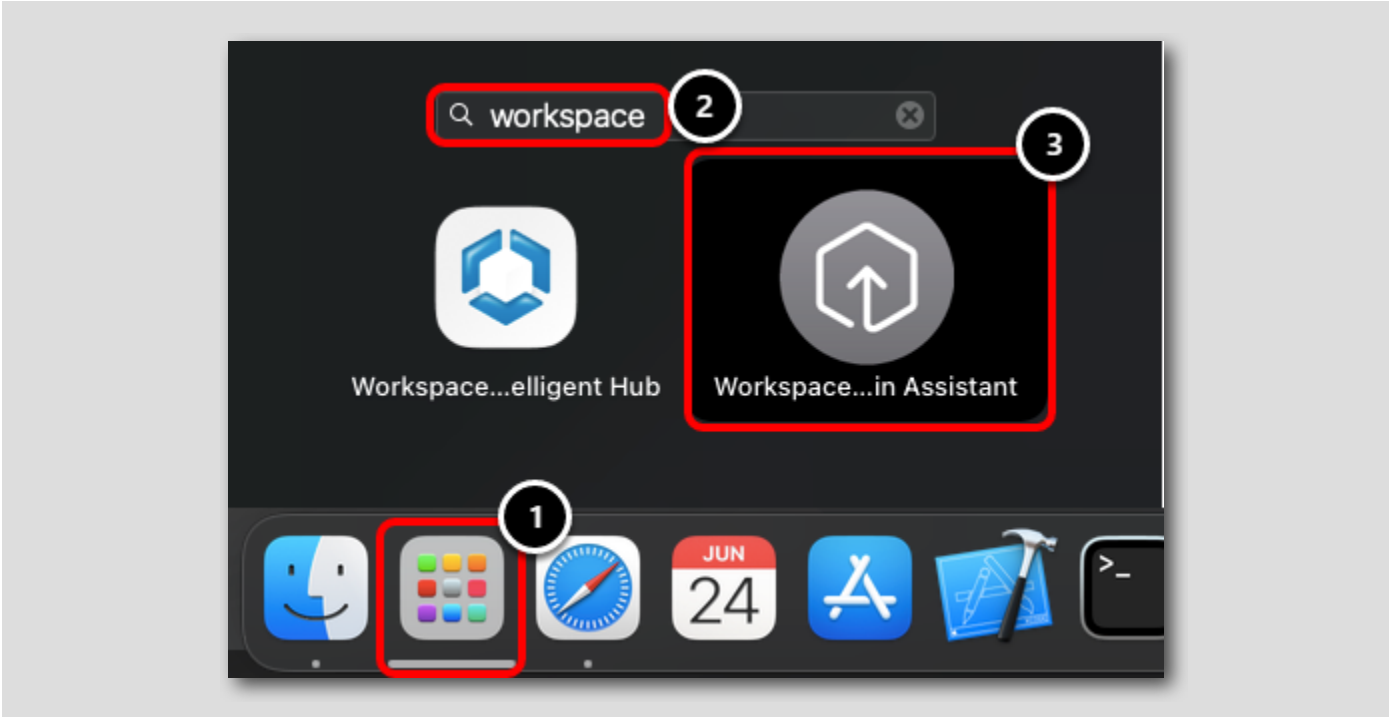
1. Click **Close** when the installer completes
2. Click **Move to Trash** to clean up the installer

Launch VMware Admin Assistant Tool

[268]

NOTE: These steps are optional as the necessary application files are included for you in the Hands-on Lab. If you wish to see how to extract the necessary files for app deployment on macOS, continue with these steps. If not, *CLICK HERE* to continue to uploading the app files.

NOTE: These steps require a macOS device.



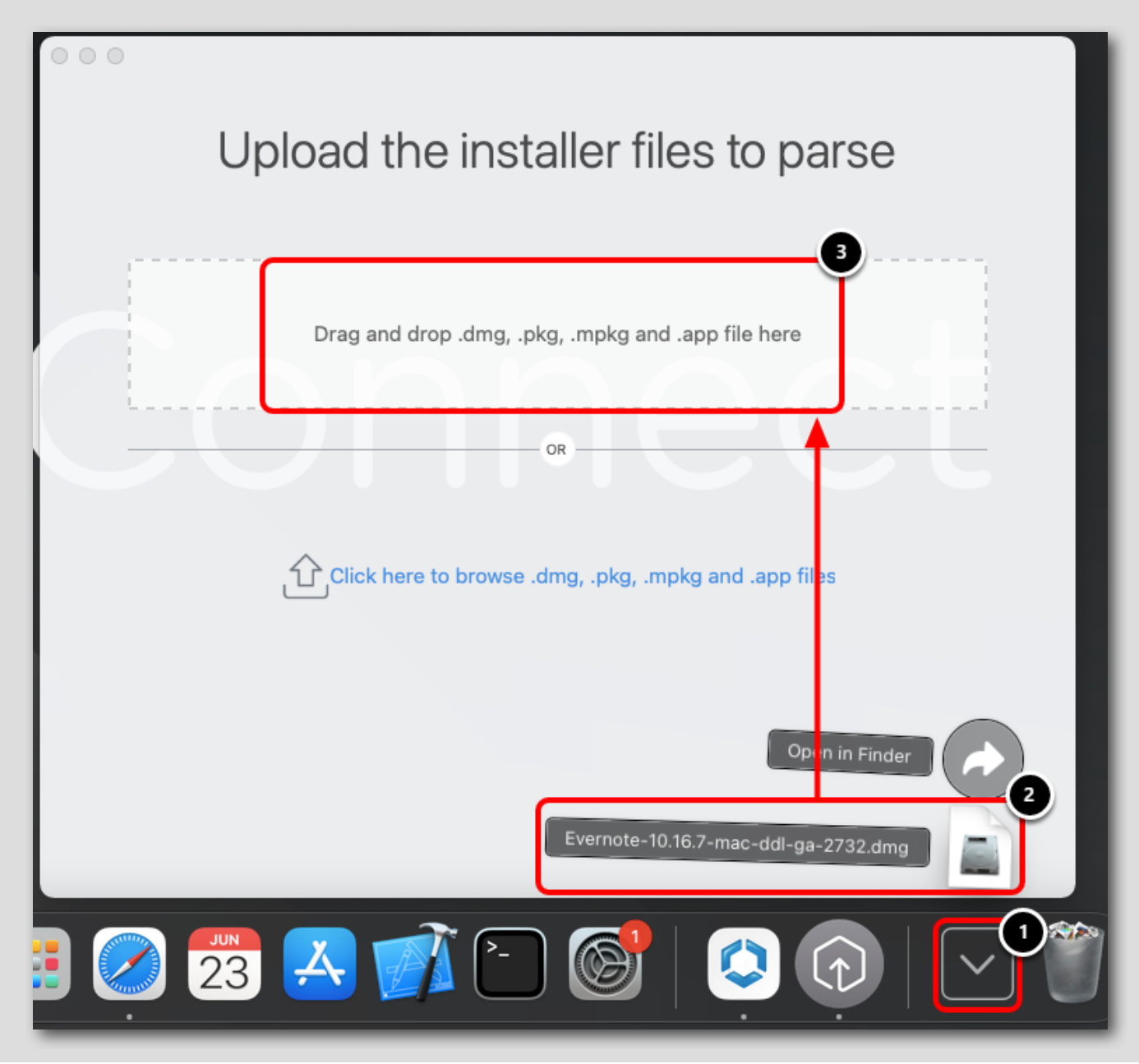
1. Launch **Launchpad**
2. Enter **`Workspace`** in the search bar
3. Click **Workspace ONE Admin Assistant**

Drag and Drop Evernote

[269]

NOTE: These steps are optional as the necessary application files are included for you in the Hands-on Lab. If you wish to see how to extract the necessary files for app deployment on macOS, continue with these steps. If not, *CLICK HERE* to continue to uploading the app files.

NOTE: These steps require a macOS device.



1. With the Workspace ONE Admin Assistant open, click the Downloads folder on the Dock.
2. Click and Drag the **Evernote DMG**.
3. Drag and Drop the **Evernote DMG** onto the Workspace ONE Admin Assistant app file upload section.

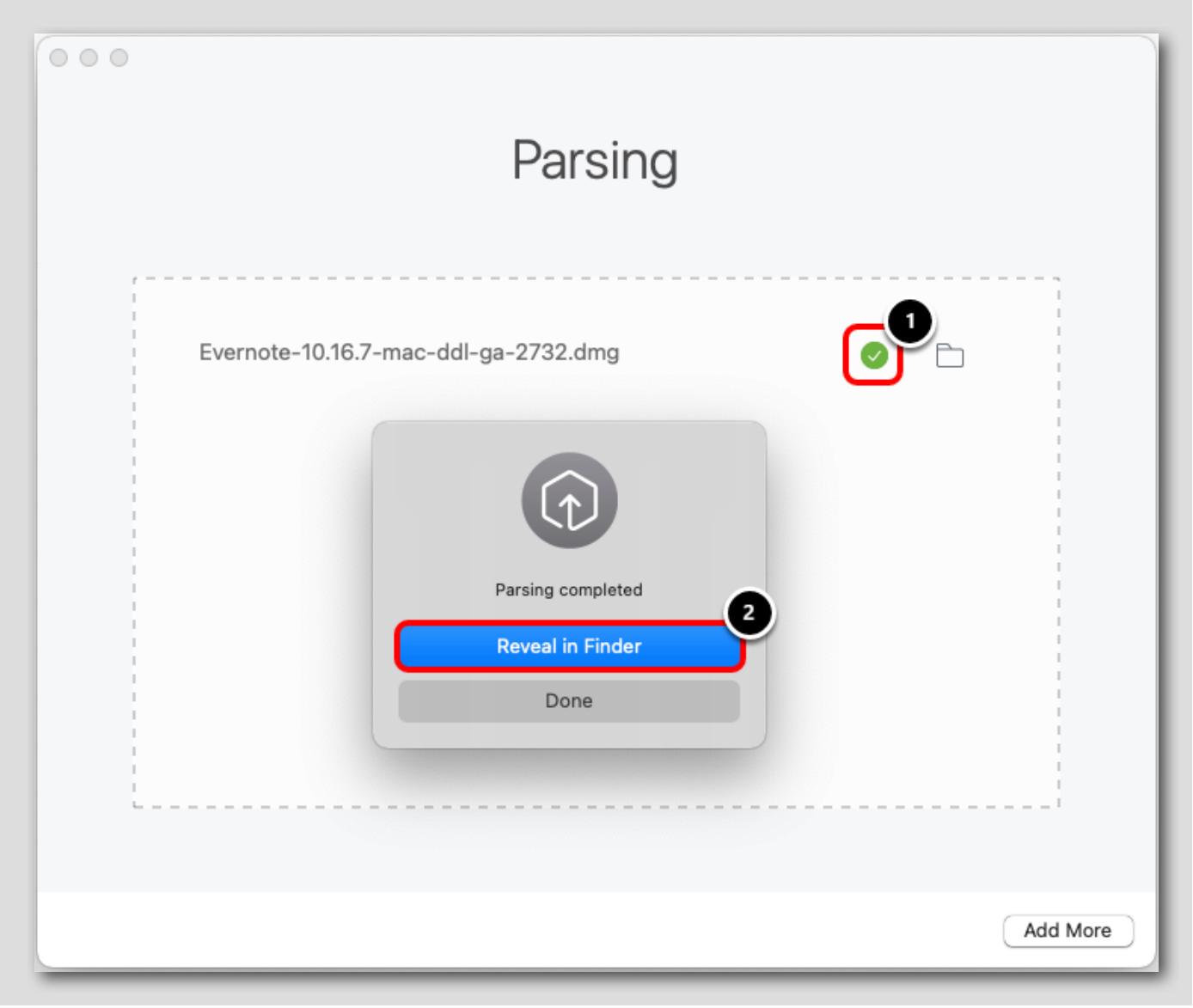
The Workspace ONE Admin Assistant Tool begins parsing the file to extract information necessary to deploy the software.

Monitor Process and Reveal Files

[270]

NOTE: These steps are optional as the necessary application files are included for you in the Hands-on Lab. If you wish to see how to extract the necessary files for app deployment on macOS, continue with these steps. If not, *CLICK HERE* to continue to uploading the app files.

NOTE: These steps require a macOS device.



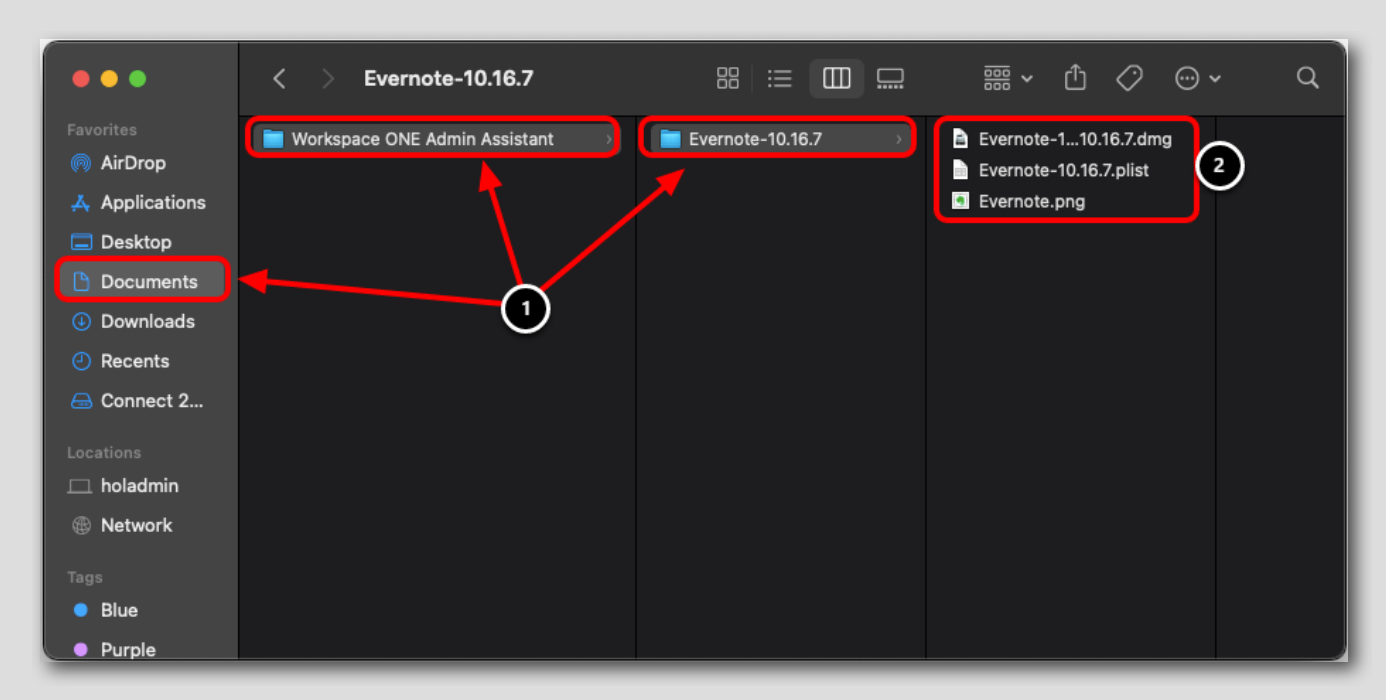
1. Monitor the progress of the parsing. The result will change to a green checkmark when it is completed, which may take 15 - 30 seconds.
2. In the pop-up window, click **Reveal in Finder**

Review Generated Files

[271]

NOTE: These steps are optional as the necessary application files are included for you in the Hands-on Lab. If you wish to see how to extract the necessary files for app deployment on macOS, continue with these steps. If not, *CLICK HERE* to continue to uploading the app files.

NOTE: These steps require a macOS device.



In the Finder window:

1. Note the Path of the Output for the Evernote files: ~/Documents/Workspace ONE Admin Assistant/Evernote-##.##.##
2. Note the output from the Assistant tool as described below:

```
Evernote-##.##.##.dmg -- The Application has been packaged into a DMG file.   (Note: MPKG and PKG fil
Evernote-##.##.##.plist -- A metadata file (referenced as the pkginfo.plist in munki documentation)
Evernote.png -- An icon image extracted from the app used for user-friendly display in the console
```

All output for the Admin Assistant tool follows the convention ~/Documents/Workspace ONE Admin Assistant/{AppName-Version}. At the time this lab was created, Evernote was at version 10.16.7 but may be different depending on when you take this lab.

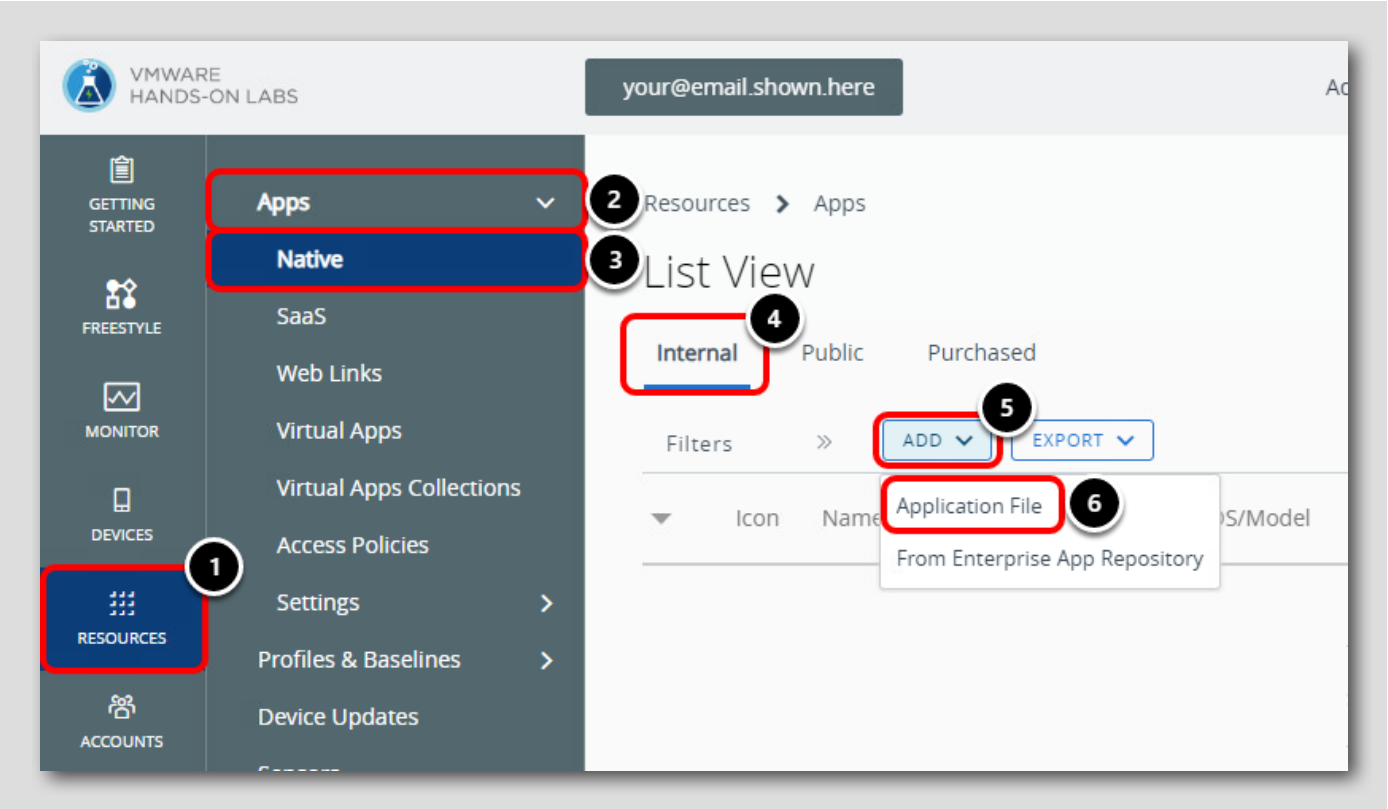
Deploy a 3rd Party macOS Application

[272]

You will now use the provided Workspace ONE Assist dmg and plist files to upload Workspace ONE Assist as a 3rd party macOS application in Workspace ONE UEM.

Add an Application File

[273]

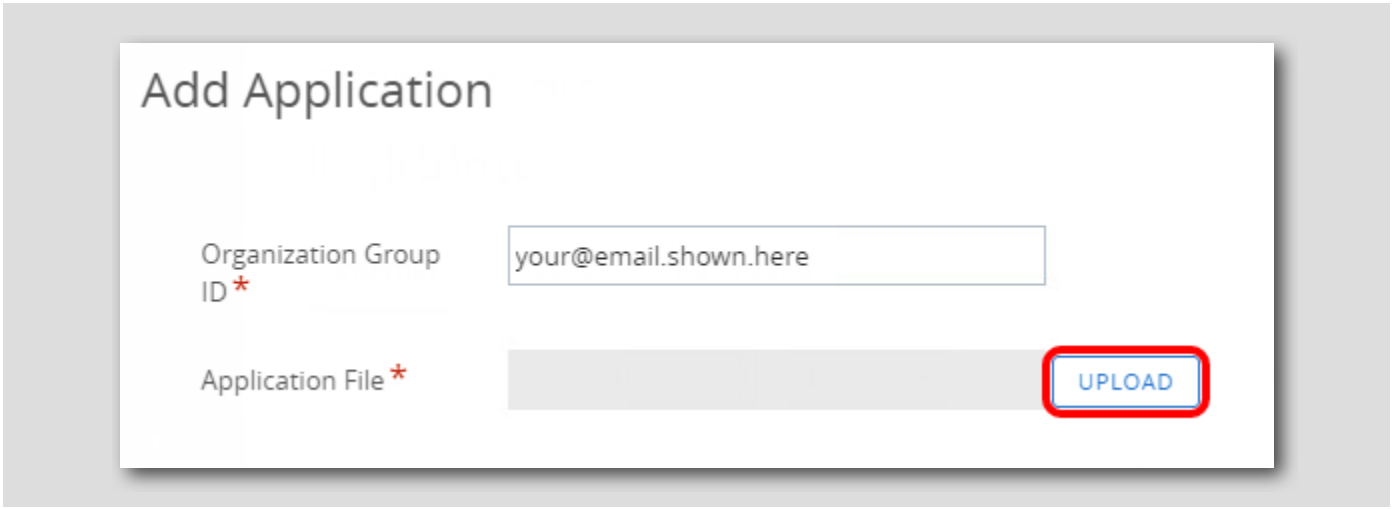


Return to the the Workspace ONE UEM Administrator Console in the Hands-on Lab interface:

1. Click **Resources**
2. Expand **Apps**
3. Click **Native**
4. Click the **Internal** tab
5. Click **Add**
6. Click **Application File**

Upload the Application File

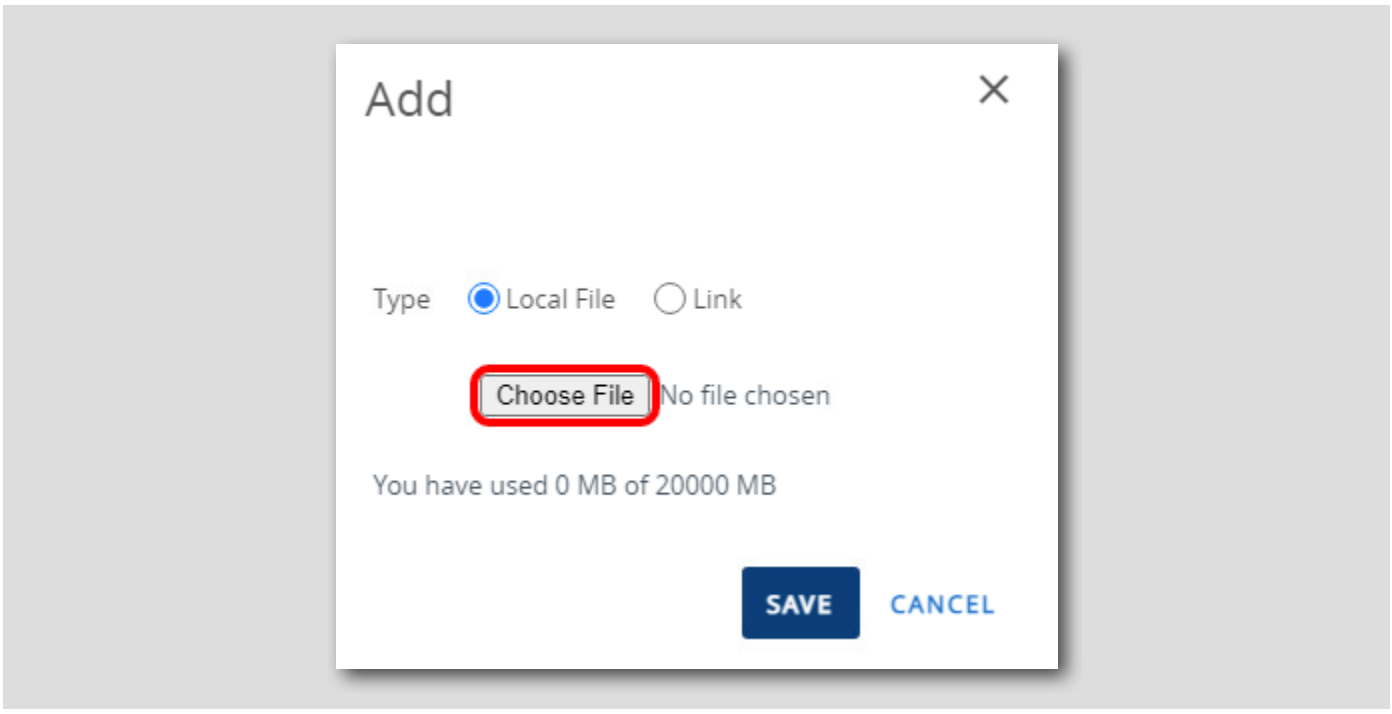
[274]



Click **Upload**.

Choose File for Upload

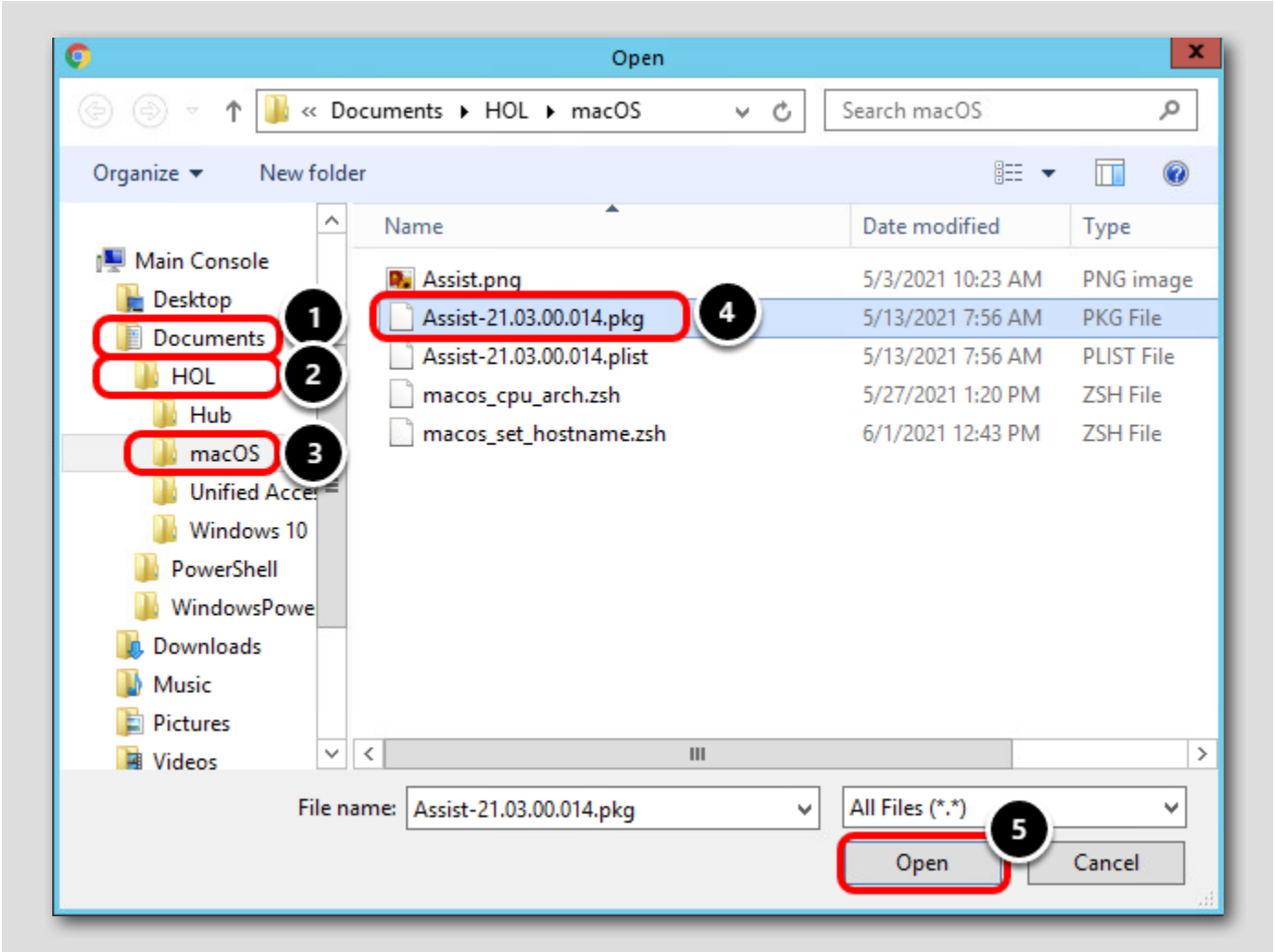
[275]



Click **Choose File**.

