HOL-2451-09-DWS (NEW)

Getting Started with the Digital Workspace

vmware®

Table of contents

Lab Overview - HOL-2451-09-DWS - Workspace ONE UEM - Getting Started with the Digital Workspace

Lab Guidance

[2]

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

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

Interested in providing a secure digital workspace to meet the demands of a modern and distributed workforce but don't know where to start? Learn the core concepts of Workspace ONE UEM (Unified Endpoint Management) and the fundamentals of enrolling and managing iOS, macOS, Windows 10, and Android devices to distribute apps, policies, restrictions, and powerful workflows. Explore the entire Anywhere Workspace solution, including insightful reports and automation with Workspace ONE Intelligence and how to provide secure access with the Unified Access Gateway.

Lab Module List:

- Module 1 - Introduction to Windows 10 Management (30 minutes) (Beginner) This lab module focuses on introducing the concepts of Unified Endpoint Management (UEM) with Workspace ONE for the Windows 10 platform. Learn how to enroll a Windows 10 device into Workspace ONE UEM and how to configure and deploy restriction profiles and applications to your enrolled device.
- Module 2 - Introduction to Apple iOS Management (30 minutes) (Beginner) This lab module focuses on introducing the concepts of Unified Endpoint Management (UEM) with Workspace ONE for the iOS platform. Learn how to enroll an iOS device with Workspace ONE UEM and deploy device profiles to add restrictions and change the behavior of your iOS devices.
- Module 3 - Introduction to Apple macOS Management (45 minutes) (Intermediate) Explore key Workspace ONE UEM administration features and concepts available for the macOS platform. This module gives you a better understanding of how macOS devices are enrolled, what management options are available, and how these options can improve and impact the user experience by configuring macOS and publishing applications.
- Module 4 - Introduction to Android Management (45 minutes) (Beginner) This module focuses on Learning the fundamentals of Android Enterprise, including how to enroll an Android device into Workspace ONE UEM and manage enrolled devices by configuring restrictions and pushing apps. Learn how Android Enterprise and Workspace ONE UEM secure your Android devices by using modern device management APIs.
- Module 5 - Introduction to Workspace ONE Intelligent Hub and Hub Services (60 minutes) (Beginner) Learn the fundamental capabilities of the Workspace ONE Intelligent Hub app and how it simplifies enrollment for Workspace ONE UEM. Explore and configure Hub Services and Workspace ONE Access to expand the Intelligent Hub app feature set to provide a unified app catalog, Single Sign-On (SSO) capabilities, people search, and more.
- Module 6 - Workspace ONE Intelligence - Introduction to Dashboards, Automation, and Reports (45 minutes) (Beginner) Explore the Workspace ONE Intelligence Console to view how Dashboards and Reports can provide deeper insights and customize inspection for your deployments at a glance. Configure Automation tasks and discover how to reduce your manual

administrative workload, increase security and automate remediation.

- Module 7 - Introduction to Freestyle Orchestrator (30 minutes) (Beginner) Freestyle Orchestrator enables Workspace ONE UEM administrators to create complex workflows that fit specific requirements with flexibility and speed. Freestyle workflows can be used to set up resources such as applications, profiles, sensors, and scripts. These workflows use conditions to apply resources to devices based on granular criteria.
- Module 8- Workspace One UEM on Linux. (30 minutes) (Beginner) Linux, As technology continues to evolve, businesses are constantly seeking innovative solutions to streamline their operations and enhance productivity. With the growing popularity of Linux as an operating system, the integration of Workspace ONE brings forth a powerful combination that empowers Organization to achieve new levels of efficiency and security.

Lab Principals:

- **Vernon Lihou**, Senior Lead SME DWS, Solution Engineering, United Kingdom

Lab Captains:

- **Lead Captain - Benjy Scoggins**, Staff Solution Engineer, USA
- **Pavitra Nagendrappa**, Colleague Support Engineer, India

Special thanks:

Bill Call & Mark McGill for outstanding support!

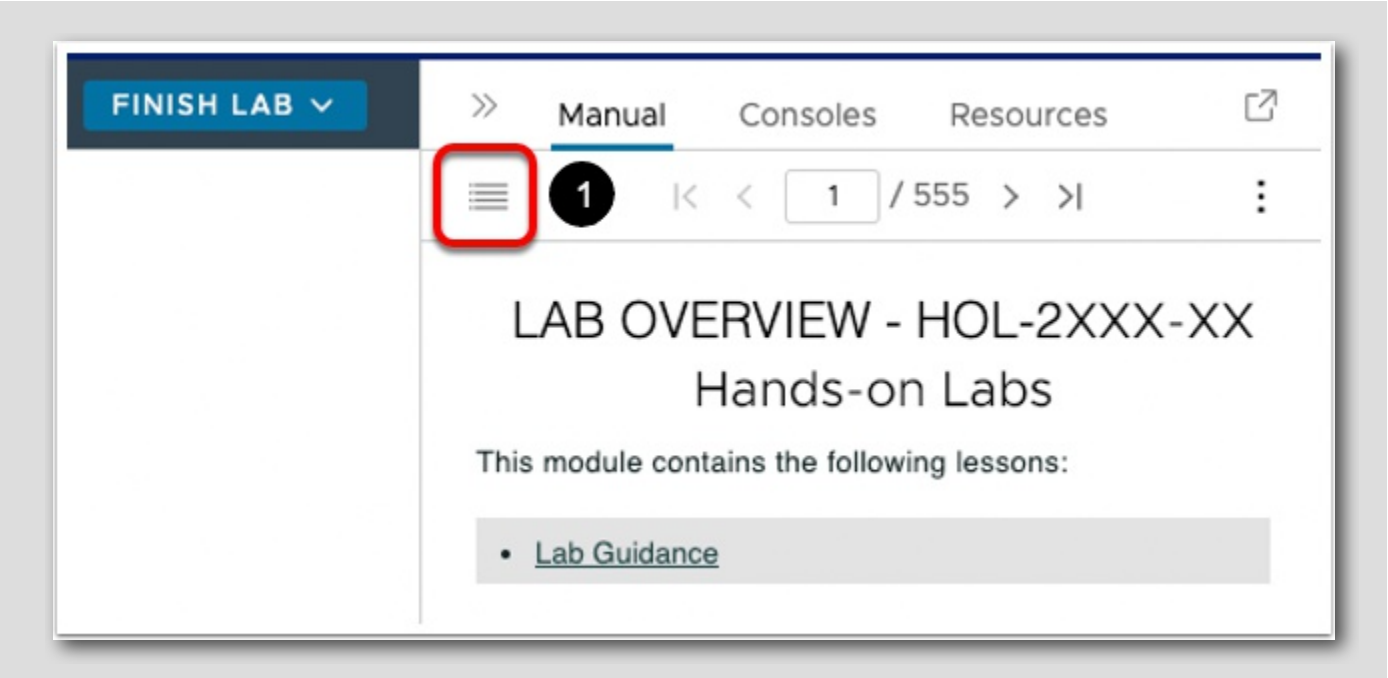
This lab manual can be downloaded from the Hands-on Labs Document site found here:

http://docs.hol.vmware.com

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

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

First time using Hands-on Labs? [3]



Welcome!

1. If this is your first time taking a lab navigate to the **Appendix** in the Table of Contents to review the interface and features before proceeding. For returning users, feel free to start your lab by clicking next in the manual.

You are ready....is your lab? [4]

The lab console will indicate when your lab has finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait for the status to update. If after 5 minutes your lab has not changed to "Ready", please ask for assistance.

Module 1 - Introduction to Windows 10 Management (30 minutes) Beginner

Introduction [6]

Learn how to enroll a Windows 10 device into Workspace ONE UEM and how to configure and deploy restriction profiles and applications to your enrolled device.

Pre-Requisites [7]

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

- A virtual machine or spare Windows device running Windows 10 (non-Home edition) with the latest updates installed.
- DO NOT access the Hands-On Lab from the same machine you will be managing.

  NOTE - We have provided a Windows 10 VM for you which has all the prerequisites setup for this lab. We recommend you use that by following the instructions in the manual for this lab.
- Administrative rights to the virtual machine or spare Windows device you will use to perform the Hands-On Lab.
- A Windows 10 Desktop app (*.msi), such as 7-Zip. A sample Windows 10 app has been provided in the lab machine for your use.

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

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

DO NOT Enroll Personal Windows 10 Devices [8]

IMPORTANT: You SHOULD NOT enroll a personal Windows 10 device for the upcoming exercise! Personal devices may be enrolled into other EMM providers which can cause undesired conflicts and issues.

Please follow the upcoming steps to enroll and use the provided Win10-01a virtual machine for this Hands-on Lab.

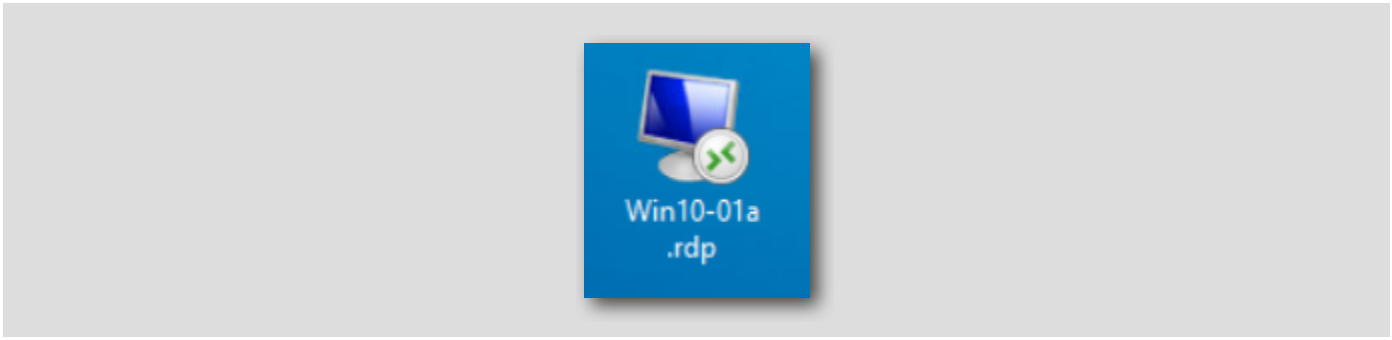
IMPORTANT: You SHOULD NOT enroll any personal device(s) for the upcoming exercise!

Personal devices may be enrolled into other UEM providers which can cause undesired conflicts and issues. - We want to avoid this!

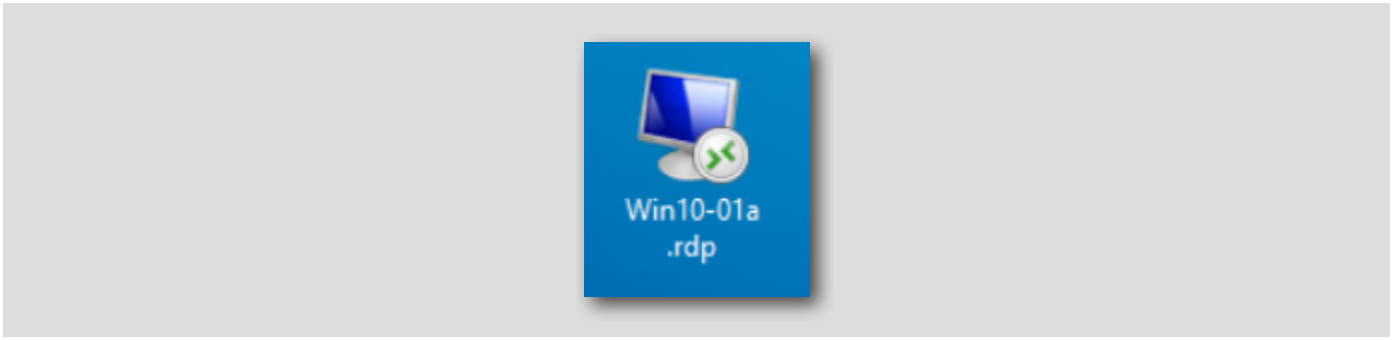
To complete this lab, we recommend you use a test device ONLY and avoid enrolling personal devices in the lab.

Connect to the Windows 10 Virtual Machine

[9]



Double-click the **Win10-01a.rdp** shortcut located on the Main Console Desktop to connect to the Windows 10 virtual machine.



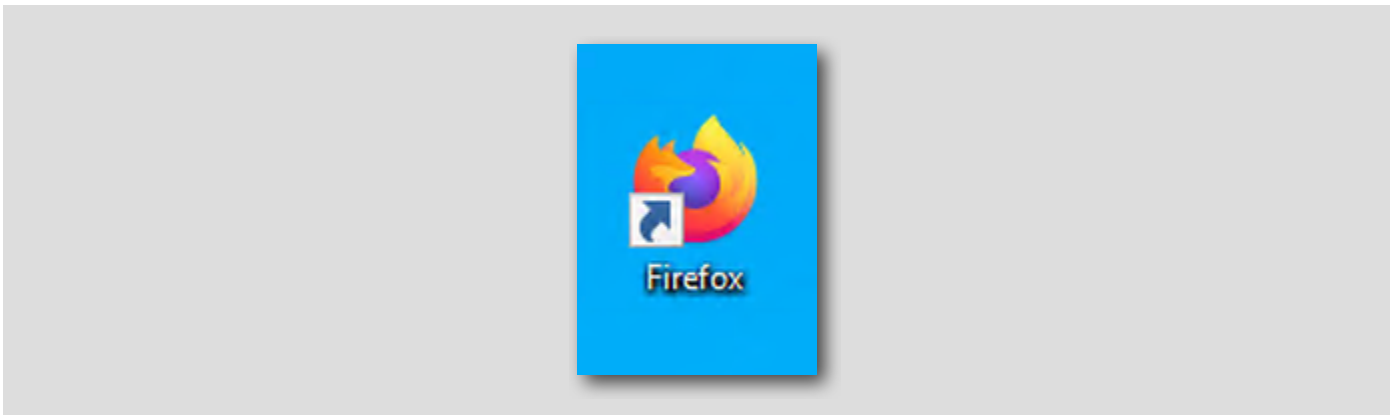
Login to the Workspace ONE UEM Console

[10]

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

Launch Firefox Browser

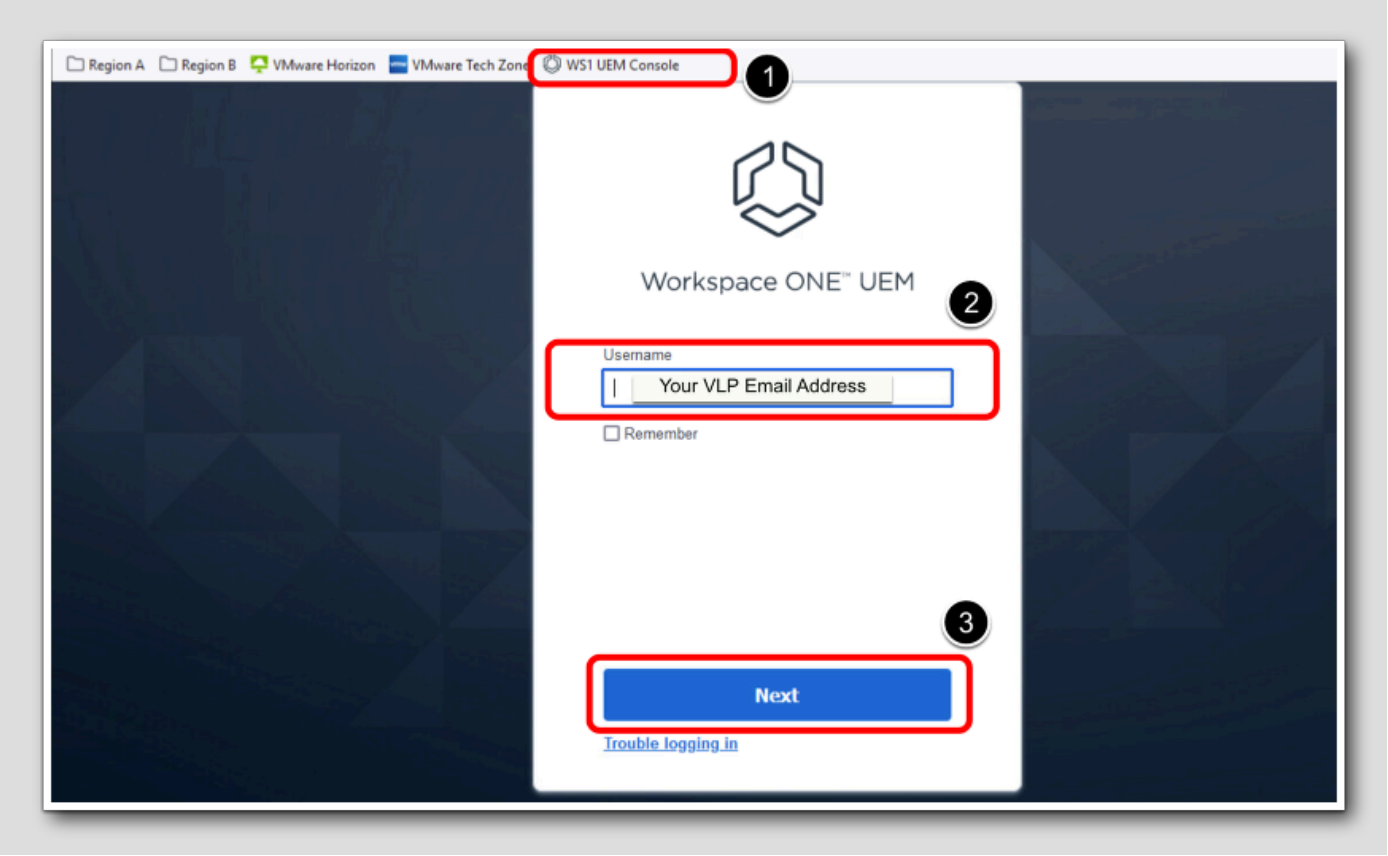
[11]



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

[12]

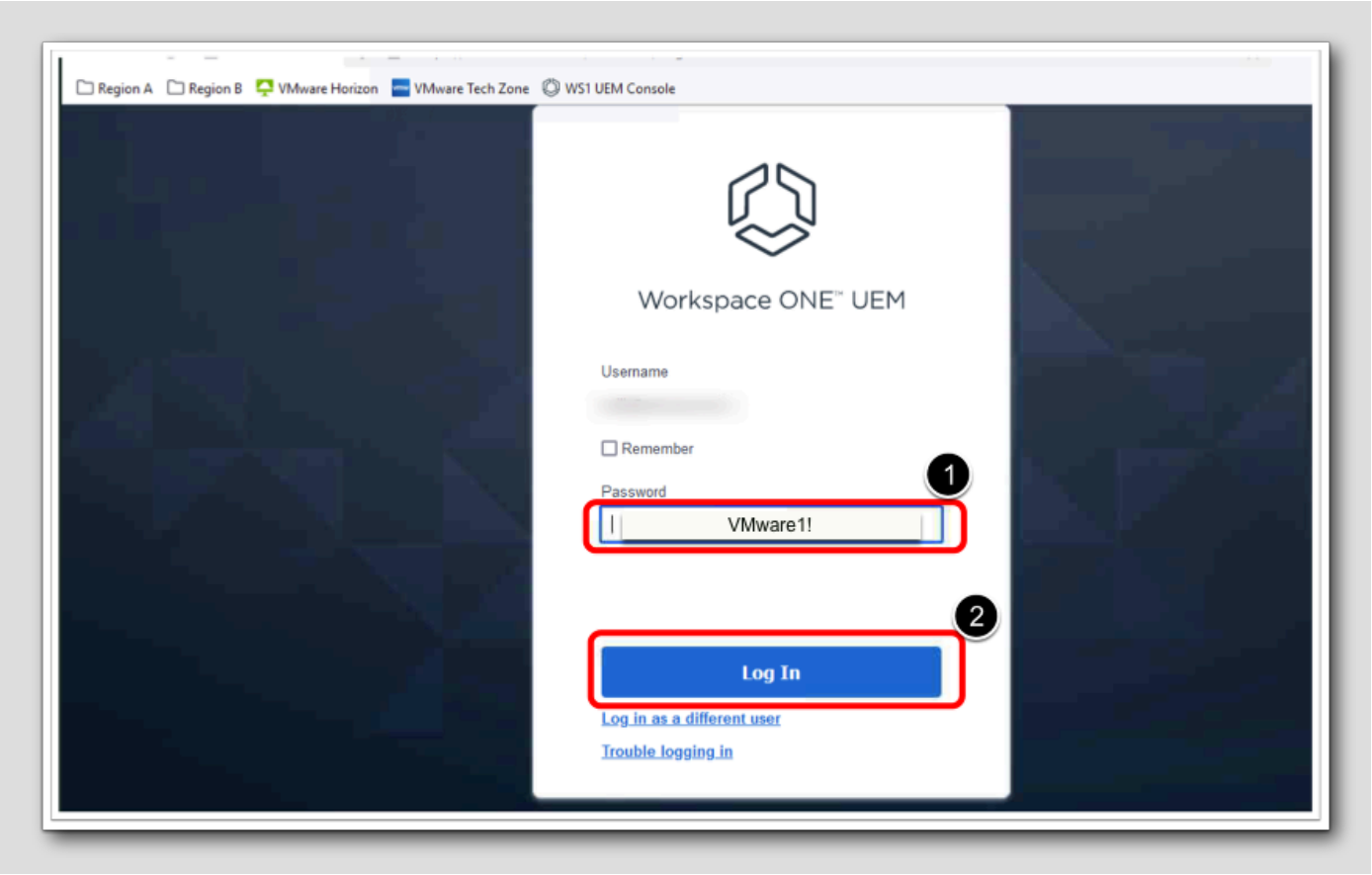


1. Select the **WS1 UEM Console** link from the Bookmark Toolbar
2. Enter your **Username**. This is the **email address** that you have associated with your **VMware Learning Platform (VLP)** account that you utilized to take Hands-on Labs.
3. Click **Next**, then advance to the next step of the lab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

[13]



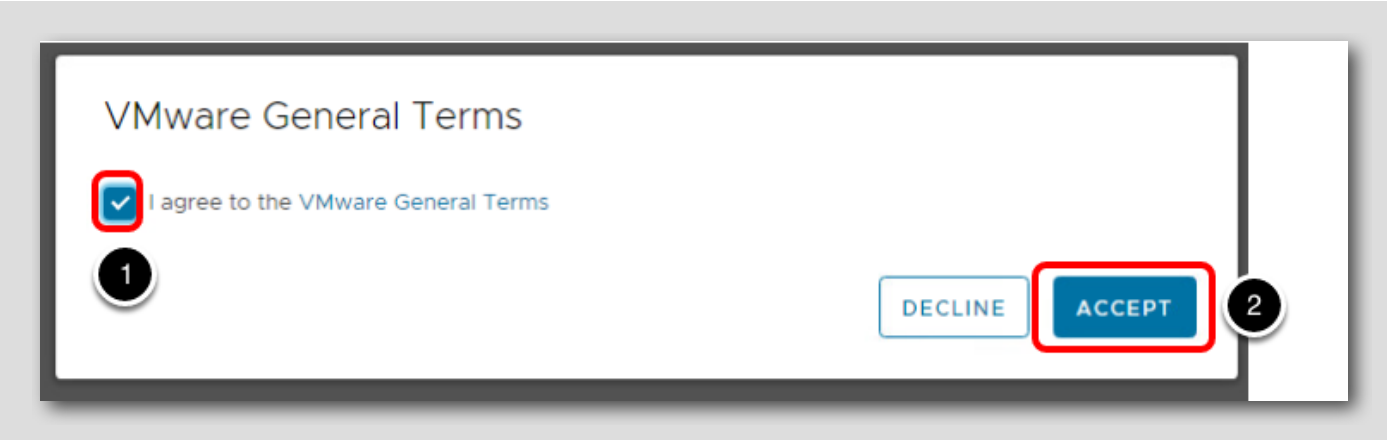
The password field will be displayed after entering your username.

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

[14]



You will be presented with the VMware General Terms.

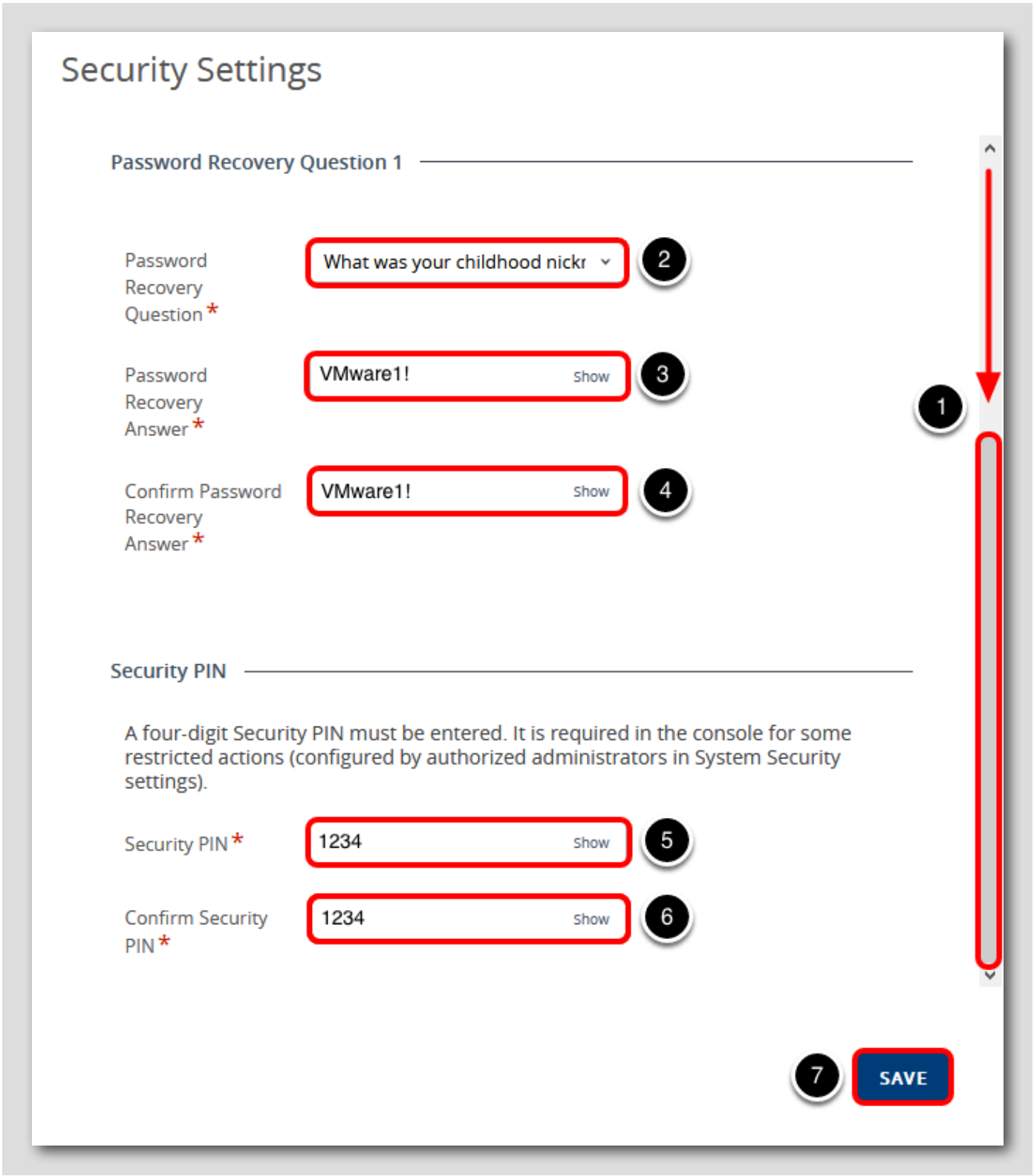
1. Select the box next to I Agree to the VMware General Terms.
2. Click the **Accept** button.

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

[15]

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

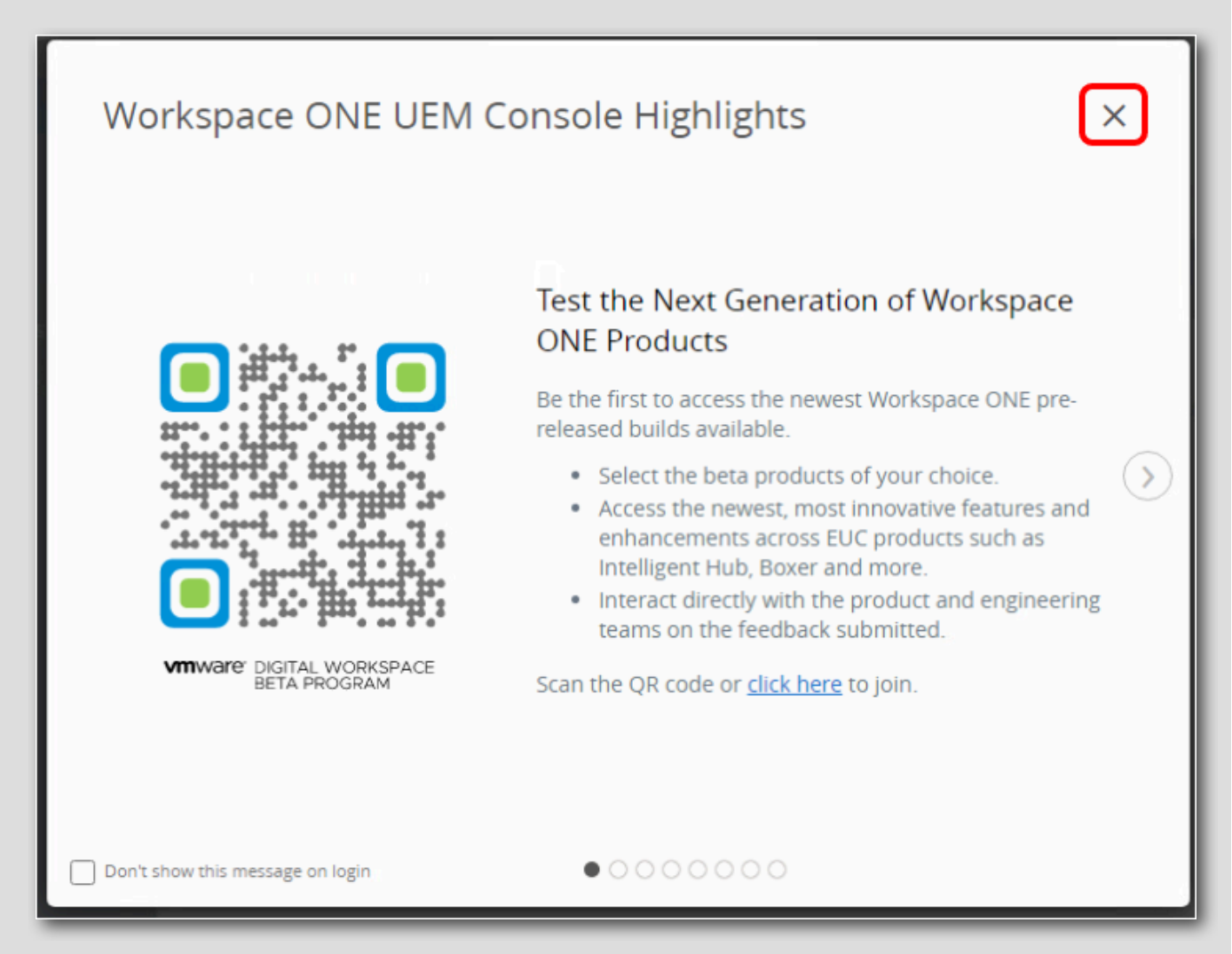

Security Settings
Password Recovery Question 1
Password Recovery Question *
What was your childhood nickr
2
Password Recovery Answer *
VMware1!
Show
3
1
Confirm Password Recovery Answer *
VMware1!
Show
4
Security PIN
A four-digit Security PIN must be entered. It is required in the console for some restricted 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

[16]



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.

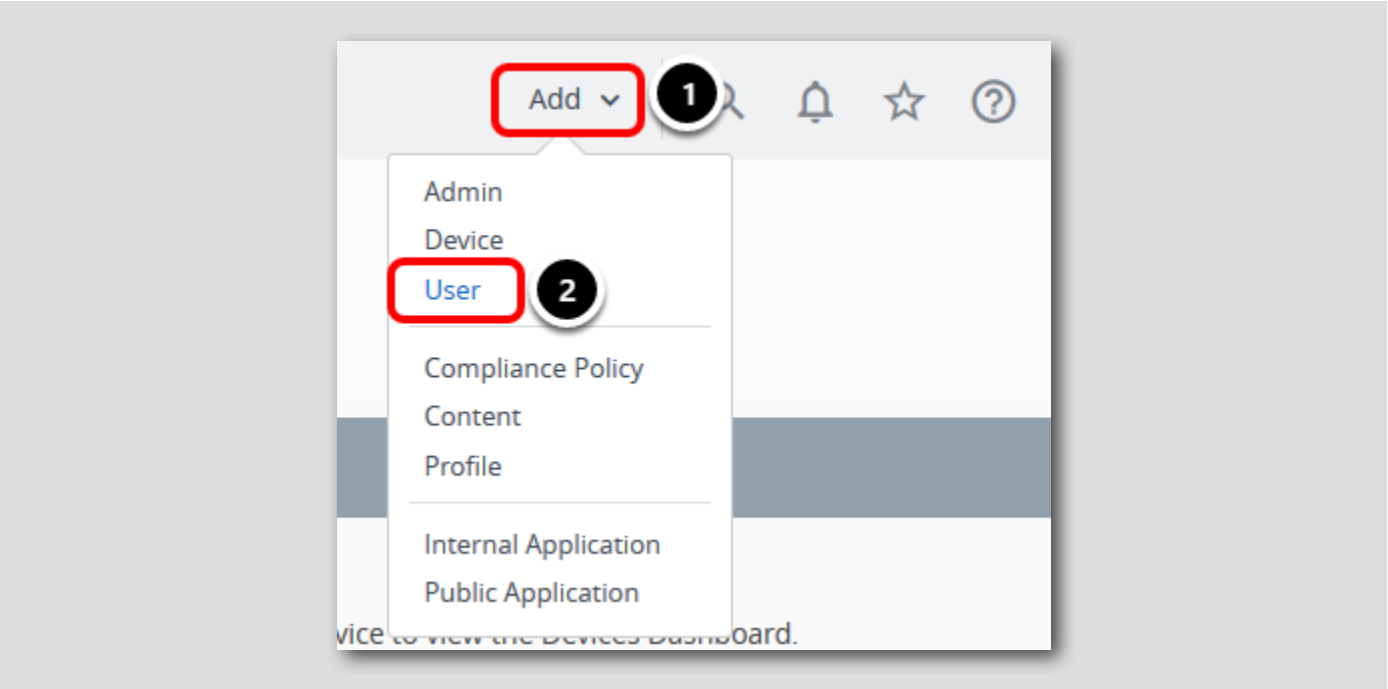
Create a Basic User Account

[17]

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

Click on Add / User

[18]

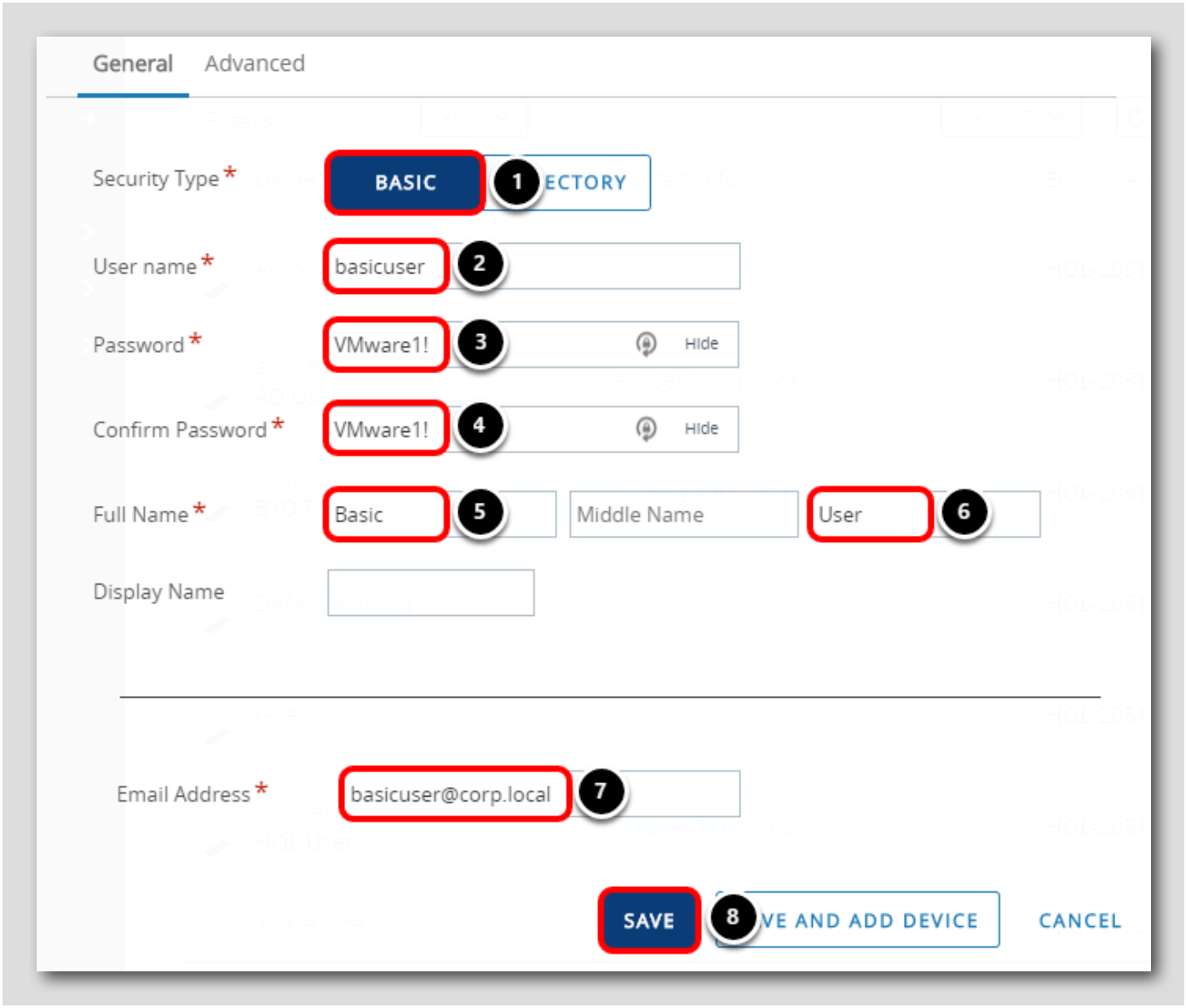


In the top right corner of the Workspace ONE UEM console,

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

Add User Information

[19]



In the pop-up window,

1. Ensure that security type is Basic
2. Enter the username as **basicuser**
3. Enter the password as **VMware1!**
4. Confirm the password as **VMware1!**
5. Enter the first name as **Basic**
6. Enter the last name as **User**
7. Enter the e-mail address as **basicuser@corp.local**

   NOTE: Use the scroll bar if you don't see the option to enter email address
8. Click on Save

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

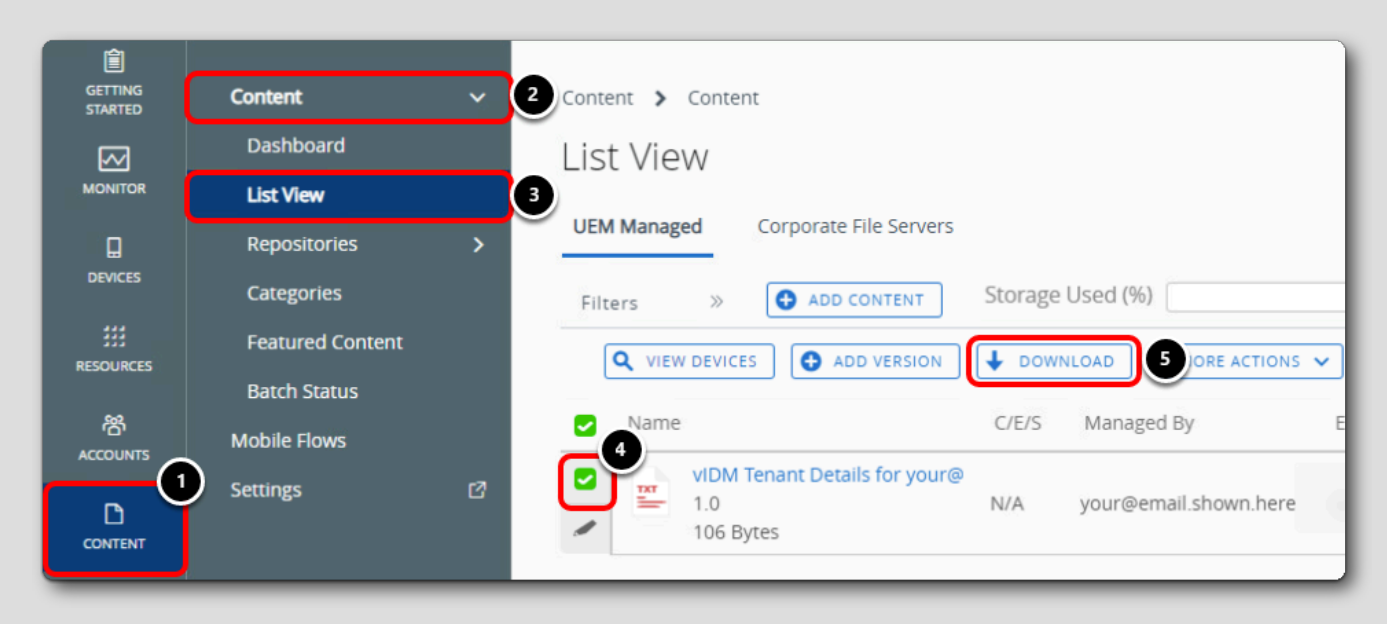
Accessing Your Workspace ONE Access Tenant Details [20]

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 [21]

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.

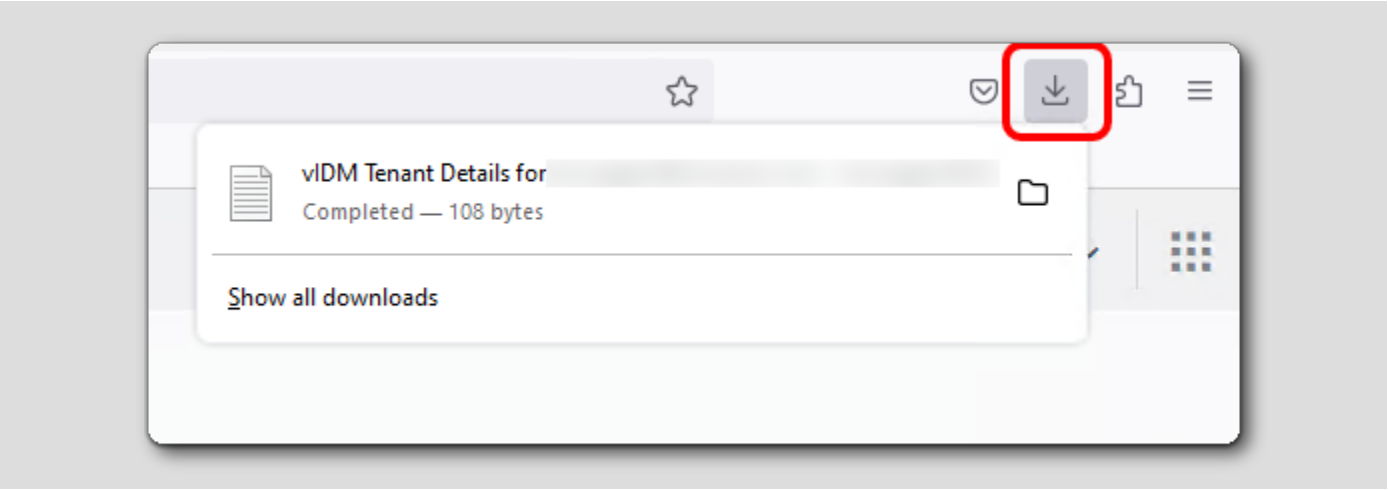


In the Workspace ONE UEM Console:

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

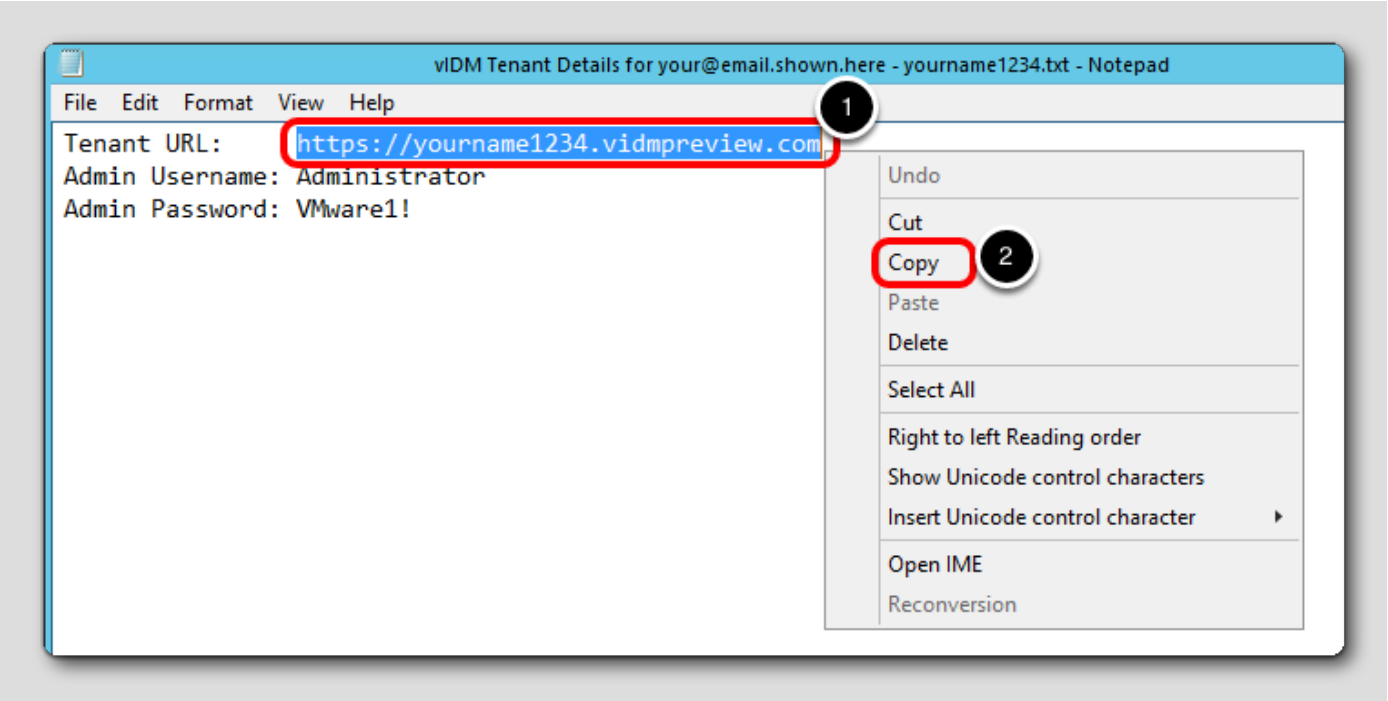
[22]



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

[23]



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

[24]

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

New Customers to Workspace ONE

[25]

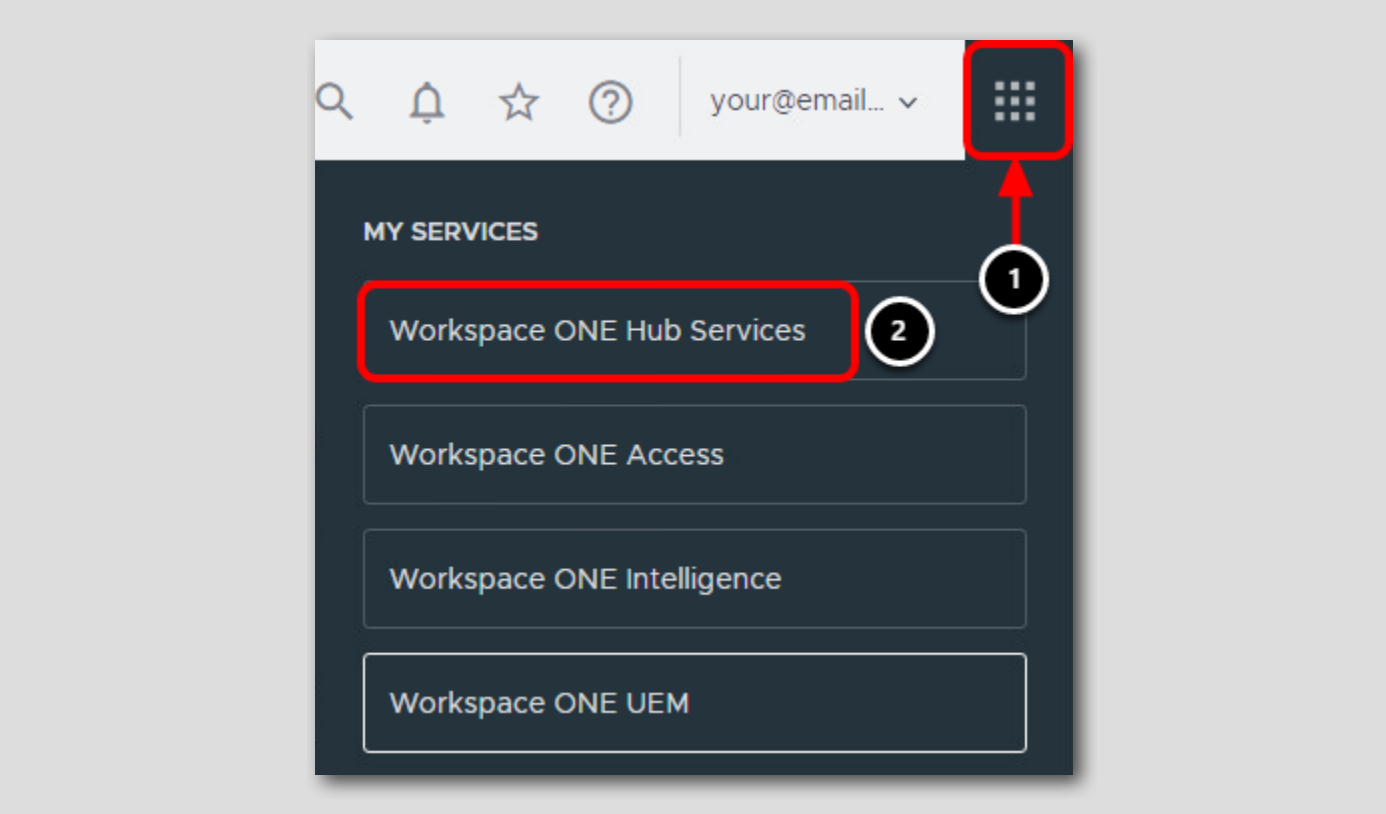
New cloud customers who purchased Workspace ONE after January 2019 have Hub Services activated automatically as part of the instance provisioning process. Workspace ONE UEM, Workspace ONE Access, and Hub Services consoles are connected together, and the Hub catalog is enabled for the Intelligent Hub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

Existing Cloud Workspace ONE UEM Customers [26]

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 [27]

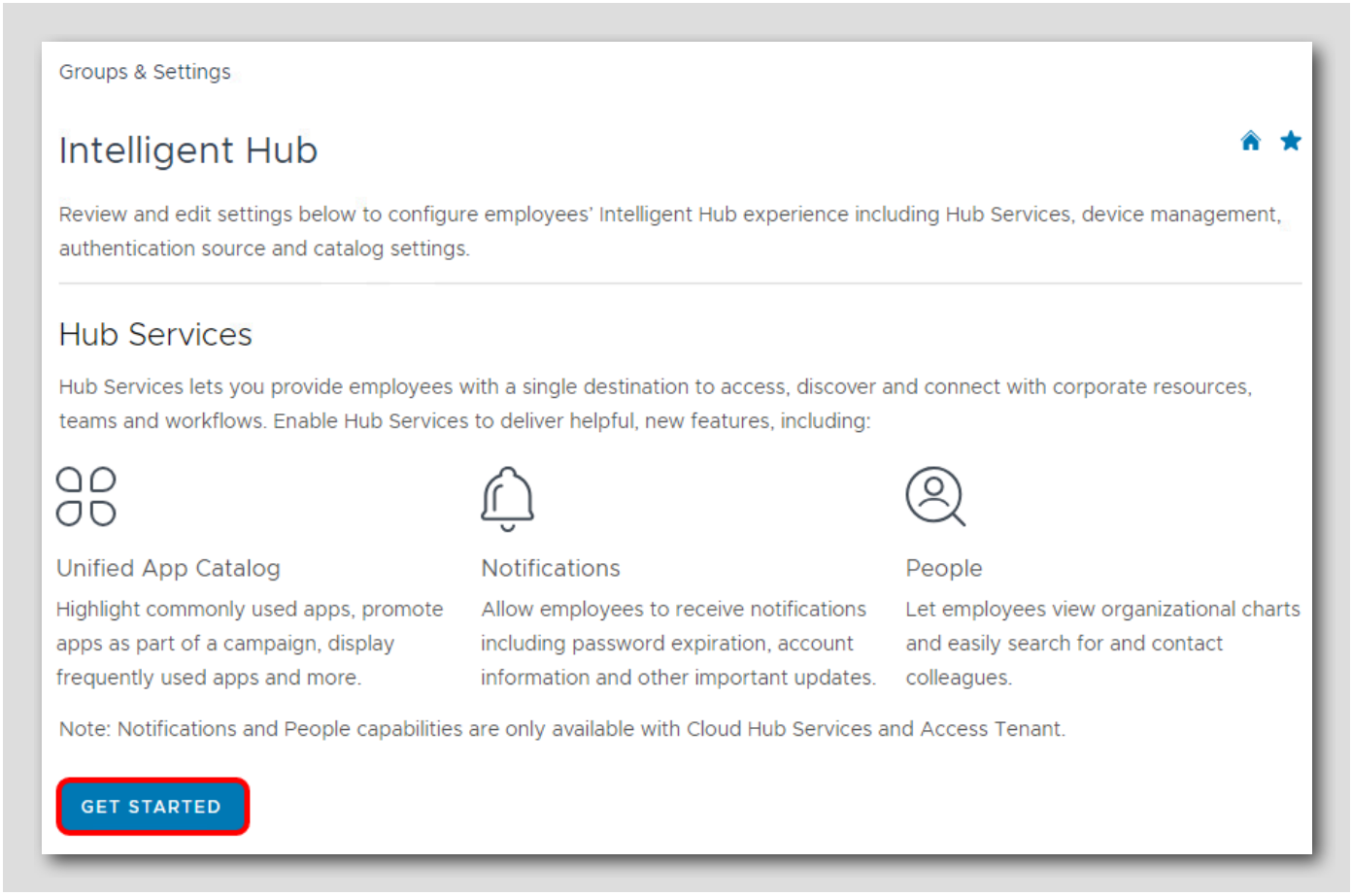


Return to the UEM console in the Firefox browser.

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

Get Started

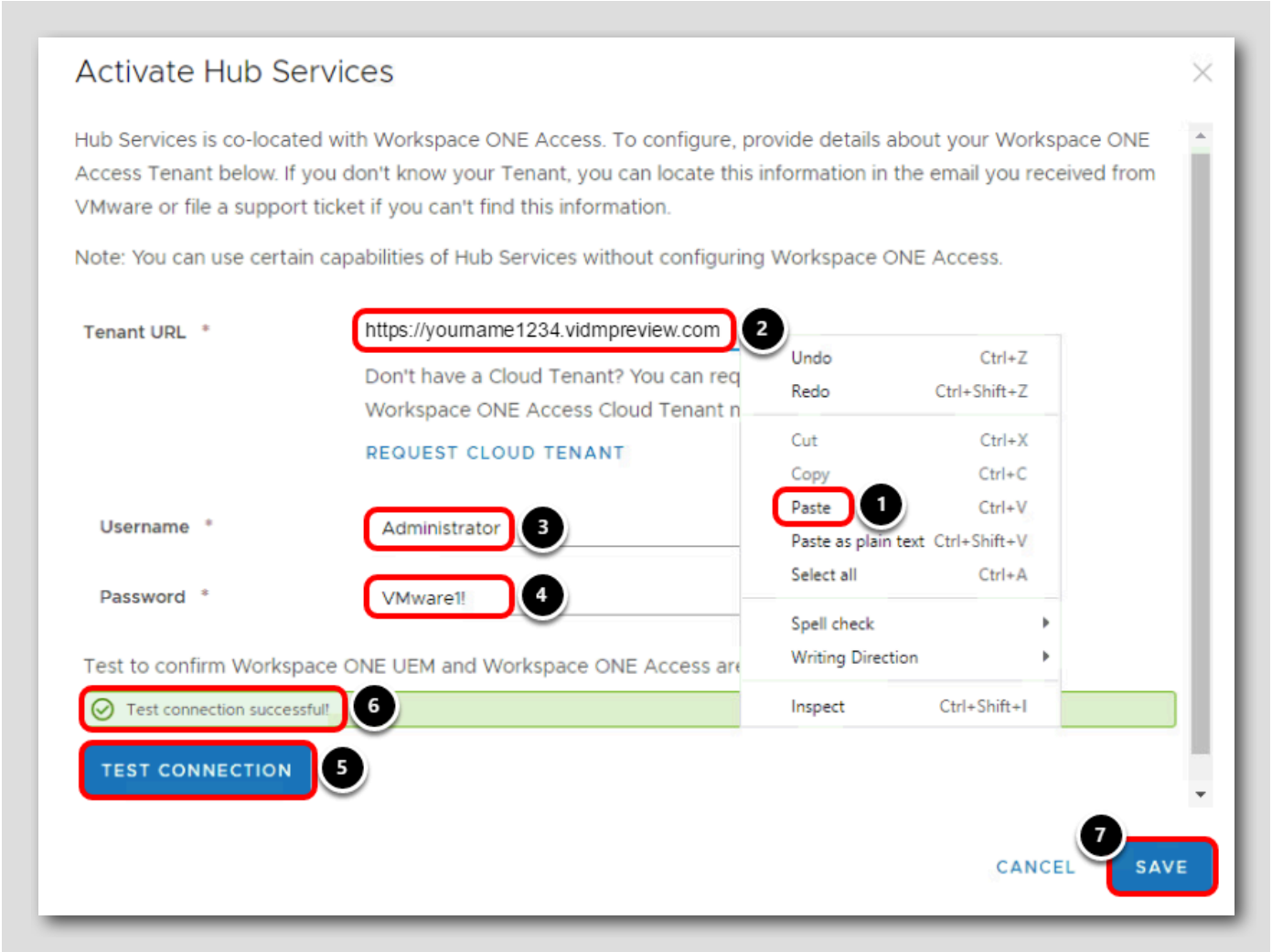
[28]



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

Activate Hub Services

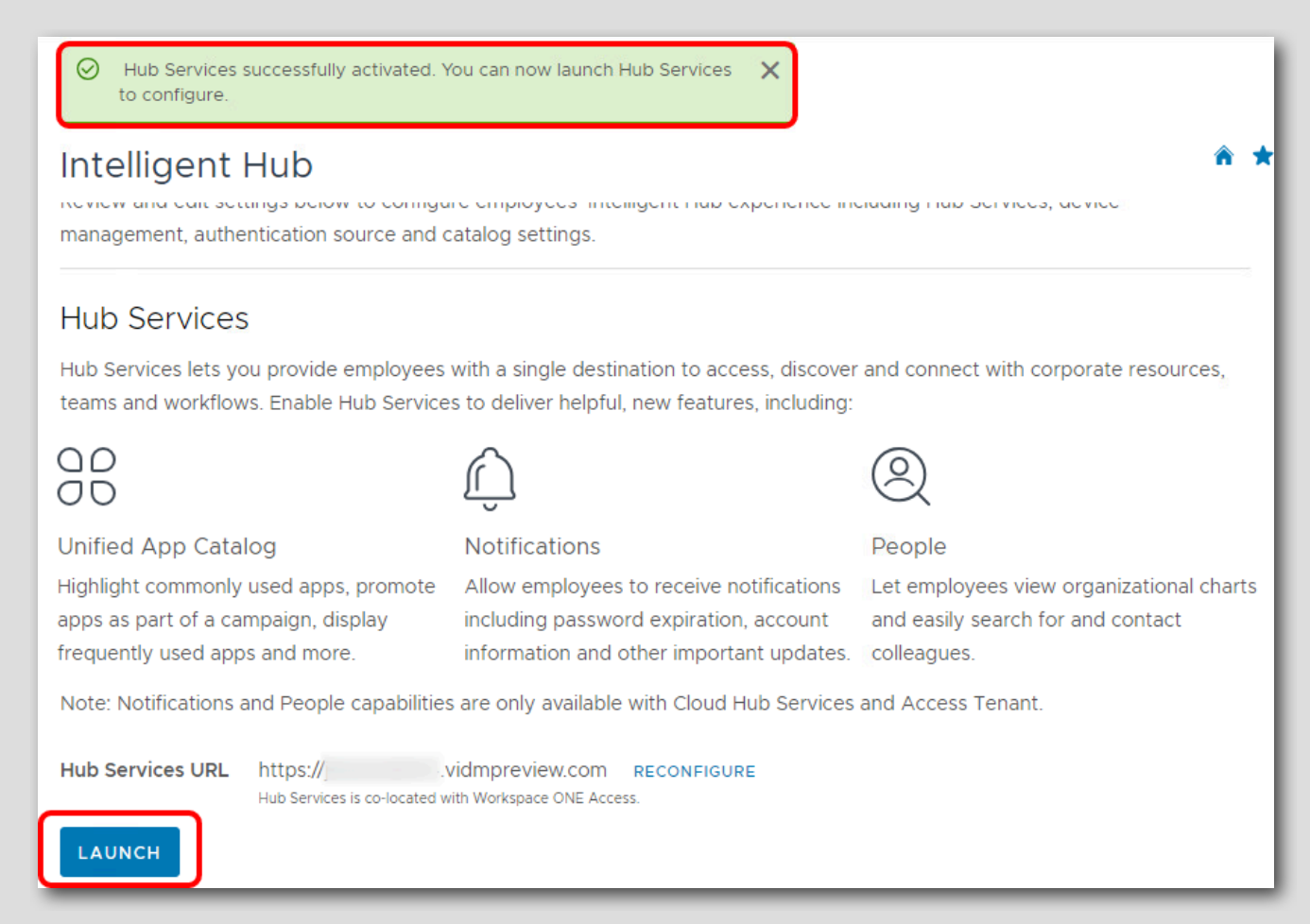
[29]



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

[30]



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

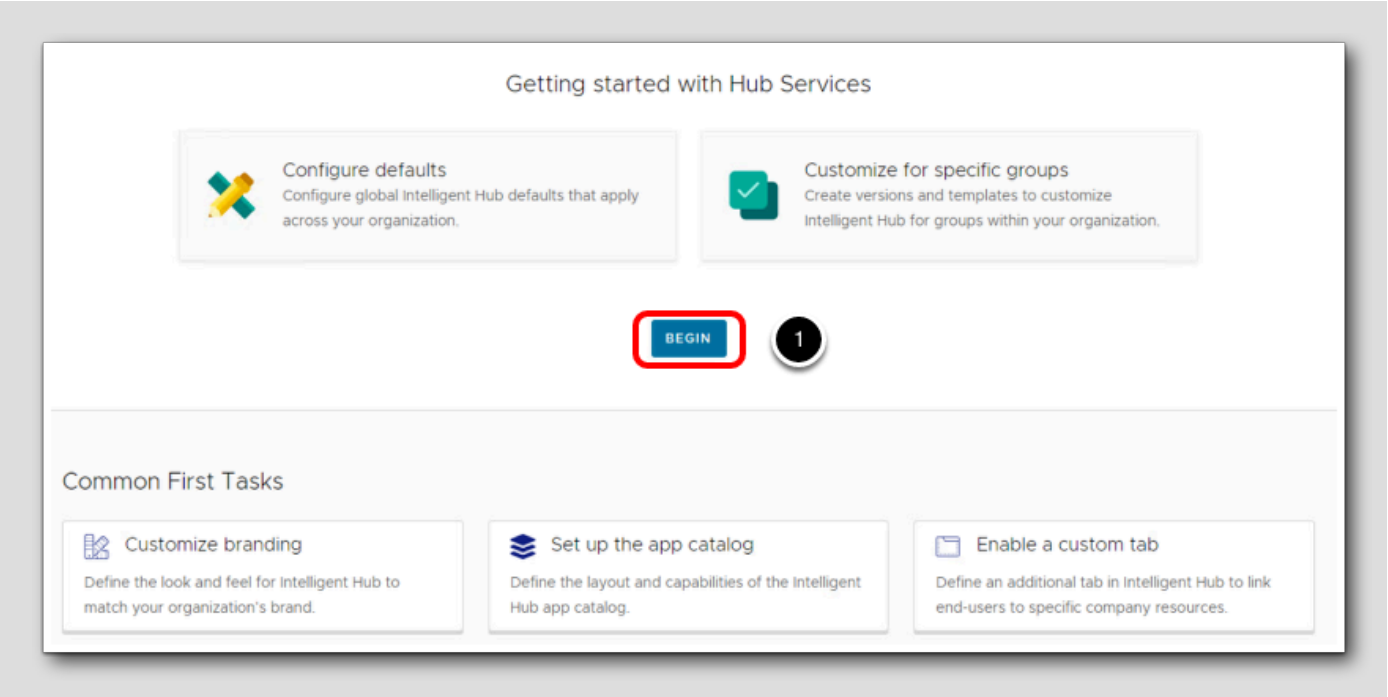
Configuring Hub Services

[31]

You will now enable the App Catalog for Windows so that the unified app catalog is displayed in the Windows 10 Intelligent Hub app.

1. Getting started with Hub Services

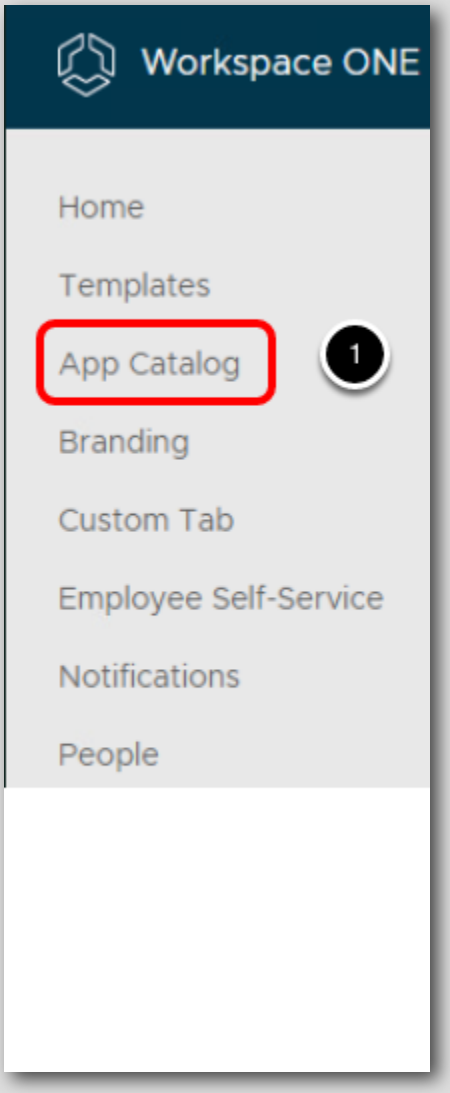
[32]



1. Click **Begin**

Configure App Catalog Settings

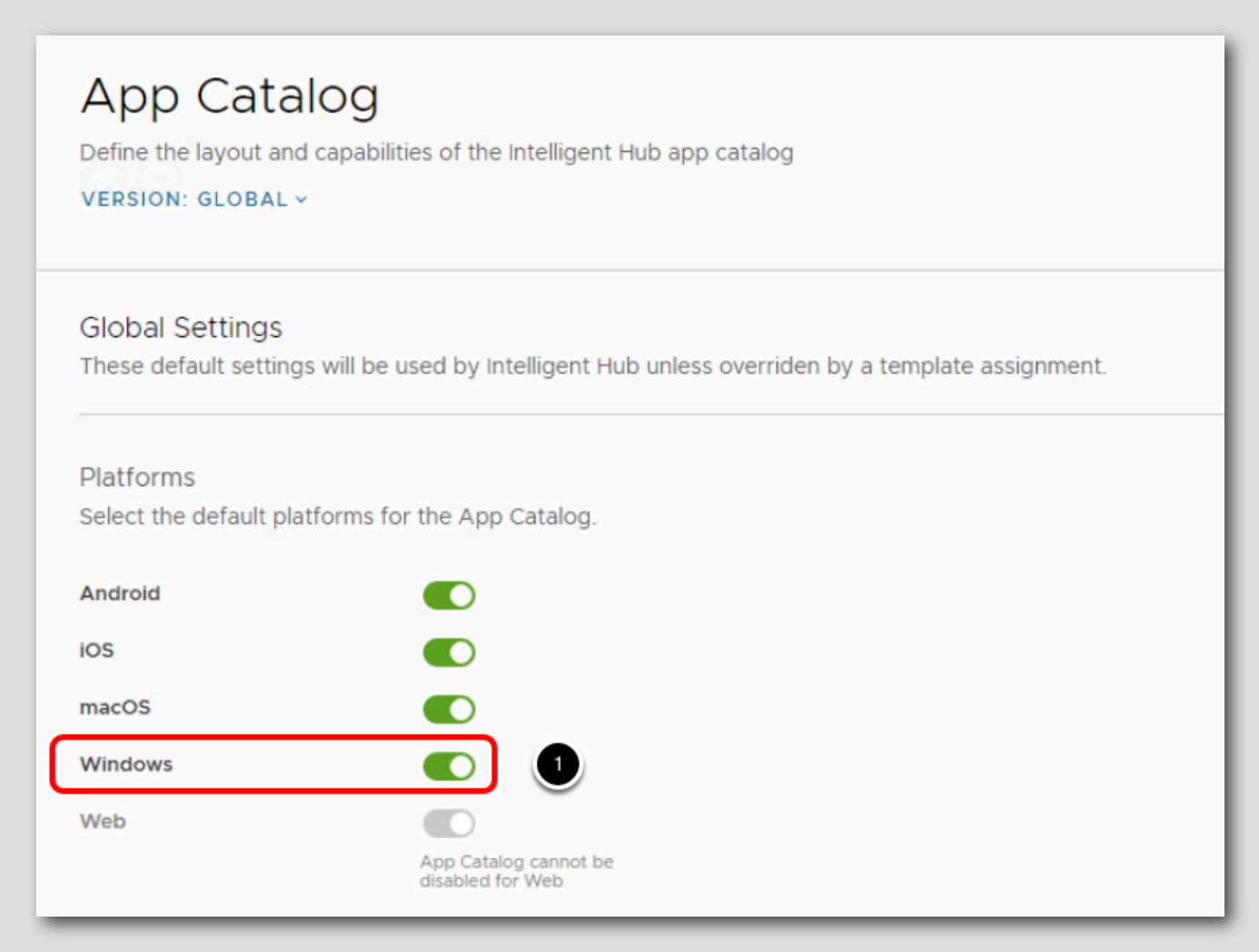
[33]



1. Click **App Catalog** on the left side of the screen.

Enable the Windows App Catalog

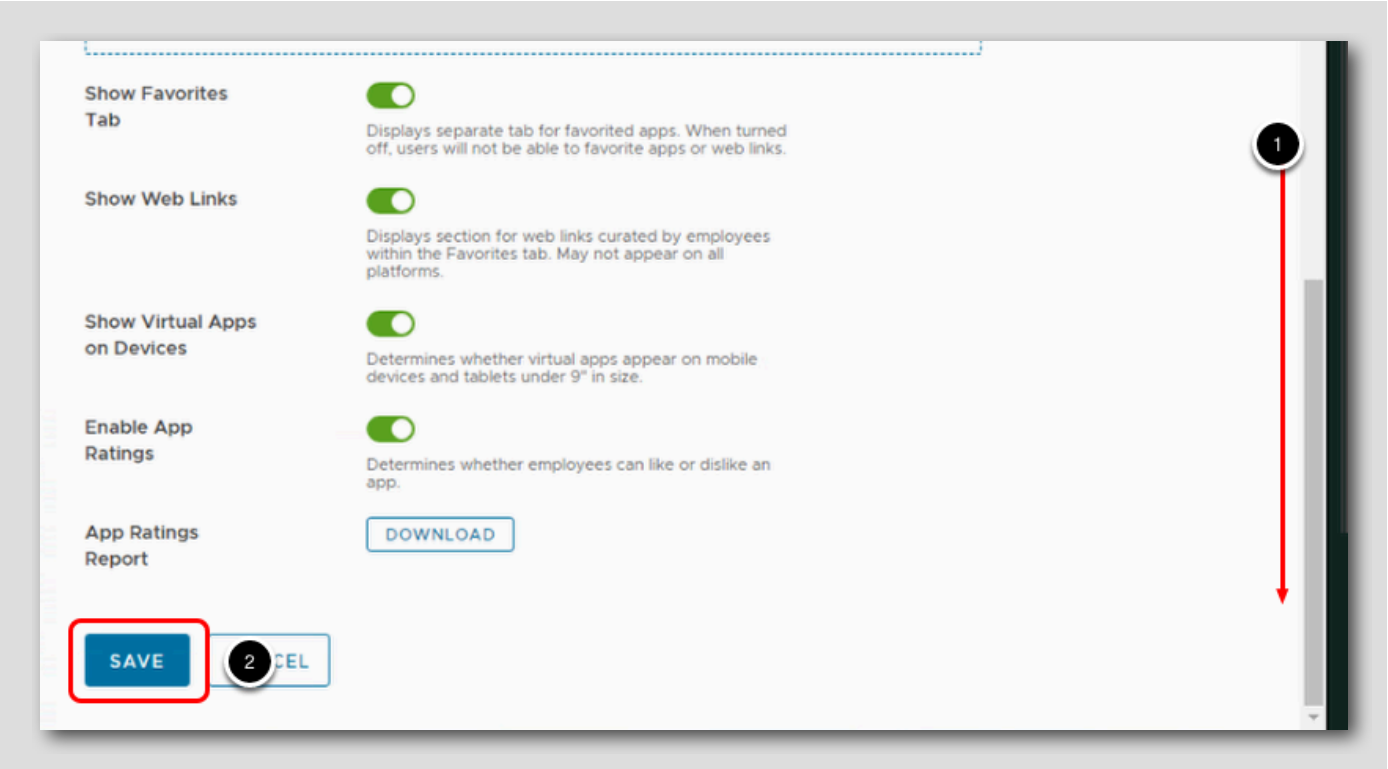
[34]



1. Select **Enabled** for Intelligent Hub App Catalog for Windows (if not already enabled).

Save the Intelligent Hub Publishing Settings

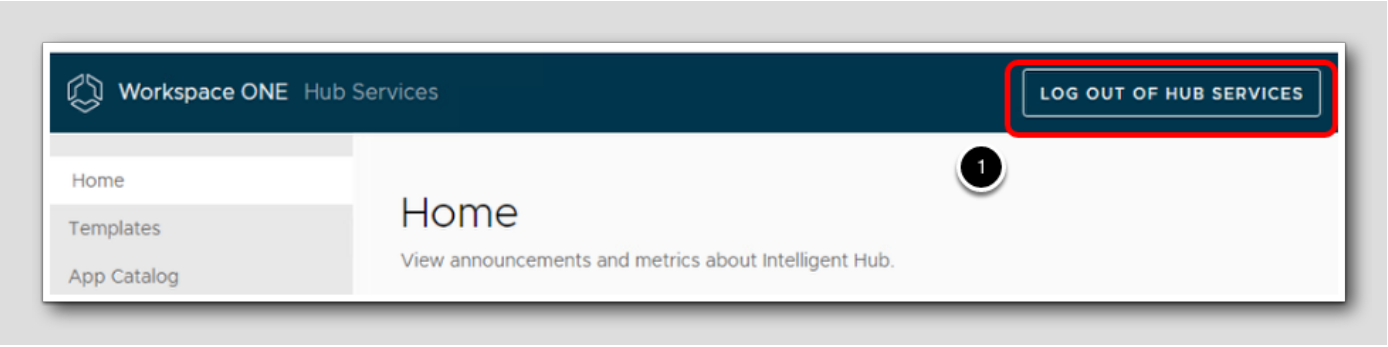
[35]



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

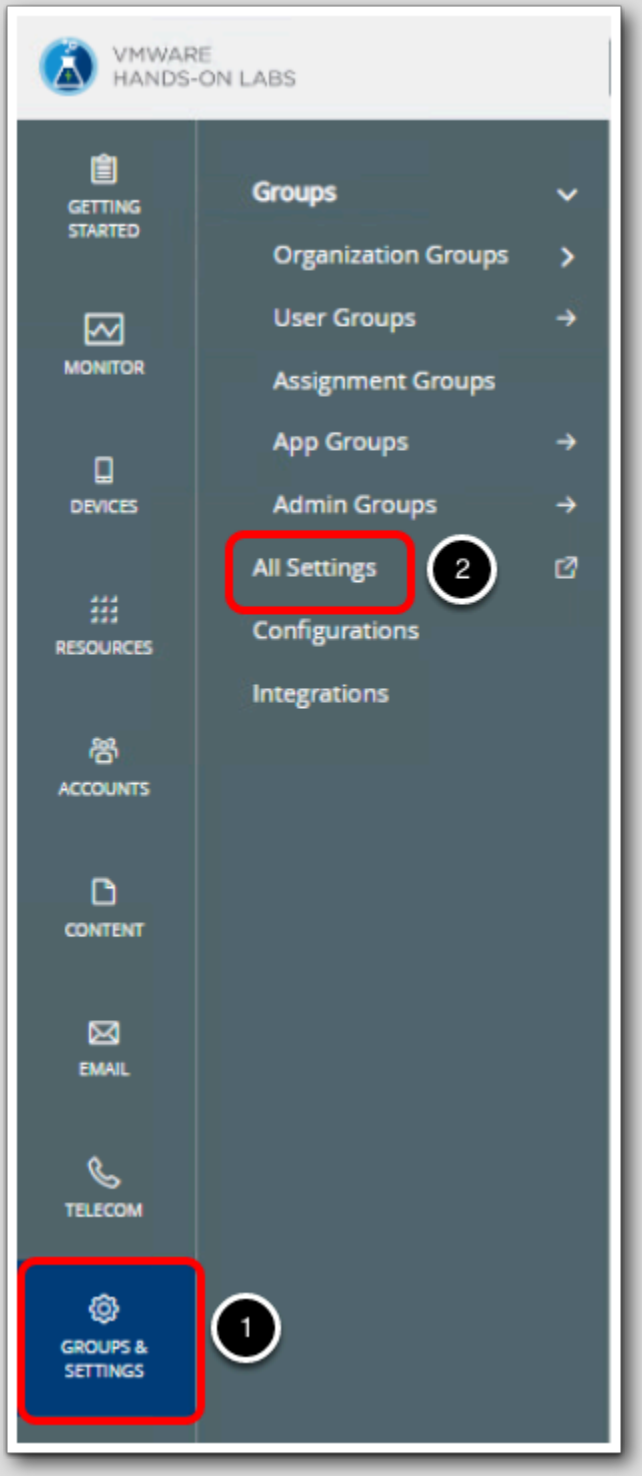
Log Out of Hub Services

[36]

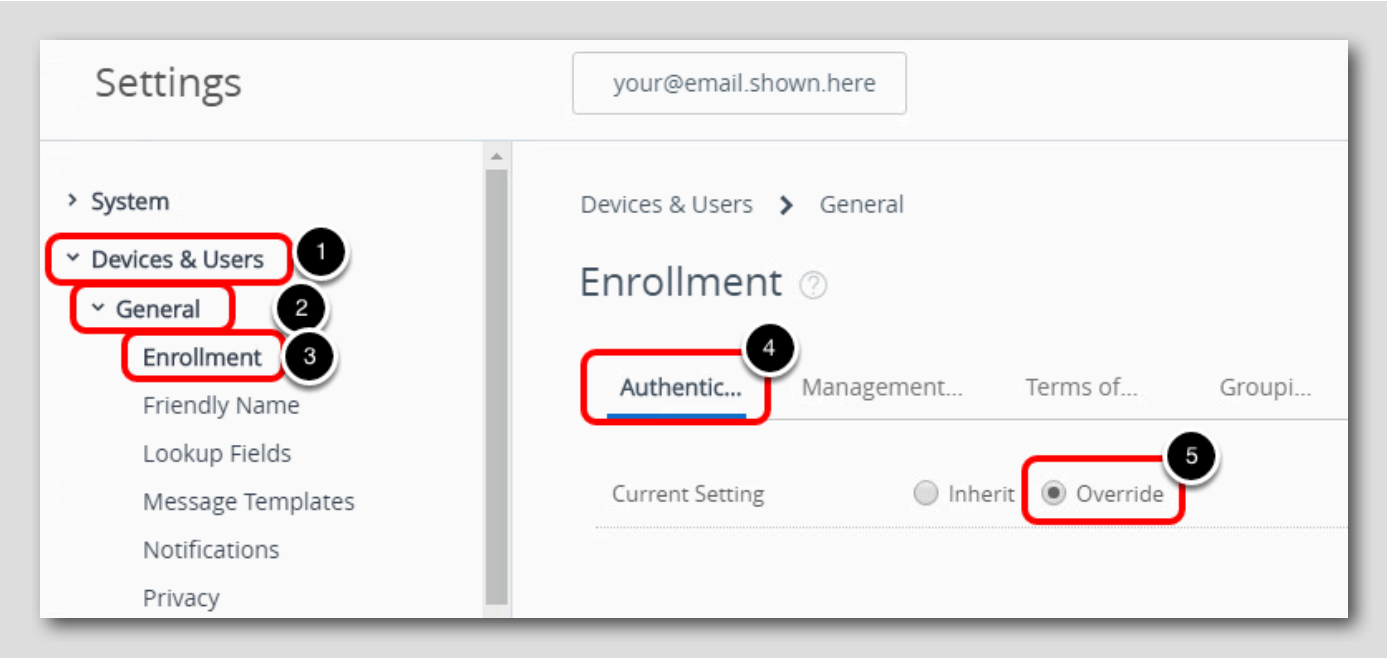


1. Select **Log Out of Hub Services**.

Configure the Source of Authentication for Intelligent Hub


VMWARE
HANDS-ON LABS
GETTING STARTED
MONITOR
DEVICES
RESOURCES
ACCOUNTS
CONTENT
EMAIL
TELECOM
GROUPS & SETTINGS
1
Groups
Organization Groups
User Groups
Assignment Groups
App Groups
Admin Groups
All Settings
2
Configurations
Integrations

1. From the menu on the left **Select** Groups & Settings
2. **Select** All Settings

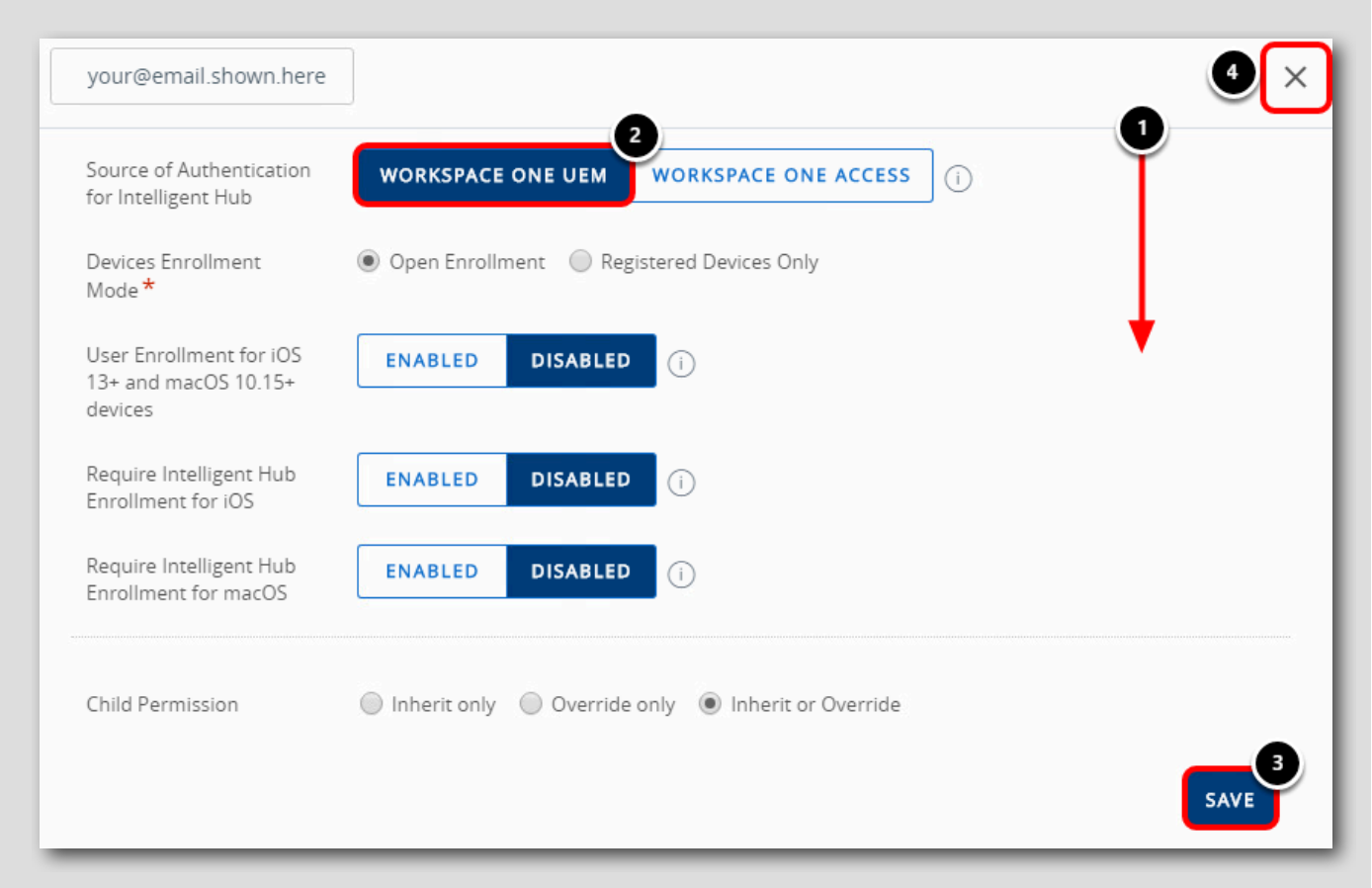


From within the Settings menu,

1. Expand **Devices & Users** in the left column
2. Expand **General**
3. Click **Enrollment**
4. Click the **Authentication** tab
5. Select **Override** for the Current Setting

Update the Source of Authentication

[38]



1. Scroll down to the bottom of the page
2. Select **Workspace ONE UEM** for the Source of Authentication for Intelligent Hub (if not already enabled)
3. Click **Save**
4. Click **Close**

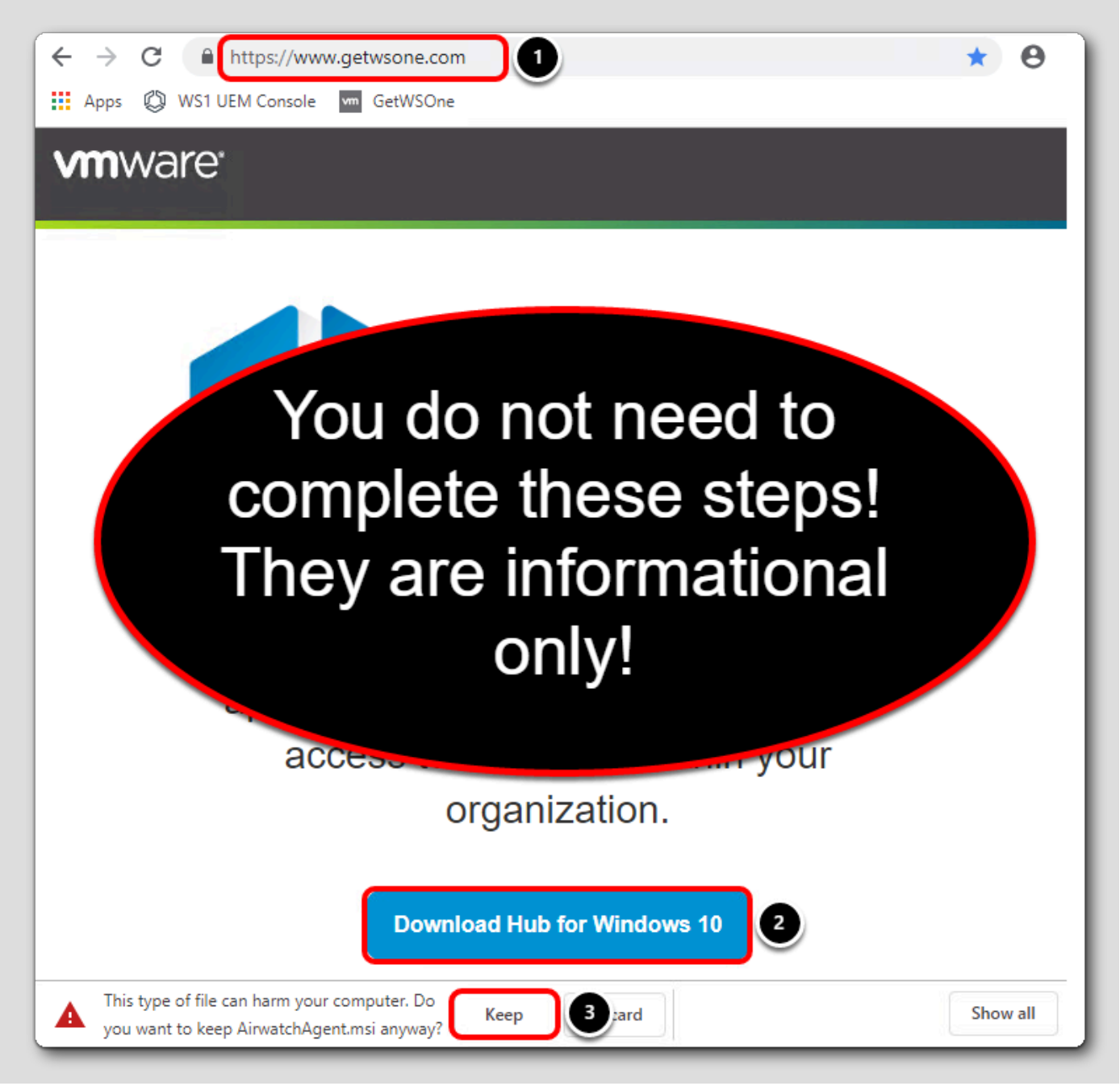
Enrolling Your Windows 10 Device with the Created Basic Account

[39]

You will now enroll the Windows 10 device in Workspace ONE UEM by using the Workspace ONE Intelligent Hub app.

Downloading the Workspace ONE Intelligent Hub app

[40]



NOTE: You do NOT need to complete these steps, the Workspace ONE Intelligent Hub has already been downloaded for you! This step is purely informative.

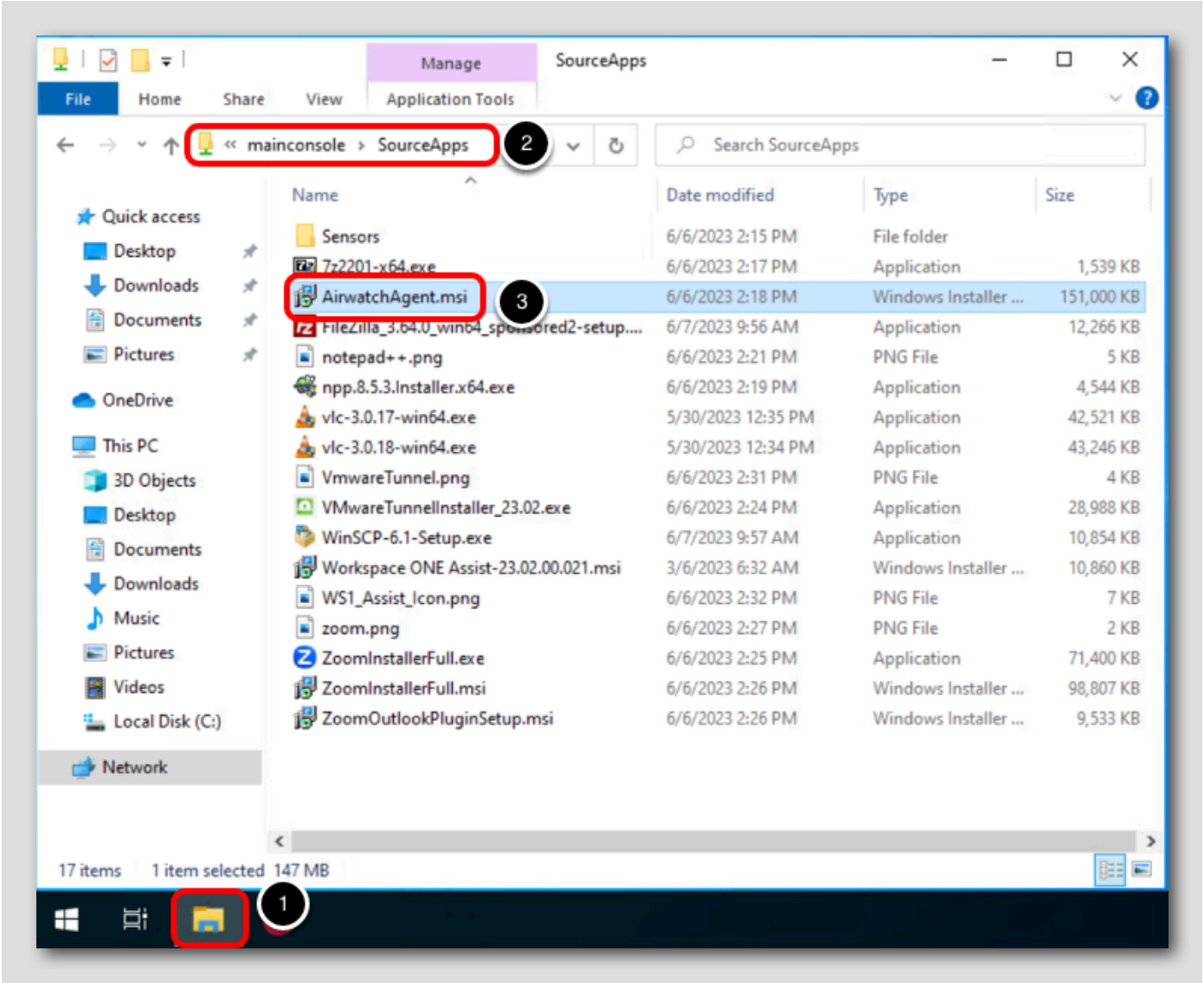
You can download the latest Workspace ONE Intelligent Hub app for your current platform by following the below steps:

1. Navigate to **`https://www.getwsone.com`** in your browser.
2. Click **Download Hub for Windows 10**.
3. Click **Keep** when warned about the AirWatchAgent.msi download.

For expediency, the Workspace ONE Intelligent Hub app has already been downloaded for you. Continue to the next step to start the installer.

Launch the Workspace ONE Intelligent Hub Installer

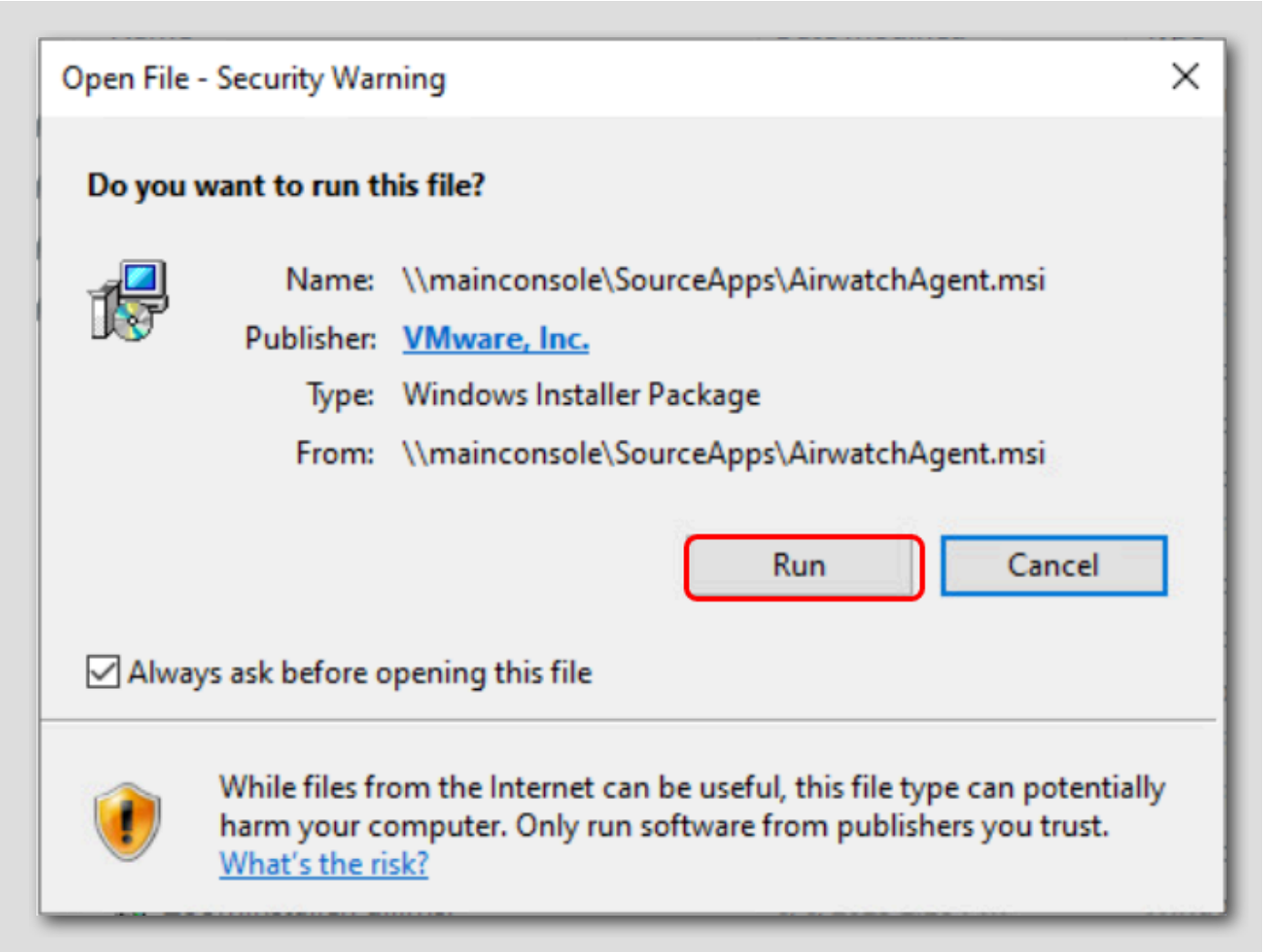
[41]



1. Click the **File Explorer** icon from the taskbar.
2. Enter `\\MainConsole\SourceApps` in the address bar and press **Return**.
3. Double-click the **AirwatchAgent.msi** file to start the installer.

NOTE: The installer may take a few seconds to launch, please be patient after clicking the AirwatchAgent.msi file.

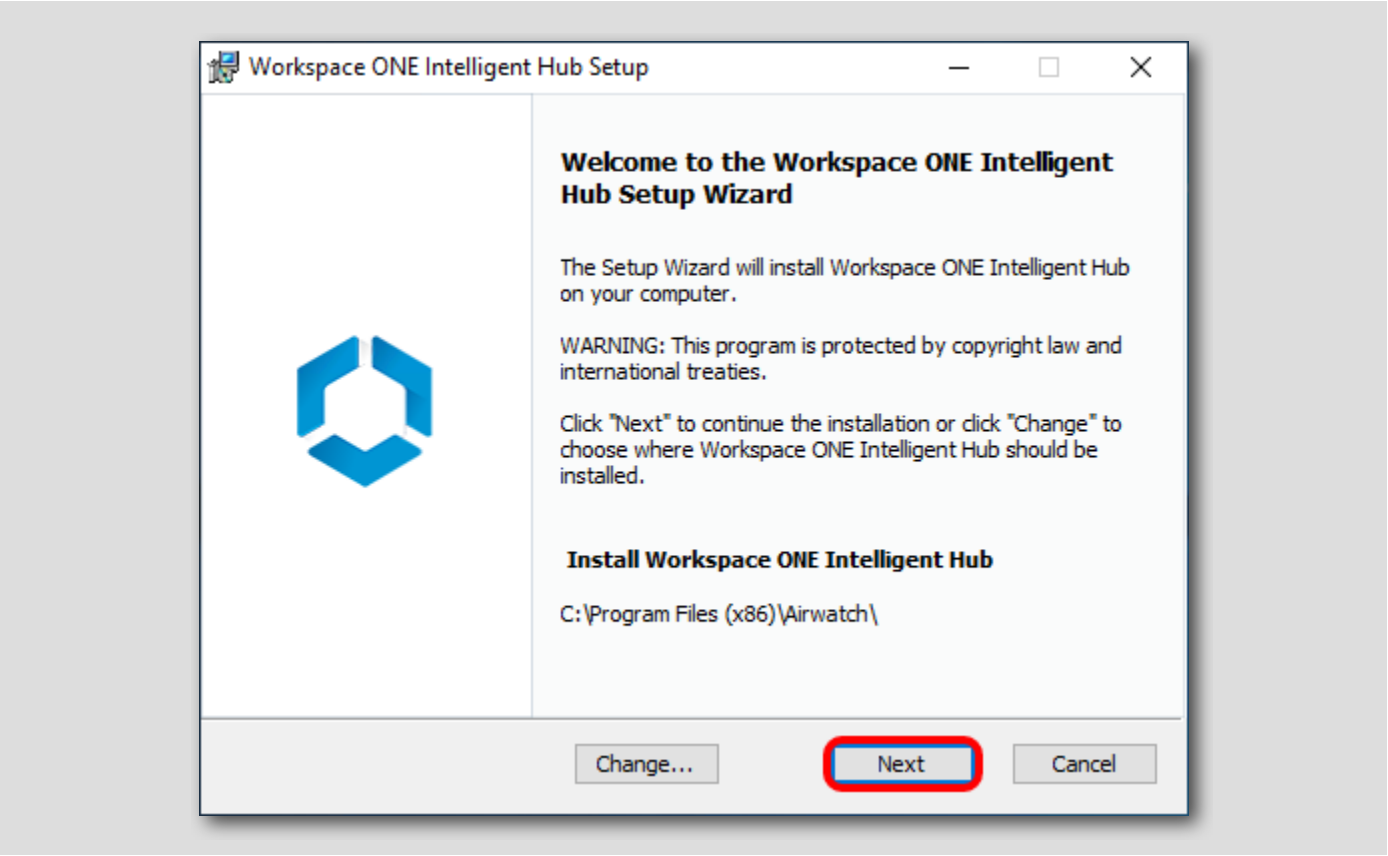
Click Run [42]



Click **Run** to proceed with the installation.

Accept the Default Install Location

[43]

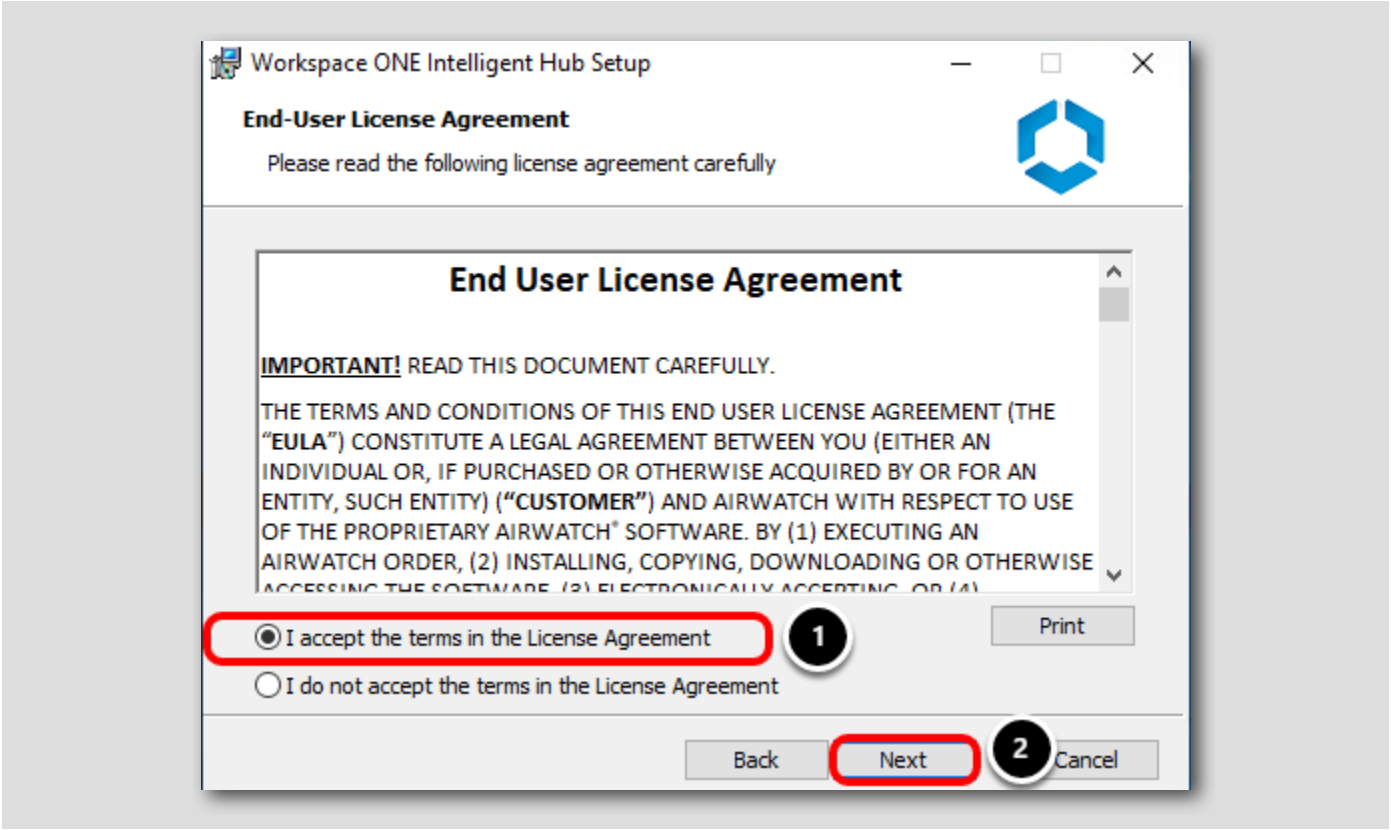


Leave the default install location and click **Next**.

NOTE: The Next button may take several seconds to enable while the required additional features are installed.

Accept the License Agreement

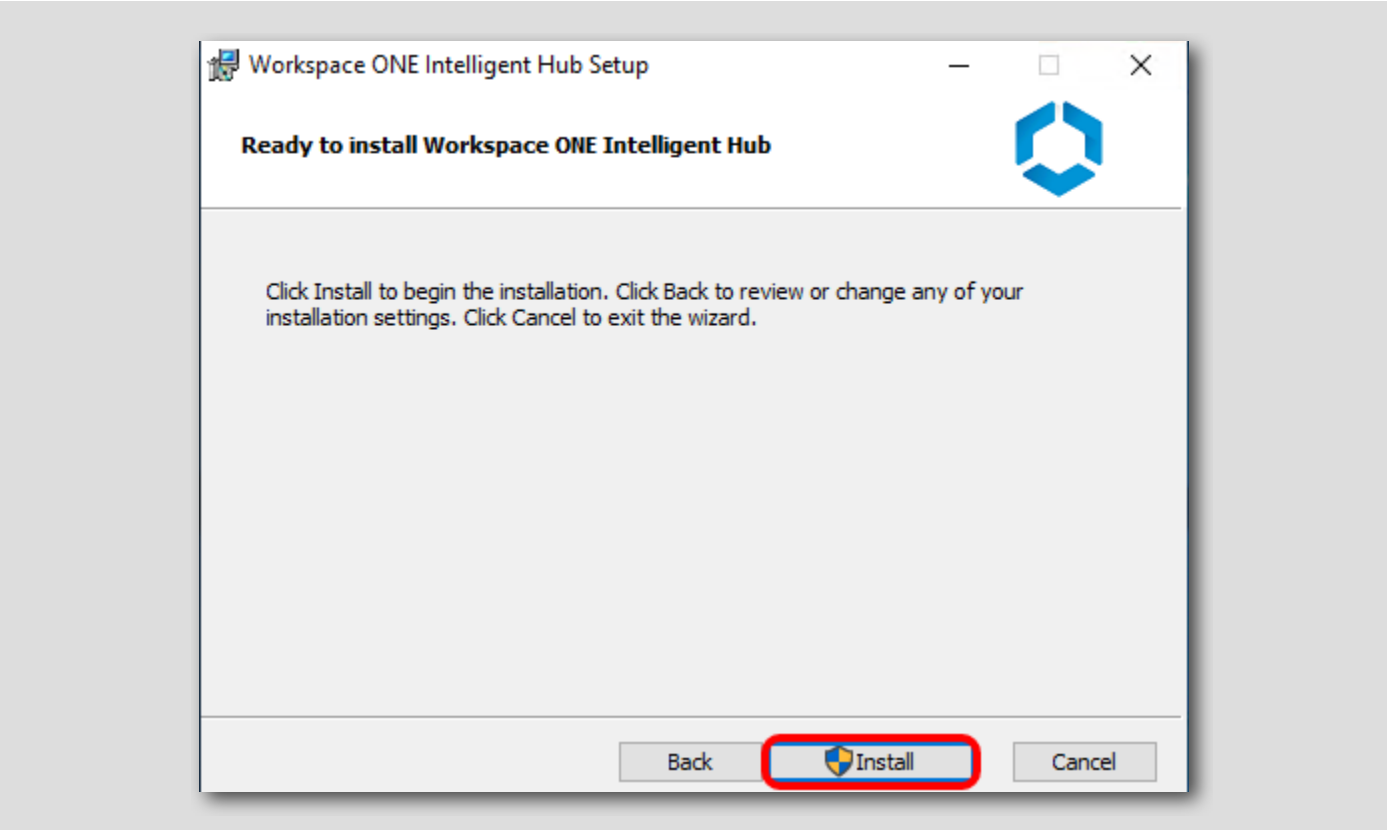
[44]



1. Select I accept the terms of the License Agreement.
2. Click **Next**.

Start the Workspace ONE Intelligent Hub Install

[45]

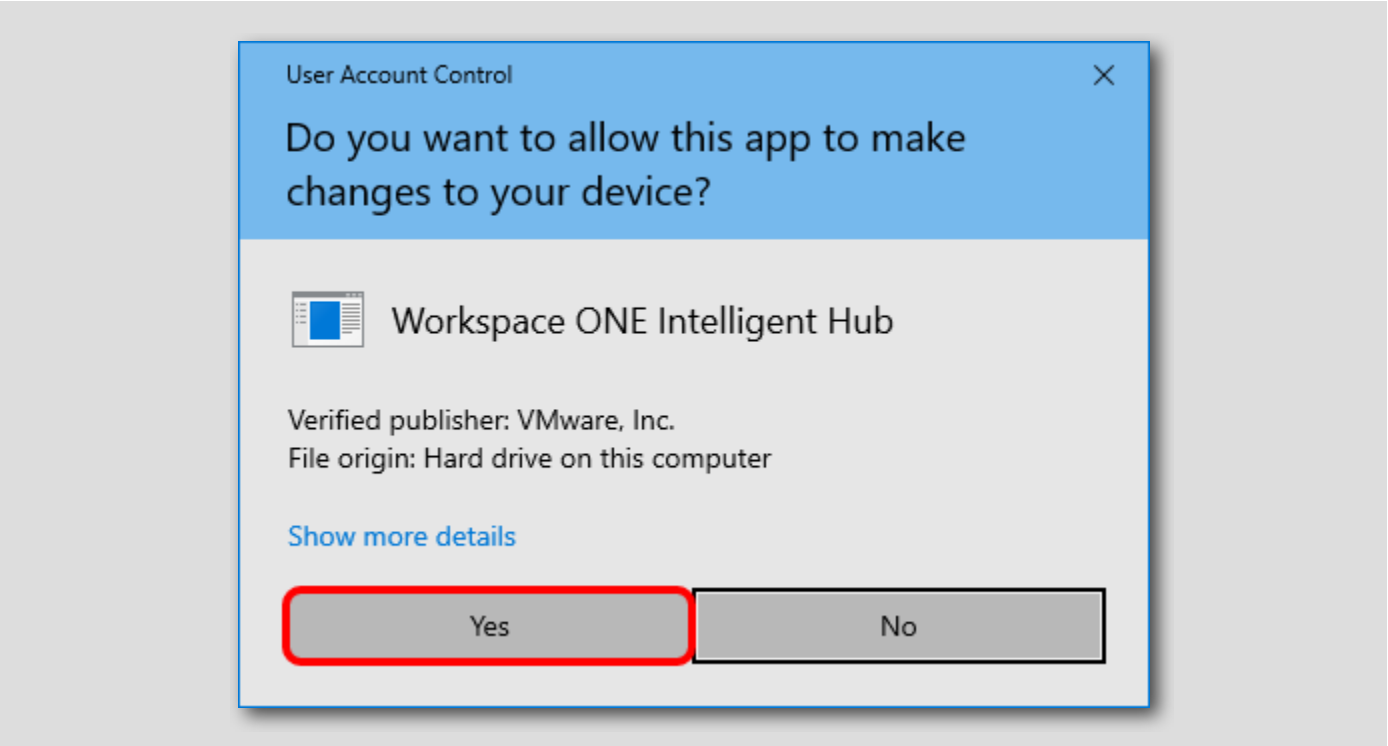


Click **Install** to start the installer.

NOTE - The Installing Hub UI Component step may take several minutes to complete. Please do not interrupt the install!

Allow the Workspace ONE Intelligent Hub Installer to Run (IF NEEDED)

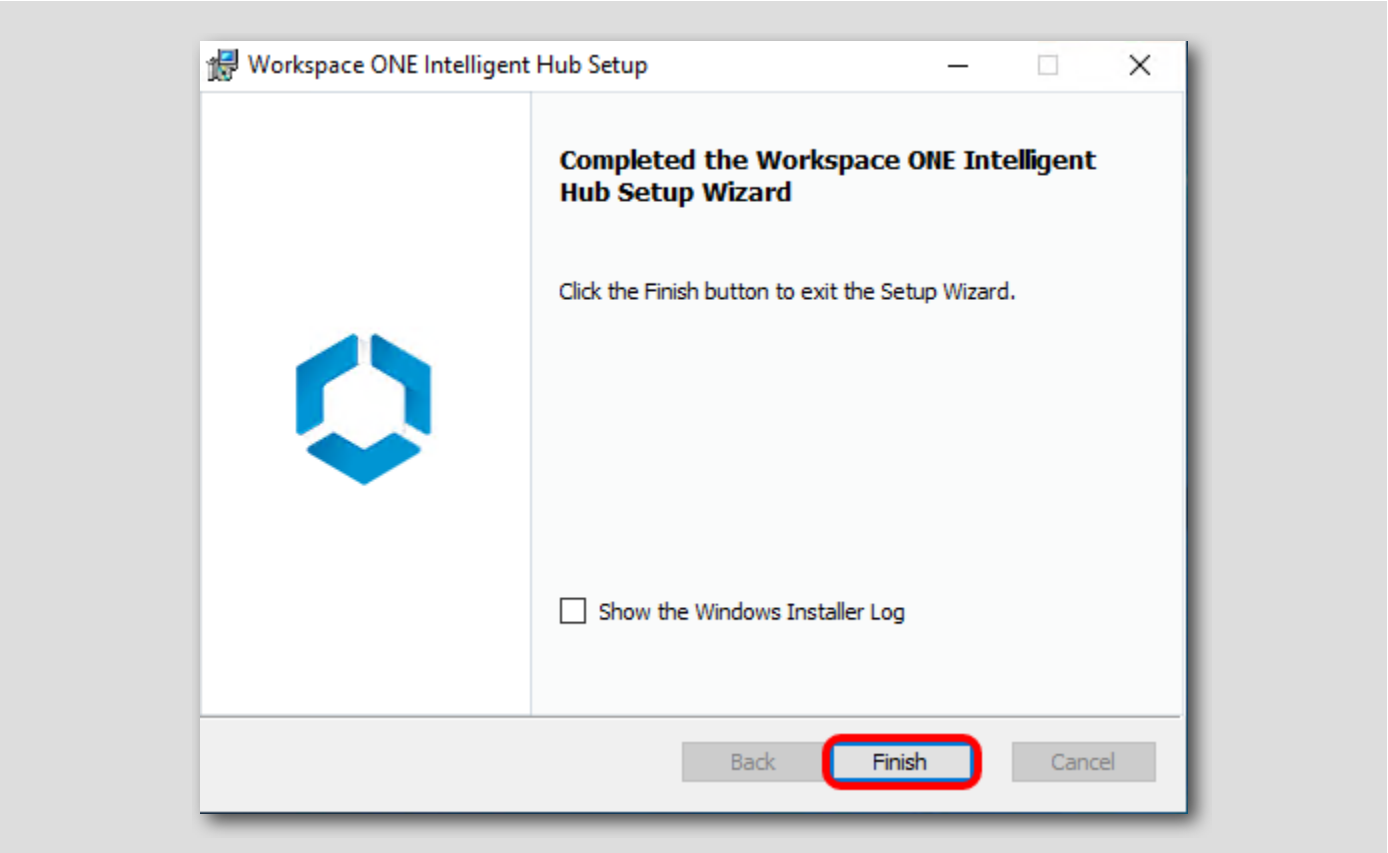
[46]



If prompted to allow the app to make changes on your device, click **Yes**. Otherwise, continue to the next step.

Complete the Workspace ONE Intelligent Hub Installer

[47]



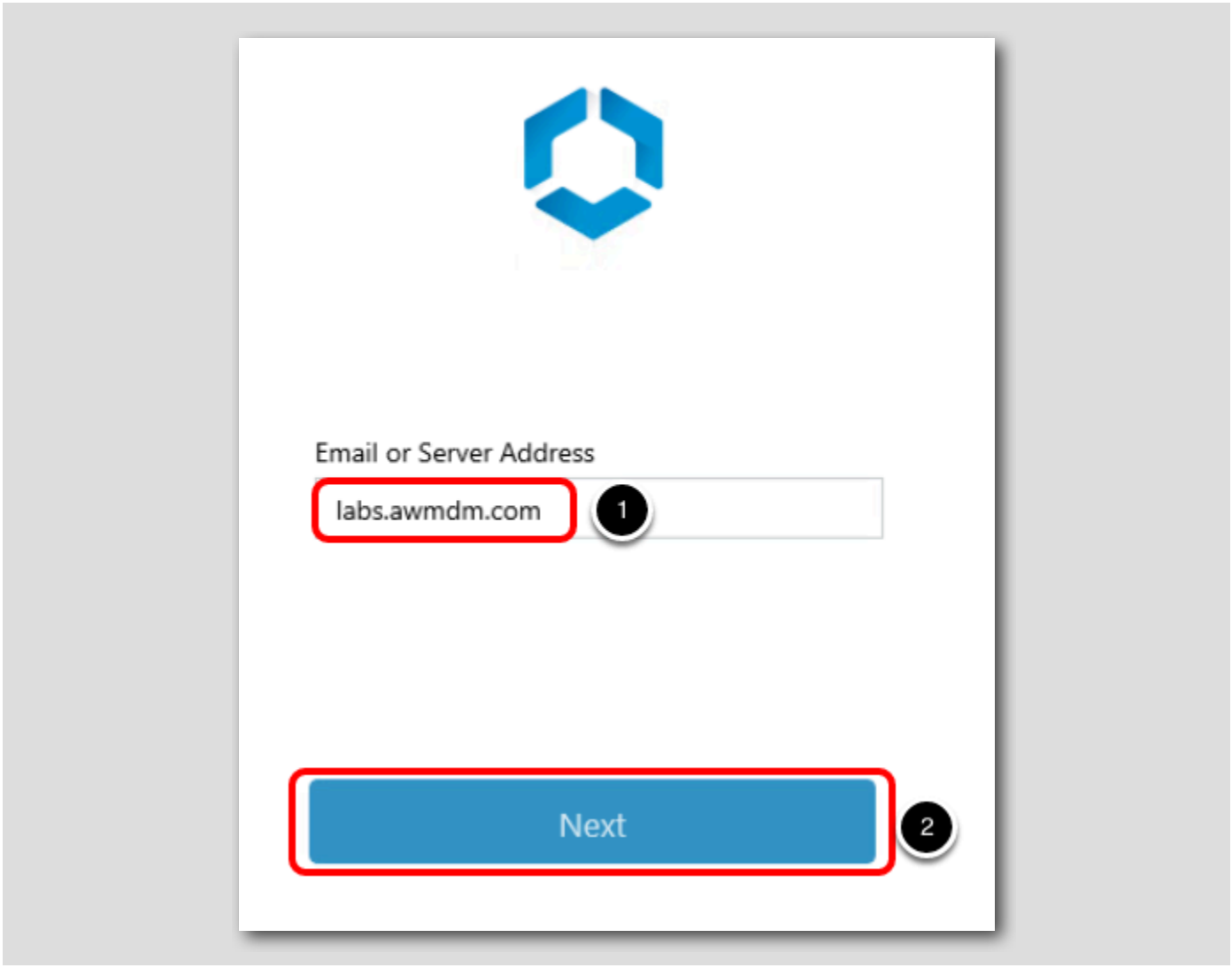
NOTE: The installer may take several minutes to complete. Please wait until you see the completed install screen before continuing.

Click **Finish** to complete the Workspace ONE Intelligent Hub installer.

NOTE: After clicking finish, the Native Enrollment application will launch to guide you through enrolling into Workspace ONE UEM. It will take around 45-60 seconds to launch the agent.

Enroll Your Windows 10 Device Using the Workspace ONE Intelligent Hub

[48]

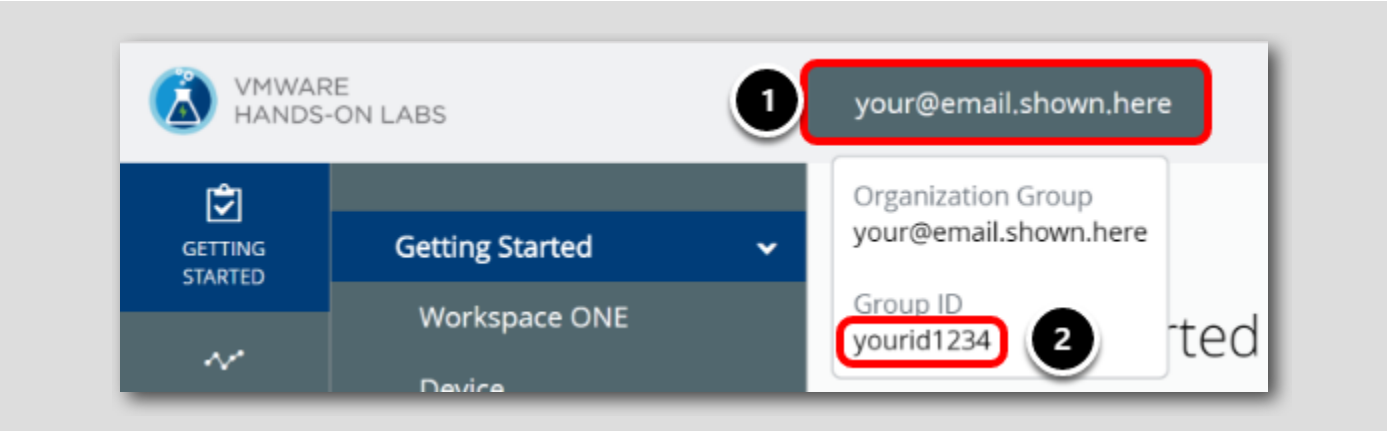


NOTE: The above screen may take 2-3 minutes to display after clicking Finish from the previous step!

1. Enter **`labs.awmdm.com`** for the Server Address.
2. Click **Next**.

Find your Group ID from Workspace ONE UEM Console

[49]

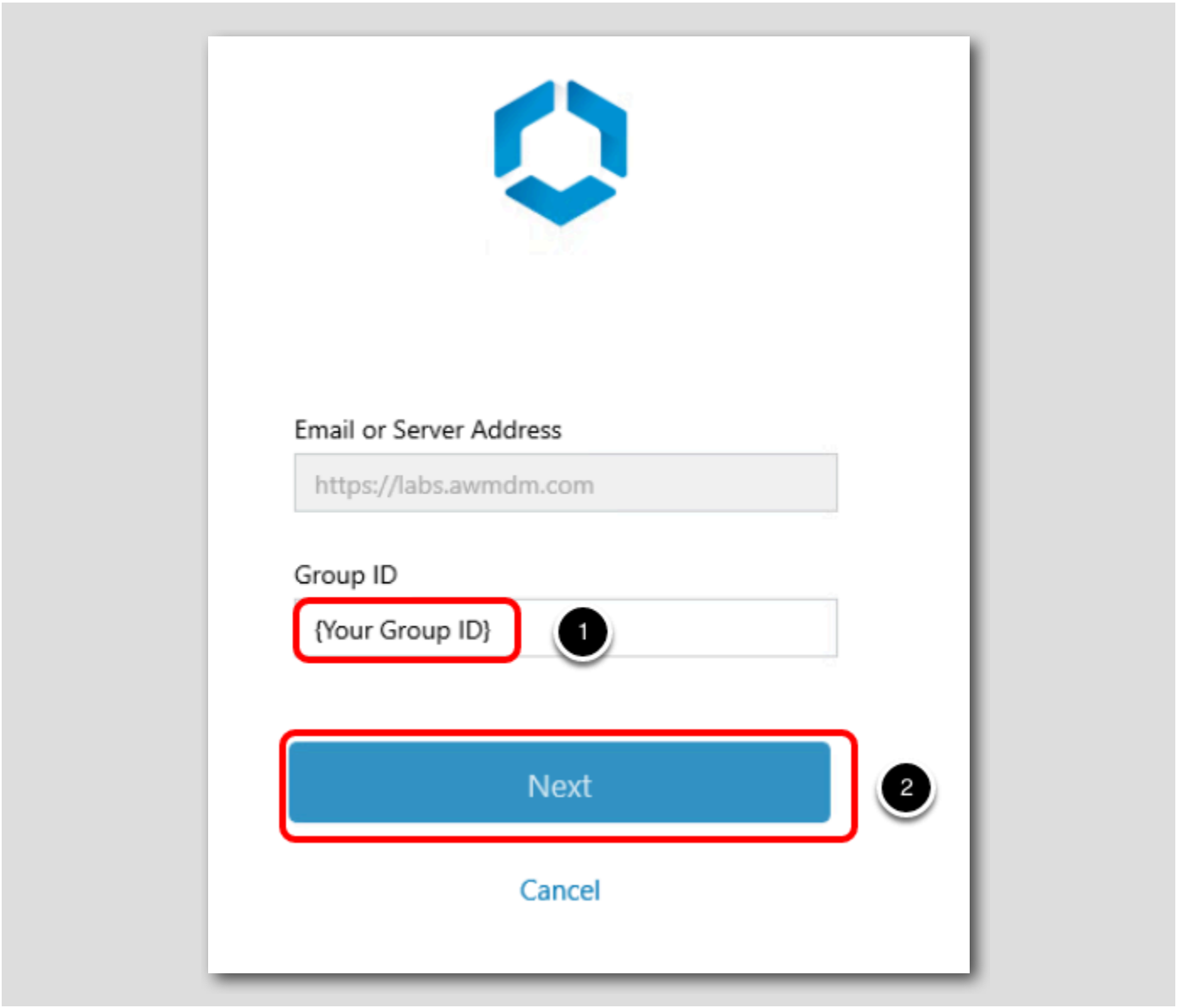


The next step is to make sure you know what your **Organization Group ID** is.

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

Enter Your Group ID

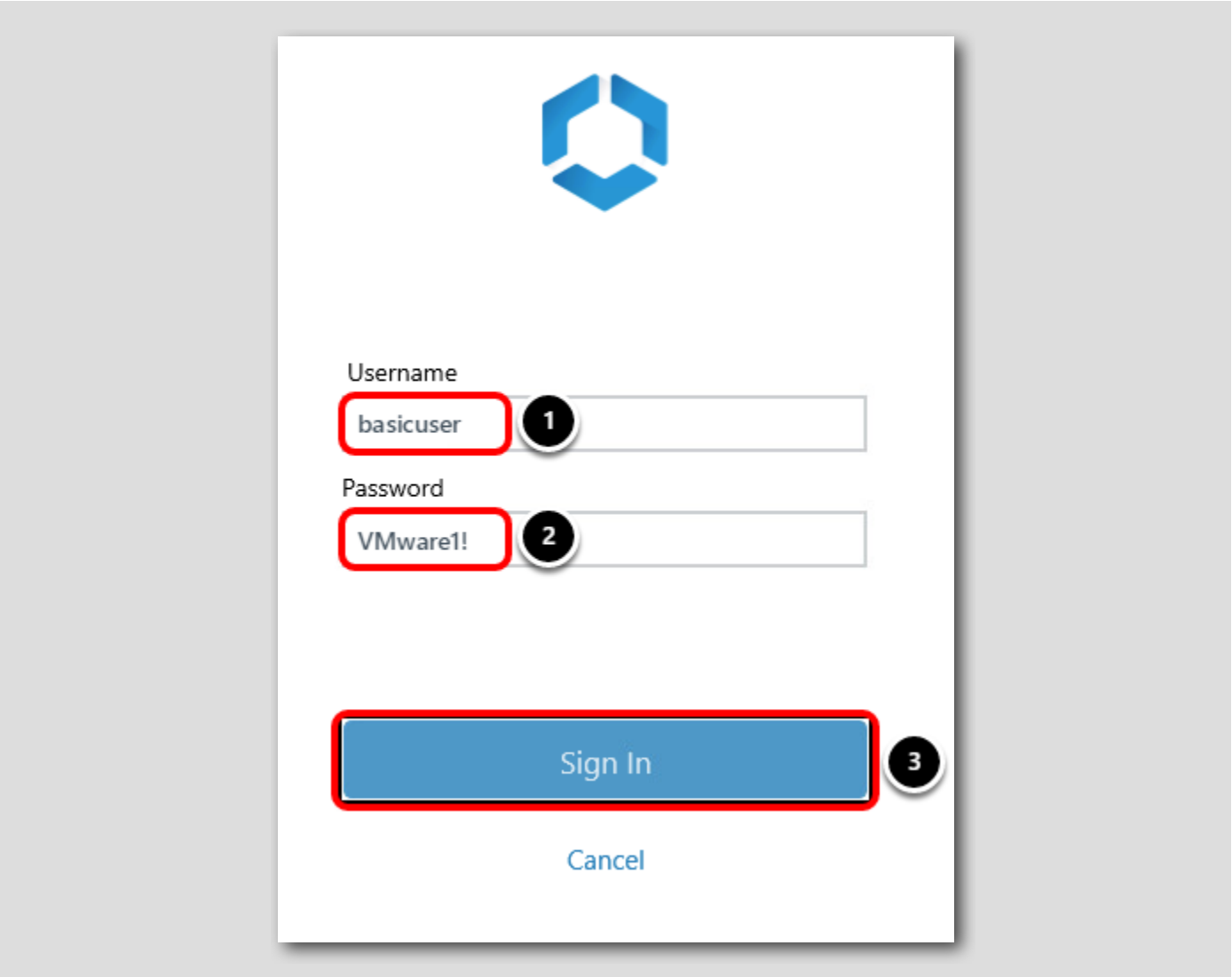
[50]



1. Enter **Your Group ID** for the **Group ID** field. If you forgot your Group ID, check the previous steps on how to retrieve it.
2. Click **Next**.

Enter Your User Credentials

[51]



1. Enter **basicuser** in the Username field.

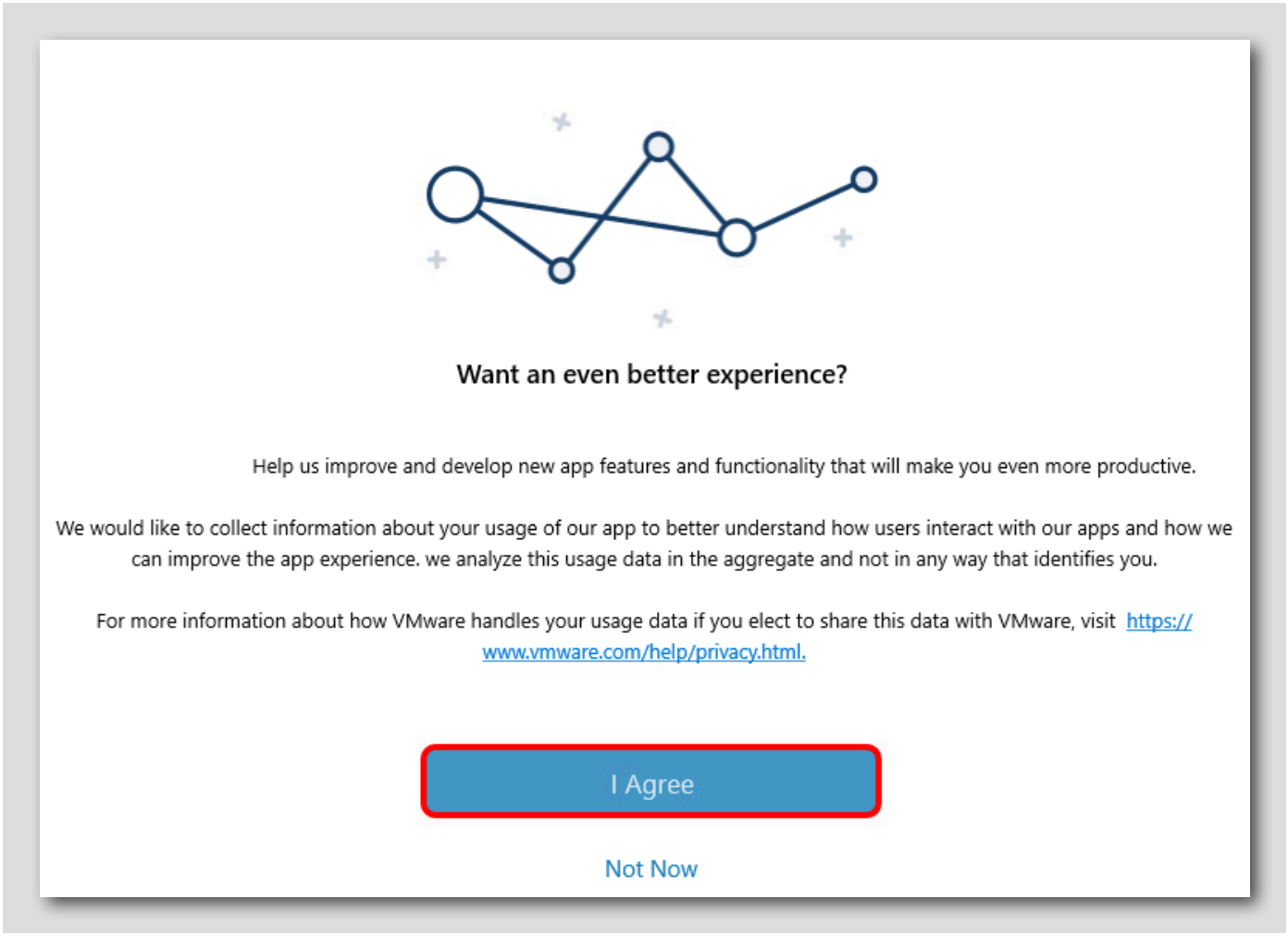
   NOTE: This was the username of the basic user account you created in previous steps in the Workspace ONE UEM Console

2. Enter **VMware1!** in the Password field.
3. Click Sign In.

NOTE: Wait while the server checks your enrollment details. This may take a few minutes.

Accept Data Policy

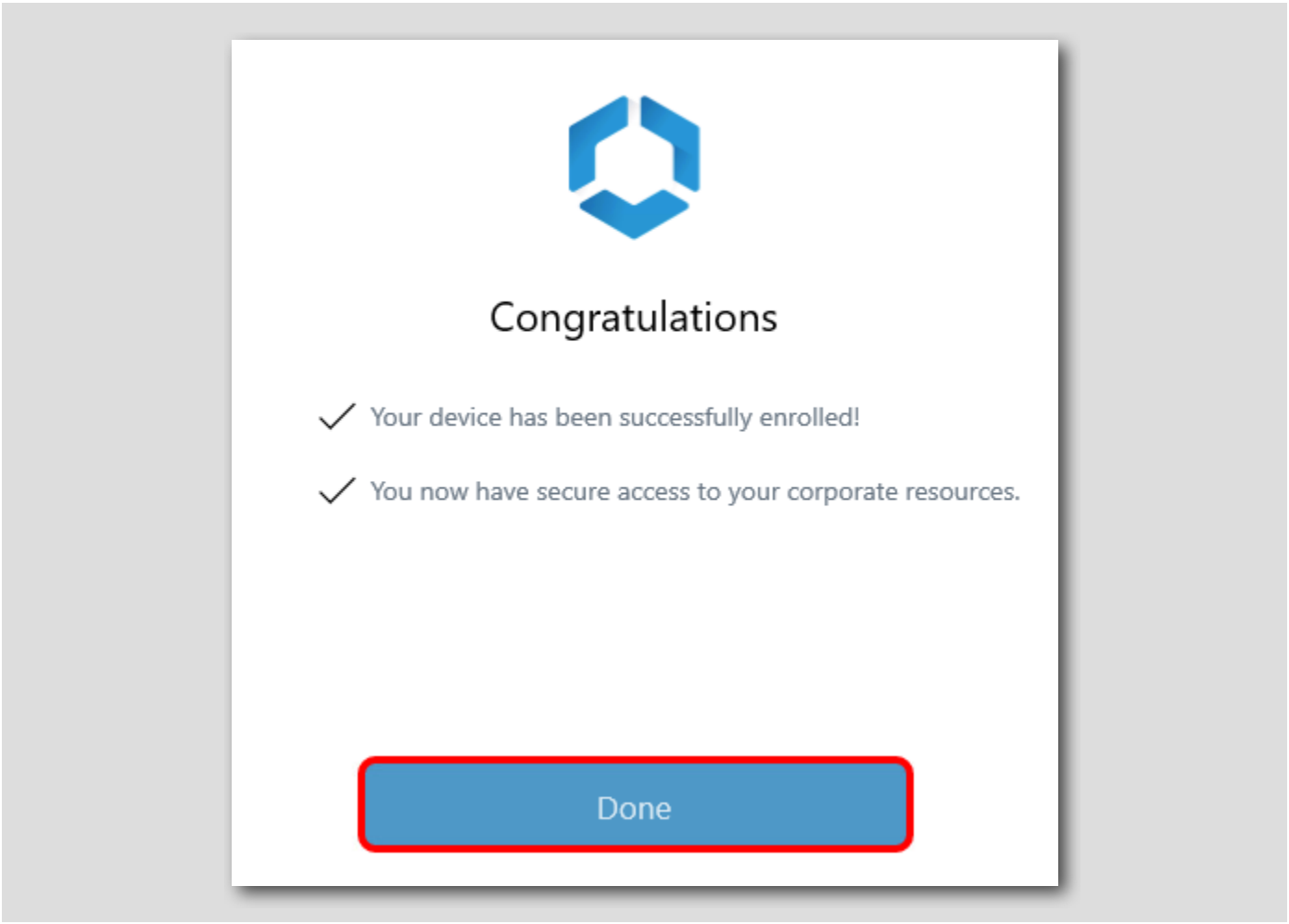
[52]



Click **I Agree**.

Finish the Workspace ONE UEM Enrollment Process

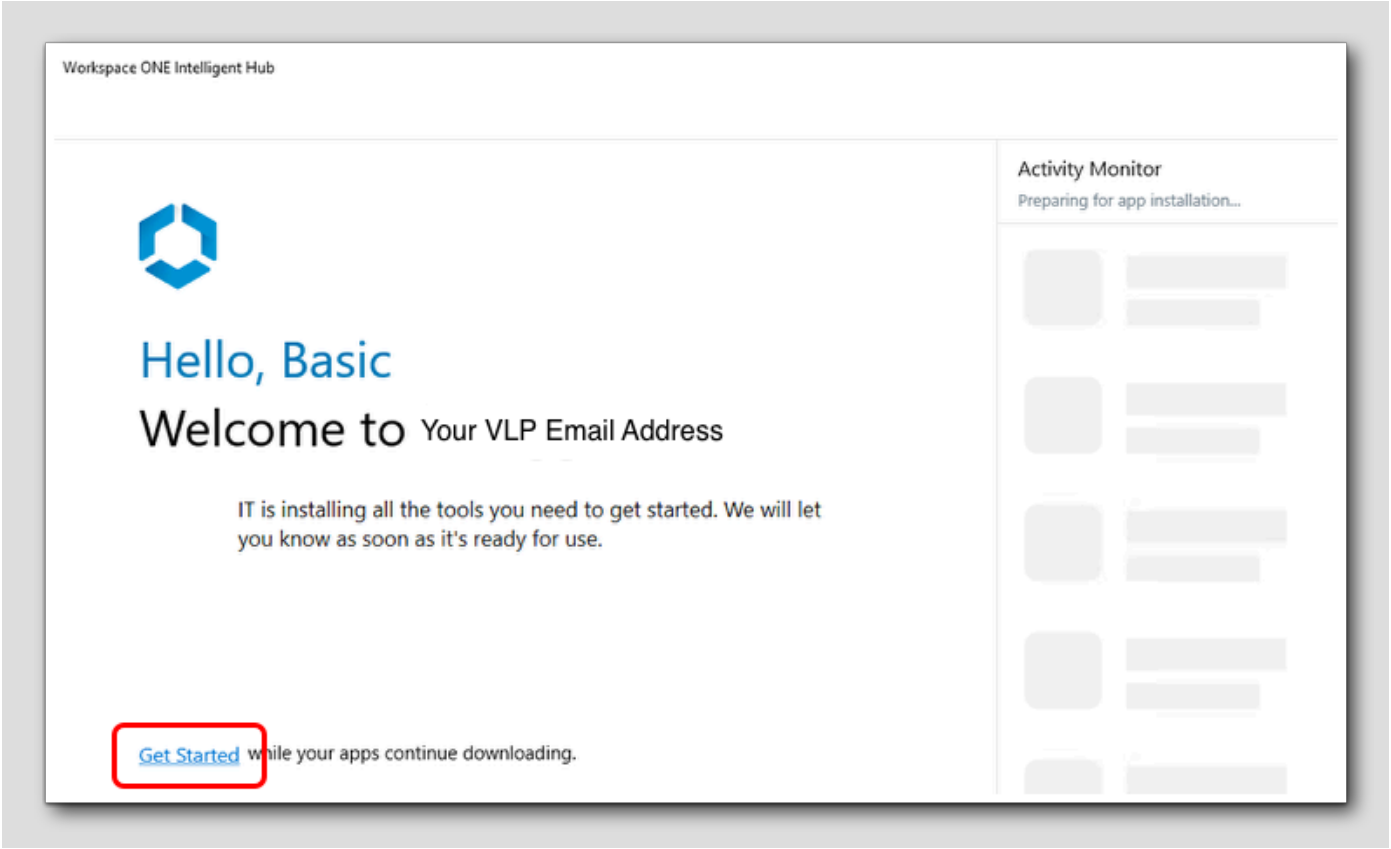
[53]



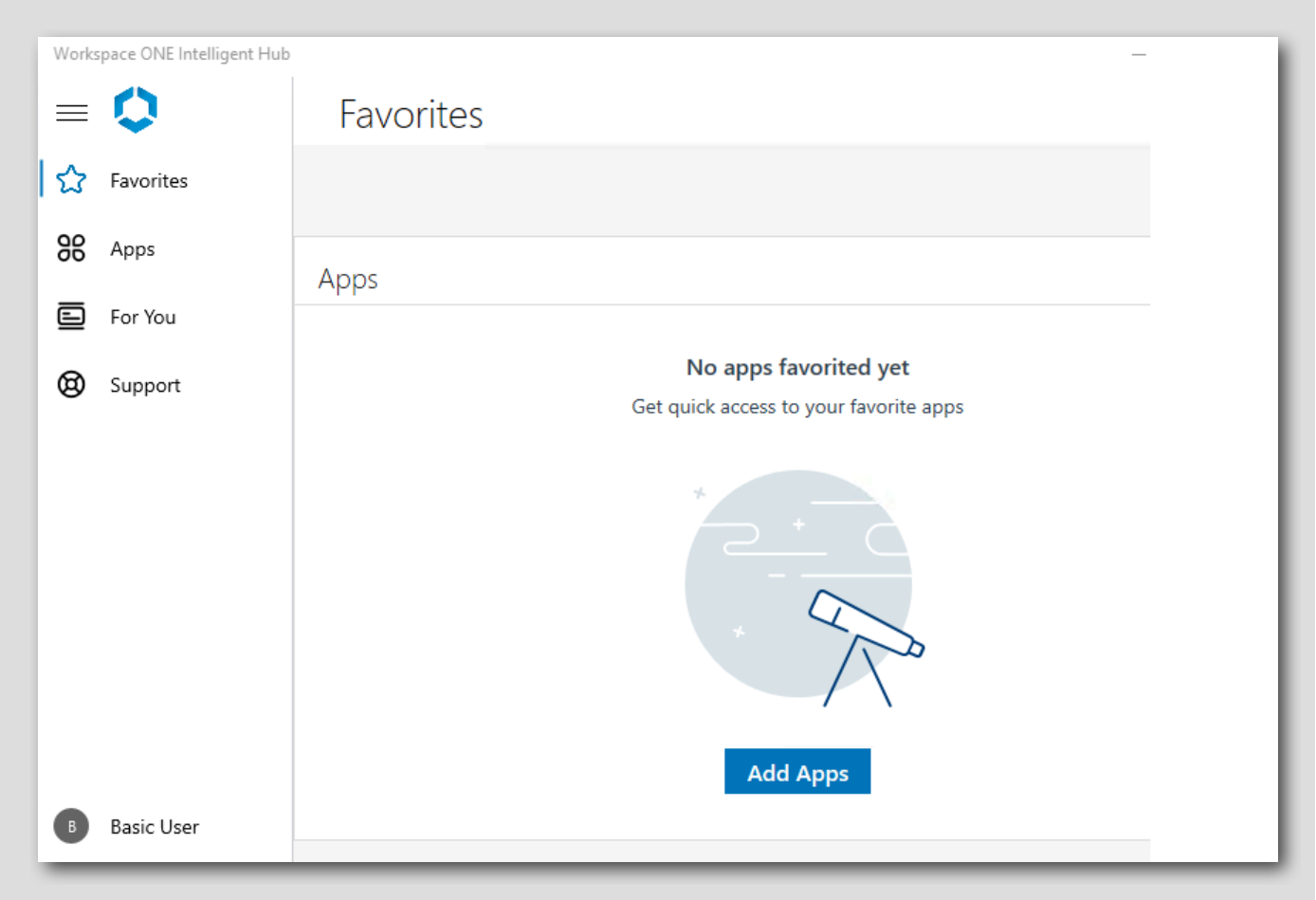
Click **Done** to end the Enrollment process. Your Windows 10 device is now successfully enrolled into Workspace ONE UEM!

View the Intelligent Hub App

[54]



Click **Get Started** to launch the Intelligent Hub



Once the enrollment is completed, the Workspace ONE Intelligent Hub app will be displayed. The Favorites and Apps tabs will be empty because we have not yet deployed any apps to your users and devices.

In the next steps, you will deploy two applications: Workspace ONE Assist and 7-Zip. Workspace ONE Assist will be deployed and installed automatically to the end user's device, while 7-Zip will be an "on demand" app, meaning users can initiate the app download and install from the app catalog if and when they need access to 7-Zip.

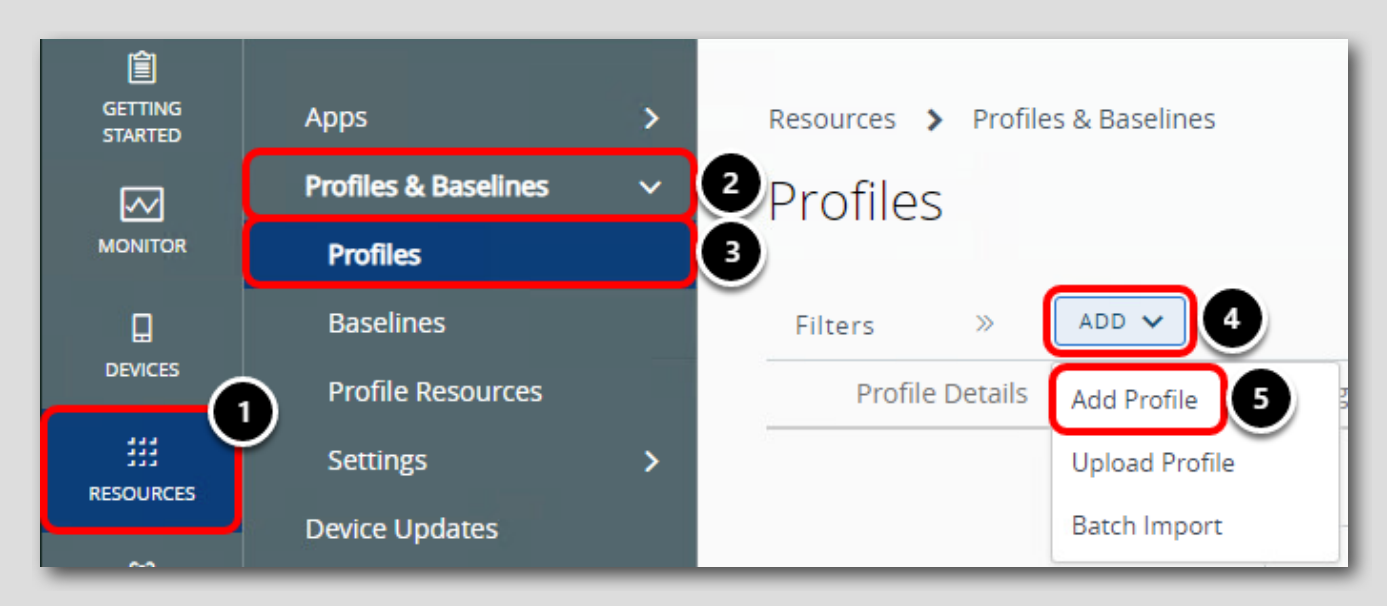
Configuring a Device Profile for Windows 10

[55]

Profiles allow you to modify how the enrolled devices behave. This exercise helps you to configure and deploy a restrictions profile that we can verify has applied to the device later in the section.

Add a Profile

[56]

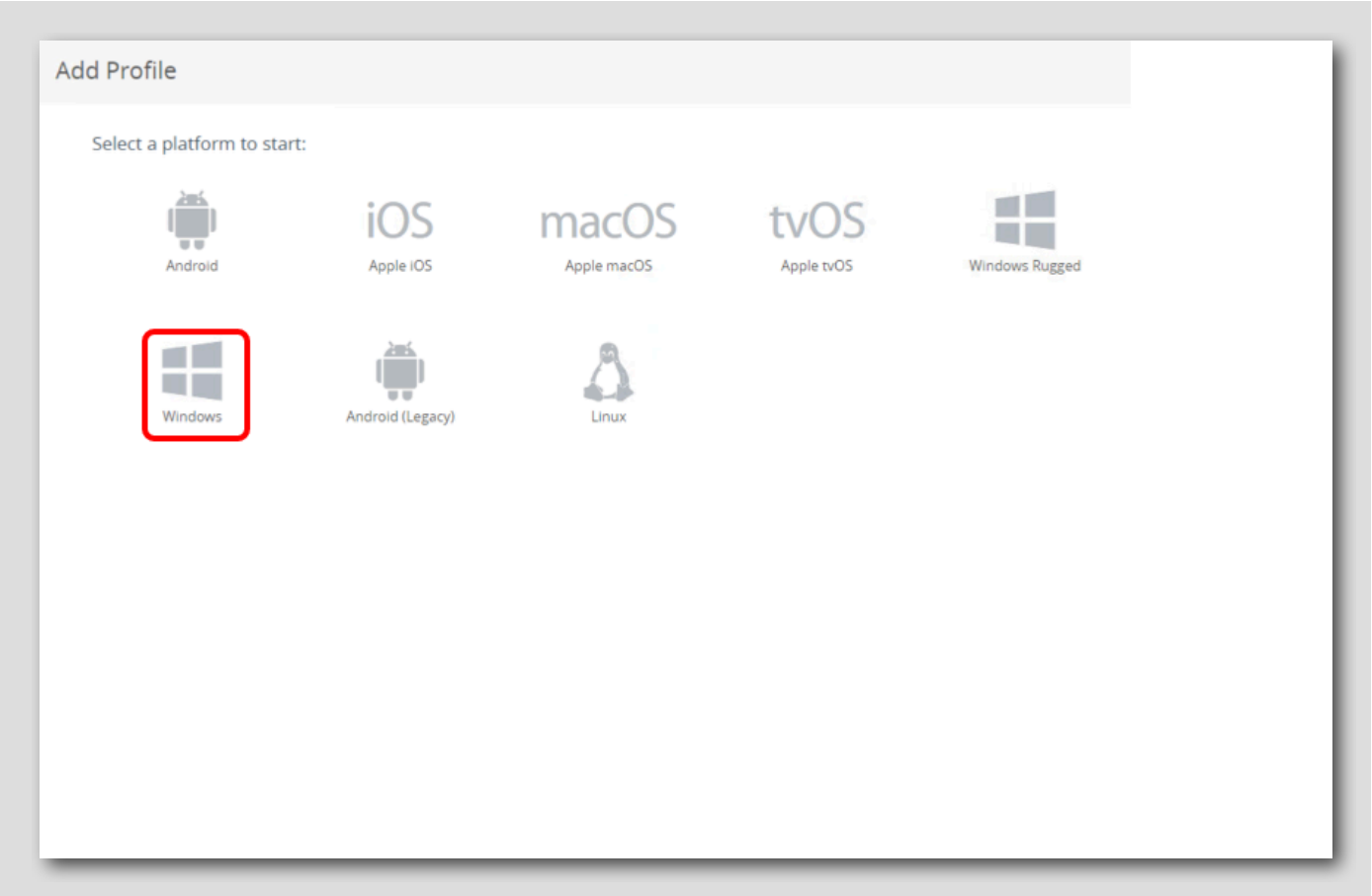


In the Workspace ONE UEM Administrator Console:

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

Add a Windows Profile

[57]

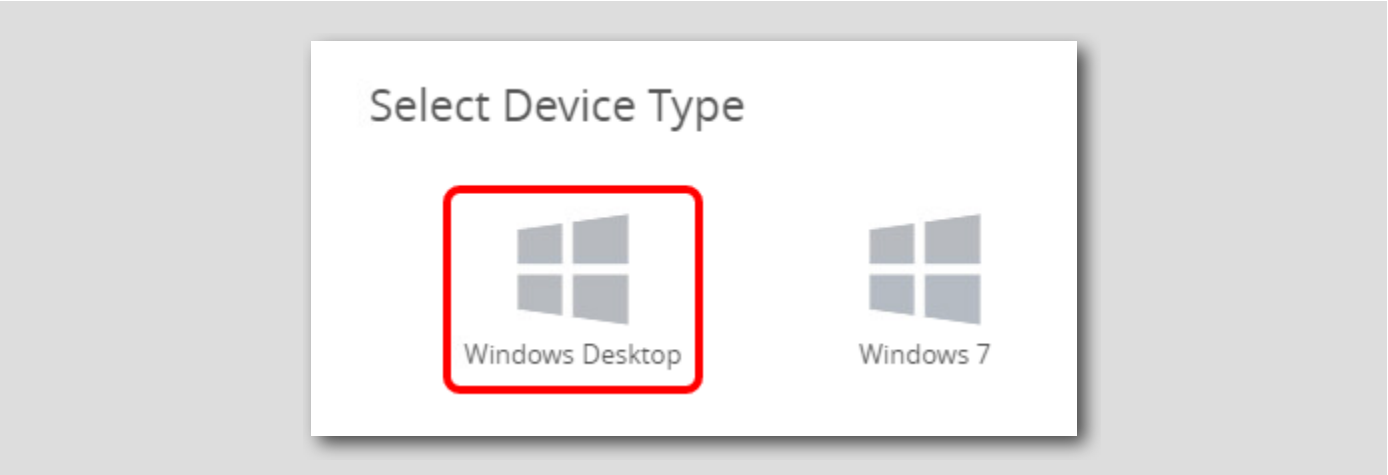


Select the **Windows** icon.

Note: Make sure that you select **Windows** and *not* Windows Rugged.

Add a Windows Desktop Profile

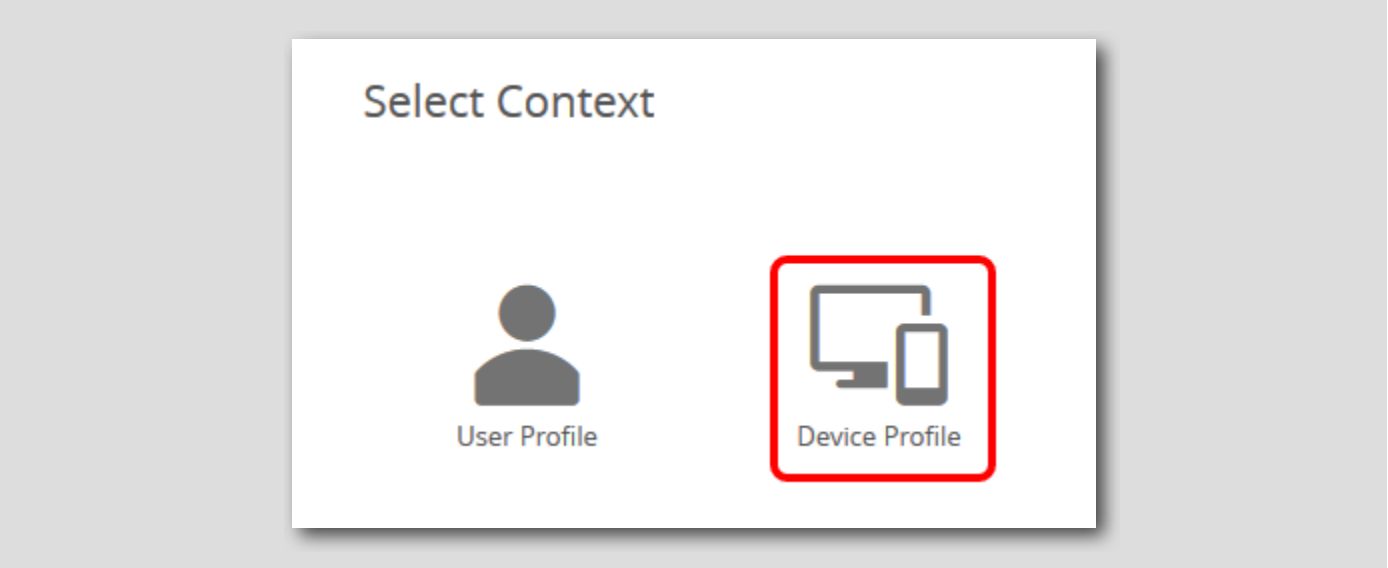
[58]



Select **Windows Desktop**.

Select Context - Device Profile

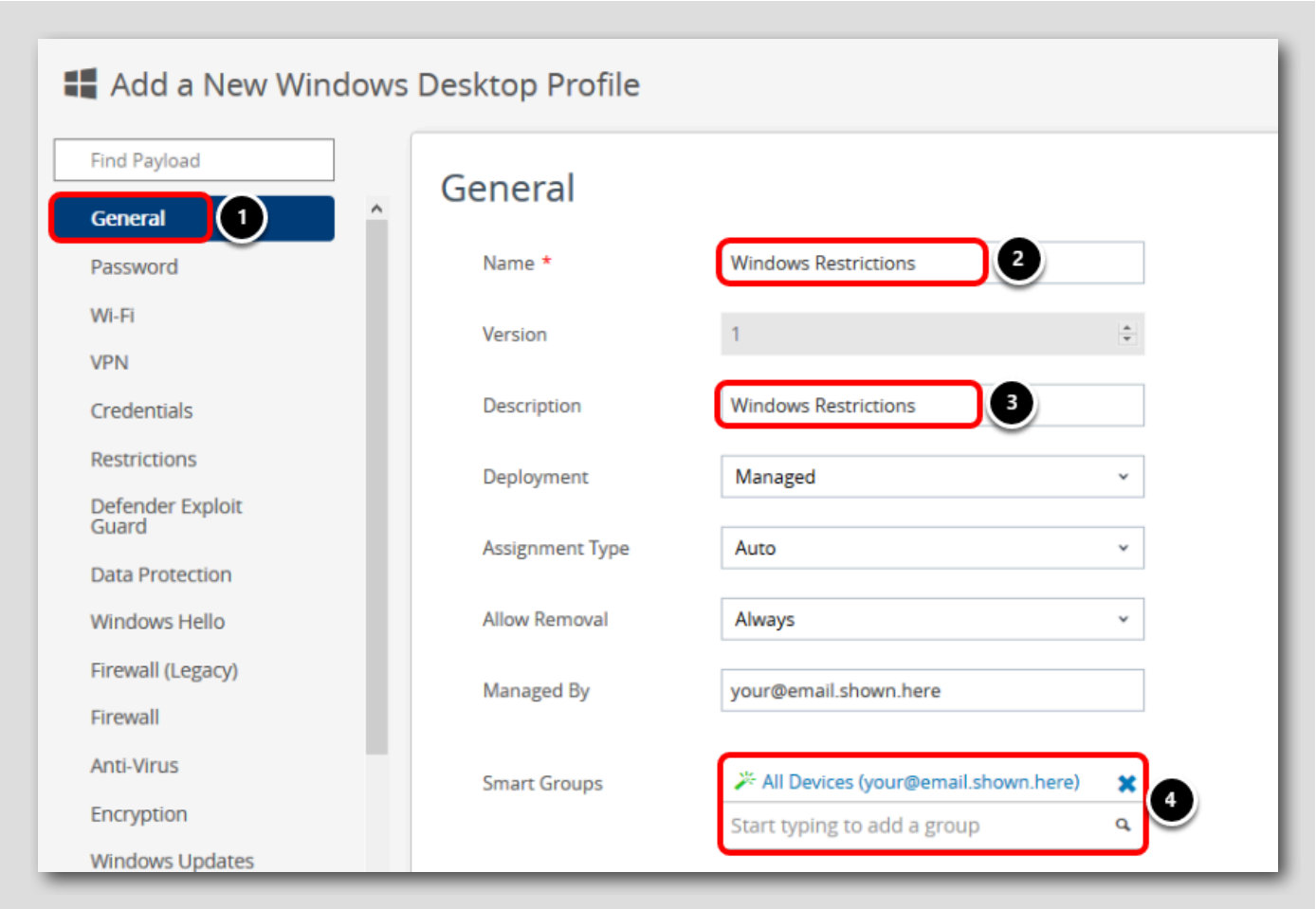
[59]



Select **Device Profile**.

Define the General Settings

[60]



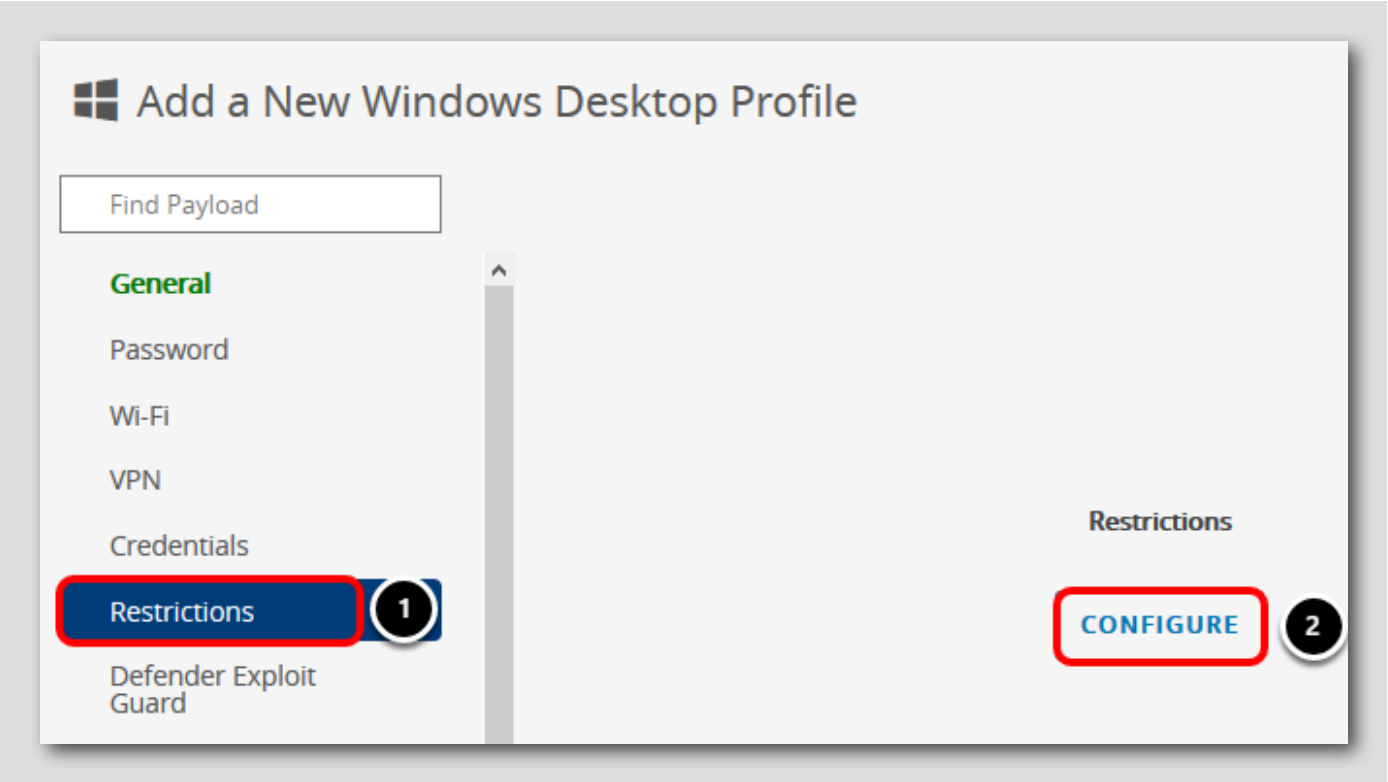
1. Select **General** if it is not already selected.
2. Enter a profile name such as **`Windows Restrictions`** in the Name text box.
3. Optionally enter **`Windows Restrictions`** into the Description field.
4. Click in the **Smart Groups** field. This will pop-up the list of created Smart Groups. Select the **All Devices** Smart Group.

   Note: You may need to scroll down to view the Smart Groups field.

Note: You DO NOT need to click **Save & Publish** at this point. This interface allows you to move around to different payload configuration screens before saving.

Select the Restrictions Payload

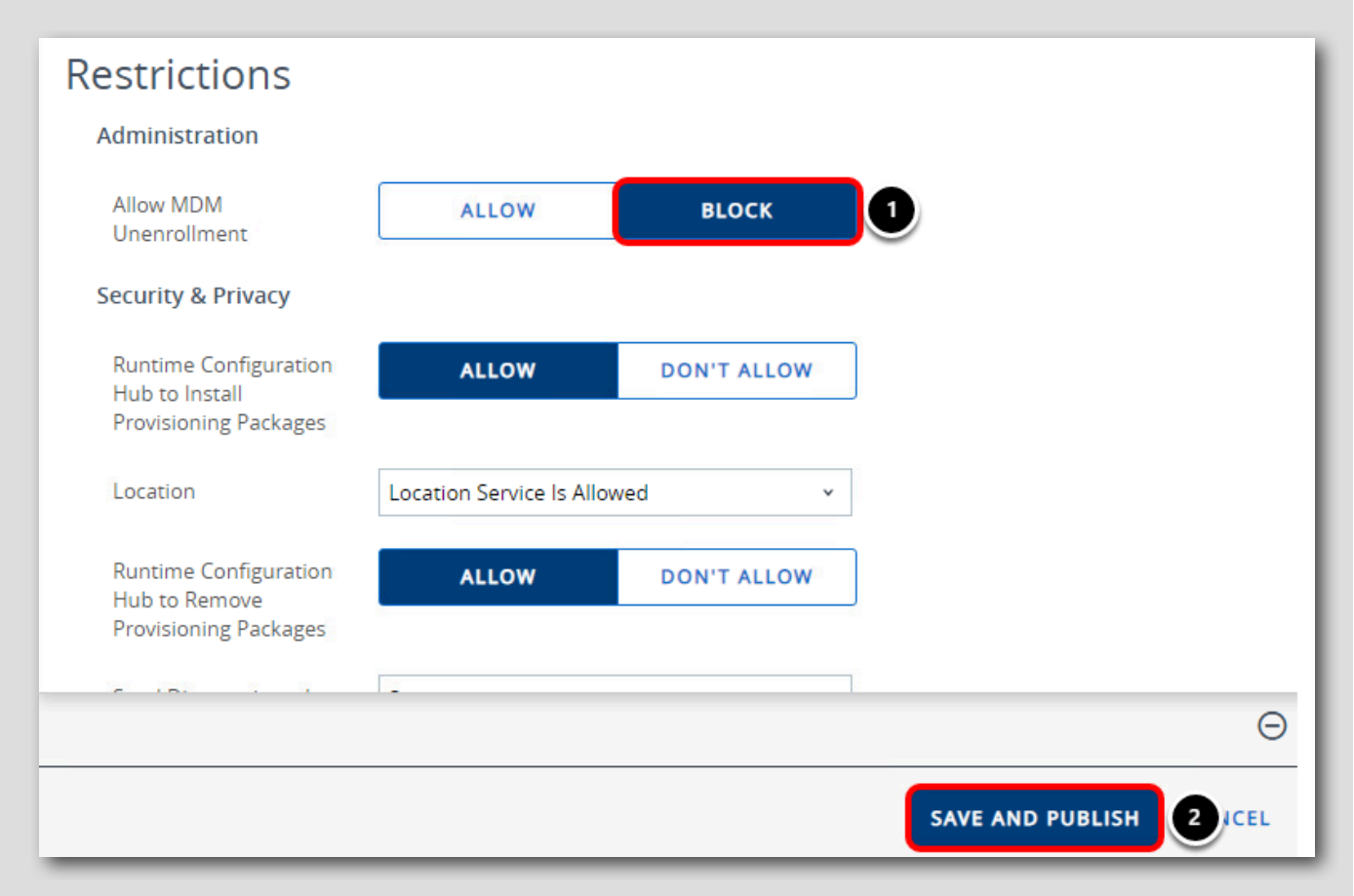
[61]



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

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

Adding a Restriction - Disable End User Unenrollment



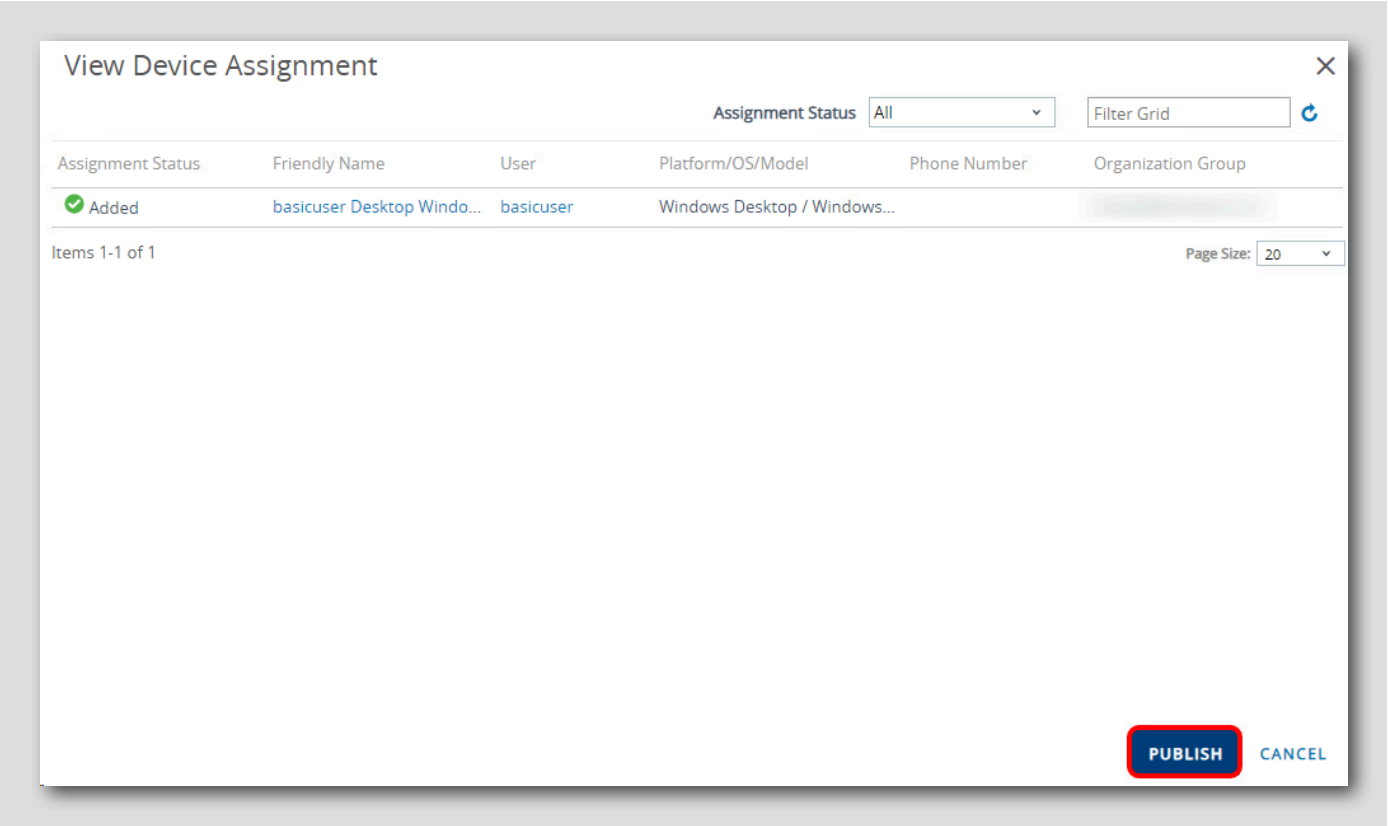
1. Select **Block** for **Allow MDM Unenrollment**.
2. Click **Save & Publish**.