Select the Assist PKG File

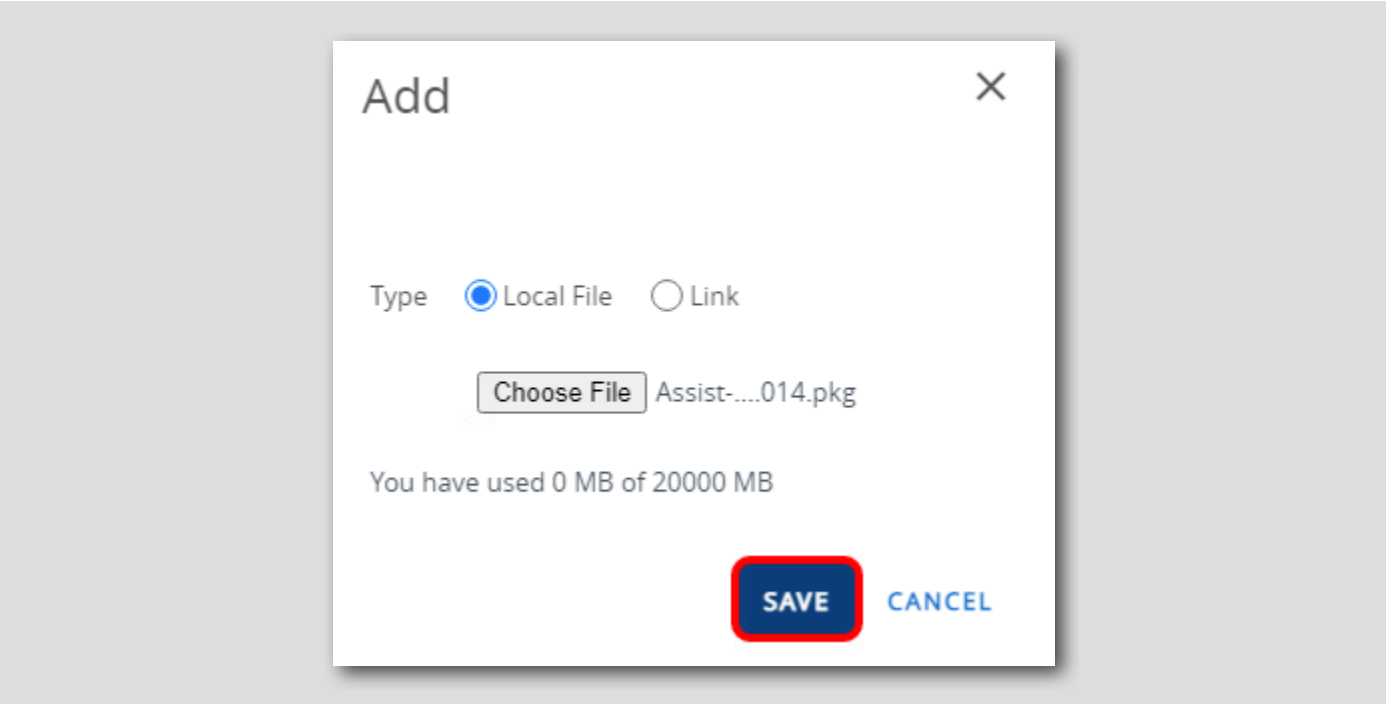
[276]



1. Click **Documents**
2. Click **HOL**
3. Click **macOS**
4. Click **Assist-21.03.00.014.pkg**
5. Click **Open**

Upload the Assist PKG File

[277]

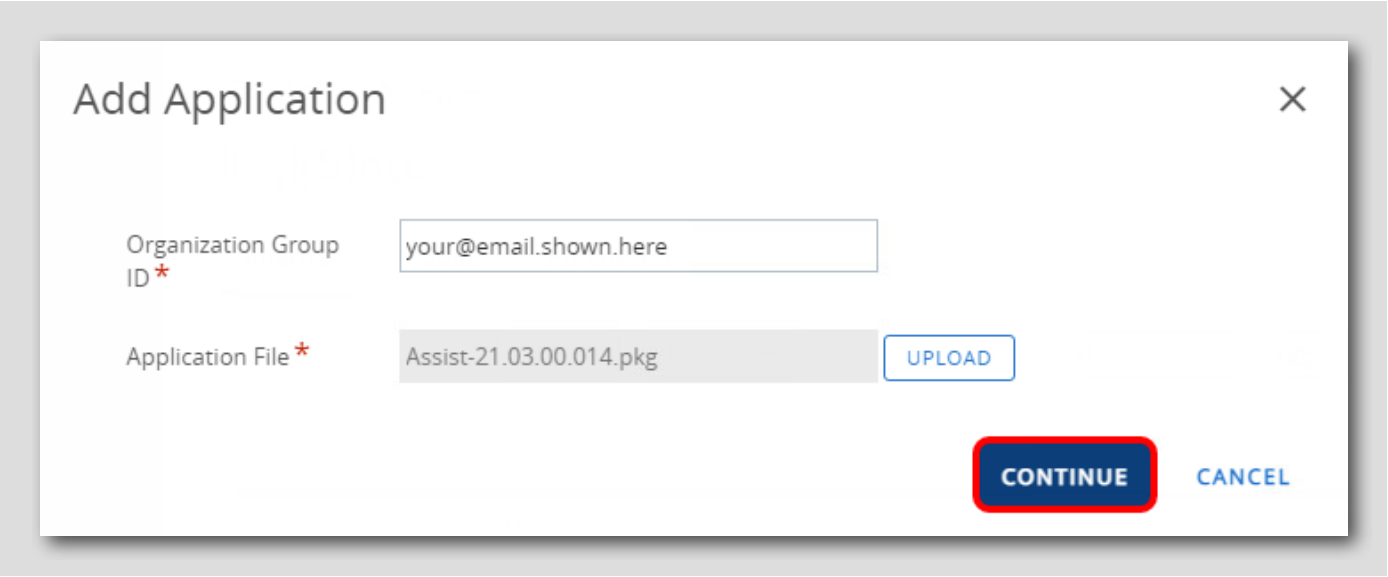


Click **Save** to upload the select Assist-21.03.00.014.pkg file.

NOTE: The pkg file may take 1-2 minutes to upload! Continue to the next step once the upload finishes.

Continue After Uploading Application

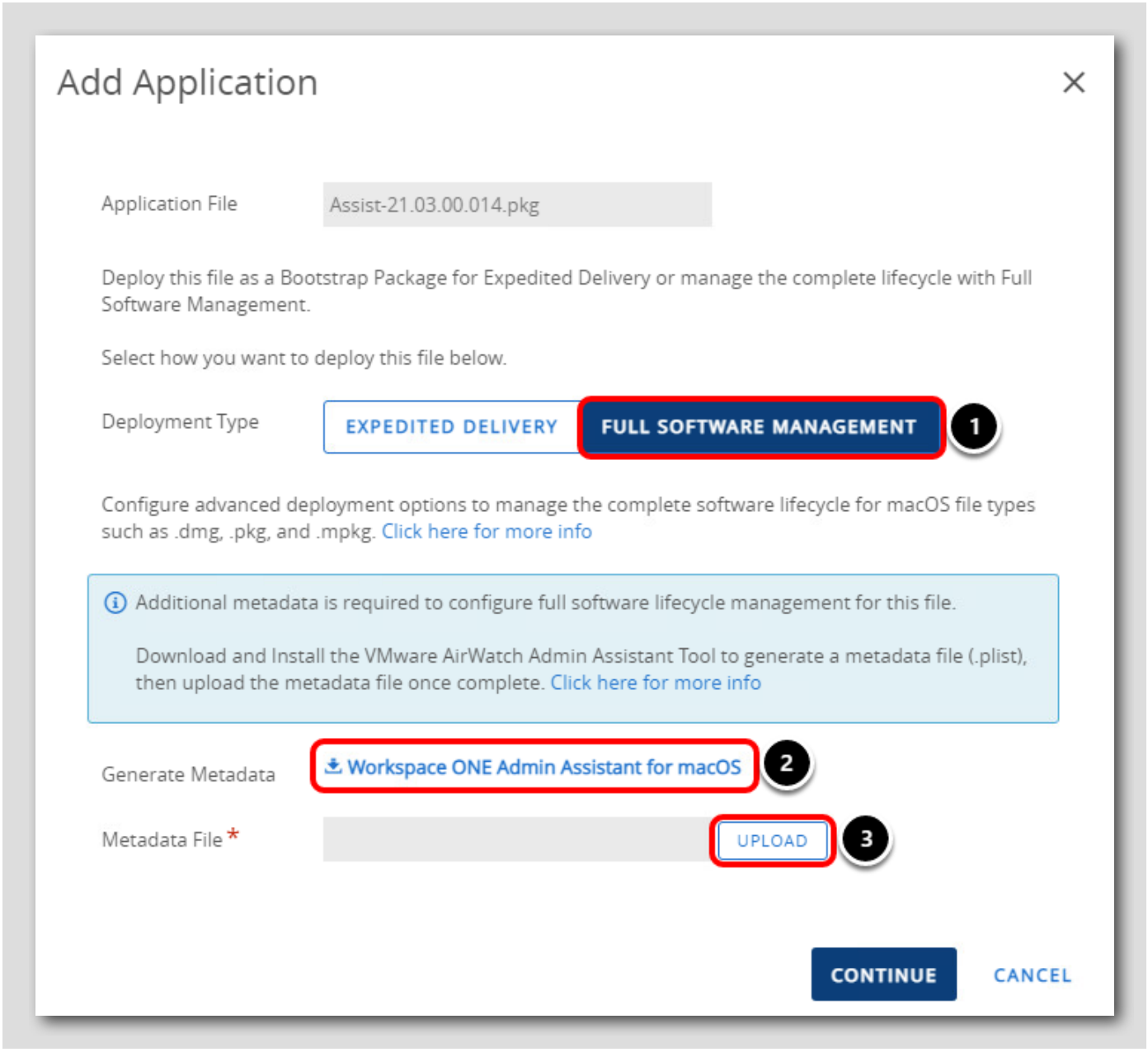
[278]



Click **Continue**.

Configure Deployment Type

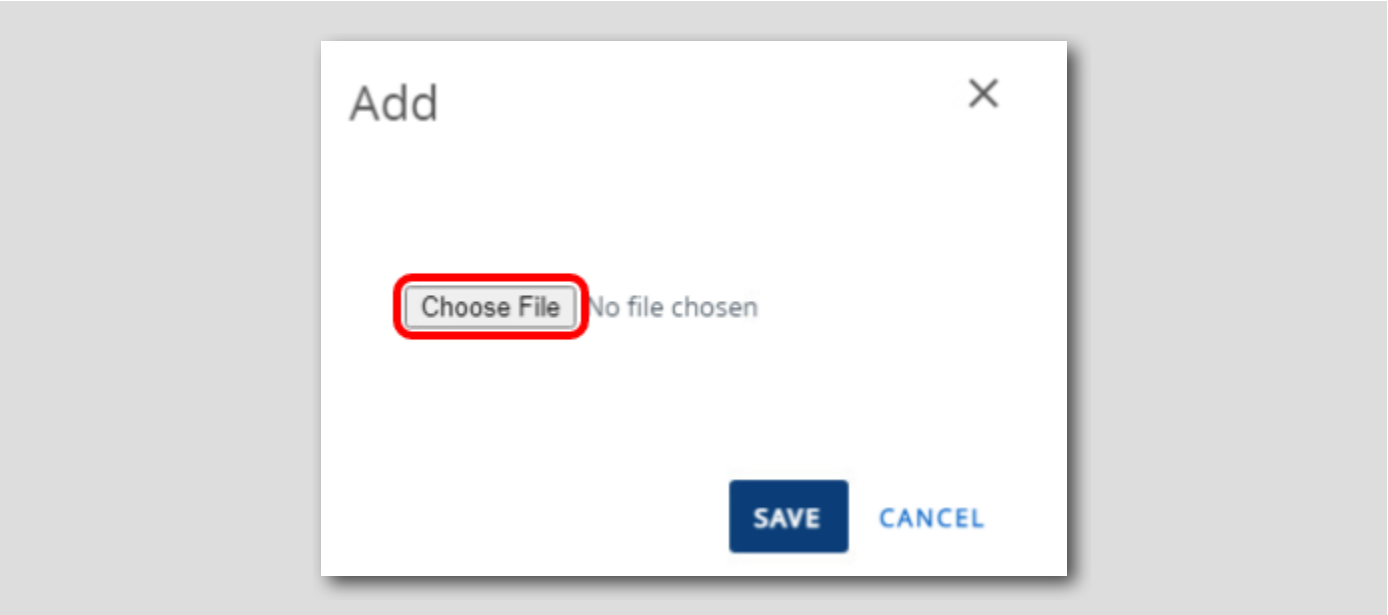
[279]



1. Select **Full Software Management** for the Deployment Type
2. The Workspace ONE Admin Assistant for macOS can be downloaded from this page if needed. This is for informational purposes only, you do not need to download the Workspace ONE Admin Assistant as we have already reviewed how to utilize the app on a macOS device in previous steps.
3. Click **Upload** to provide the Metadata file for this app.

Choose Metadata File

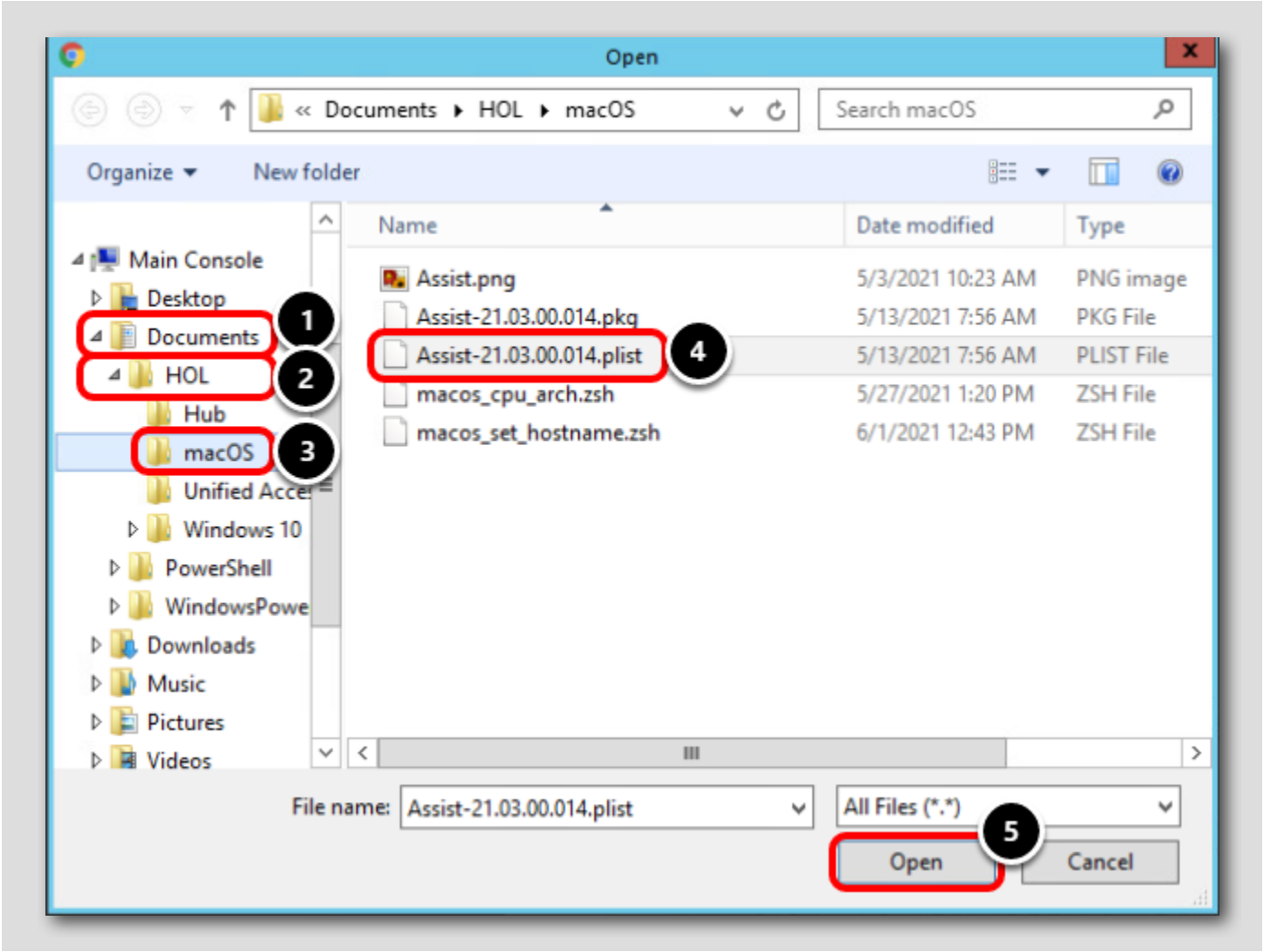
[280]



Click **Choose File**.

Select the Workspace ONE Assist plist File

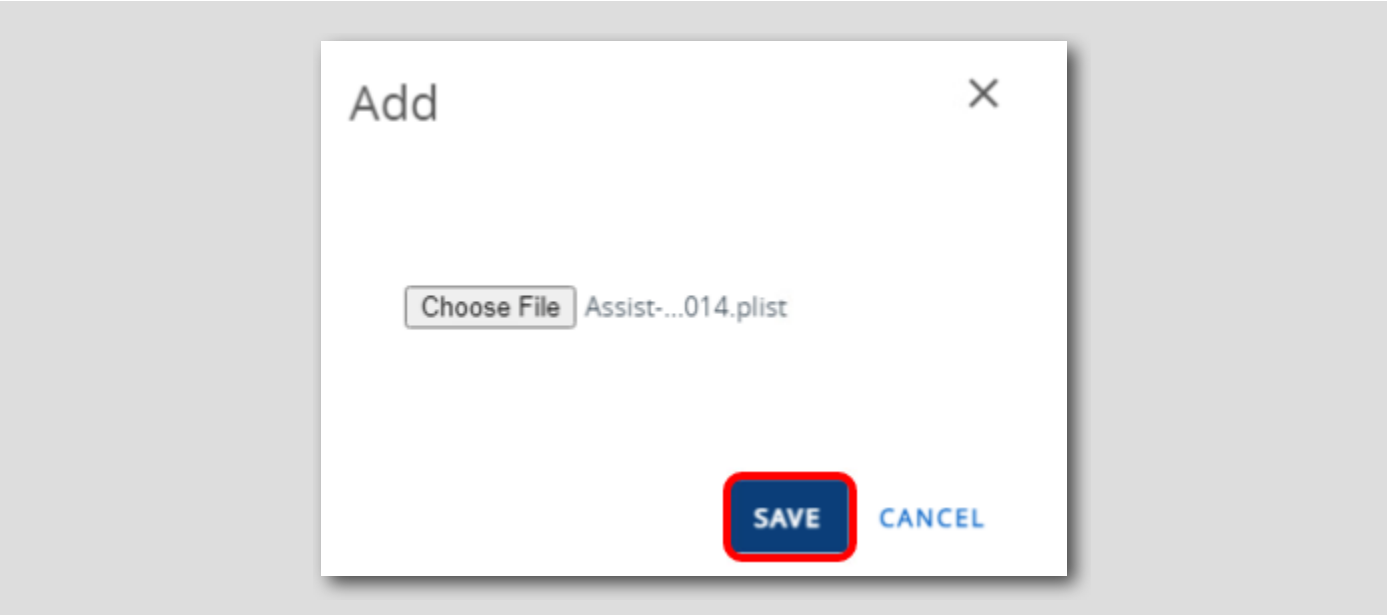
[281]



1. Click **Documents**
2. Click **HOL**
3. click **macOS**
4. Click **Assist-21.03.00.014.plist**
5. Click **Open**

Upload the Assist plist File

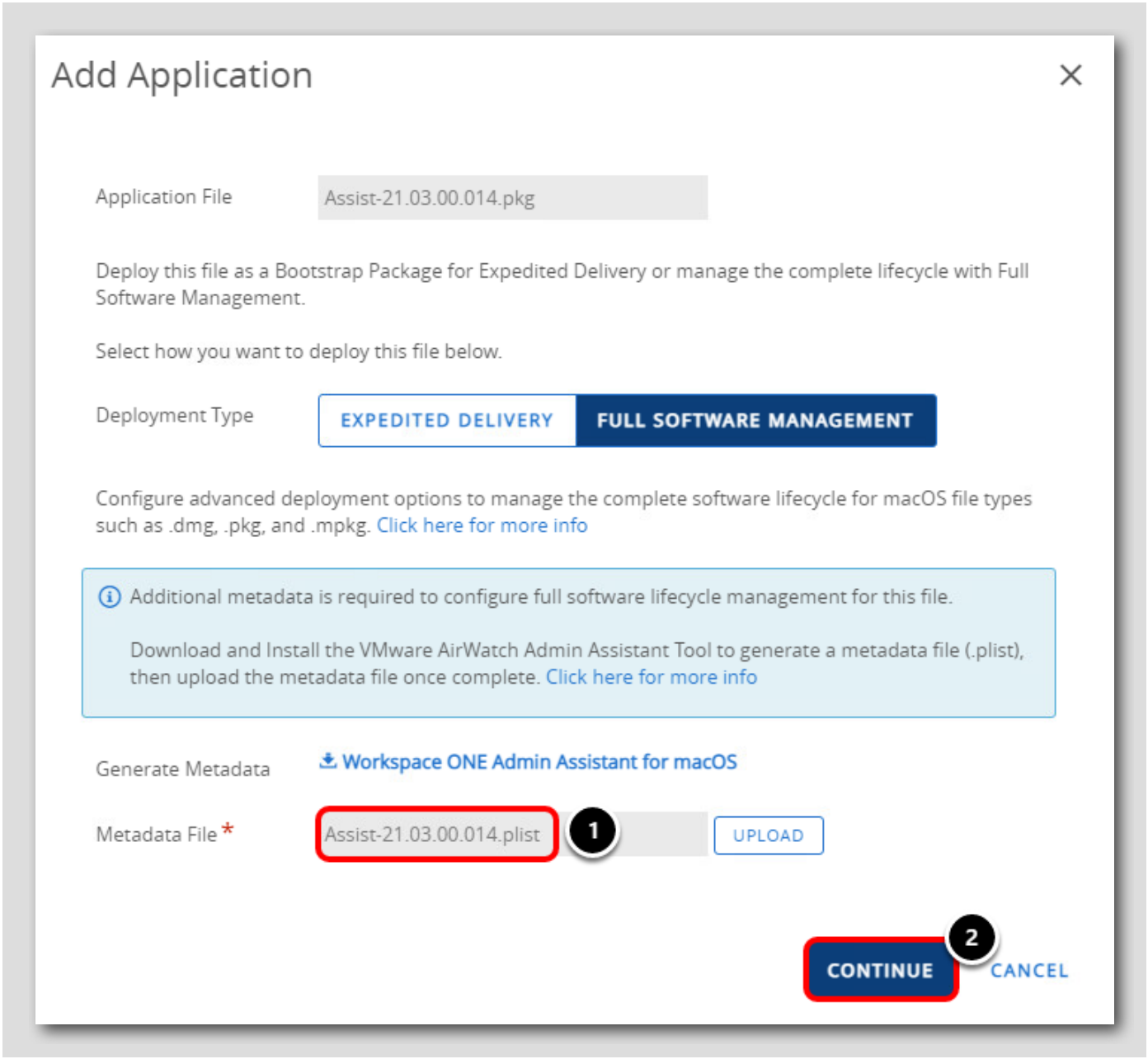
[282]



Click **Save** to upload the selected Assist-21.03.00.014 plist file.

Continue after Metadata File Upload

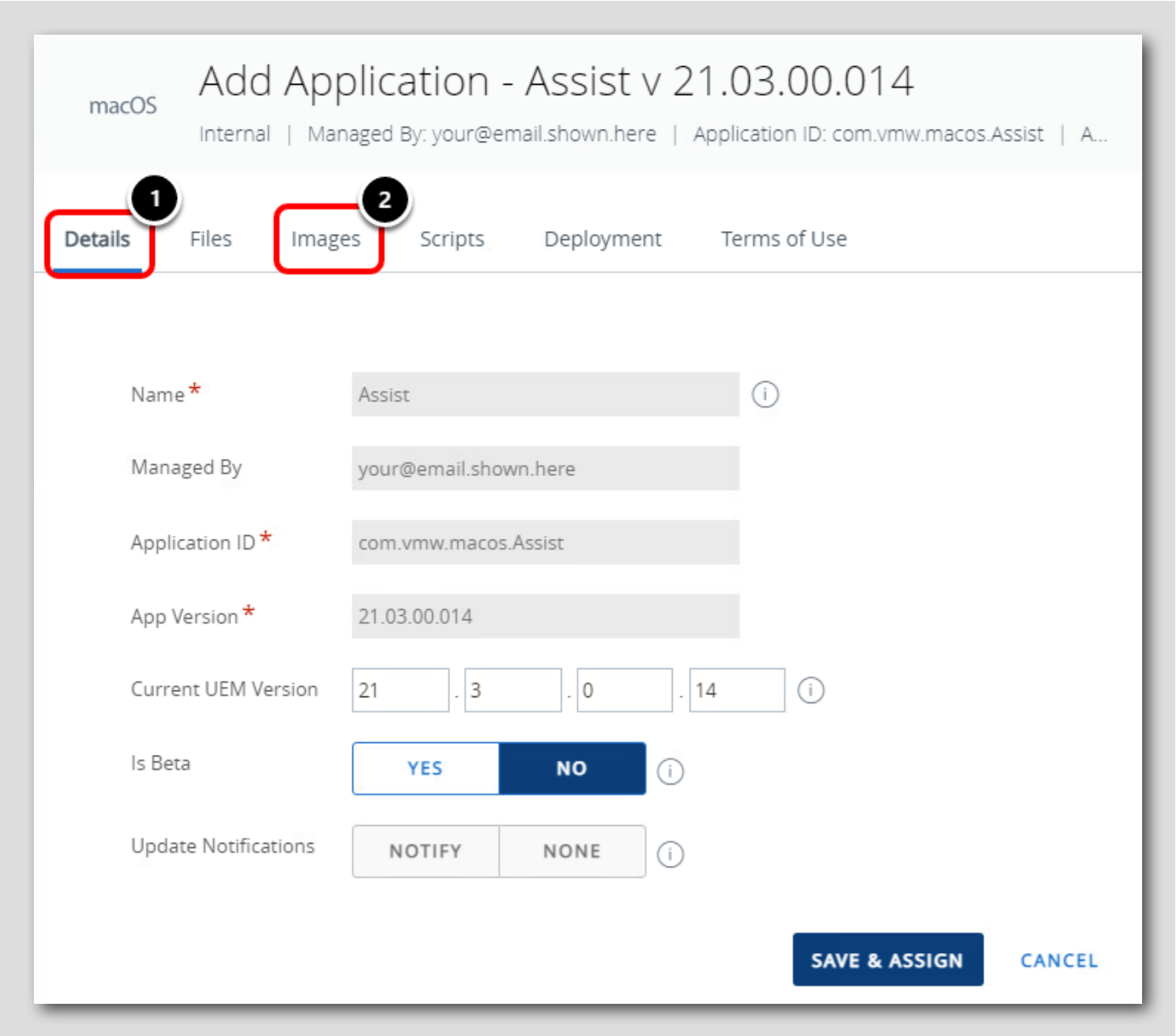
[283]



1. The Assist metadata file is now uploaded.
2. Click **Continue**.

Configure the Application

[284]

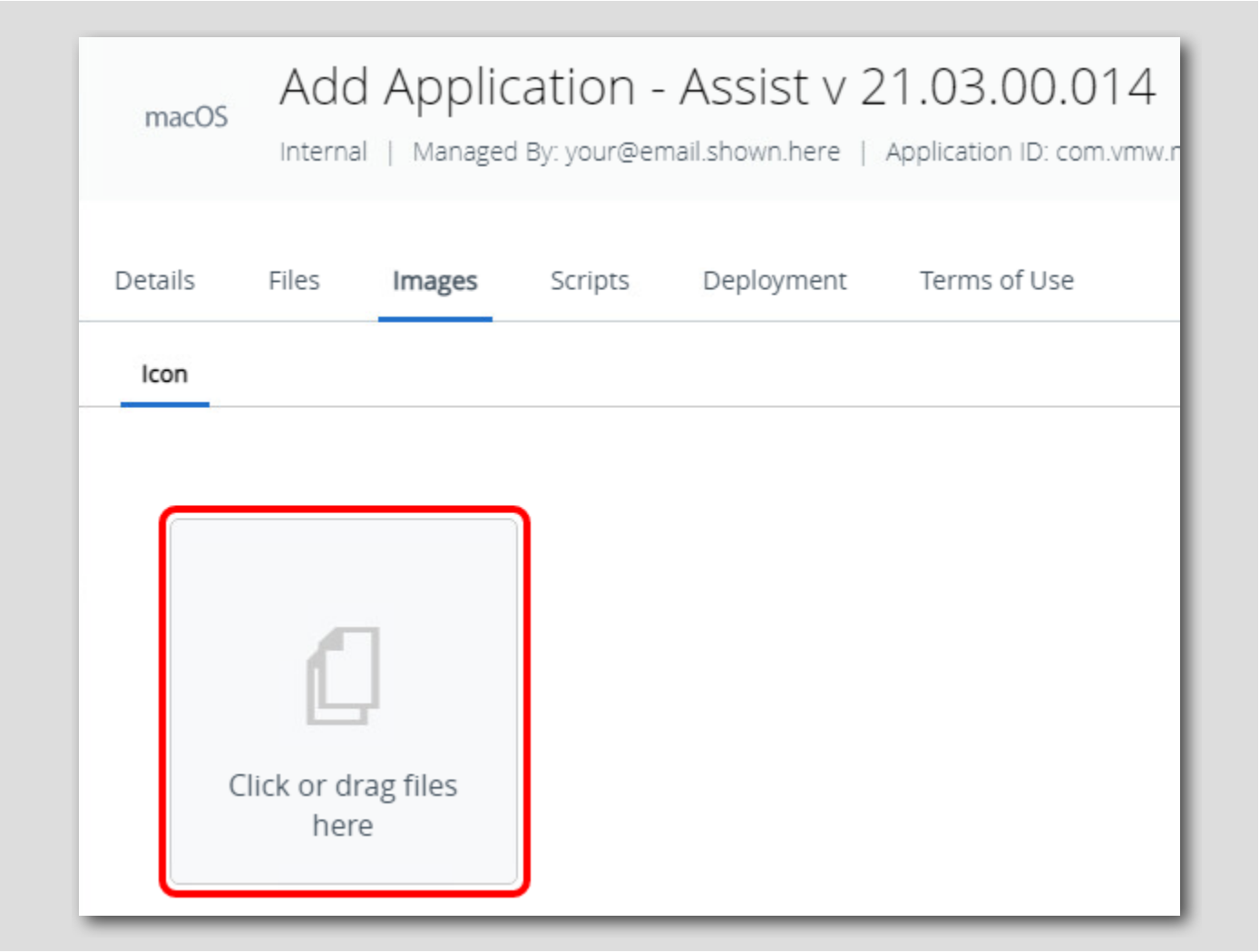


The Workspace ONE Assist application and corresponding metadata have been uploaded to Workspace ONE UEM!