NOTE: Some restrictions require a certain version of Windows or higher to apply to a device. A few references are available for you to determine which version of Windows is required, including:

- VMware Policy Builder: `https://www.vmwarepolicybuilder.com`
- Configuration Service Provider (CSP) Reference: `http://aka.ms/CSPList`
- Whats New in MDM Enrollment and Management: `https://docs.microsoft.com/en-us/windows/client-management/mdm/new-in-windows-mdm-enrollment-management`

Publish the Restrictions Profile

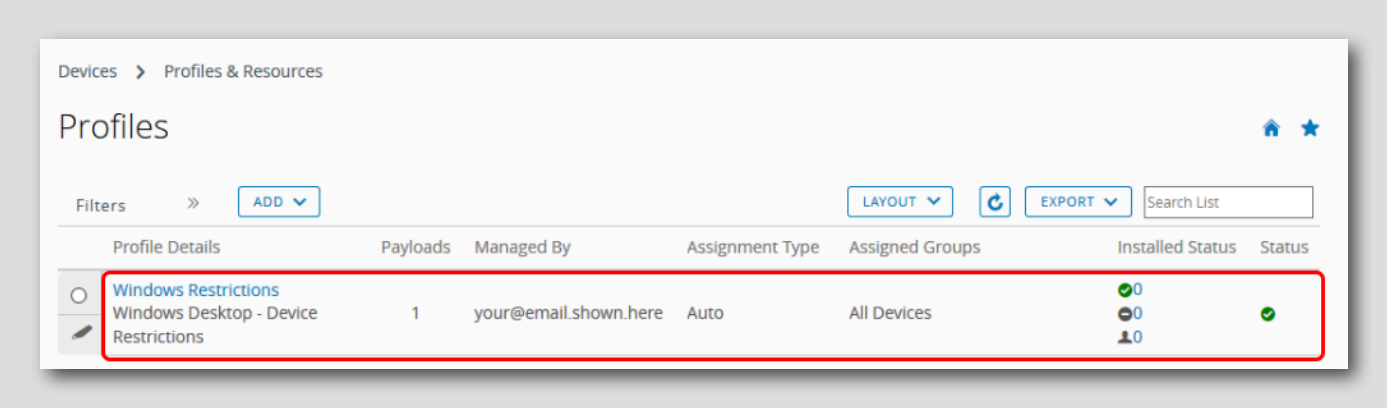
[63]



A preview of devices that will receive this profile based on the assigned smart groups is shown. Click **Publish**.

Verify the Restrictions Profile Now Exists

[64]



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

Note: If you need to edit the Restrictions Profile, this is where you would do so. To edit the profile, click the profile name, then select Add Version. Update the profile and click Save & Publish to push the new settings to the assigned devices.

Create Sensors for Windows

[65]

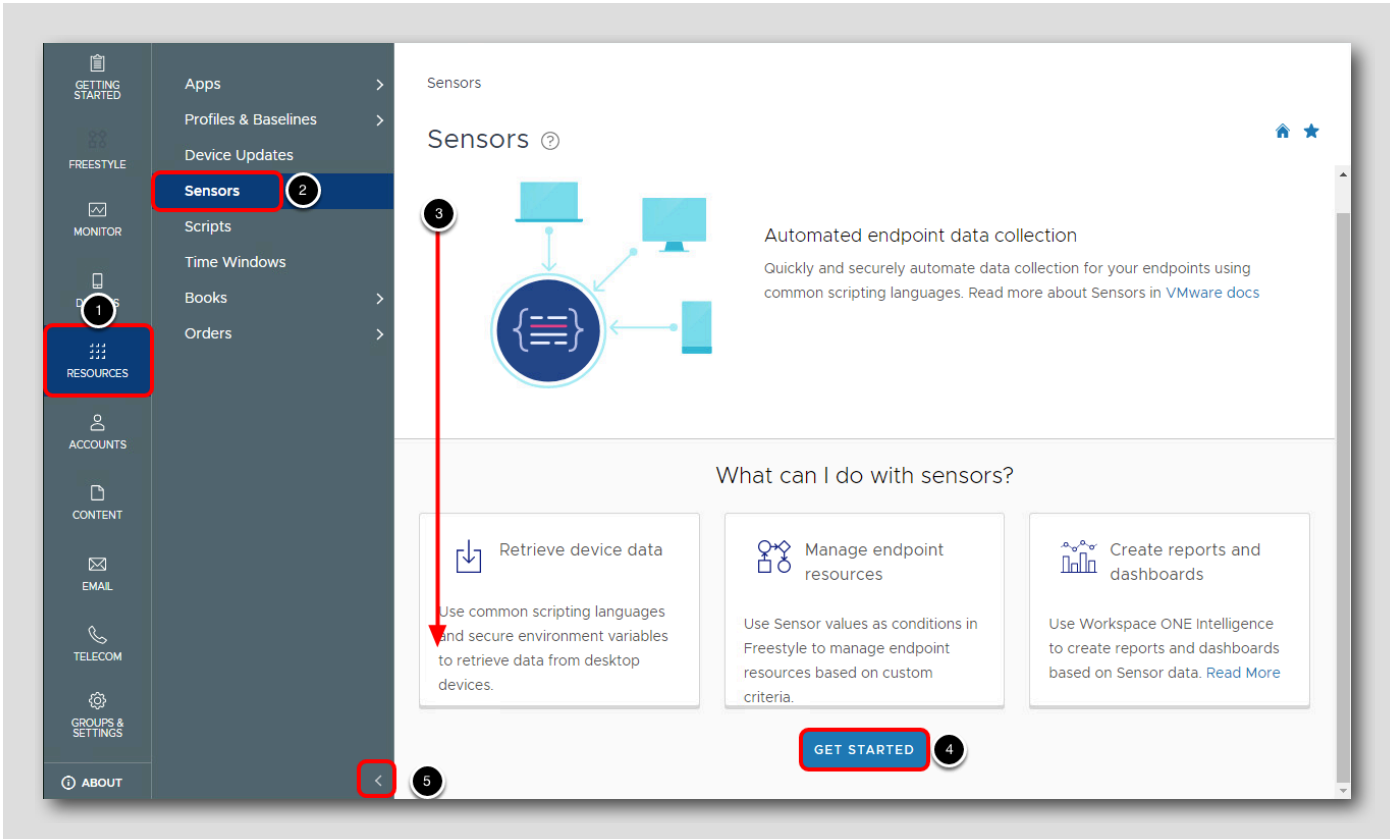
Sensors allow you to quickly and securely automate data collection from your endpoints with common scripting languages. macOS Sensors support Bash, Python 3, and Zsh, and Windows Sensors support PowerShell. Any data point that can be queried using these languages can be returned as a Sensor!

The data collected from Sensors can be used as conditions in Freestyle Orchestrator to take different actions based on the returned values. You can learn more about Freestyle Orchestrator in *Module 7 - 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 Windows that will query if there is a Trusted Platform Module (TPM) present on the endpoint.

Navigate to Sensors

[66]

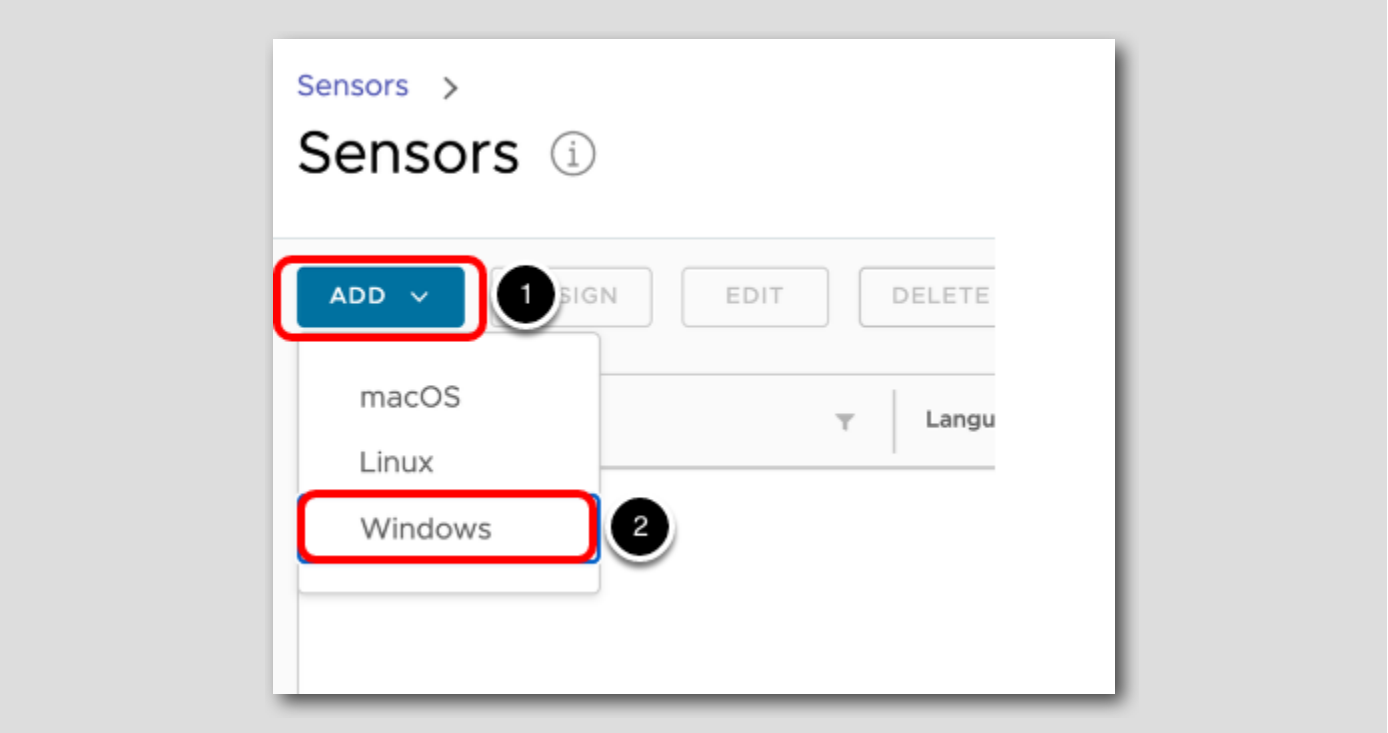


The first time you access the Sensors page, an overview will be presented with a link to the VMware Docs articles for *macOS Sensors* and *Windows Sensors*. Refer to these links for additional documentation around Sensors.

1. Click **Resources**
2. Click **Sensors**
3. **Scroll down** to the bottom of the page
4. Click **Get Started**
5. If you are unable select Get Started **Click** the arrow to show/hide the side bar, this will allow you to choose Get Started and continue the lab.

Add a Windows Sensor

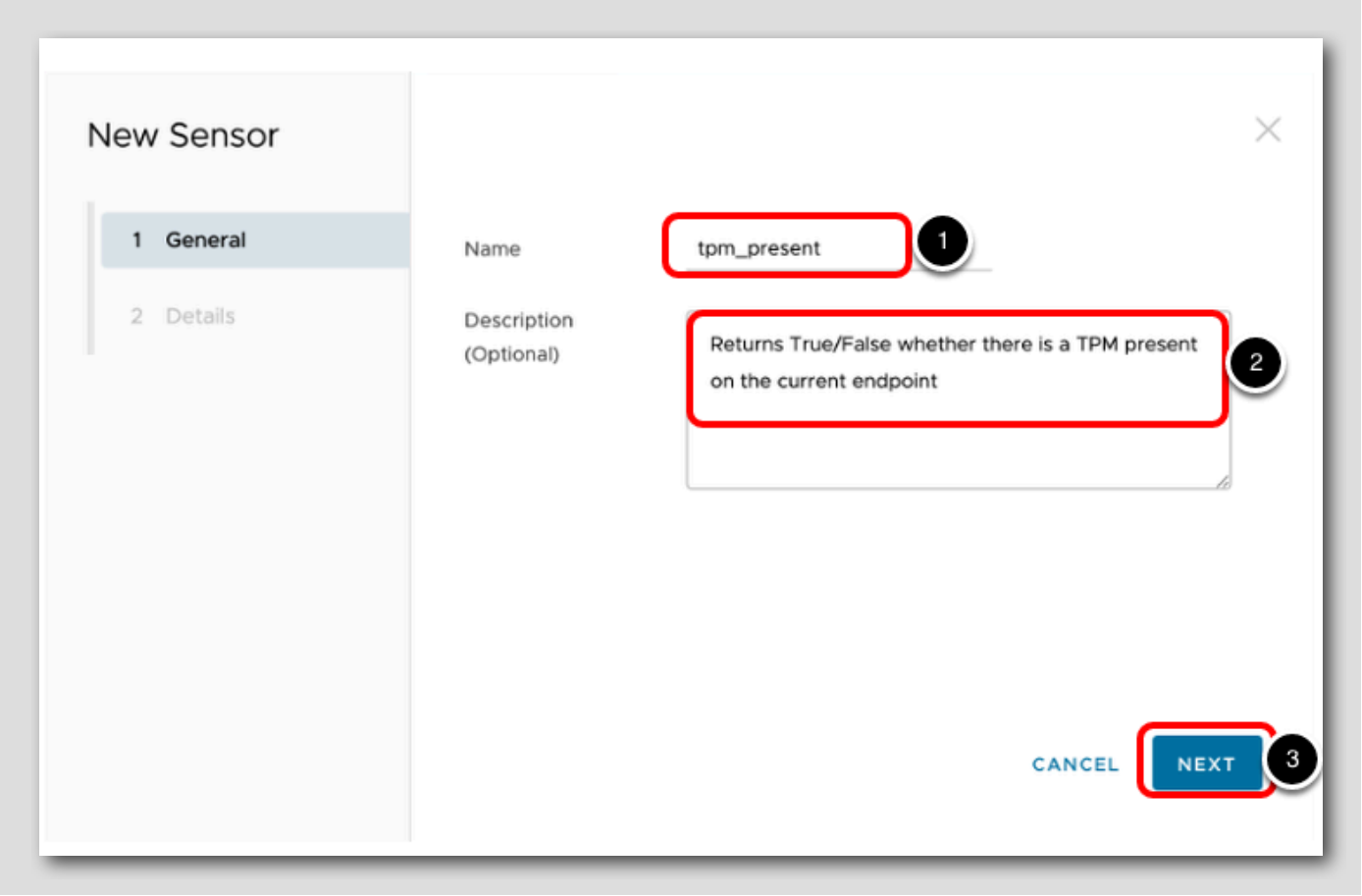
[67]



1. Click **Add**
2. Click **Windows**

Add General Information

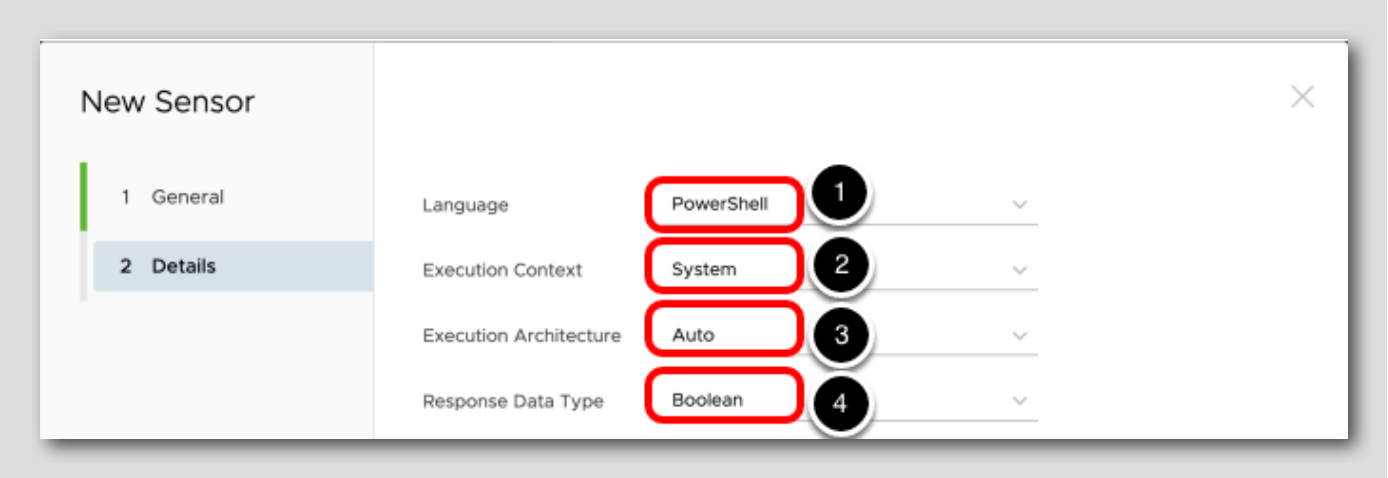
[68]



1. Enter **`tpm_present`** for the Name
2. Optionally enter **`Returns True/False whether there is a TPM present on the current endpoint`** for the description
3. Click **Next**

Enter the Sensor Details

[69]



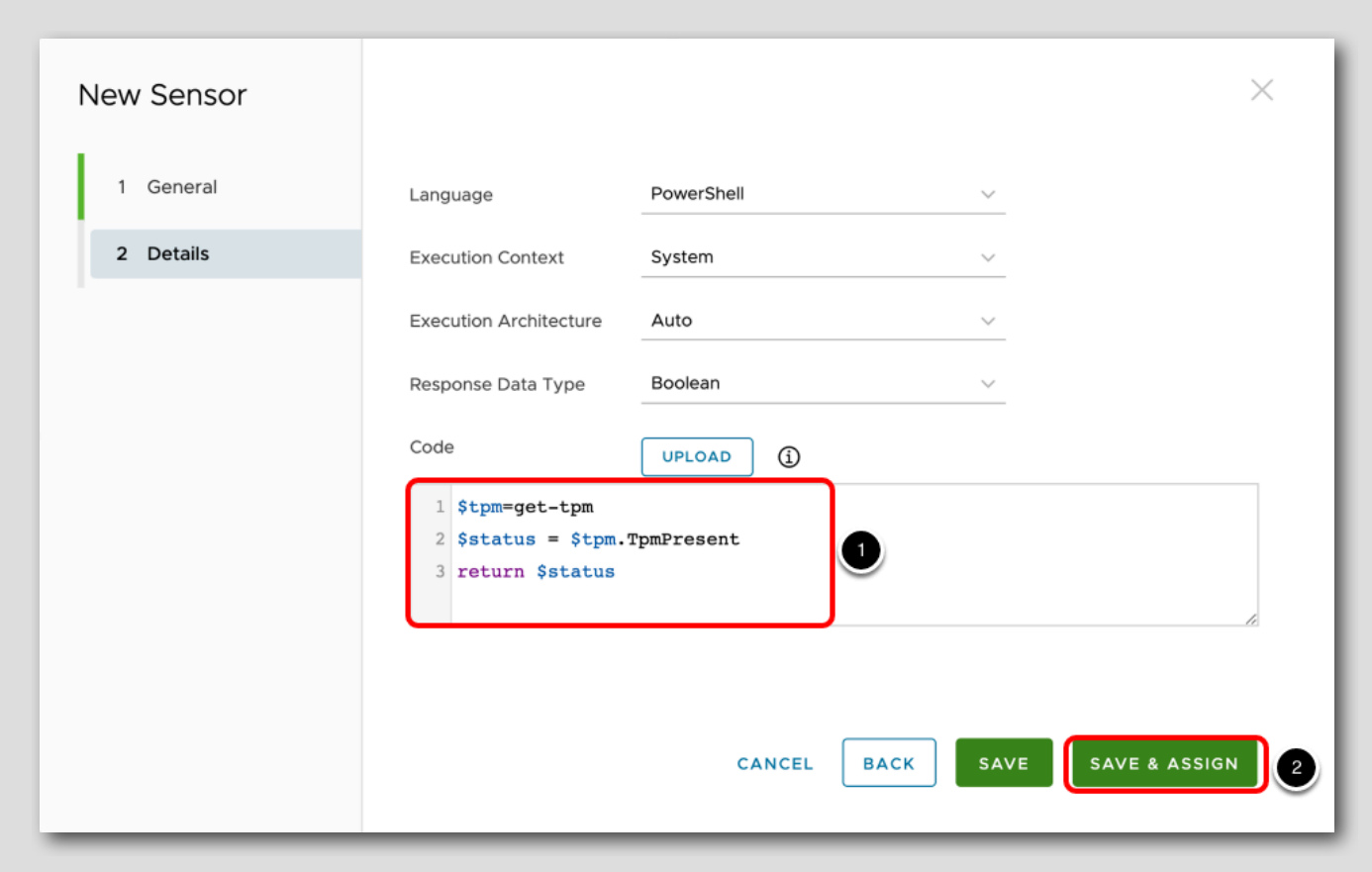
1. Check that **PowerShell** is selected for the Language
2. Select **System** for the Execution Context
3. Select **Auto** for the Execution Architecture
4. Select **Boolean** for the Response Data Type

Currently PowerShell is the only supported language for Windows Sensors.

This sensor will run in the System context since a TPM module is not specific to any user. If you wanted to retrieve information specific to the currently logged in user, such as their username, you would use the Current User context.

The Response Data Type will determine which filter types are available for the Sensor data in Intelligence. This sensor will return True or False depending if a TPM is present.

Copy and Paste the Sensor Code



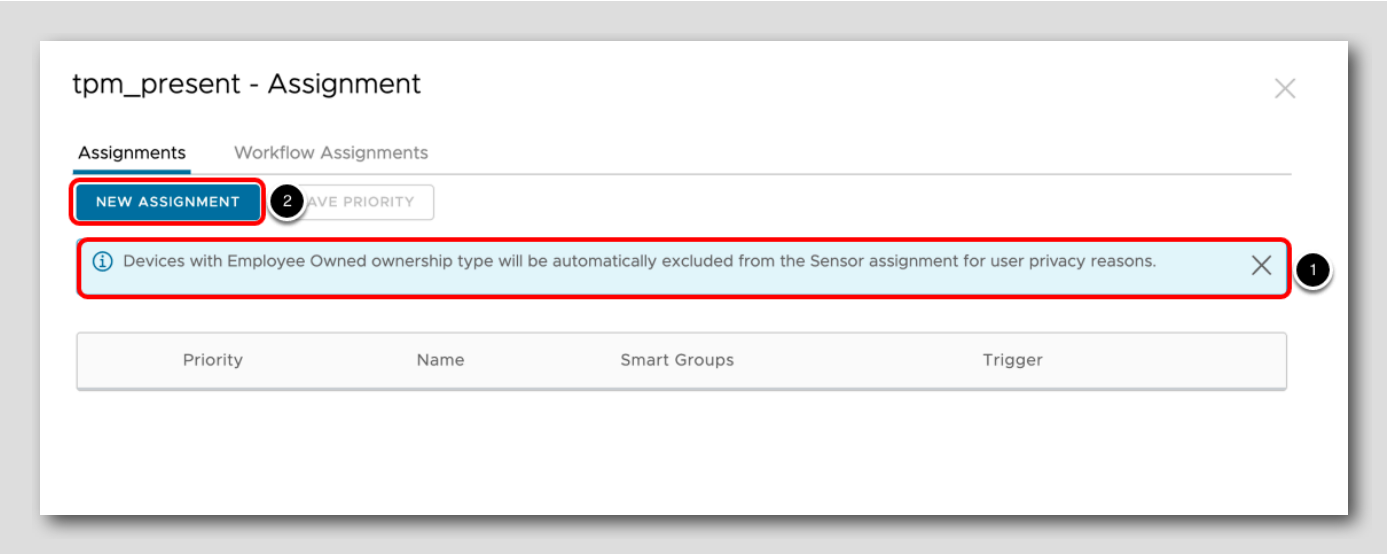
1. Click and drag to highlight the below code block, then drag and drop it the **Code** section to paste the necessary sensor code
2. Click **Save & Assign**

In this exercise we manually typed in the code, but you can also upload a file containing the code.

```
$tpm=get-tpm
$status = $tpm.TpmPresent
return $status
```

Assign a Windows Sensor

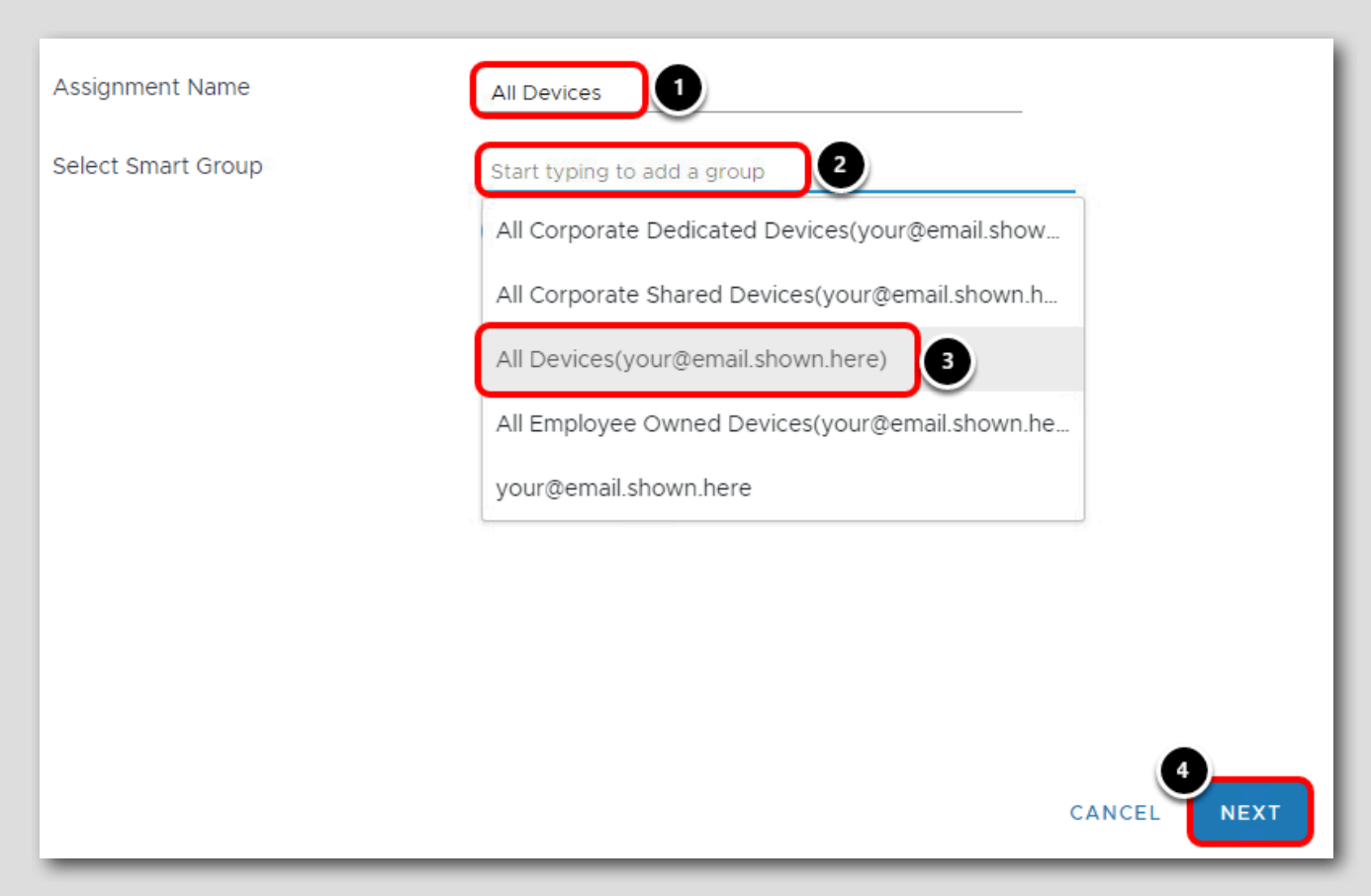
[71]



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

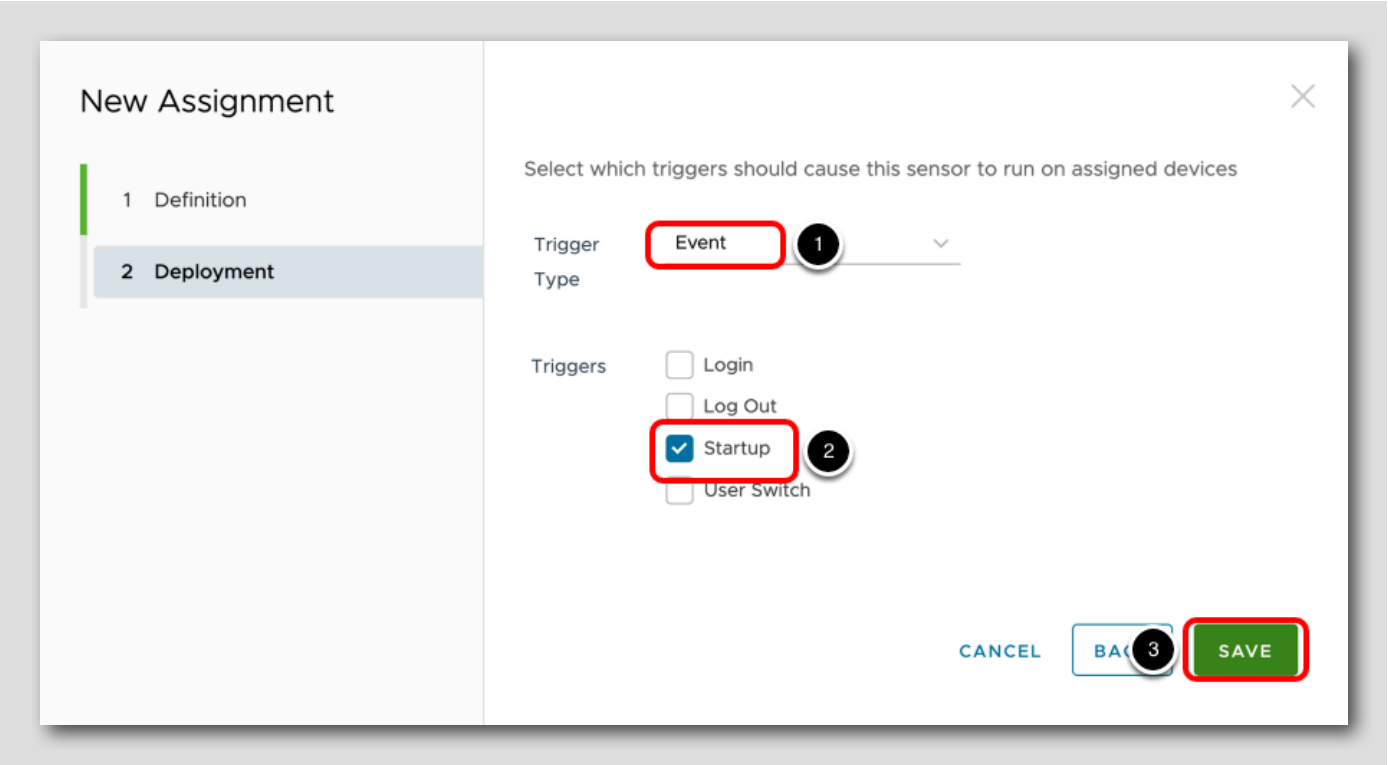
[72]



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

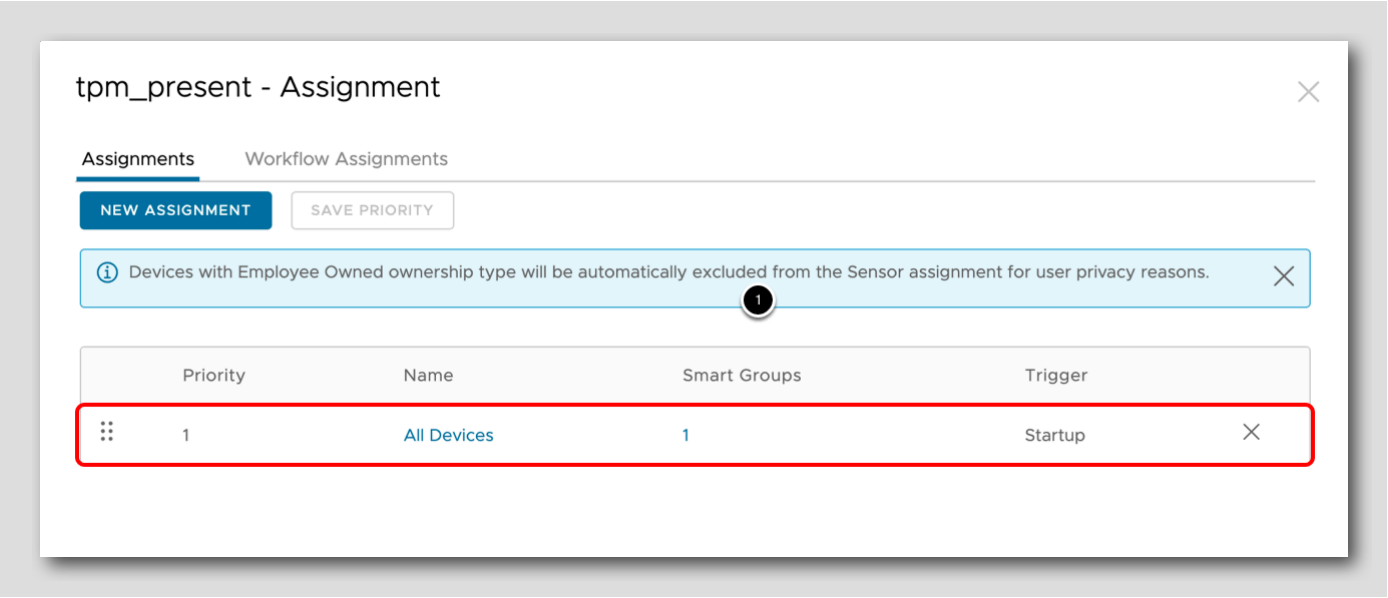


1. Select **Event** for the Trigger Type
2. Check **Startup** for the Trigger
3. Click **Save**

You can select more than one Trigger to have your Sensor run during multiple events.

Confirm Sensor Creation

[74]



1. Your Sensor is now created
2. Click **Close** to return to the Sensors page.

You have now successfully created and assigned a Windows Sensor which will report back if the endpoint has a Trusted Platform Module (TPM) present. Once you enroll a device in later steps, you will view this sensor and confirm the value.

Sensors are an extremely powerful and flexible way to automate data collection from your endpoints. Consider what other use cases you could accomplish with Sensors, and check out the *Windows Sensors examples in VMware Docs* for ideas.

Delivering On Demand Apps on Windows 10

[75]

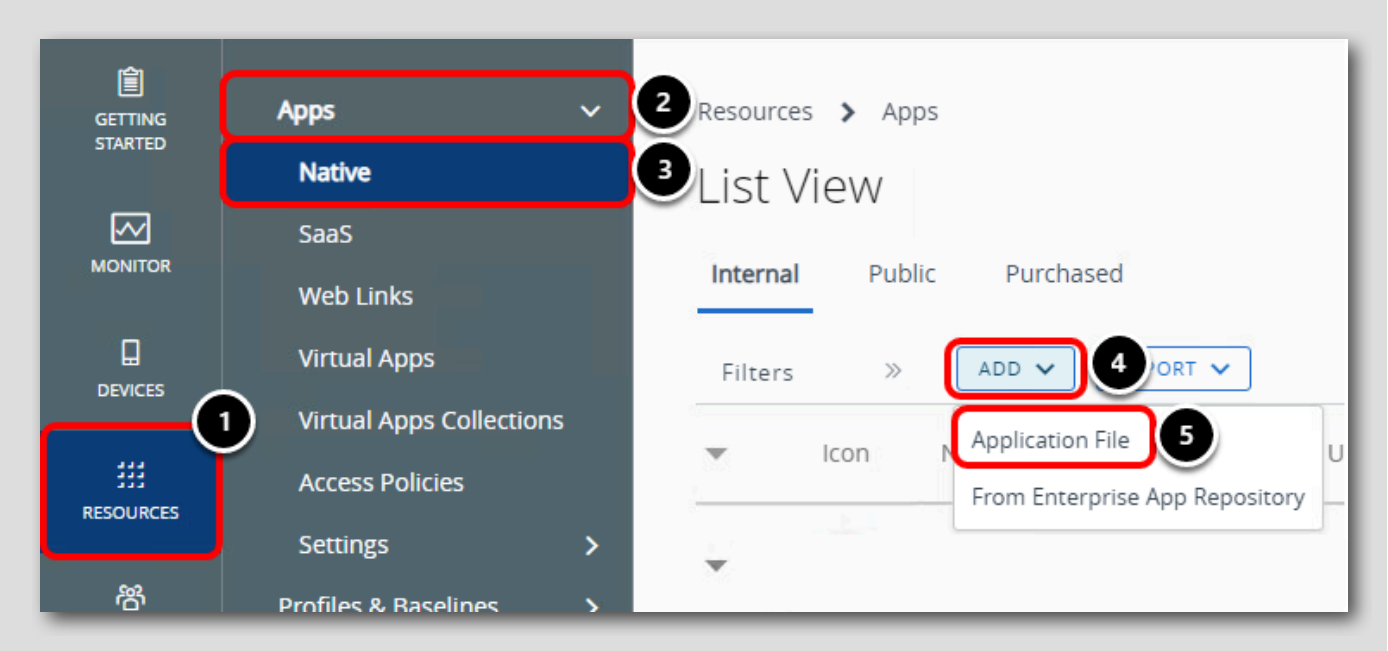
There are two ways to distribute applications: On Demand and Auto.

- **On Demand** allows users to initiate the download and install of an app presented in the Intelligent Hub app catalog when they decide that they need access to the app.
- **Auto** will download and install the app automatically on the device without requiring the user to interact with the app from the Intelligent Hub app catalog.

This exercise will show how to deploy the 7-Zip executable as an On Demand app.

Add Internal Application

[76]

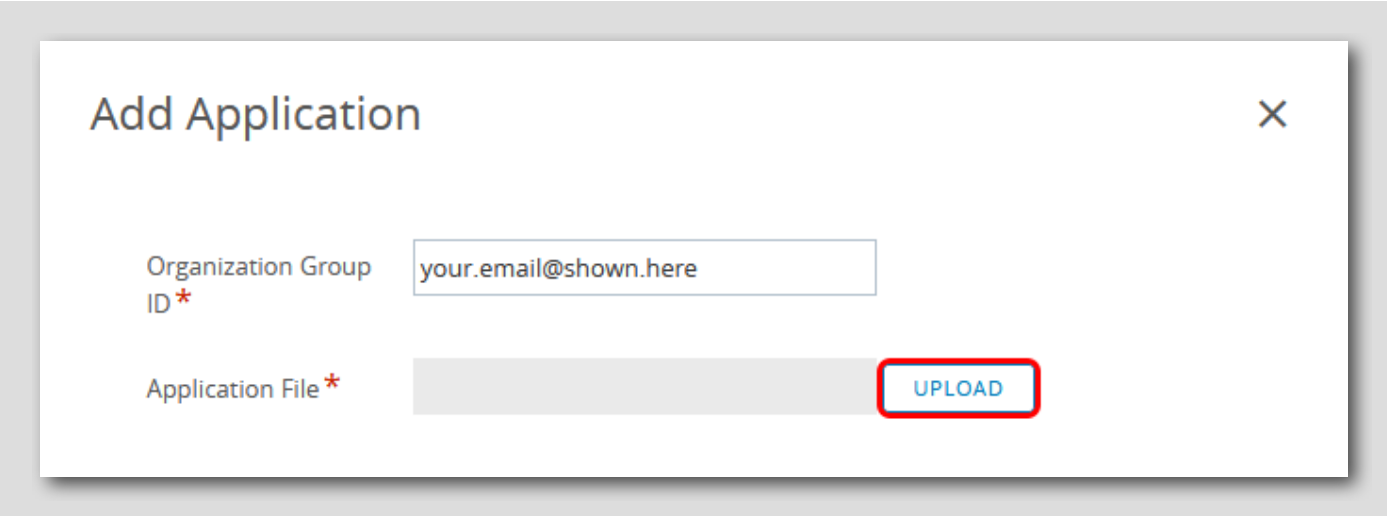


In the Workspace ONE UEM Administrator Console:

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

Upload Application

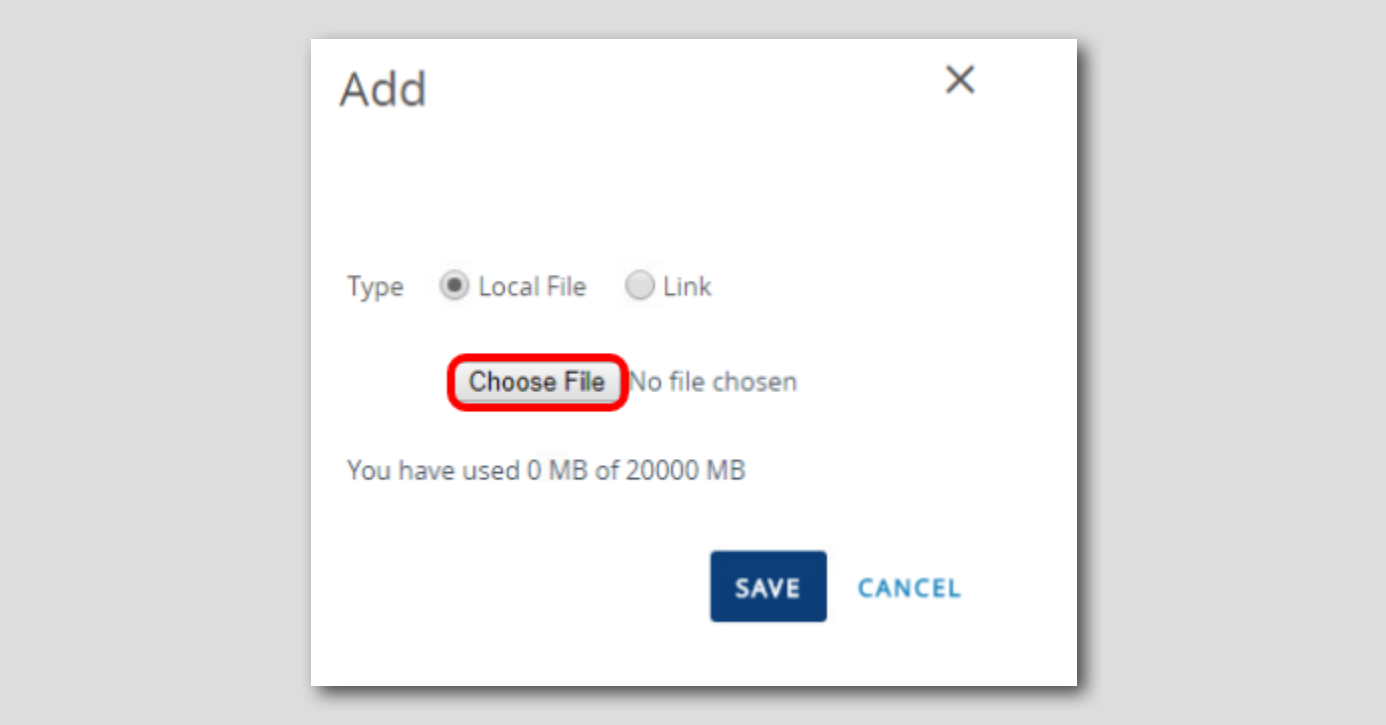
[77]



Click **Upload**.

Find the Application Installer

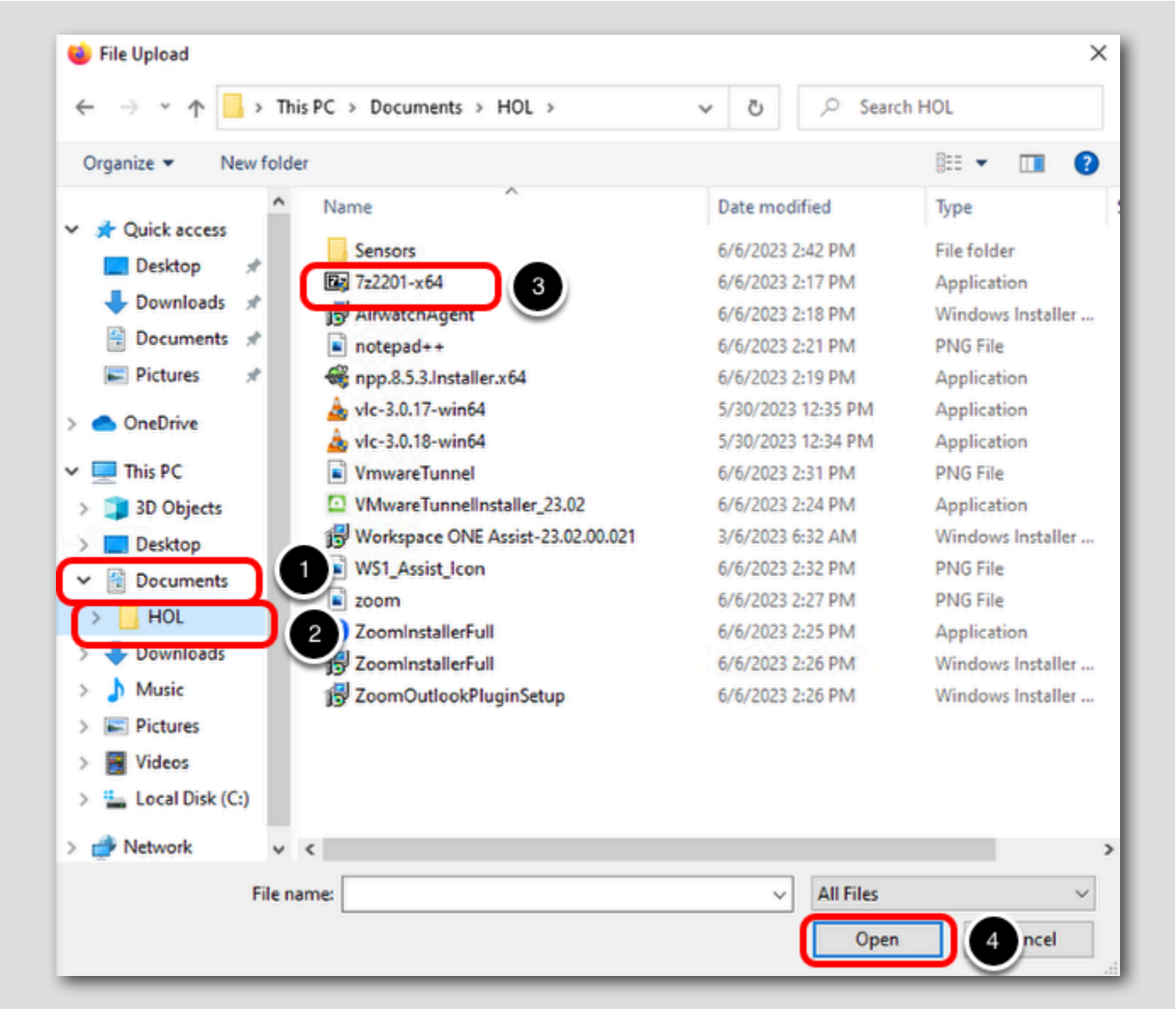
[78]



Click the **Choose File** button.

Upload the 7-Zip EXE File

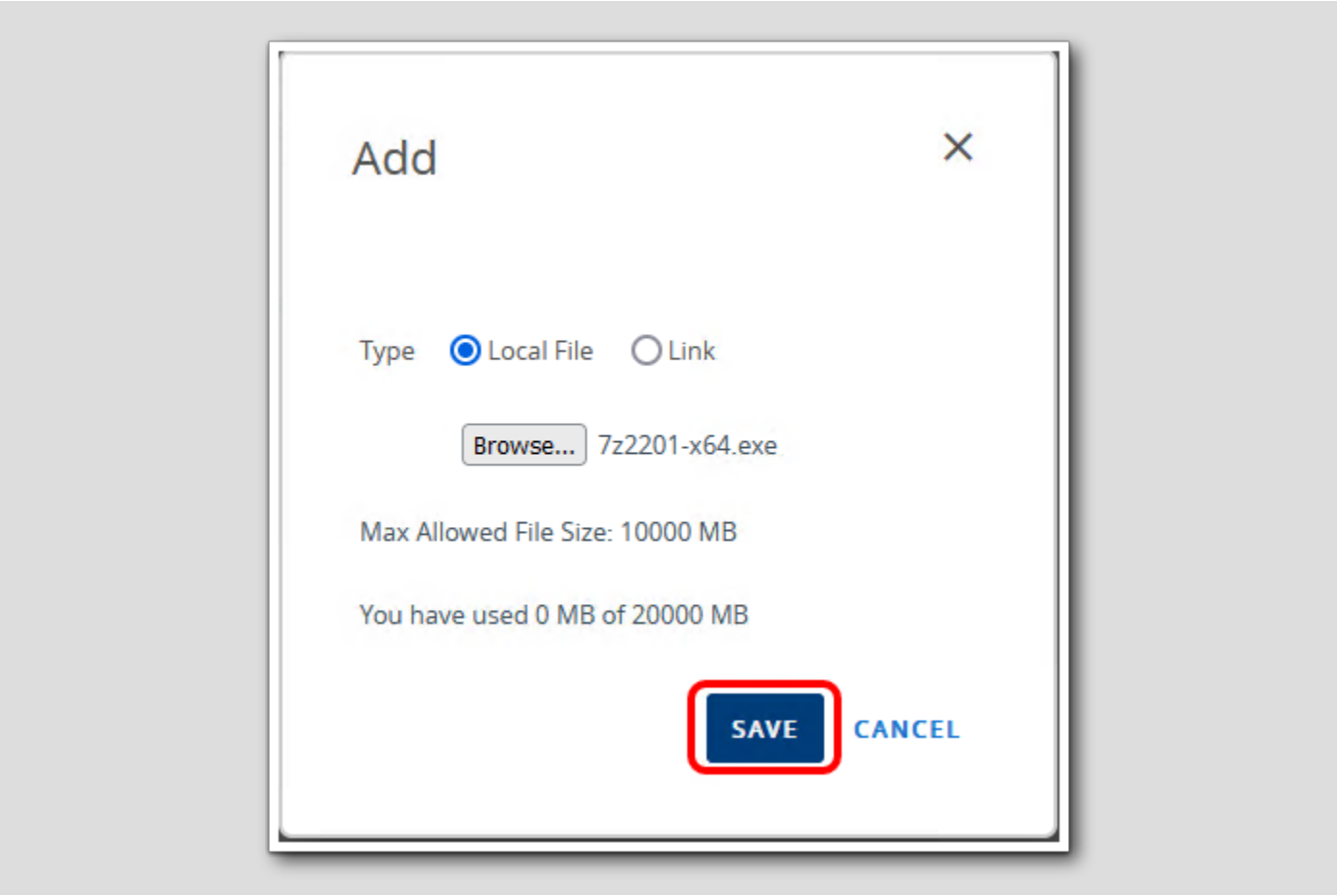
[79]



1. Click **Documents**.
2. Click **HOL**.
3. Select the **7z2201-x64** executable file.
4. Click **Open**.

Save the EXE File

[80]

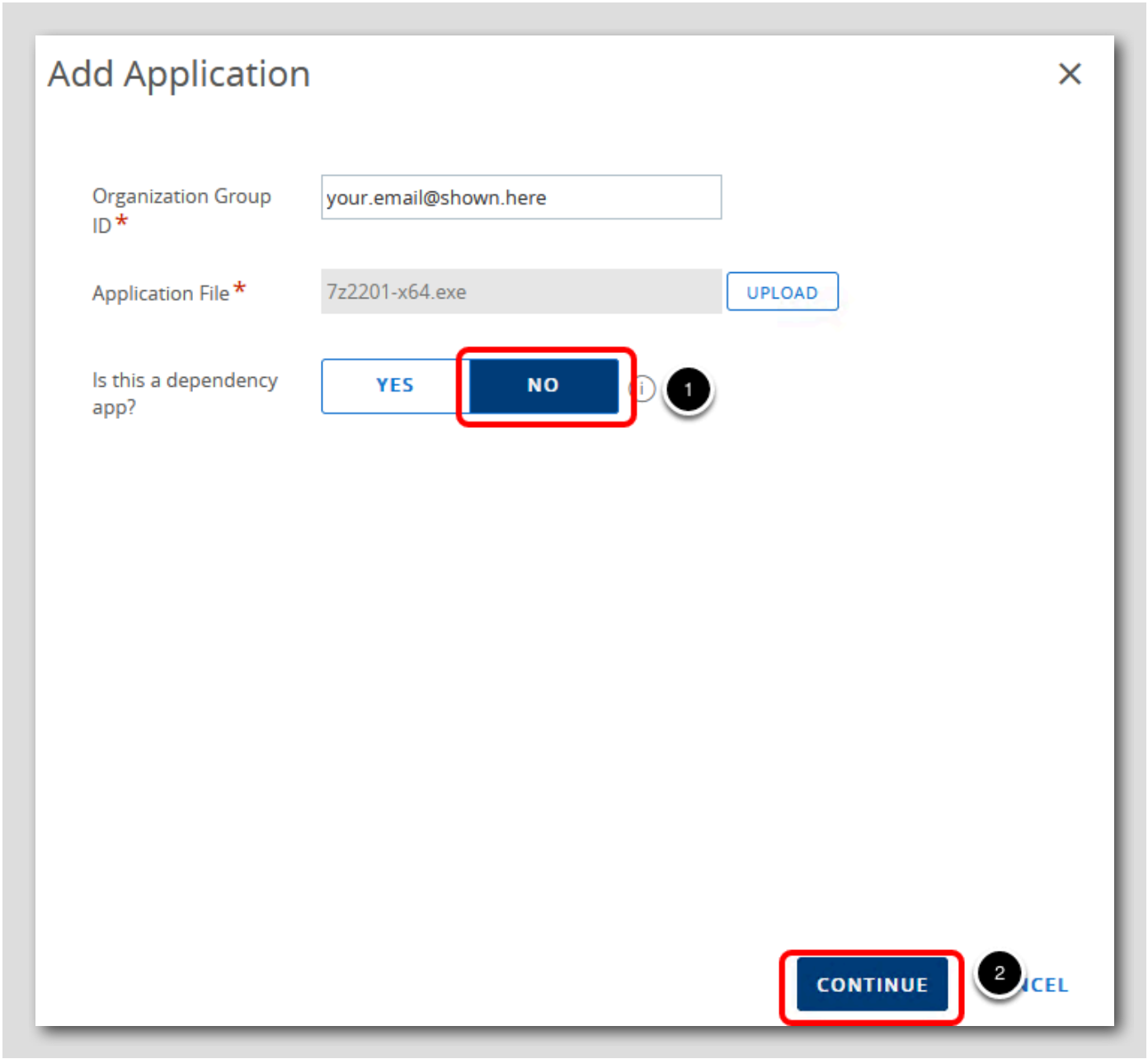


Click **Save**.

NOTE: The app upload may take a few minutes to complete! Continue to the next step once the upload completes. If you see "An error has occurred HTTP Status Code 0" please try the upload again as internet bandwidth is variable.

Continue to the App Settings

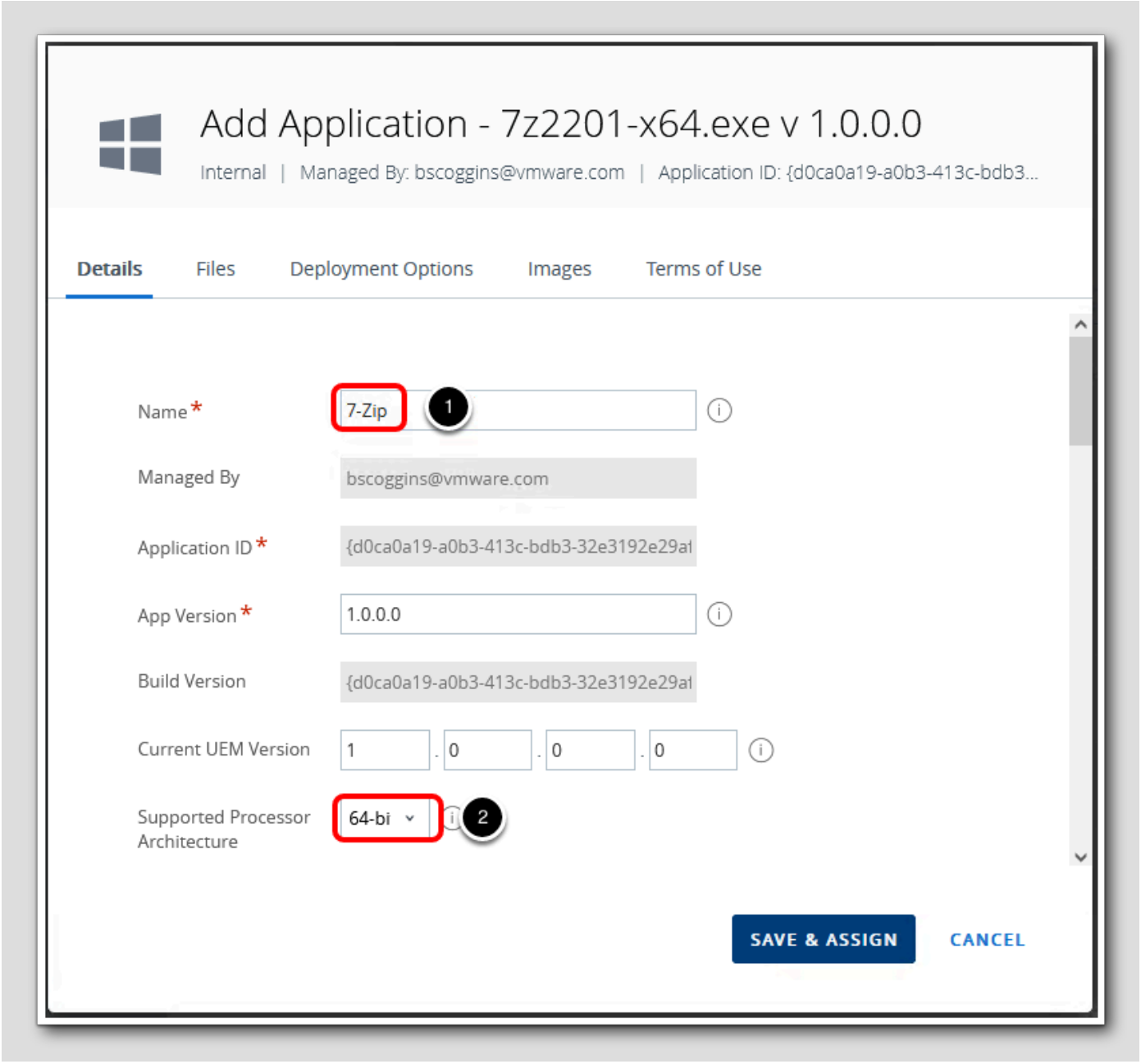
[81]



1. Select **No** for **Is this a dependency app?**
2. Click **Continue**.

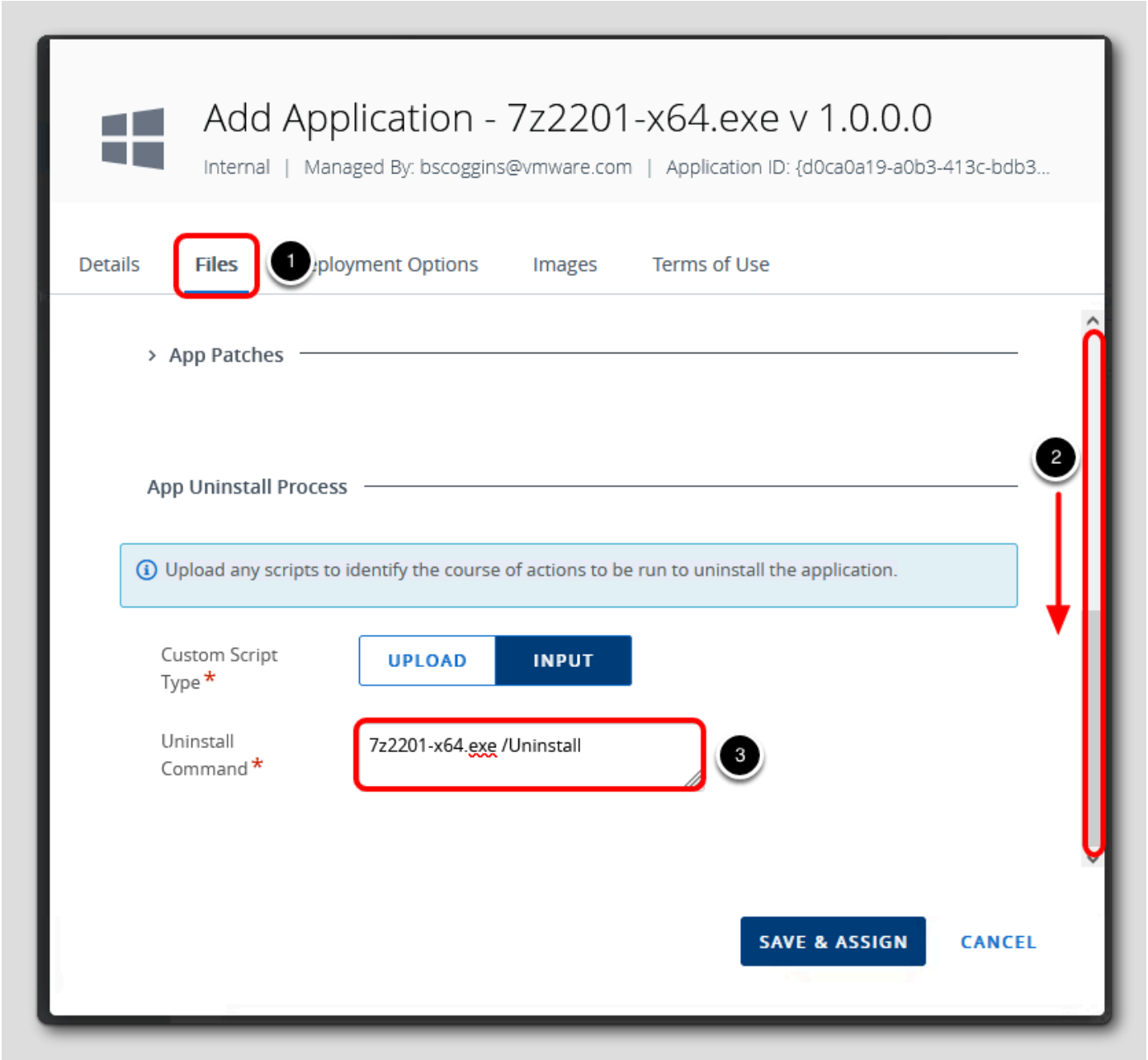
Configure App Details

[82]



1. Enter a name for your application: **`7-Zip`**. This name will be displayed in the app catalog to your users.
2. Select **64-bit** for the **Supported Processor Architecture**.

Configure Application Files



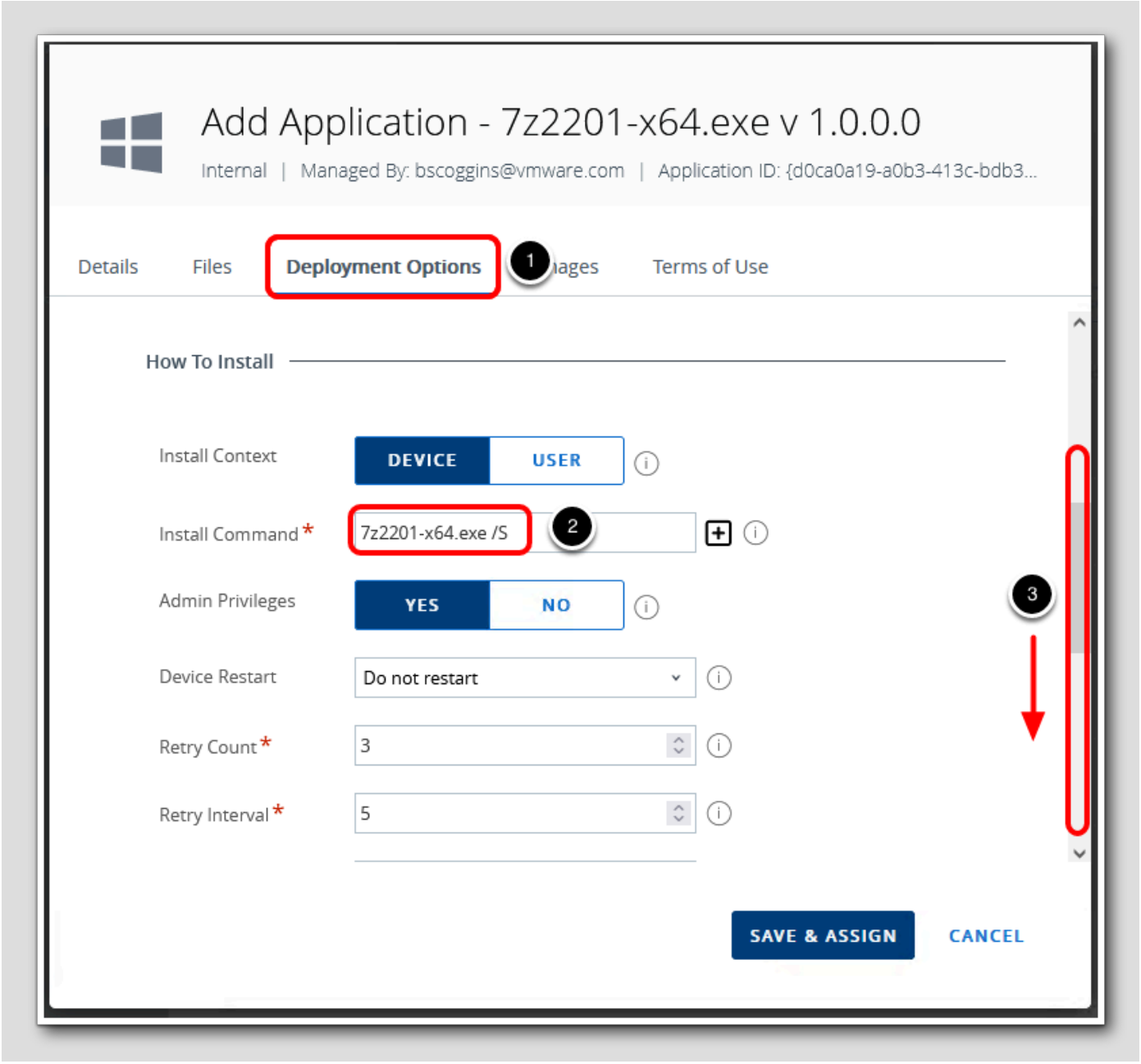
1. Select the **Files** tab.
2. Scroll down to find the **App Uninstall Process** section.
3. Enter the following for **Uninstall Command**: `7z2201-x64.exe /Uninstall`

NOTE: Remember that you can copy and paste text from the manual into the lab to avoid typing mistakes!

NOTE: For more information about copying text from the manual, see the Guidance section.

Select Deployment Options

[84]



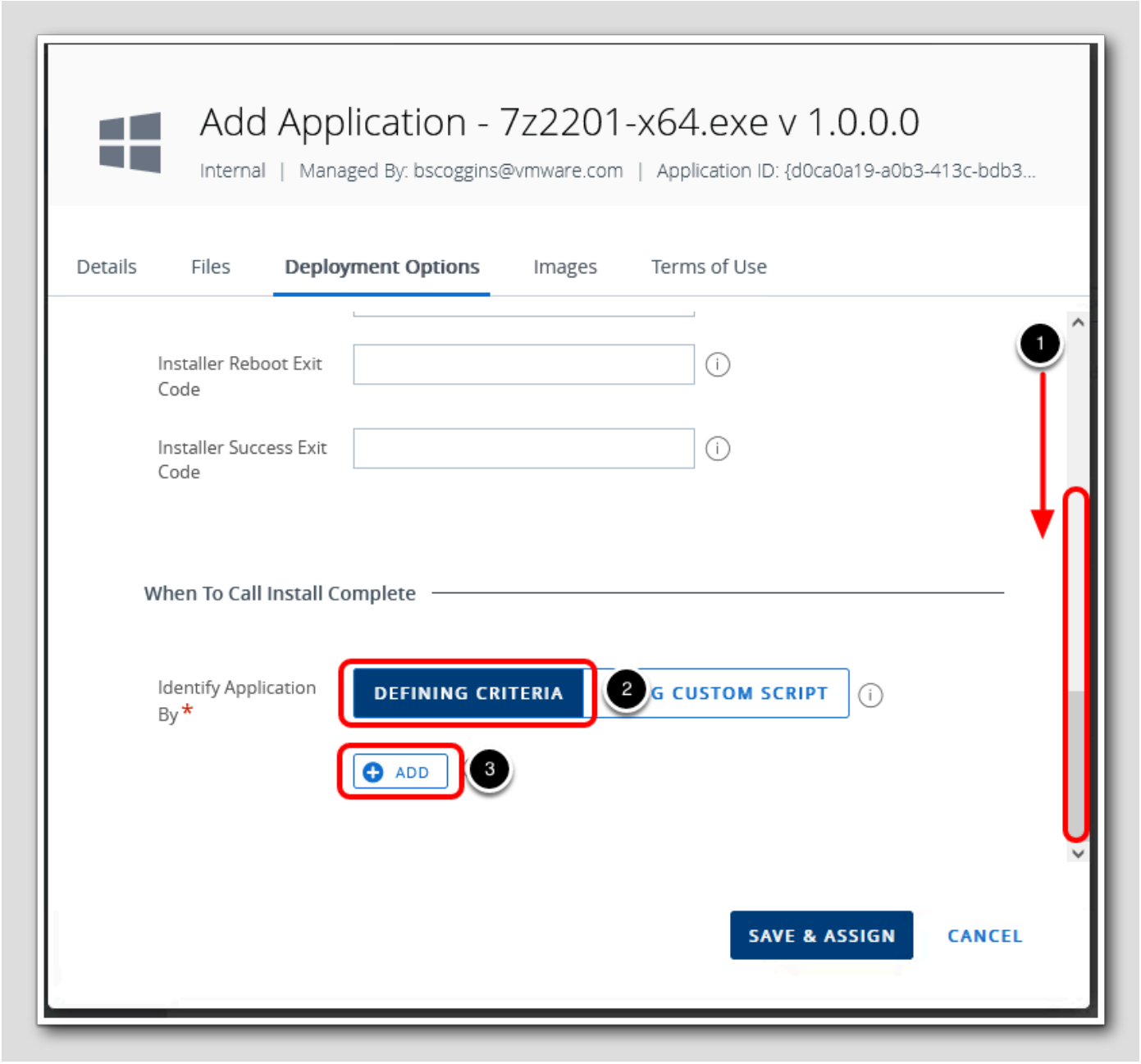
1. Select **Deployment Options**.
2. Scroll down until you see the option for **Install Command**.
3. Enter **Install Command** as: **`7z2201-x64.exe /S`**

NOTE: Remember that you can copy and paste text from the manual into the lab to avoid typing mistakes!

NOTE: For more information about copying text from the manual, see the Guidance section.

Add Identify Application Condition

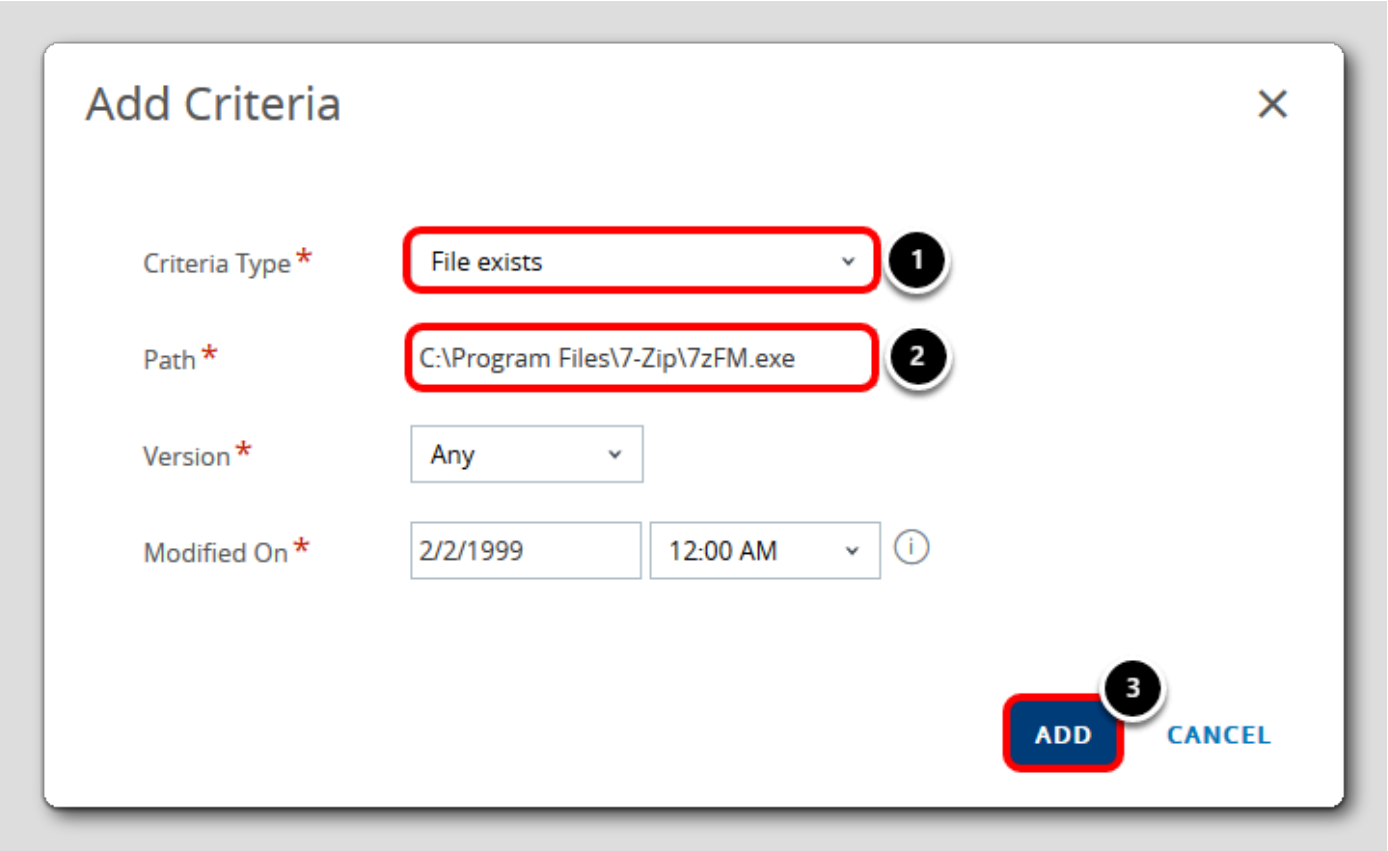
[85]



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

Configure the Install Complete Defining Criteria

[86]



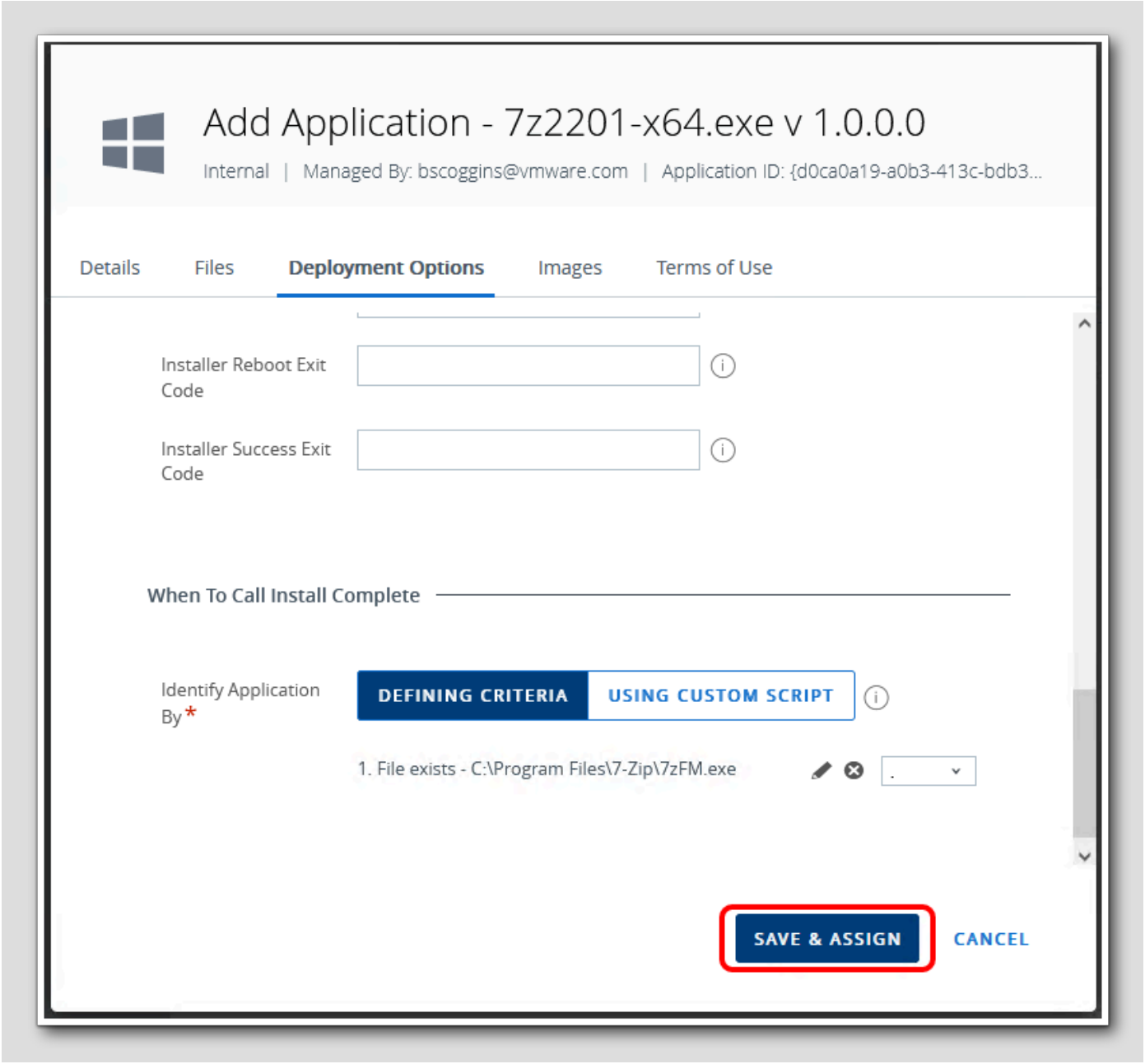
1. Select **File Exists** for the **Criteria Type**.
2. Enter **`C:\Program Files\7-Zip\7zFM.exe`** for the **Path**.
3. Click **Add**.

NOTE: Remember that you can copy and paste text from the manual into the lab to avoid typing mistakes!

NOTE: For more information about copying text from the manual, see the Guidance section.

Save and Assign the Application

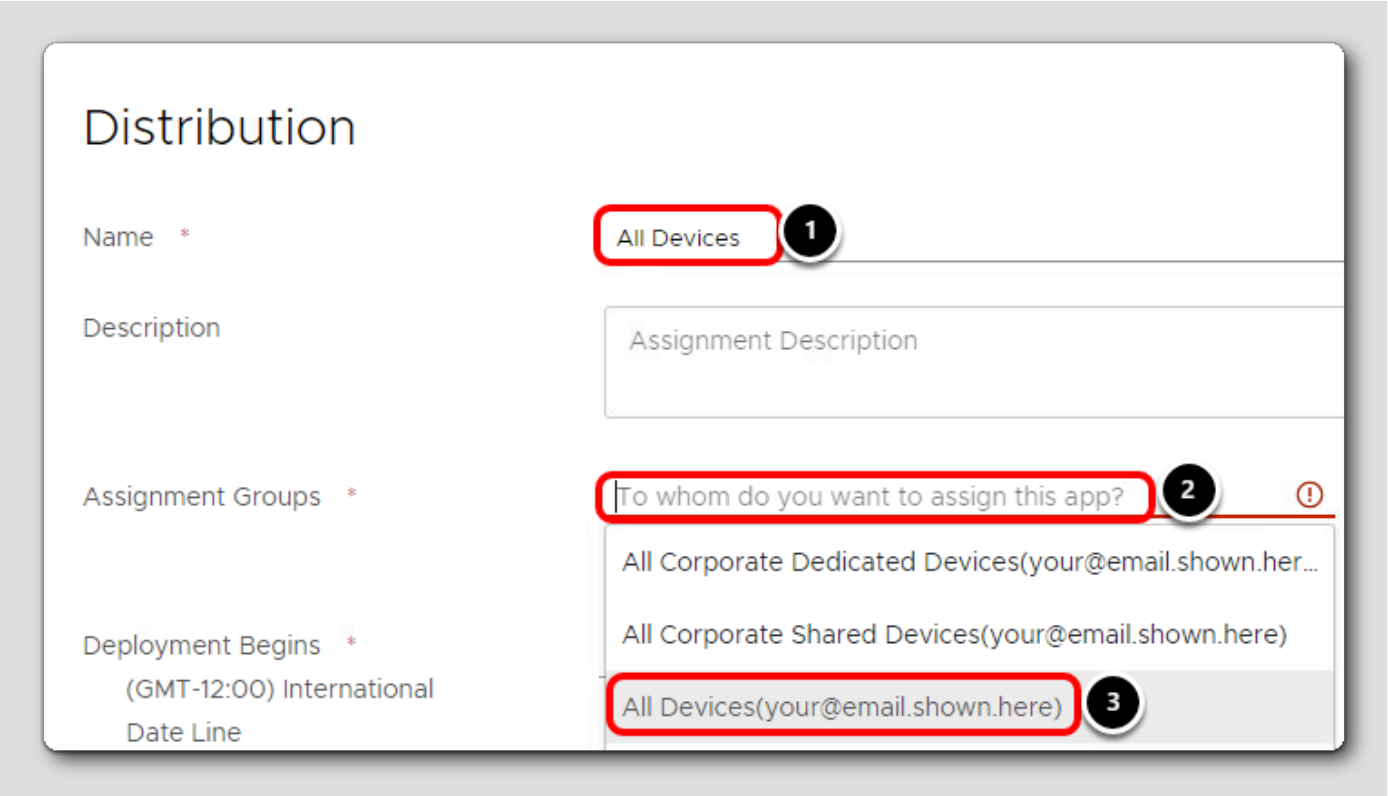
[87]



Click **Save & Assign**.

Configure Assignment Distribution

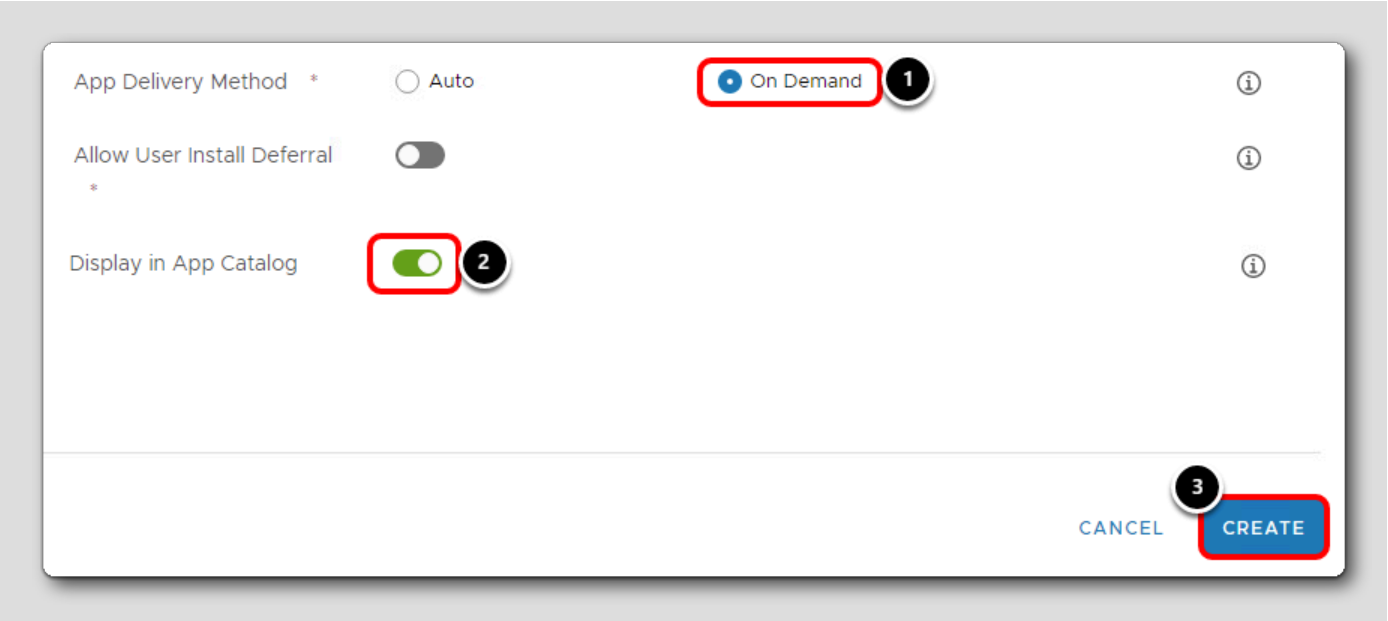
[88]



1. Enter **`All Devices`** for the Name.
2. Click the **Assignment Groups** field.
3. Select **All Devices (your@email.shown.here)** from the list.

Add Assignment Group and Push Mode

[89]

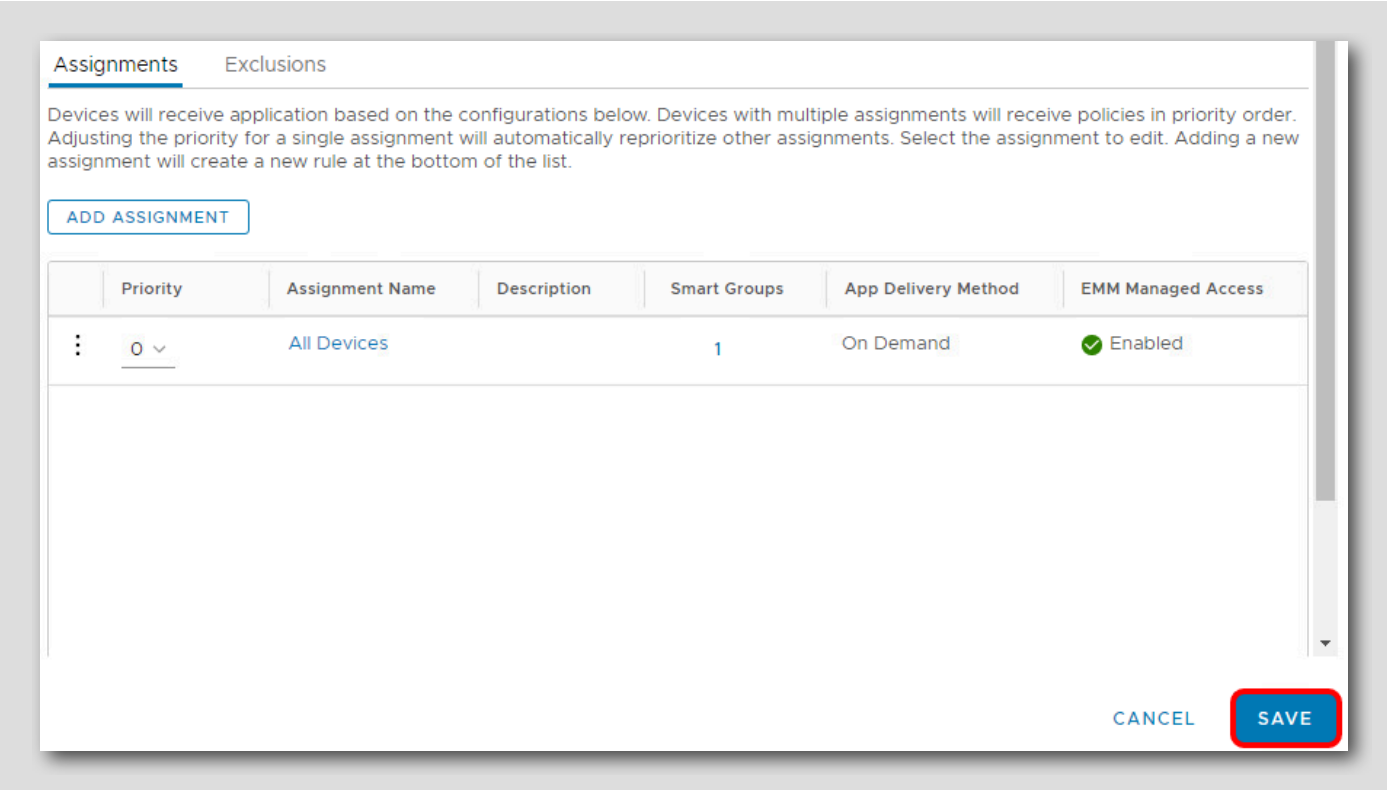


1. Select **On Demand** for the **App Delivery Method**. This will make the app available to your assigned users in the app catalog.
2. **Enable** the **Display in App Catalog** setting.
3. Click **Create**.

Note: You now have the ability to choose if the app is displayed in the app catalog or not. This is helpful when deploying driver updates or scripted actions and don't want the end-user to see this in the catalog.

Save the Assignments

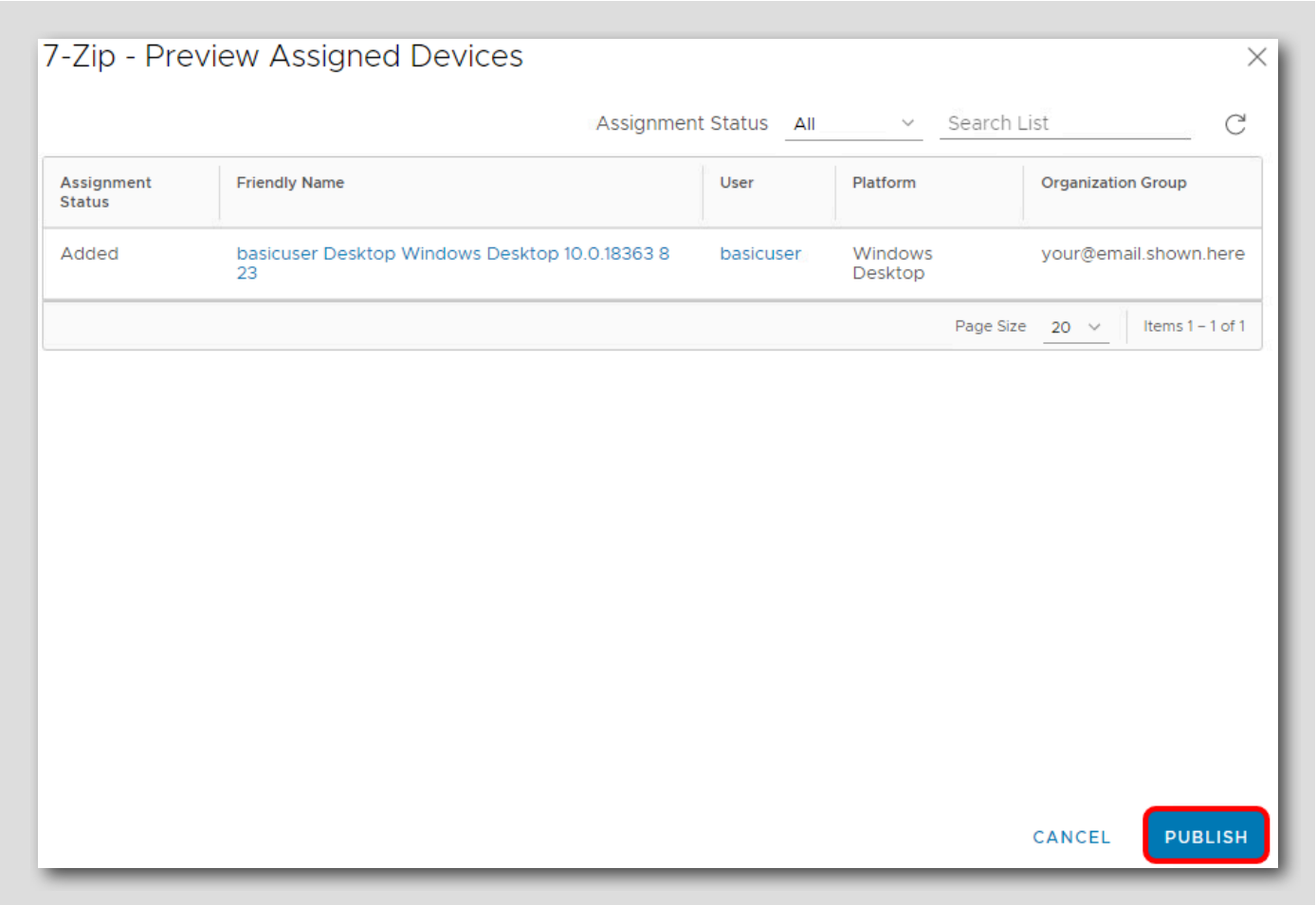
[90]



Click **Save** to save the app assignments.

Publish the Application

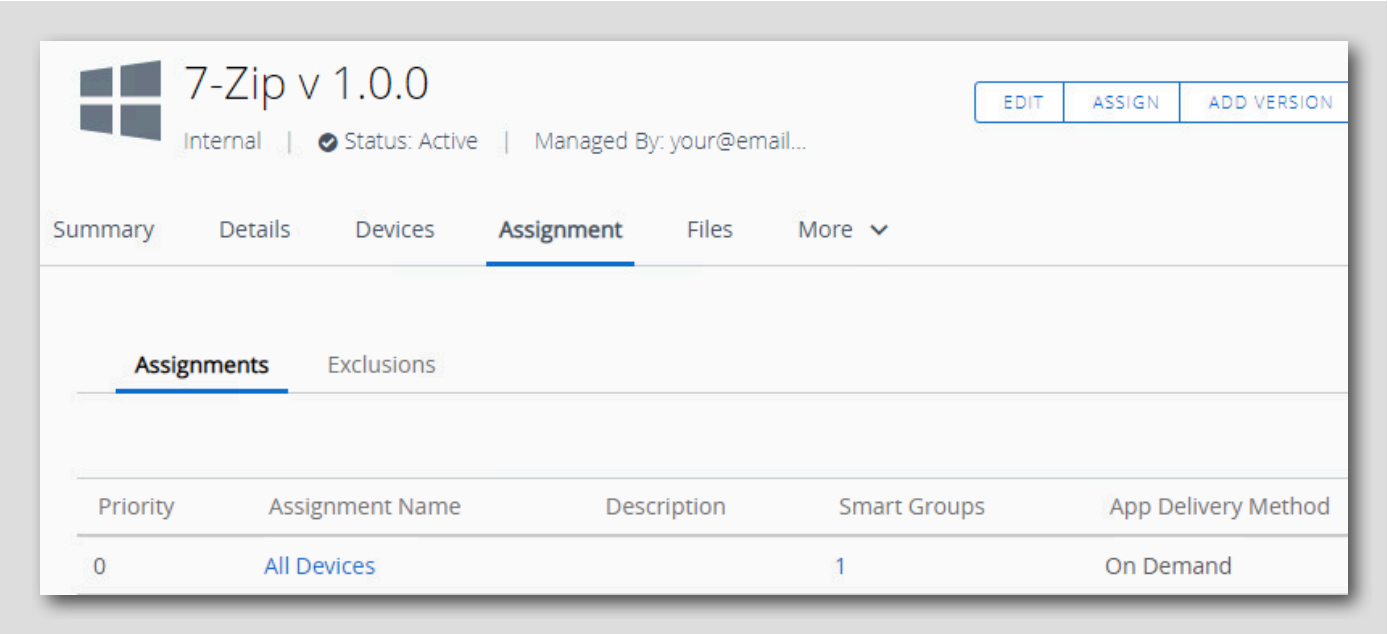
[91]



Click **Publish** to publish the application to the list of devices shown.

Confirm App Creation

[92]



The 7-Zip application has been created and assigned to the All Devices smart group as an On Demand app, meaning it will not be automatically installed on the end user device when it is enrolled. This allows the app to be installed by the end user through the app catalog or by an administrator through the Workspace ONE UEM administrator console.

Continue to the next step.

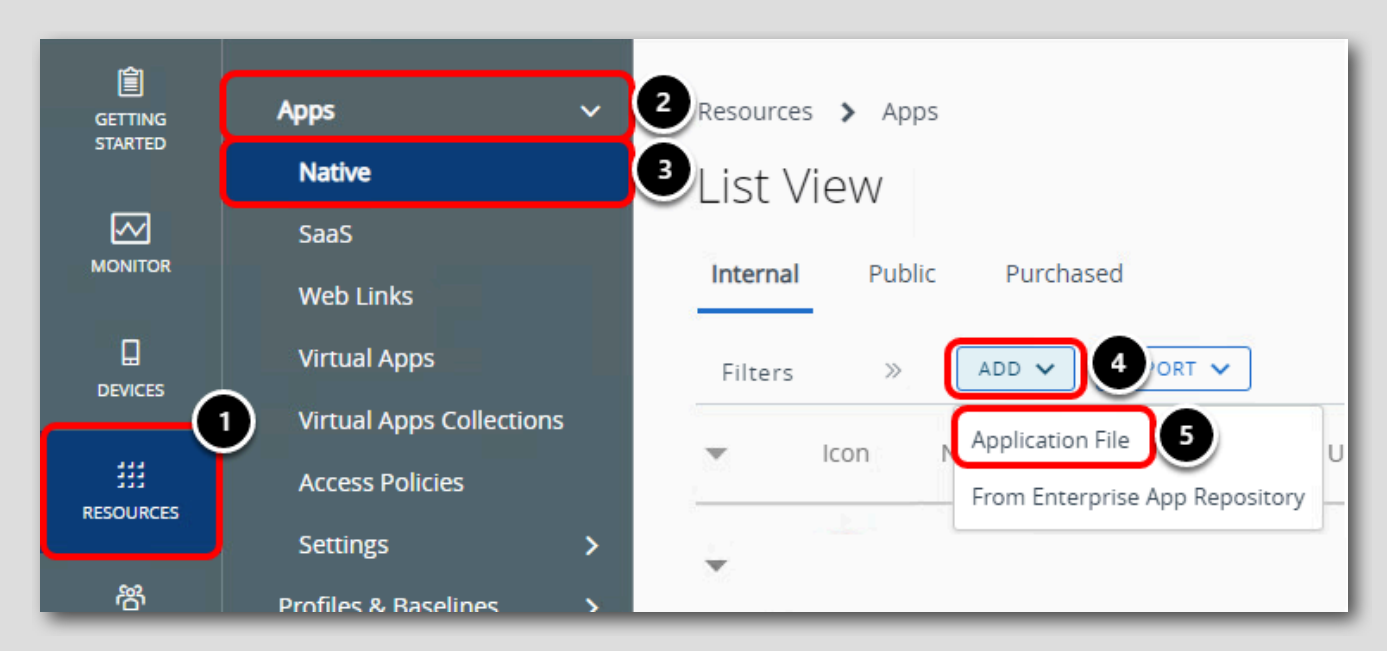
Delivering Auto Apps on Windows 10

[93]

You will now distribute an Auto app, which will automatically download and install the app to the user's device without requiring them to interact with the app within the Intelligent Hub app catalog.

Add Internal Application

[94]

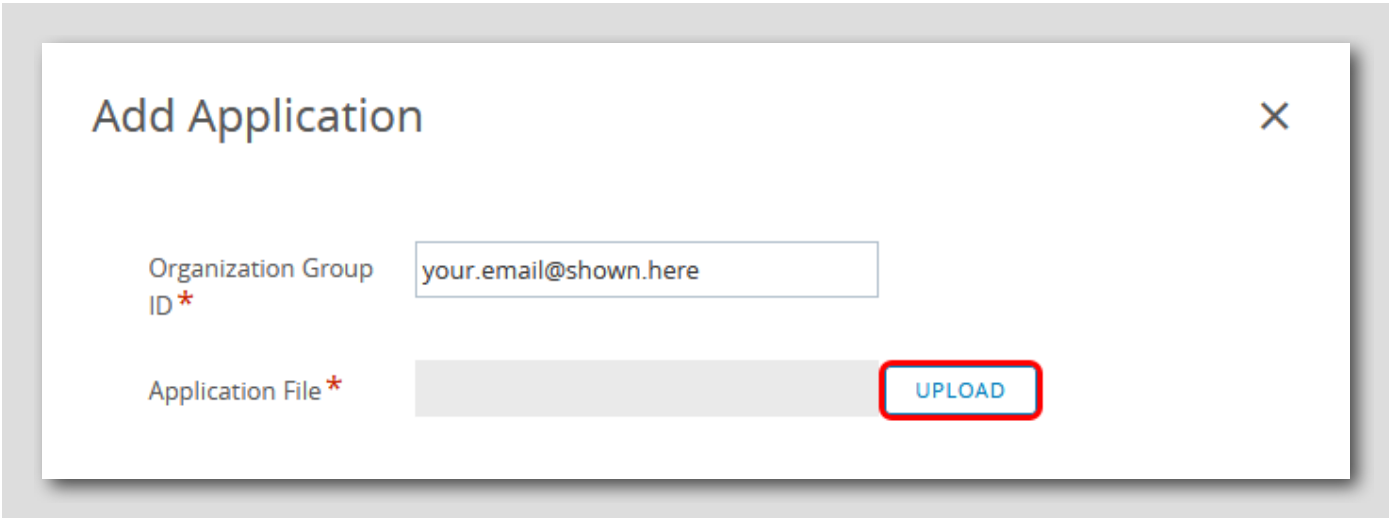


In the Workspace ONE UEM Administrator Console:

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

Upload Application

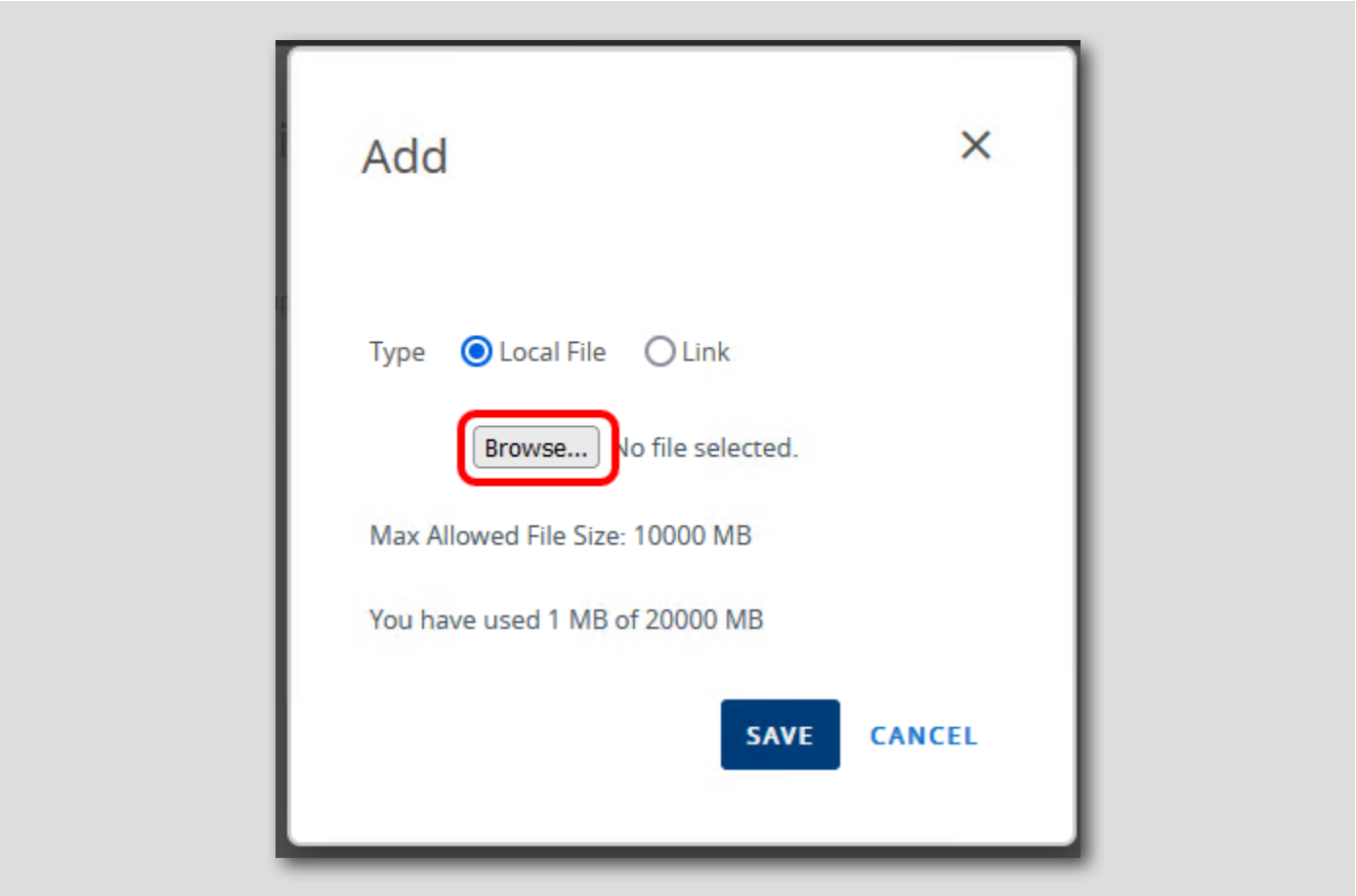
[95]



Click **Upload**.

Find the Application MSI

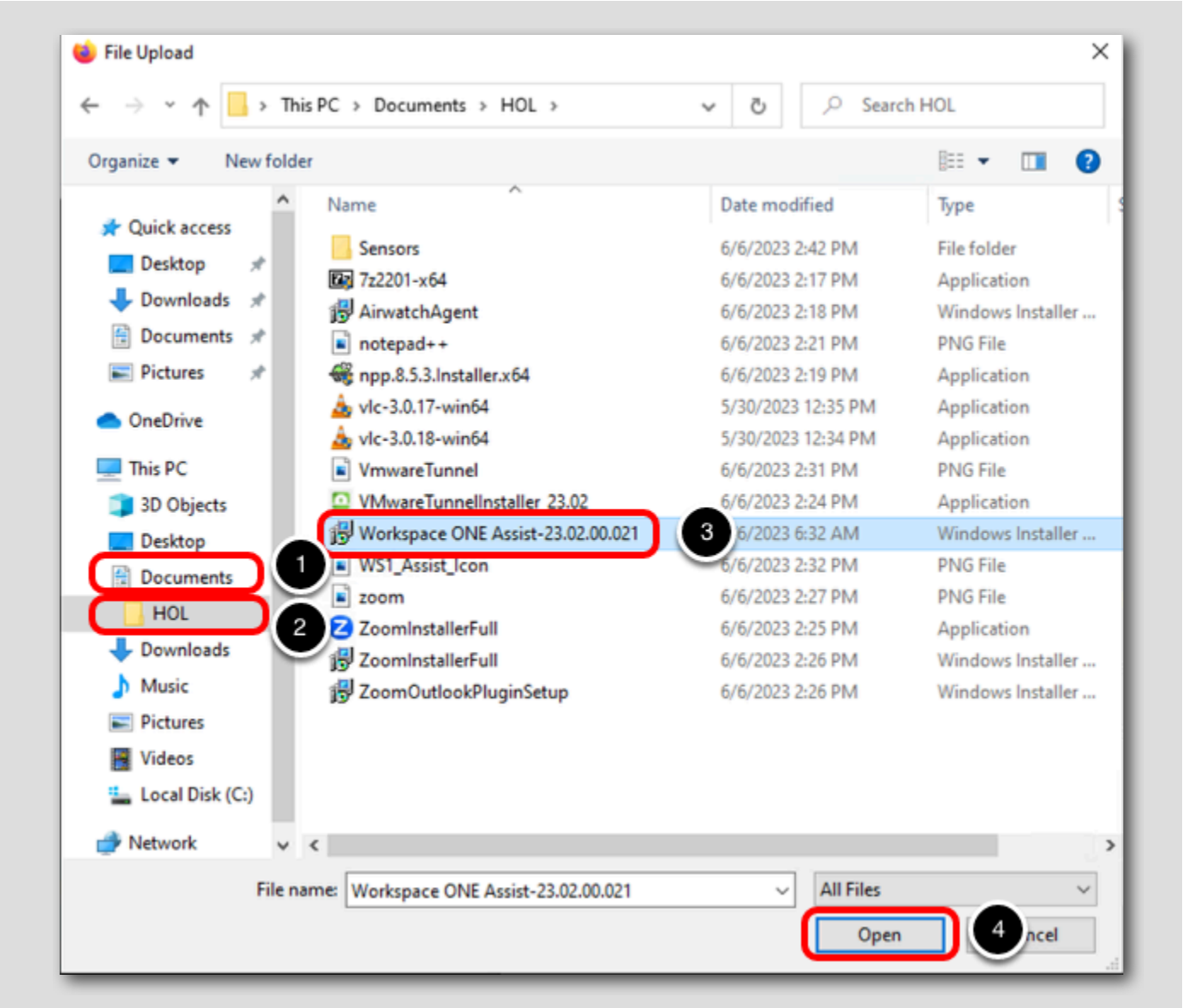
[96]



Click the **Browse** button.

Upload the Workspace ONE Assist MSI File

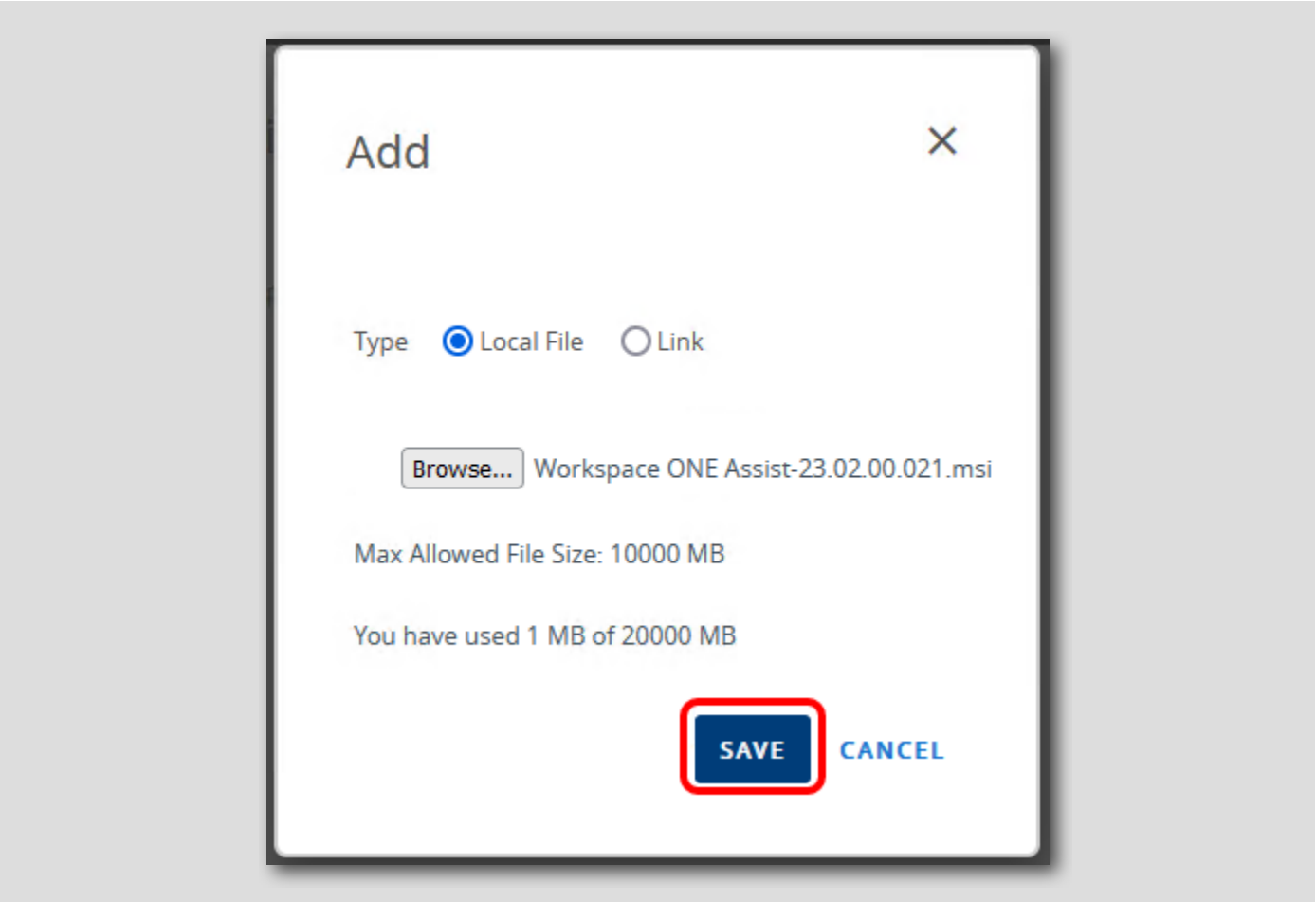
[97]



1. Click **Documents**
2. Click **HOL**
3. Select the **Workspace ONE Assist-23.02.00.021.msi** file
4. Click **Open**

Save the MSI File

[98]

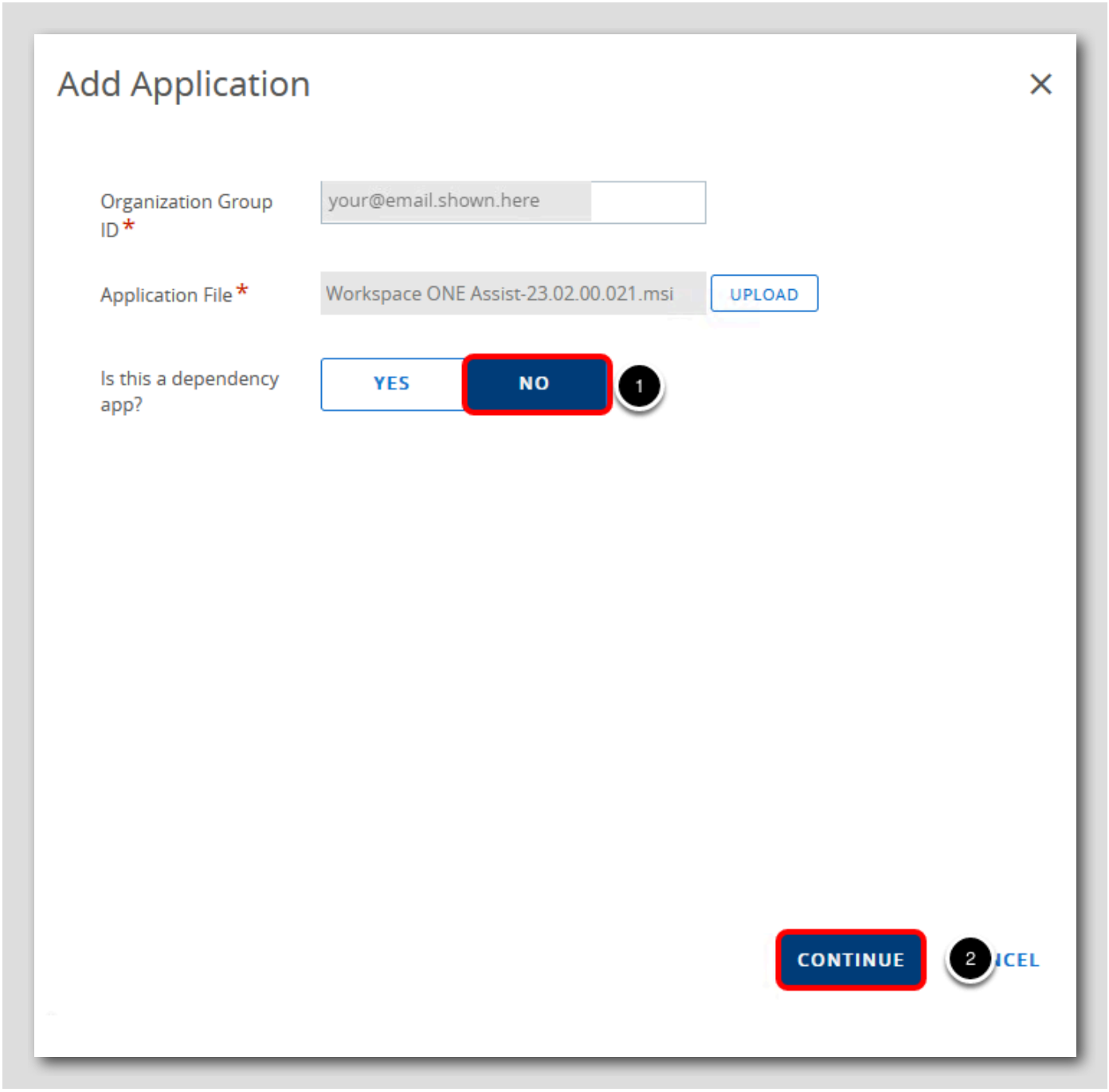


Click **Save**.

NOTE: The app upload may take a few minutes to complete! Continue to the next step once the upload completes. If you see "An error has occurred HTTP Status Code 0" please try the upload again as internet bandwidth is variable.

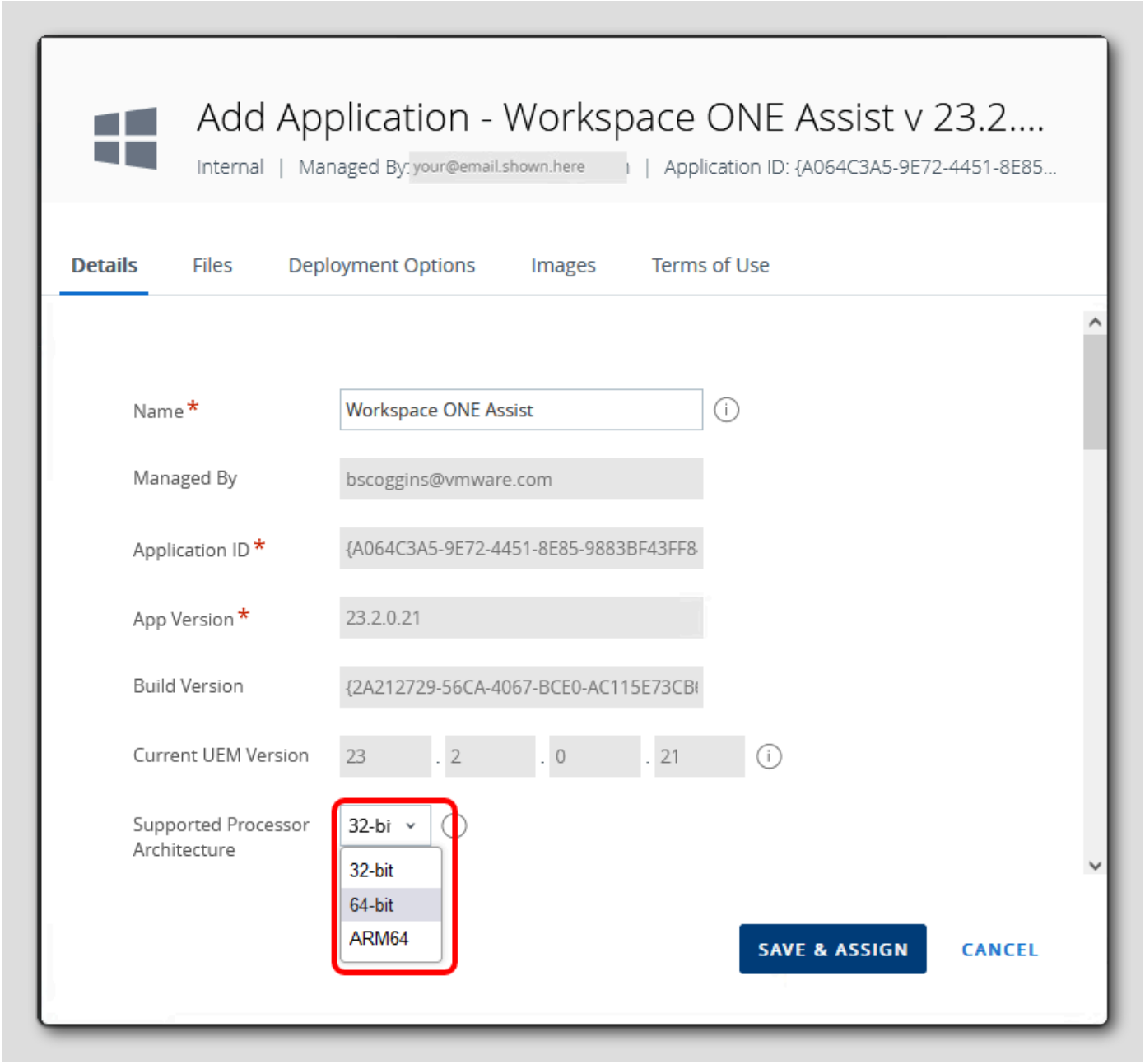
Continue to the App Settings

[99]



1. Select **No** for **Is this a dependency app?**
2. Click **Continue**.

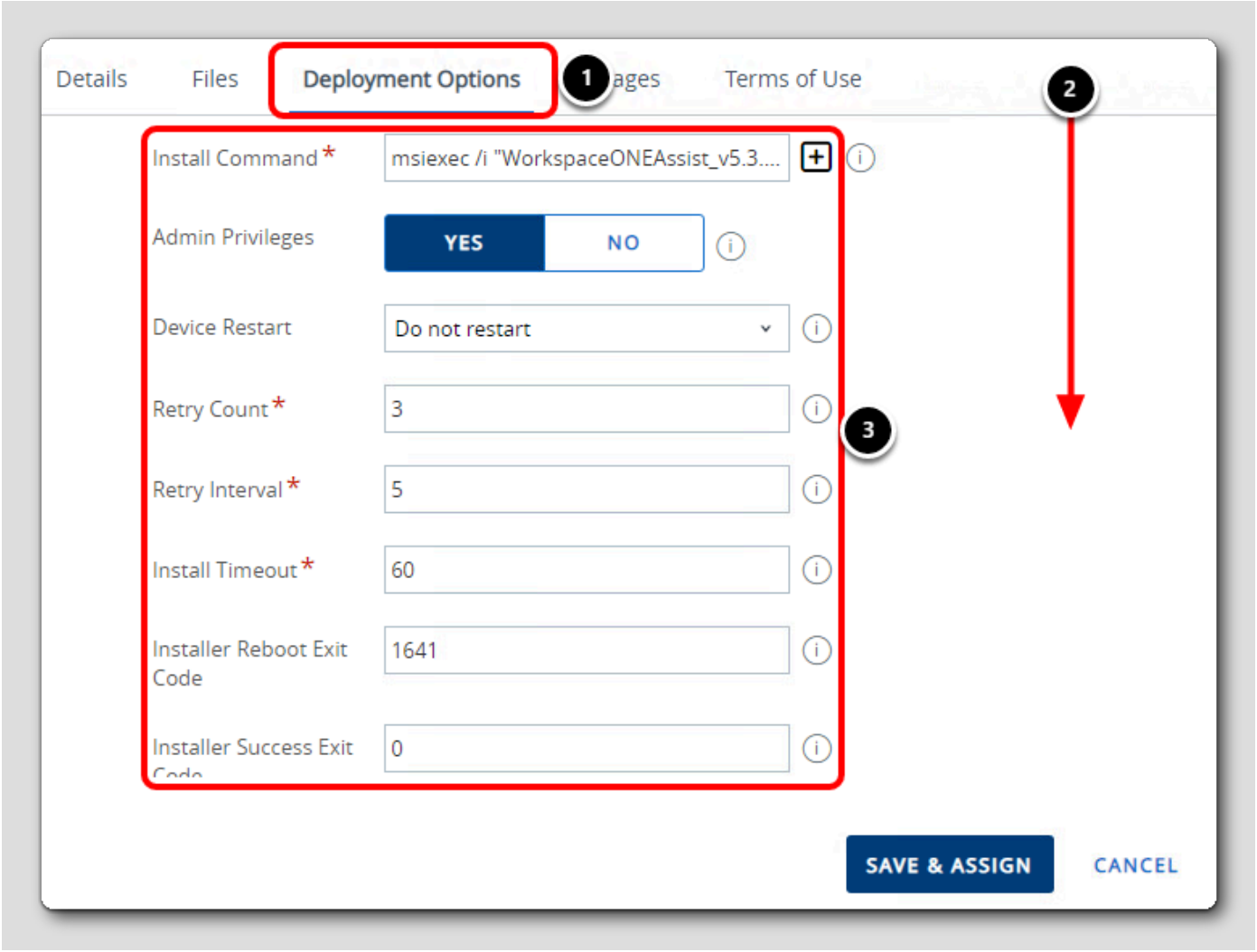
Configure App Details



Select **64-bit** for the **Supported Processor Architecture**.

Confirm Deployment Options

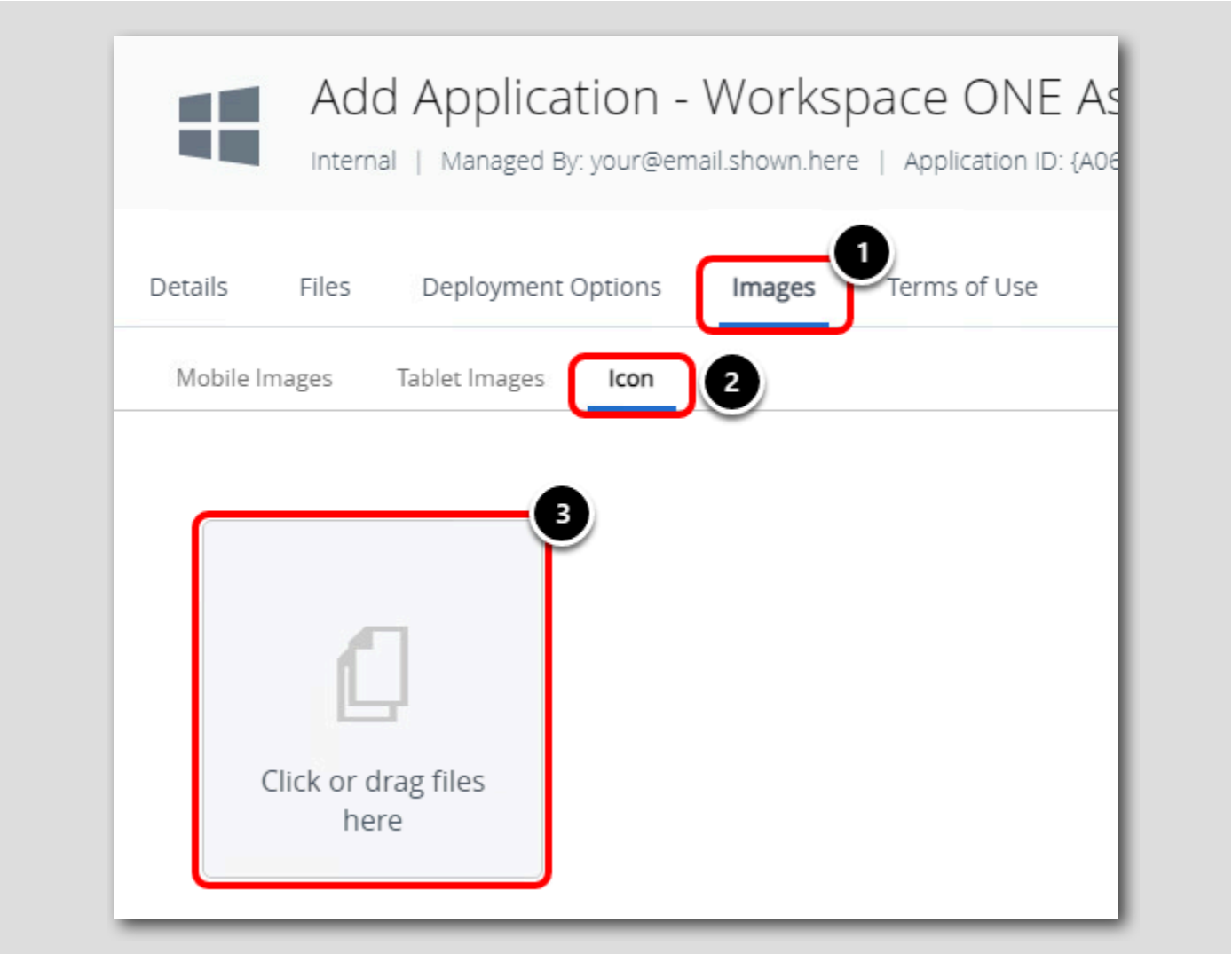
[101]



1. Select the **Deployment Options** tab.
2. Scroll down to find the **How To Install** section.
3. Notice that the **Install Command** and **installer codes** have been entered automatically from the details within the MSI, unlike when working with the EXE file previously.

Add Application Image

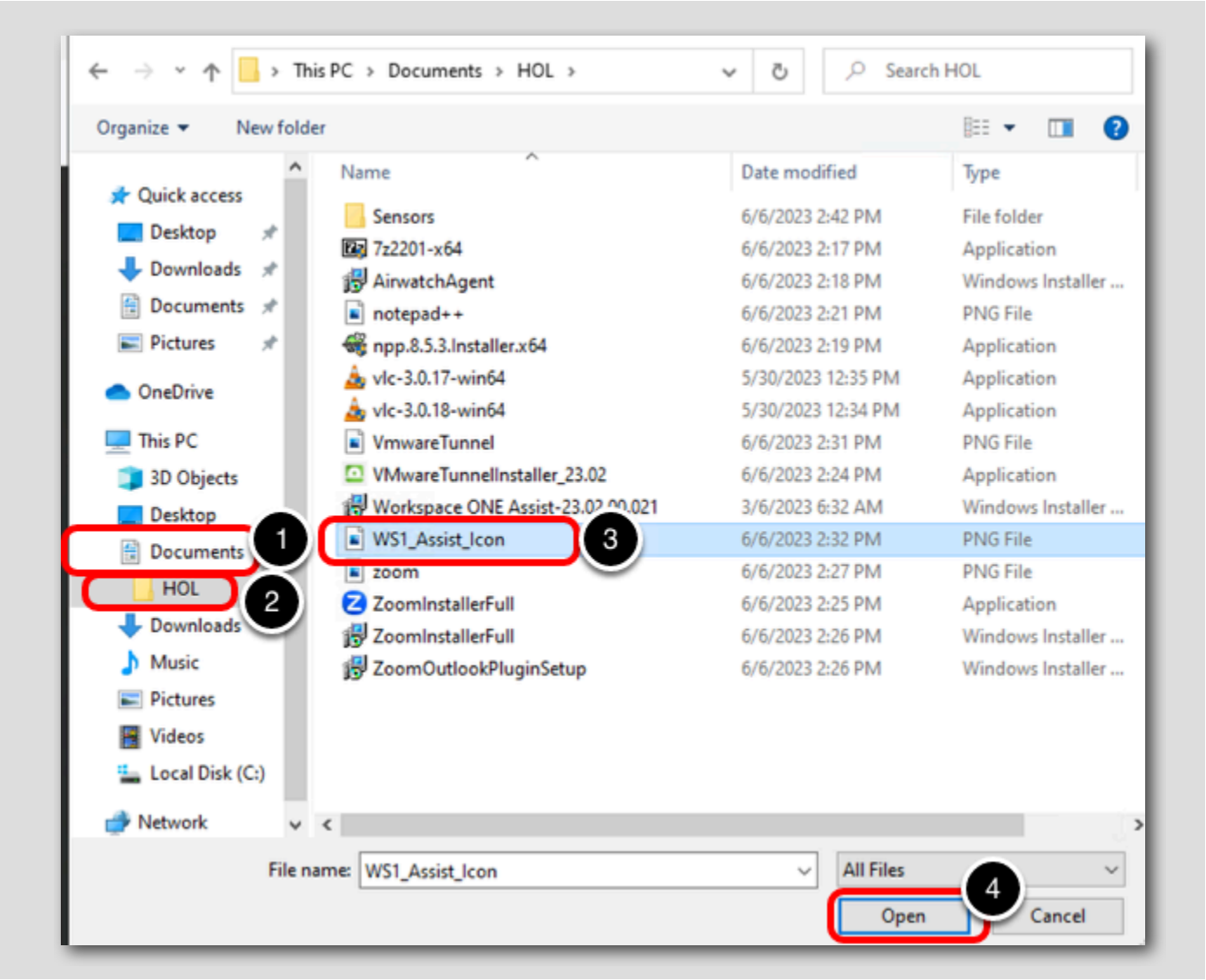
[102]



1. Click the **Images** tab
2. Click the **Icon** tab
3. Click the area labeled **Click or drag files here**

Upload the Workspace ONE Assist Icon

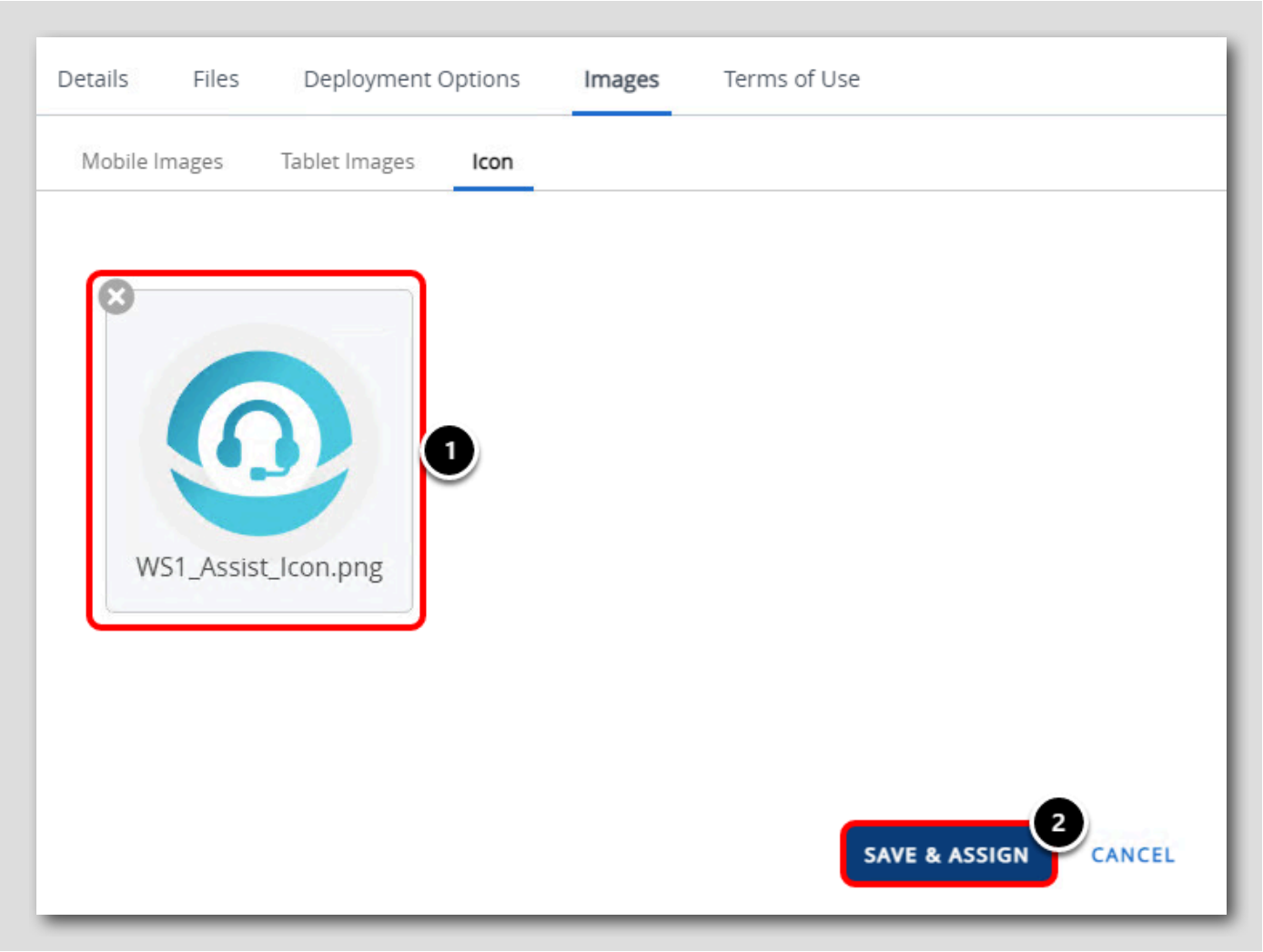
[103]



1. Click **Documents**
2. Click **HOL**
3. Click to select **WS1_Assist_Icon.png**
4. Click **Open**

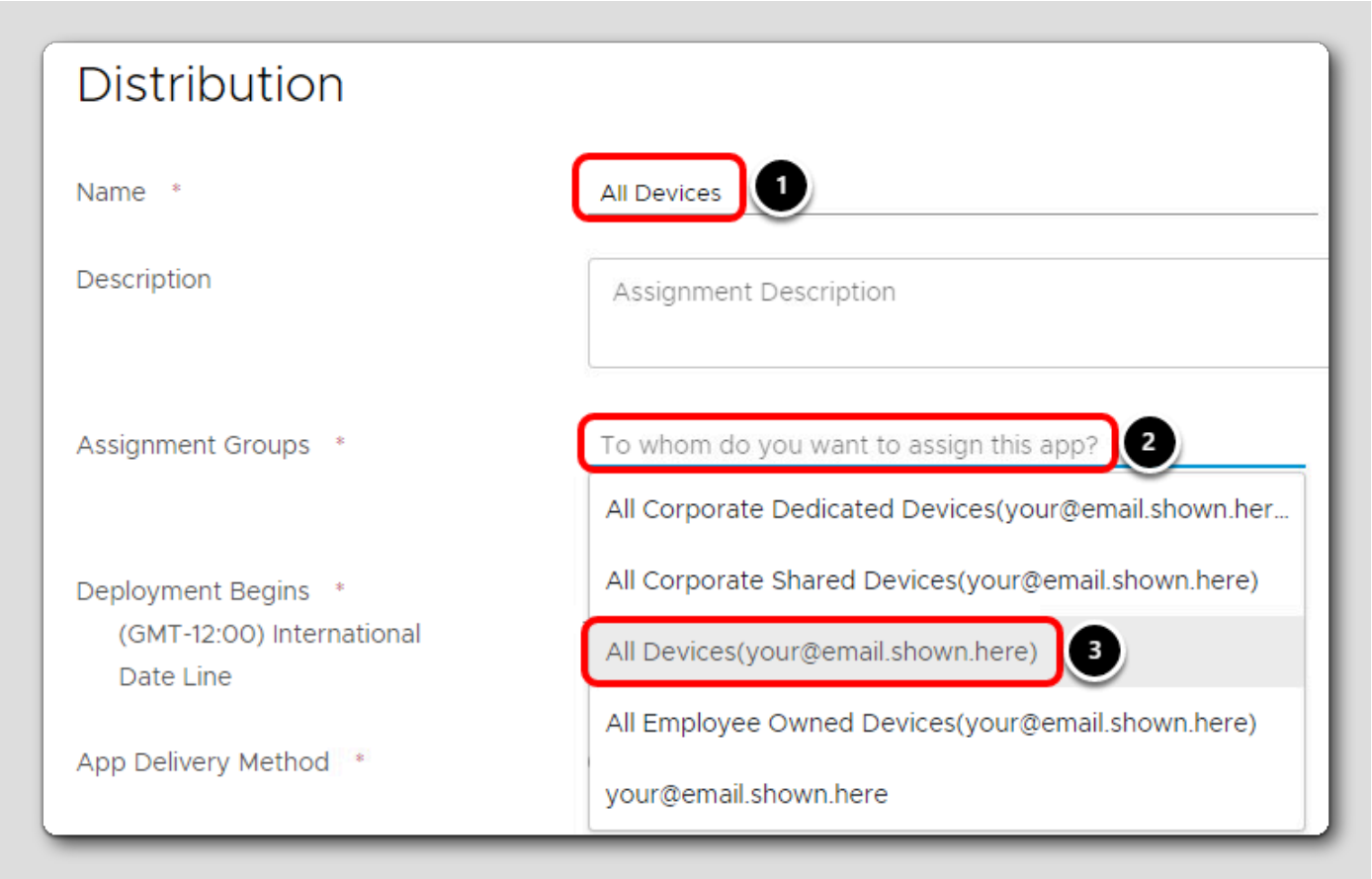
Proceed to Save and Assign

[104]



1. Confirm that the Workspace ONE Assist icon was successfully uploaded
2. Click **Save & Assign**

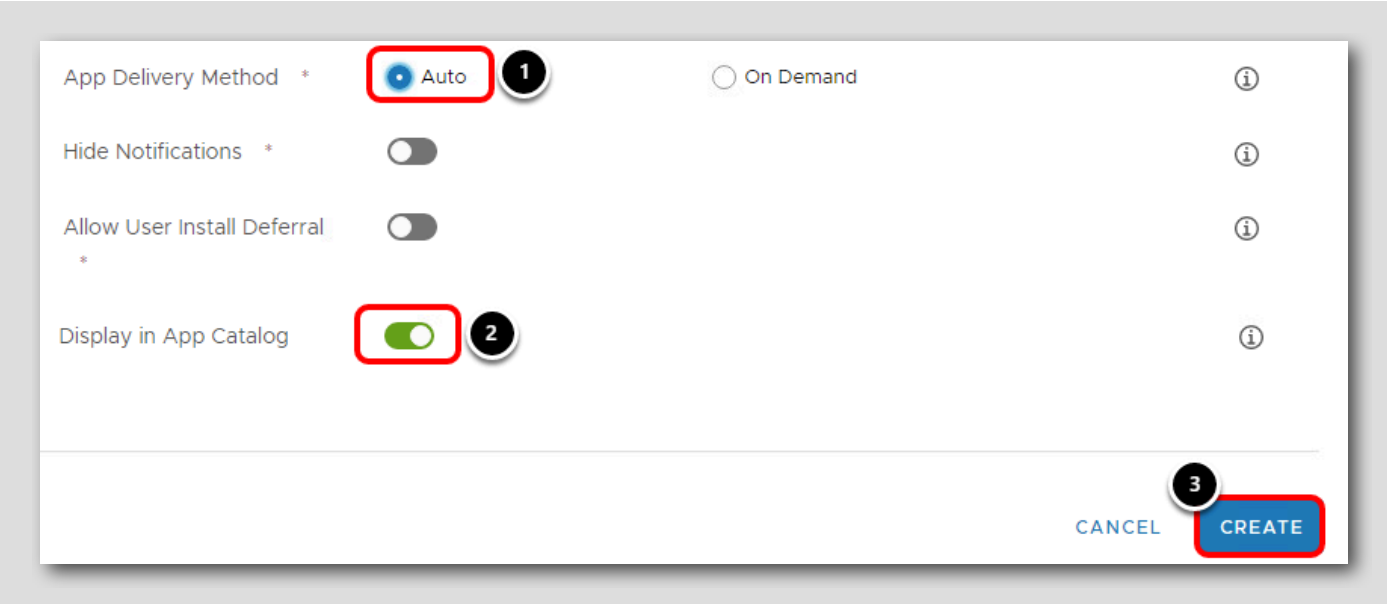
Save and Assign the Application



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

Configure App Delivery Method

[106]

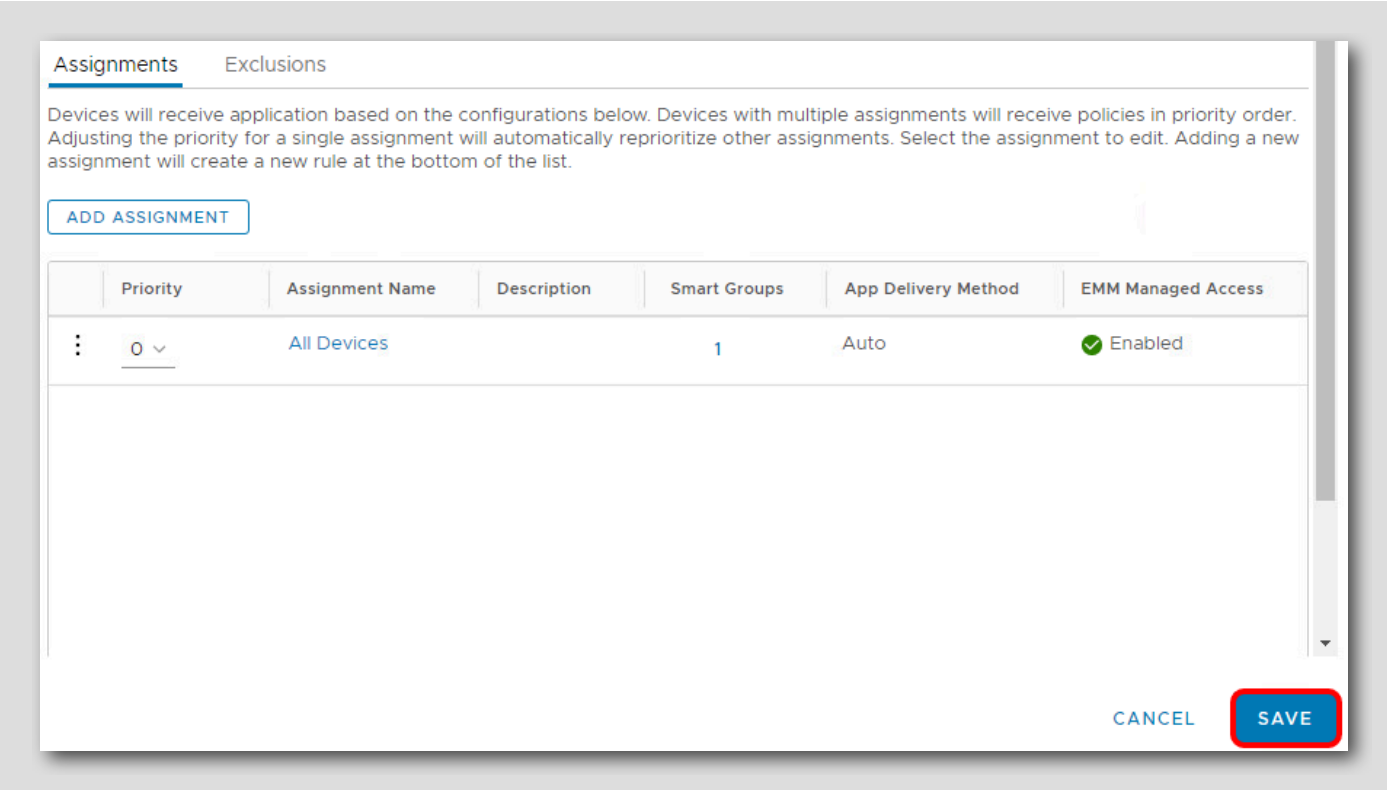


1. Select **Auto** for the **App Delivery Method**. This will automatically deploy and install the app for your users, making it available right away without any interaction with the app catalog.
2. **Enable** the **Display in App Catalog** setting.
3. Click **Create**.

NOTE: You now have the ability to choose if the app is displayed in the app catalog or not. This is helpful when deploying driver updates or scripted actions and don't want the end-user to see this in the catalog.

Save the Assignments

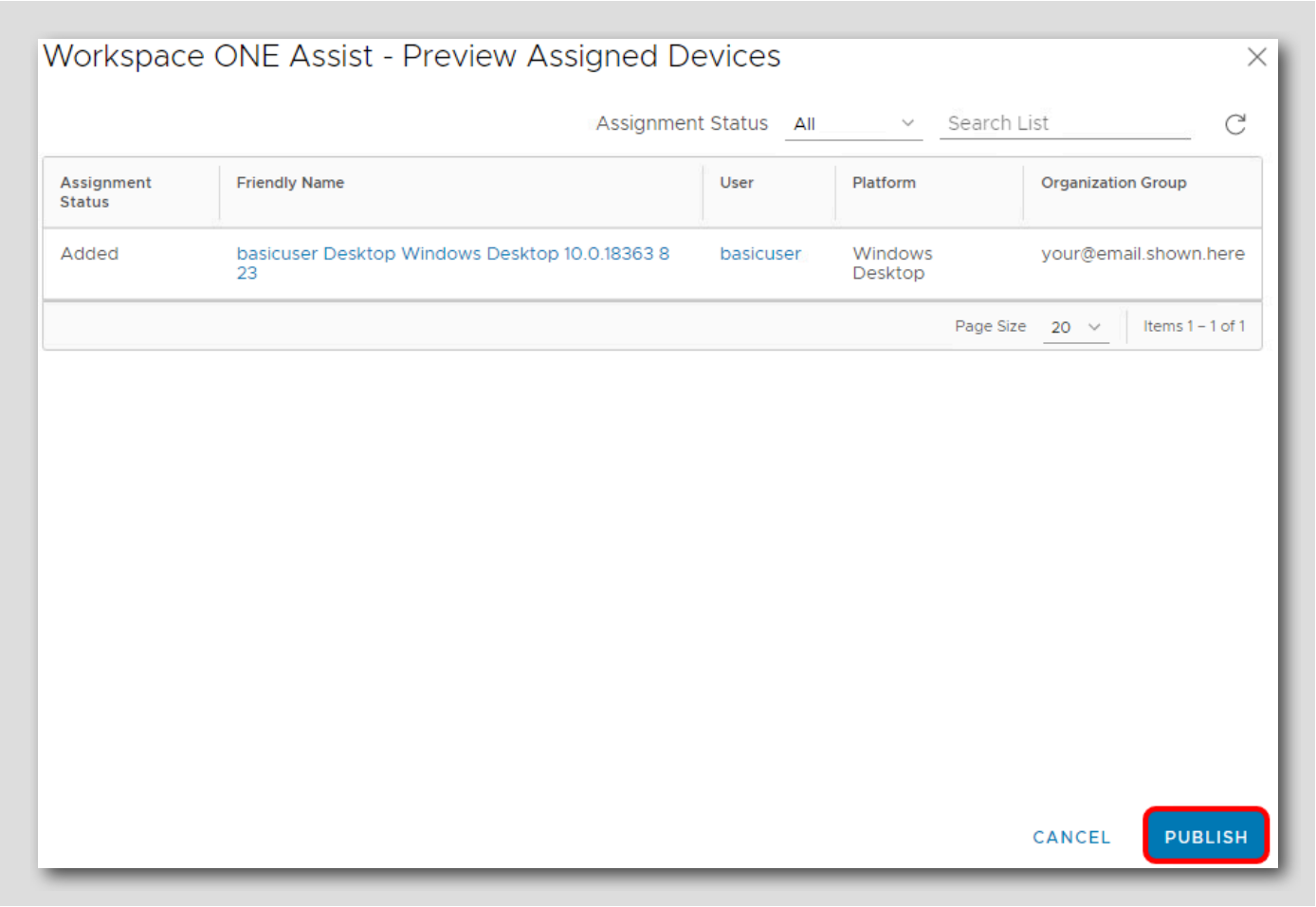
[107]



Click **Save** to save the app assignments.

Publish the Application

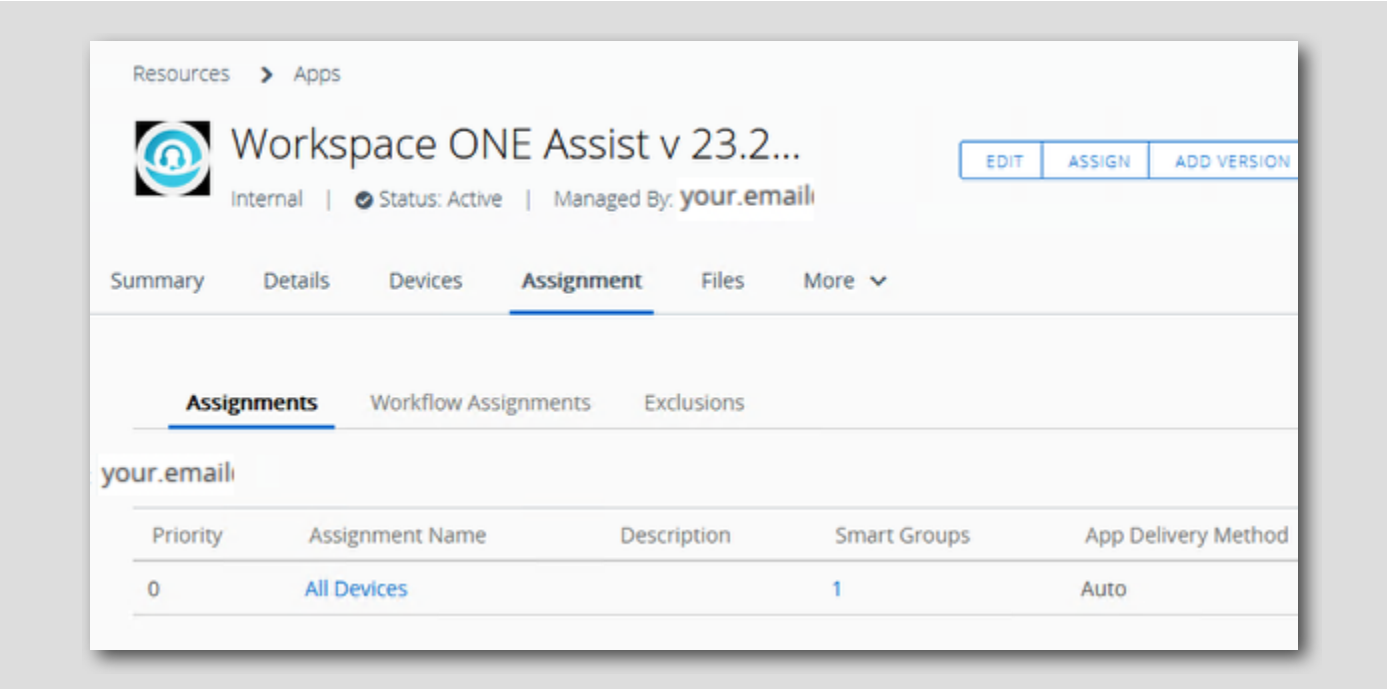
[108]



Click **Publish** to publish the application to the list of devices shown.

Confirm App Creation

[109]



The Workspace ONE Assist application has been created and assigned to the All Devices smart group and the App Delivery Method was set to Auto, meaning the app will be automatically downloaded and installed without requiring any user interaction when a Windows 10 device is enrolled into the organization.

Continue to the next step.

Validate Device Enrollment

[110]

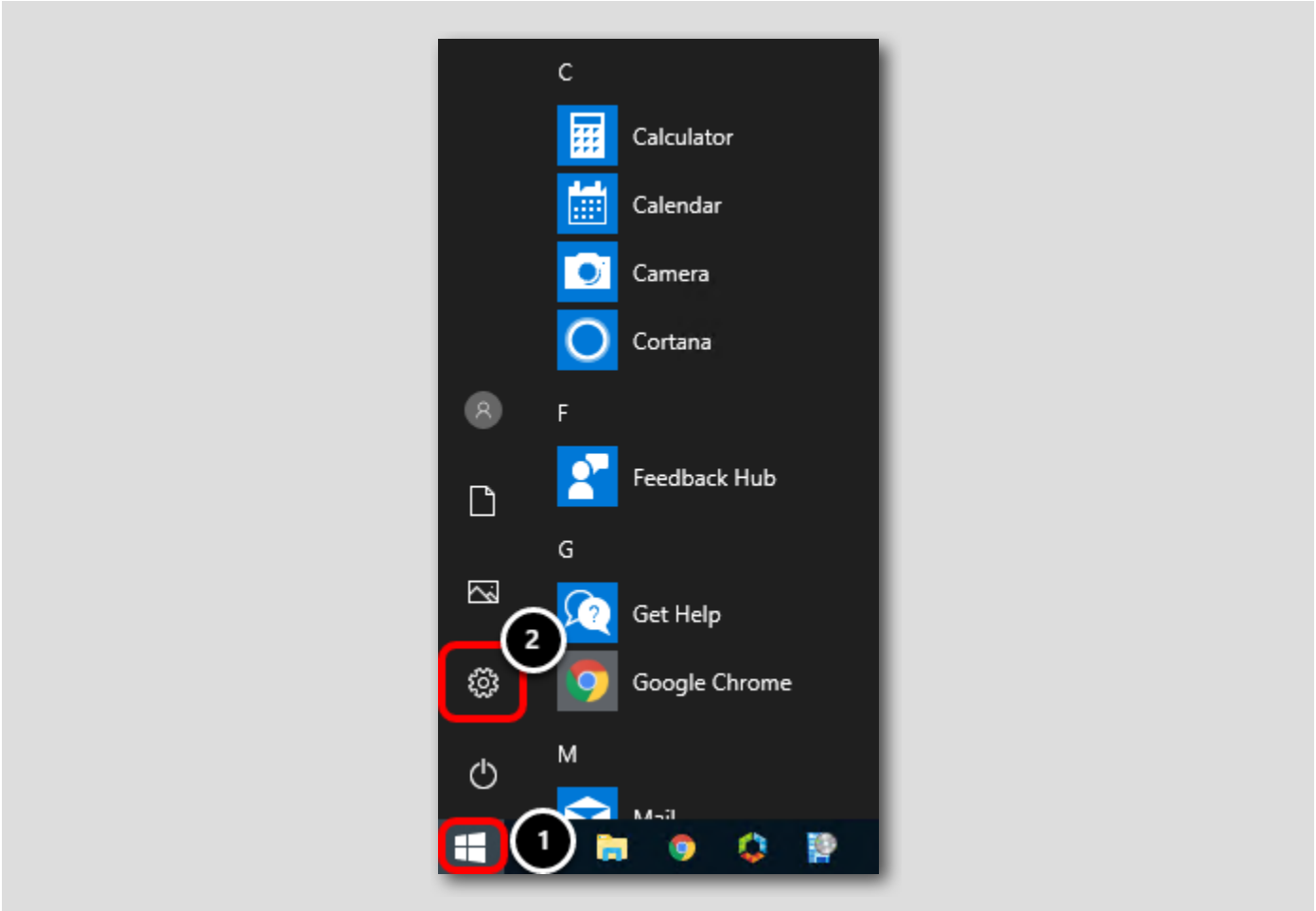
Your device was enrolled and received three configurations:

1. A Restriction Profile which prevents end users from unenrolling the Windows 10 device
2. The 7-Zip app was deployed as an On Demand app
3. The Workspace ONE Assist app was deployed as an Auto app

You will now confirm that the Restriction Profile was installed by verifying that the restrictions are applied on your device and that the two apps are available according to their deployment type (On Demand vs. Auto).

Review New Unenrollment Settings

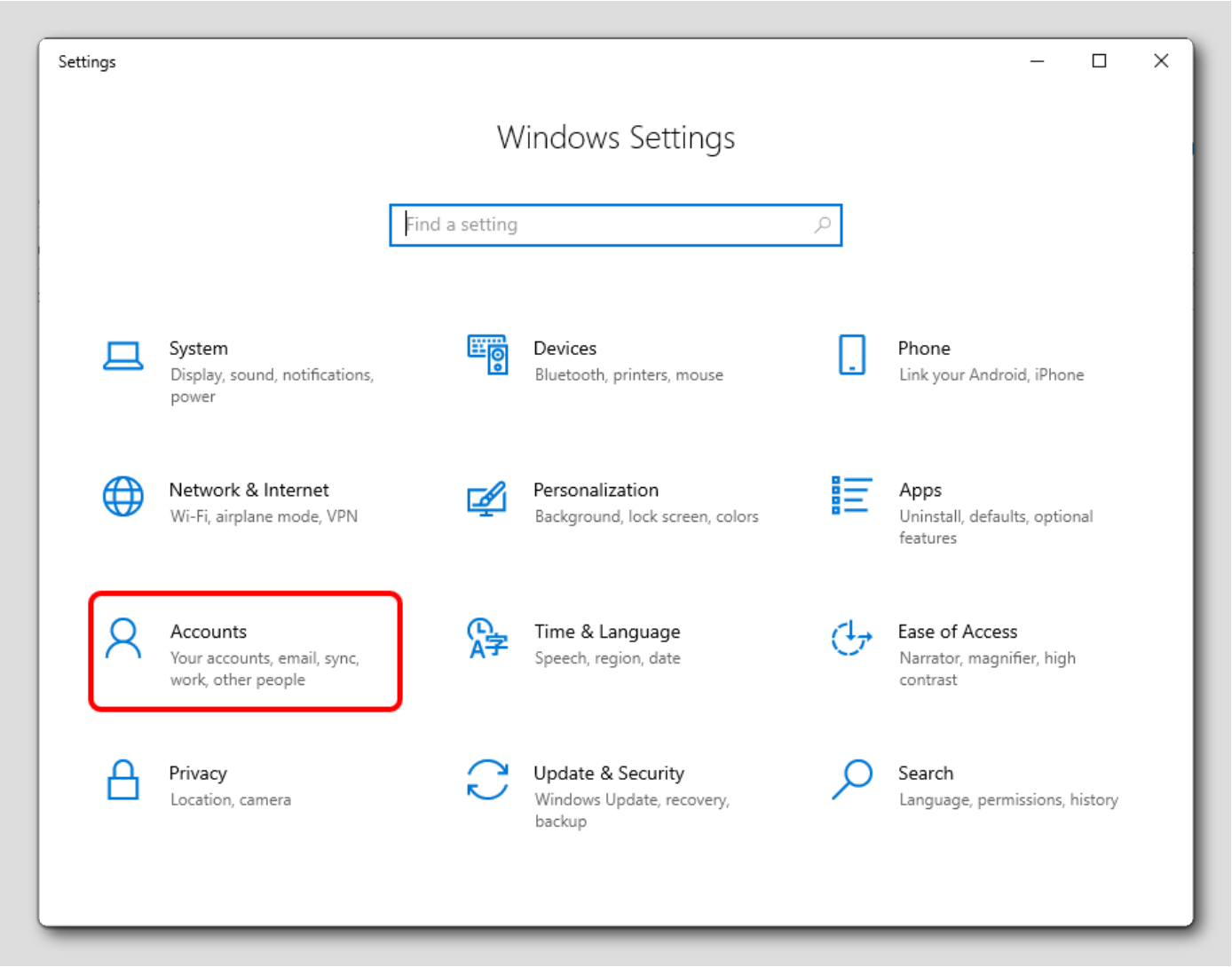
[111]



1. Click the **Windows Start** button
2. Click the **Windows Settings** button

Accounts

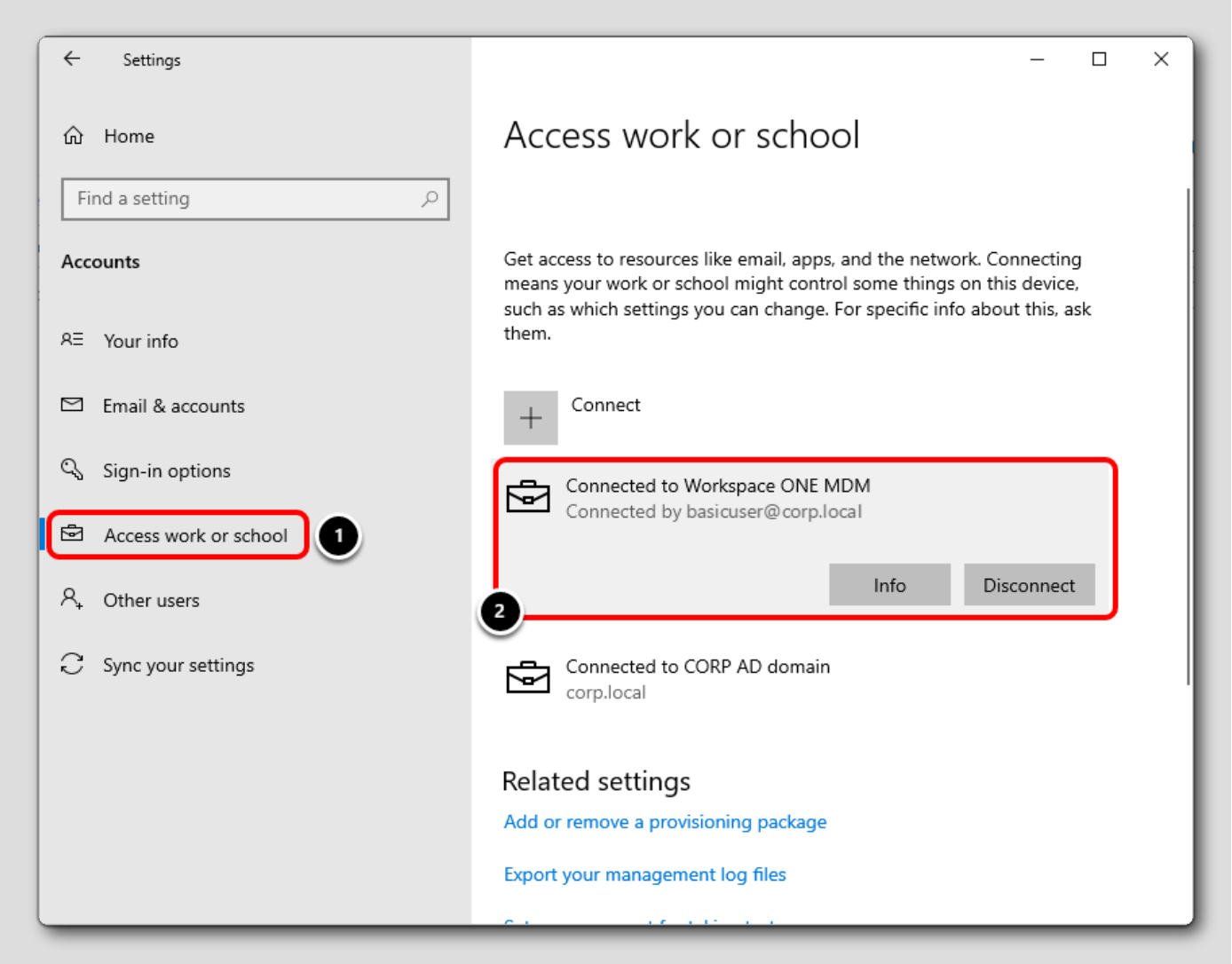
[112]



Click on **Accounts**.

Access Work or School

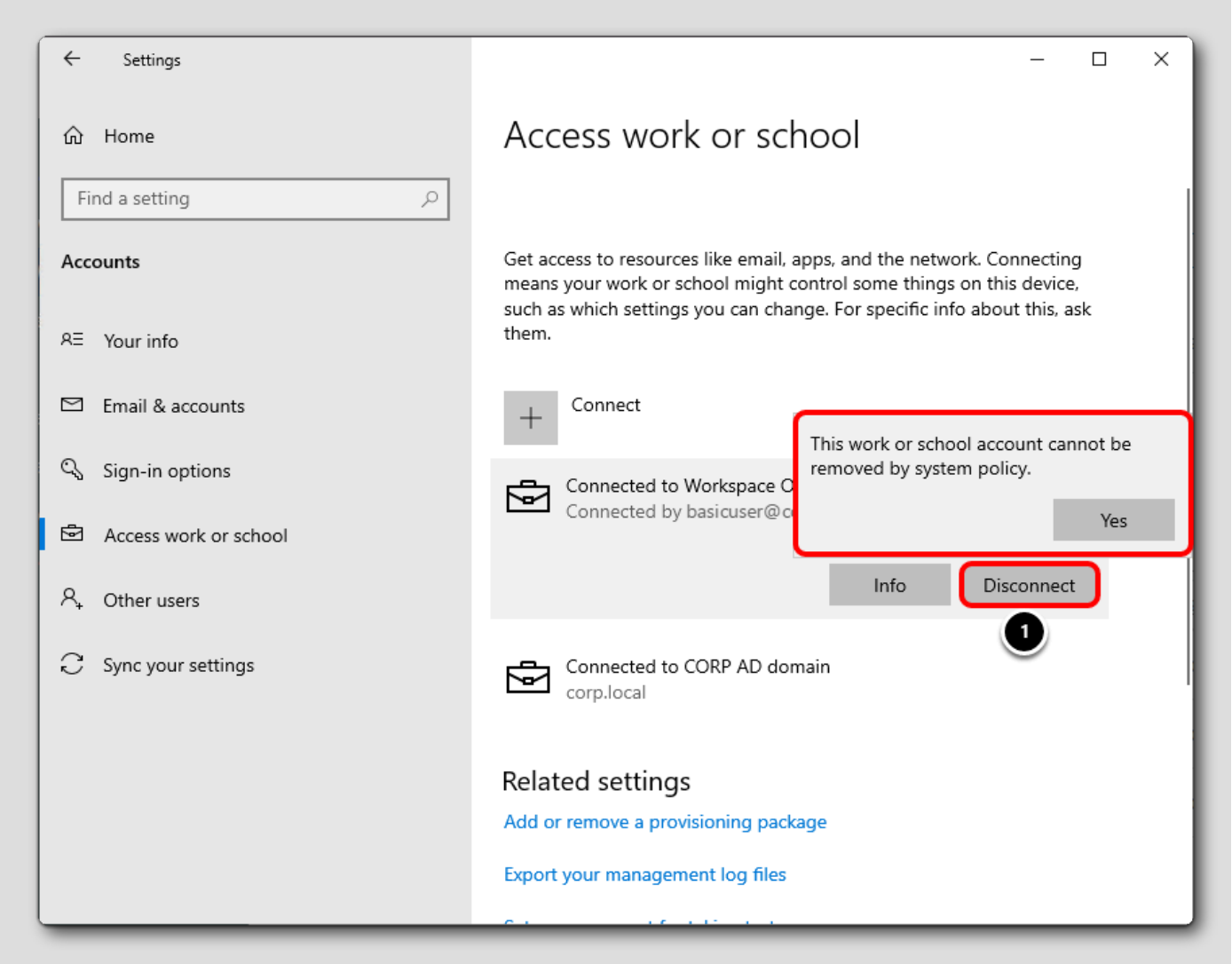
[113]



1. Click on **Access work or school**.
2. Click on **Connected to Workspace ONE MDM**.

End-User Can't Unenroll

[114]

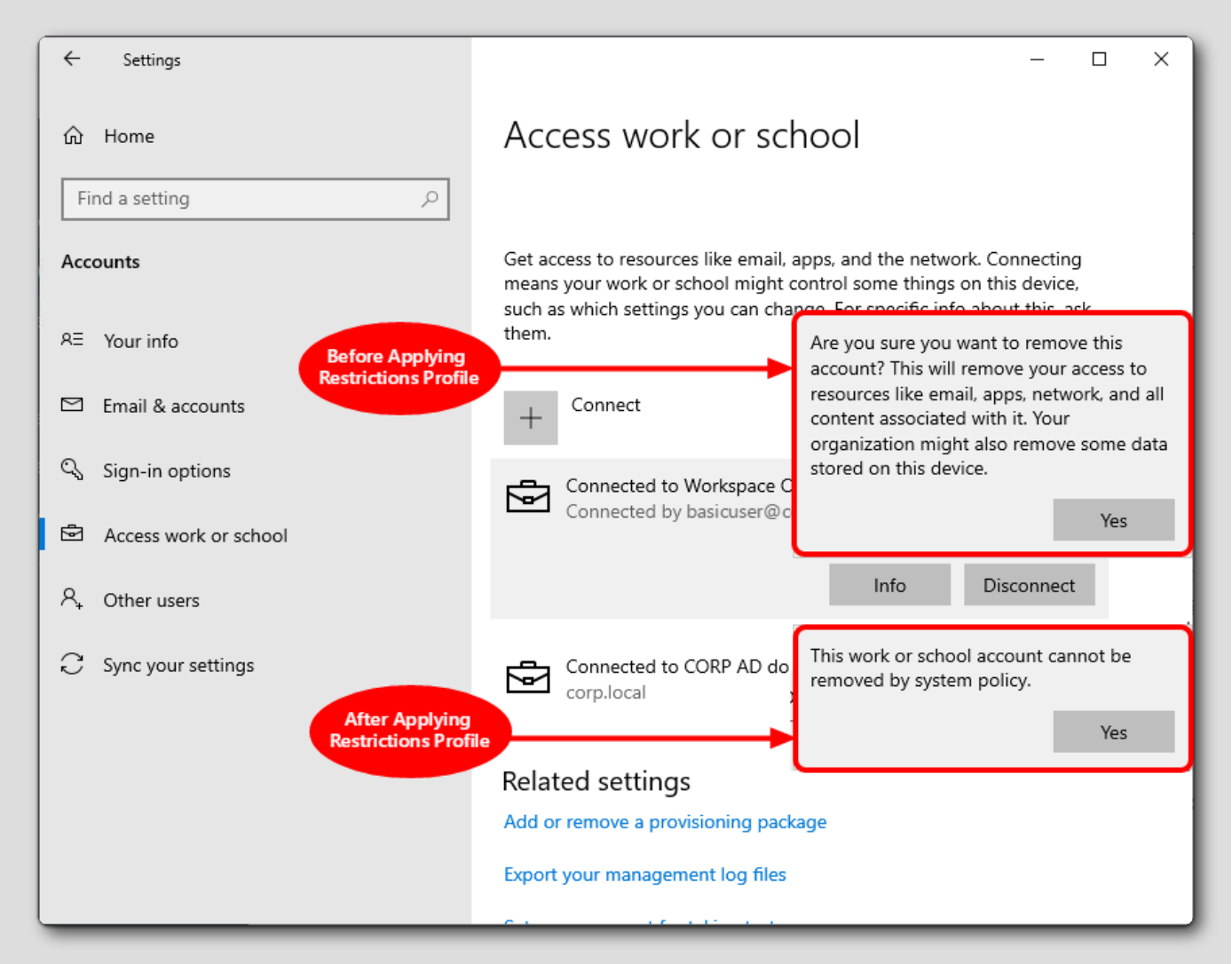


1. Click **Disconnect**.

Notice, the end-user now does not have the ability to unenroll their device from Workspace ONE UEM management.

Before and After Restrictions

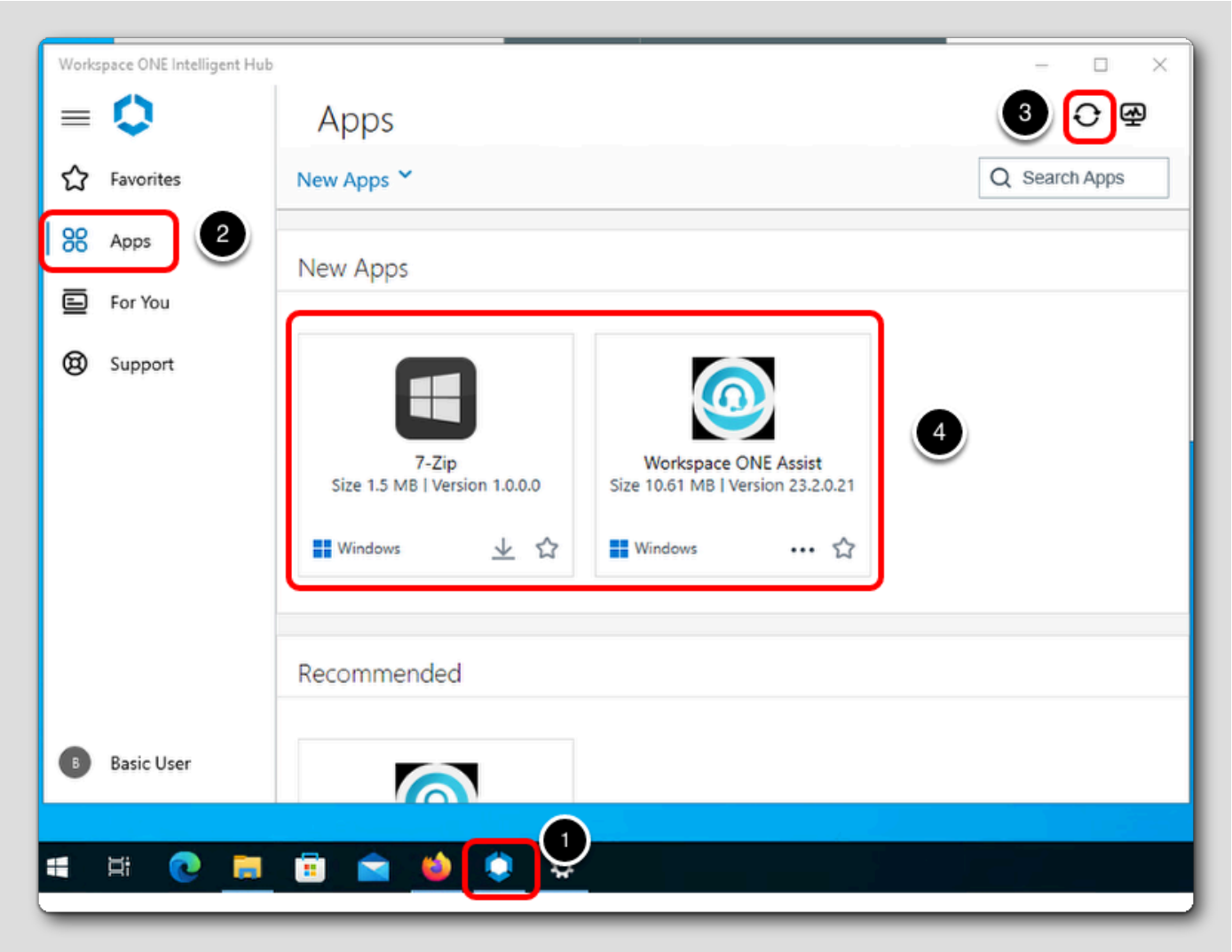
[115]



Here you can see the before and after results of applying the Allow or Don't Allow MDM Unenrollment policy on the Windows 10 device.

Confirm Applications

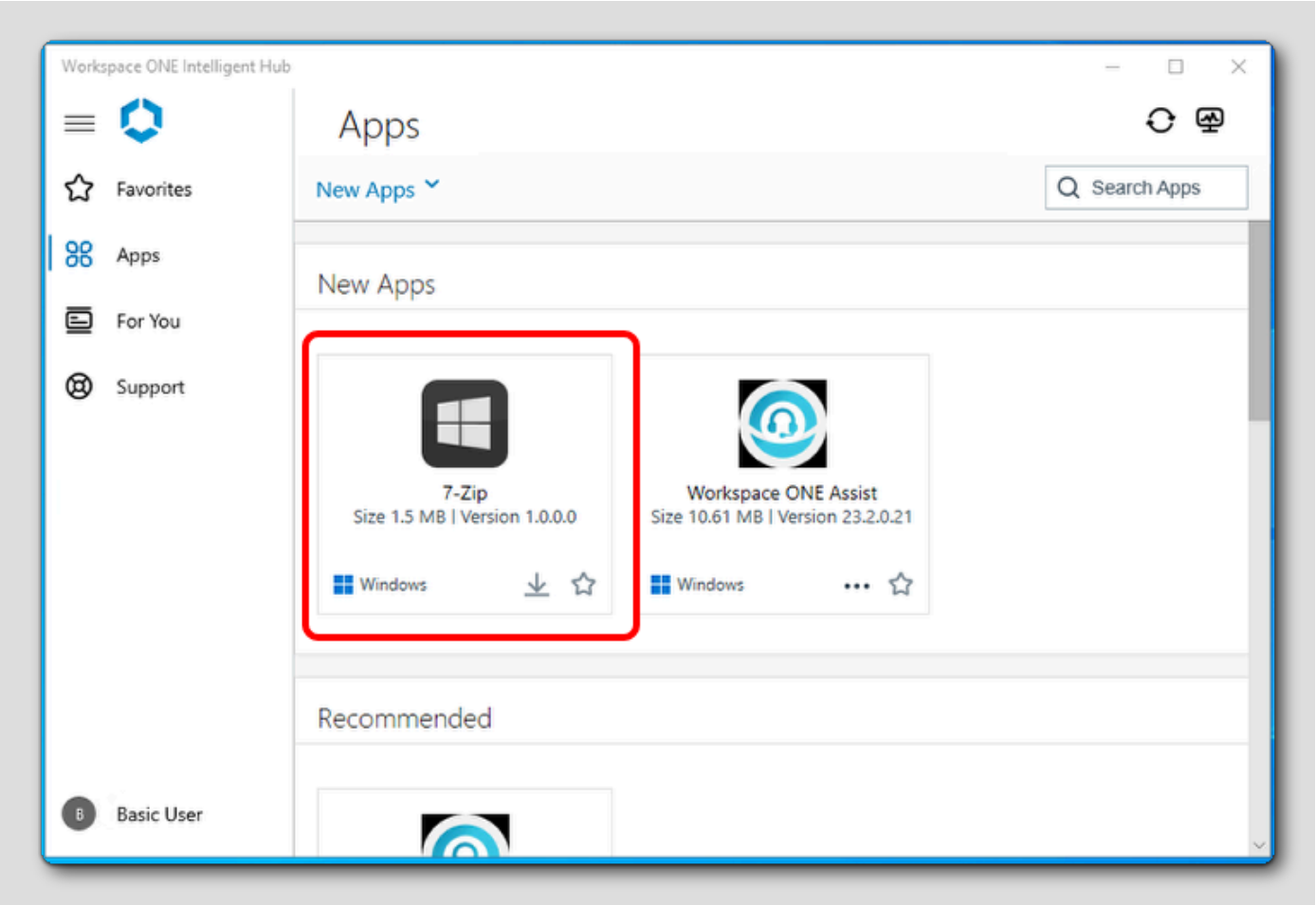
[116]



1. Click the **Workspace ONE Intelligent Hub app** from the task bar.
2. Click the **Apps** tab to view the app catalog.
3. Click **Refresh** to view the new apps that have been made available.
4. Confirm that the **7-Zip** and **Workspace ONE Assist** apps both display under the New Apps section.

Install the 7-Zip Application

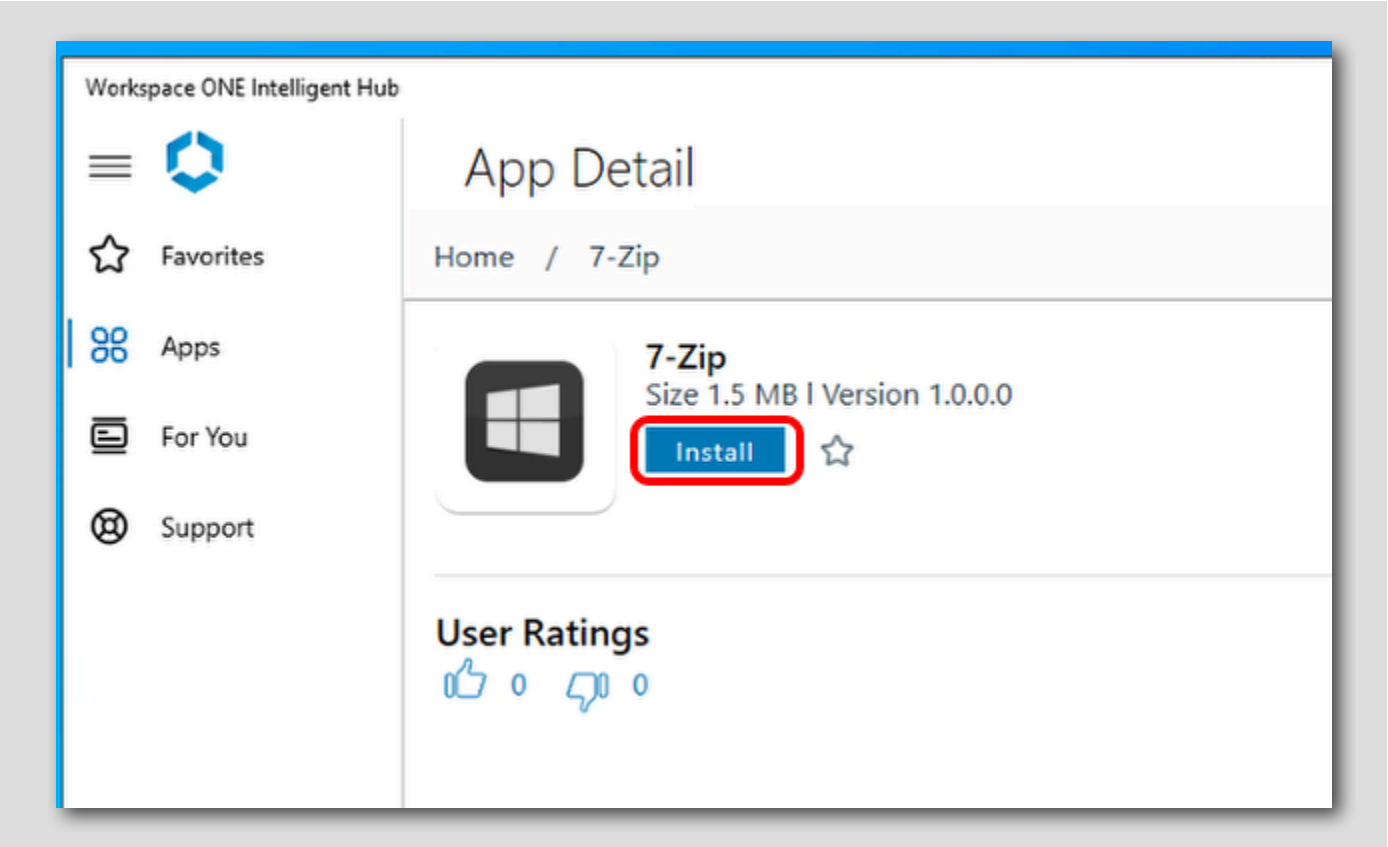
[117]



Click the **7-Zip** app.

Start the 7-Zip Install

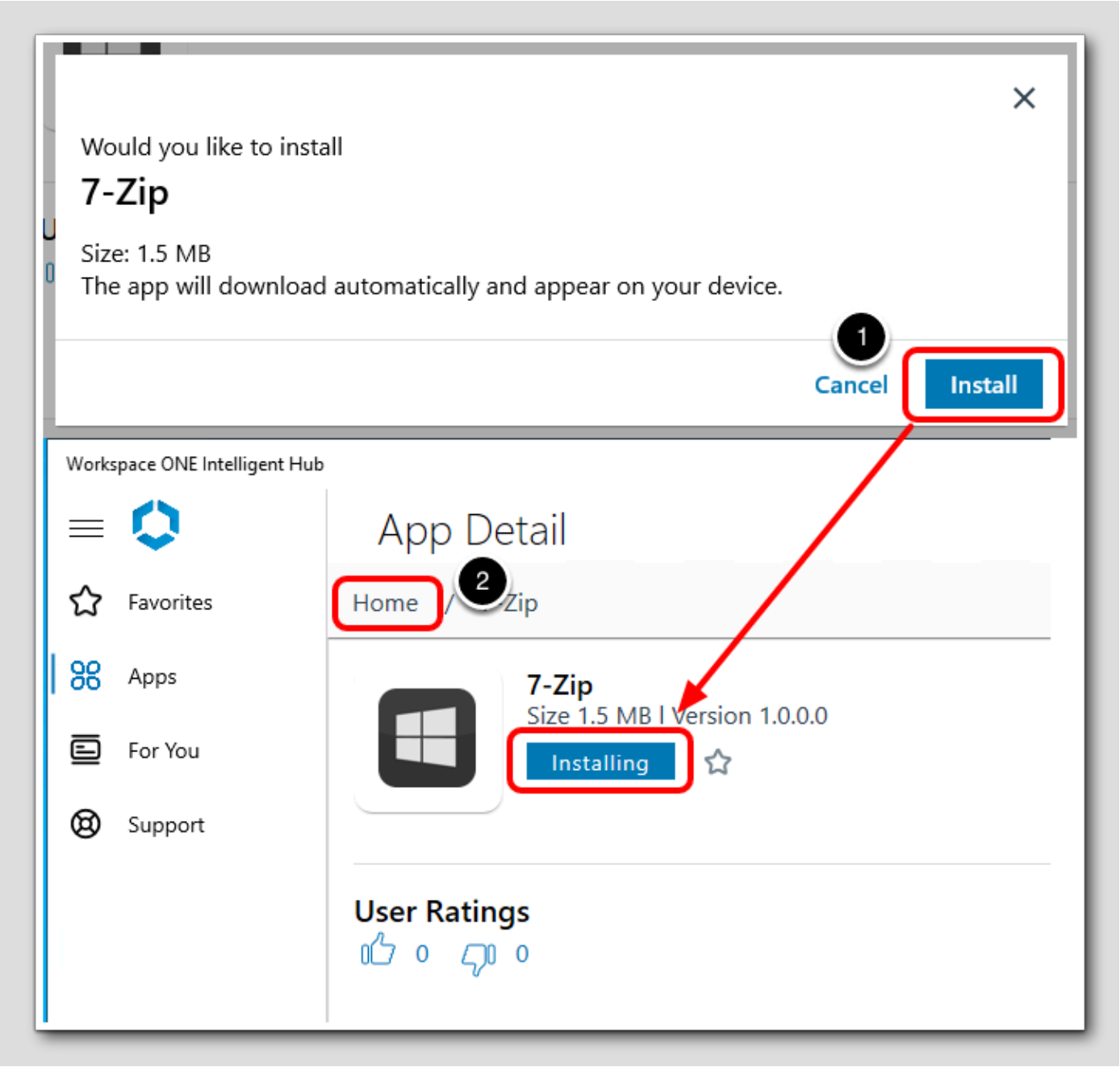
[118]



Click **Install**.

Confirm the Install

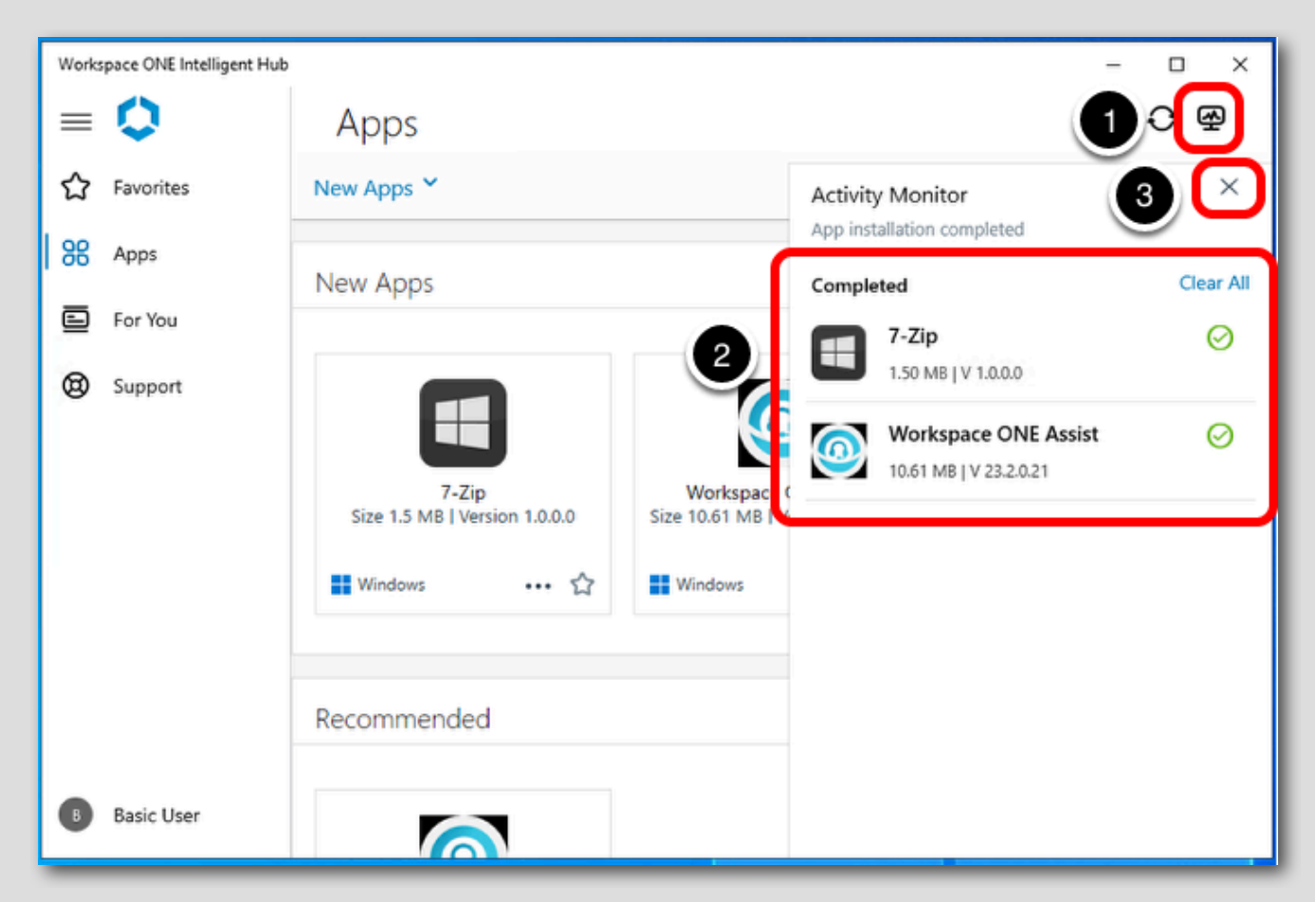
[119]



1. Click **Install** for the pop-up. The status of the 7-Zip app will change to **Installing**.
2. Click **Home** to return to the app catalog.

Monitoring the Install

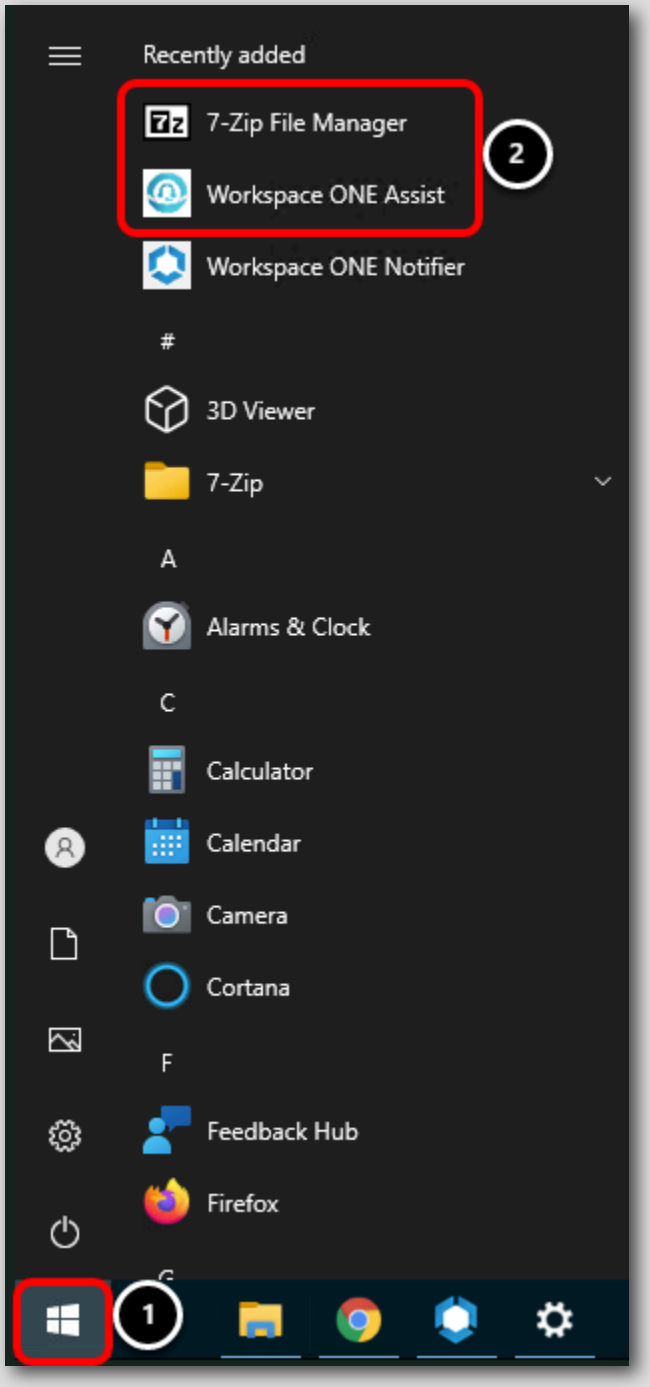
[120]



1. Click the **Downloads** button to open the Activity Monitor.
2. The Activity Monitor allows you to view progress on your application downloads and if they have completed. Wait until both 7-Zip and Workspace ONE Assist finish installing, then continue to the next step.
3. Click **X to** close the Activity Monitor.

Confirm the Apps Installed

[121]



1. Click the **Windows** button.
2. Confirm that both **7-Zip** and **Workspace ONE Assist** appear under the Recently Added section. Feel free to launch the apps if you wish, then continue to the next step.

Validation Conclusion

[122]

You were able to confirm that the Restriction Profile took affect on the device as intended and that the two applications you made available, Workspace ONE Assist and 7-Zip, were presented to the user from the app catalog and were successfully installed!

Un-enrolling your Windows 10 Device

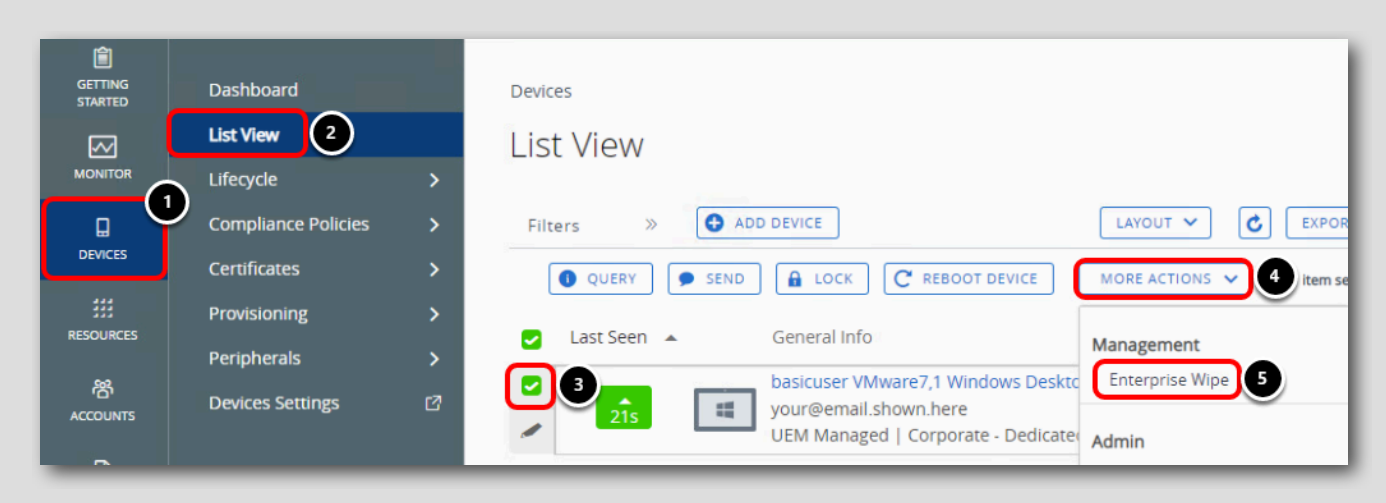
[123]

In this section, we are going to un-enroll our Windows 10 VM so that we can use it for other lab modules.

We will use the **Enterprise Wipe** wipe command to remove all of the managed content that was pushed to the device (such as profiles and apps) by Workspace ONE while not modifying any personal content or data on the device.

Enterprise Wipe from Workspace ONE UEM Console

[124]

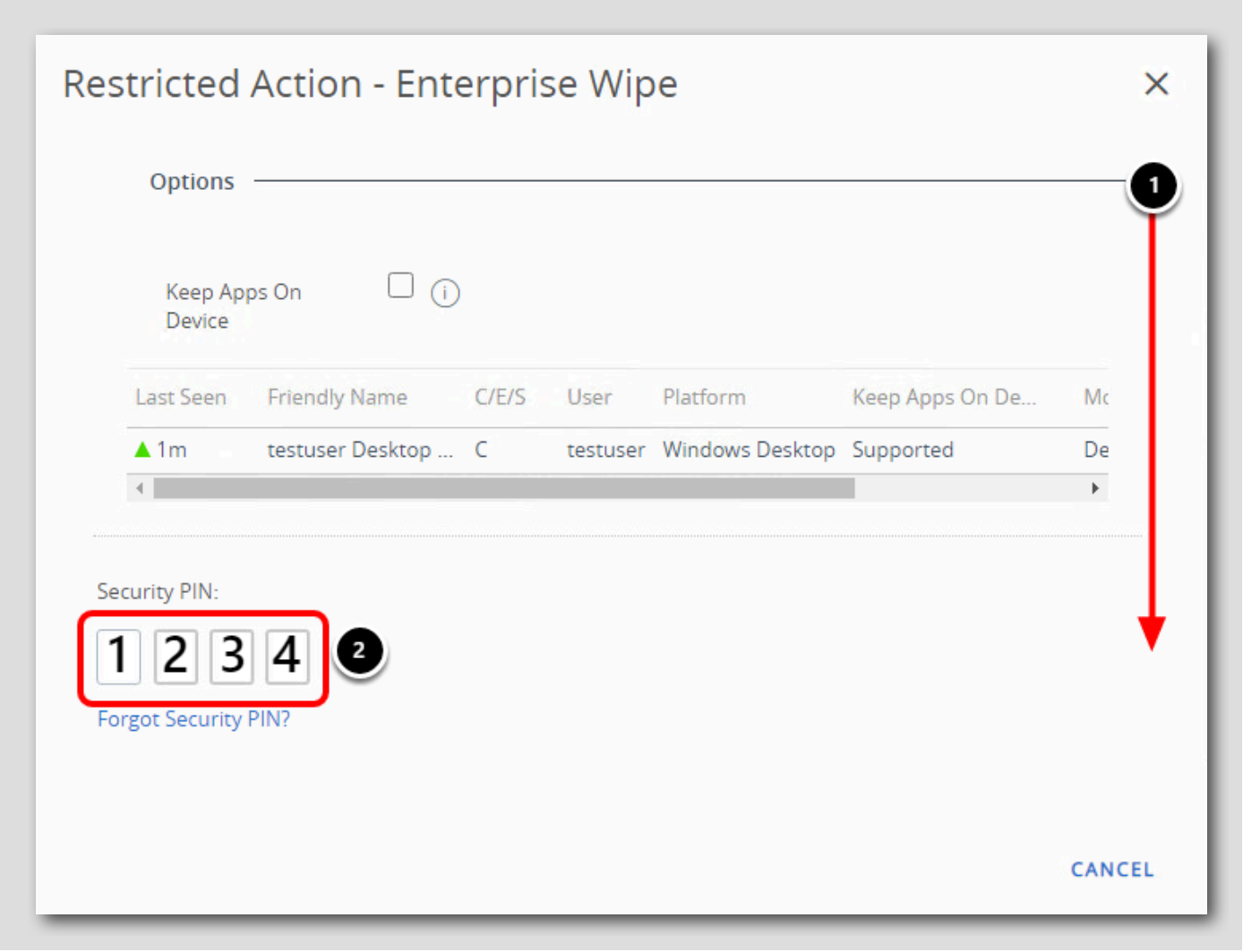


Return to the Workspace ONE UEM Administrator Console in Google Chrome,

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

Enter PIN and Enterprise Wipe Device

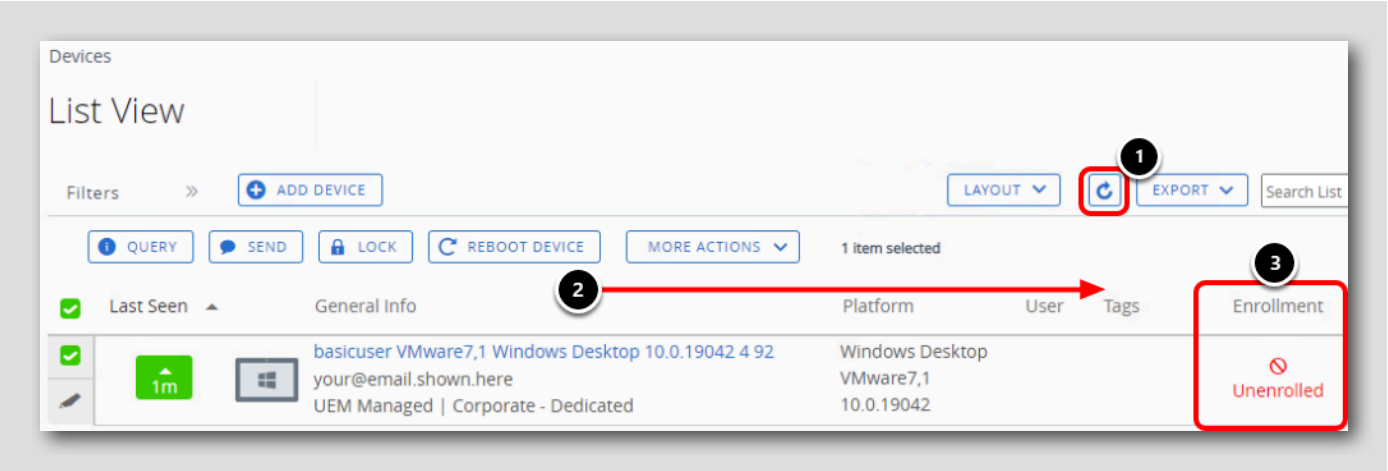
[125]



1. You may need to scroll down to find the Security PIN input
2. Enter the Security PIN that you created when you first logged into the Workspace ONE UEM administration console, which was **1234**. If you used a different PIN, enter that one instead.
3. Click **Delete**

Validate Enterprise Wipe

[126]

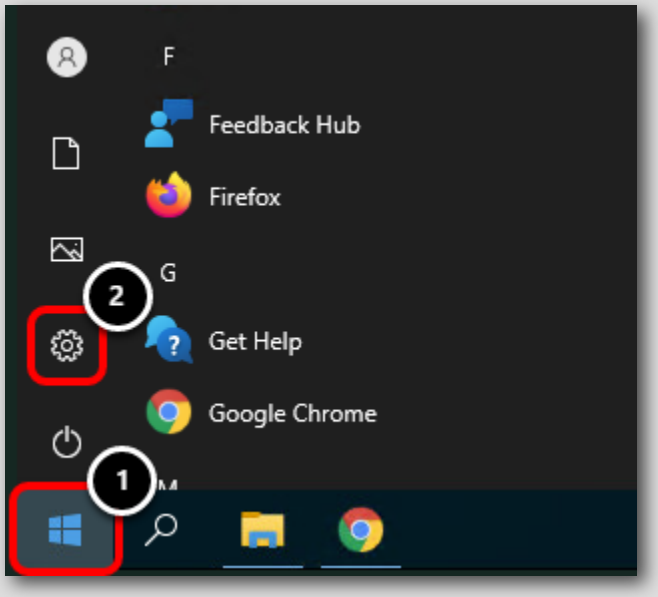


NOTE: The Enterprise Wipe may take several minutes to process.

1. Click the **Refresh** icon periodically to refresh the page to check if the Enterprise Wipe has processed
2. If needed, scroll to the right to find the Enrollment column
3. Notice that the Enrollment status for the device changes to **Unenrolled** once the Enterprise Wipe command is processed

Navigate to Windows 10 Settings

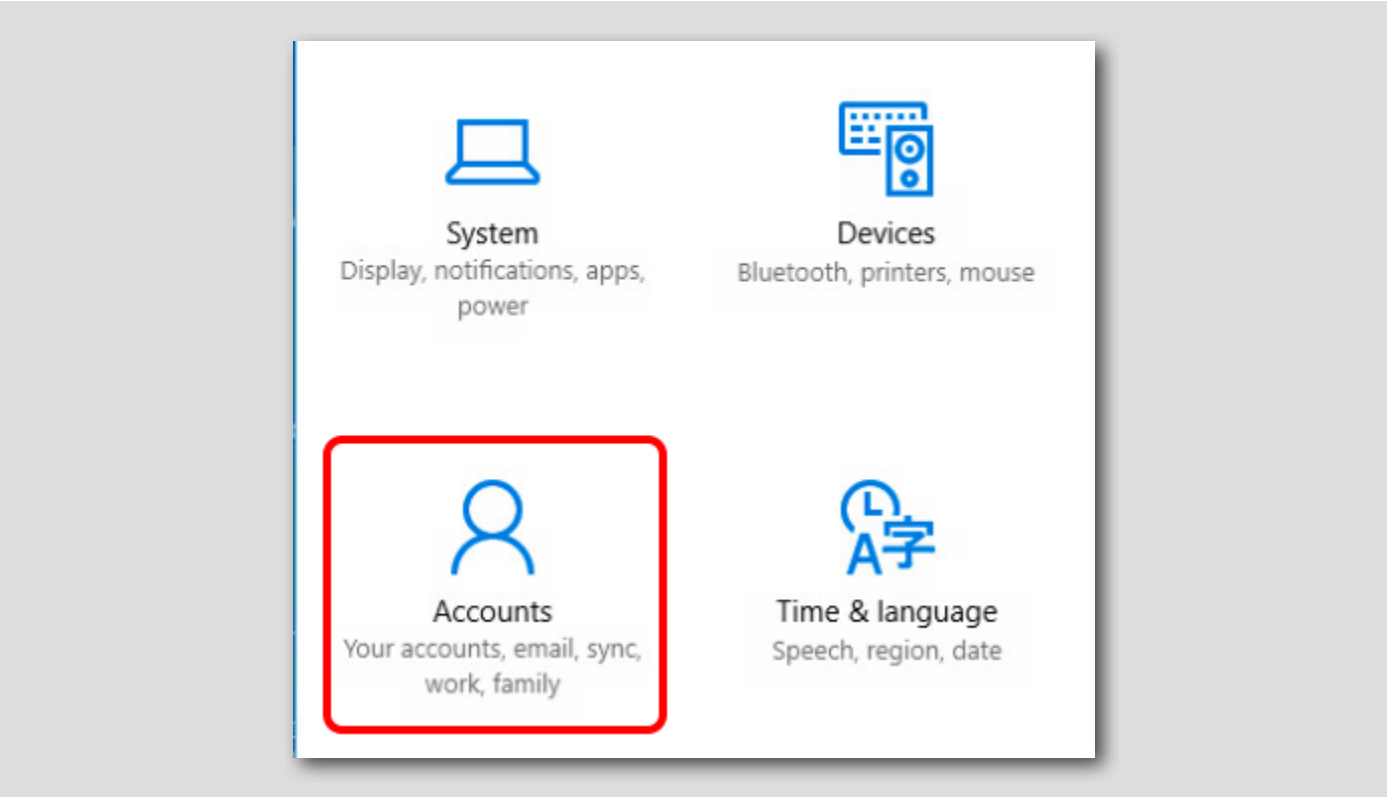
[127]



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

Access Accounts Settings

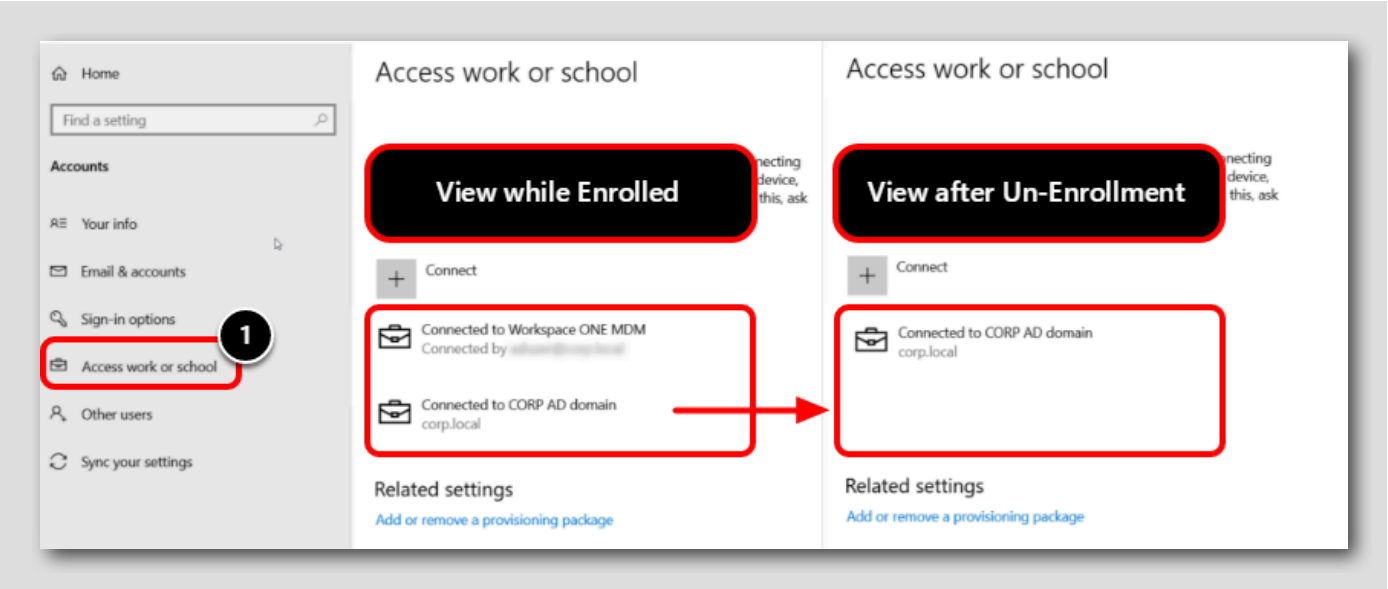
[128]



From the Settings Menu, access **Accounts**

Validate That No Management Account Exists

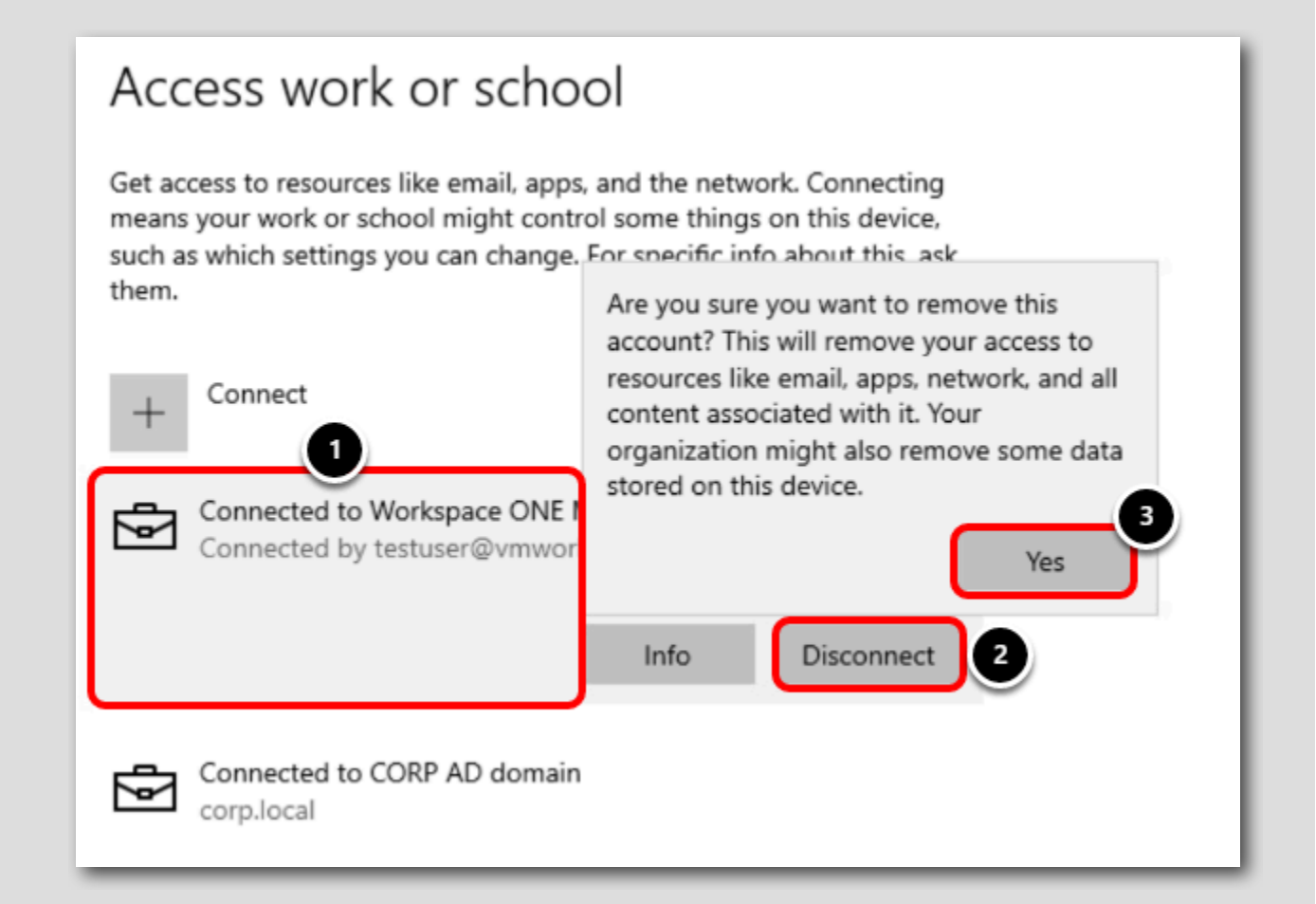
[129]



1. Click on Access work or school
2. Validate that you DO NOT see any account connected to Workspace ONE MDM.

NOTE: The CORP AD domain is the local domain in this lab and is not controlled by Workspace ONE UEM Enrollment, so you will see this connection when your device is enrolled or unenrolled.

NOTE: If the Access Work or School page was opened from earlier, you may need to refresh or navigate away from the page and return to see the changes.

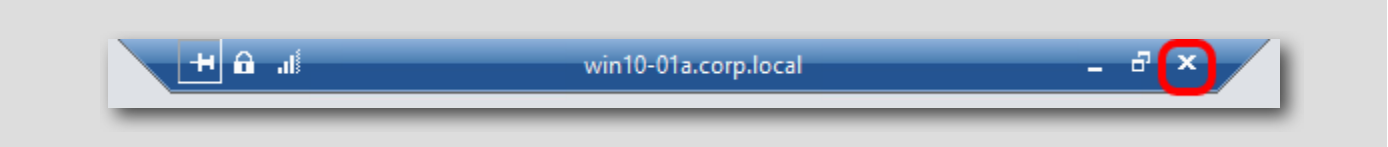


1. Click the **Connected to Workspace ONE UEM** account
2. Click **Disconnect**
3. Click **Yes**

Return to the Main Console

[130]

Click **Close (X)** on the Remote Desktop Connection bar at the top of the screen to return to the Main Console to finish making configurations within the Workspace ONE UEM Console.



Summary

[131]

In addition to managing mobile devices, Workspace ONE UEM can also manage your Windows 10 devices. This quick look into Windows 10 management should provide a clearer picture of how you can manage your Windows 10 devices by configuring restrictions and profiles and deploying applications alongside your mobile workforce.

This concludes the Basic Windows 10 Management module.

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

[132]

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*!


Your Personal journey from zero to IT Superhero
How the products work – beginner to expert
Quick start for your first proof of concept
TECH ZONE
Hands on Labs, Tools and Best Practices
Guide to production deployments & operations
Latest product information

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!

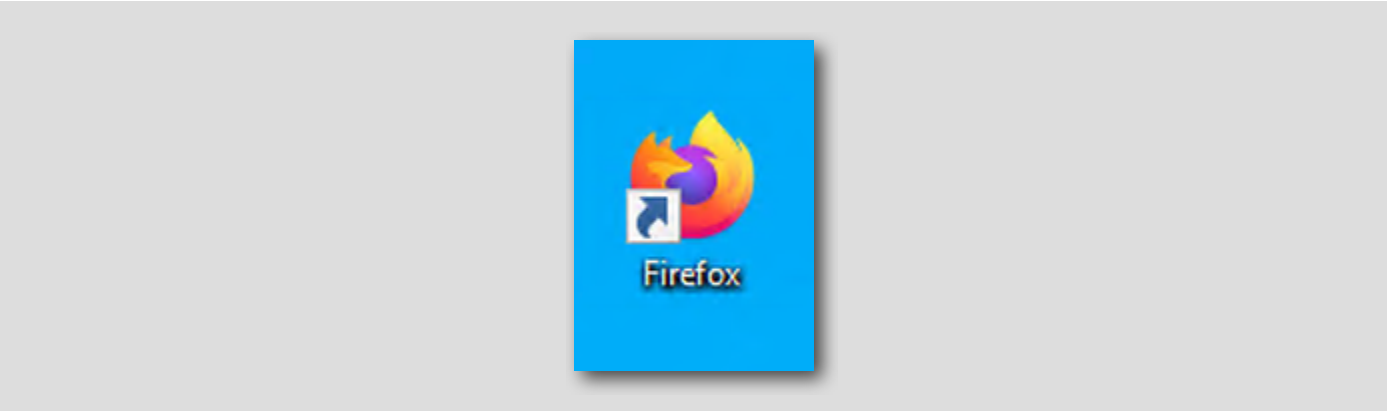
Personal devices may be enrolled into other UEM providers which can cause undesired conflicts and issues.

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.

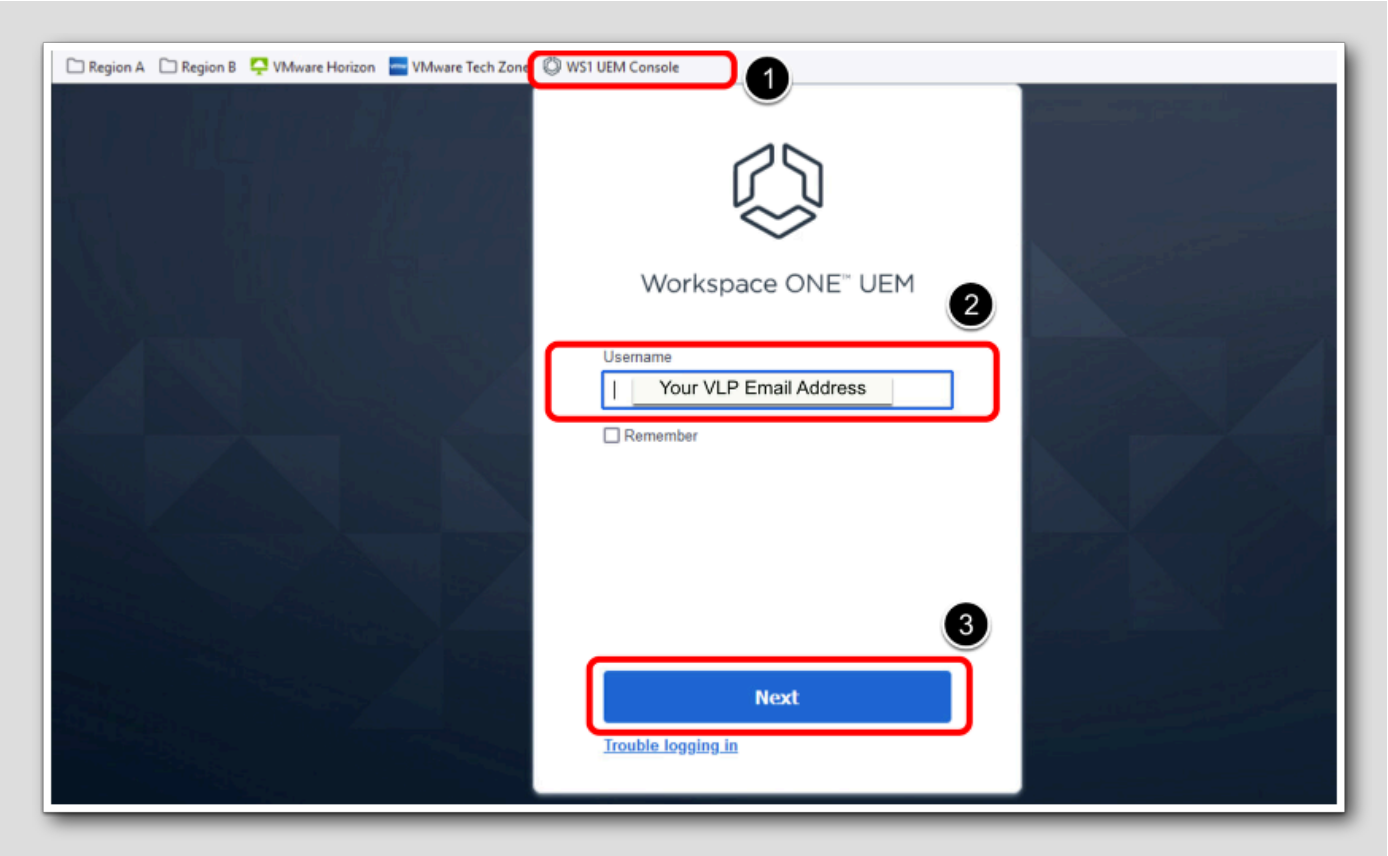
Launch Firefox Browser [137]



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]

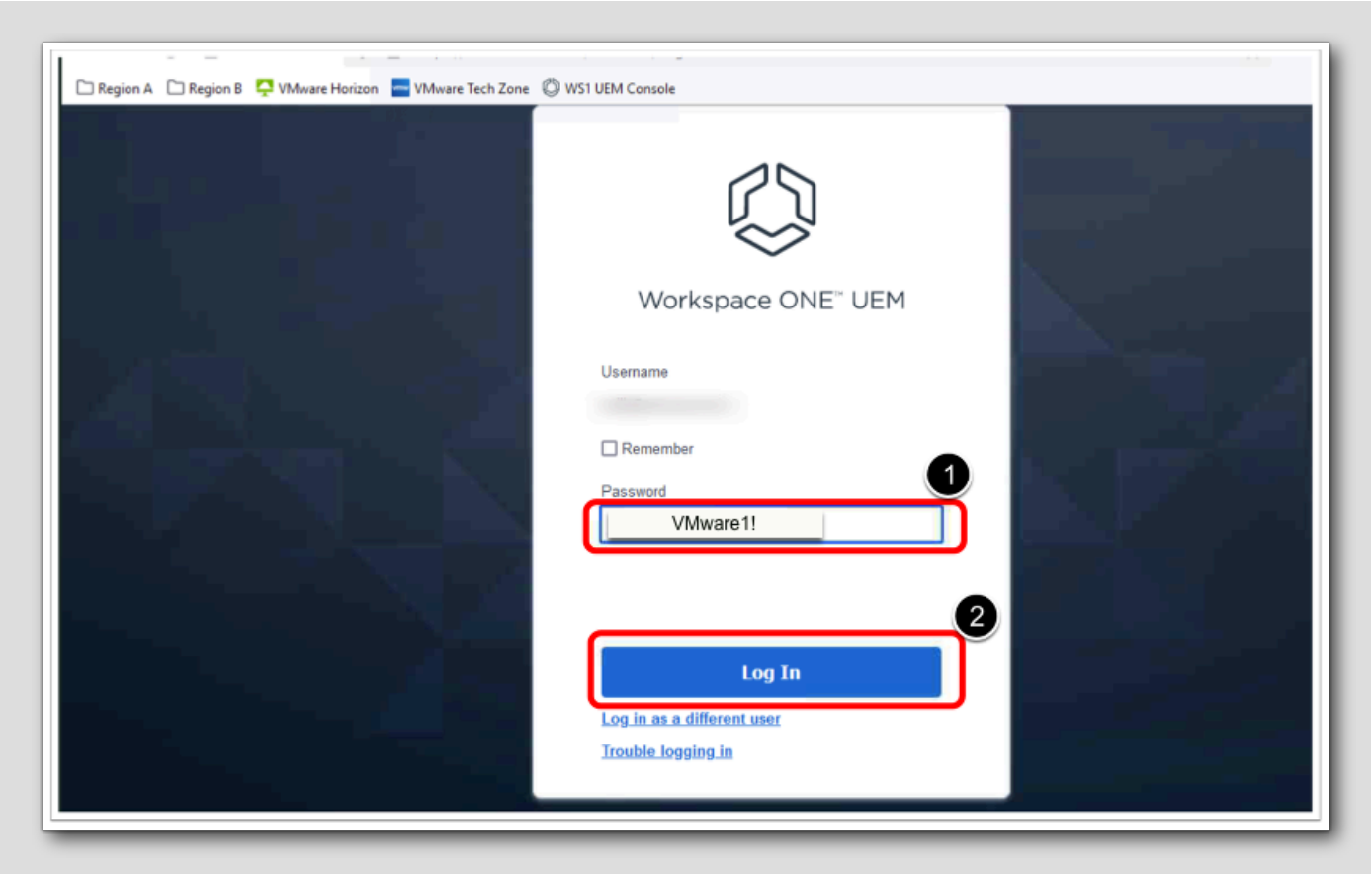


1. Select the **WS1 UEM Console** link from the Bookmark Toolbar
2. Enter your **Username**. This is the **email address** that you have associated with your **VMware Learning Platform (VLP)**account that you utilized to take Hands-on Labs.
3. Click **Next**, then advance to the next step of the lab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



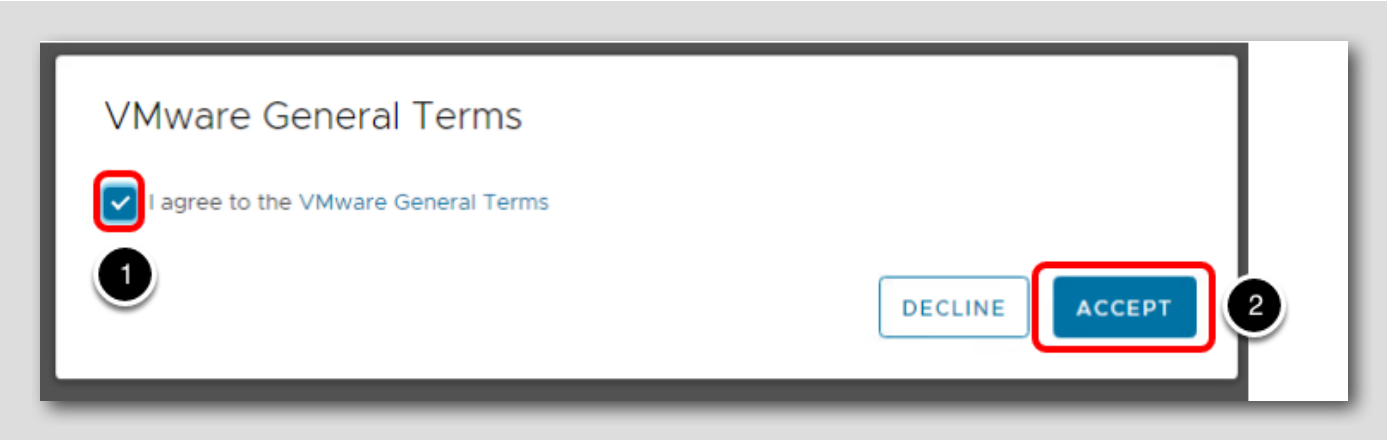
The password field will be displayed after entering your username.

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.

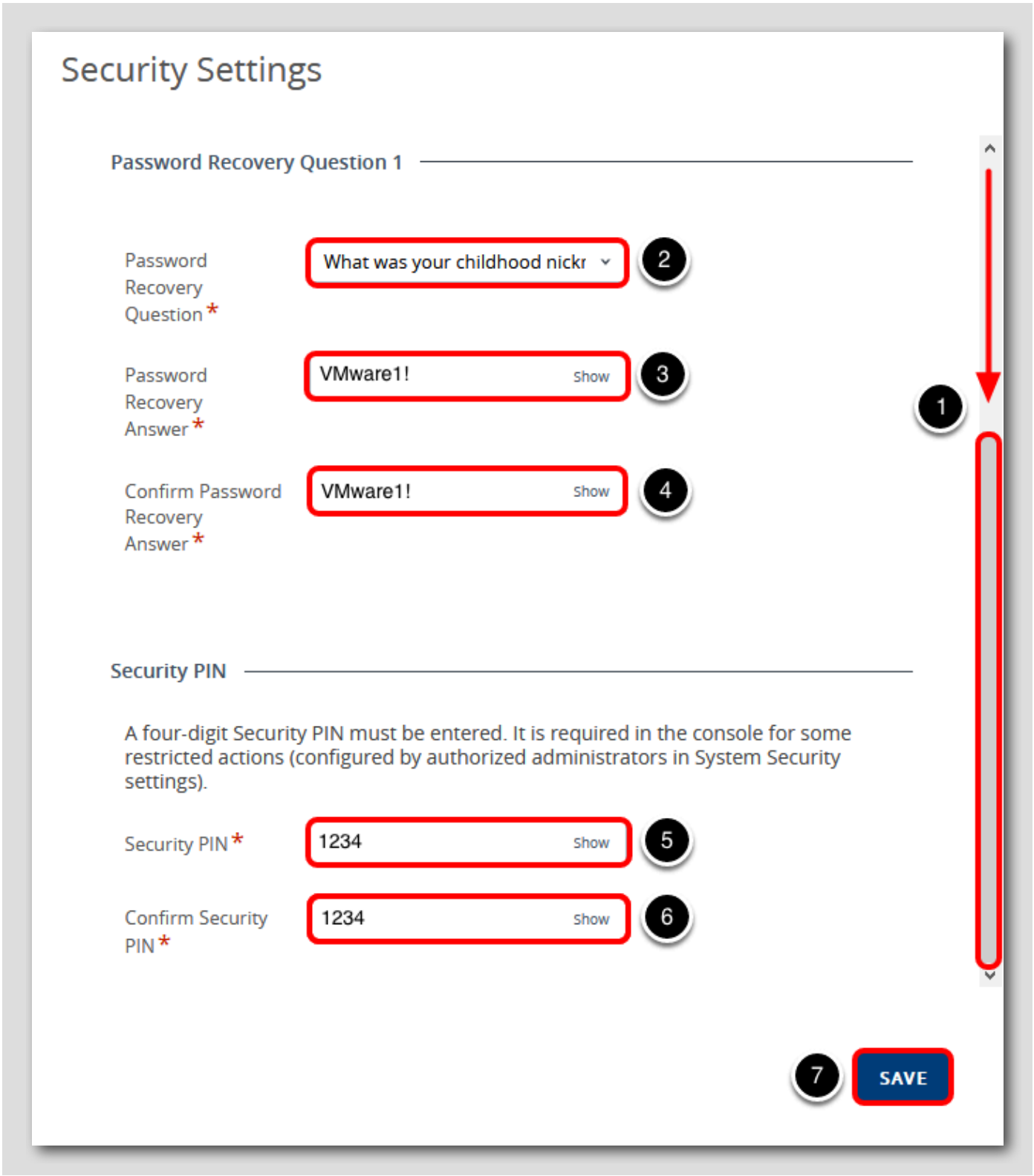
1. Select the box next to I Agree to the VMware General Terms.
2. Click the **Accept** button.

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

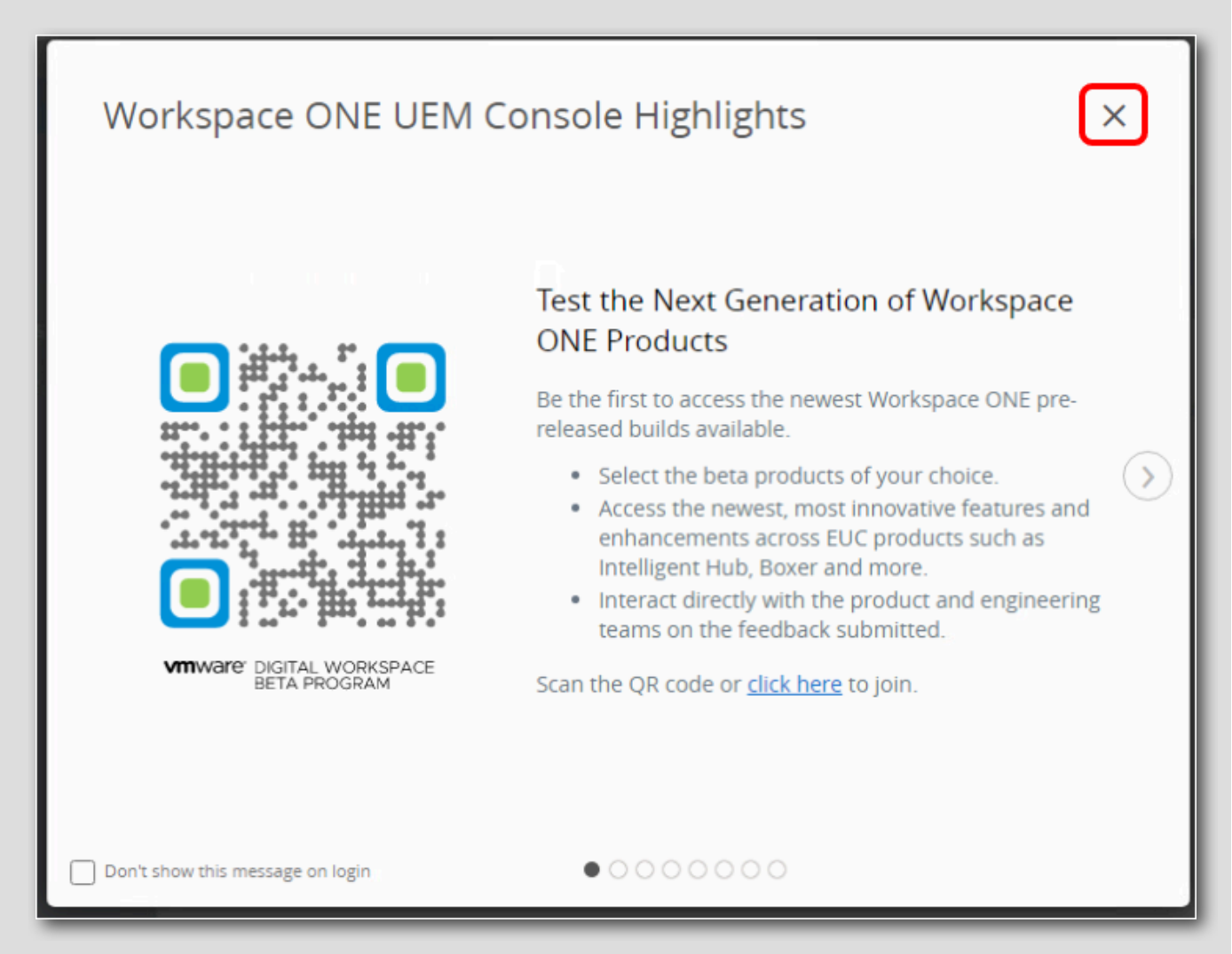

Security Settings
Password Recovery Question 1
Password Recovery Question *
What was your childhood nickr
2
Password Recovery Answer *
VMware1!
Show
3
1
Confirm Password Recovery Answer *
VMware1!
Show
4
Security PIN
A four-digit Security PIN must be entered. It is required in the console for some restricted 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.

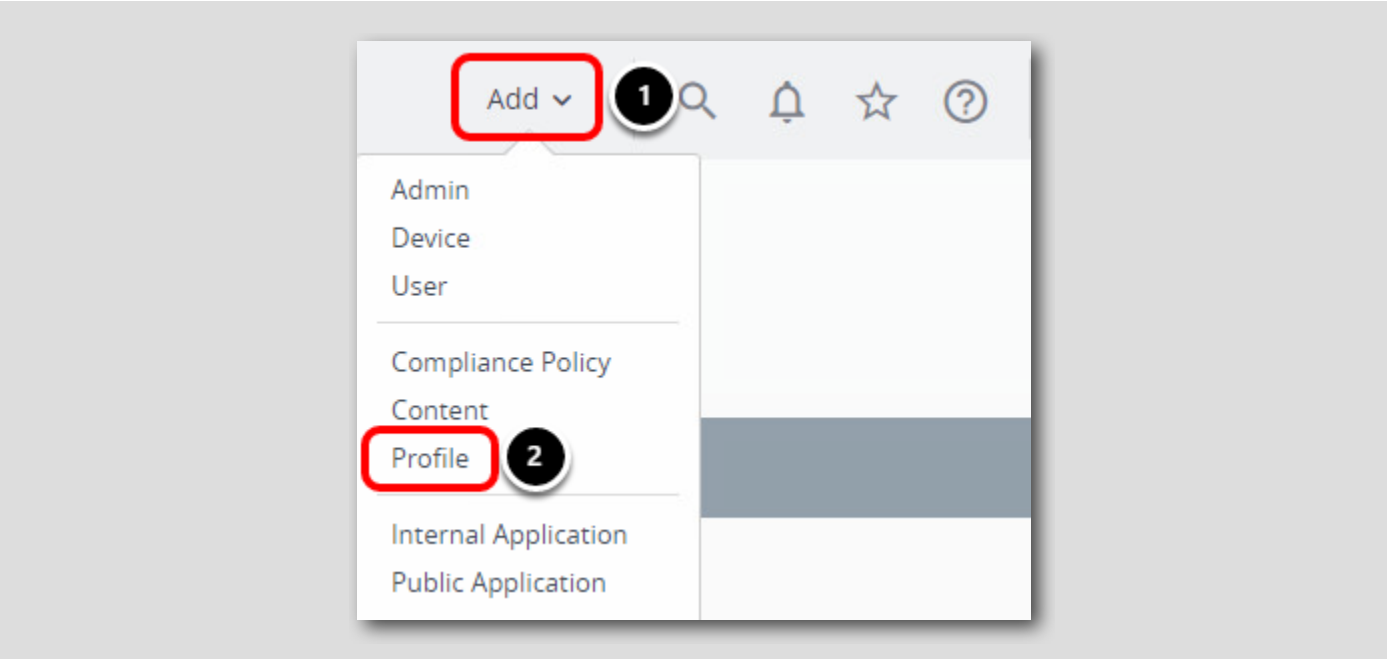
Create a Device Restriction Profile

[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]

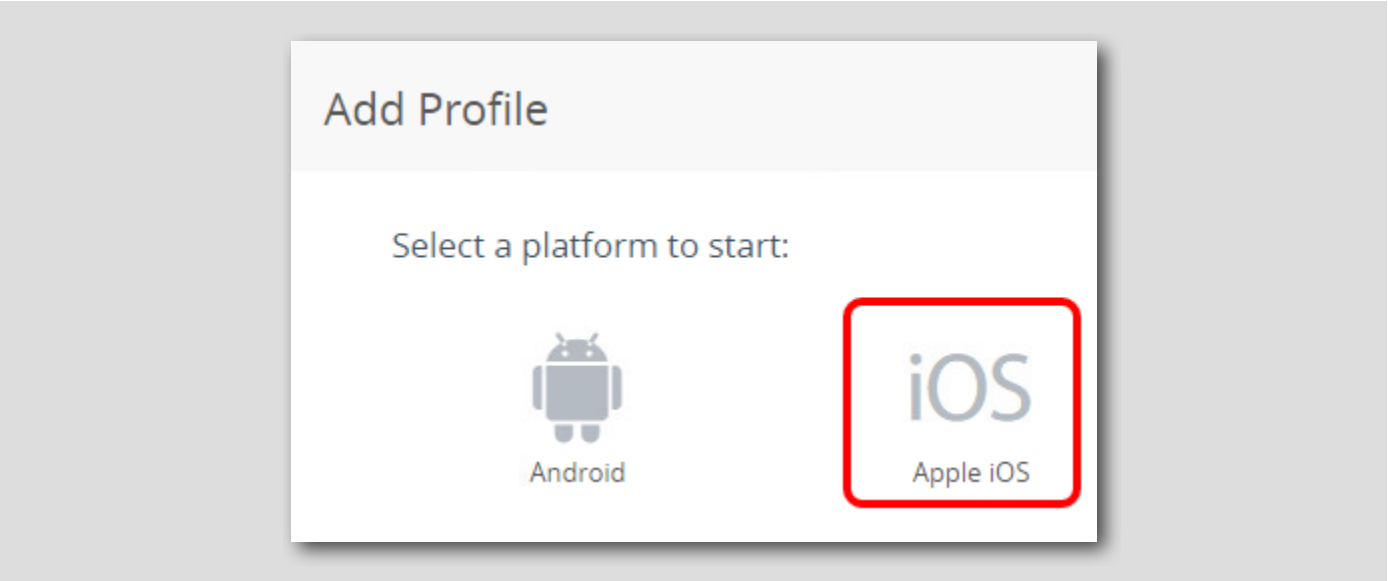


In the top right corner of the Workspace ONE UEM console,

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

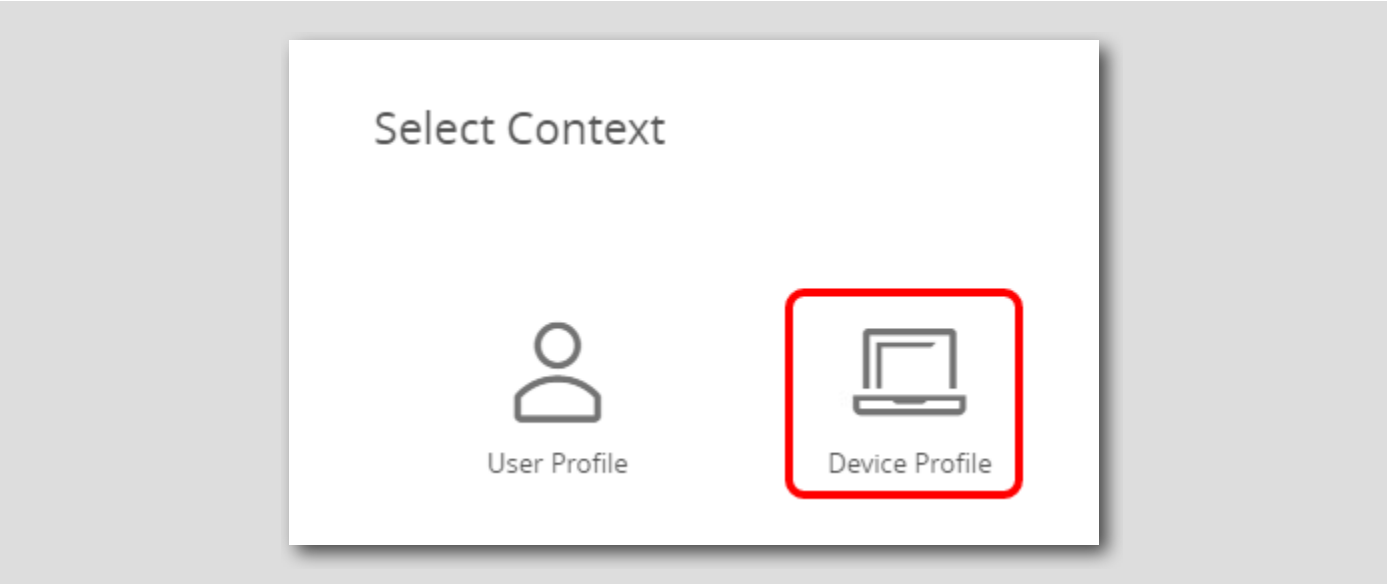
Select Platform

[145]



Select the Context

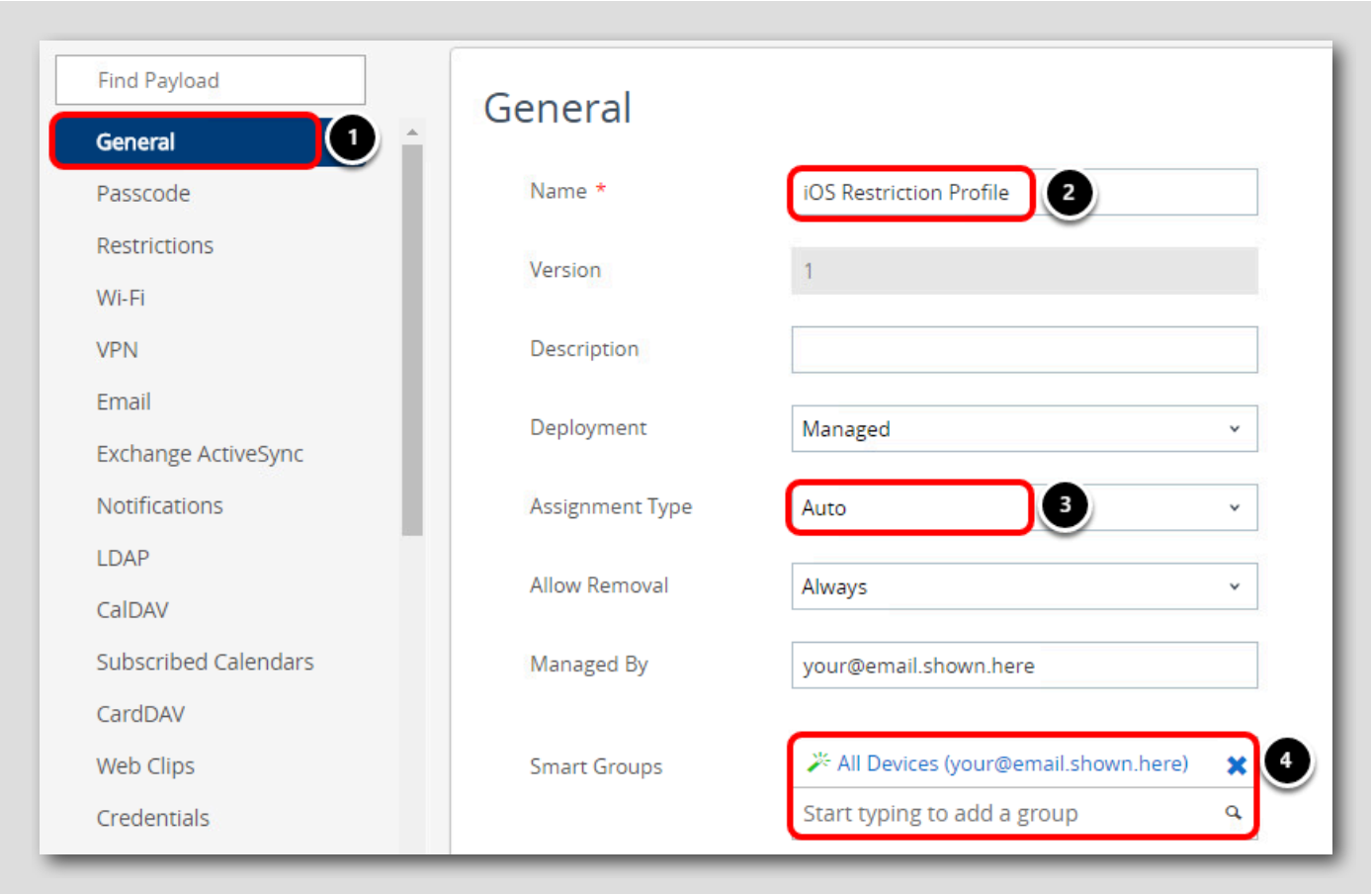
[146]



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)**

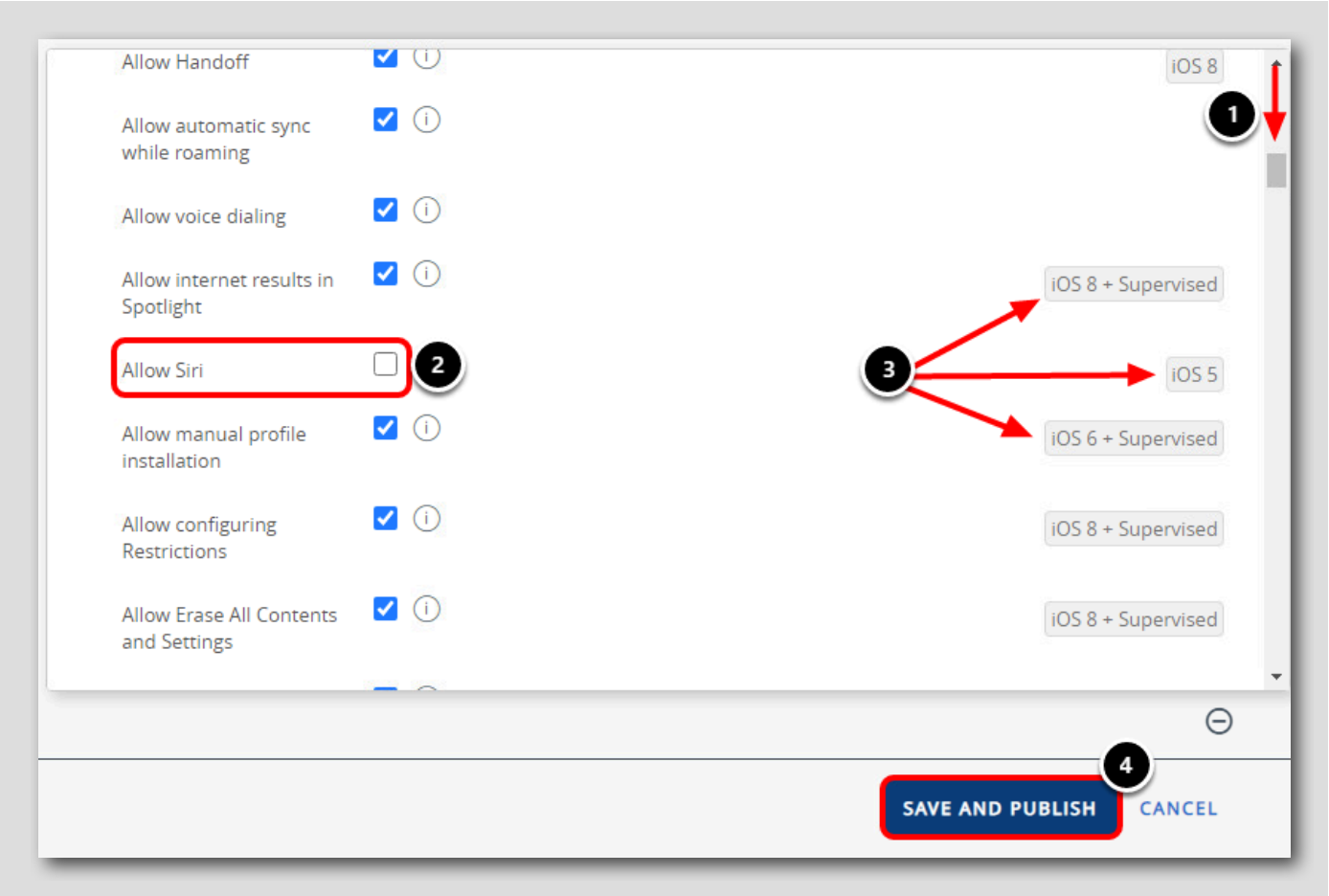
Configure Restriction Payload

[148]

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

Disable Siri

[149]

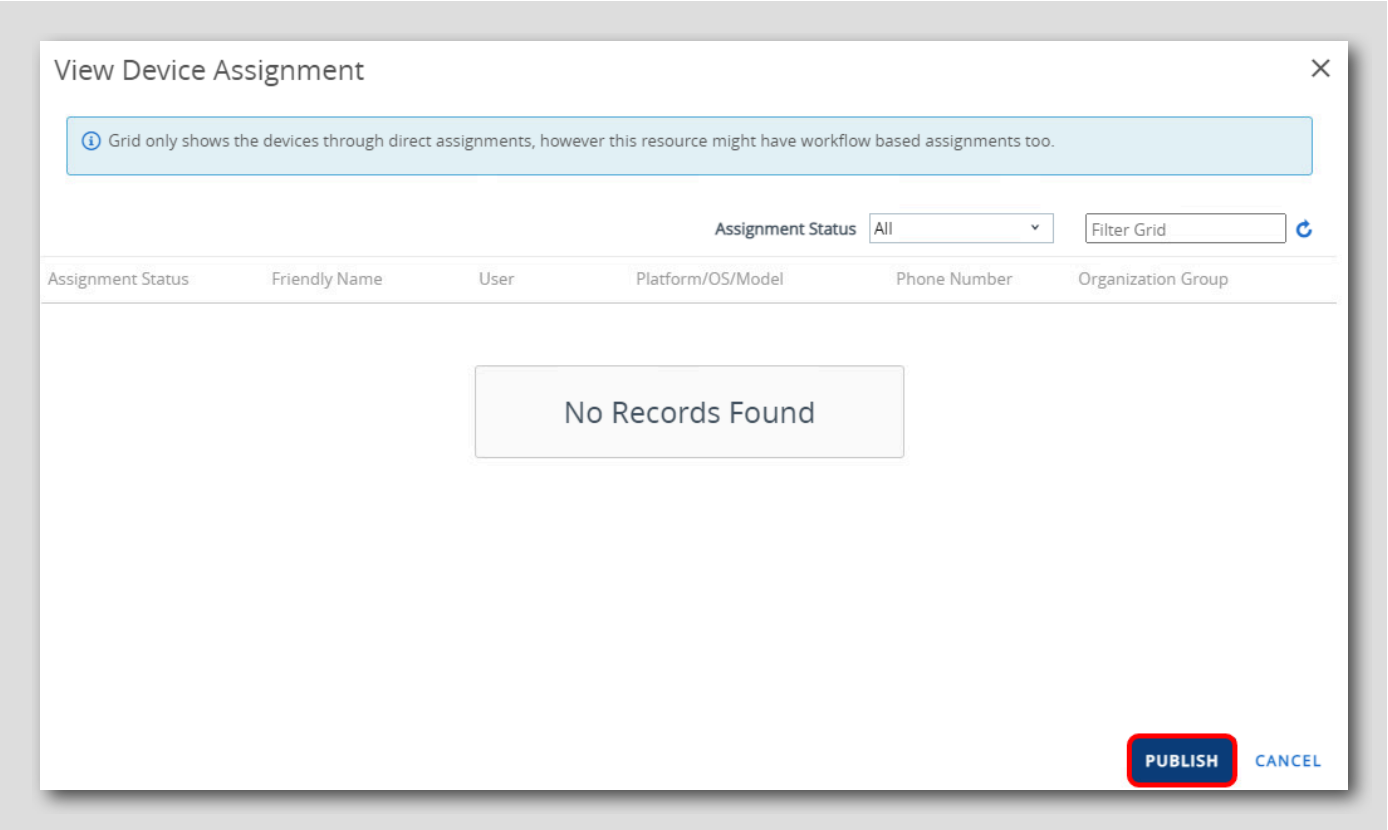


1. Scroll down approximately one page to find the **Allow Siri** option.
2. Uncheck the **Allow Siri** checkbox listed under the Device Functionality section. This will disable Siri on the device.
3. Take note of the **iOS version** and **Supervised** requirements for each restriction. The target device 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

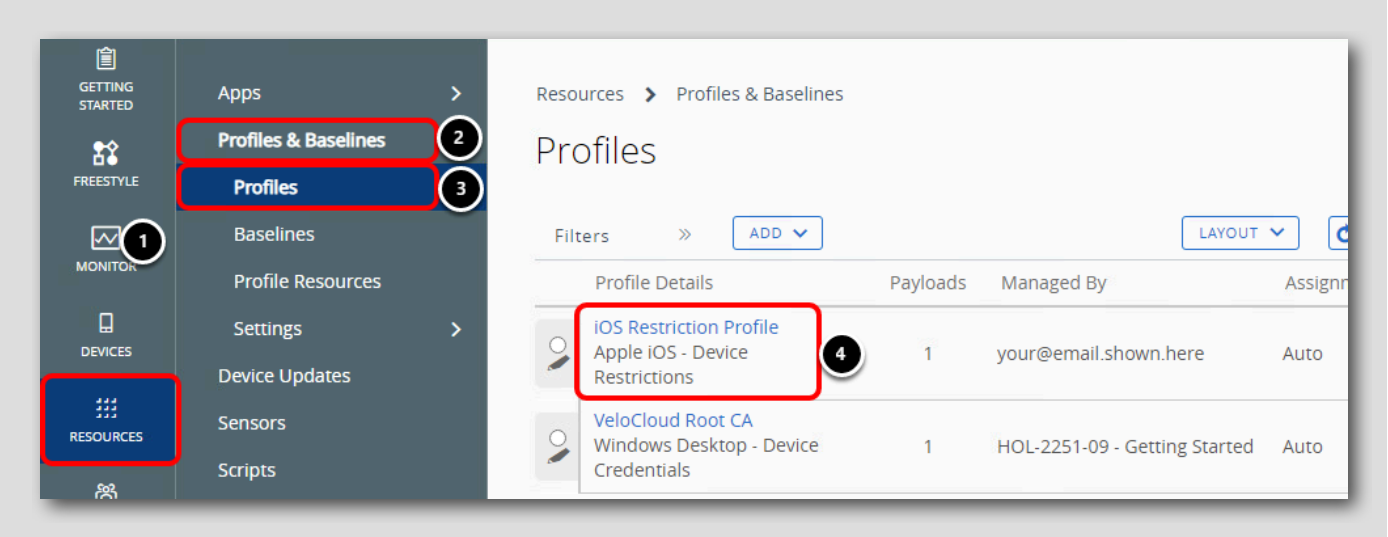
[150]



Click **Publish**.

Validate profile creation

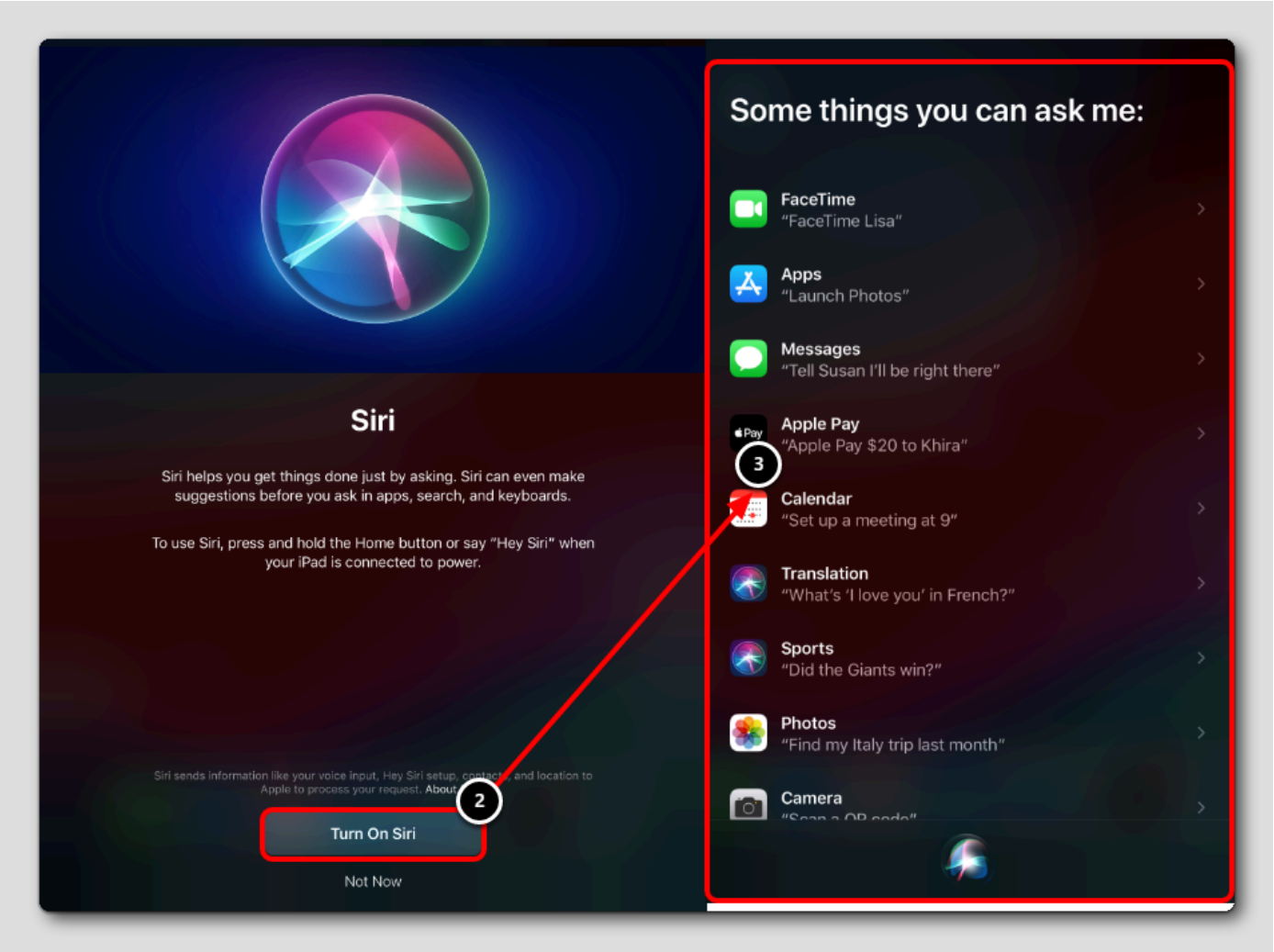
[151]



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

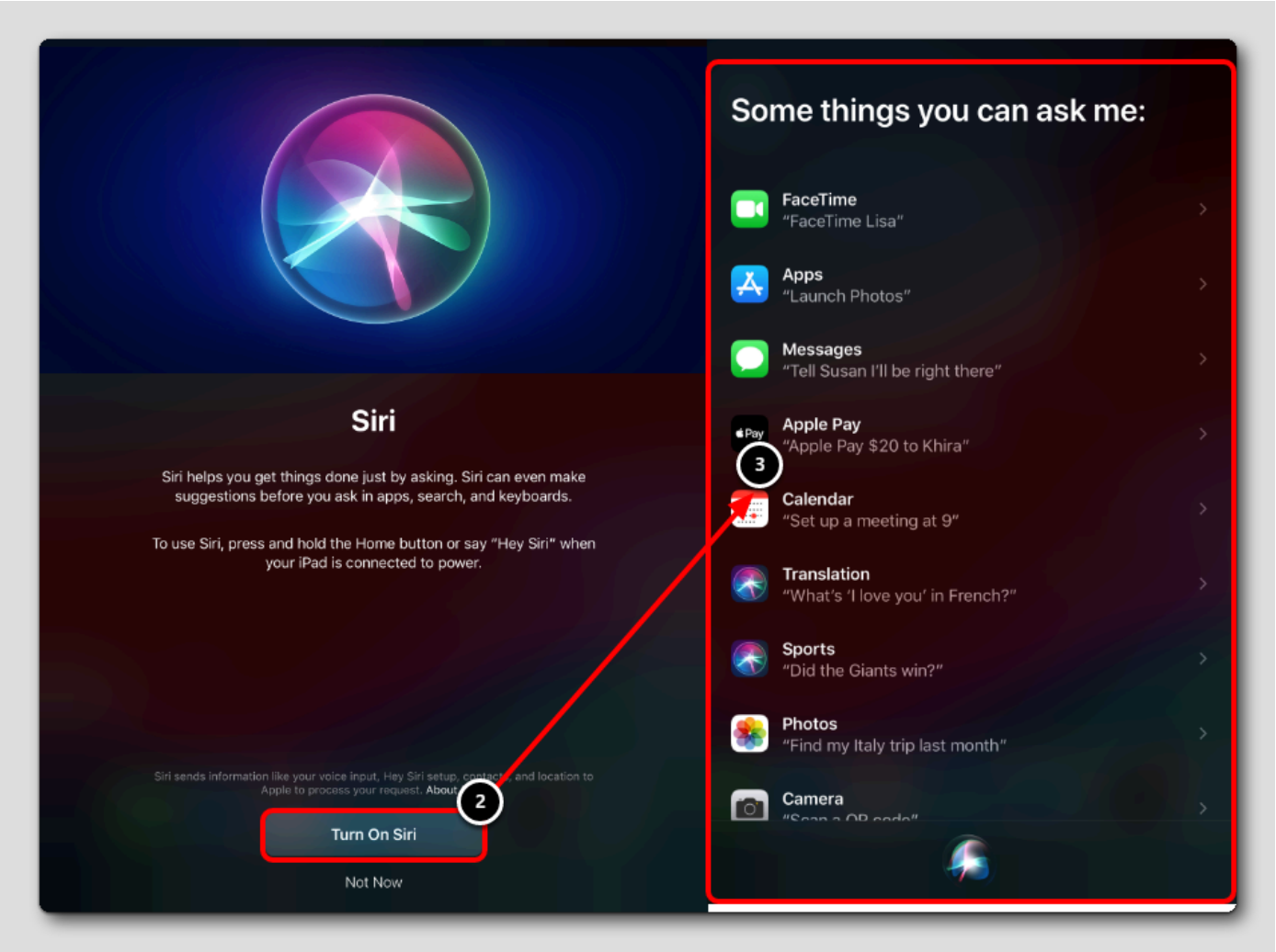
Validate Device Configuration Before Enrollment

[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.



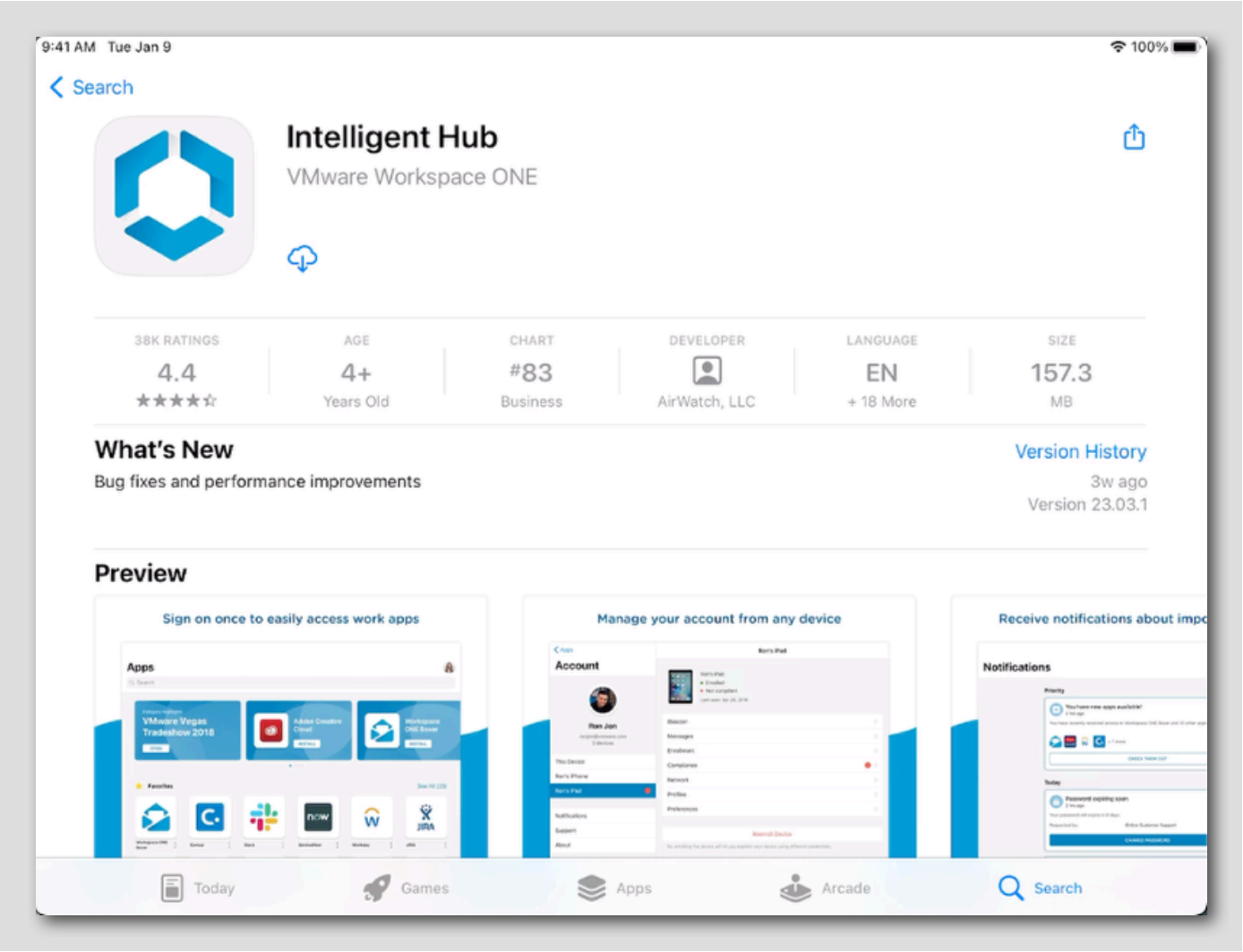
iOS Device Enrollment using testuser

[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.

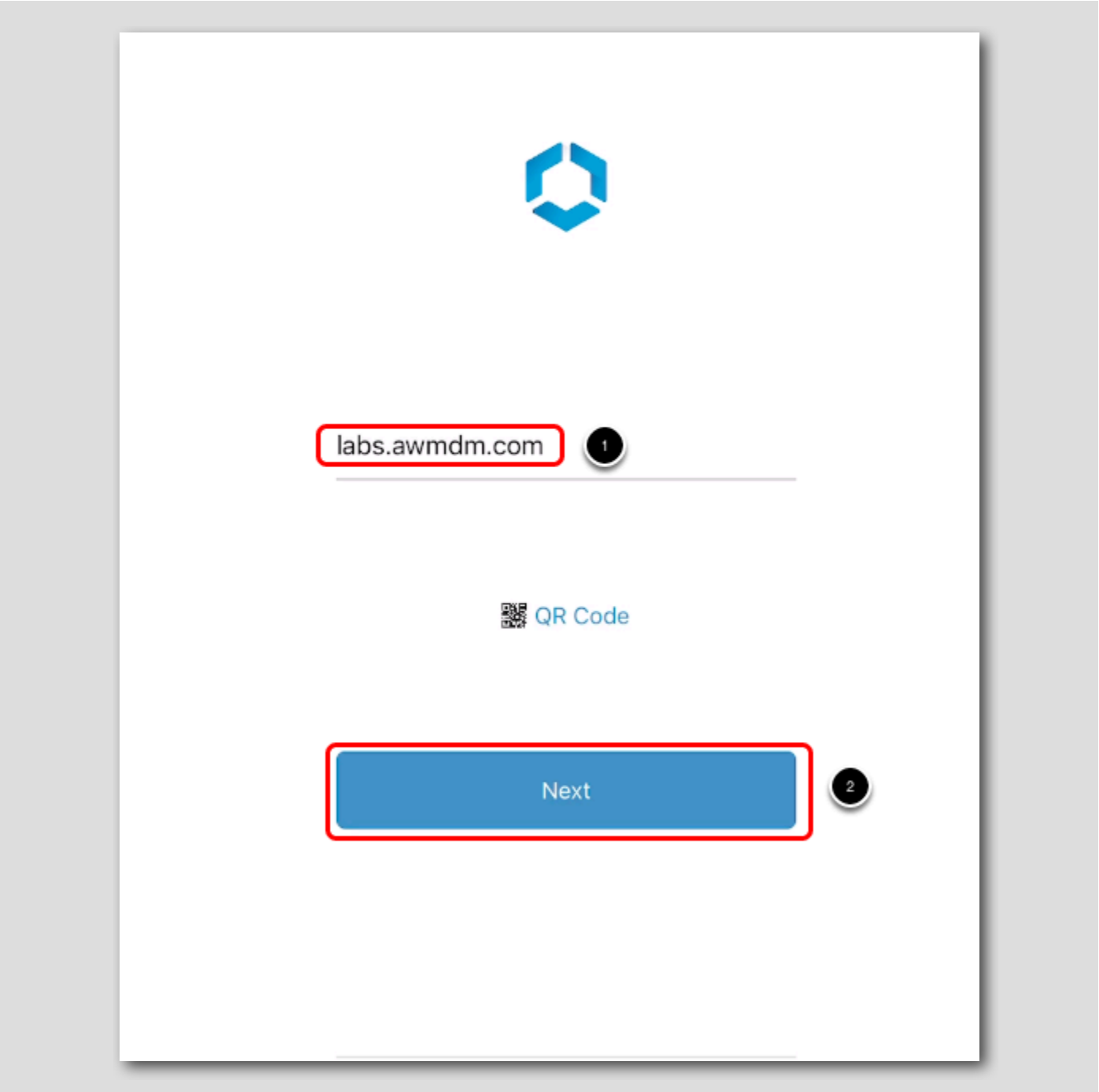
Launching the Workspace ONE Intelligent Hub

[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]



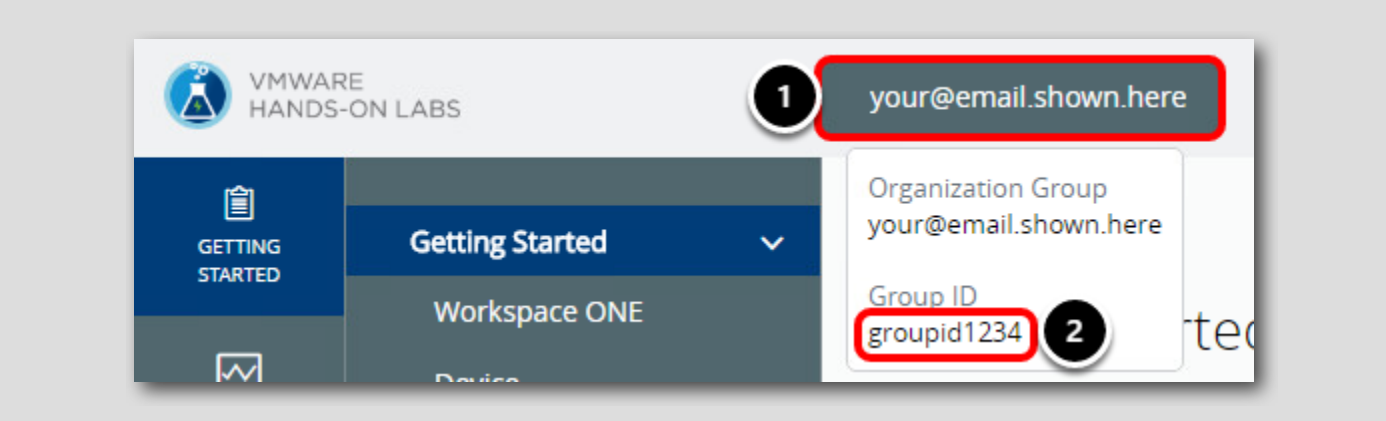
Once the Hub has launched you can enroll the device. To do so, follow the below steps.

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]



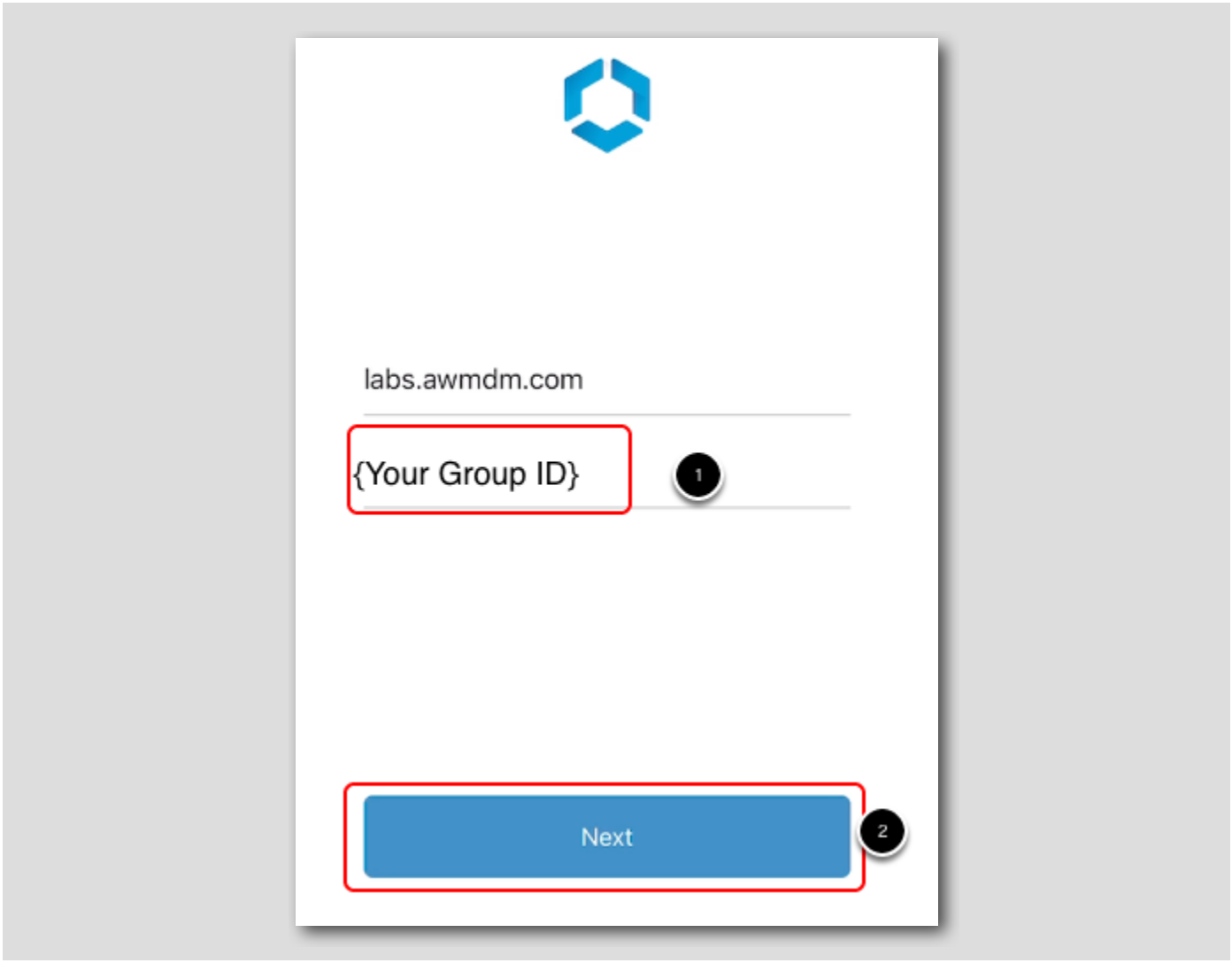
Return to the Workspace ONE UEM Console,

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]



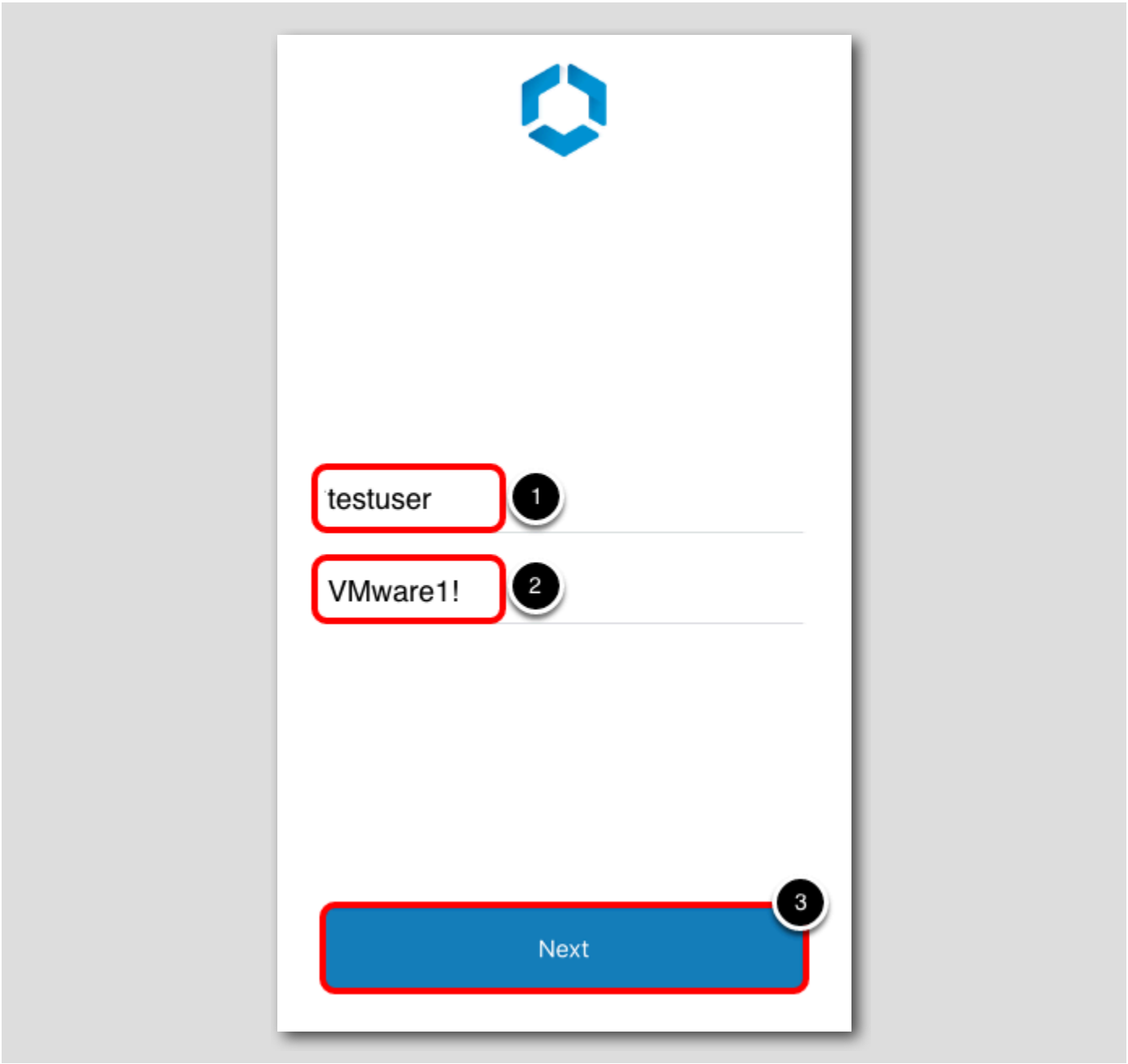
Return to the Workspace ONE Intelligent Hub application on your iOS Device,

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]

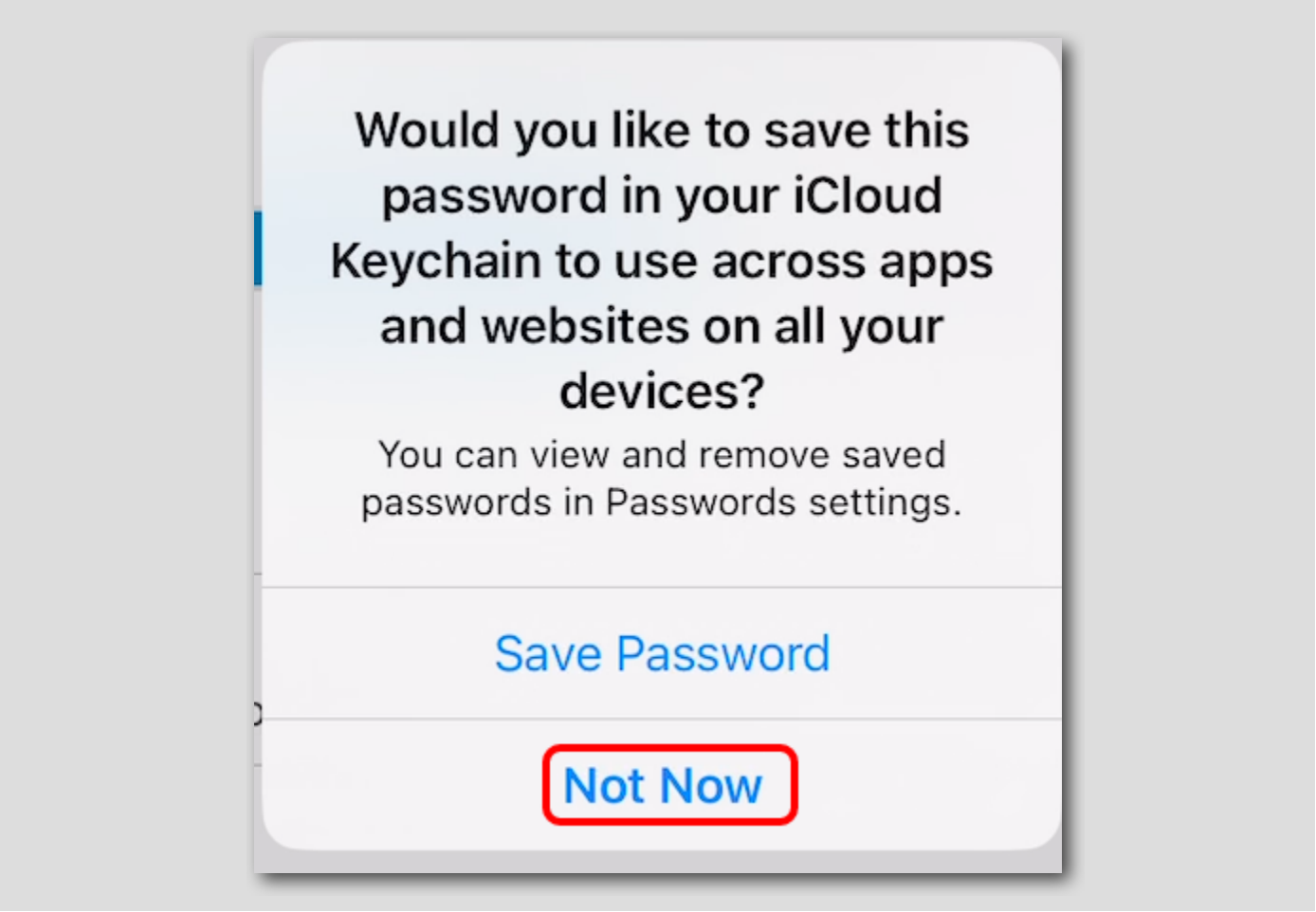


You will now provide user credentials to authenticate to Workspace ONE UEM.

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

Skip Password Save

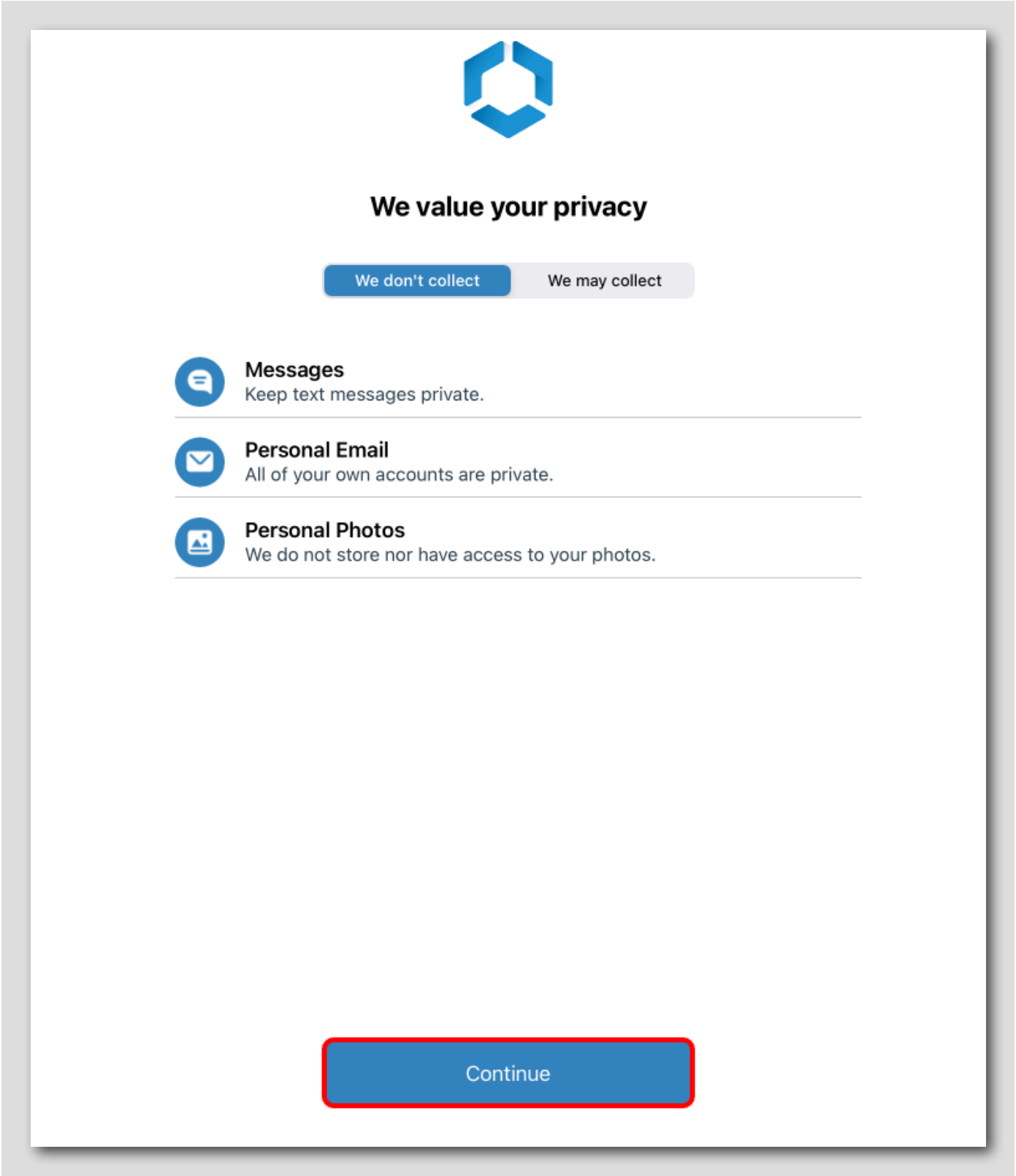
[160]



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

Review privacy notice

[161]

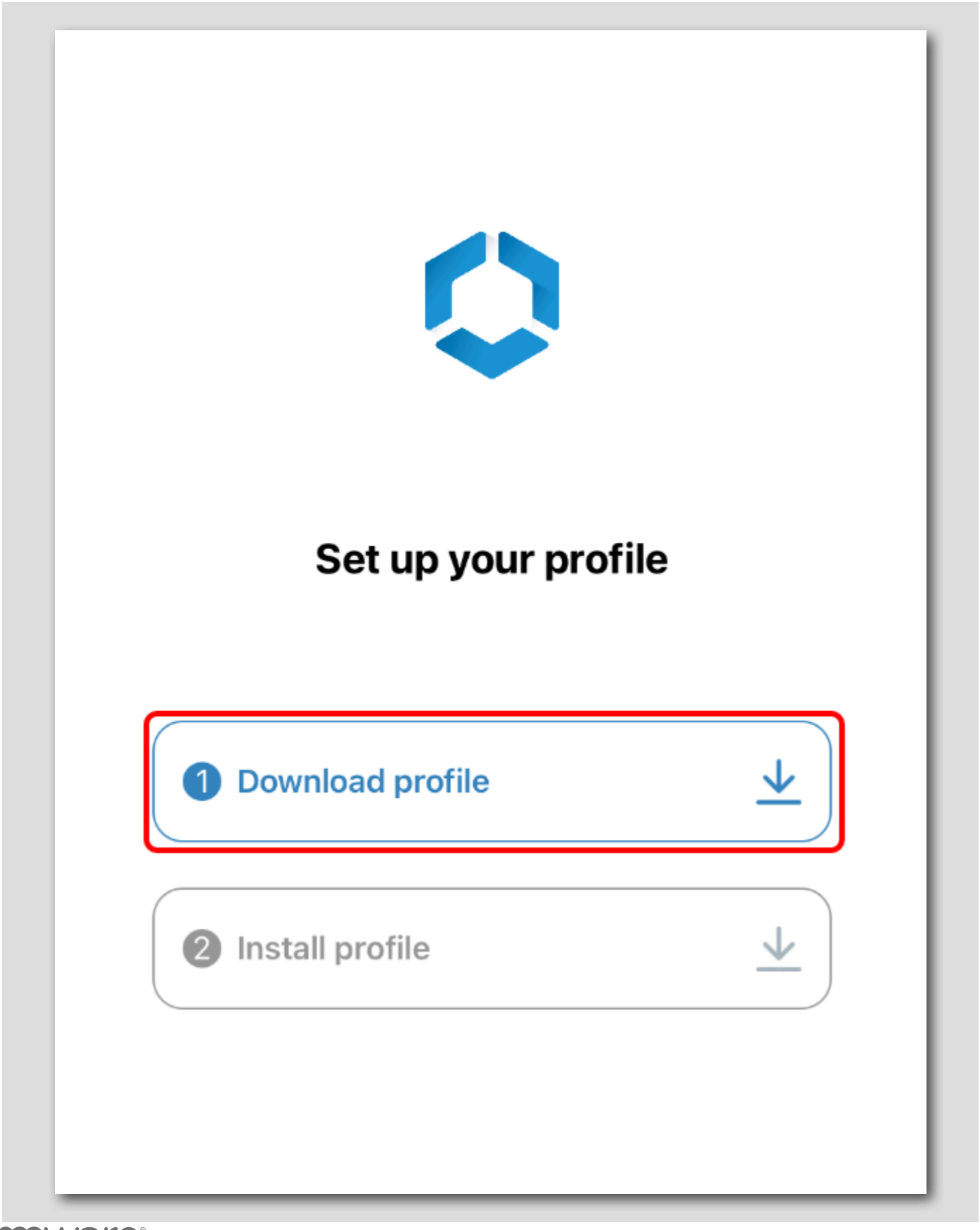

We value your privacy
We don't collect
We may collect
Messages
Keep text messages private.
Personal Email
All of your own accounts are private.
Personal Photos
We do not store nor have access to your photos.
Continue

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

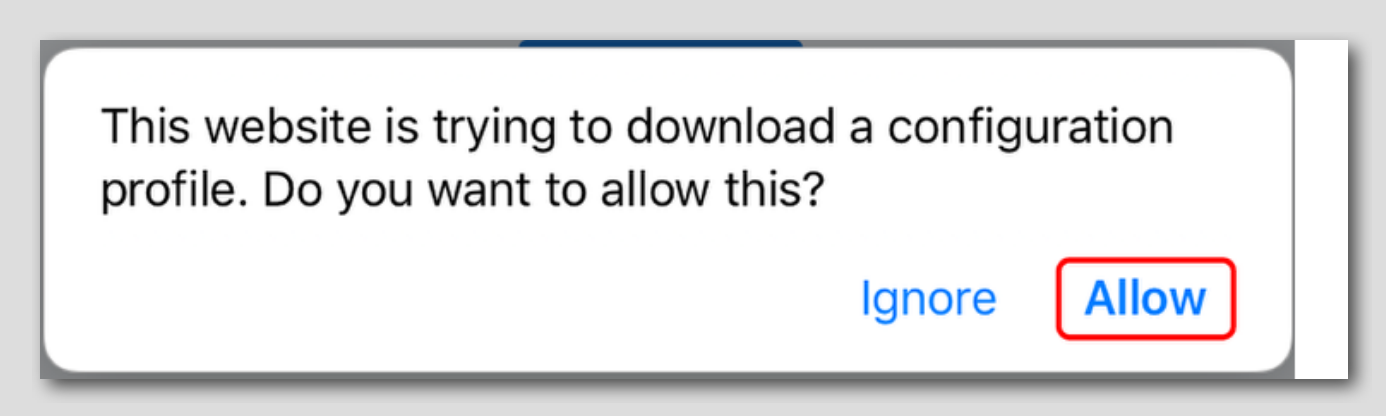

Set up your profile
1 Download profile
2 Install profile

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

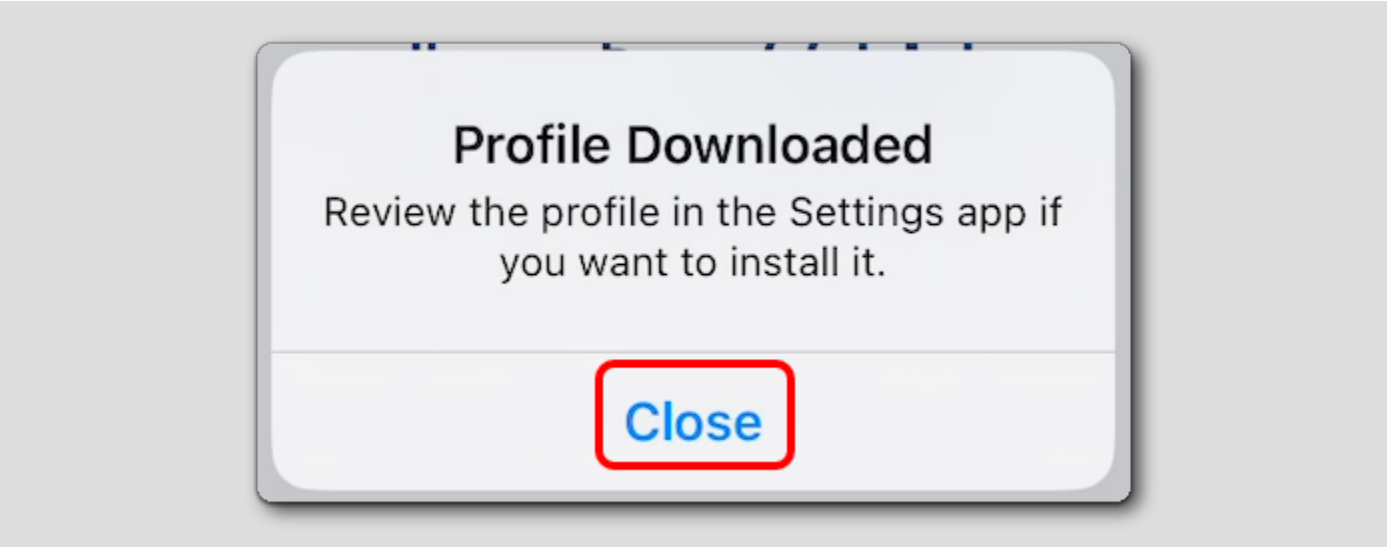
[163]



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

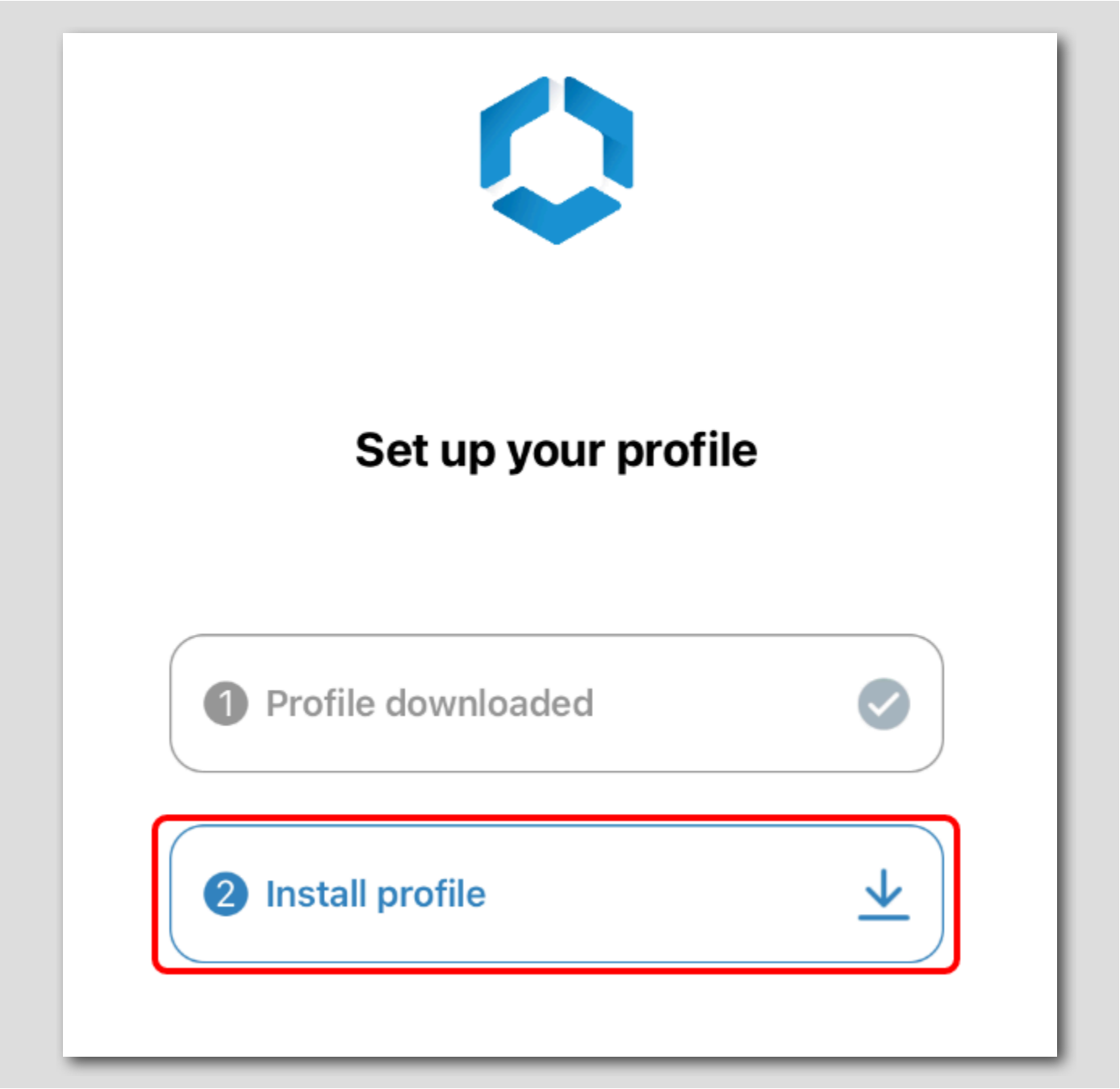
1. When prompted to download the profile, tap on **Allow**

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.

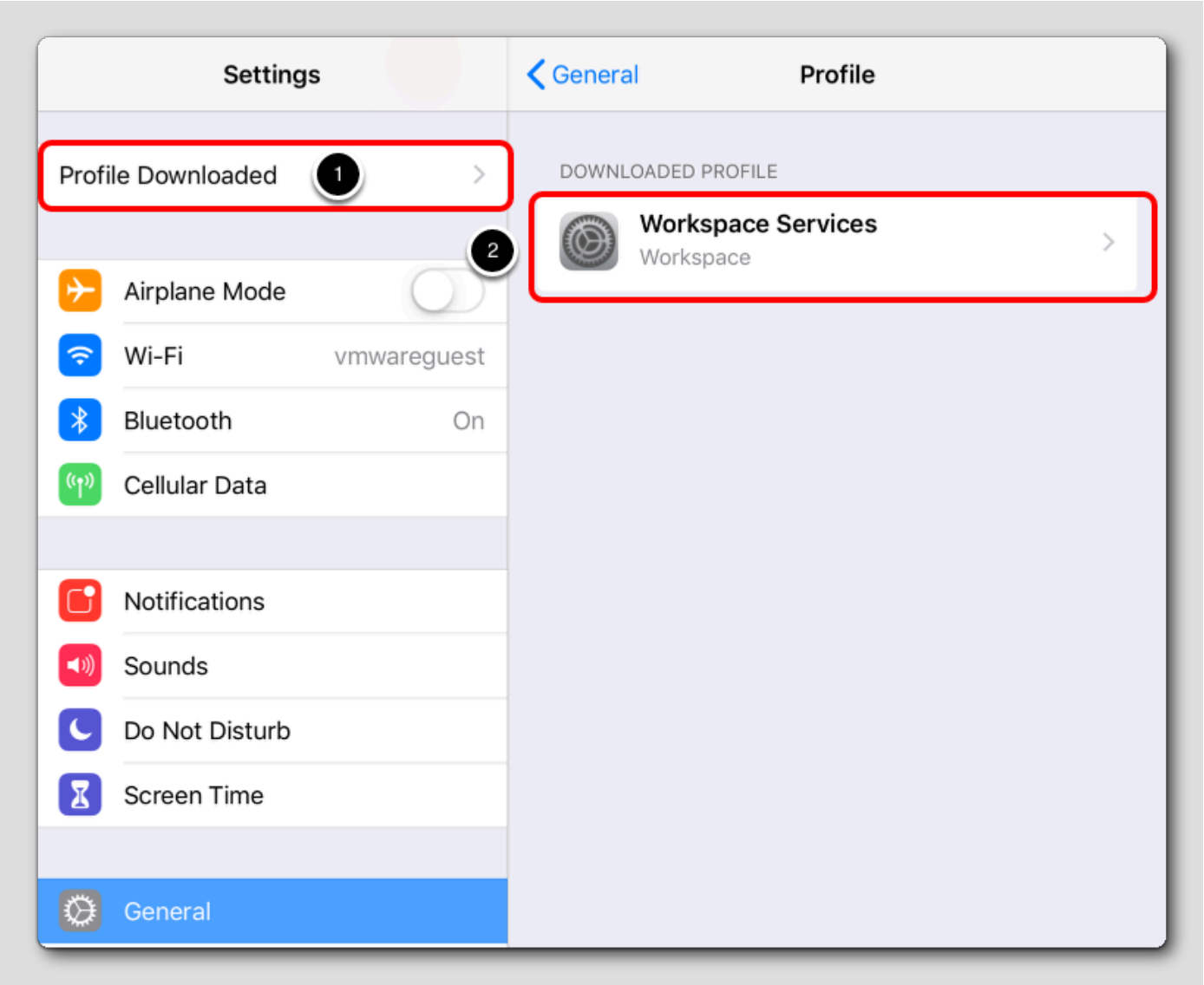
4. Once the profile is installed, return to **Hub** to complete your enrollment.

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]

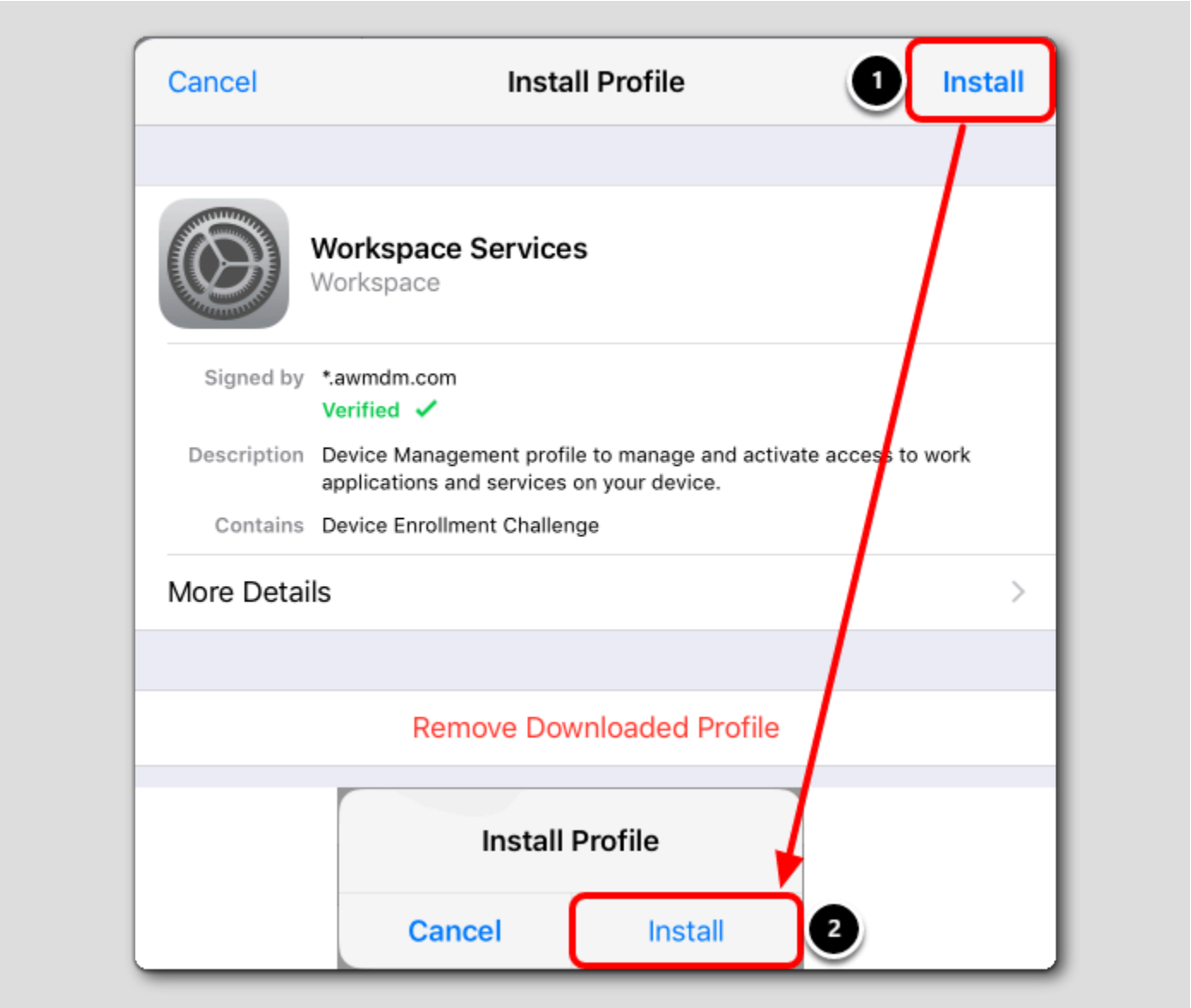


In the Settings app.

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

Install the Workspace ONE MDM Profile

[168]



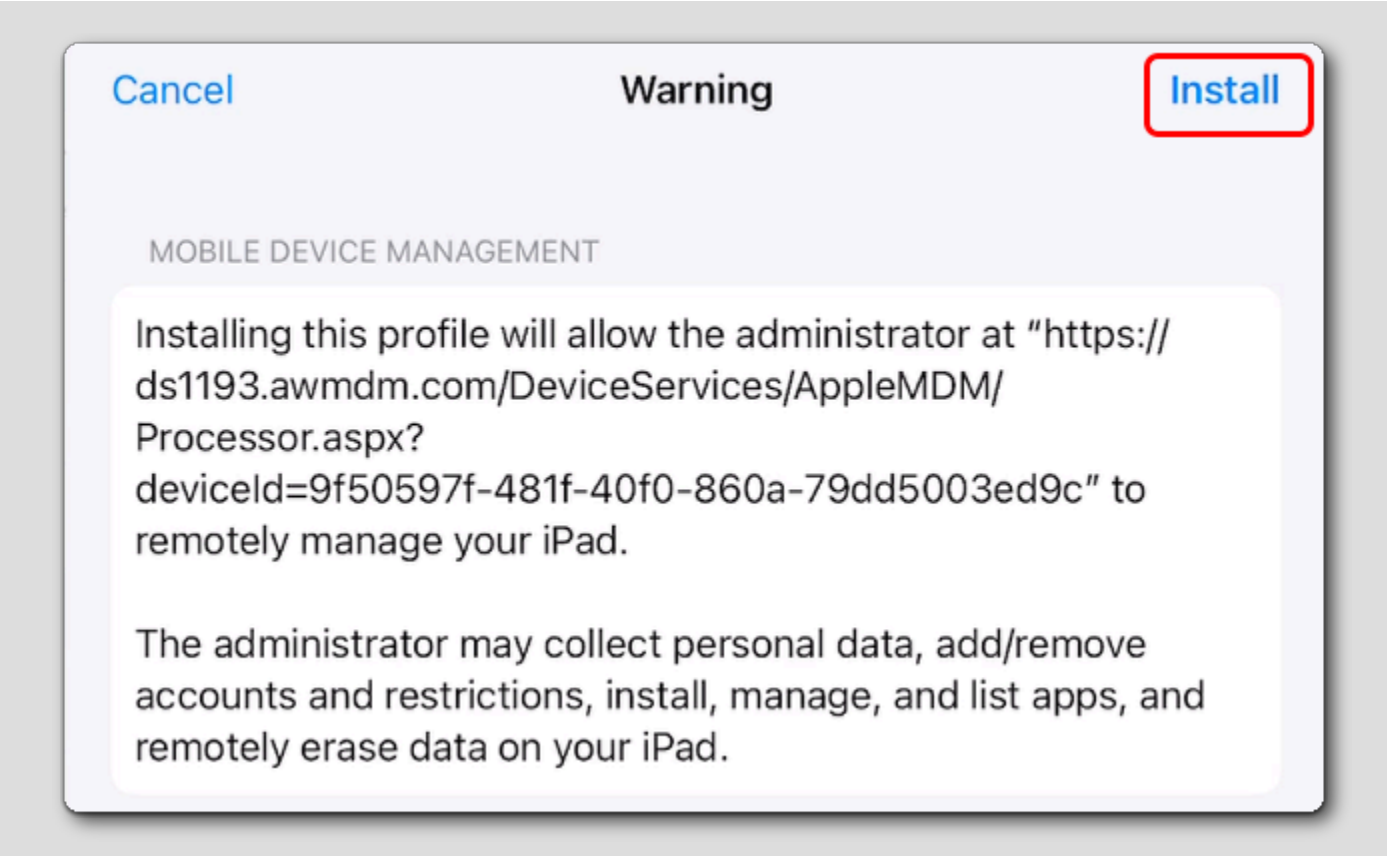
1. Tap **Install** in the upper right corner of the Install Profile dialog box.

   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

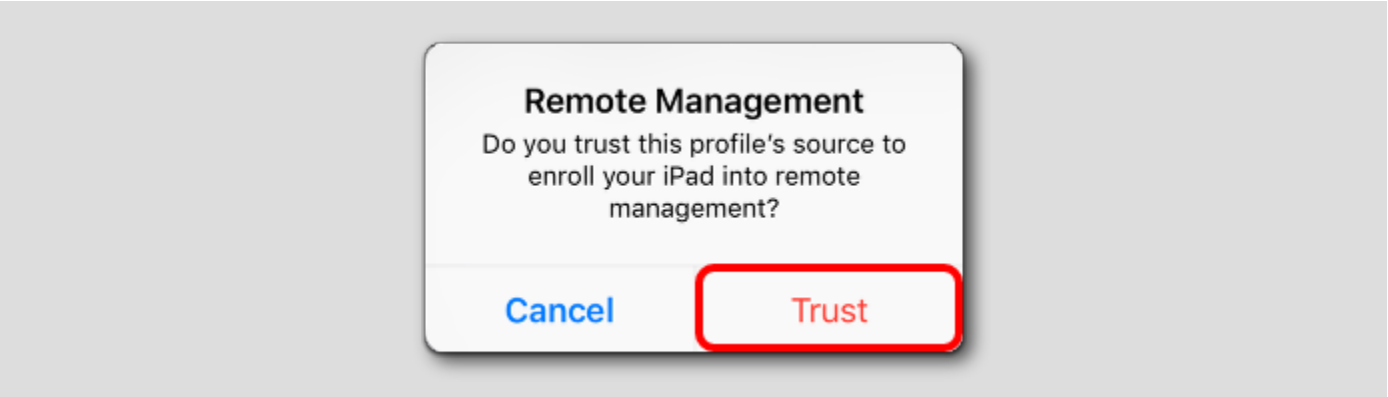
[169]



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]

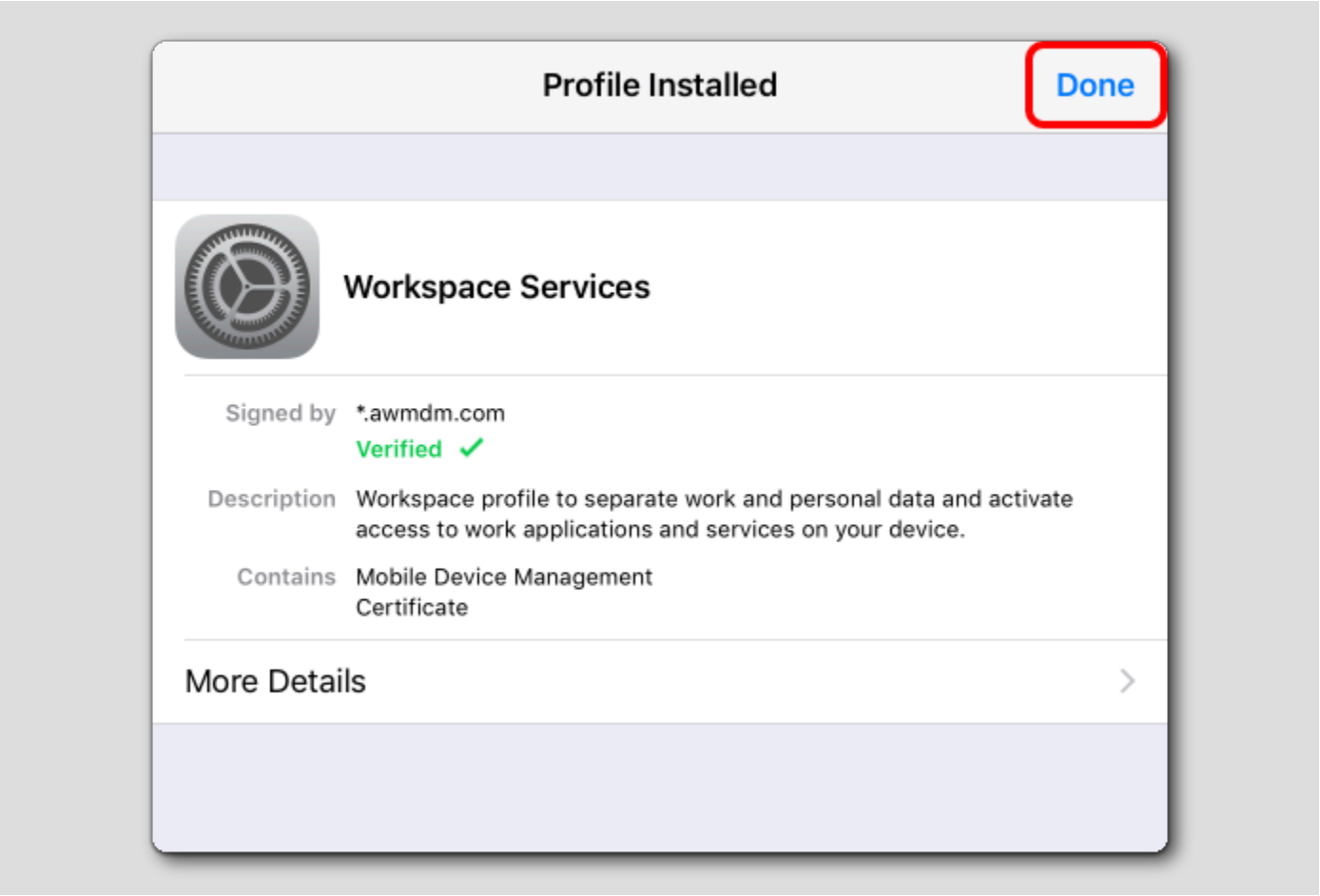


You should now see the iOS request to trust the source of the MDM profile.

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.

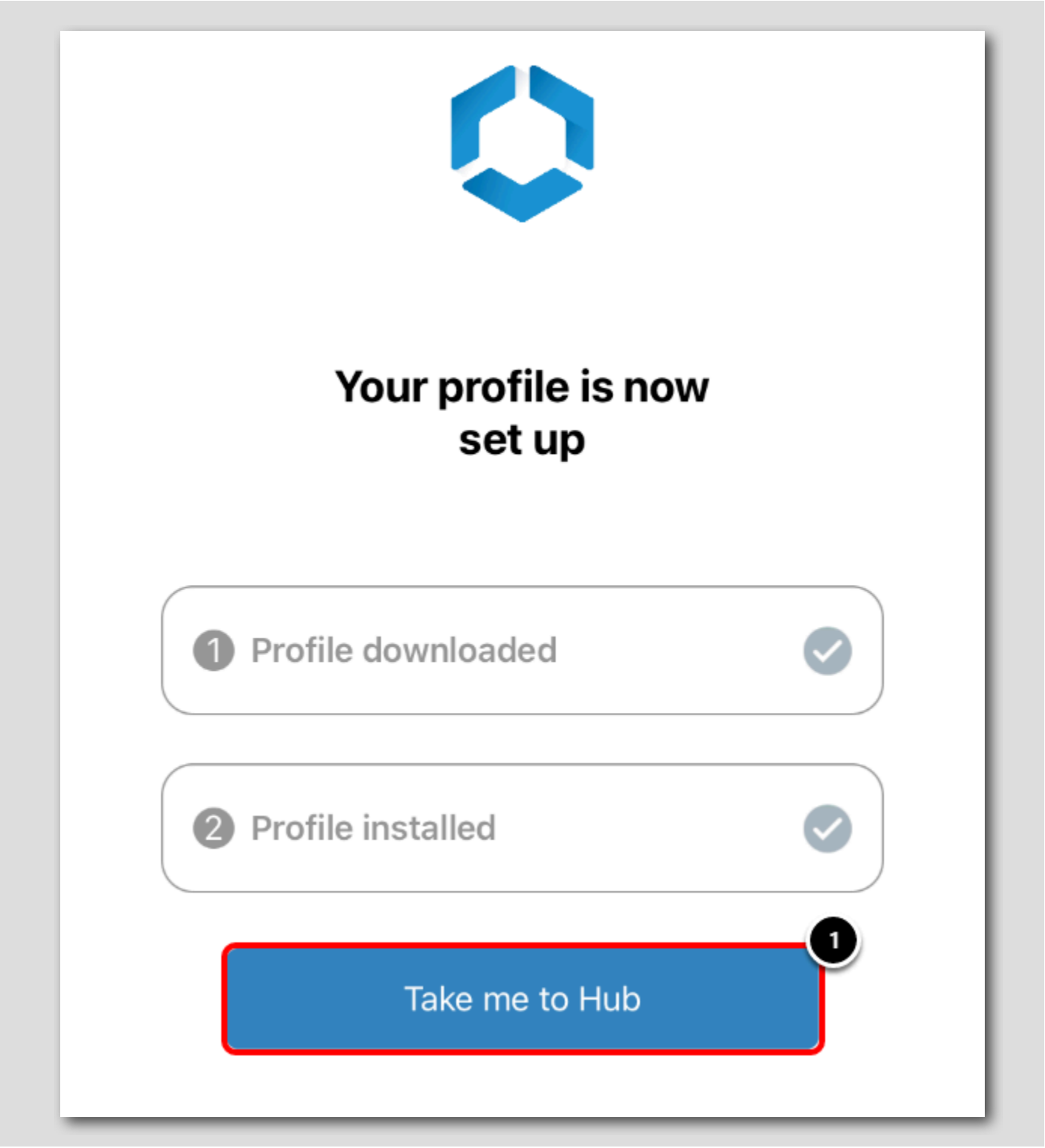
Navigate to Workspace ONE Intelligent Hub

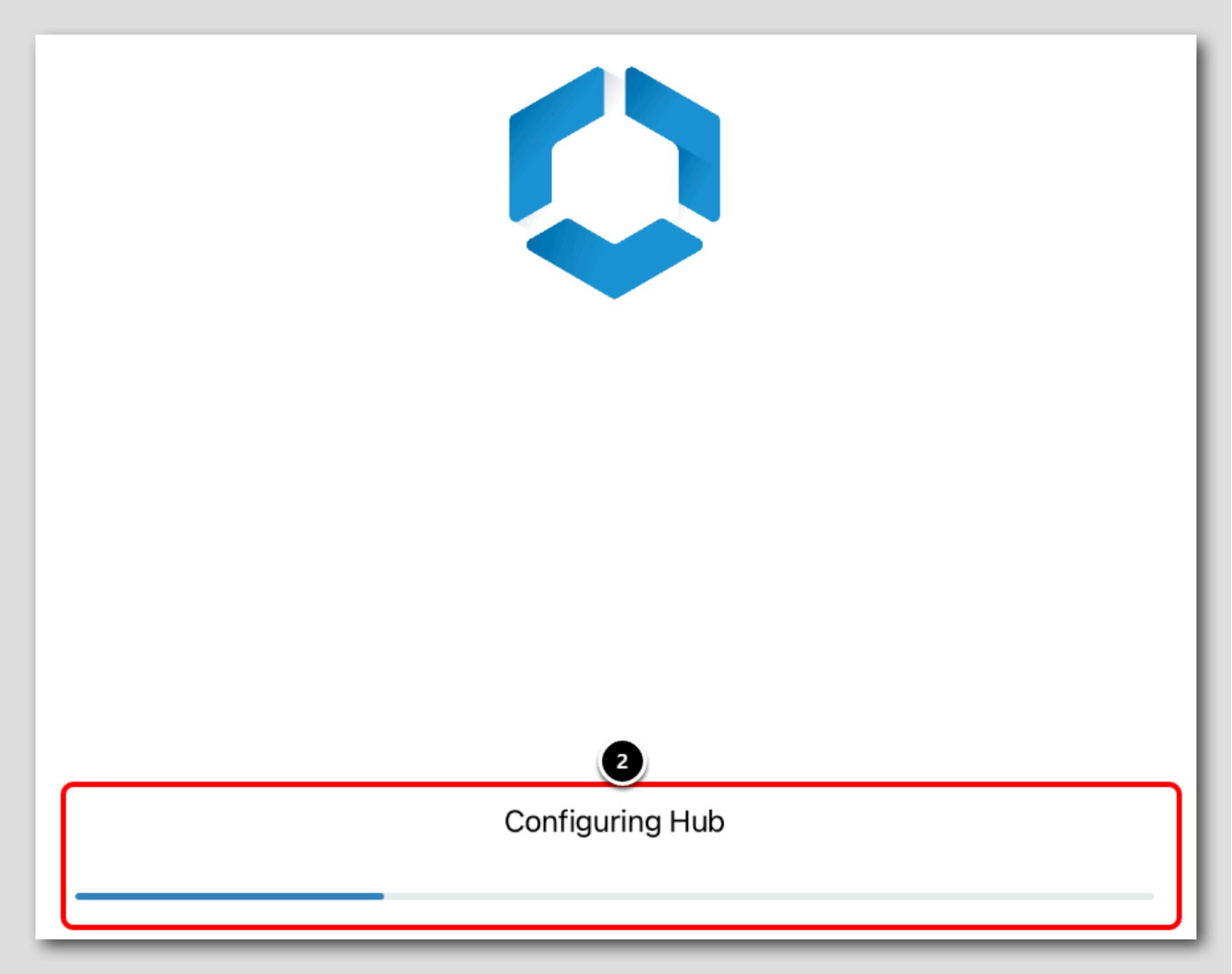
[172]

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

Continue to Hub

[173]



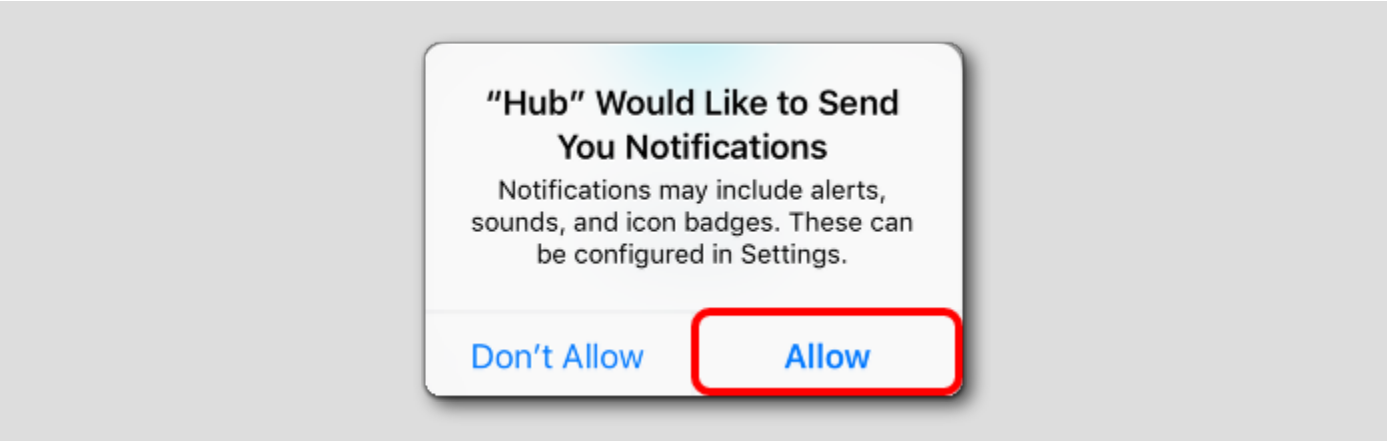


You will see that the profile is not successfully configured.

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.

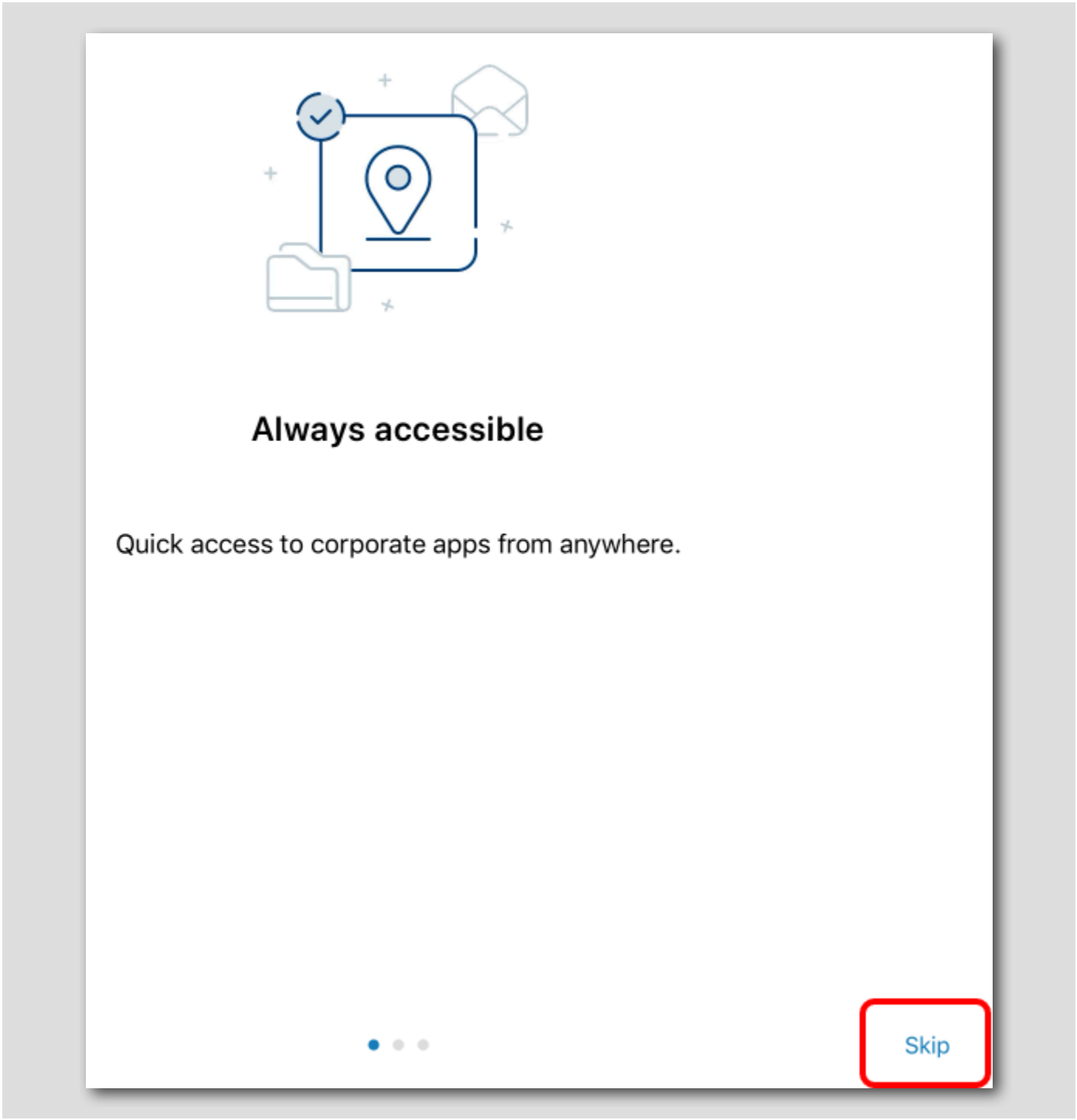
Accept Notifications for Hub (IF NEEDED)

[174]



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

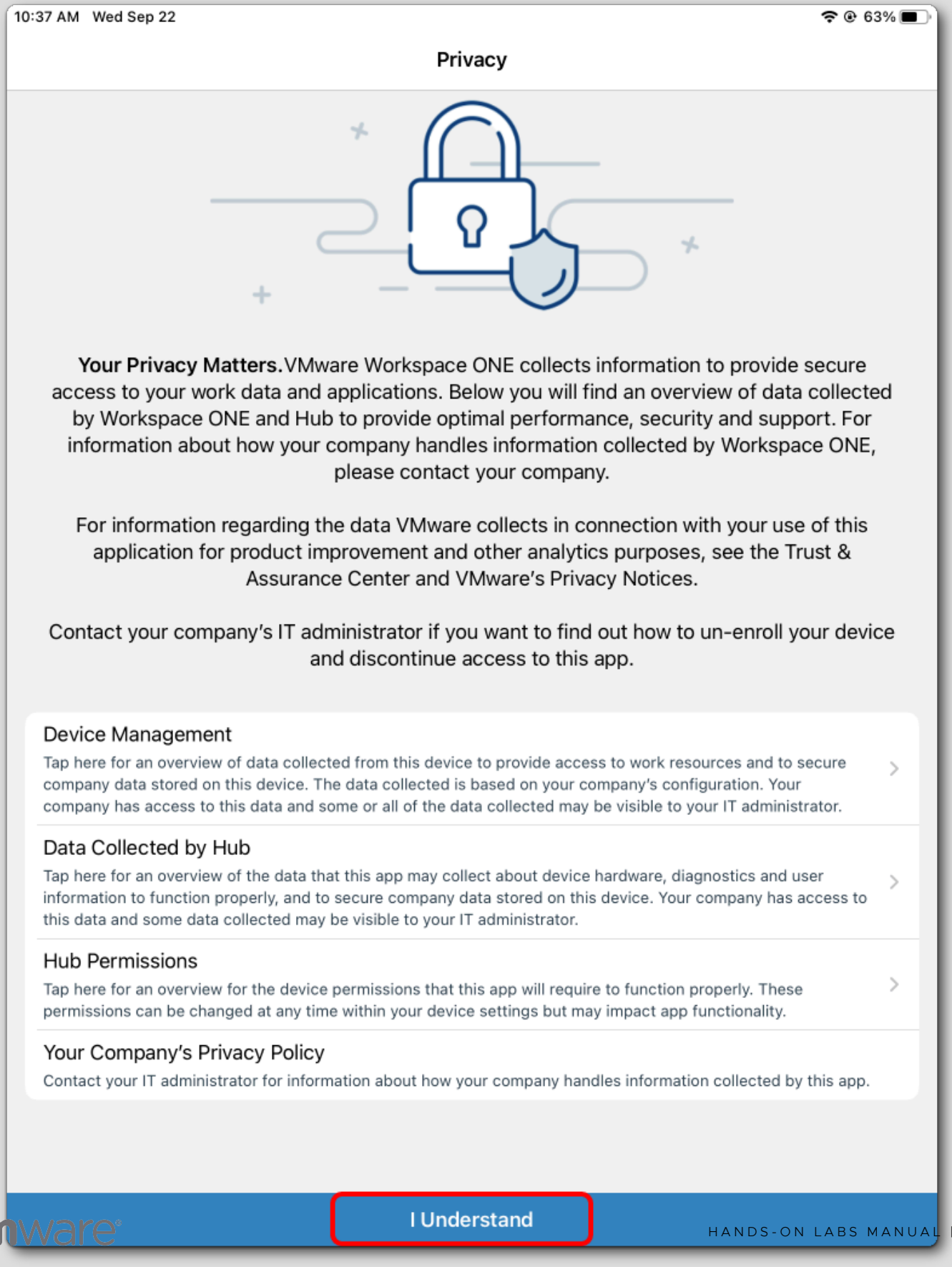
Skip the Introduction (IF PROMPTED) [175]



Click **Skip**.

Confirm the Privacy Policy

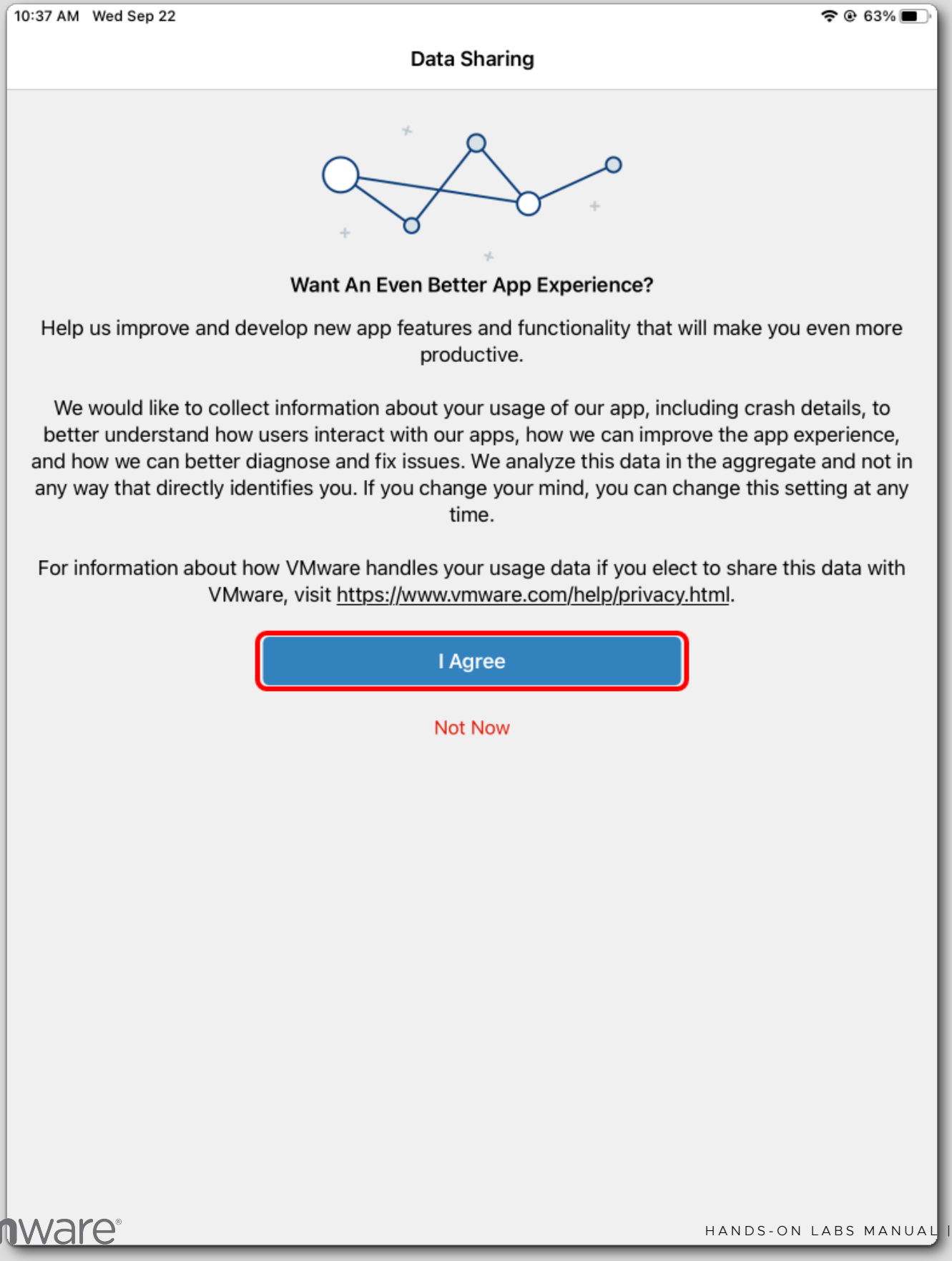
[176]


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

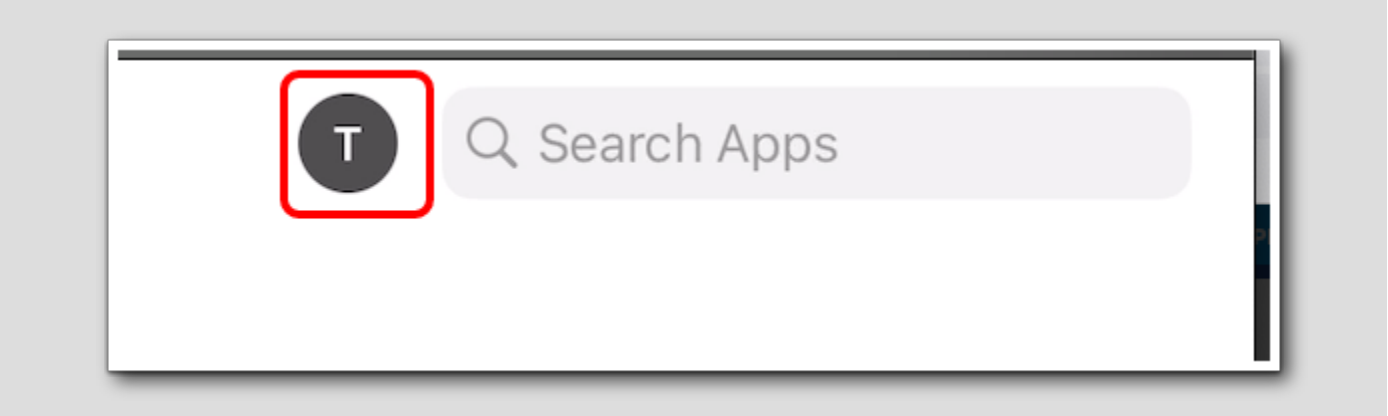
[177]

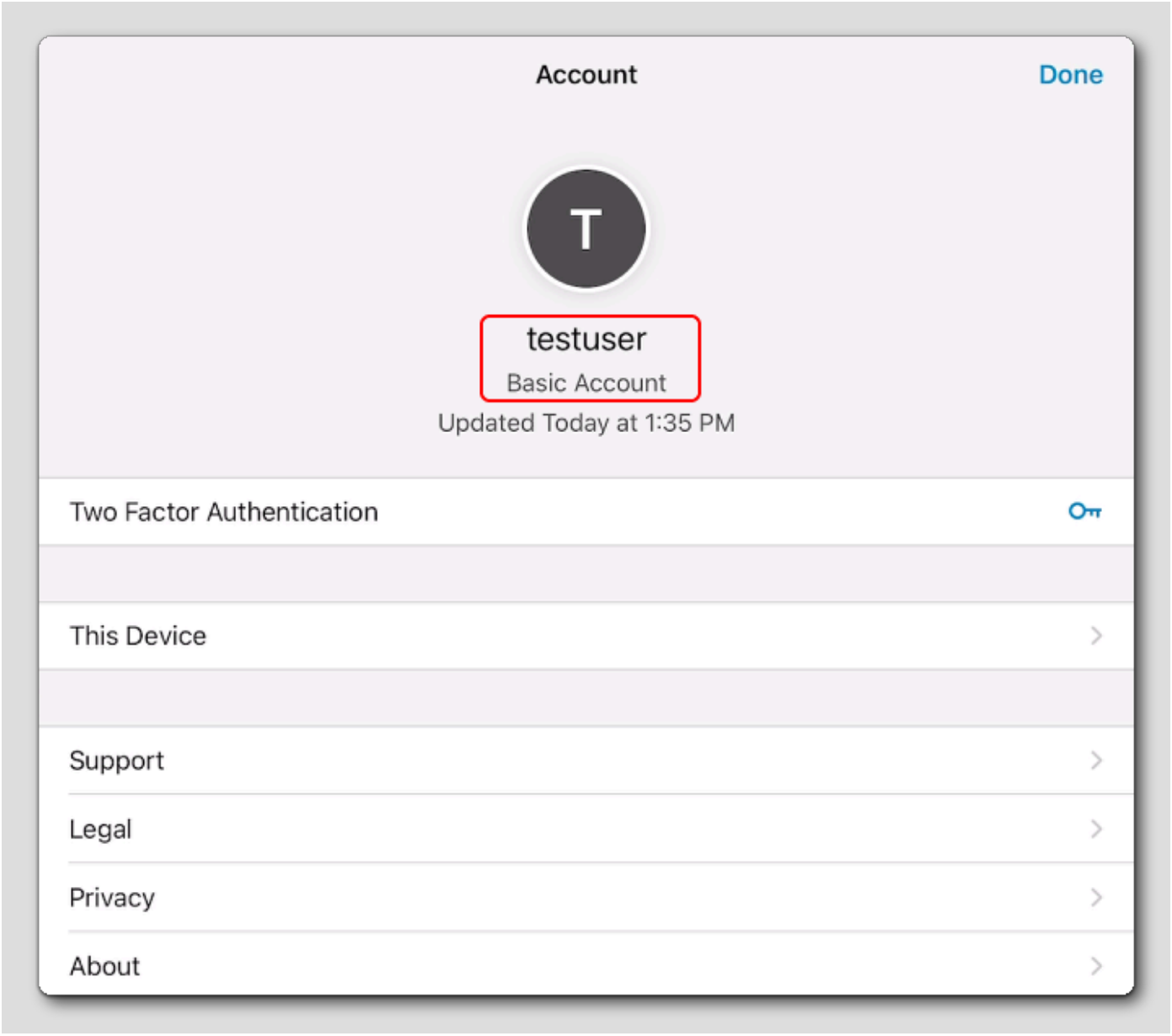

10:37 AM Wed Sep 22
63%
Data Sharing
Want An Even Better App Experience?
Help us improve and develop new app features and functionality that will make you even more productive.
We would like to collect information about your usage of our app, including crash details, to better understand how users interact 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.