1. The **Details** tab contains the application ID, version, supported device models, and more. This information is gathered from the provided plist metadata. Feel free to review the Details and other tabs as desired but do not make any changes!
2. Click the **Images** tab.

Configure an Application Icon

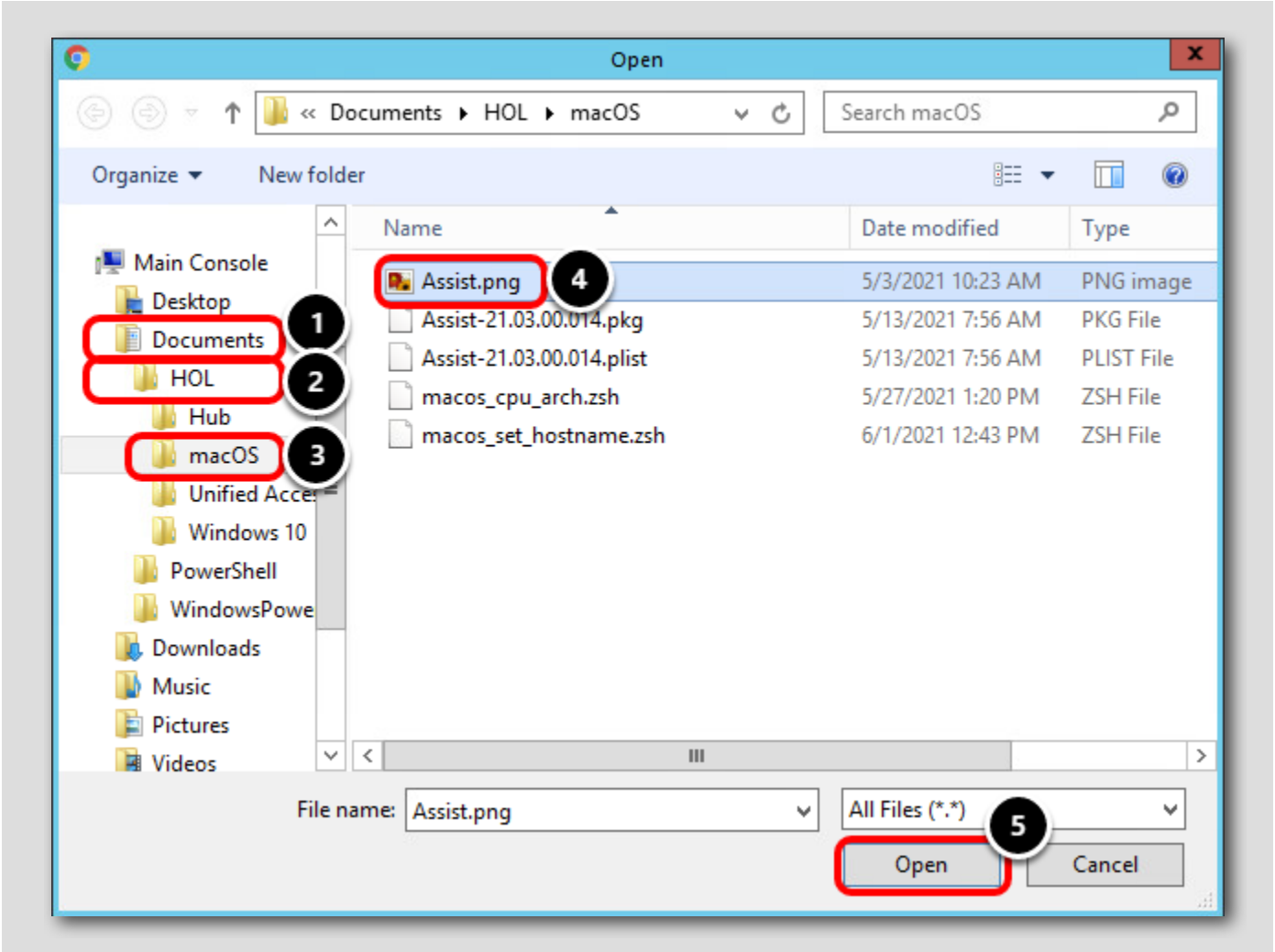
[285]



You will need to add an icon for the application, which will be displayed in the app catalog and on the user's device once installed. Click the **click or drag files here** area to upload an image.

Select the Assist Icon

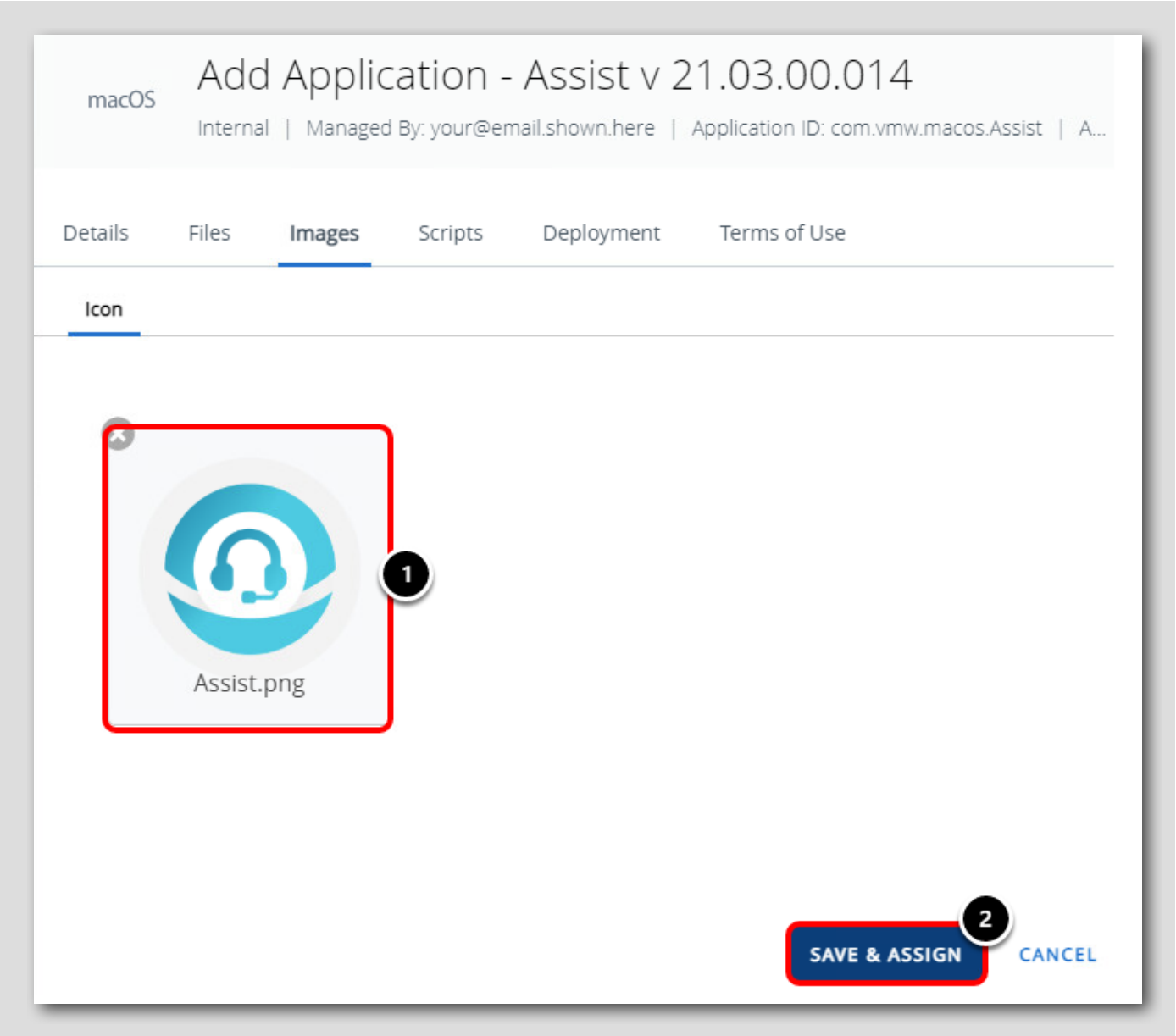
[286]



1. Click **Documents**
2. Click **HOL**
3. Click **macOS**
4. The Workspace ONE Admin Assistant tool will also extract and provide an image to use. That image has been made available to you as Assist.png. Click **Assist.png**.
5. Click **Open**

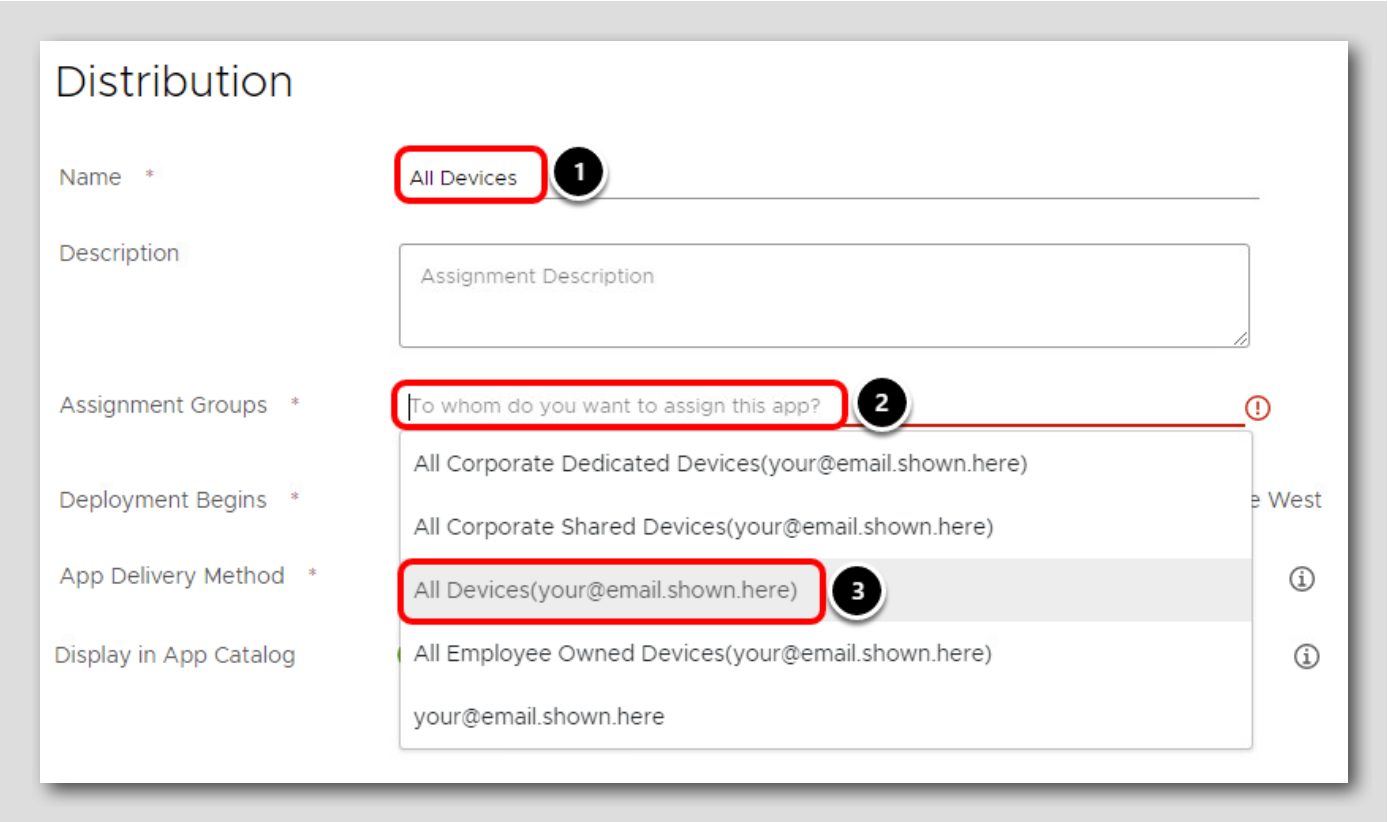
Confirm the Icon and Save

[287]



1. You can preview the uploaded icon here.
2. Click **Save & Assign** to configure which devices and users will receive the uploaded Workspace ONE Assist application.

Configure Application Assignment

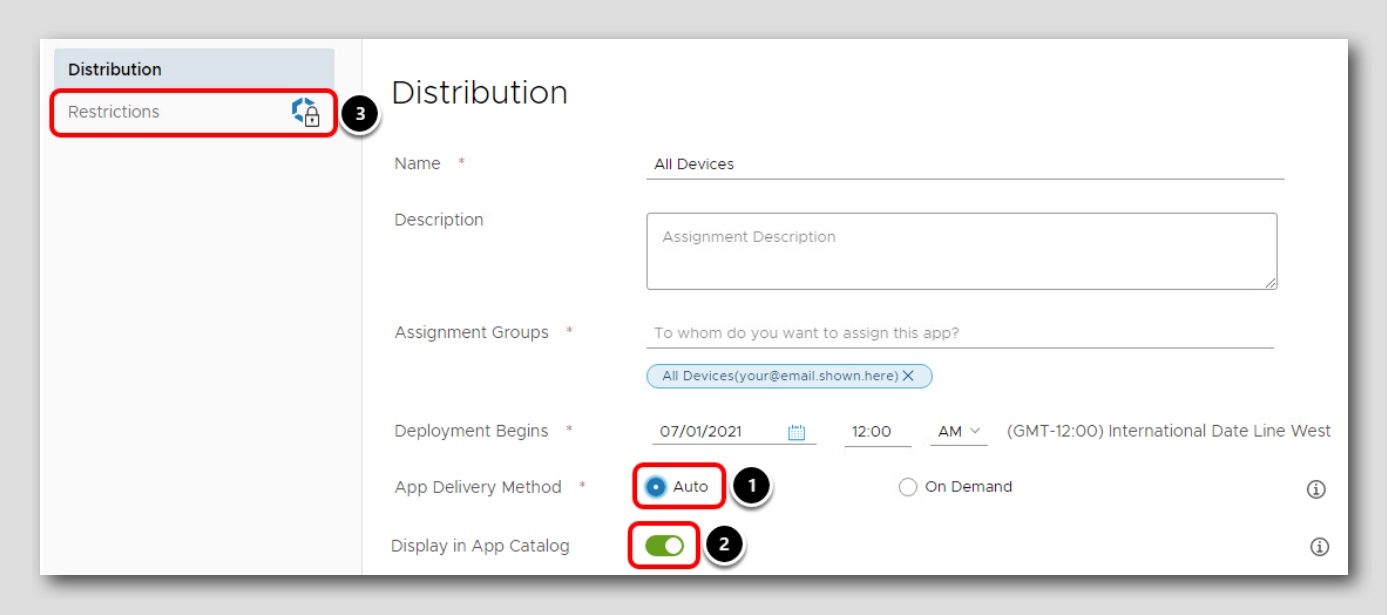


The Application Assignment determines which users and devices will receive the Workspace ONE Assist and how the app will be delivered. You will create an assignment rule that will publish the application automatically (installs the app without requiring user input) to all devices in your organization.

1. Enter a descriptive name for the assignment, such as **`All Devices`**.
2. Click the **Assignment Groups** section to see a list of available assignment groups.
3. Select **All Devices (your@email.shown.here)**. This will cause the app to be distributed to all eligible devices enrolled in your organization.

Update App Delivery Method

[289]



1. Select **Auto** for the App Delivery Method.

   Auto means the application will be published and installed on the device as soon as possible and without any user interaction needed. On Demand makes the app available to the device but does not begin an install, which can either be triggered by the user through the App Catalog or Self Service Portal or by an Administrator through the Workspace ONE UEM administration console.

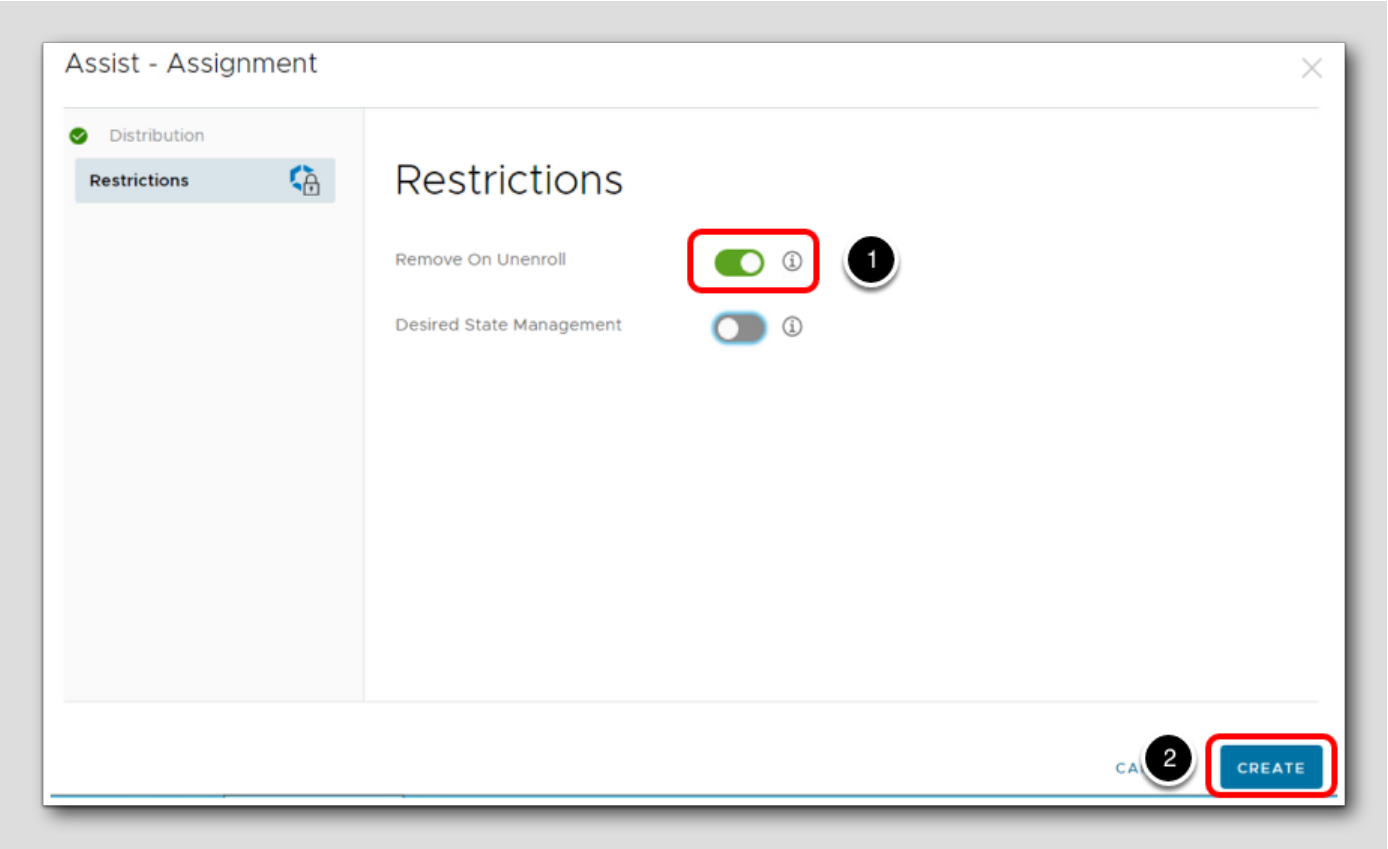
2. Keep the Display in App Catalog option as **Enabled**.

   This will show the Workspace ONE Assist app to the user in the app catalog, allowing them to install or reinstall the app if needed.

3. Click **Restrictions**.

Enable App Restrictions

[290]

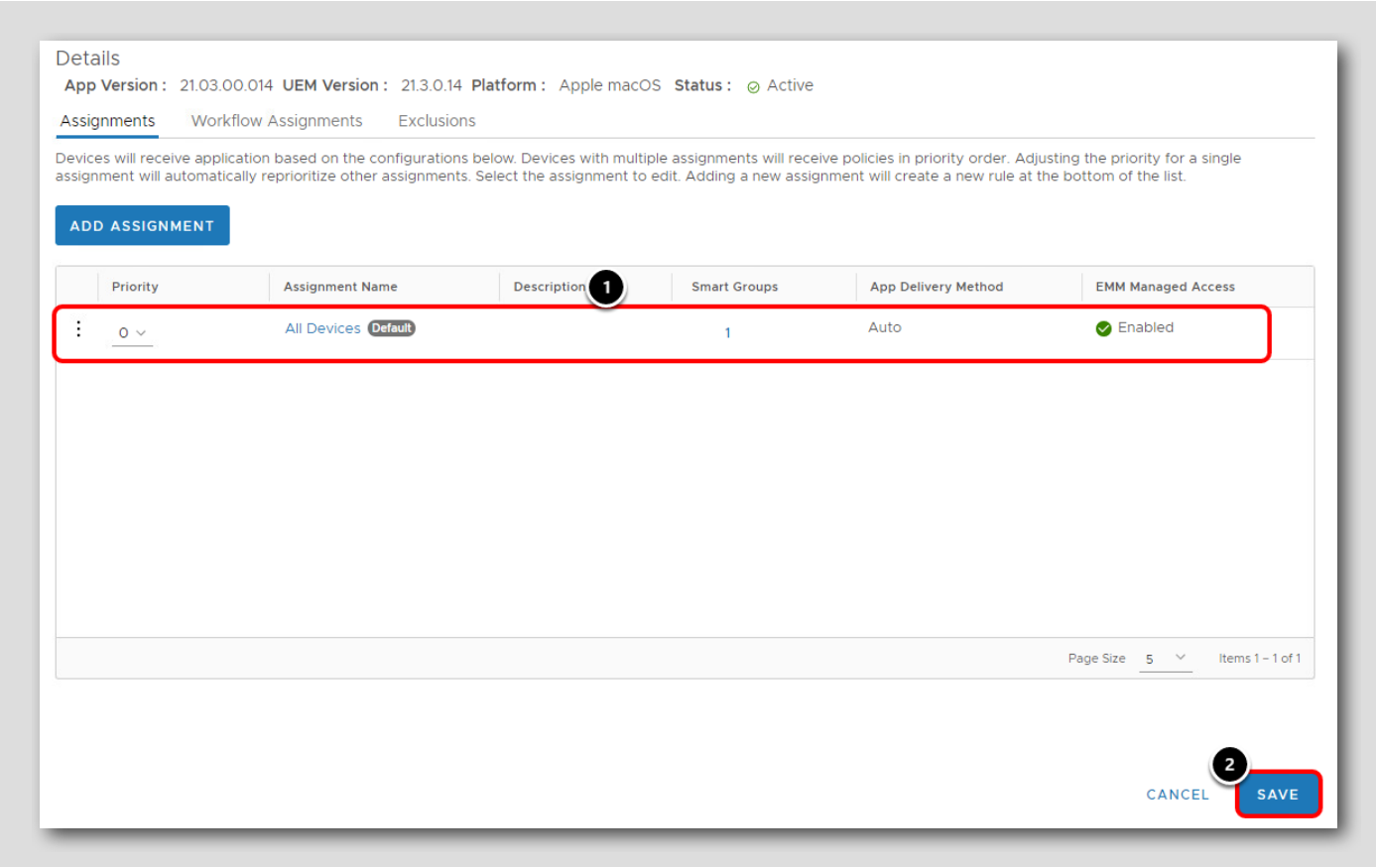


Restrictions can be applied to the assignment to change the behavior of the application.

1. Click to **enable** the Remove on Unenroll restriction. This means that the Workspace ONE Assist app will be automatically removed from the user's device when the device is unenrolled (meaning it is no longer managed by Workspace ONE UEM).
2. Click **Create**.

Save the App Assignment

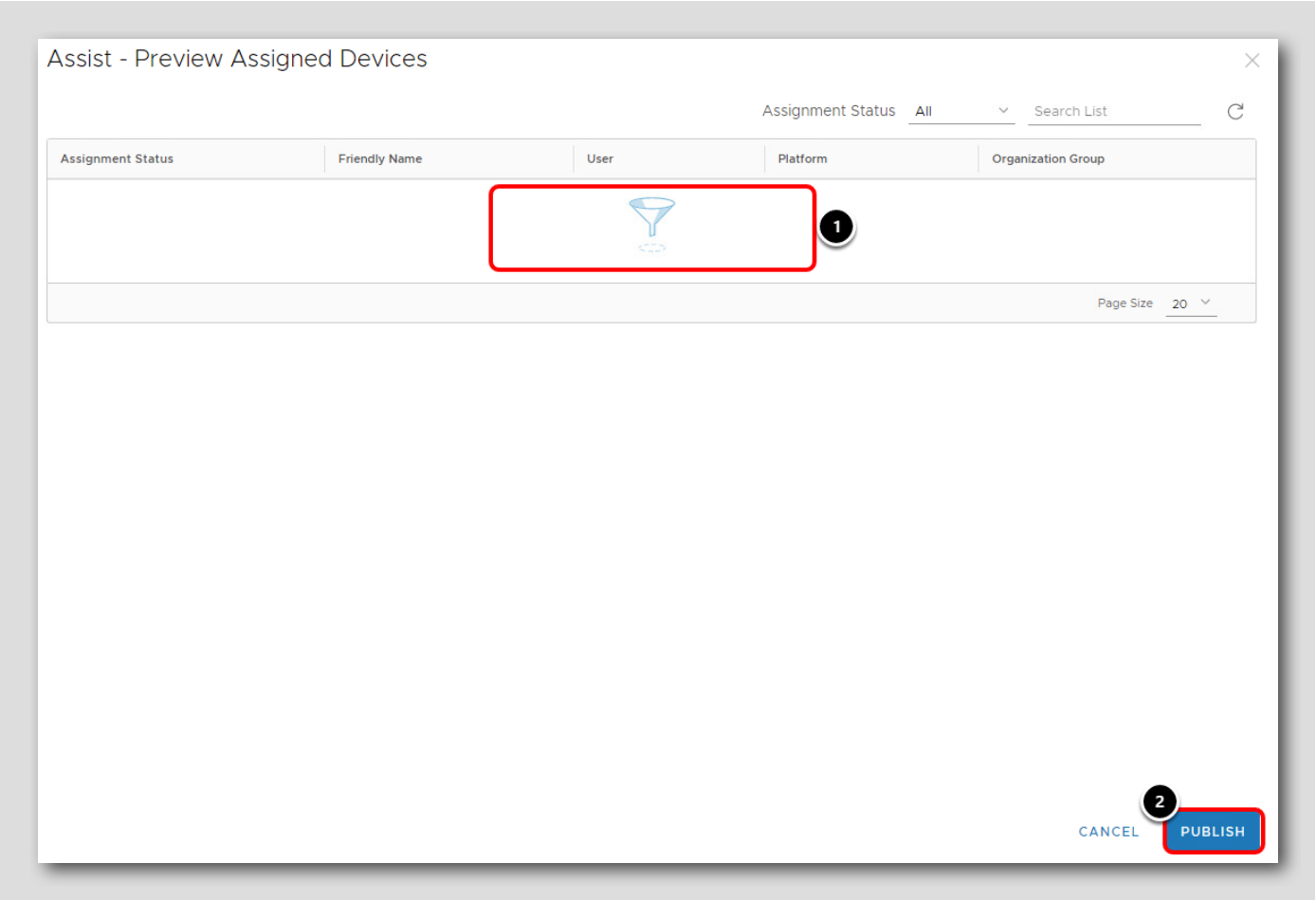
[291]



1. You can confirm and edit your Assignments from this view. You can have multiple assignments that can be ordered by priority to determine which one is applied to devices that overlap multiple assignment types. For this simple use case, you will just leverage the single assignment to apply to all macOS devices in your organization.
2. Click **Save**.

Publish the Application

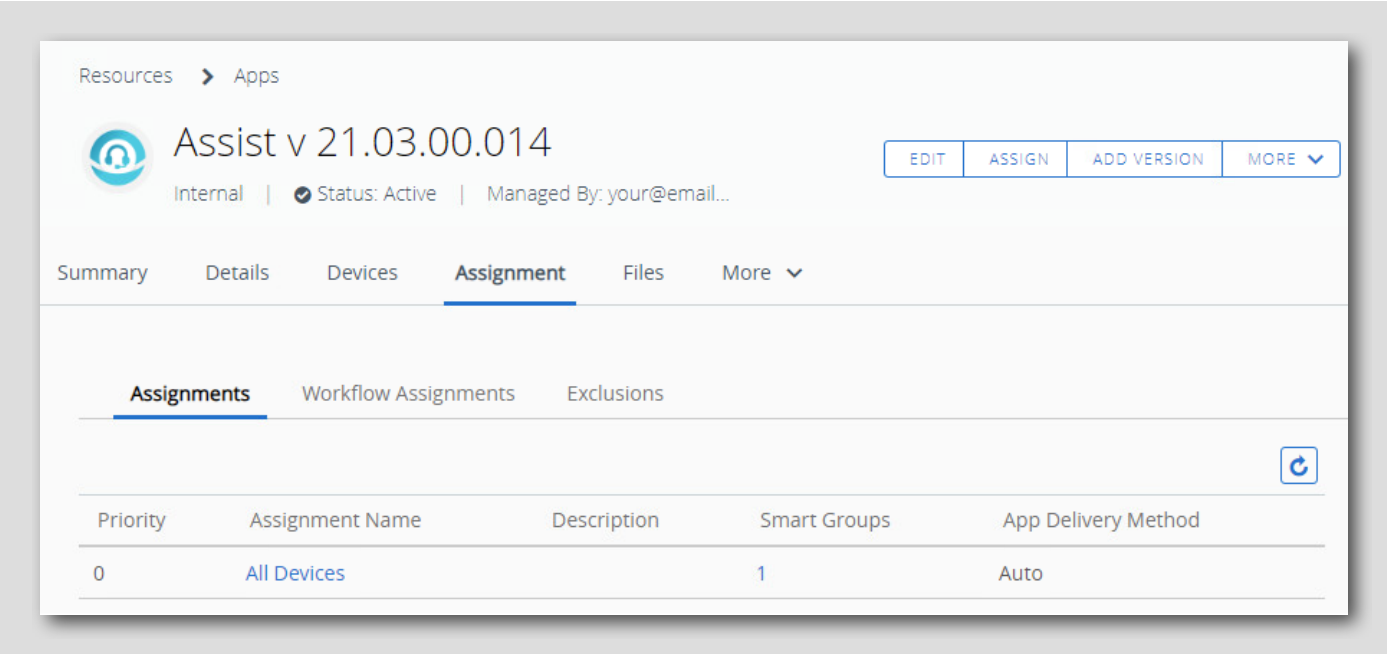
[292]



1. A list of devices that will receive this app are displayed here. The list is empty because you have not yet enrolled a macOS device.
2. Click **Publish**.

Confirm the Application was Published

[293]



The Workspace ONE Assist app is now published! Any macOS device enrolled into your organization will now automatically be assigned the Workspace ONE Assist app and it will install without user interaction. When the device is unenrolled, the app will automatically be removed from the device.

You can return to this view (Resources > Native > Internal) and click the Workspace ONE Assist app to make changes to it in the future as needed, such as updating the assignments, adding a new app version, etc.

Continue to the next step.

Configure Post-Enrollment Onboarding Experience

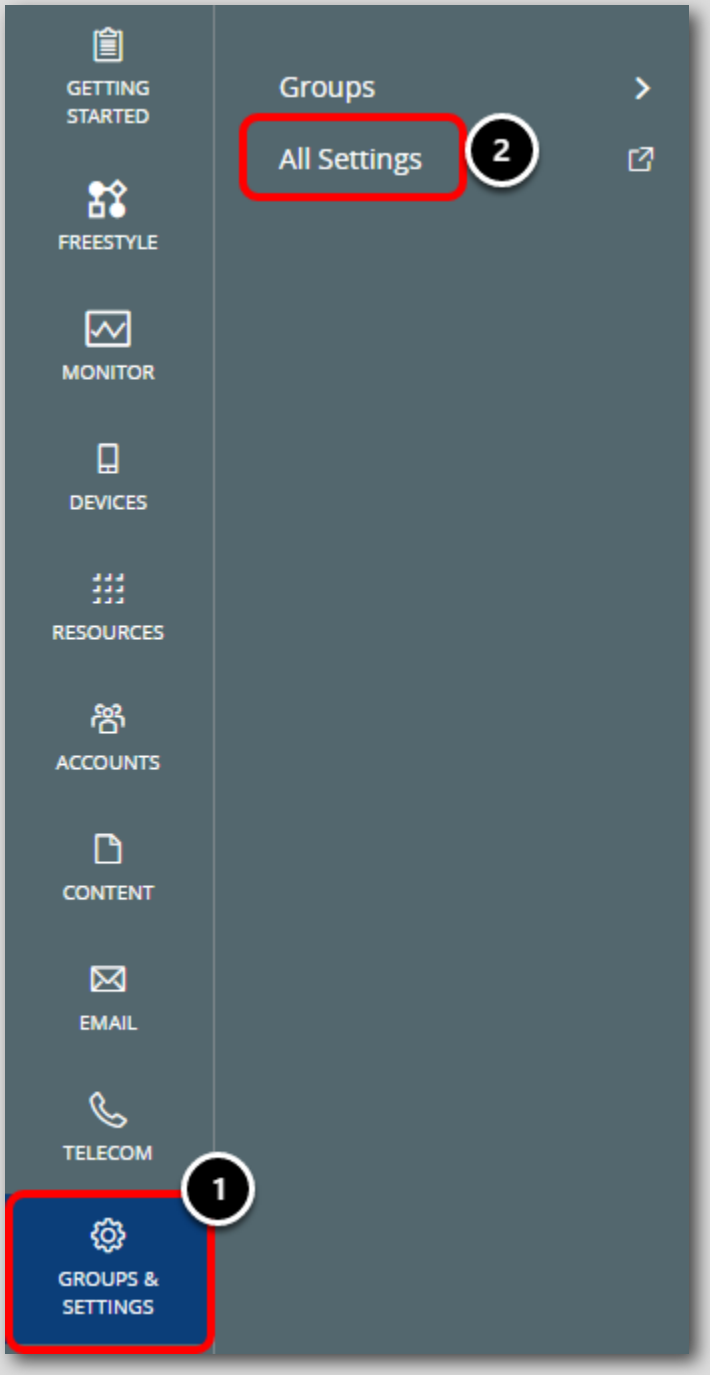
[294]

Administrators can now keep users informed on the device provisioning process after enrollment completes by enabling the post-enrollment onboarding experience in Workspace ONE UEM Intelligent Hub. After enrollment is finished, Intelligent Hub will display a new window which tracks all incoming application installs. Administrators can enable and customize the experience in the Workspace ONE UEM administrator console.

This feature requires Workspace ONE UEM 21.05 or later and and Workspace ONE Intelligent Hub 21.04 or later.

Enable Post-Enrollment Onboarding Experience

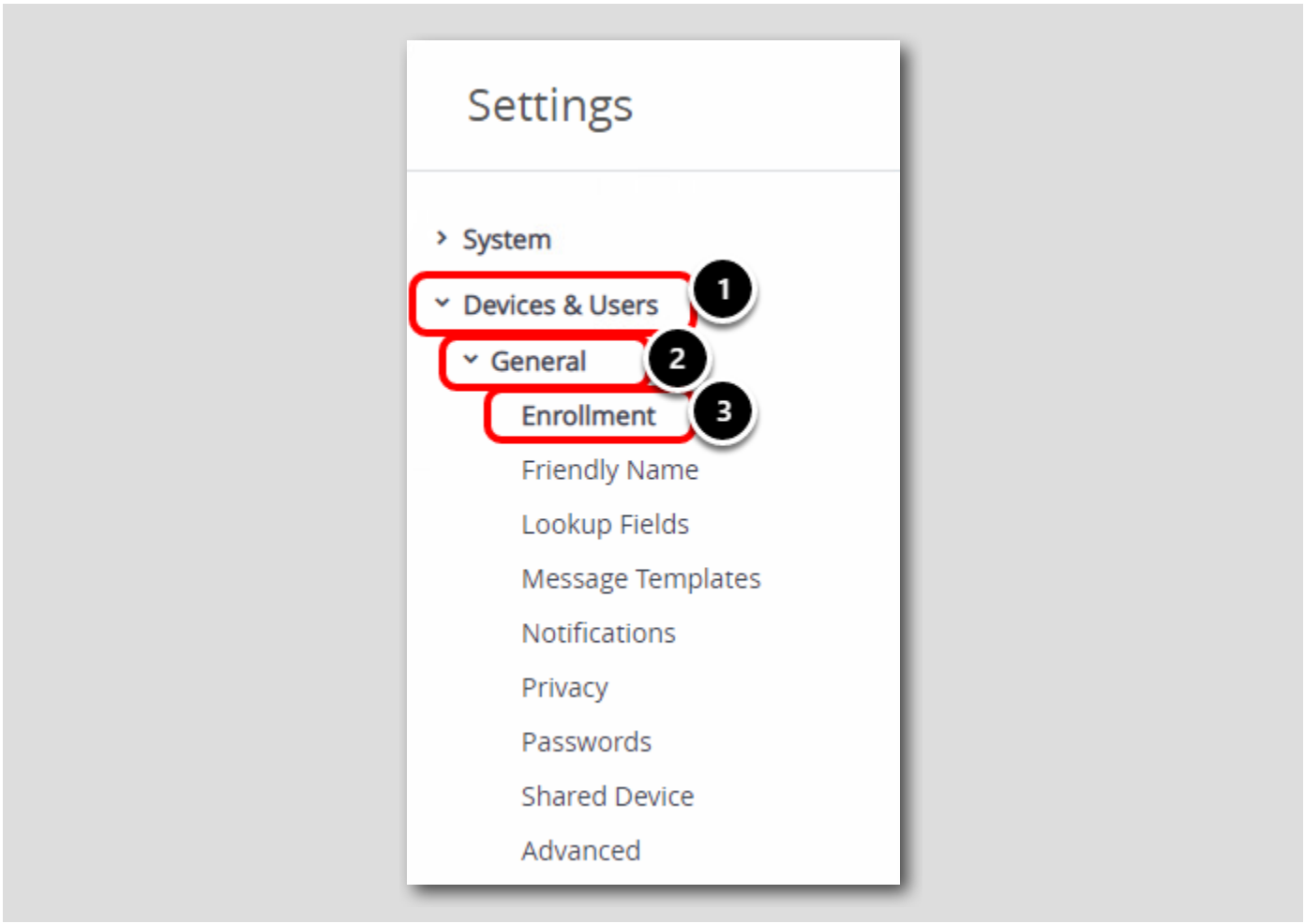
[295]



1. Click **Groups & Settings**
2. Click **All Settings**

Navigate to Enrollment Settings

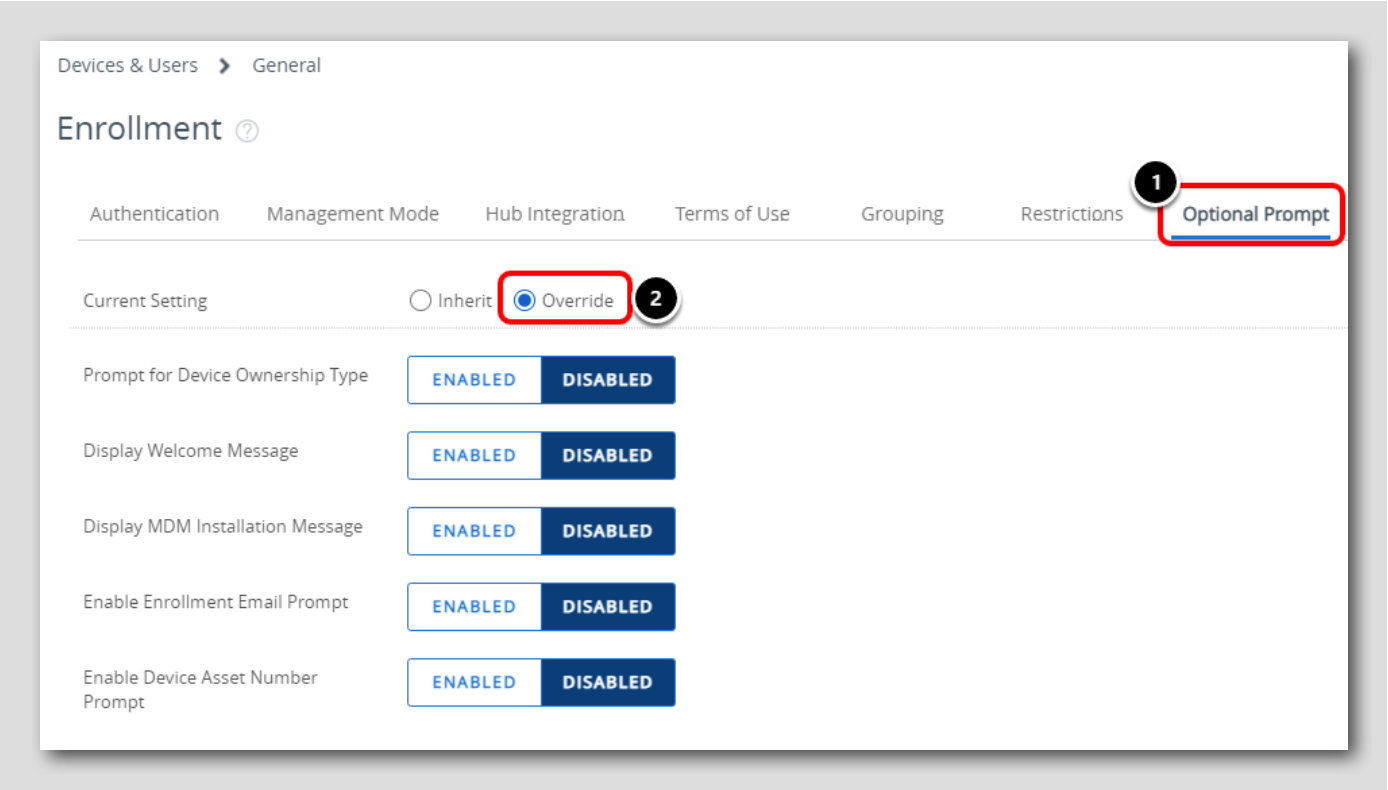
[296]



1. Expand **Devices & Users**
2. Expand **General**
3. Click **Enrollment**

Configure Optional Prompt

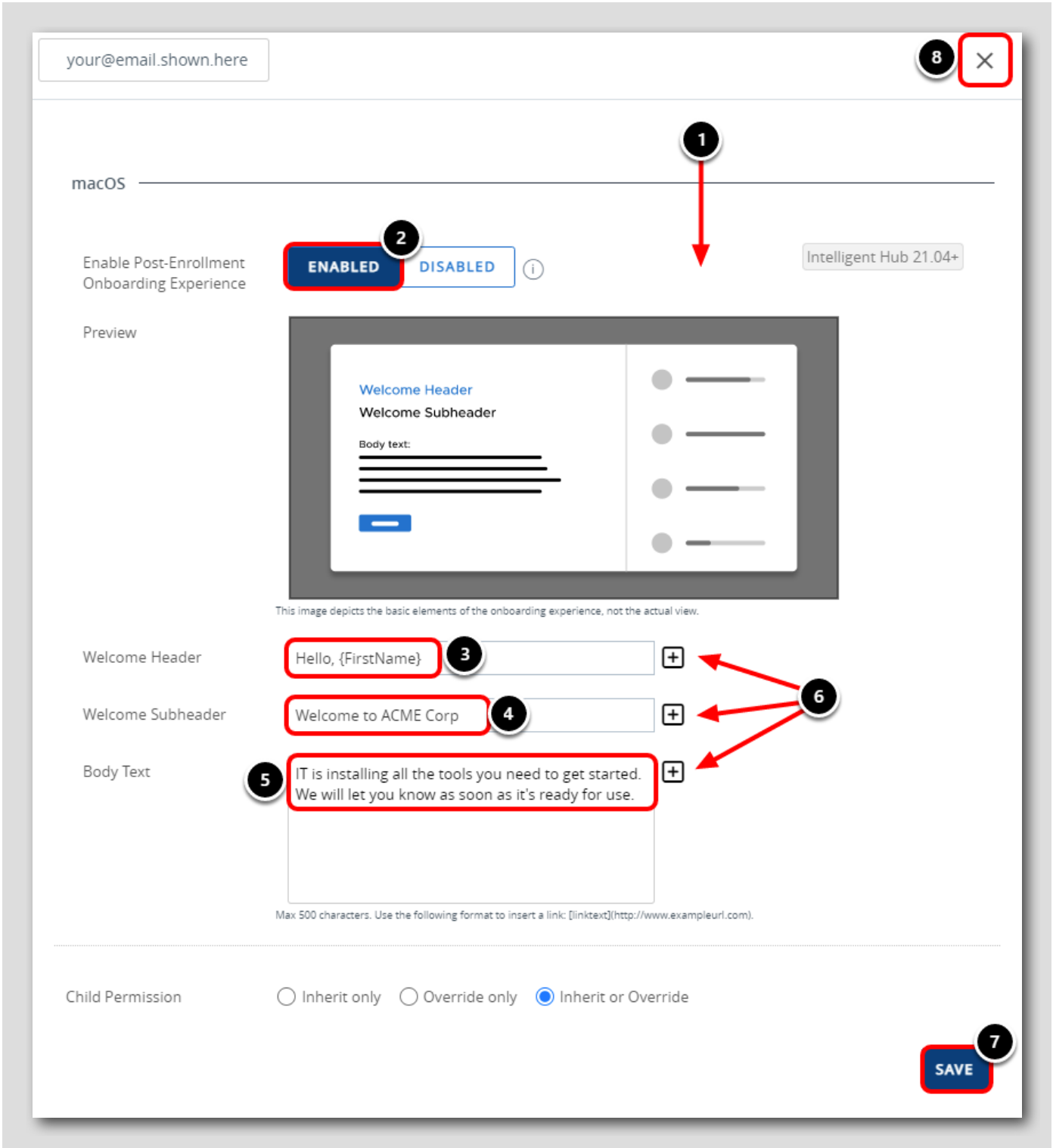
[297]



1. Click the **Optional Prompt** tab
2. Select **Override** for Current Setting to make changes

Configure the Post-Enrollment Onboarding Experience

[298]



1. Scroll down to the bottom to find the macOS Settings
2. Select **Enabled** for the Enable Post-Enrollment Onboarding Experience option, then scroll down.
3. Leave the Welcome Header as the default **`Hello, {FirstName}`**, which will greet the user by their first name
4. Update the Welcome Subheader to **`Welcome to ACME Corp`**
5. Use the default Body Text or supply your own. Note that there is a 500 character count limit
6. When configuring the fields, you can use the **Plus (+)** button to see supported Lookup Values for this field. Lookup values, such as **`{FirstName}`**, will retrieve the value at runtime and replace it with the current value, allowing for easy dynamic variable retrieval.
7. Click **Save**
8. Click **Close**

The post-enrollment onboarding experience is now enabled and configured. This will provide a better user onboarding experience as users can easily track the progress on applications that are downloading and installing.

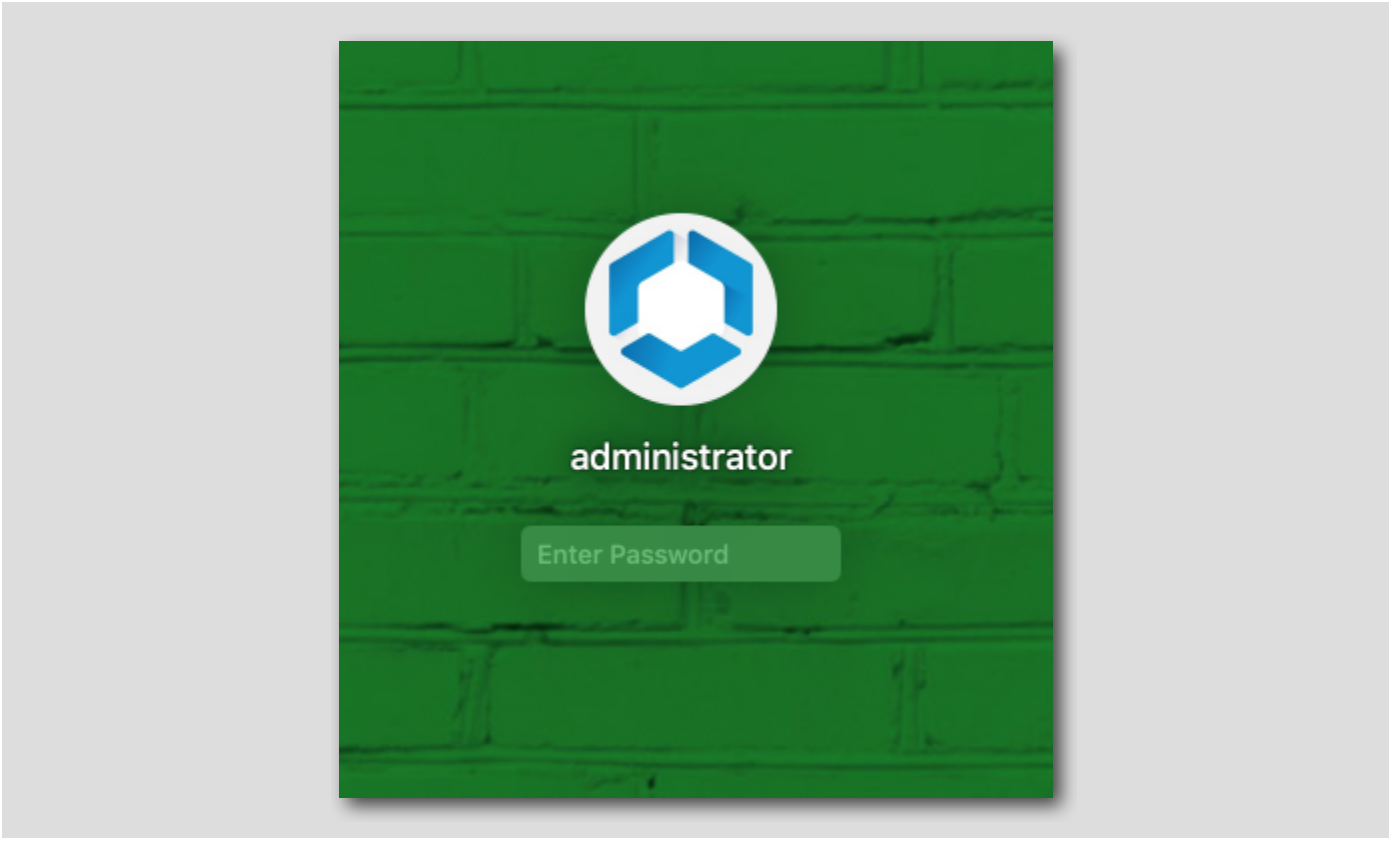
Installing the Workspace ONE Intelligent Hub for macOS [299]

NOTE: These steps require a macOS device. If you do not have a macOS device, you can follow these steps in the manual to see the end result.

In this exercise, you will download and install the Workspace ONE Intelligent Hub on a macOS device.

Login to a macOS Device [300]

NOTE: These steps require a macOS device. If you do not have a macOS device, you can follow these steps in the manual to see the end result.

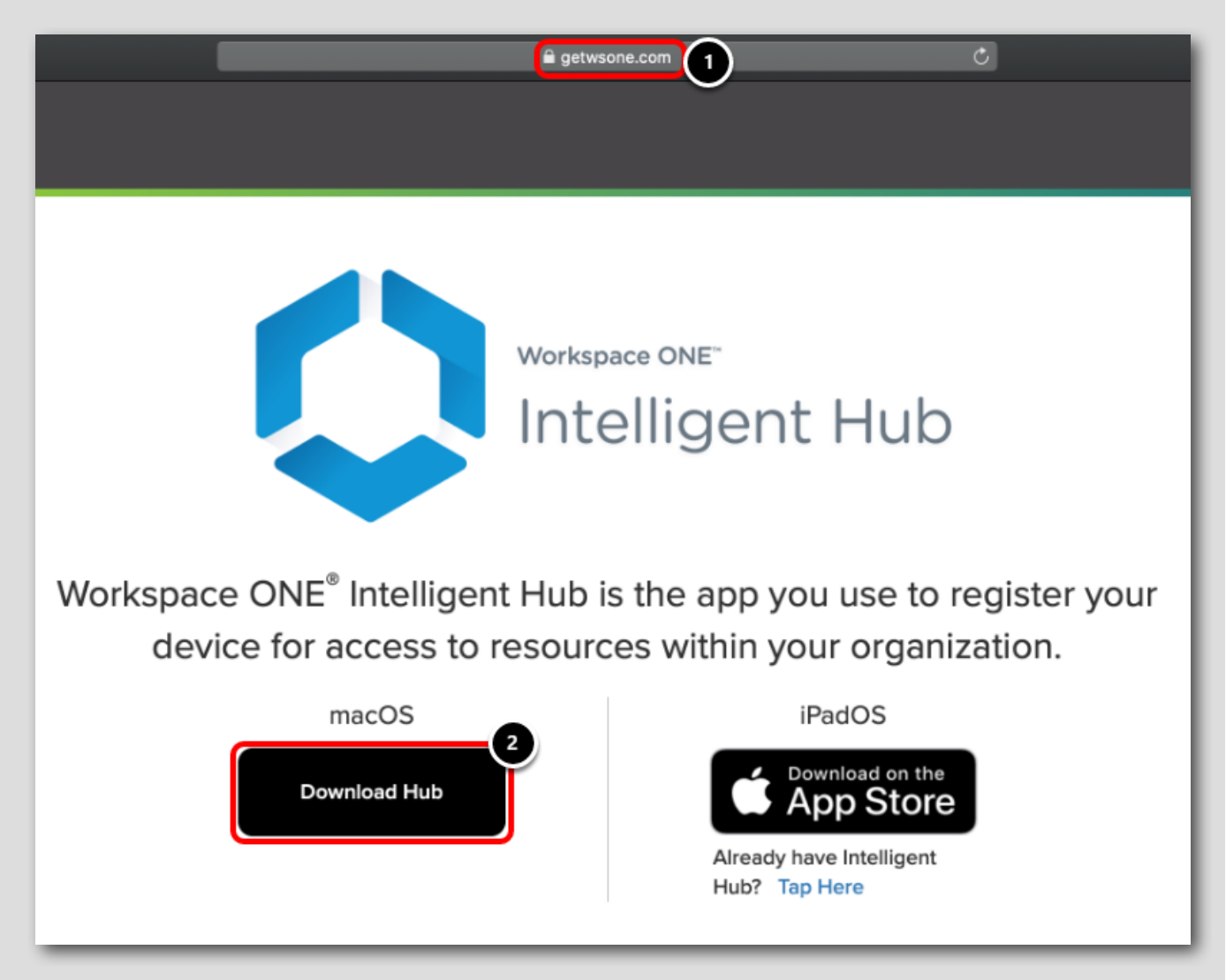


Login to a macOS device as an administrator account.

Download the Workspace ONE Intelligent Hub

[301]

NOTE: These steps require a macOS device. If you do not have a macOS device, you can follow these steps in the manual to see the end result.



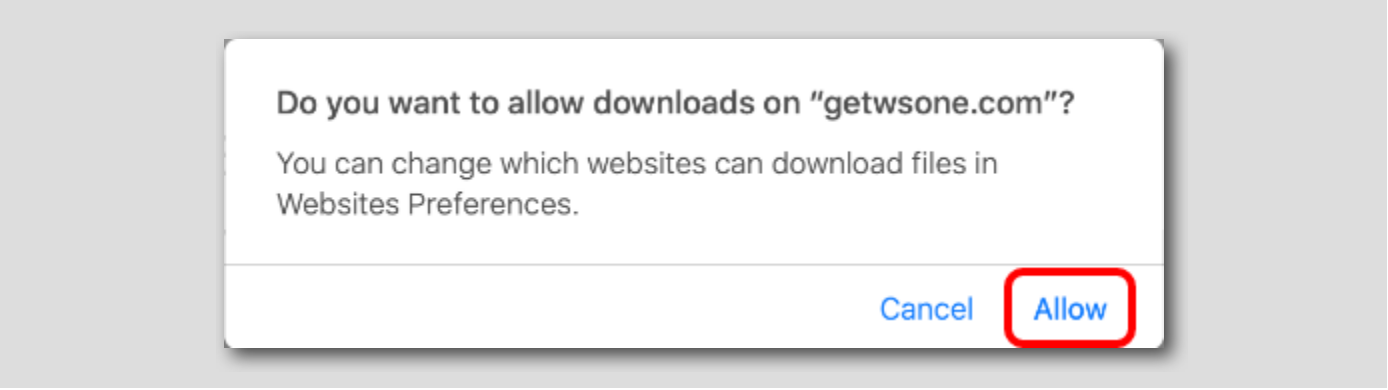
Open Safari or your preferred web browser.

1. Enter **`https://www.getwsone.com`** in the URL field, then press **ENTER**.
2. Click **Download Hub** under the macOS section. The Workspace ONE Intelligent Hub installer begins to download and will save to the downloads folder by default.

Allow Downloads (IF NEEDED)

[302]

NOTE: These steps require a macOS device. If you do not have a macOS device, you can follow these steps in the manual to see the end result.

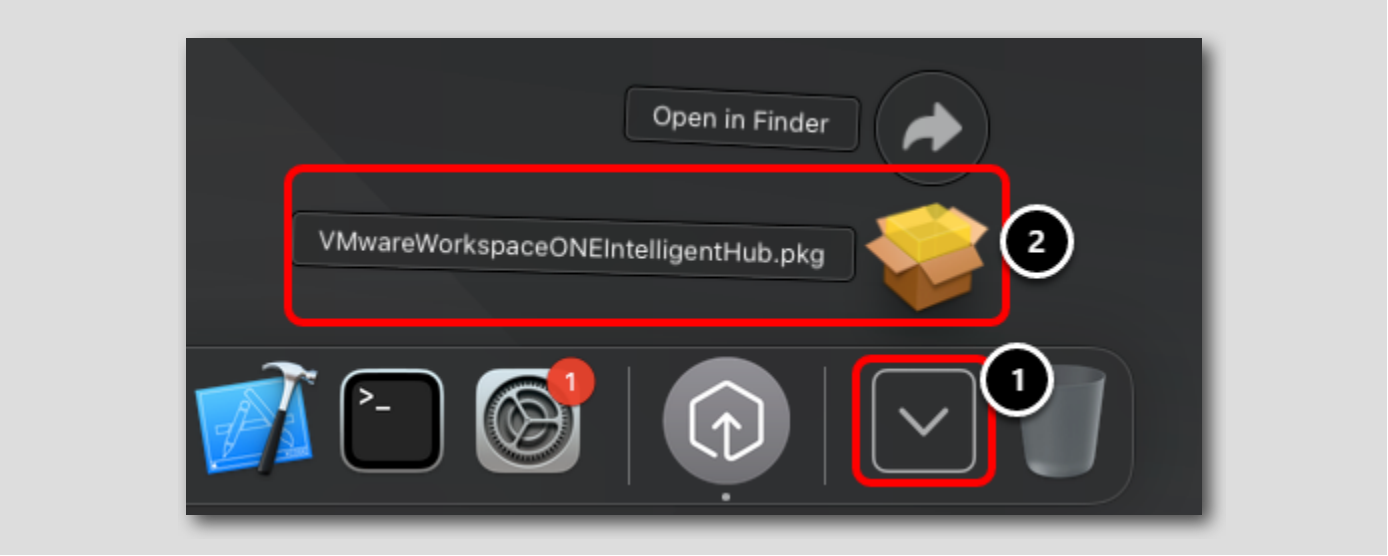


If prompted to allow downloads on "getwsone.com", click **Allow**. Otherwise, continue to the next step.

Install the Workspace ONE Intelligent Hub

[303]

NOTE: These steps require a macOS device. If you do not have a macOS device, you can follow these steps in the manual to see the end result.