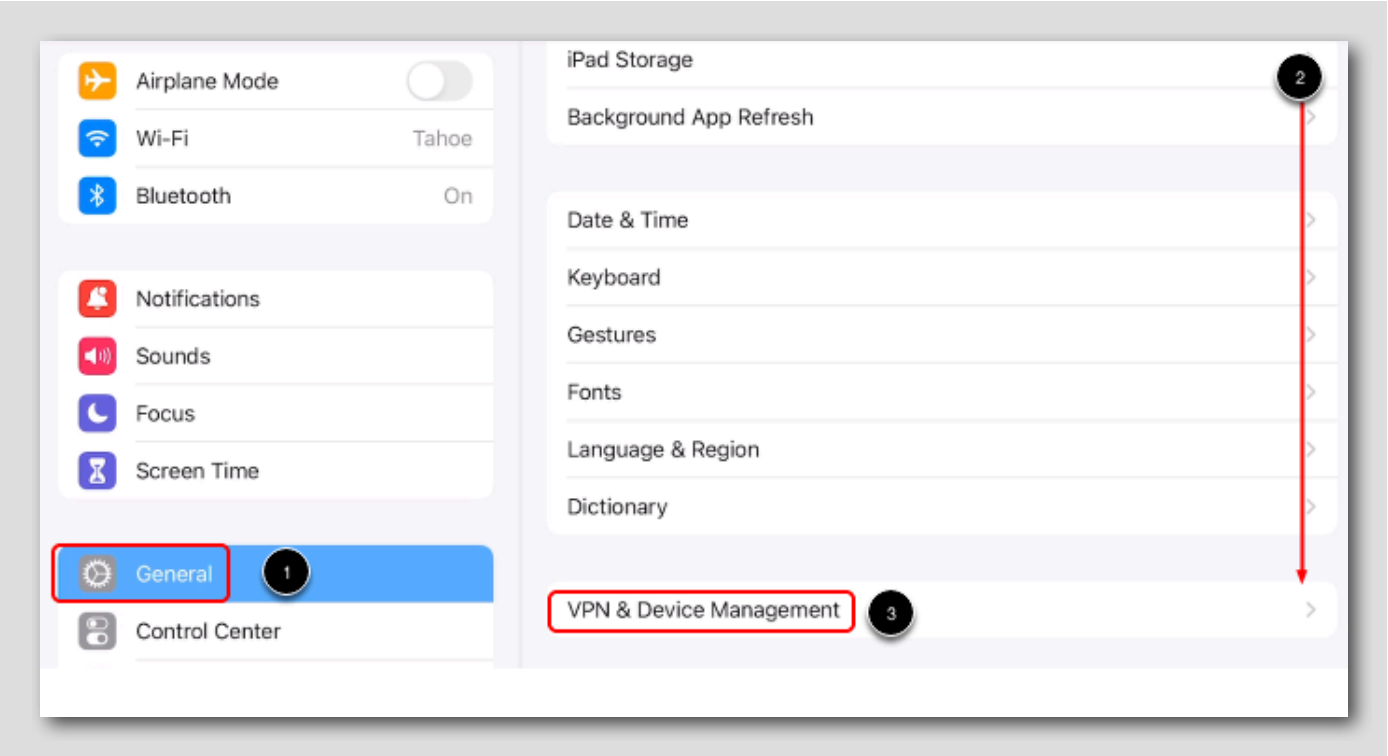
Validate the Restriction Profile in Settings

[180]

Tap the **Settings** app.

Navigate to Profiles & Device Management

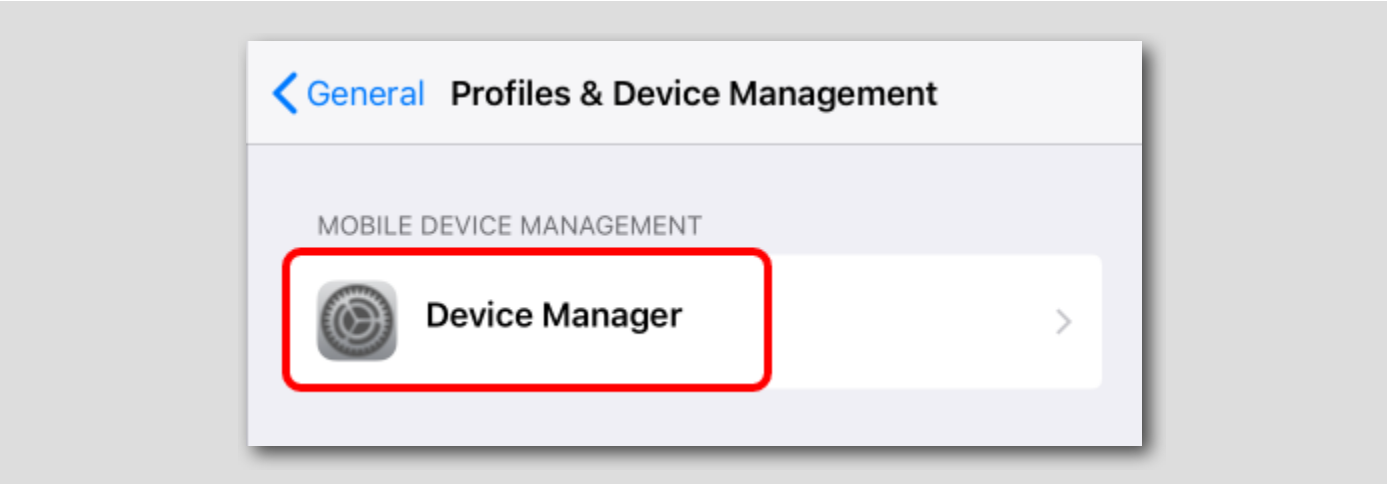
[181]



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

Open the Device Manager Profile

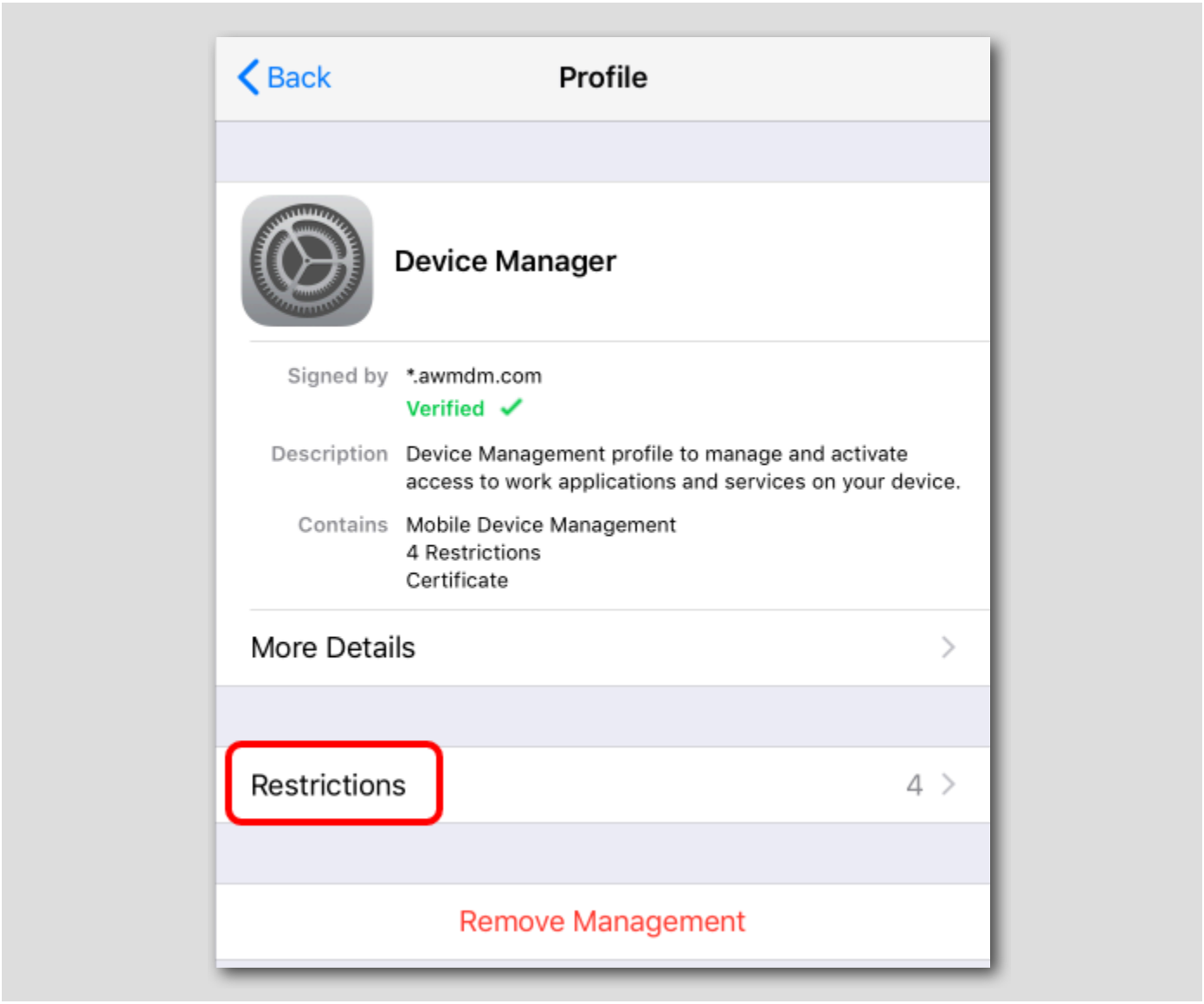
[182]



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

Inspect Restrictions

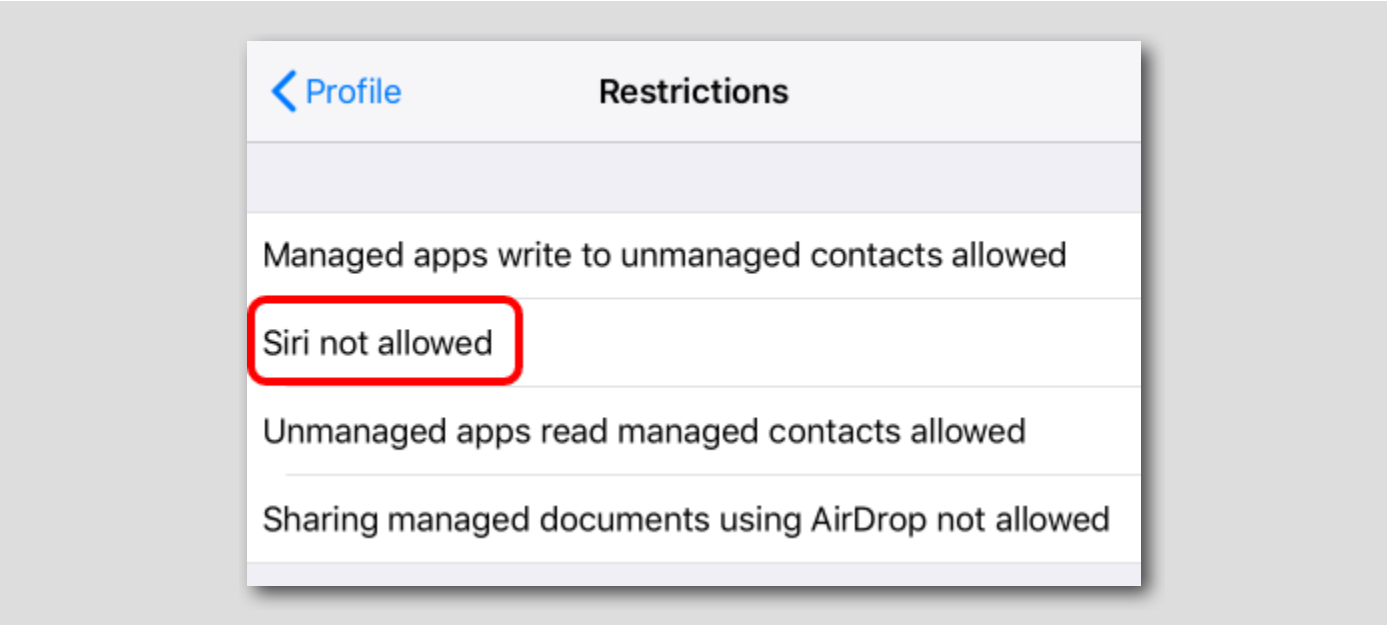
[183]



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]

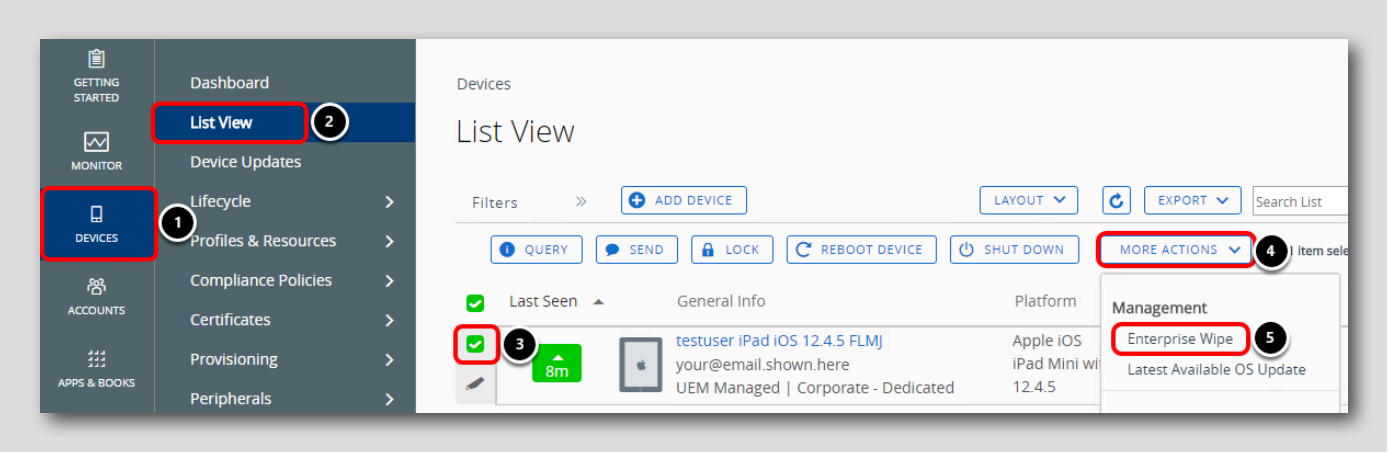
You are now going to un-enroll the iOS device from Workspace ONE UEM.

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]

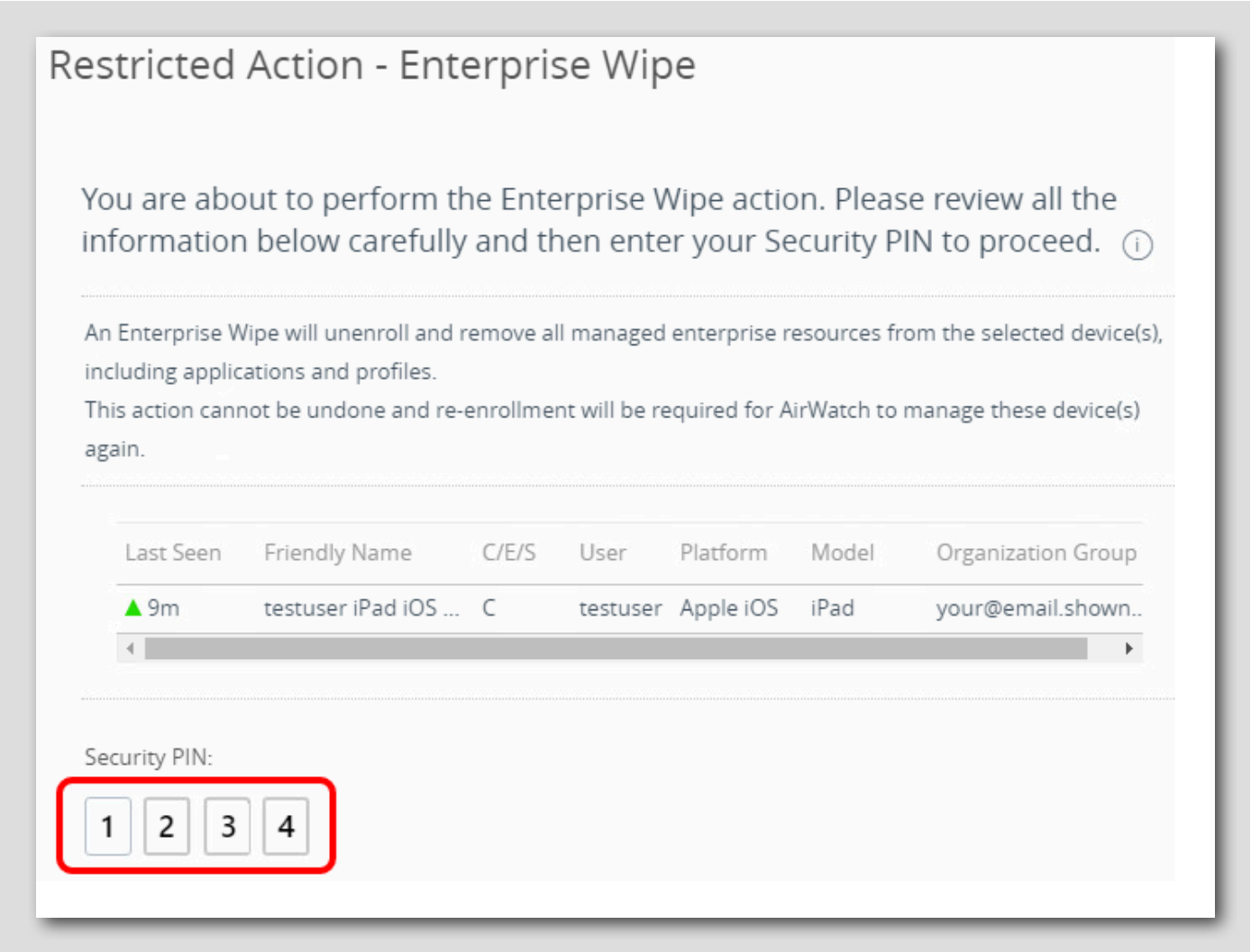


Enterprise Wiping will remove all the settings and content that were pushed to the device after it was enrolled. It will not affect anything that was on the device prior to enrollment.

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:

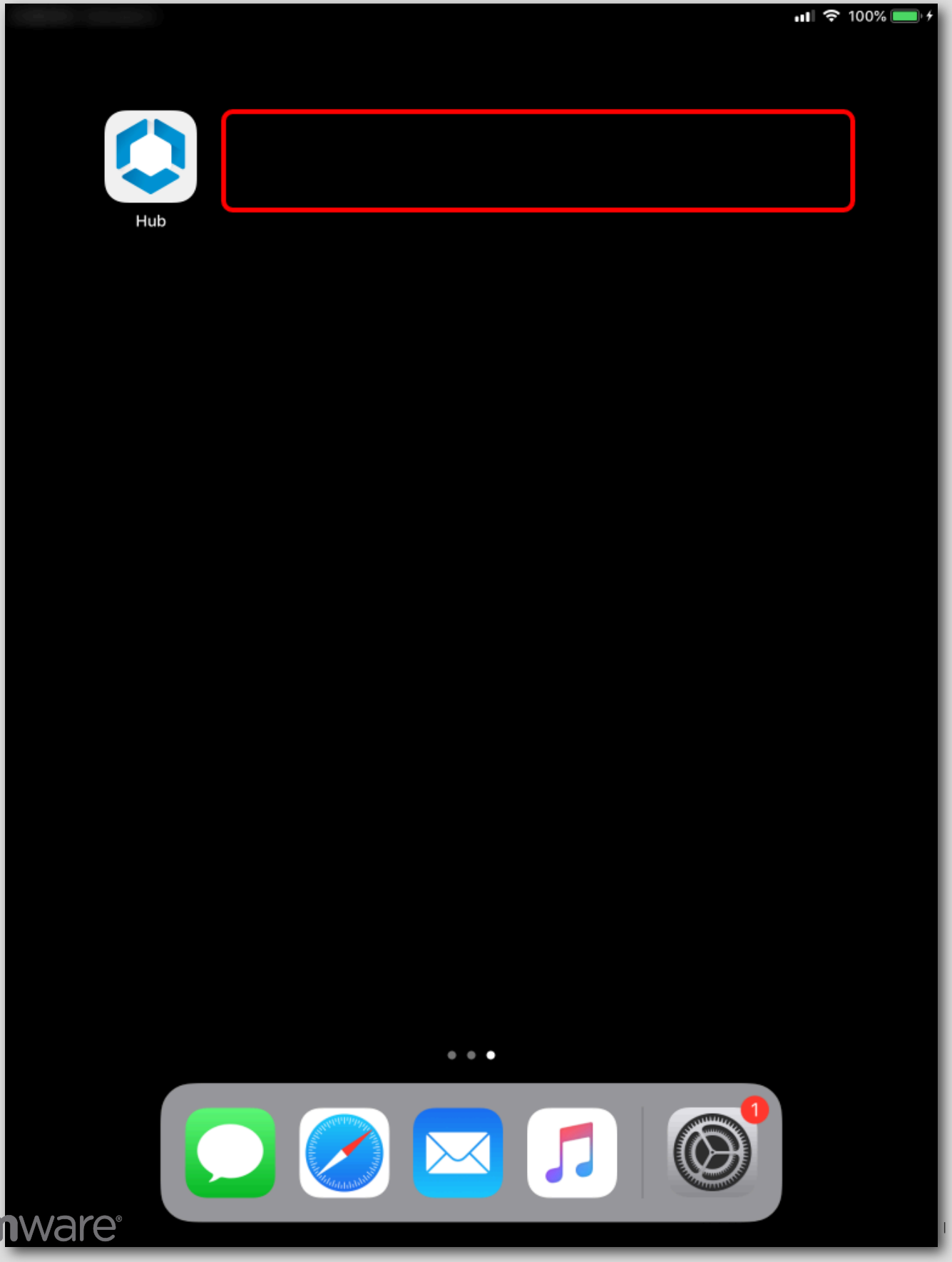
1. On your device, tap the **Workspace ONE Intelligent Hub** application
2. Tap **This Device**
3. Tap **Send Data** near the top of the screen. If this does not make the device check in and immediately un-enroll, continue to Step #4.
4. If the above doesn't make it immediately un-enroll, then tap **Connectivity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

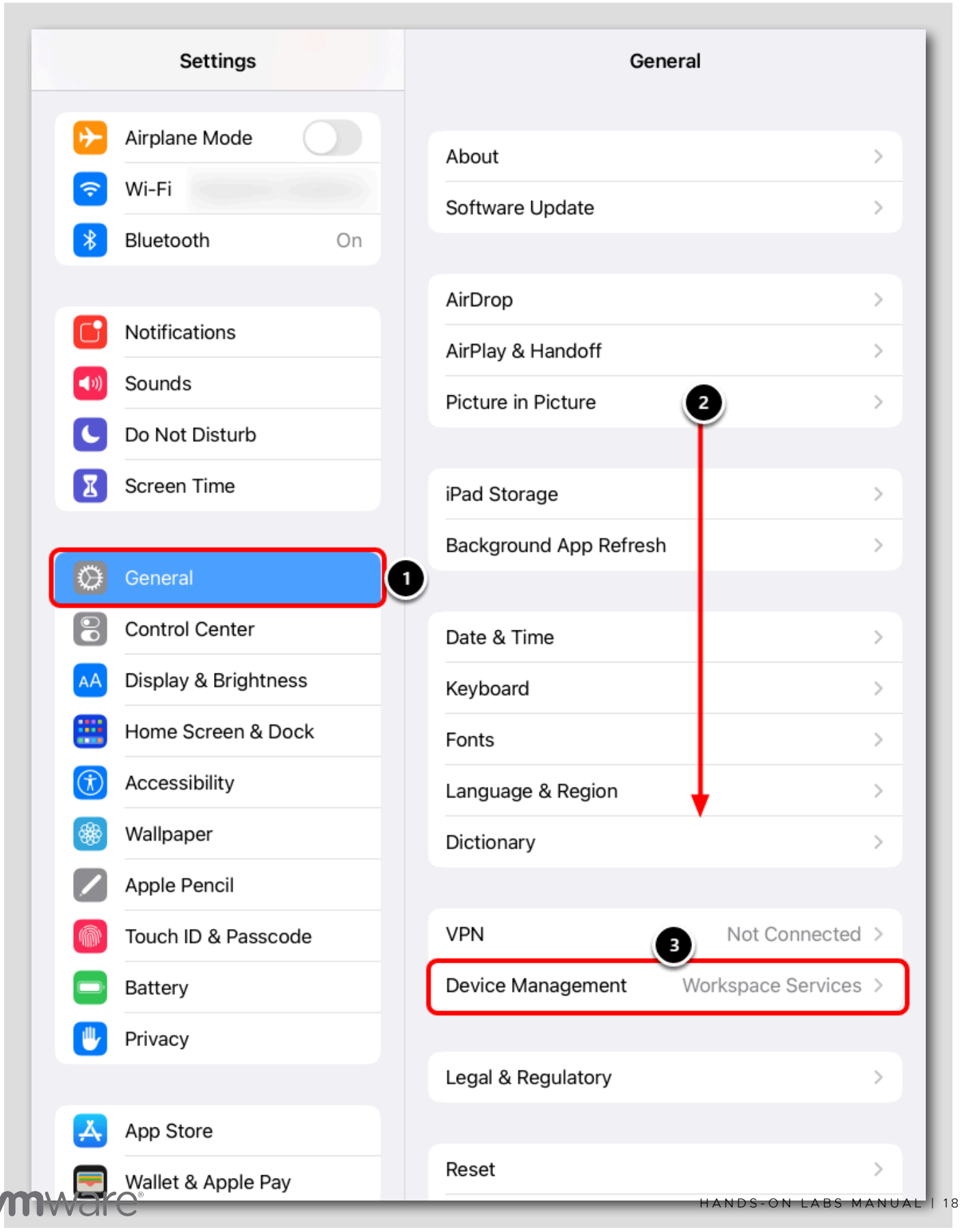
[189]


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

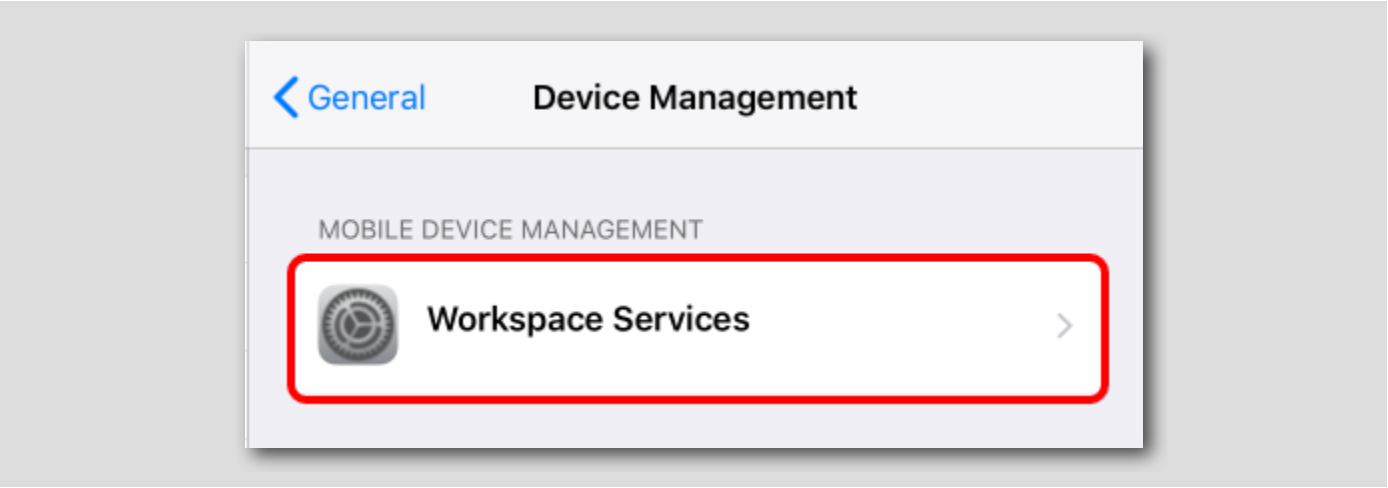

Settings
Airplane Mode
Wi-Fi
Bluetooth
On
Notifications
Sounds
Do Not Disturb
Screen Time
General
1
Control Center
Display & Brightness
Home Screen & Dock
Accessibility
Wallpaper
Apple Pencil
Touch ID & Passcode
Battery
Privacy
App Store
Wallet & Apple Pay
General
About
Software Update
AirDrop
AirPlay & 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

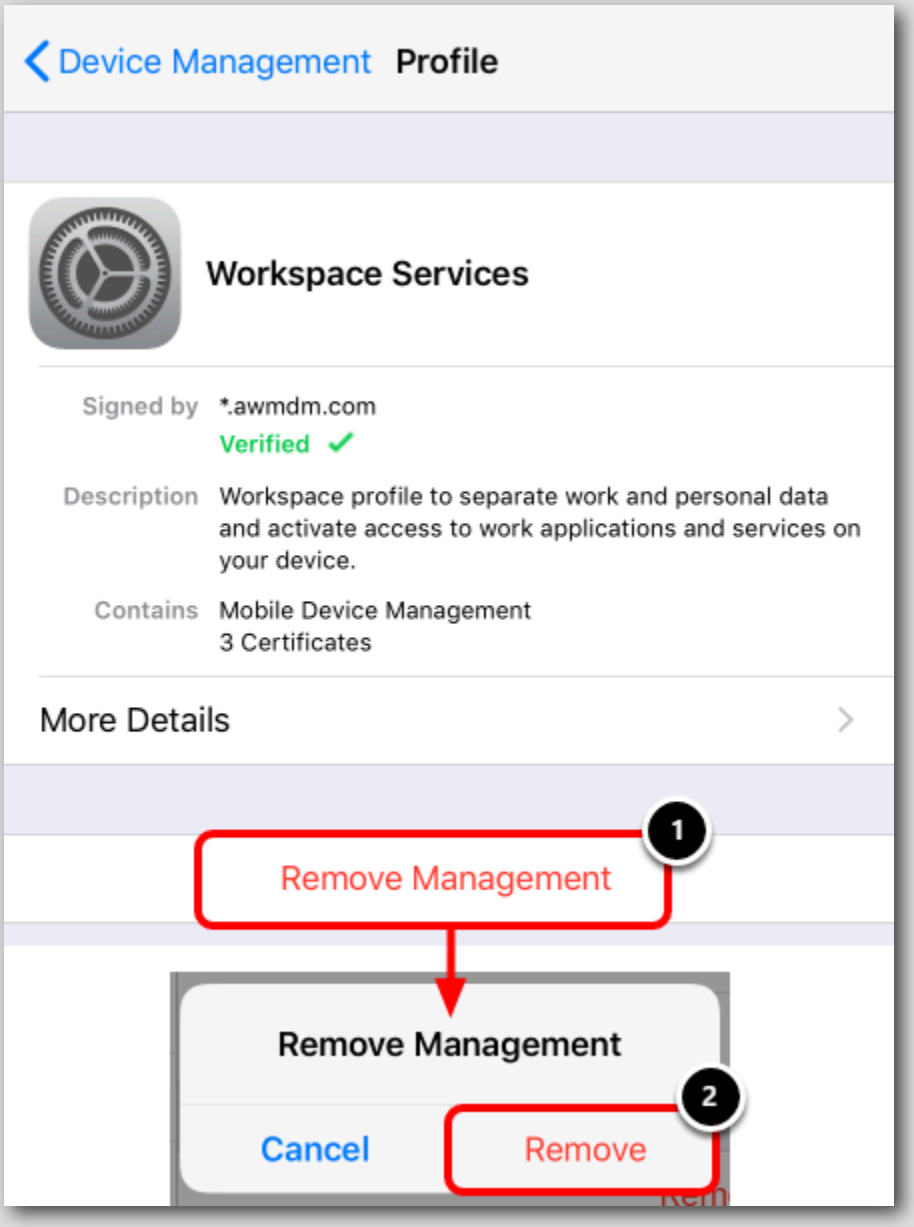
[191]



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.

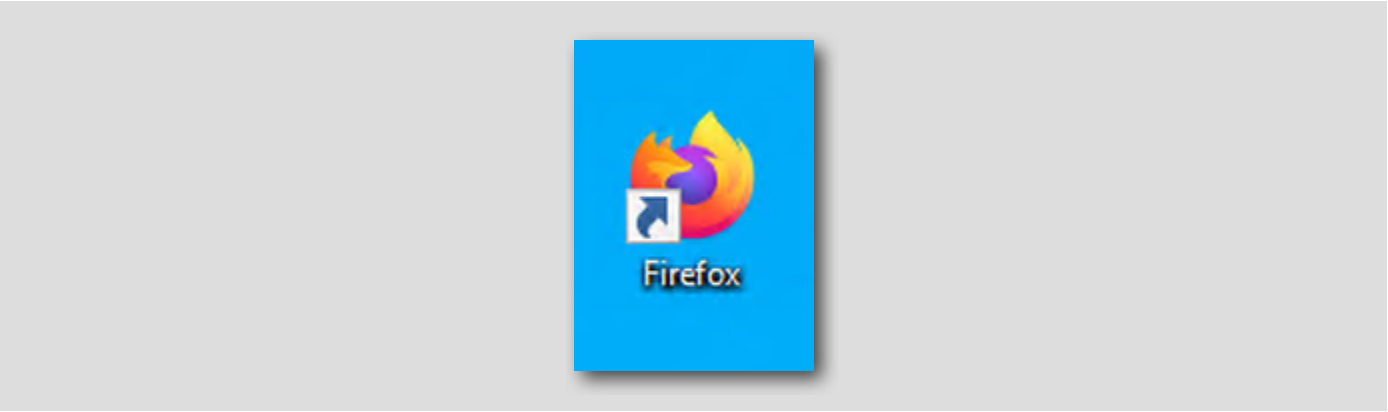
Login to the Workspace ONE UEM Console

[200]

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

Launch Firefox Browser

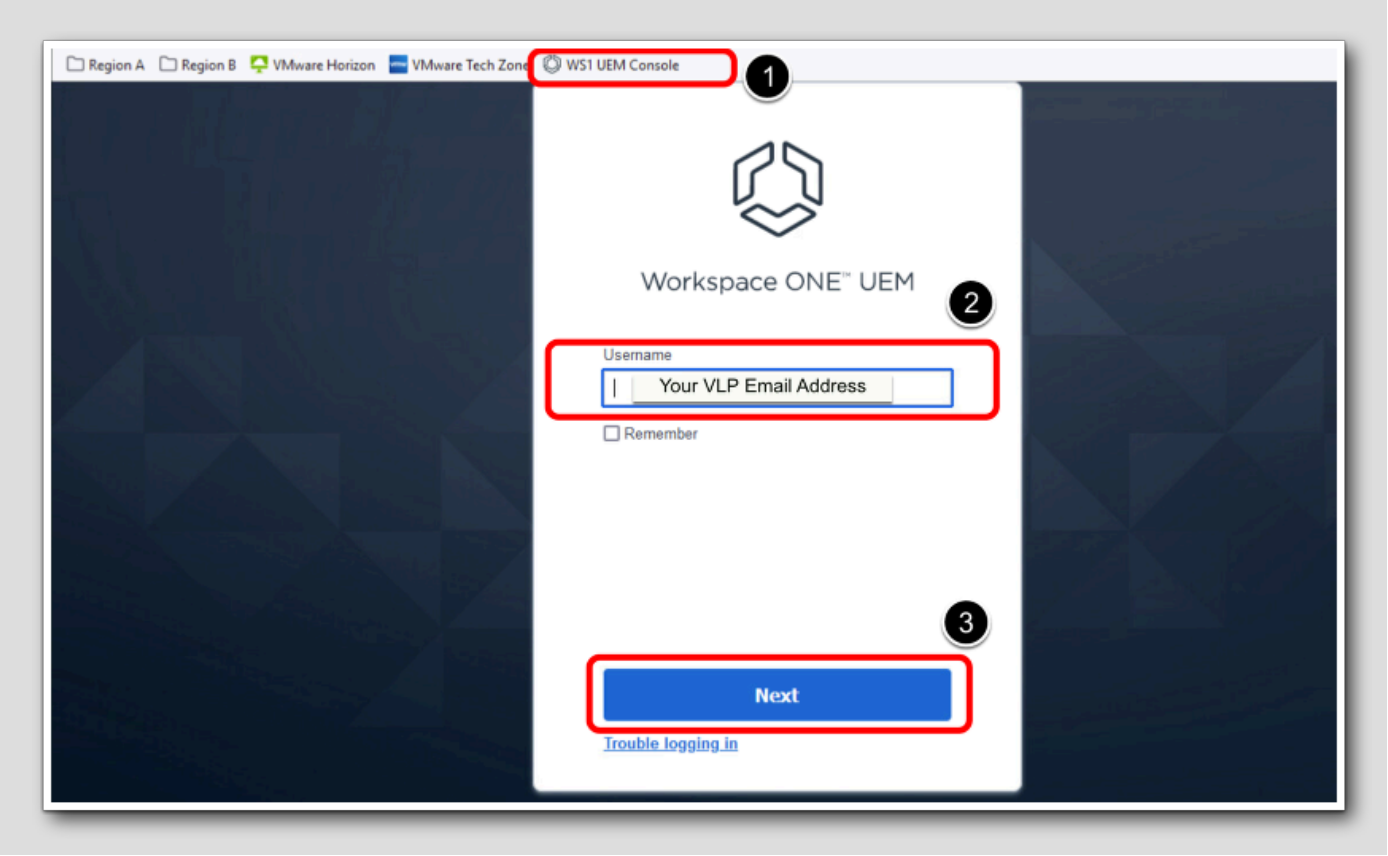
[201]



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]

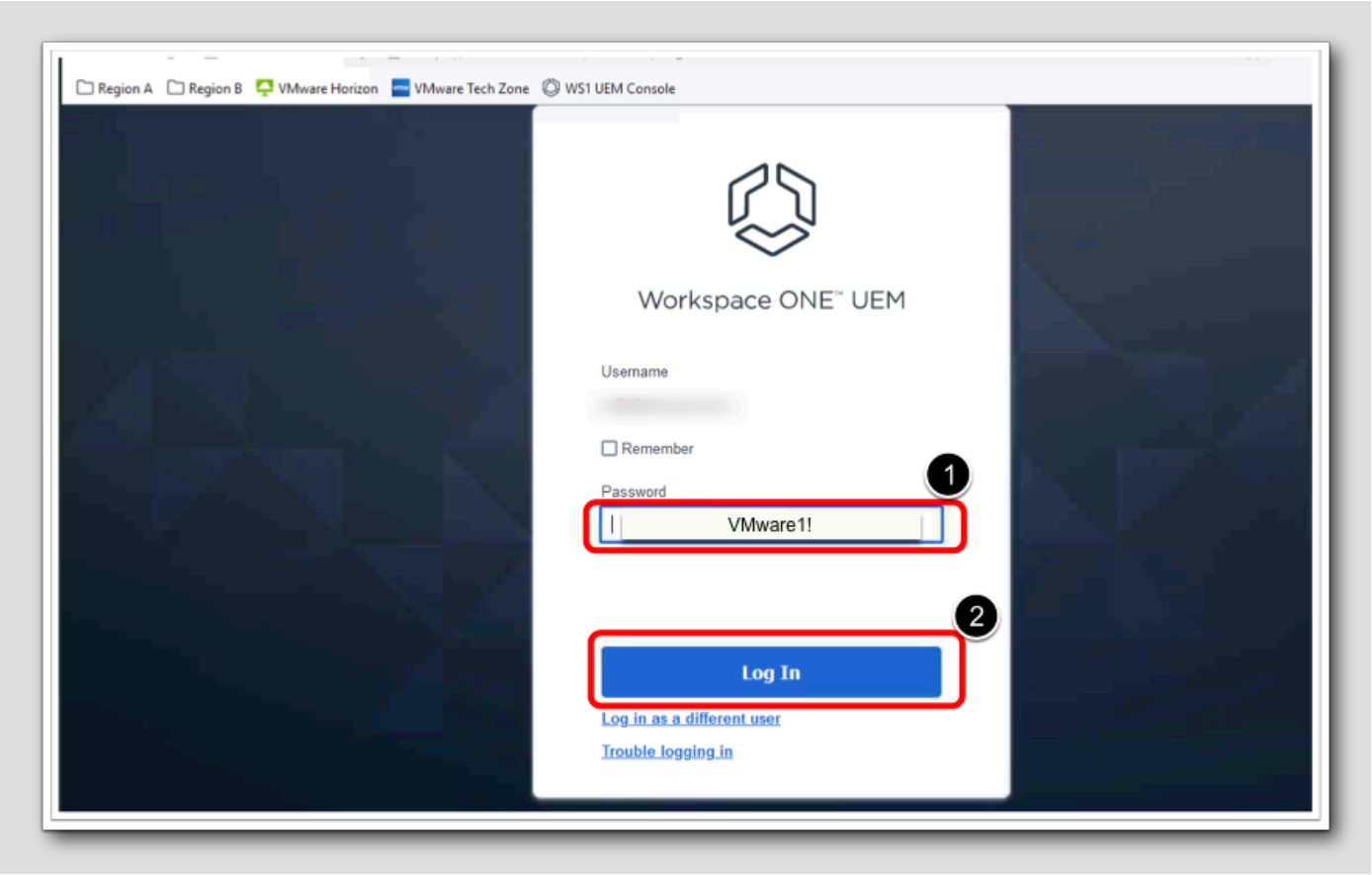


1. Select the **WS1 UEM Console** link from the Bookmark Toolbar
2. Enter your **Username**. This is the **email address** that you have associated with your **VMware Learning Platform (VLP)** account that you utilized to take Hands-on Labs.
3. Click **Next**, then advance to the next step of the lab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



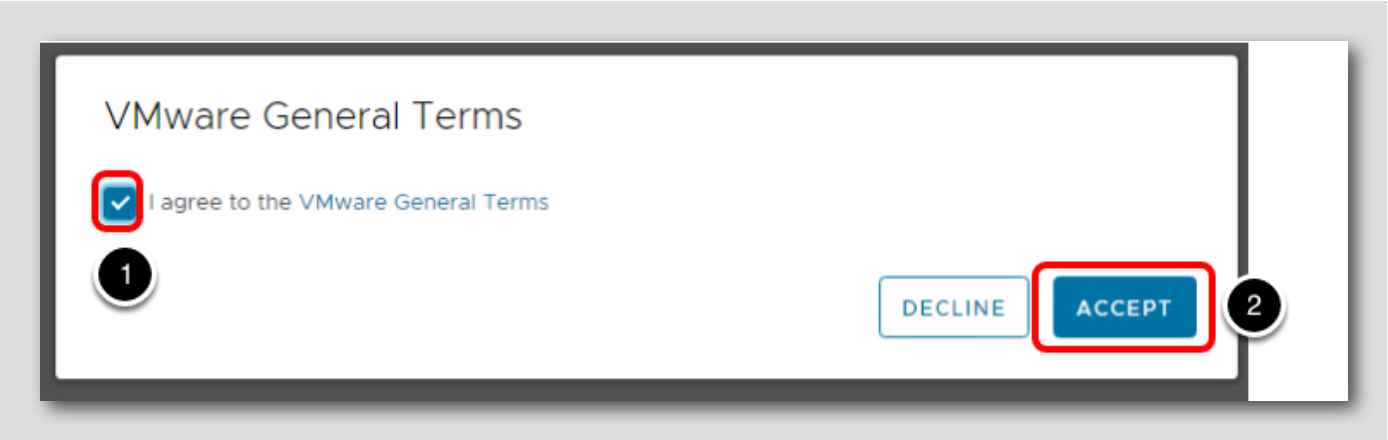
The password field will be displayed after entering your username.

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.

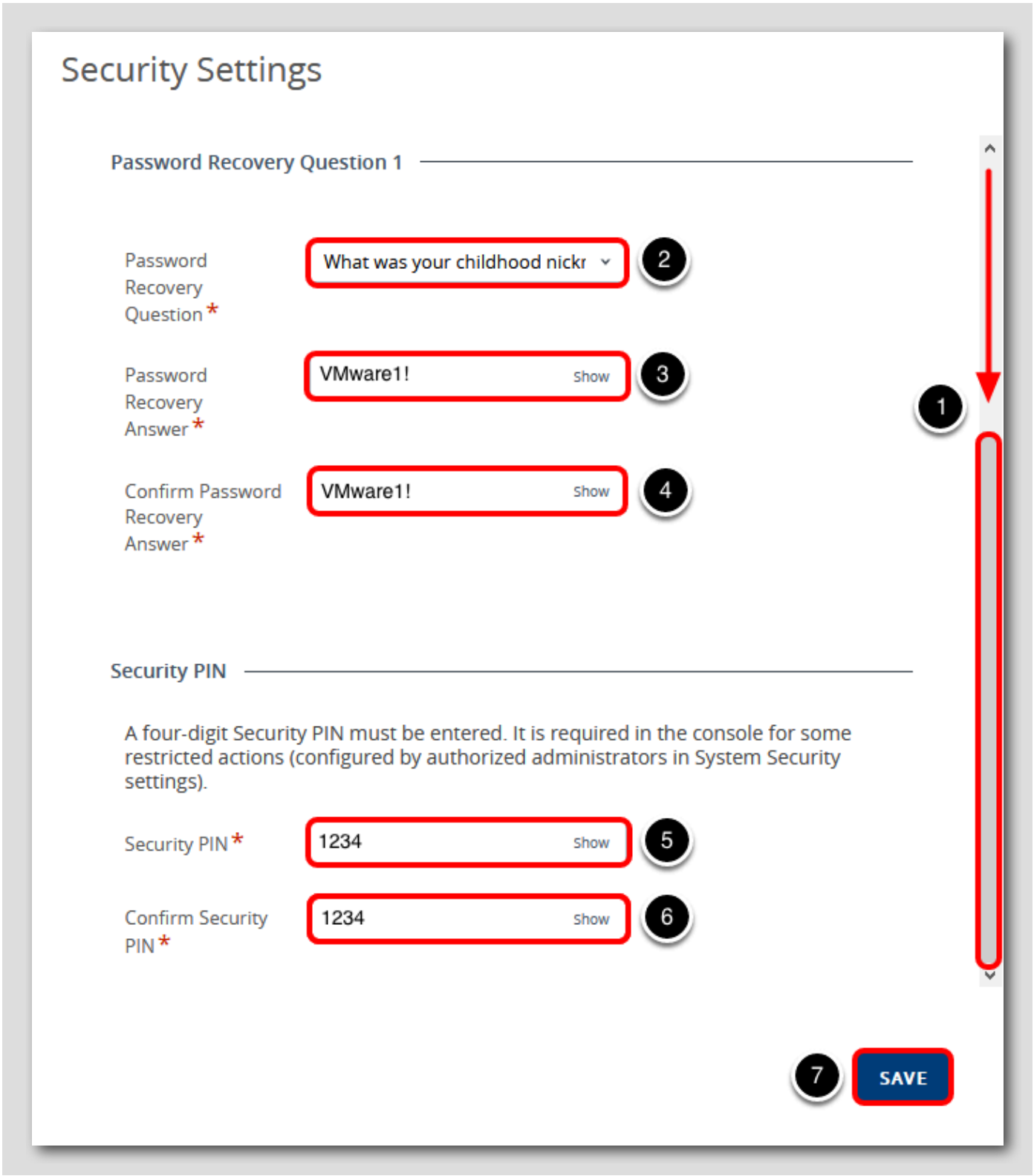
1. Select the box next to I Agree to the VMware General Terms.
2. Click the **Accept** button.

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

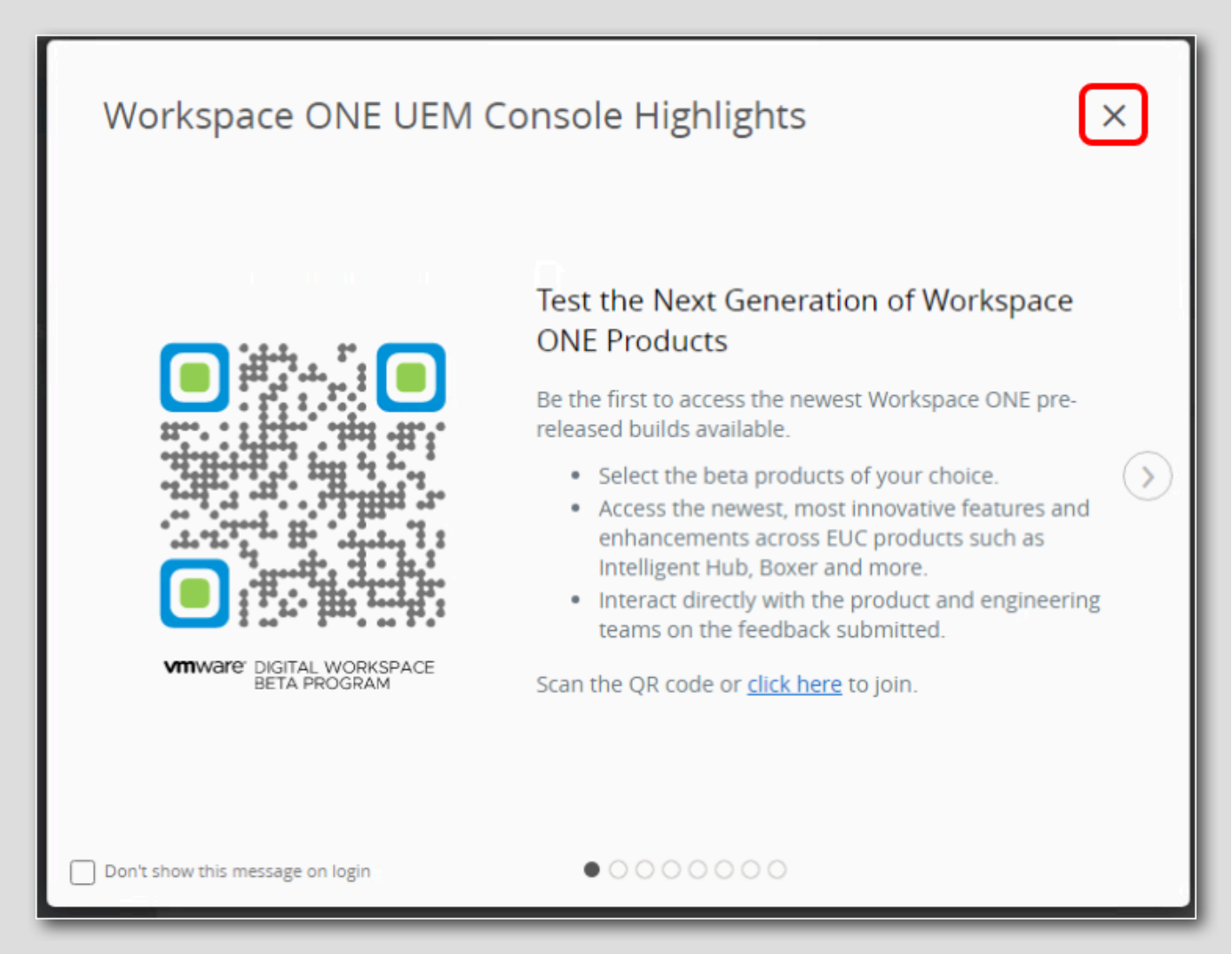

Security Settings
Password Recovery Question 1
Password Recovery Question *
What was your childhood nickr
2
Password Recovery Answer *
VMware1!
Show
3
Confirm Password Recovery Answer *
VMware1!
Show
4
1
Security PIN
A four-digit Security PIN must be entered. It is required in the console for some restricted 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]

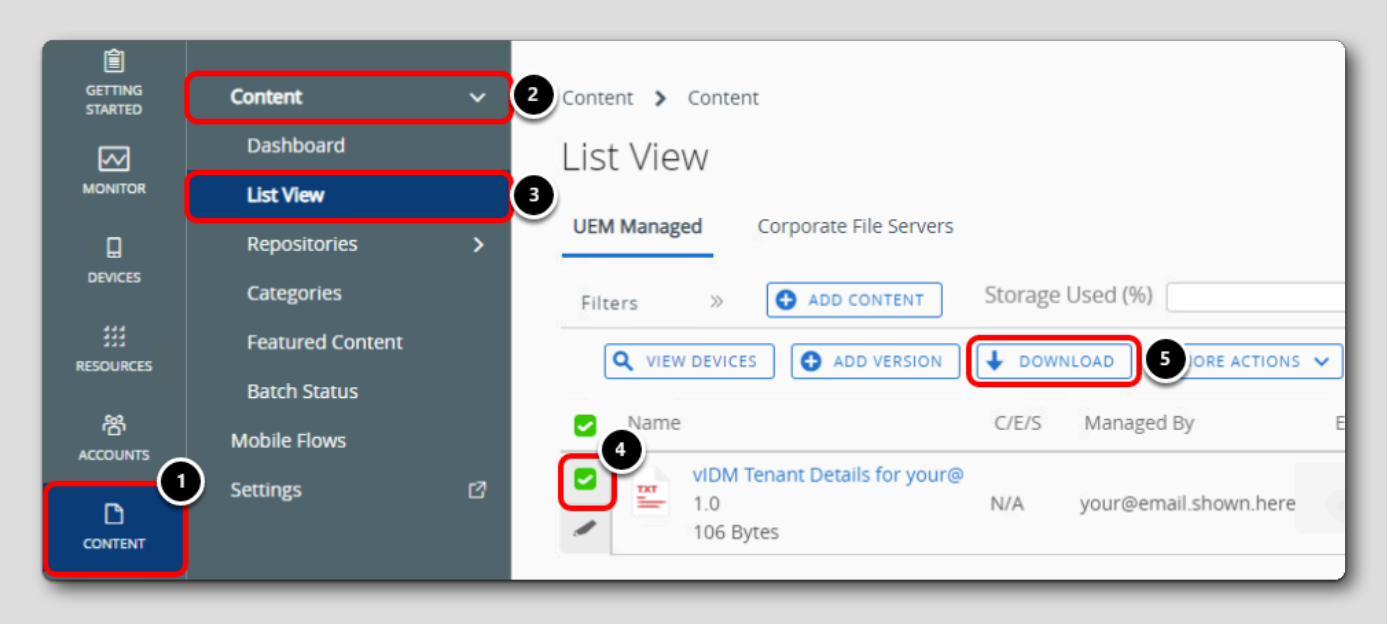
Workspace ONE Intelligent Hub end-user services are configured via the Hub Services admin console. Hub Services is co-located with Workspace ONE Access. Think of Hub Services as the server-side component and Intelligent Hub as the end-user client.

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.

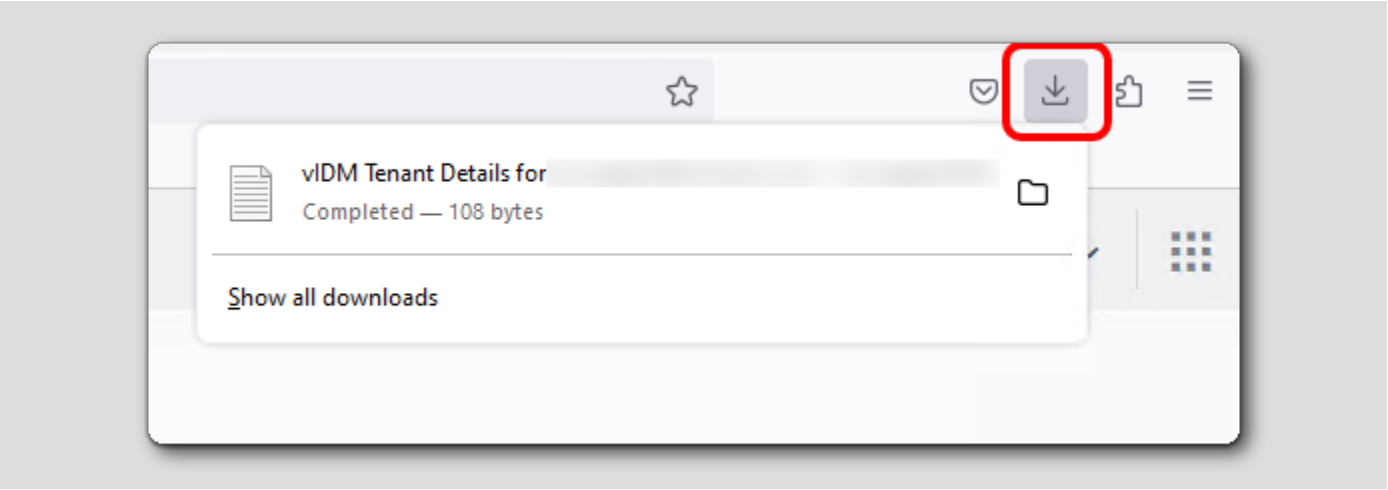


In the Workspace ONE UEM Console:

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

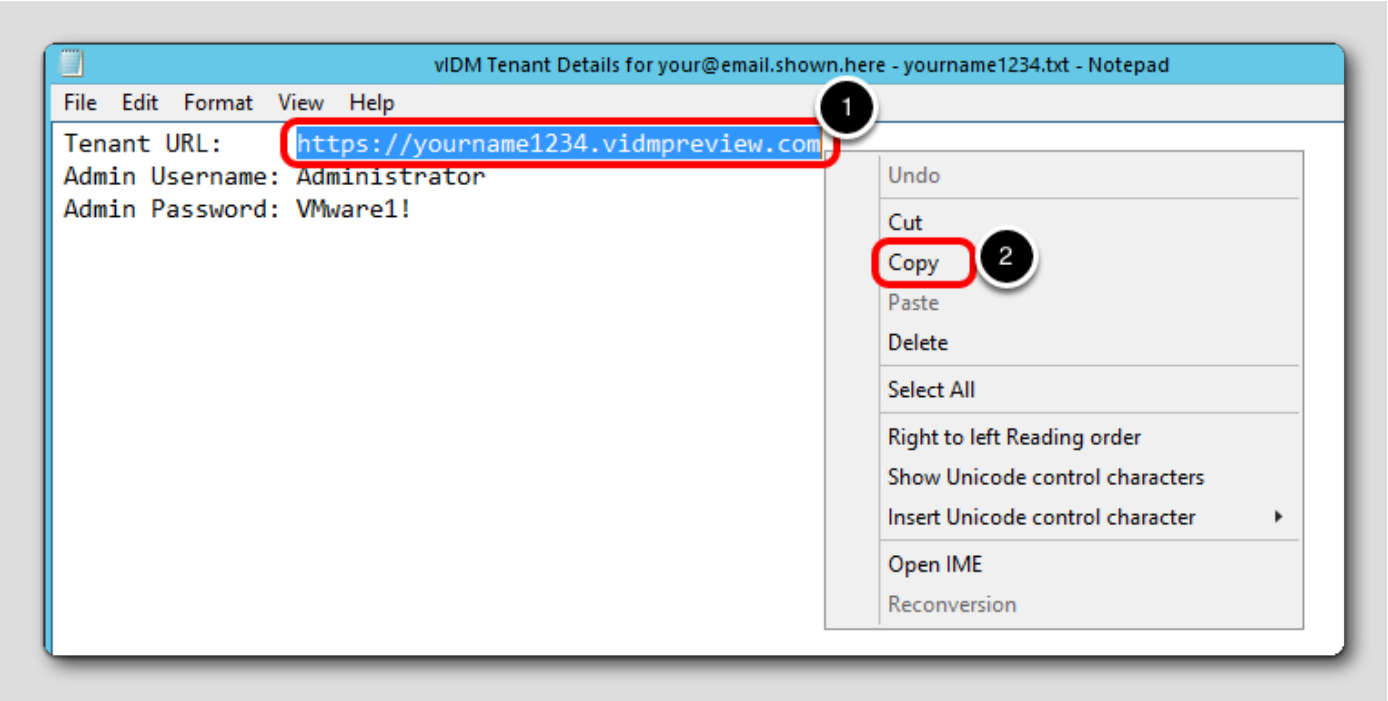
[209]



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]

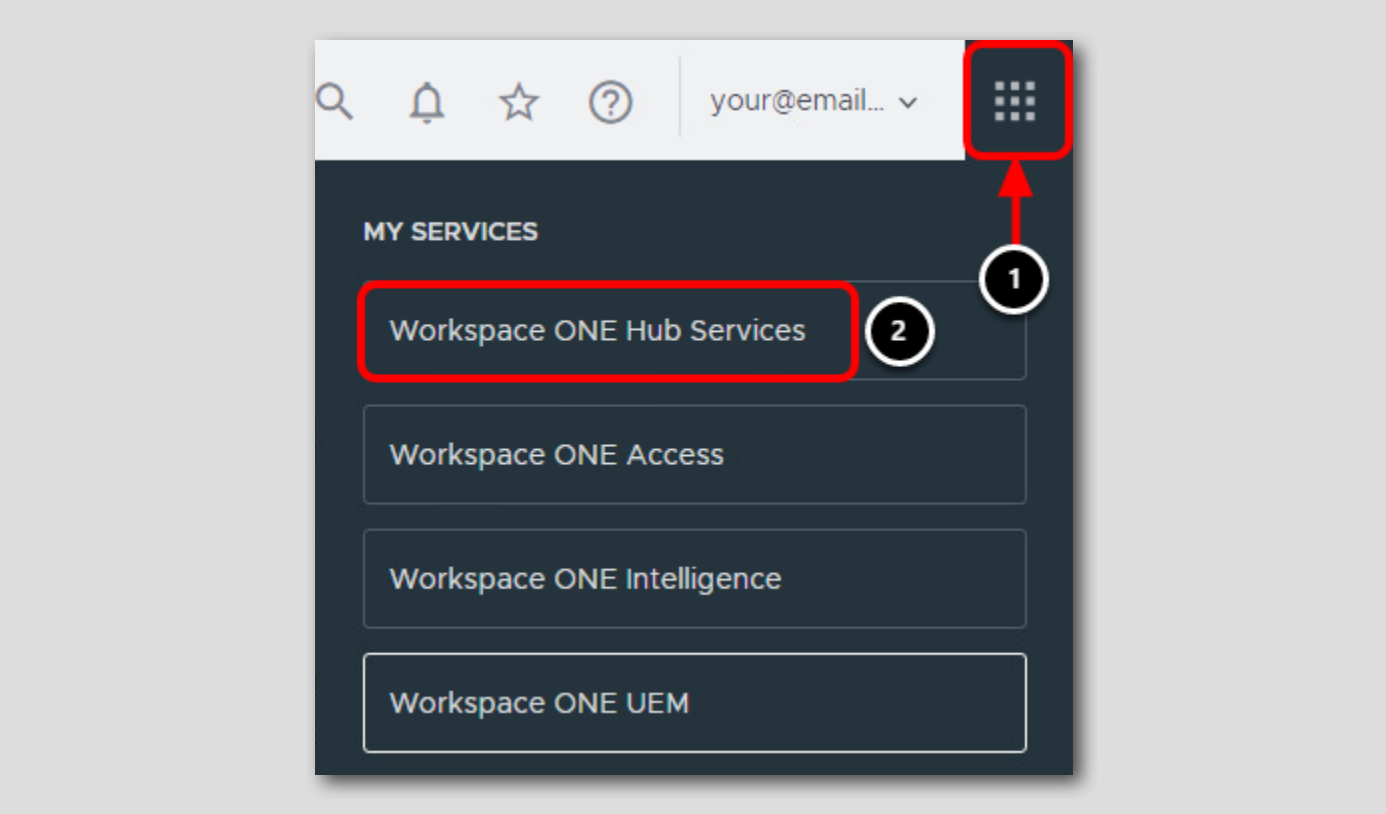
New cloud customers who purchased Workspace ONE after January 2019 have Hub Services activated automatically as part of the instance provisioning process. Workspace ONE UEM, Workspace ONE Access, and Hub Services consoles are connected together, and the Hub catalog is enabled for the Intelligent Hub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

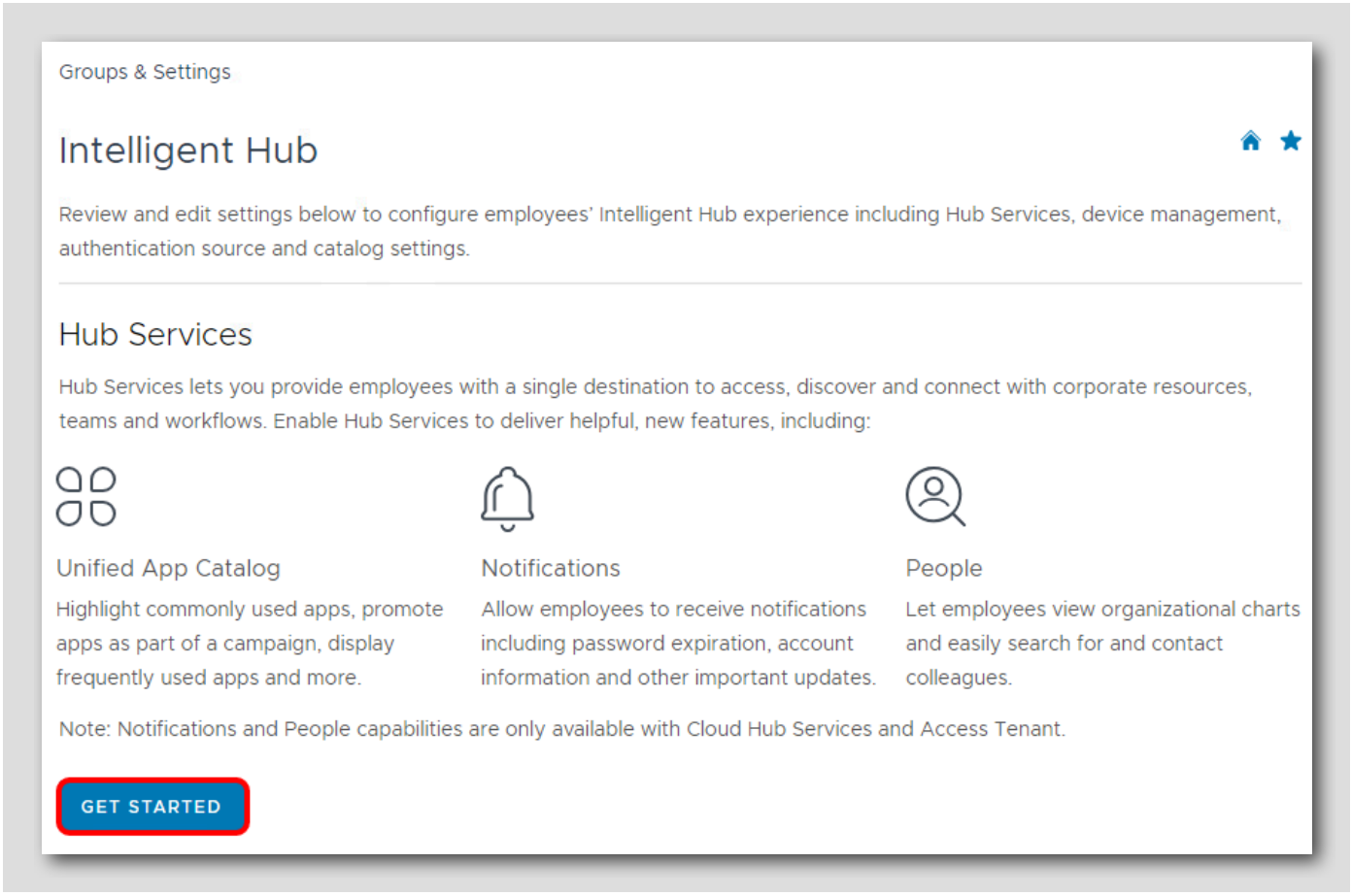


Return to the UEM console in the Firefox browser.

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

Get Started

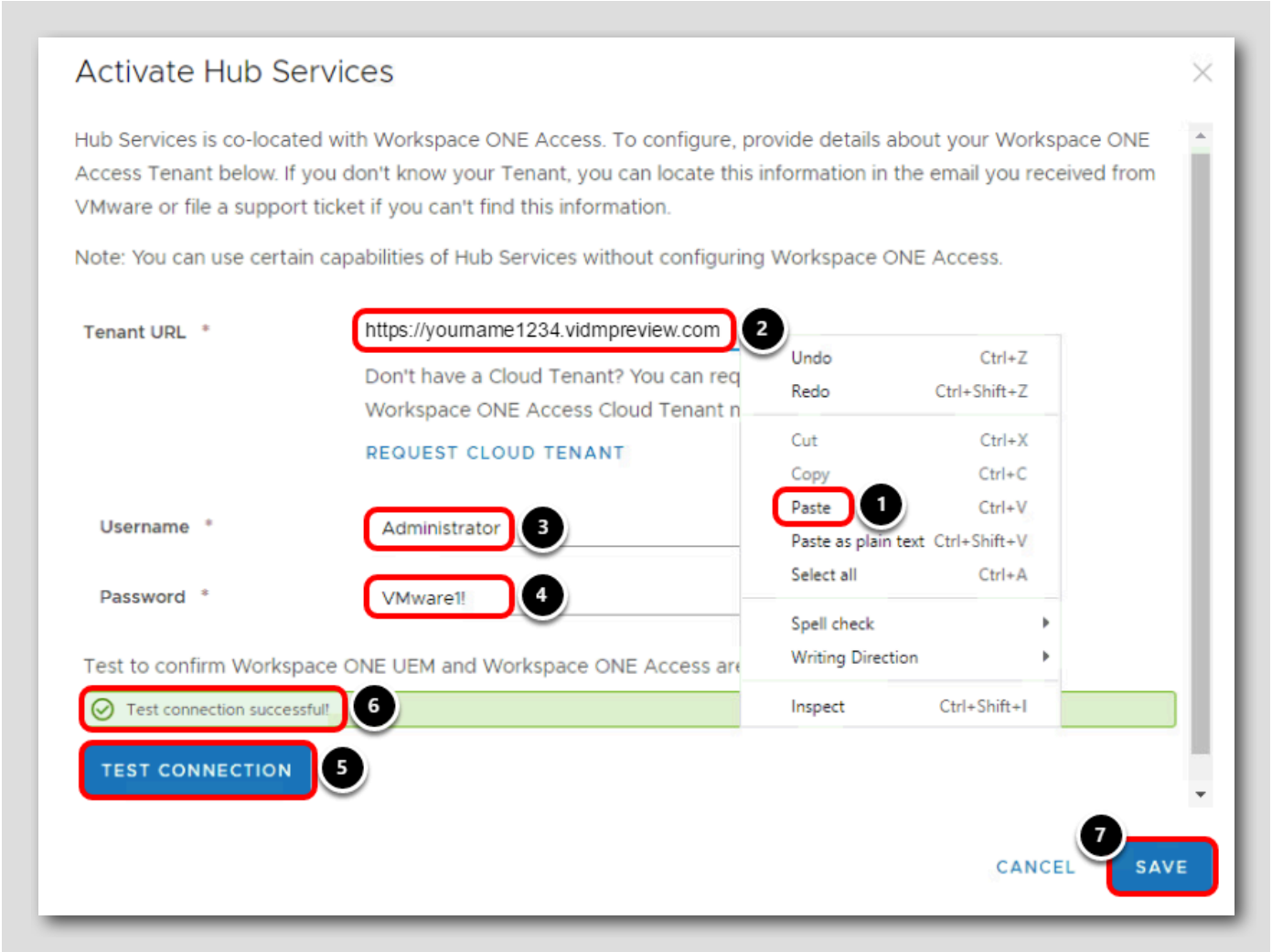
[215]



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

Activate Hub Services

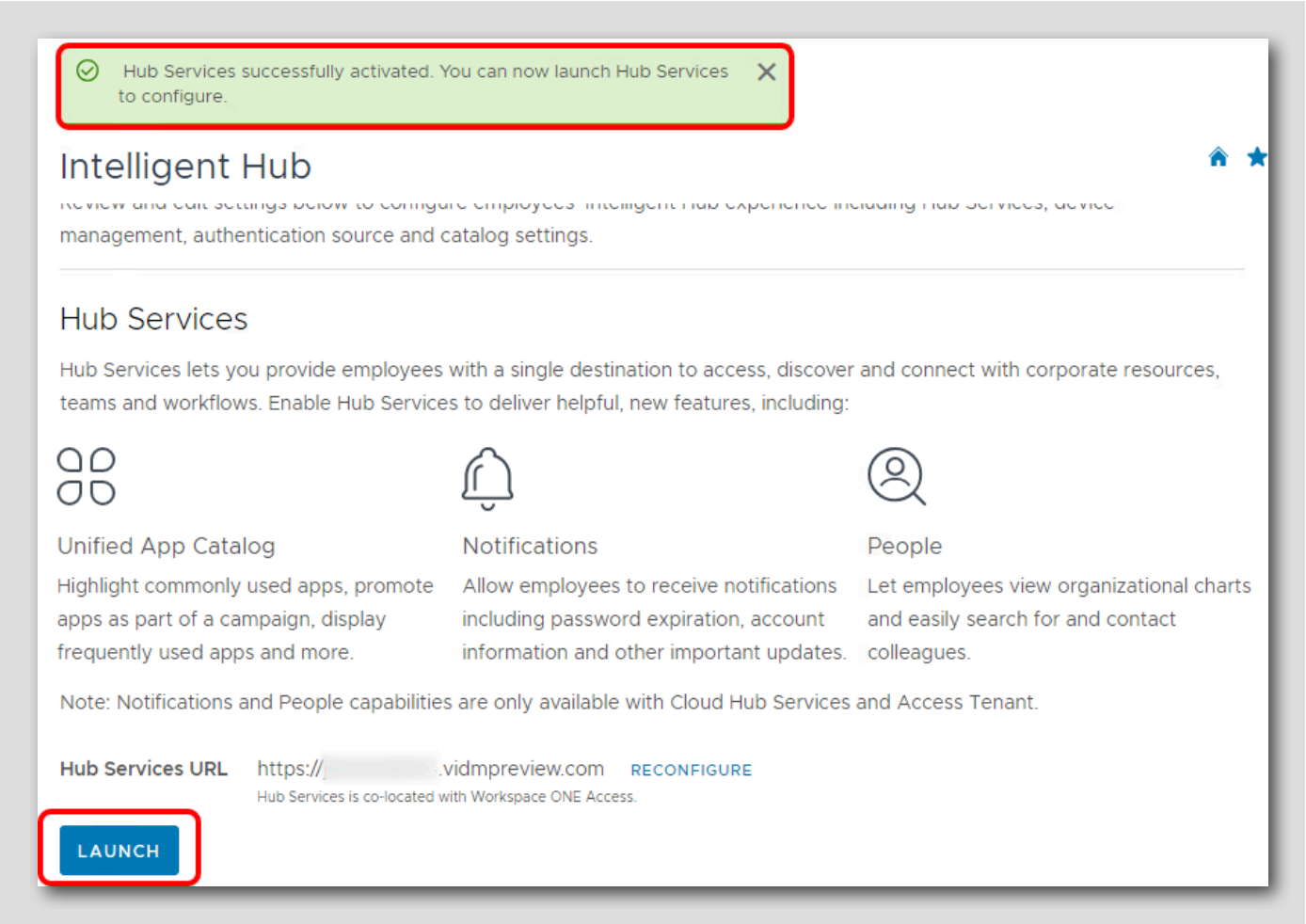
[216]



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

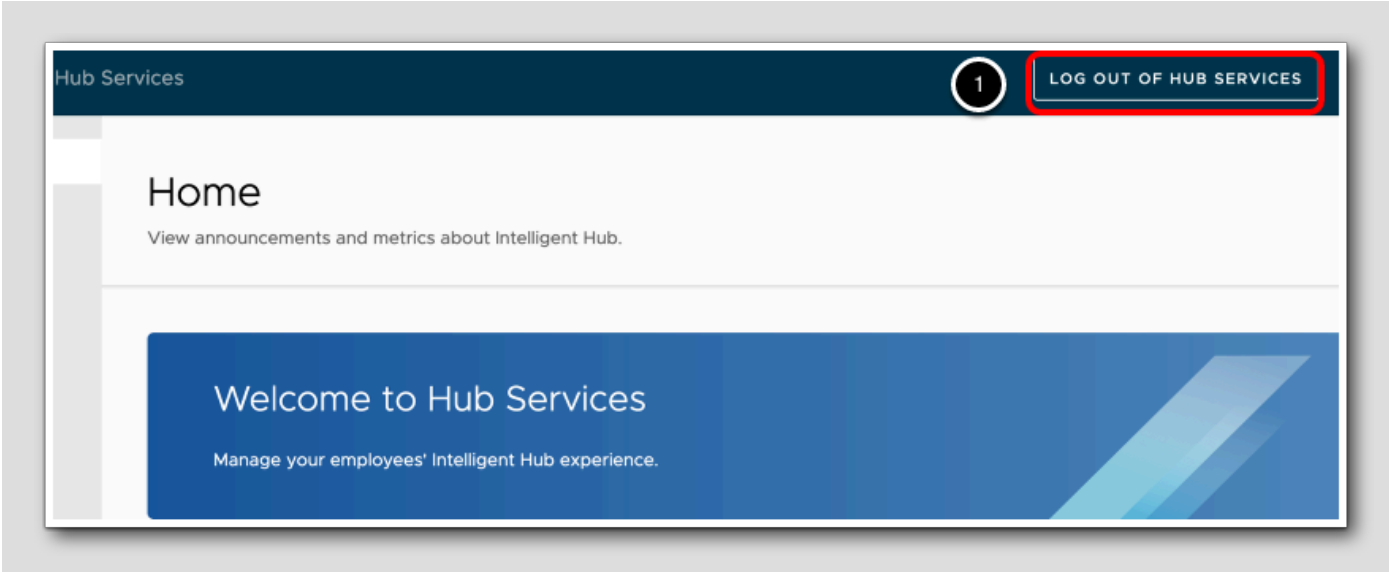
[218]

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

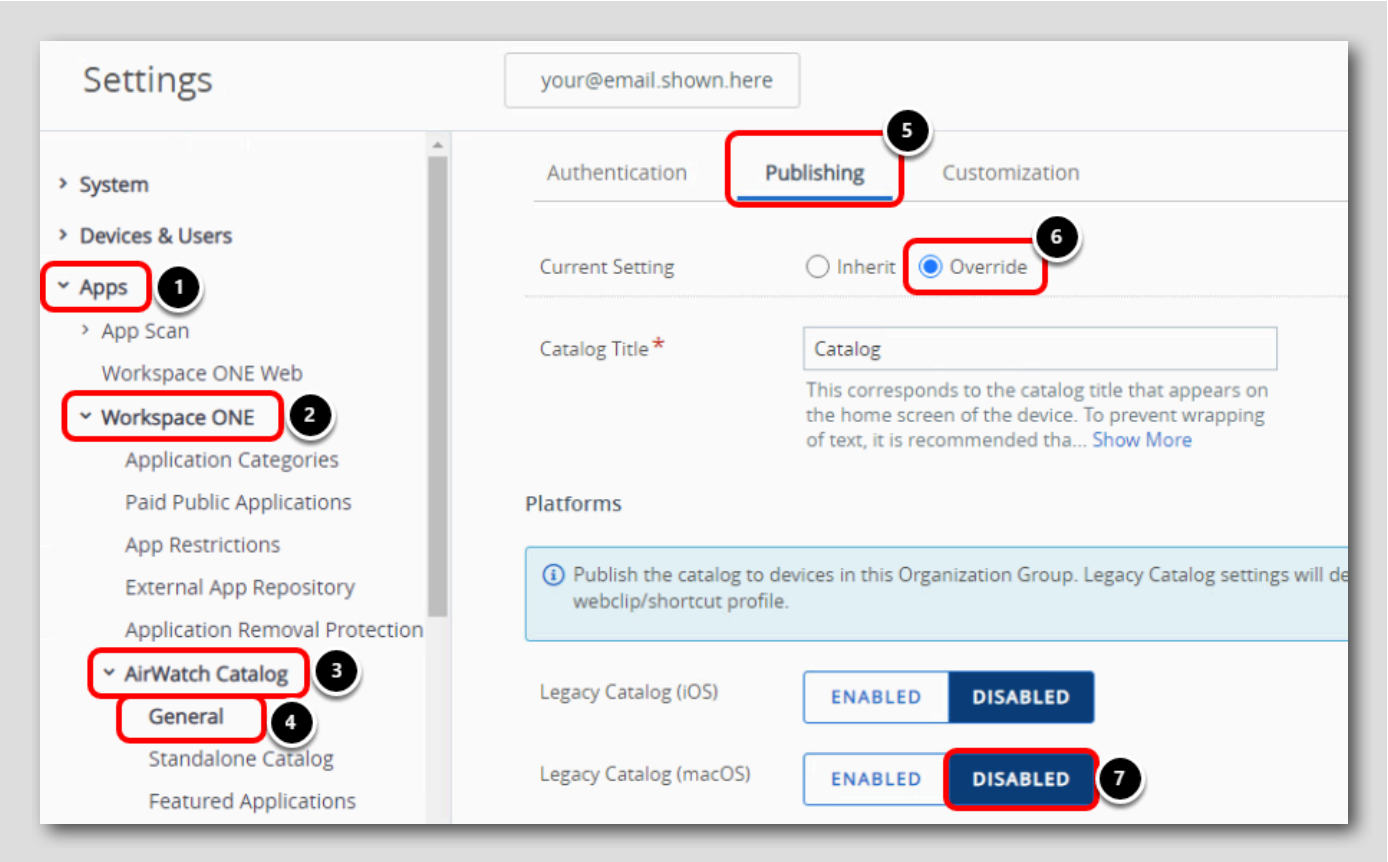
[220]

In the Workspace ONE UEM Console

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

Override the Legacy Catalog Settings

[221]

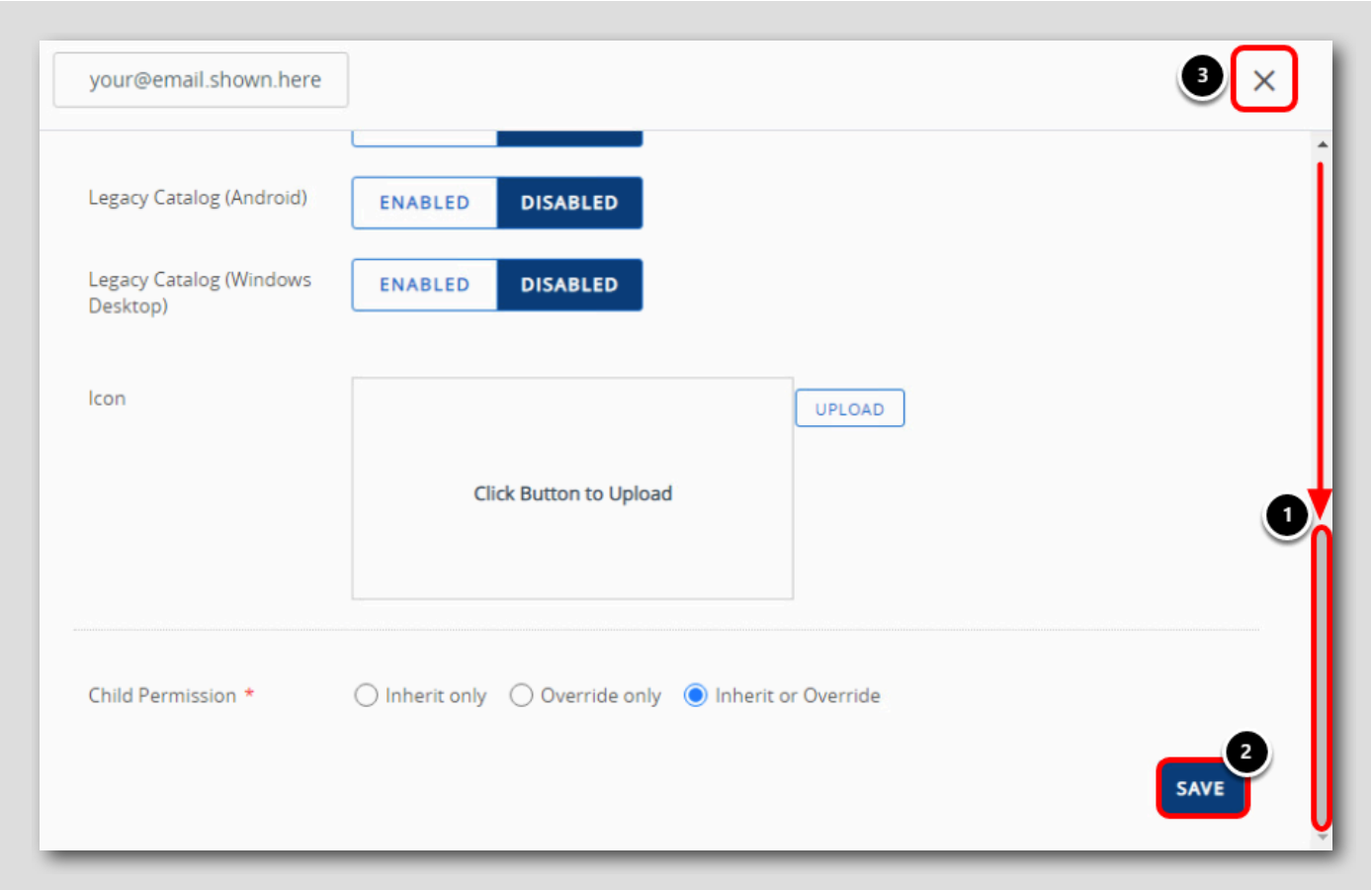


1. Click **Apps**
2. Click **Workspace ONE**
3. Click **AirWatch Catalog**
4. Click **General**
5. Click **Publishing**
6. Select **Override** for Current Setting
7. Select **Disabled** for Legacy Catalog (macOS)

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.

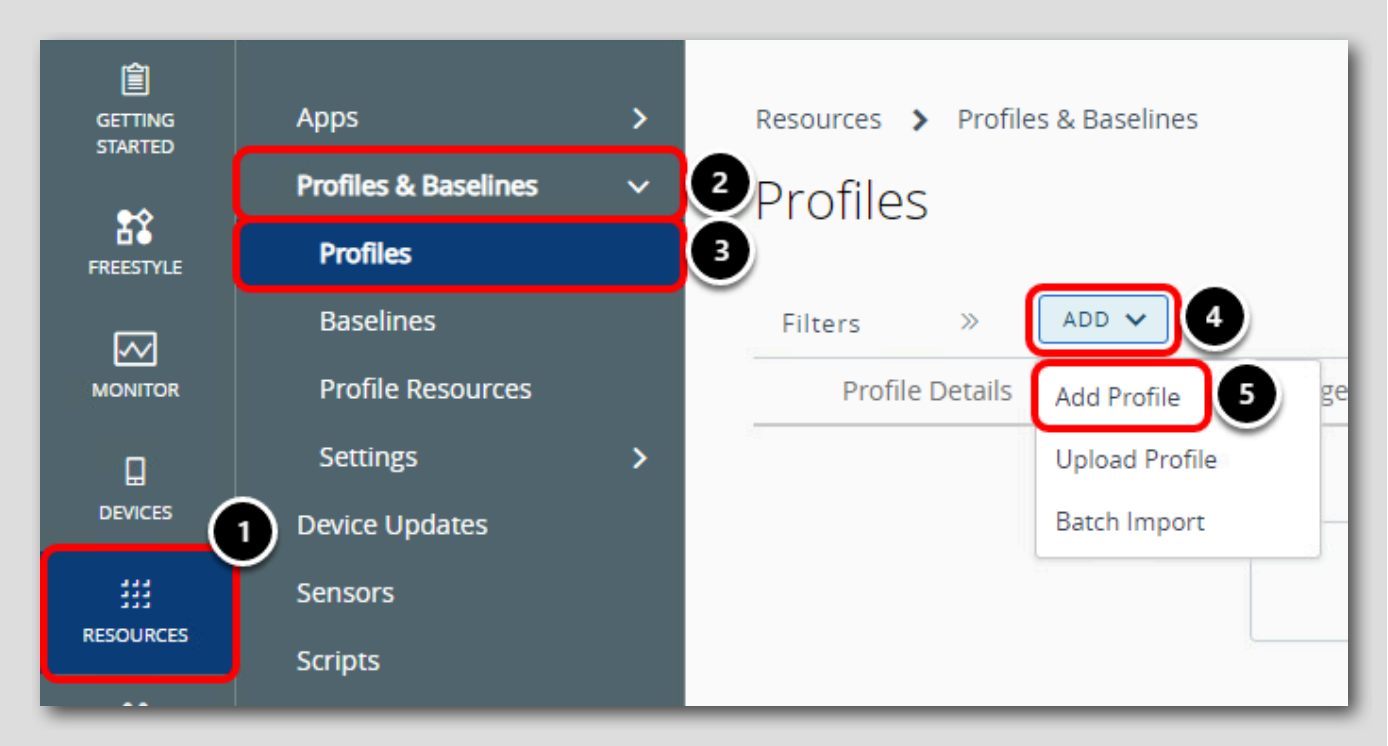
Every Profile must have all required fields in the General section properly filled out and at least one payload configured.

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]

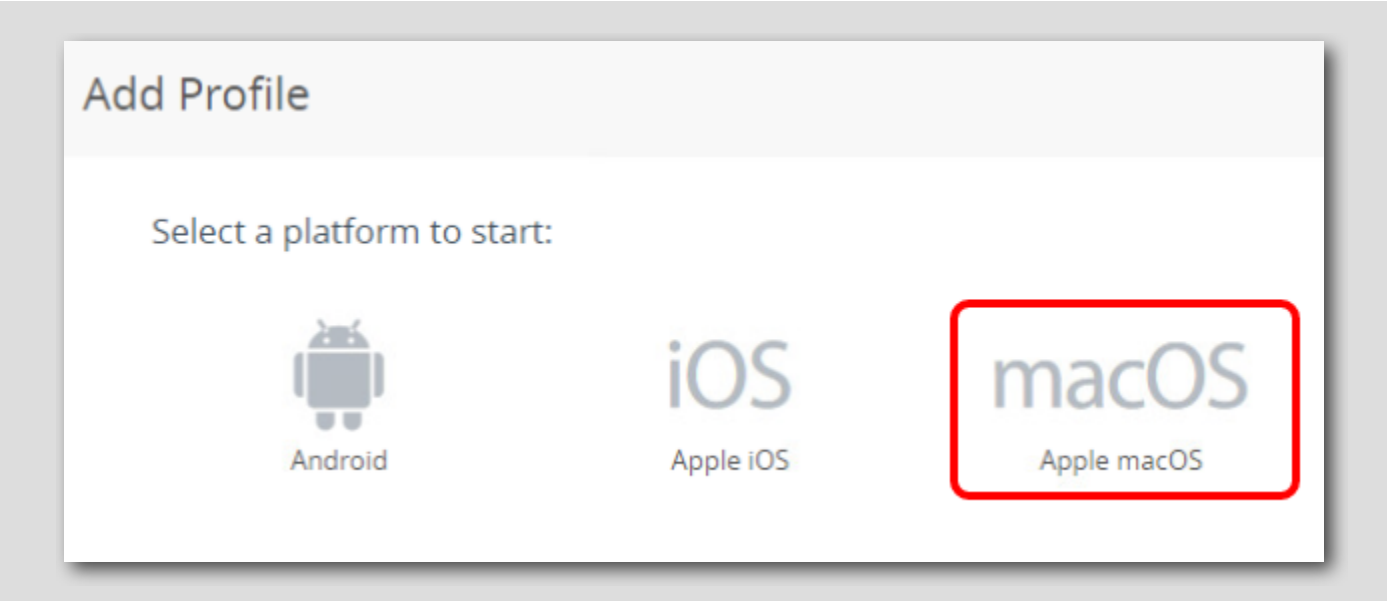


Return to the Workspace ONE UEM administration console in Google Chrome:

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

Select Profile Platform

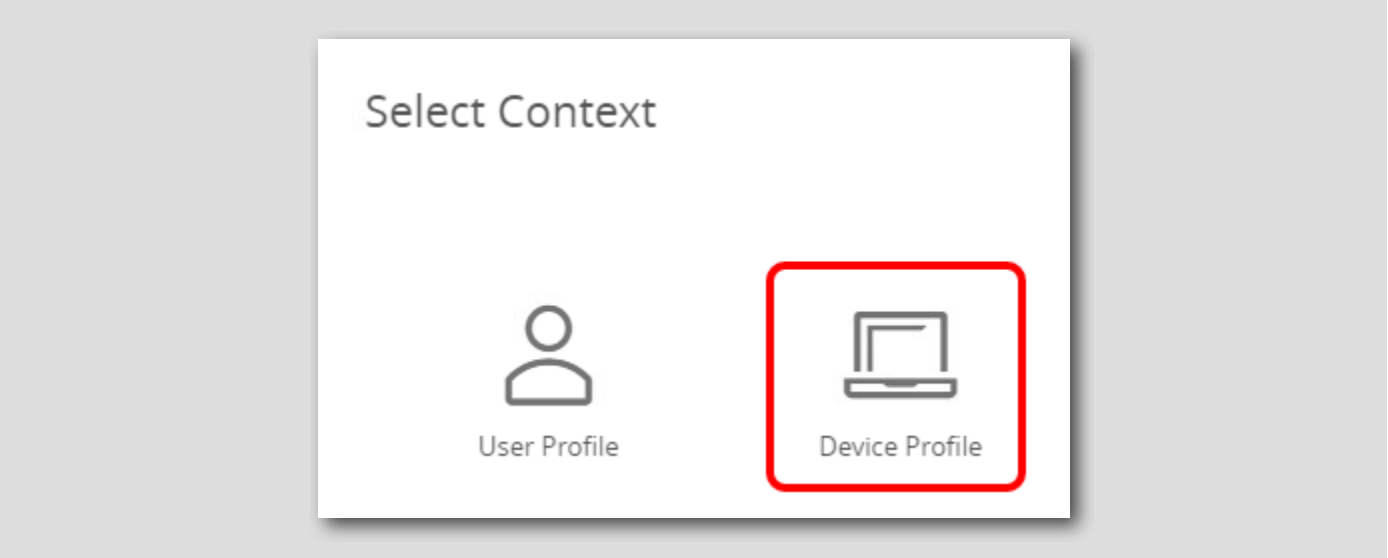
[225]



Click **macOS**.

Select the Profile Context

[226]

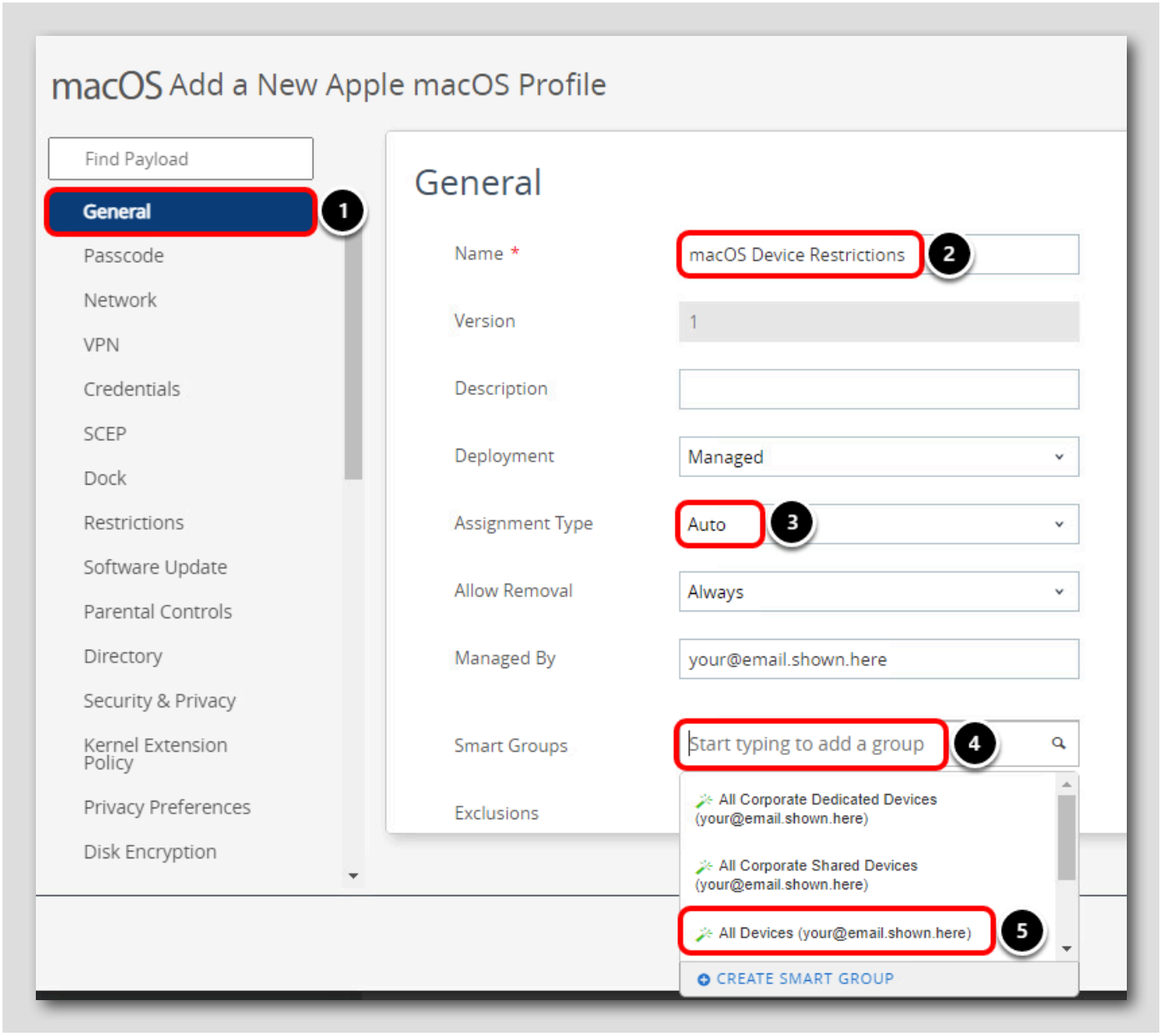


There are two contexts for Profiles: User and Device. User Profiles will apply the configuration to only the logged in user on the device. Device Profiles will apply the configuration to the entire device.

Click **Device Profile**.

Configure General Payload

[227]



Configure the device profile as follows:

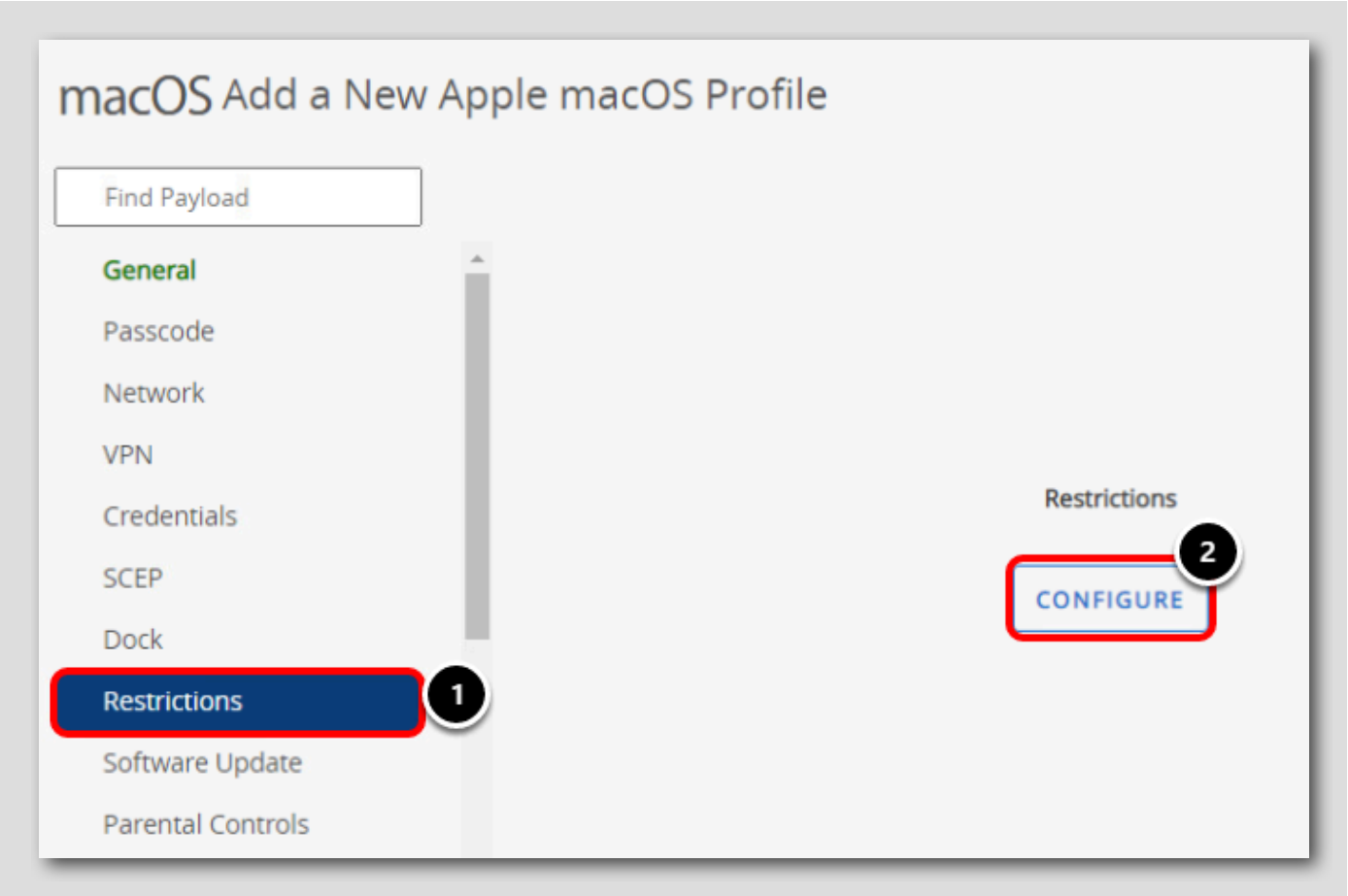
1. Select the **General** payload if not already selected
2. Enter **`macOS Device Restrictions`** for the profile name
3. Confirm **Auto** is selected for the Assignment Type
4. Scroll down to view the Smart Groups field and click in the search box
5. Select the **All Devices (your@email.shown.here)**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

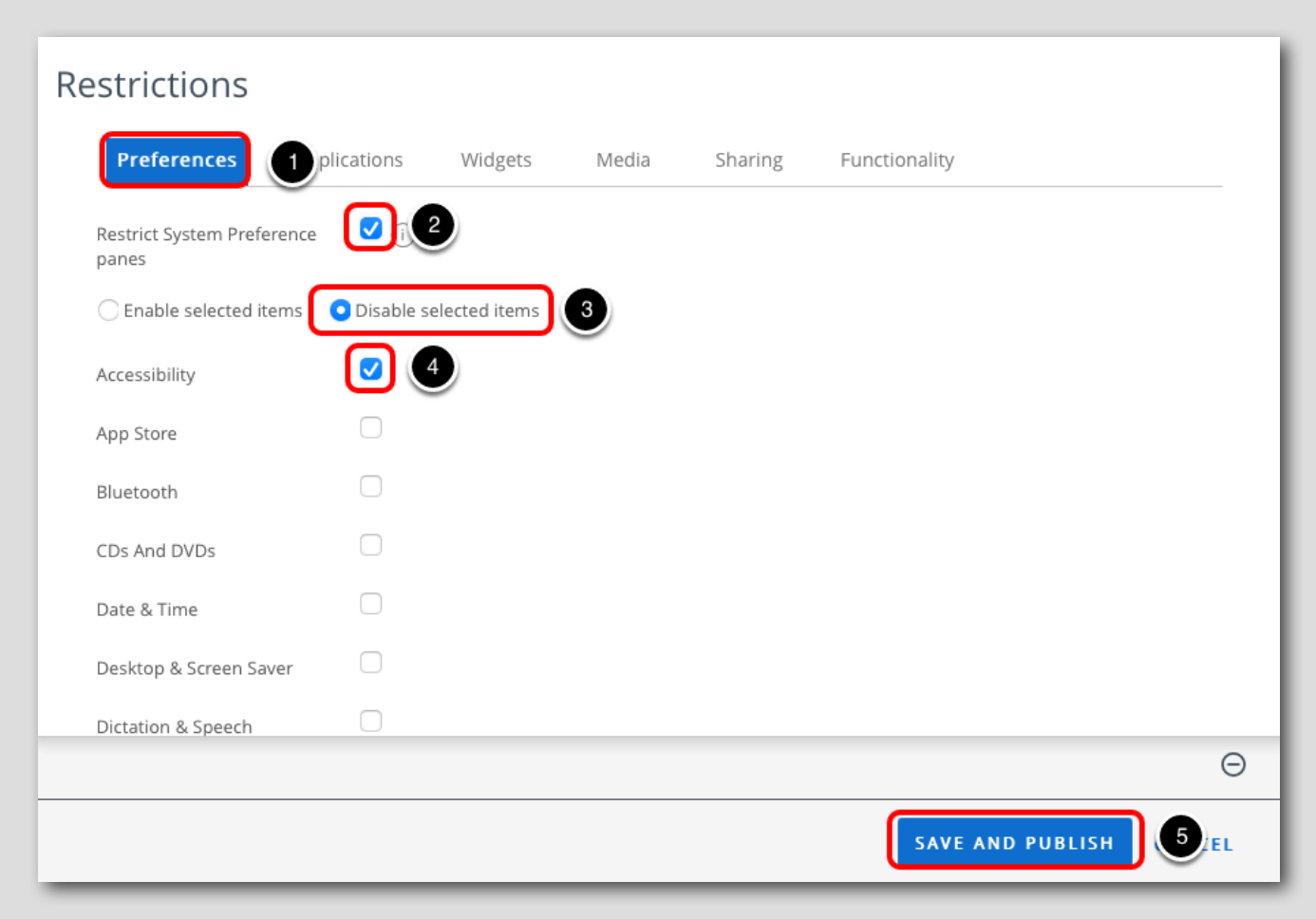


1. Click the **Restrictions** payload
2. Click **Configure**

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]

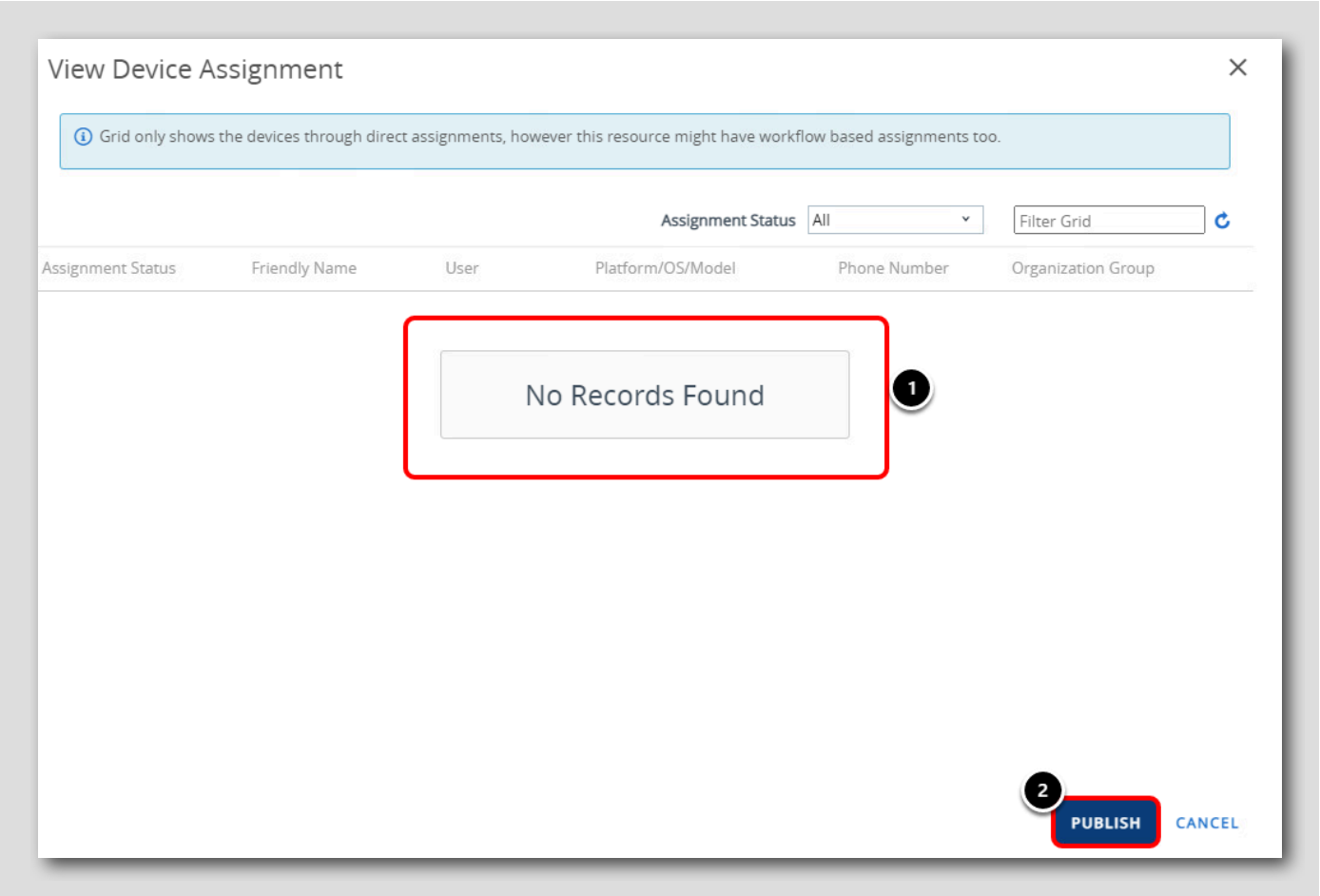


1. Click the **Preferences** tab
2. **Enable** the Restrict System Preference panes checkbox
3. Select **Disable Selected Items**
4. Enable the **Accessibility** checkbox
5. Click **Save & Publish**

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

Preview and Publish Profile

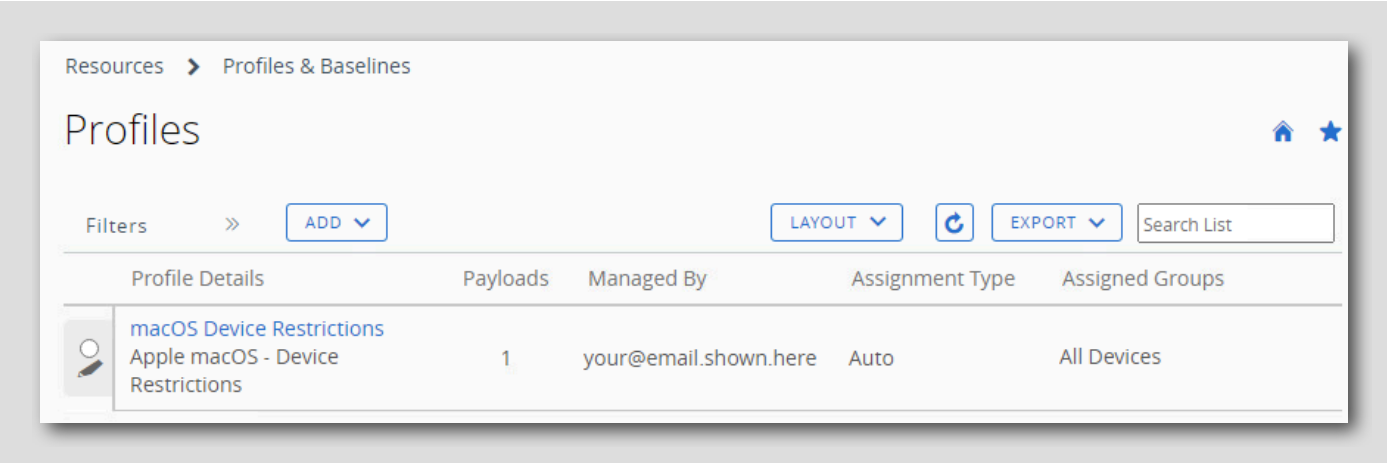
[230]



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]

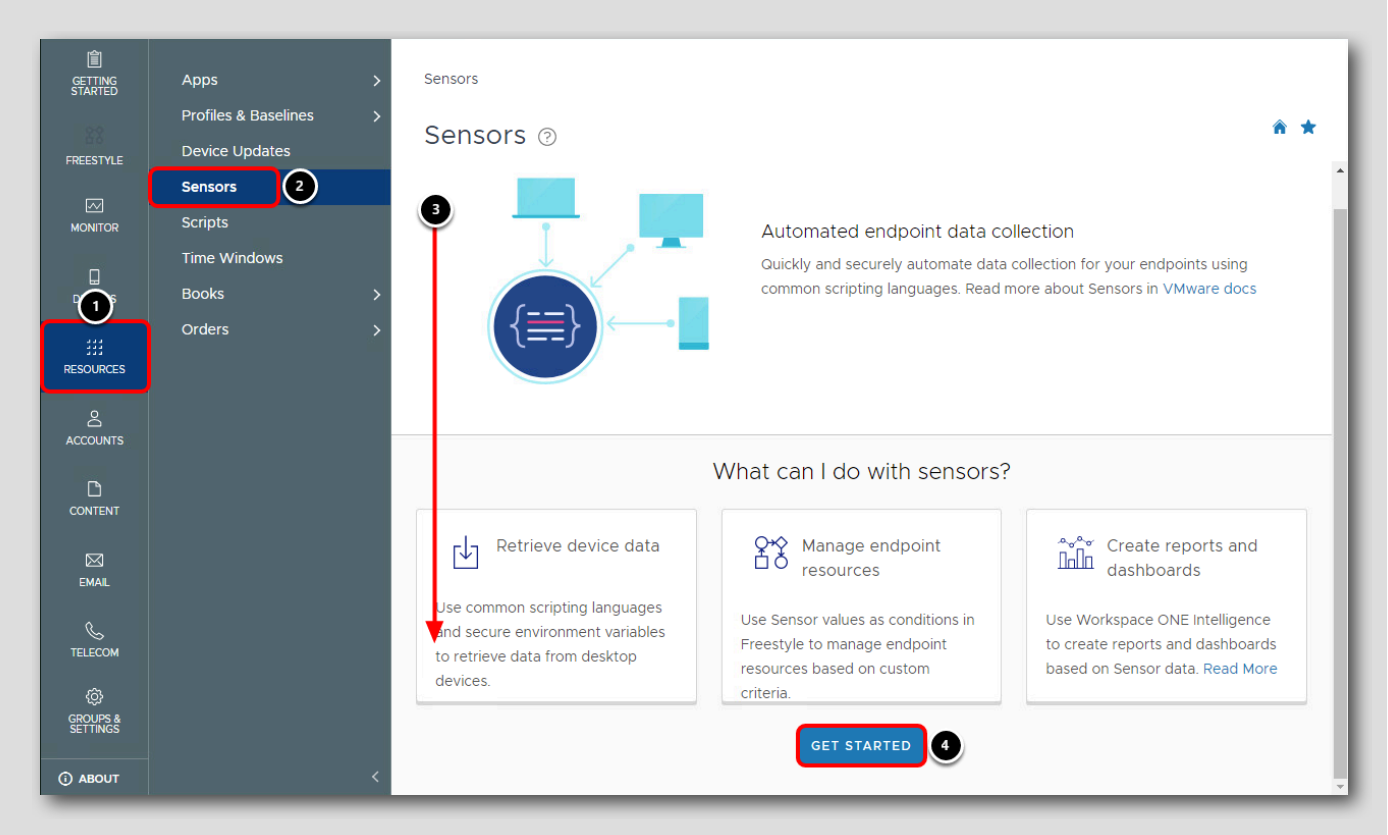
Sensors allow you to quickly and securely automate data collection from your endpoints with common scripting languages. macOS Sensors supports Bash, Python 3, and Zsh, and Windows Desktops support PowerShell.

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]

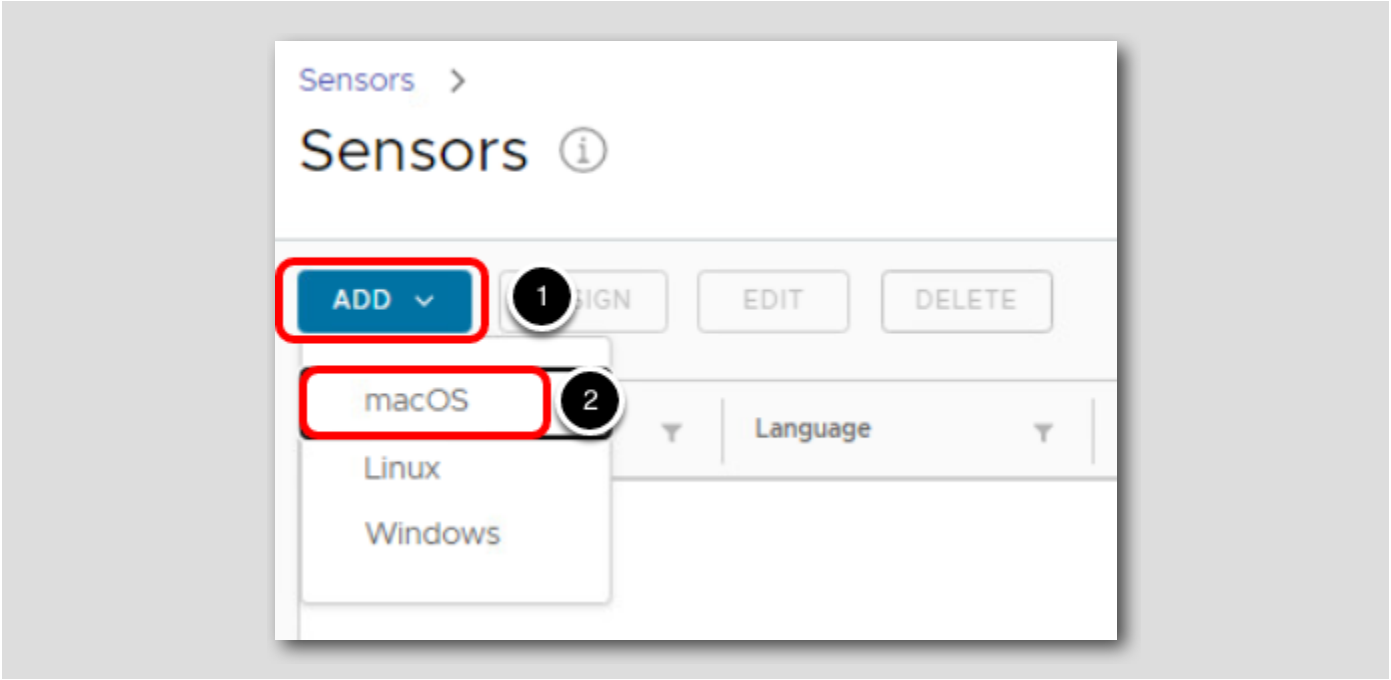


The first time you access the Sensors page, an overview will be presented with a link to the VMware docs articles for *macOS Sensors* and *Windows Desktop Sensors*. Refer to these links for additional documentation around Sensors.

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

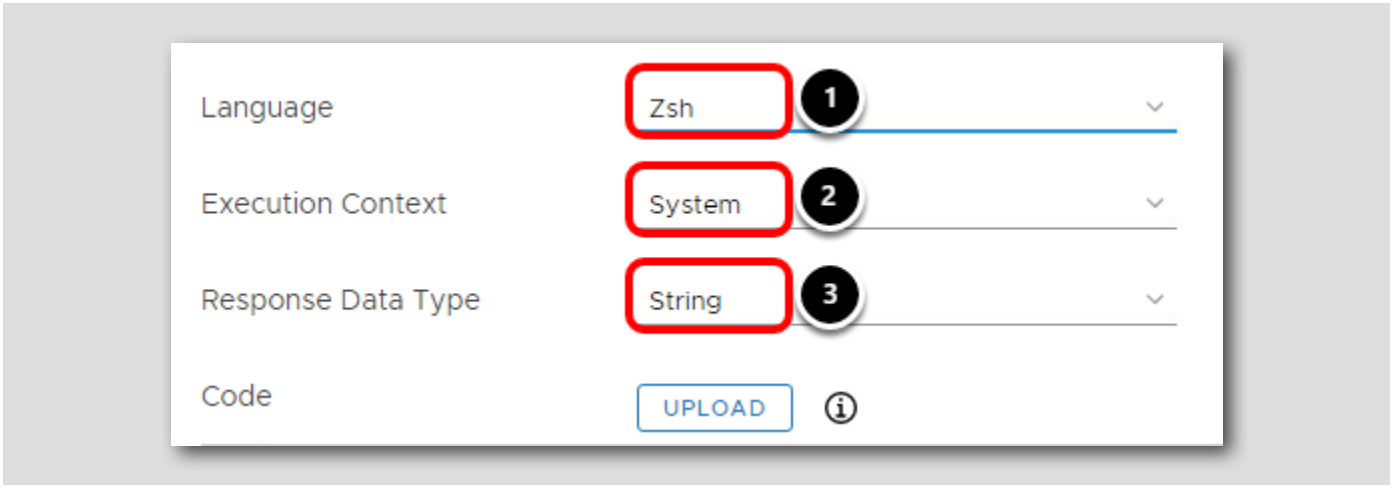
[235]

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

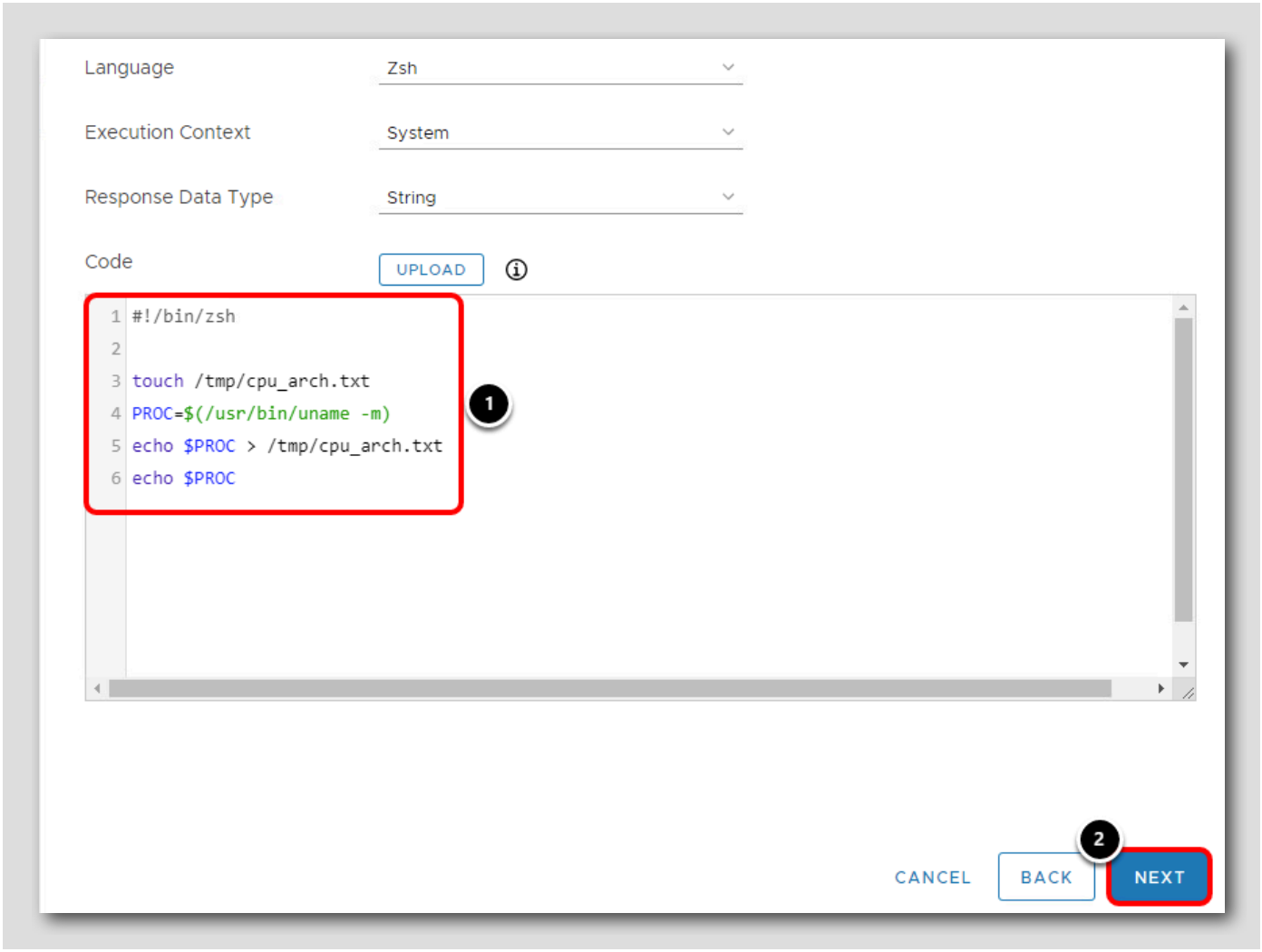
[236]



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**.