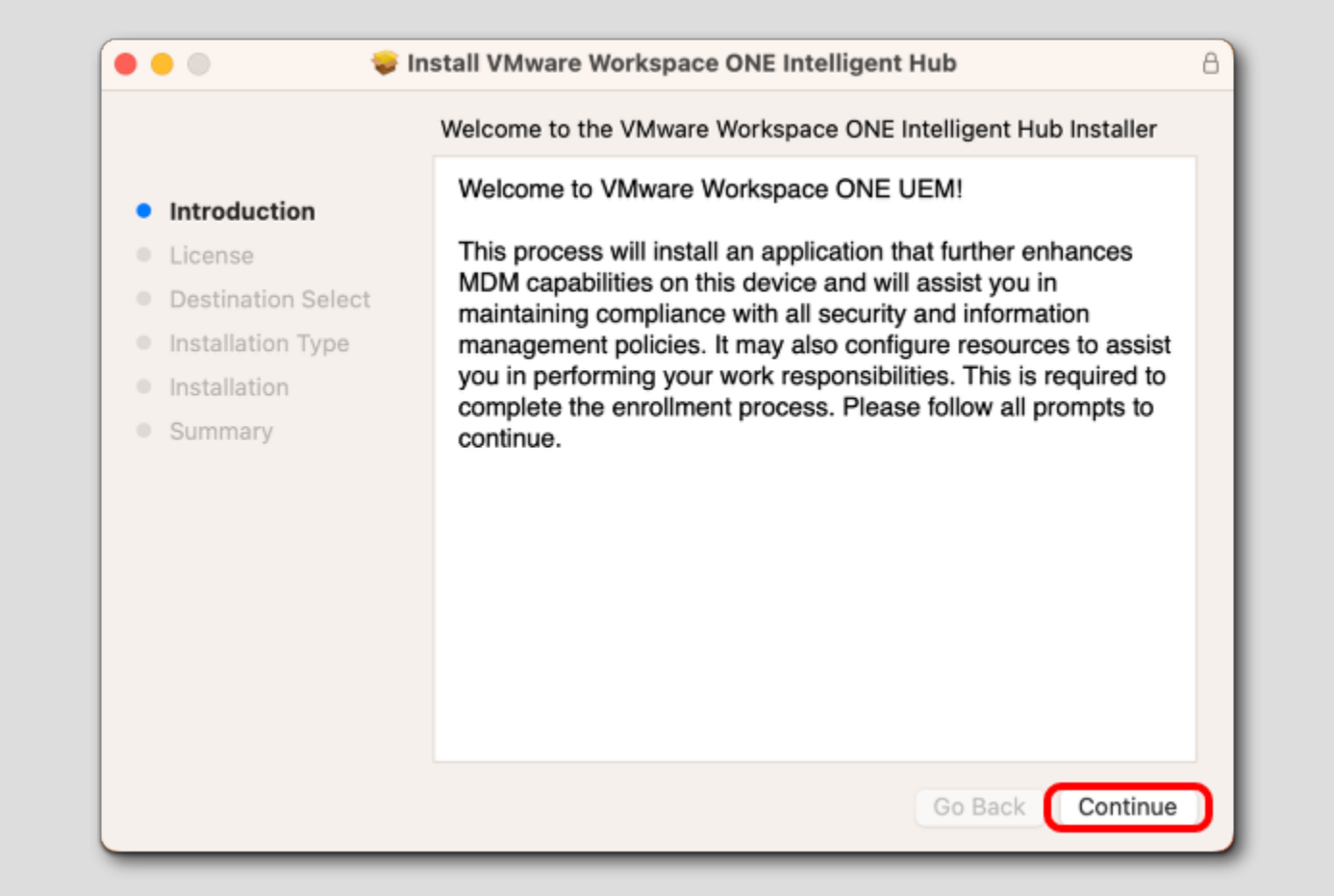


1. Click the **Downloads** folder in the dock (next to the Trash Bin).
2. Click the **VMwareWorkspaceONEIntelligentHub.pkg** file to begin the installer.

Continue at Introduction Screen

[304]

NOTE: These steps require a macOS device. If you do not have a macOS device, you can follow these steps in the manual to see the end result.

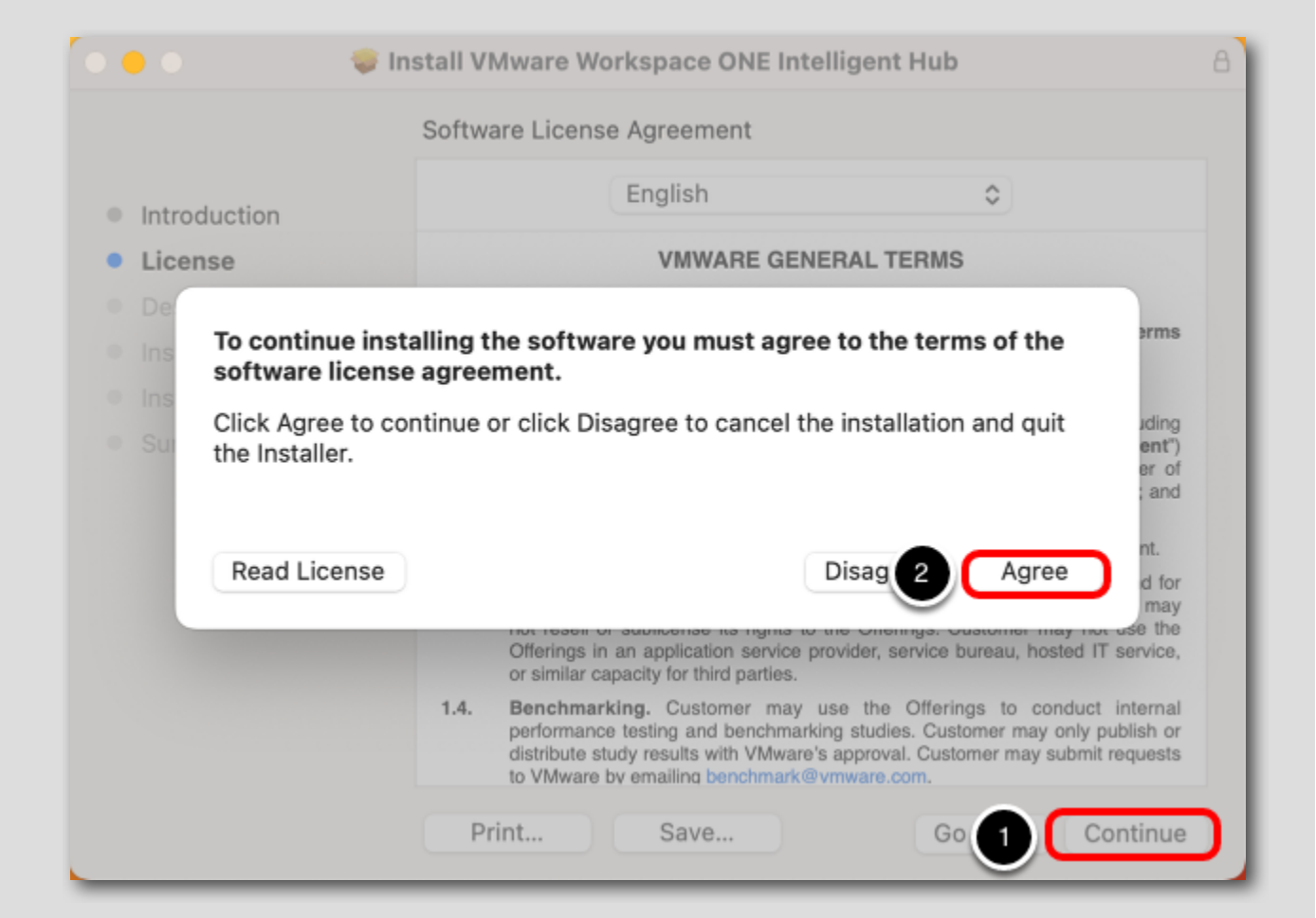


Click **Continue**.

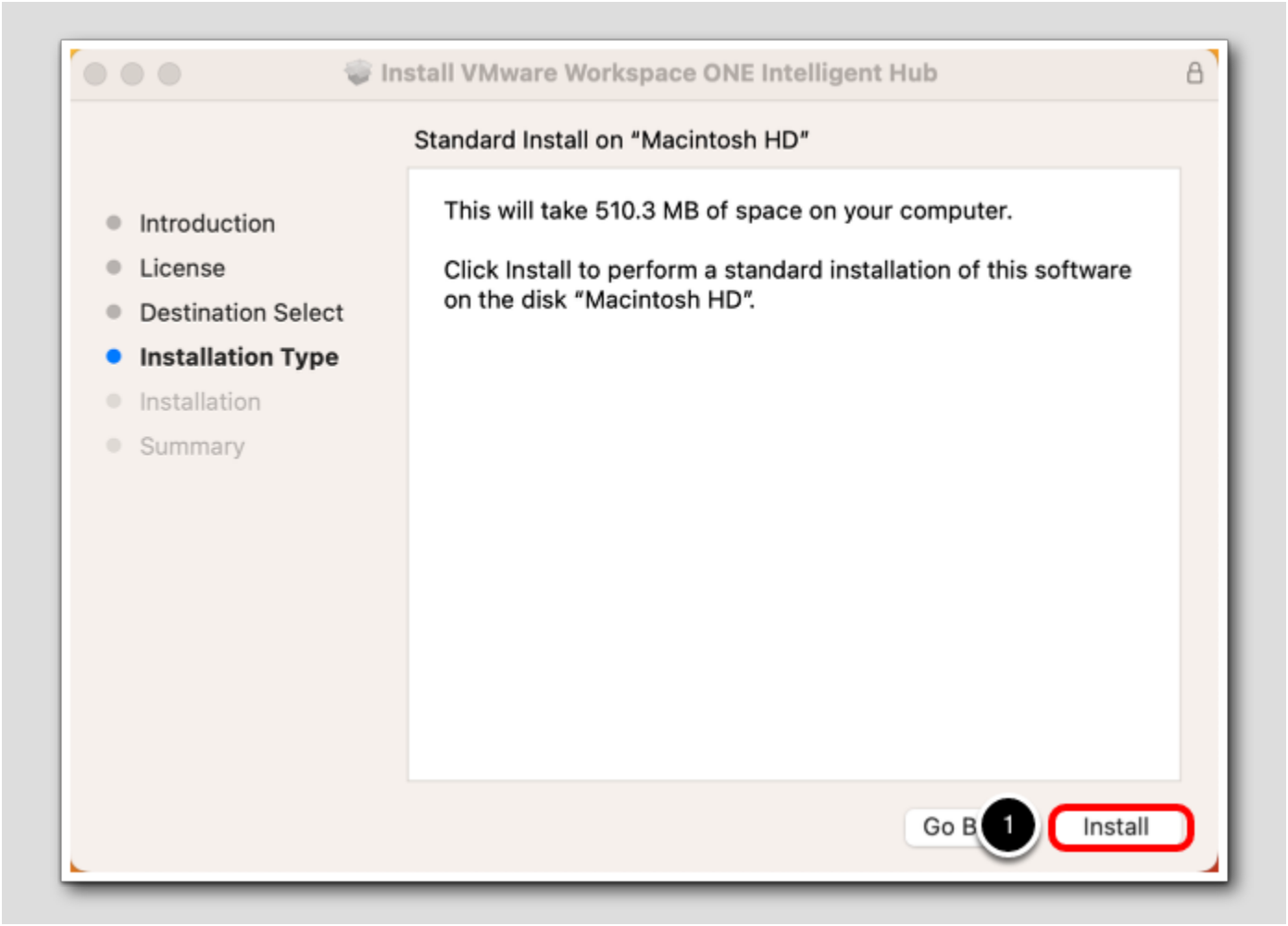
Continue and Agree to Terms

[305]

NOTE: These steps require a macOS device. If you do not have a macOS device, you can follow these steps in the manual to see the end result.



1. On the License page, click **Continue**.
2. Click **Agree** (to the license terms).

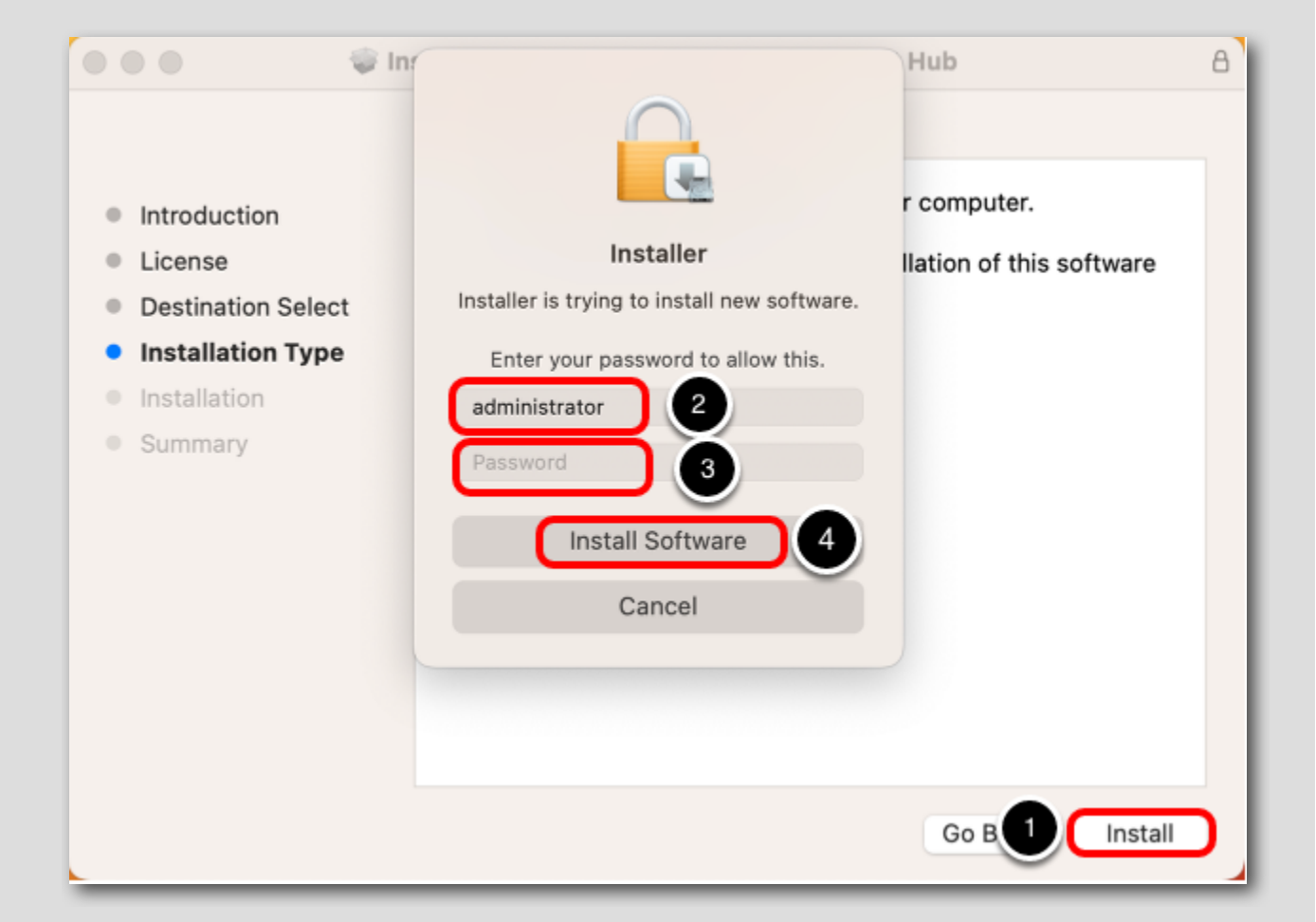


1. On the Standard Install page, click **Install**.

Begin Install

[306]

NOTE: These steps require a macOS device. If you do not have a macOS device, you can follow these steps in the manual to see the end result.



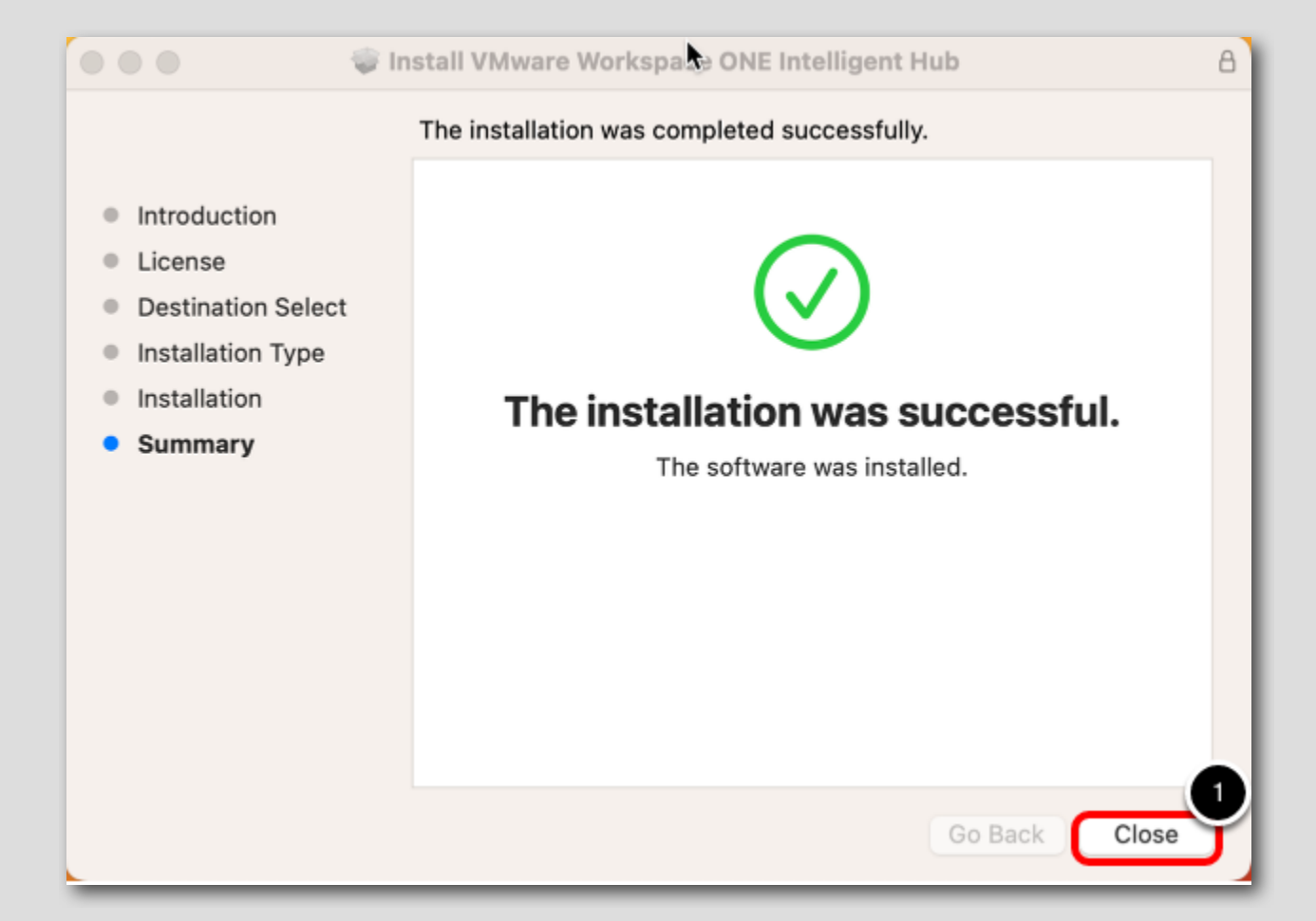
1. Click **Install**. You are now prompted to enter the computers administrator credentials.
2. Enter the username for the device.
3. Enter the password for the device.
4. Click the **Install Software** button.

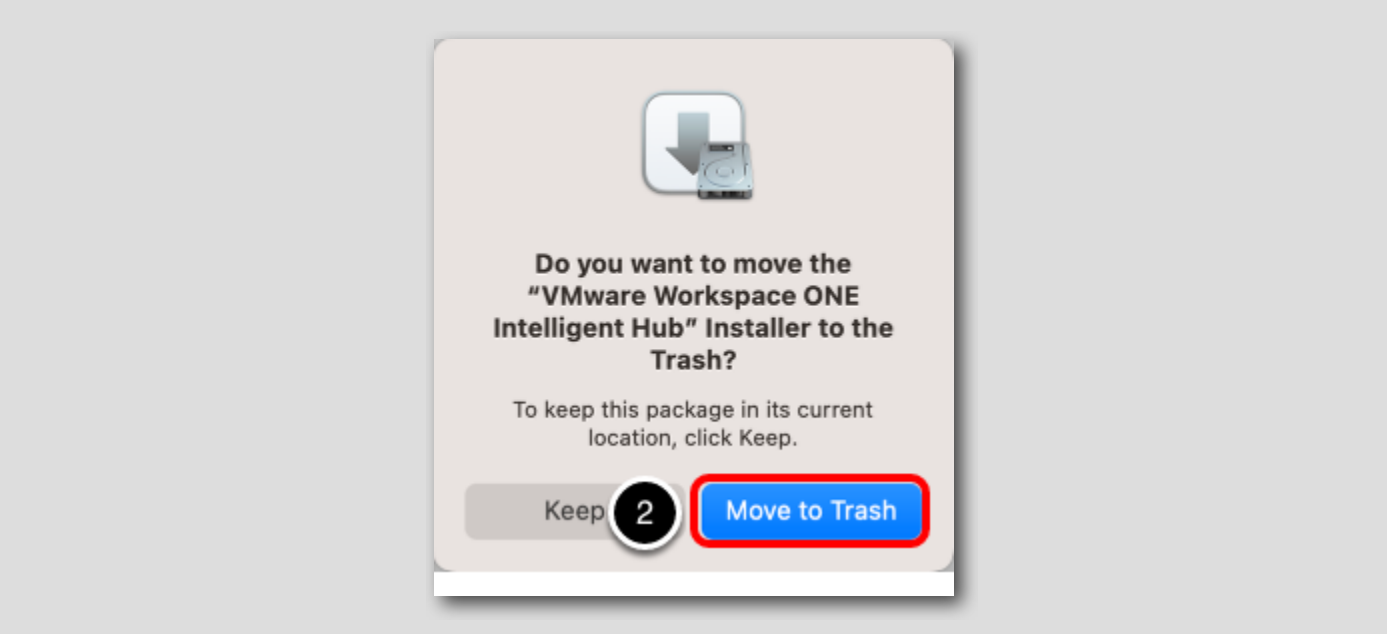
NOTE: The install may take a few minutes, please be patient while the install completes.

Close and Move to Trash

[307]

NOTE: These steps require a macOS device. If you do not have a macOS device, you can follow these steps in the manual to see the end result.





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

Enroll a macOS Device

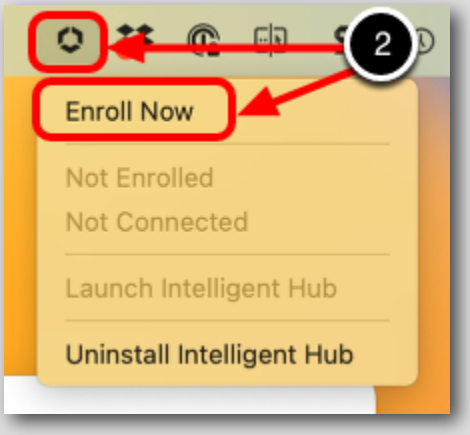
[308]

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

This enrollment flow is considered *User-Approved* per the functionality introduced in macOS High Sierra.

Begin macOS Enrollment Process

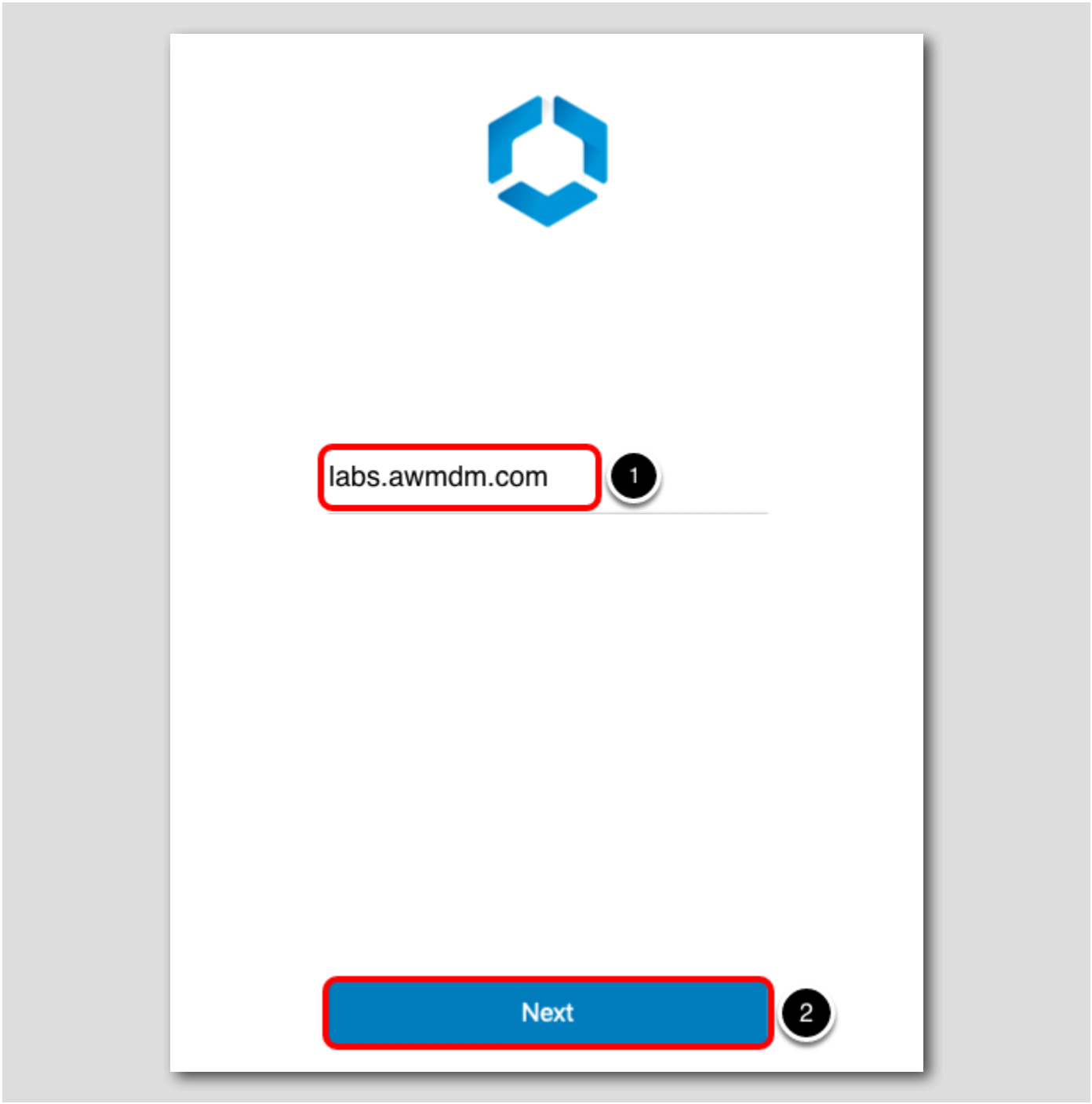
[309]



1. When the Hub Notification displays, click **Enroll Now** to start the enrollment process.
2. Alternatively, you can click the **Hub Icon** from the top bar and click **Enroll Now** to start the enrollment process.

Enter the Enrollment Server URL

[310]

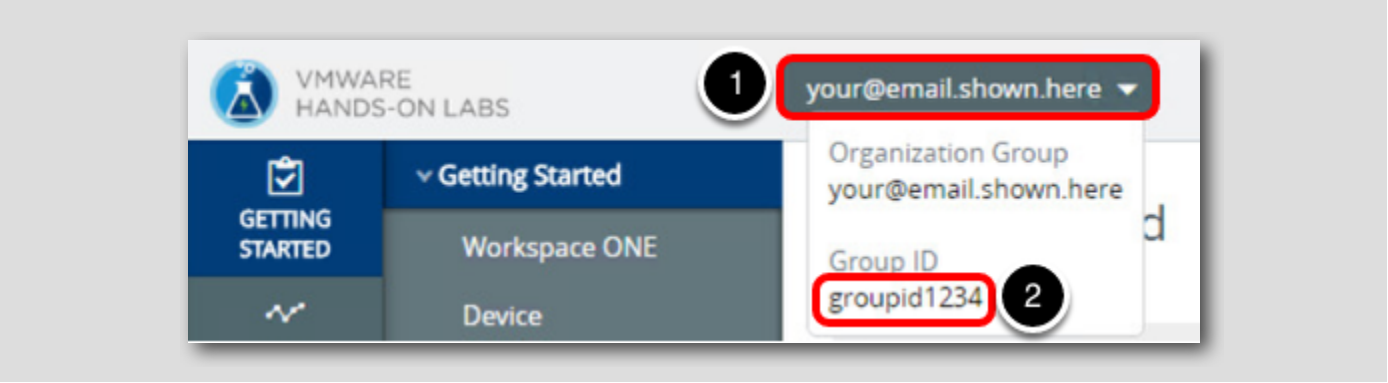


1. Enter **`labs.awmdm.com`** in the Email or Server Address field
2. Click **Next**

Note: The Enrollment Wizard may take a small amount of time to launch based on the capabilities of the hardware. If you do not see the Enrollment Wizard immediately, be patient and wait for it to appear.

Find your Group ID in the Workspace ONE UEM Console

[311]



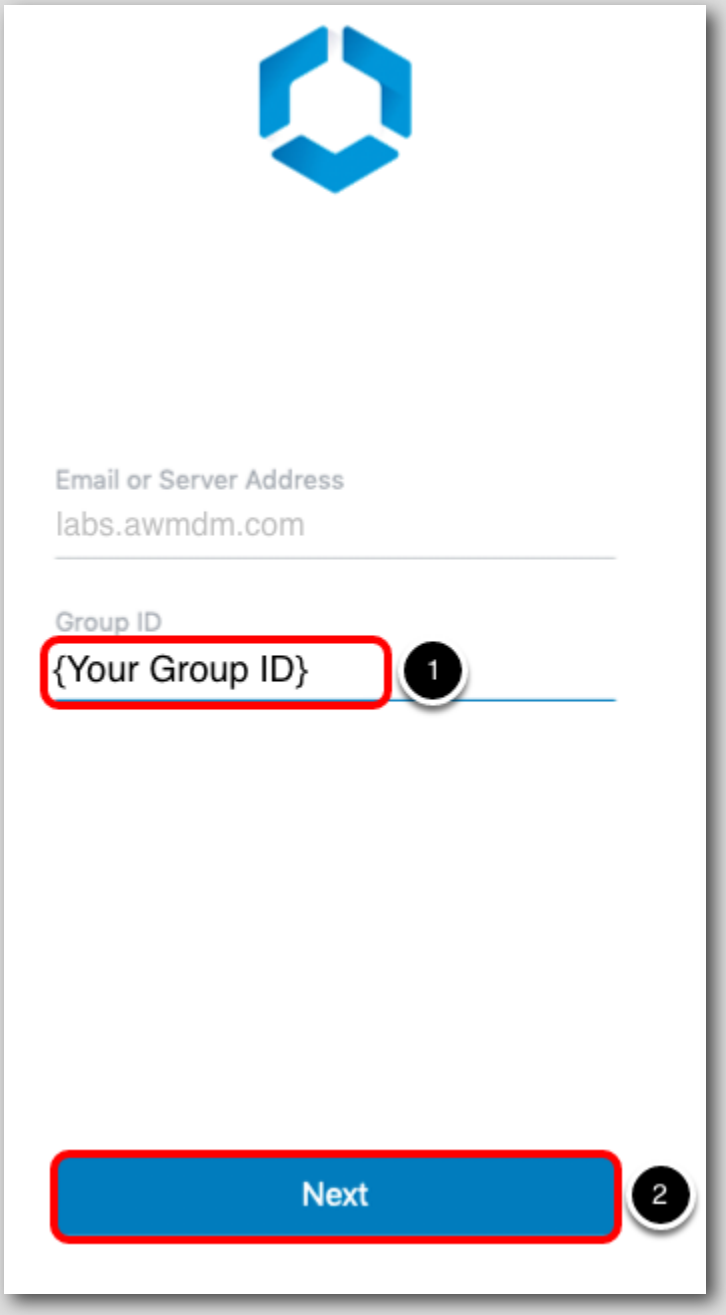
Return to the Workspace ONE UEM Console,

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

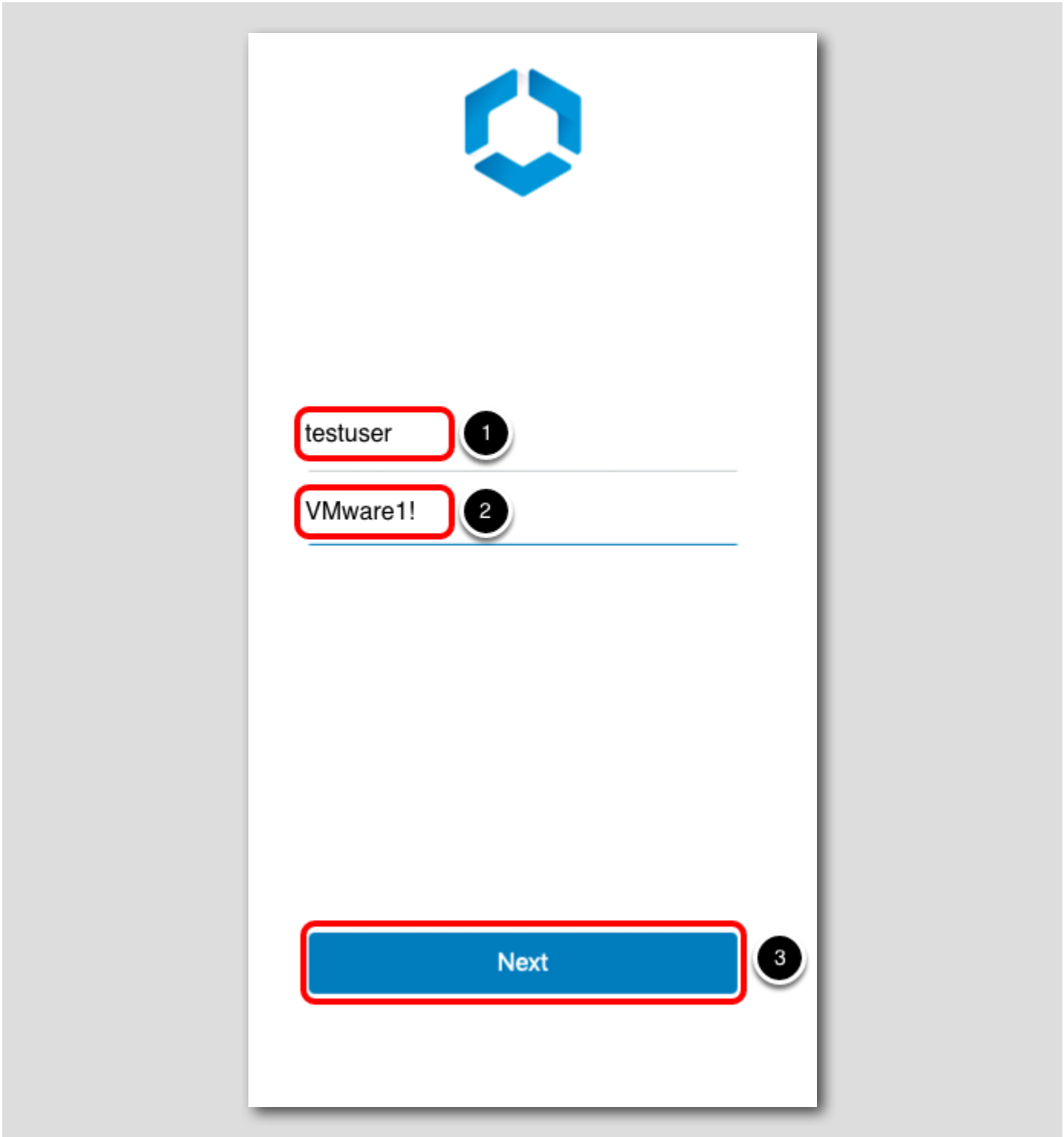
[312]



1. Enter your **Group ID**. This was documented in the previous steps titled Retrieve Your Group ID.
2. Click **Next**.

Enter Enrollment Credentials

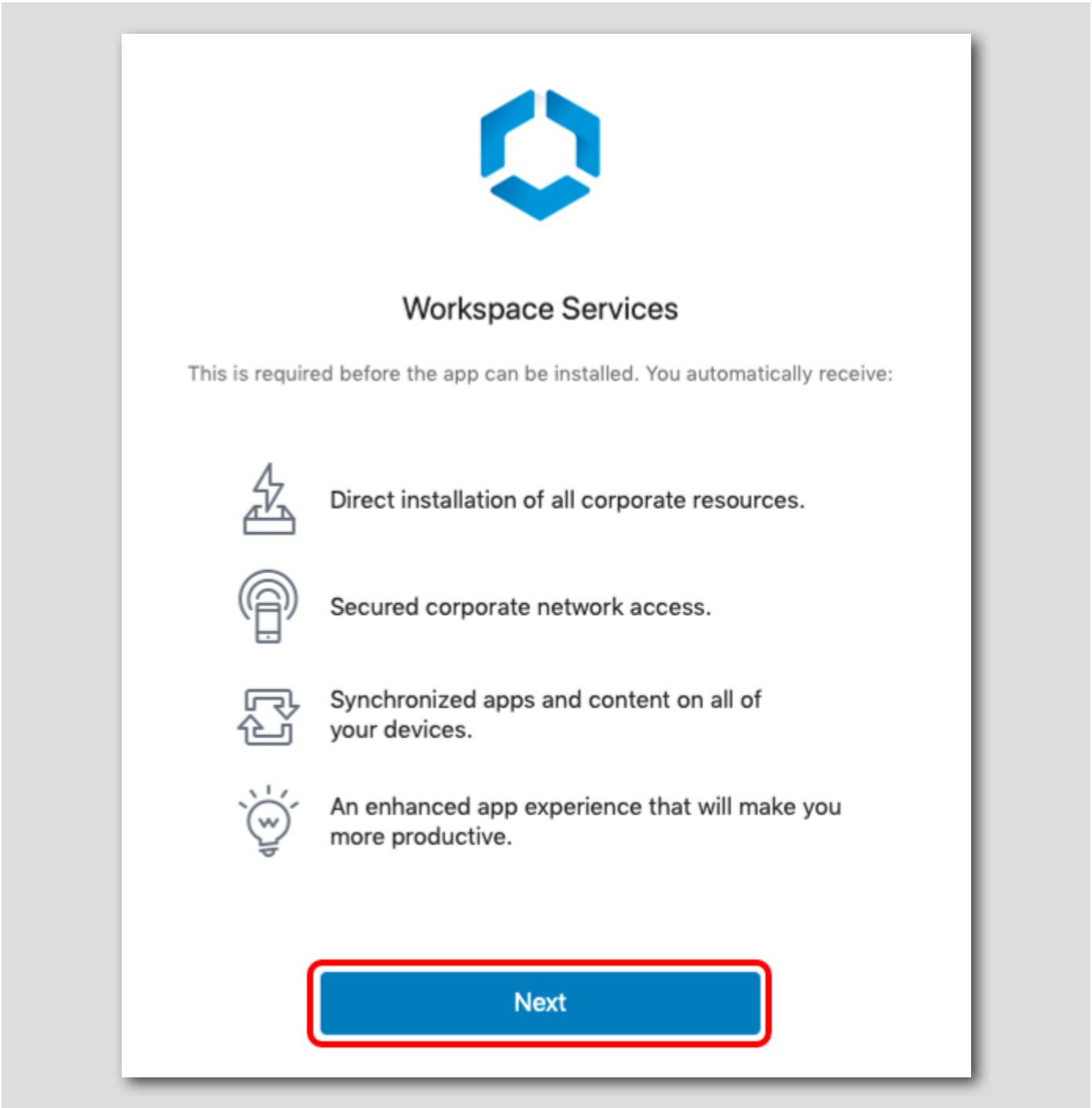
[313]



1. Enter **testuser** for the enrollment username.
2. Enter **VMware1!** for the password.
3. Click **Next**.

Enable Device Management

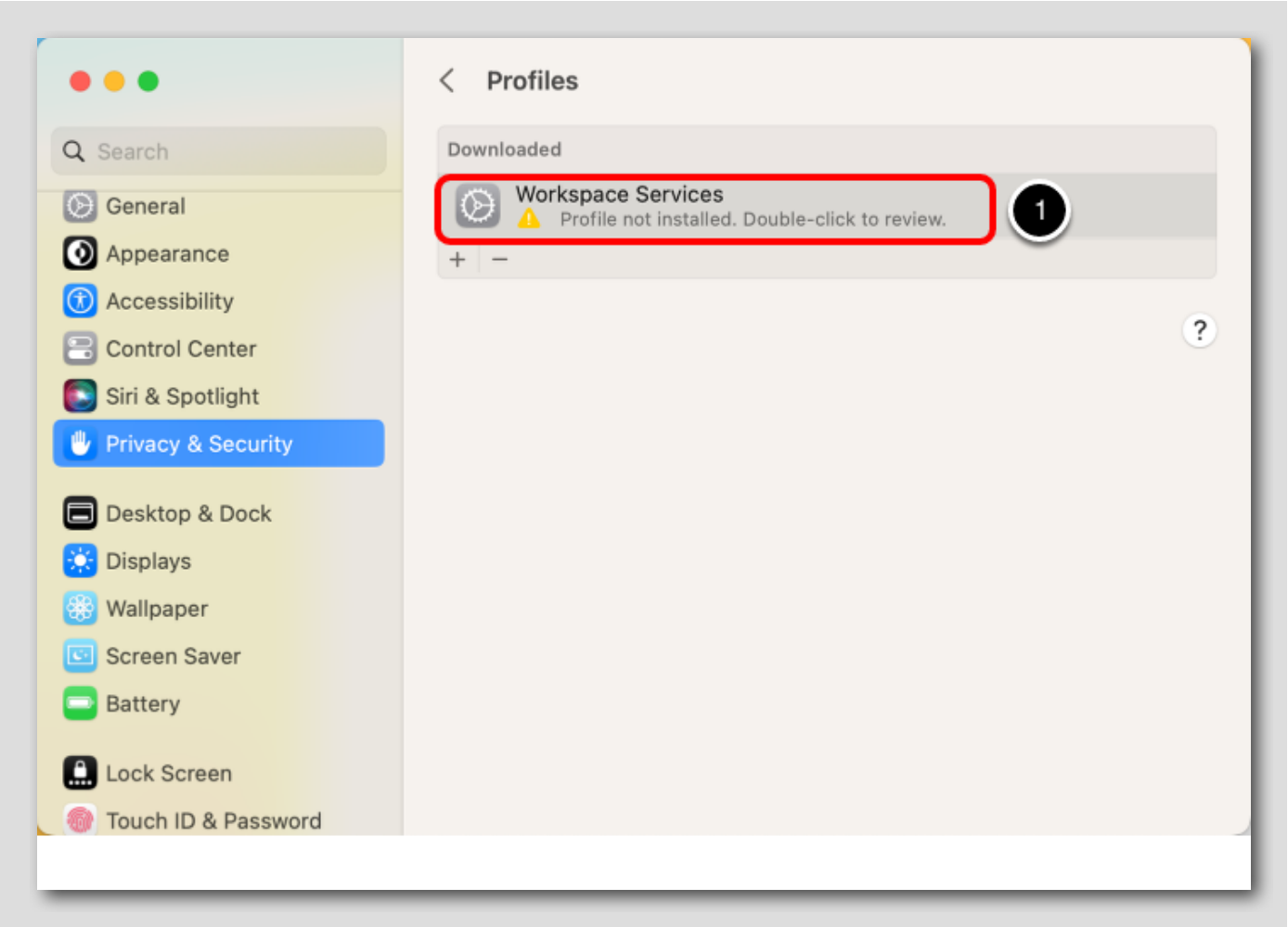
[314]

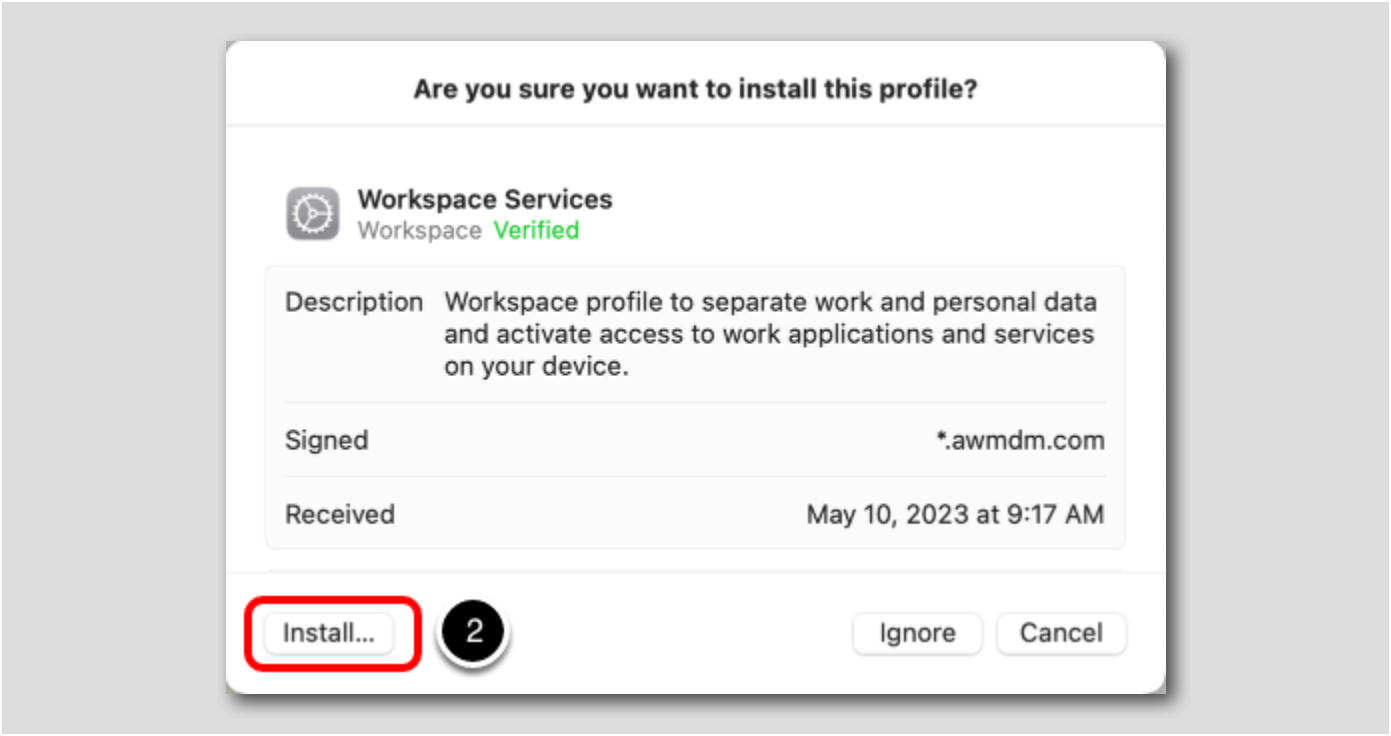


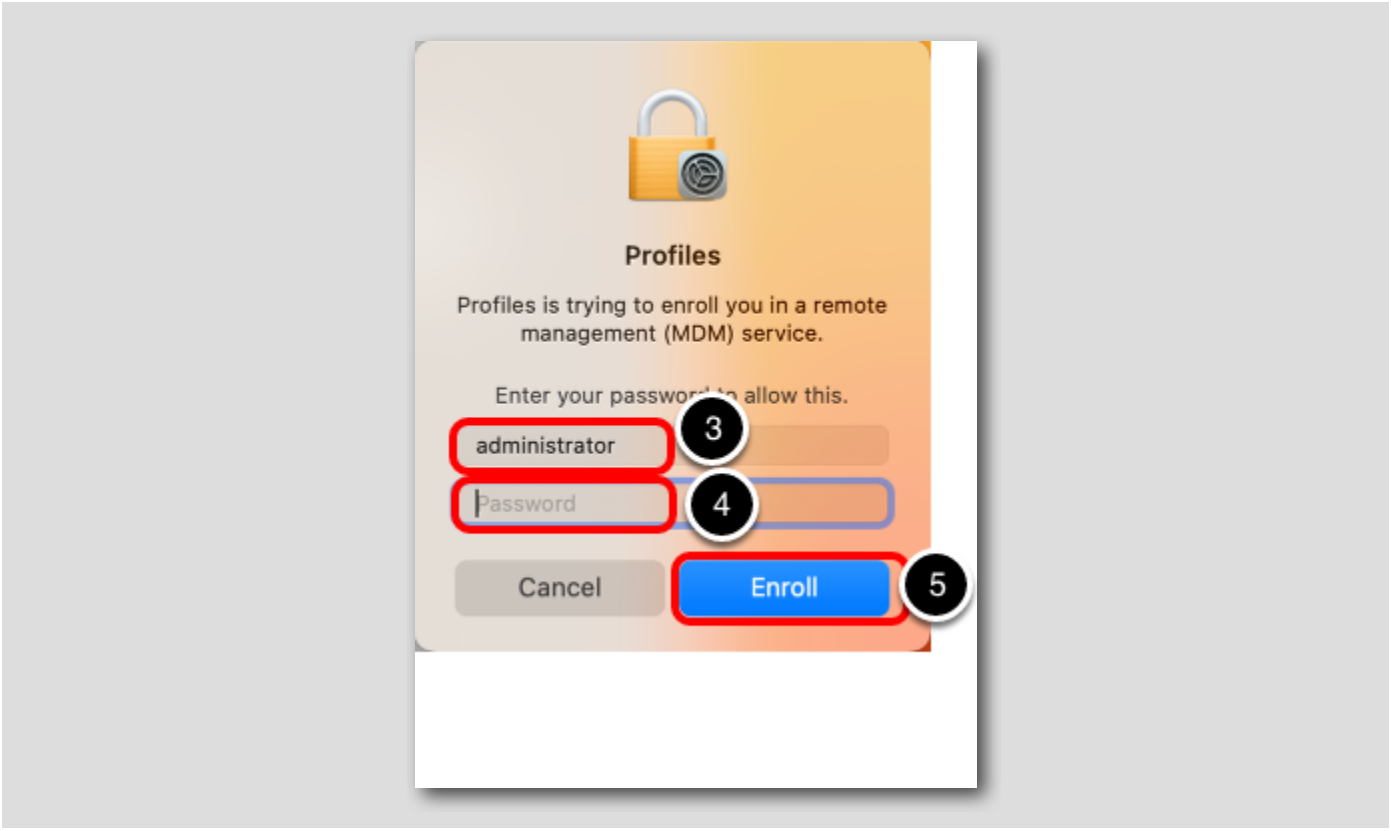
Click **Next** to enable device management.

Install the Workspace Services Profile

[315]




Are you sure you want to install this profile?
Workspace Services
Workspace Verified
Description
Workspace profile to separate work and personal data and activate access to work applications and services on your device.
Signed
*.awmdm.com
Received
May 10, 2023 at 9:17 AM
Install...
2
Ignore
Cancel

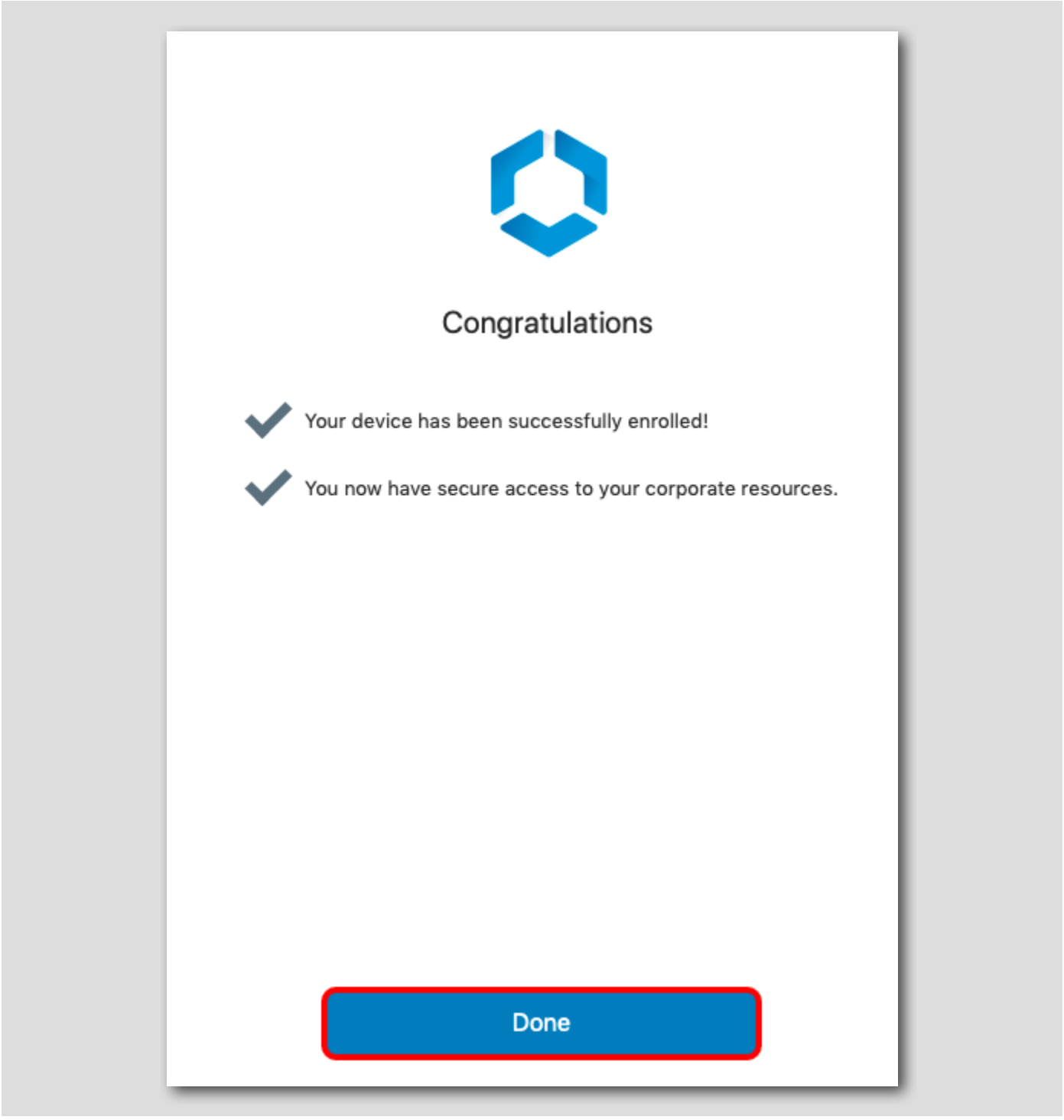


After a few seconds, the Profiles System Preferences page will be displayed and prompt you to install the Workspace Services profile, which enrolls the device into mobile device management (MDM) with Workspace ONE UEM.

1. Click **Install** for the Workspace Services profile.
2. Click **Install** when prompted.
3. Enter the **username** of the device user.
4. Enter the **password** of the device user.
5. Click **Enroll**.
6. Click **Close** on the System Preferences window to close it.

Continue after Device Enrollment

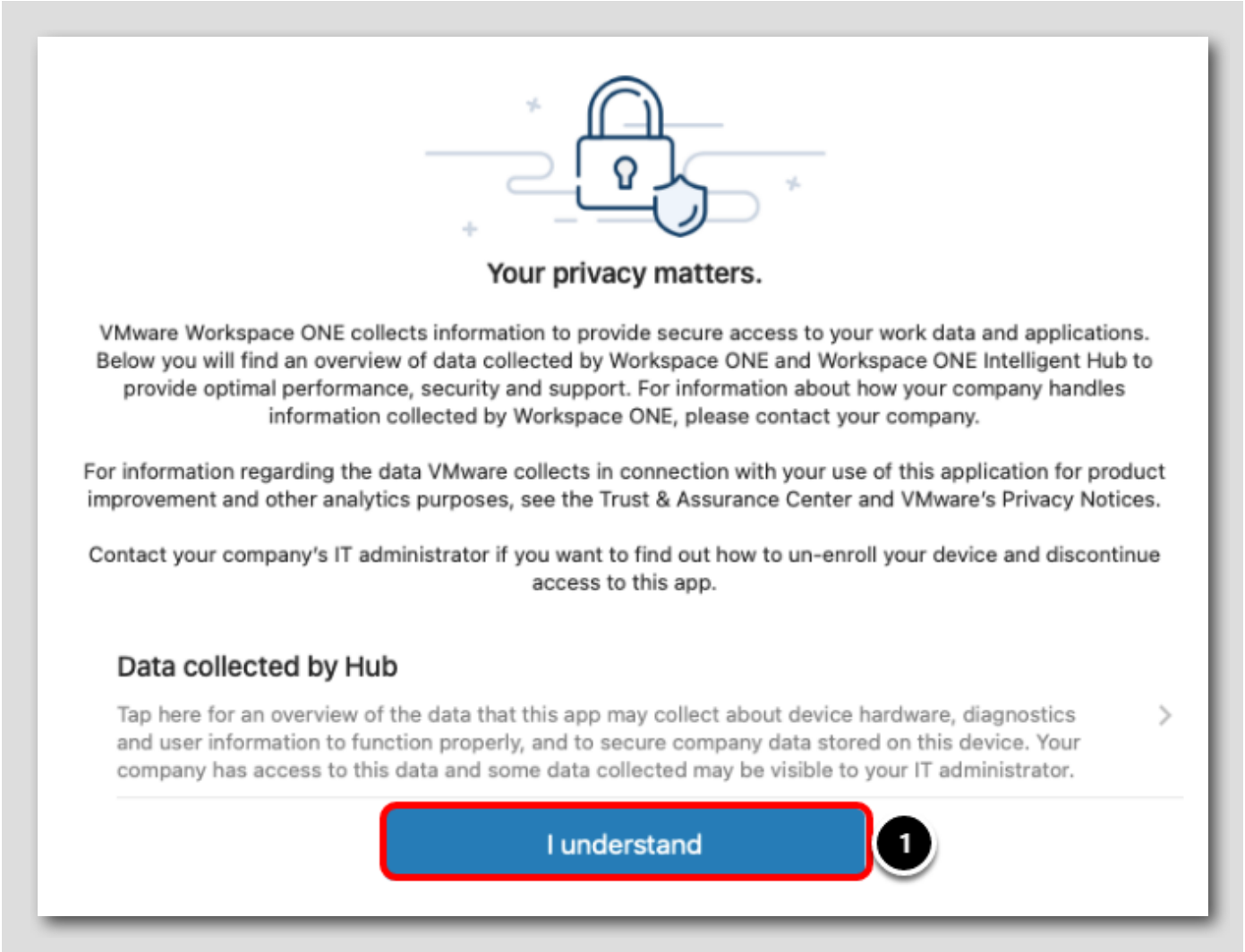
[316]

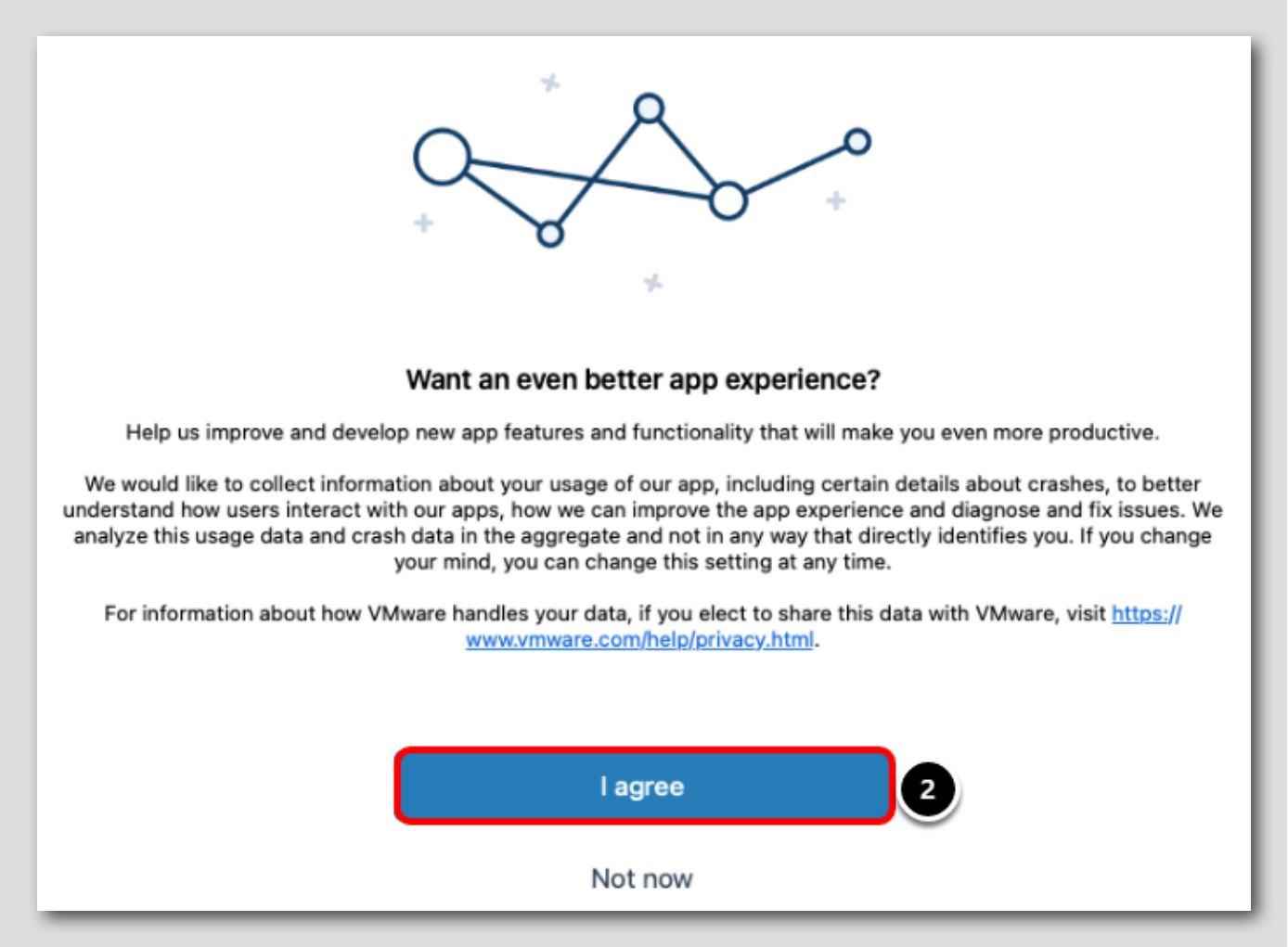


Return to the Workspace ONE Intelligent Hub app and click **Done** when the installation completes.