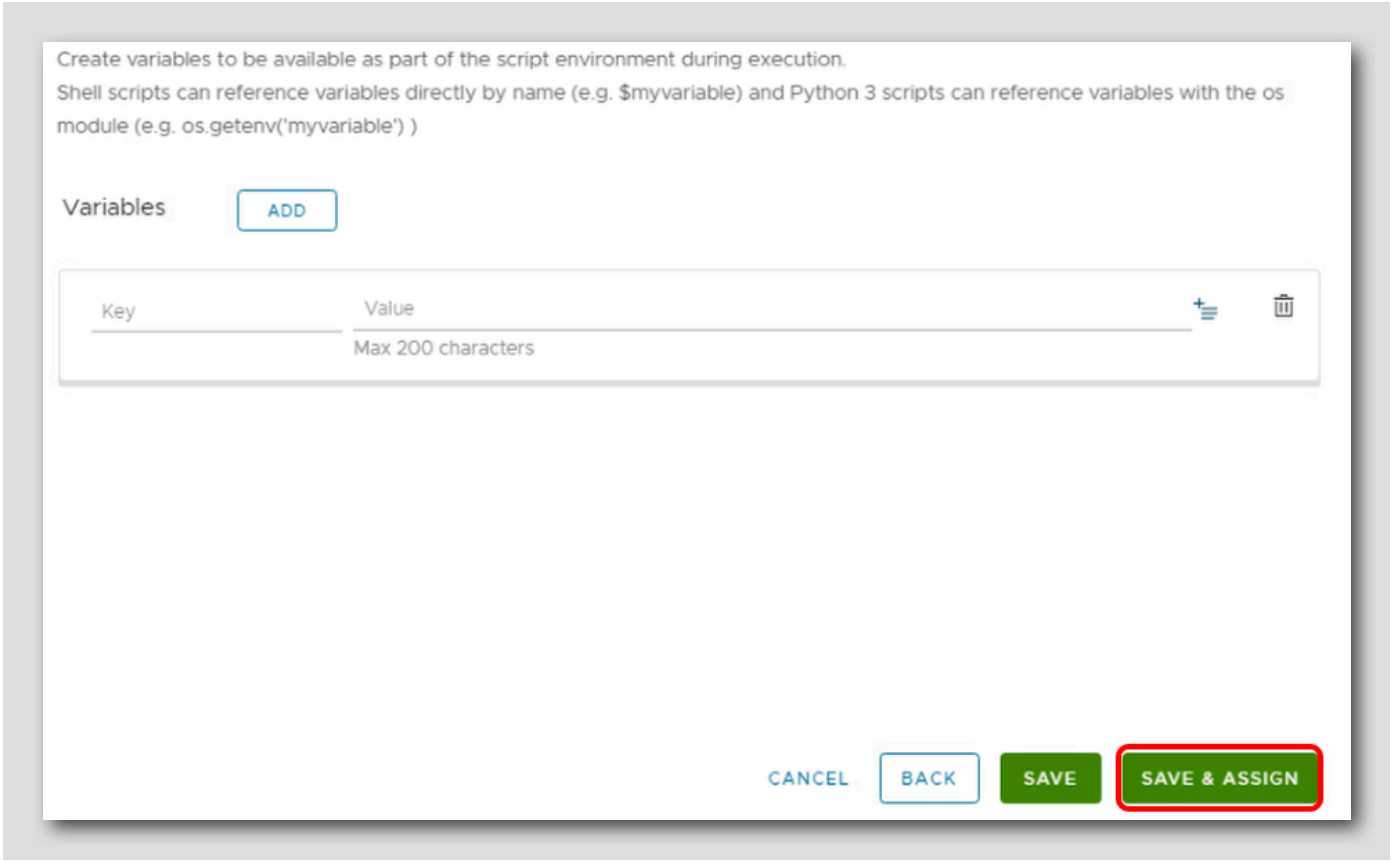
Note: We manually entered the code in this exercise but you can also upload a file containing the code instead.

```
#!/bin/zsh

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

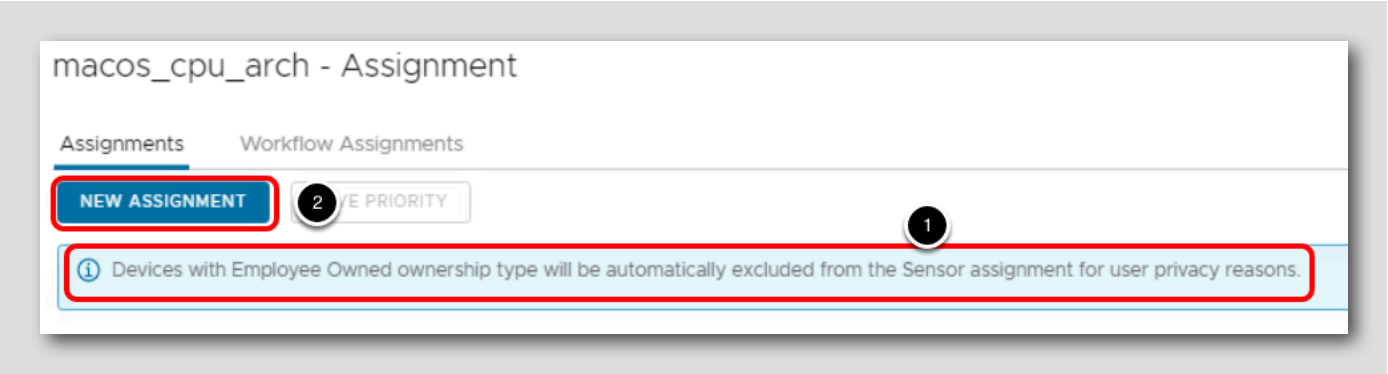
Save & Assign the Sensor

[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.

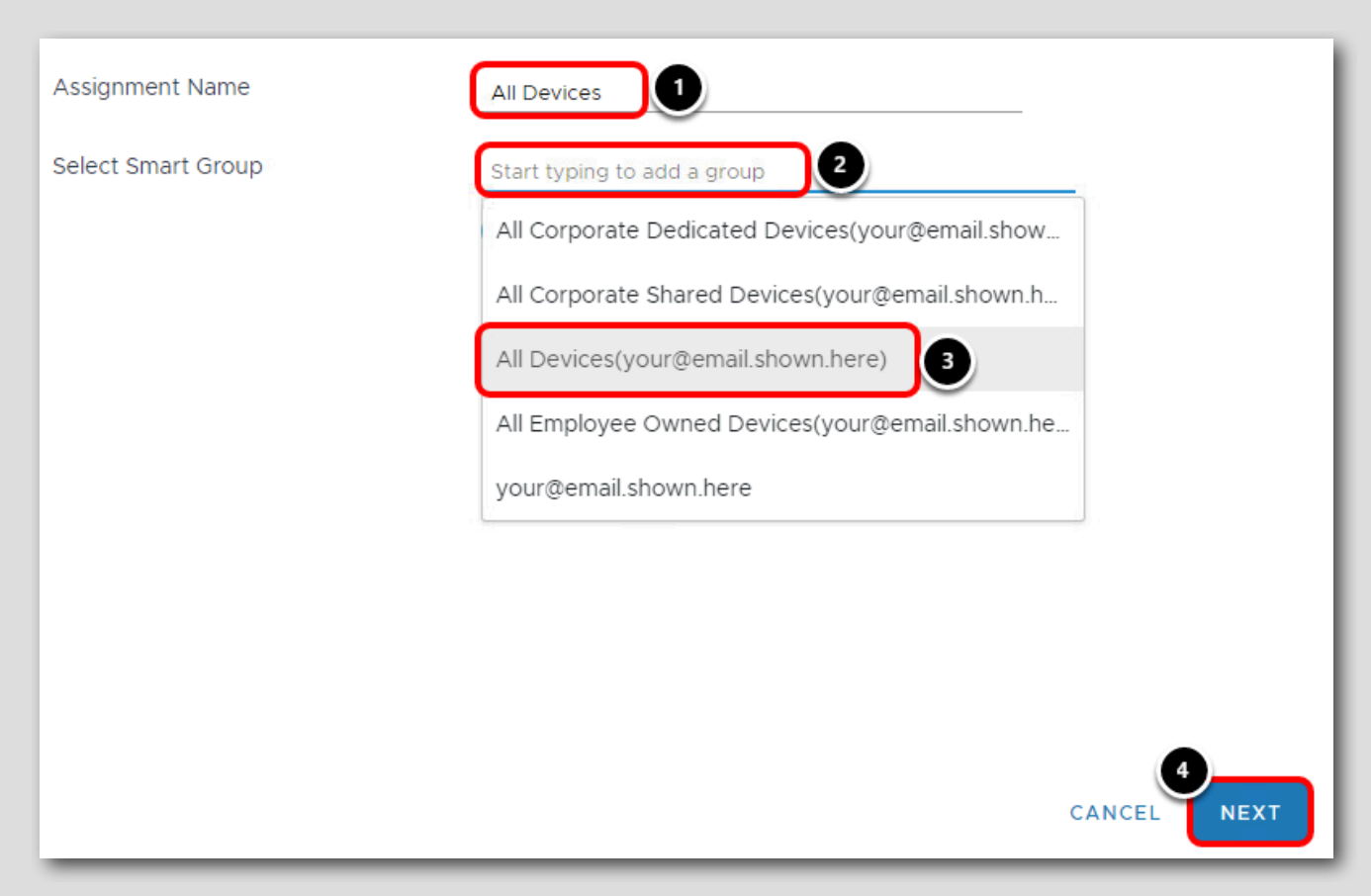
Assign a macOS Sensor



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]

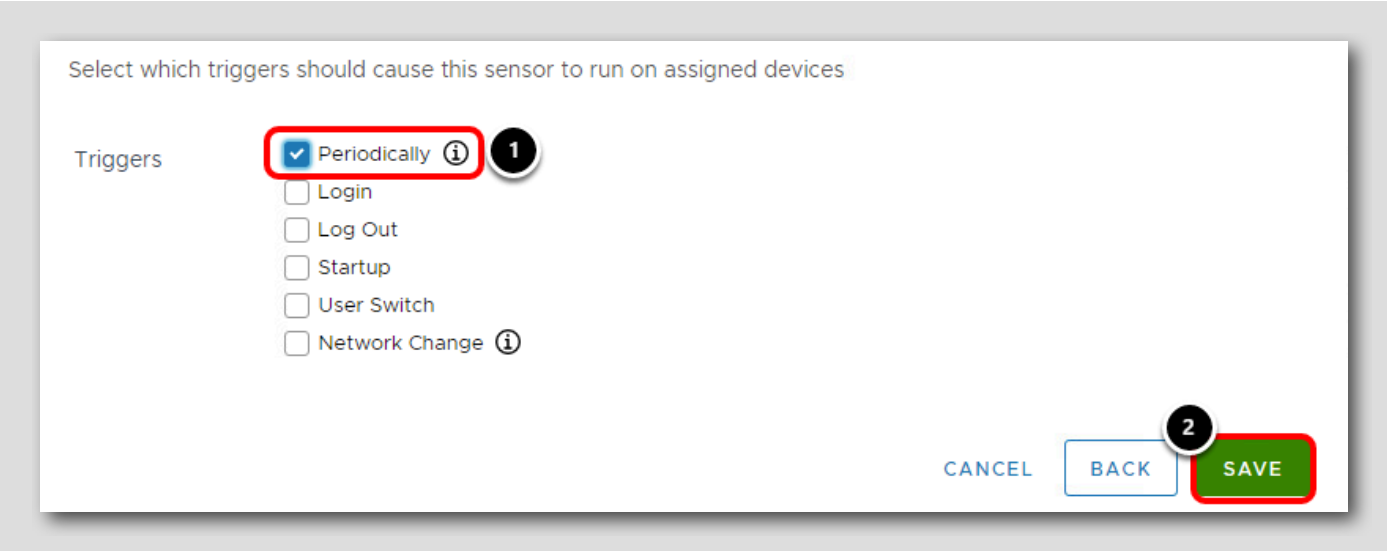


1. Enter **`All Devices`** for the Assignment Name
2. Click the **Select Smart Group** field
3. Select the **All Devices (your@email.shown.here)** group
4. Click **Next**

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]

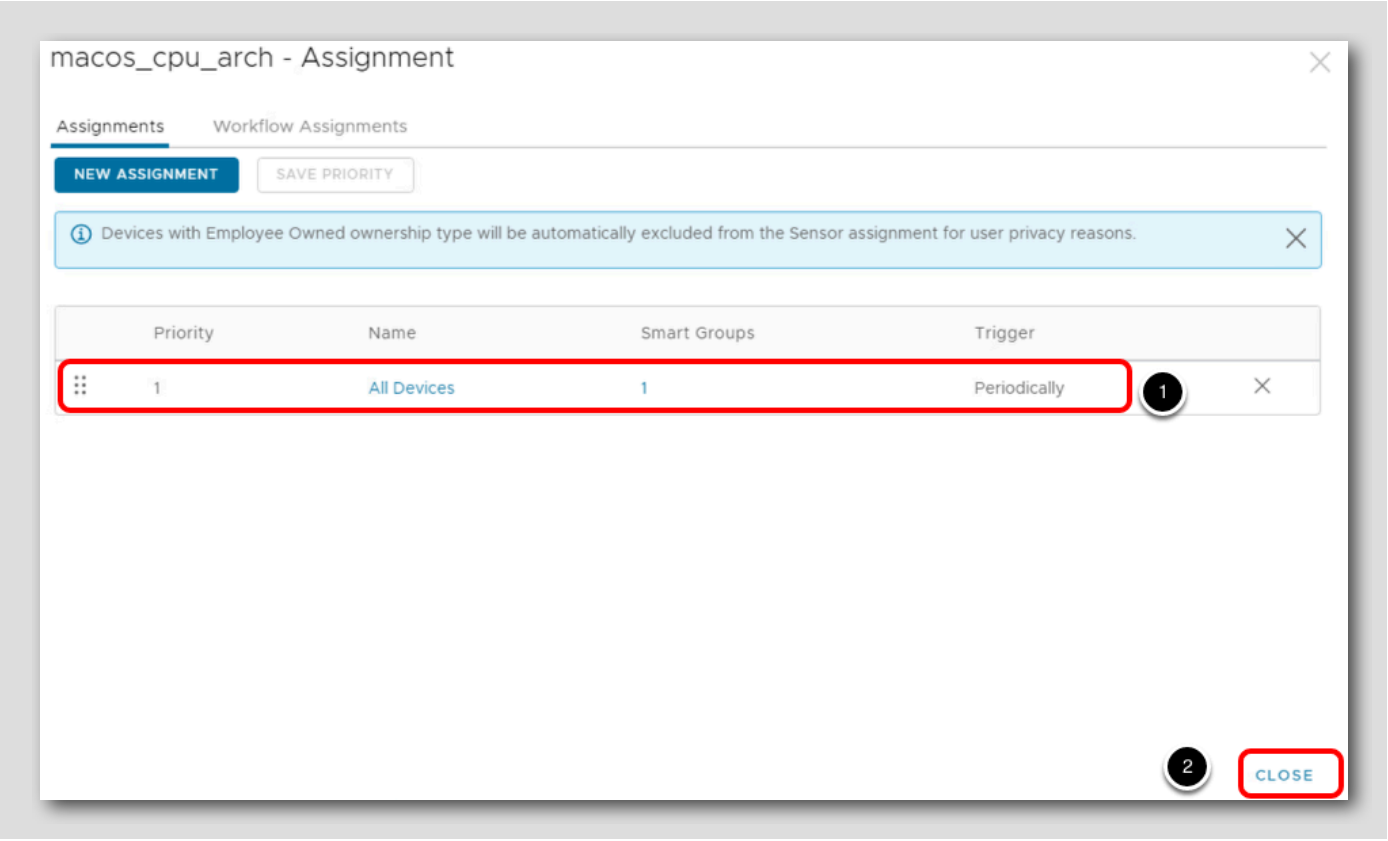


1. Select **Periodically** for the Triggers
2. Click **Save**

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.

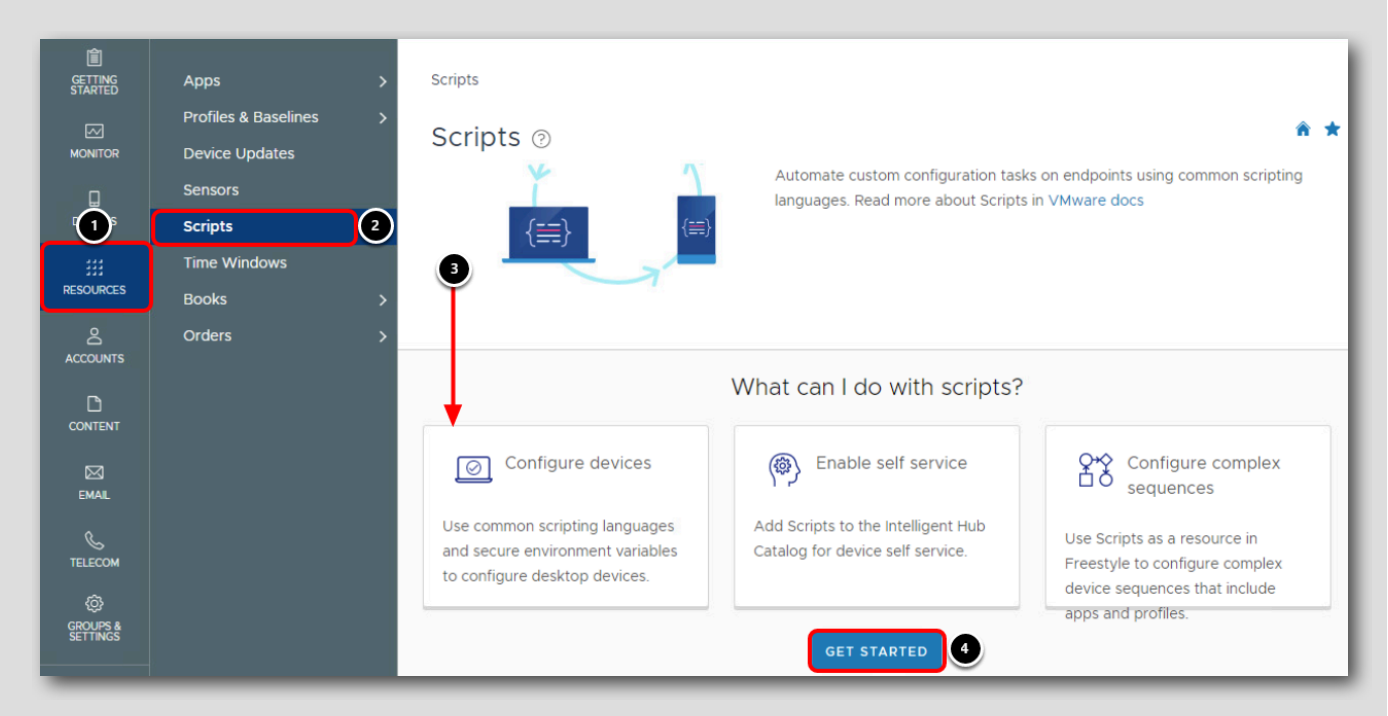
Create Scripts

[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]

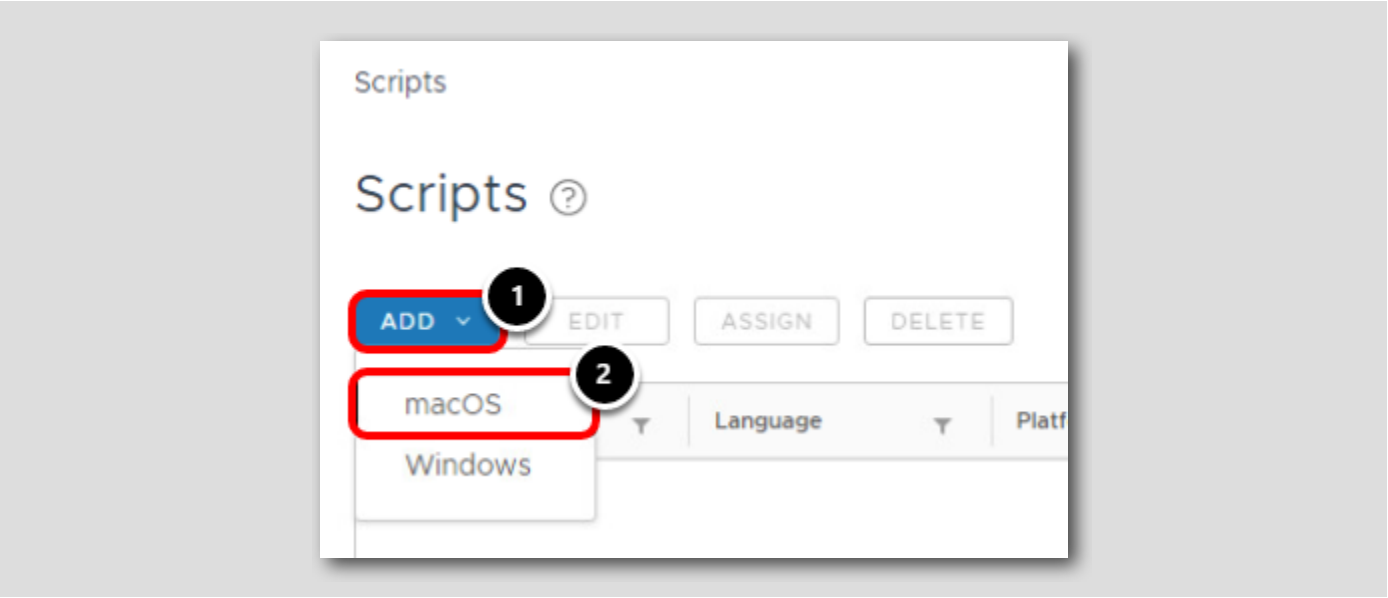


The first time you access the Scripts page, an overview will be presented with a link to the VMware docs articles for *macOS Scripts* and *Windows Desktop scripts*. Refer to these links if you desire more documentation around Scripts.

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

Add a macOS Script

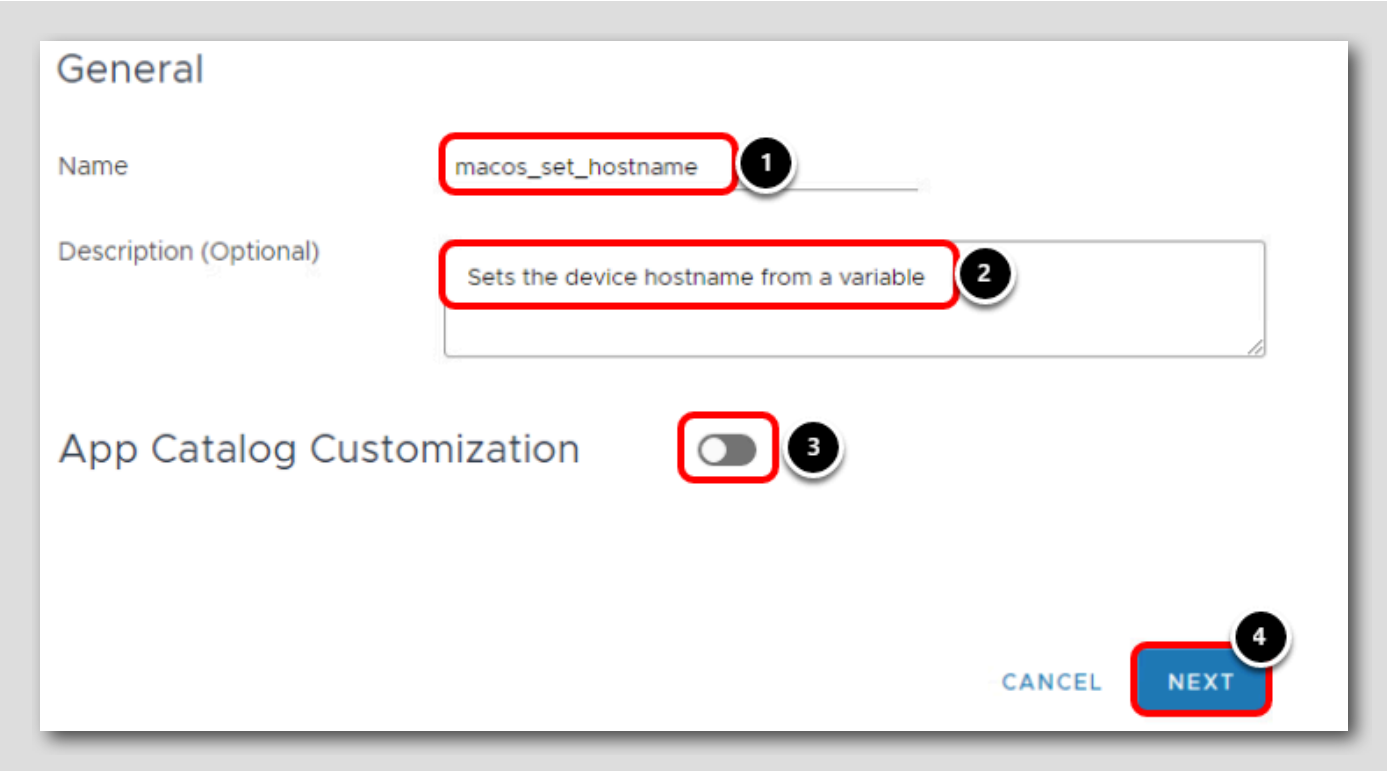
[245]



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

Add General Information

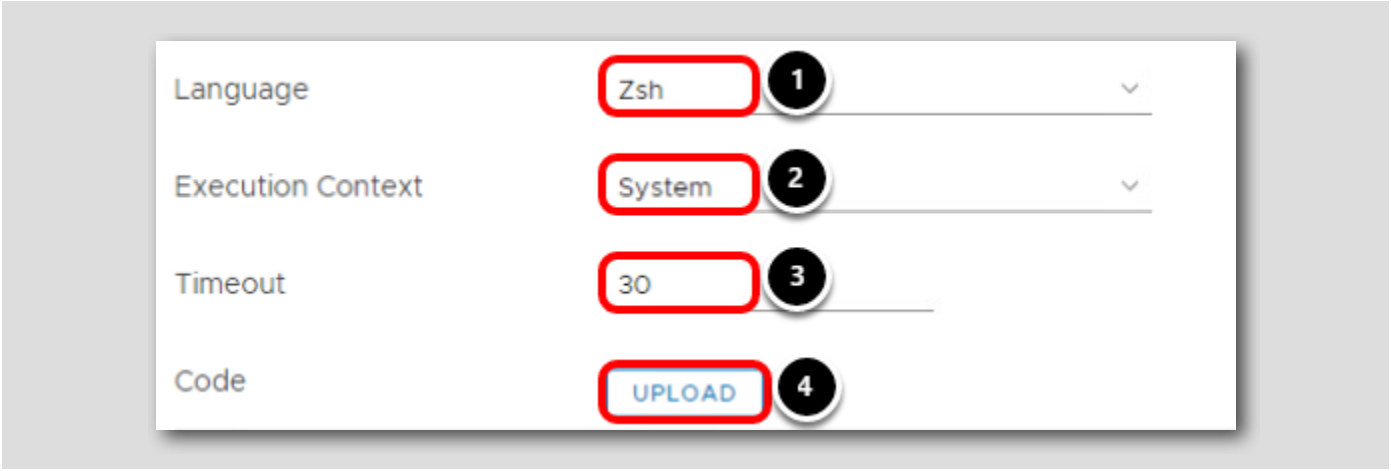
[246]



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]

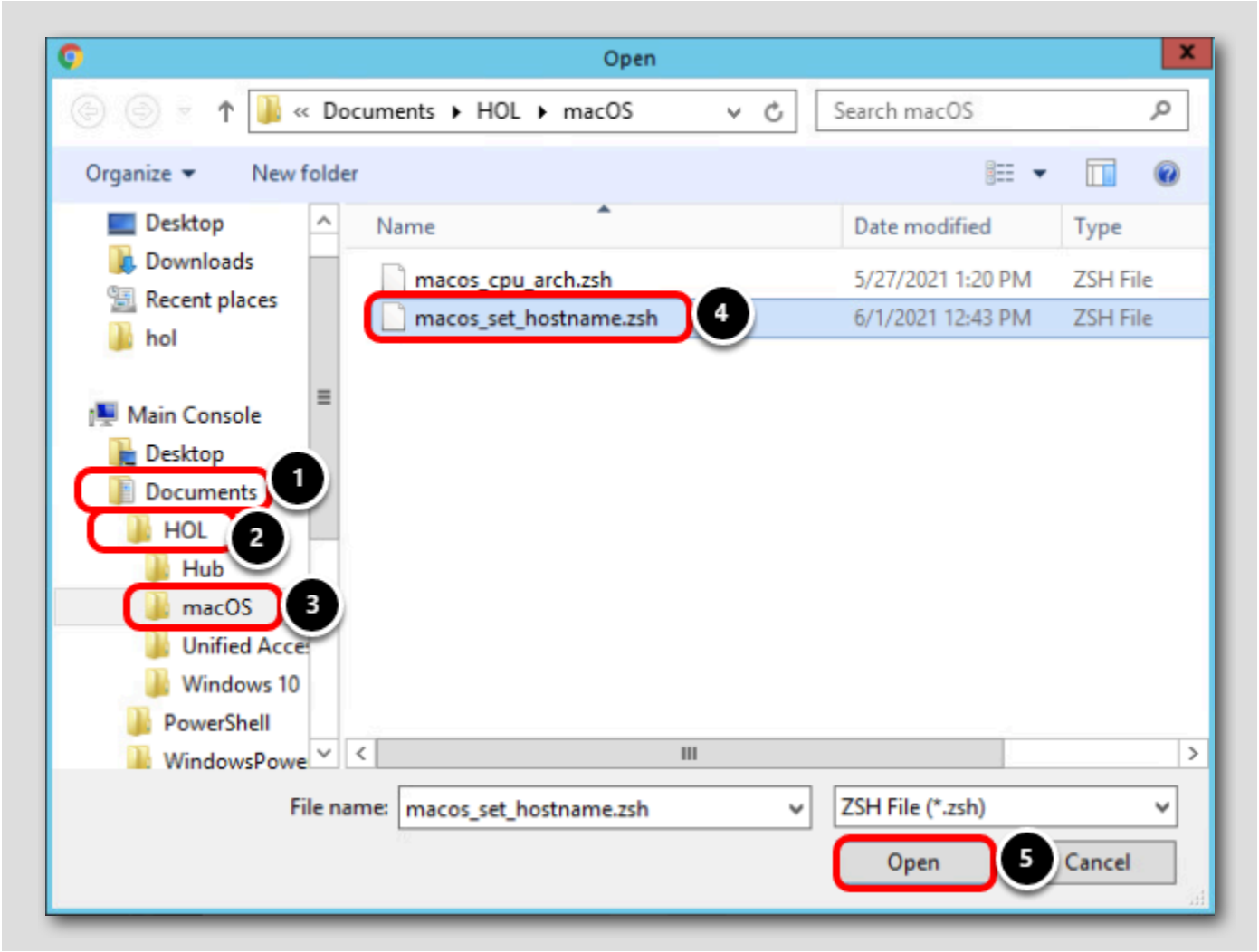


1. Select Zsh for the language
2. Select System for the Execution Context
3. Enter **`30`** as the Timeout value
4. Click Upload to select a file containing the code you wish to use for this Script. Optionally, you could enter the code in the Code window below this section.

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

Upload the macos_set_hostname.zsh File

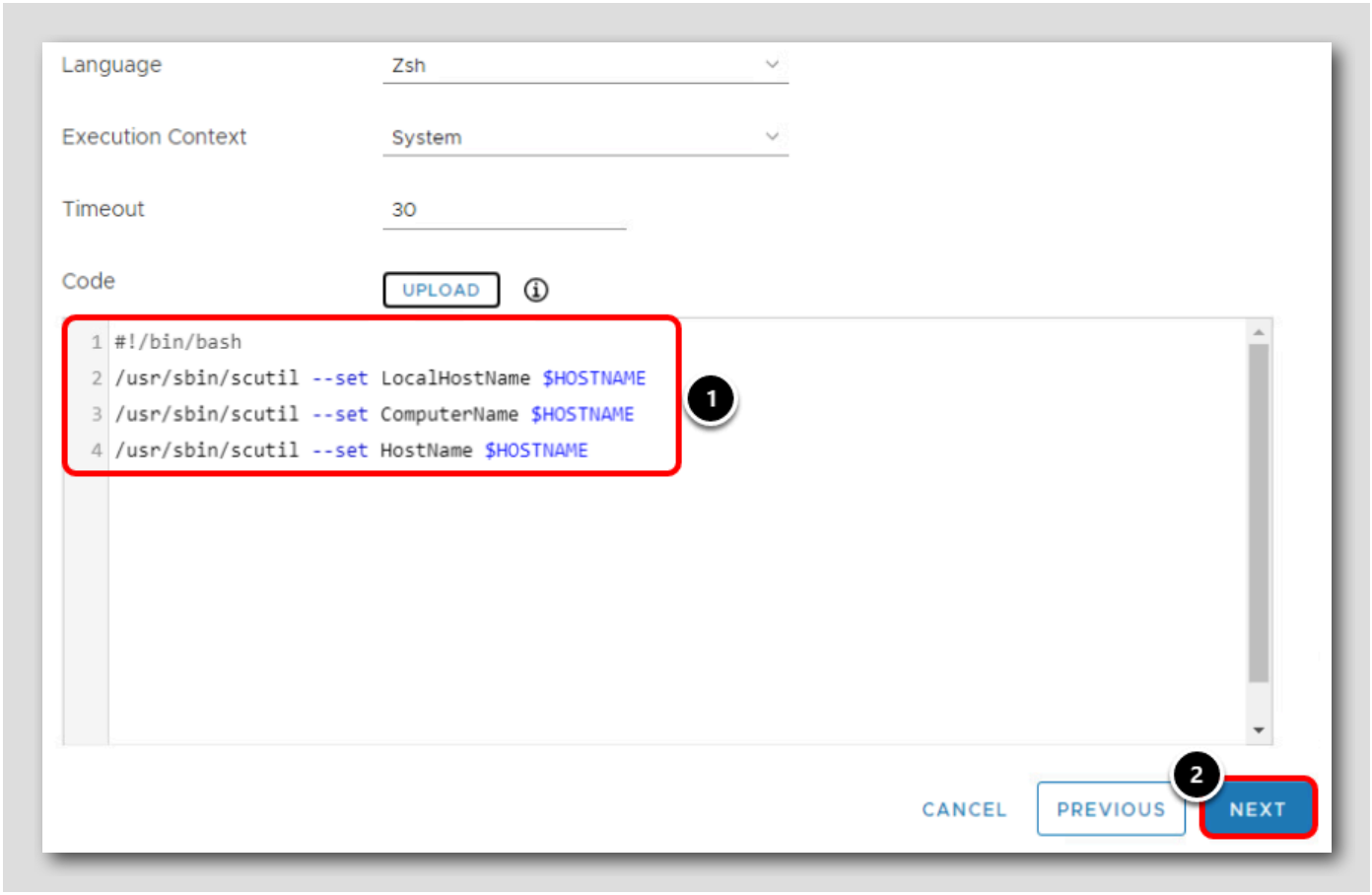
[248]



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

Confirm Script Details

[249]

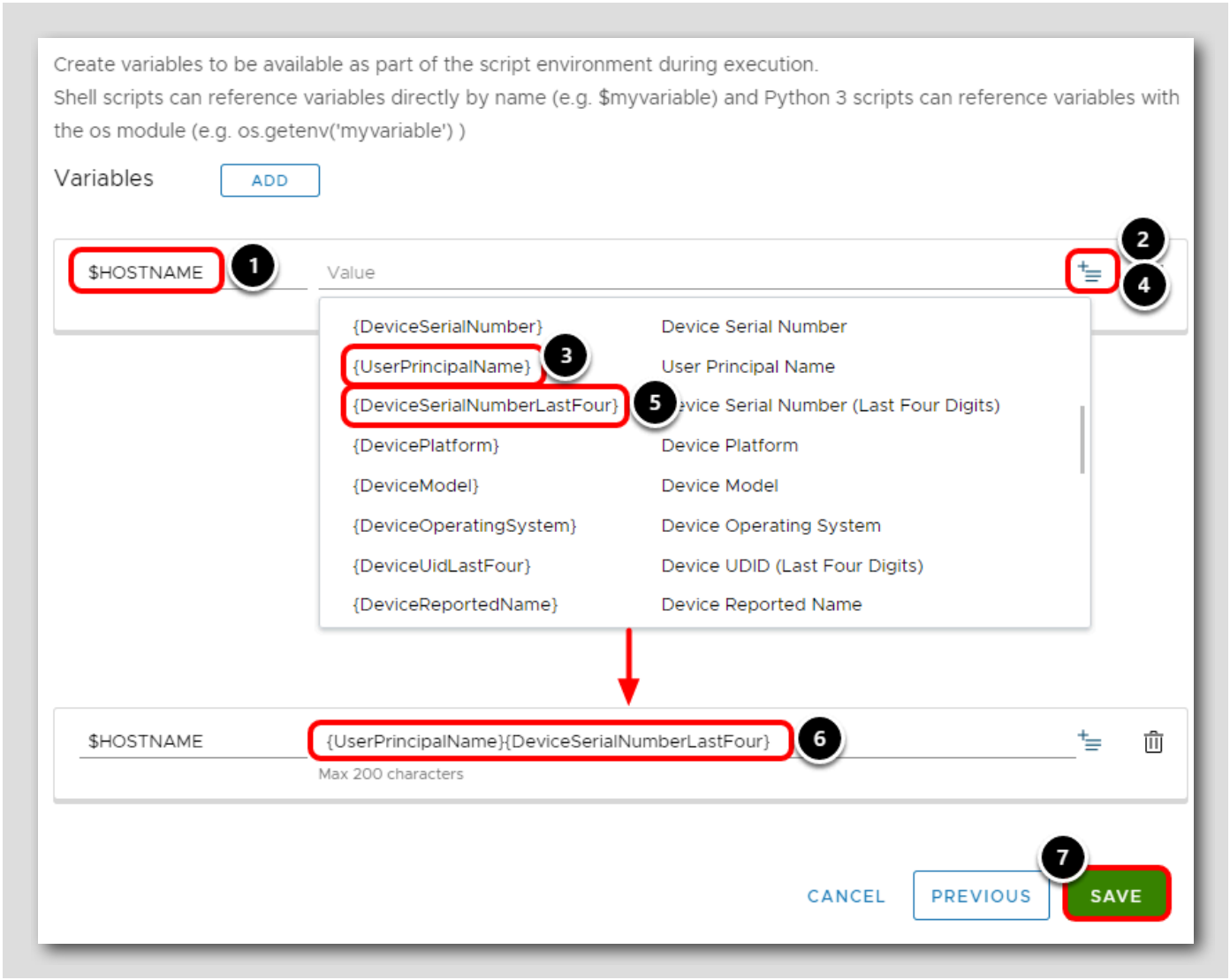


1. Confirm that the script uploaded. Alternatively, you can choose to type the code directly into the window.
2. Click **Next**.

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

Set a Value for the Hostname Variable

[250]



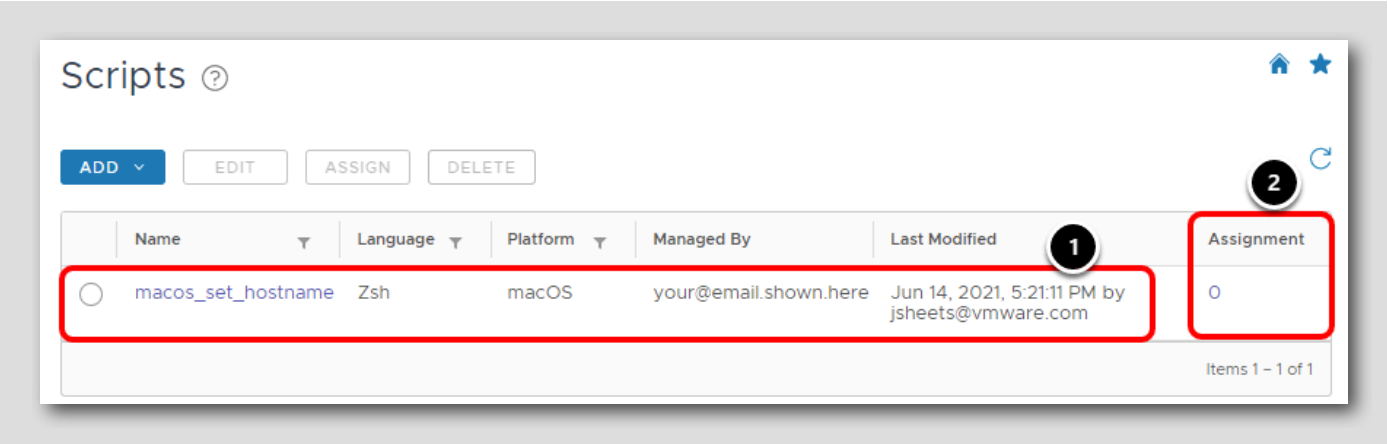
The value of the $HOSTNAME variable can be statically set, or dynamically set by using lookup values. Lookup values retrieve the value from the device at runtime to allow for dynamic values. For example, the **{UserPrincipalName}** lookup value will substitute the actual user principal name of the enrolled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

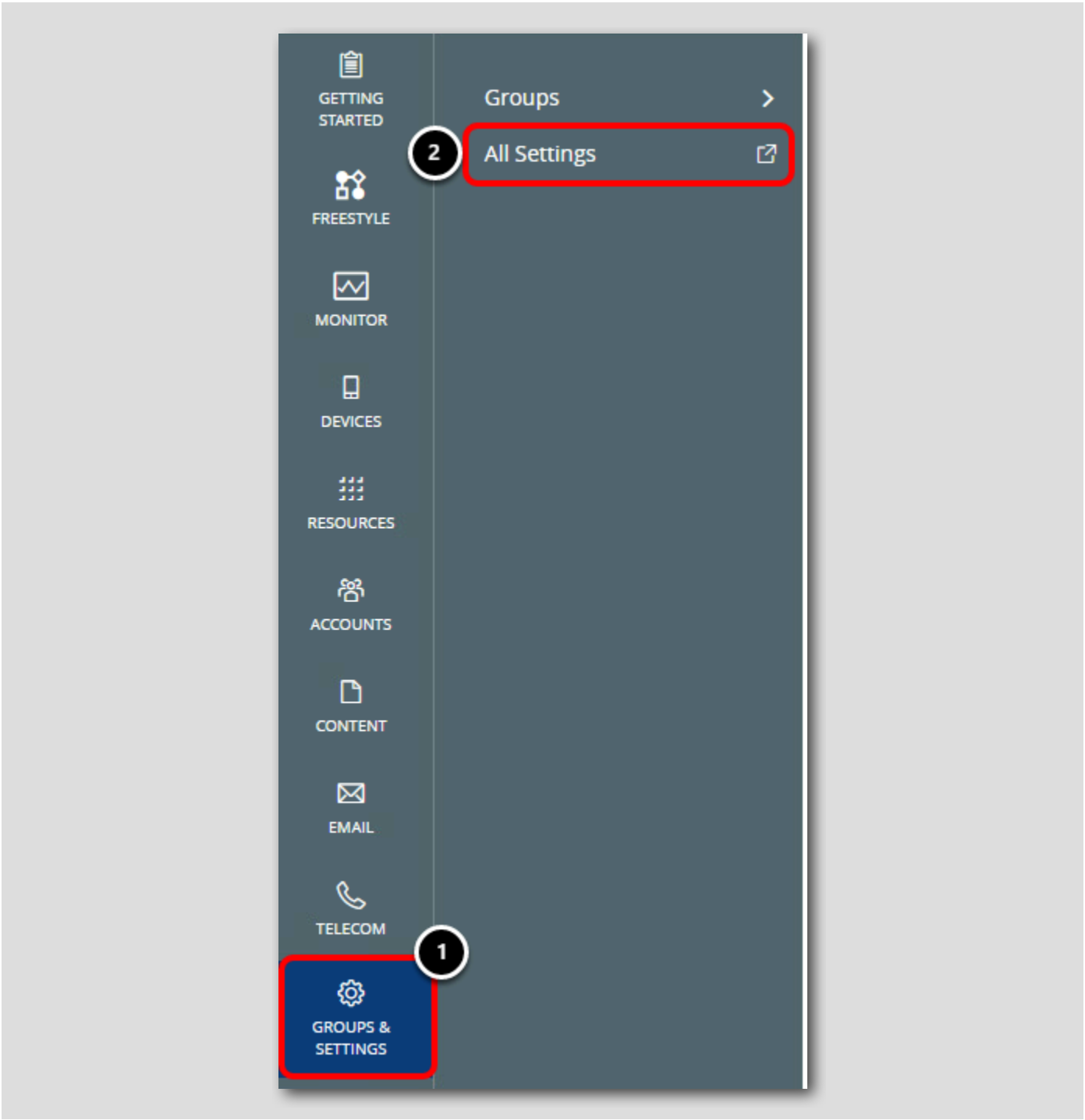
Prior to deploying a macOS Application, VMware Workspace ONE UEM administrators must enable their environments for Software Management. The following items are pre-requisites for macOS Software Management:

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]

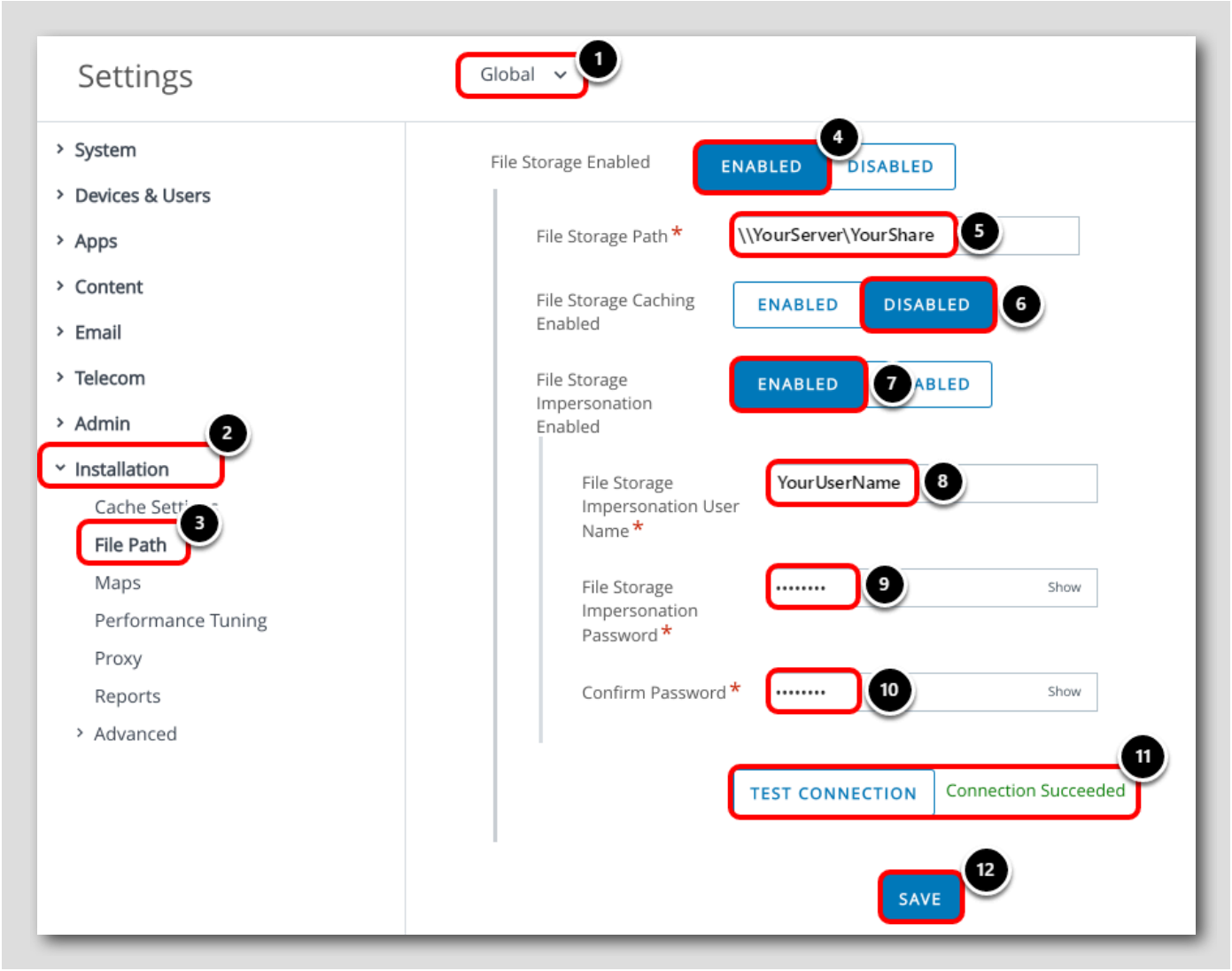


NOTE: The steps in this section have already been completed for you in the Hands-On Lab. You DO NOT need to Enable Software Management as it has already been completed on your behalf.

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

Enable File Storage (REFERENCE ONLY)

[256]

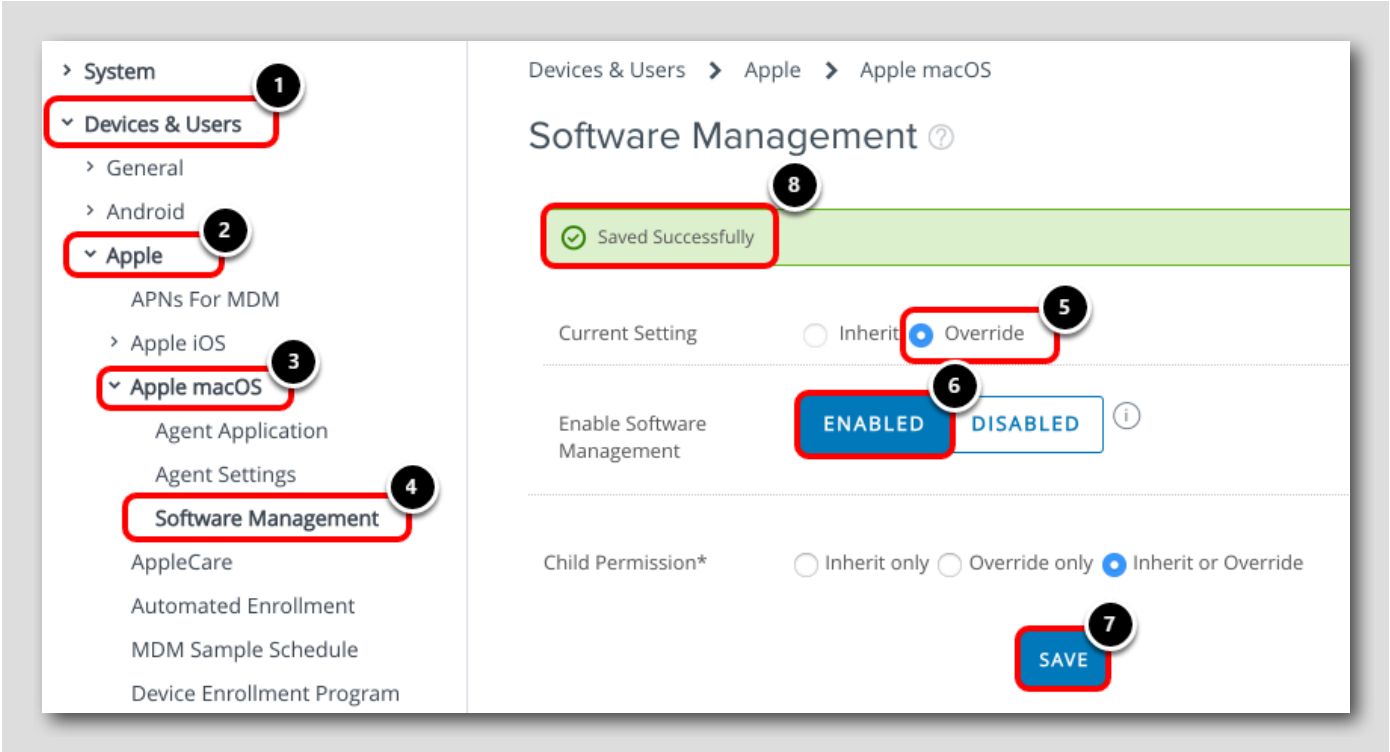


NOTE: The steps in this section have already been completed for you in the Hands-On Lab. You DO NOT need to Enable Software Management as it has already been completed on your behalf.

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.

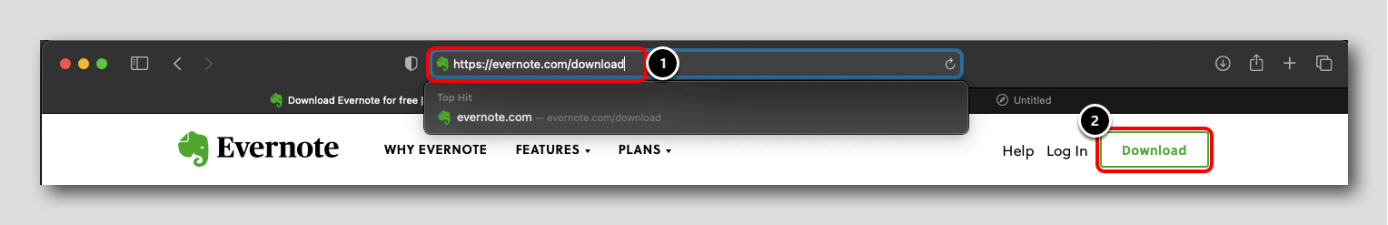
In this section, you will download the Workspace ONE Admin Assistant tool and use it to prepare another 3rd-Party application for deployment.

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**.

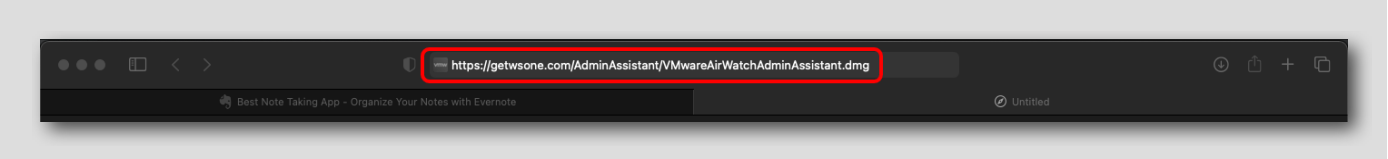
The DMG file for Evernote will download to the Downloads folder.

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`**

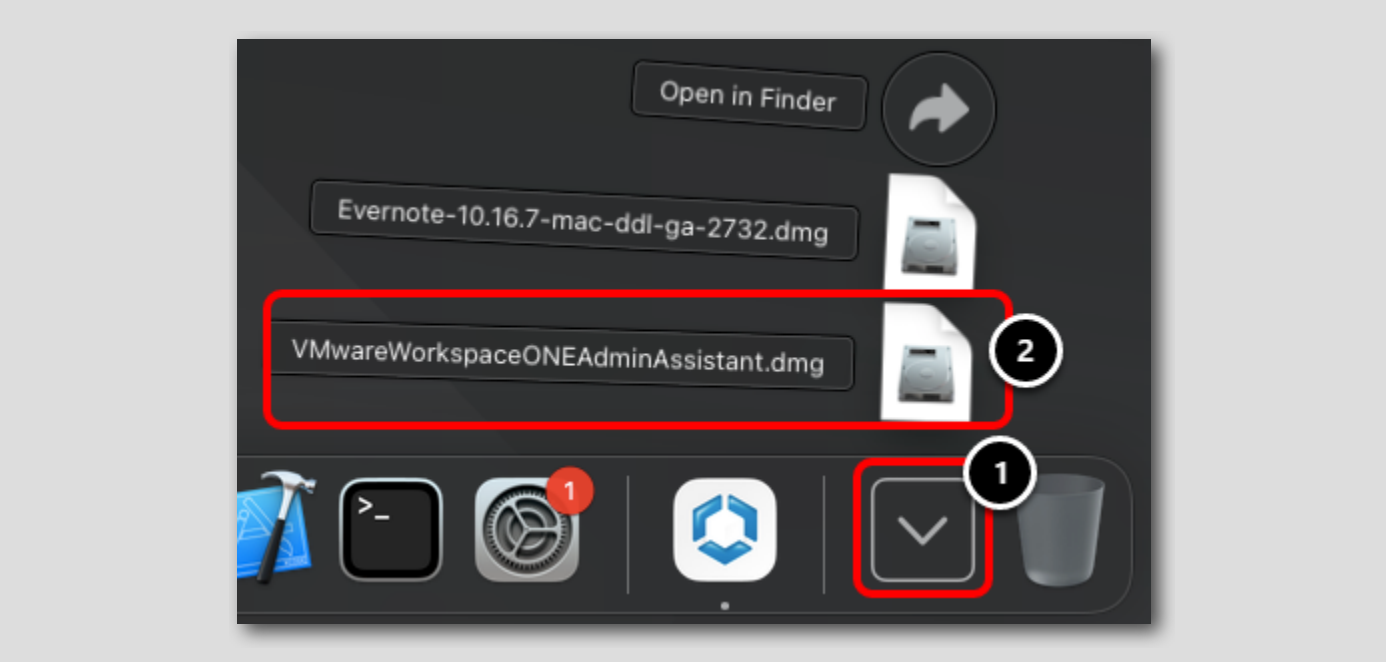
The DMG file will download to the Downloads folder.

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:

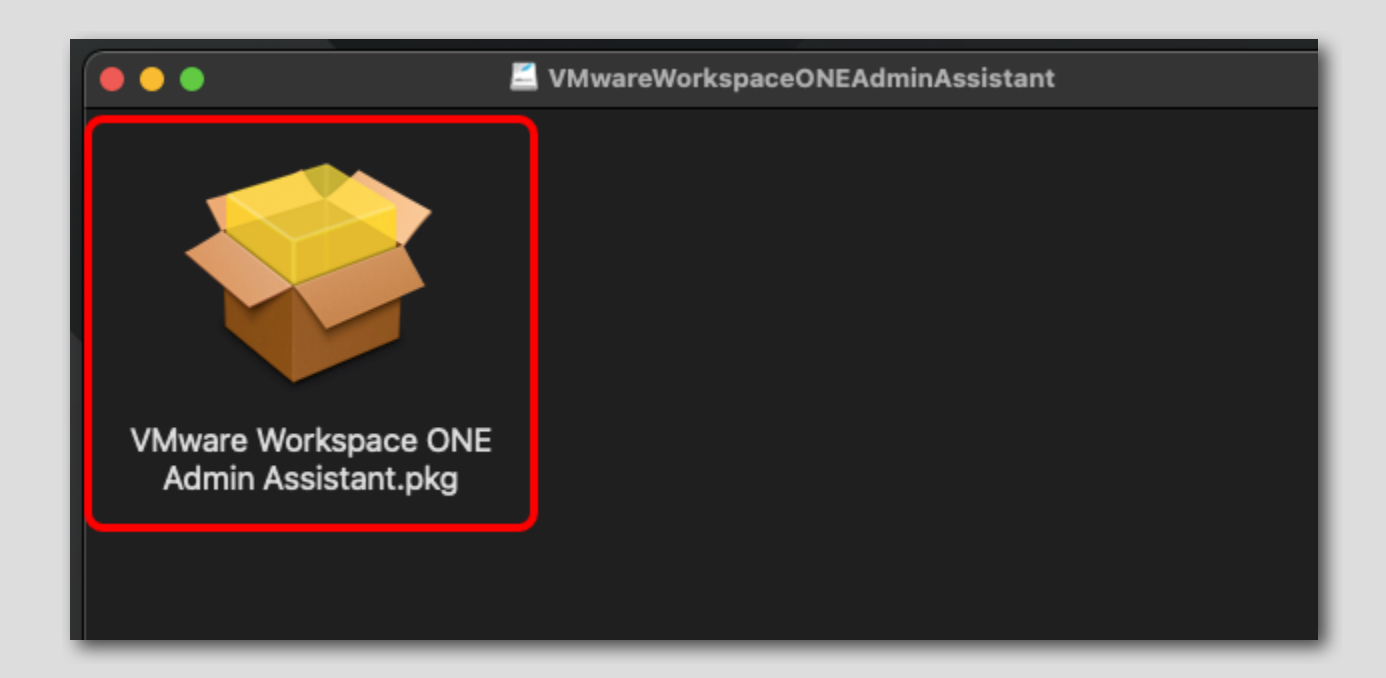
1. Click the **Downloads** folder.
2. Click **VMwareWorkspaceONEAdminAssistant.dmg**.

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.



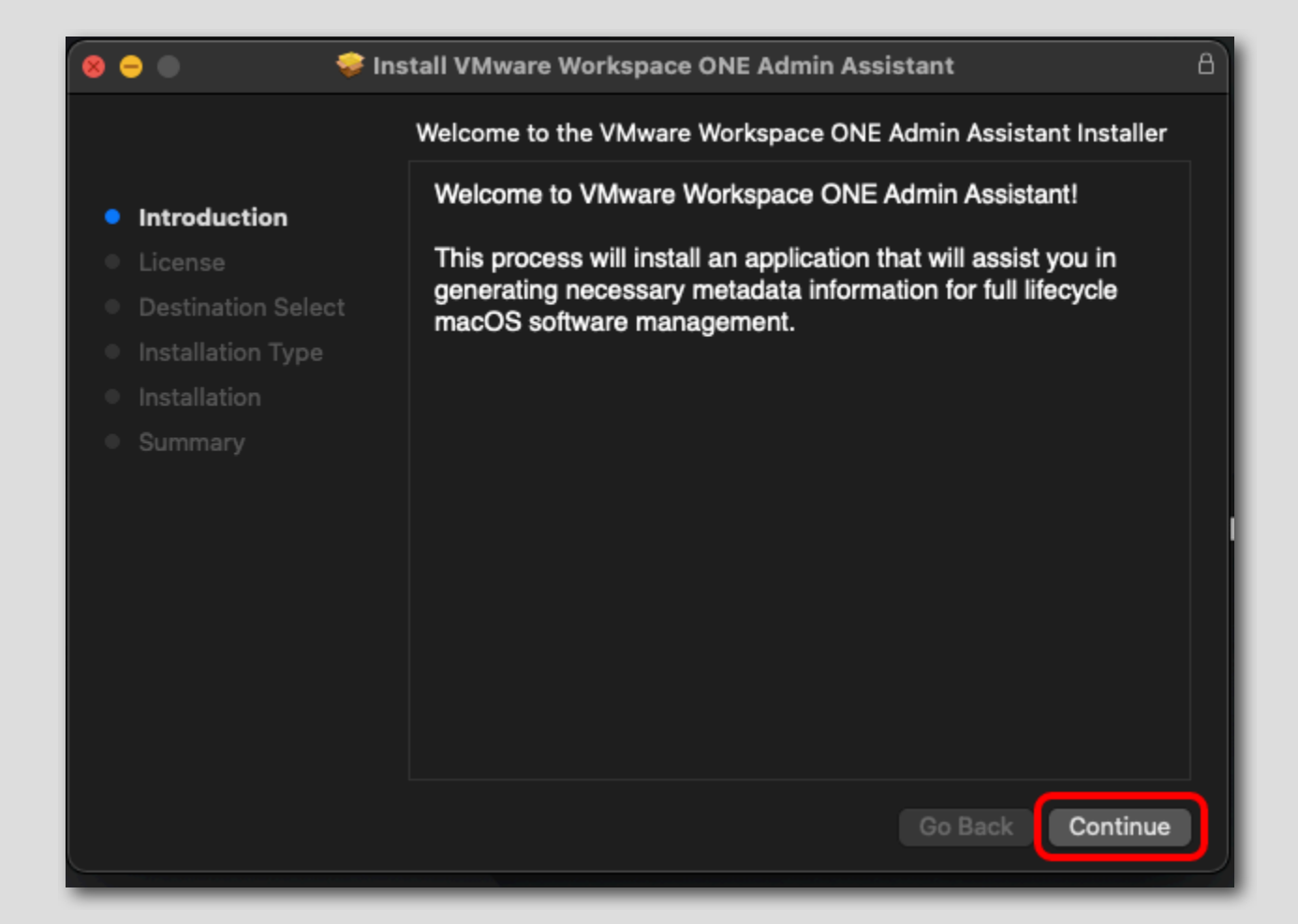
Double-click the **VMware Workspace ONE Admin Assistant.pkg** file

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.

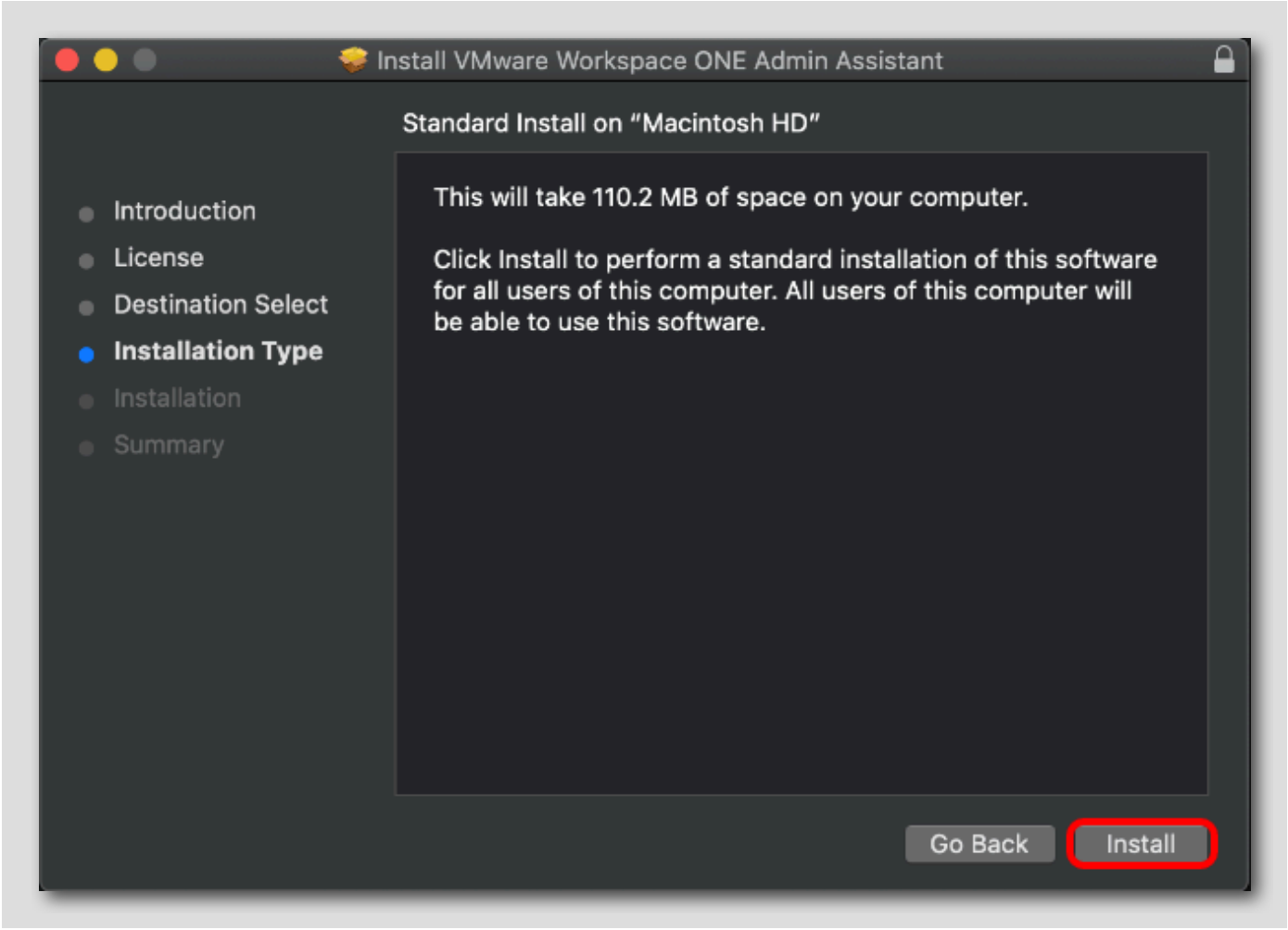
1. Review the License Agreement and click **Continue**
2. Click **Agree**.

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.



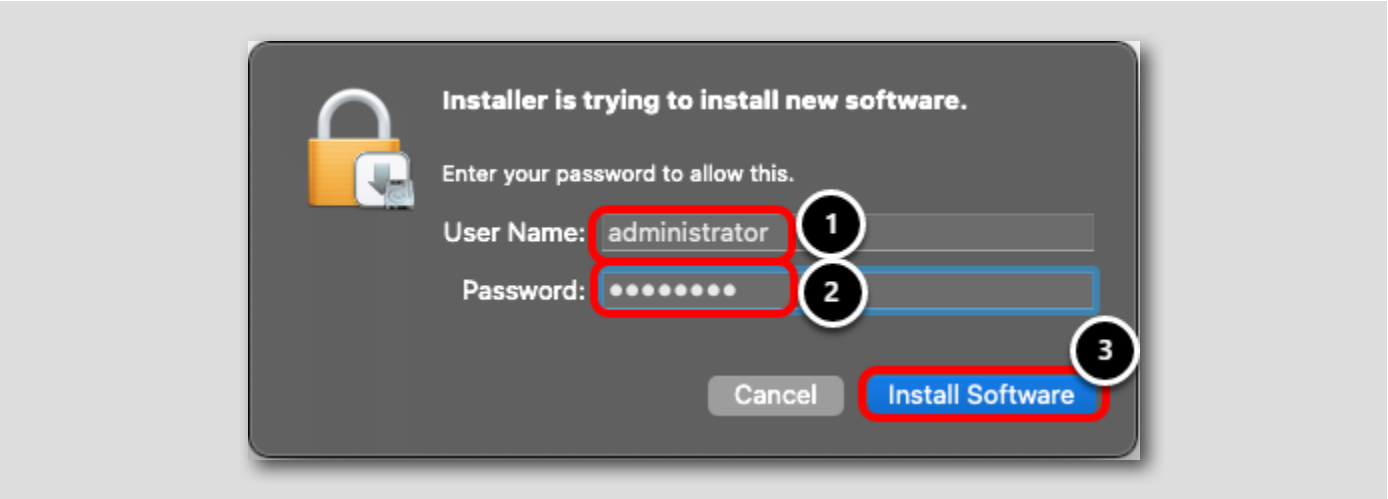
Click **Install**.

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.

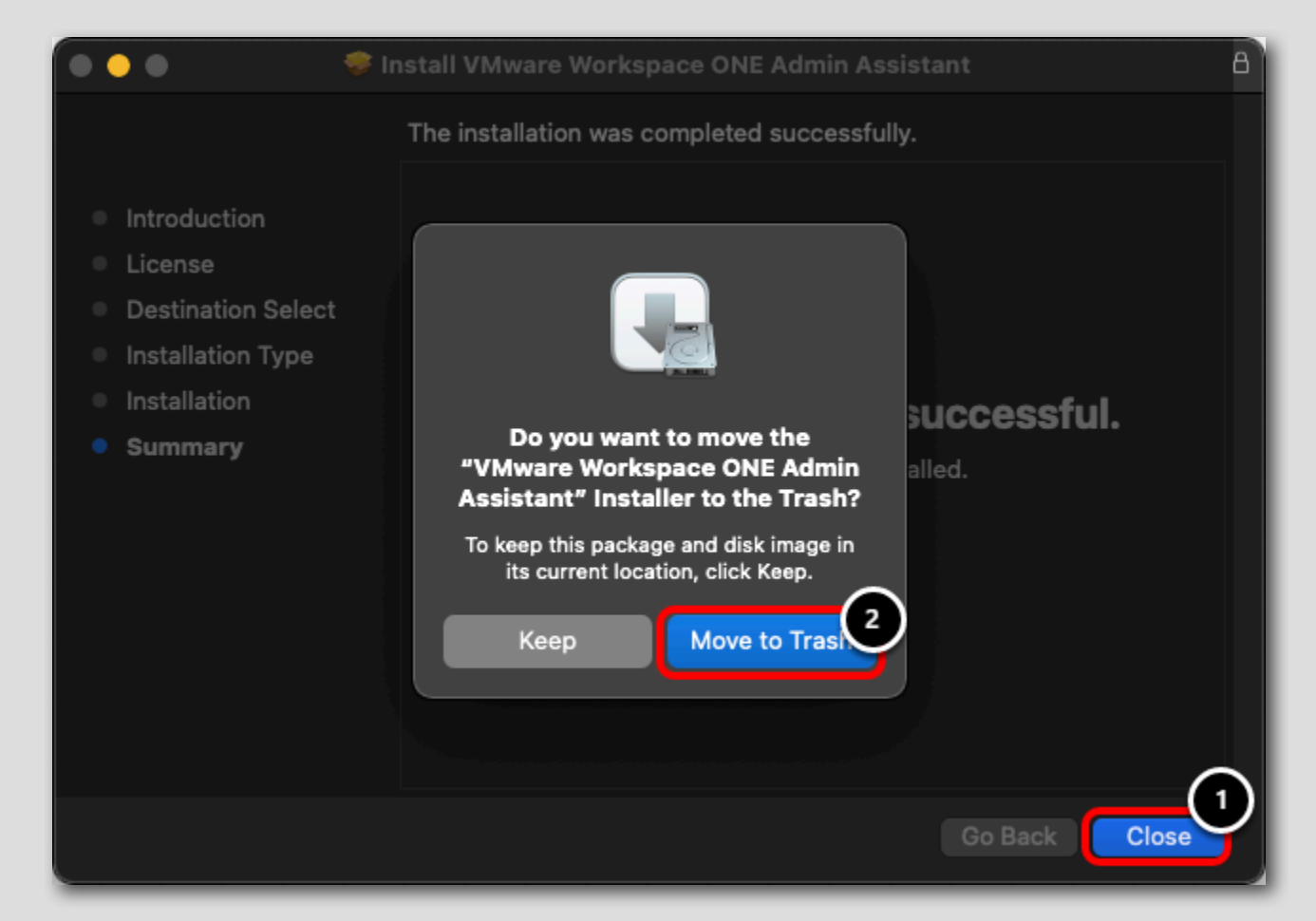
1. Enter the username for the device
2. Enter the password for the device
3. Click **Install Software**

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.



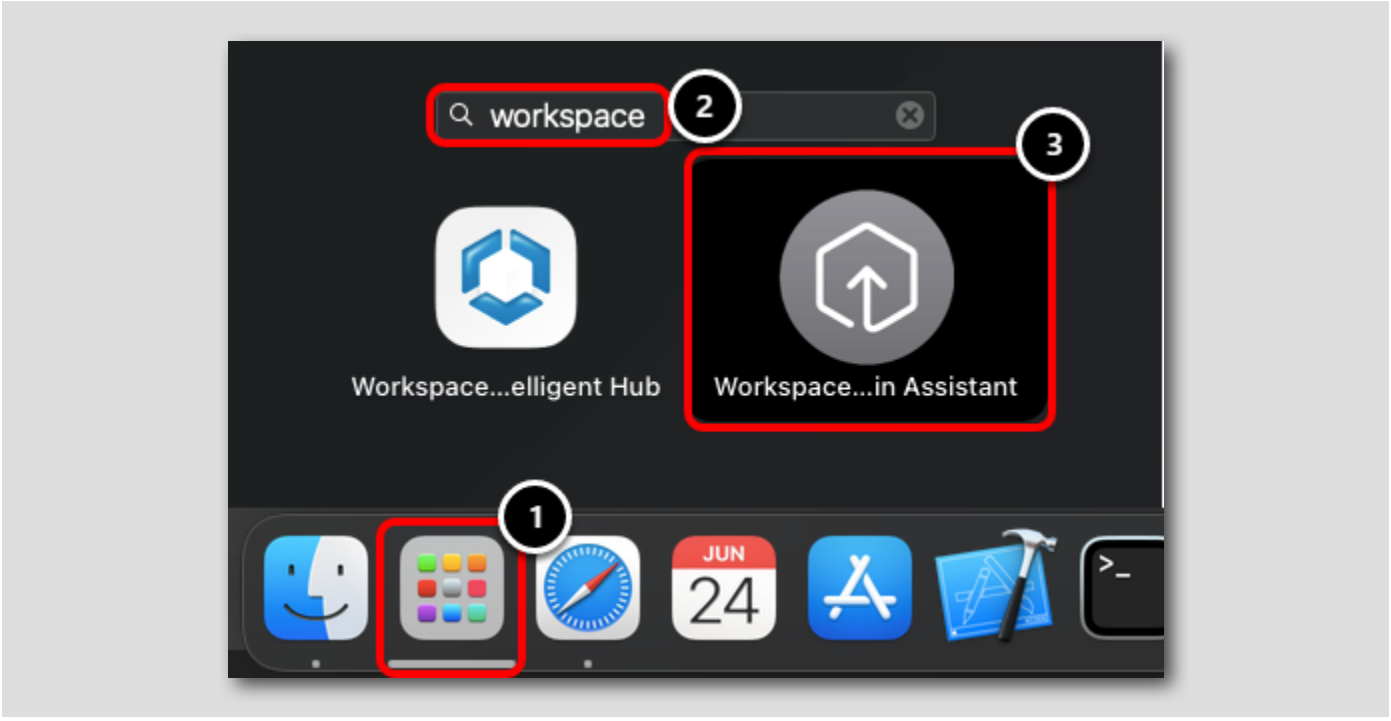
1. Click **Close** when the installer completes
2. Click **Move to Trash** to clean up the installer

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.



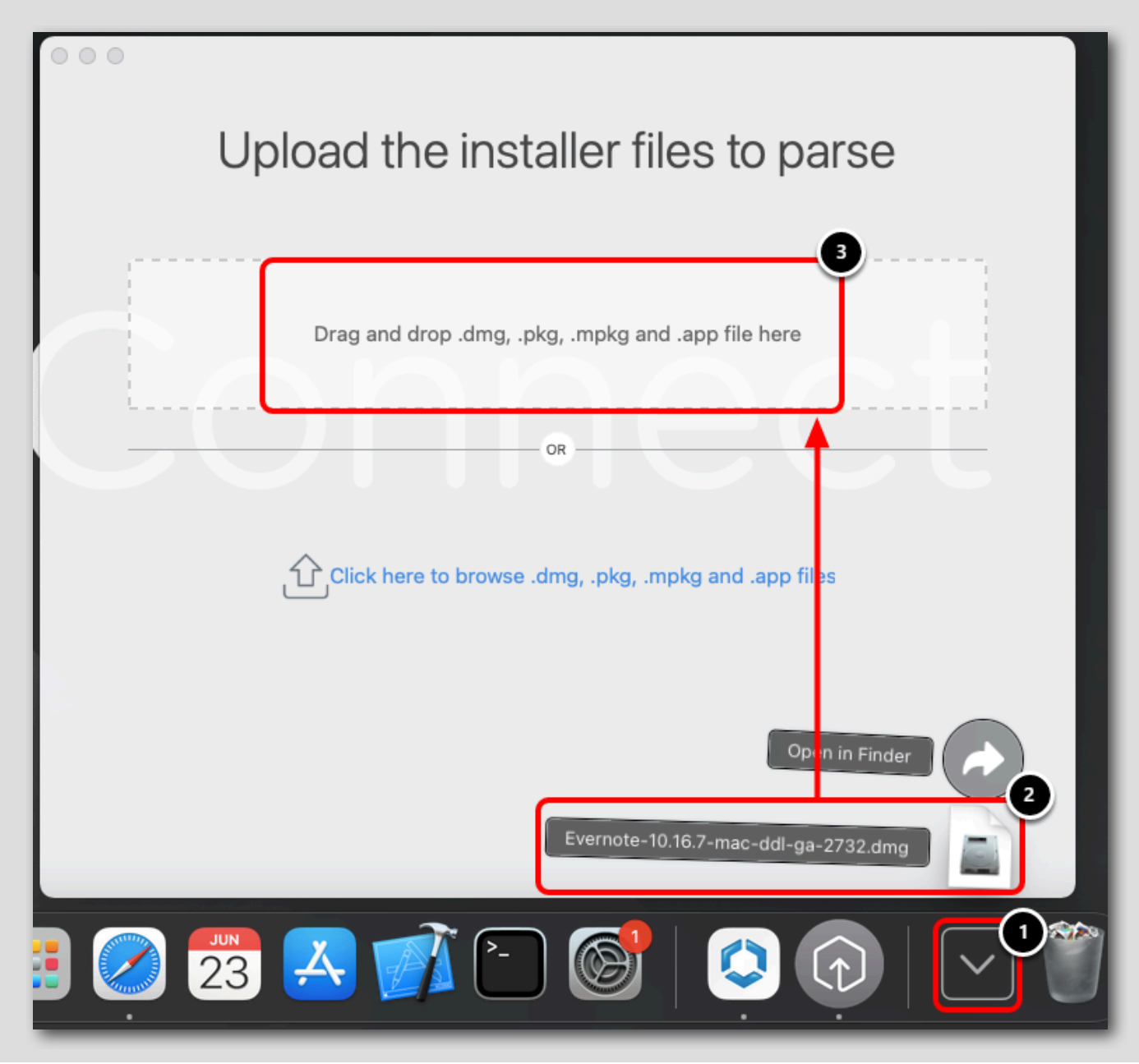
1. Launch **Launchpad**
2. Enter **`Workspace`** in the search bar
3. Click **Workspace ONE Admin Assistant**

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.

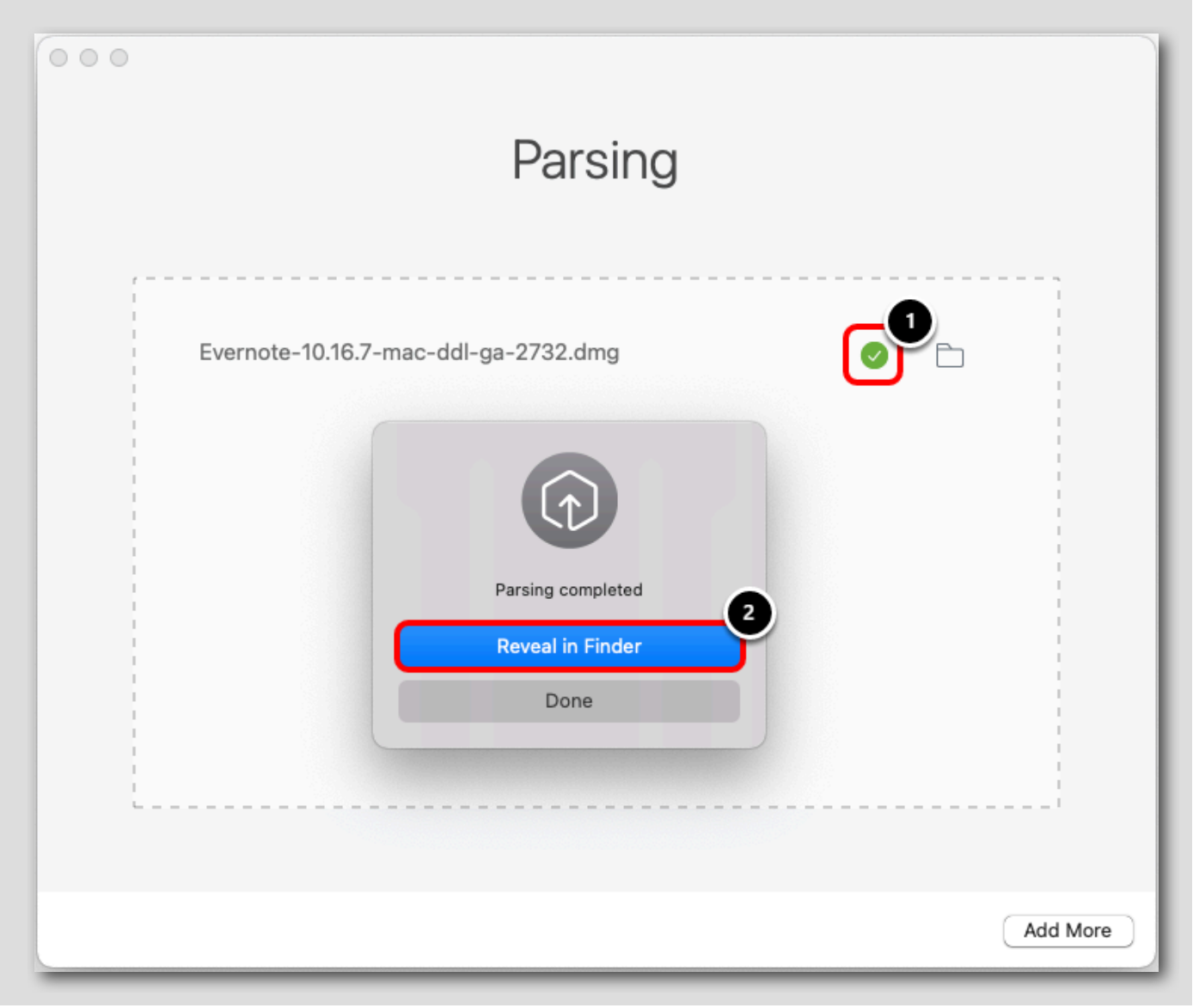
The Workspace ONE Admin Assistant Tool begins parsing the file to extract information necessary to deploy the software.

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.



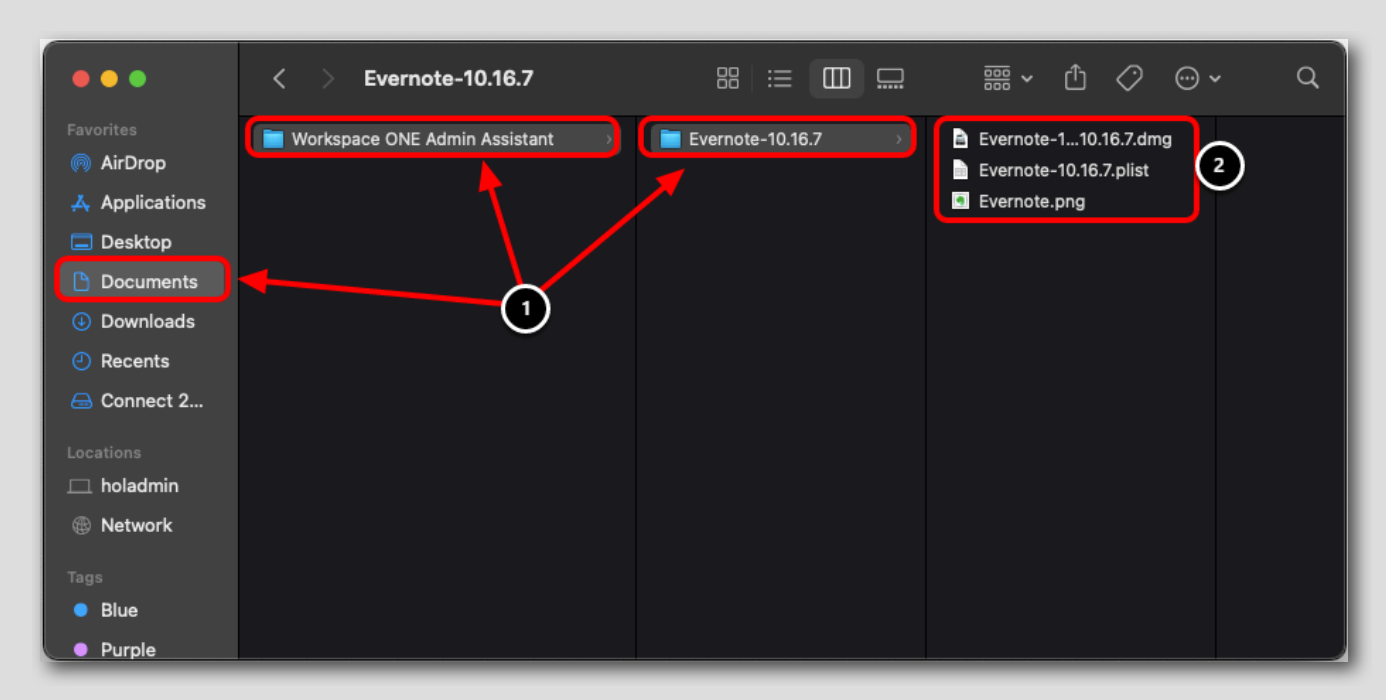
1. Monitor the progress of the parsing. The result will change to a green checkmark when it is completed, which may take 15 - 30 seconds.
2. In the pop-up window, click **Reveal in Finder**

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.

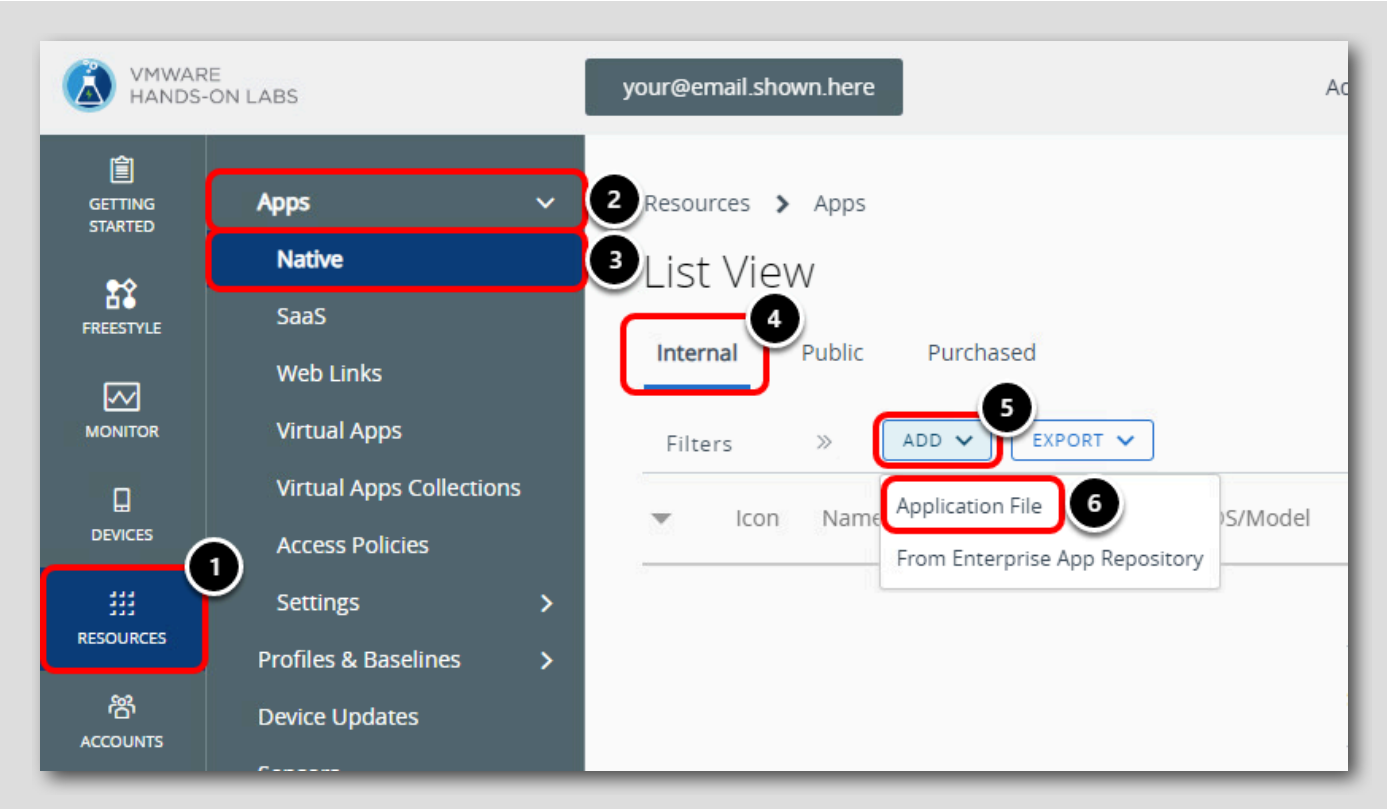
Deploy a 3rd Party macOS Application

[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]

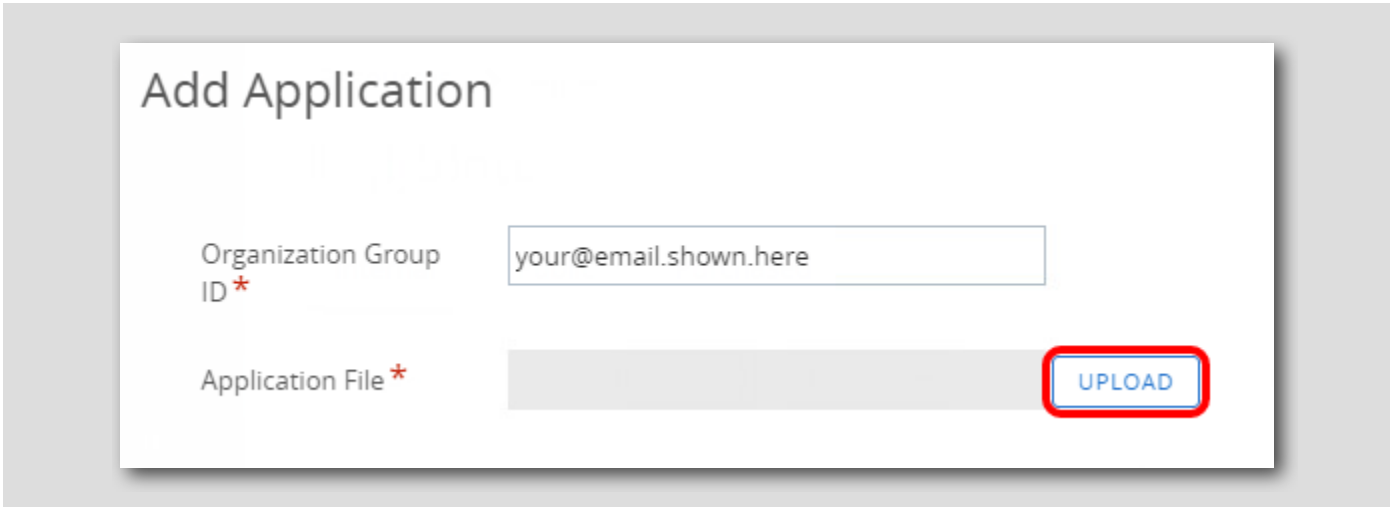


Return to the the Workspace ONE UEM Administrator Console in the Hands-on Lab interface:

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

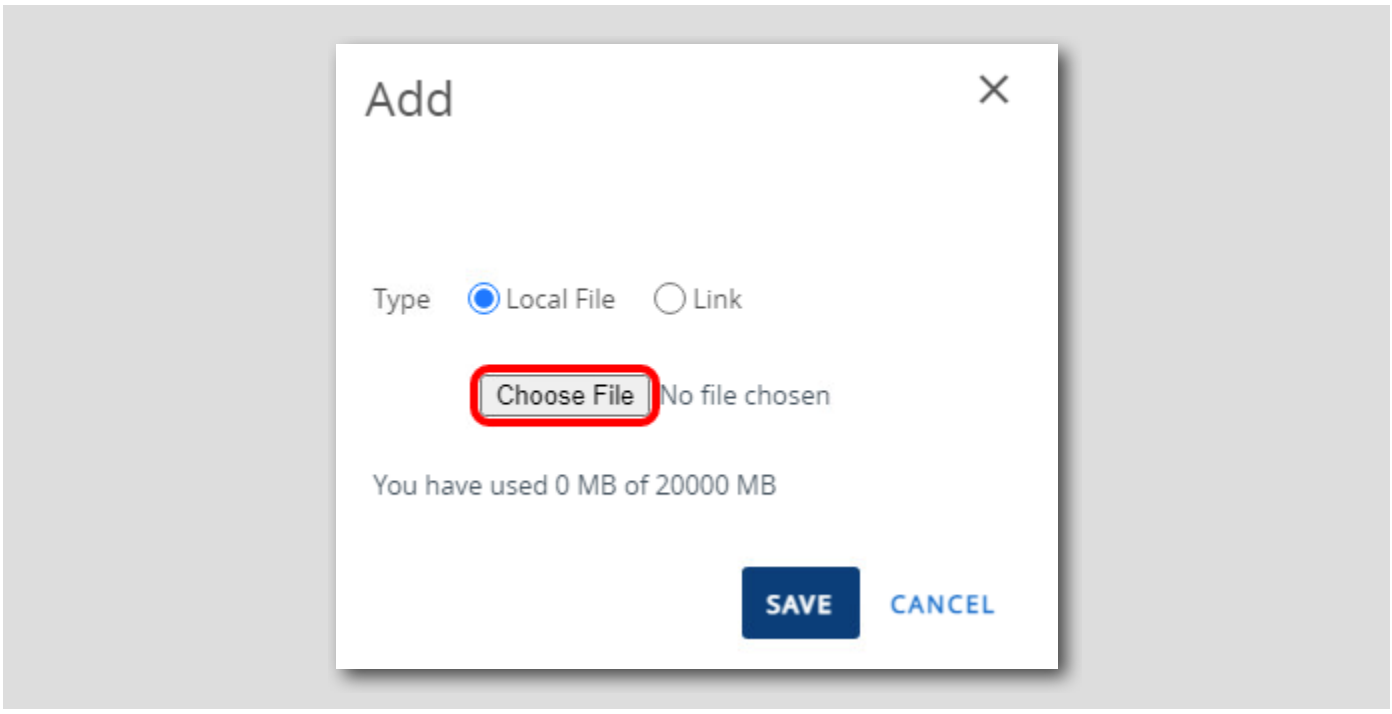
[274]



Click **Upload**.

Choose File for Upload

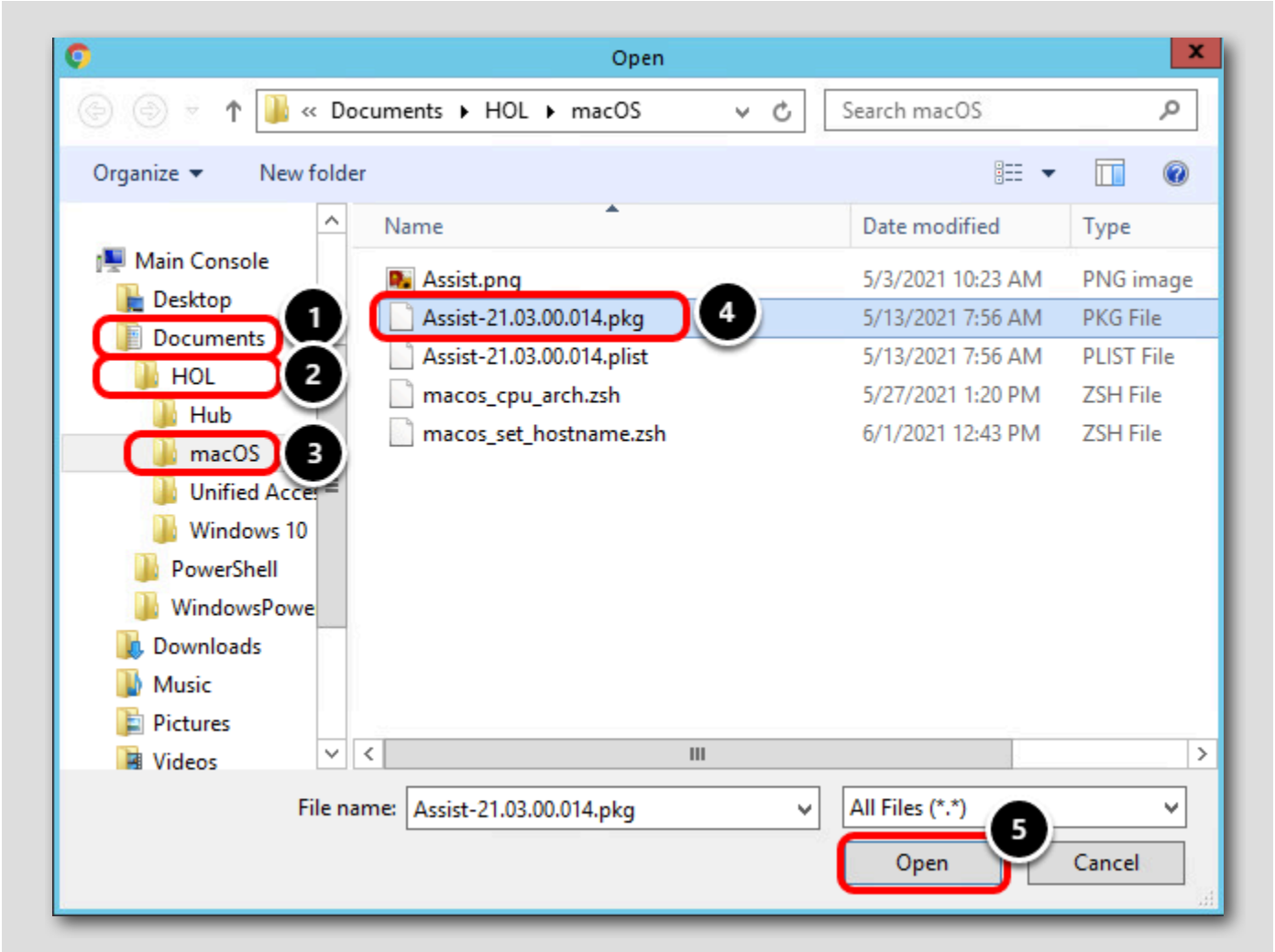
[275]



Click **Choose File**.

Select the Assist PKG File

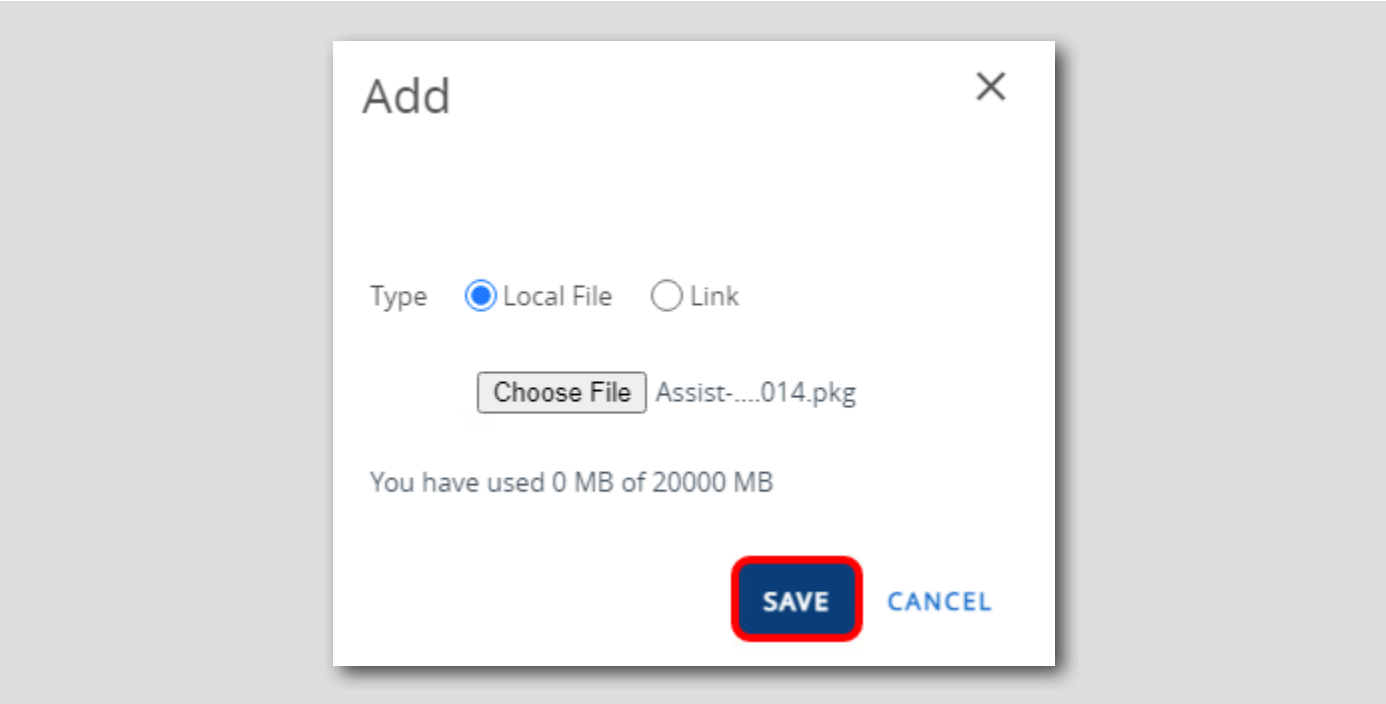
[276]



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]

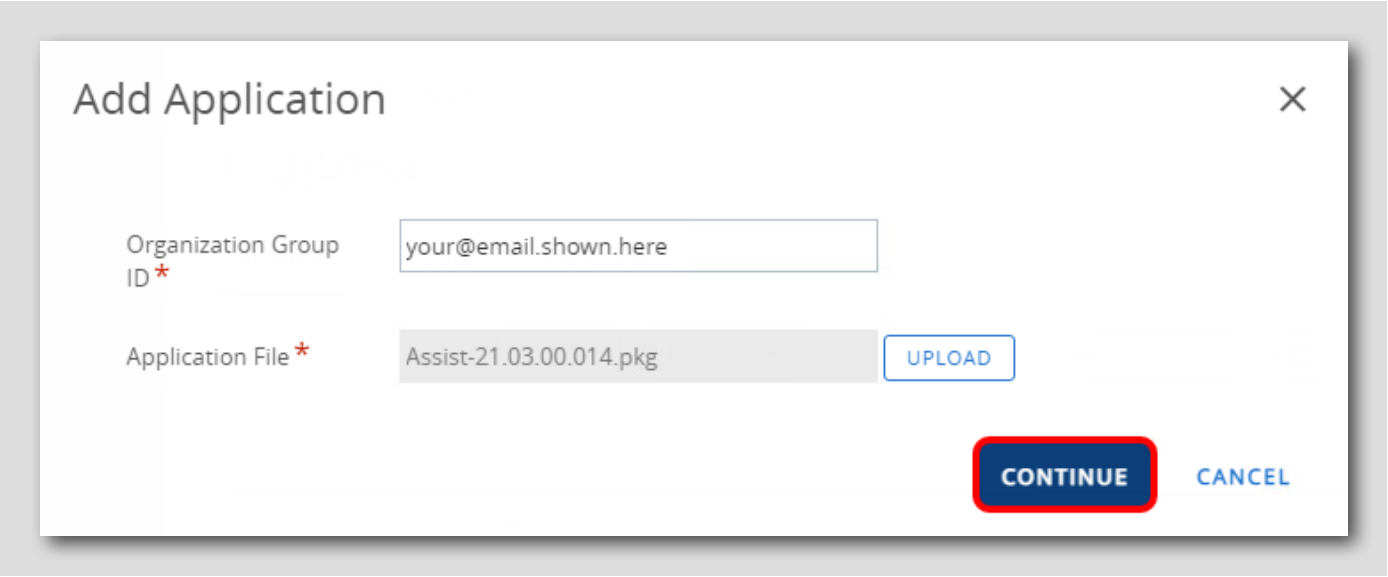


Click **Save** to upload the select Assist-21.03.00.014.pkg file.

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

Continue After Uploading Application

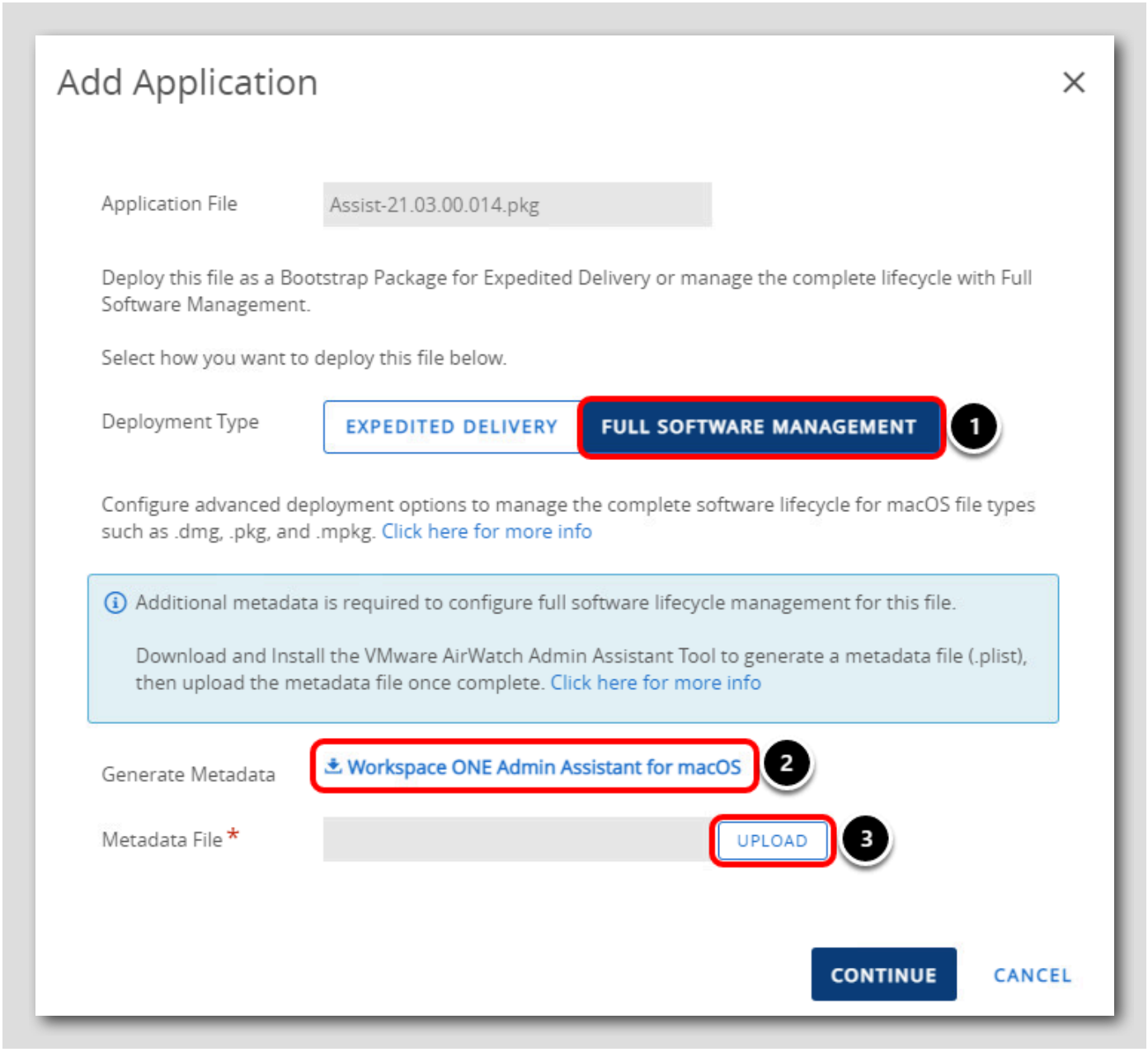
[278]



Click **Continue**.

Configure Deployment Type

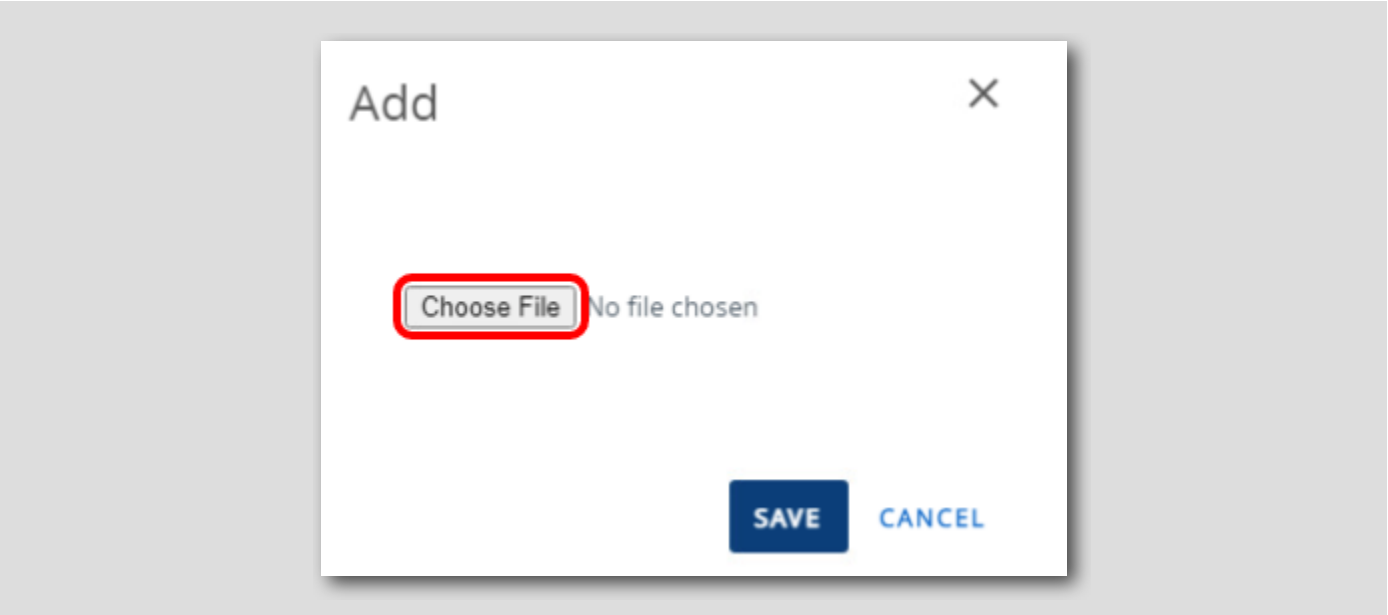
[279]



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

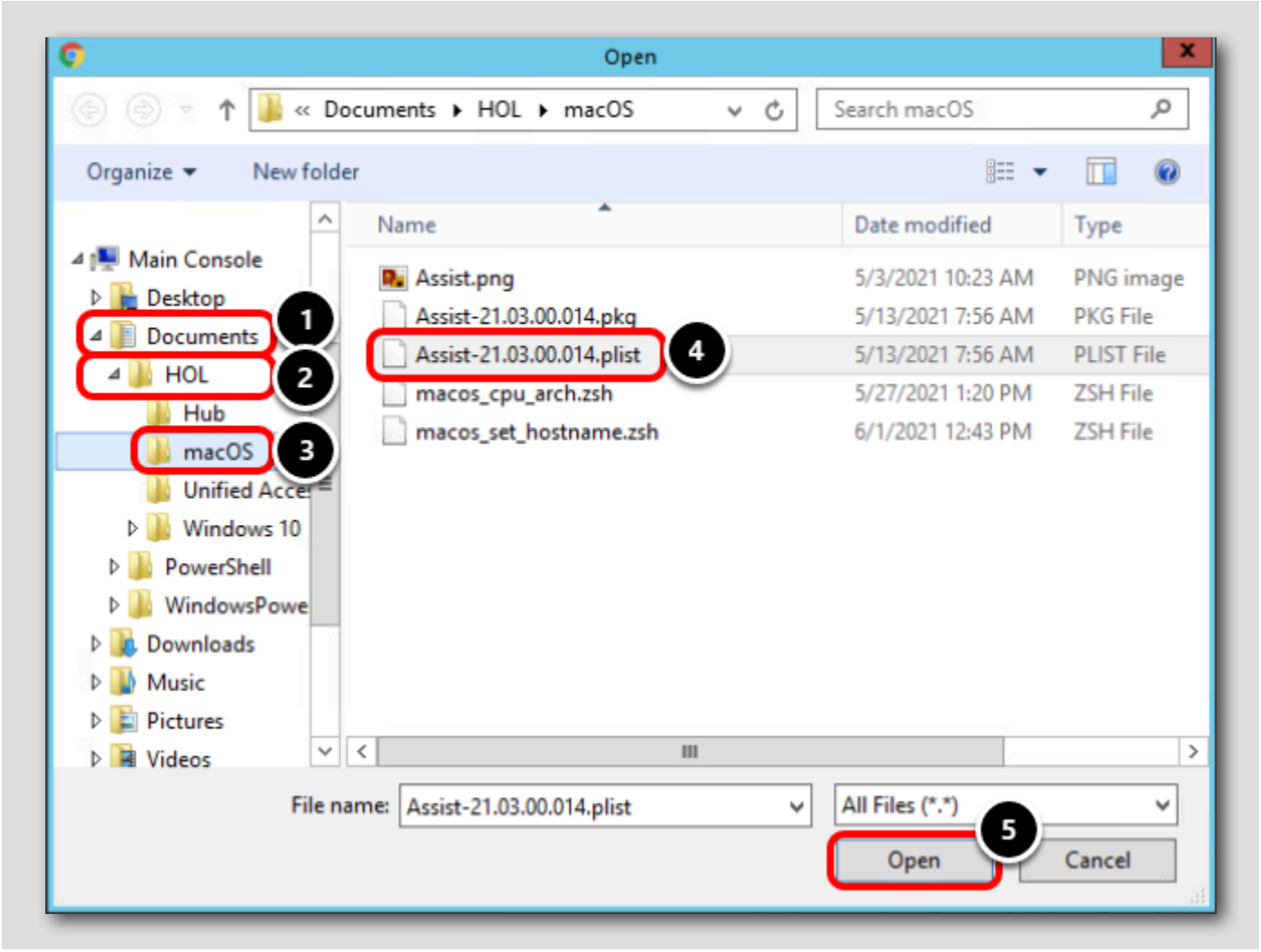
[280]



Click **Choose File**.

Select the Workspace ONE Assist plist File

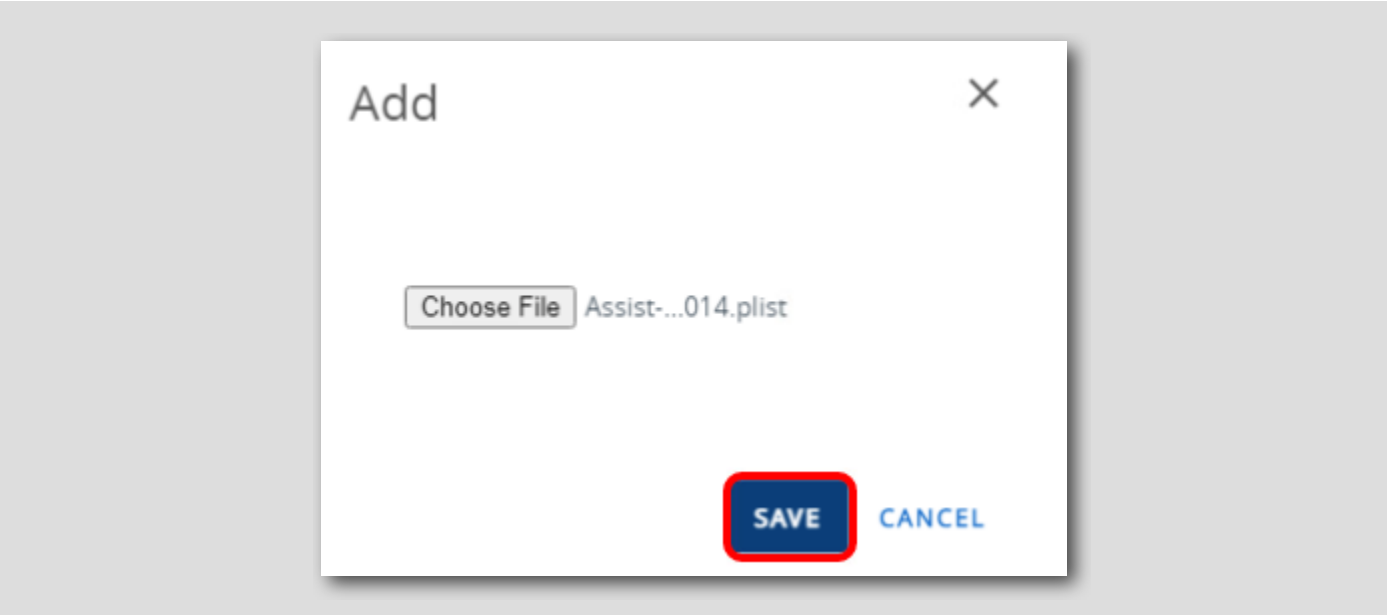
[281]



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

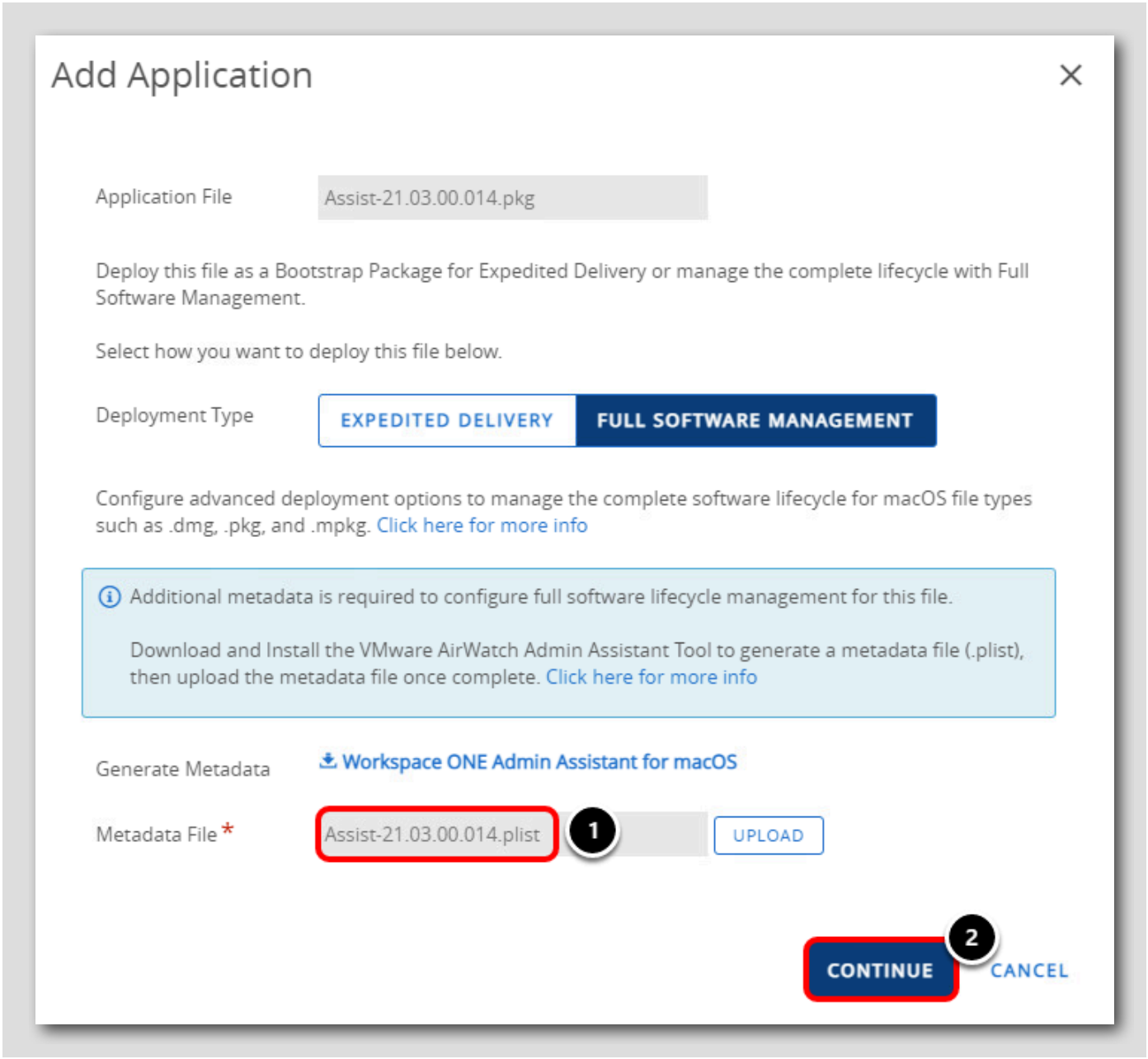
[282]



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

Continue after Metadata File Upload

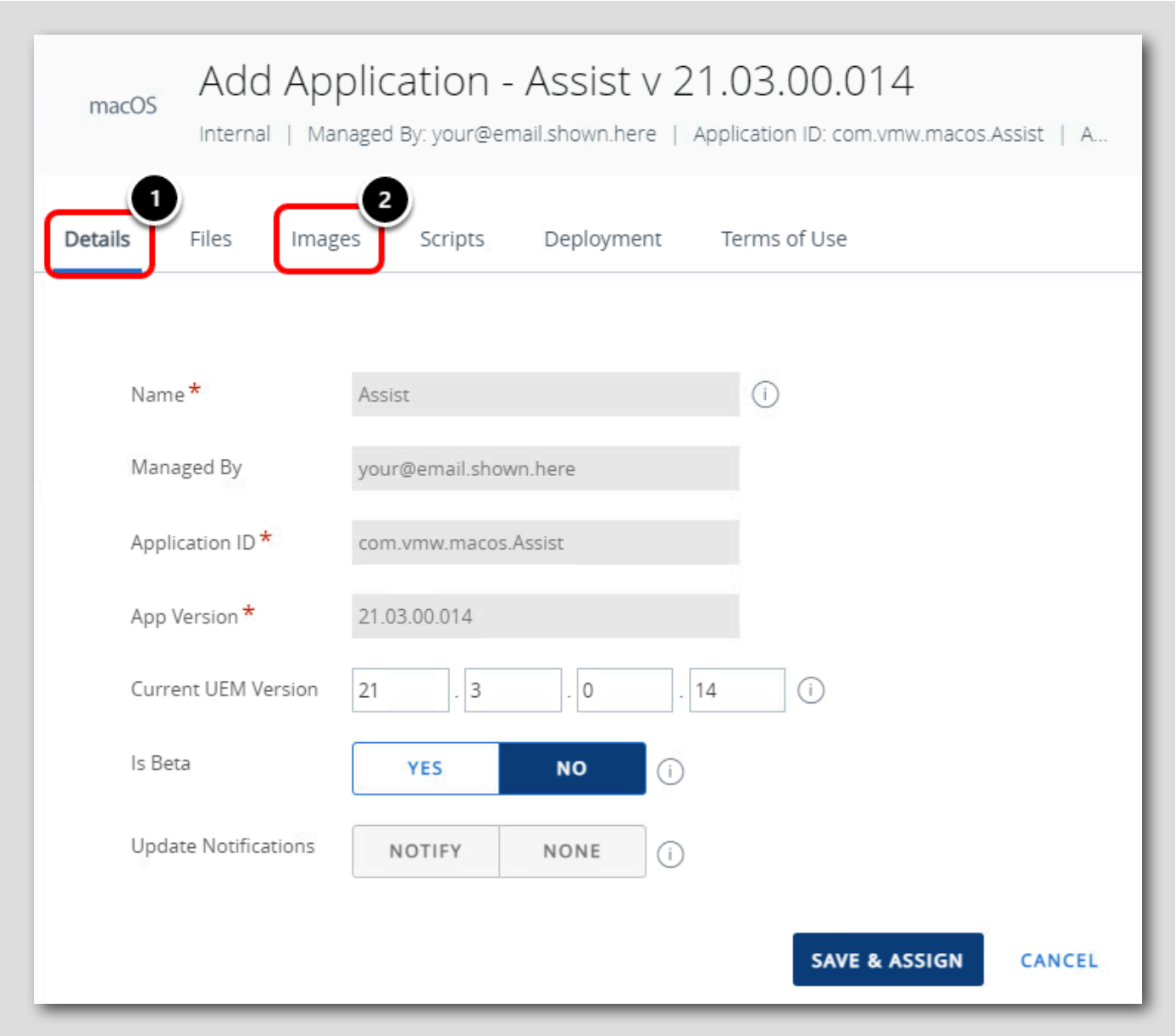
[283]



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

Configure the Application

[284]

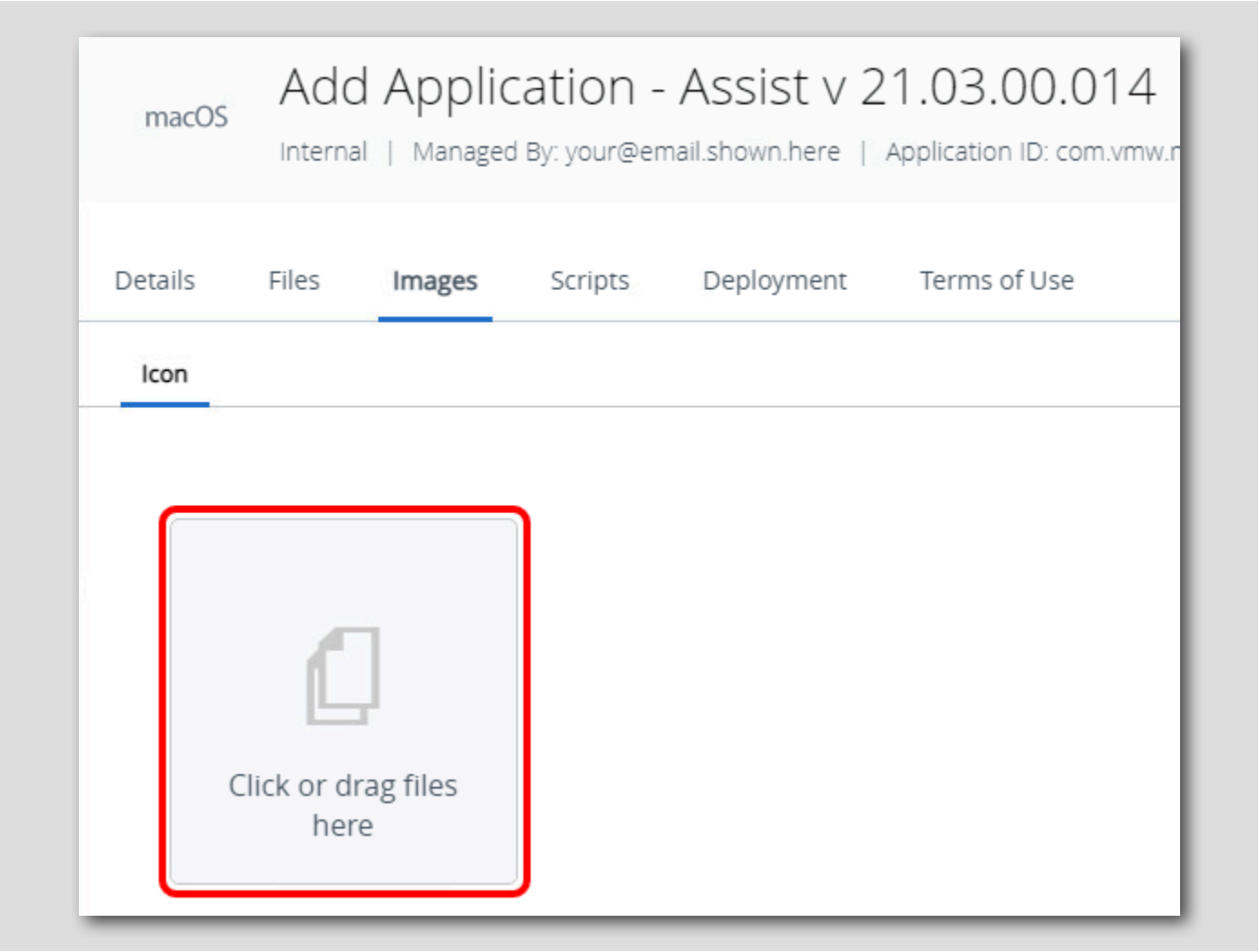


The Workspace ONE Assist application and corresponding metadata have been uploaded to Workspace ONE UEM!

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

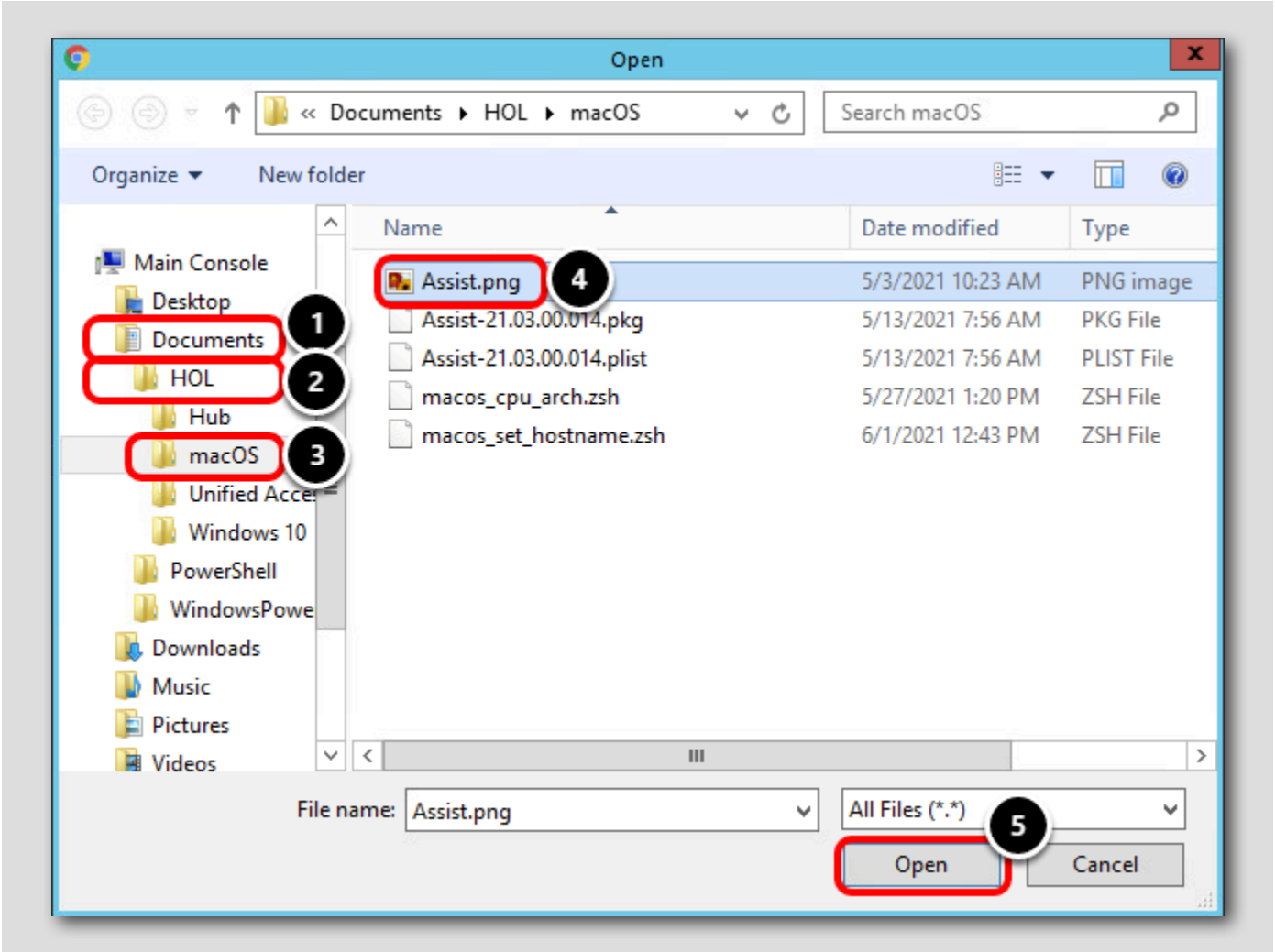
[285]



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

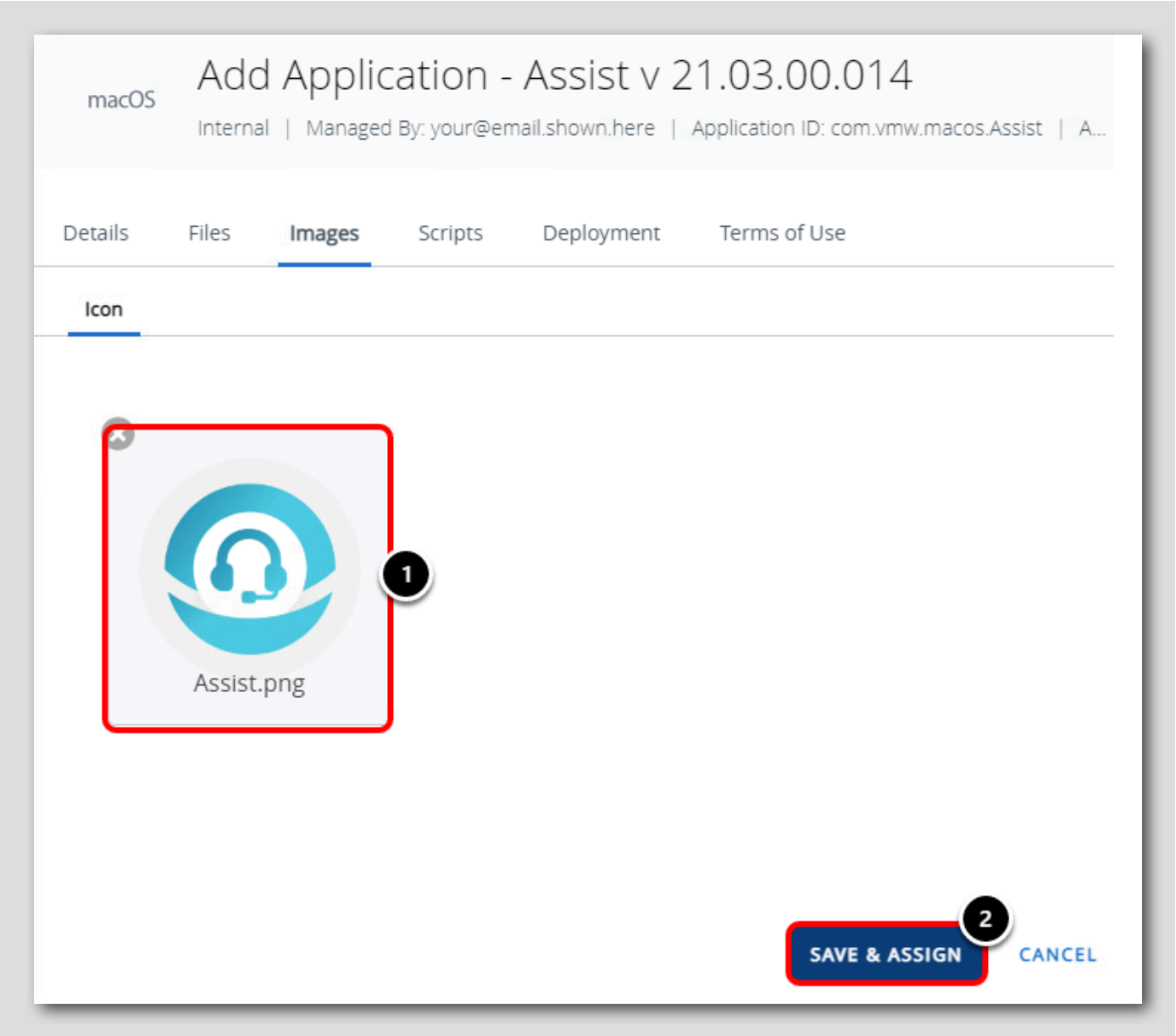
[286]



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**

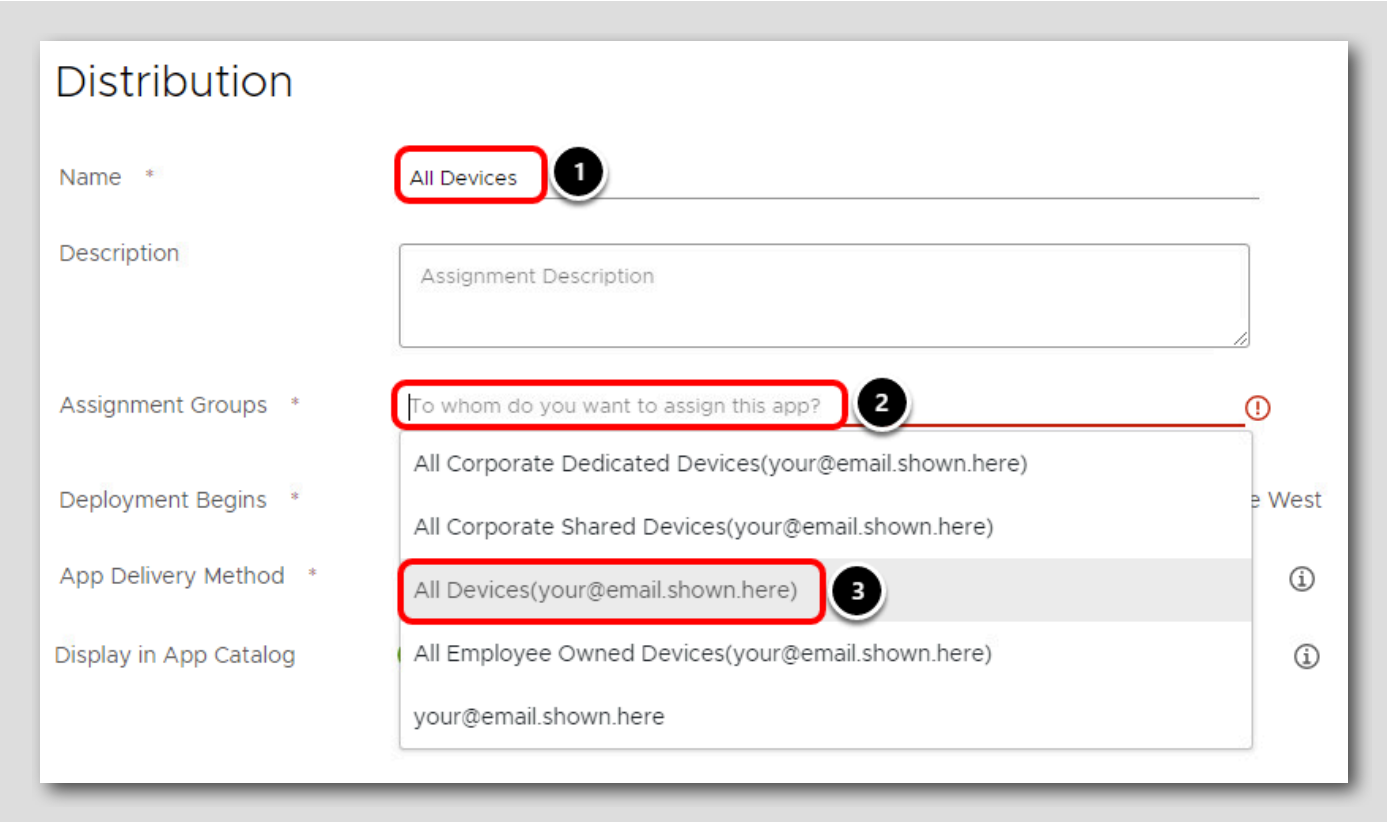
Confirm the Icon and Save

[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

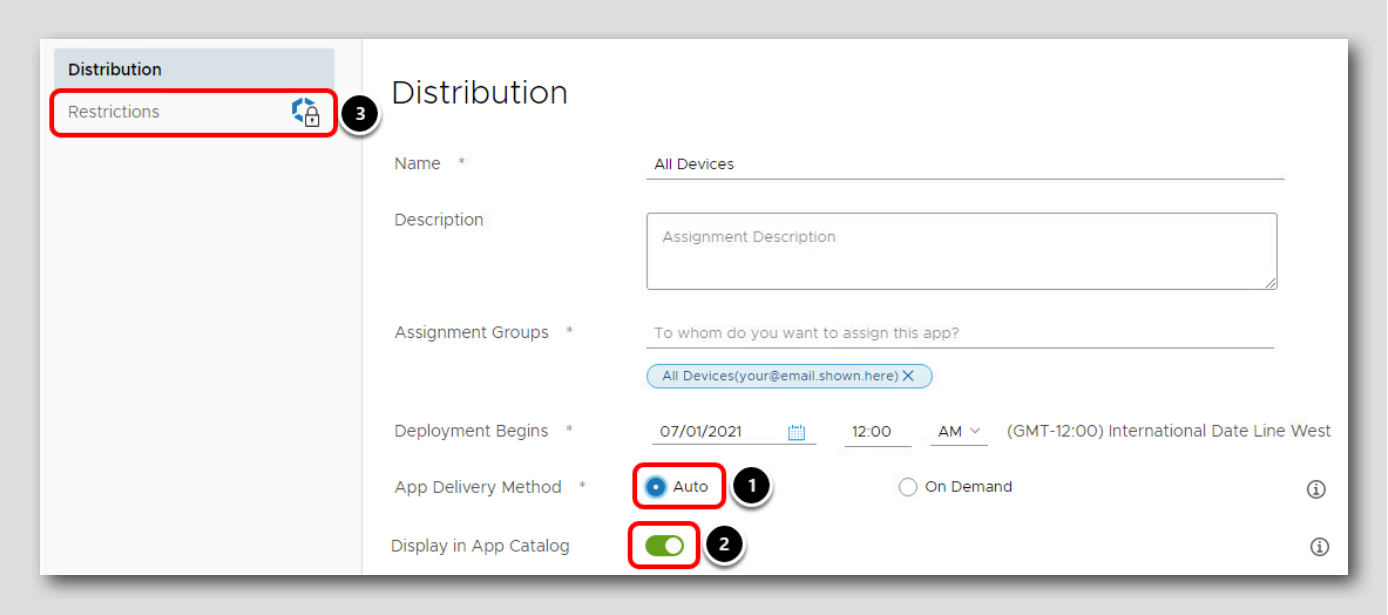


The Application Assignment determines which users and devices will receive the Workspace ONE Assist and how the app will be delivered. You will create an assignment rule that will publish the application automatically (installs the app without requiring user input) to all devices in your organization.

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.

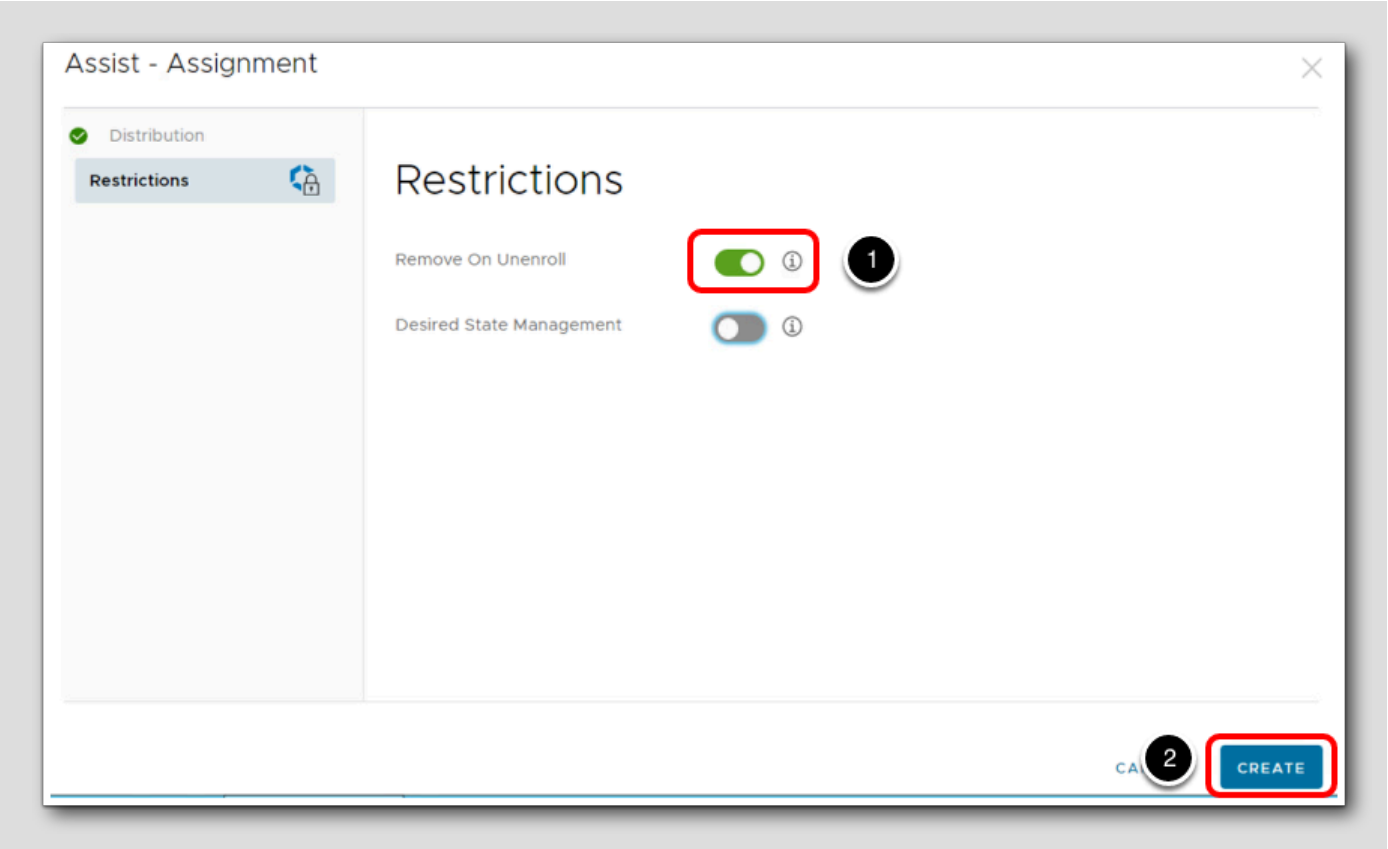
2. Keep the Display in App Catalog option as **Enabled**.

   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]

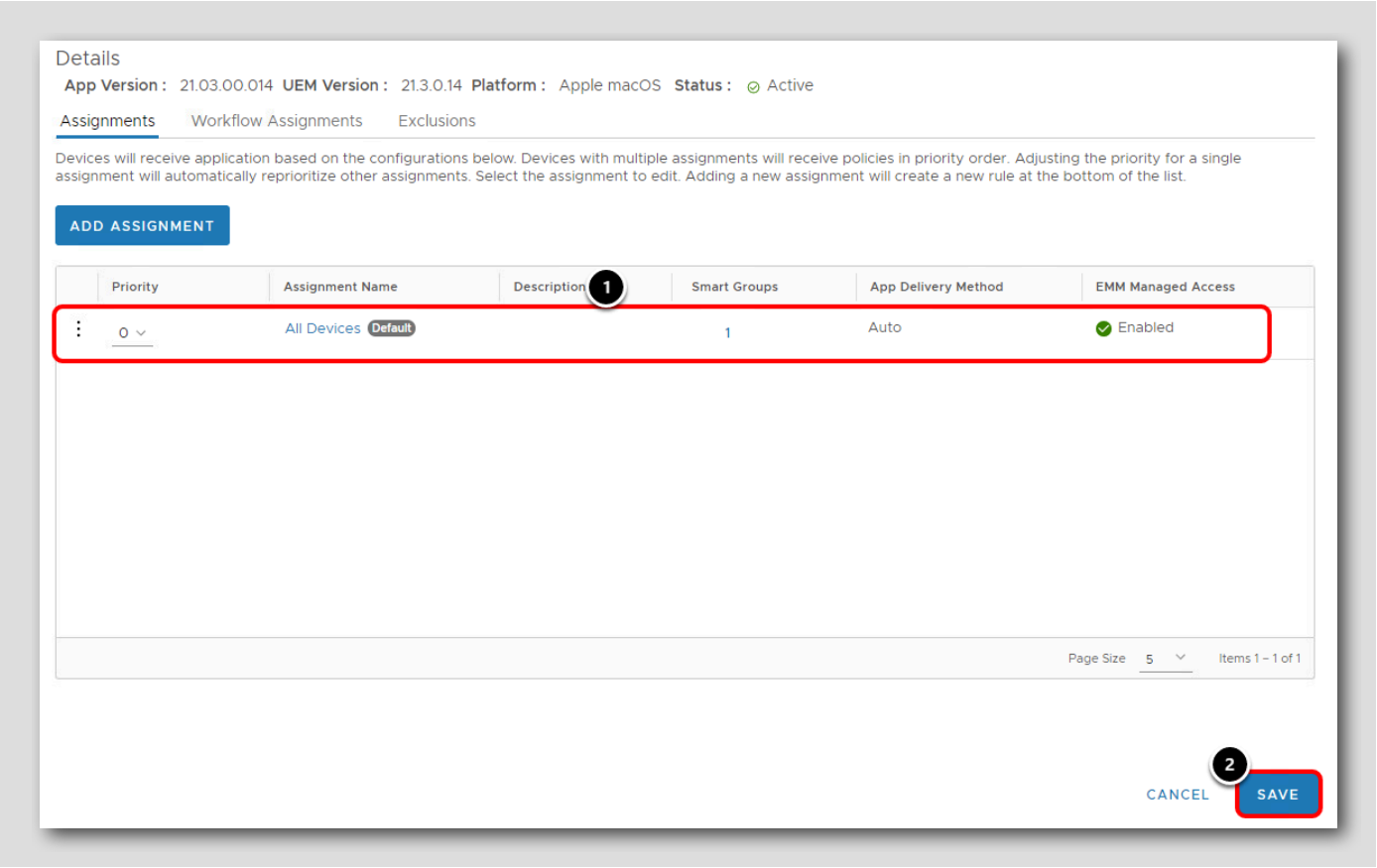


Restrictions can be applied to the assignment to change the behavior of the application.

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

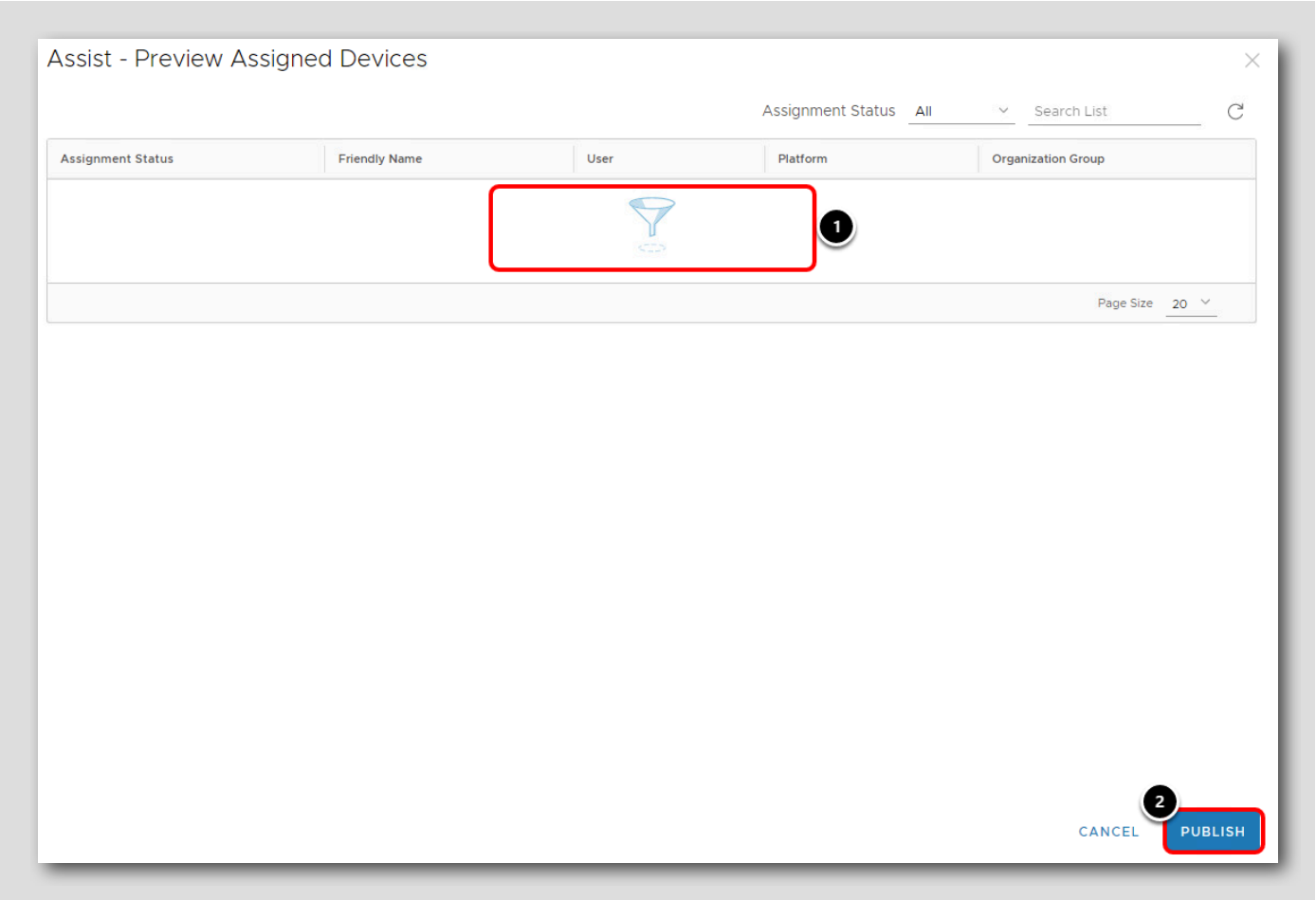
[291]



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

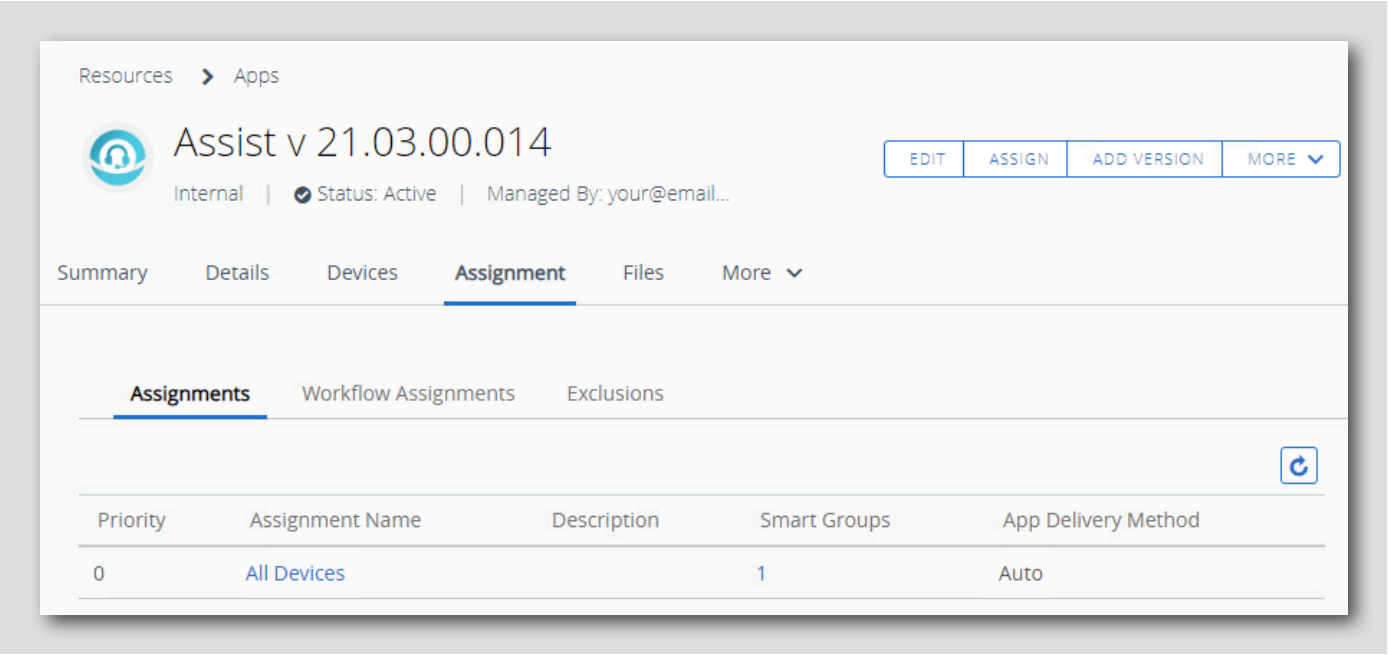
[292]



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

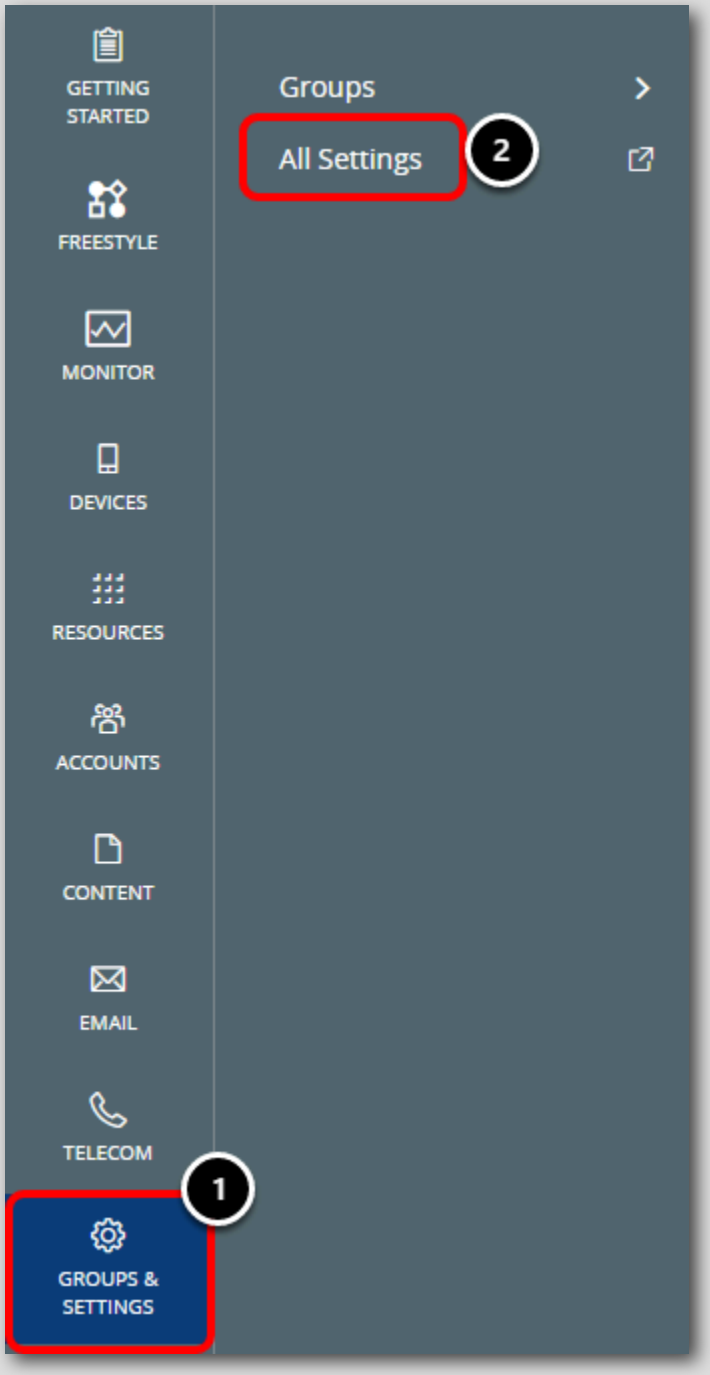
[294]

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

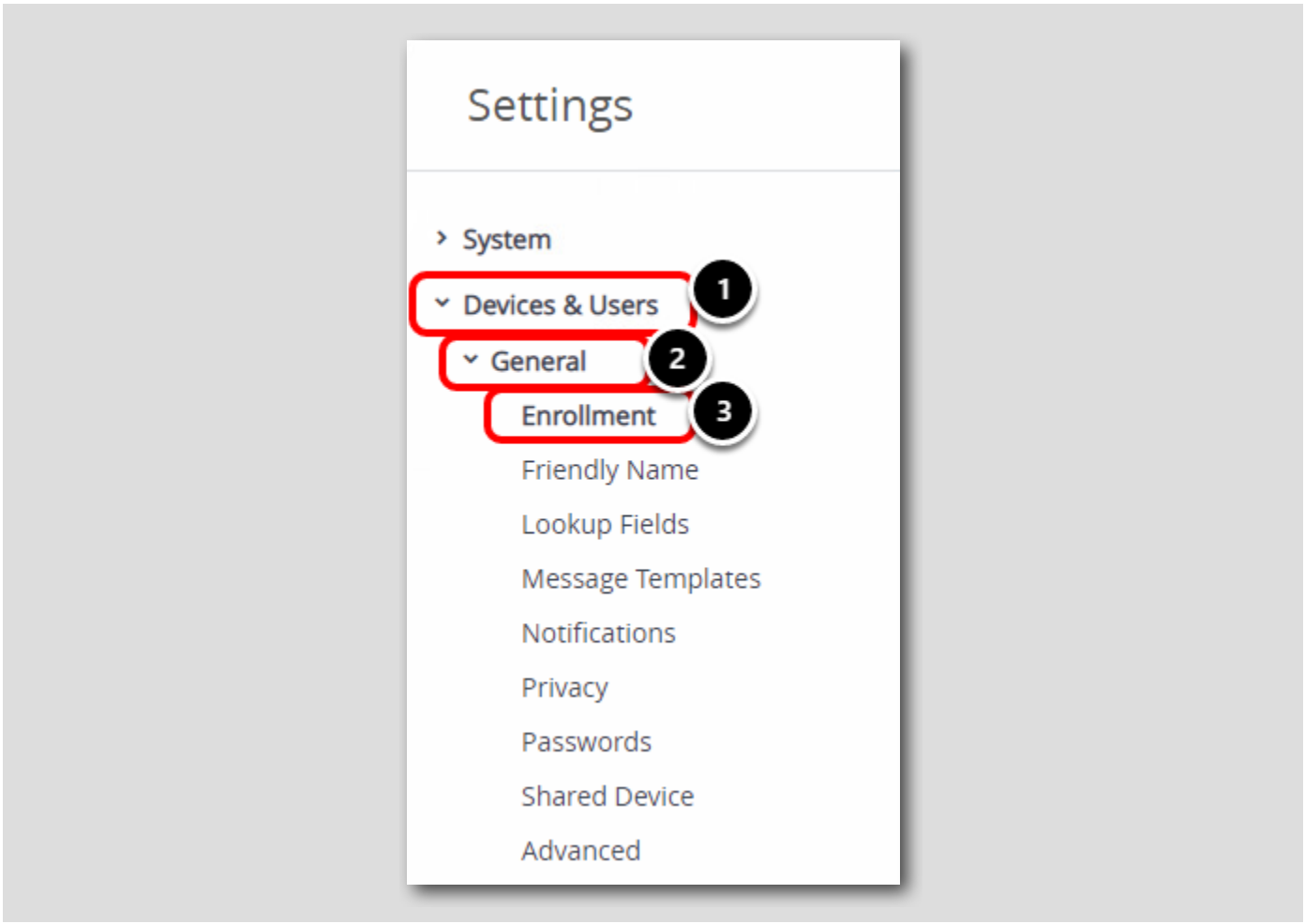
[295]



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

Navigate to Enrollment Settings

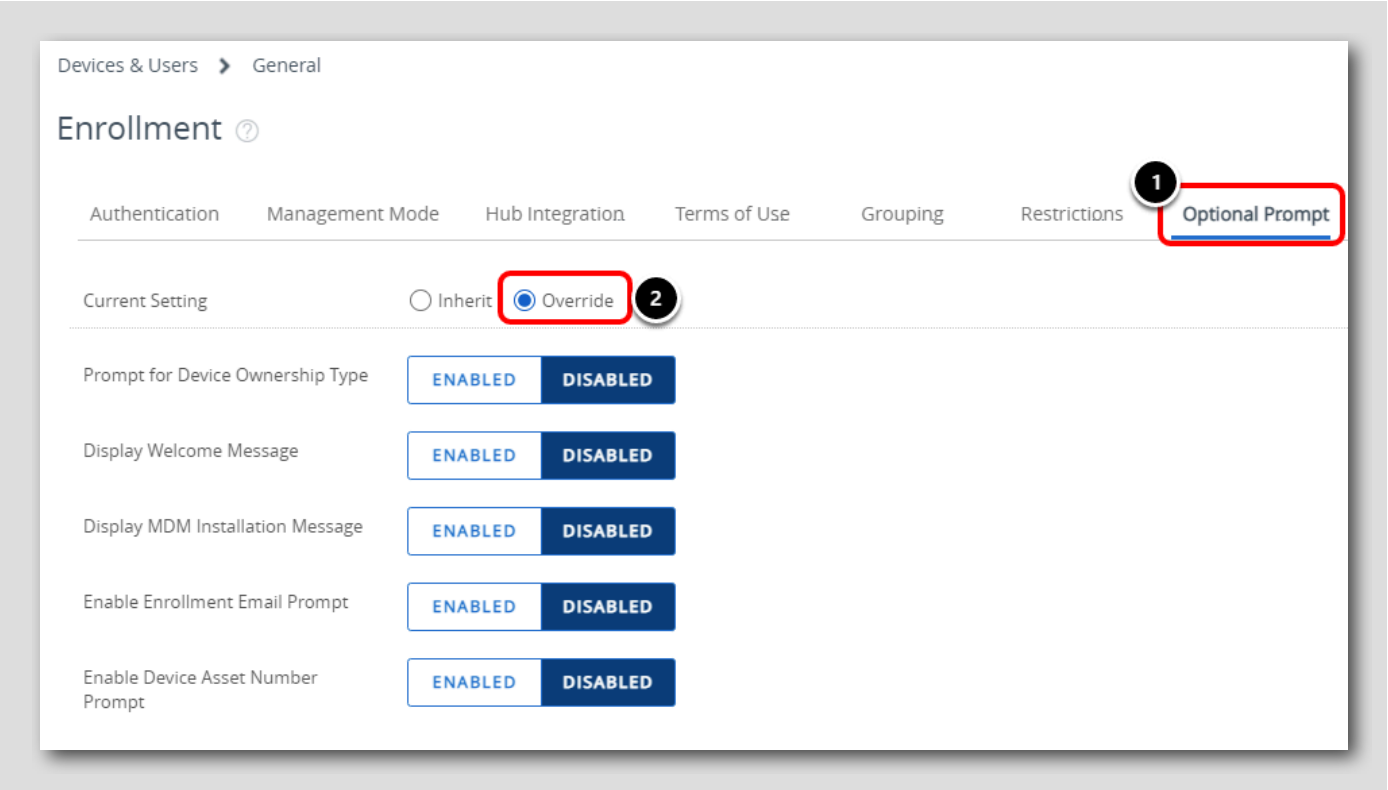
[296]



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

Configure Optional Prompt

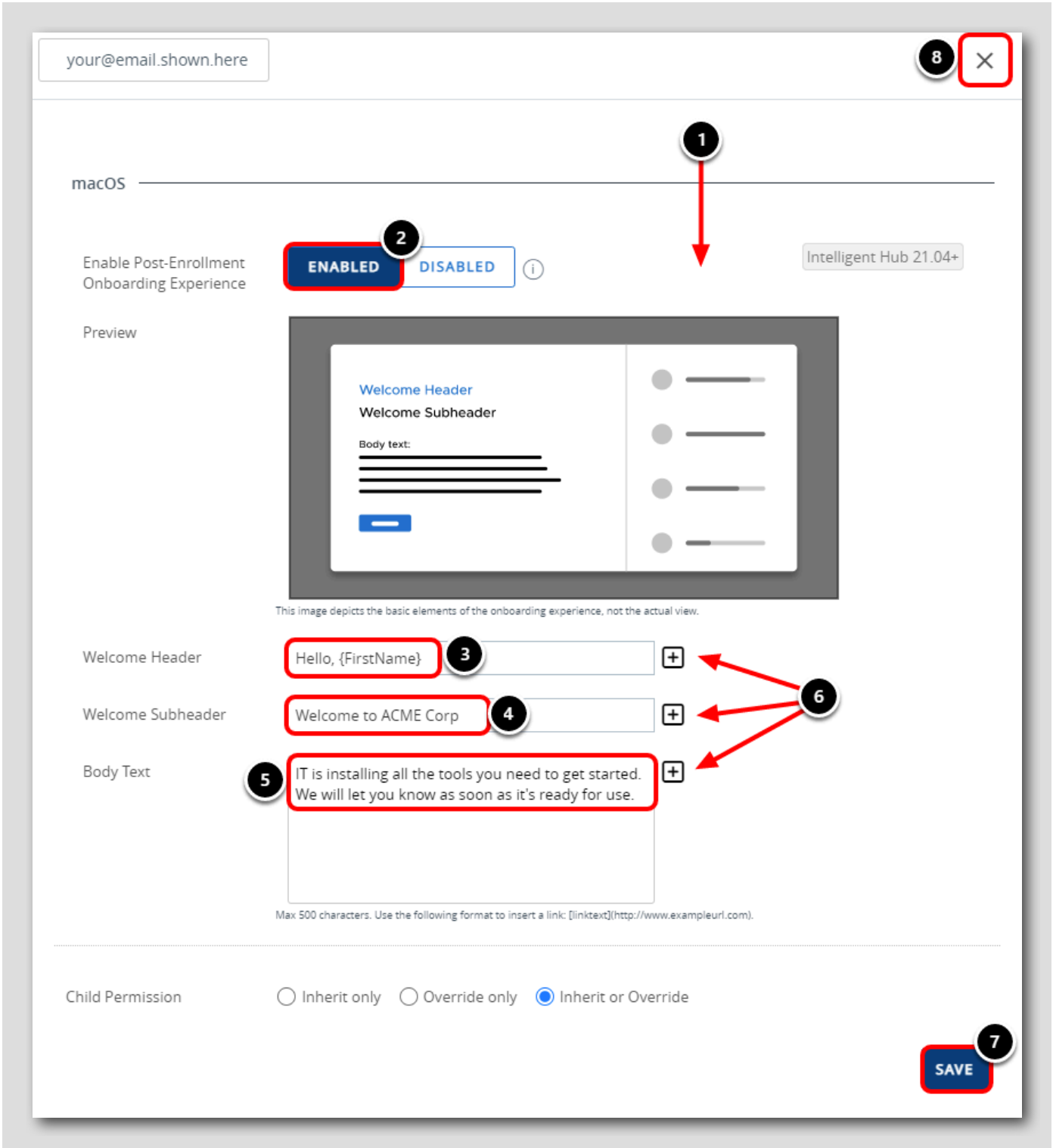
[297]



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]

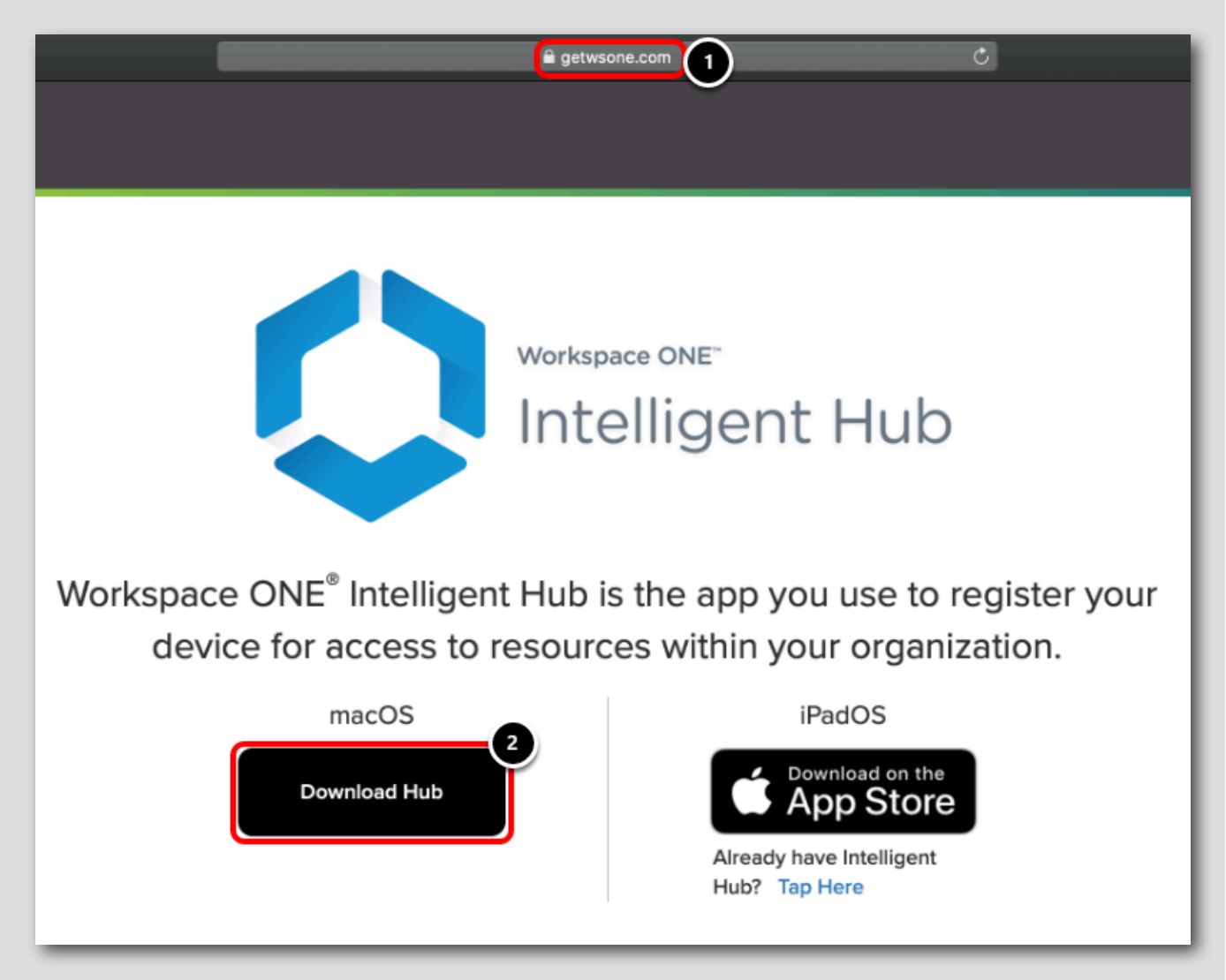
NOTE: These steps require a macOS device. If you do not have a macOS device, you can follow these steps in the manual to see the end result.

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.

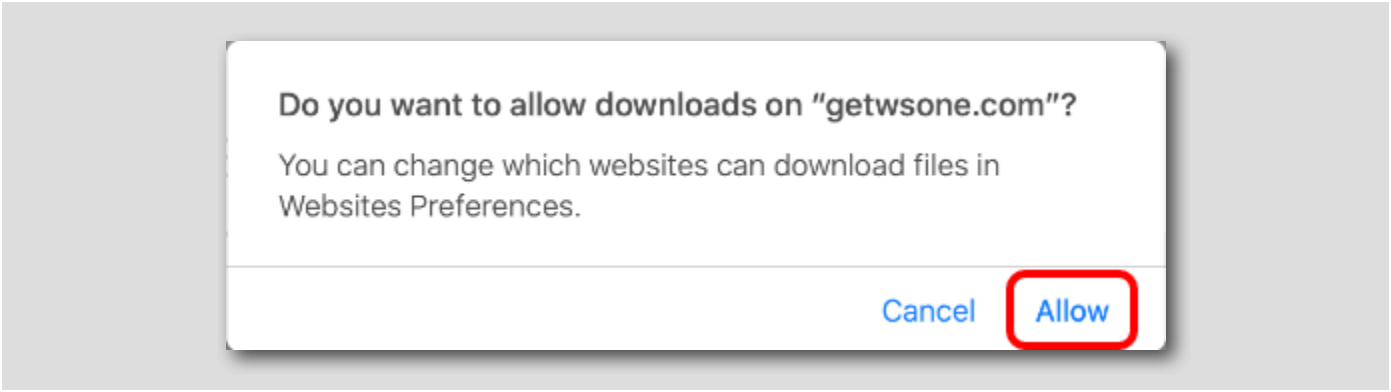


Open Safari or your preferred web browser.

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]

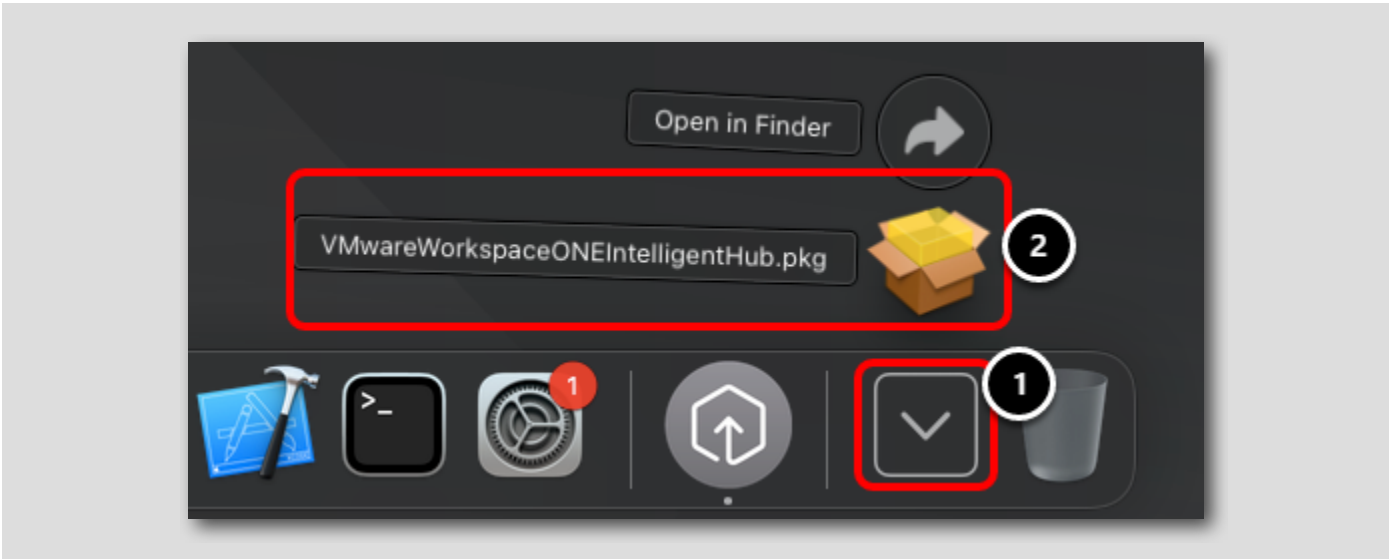
NOTE: These steps require a macOS device. If you do not have a macOS device, you can follow these steps in the manual to see the end result.



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.

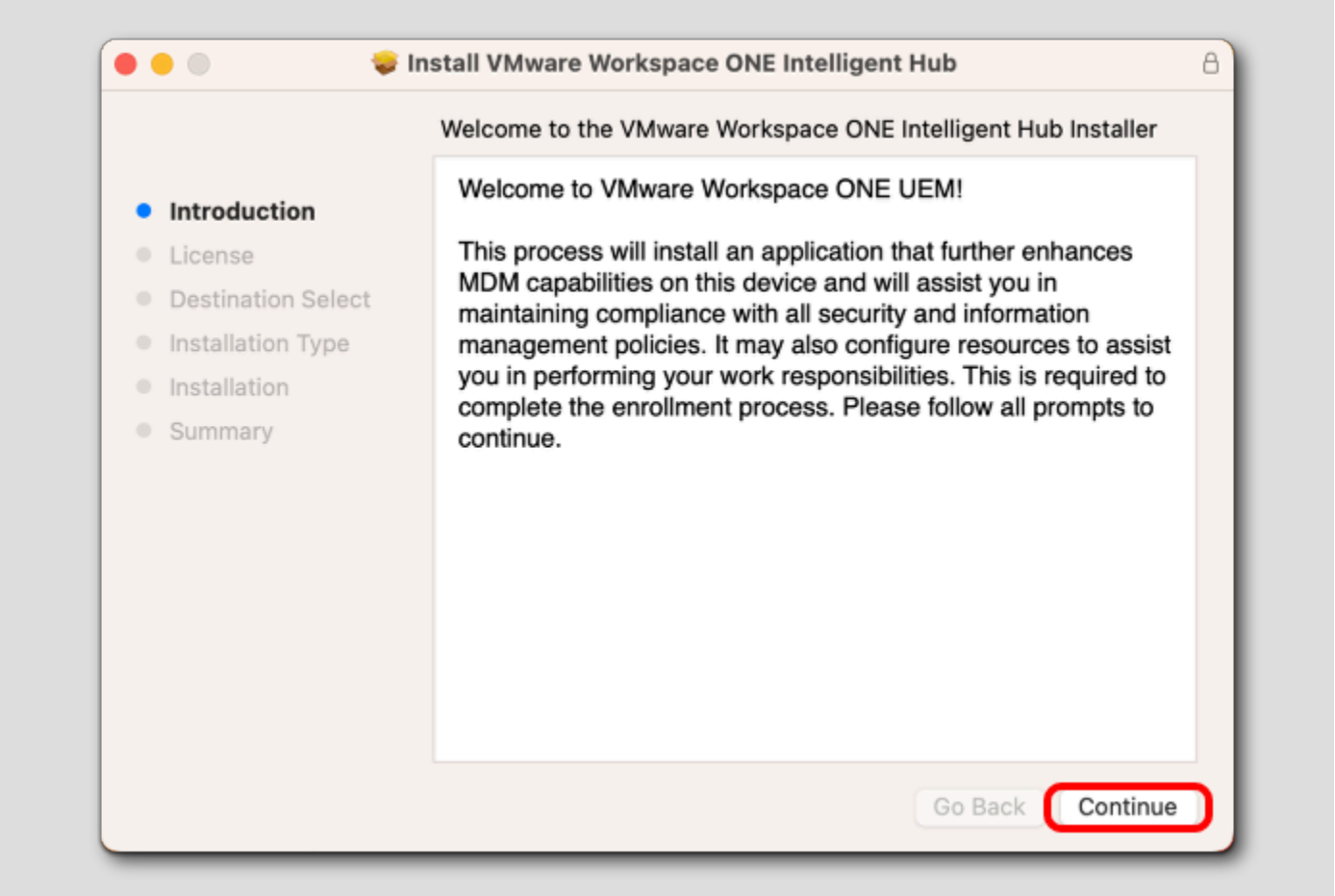


1. Click the **Downloads** folder in the dock (next to the Trash Bin).
2. Click the **VMwareWorkspaceONEIntelligentHub.pkg** file to begin the installer.

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.

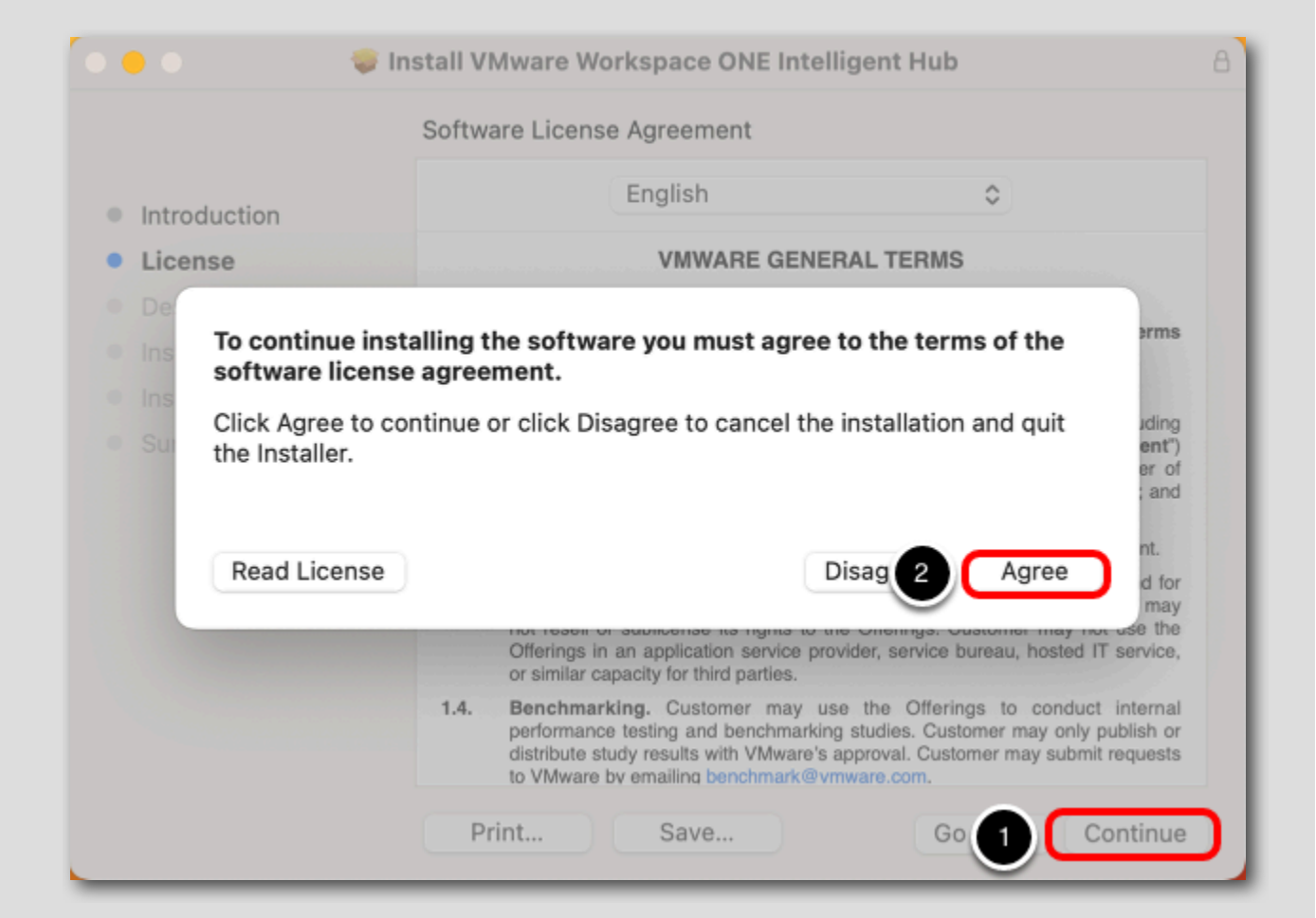


Click **Continue**.

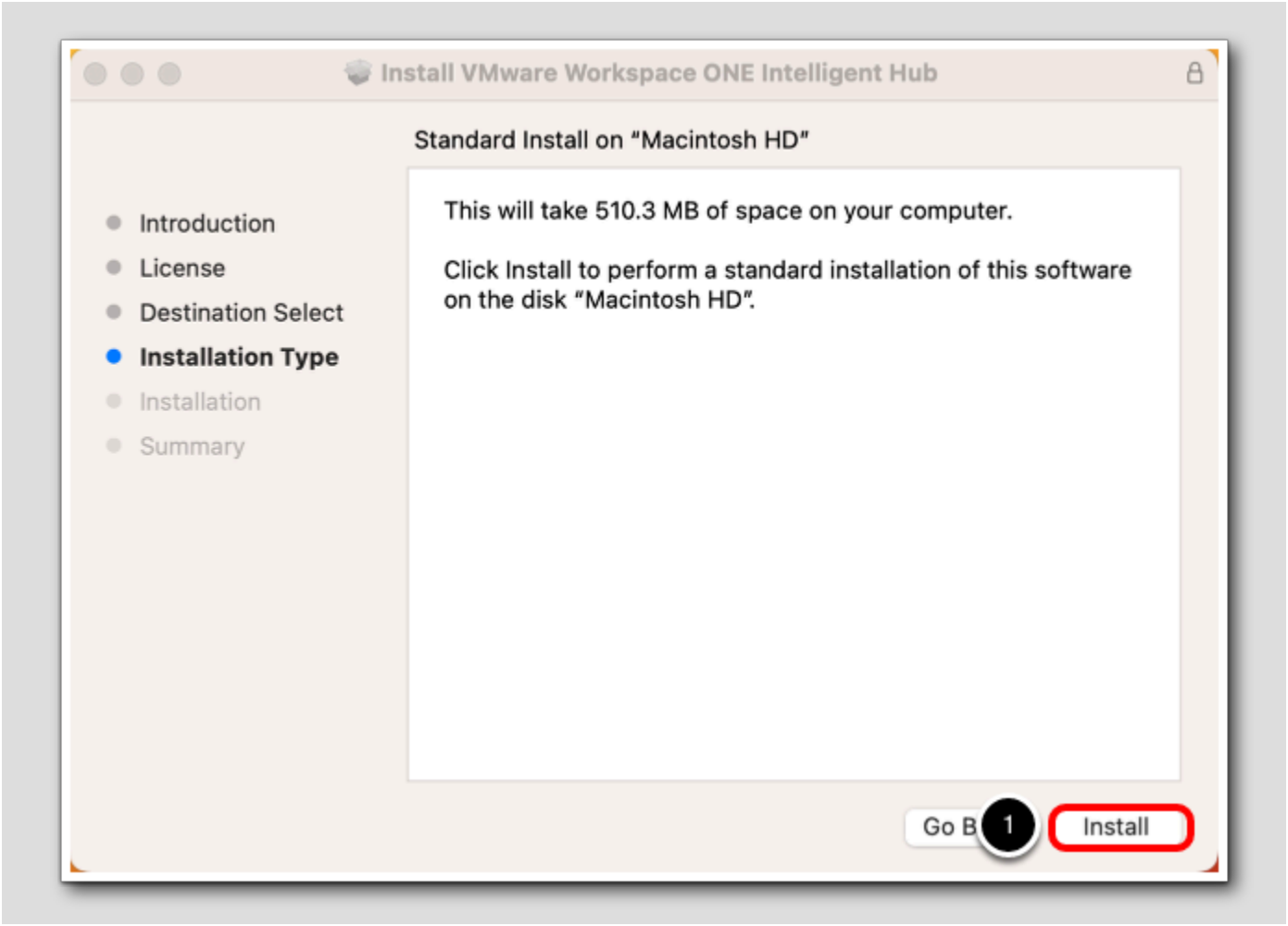
Continue and Agree to Terms

[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).

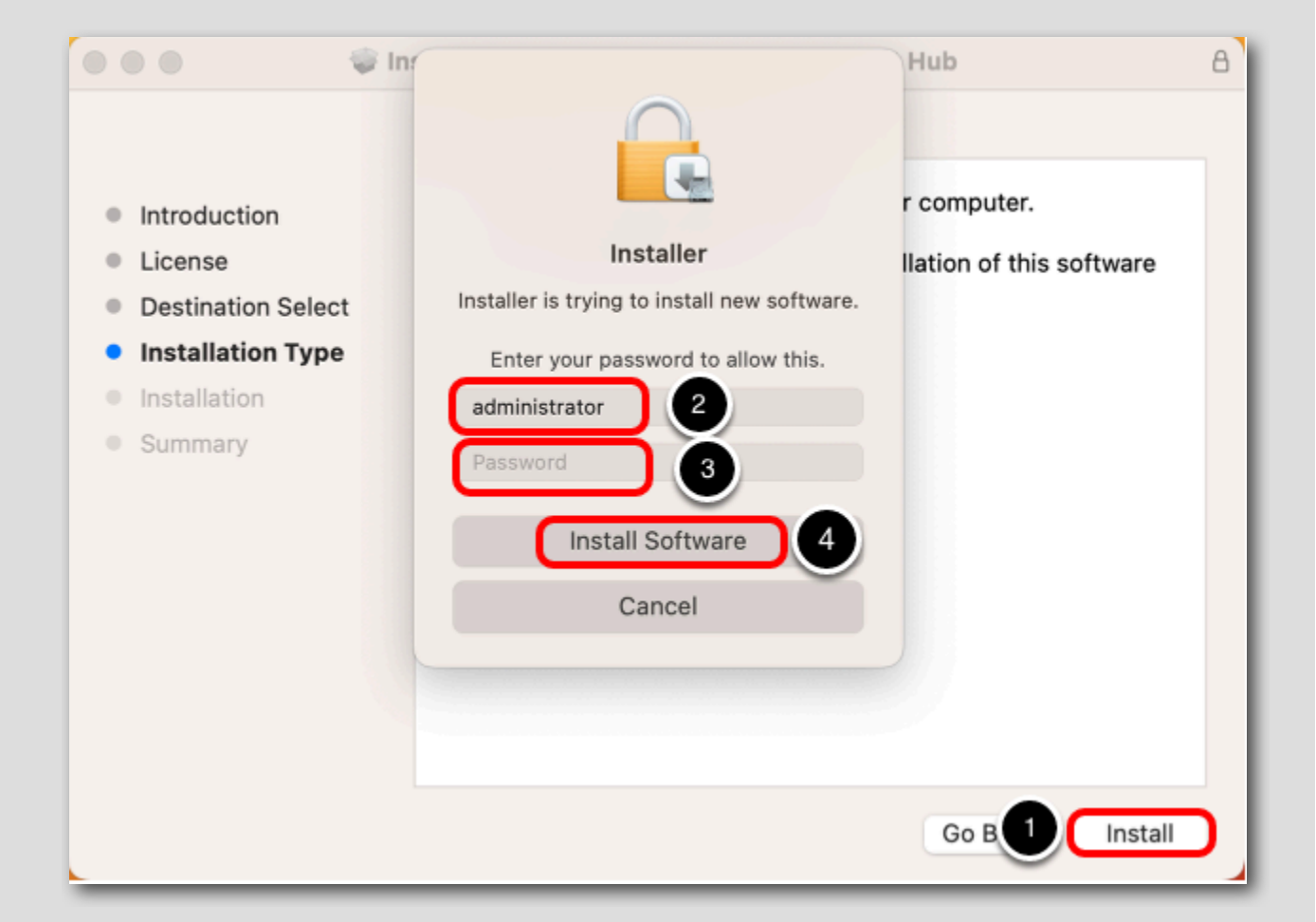


1. On the Standard Install page, click **Install**.

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.



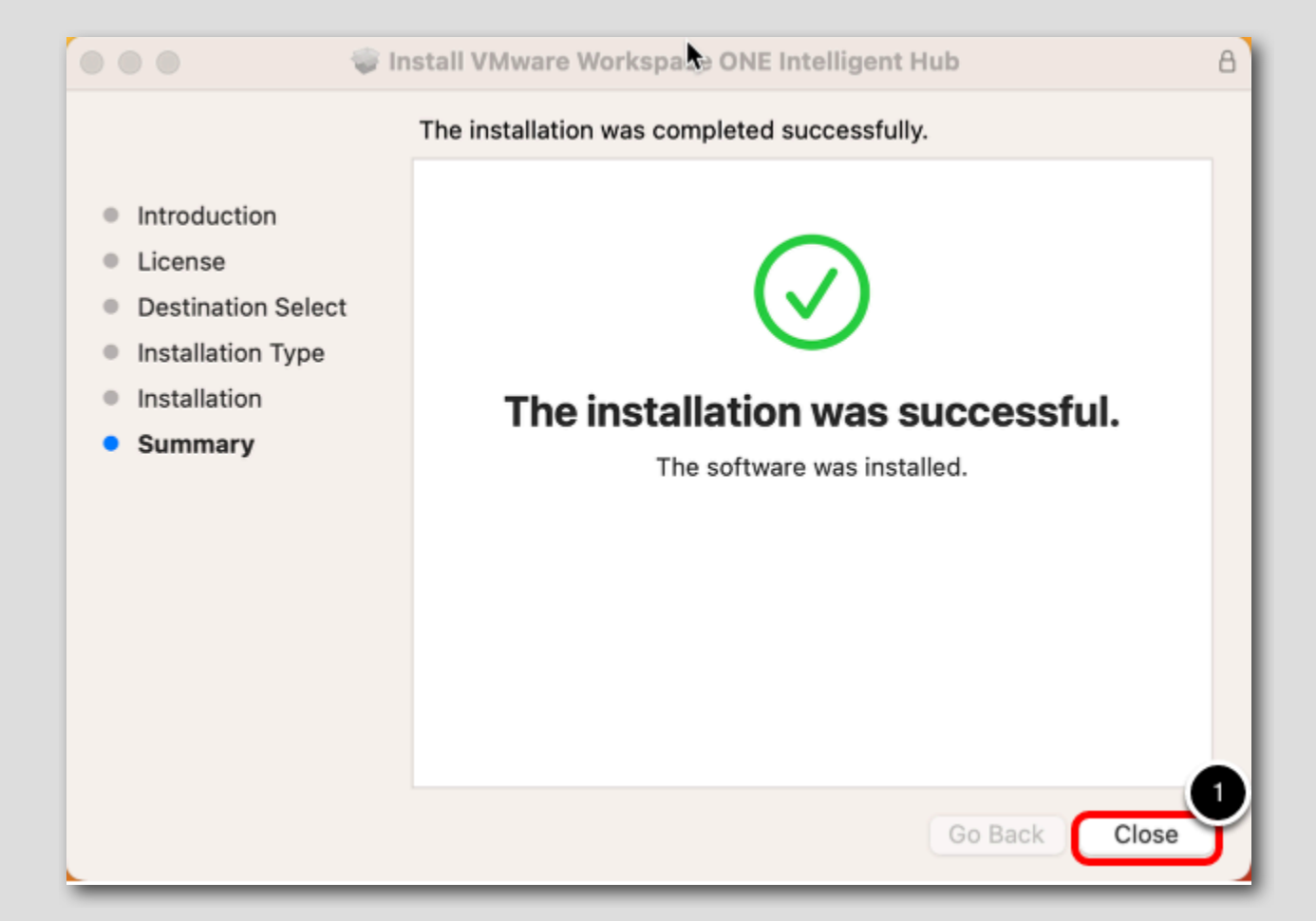
1. Click **Install**. You are now prompted to enter the computers administrator credentials.
2. Enter the username for the device.
3. Enter the password for the device.
4. Click the **Install Software** button.

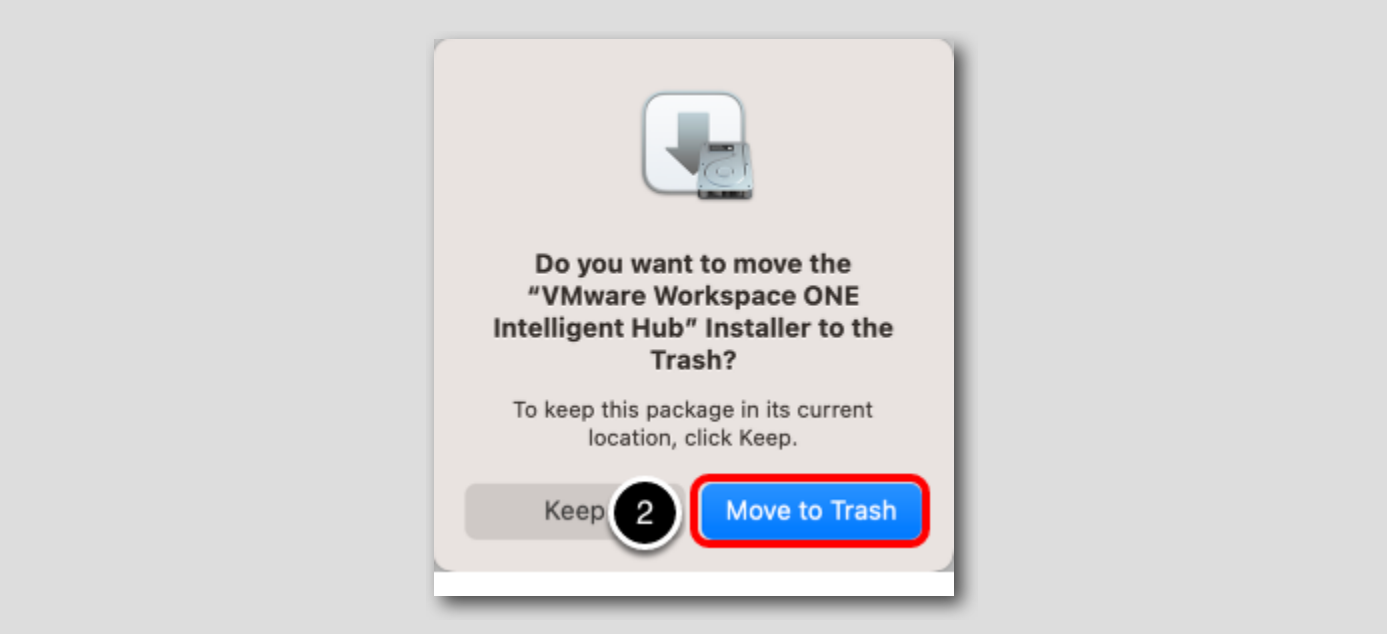
NOTE: The install may take a few minutes, please be patient while the install completes.

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

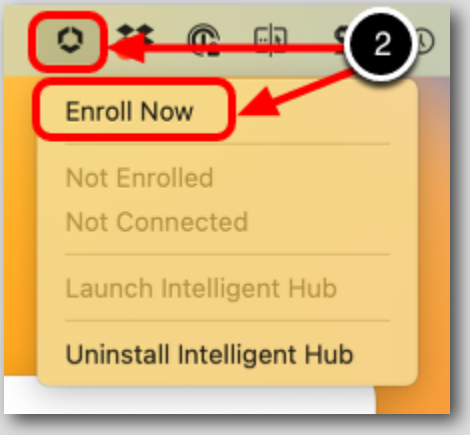
[308]

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

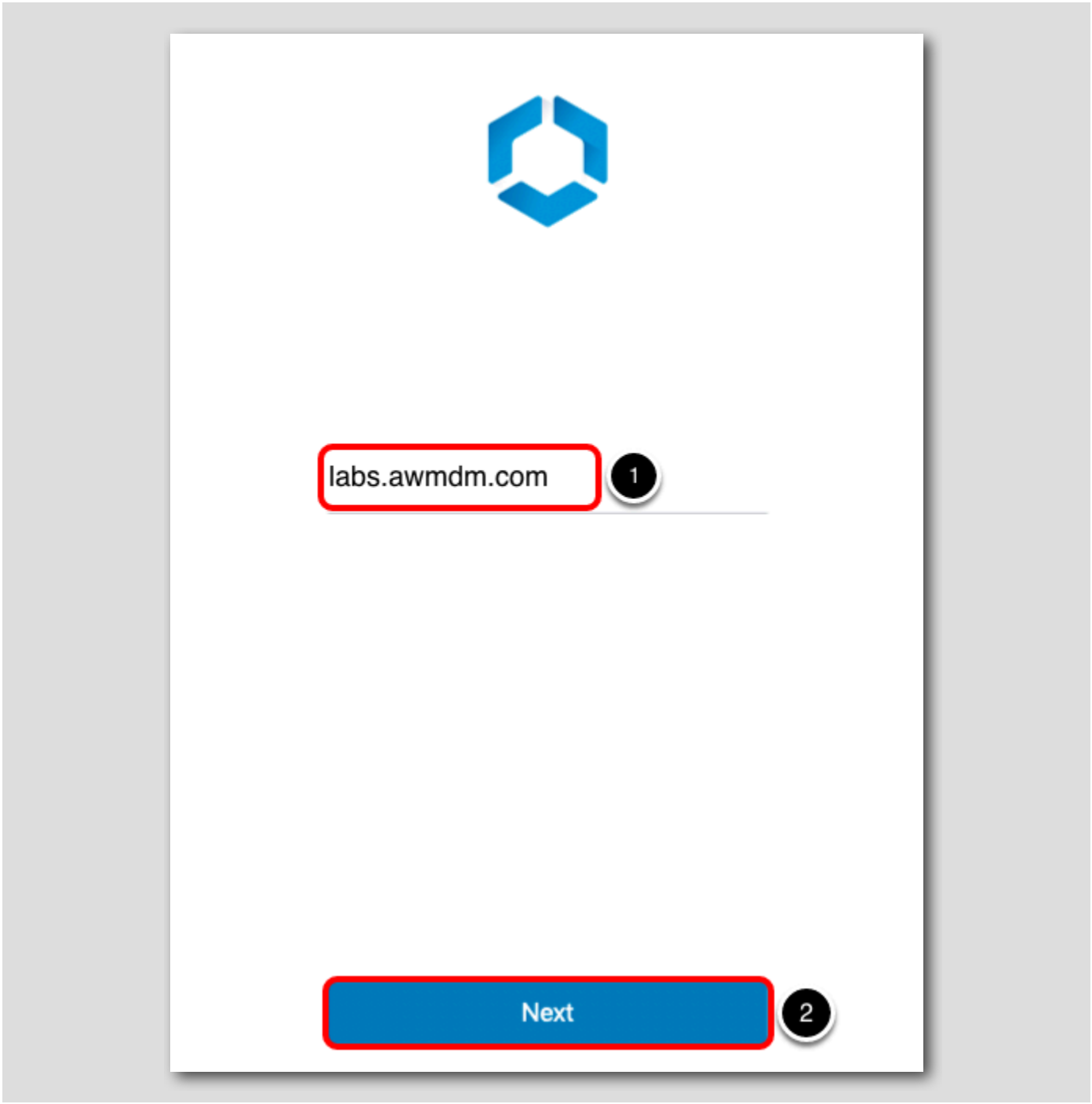
[309]



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]

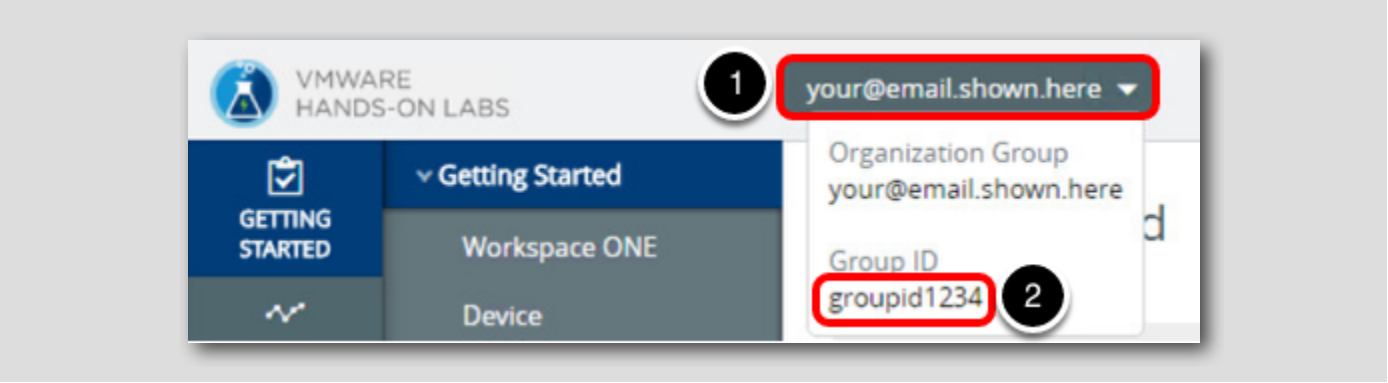


1. Enter **`labs.awmdm.com`** in the Email or Server Address field
2. Click **Next**

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]



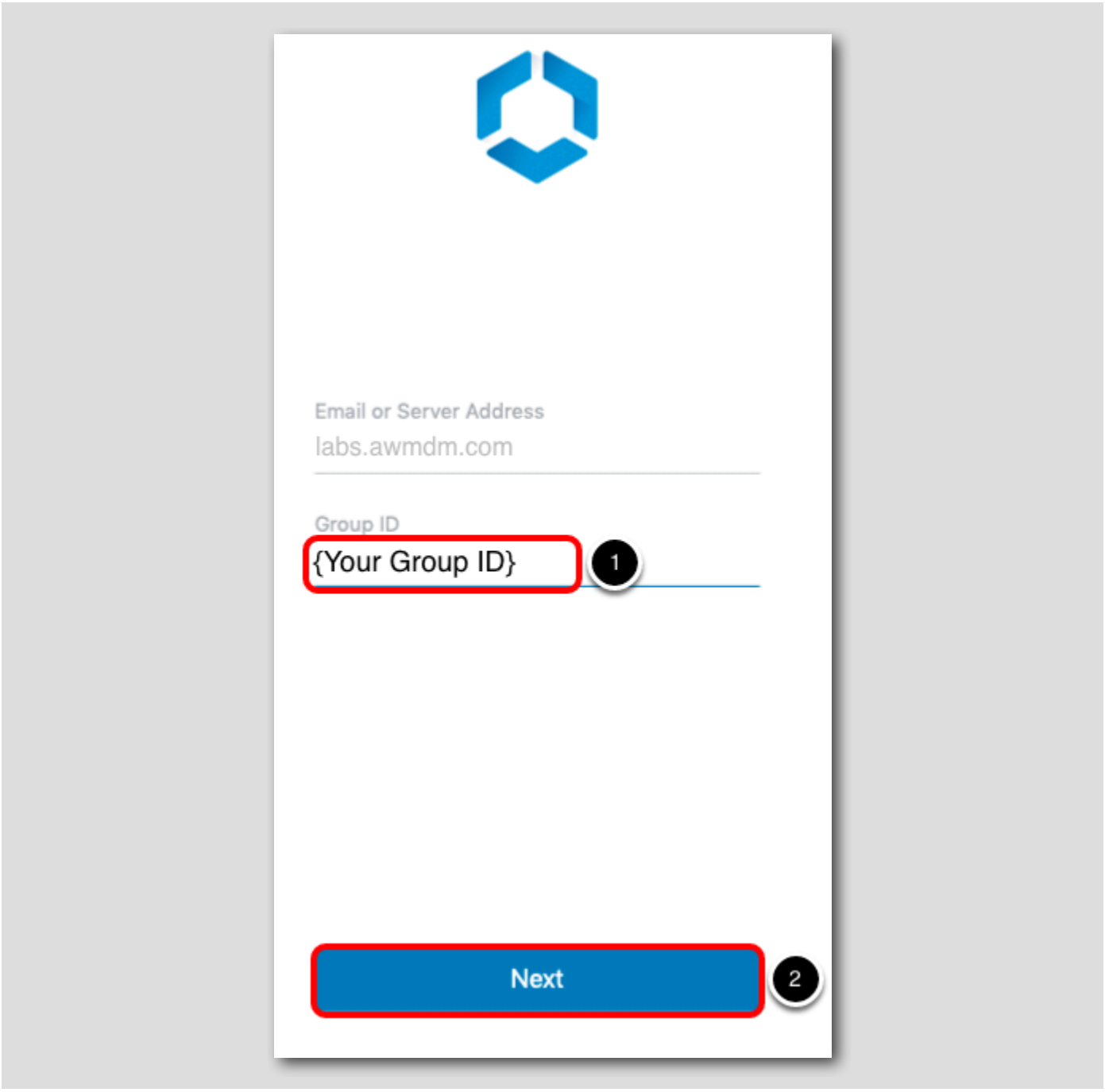
Return to the Workspace ONE UEM Console,

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

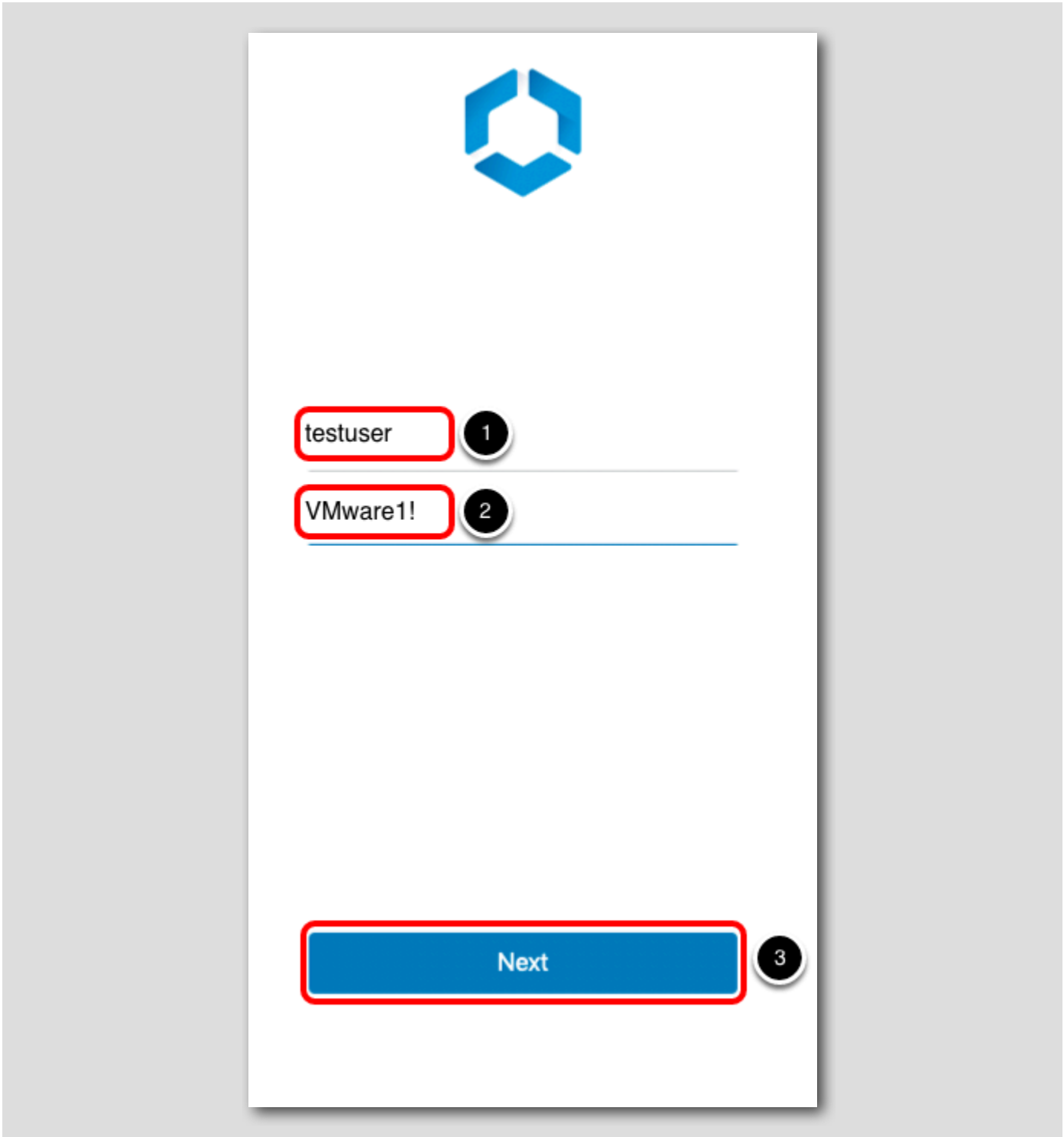
[312]



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

Enter Enrollment Credentials

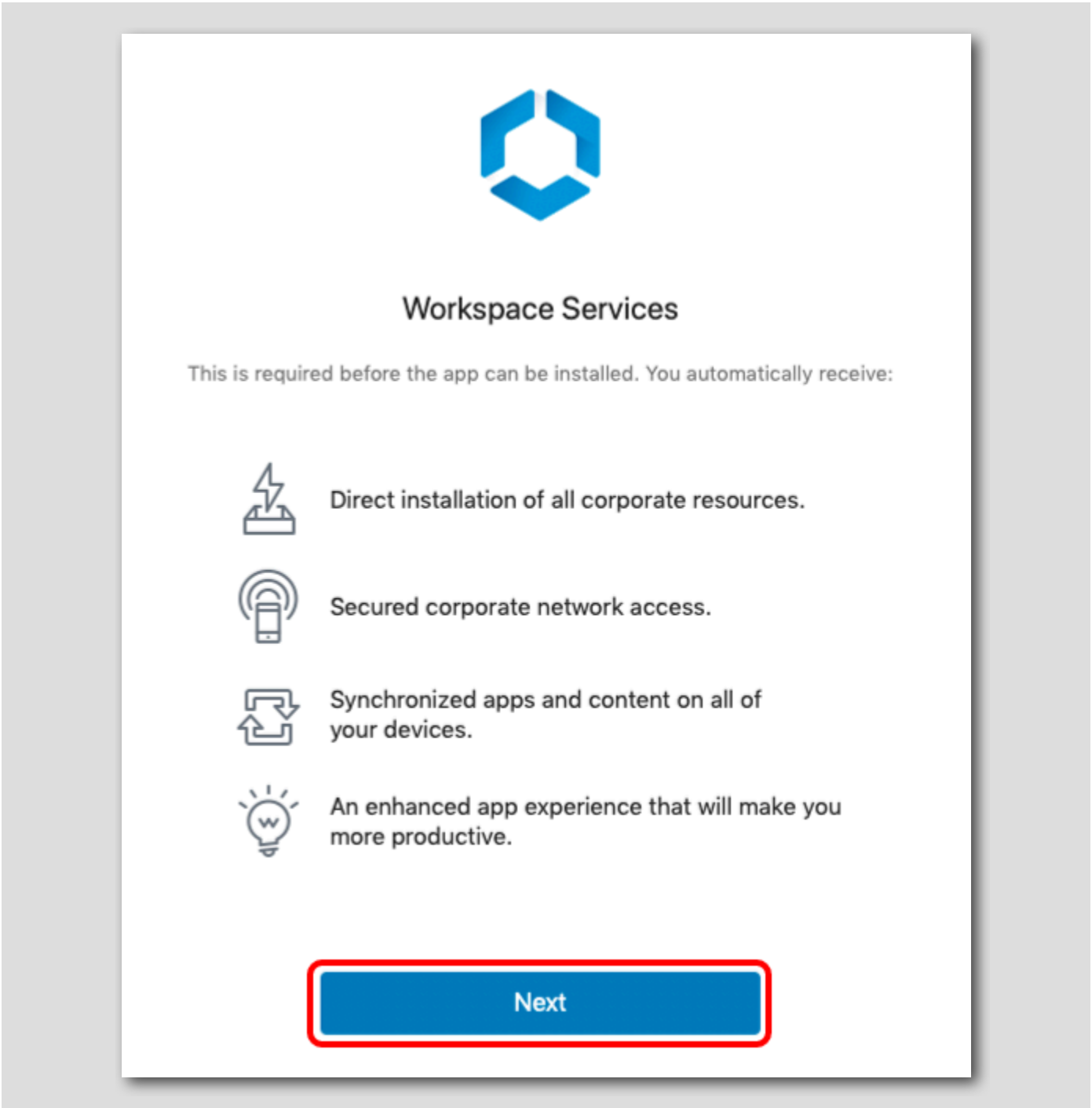
[313]



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

Enable Device Management

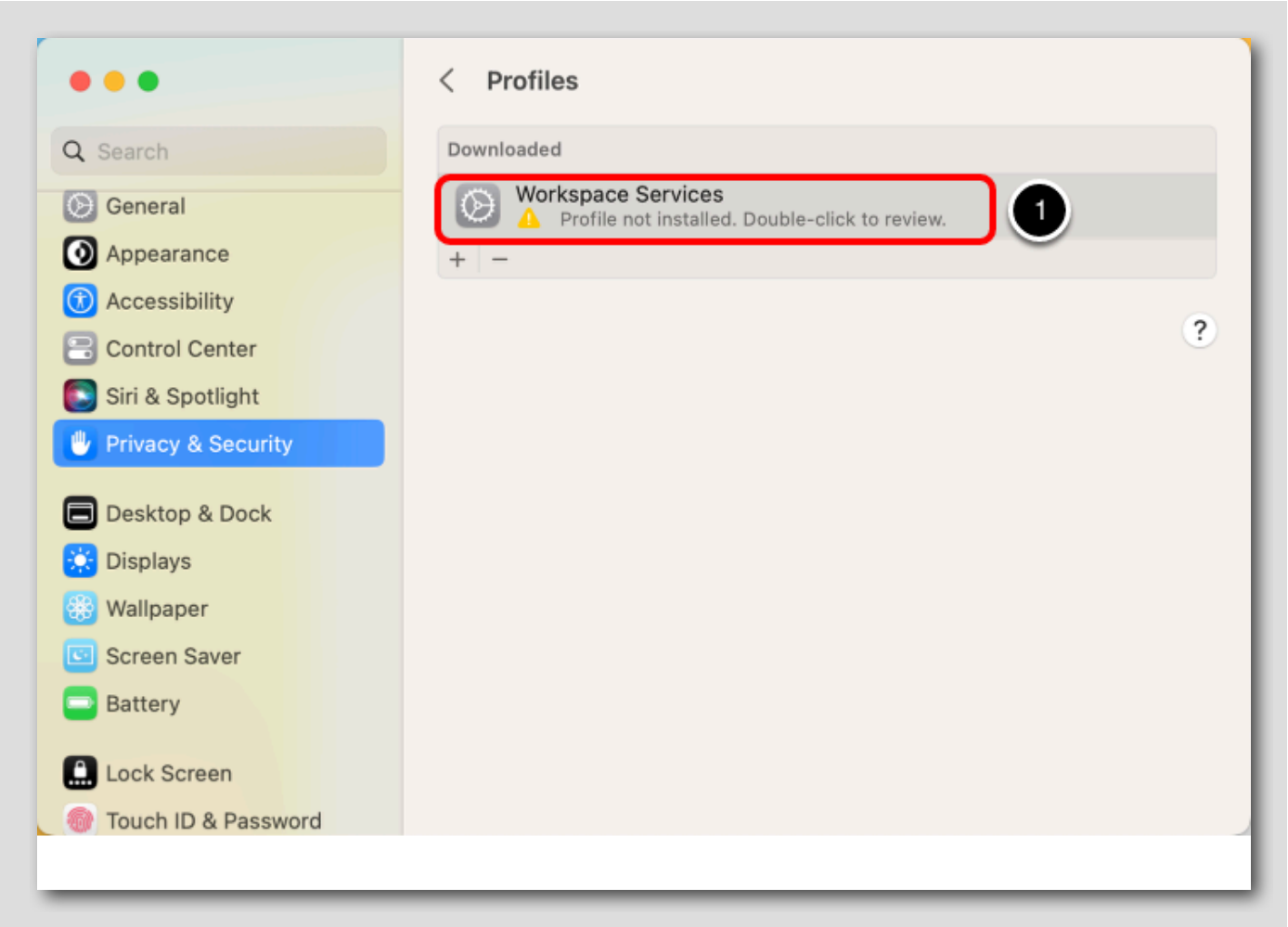
[314]

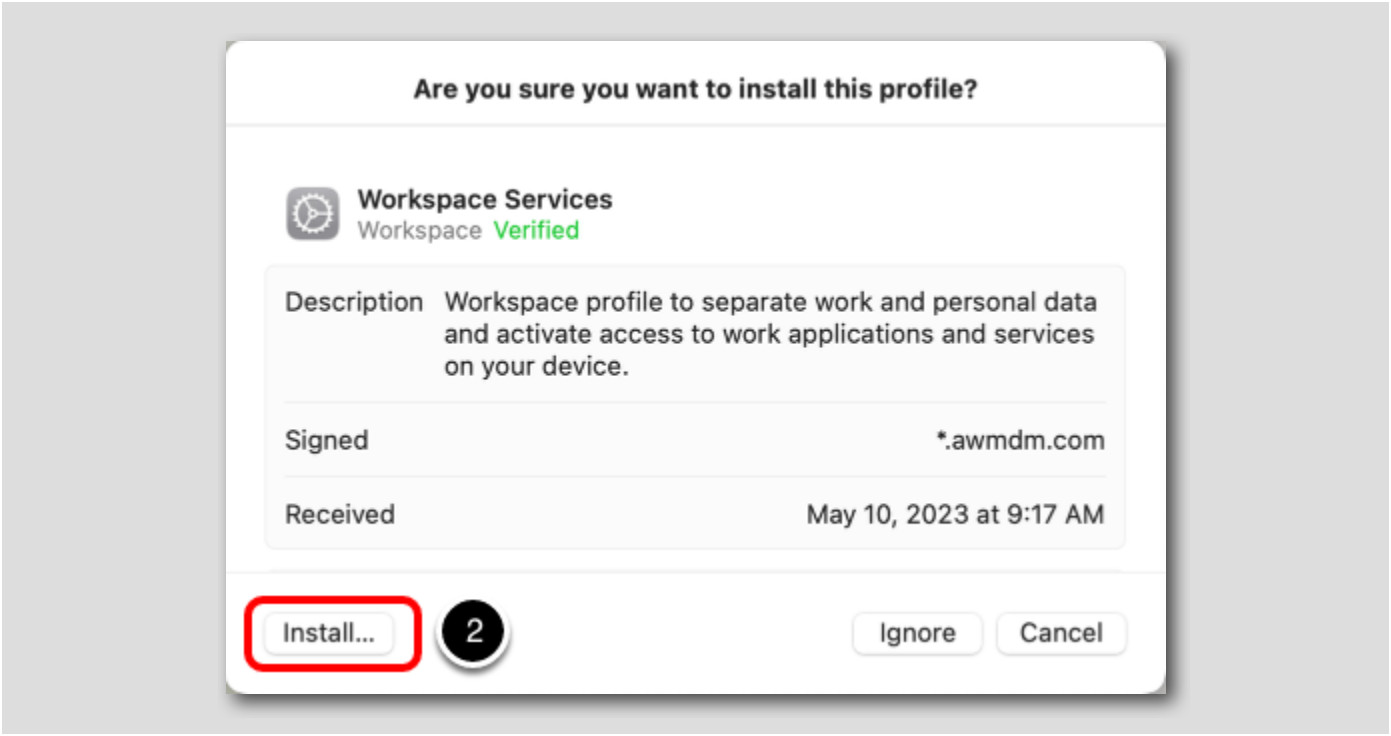


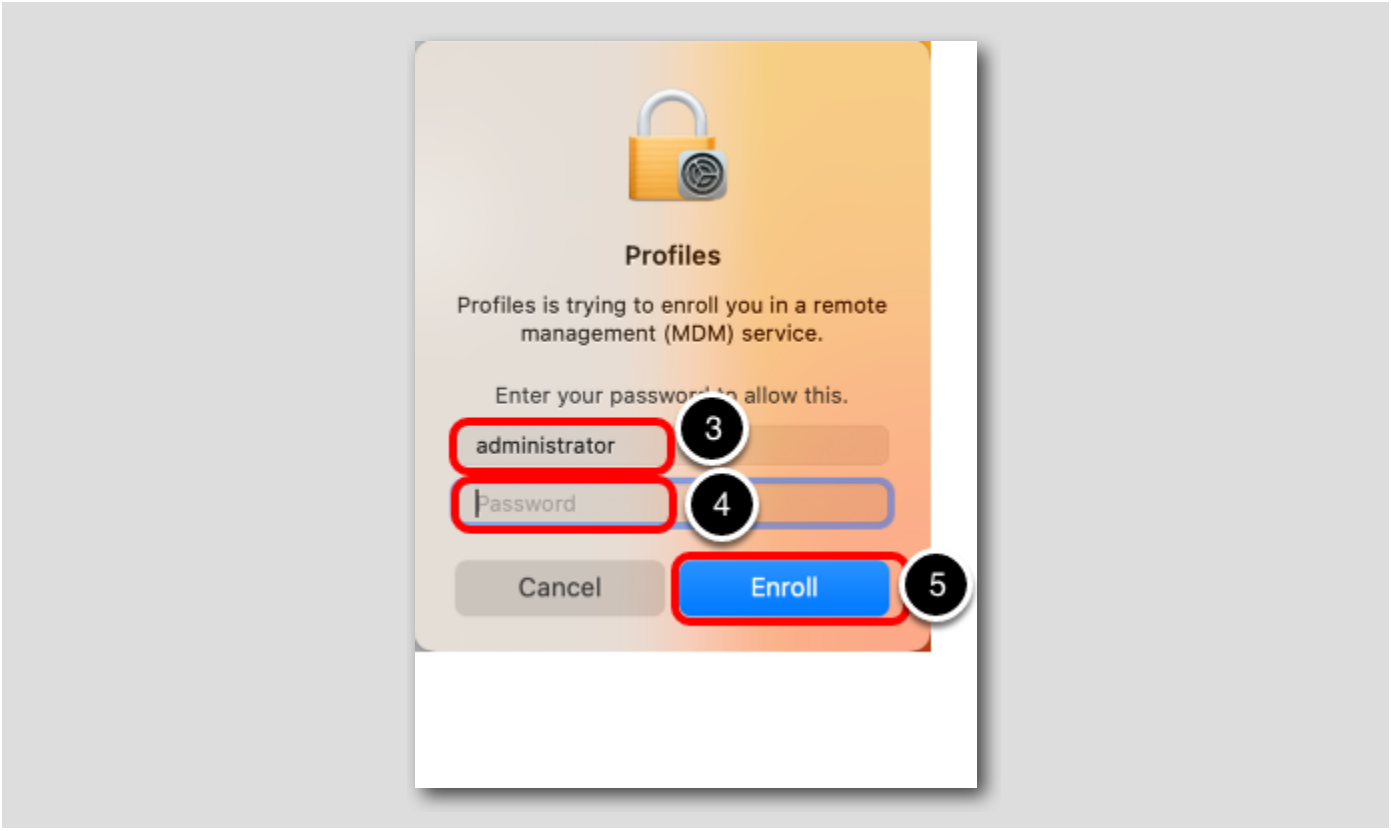
Click **Next** to enable device management.

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

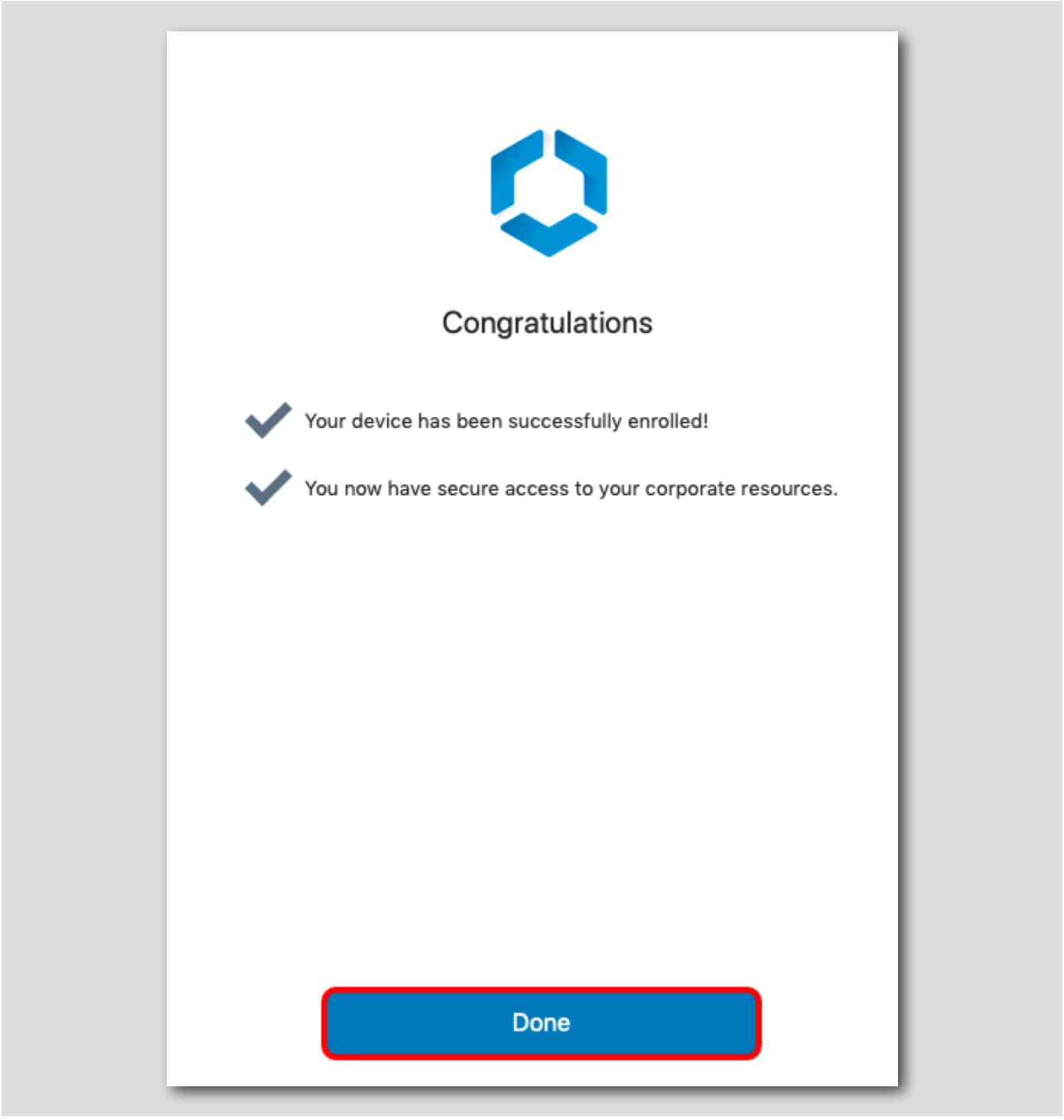


After a few seconds, the Profiles System Preferences page will be displayed and prompt you to install the Workspace Services profile, which enrolls the device into mobile device management (MDM) with Workspace ONE UEM.

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

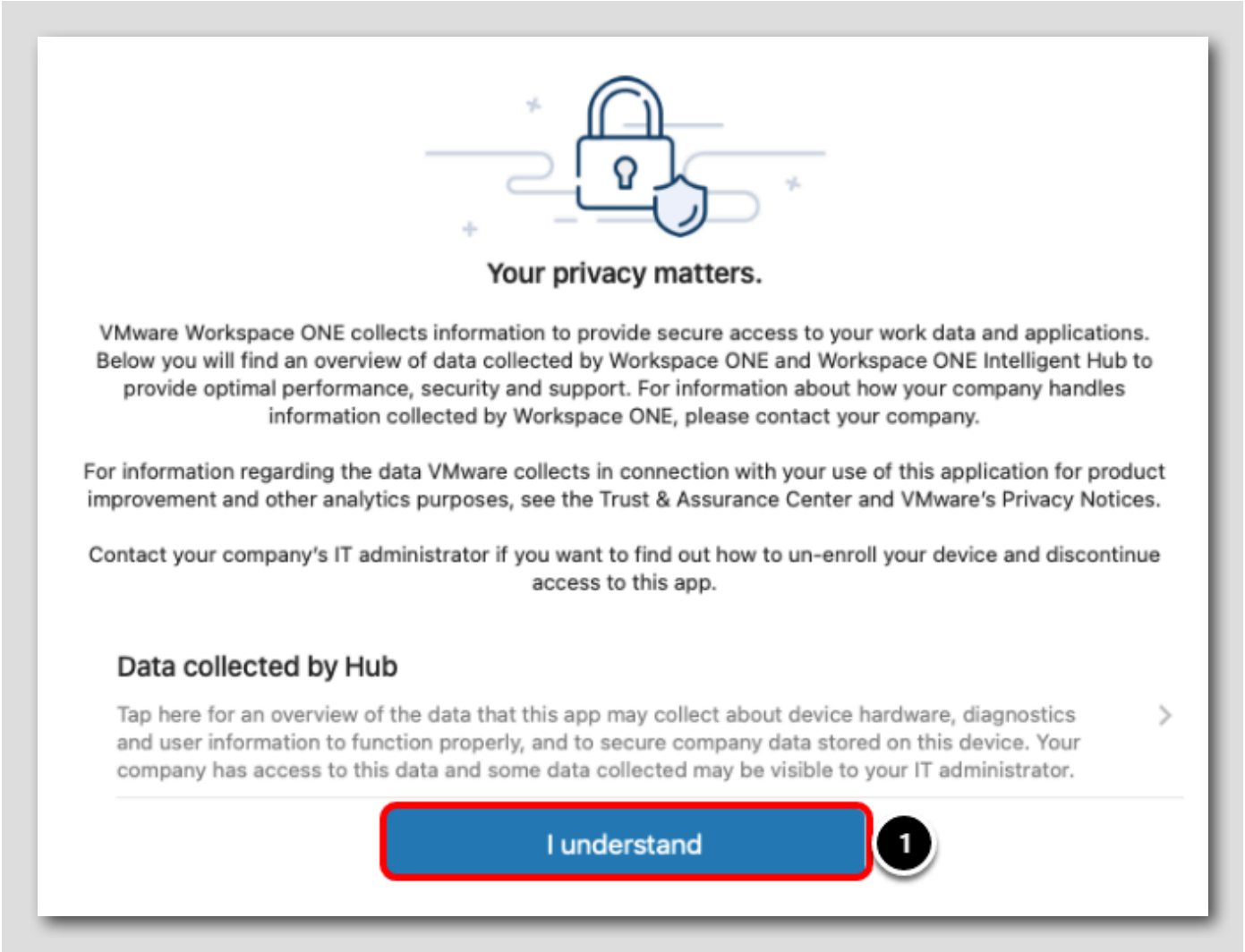
[316]

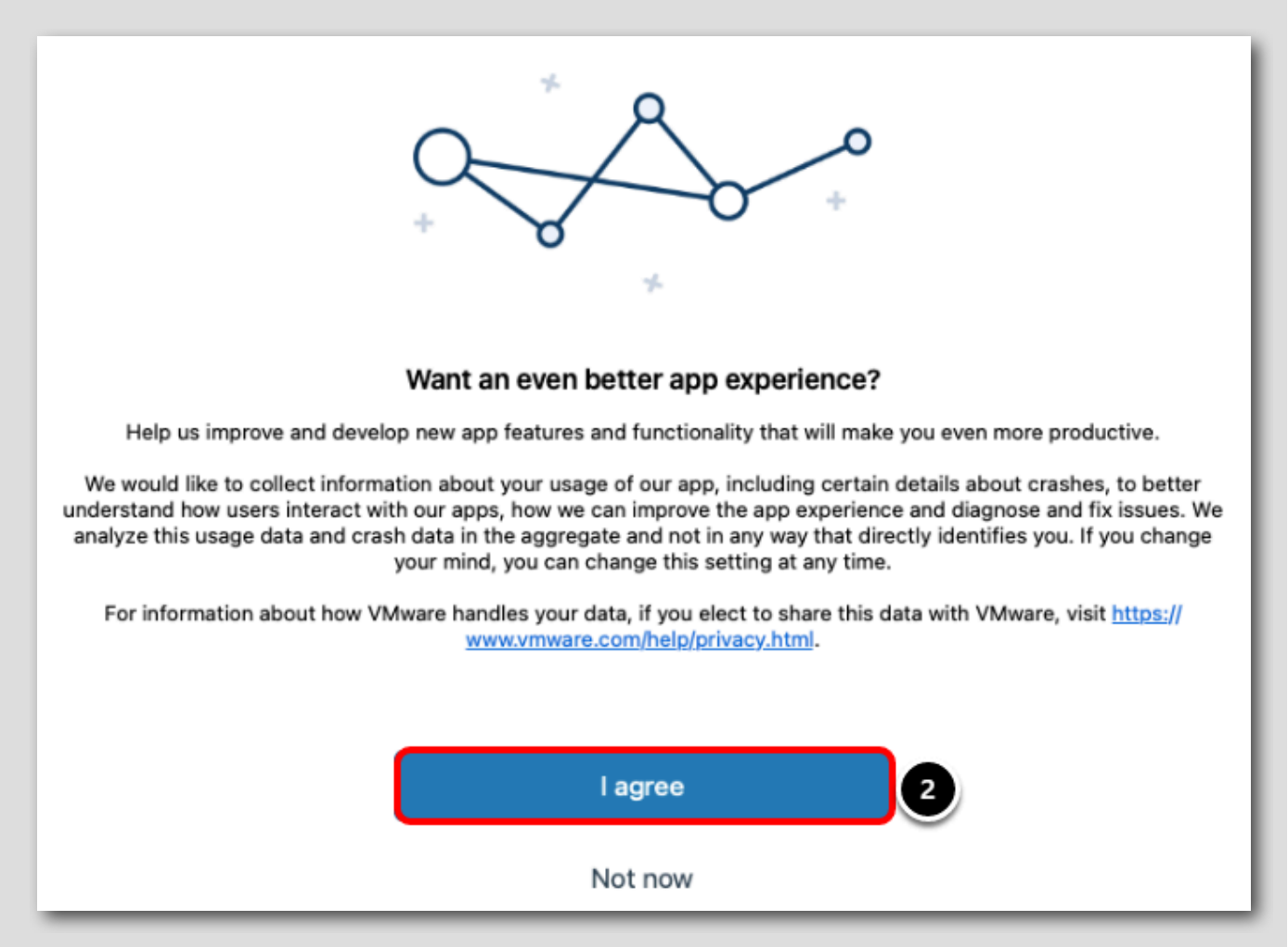


Return to the Workspace ONE Intelligent Hub app and click **Done** when the installation completes.

Accept Privacy and Data Sharing Prompts

[317]





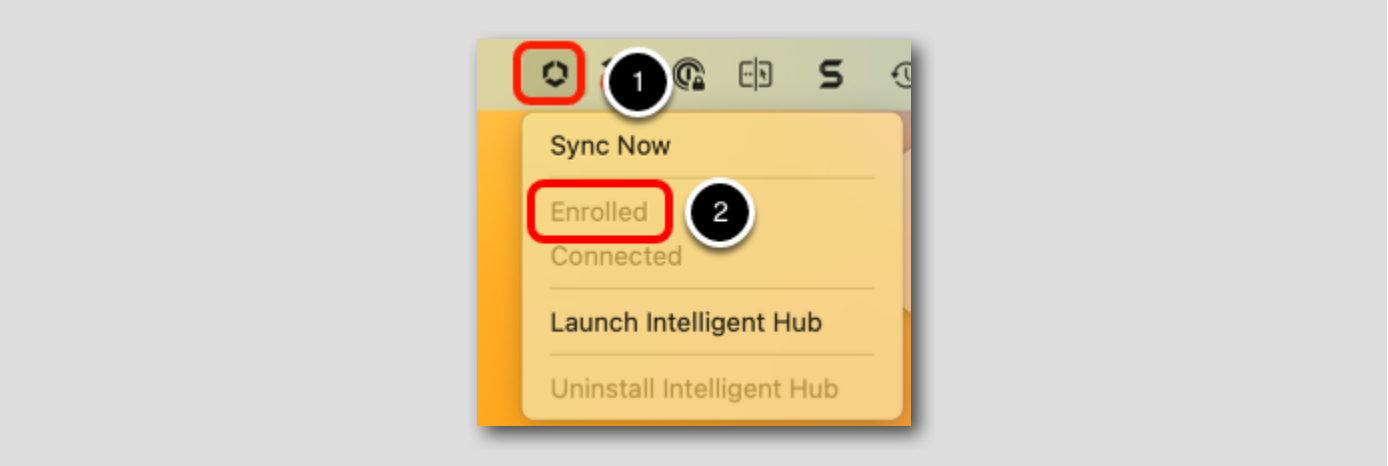
When prompted:

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

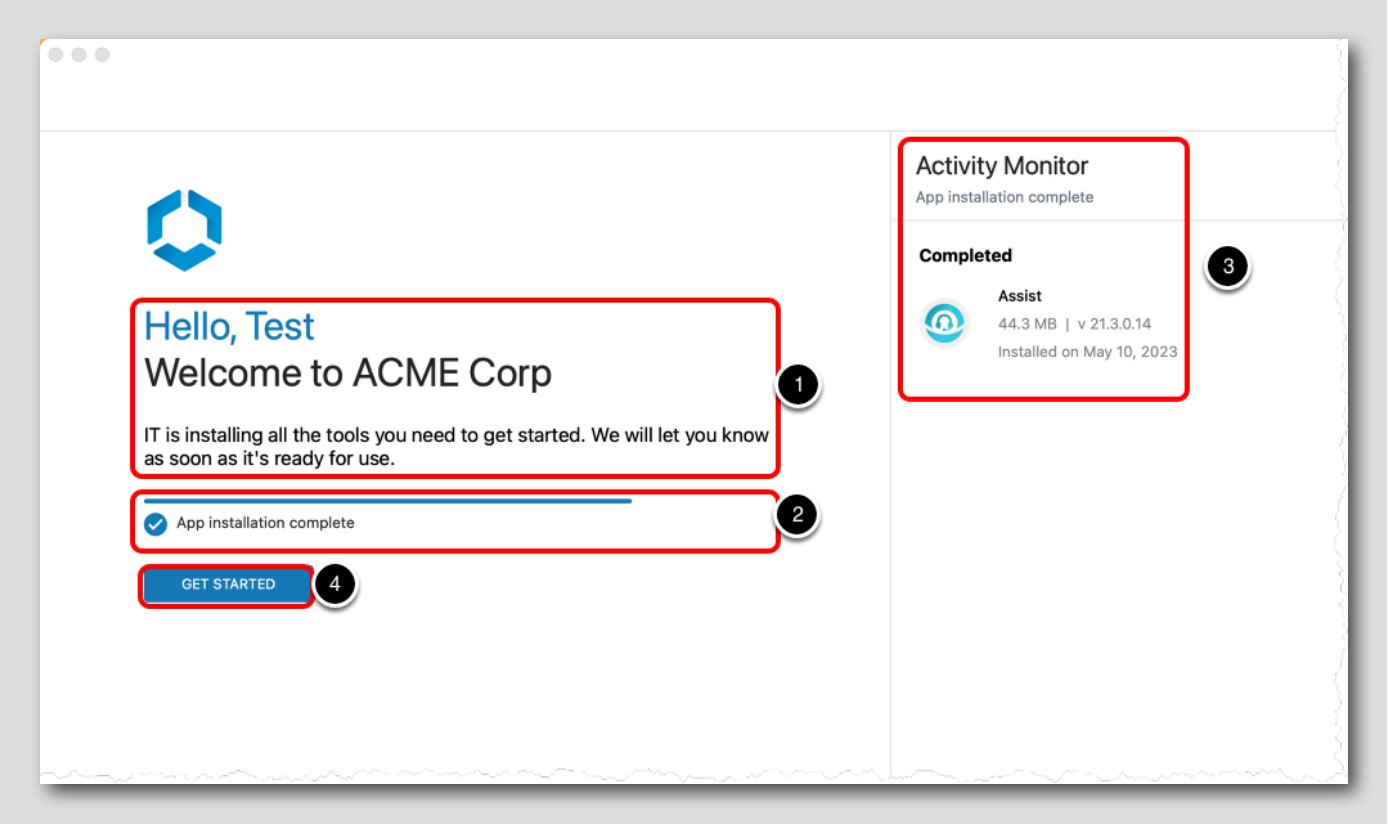
[319]

- 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

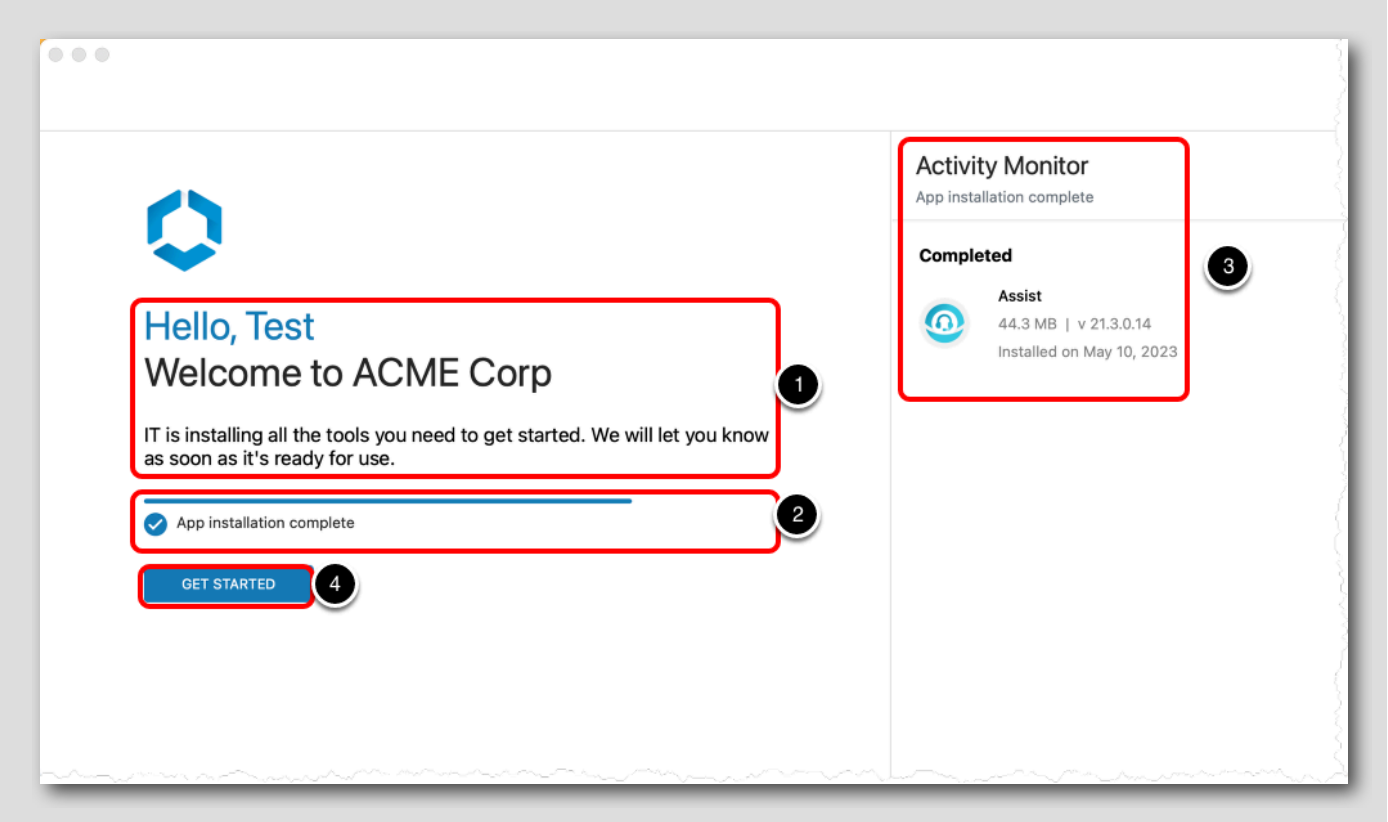
[320]

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



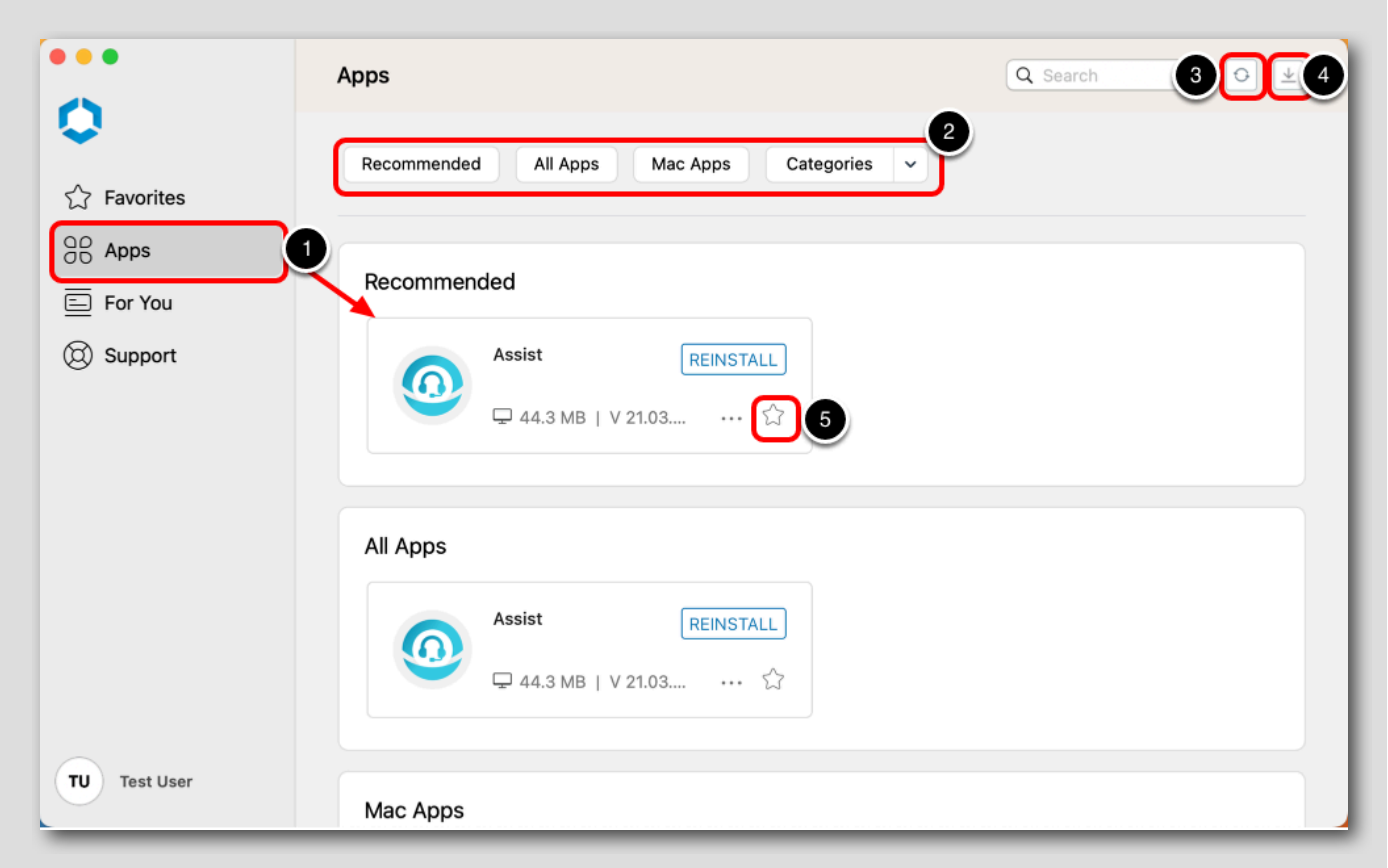
1. Confirm that the Header (**`Hello, {FirstName}`**), Subheader (**`Welcome to ACME Corp`**), and Body Text display your configured message for a personalized onboarding experience.
2. The app installation progress is shown here.
3. All apps that were configured to install on enrollment are shown in 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]



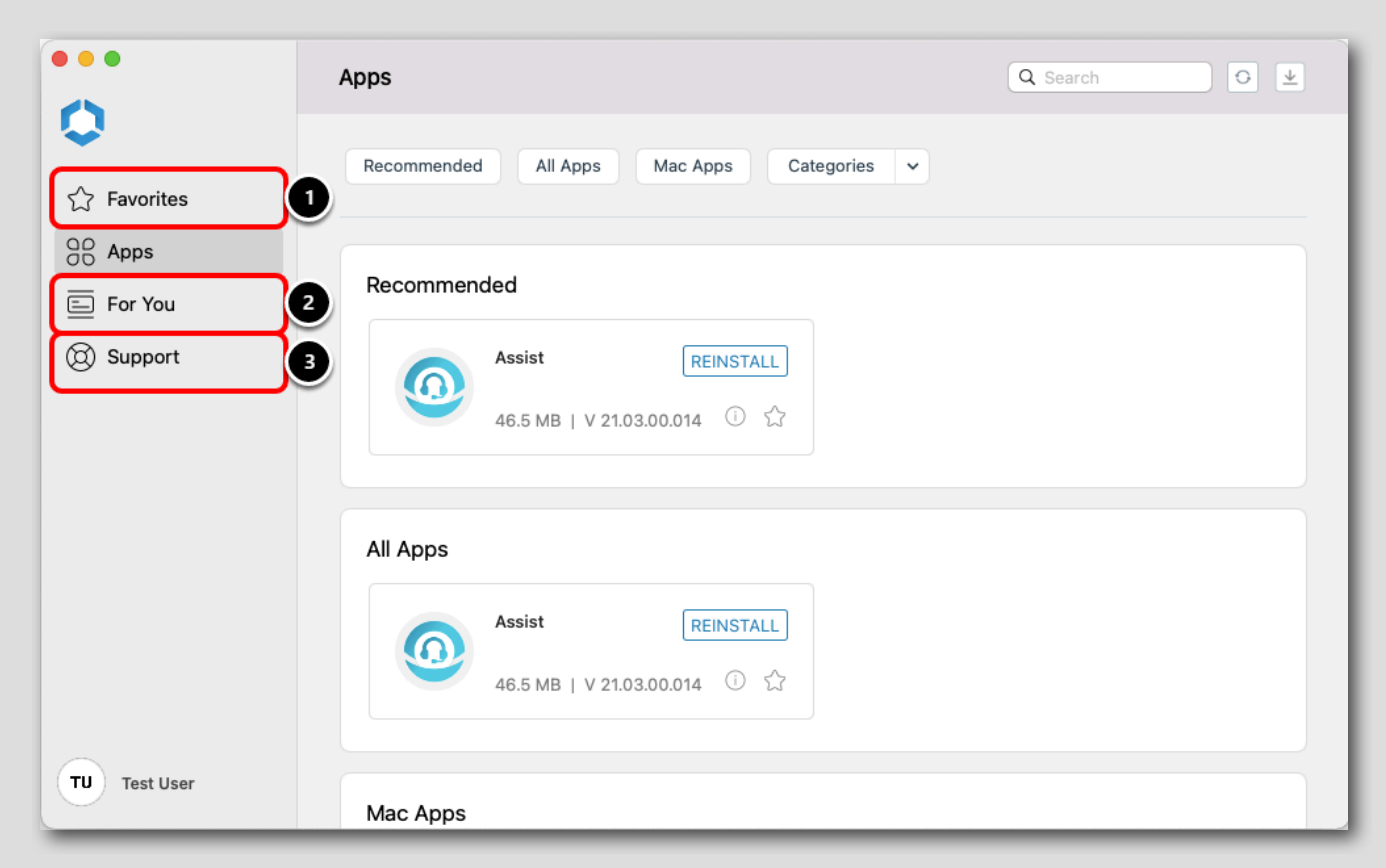
The modern unified app catalog provided by Hub Services is displayed due to the configurations that you made. This enables the following features:

- 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]



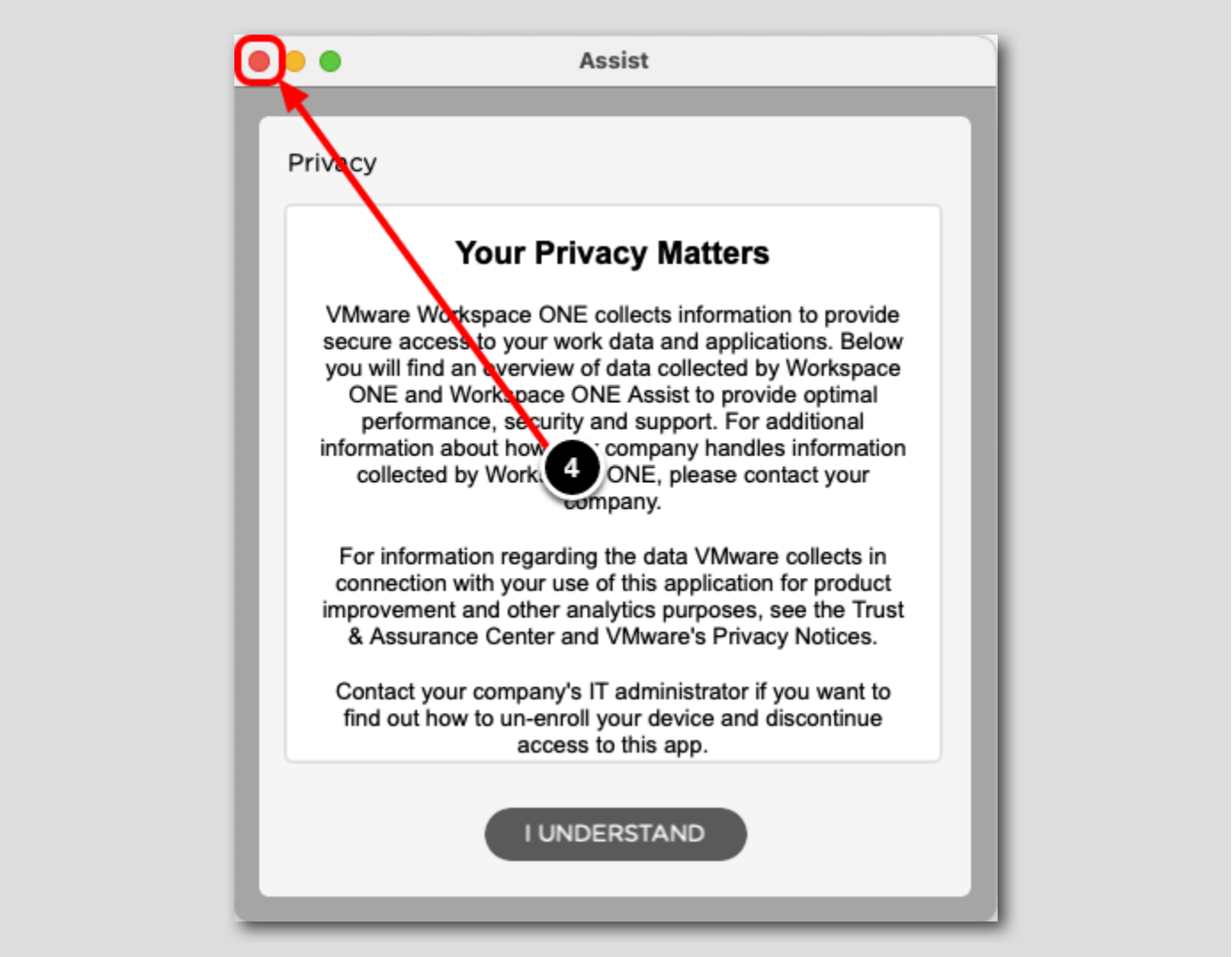
If desired, explore the other features in Intelligent Hub before continuing to the next step to verify the other configurations you published to the device.

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]

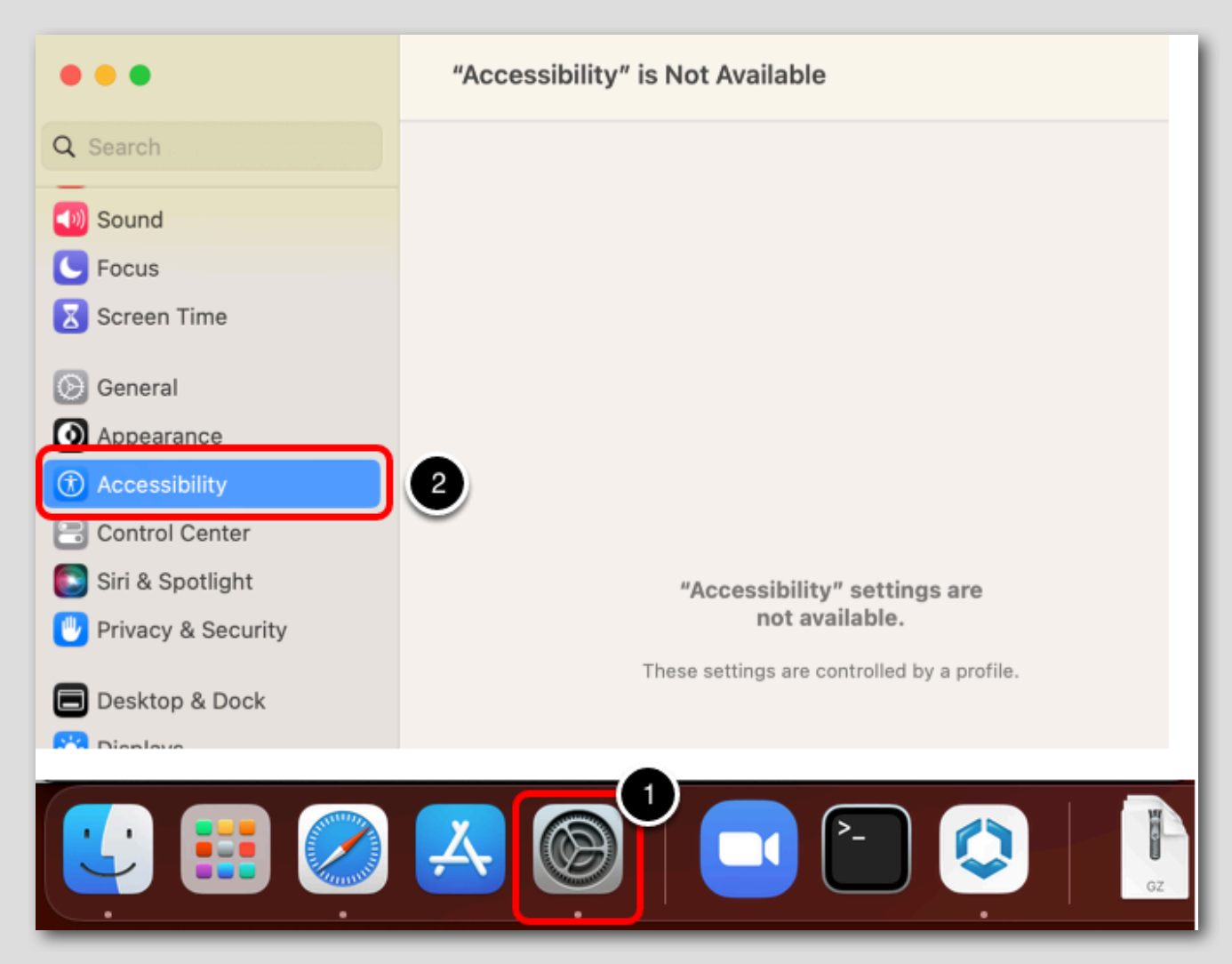


1. Open **Launchpad**
2. Search for **`Assist`**
3. Click the **Assist** app that was installed by Workspace ONE UEM
4. After confirming that the app launches, click the **Close** button to close the app

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

Validate the Restrictions Profile

[324]



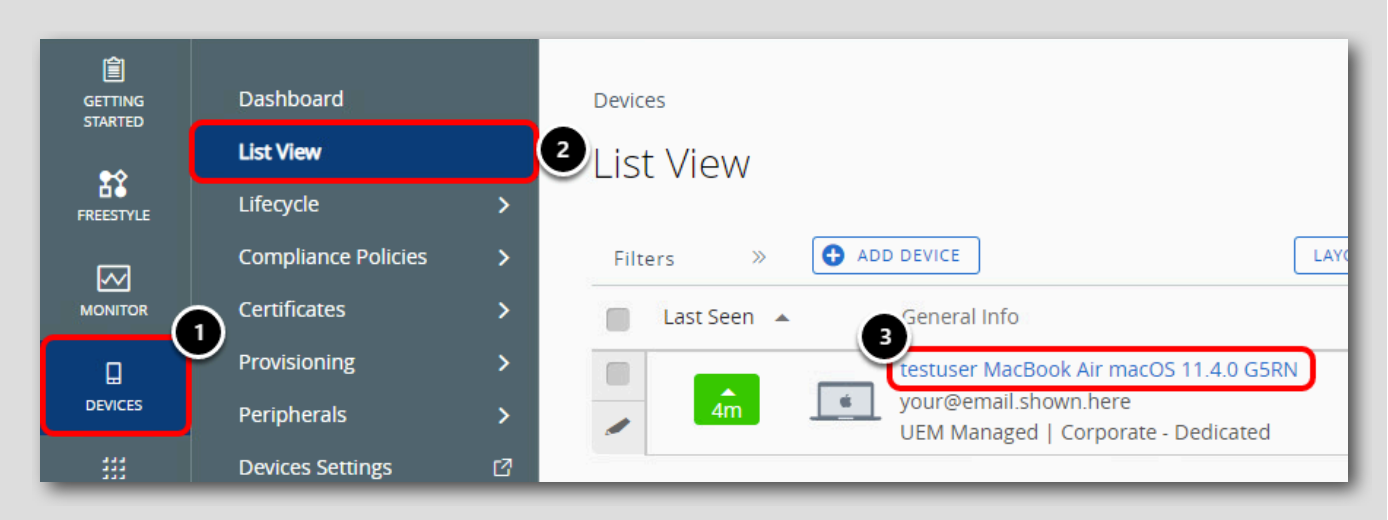
1. Open **System Preferences**.
2. Confirm that the **Accessibility** options are disabled.

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]

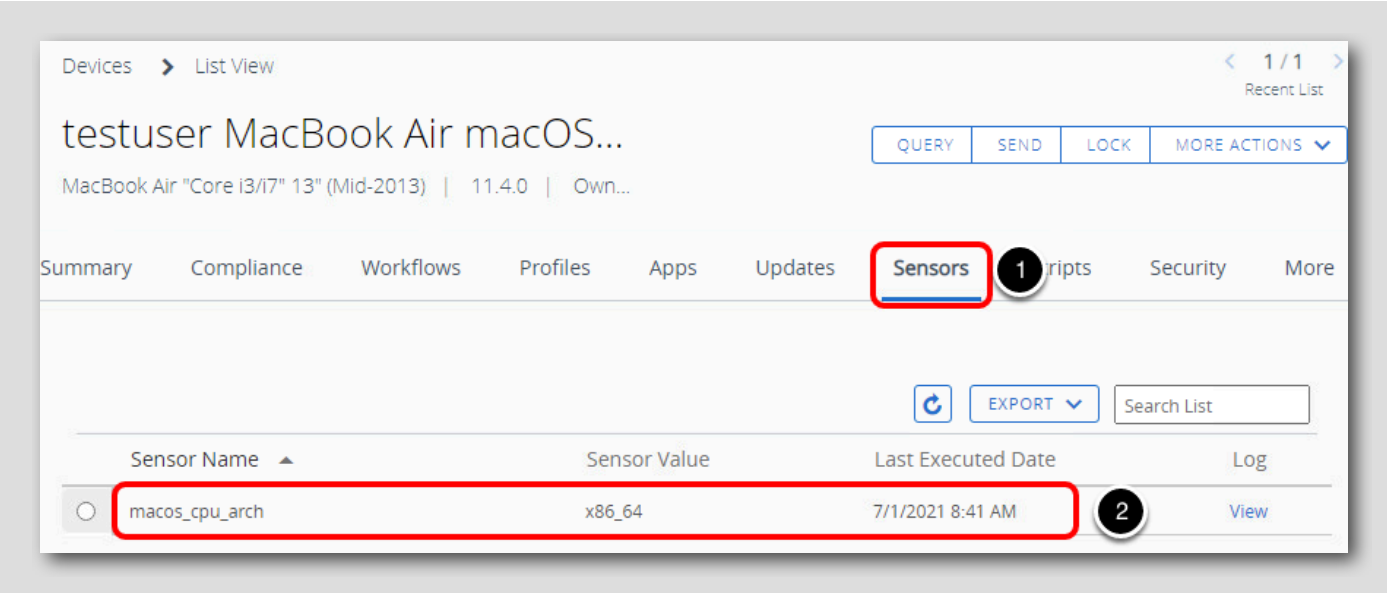


Return to the Workspace ONE UEM administrator console:

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

View the Device Sensors

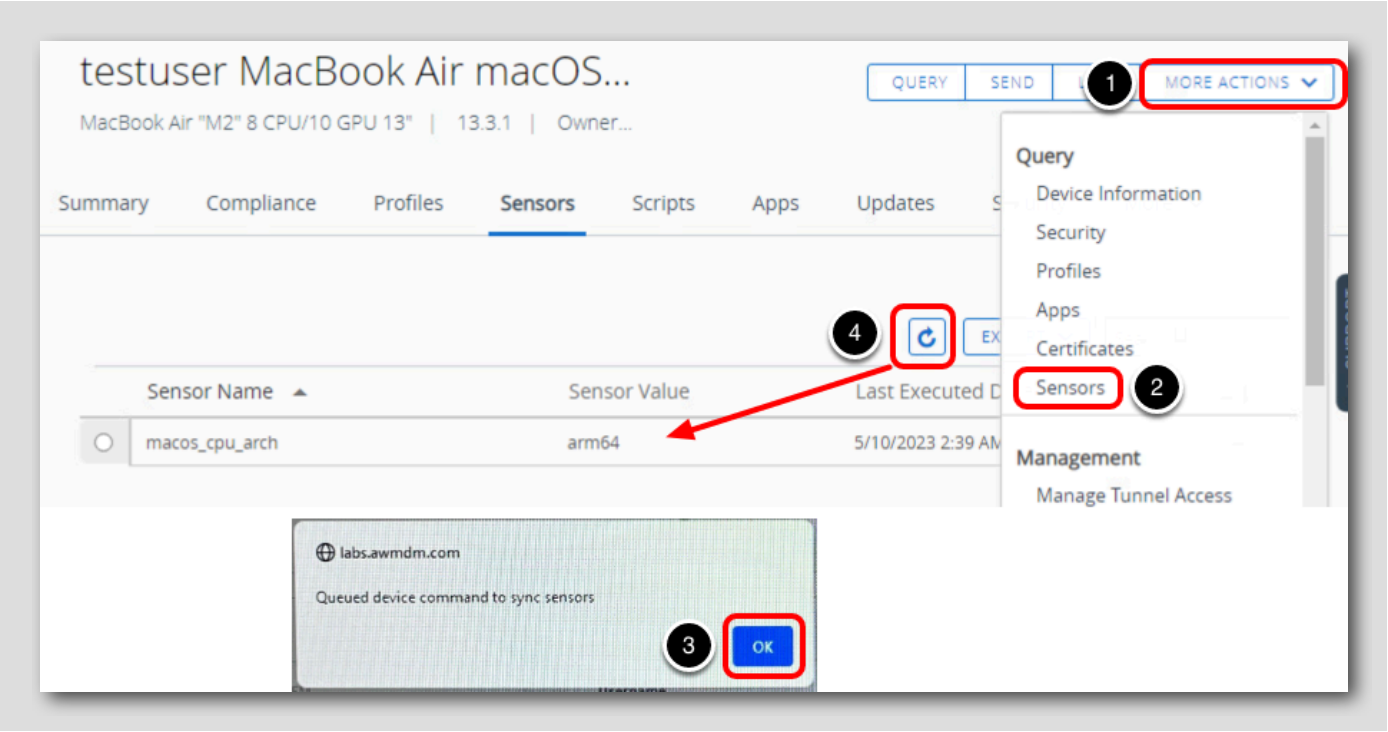
[326]



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

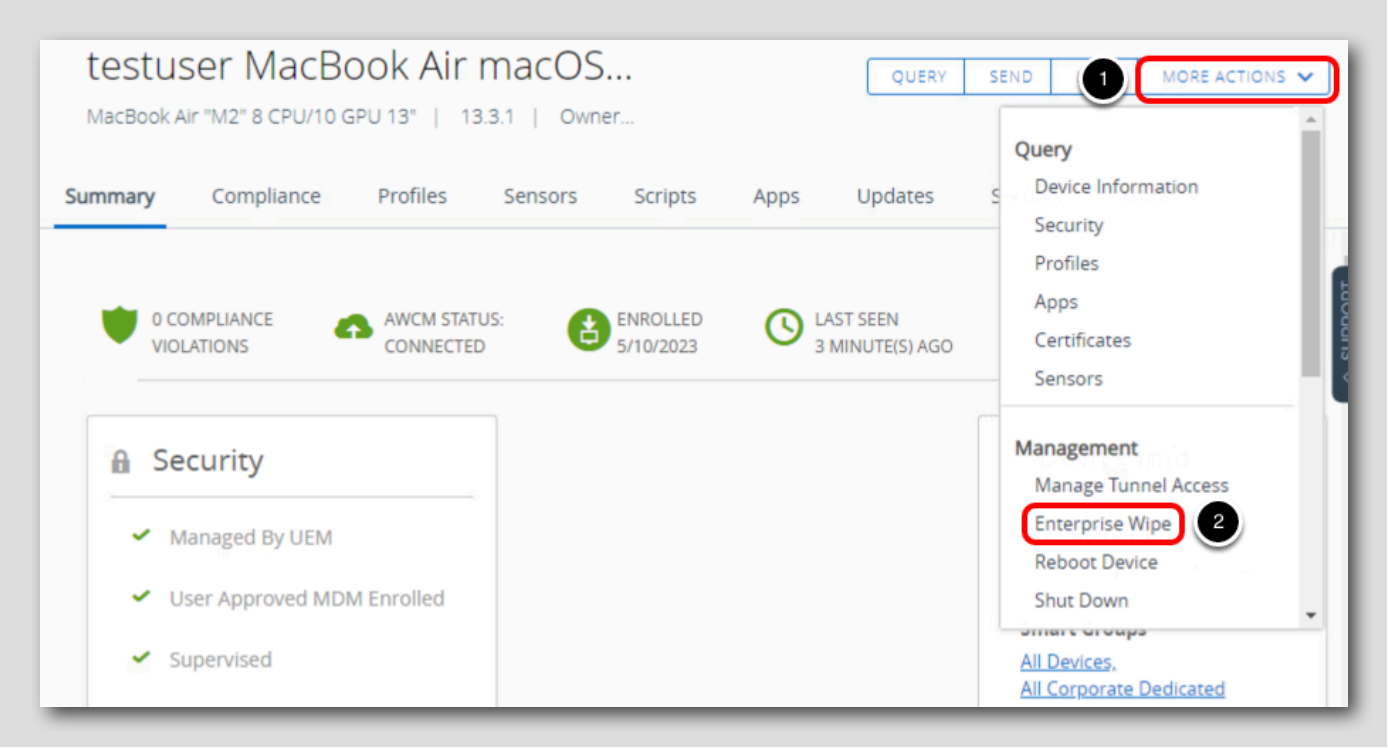
Enterprise Wipe a macOS Device

[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

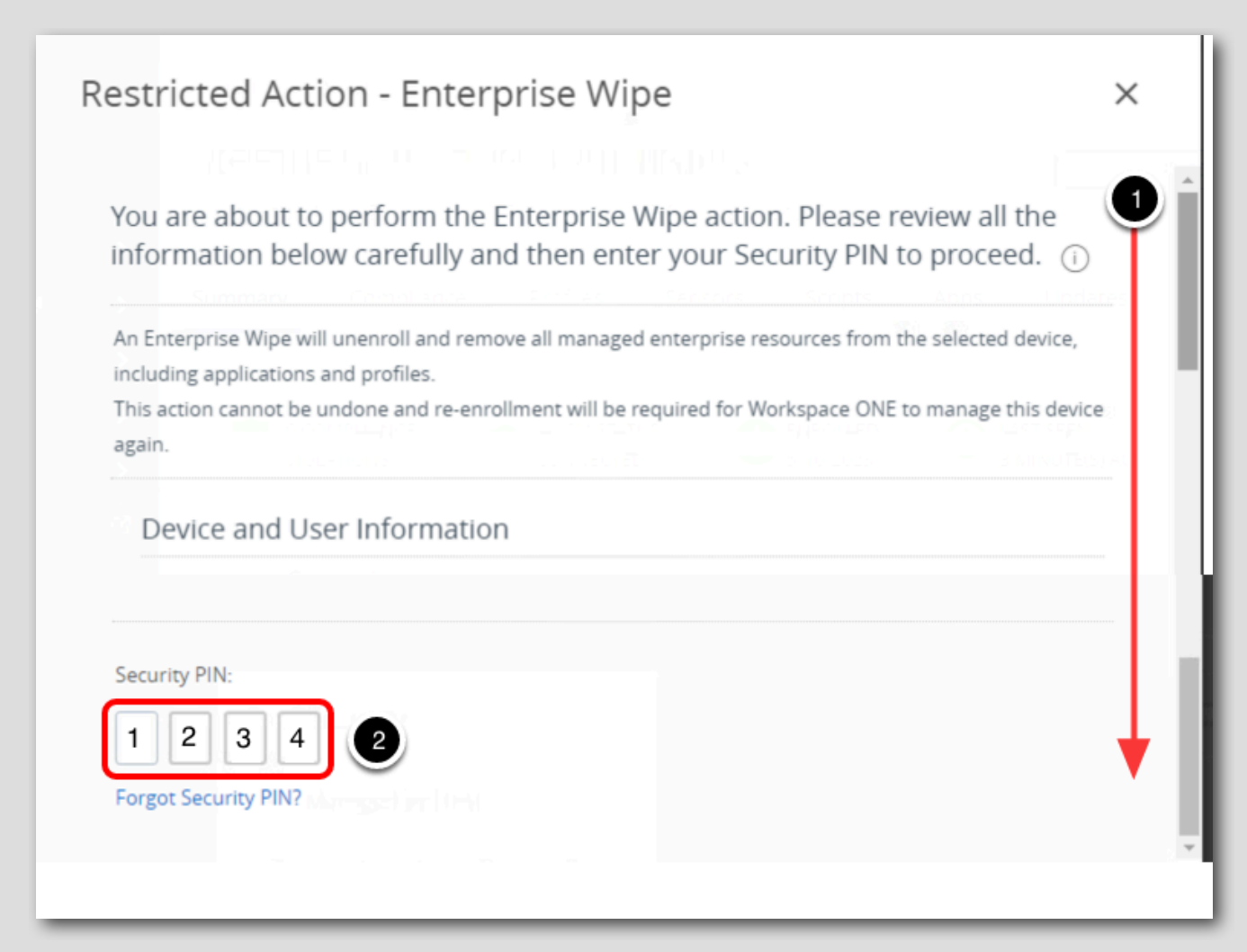
[329]



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]

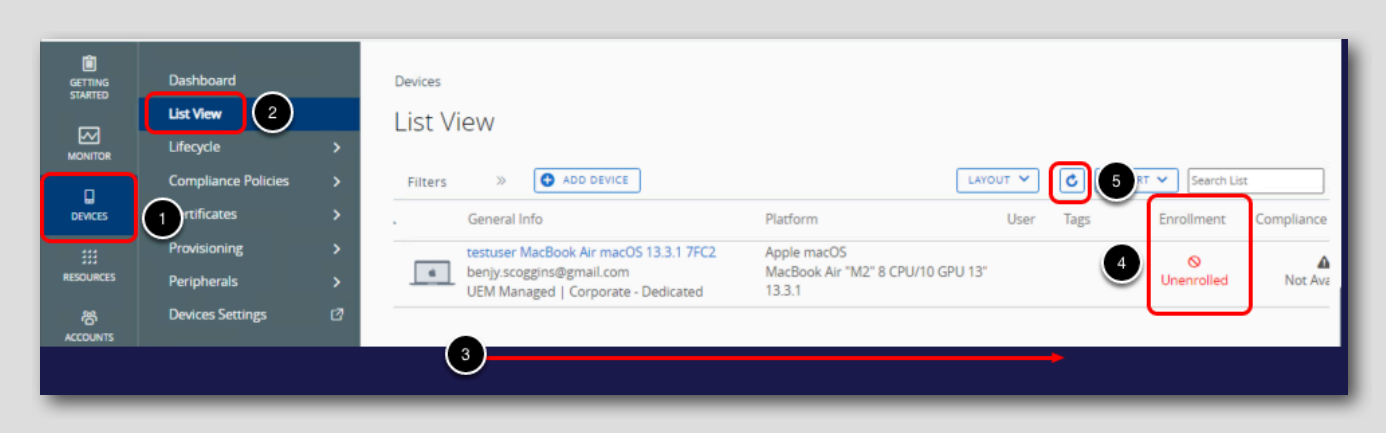


1. Scroll down until you see the section to Enter Security PIN.
2. Enter your security PIN **1234** to initiate the Enterprise Wipe.

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

Confirm Enterprise Wipe

[331]



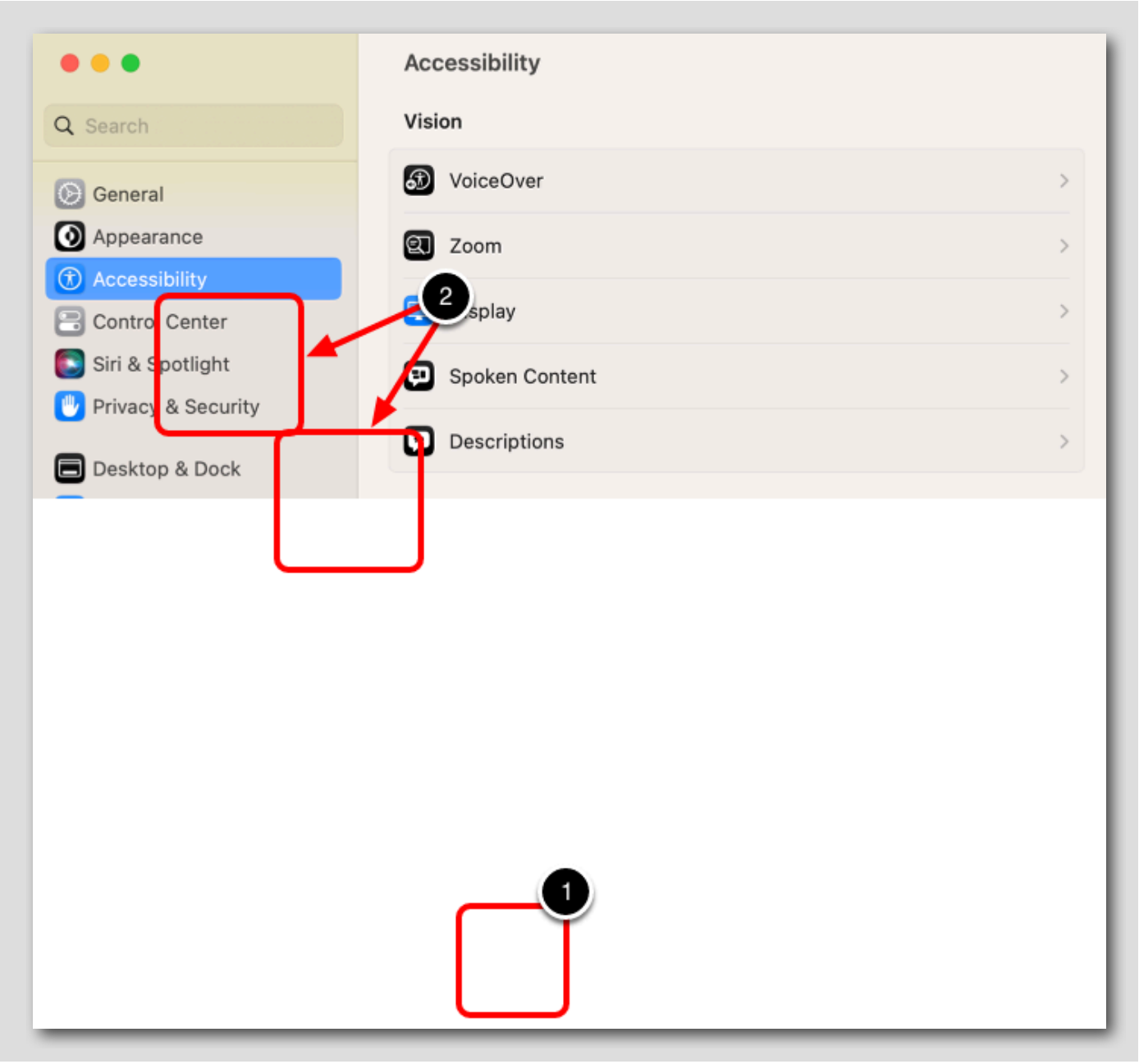
1. Click **Devices**
2. Click **List View**
3. Scroll to the right to find the Enrollment column for the macOS device
4. Confirm that the Enrollment column shows **Unenrolled**
5. If the device is not Unenrolled yet, periodically click the **Refresh** button to check the status

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.

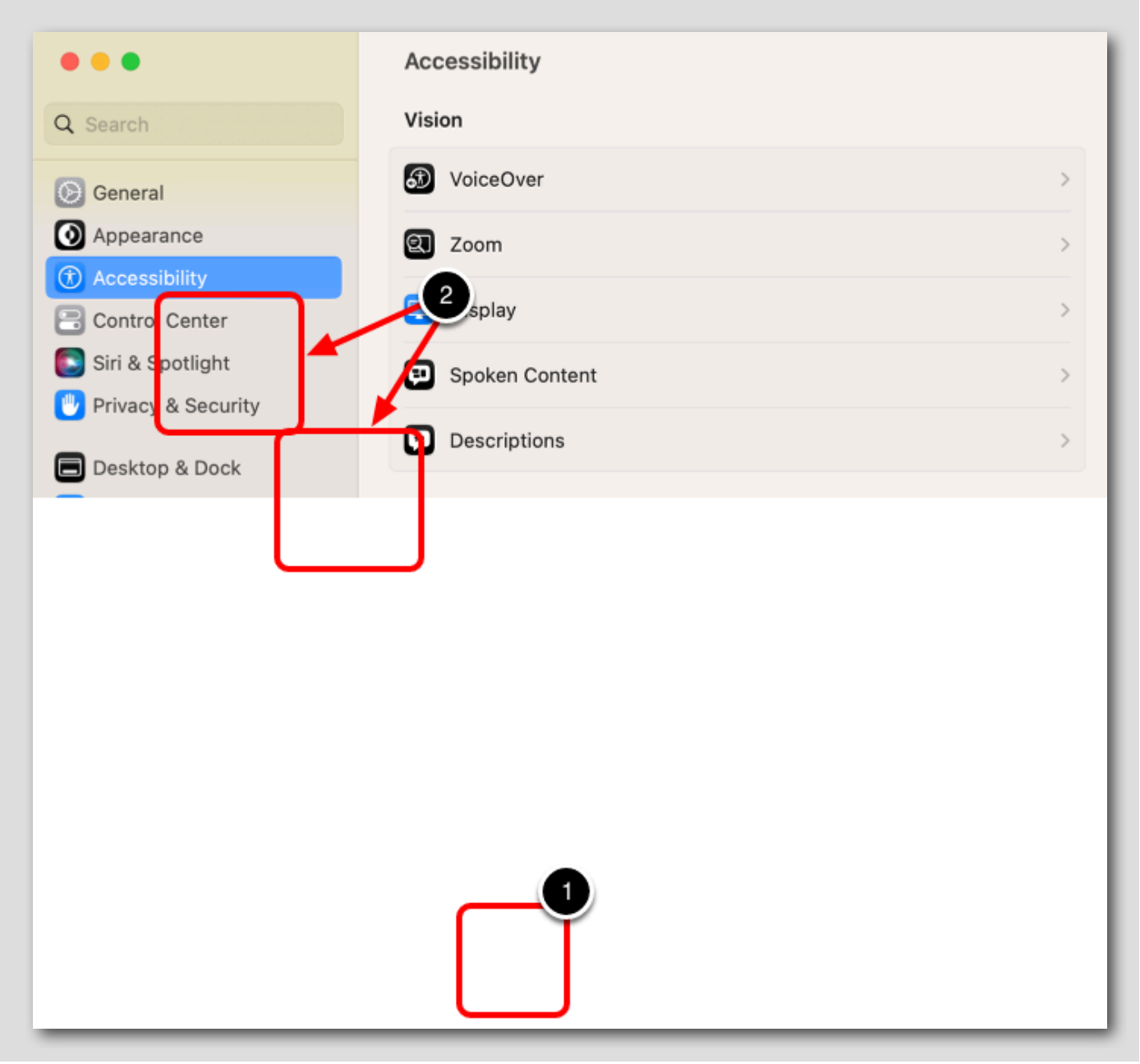
Validate the Enterprise Wipe on the macOS Device

[332]



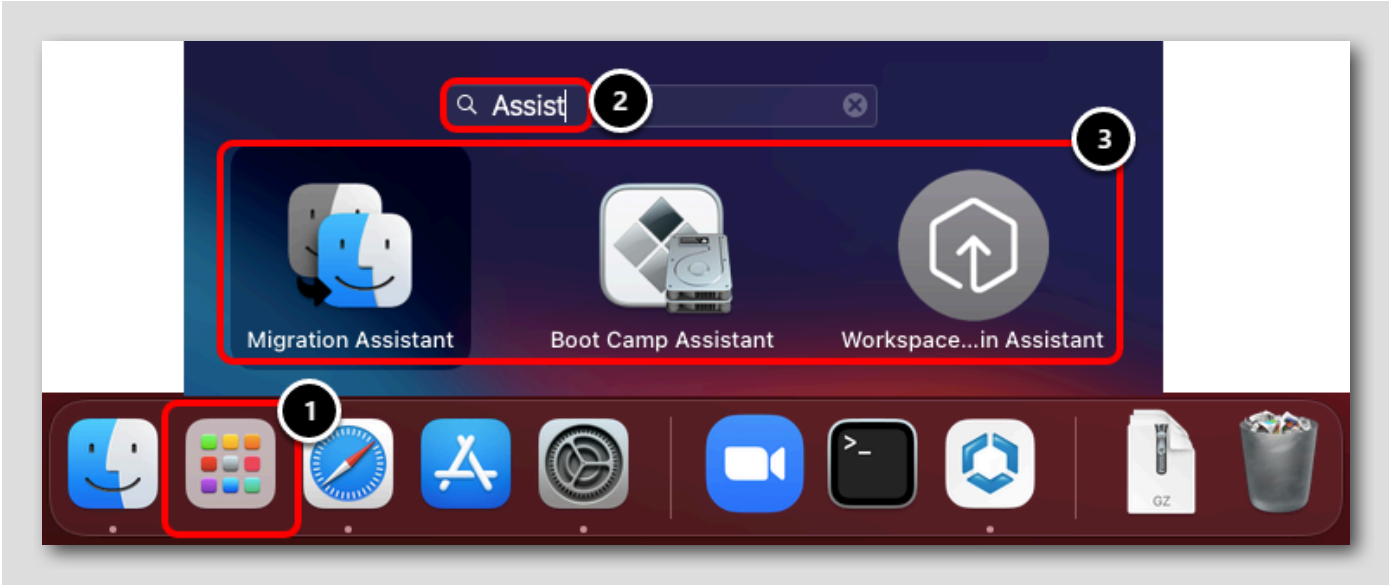
1. Open **System Preferences**.
2. Confirm that the **Desktop & Screen Saver** and **Accessibility** settings are able to be configured again.

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.

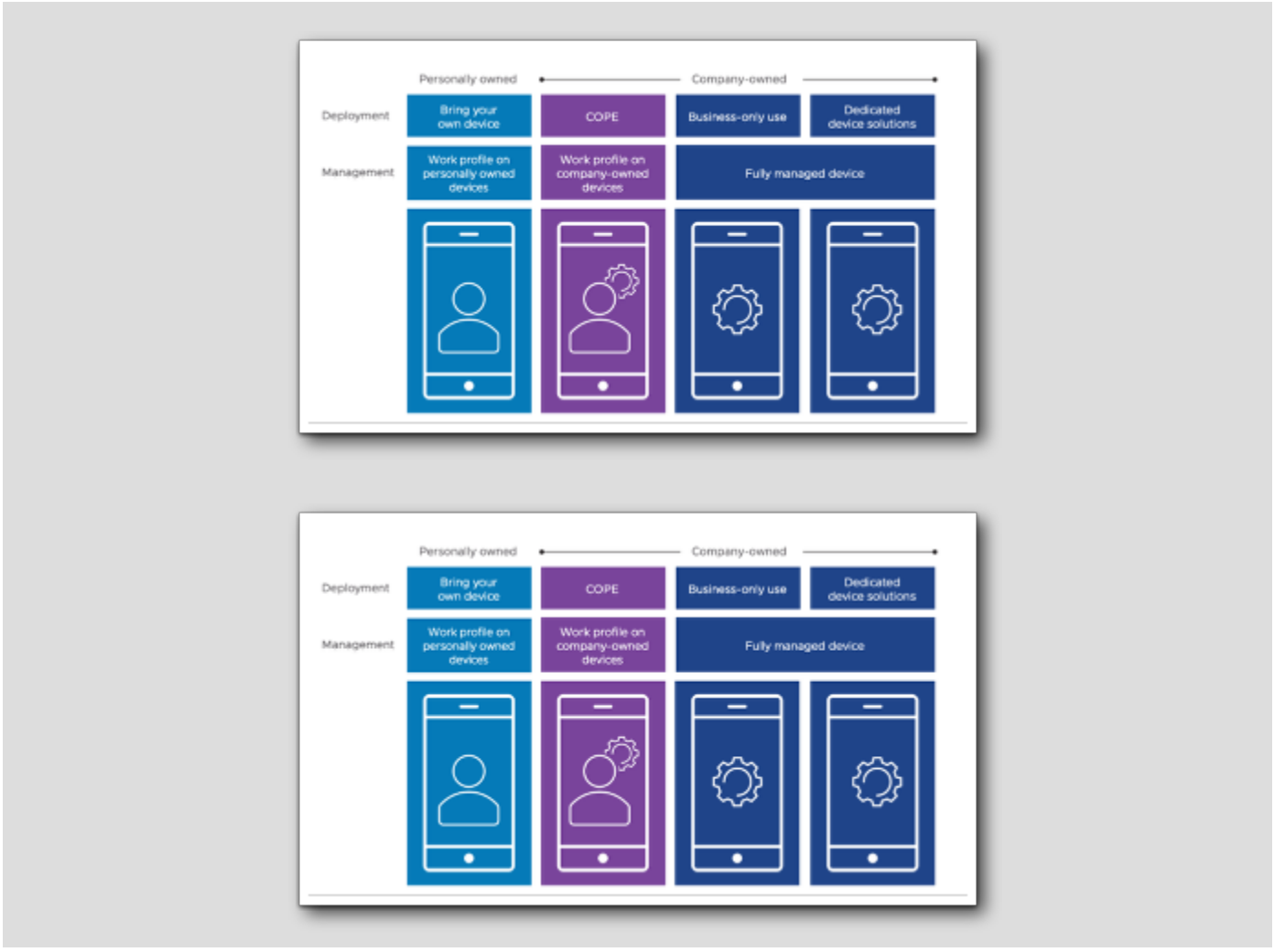
Interested? Check us out at *https://techzone.vmware.com*!

Module 4 - Introduction to Android Management (30 minutes) Beginner

Introduction

[337]

Learn the fundamentals of Android Enterprise, including how to enroll an Android device into Workspace ONE UEM and manage enrolled devices by configuring restrictions and pushing apps. Learn how Android Enterprise and Workspace ONE UEM secure your Android devices by using modern device management APIs.



What is Android Enterprise?

[338]

What is Android Enterprise?

Android enterprise debuted with 5.0 Lollipop in 2014 as an optional solution manufacturers could add to their OS images in order to integrate a common set of device management and Enterprise Mobility Management (EMM) APIs. From 6.0 Marshmallow, it was no longer optional and has since been a mandatory component for all Google Mobile Service (GMS) certified manufacturers.

What does Android Enterprise Offer?

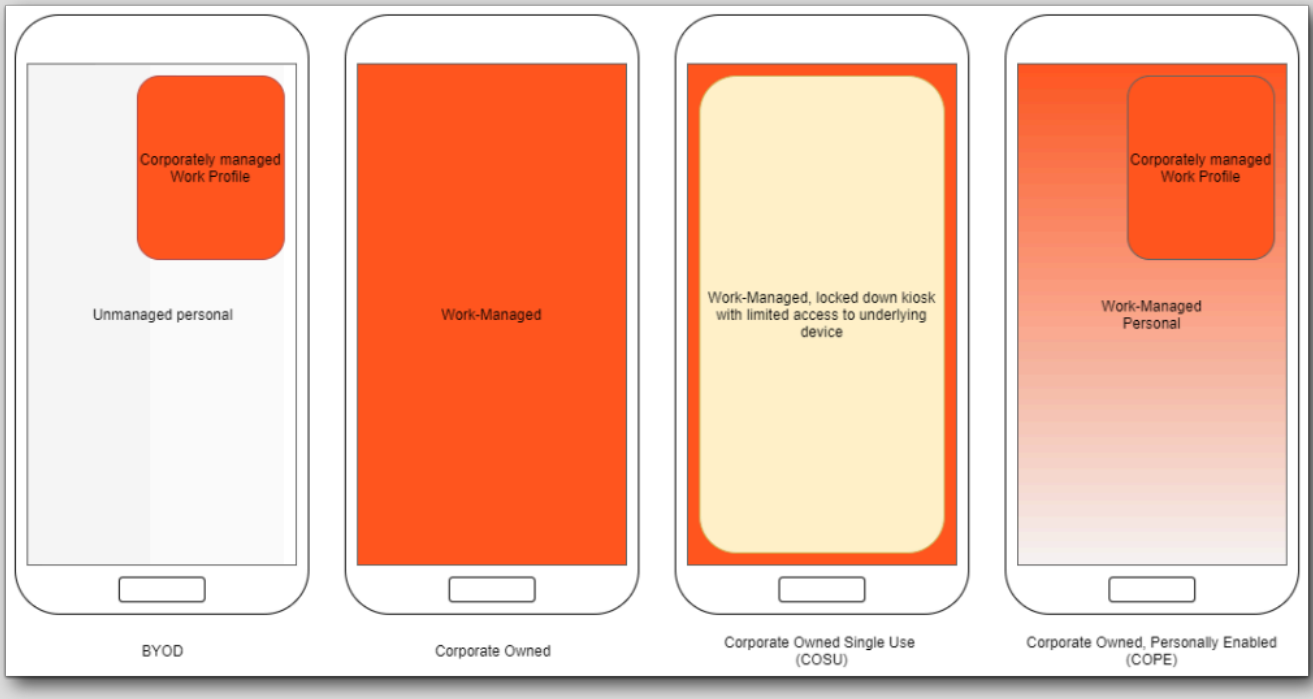
[339]

Android Enterprise offers a wide variety of rich features that cover numerous device management scenarios:

- A rich **Enterprise Mobility Management (EMM)** experience. This allows device administrators to send configurations, applications, and policies down to any Android Enterprise (AE) device, providing a secure method of managing devices and corporate data no matter where your devices are.
- **Work Profile** mode for BYOD (Bring Your Own Device) scenarios, which allows for a device to have a separate work container from their personal apps and data.
- **Work-Managed** mode (previously called **device owner**), which provides corporations a larger suite of options for securing corporate owned devices that are not intended for personal use.
- **Corporately Owned, Single Use** (COSU) mode, which provides corporations with a kiosk-like experience. The Work-Managed device is locked down in a Kiosk-like state, granting access to a few applications or resources instead of the entire underlying device operating system.