Accept Privacy and Data Sharing Prompts

[317]





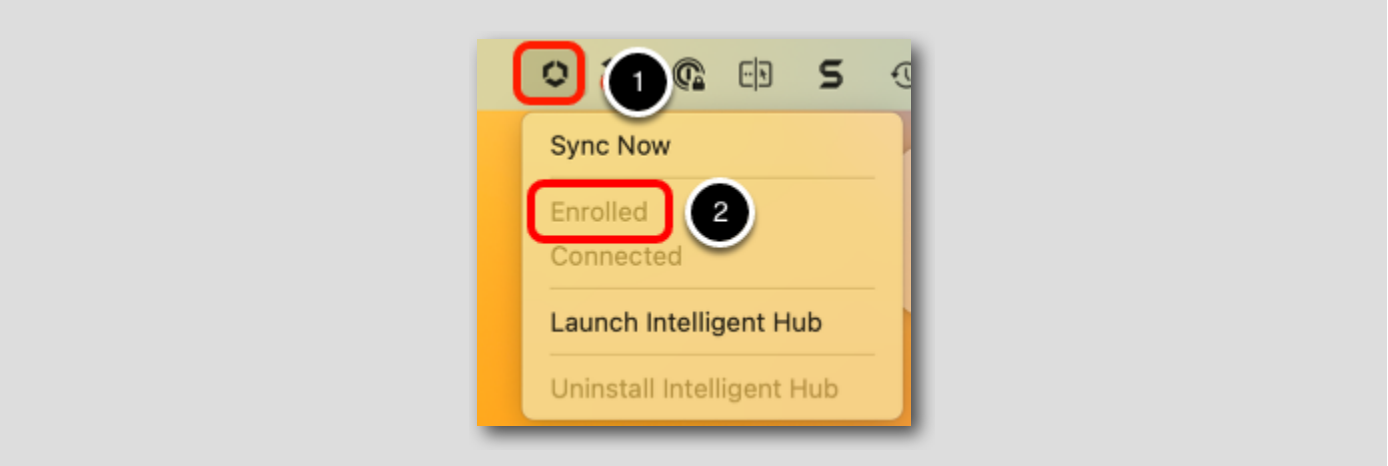
When prompted:

1. Click **I Understand** for the Privacy Policy
2. Click **I agree for** the Data Sharing Policy

Validate Mac Enrollment

[318]

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



In upper-right corner:

1. Note the Workspace ONE icon in the menu bar. Click the icon to view the menu.
2. Note the menu shows your device as **Enrolled**.

Key Takeaways

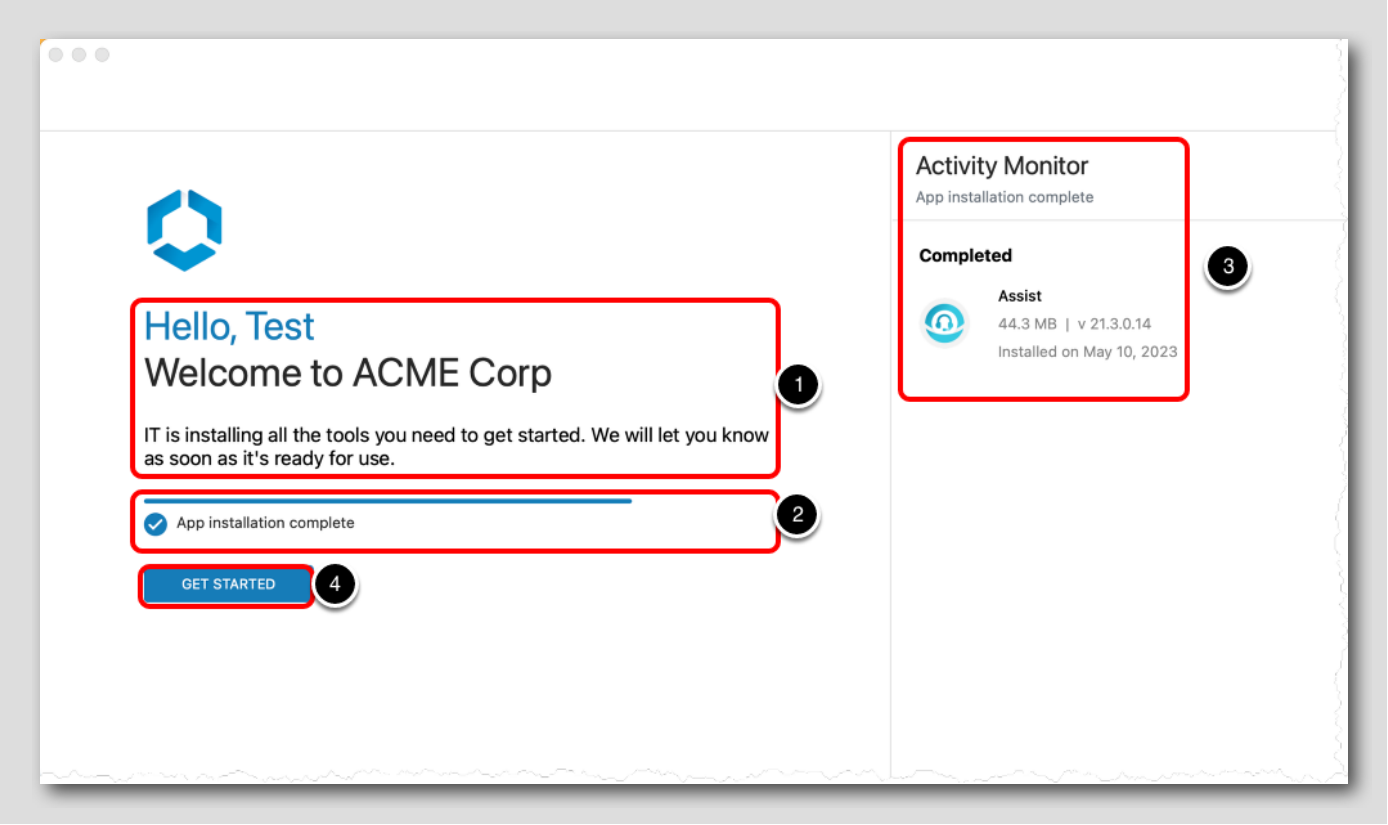
[319]

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

Validate Configurations on an Enrolled macOS Device

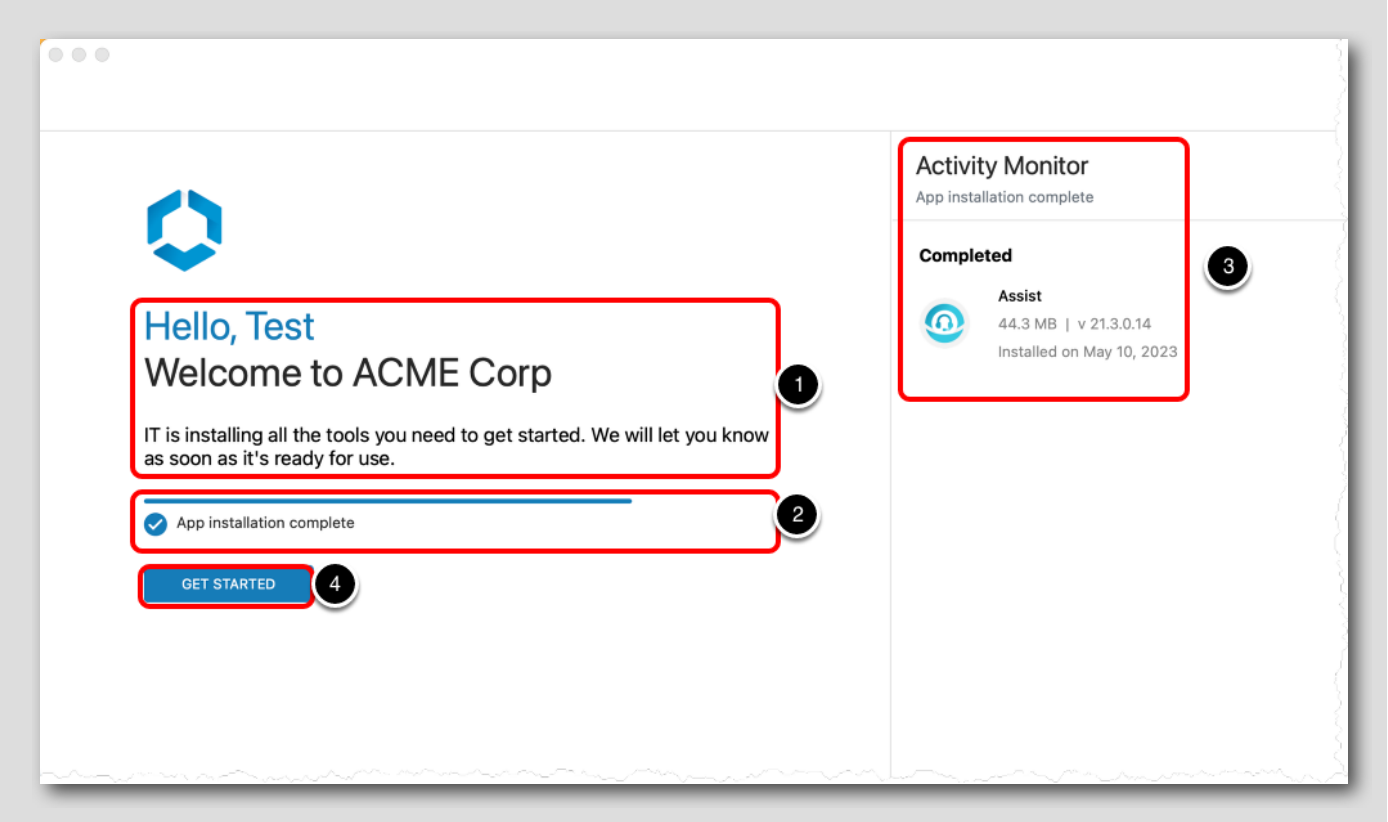
[320]

The Workspace ONE Intelligent Hub will now display the onboarding settings that were configured previously in the Workspace ONE UEM administrator console.



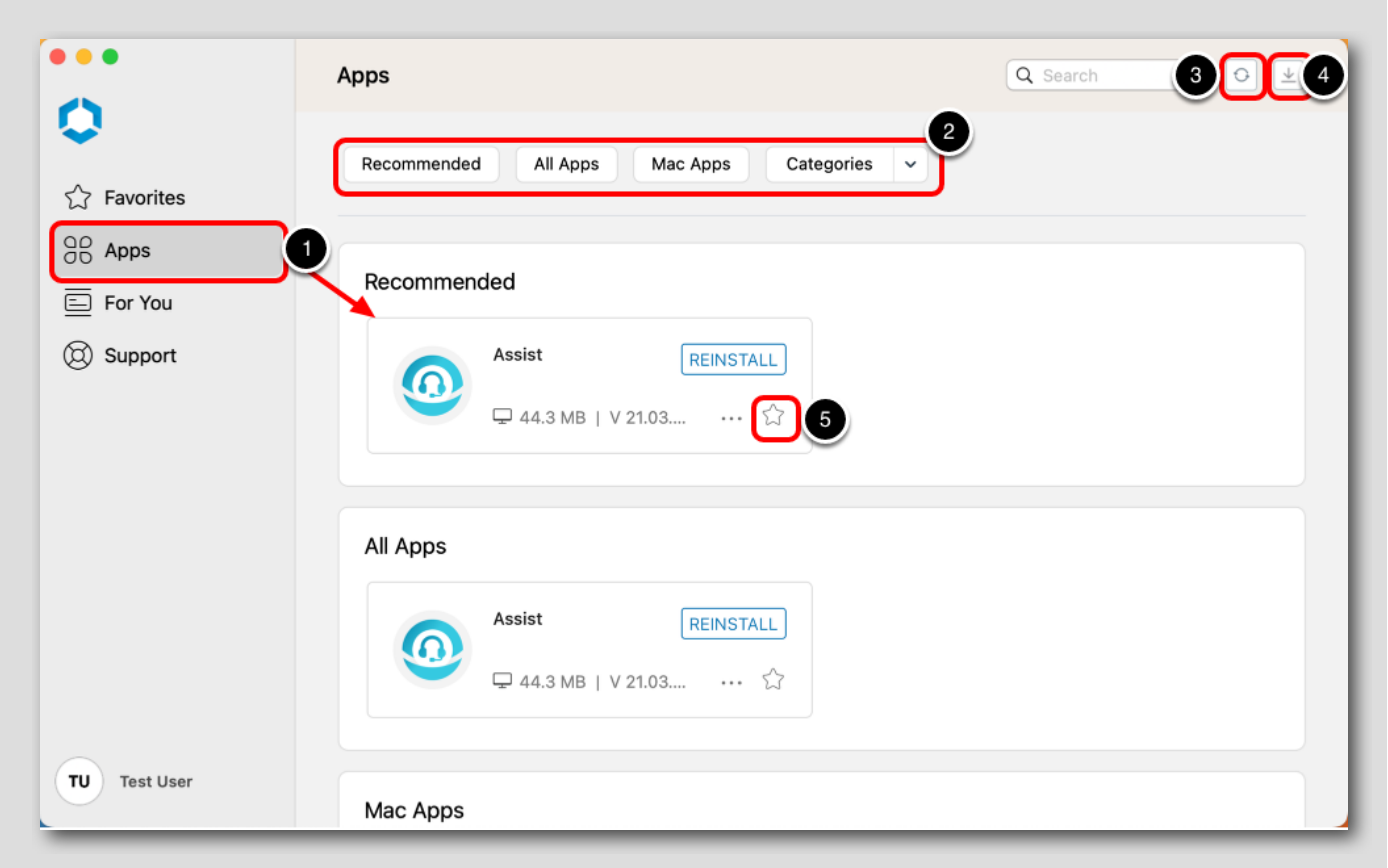
1. Confirm that the Header (**`Hello, {FirstName}`**), Subheader (**`Welcome to ACME Corp`**), and Body Text display your configured message for a personalized onboarding experience.
2. The app installation progress is shown here.
3. All apps that were configured to install on enrollment are shown in the Activity Monitor for easy and clear monitoring.
4. Once the Workspace ONE Assist app finishes installing, click Get Started.

*Note: Users can click **Get Started** at any point to continue to the Hub app catalog before everything is completed, but this provides a clear method for monitoring if their device is fully configured or not before they begin using it.*


Activity Monitor
App installation complete
Completed
Assist
44.3 MB | v 21.3.0.14
Installed on May 10, 2023
3
Hello, Test
Welcome to ACME Corp
IT is installing all the tools you need to get started. We will let you know as soon as it's ready for use.
1
App installation complete
2
GET STARTED
4

View Intelligent Hub App

[321]



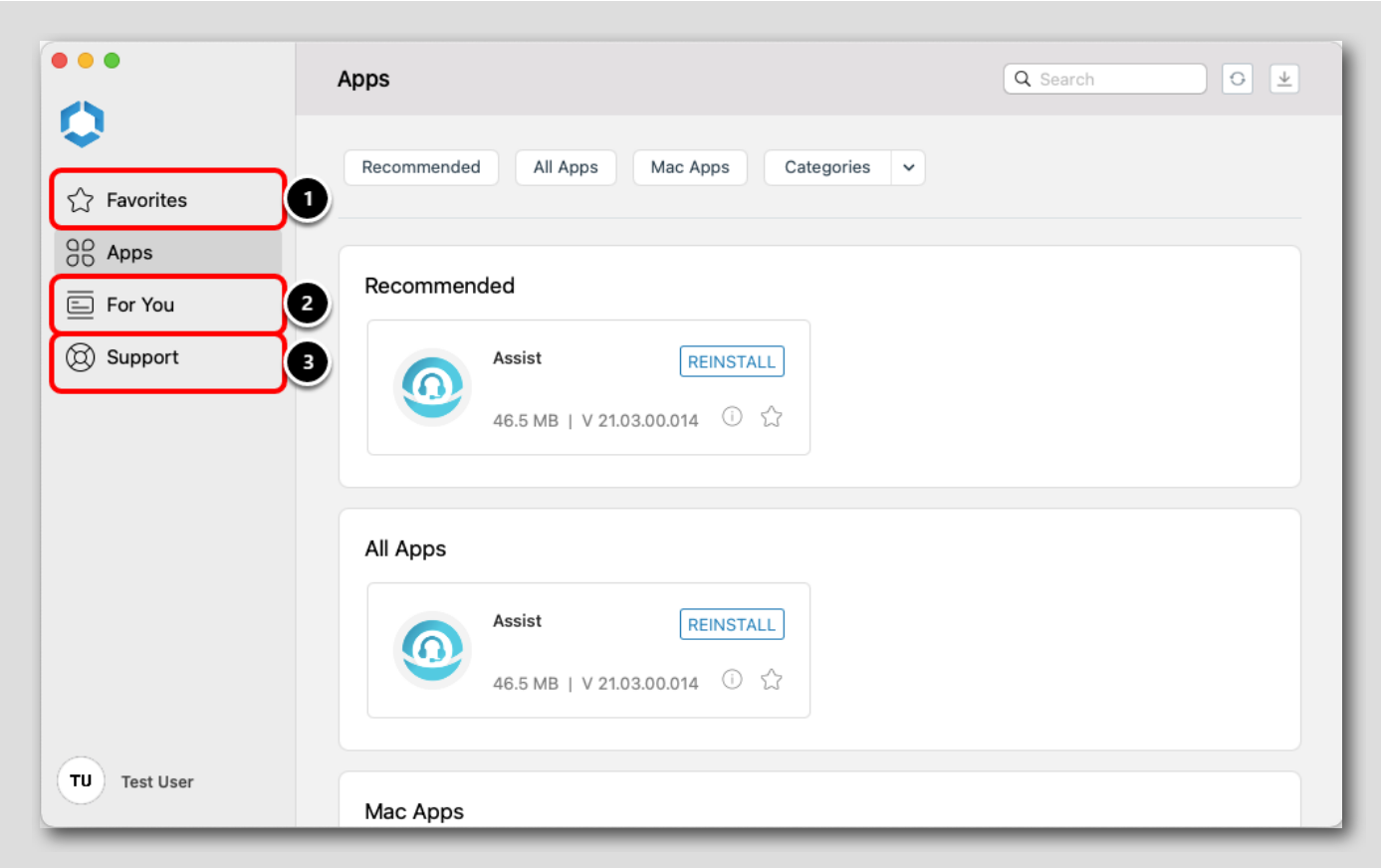
The modern unified app catalog provided by Hub Services is displayed due to the configurations that you made. This enables the following features:

- Favorites
- Apps
- For You (Notifications)
- Support

1. Click the **Apps** tab. A list of available apps are shown on this page for the user to interact with. This could include virtual apps made available through Horizon in addition to native apps!
2. A list of **filters** are available based on the apps you have published to help the user find what they need.
3. The **Refresh** button will reload the app catalog.
4. The **Activity Monitor** can be viewed to track progress on new app installs that the user or administrator triggers on the device.
5. Apps can be added to your Favorites for easy access. Click the **star icon** to add Assist as a Favorite App.

Other Intelligent Hub Features (Optional)

[322]



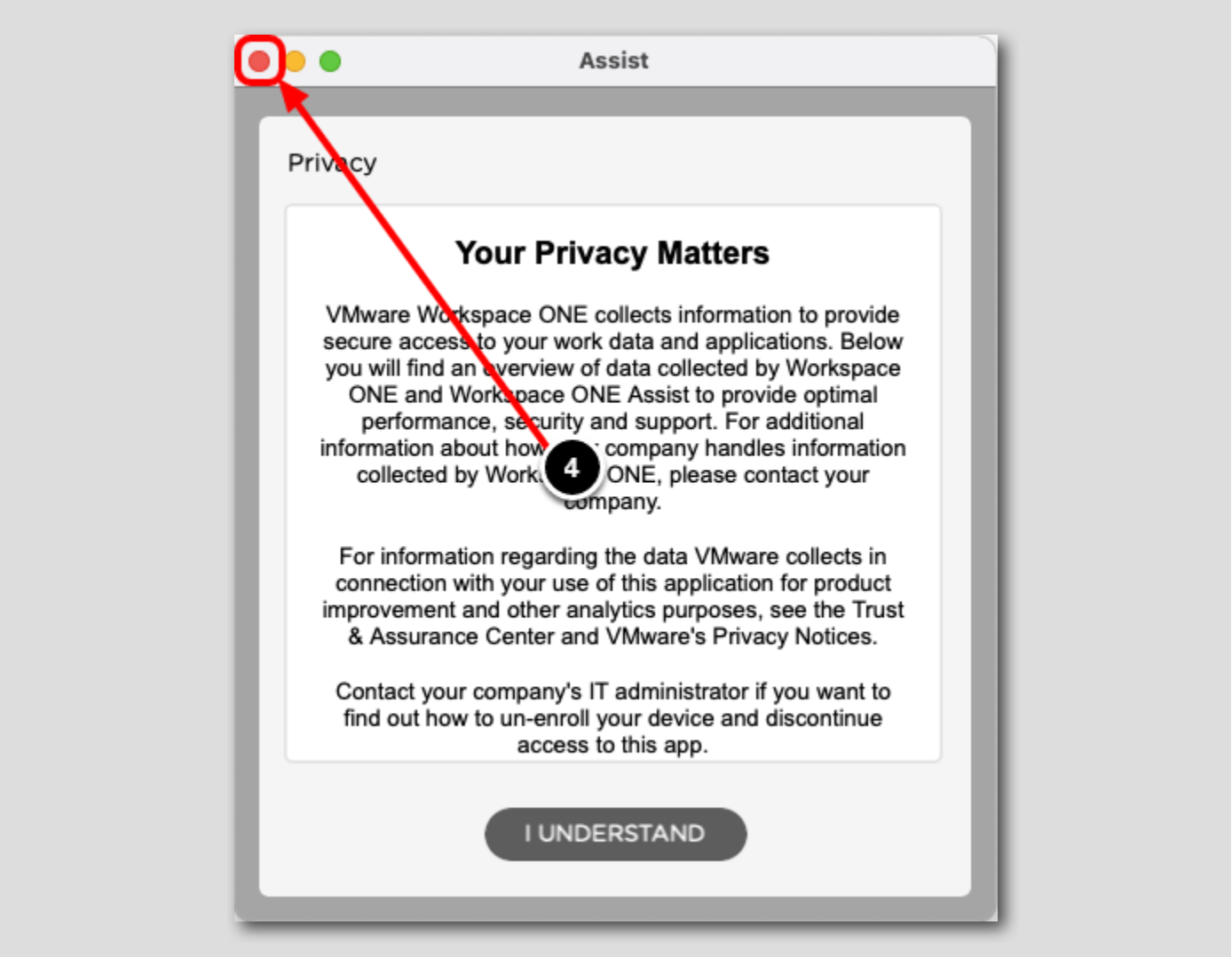
If desired, explore the other features in Intelligent Hub before continuing to the next step to verify the other configurations you published to the device.

1. The **Favorites** tab shows a list of apps that you have marked as a favorite for quick access.
2. The **For You** tab is a list of notifications sent by your administrators. This rich notifications can be configured in Hub Services. You can learn more about these notifications in the Introduction to Workspace ONE Intelligent Hub and Hub Services module.
3. The **Support** tab provides a list of devices that are enrolled to your user account, a method for collecting logs, and configurable contact details to reach your administrators.

Continue to the next step when ready.

Validate the Workspace ONE Assist Install

[323]

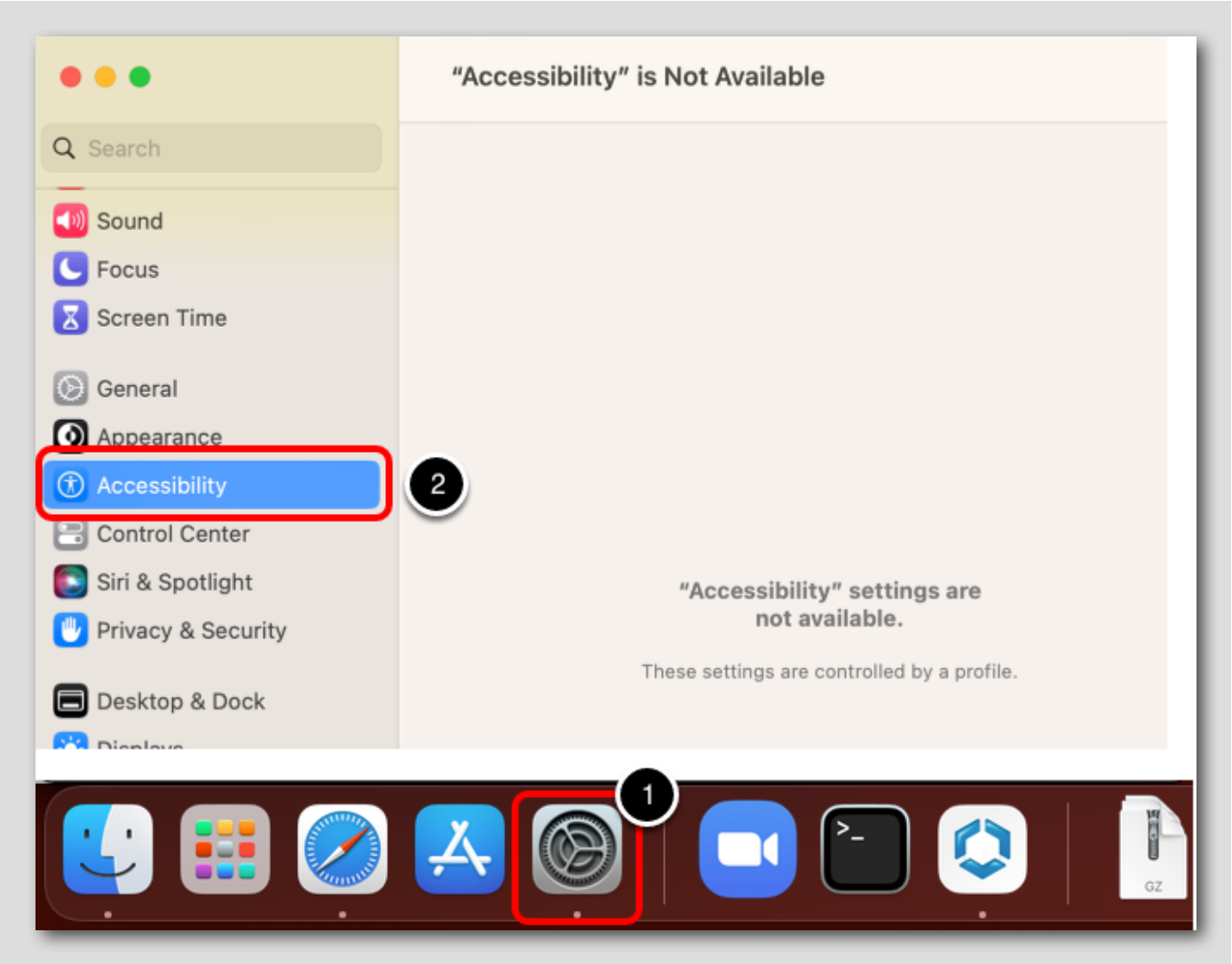


1. Open **Launchpad**
2. Search for **`Assist`**
3. Click the **Assist** app that was installed by Workspace ONE UEM
4. After confirming that the app launches, click the **Close** button to close the app

This confirms that the Workspace ONE Assist app was successfully downloaded and installed on the device.

Validate the Restrictions Profile

[324]



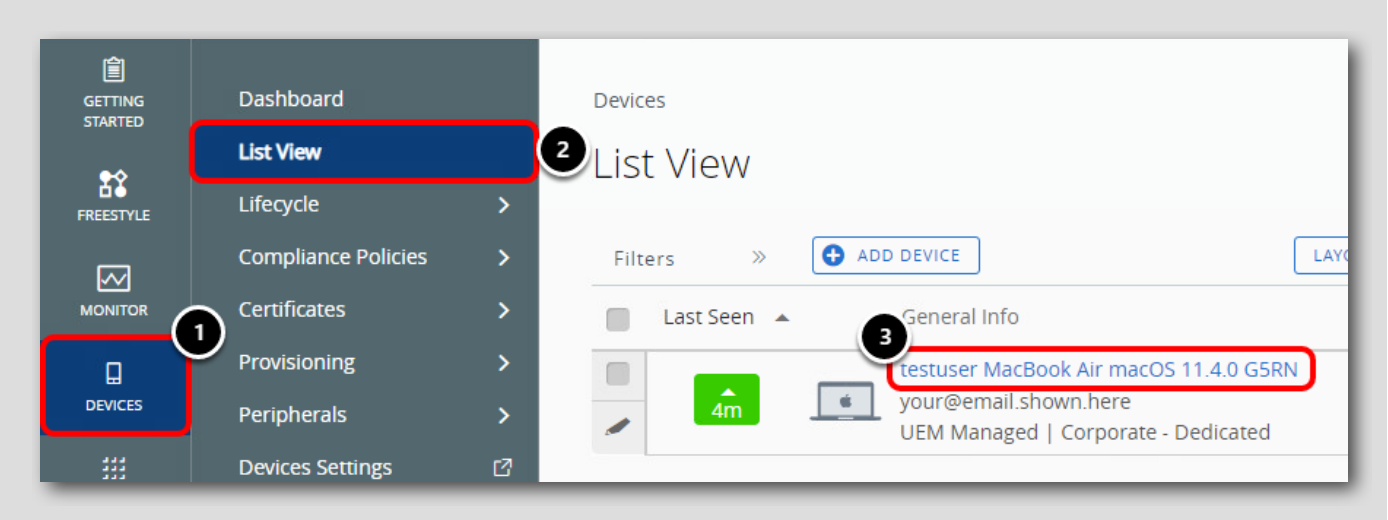
1. Open **System Preferences**.
2. Confirm that the **Accessibility** options are disabled.

This confirms that the Restriction Profile you created to block these configurations in System Preferences has successfully applied to the device.

NOTE: If these options are still accessible, you may need to close and re-open System Preferences.

Validate the Device Sensor

[325]

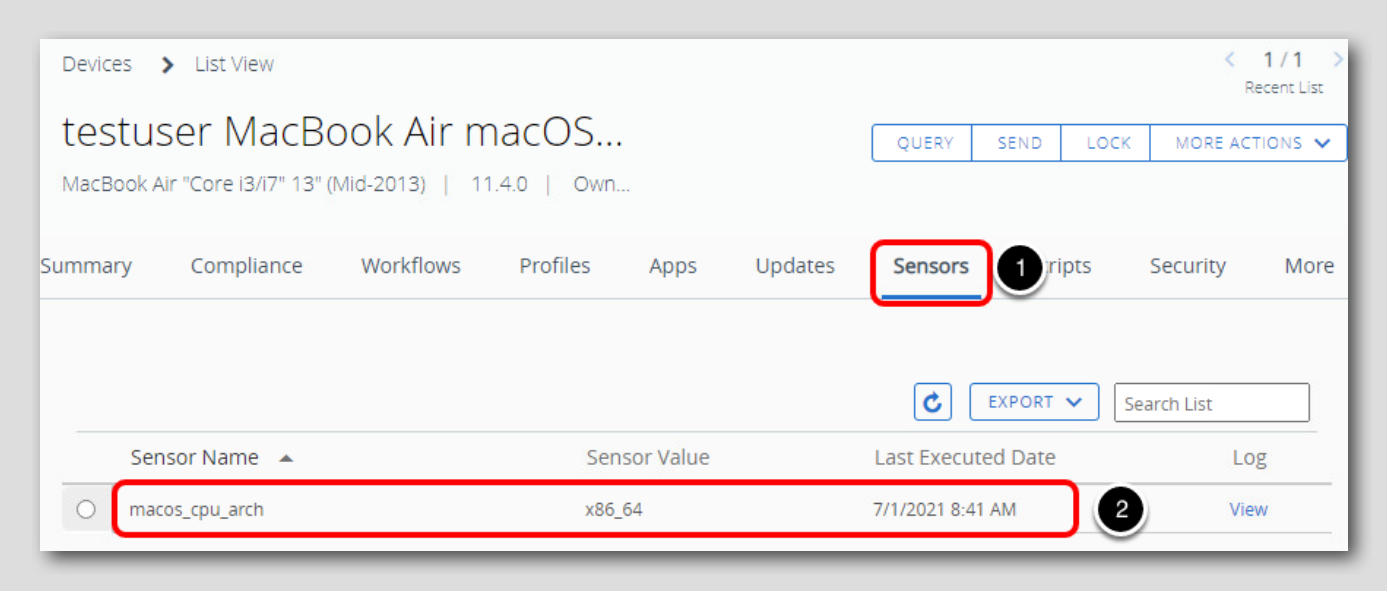


Return to the Workspace ONE UEM administrator console:

1. Click **Devices**
2. Click **List View**
3. Click the **enrolled macOS device** to view the Device Details page

View the Device Sensors

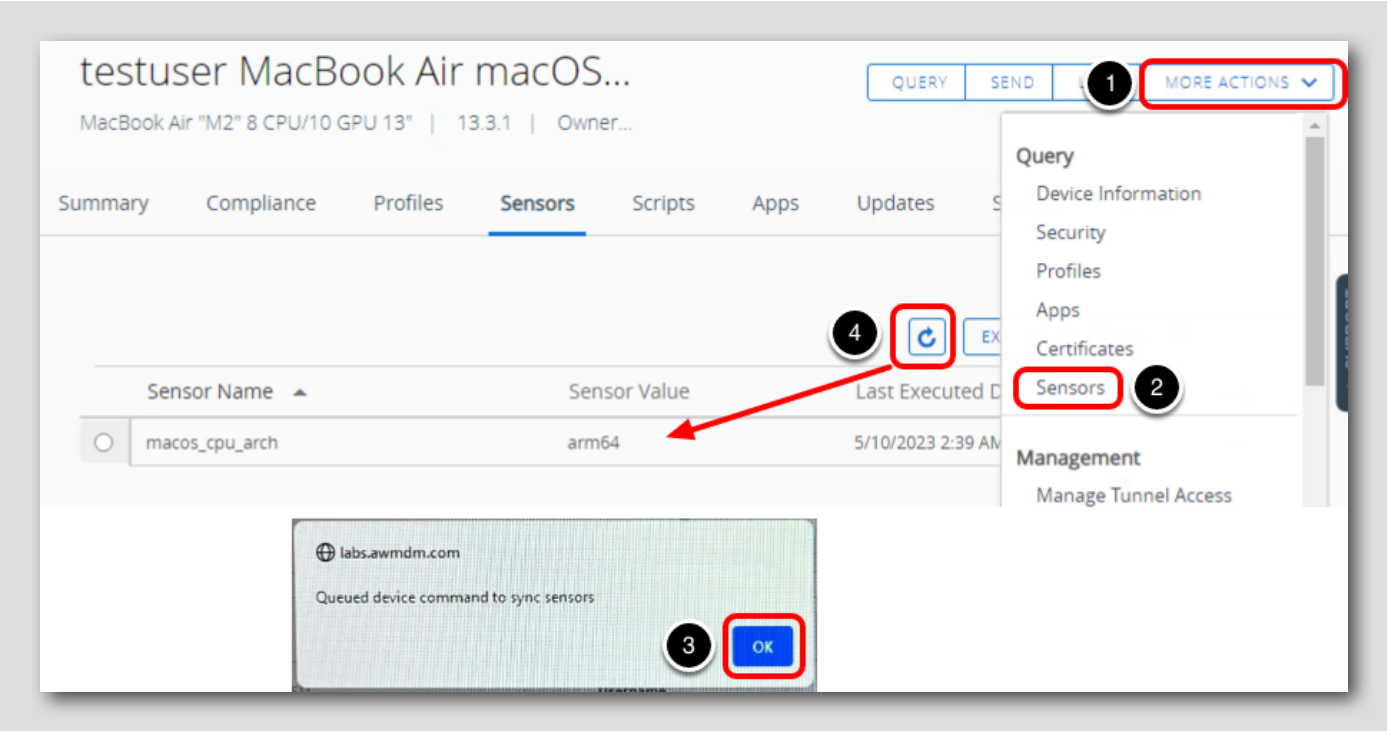
[326]



1. Click the **Sensors** tab
2. Confirm that the **macos_cpu_arch** sensor that was created is displayed. A Sensor Value of either **x86_64** (for Intel chips) or **ARM** (for M series chips) will be displayed based on what your device's processor is.

If the Sensor has not processed on the device yet, you can force the Sensor to process by querying the Sensors on the device.

You can skip this and proceed to the next step if your Sensor has already executed.



1. Click **More Actions**
2. Click **Sensors**
3. Click **OK**
4. Click **Refresh** periodically and check if the macos_cpu_arch sensor is reporting data after executing

Key Takeaways

[327]

This completes your verification of the configurations you made for your macOS device! In summary, you configured and confirmed the following:

1. The Hub Services unified app catalog and other features were available on the device through the Intelligent Hub app
2. The Restriction profile to block the Desktop & Screen Saver and Accessibility settings in System Preferences was successful
3. The Sensor to detect the device's processor was deployed to the device and accessible from the Workspace ONE UEM administrator console
4. The Workspace ONE Assist app was successfully uploaded and deployed to the device
5. The custom Post-Enrollment Onboarding Experience was available on the device to help the user understanding if the onboarding process had been completed and what assets were included in onboarding

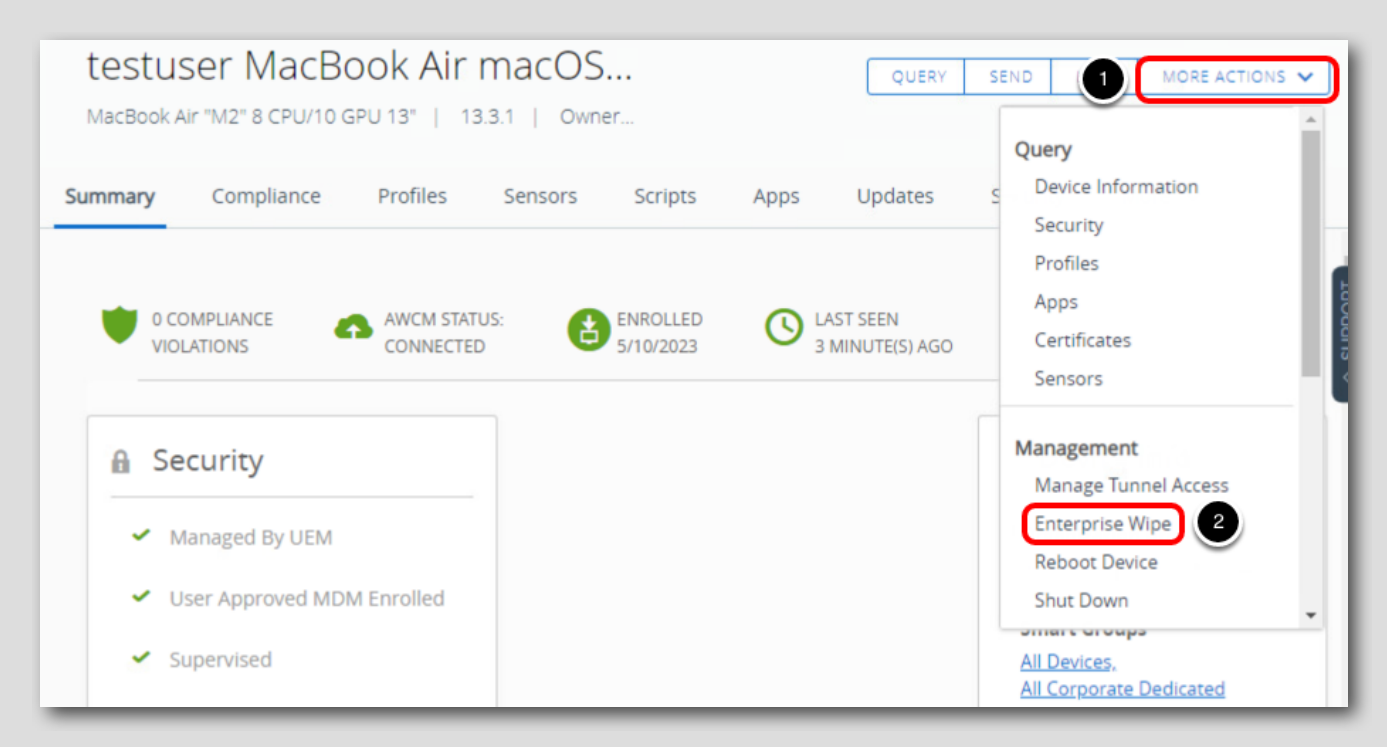
Enterprise Wipe a macOS Device

[328]

An Enterprise Wipe removes corporate data that was added to the device while leaving personal data intact. This can be used to retire devices from your organization or wipe lost devices to ensure that corporate apps and data are removed.

Initiate Enterprise Wipe

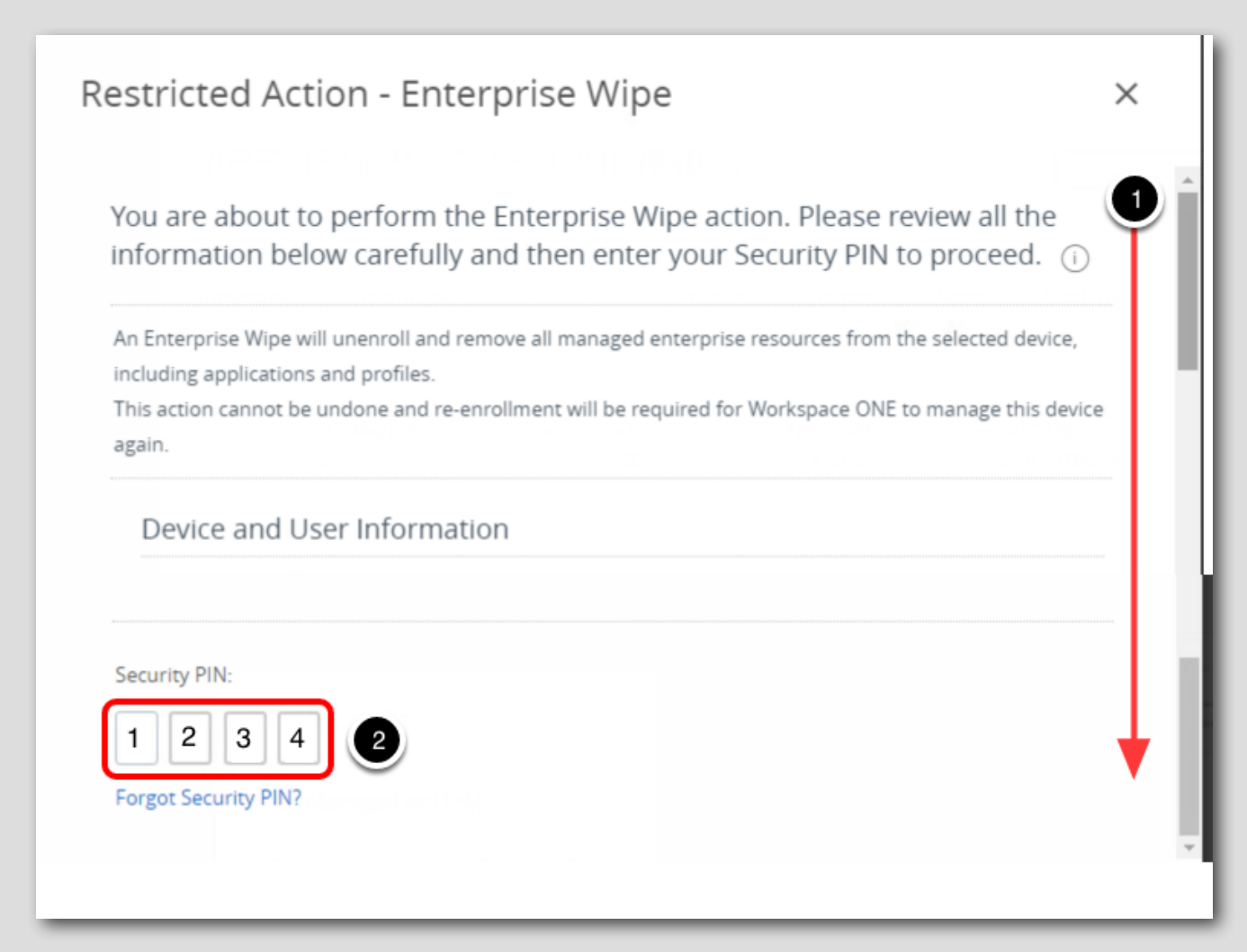
[329]



1. From the toolbar in the device details header, select **More Actions**.
2. Select **Enterprise Wipe** under the **Management** header in the drop-down menu.

Enter Security PIN to Confirm Wipe

[330]

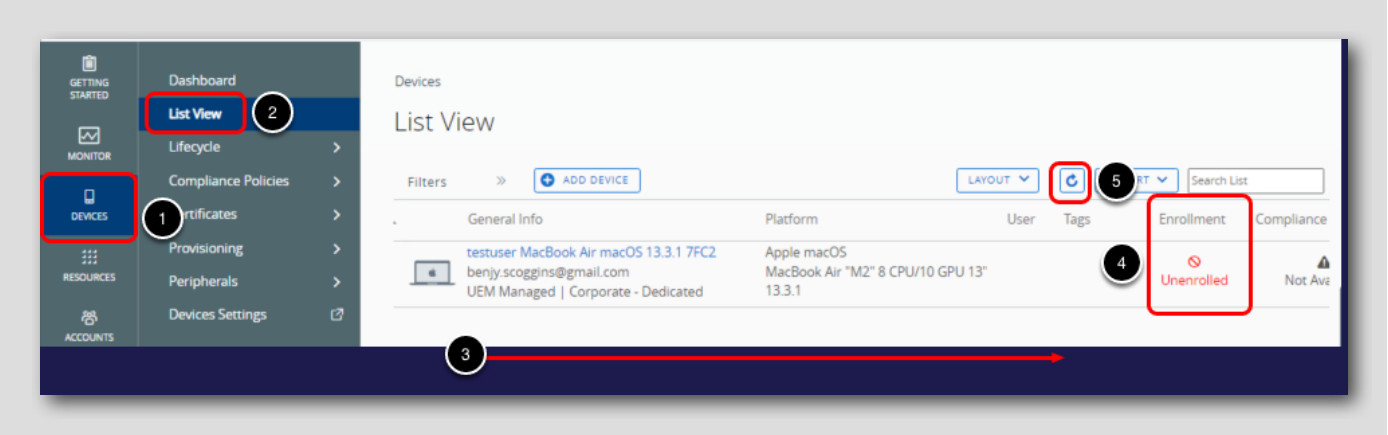


1. Scroll down until you see the section to Enter Security PIN.
2. Enter your security PIN **1234** to initiate the Enterprise Wipe.

Note: If you provided another PIN at the beginning of the lab, provide that security PIN instead.

Confirm Enterprise Wipe

[331]



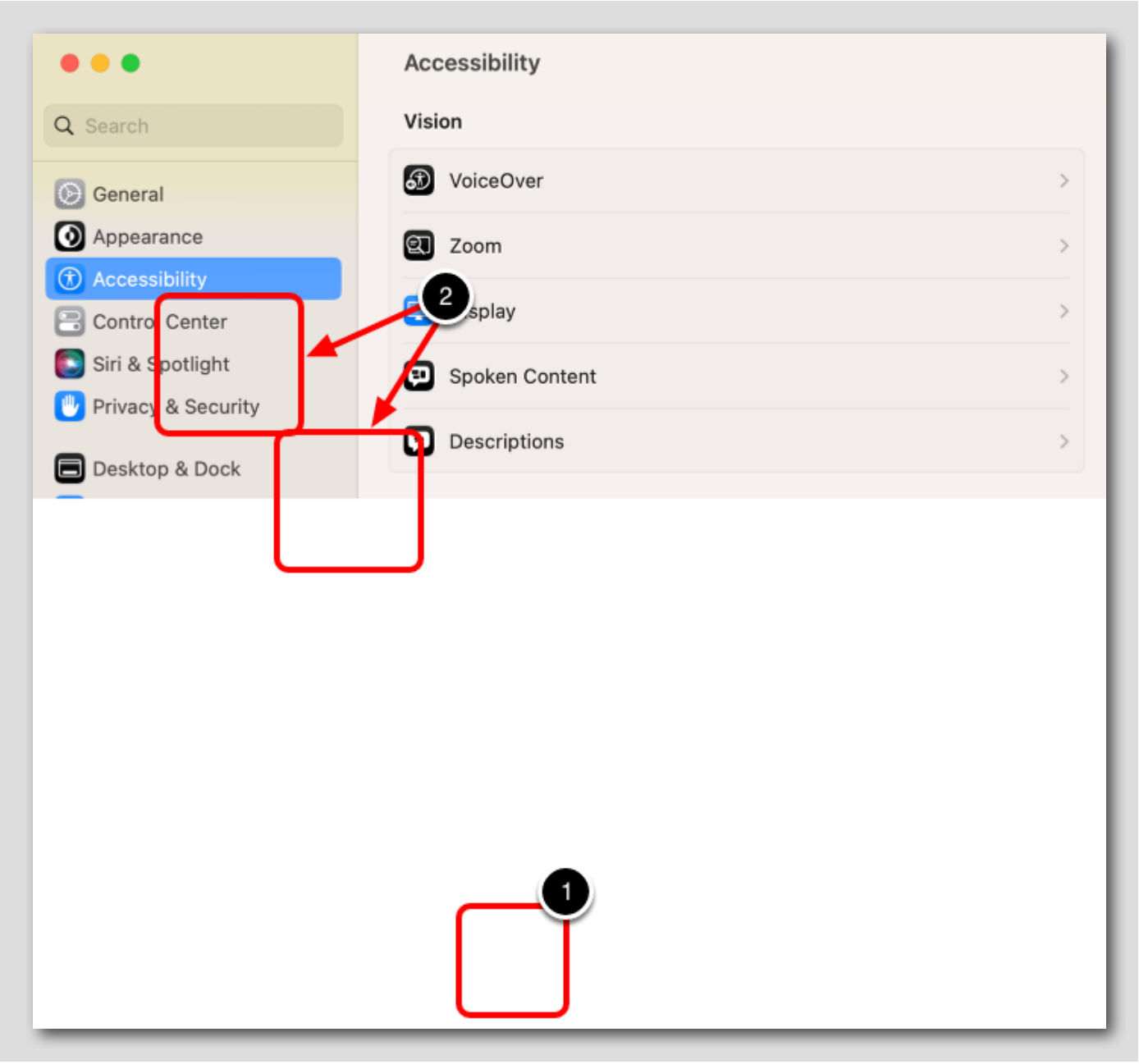
1. Click **Devices**
2. Click **List View**
3. Scroll to the right to find the Enrollment column for the macOS device
4. Confirm that the Enrollment column shows **Unenrolled**
5. If the device is not Unenrolled yet, periodically click the **Refresh** button to check the status

The Enterprise Wipe may take a few minutes to complete. Once completed, the corporate data and apps that were pushed to the device will be removed while leaving the personal data intact.

Once the Enrollment column reports Unenrolled, continue to the next step.

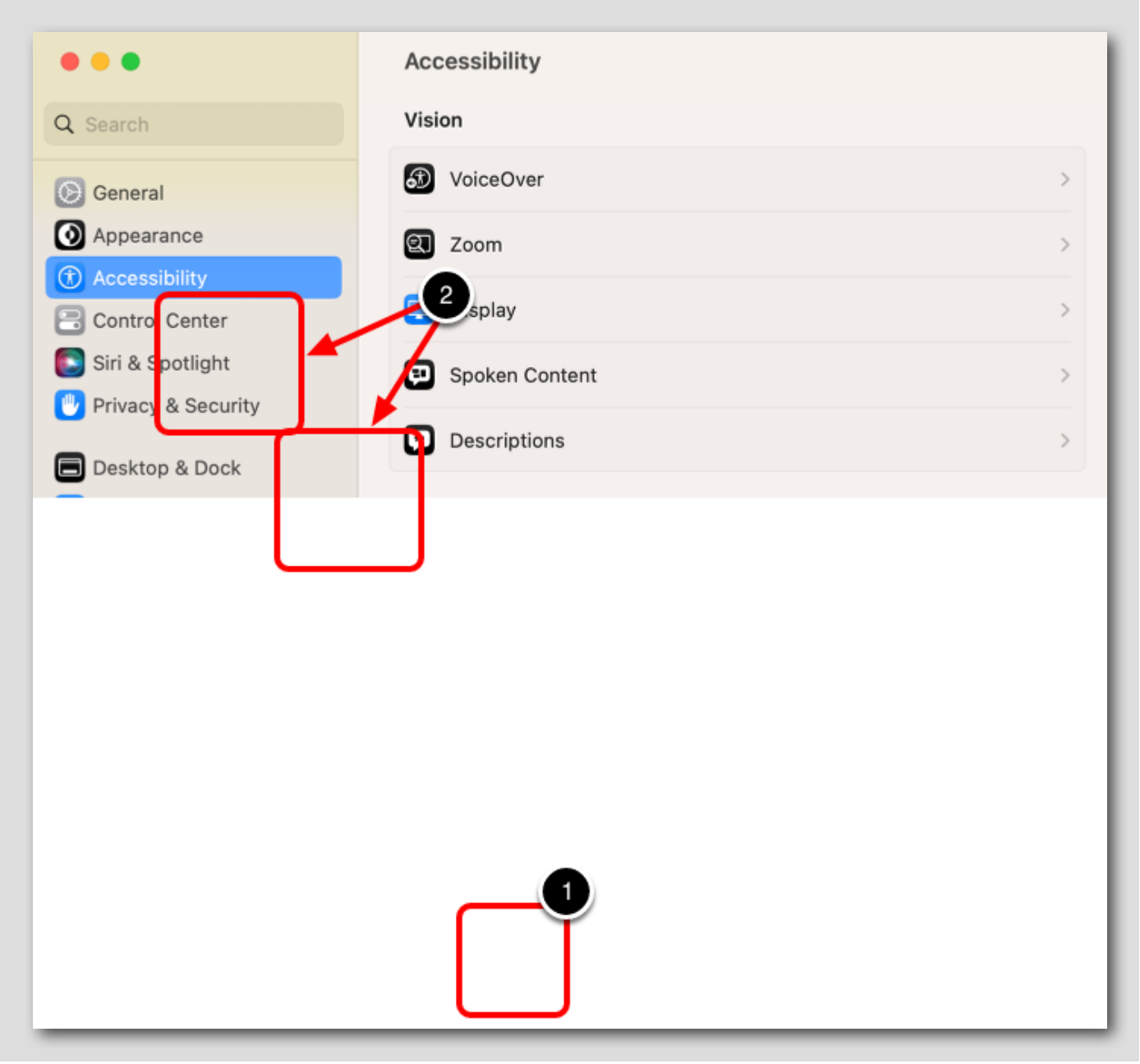
Validate the Enterprise Wipe on the macOS Device

[332]



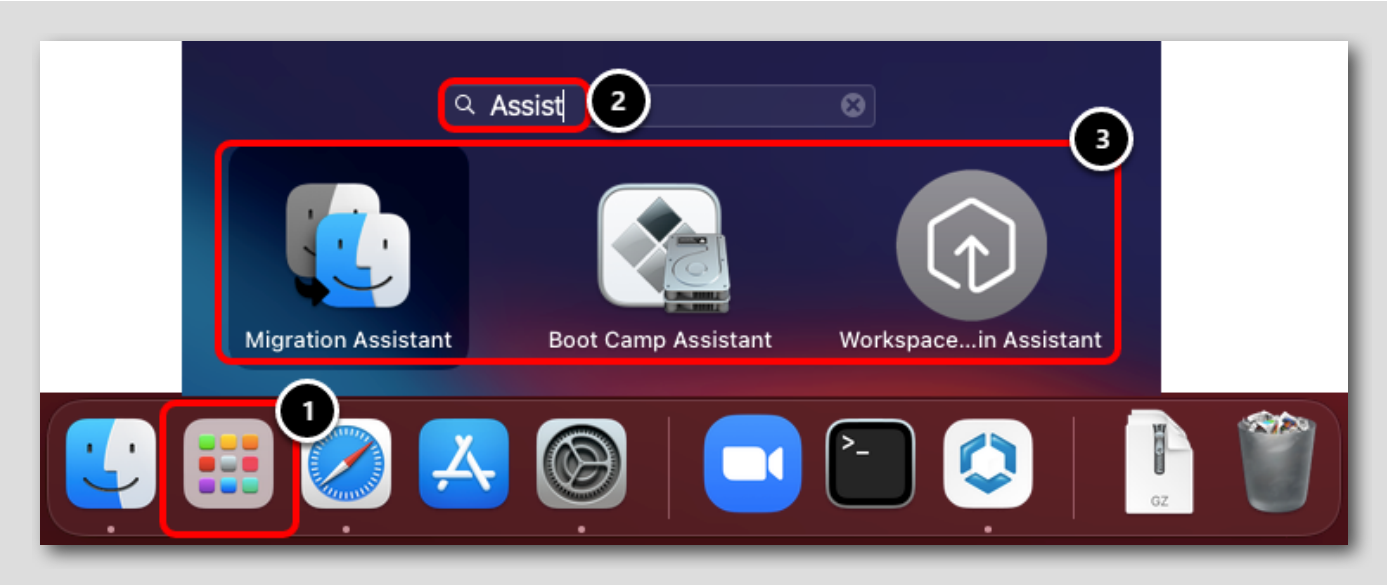
1. Open **System Preferences**.
2. Confirm that the **Desktop & Screen Saver** and **Accessibility** settings are able to be configured again.

This confirms that the Restrictions Profile was removed when the device was unenrolled.


Accessibility
Search
Vision
General
Appearance
Accessibility
Control Center
Siri & Spotlight
Privacy & Security
Desktop & Dock
VoiceOver
Zoom
Spoken Content
Descriptions
2
1

Verify Workspace ONE Assist Was Removed

[333]



1. Open **Launchpad**
2. Enter **`Assist`** in the search bar
3. Confirm that Workspace ONE Assist is not in the returned list of apps

Since the Workspace ONE Assist app was pushed with the Remove On Unenroll restriction, Workspace ONE Assist will be removed from the device when it is unenrolled.

Summary

[334]

This lab covered basic macOS administration using VMware Workspace ONE UEM and a user-initiated enrollment workflow. 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.

Note that this Hands-On Lab *does not* cover the full breadth and capabilities for managing macOS with Workspace ONE. Please see VMware's TechZone for videos, blogs, and documentation that can help you with advanced topics in macOS management, such as:

- Apple Business Manager and Automated Device Enrollment
- Device Staging and Enroll-on-Behalf
- Volume Purchased Applications
- Kiosk Mode
- Certificates and Identity/Directory Integration
- Mail Integration
- ... and More!

Level Up Your VMware End User Computing Knowledge with VMware Tech Zone

[335]

Interested in learning more about VMware End User Computing (EUC) but don't know where to start? Look no further than *https://techzone.vmware.com*, your fastest path to understanding, evaluating, and deploying VMware End User Computing products!

Tech Zone focuses on providing practical product guidance, curated activity paths, and technical content to take you from zero to hero! Our mission at Tech Zone is to provide you with the resources you need to keep leveling up your knowledge no matter where you are in your digital workspace journey.

Interested? Check us out at *https://techzone.vmware.com*!

Return to Lab Guidance

[726]

Use the Table of Contents to return to the Lab Overview page or another module.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.
 Lab SKU: HOL-2451-09-DWS (NEW) Version: 20231106-093218