- **Corporate Owned, Personally Enabled** (COPE) joins the Work Profile and Work-Managed modes to provide a fully managed device with personal space.
- **Zero-Touch Enrollment** for out of the box Android 8.0 and higher devices, providing a streamlined enrollment experience for end users.
- A corporate-managed **Managed Google Play portal**, allowing administrators to explicitly approve applications to an application store that can be accessed by end users.
- **Silent Application Installation** without requiring a user provided Google account on the device.
- **App Configuration**, enabling device administrators to deploy key-value pairs to managed applications to modify the end user experience.
- **Mandatory Device Encryption** to ensure that your corporate resources are secured and protected on the device.

Understanding Device Management Scenarios

[340]



The above graphic shows the big picture differences between various device management scenarios.

Bring Your Own Device (BYOD):

- Commonly used where employees or end users have their own personal devices that need access to corporate resources.
- To avoid managing the end user's personal data or apps, a **Work Profile** can be deployed to keep the corporate apps and data separate from their personal apps and data.
- This grants device administrators the ability to securely control access to corporate resources from a personal device without managing the full personal device.

Corporate Owned:

- Commonly used where corporations own devices that are given to employees or end users to fulfill their role or task.
- **Work-Managed** mode allows for the entire device to be managed and controlled, allowing for a wider range of configurations.
- **Work-Managed** mode does not provide an un-managed personal space and should only be used for corporate owned devices.

Corporate Owned Single Use (COSU):

- Commonly used where corporations own devices that are used as Kiosks or have Kiosk-like applications running on them.
- Corporate Owned Single Use leverages **Work-Managed** mode to manage the entire device, but does not grant the end user access to the full underlying device operating system.

Work Profile for Company-Owned Devices (Formerly calles as COPE-Corporate-Owned Personally Enabled):

- Work Profile for Company-Owned Devices, formerly known as Corporate-Owned Personally Enabled (COPE) devices, are fully managed company-owned devices that have a dedicated work profile inflated on them and are also enabled for the end-user's personal use.
- Commonly used where corporations own devices that are given to employees or end users that permits some level of personal usage while still being corporately controlled.
- Corporate Owned, Personally Enabled leverages a **Work-Managed** personal space for varying amounts of personal usage while employing a **Work Profile** to control corporate resources, data, and apps.
- This joins the ideas of **Work Profile** and **Work-Managed** modes into a single device.

Overall, The below picture showcases the idea of Understanding Android Enterprise Modes

Different Enrollment Methods

[341]

In addition to providing different device management scenarios, there are also multiple ways in which devices can be enrolled into Android Enterprise.

Near-Field Communication (NFC) Enrollment [342]

With the Near-Field Communication (NFC) bump method, a NFC programmer app is setup on a designated programmer device. Subsequent devices are "bumped" into the programmer device to pass the necessary initial policies (such as Wi-Fi, device configurations, etc.) to the bumped device via NFC.

The process will vary slightly in terms of pre-applied settings, what agent is downloaded in order to enroll the device on the relevant platform, etc. Workspace ONE UEM allows for the additional configuration of a named account to directly enroll the device against.

Hashtag (#) Enrollment or Device Policy Controller (DPC) Identifier Enrollment [343]

This method was introduced in Android 6.0 Marshmallow. When prompted to add or create an account on a freshly wiped (or directly from the box) device, rather than enter in a Google account, the administrator would type in **afw#hub** and then the device would download the Workspace ONE Intelligent Hub app and begin the enrollment process with the correct configurations.

QR Enrollment [344]

By tapping on **Welcome** 6 times when the device boots into the setup Wizard, it will prompt the device to connect to Wi-Fi and start QR enrollment.

In Android 9.0 P, the QR payload is bundled into the system and therefore doesn't require a download. This offers faster provisioning as the device no longer needs to connect to the internet to download the QR package and the ability to add Wi-Fi credentials to the QR code.

Zero-Touch Enrollment [345]

Devices are purchased through authorized resellers, assigned to Workspace ONE UEM and then later, when the end-user first takes the device freshly out of the box, will be ready to enroll as a work-managed device straight away. With Zero-Touch enrollment, administrators can send enrolled and configured devices directly to end-users to authenticate with.

DO NOT Enroll Personal Android Devices [346]

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

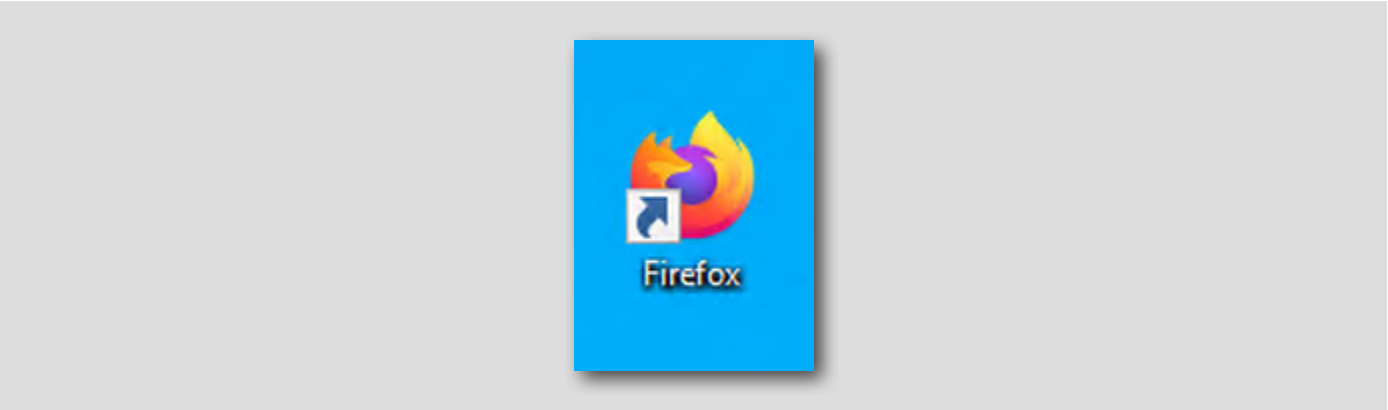
Personal devices may be enrolled into other UEM providers which can cause undesired conflicts and issues.

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 [347]

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

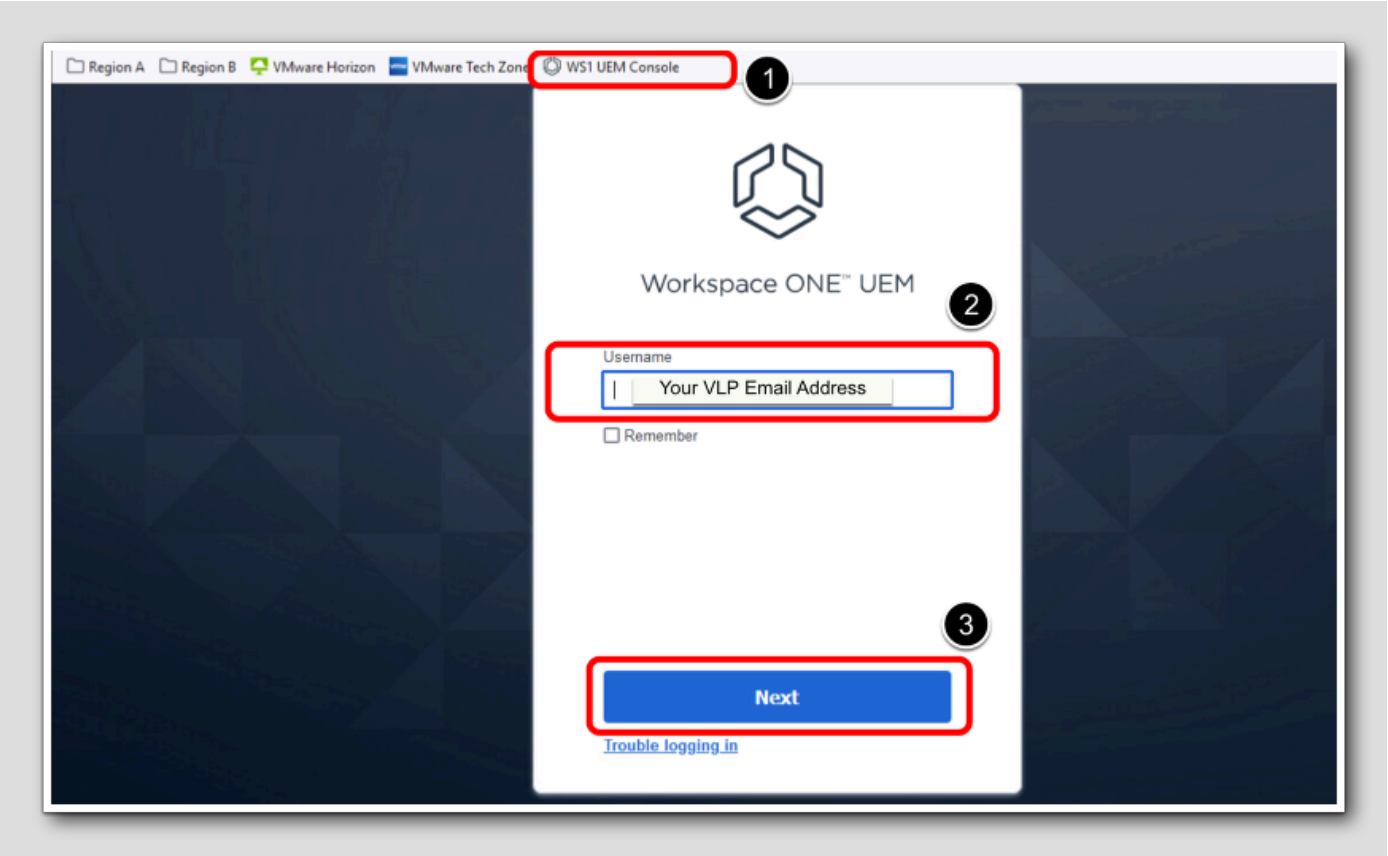
Launch Firefox Browser [348]



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

[349]

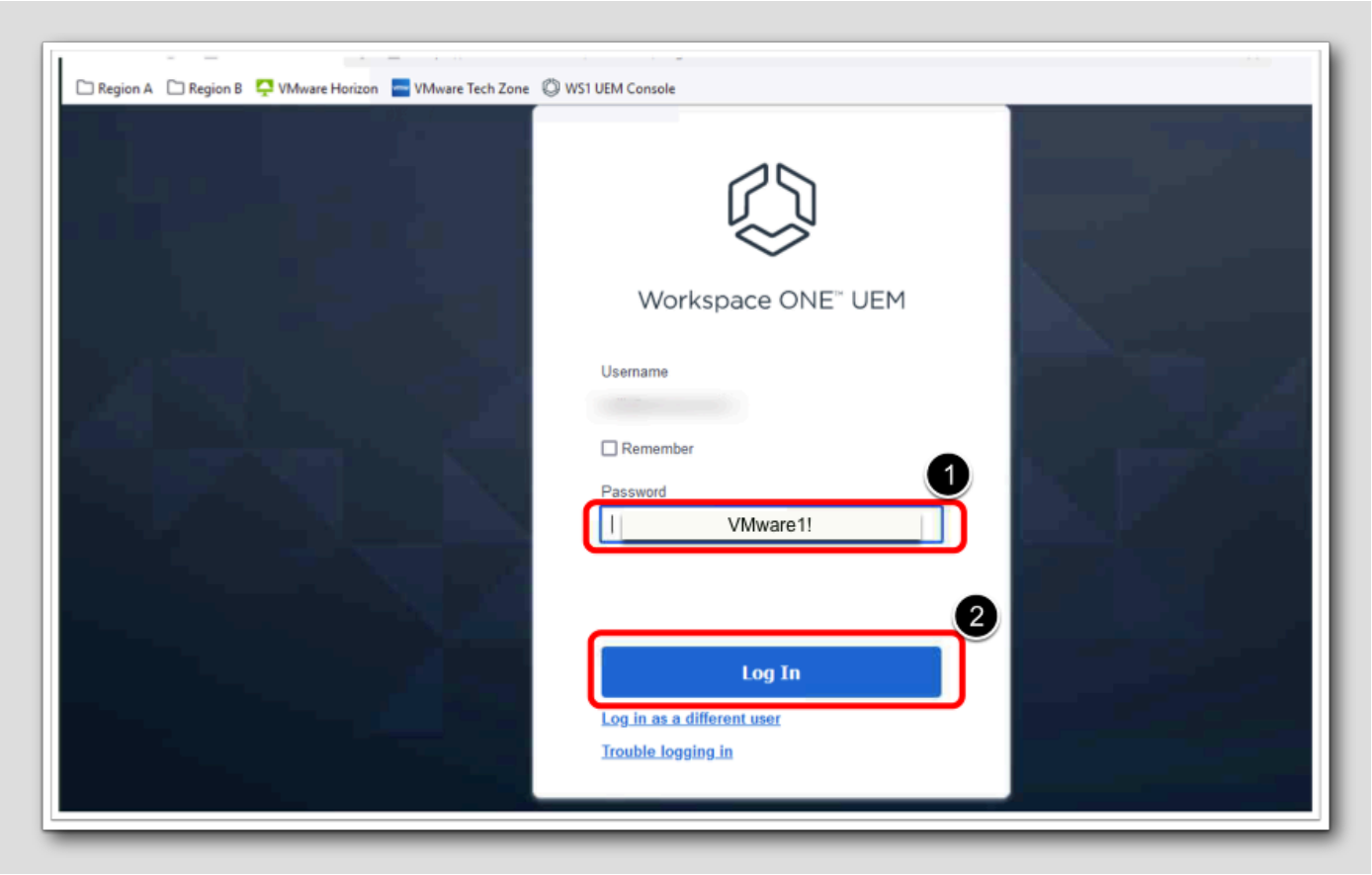


1. Select the **WS1 UEM Console** link from the Bookmark Toolbar
2. Enter your **Username**. This is the **email address** that you have associated with your **VMware Learning Platform (VLP)** account that you utilized to take Hands-on Labs.
3. Click **Next**, then advance to the next step of the lab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

[350]



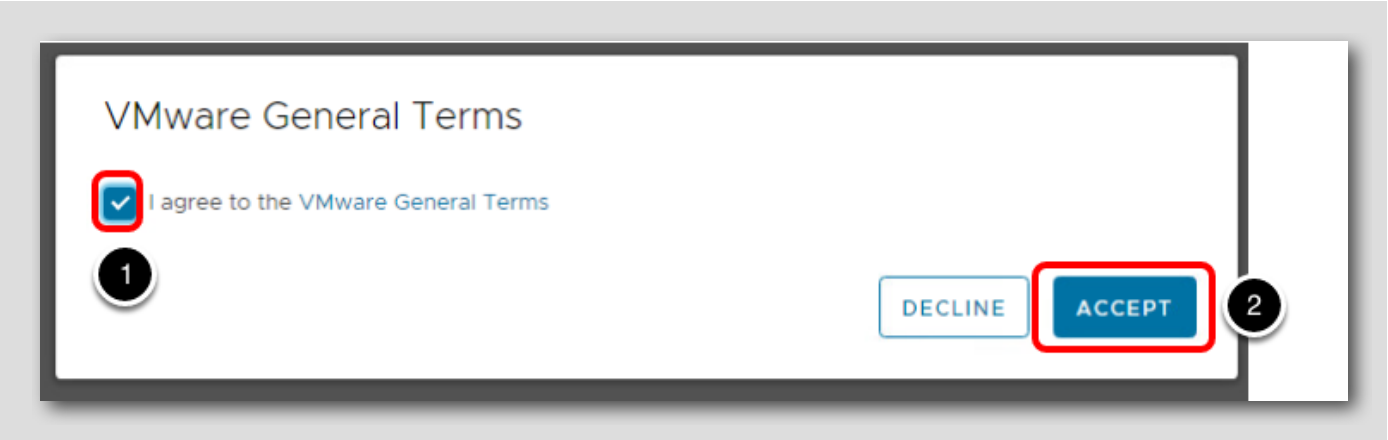
The password field will be displayed after entering your username.

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

[351]



You will be presented with the VMware General Terms.

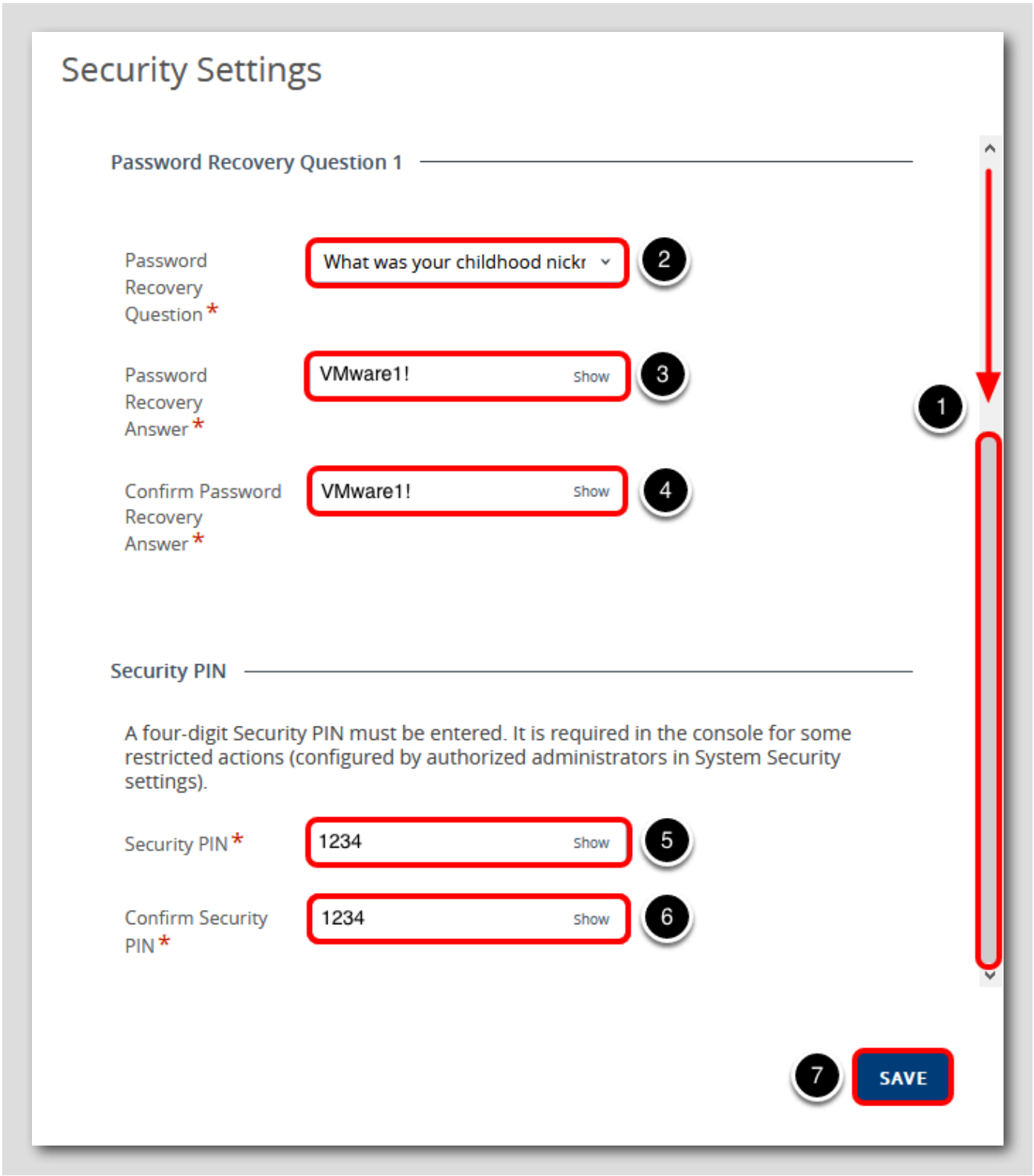
1. Select the box next to I Agree to the VMware General Terms.
2. Click the **Accept** button.

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

[352]

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

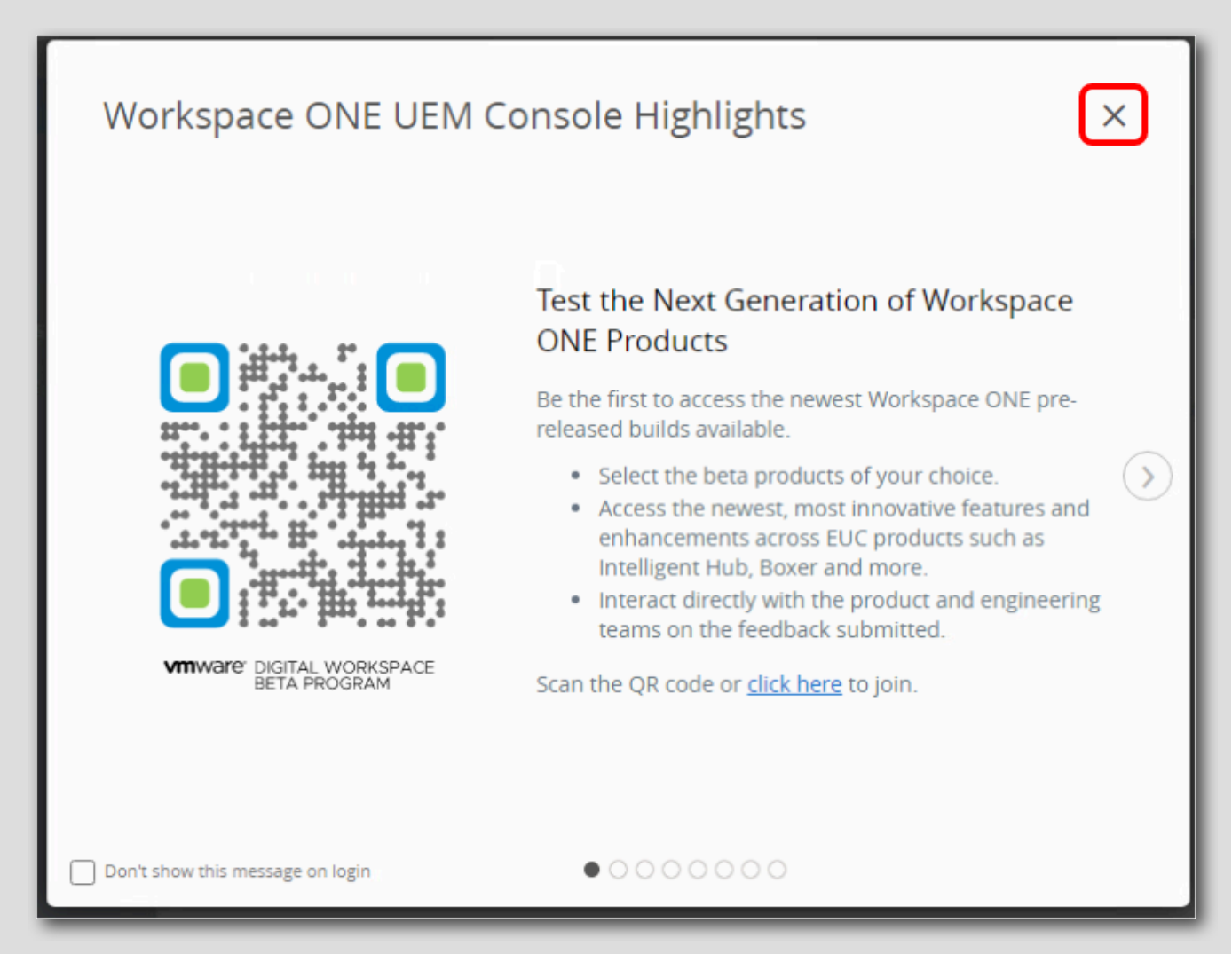

Security Settings
Password Recovery Question 1
Password Recovery Question *
What was your childhood nickr
2
Password Recovery Answer *
VMware1!
Show
3
1
Confirm Password Recovery Answer *
VMware1!
Show
4
Security PIN
A four-digit Security PIN must be entered. It is required in the console for some restricted 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

[353]



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.

Configuring Android Enterprise for Workspace ONE UEM

[354]

We will be covering some of the Android basic functionality.

When running on Android 5.0 Lollipop devices, Android Enterprise is built into the operating system with no need for an additional application.

To begin using Android Enterprise inside the Workspace ONE UEM Console, you need to register your enterprise with Google. This creates your Android Enterprise admin account which connects with Workspace ONE UEM to manage your enterprise devices. Users will not be able to use Android Enterprise features from their devices until registered with Workspace ONE UEM. The Android Enterprise setup wizard simplifies the process. To simplify your experience, this initial process has been done for you. If you are interested in learning more about this process please talk to your Workspace ONE UEM Sales Engineer or Representative.

NOTE: Once a Google Admin Account is bound to Workspace ONE UEM, you cannot reuse this Google Admin for another organization. Due to this limitation, you would be unable to use the Google Admin Account we have already bound to Workspace ONE UEM for this lab.

Open Settings (FOLLOW ALONG)

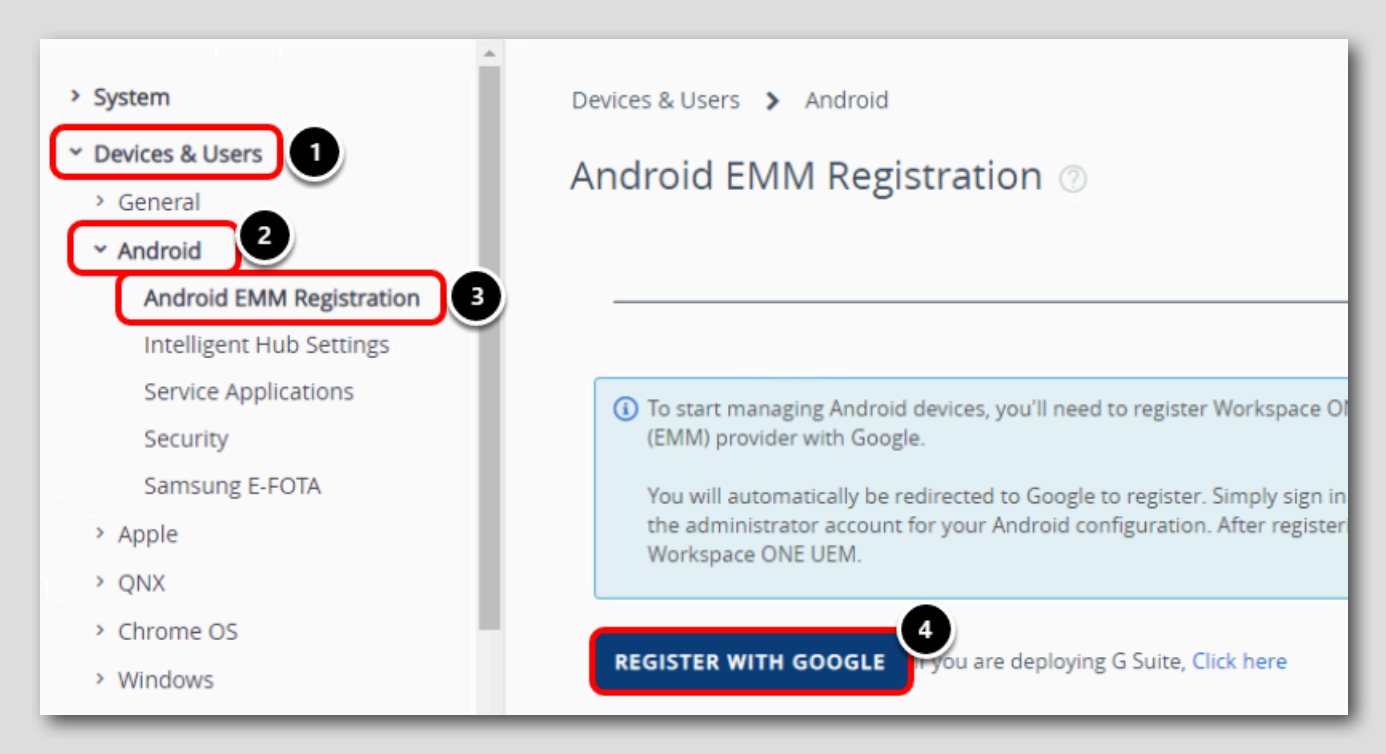
[355]

NOTE - The following changes have already been configured for you as part of the lab!

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

Open Android Enterprise Configuration (FOLLOW ALONG)

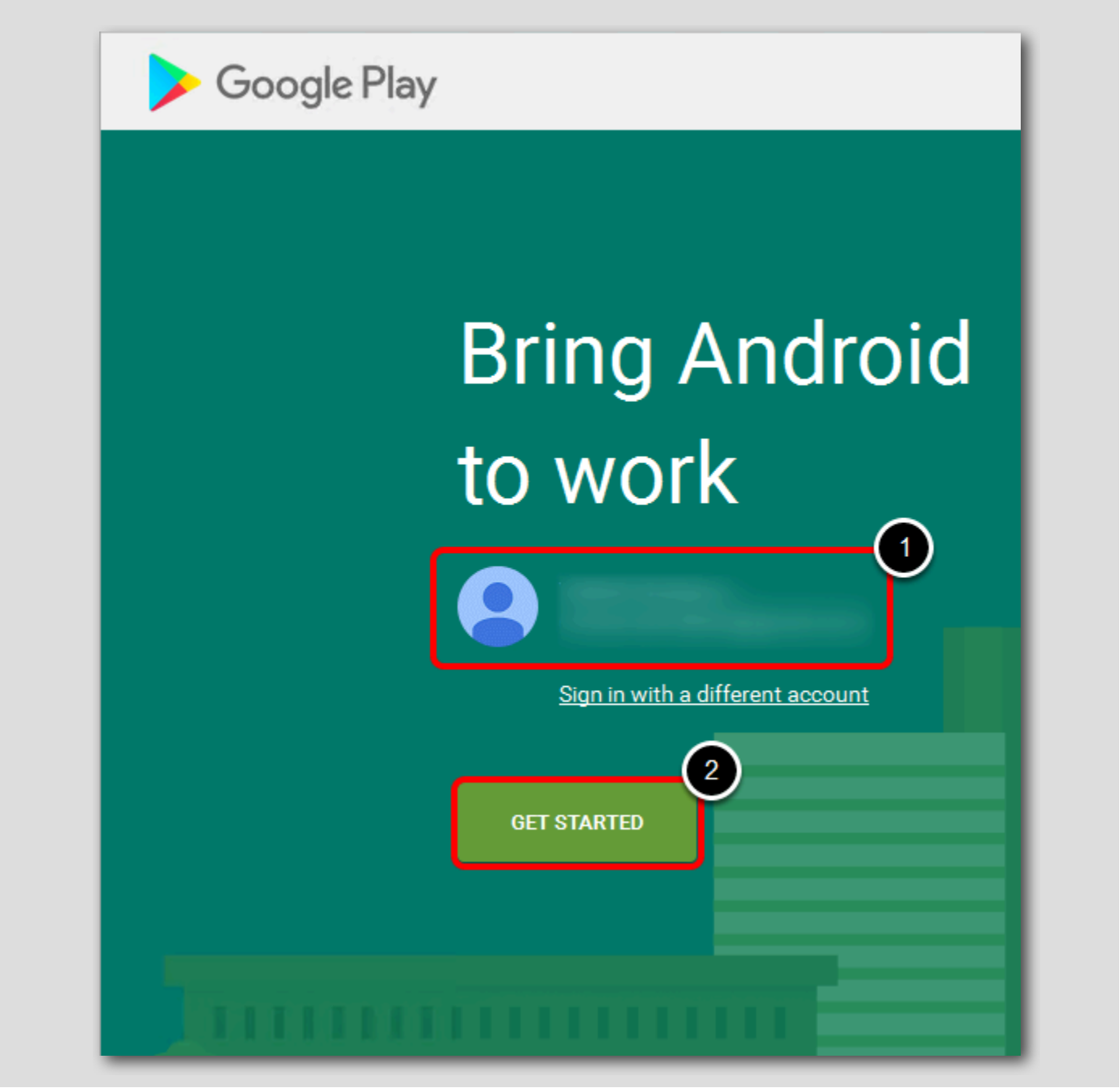
[356]



NOTE - The following changes have already been configured for you as part of the lab!

1. Click **Devices & Users**
2. Expand **Android**
3. Click **Android EMM Enterprise**
4. Click **Register with Google**

Provide Google Admin Account (FOLLOW ALONG) [357]

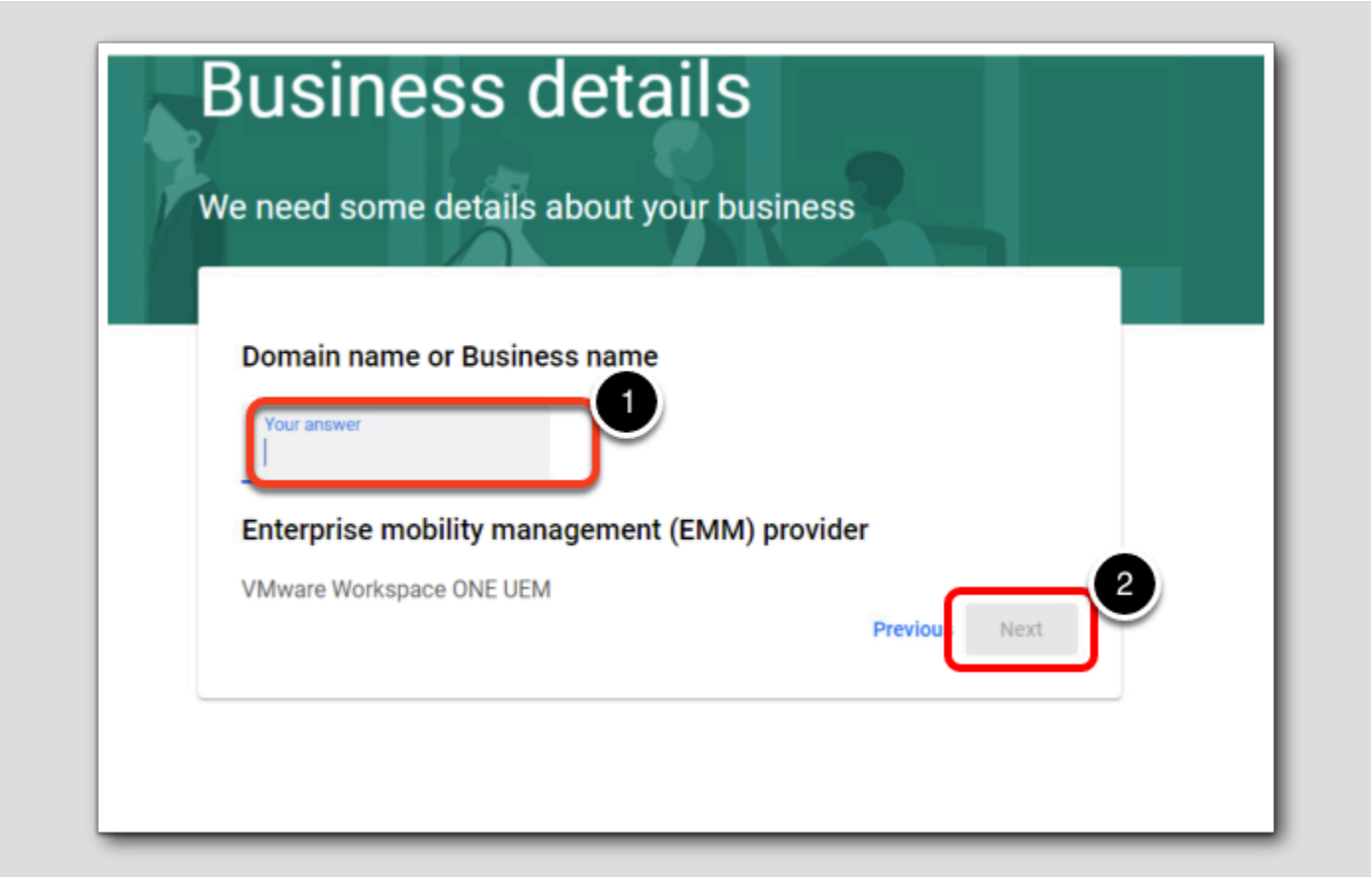


NOTE - The following changes have already been configured for you as part of the lab!

1. Confirm you are logged into your **Google Admin Account** that you wish to associate with your Android Enterprise configuration.

   NOTE - Once you register a Google Admin Account to Android Enterprise, you cannot disassociate your Google Admin Account from that Organization. Ensure the Google Admin Account shown is the account you wish to associate with your Organization!
2. Click **Get Started**

Provide your Organization Details (FOLLOW ALONG) [358]



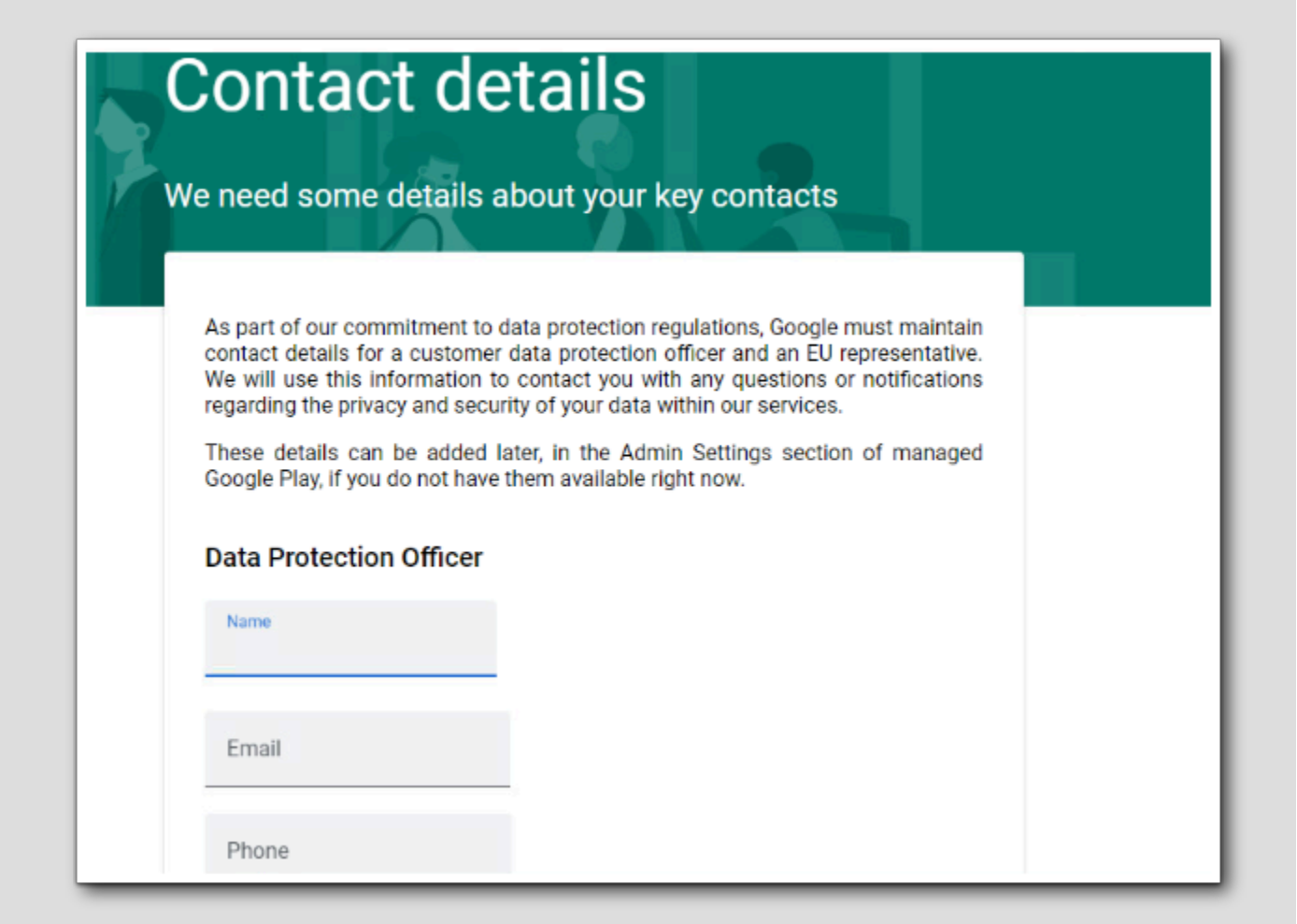
NOTE - The following changes have already been configured for you as part of the lab!

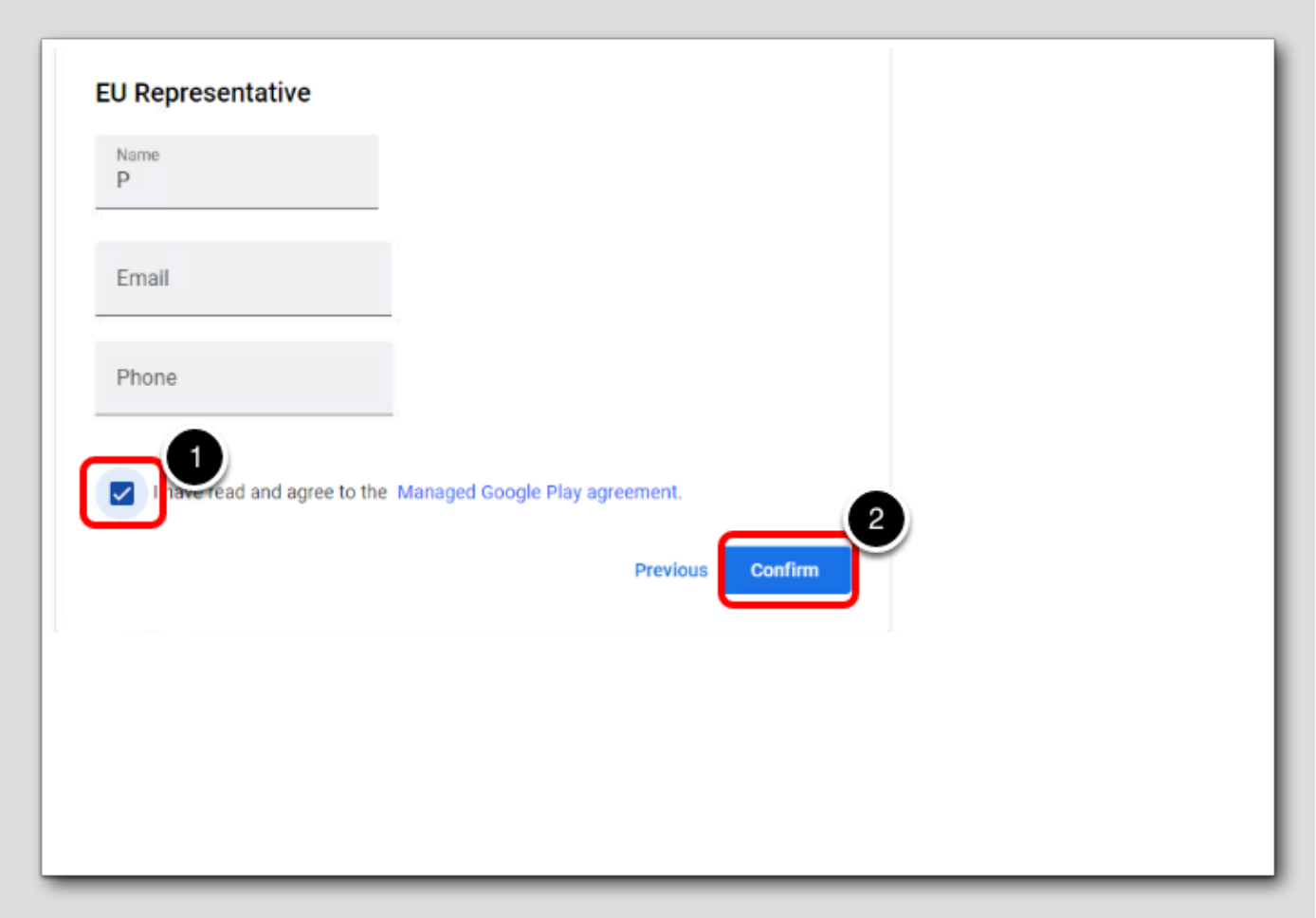
1. Enter your **Domain name or Business name**..
2. Click **Next**

Enter Contact Details (OPTIONAL)

[359]

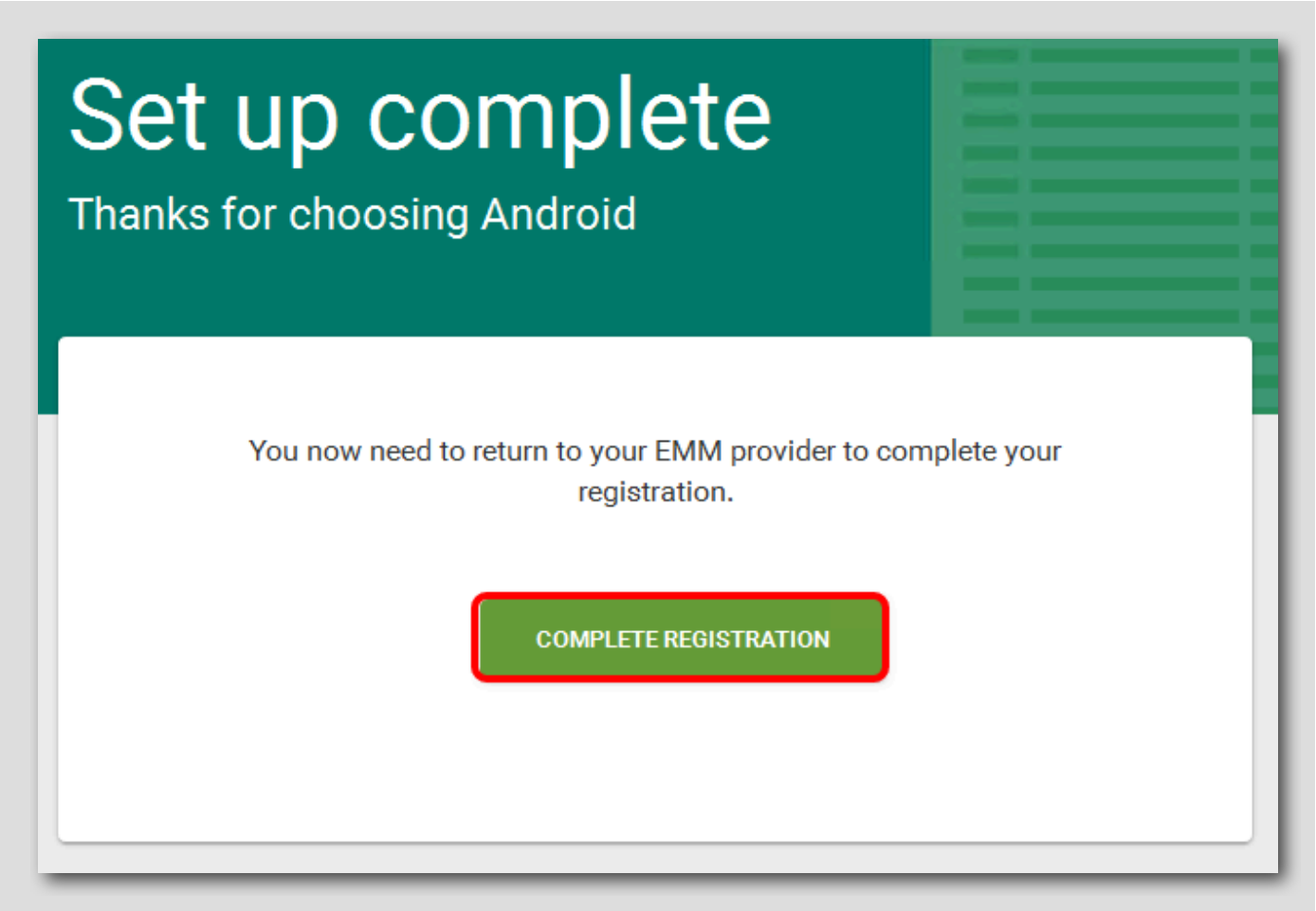
This information can be added later, in the Admin Settings section of managed Google Play console, if you do not have them available right now. Scroll down to agree to the listed Terms & Conditions, then select Confirm.




EU Representative
Name
P
Email
Phone
1
I have read and agree to the Managed Google Play agreement.
2
Previous
Confirm

Complete Registration (FOLLOW ALONG)

[360]

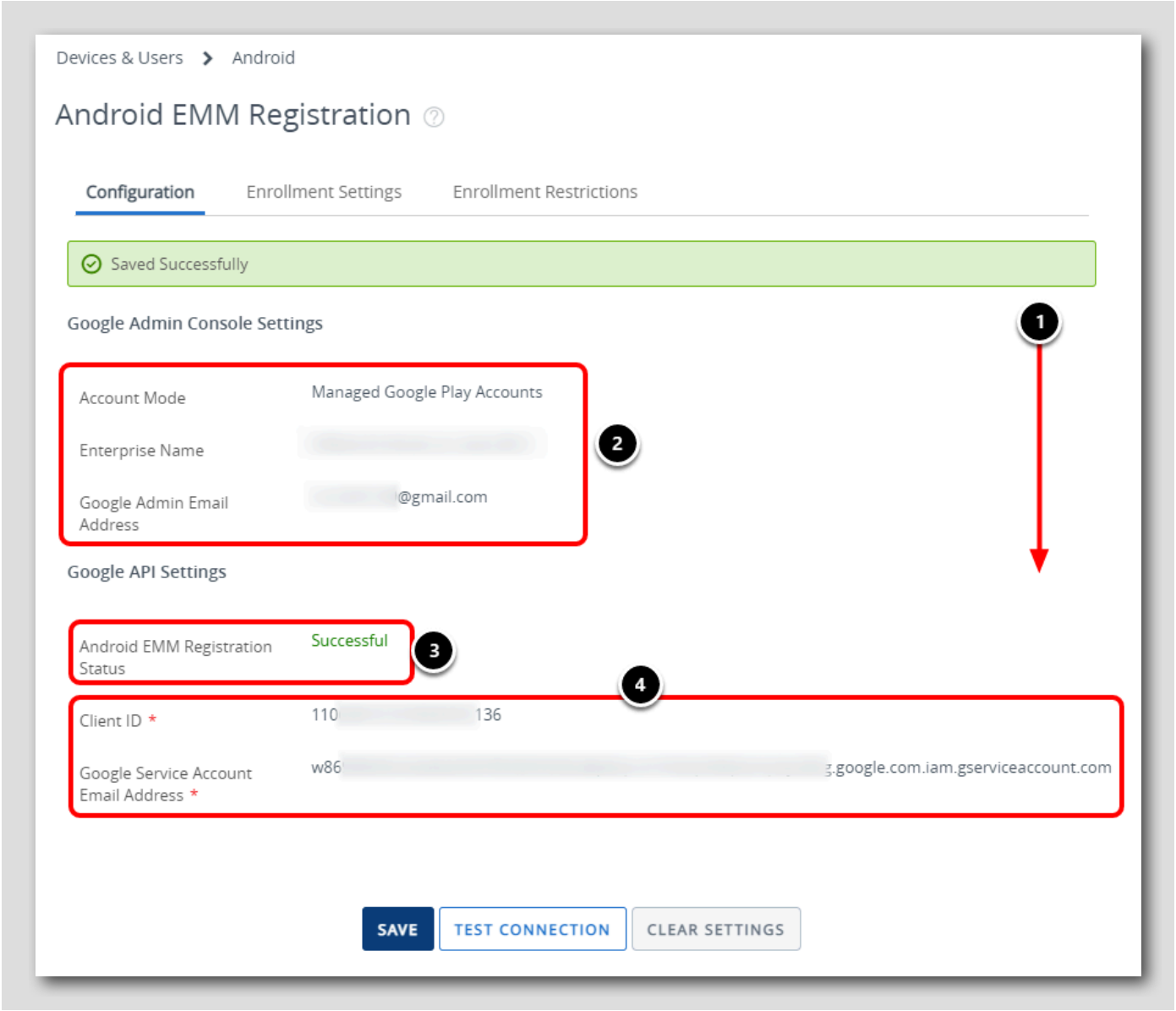


NOTE - The following changes have already been configured for you as part of the lab!

Click **Complete Registration** to return to the Workspace ONE UEM Android Enterprise configuration

Confirm Android Enterprise Integration (FOLLOW ALONG)

[361]



NOTE - The following changes have already been configured for you as part of the lab!

Back in the Workspace ONE UEM Console,

1. On the Android Enterprise Configuration page, scroll down until you see the **Google Admin Console Settings** and **Google API Settings** sections.
2. Under Google Admin Console Settings, note that the account information you provided during the Android Enterprise configuration step is displayed here.
3. Confirm that **your Android Enterprise Registration Status** is shown as **Successful**.
4. Note that the **Client ID** and **Google Service Account Email Address** have been created and configured for you automatically. No additional configurations with Android Enterprise or the Google Developers Console are required.

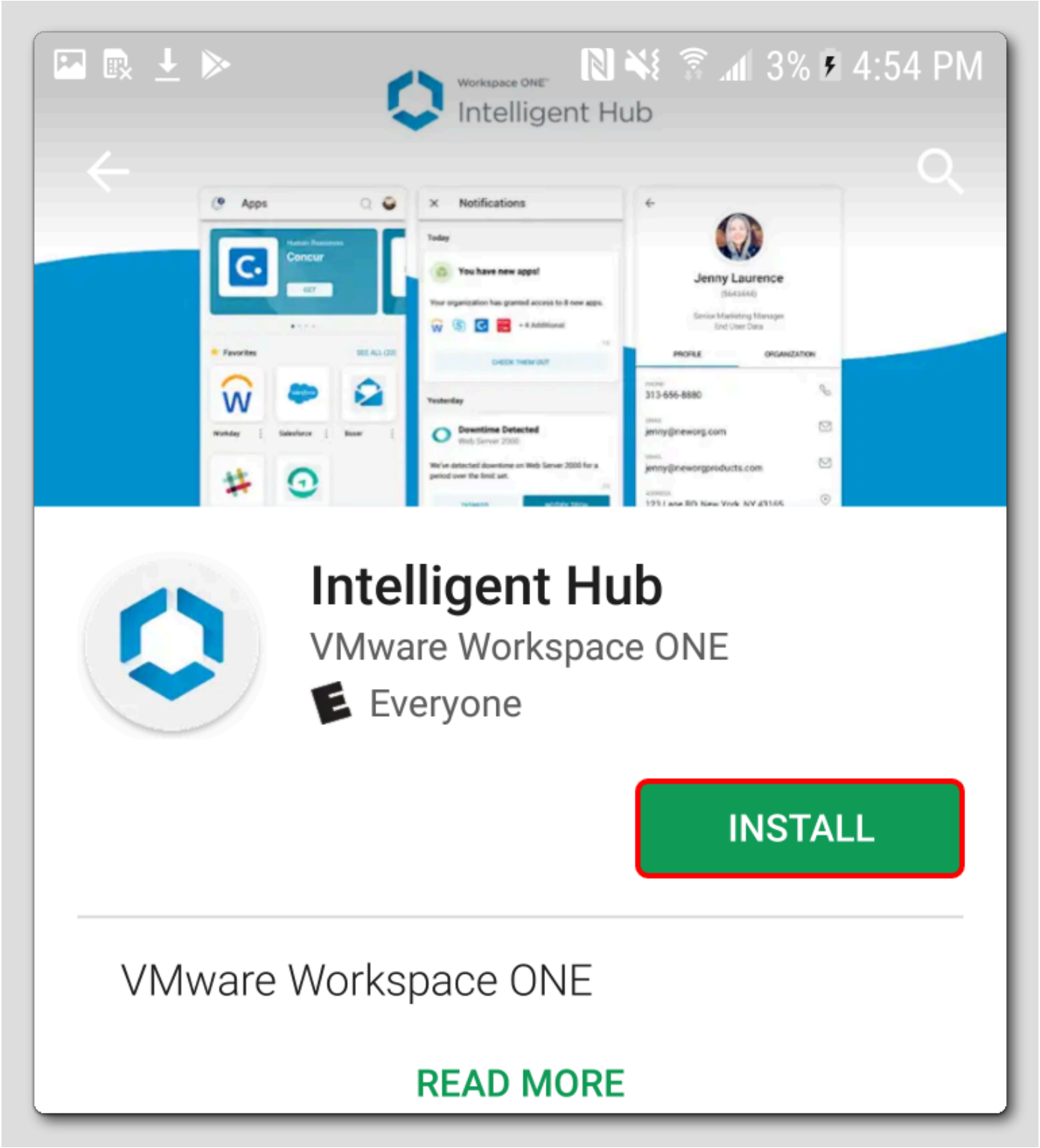
Your Organization Group is now successfully configured with Android Enterprise!

Device Enrollment with Android Enterprise (Work Profile) [362]

In this section, we will be enrolling your device with Workspace ONE UEM and get it set up with Android Enterprise.

NOTE - The screenshots in this article will differ depending on the make and model of the Android device you are using.

Download the Workspace ONE Intelligent Hub (IF NEEDED)


3% 4:54 PM
Workspace ONE
Intelligent Hub
Apps
Concur
Favorites
Notifications
Today
You have new apps!
Yesterday
Downtime Detected
Jenny Laurence
PROFILE
ORGANIZATION
313-656-8880
jenny@neworg.com
jenny@neworgproducts.com
Intelligent Hub
VMware Workspace ONE
Everyone
INSTALL
VMware Workspace ONE
READ MORE

If you do not have the Workspace ONE Intelligent Hub app on your device, you will need to download it the app before continuing.

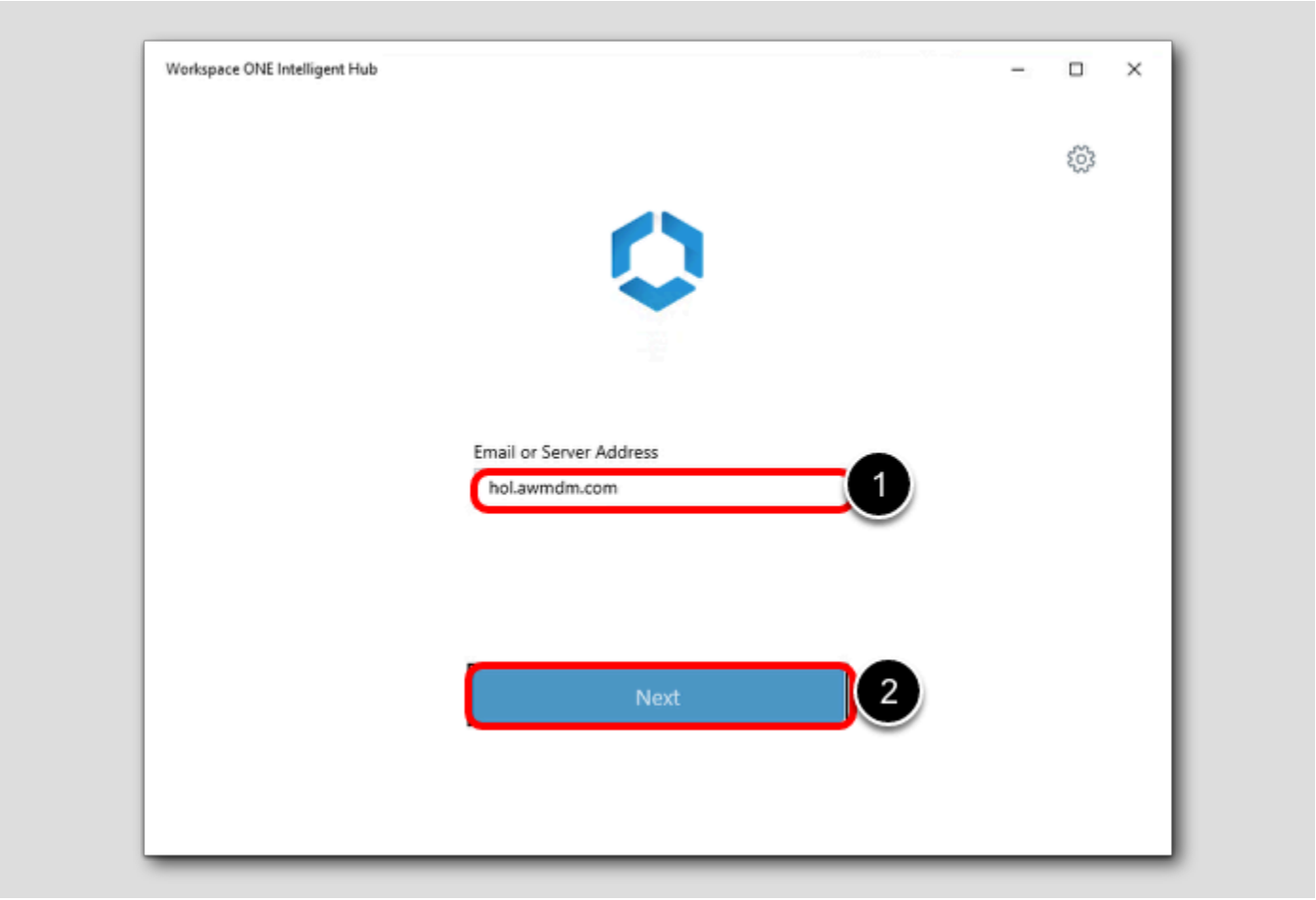
To install the Workspace ONE Intelligent Hub app, you can open the Google Play Store app and download the free **Workspace ONE Intelligent Hub** app or navigate to **`https://www.getwsone.com`** in your device browser and follow the **Get it on Google Play** link to the **Workspace ONE Intelligent Hub** page in the Google Play Store.

Launching the Workspace ONE Intelligent Hub App [364]

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

Provide the Workspace ONE UEM Server URL

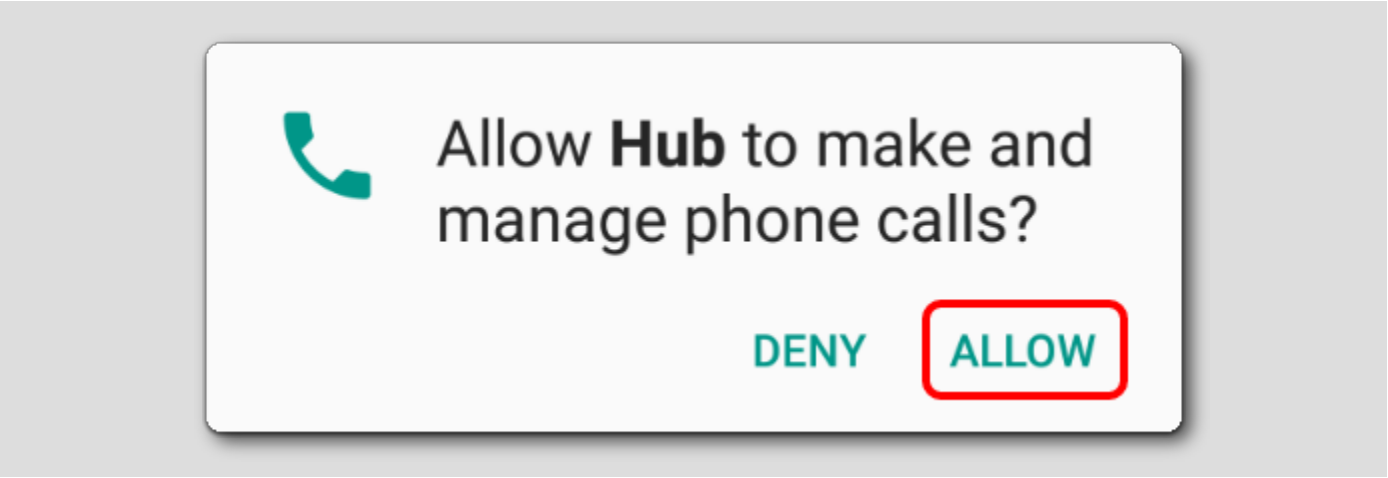
[365]



1. Enter **`hol.awmdm.com`** or the Server URL.
2. Tap **NEXT**.

Allow Phone Permission for Hub (IF NEEDED)

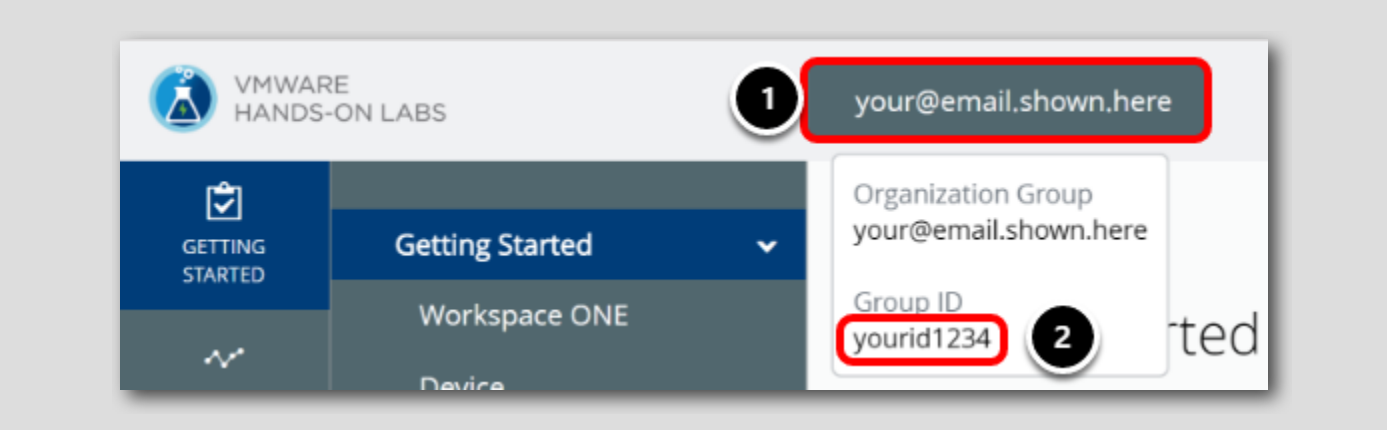
[366]



Tap **Allow**.

Find your Group ID from Workspace ONE UEM Console

[367]

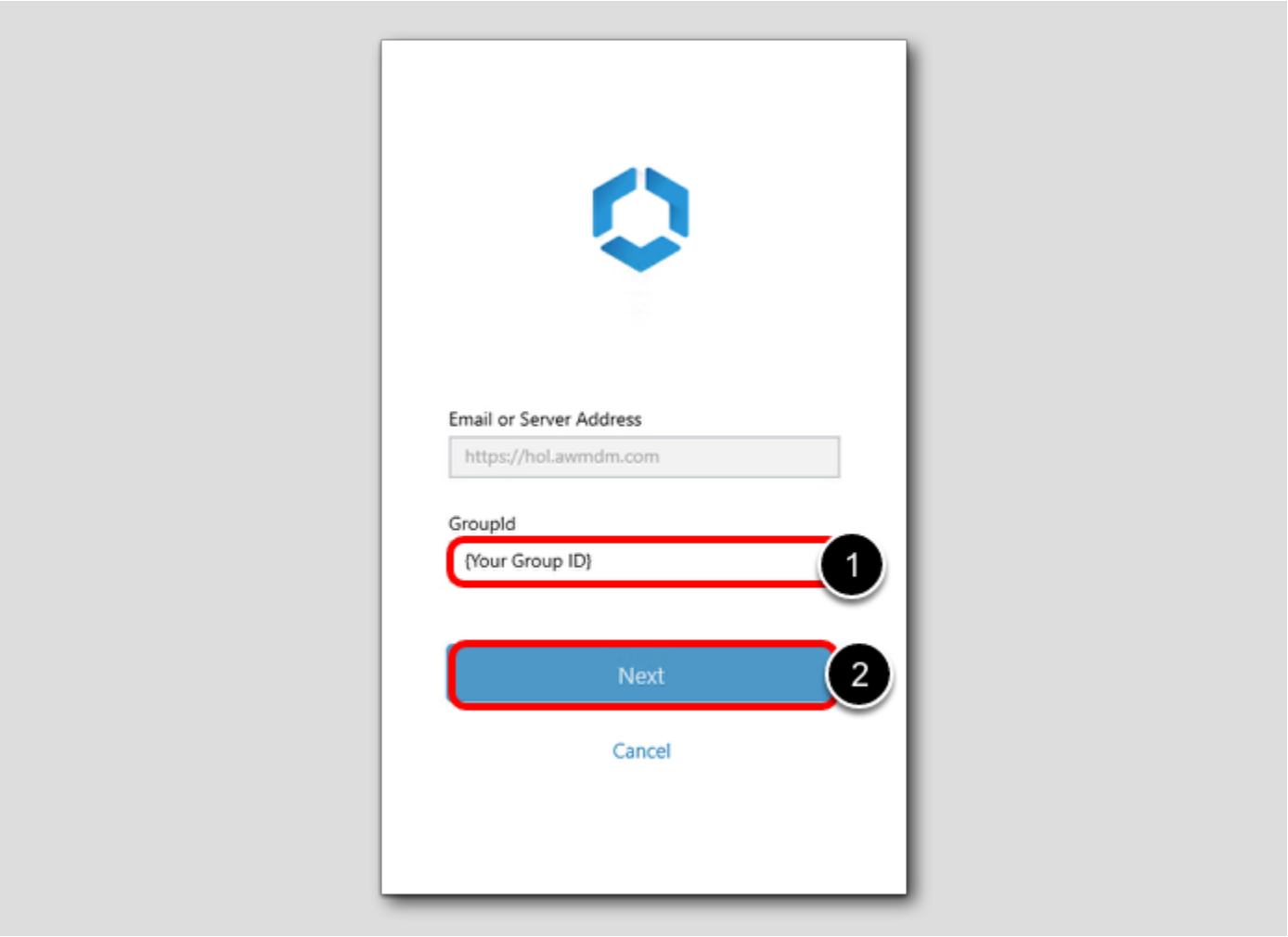


The next step is to make sure you know what your **Organization Group ID** is.

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

Attach the Workspace ONE Intelligent Hub to the HOL Sandbox

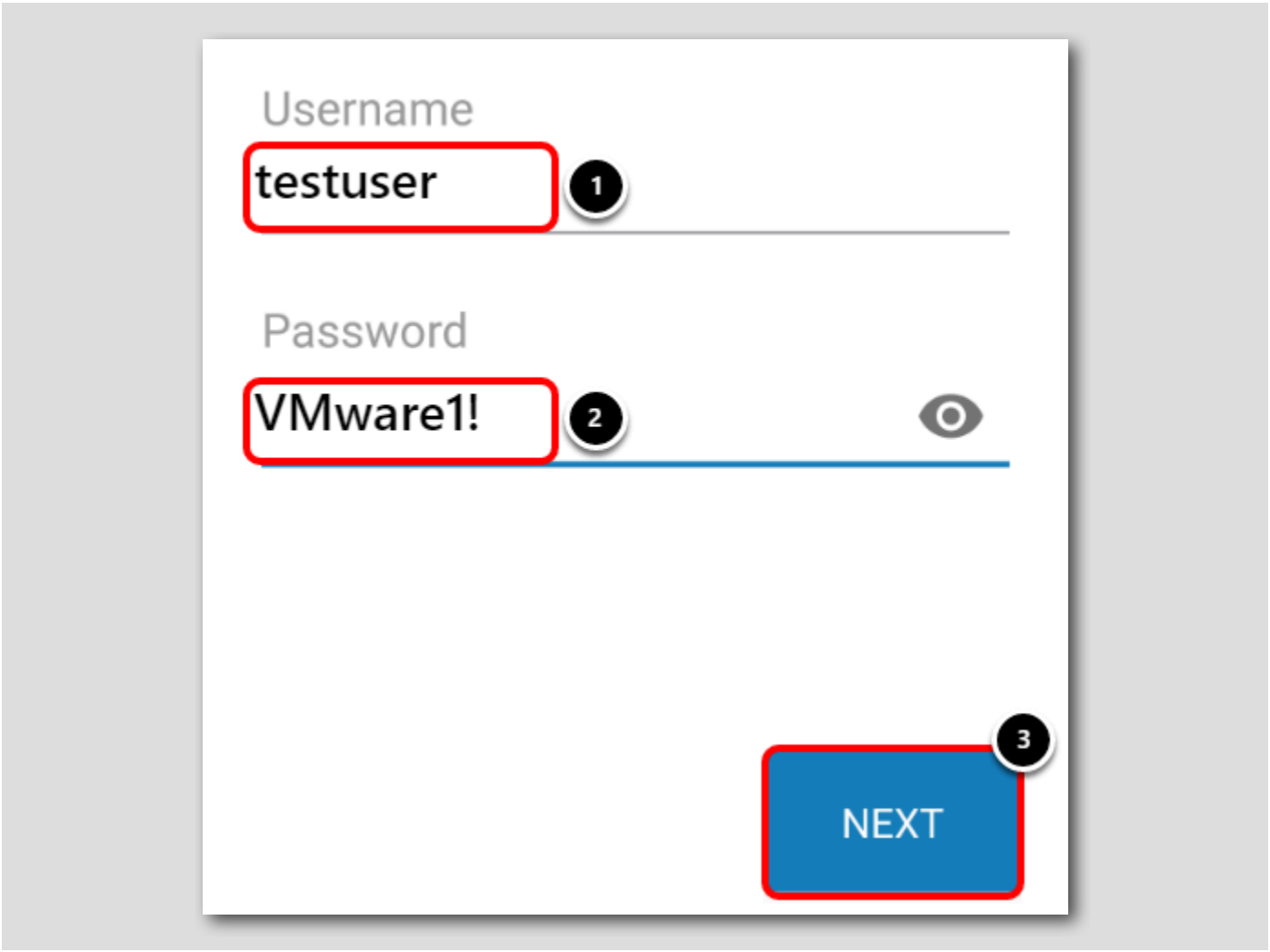
[368]



1. Enter your **Group ID** for the **Group ID** field. This was noted previously in the **Finding your Group ID** step.
2. Tap **NEXT**.

Provide User Credentials

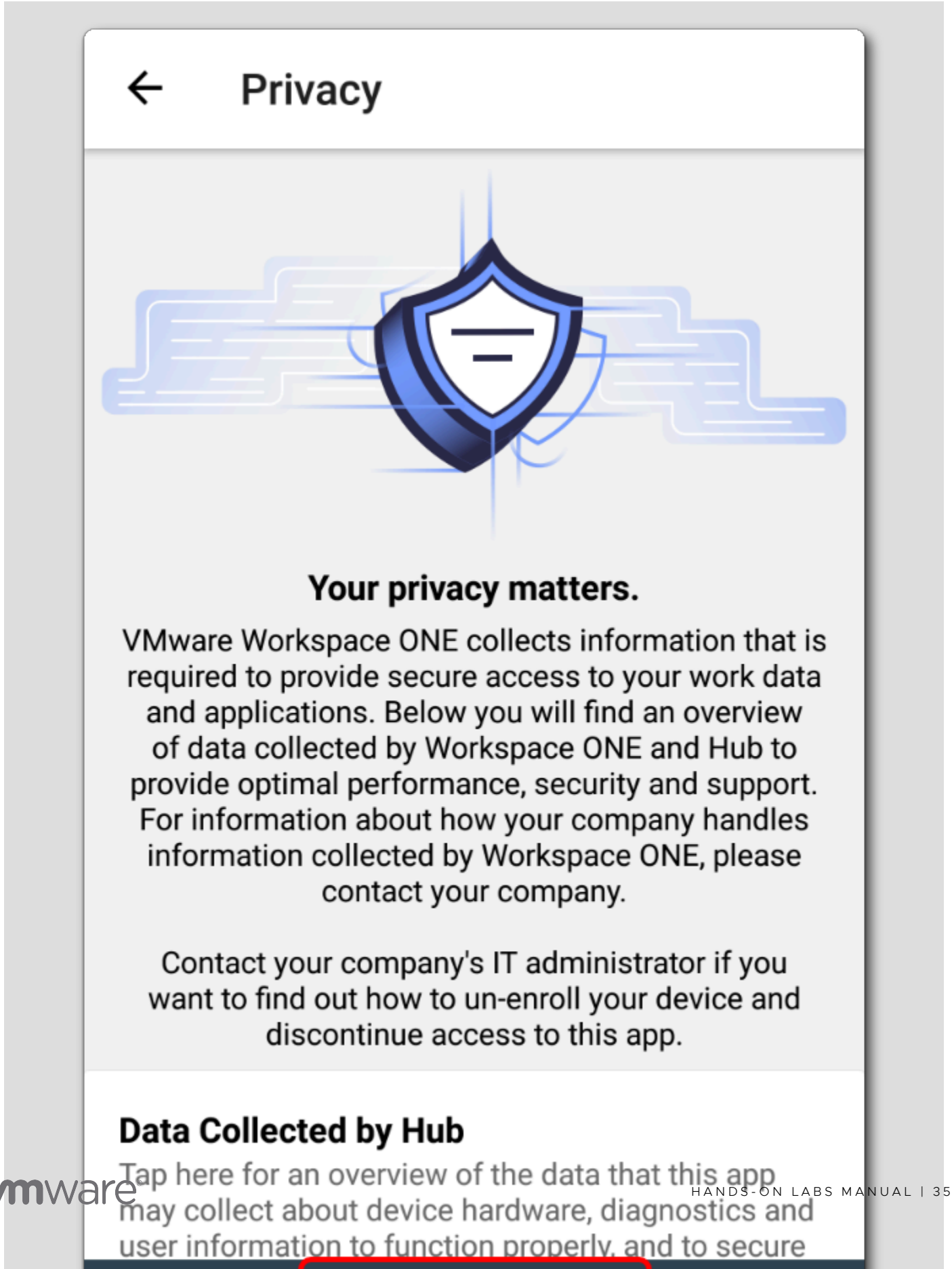
[369]



1. Enter **`testuser`** for the Username field.
2. Enter **`VMware1!`** for the Password field.
3. Tap Continue.

Confirm the Privacy Policy

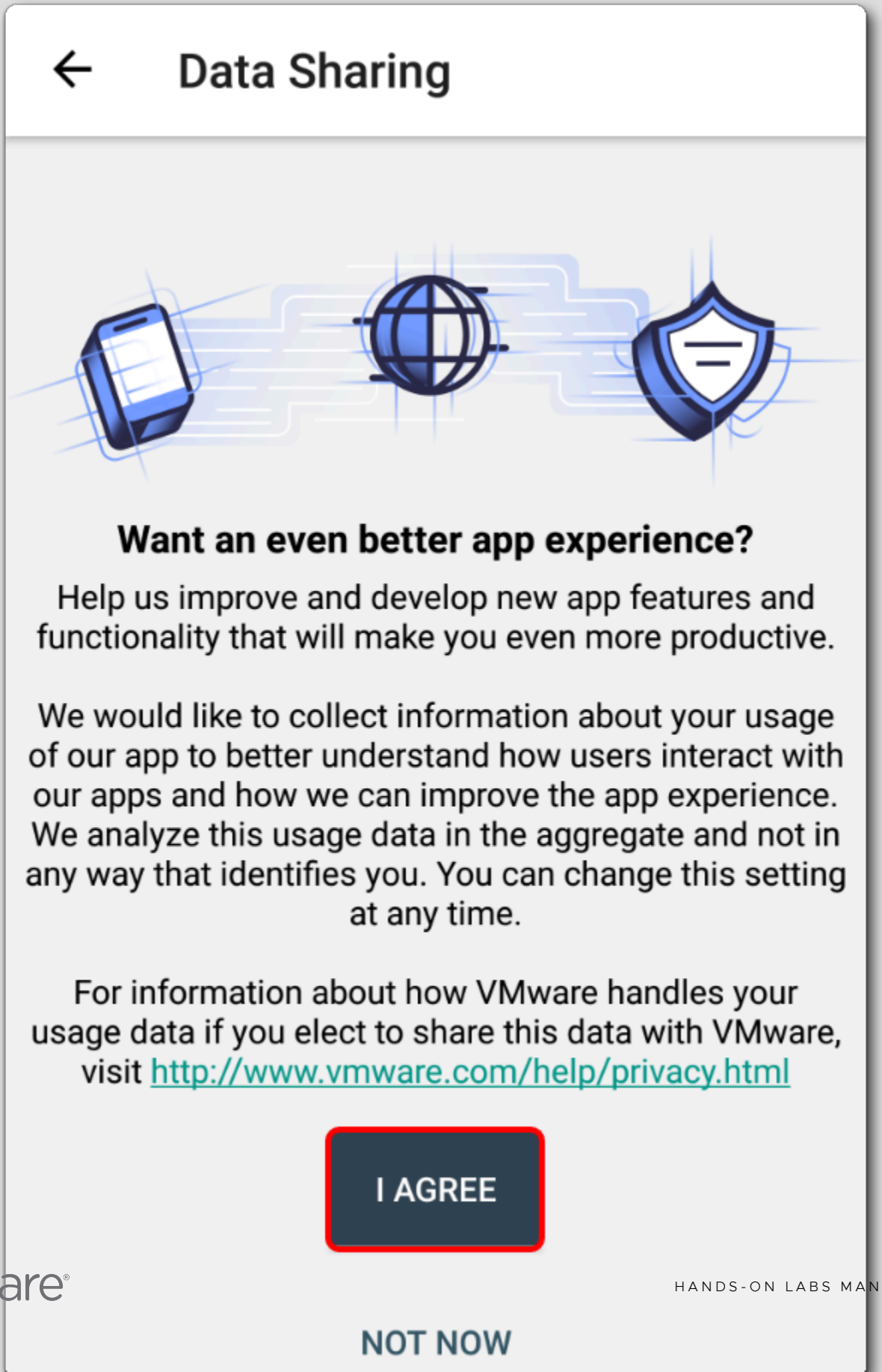
[370]


Privacy
Your privacy matters.
VMware Workspace ONE collects information that is required 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.
Contact your company's IT administrator if you want to find out how to un-enroll your device and discontinue access to this app.
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

Tap **I Understand** for the Privacy Policy.

Accept the Data Sharing Policy

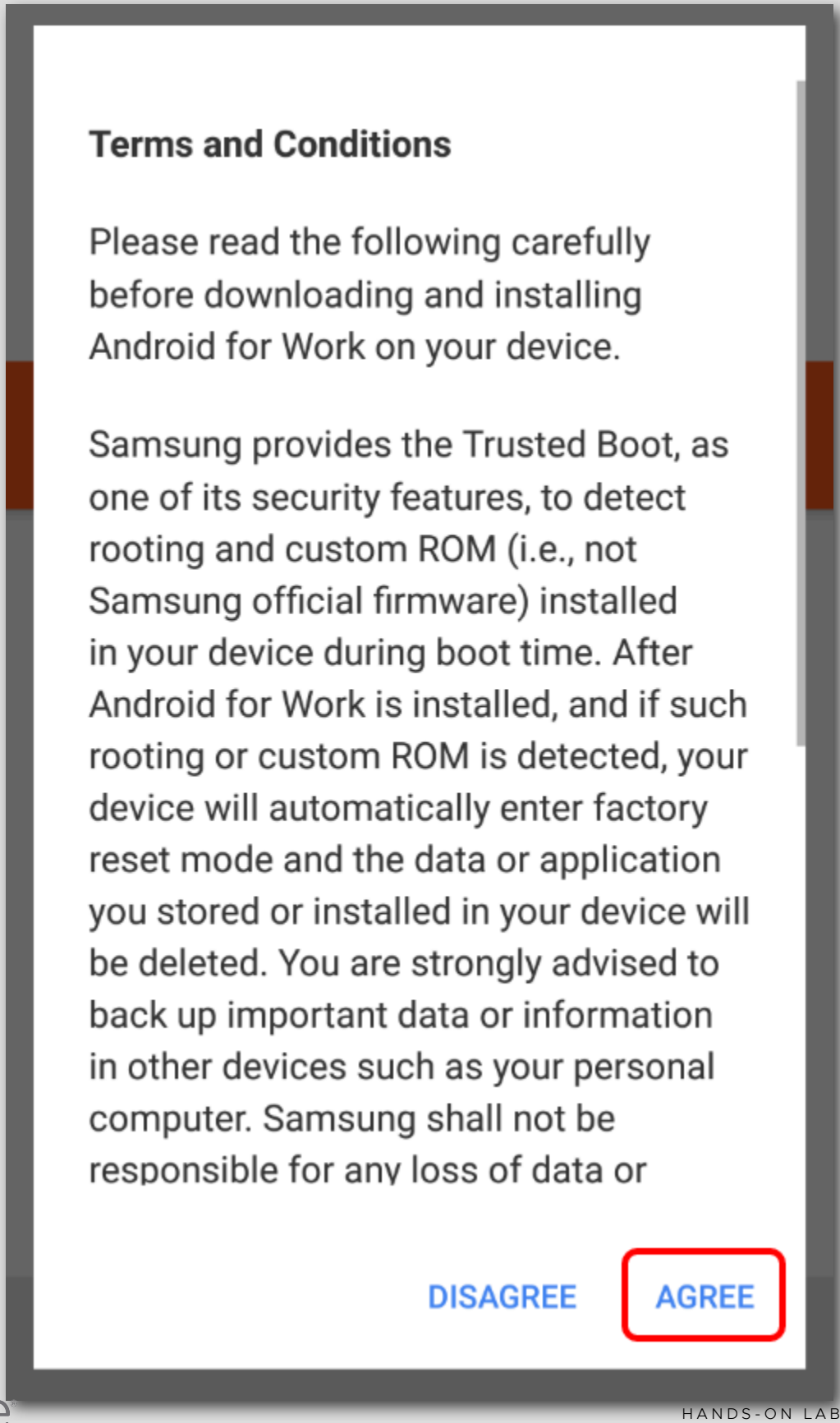
[371]


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 to better understand how users interact with our apps and how we can improve the app experience. We analyze this usage data in the aggregate and not in any way that identifies you. 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 http://www.vmware.com/help/privacy.html
I AGREE
NOT NOW

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

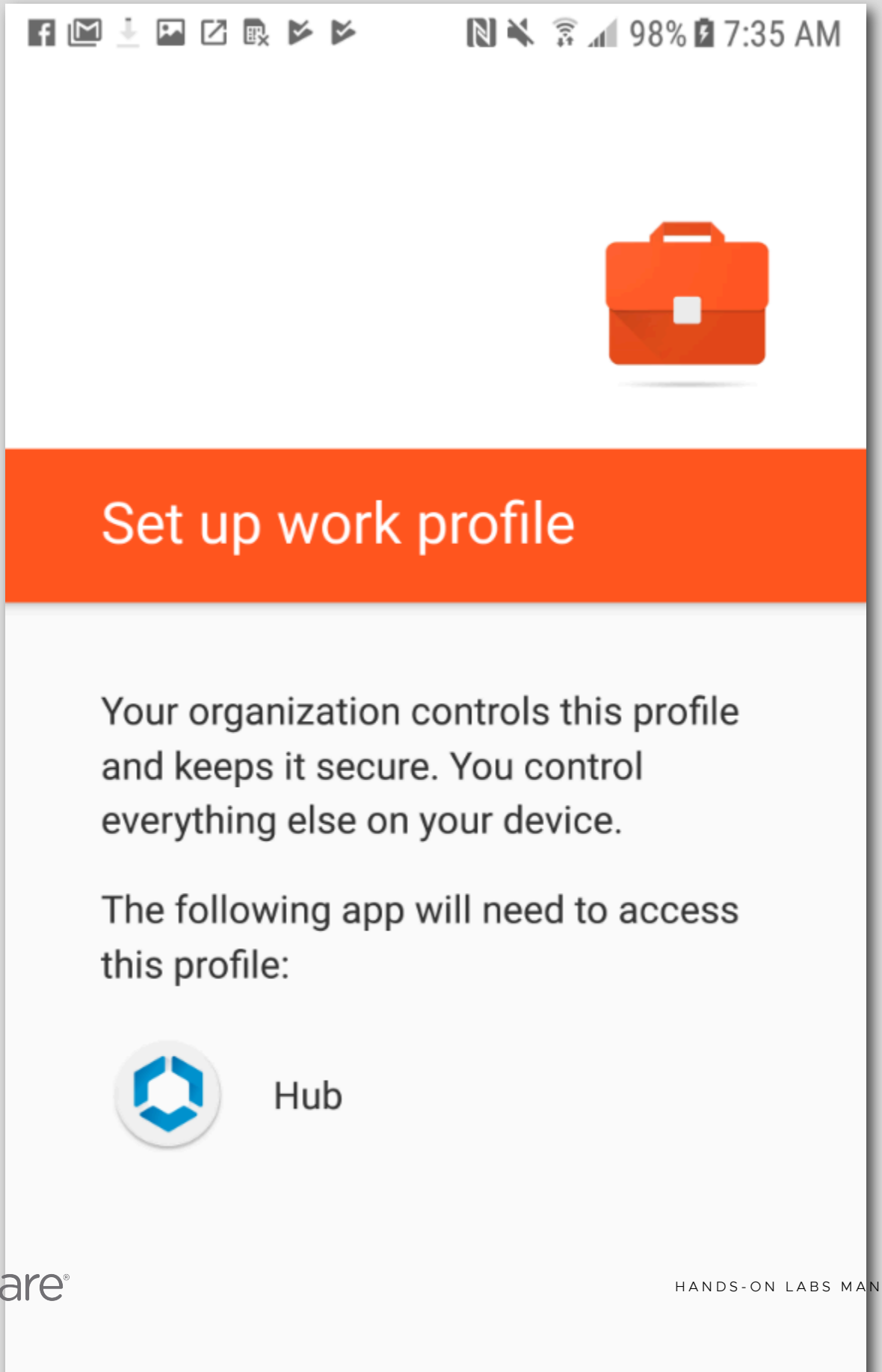
Accept the Terms and Conditions

[372]


Terms and Conditions
Please read the following carefully before downloading and installing Android for Work on your device.
Samsung provides the Trusted Boot, as one of its security features, to detect rooting and custom ROM (i.e., not Samsung official firmware) installed in your device during boot time. After Android for Work is installed, and if such rooting or custom ROM is detected, your device will automatically enter factory reset mode and the data or application you stored or installed in your device will be deleted. You are strongly advised to back up important data or information in other devices such as your personal computer. Samsung shall not be responsible for any loss of data or
DISAGREE
AGREE

Tap **Agree**.

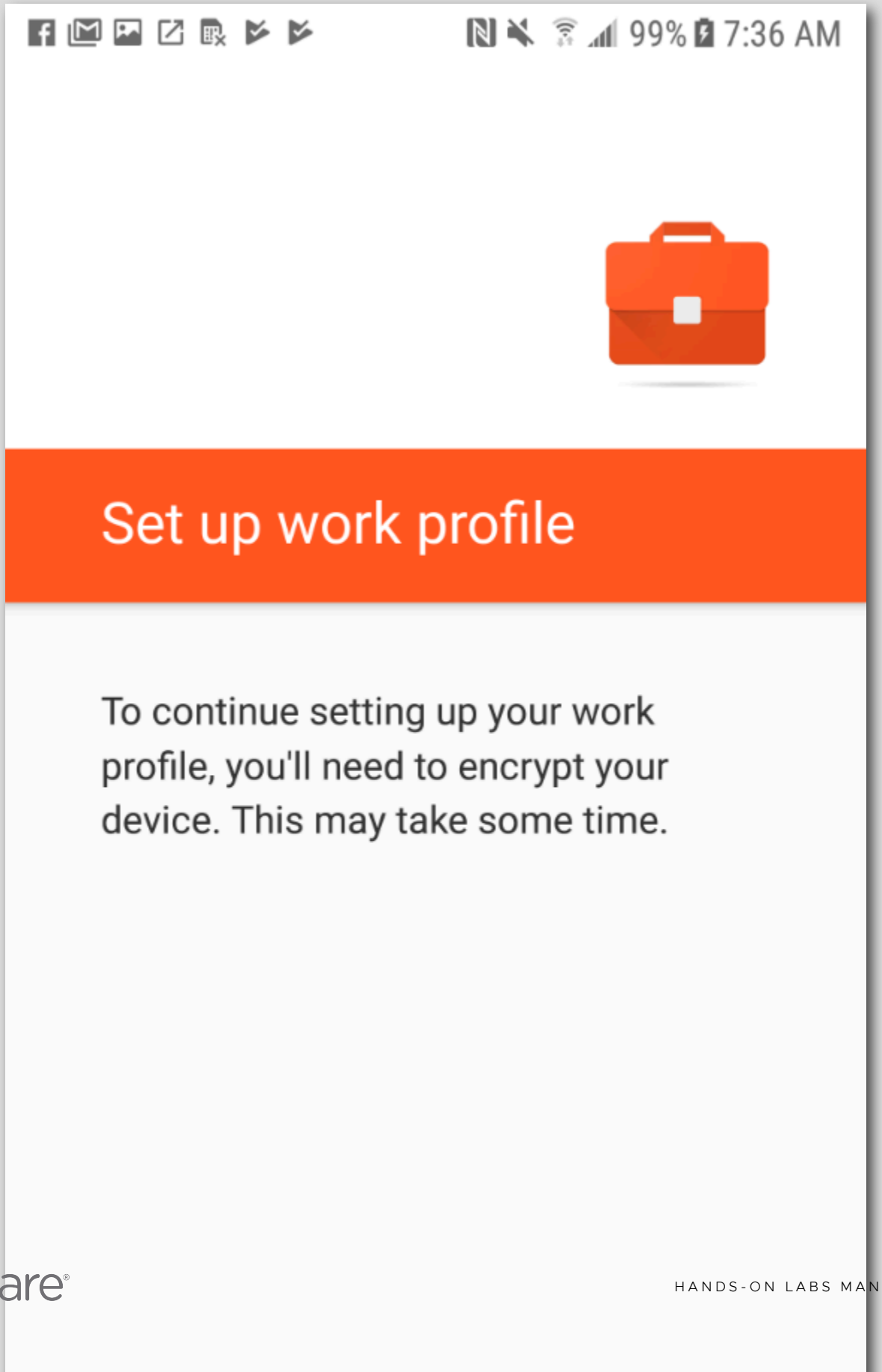
Set Up the Android Enterprise Work Profile


98% 7:35 AM
Set up work profile
Your organization controls this profile and keeps it secure. You control everything else on your device.
The following app will need to access this profile:
Hub

Tap **NEXT**.

NOTE - This may take some time, please be patient while the Setup process completes.

(Optional) Device Encryption

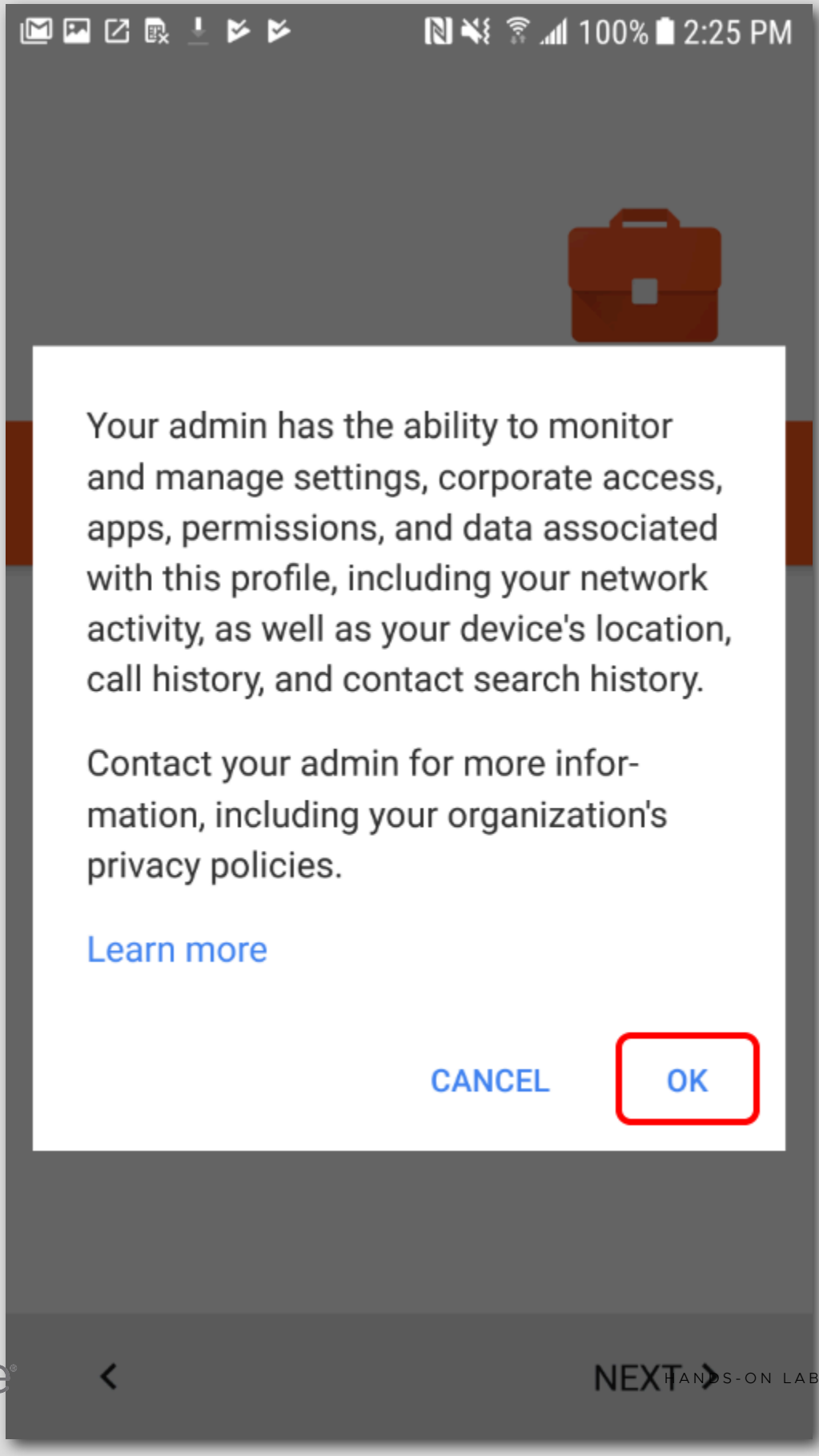

99% 7:36 AM
Set up work profile
To continue setting up your work profile, you'll need to encrypt your device. This may take some time.

If your device is encrypted, you will not see this page and can continue to the next step.

If your device is not encrypted, you will be prompted to encrypt it and must tap ENCRYPT to continue. Encrypting the device can take several minutes or potentially longer depending on the amount of data on the device.

Administrator Rights

[375]

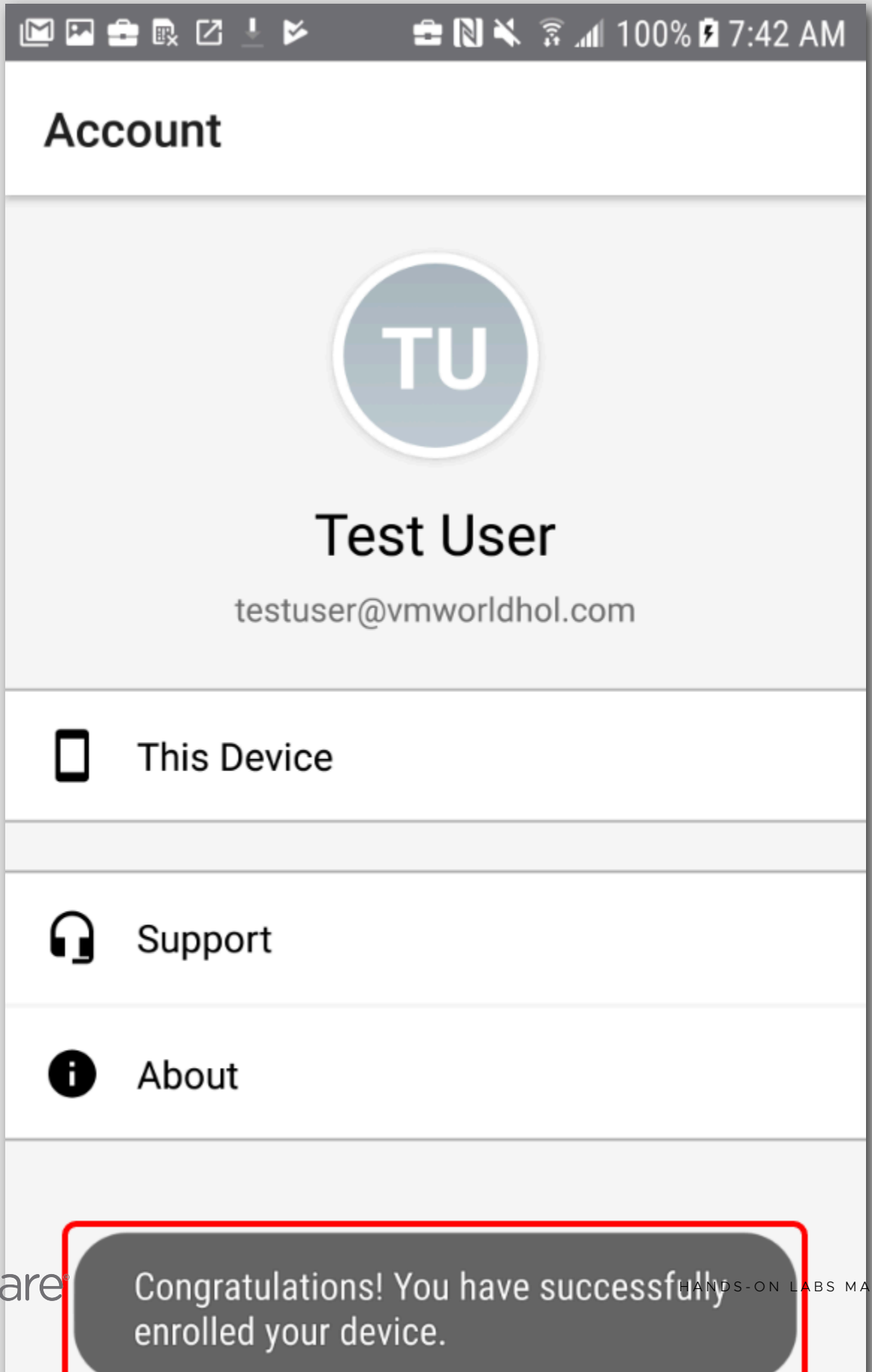

100% 2:25 PM
Your admin has the ability to monitor and manage settings, corporate access, apps, permissions, and data associated with this profile, including your network activity, as well as your device's location, call history, and contact search history.
Contact your admin for more information, including your organization's privacy policies.
Learn more
CANCEL
OK
NEXT

Tap OK to confirm the Privacy Policy.

NOTE - Enrollment time may vary depending on your network connectivity. Typically, it takes around 1 minute to complete. Please be patient while this process completes.

IMPORTANT - During the enrollment process, you will see several processing screens. Please note that you do not need to interact with the device further until you see the Workspace ONE Intelligent Hub app confirming your enrollment (next page).

Confirm Device Enrollment

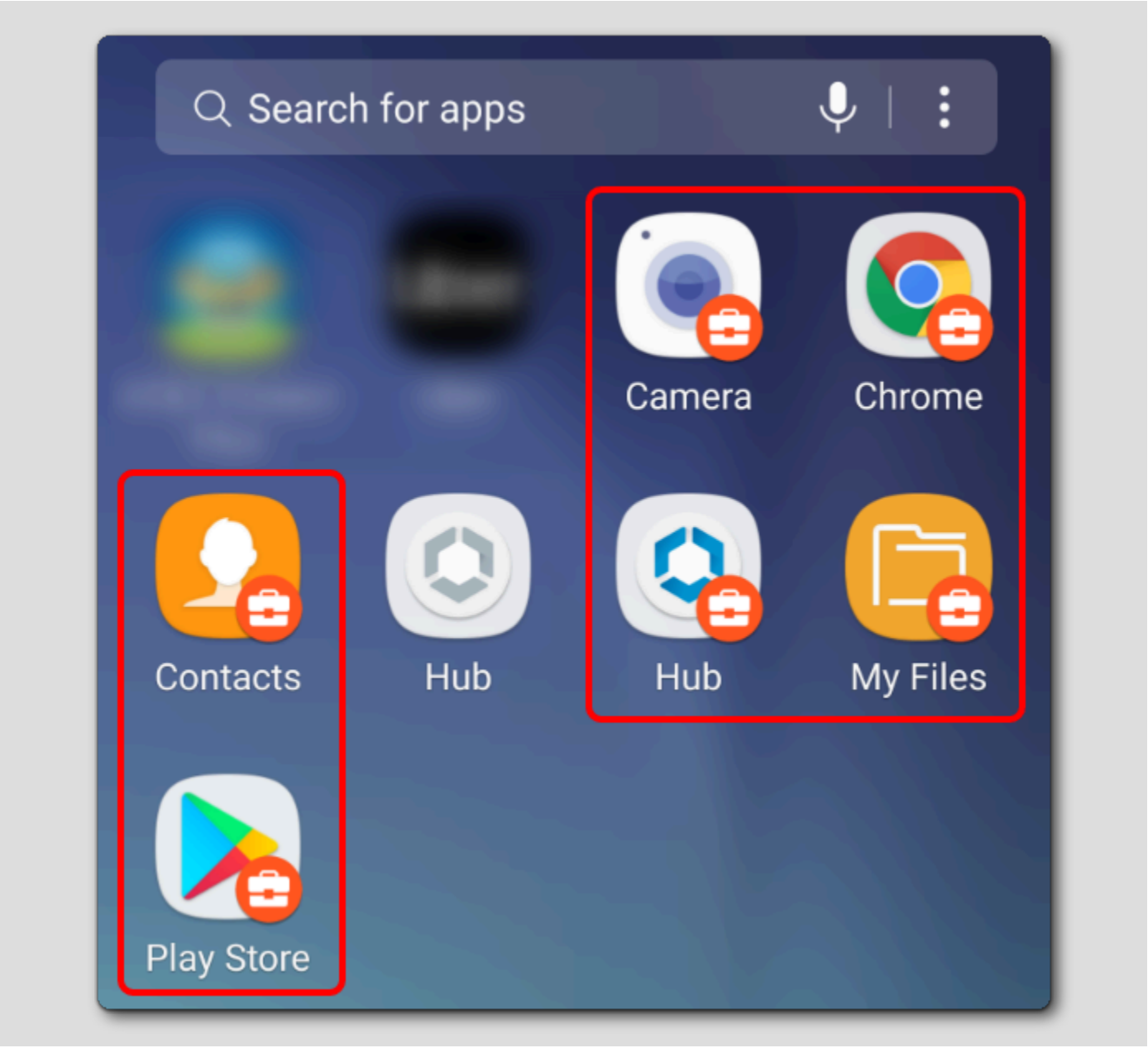

100% 7:42 AM
Account
TU
Test User
testuser@vmworldhol.com
This Device
Support
About
Congratulations! You have successfully enrolled your device.

You have now completed enrolling your device using the Workspace ONE Intelligent Hub. After the enrollment process completes, the Workspace ONE Intelligent Hub app will display the notification **Congratulations! You have successfully enrolled your device.**

You can now **Exit** the Workspace ONE Intelligent Hub app.

Badged Apps

[377]



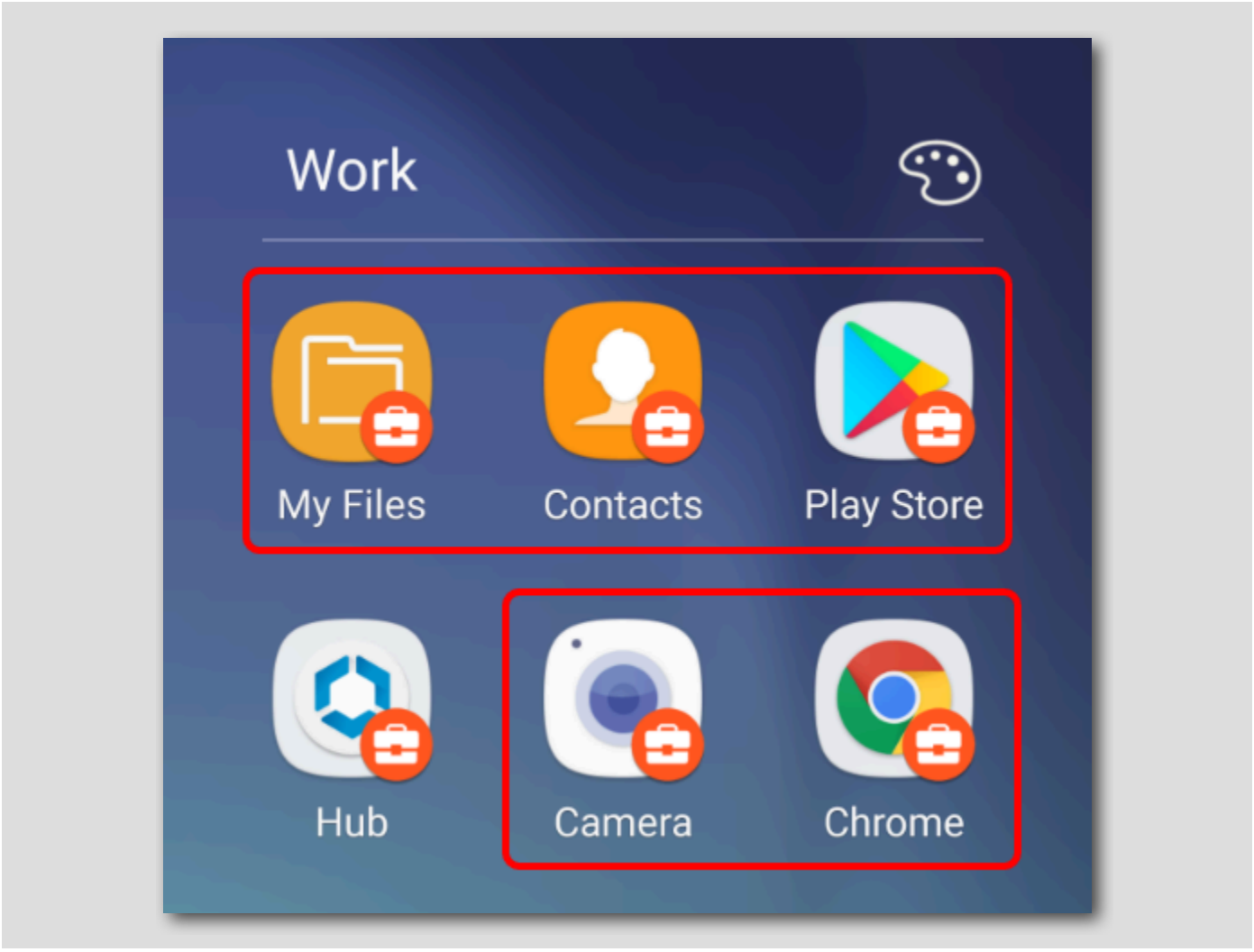
On your Android device, you should now see the new Work applications. Android Enterprise apps are differentiated by an orange briefcase icon also referred to as Badged Apps.

In the Applications view, your Work apps and Personal apps are shown in a unified launcher. For example, your device will show both a personal icon for Google Chrome and a separate icon for Work Chrome denoted by the badge. The Workspace ONE Intelligent Hub is badged and exists only within the Work Profile data space.

IMPORTANT - There is no control over personal apps nor will the Hub app have access to personal information. There are a handful of system apps that come with the Work Profile by default such as Work Chrome, Google Play, Google settings, Contacts and Camera.

Work Container

[378]



On some devices, you may also notice the Work container on your device depending on the OS version. This Work container can be utilized for quick access to your Work (Badged) Apps.

Android Enterprise Profiles

[379]

In this section, we are going to create Android Enterprise profiles to modify devices restrictions and to assist in protecting sensitive data. Profiles serve many different purposes, from letting you enforce corporate rules and procedures to tailoring and preparing Android Enterprise capable devices for how they will be used.

IMPORTANT: If your device is enrolled with Android Enterprise, then ONLY Android Enterprise profiles will take effect on the device. Android device profiles will NOT take effect.

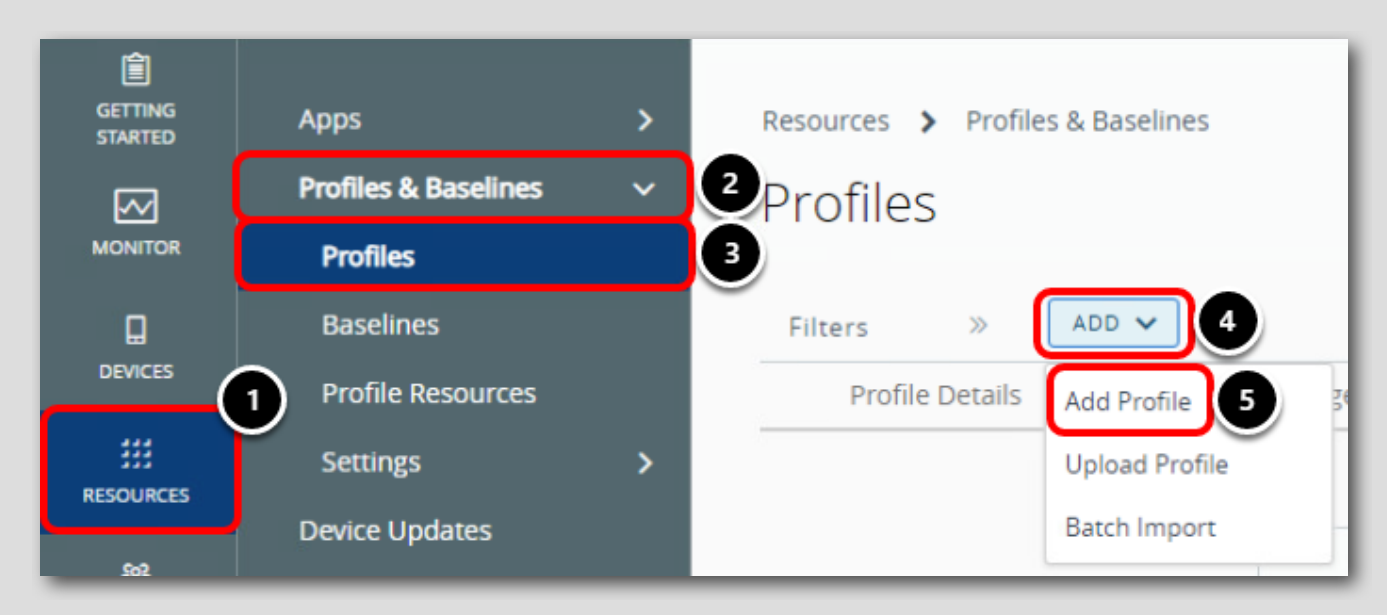
Restriction Profile Overview

[380]

Restriction profiles provide a second layer of device data protection by allowing you to specify and control how, when and where your employees use their devices. The Restriction profiles lock down native functionality of Android Enterprise devices and vary based on device enrollment.

Create a New Profile

[381]

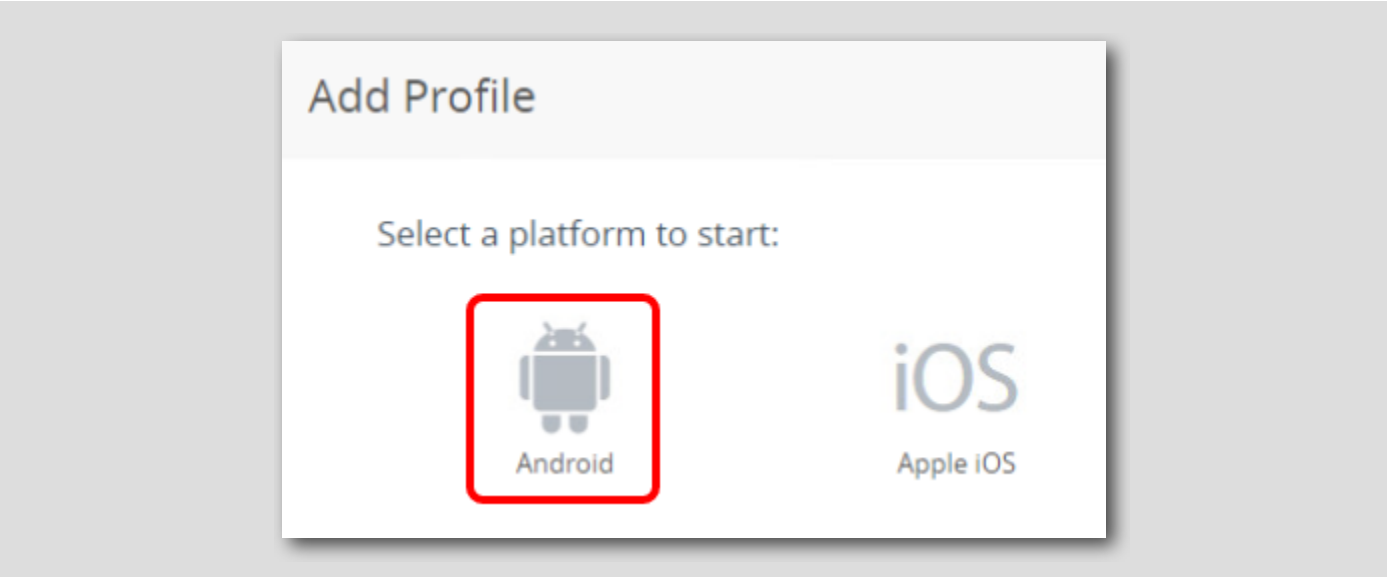


In the Workspace ONE UEM Administrator Console,

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

Select the Android Platform

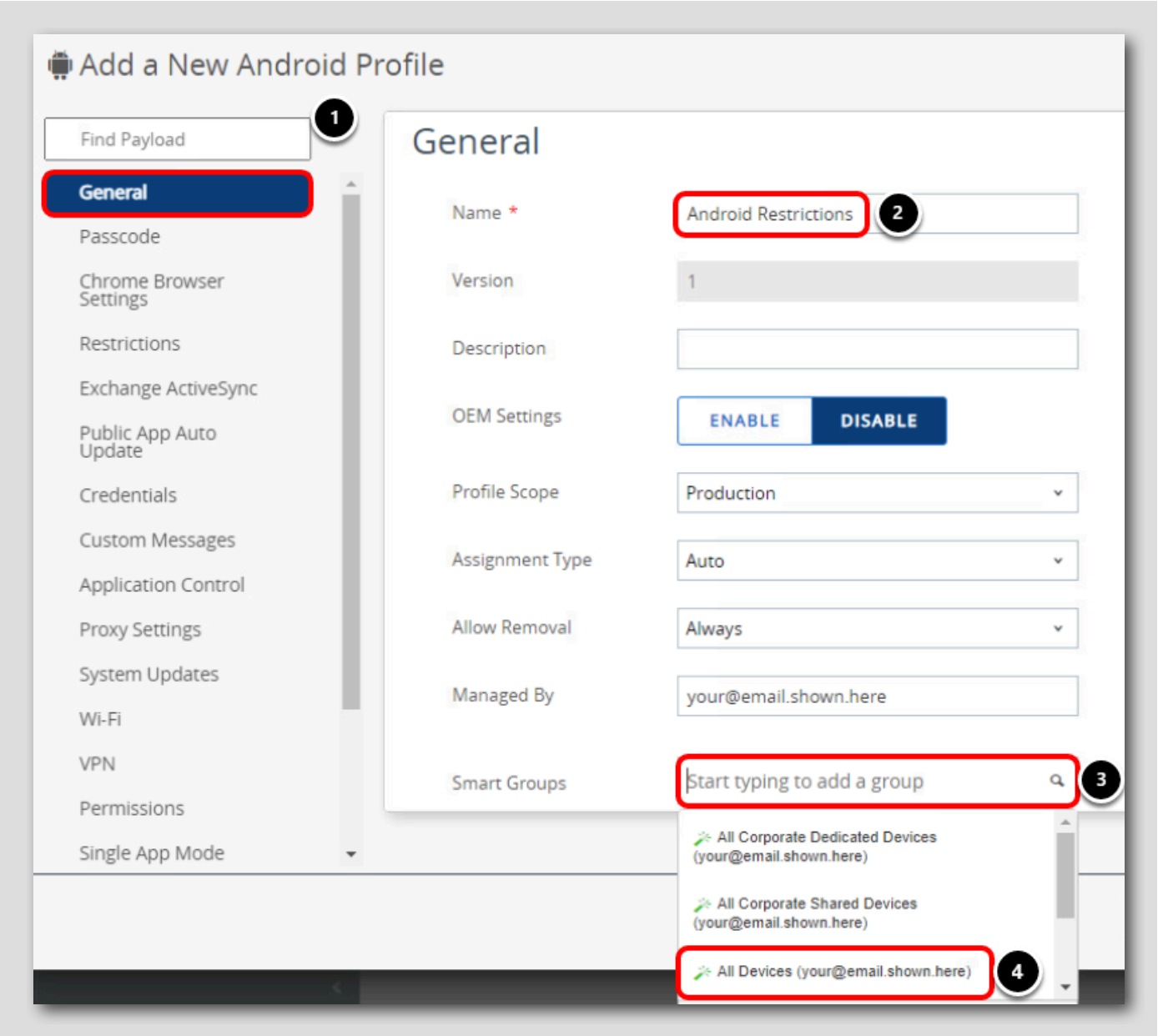
[382]



Click **Android**

Configure the General Settings

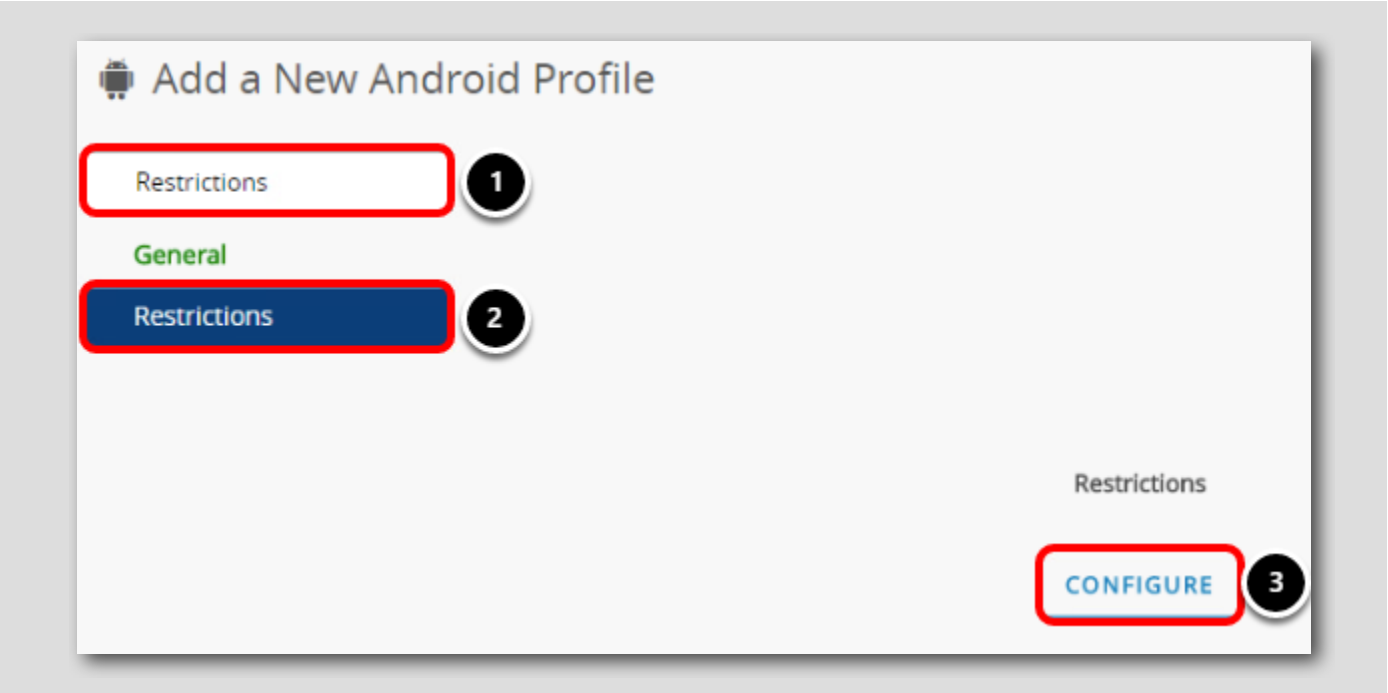
[383]



1. Ensure the **General** payload is selected
2. Enter **`Android Restrictions`** for the Name field
3. Click Smart Groups to display the list of available assignments.
4. Select the **All Devices (your@email.shown.here)** group.

Configure Restrictions

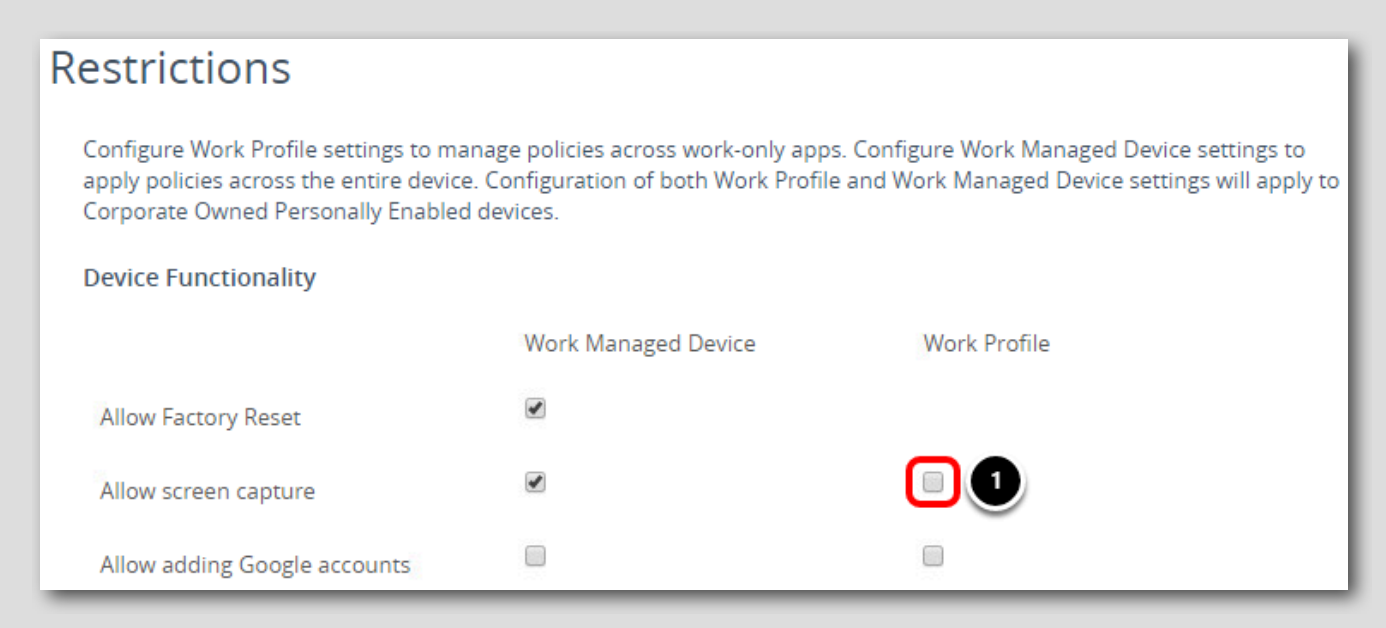
[384]



1. Enter **Restrictions** in the payload search box
2. Click the **Restrictions** payload
3. Click **Configure**

Configure Screen Capture Restrictions

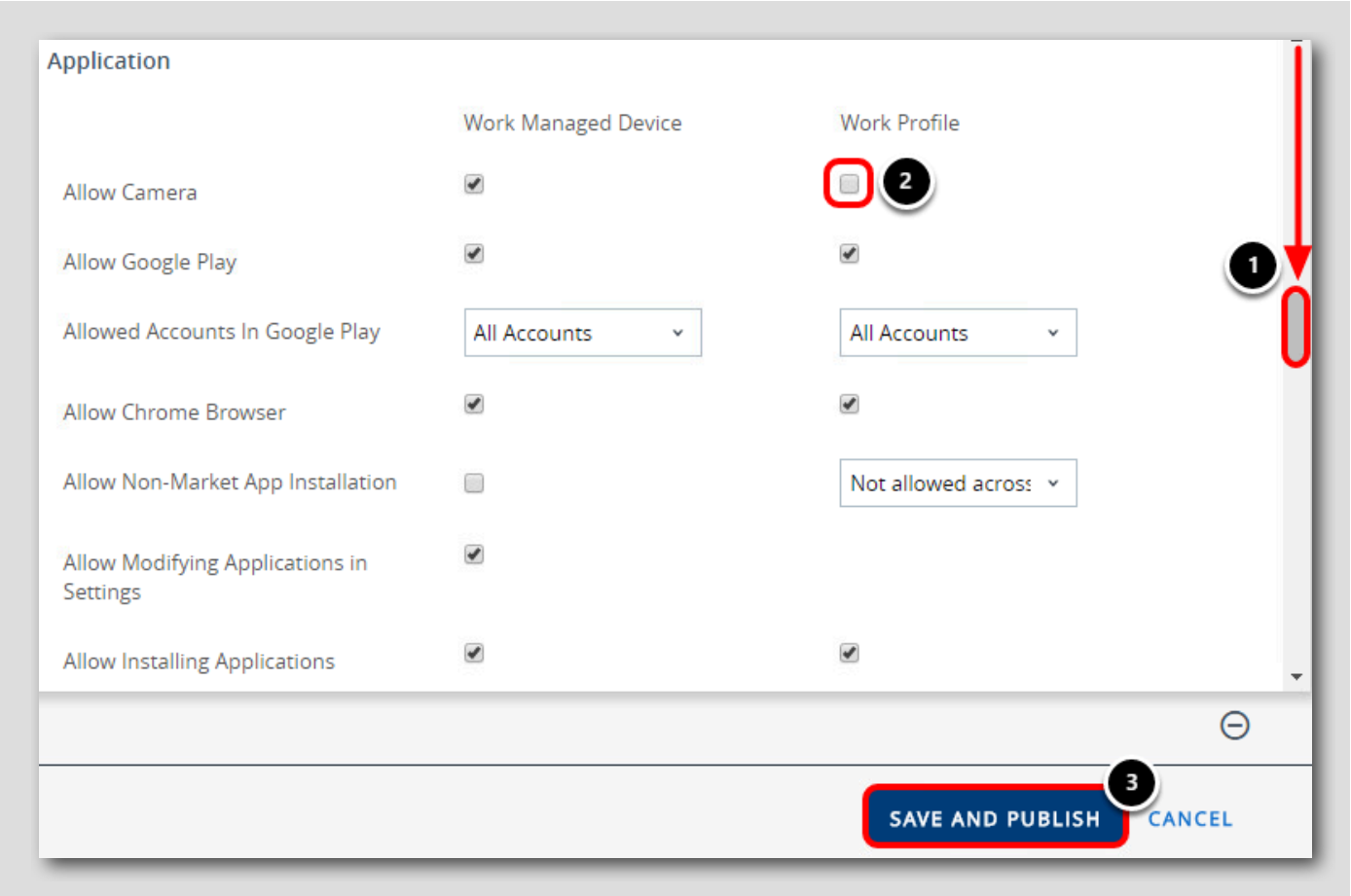
[385]



Uncheck the **Allow Screen Capture** checkbox for the **Work Profile** column.

Configure Camera Restrictions

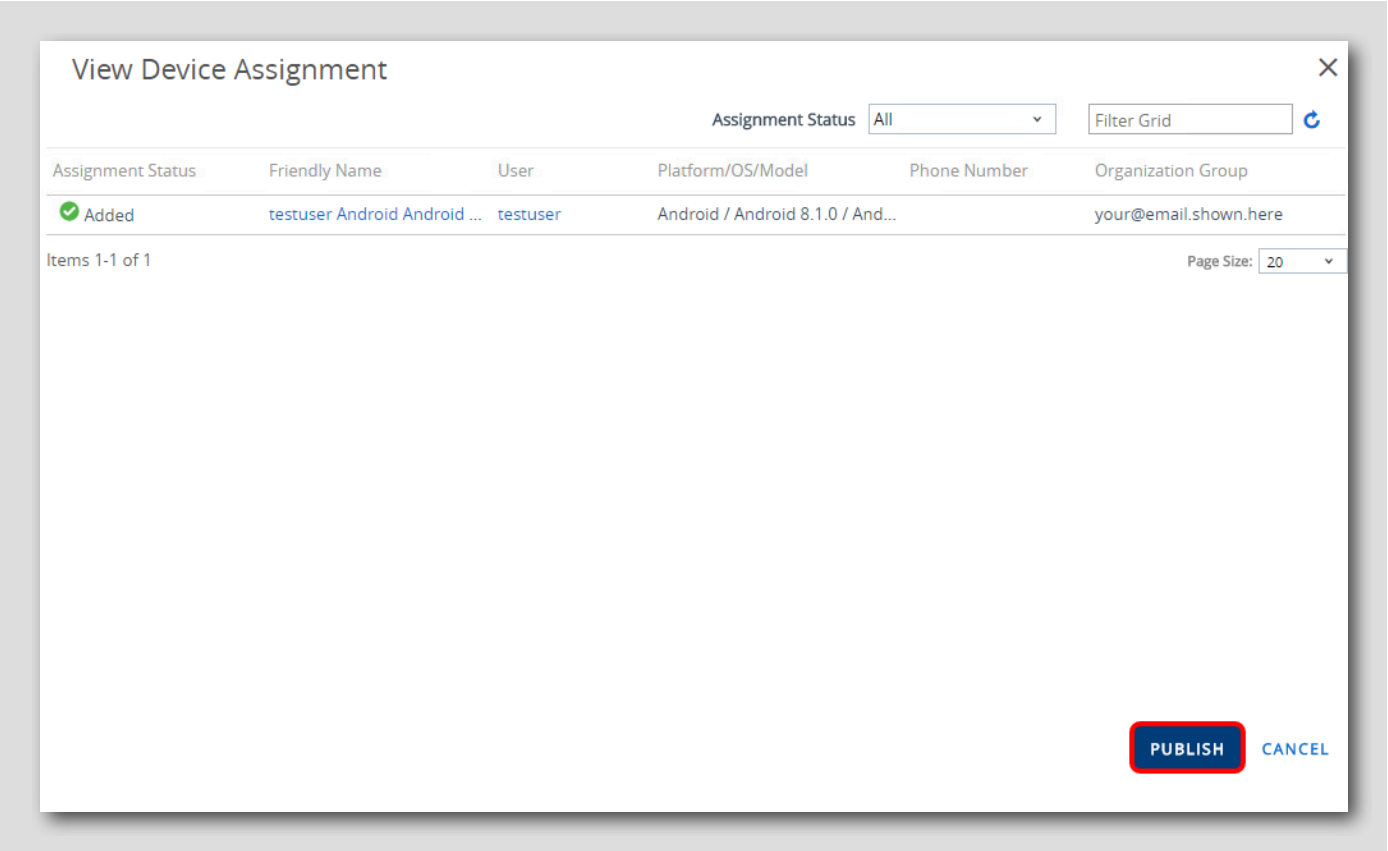
[386]



1. Scroll down to find the **Applications** section
2. Uncheck the **Allow Camera** checkbox for the **Work Profile** column
3. Click **Save And Publish**

Publish the Profile

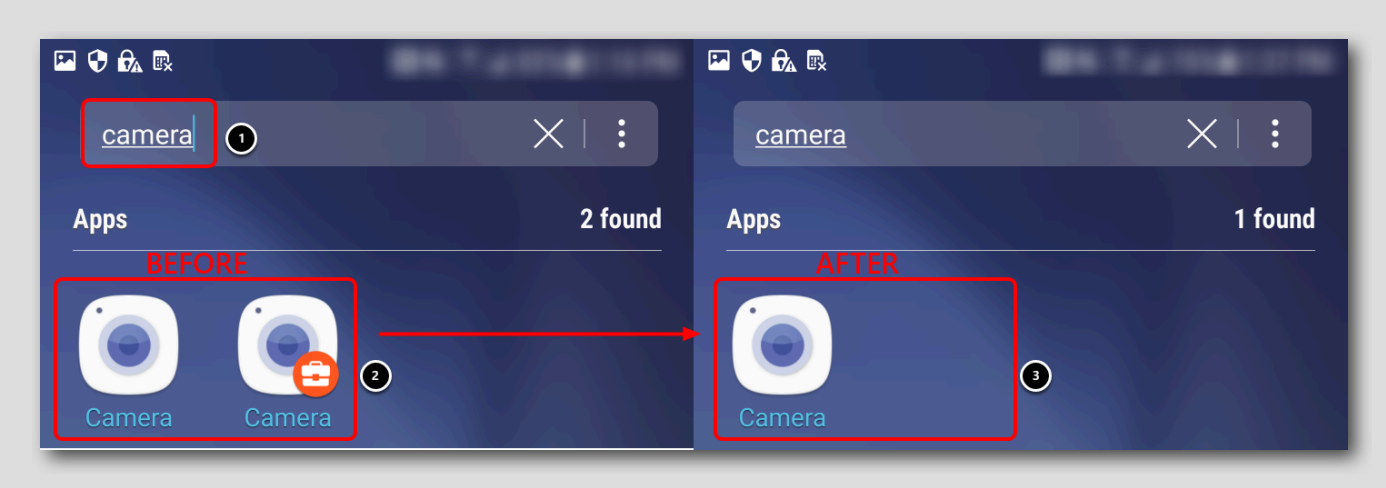
[387]



Click **Publish**.

Verify the Android Enterprise Camera Restrictions

[388]

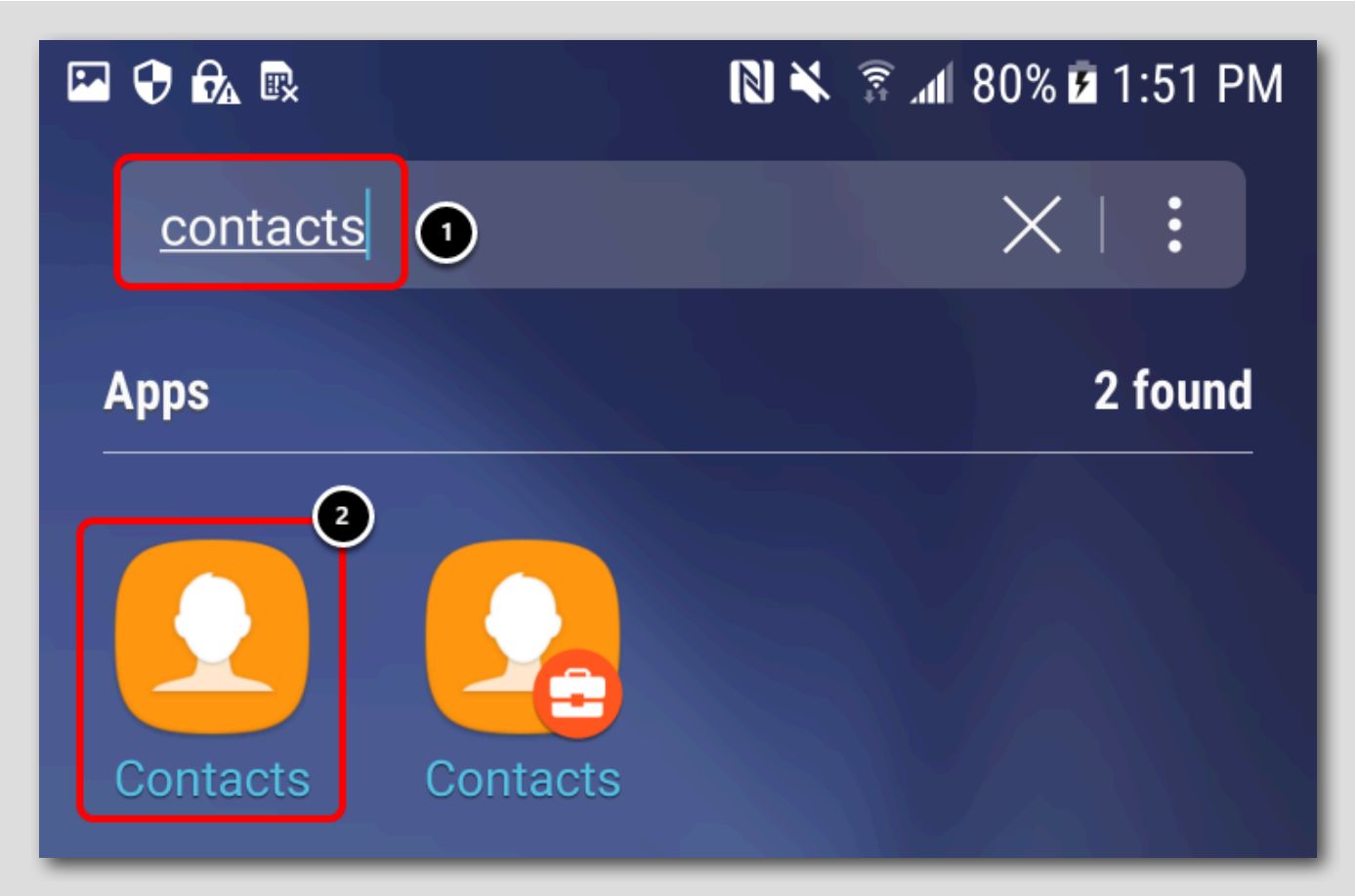


On your device, notice that after we push the profile your device will no longer have the badged camera application available but your personal side (unbadged) camera will still be available for usage. This confirms the camera restriction that you setup on the Workspace ONE UEM Android profile that was previously created.

1. Search for **`camera`** on the device
2. Before the profile takes affect, notice that the Camera work (badged) app exists alongside the personal (unbadged) app
3. After the profile takes affect, notice that the Camera work (badged) app has been removed

NOTE - Due to lab network limitations, it may take a few minutes for the badged Camera application to be removed. If you still see it on your device, please wait until the application is successfully removed.

Screenshot in a non-badged app [389]

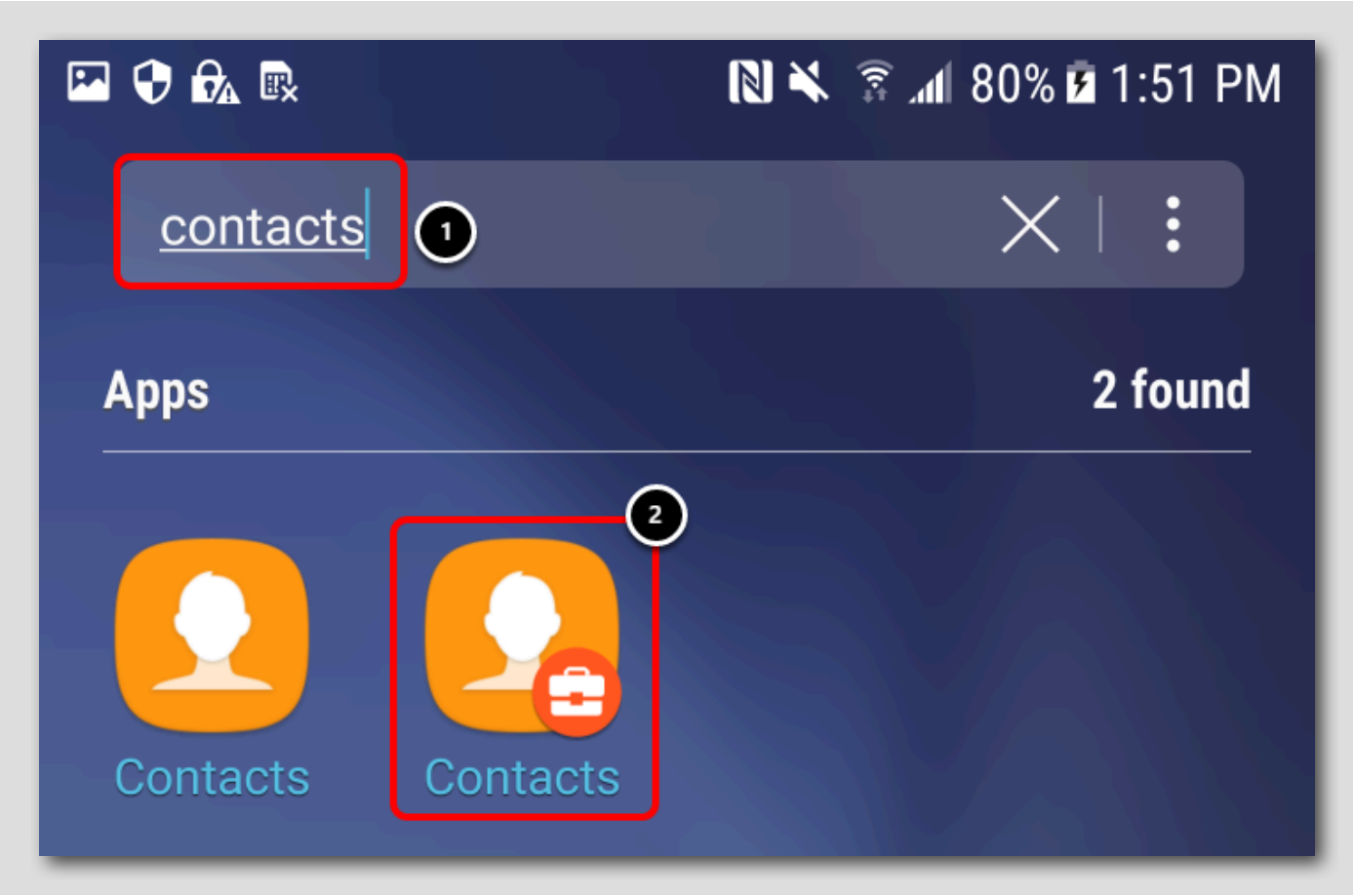


1. Search for **contacts** on the device
2. Open your **Personal (non-badged) Contacts** app
3. Take a screen shot (Power button and volume down / Power Button + Home Button at the same time for 2 seconds), notice that the screenshot was successful.

NOTE - The shortcut to change screenshot may vary depending on your device model. Please see a lab assistant in case assistance is required.

Verify the Android Enterprise Screenshot Restriction

[390]



1. Search for **`contacts`** on the device
2. Open your **Work (badged) Contacts** app
3. Take a screen shot (Power button and volume down / Power Button + Home Button at the same time for 2 seconds), notice that the screenshot was NOT successful.

This shows the screenshot restriction that we applied on the Workspace ONE UEM Android profile created previously.

Approving Applications

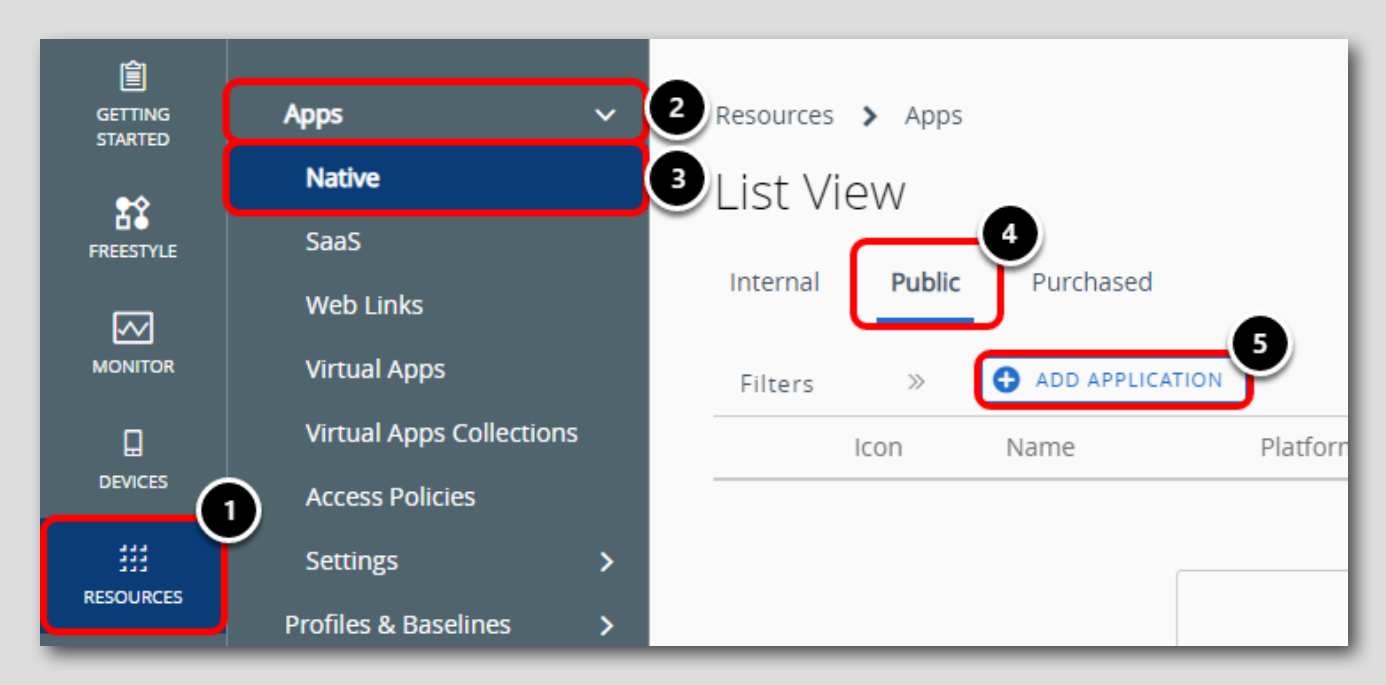
[391]

This section is designed to walk you through the process of approving applications for integration between Workspace ONE UEM and Android Enterprise. Applications that you push through the integration of Workspace ONE UEM and Android Enterprise have the same functionality as their counterparts from the Google Play Store. However, you can use Workspace ONE UEM features to add functionality and security to these applications.

- To add convenience of use, configure the Send Application Configuration option. Application configurations allow you to pre-configure supported key-value pairs and to push them down to devices along with the application. Examples of supported values may include usernames, passwords, and VPN settings. Support values depends upon the application.
- To add secure features, use Workspace ONE UEM profiles for Android Enterprise. Profiles allow you to set passcodes, apply restrictions, and use certificates for authentication.

Add Public Application

[392]

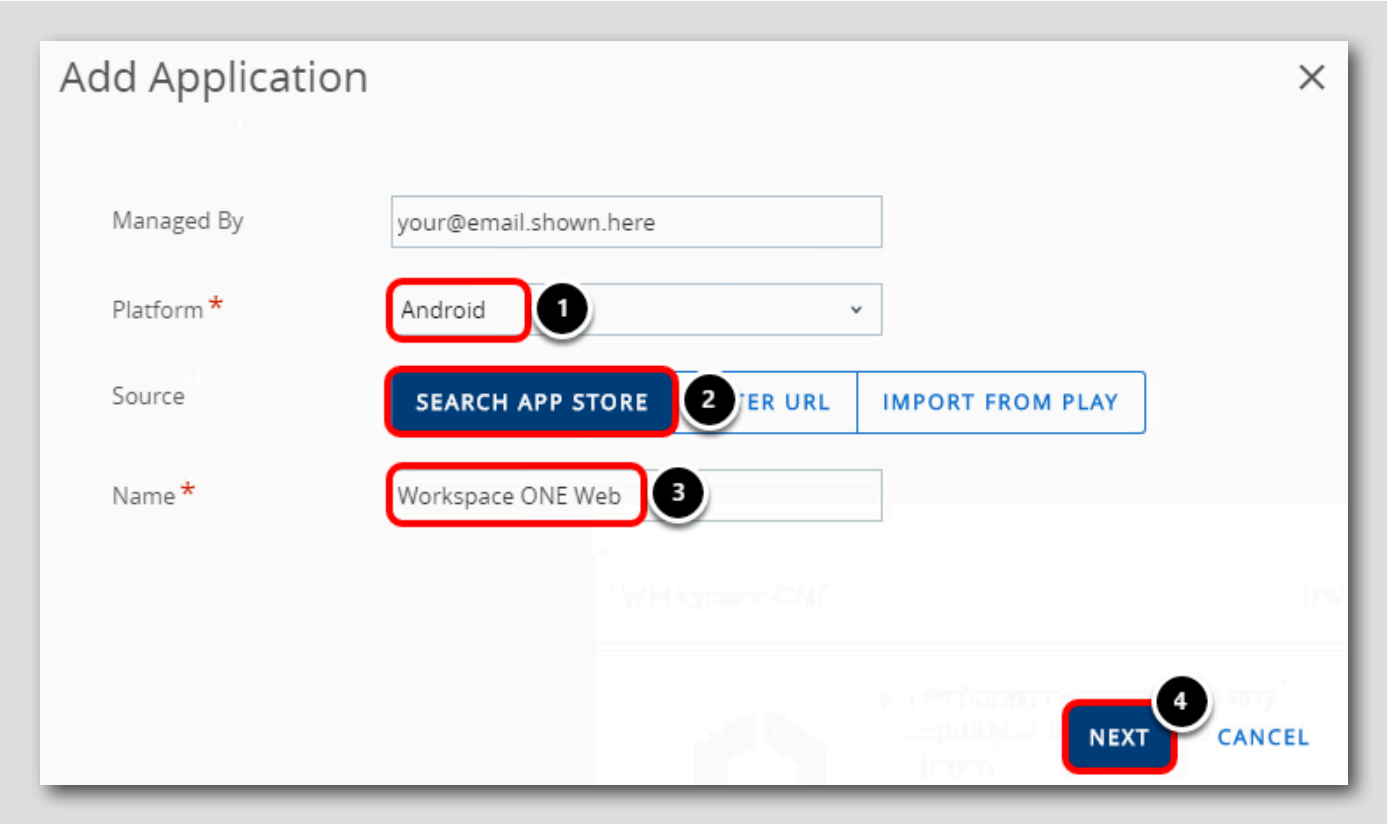


In the Workspace ONE UEM Administrator Console,

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

Search for Public Application

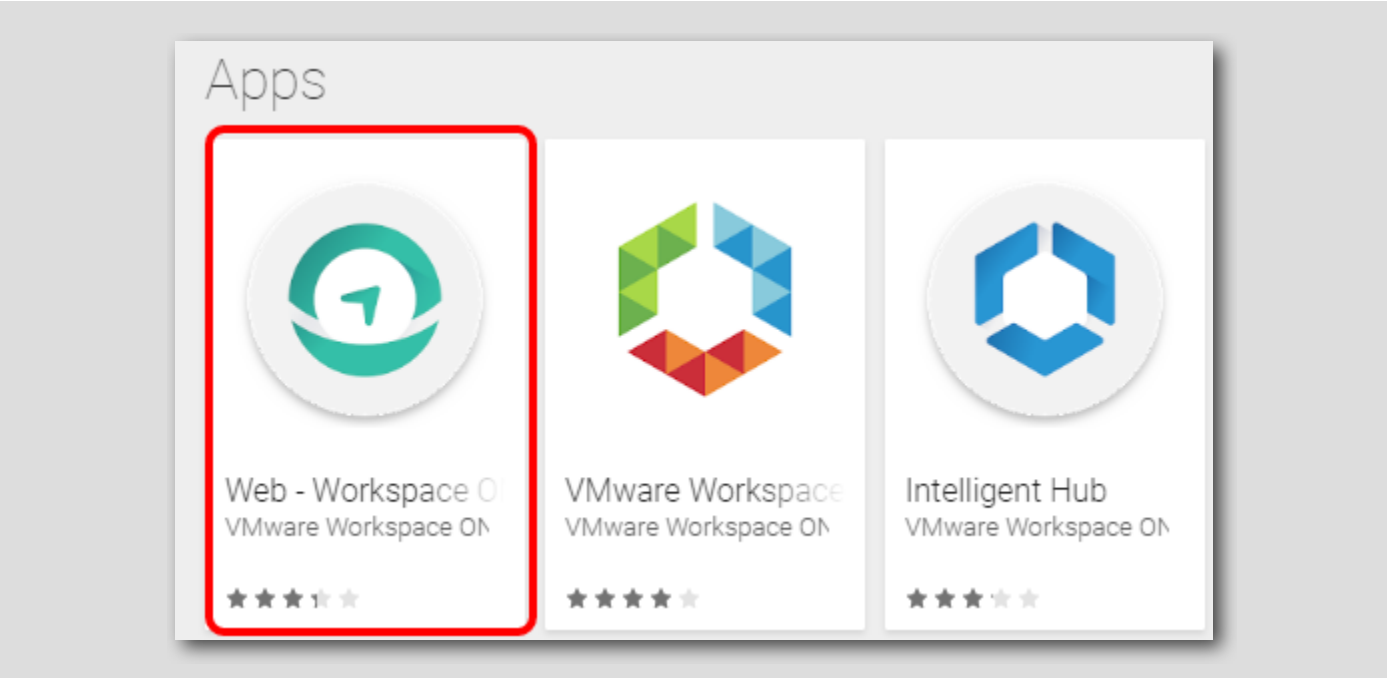
[393]



1. Select **Android** from the Platform drop-down menu
2. Select **Search App Store** for the Source
3. Enter **`Workspace ONE Web`** in the Name text box
4. Click **Next**

Select the Workspace ONE Web App

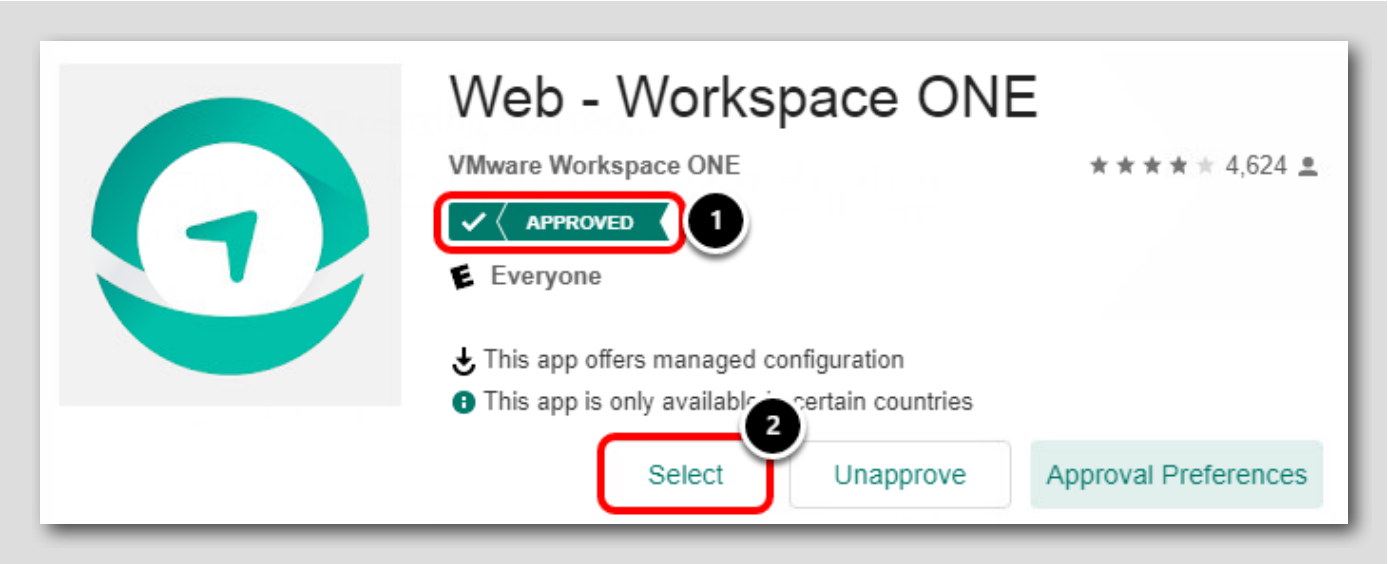
[394]



Click the **Web - Workspace ONE** app.

Selecting and Approving Apps

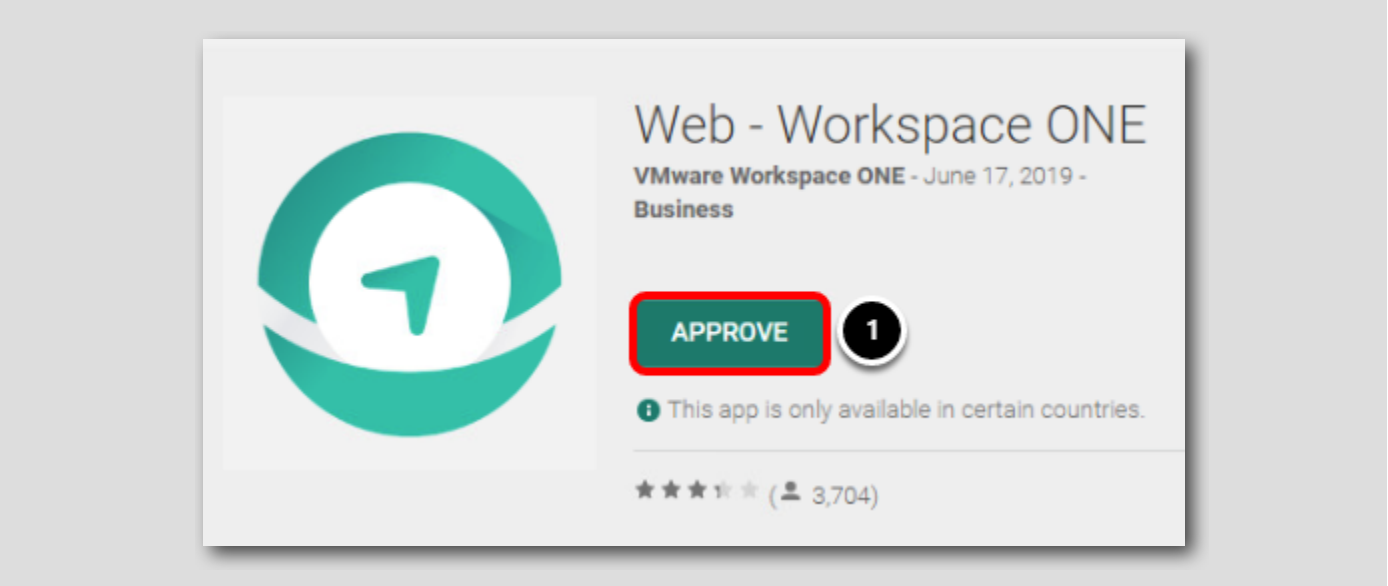
[395]

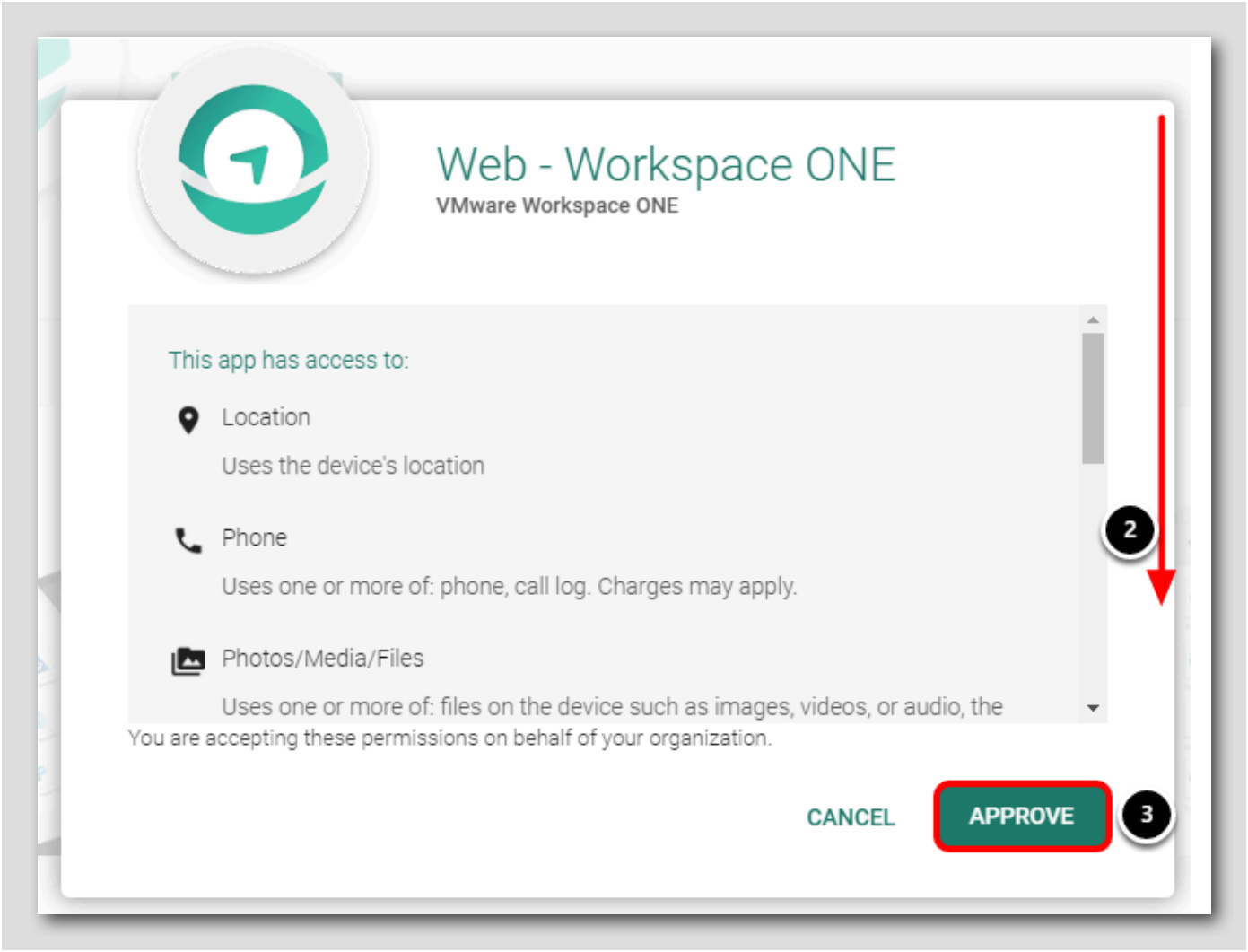


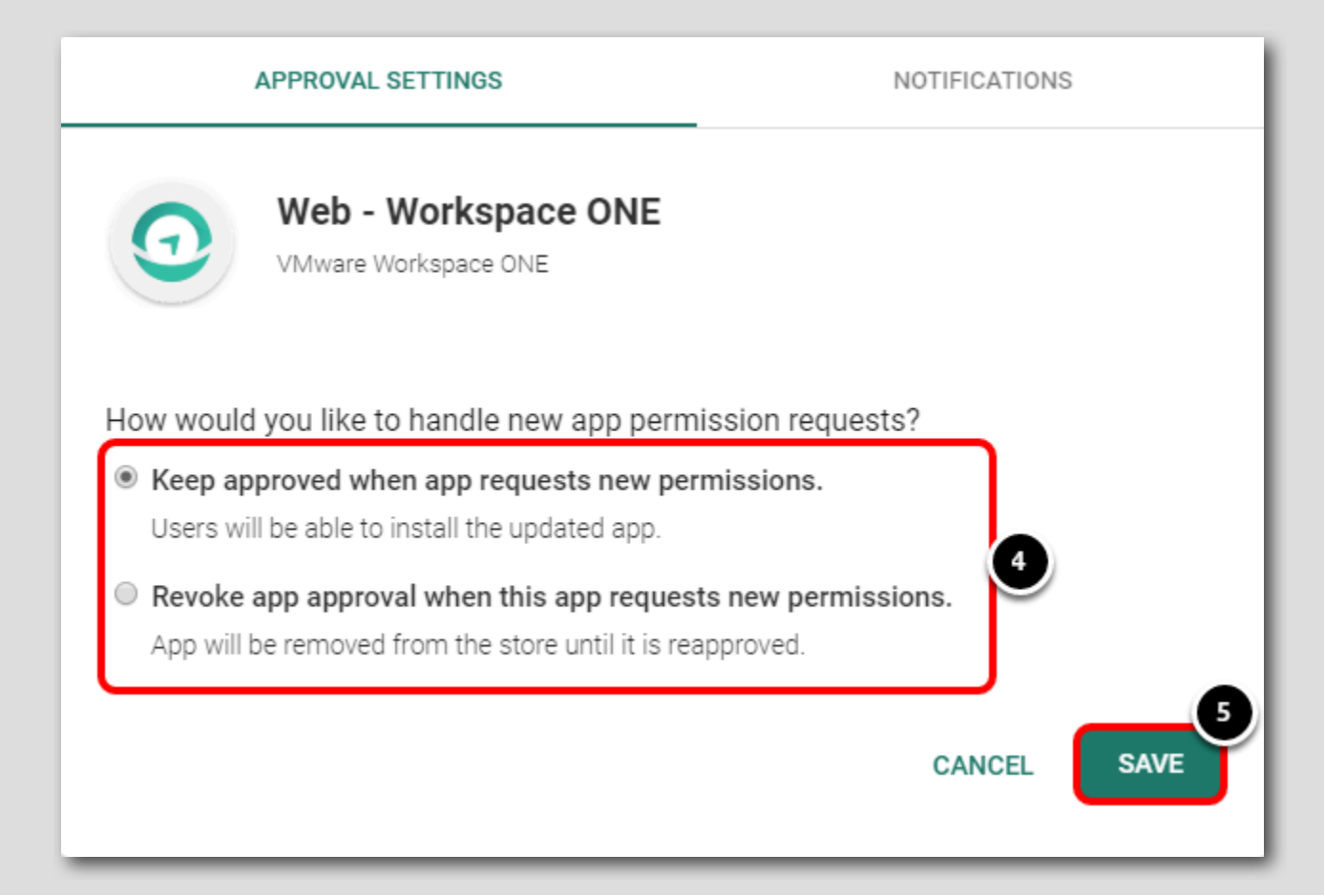
1. Notice that the application is already marked as **Approved**. This is because the Android EMM Registration settings were configured at a parent level organization group and your organization group is inheriting these settings. Apps only need to be approved once, which has already been done for you.
2. Click **Select** to proceed.

Continue to the next step, or view the below steps to see the necessary approval steps for a new app.

IMPORTANT: The below steps are purely informative and can be skipped if desired. They are included to show the approval process for new applications.


Web - Workspace ONE
VMware Workspace ONE - June 17, 2019 - Business
APPROVE
1
This app is only available in certain countries.
(3,704)


Web - Workspace ONE
VMware Workspace ONE
This app has access to:
Location
Uses the device's location
Phone
Uses one or more of: phone, call log. Charges may apply.
Photos/Media/Files
Uses one or more of: files on the device such as images, videos, or audio, the
You are accepting these permissions on behalf of your organization.
CANCEL
APPROVE
2
3

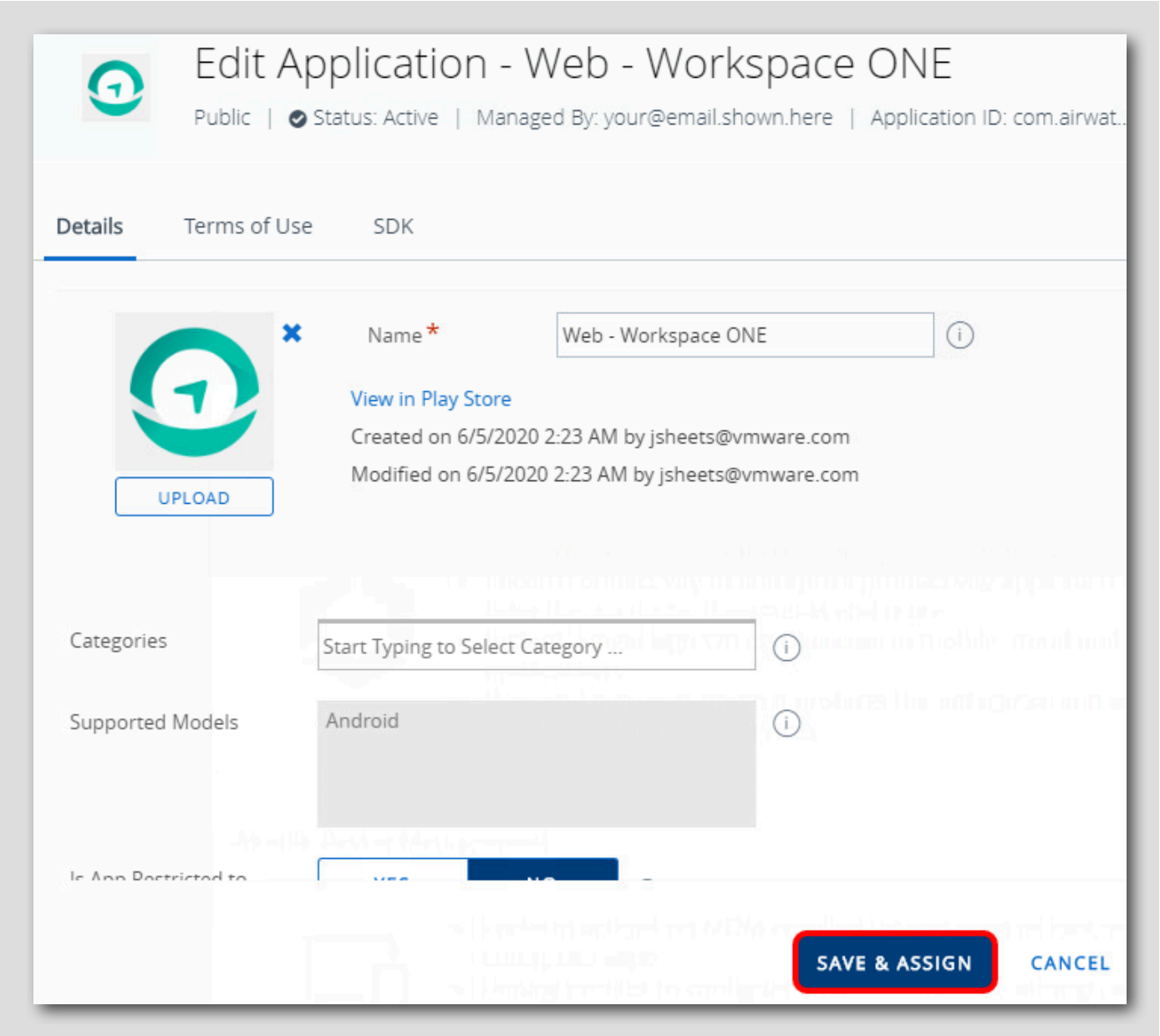


1. Click **Approve** for the desired app.
2. Scroll through the list of items the app has access to.
3. Click **Approve**.
4. Review and select how you would like to handle new app permission requests. This allows you to choose between a manual approval or automatic approval if the app requests new permissions in the future from what we were displayed on the previous screen.
5. Click **Save**.

This process would then return the administrator to the first step in this process, allowing them to click Select and continue adding the desired app.

Publish Public App

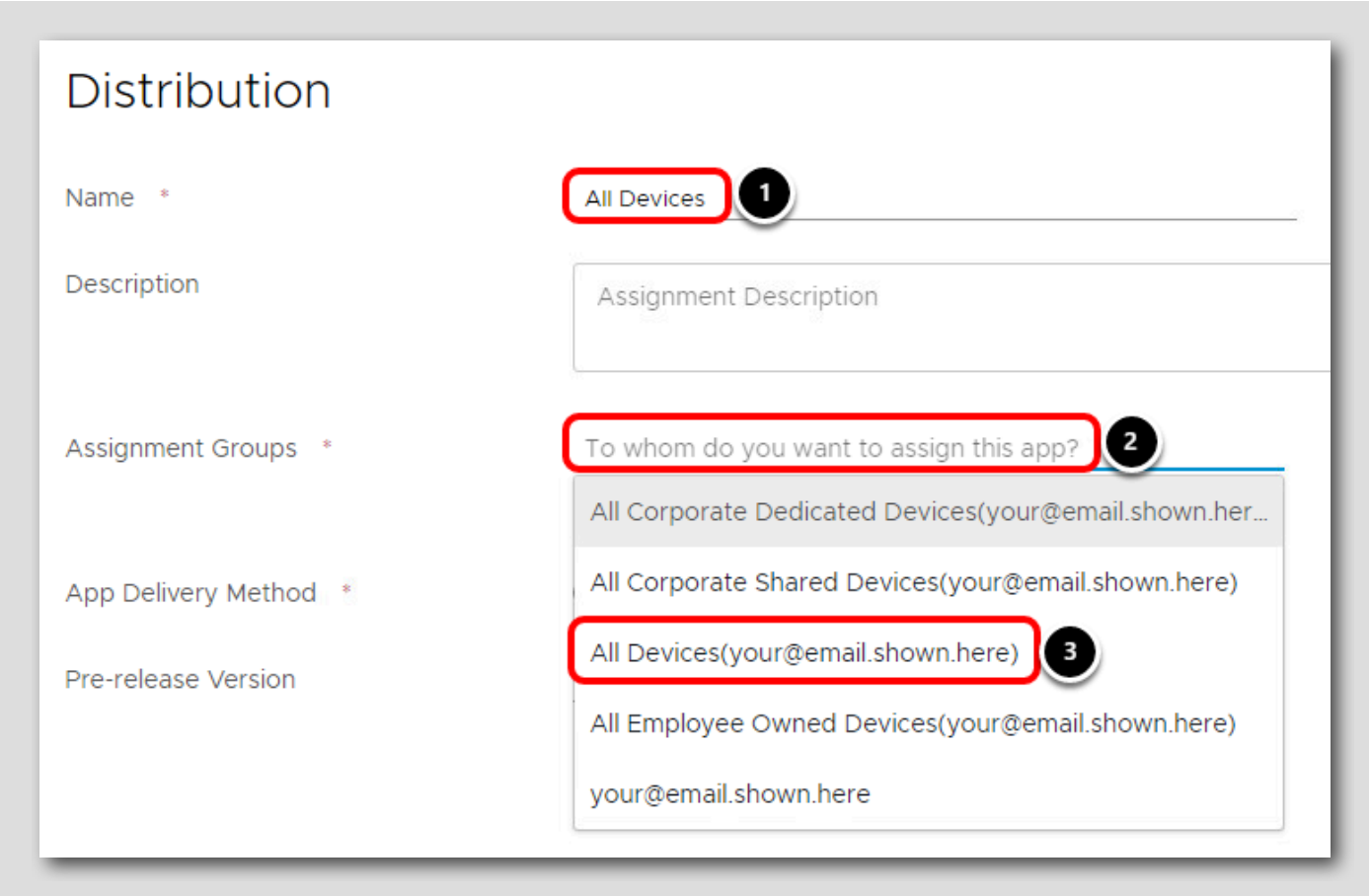
[396]



Click **Save & Assign**.

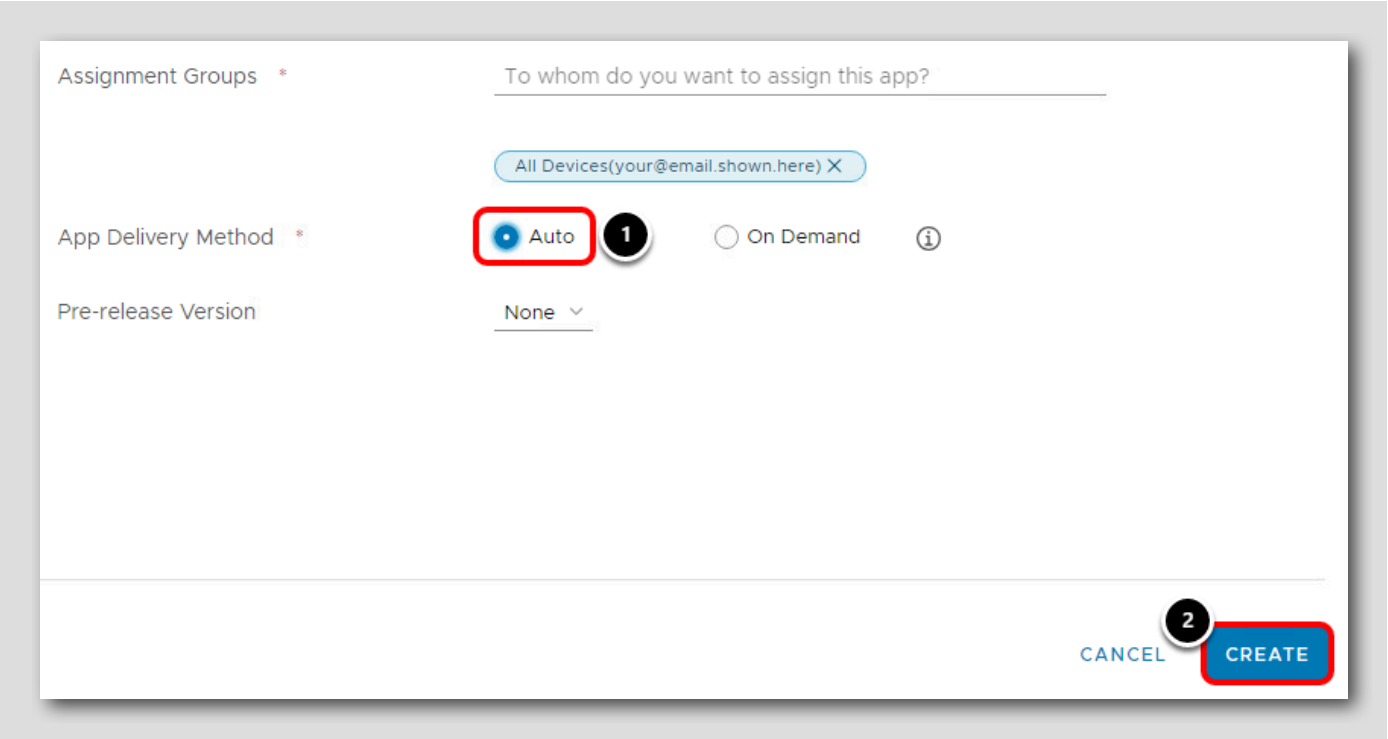
Add Assignment Distribution

[397]



1. Enter **`All Devices`** for the distribution Name
2. Click in the **Assignment Groups** field
3. Select the **All Devices (your@email.shown.here)** group

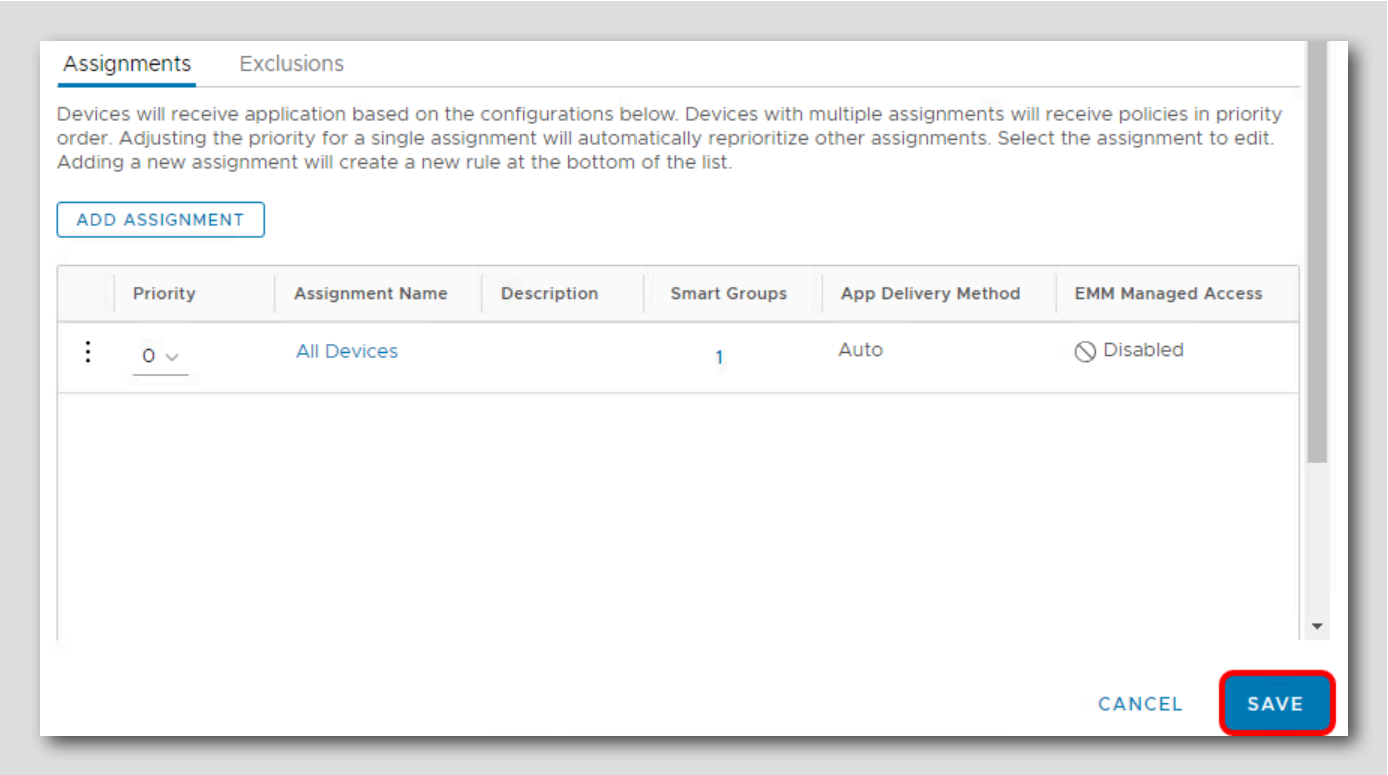
Configure Assignment



1. Select **Auto** for the App Delivery Method.
2. Click **Create**

Save and Publish Workspace ONE Web

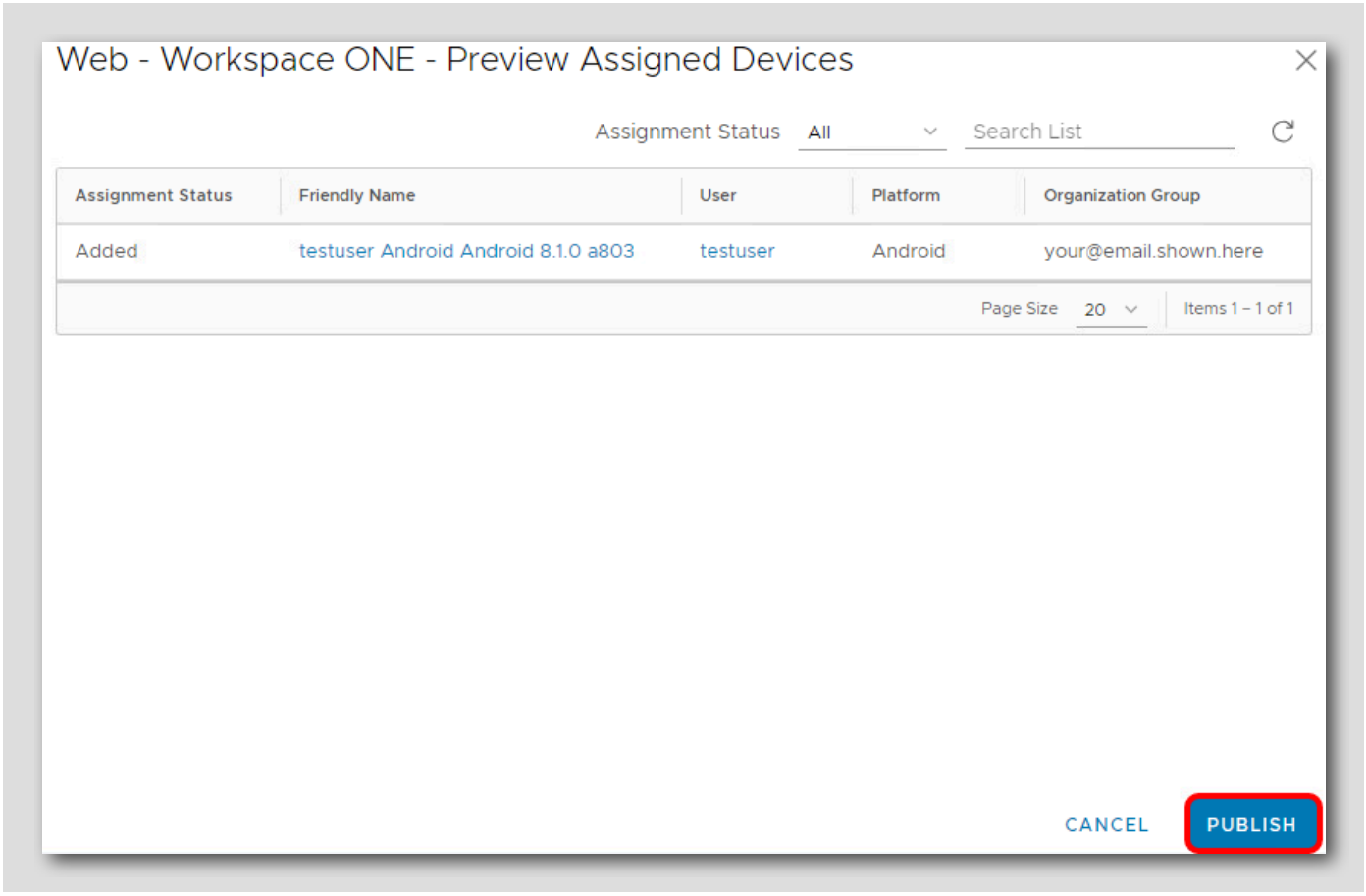
[399]



Click **Save**.

Preview Assigned Devices and Publish

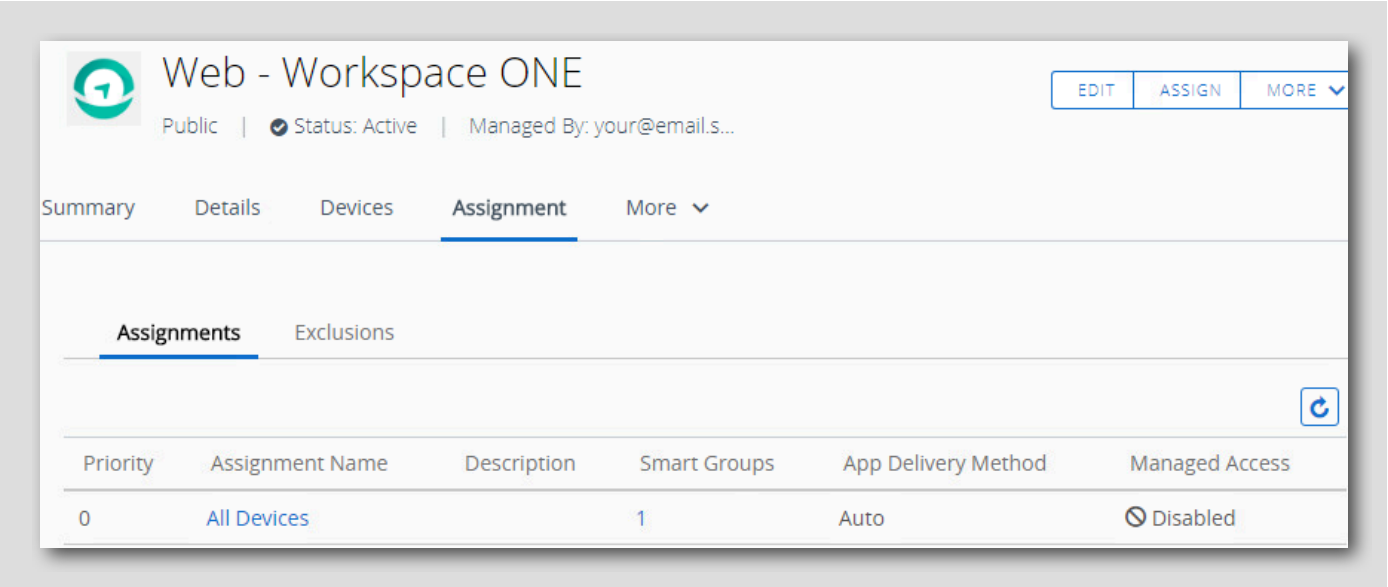
[400]



Click **Publish**.

Confirm Application Creation

[401]



Confirm that the Workspace ONE Web app was approved and created and assigned to the All Devices group.

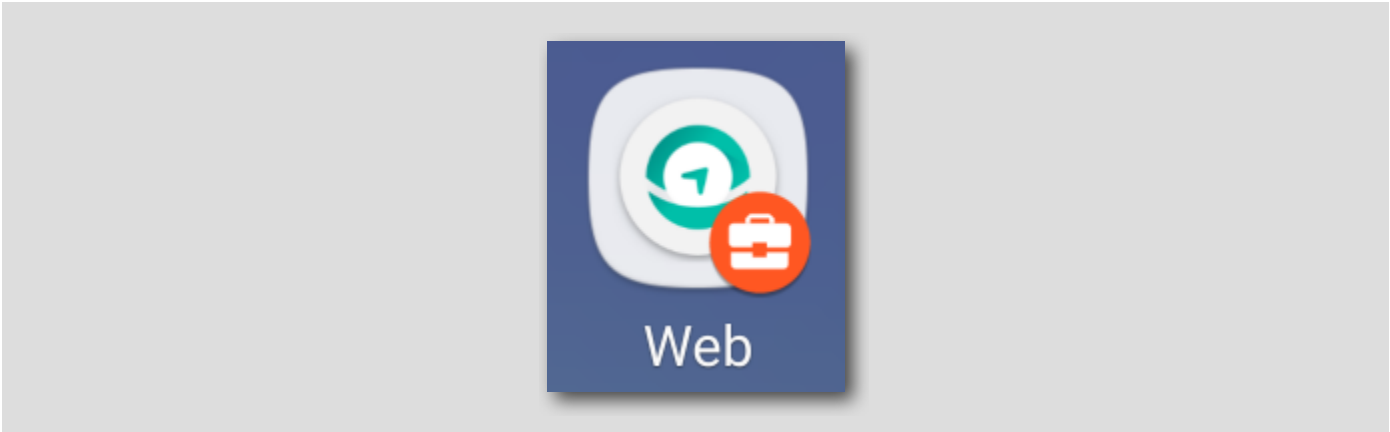
Verify Work Apps

[402]

In the previous section, we learned how we can approve and push an Android application from the Workspace ONE UEM Console. In this section, we will verify that Work apps installed correctly on our enrolled Android device.

Confirm the Published Workspace ONE Web Application Downloaded

[403]

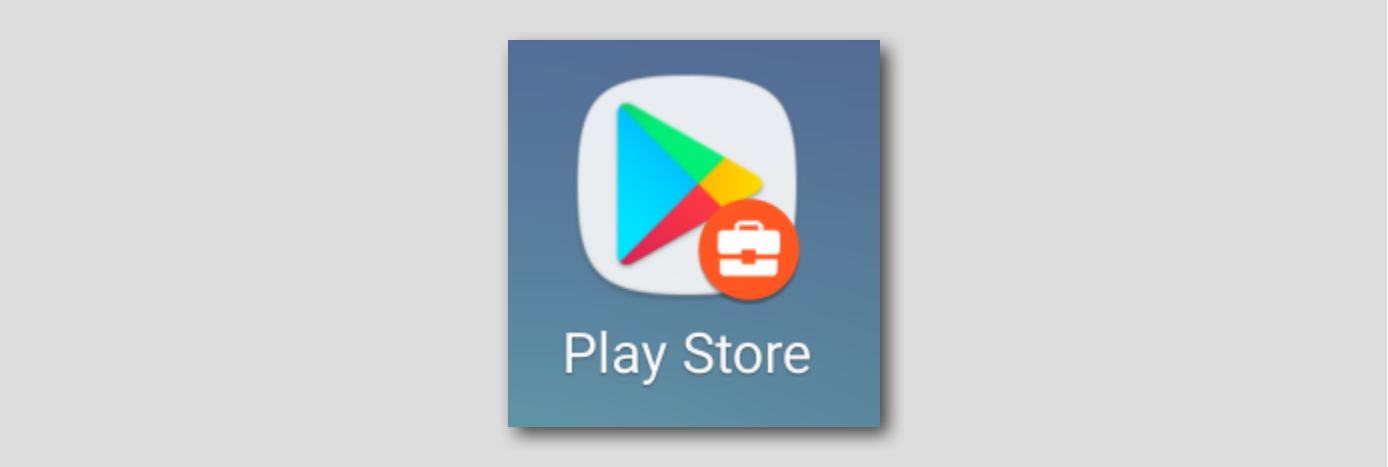


Return to your testing Android device and confirm that the **Workspace ONE Web** application has downloaded and displays as a Work app.

NOTE - Depending on lab network traffic, you may need to wait several minutes for the download to complete.

Using this process, you can rapidly approve new applications and deploy them to your users.

Open the Badged Android Enterprise Play Store App [404]

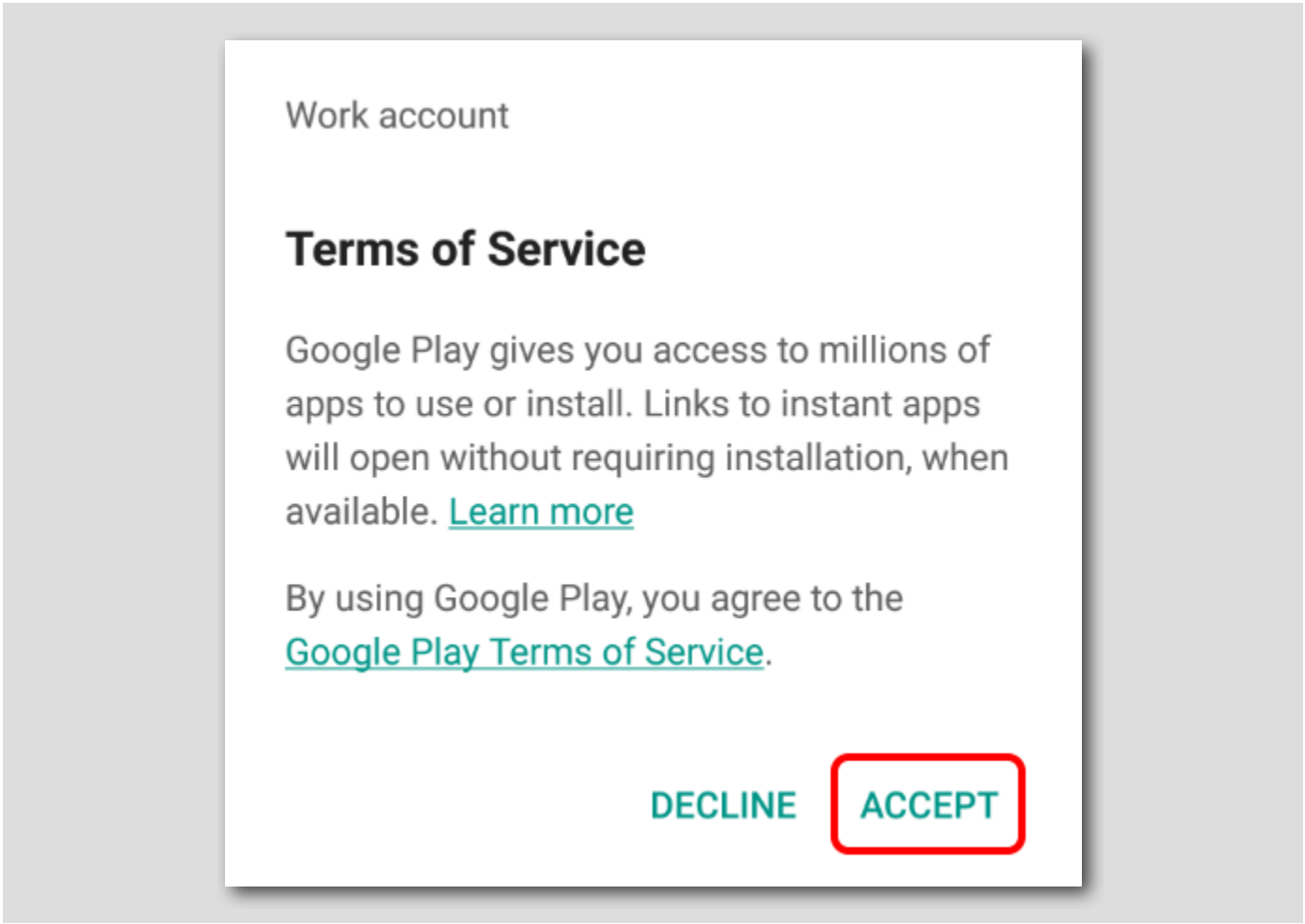


Open your **Work Play Store** application on your Android device.

NOTE - The screenshot may differ depending on device model and OS.

Accept Google Play Terms of Service (IF NEEDED)

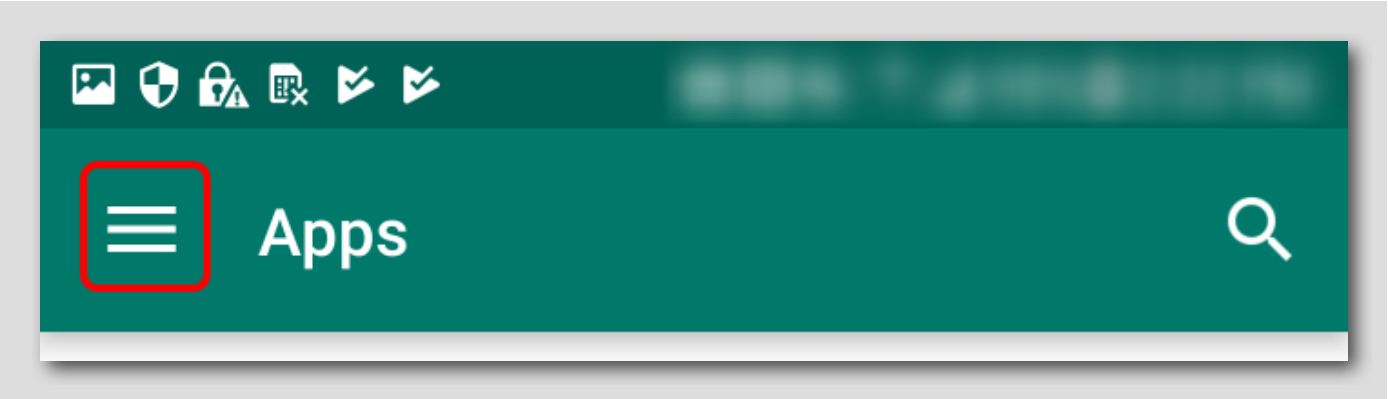
[405]



If you are prompted with the Google Play Terms of Service, tap **Accept**. Otherwise, continue to the next step.

Open Play Store Menu

[406]

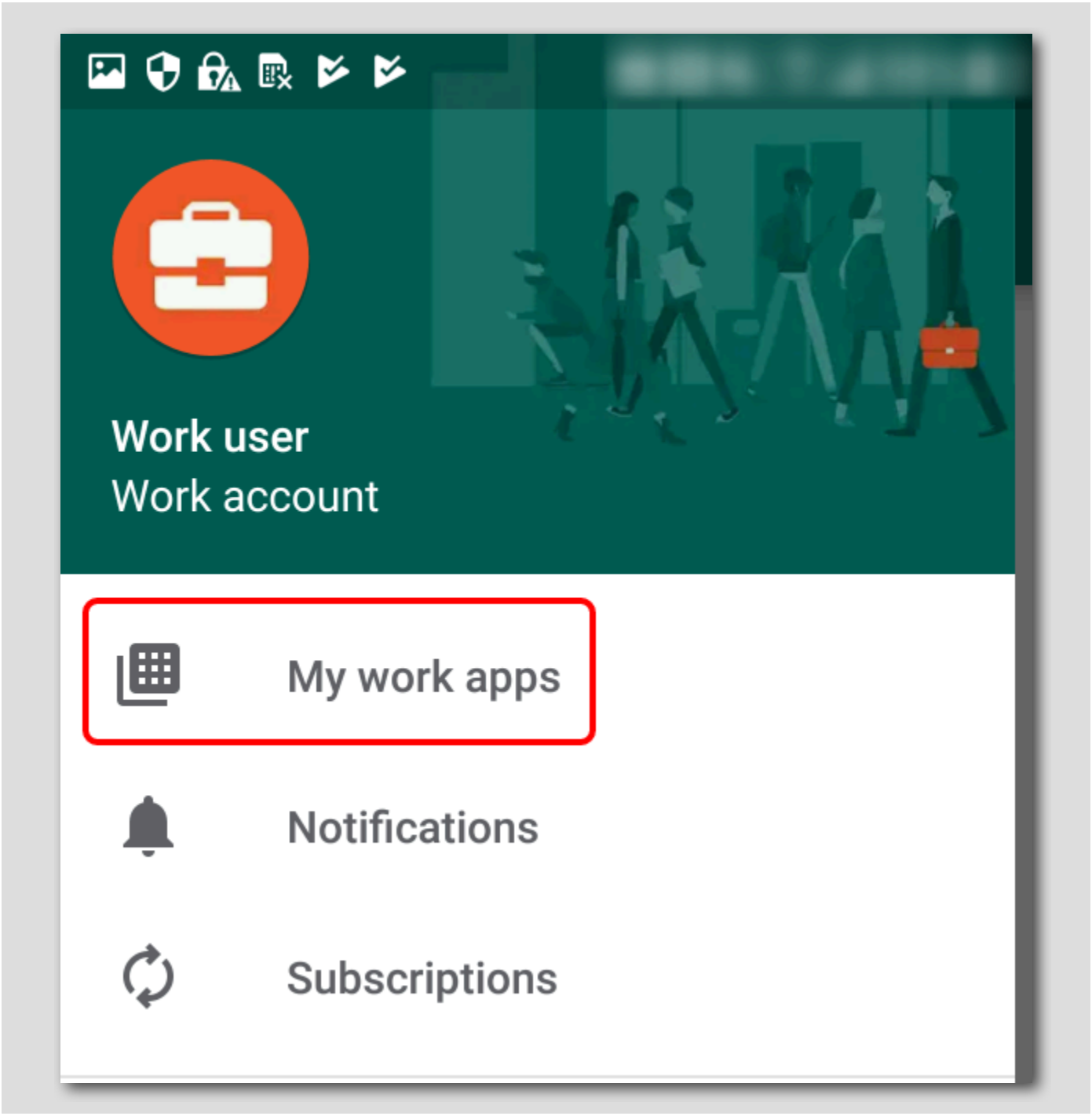


Tap the **Menu** button in the top-left corner.

NOTE - The screenshot may differ depending on device model and OS.

View Play Store Work Apps

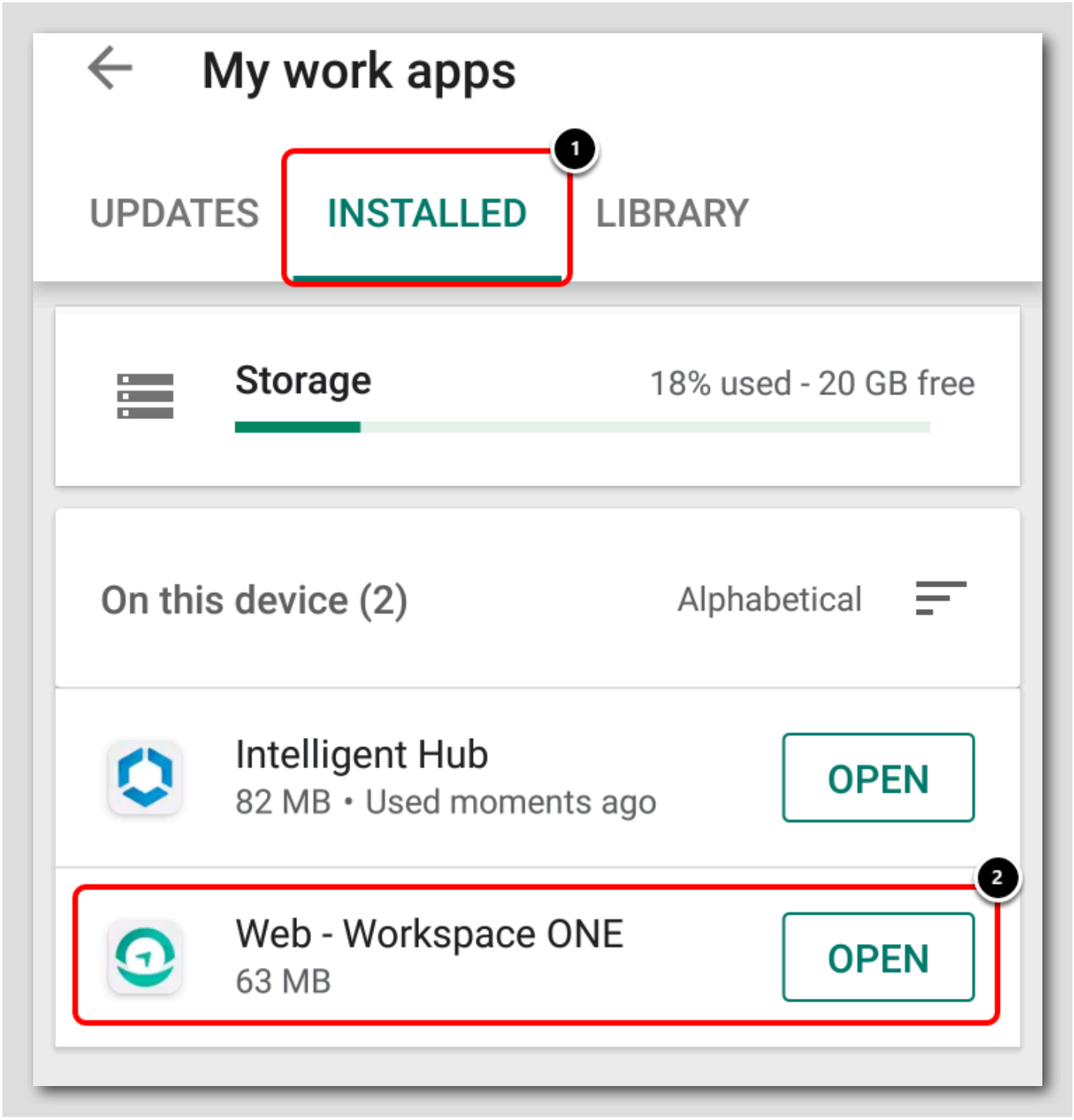
[407]



Tap **My Work Apps** from the menu.

NOTE - The screenshot may differ depending on device model and OS.

Verify Workspace ONE Web Is Available As A Work App [408]



1. Tap **Installed**.
2. Confirm that the **Workspace ONE Web** application is in your list of Work applications. You may need to scroll down to find the application.

NOTE - The screenshot may differ depending on device model and OS.

The Workspace ONE Web app is listed as a Work app because it was approved as a Work app through the Workspace ONE UEM Console while adding and assigning the application to your users. This streamlines and rapidly improves the process of approving and deploying Work apps to your Android devices!

Un-enrolling Your Android Device

[409]

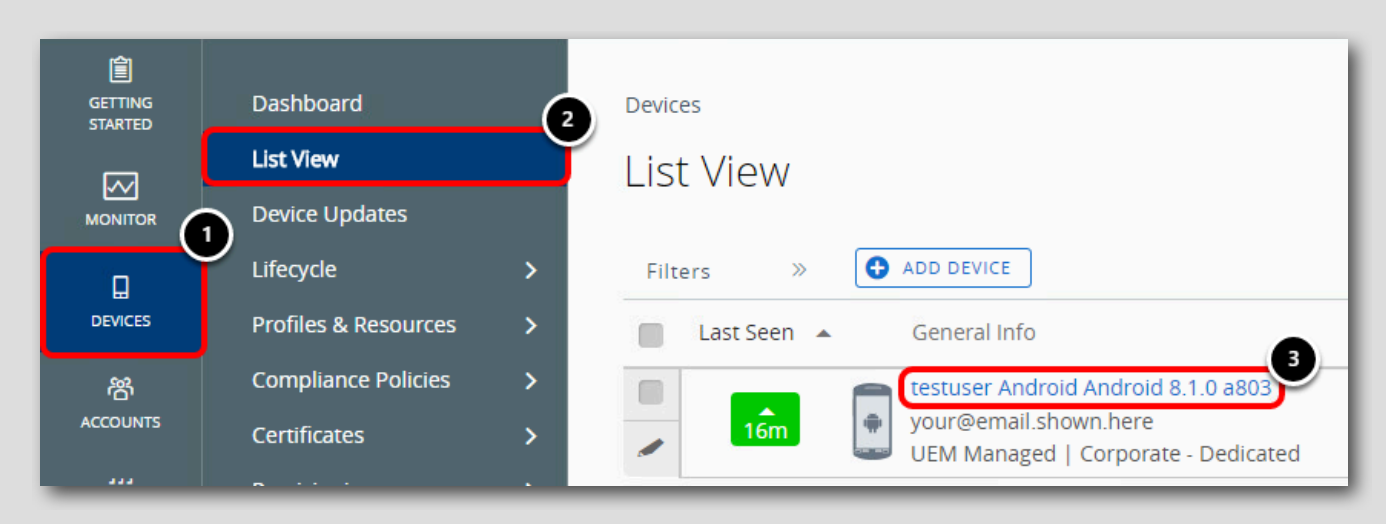
You are now going to un-enroll the Android device from Workspace ONE UEM.

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 app controls.

NOTE: The Enterprise Wipe will NOT remove the Workspace ONE Intelligent Hub application from the device as this was downloaded manually before Workspace ONE UEM had control of the device.

Enterprise Wipe (un-enroll) your Android device

[410]



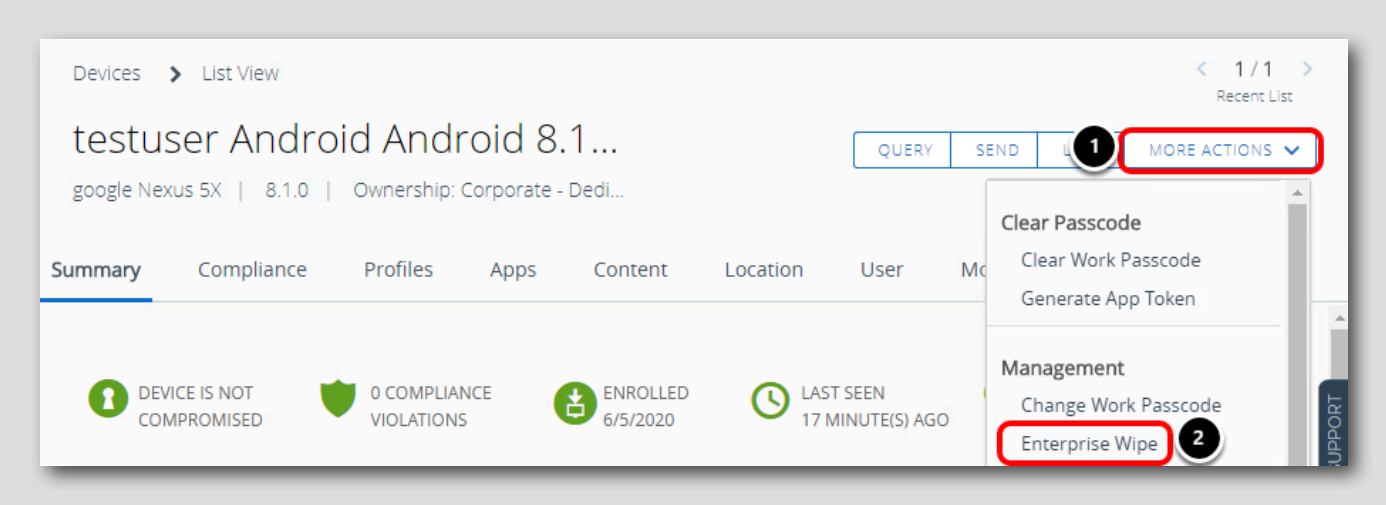
Enterprise Wipe will remove all the settings and content that were pushed to the device when it was enrolled. It will not affect anything that was on the device prior to enrollment.

To Enterprise Wipe your device, return to the Workspace ONE UEM Admin Console.

1. Click **Devices** on the left column
2. Click **List View**
3. Click the **link** for the device that you enrolled

Find the Enterprise Wipe Option

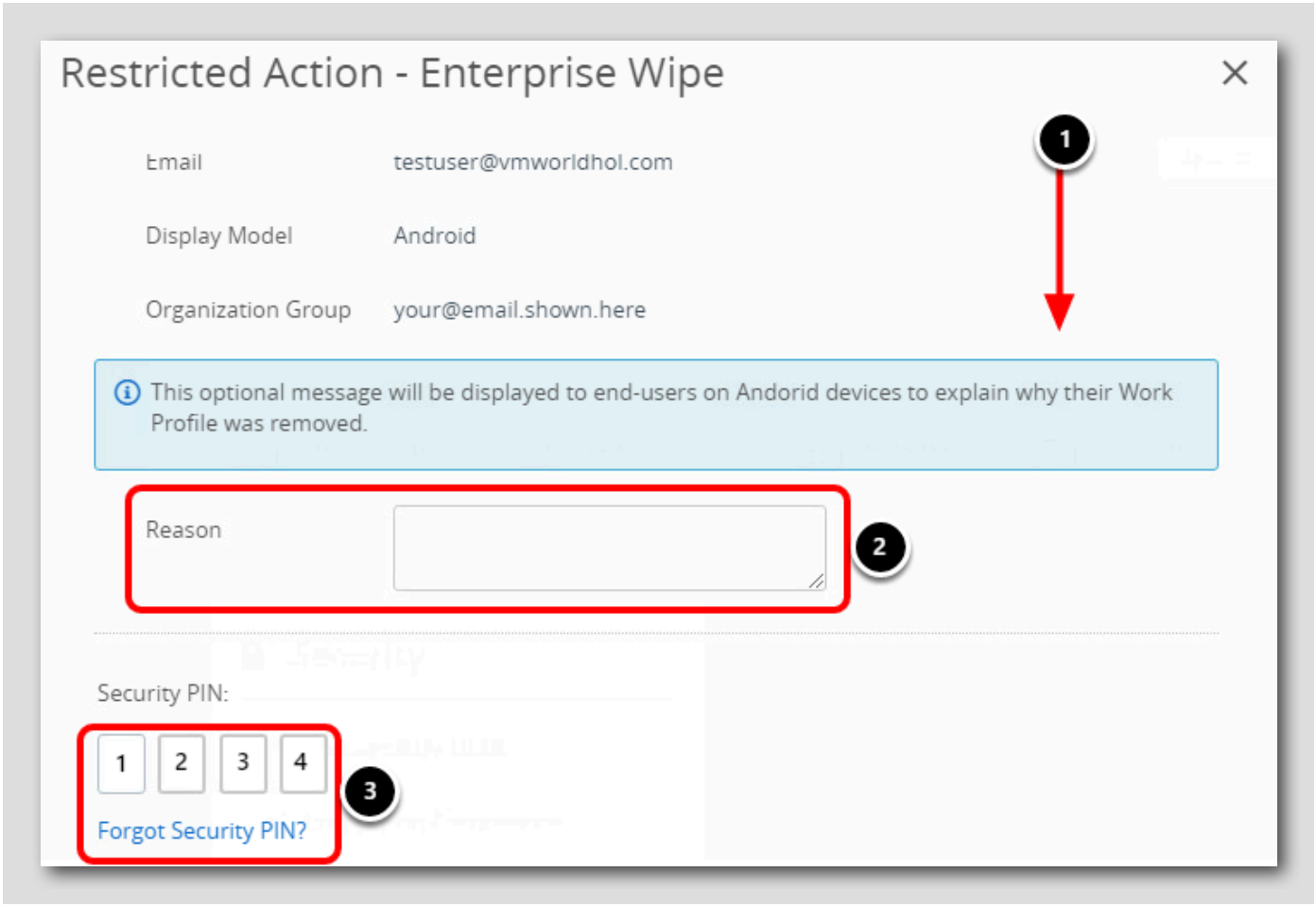
[411]



1. Click **More Actions**
2. Click **Enterprise Wipe** under Management

Enter your security PIN

[412]



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

1. Scroll down to the bottom of the Enterprise Wipe prompt.
2. Note the optional field to send a reason to your end user stating why their Work Profile was removed.
3. 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.

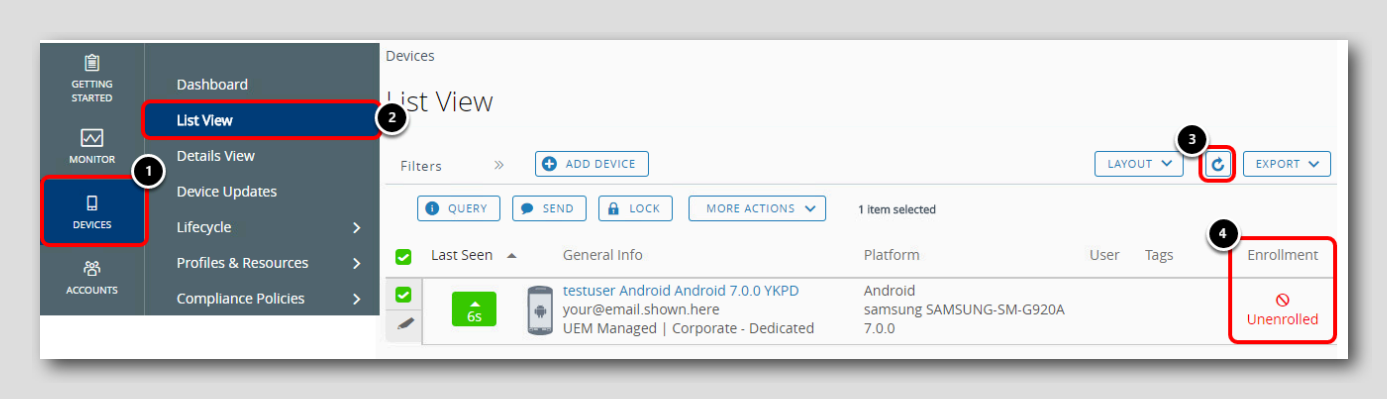
NOTE: If the Enterprise Wipe does not immediately occur, follow the below steps to force a device sync:

1. On your device, open the **Workspace ONE Intelligent Hub** application.
2. Tap **This Device**.
3. Scroll down to the bottom and click **Sync Device**. This will force the device to check in to Workspace ONE UEM to be notified that it should be unenrolled. Wait a moment a see if the command is processed, if not, skip to step #4.
4. Tap **Enrollment**.
5. Tap **Unenroll Device**. This allows you to process the Unenrollment command from the device manually.

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.

Confirming the Device was Un-Enrolled (Console)

[413]

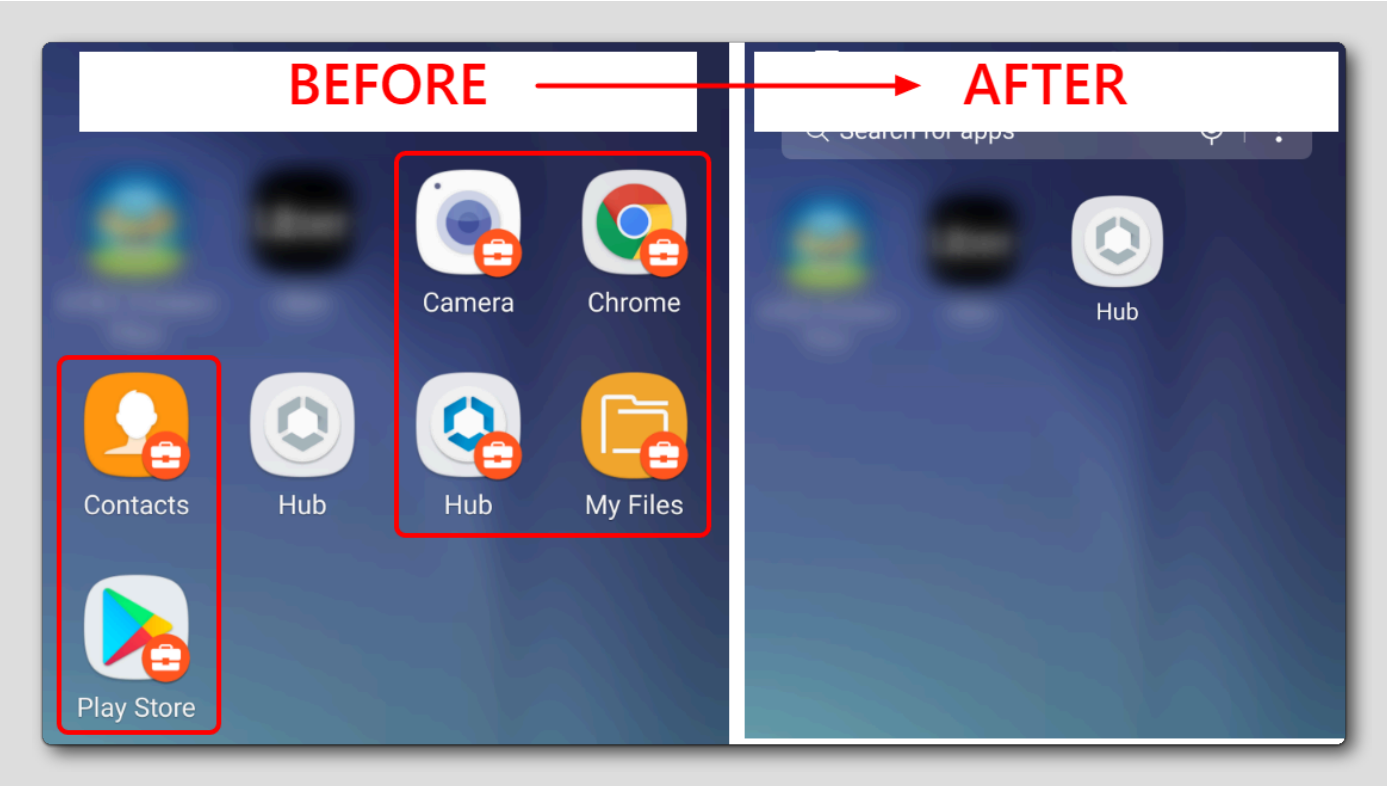


1. Click **Devices**
2. Click **List View**
3. Click the **Refresh** button on the Device List View screen.
4. Check if the device is showing **Unenrolled** for the Enrollment status. If not, continue to refresh the page until the device shows as Unenrolled.

NOTE: Depending on internet connectivity of the device, this could take a couple of minutes.

Confirm the Device was Un-Enrolled (Device)

[414]



On the device, notice that the badged apps are removed after the device is unenrolled and any configurations pushed to the device after enrollment has been removed.

Learn More about Android Enterprise

[415]

This is just a sampling of the functionality you will see with Android Enterprise integrated with Workspace ONE UEM. To learn more about features and functions please contact your VMware End User Computing representative or visit our website at *http://www.workspaceone.com/* or the website for Android Enterprise at *https://www.android.com/enterprise*.

Summary

[416]

The work profile is designed specifically for personal (BYOD) devices. Using Android in the enterprise, Workspace ONE UEM creates a "Work profile", a container which separates the personal space and the corporate space in a device. Workspace ONE UEM can fully control the work profile but has zero control over the personal profile.

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

[417]

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*!

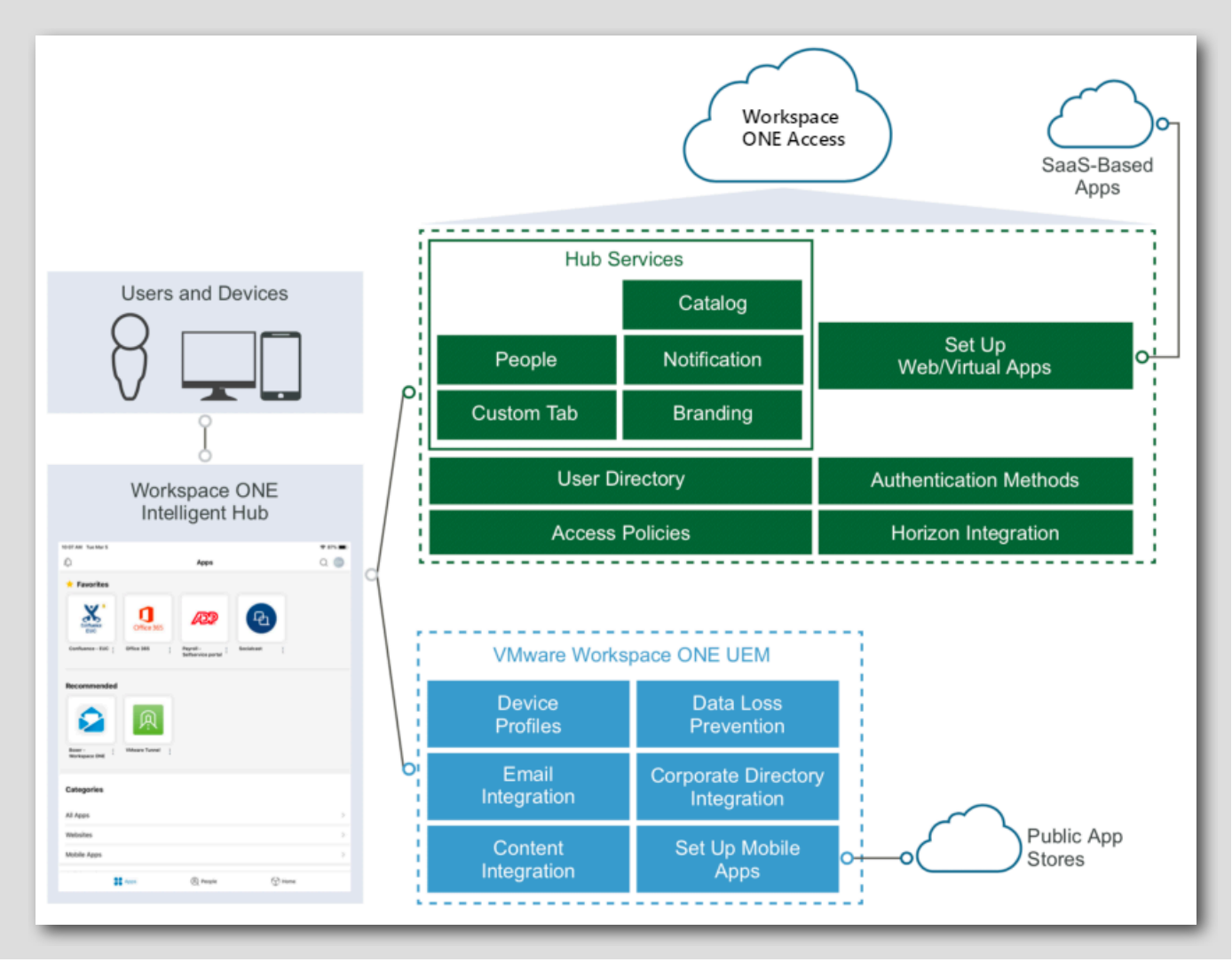

Your Personal journey from zero to IT Superhero
How the products work – beginner to expert
Quick start for your first proof of concept
TECH ZONE
Hands on Labs, Tools and Best Practices
Guide to production deployments & operations
Latest product information

Module 5 - Introduction to Workspace ONE Intelligent Hub and Hub Services (60 minutes) Beginner

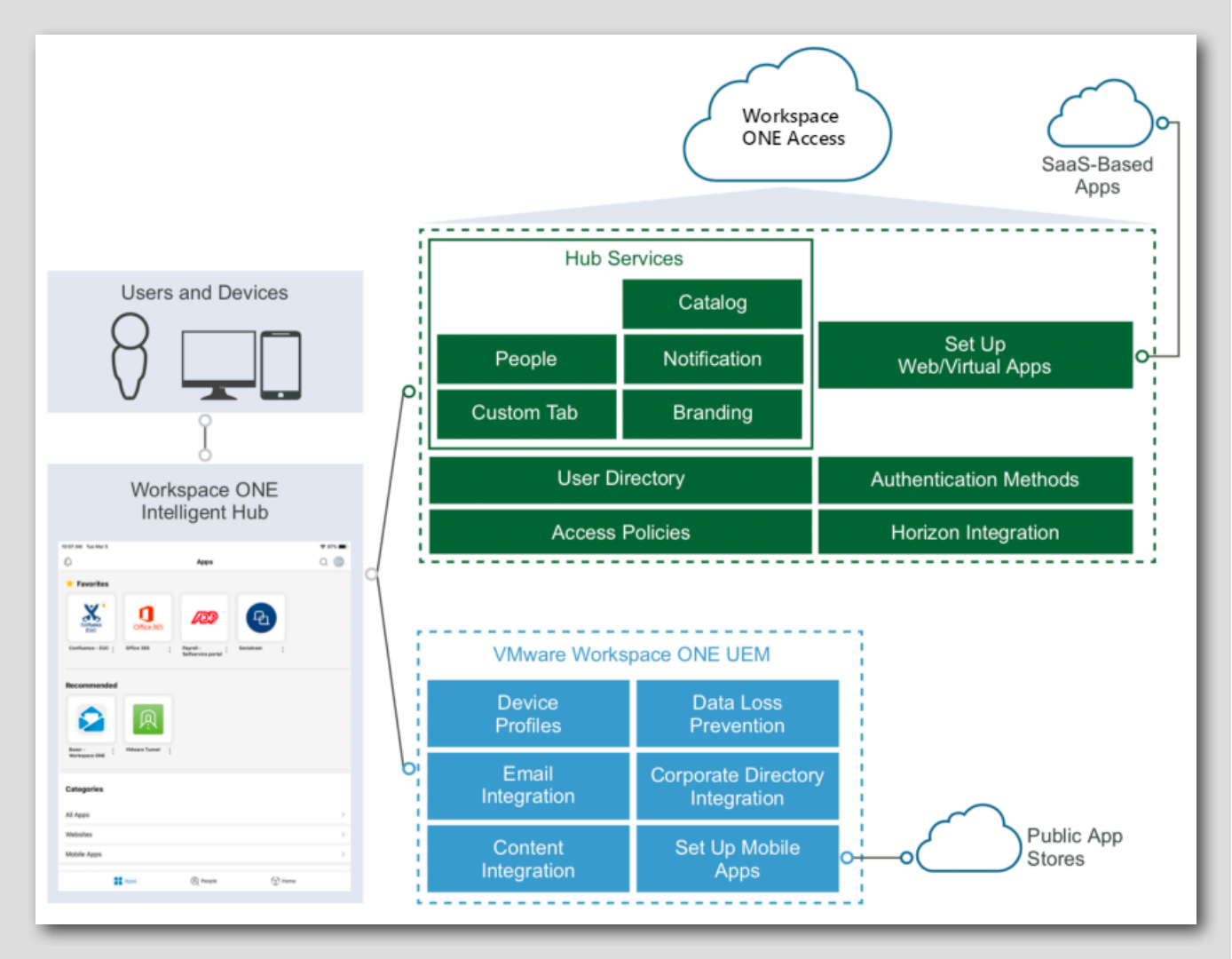
Introduction

[419]

Workspace ONE Intelligent Hub is VMware's next generation employee engagement application that allows you to securely access, discover, stay connected, and be productive from anywhere. It replaces the legacy Agent application and combines with Hub Services to enhance the identity, application, and enterprise mobility management capabilities offered by Workspace ONE.



Intelligent Hub integrates a unified app catalog, access control, and application management on iOS, Android, macOS, Windows 10 and via a browser. The prerequisite for many of the Intelligent Hub features is to activate the Hub Services component within Workspace ONE Access. After Hub Services activation, you can customize Intelligent Hub features based on whether your deployment is integrated with Workspace ONE Access or not.



Hub Services without Workspace ONE Access [420]

Without integrating with Workspace ONE Access, you can configure a Hub Catalog to allow access to native mobile apps and web apps, create a custom tab, and brand the Workspace ONE Intelligent Hub app to add your company's logo and color profile.

Hub Services with Workspace ONE Access [421]

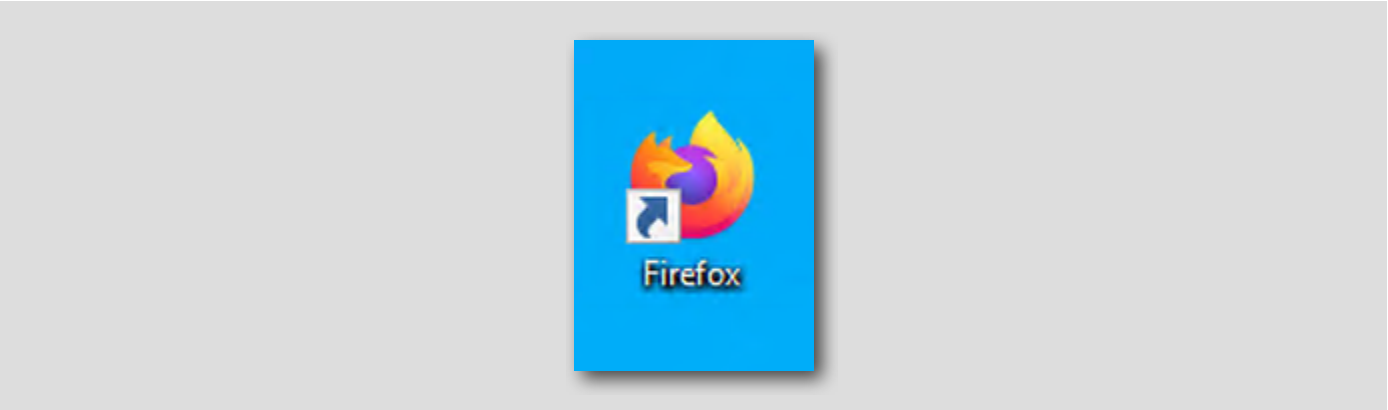
When Workspace ONE Access is integrated with Workspace ONE UEM, you can create a full digital workspace experience for users with additional Hub features, such as People Search and Notifications, and identity-related features, such as authentication and single sign-on.

In this lab, you will configure several of the features within Hub Services and view the result in the browser version of Intelligent Hub.

Login to the Workspace ONE UEM Console [422]

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

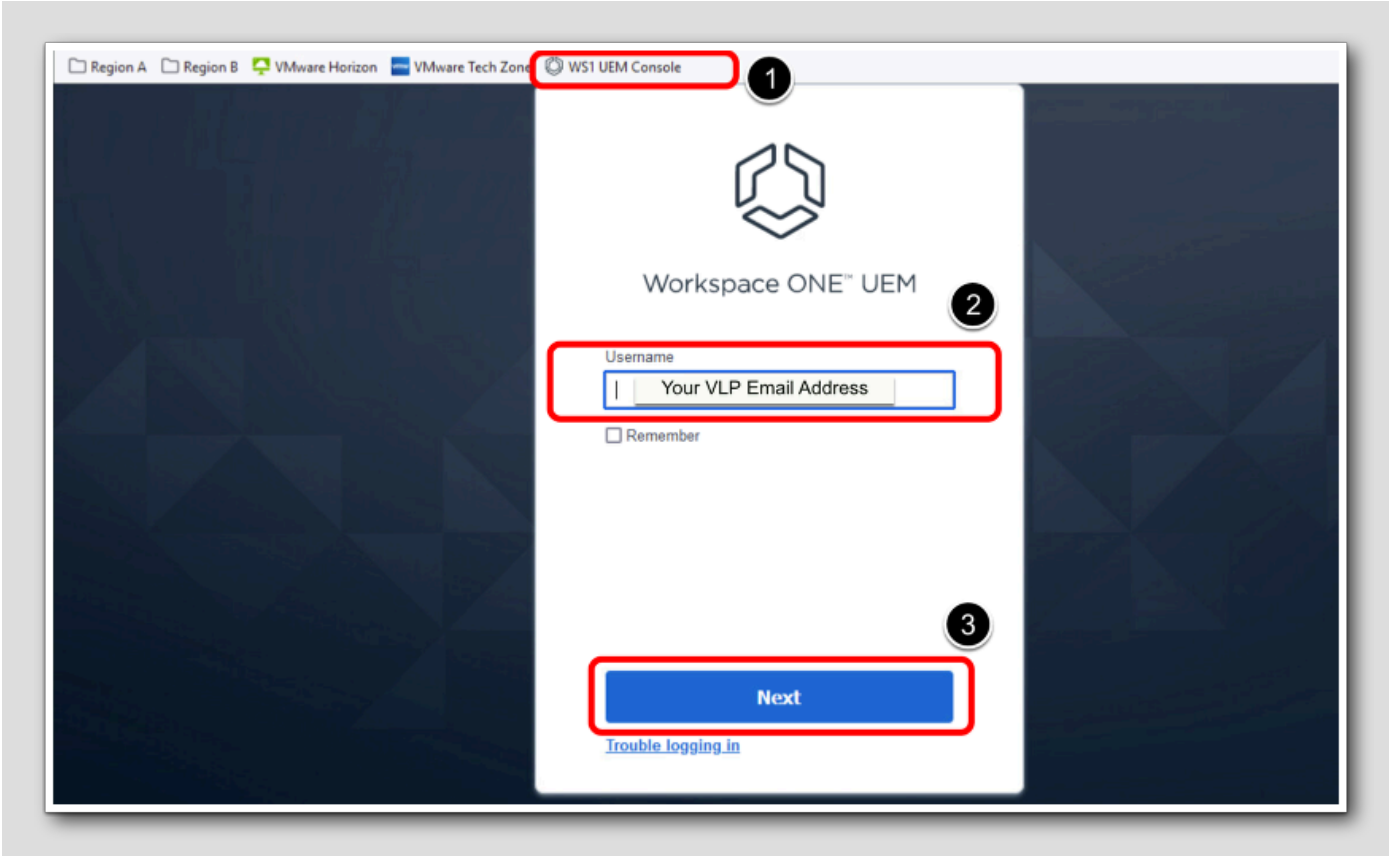
Launch Firefox Browser [423]



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

[424]

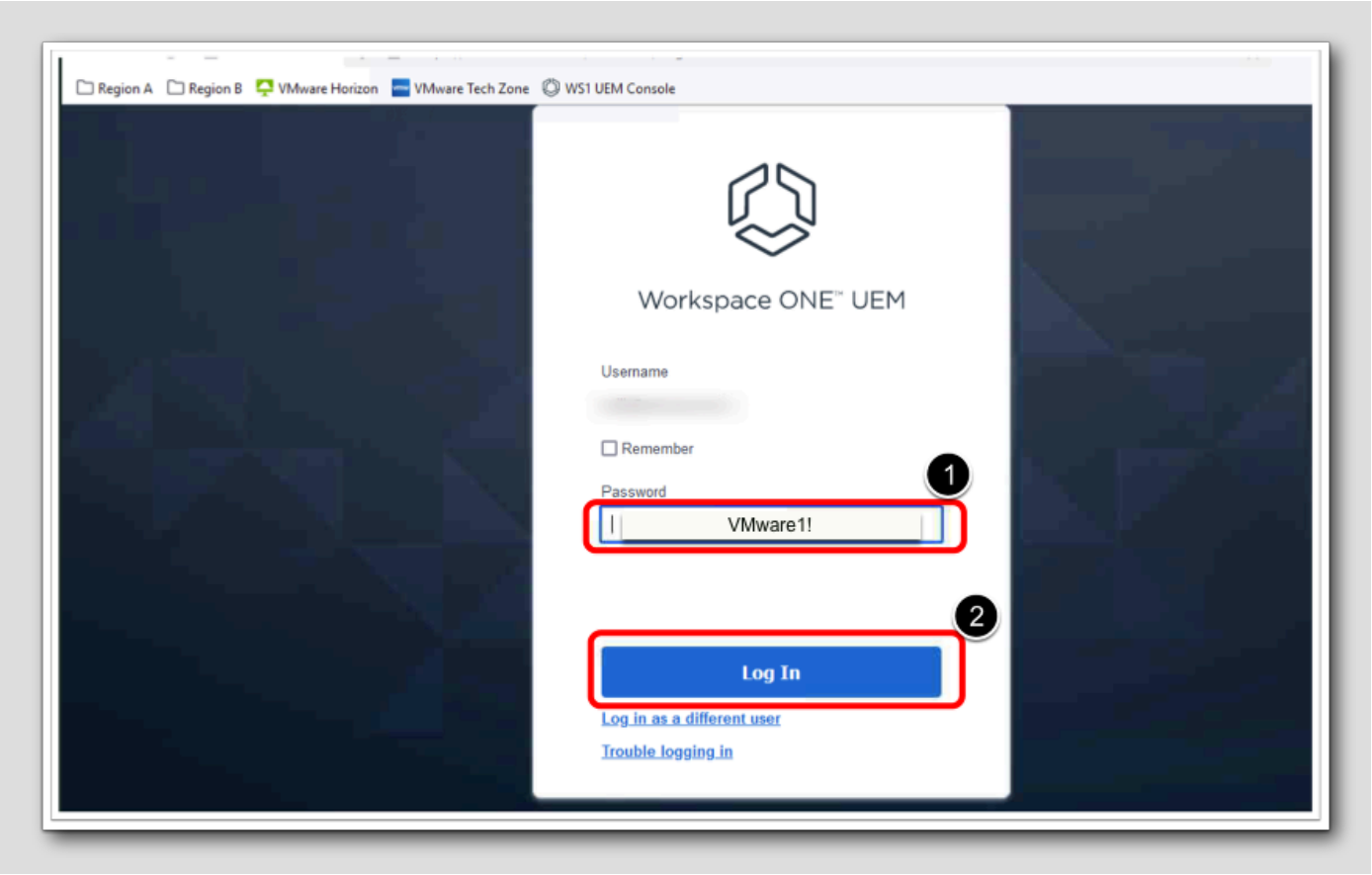


1. Select the **WS1 UEM Console** link from the Bookmark Toolbar
2. Enter your **Username**. This is the **email address** that you have associated with your **VMware Learning Platform (VLP)** account that you utilized to take Hands-on Labs.
3. Click **Next**, then advance to the next step of the lab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

[425]



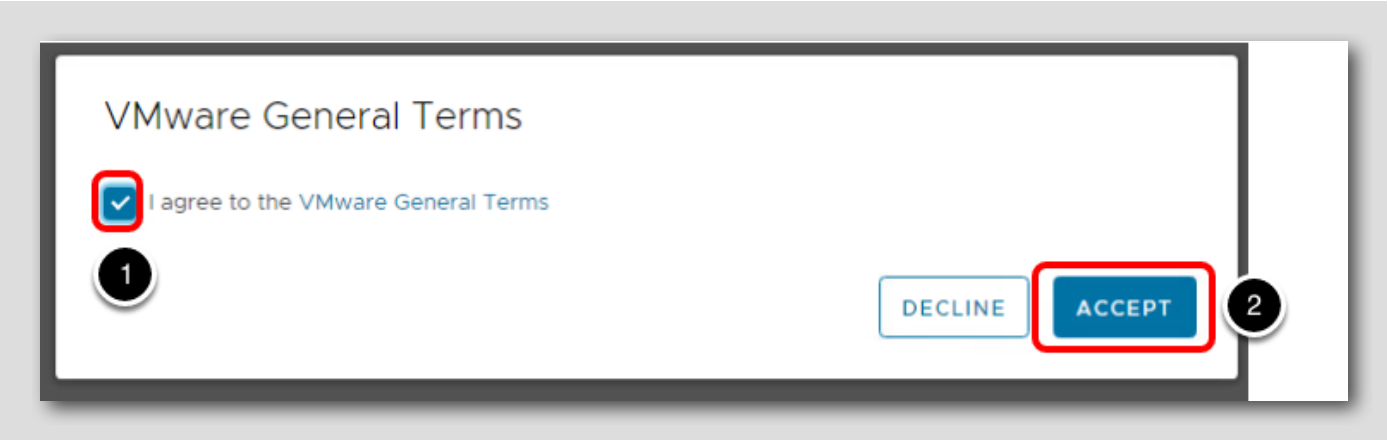
The password field will be displayed after entering your username.

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

[426]



You will be presented with the VMware General Terms.

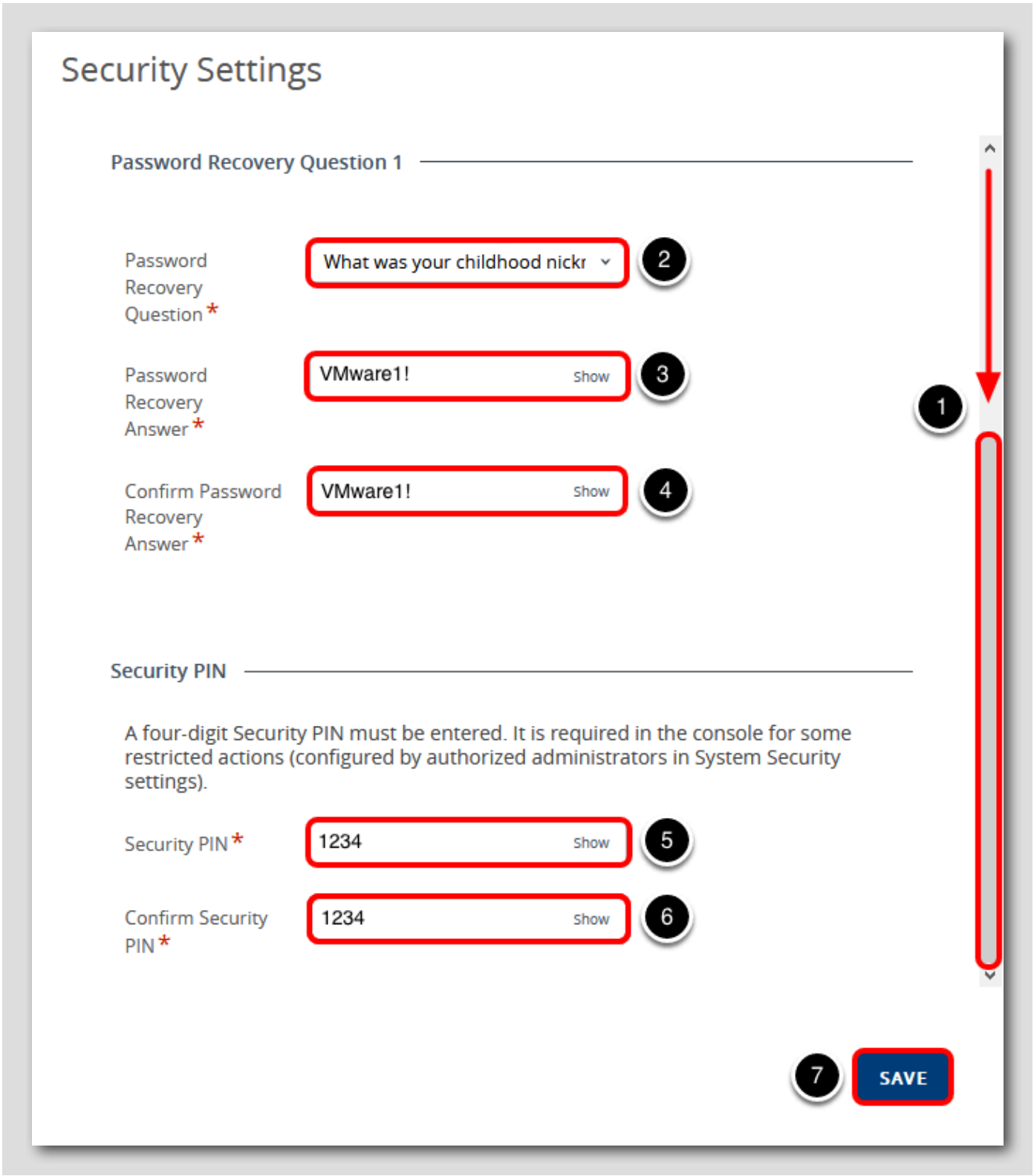
1. Select the box next to I Agree to the VMware General Terms.
2. Click the **Accept** button.

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

[427]

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

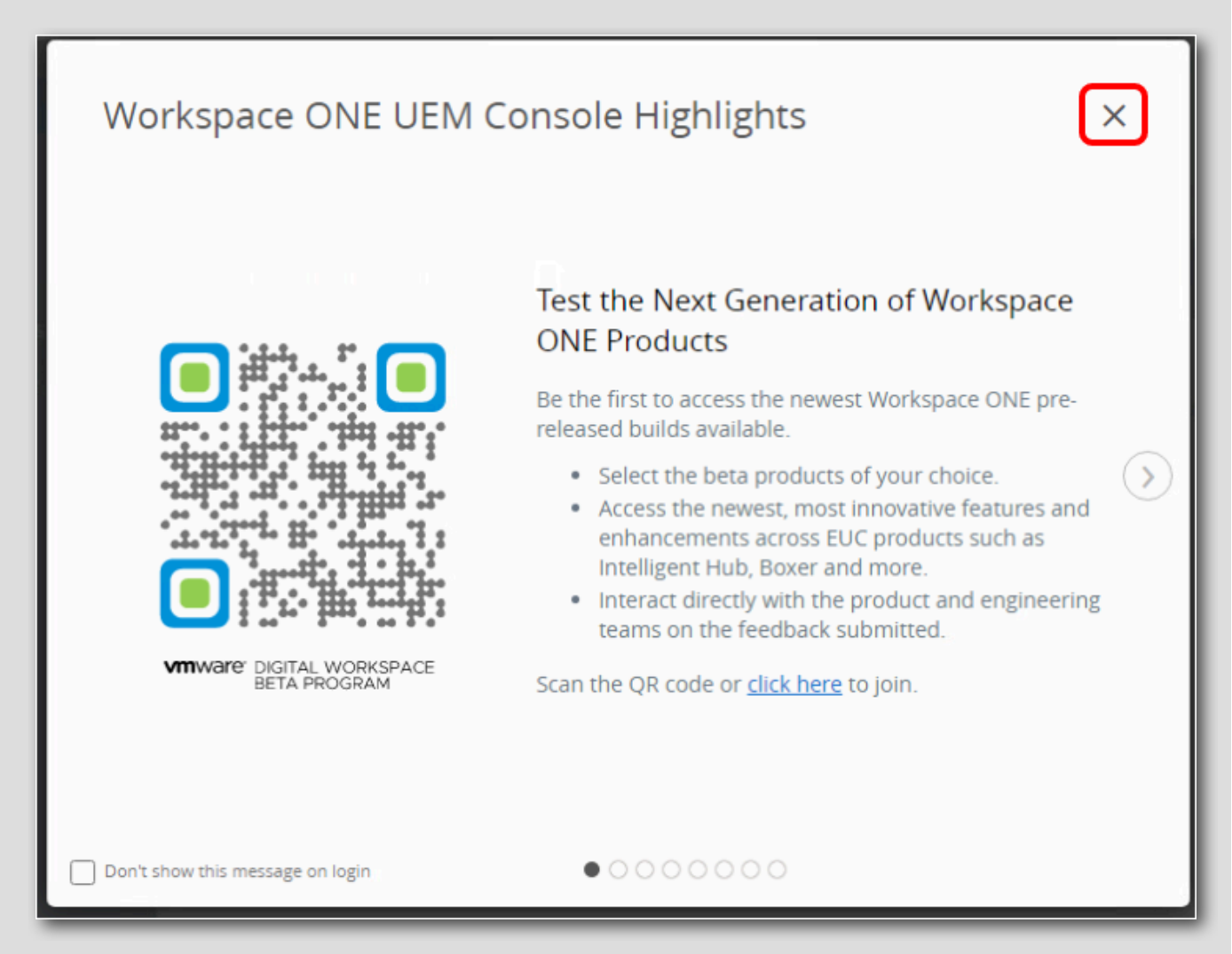

Security Settings
Password Recovery Question 1
Password Recovery Question *
What was your childhood nickr
2
Password Recovery Answer *
VMware1!
Show
3
1
Confirm Password Recovery Answer *
VMware1!
Show
4
Security PIN
A four-digit Security PIN must be entered. It is required in the console for some restricted 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

[428]



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

[429]

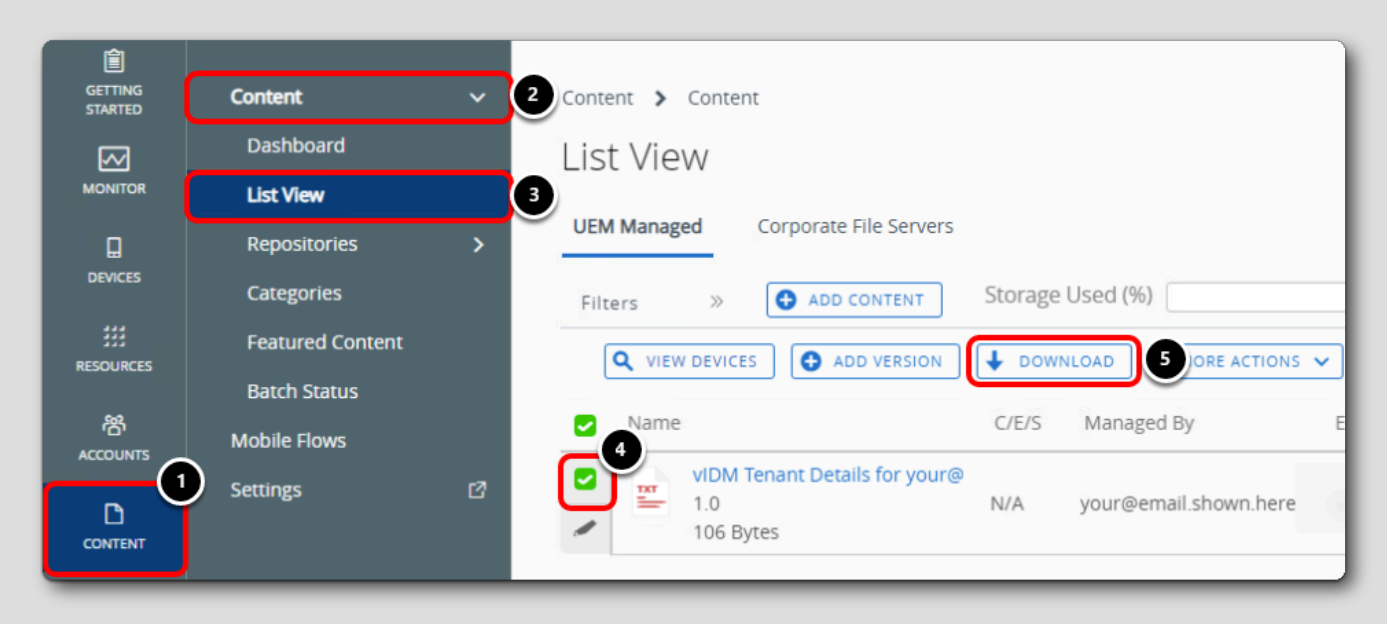
Workspace ONE Intelligent Hub end-user services are configured via the Hub Services admin console. Hub Services is co-located with Workspace ONE Access. Think of Hub Services as the server-side component and Intelligent Hub as the end-user client.

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

[430]

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.

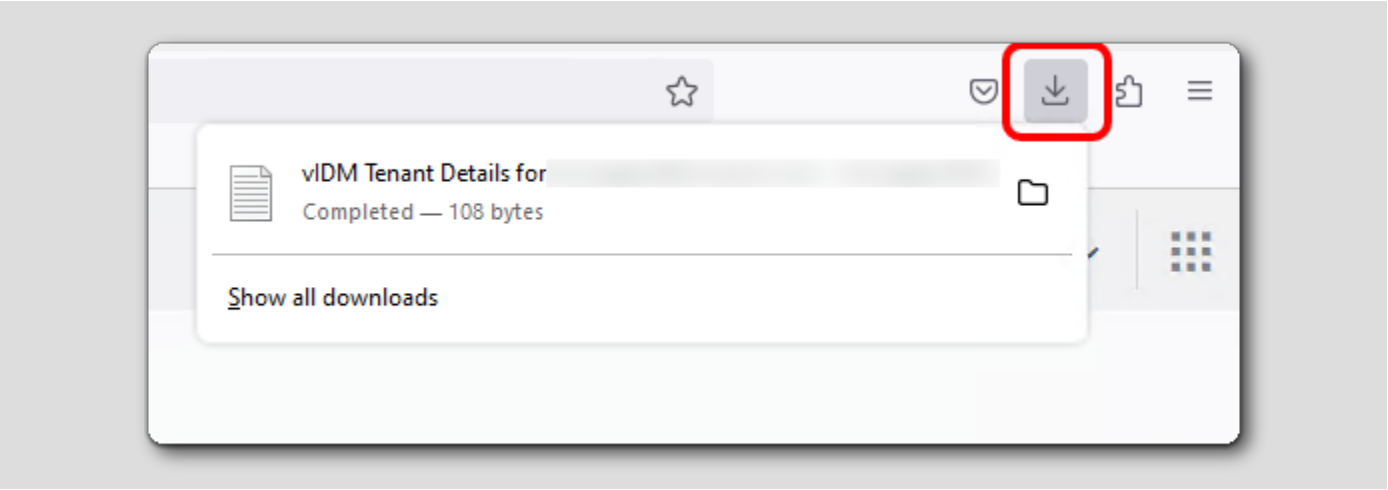


In the Workspace ONE UEM Console:

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

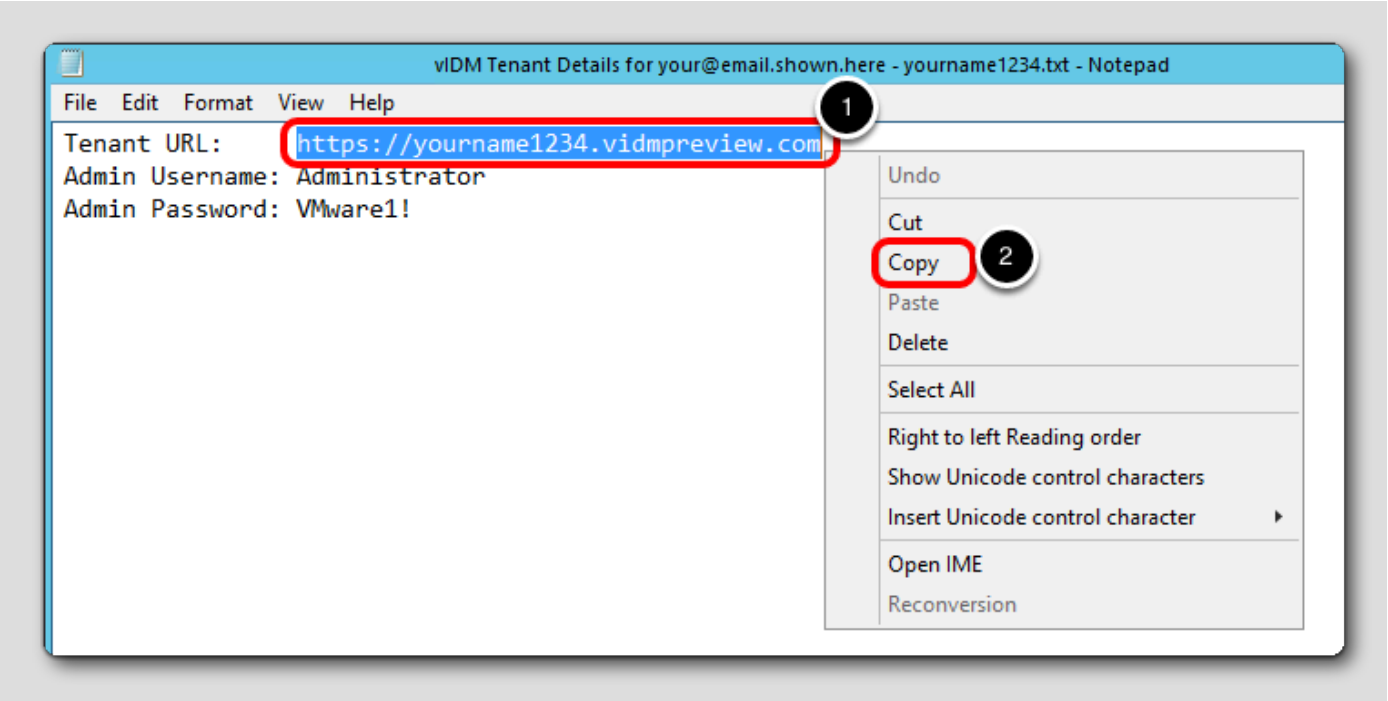
[431]



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

[432]



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.

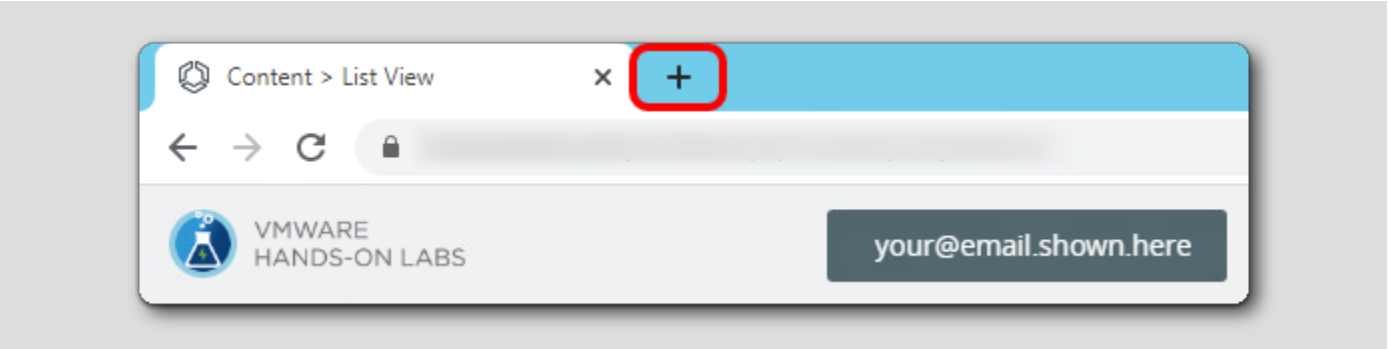
Log into Workspace ONE Access Admin Console

[433]

In this section, we login to the Workspace ONE Access admin console and access the Hub Services admin console.

Open a New Browser Tab

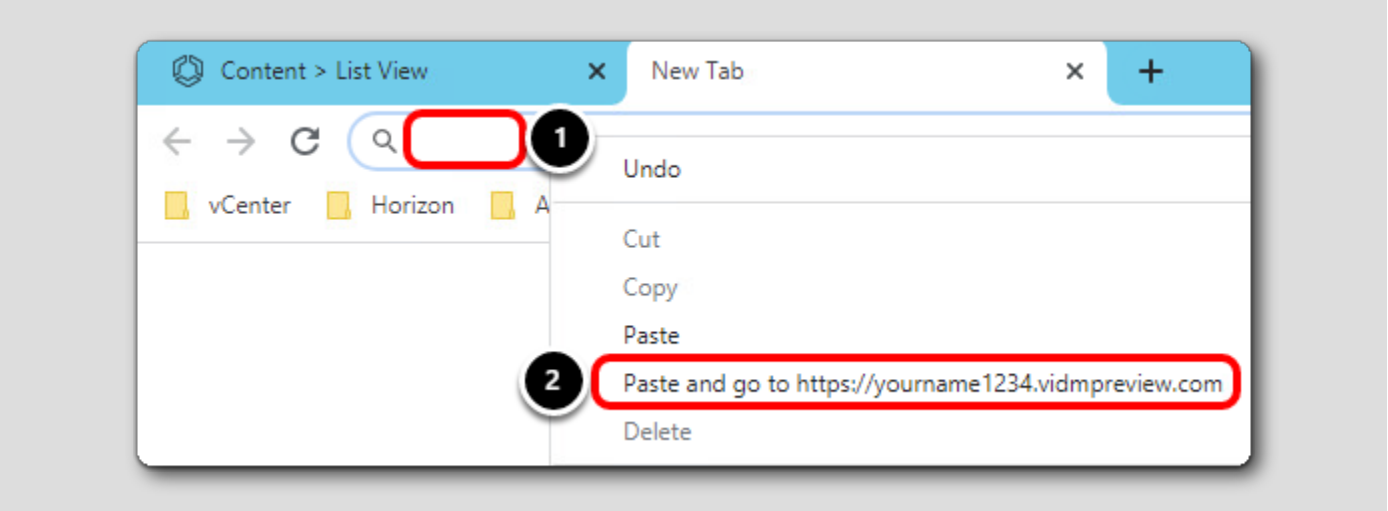
[434]



Click the Add **Tab button** in the browser to open a new tab.

Navigate to Your Workspace ONE Access Tenant URL

[435]

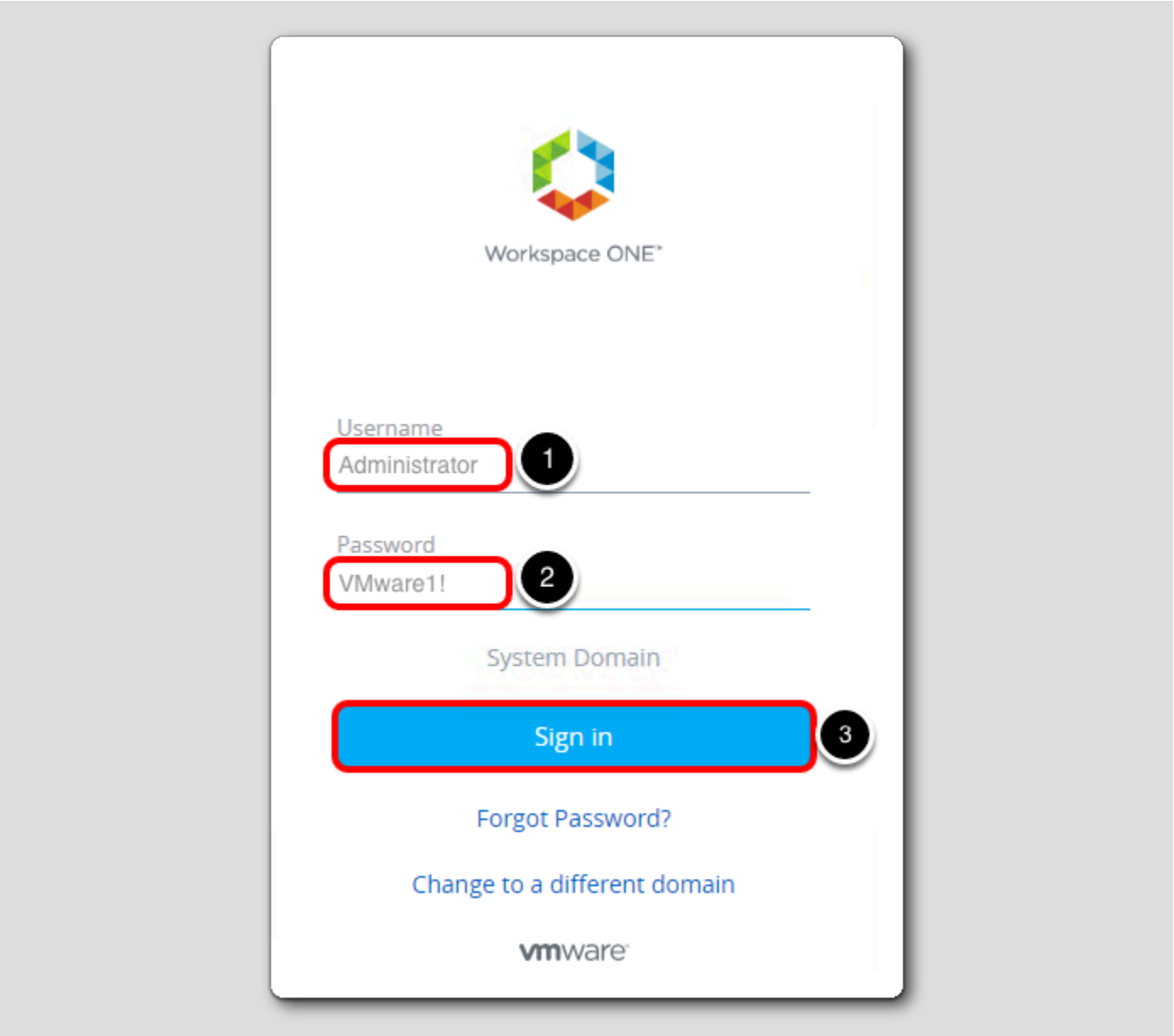


1. Right-click **inside the address bar** in the new tab.
2. Click **Paste and go to** the URL.

NOTE: This is the Workspace ONE Access tenant URL you received from the previous steps. If you did not copy or note this information from the previous step, return to those previous steps and note your Workspace ONE Access tenant URL.

Login to Your Workspace ONE Access Tenant

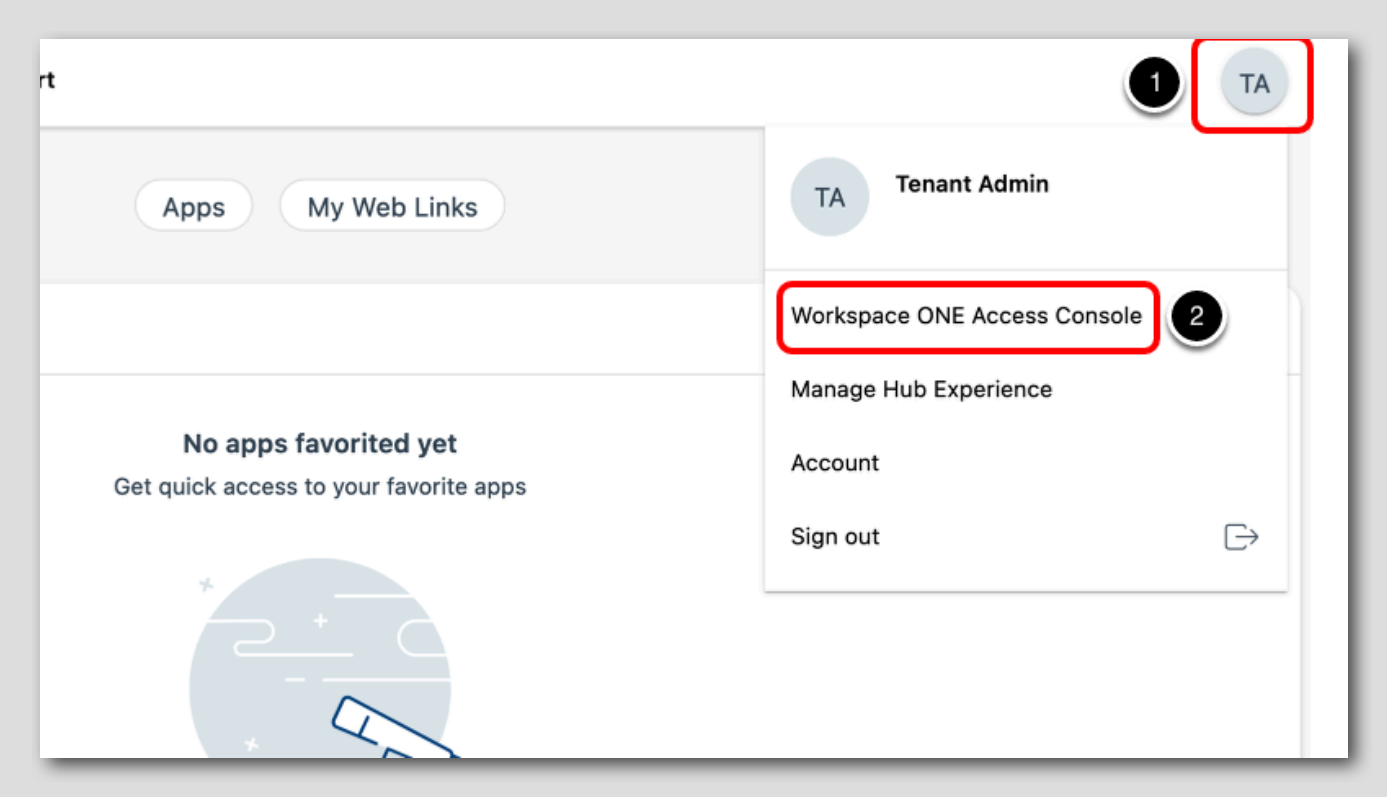
[436]



1. Enter **`Administrator`** for the Username
2. Enter **`VMware1!`** for the Password
3. Click **Sign In**

Navigate to the Administrator Console

[437]



After logging in, you will see the Intelligent Hub User Portal as pictured above. You will need to navigate to the Administrator Console.

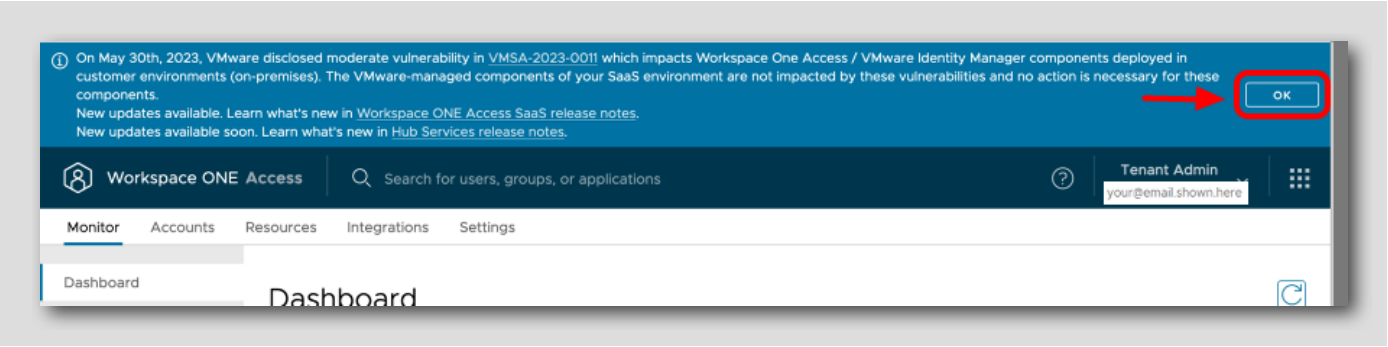
1. Click the **User dropdown circle** in the top-right corner.
2. Click **Workspace ONE Access Console.**

This will open the Administration Console in a separate tab in your browser.

NOTE: If you do not see the above view, you are already in the Administration Console and can skip this step.

(Optional)Dismiss the Release Notes Banner

[438]



If you see a banner about Security Updates or Release Notes details, click **OK** on the far right to dismiss it.

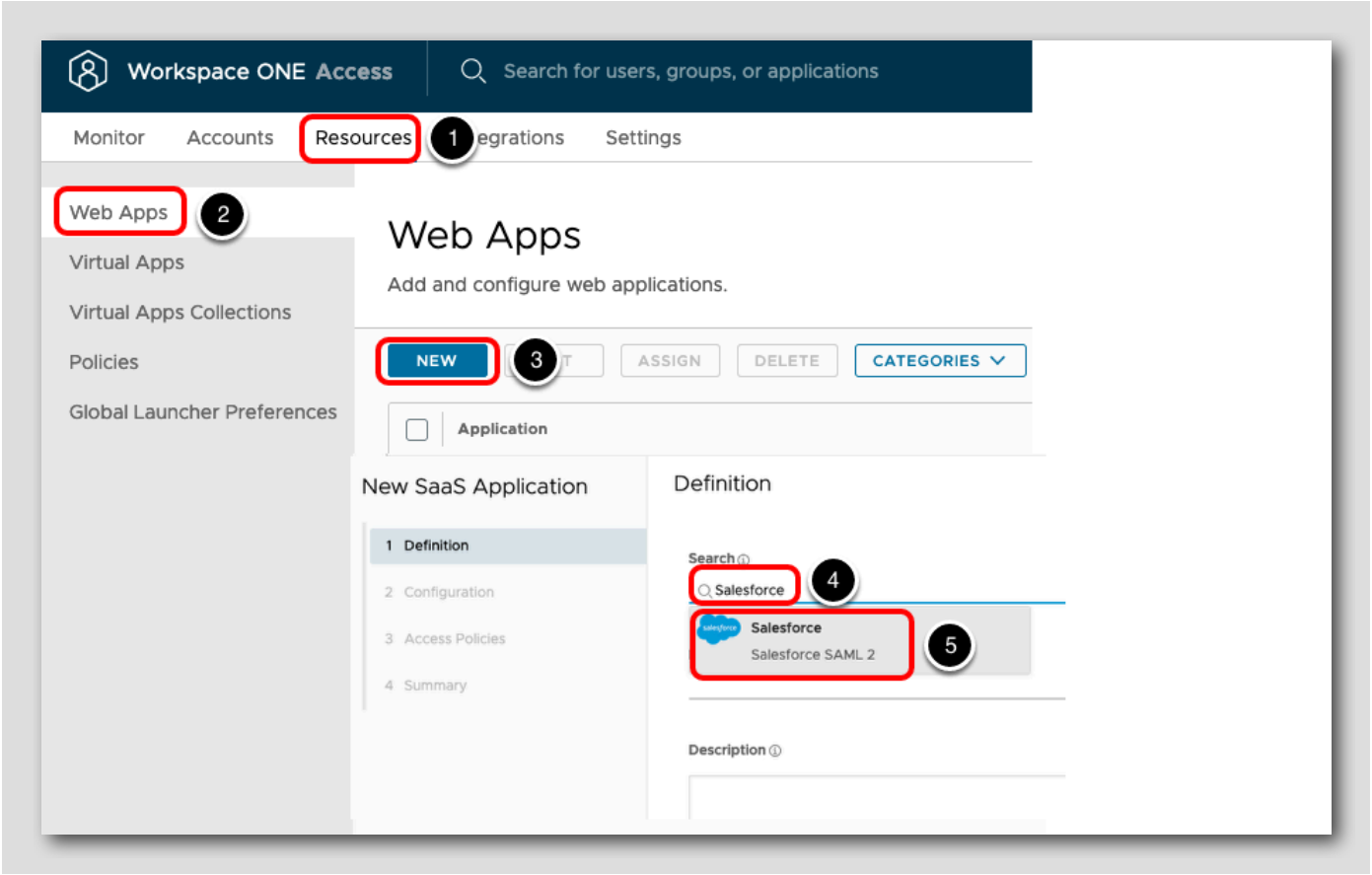
Add a SaaS App to the App Catalog

[439]

We will add an example SaaS App to our app catalog to utilize in a later section.

Navigate to the Workspace ONE Access App Catalog and Add SaaS App

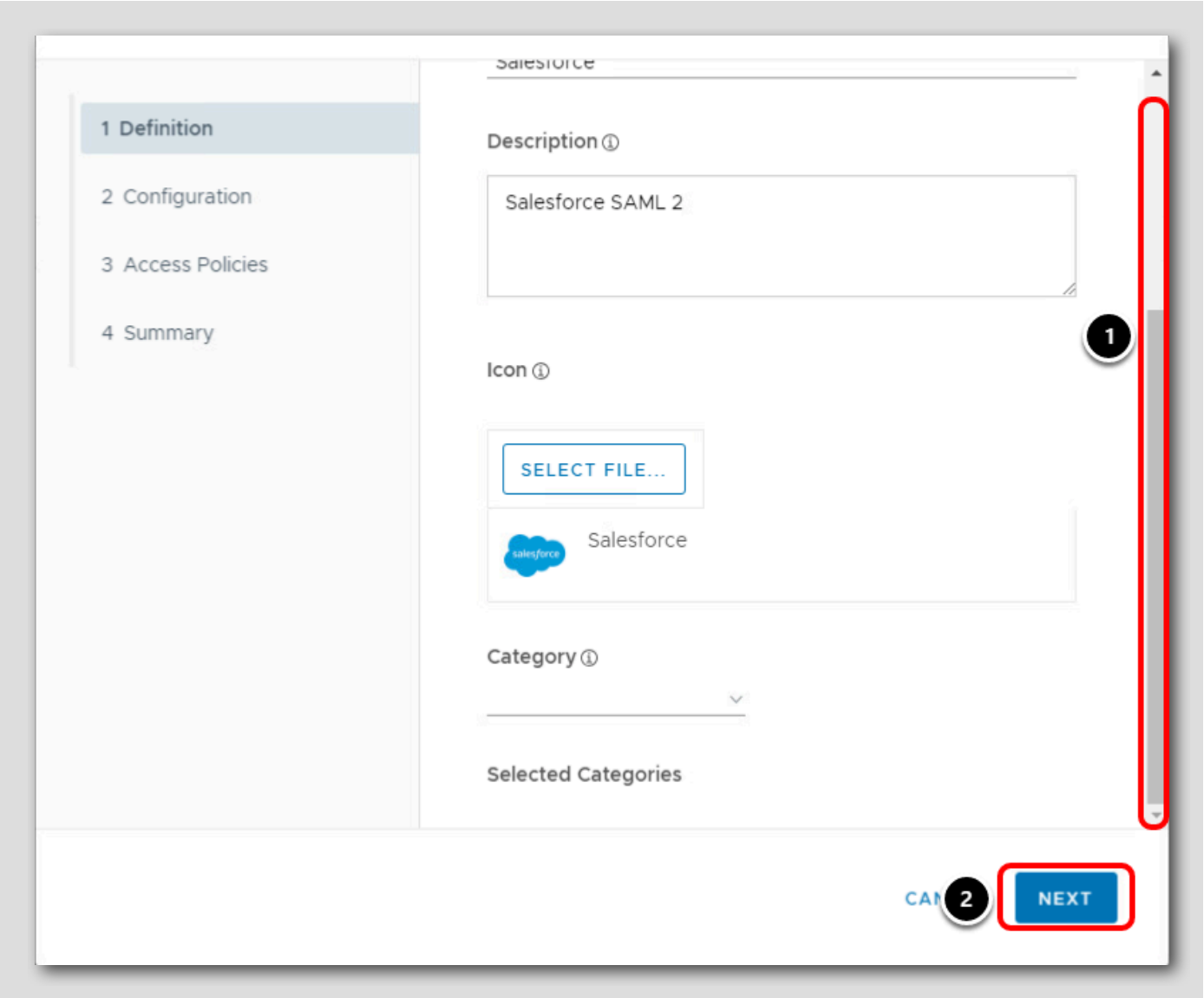
[440]



1. Click the **Resources tab**
2. Click the **Web Apps**
3. Click **New**
4. Type **`Salesforce`** into the Search field.
5. **Click** on **Salesforce** in the search results.

New SaaS App Definition Section

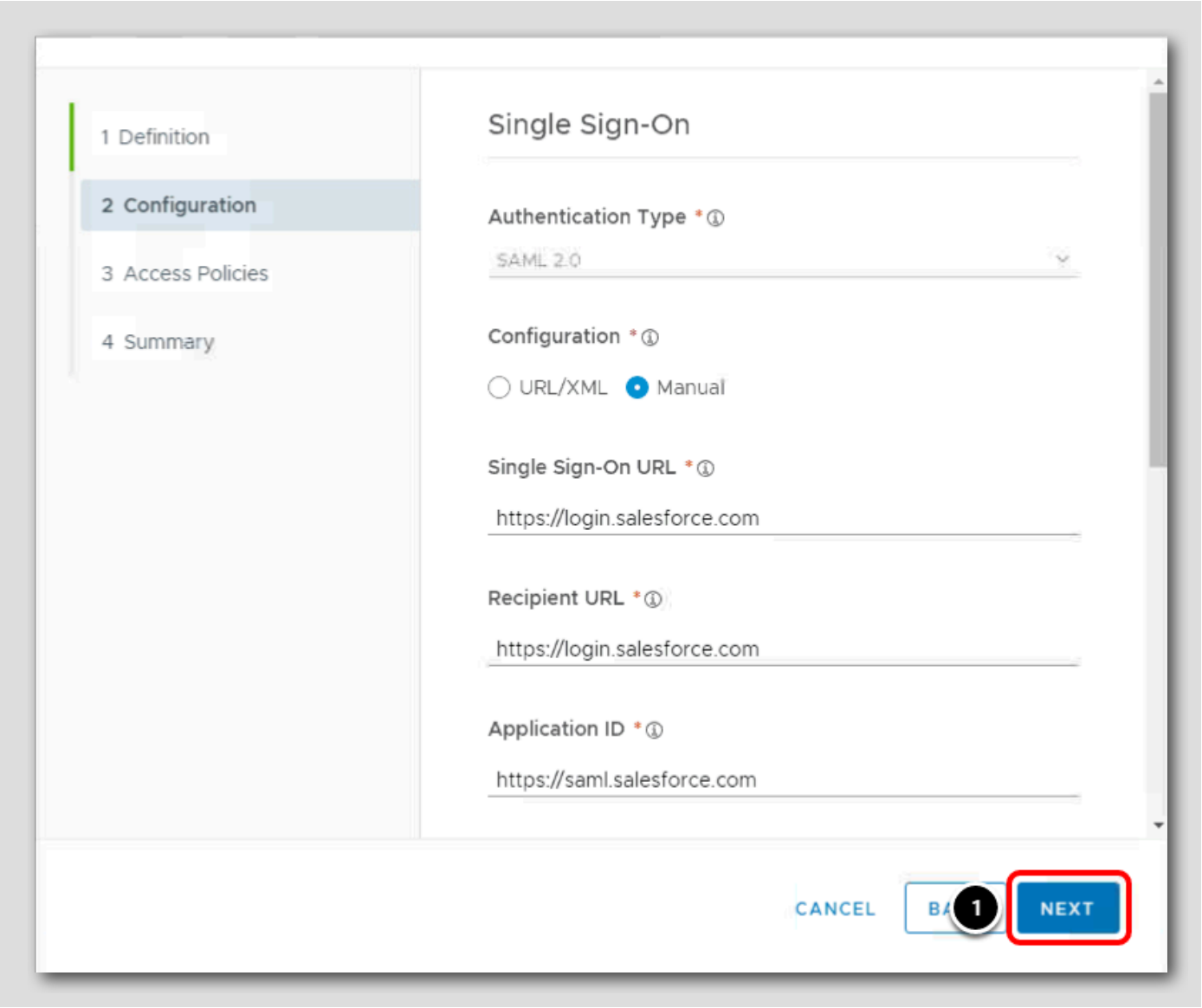
[441]



1. Scroll down
2. Click the **NEXT** button

New SaaS App Configuration Section

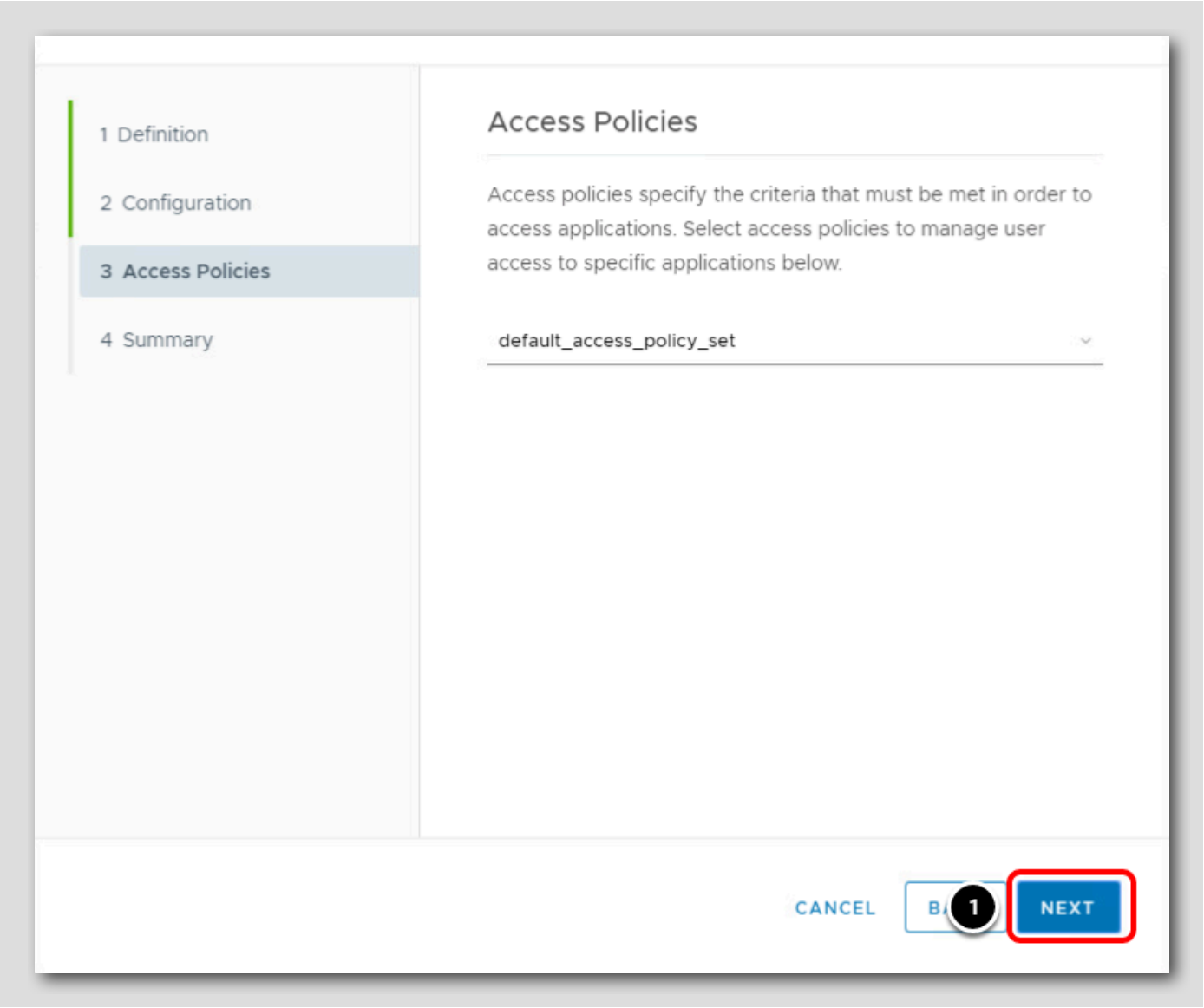
[442]



1. Keep default settings and click **NEXT**

New SaaS App Access Policies Section

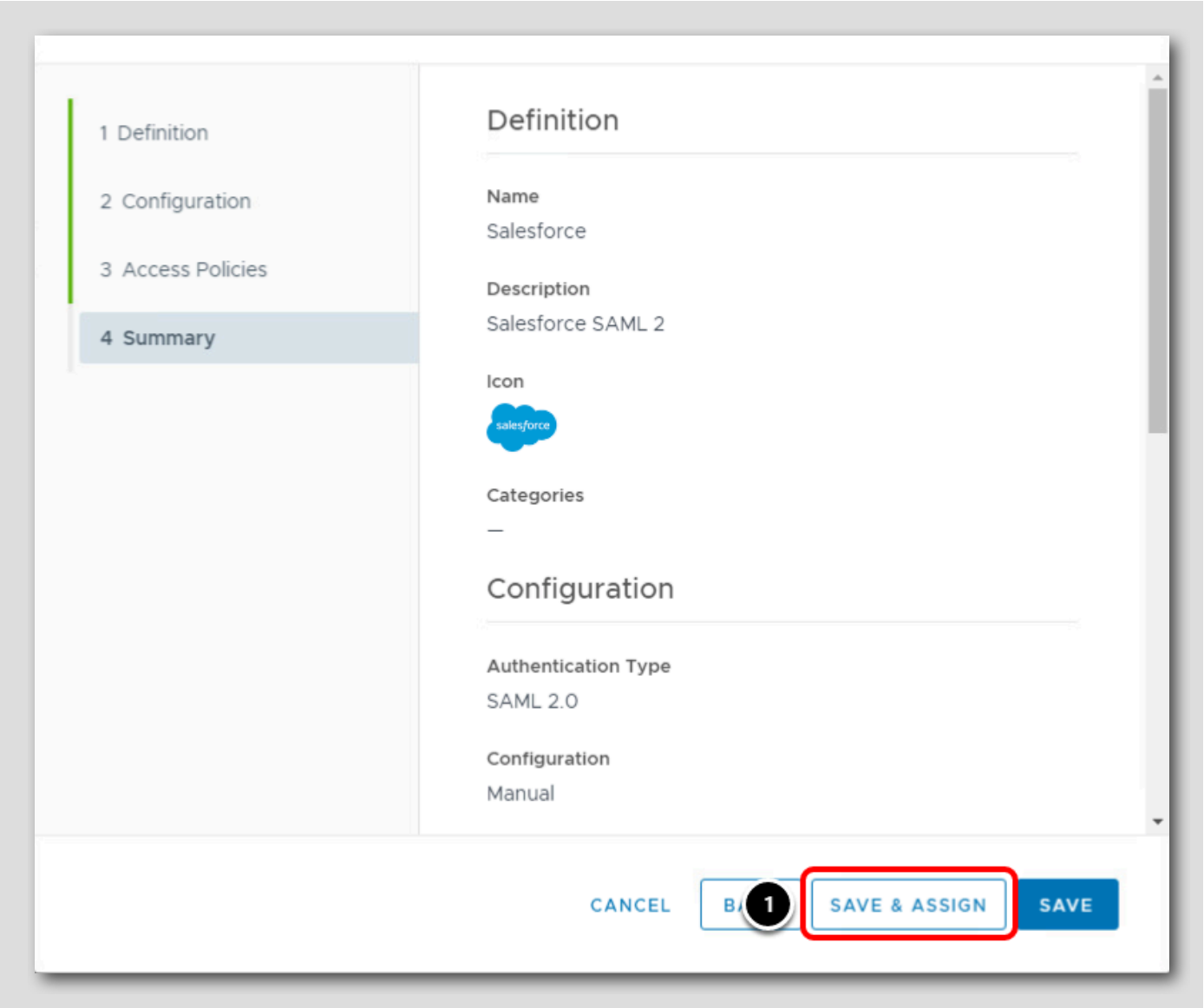
[443]



1. Keep default access policy and click **NEXT**

New SaaS App Summary Section

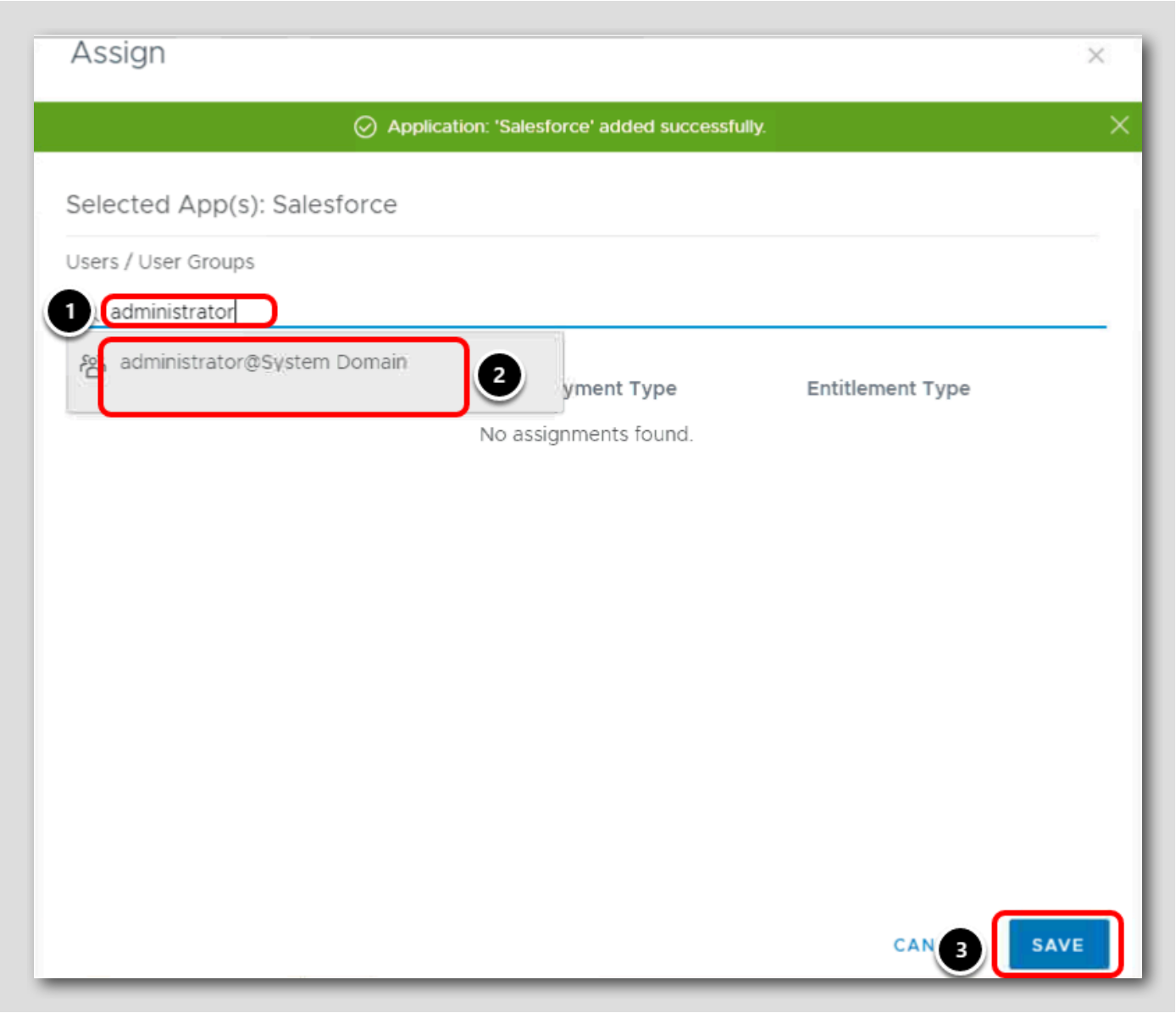
[444]



1. Click **SAVE & ASSIGN**

Assign New SaaS App to User

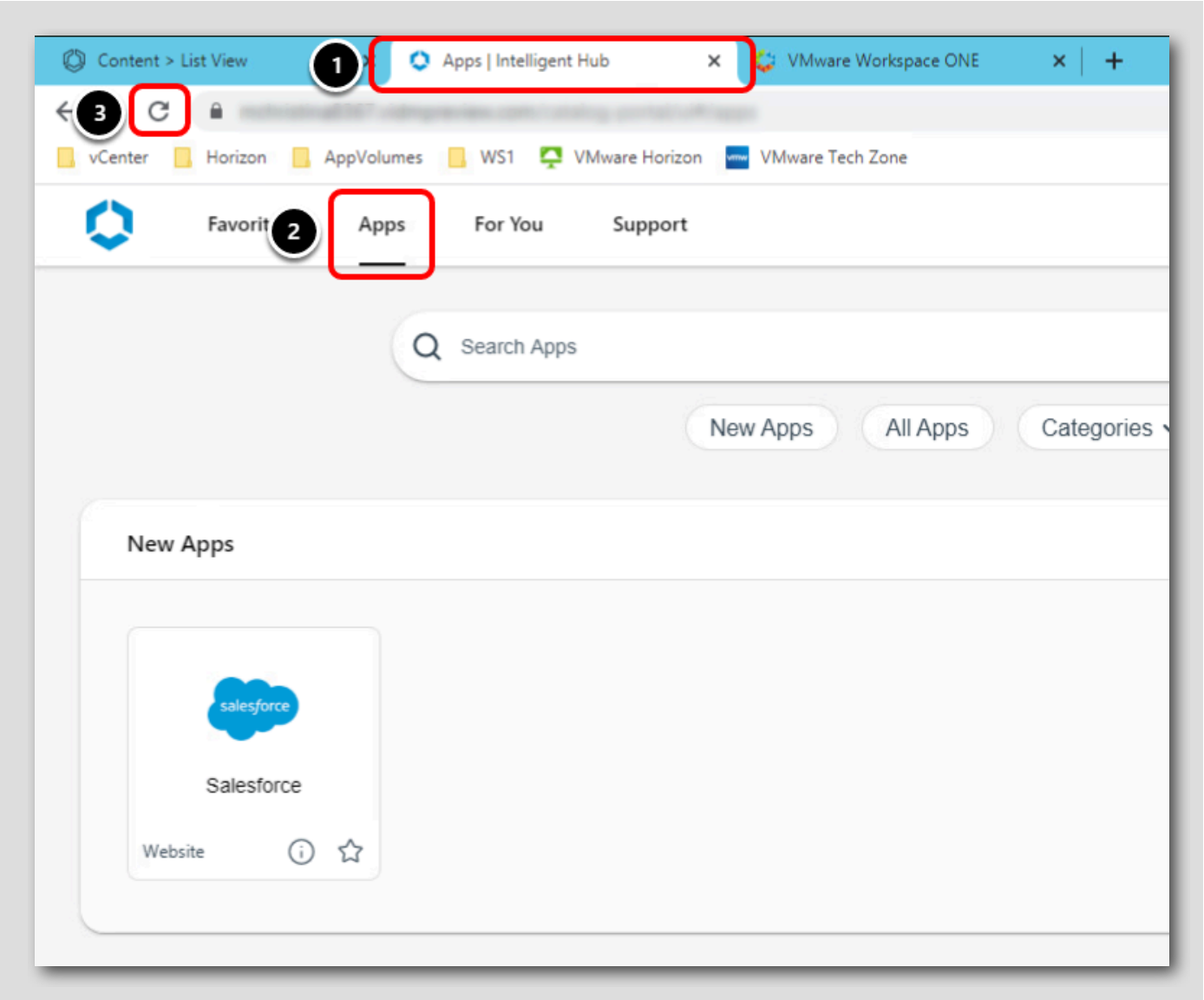
[445]



1. Type **administrator** into the Users / User Groups search field
2. Click **administrator@System Domain** in the search results
3. Click **SAVE**

Confirm SaaS App Added to User's Catalog

[446]



1. Click back to the **second tab in the browser**, which is the Intelligent Hub User Portal.
2. Click the **Apps tab** to view the App Catalog.
3. Click the **refresh button** in the browser to refresh the catalog. You will now see Salesforce in the App Catalog.

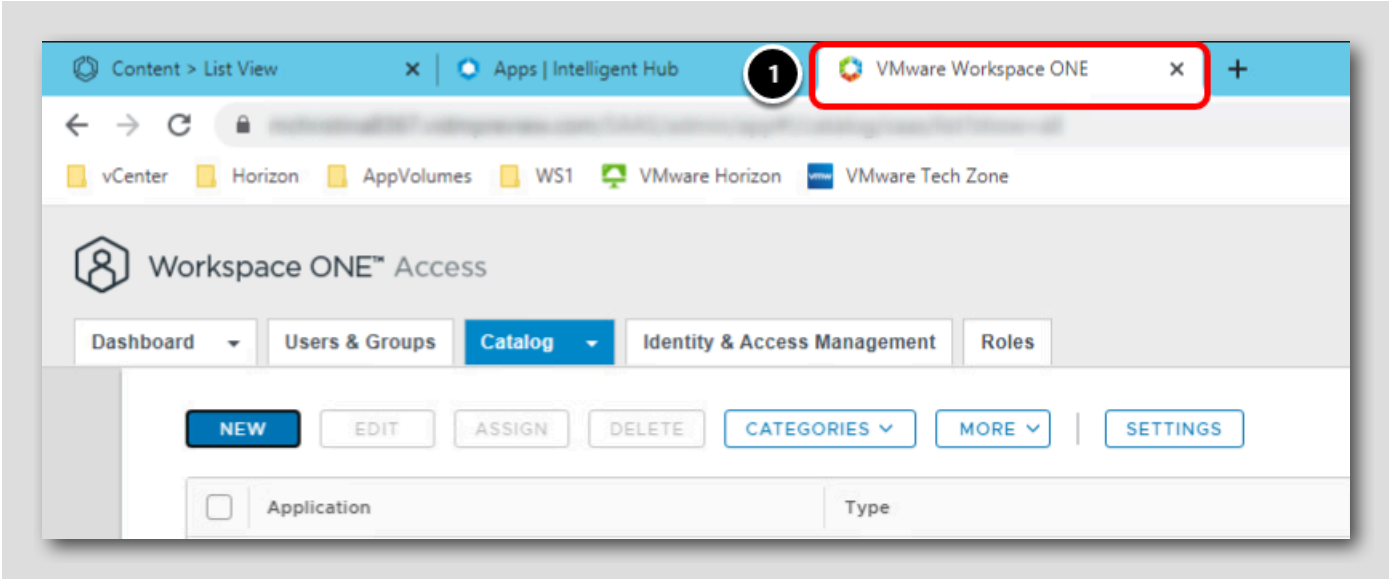
Navigate to Hub Services Admin Console and Complete Hub Templates Wizard

[447]

The following section will get you started in the Hub Services admin console and introduce you to Hub Templates.

Return to the Workspace ONE Access Admin Console

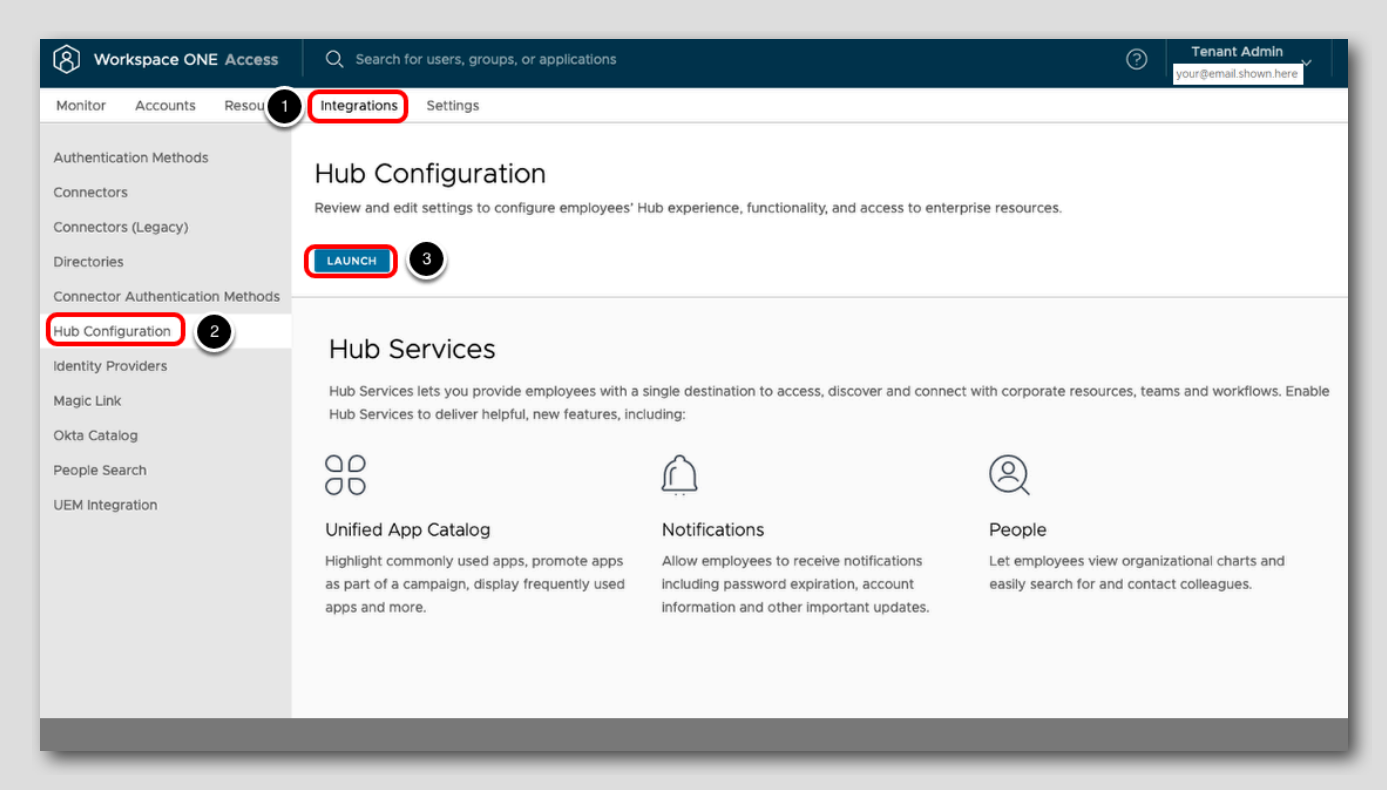
[448]



1. Click the third tab in the browser to return to the Workspace ONE Access admin console.

Launch Hub Services

[449]



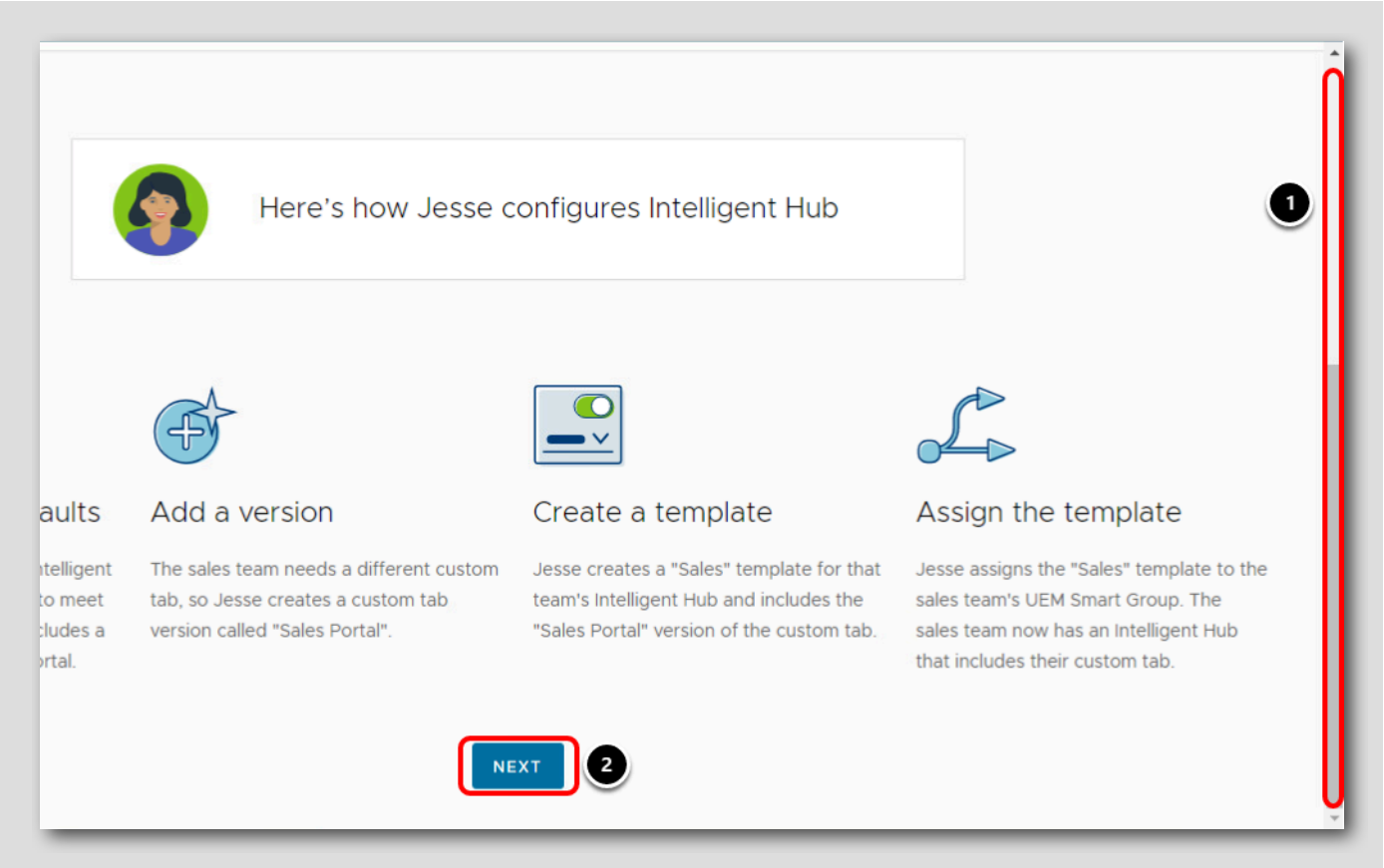
1. Click the **Integrations tab**
2. Click on **Hub Configuration**
3. Click **Launch**

Hub Templates Wizard

[450]

The 20.08 release of Hub Services had a significant addition to support wider adoption of Hub Services and Intelligent Hub features called Hub Templates. Before 20.08, any Hub Services configurations for Intelligent Hub were all or nothing - all employees received the same configurations. This limited the administrator's ability to roll out features in phases or accommodate different teams or divisions. Now admins can create one or more templates with unique Hub Services capabilities and assign them to UEM Smart Groups or Workspace ONE Access User Groups to control the Intelligent Hub experience for their employees. Hub Templates is available with Hub Services 20.08 SaaS release and later and requires UEM 20.08 at minimum and at least the 20.08 version of the Intelligent Hub clients.

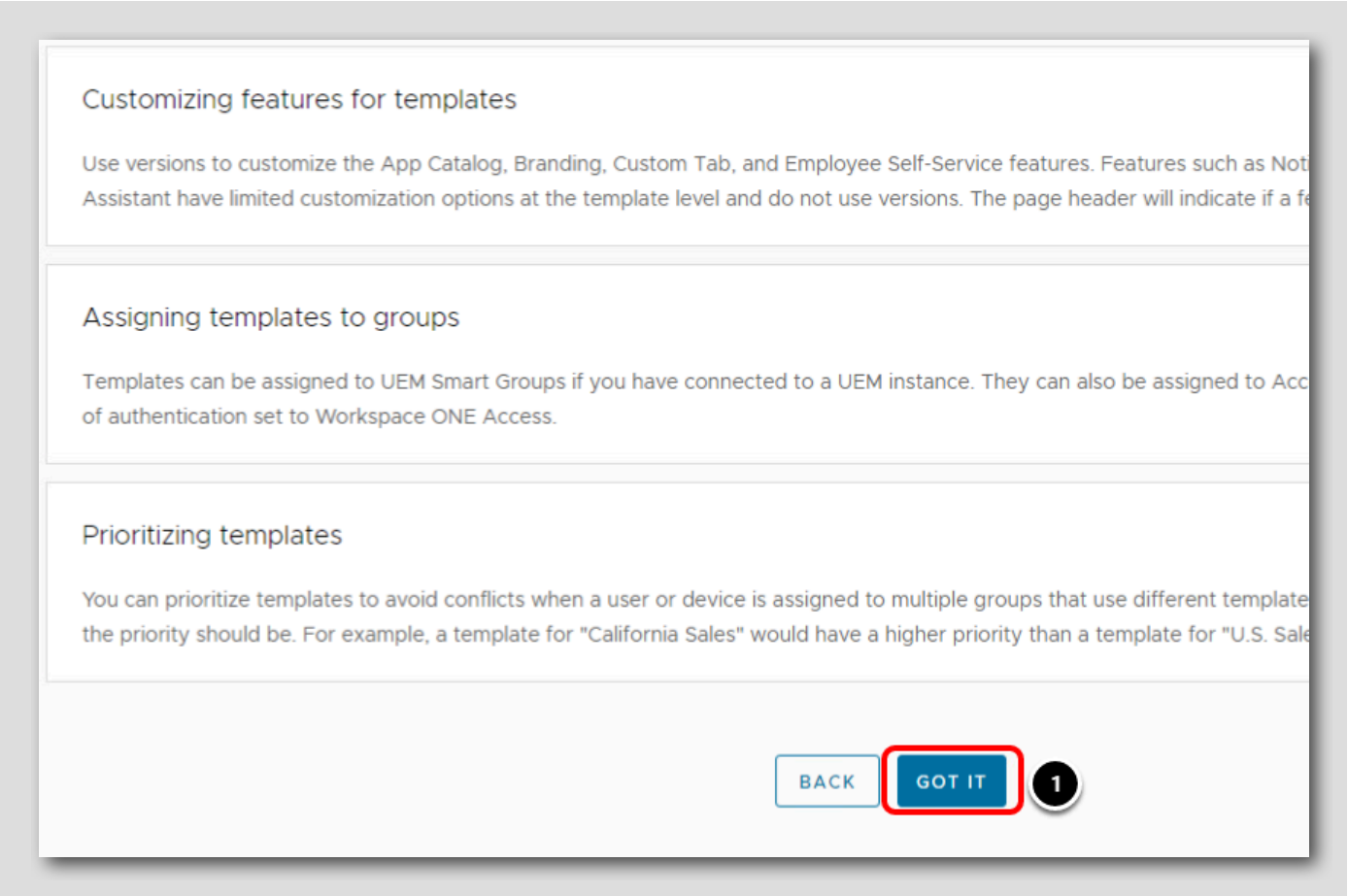
For environments that already have Hub Services enabled, after upgrading to 20.08, admins will see the migration wizard. The admin can choose whether to migrate the app catalog settings from the UEM console, or create new global settings.



1. This screen provides an introduction to Hub Templates. **Scroll down** to find the Next button.
2. Click the **Next button.**

Hub Templates Wizard (continued)

[451]

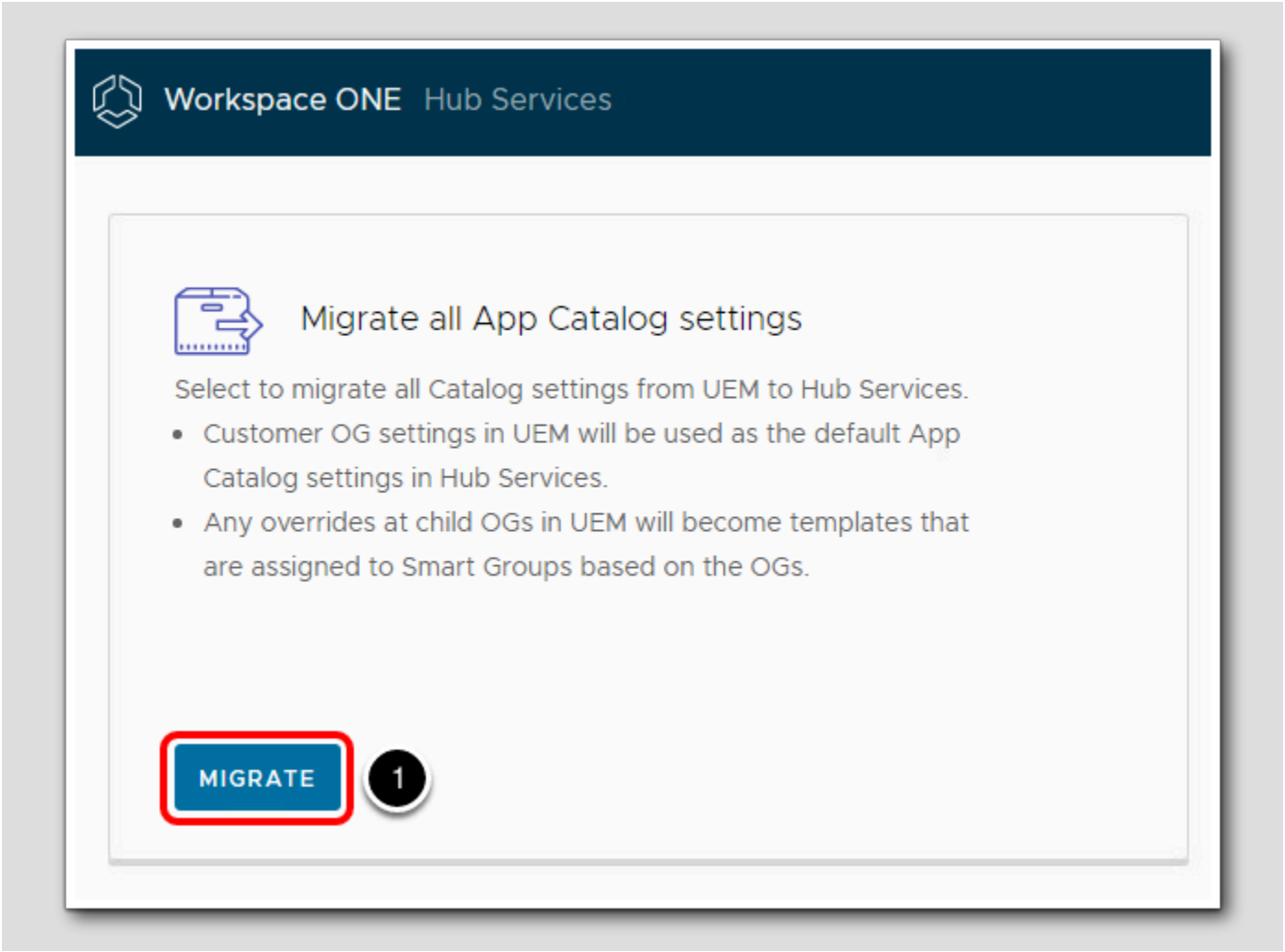


1. You can read more about Hub Templates configuration steps. Then click the **GOT IT button**.

Migrate App Catalog Settings

[452]

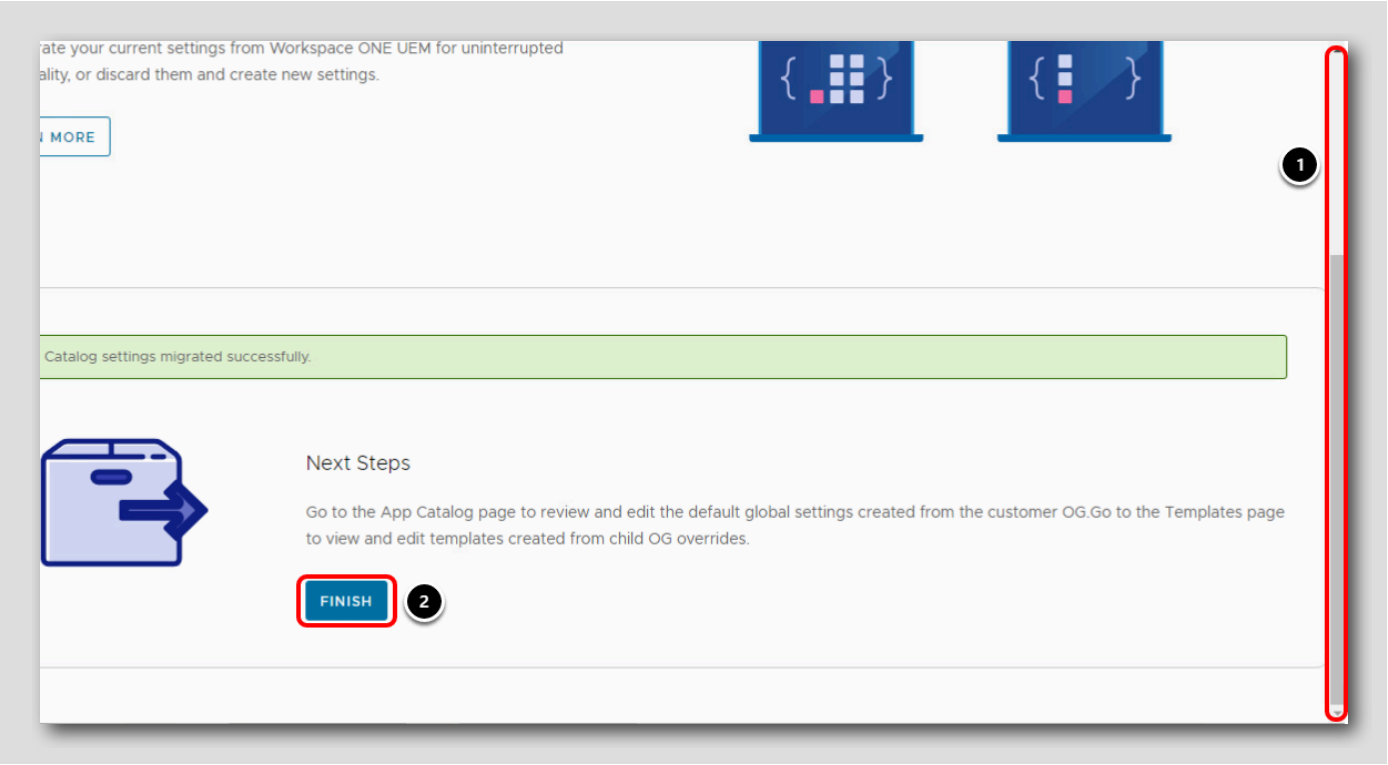
Starting with the 20.08 UEM release, all Intelligent Hub app catalog settings are now in the Hub Services console. For environments with Hub Services already configured, the administrator can choose to migrate app catalog settings from Workspace ONE UEM.



1. Click the **Migrate button**.

Confirm Migration

[453]



1. Scroll down to find the FINISH button.
2. Click the FINISH button.

Add App Catalog and Custom Tab Versions

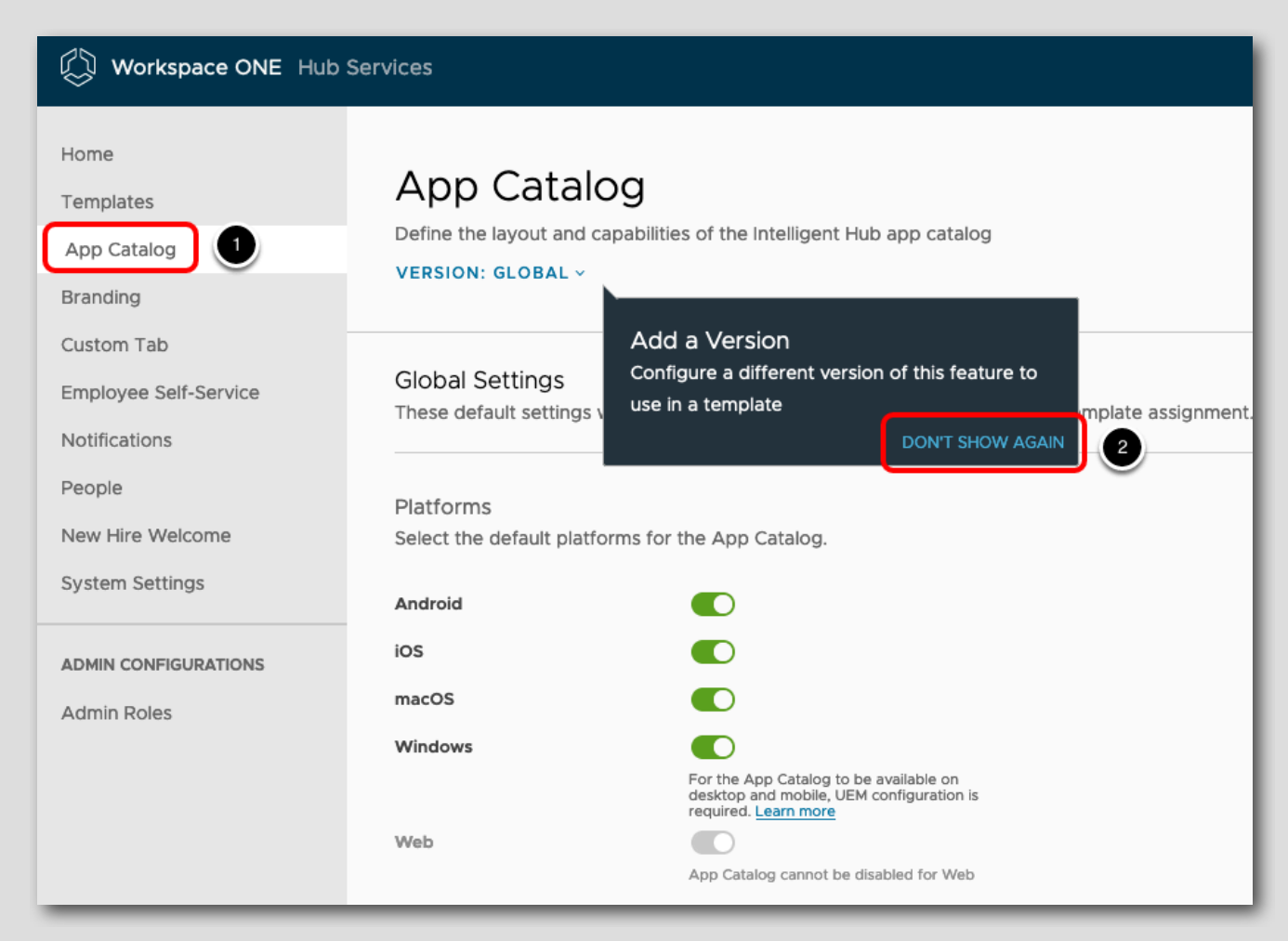
[454]

Before we can create a template for Intelligent Hub settings, we first need to configure a few of the available features for our end users.

Access the App Catalog Settings

[455]

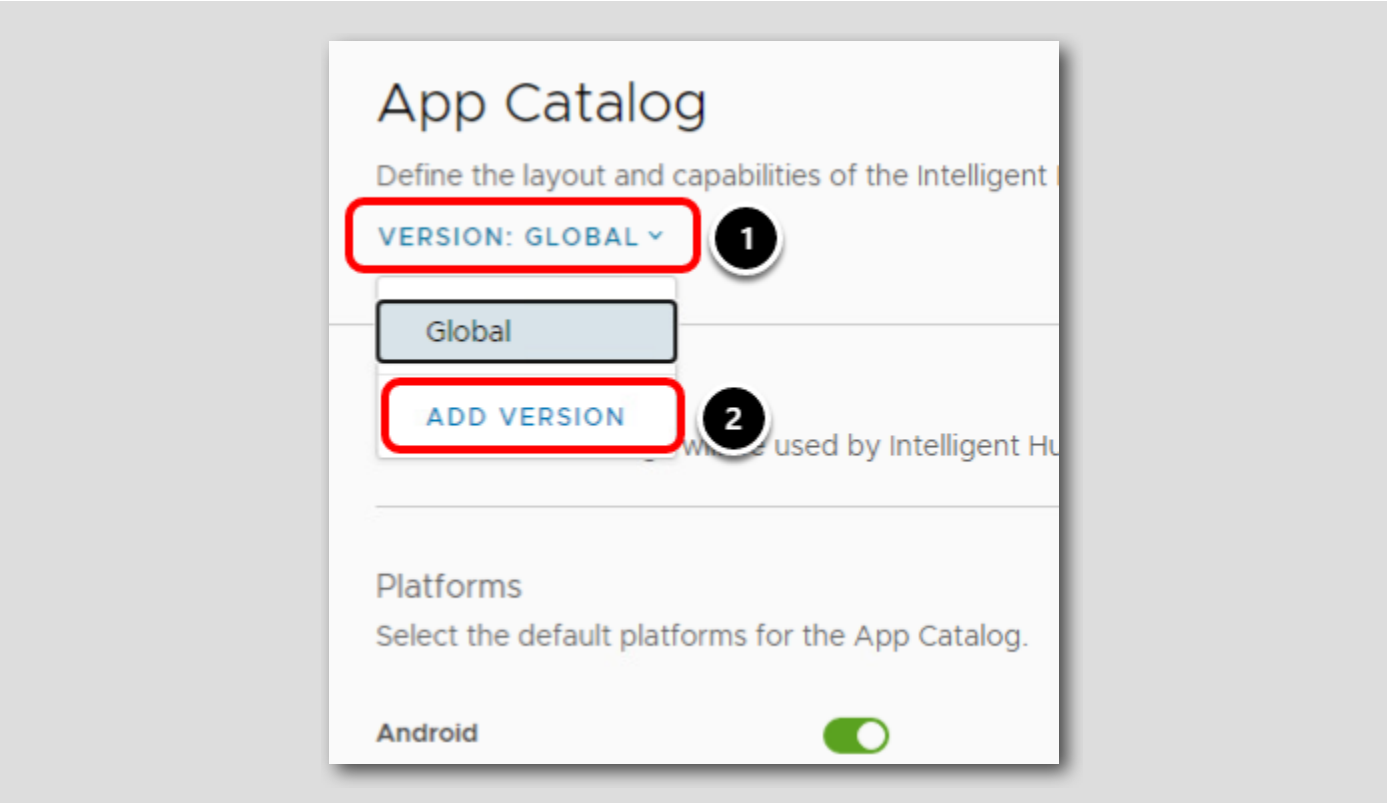
The App Catalog tab allows you to define the layout and capabilities of the Intelligent Hub app catalog that is presented to your users. We will modify the catalog by adding a promotion for the Salesforce app, highlighting this app in our catalog, and then disable the use of Virtual Apps on mobile devices.



1. Click the **App Catalog** menu item on the left.
2. You may see a notification to Add a Version indicating we can create different versions of the app catalog for different groups of users. Click **DON'T SHOW AGAIN**.

Add App Catalog Version

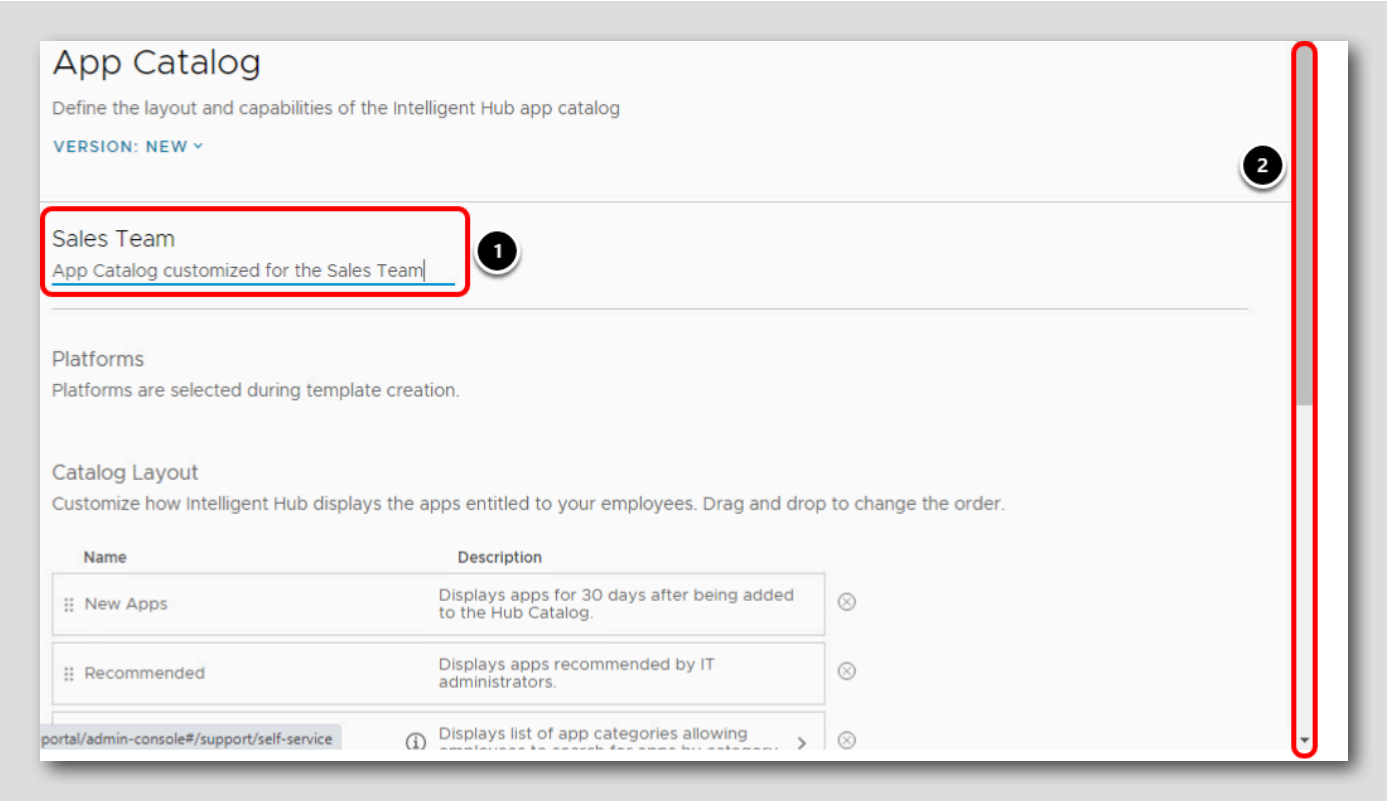
[456]



1. Click the **VERSION: GLOBAL** dropdown.
2. Click **ADD VERSION**.

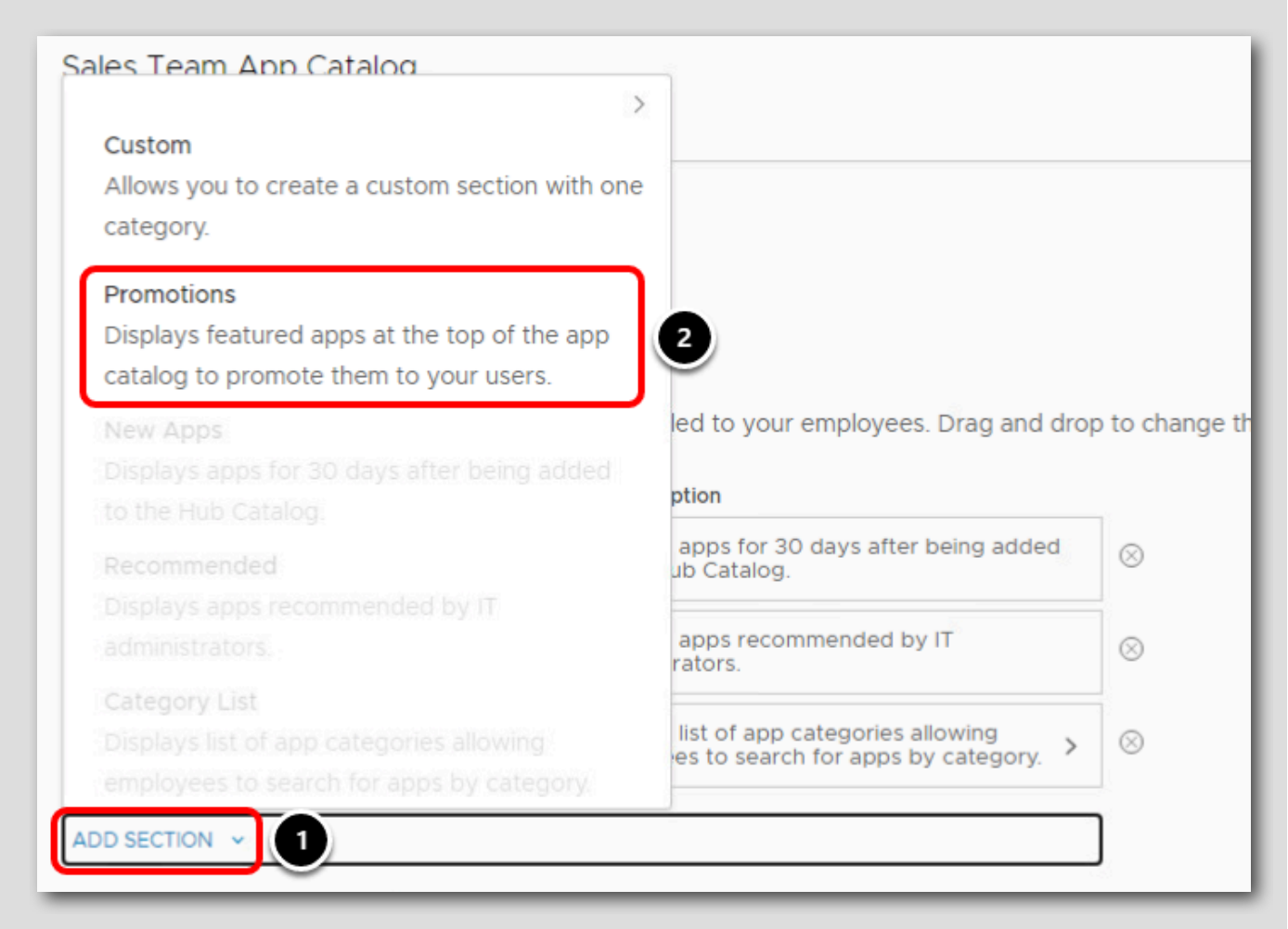
Name the App Catalog Version for the Sales Team

[457]



1. Enter the version name **`Sales Team`** and add description **`App Catalog customized for the Sales Team`**.
2. Scroll down and look for the **ADD SECTION dropdown** under the Catalog Layout section.

Customize the App Catalog Layout for the Sales Team

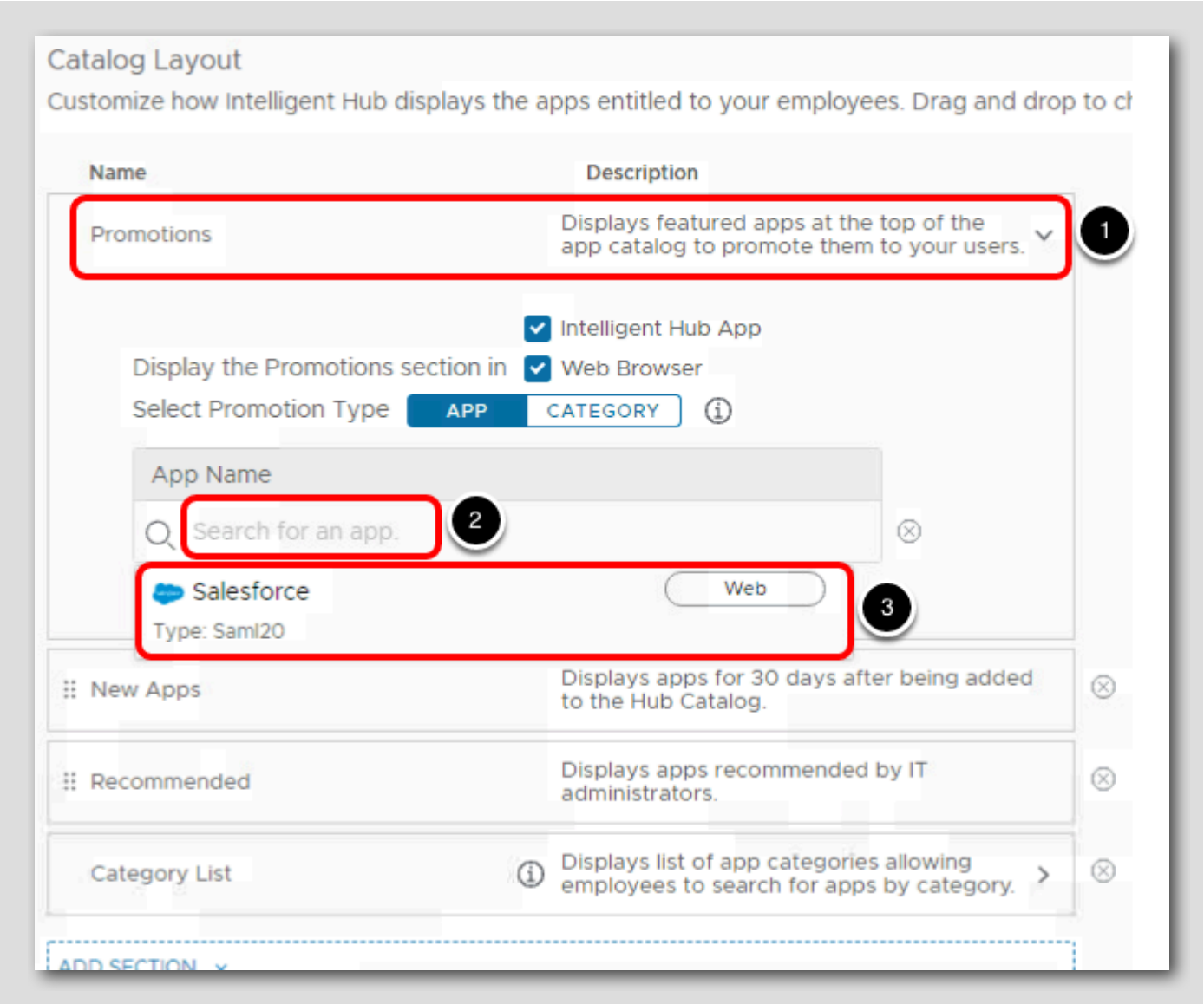


1. Click **ADD SECTION**
2. Click **Promotions**

The Sales Team app catalog will now show a Promotions section at the top, followed by New Apps, Recommended and Category List sections.

Customize the Promotion Section

[459]

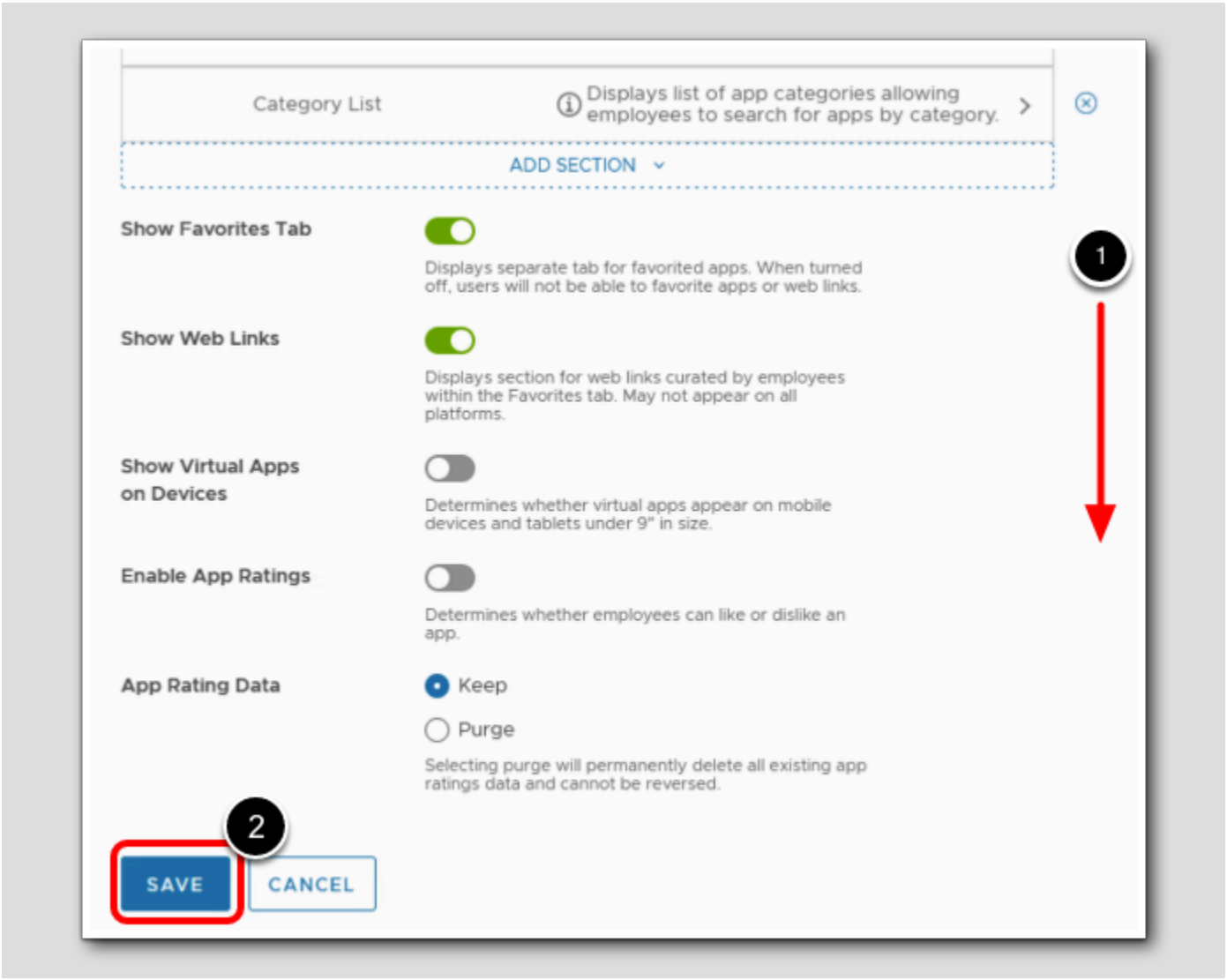


1. Click the **Promotions** section to expand it.
2. Click in the **App Name** search box. If you have multiple apps, you can type here to limit the shown results.
3. Select the **Salesforce** result from the list.

This will cause the Salesforce app to be promoted to your end users. Consider promoting important or heavily used apps you are encouraging your end users to utilize!

Save the Catalog Layout for the Sales Team

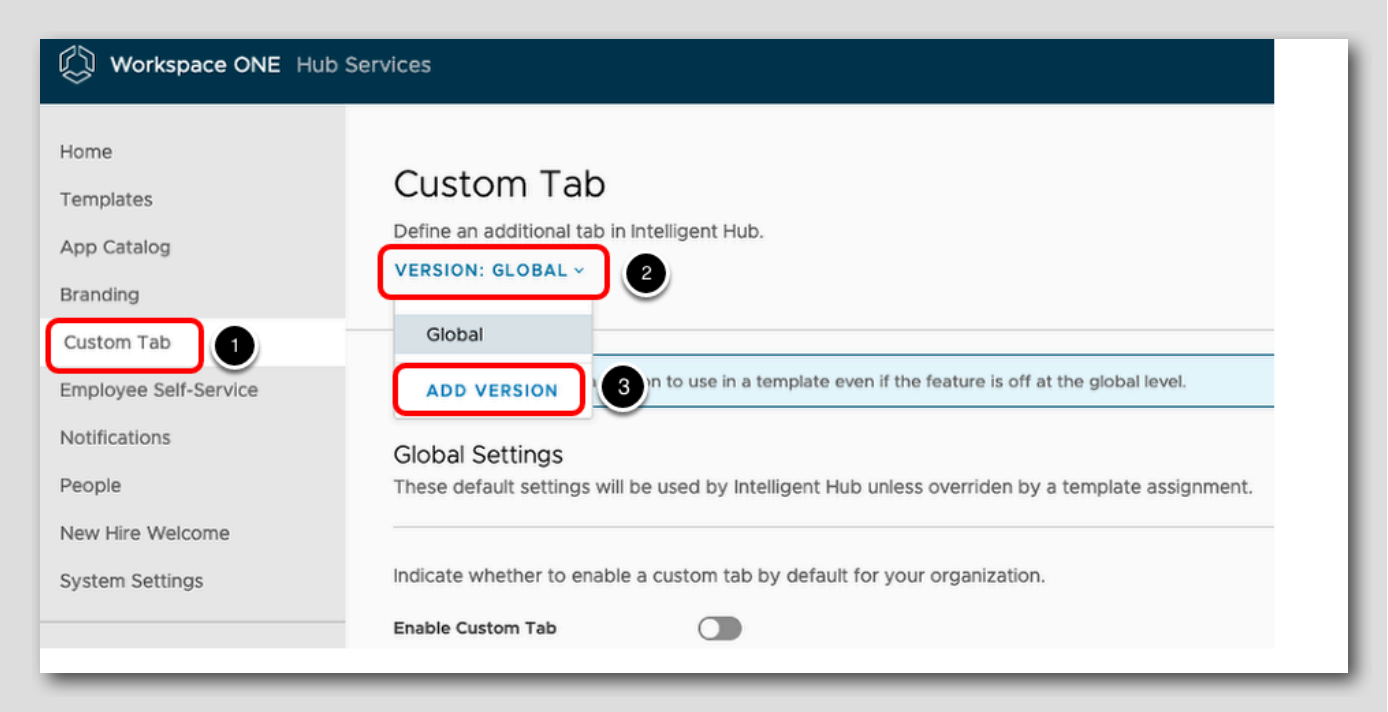
[460]



1. Scroll down past the Catalog Layout section to find the save button.
2. Click **SAVE**.

Configure the Custom Tab

[461]



The Custom Tab is a URL that directs users to your company intranet site or to another resource that you want to easily share with your users.

1. Select the **Custom Tab** menu item on the left.
2. Click the **VERSION: GLOBAL** dropdown.
3. Click **ADD VERSION**.

Custom Tab Settings

[462]

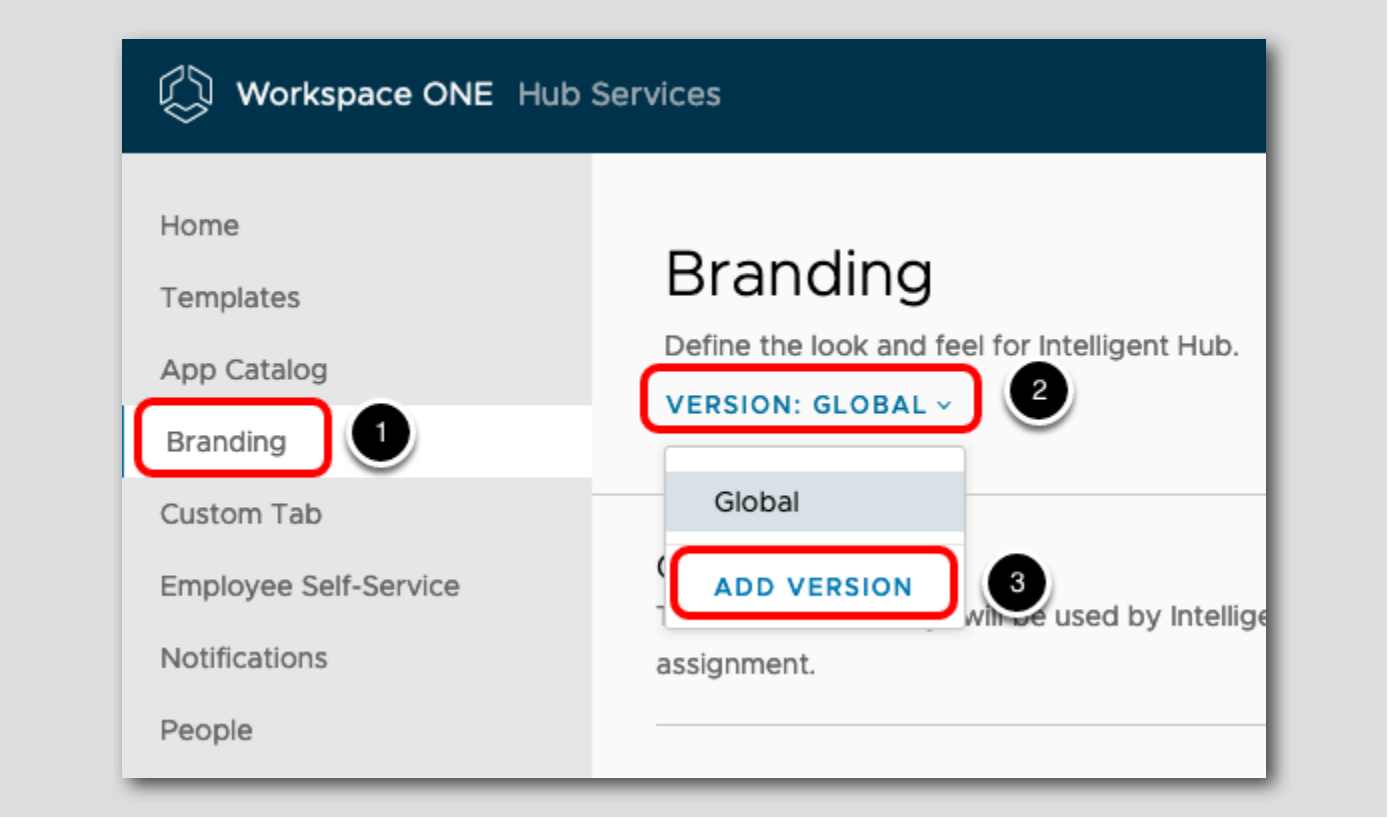
1. Enter the Version Name as **`Custom Tab for Sales Team`**
2. Enter the Description as **`Direct Sales Team to product resources`**
3. Turn the **Web toggle ON** so this Custom Tab will show in the browser version of the Intelligent Hub.
4. Enter the URL as **`https://www.vmware.com`**
5. Select **Last** for the **Position**.
6. Click **Save** (you may need to scroll down to see the Save button).

Configure Branding for Intelligent Hub [463]

By default, VMware branding is used within the Intelligent Hub. However, you can customize the logo, text color, and background color that appears in the Intelligent Hub app and browser views.

In this section, we will change the Company Logo and the Organization Name in the Branding Settings for the Intelligent Hub.

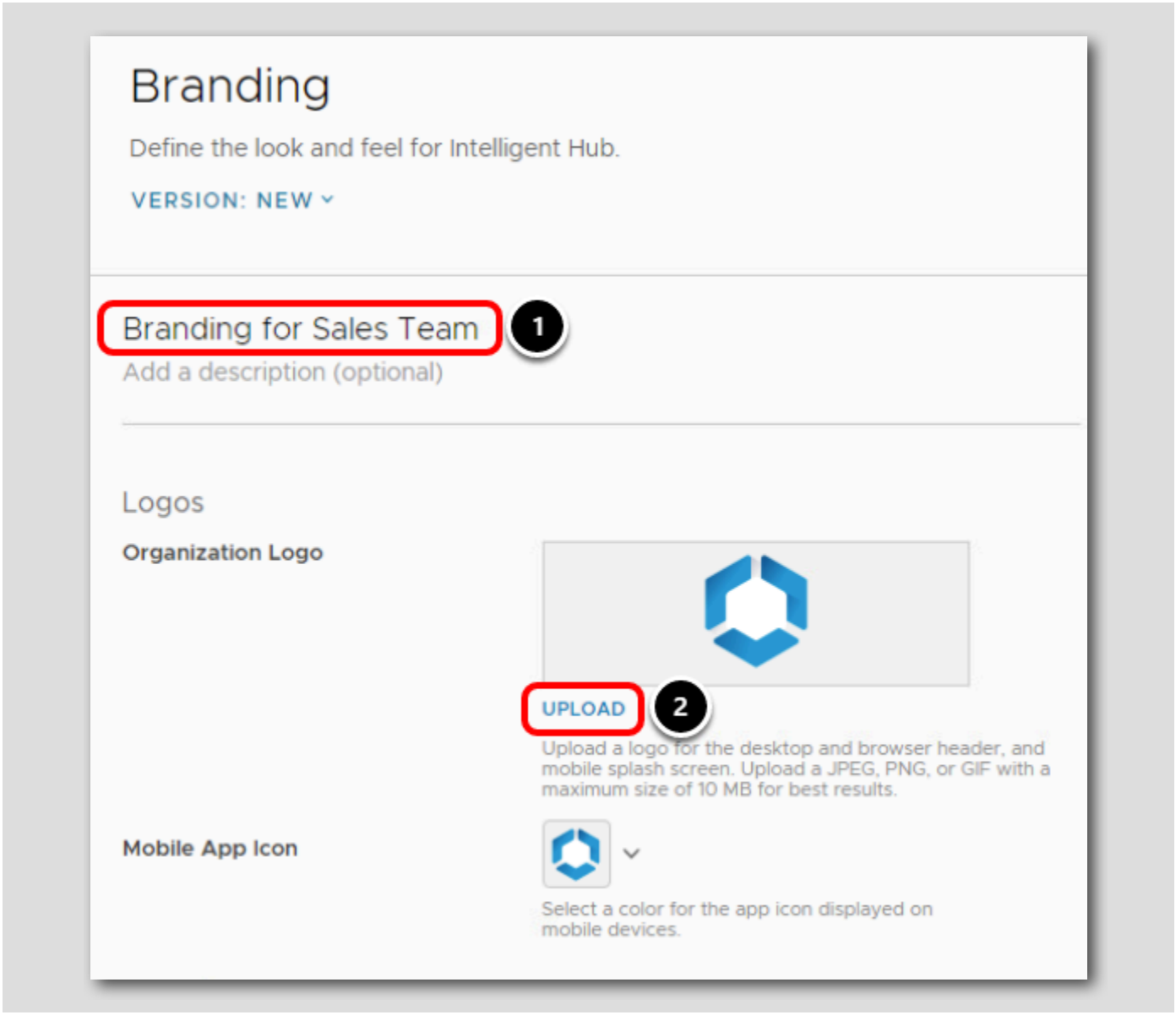
Add Branding Version [464]



1. Click on the **Branding** menu item on the left to customize branding for Intelligent Hub.
2. Click the **VERSION: GLOBAL** dropdown.
3. Click **ADD VERSION**.

Name Branding Version and Upload Logo

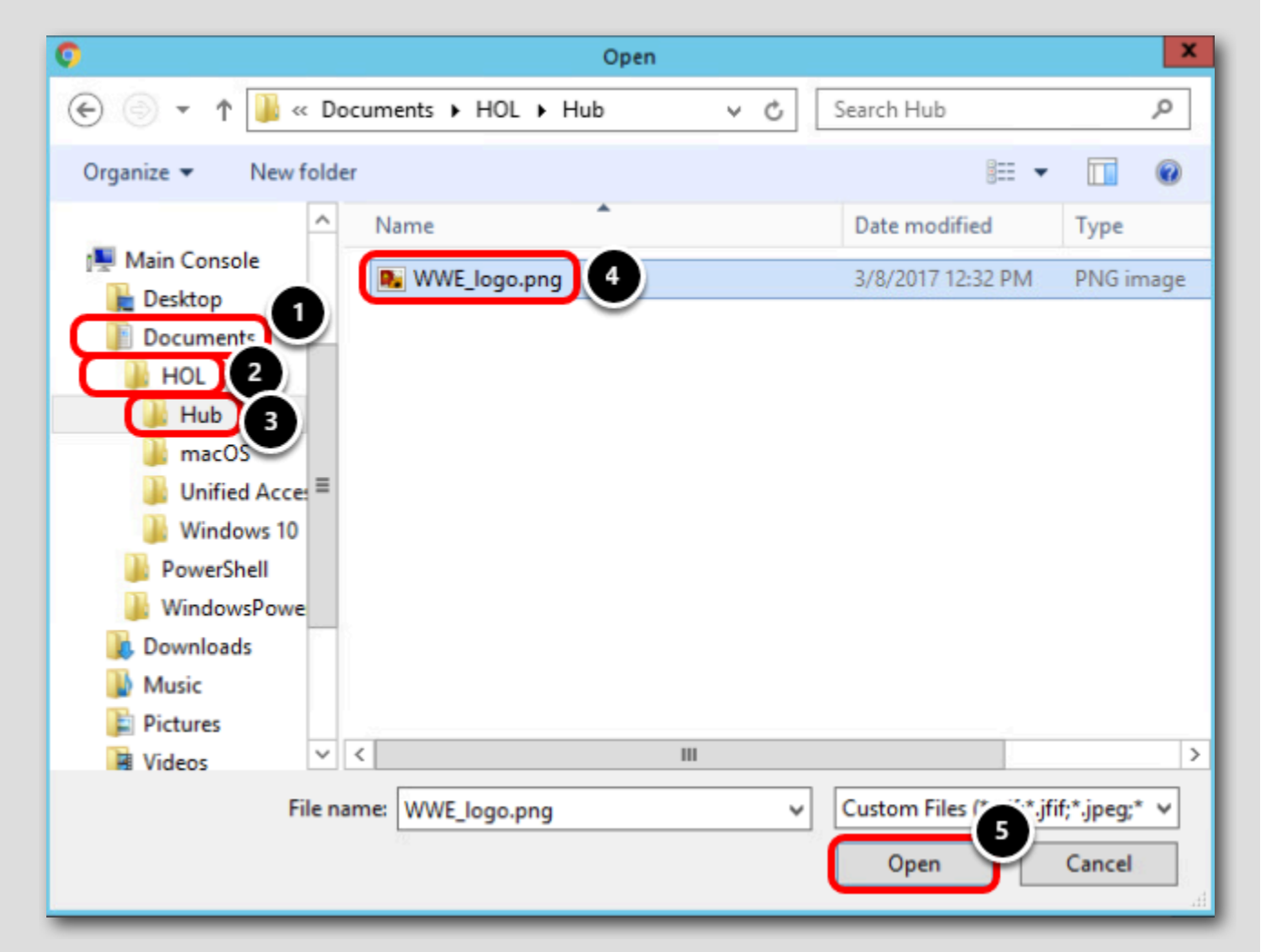
[465]



1. Name the version **`Branding for Sales Team`**.
2. Click the Organization Logo **UPLOAD** link.

Navigate to the Company Logo File

[466]

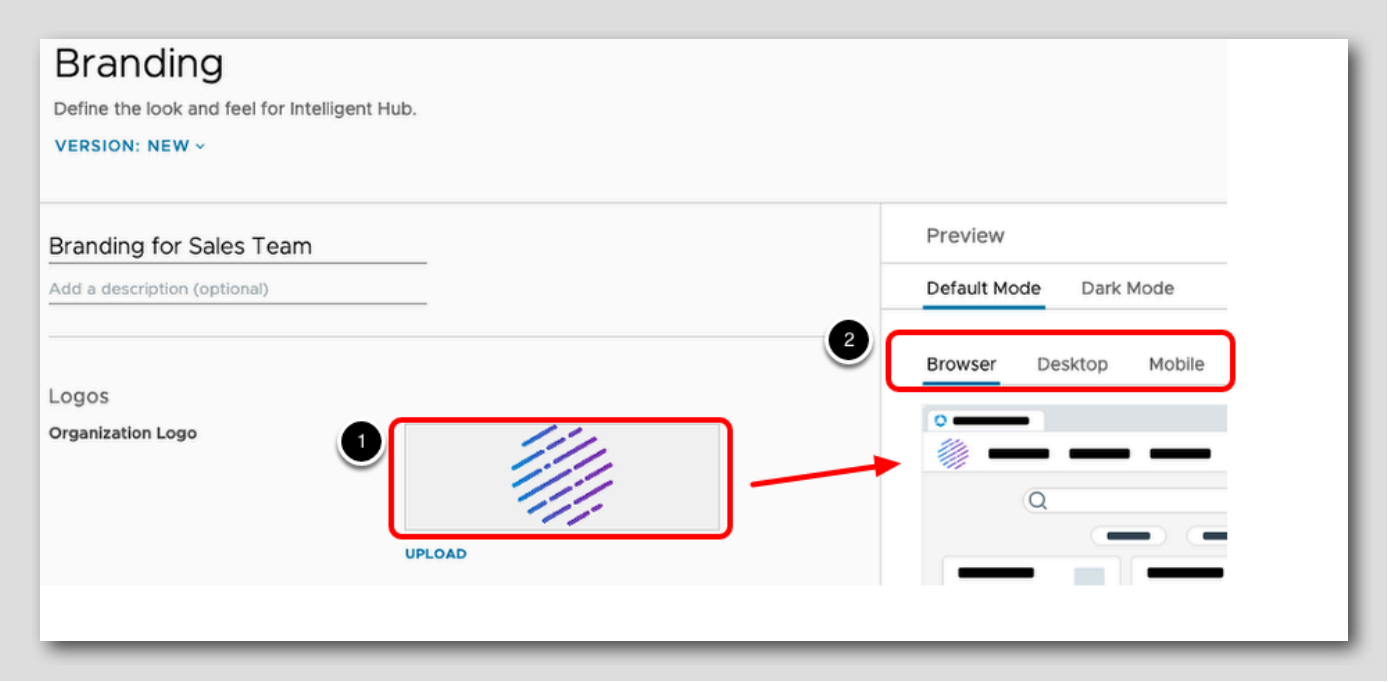


From the pop-up window,

1. Expand **Documents**
2. Expand **HOL**
3. Click on **Hub** folder
4. Select **WWE_logo.png**
5. Click **Open**

Preview the Branding Changes

[467]



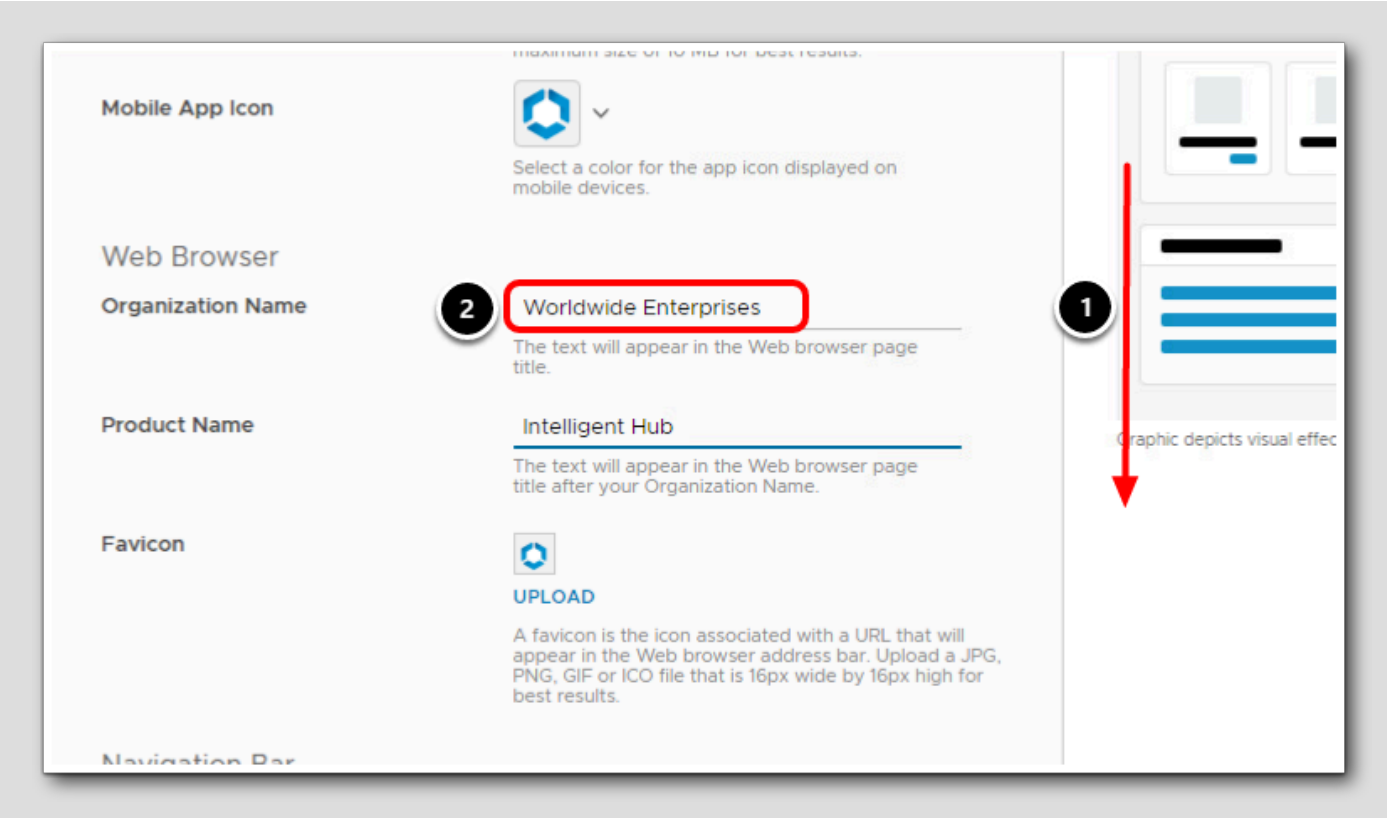
1. Notice that after you updated the Company Logo setting, your Preview pane updated to reflect what your users will see.
2. The Preview pane allows you to switch between Browser, Desktop, and Mobile views to see how your changes will be reflected on each platform.

Other settings on this page will be reflected here as well for a quick preview before you publish changes to your users.

Continue to the next step.

Change the Organization Name

[468]



1. Scroll down to the Web Browser section.
2. Change the Organization Name from VMware to **`Worldwide Enterprises`**.

Save the Branding Changes

[469]

1. Scroll to the bottom of the Branding section.
2. Click **SAVE** to save the branding configurations.

NOTE: There are other branding options such as background and icon color, but to limit the scope of the lab, we are going to only modify the organization name and company logo for demonstration purposes. Feel free to make additional configurations on your own if you wish to see them in action later.

Hub Services Notifications

[470]

The Intelligent Hub notifications framework is a robust, flexible cloud-hosted service designed to generate and serve actionable, real-time notifications to your employees. Users can receive notifications in their Hub portal in a browser and the Intelligent Hub app on their devices.

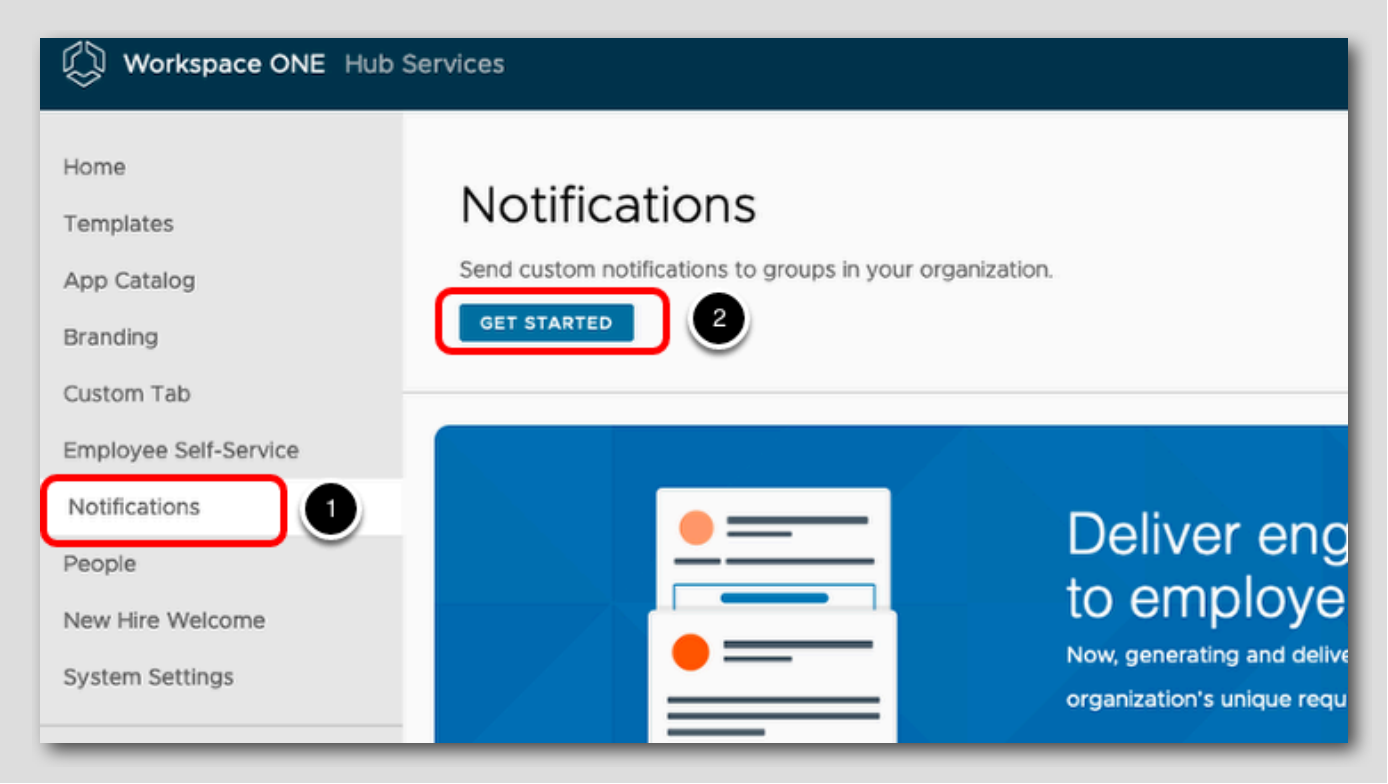
Let's take a look at the types of notifications available:

1. New Apps Available - A notification to announce that new applications are available in the catalog is automatically generated in Hub Services. Users can select new apps and save them to their device from the notification message.
2. Custom Notification - You can either use templates from the Notification wizard within the Hub Services admin console or use the Notification API to automate notifications. These notifications allow you to send reminders, critical information or call for action on user devices.
3. Notifications via Workspace ONE Experience Workflows - You can integrate 3rd-party business applications with Hub Services, such as approval notifications from Salesforce, Concur or Coupa, directly to the For You tab in Intelligent Hub.

In this section, we will create a Custom Notification using the wizard within the Hub Services admin console.

Get Started with Notifications

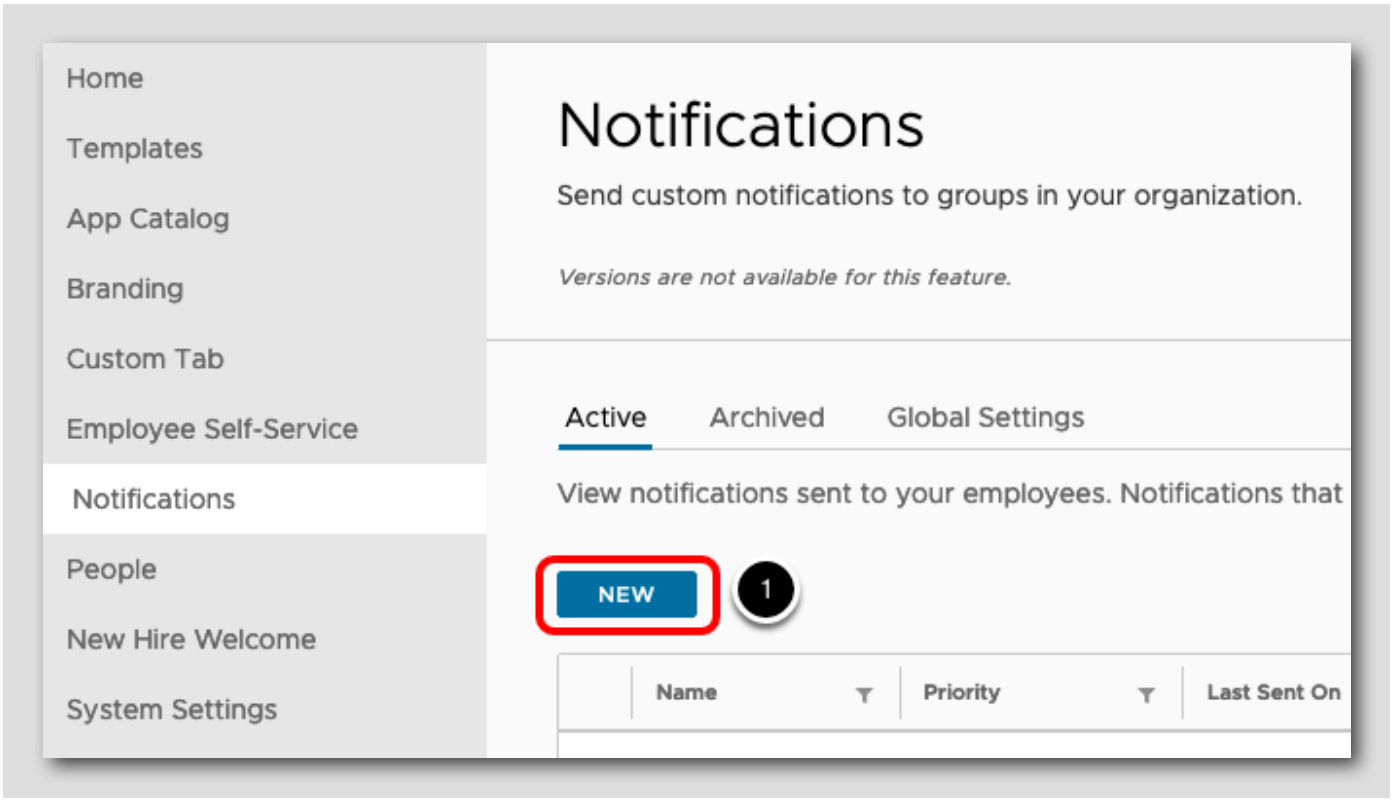
[471]



1. Click the **Notifications** menu item on the left.
2. Click **GET STARTED** to continue.

Notifications Tab in Hub Services

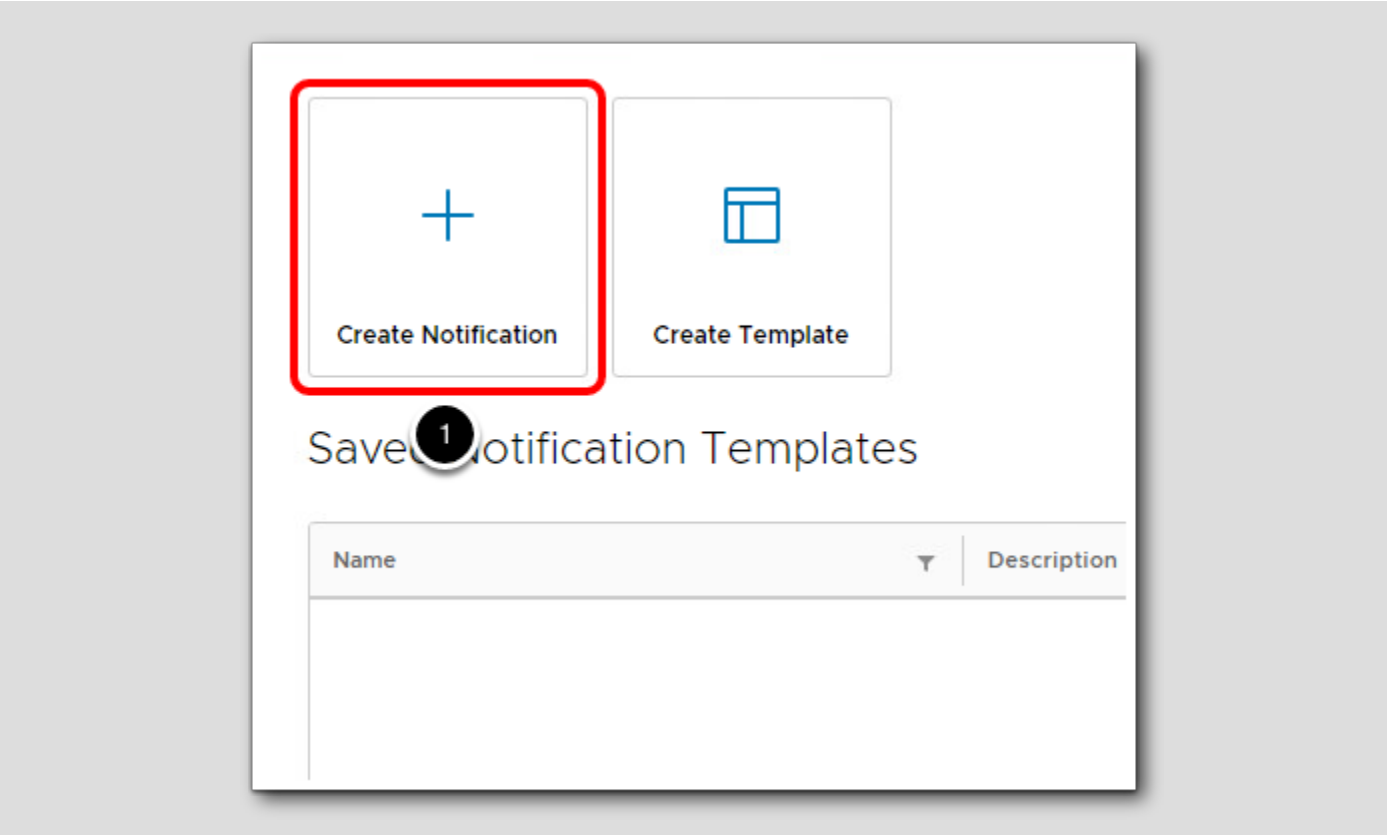
[472]



1. Click the **NEW button**.

Select Notification Action

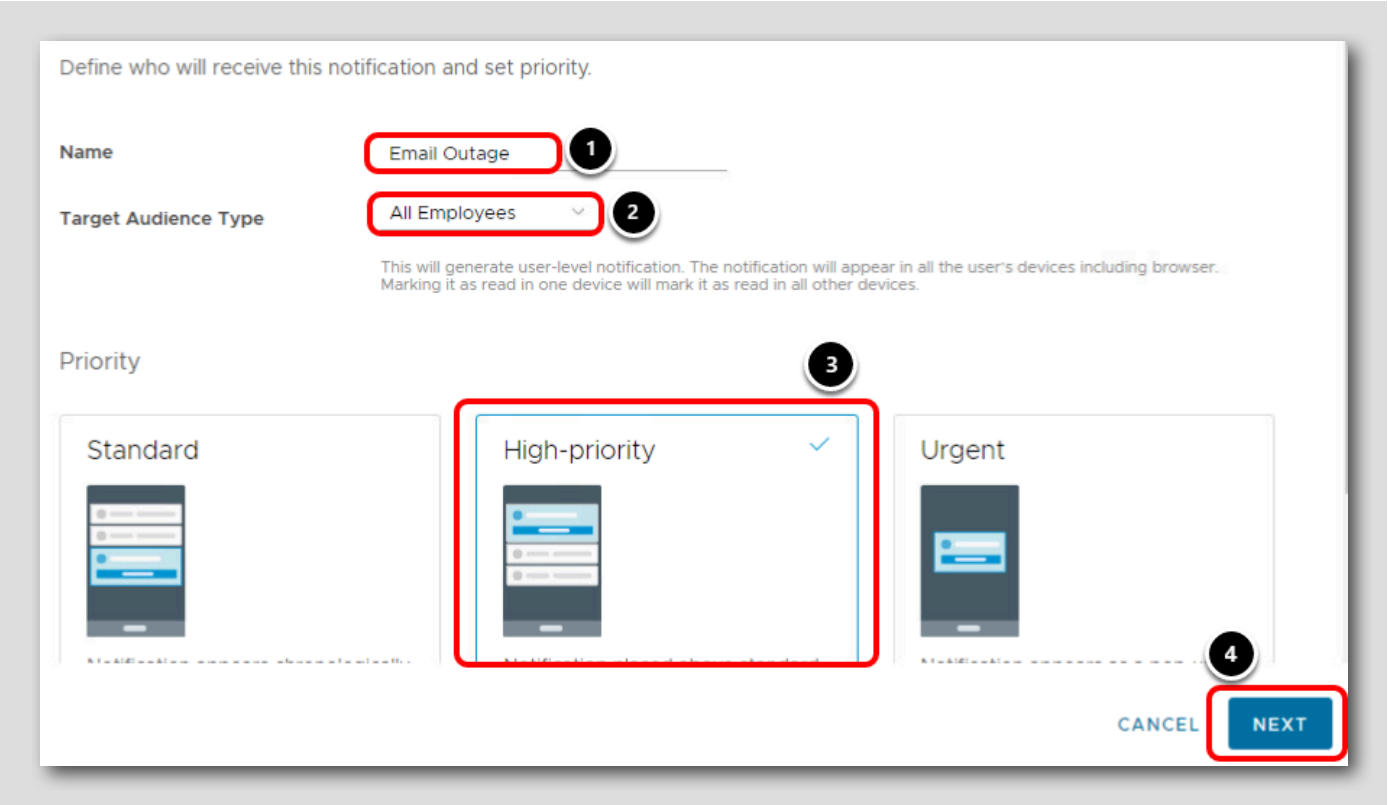
[473]



1. Select **Create Notification**.

Set Notification Definition

[474]

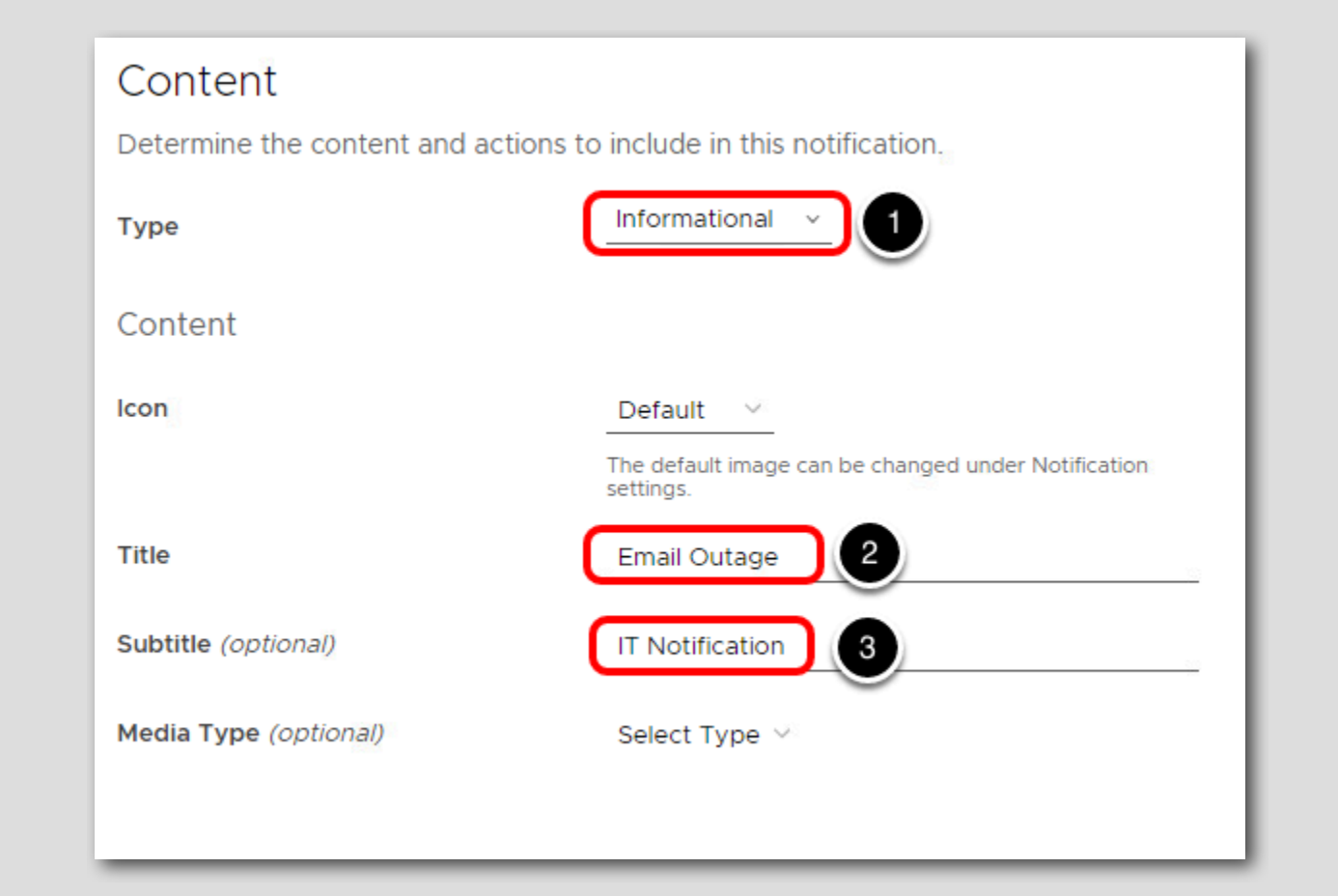


1. Enter **`Email Outage`** for the Name.
2. Select **All Employees** from the **Target Audience Type** dropdown.
3. Select **High-priority** Priority type.
4. Click **NEXT**.

Notifications can be set to Standard, High-priority or Urgent priority levels. High-priority notifications will display at the top of the For You tab within Intelligent Hub. Urgent notifications will display as a pop-up window within Intelligent Hub and must be dismissed by the user.

Set Notification Content

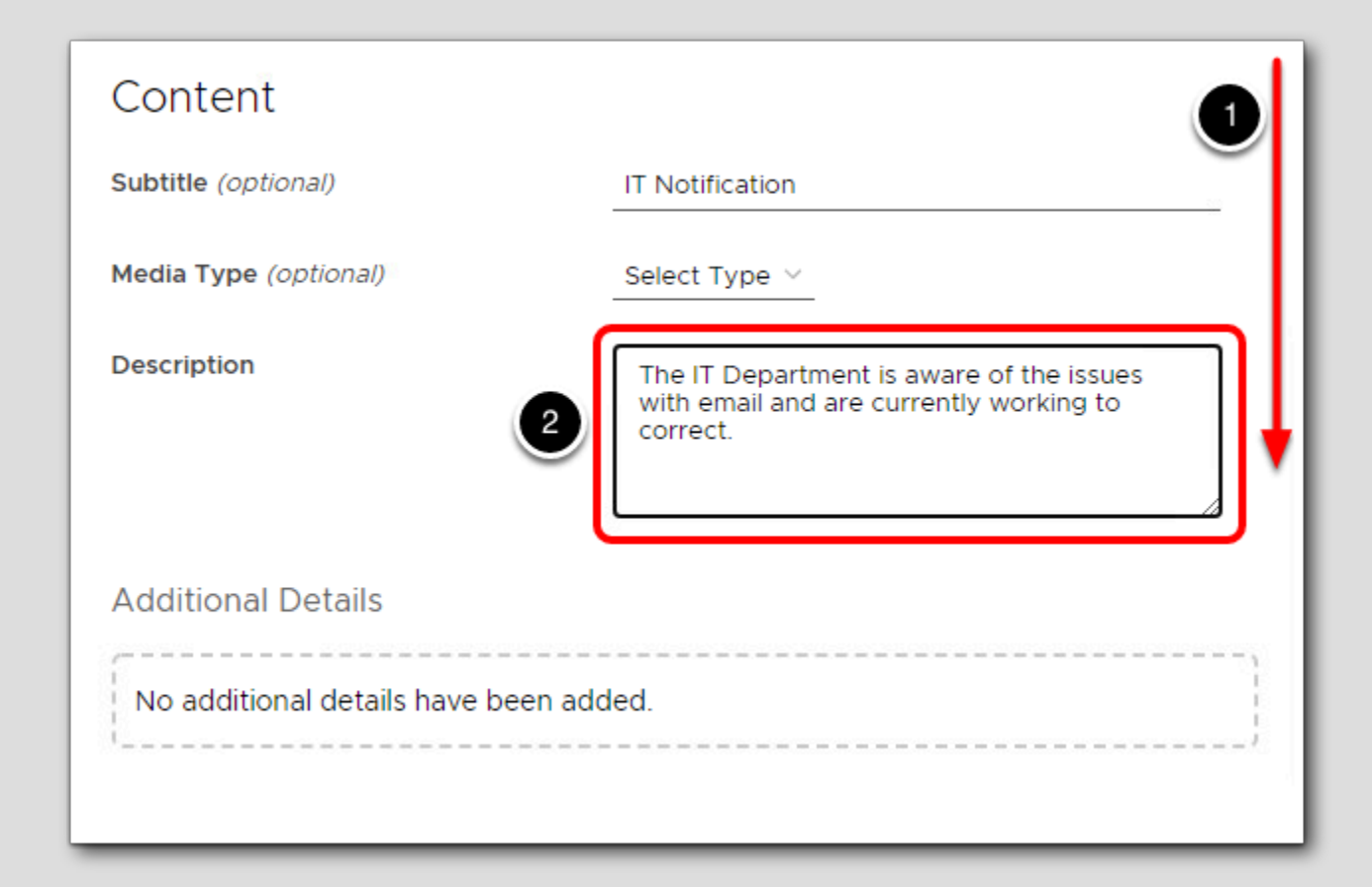
[475]



1. Notifications can either be Informational or Actionable. Actionable Notifications contain buttons the user must click to accept, reject, approve or otherwise acknowledge the notification or take action. Informational Notifications simply present some information for the user to read. Select **Informational** from the Template dropdown.
2. Enter **`Email Outage`** for **Title**.
3. Enter **`IT Notification`** for **Subtitle**.

Continue Notification Content

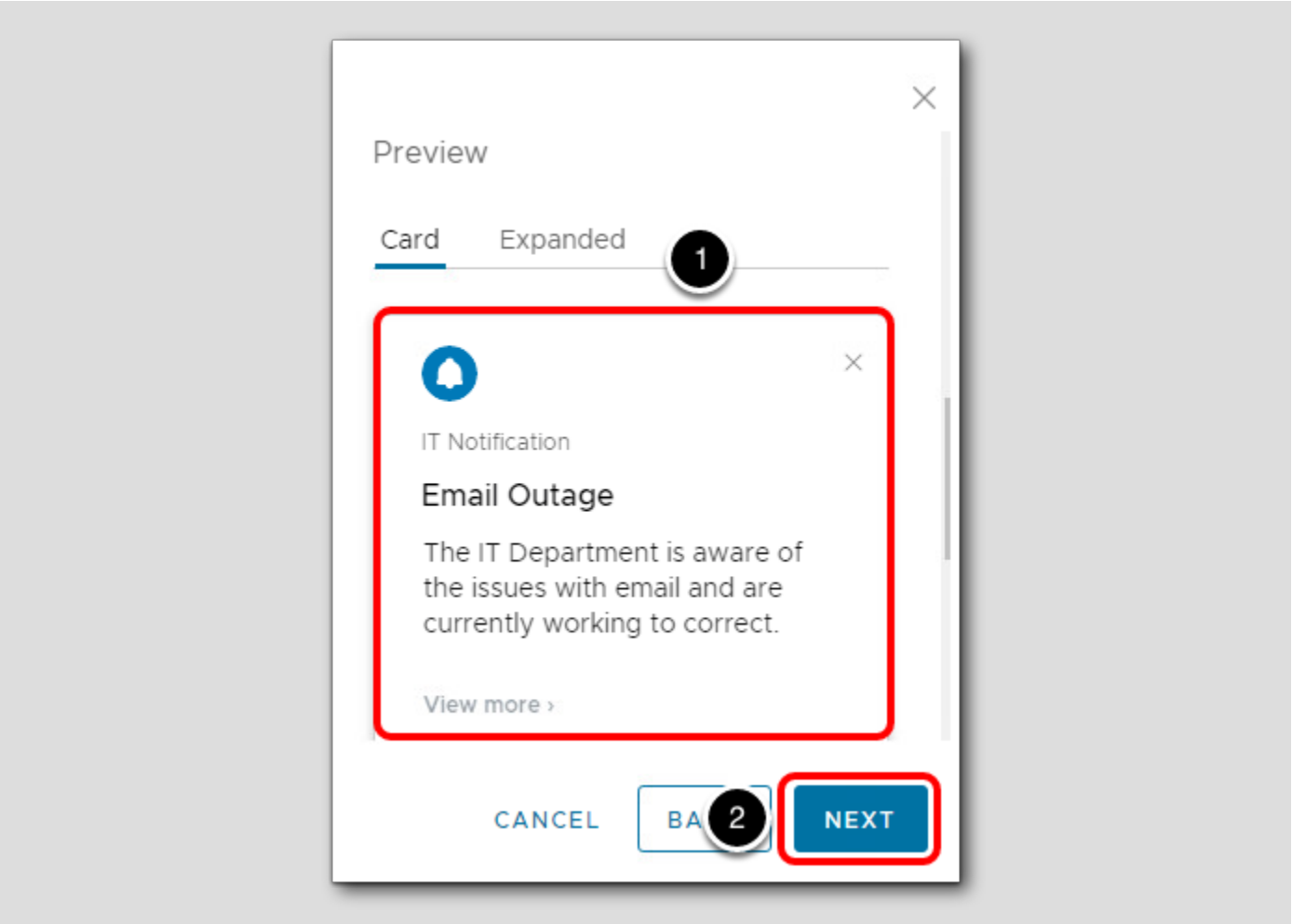
[476]



1. Scroll down to find the Description field.
2. Enter **`The IT Department is aware of the issues with email and are currently working to correct.`** for Description.

Preview Notification

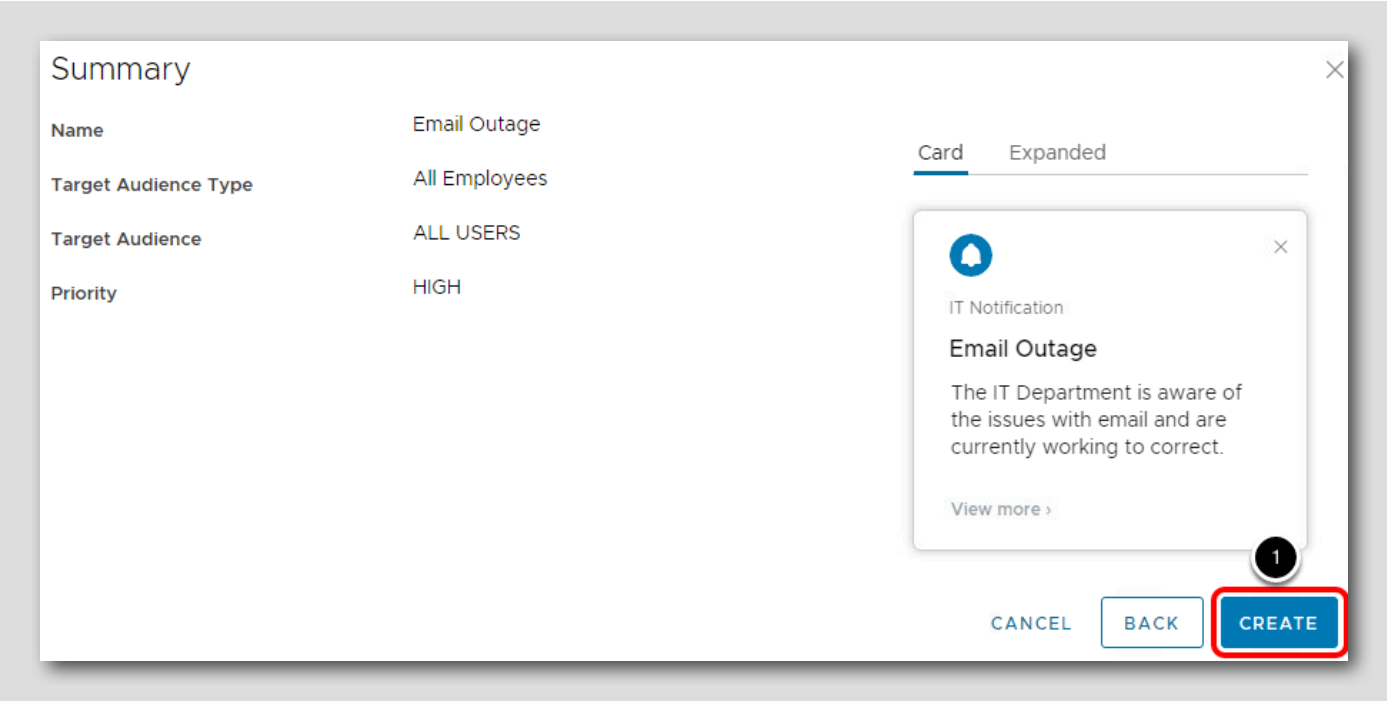
[477]



1. You are able to view a preview of the notification within the Hub Services console on the right side of the screen as you are changing the content.
2. Click **NEXT**.

Review Summary of Notification

[478]

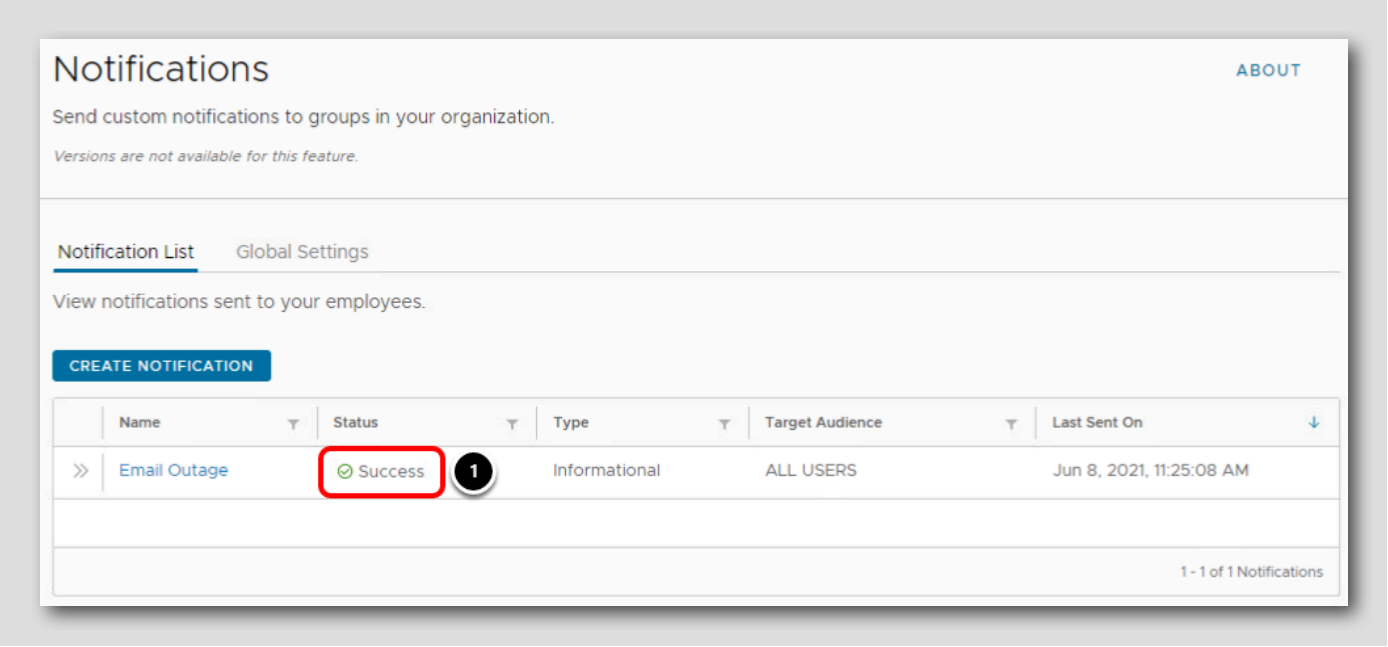


1. Review the notification settings and click **CREATE**.

Although this is just an example scenario for the purposes of this lab, the Hub Services Notification framework is particularly useful when email and other communication mediums are unavailable.

Validate the Notification Status

[479]

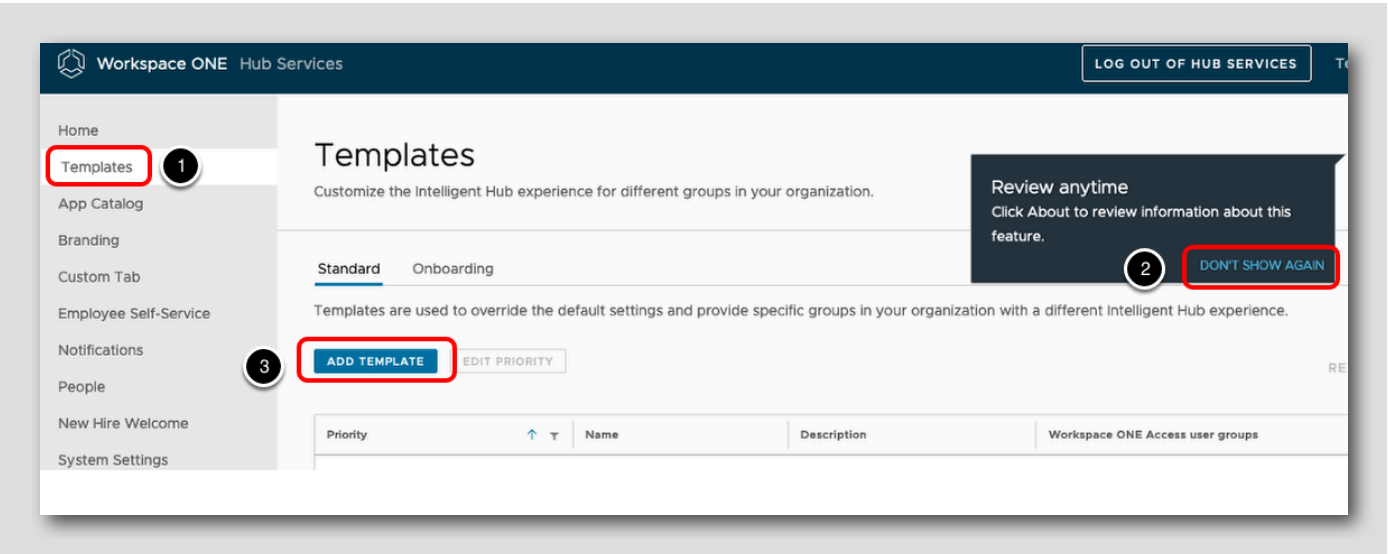


It will take about 10 - 15 seconds to send the notification.

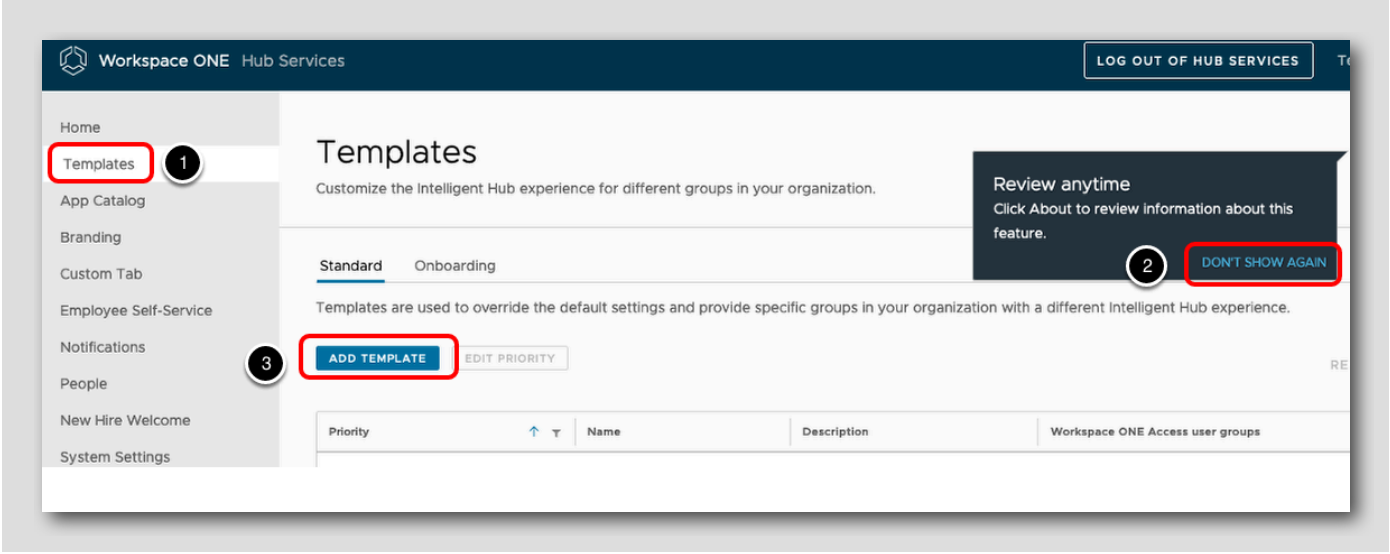
1. Confirm that you see the status as **Success** for the Email Outage Notification you created in this section.

Assign Hub Settings to a New Template

[480]

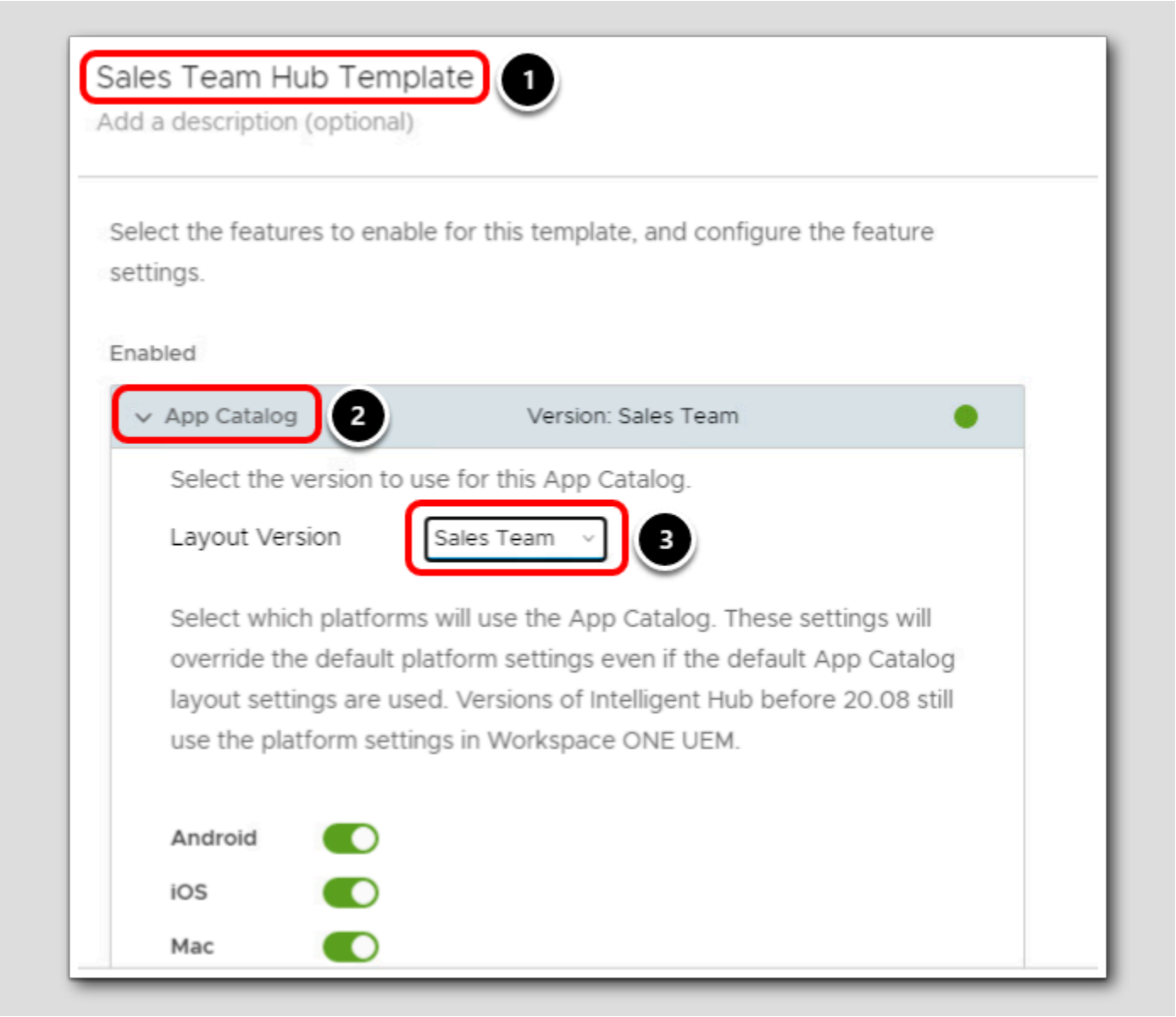


1. Click the **Templates** menu item on the left.
2. If you see the Review anytime popup, click **DON'T SHOW AGAIN** to dismiss.
3. Click **ADD TEMPLATE** to create a new Intelligent Hub template for the Sales Team.



Modify New Hub Template for Sales Team

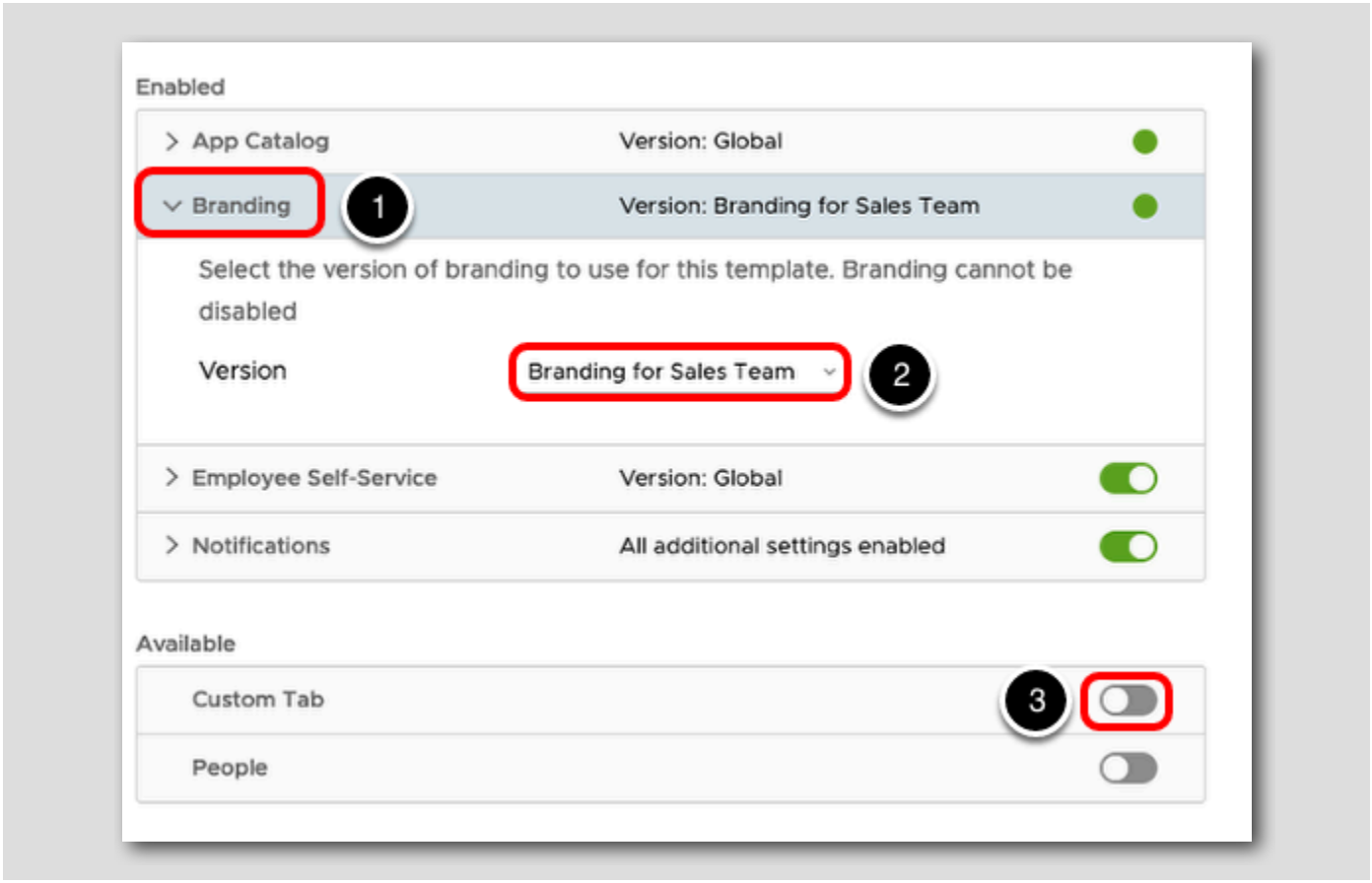
[481]



1. Enter **`Sales Team Hub Templete`** to name the new template.
2. Click **App Catalog** to expand that section.
3. Select **Sales Team** from the **Layout Version** dropdown. This is the catalog layout version we created earlier in this module.

Modifying Branding for Sales Team Hub Template

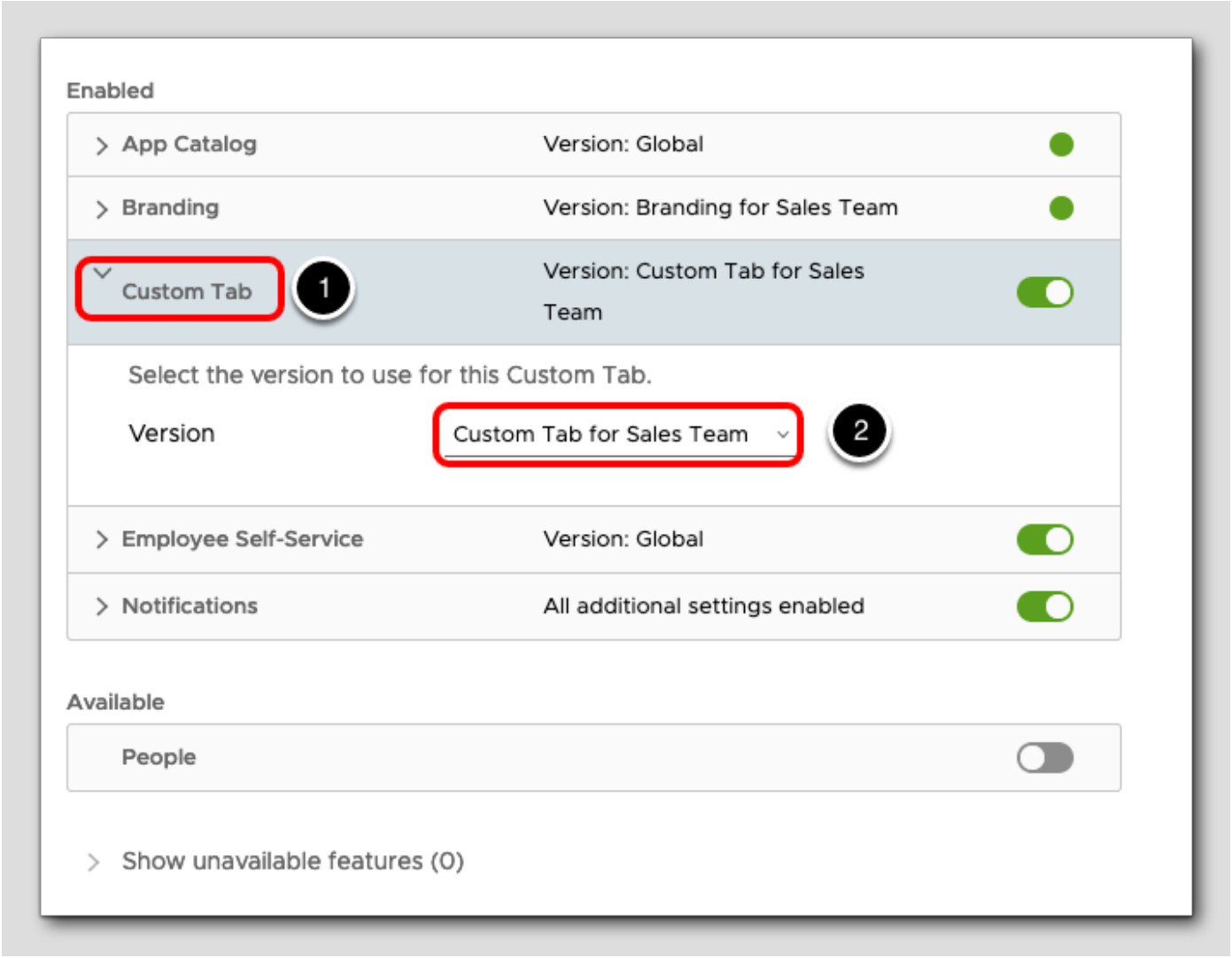
[482]



1. **Scroll down** to find the Branding Settings.
2. **Expand** the Branding section.
3. Select the **Branding for Sales Team** version in the dropdown.
4. **Toggle** the **Custom Tab ON** so that it turns green. When turned on, Custom Tab will move to the list of Enabled services and will be removed from the Available services section.

Modifying Custom Tab for Sales Team Hub Template

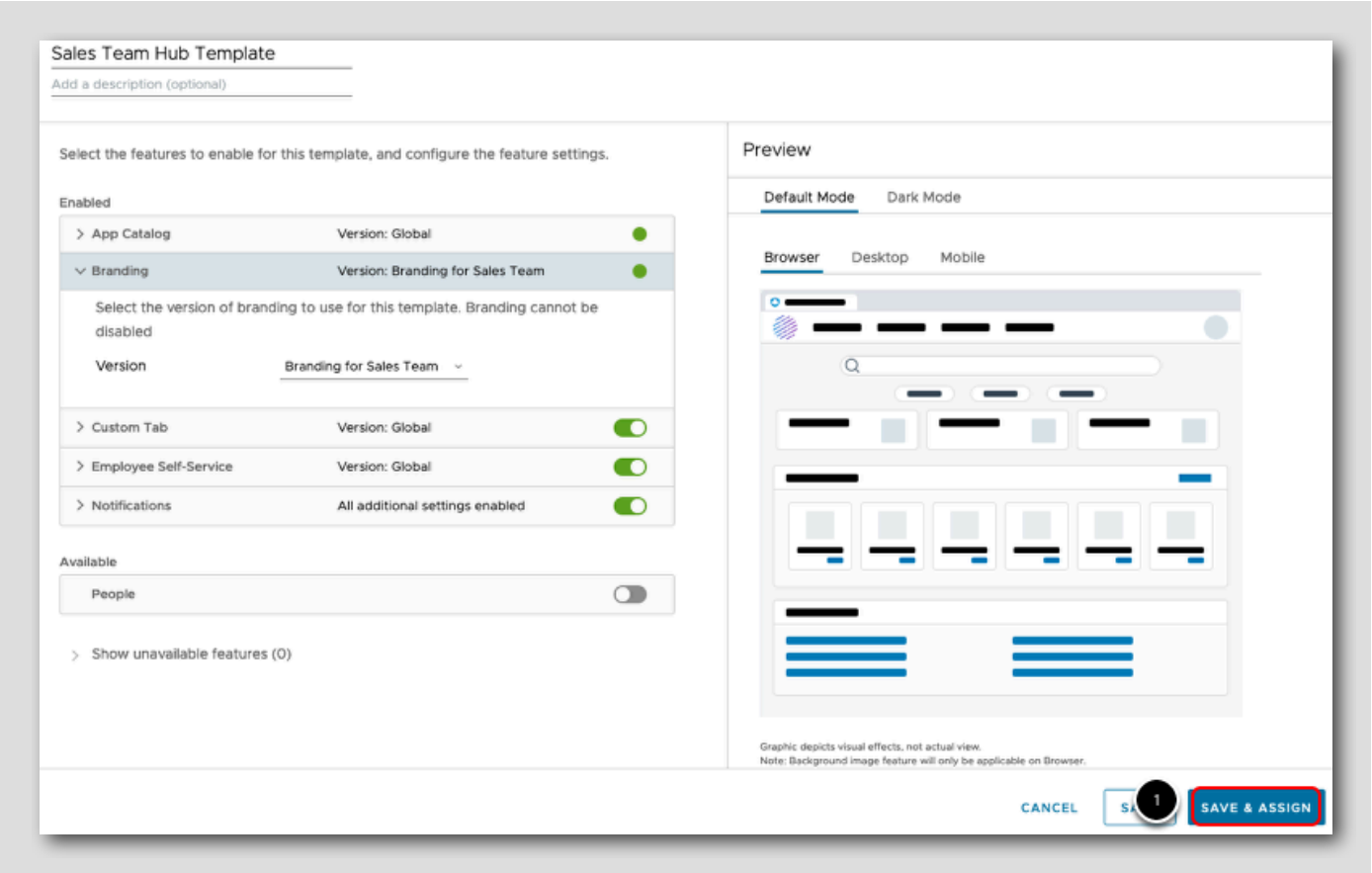
[483]



1. **Expand** the Custom Tab section.
2. Select the **Custom Tab for Sales Team** version in the dropdown.

Save the New Hub Template

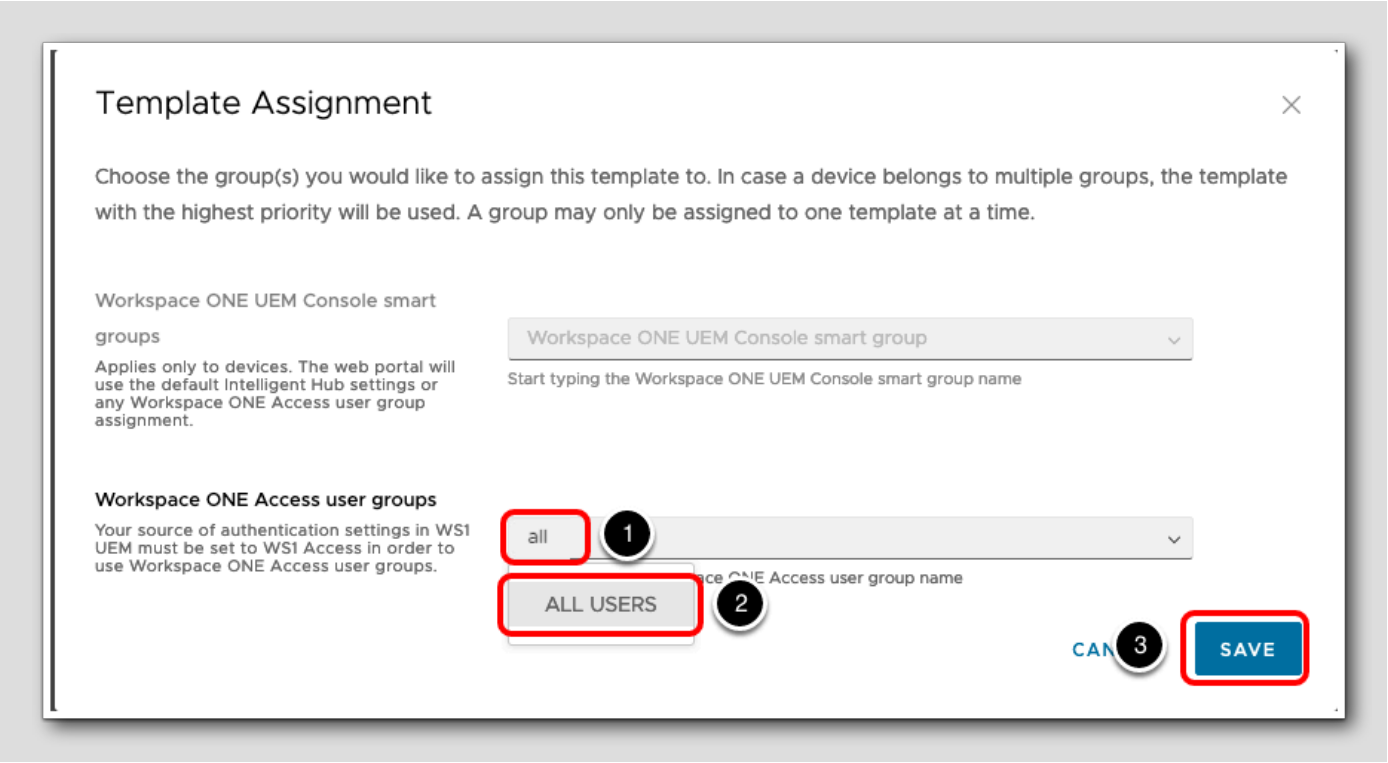
[484]



1. Click **SAVE & ASSIGN**.

Assign Hub Template to User Group

[485]

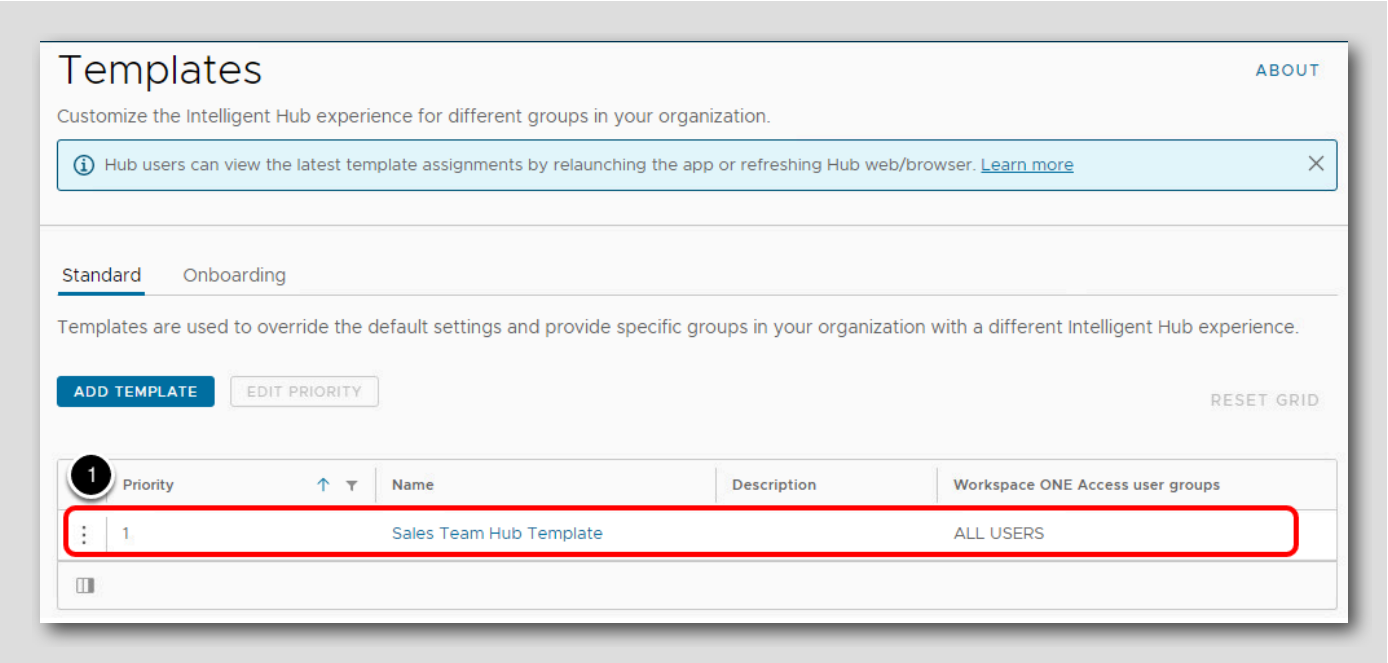


In the Template Assignment dialog box that pops up:

1. Type **all** into the Access User Groups search bar.
2. Click **ALL USERS** search result.
3. Click the **SAVE** button.

Confirm Hub Template Assignment

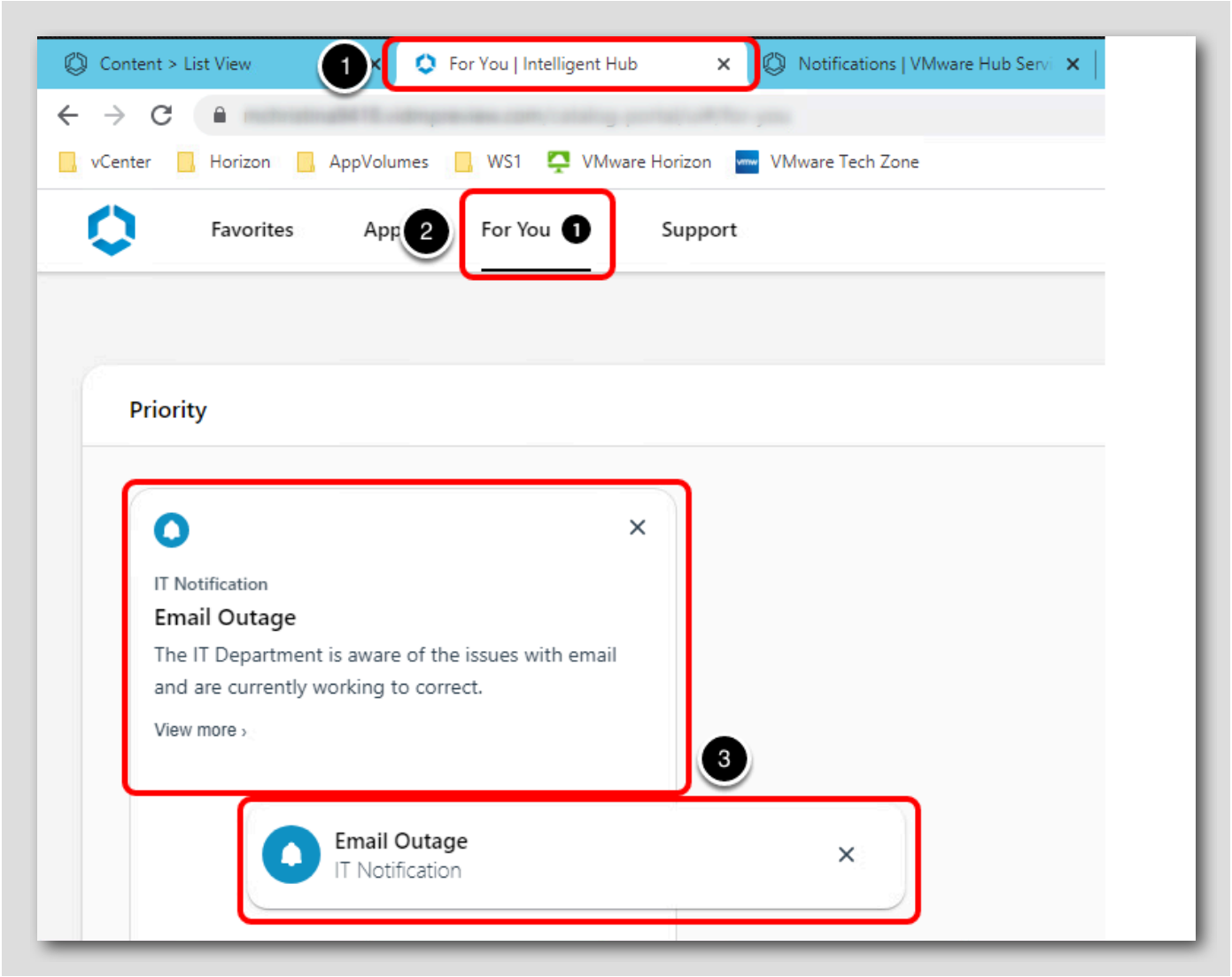
[486]



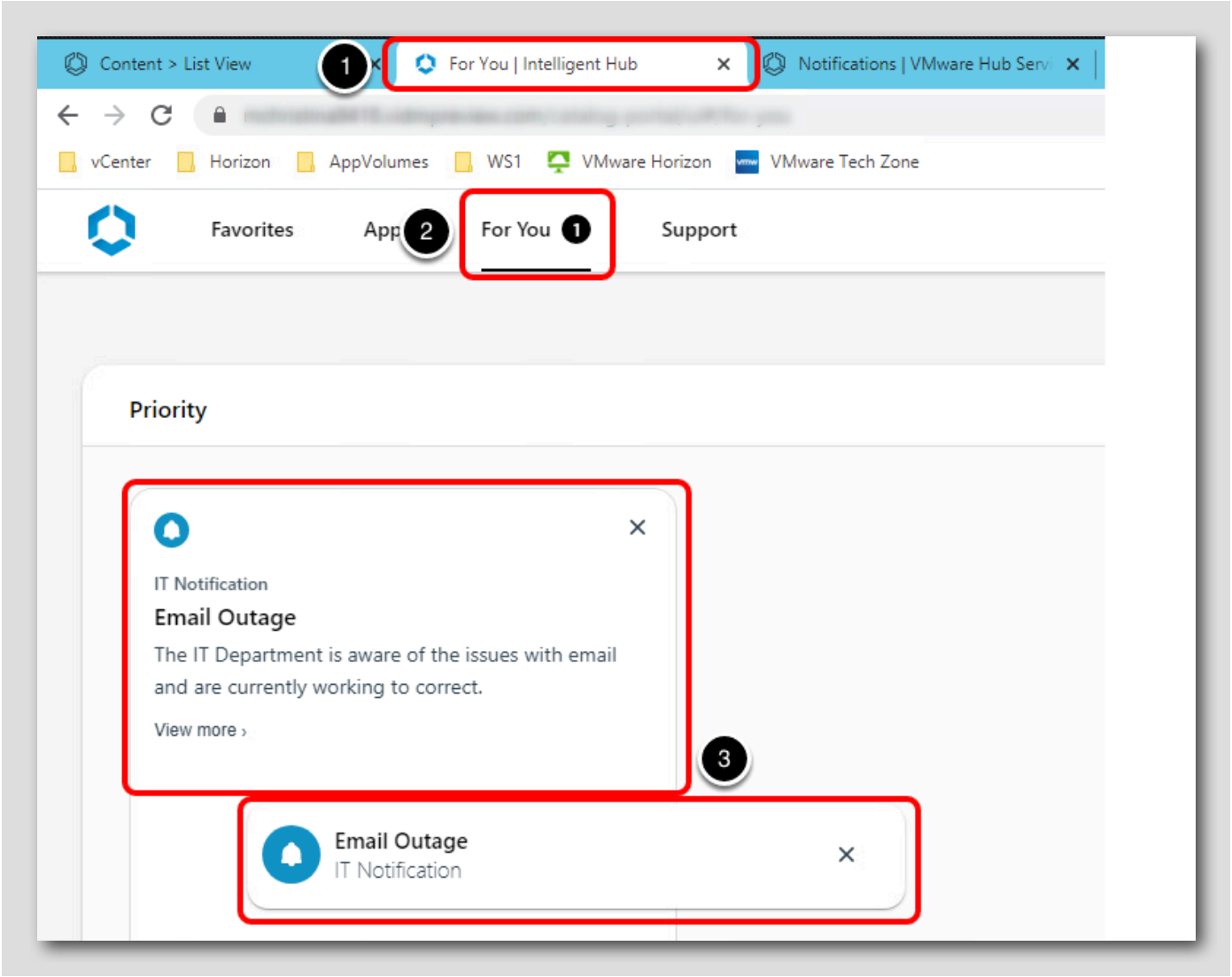
1. We can see the Hub Template for the Sales Team is assigned to ALL USERS. Priority can be utilized to manage any conflicts for users that exist in more than one user group.

Review Customizations in Intelligent Hub

[487]

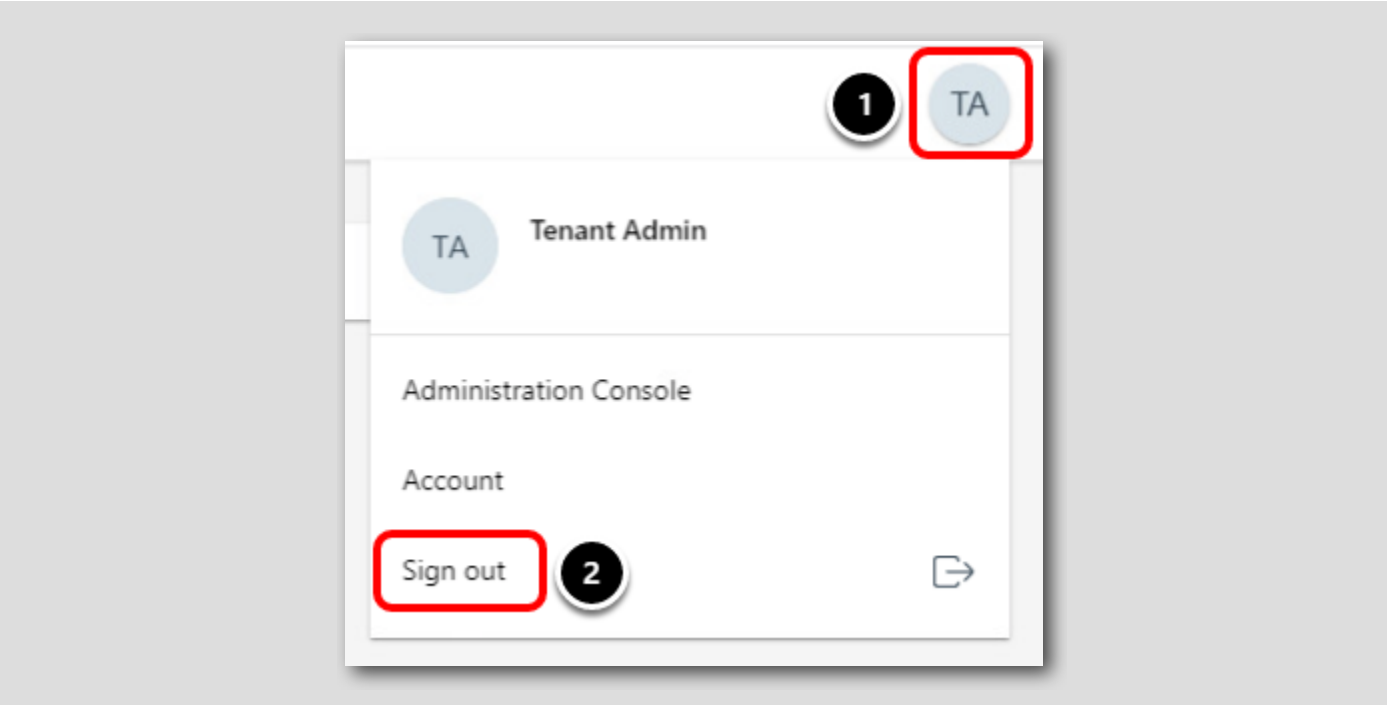


1. Click the **second tab** in the browser, which is the Intelligent Hub User Portal.
2. Click the **For You tab** in Intelligent Hub. Notice the Notification count as 1 on the tab to indicate there is one new notification.
3. Notice the IT Notification we created immediately shows in the Priority section of the For You tab - no browser refresh required. **Click** the **X** in the top right of each notification to dismiss and move the notification to the history.


Content > List View
1
For You | Intelligent Hub
Notifications | VMware Hub Serv
vCenter
Horizon
AppVolumes
WS1
VMware Horizon
VMware Tech Zone
Favorites
App
2
For You
1
Support
Priority
IT Notification
Email Outage
The IT Department is aware of the issues with email and are currently working to correct.
View more ›
3
Email Outage
IT Notification

Log Out of Intelligent Hub

[488]

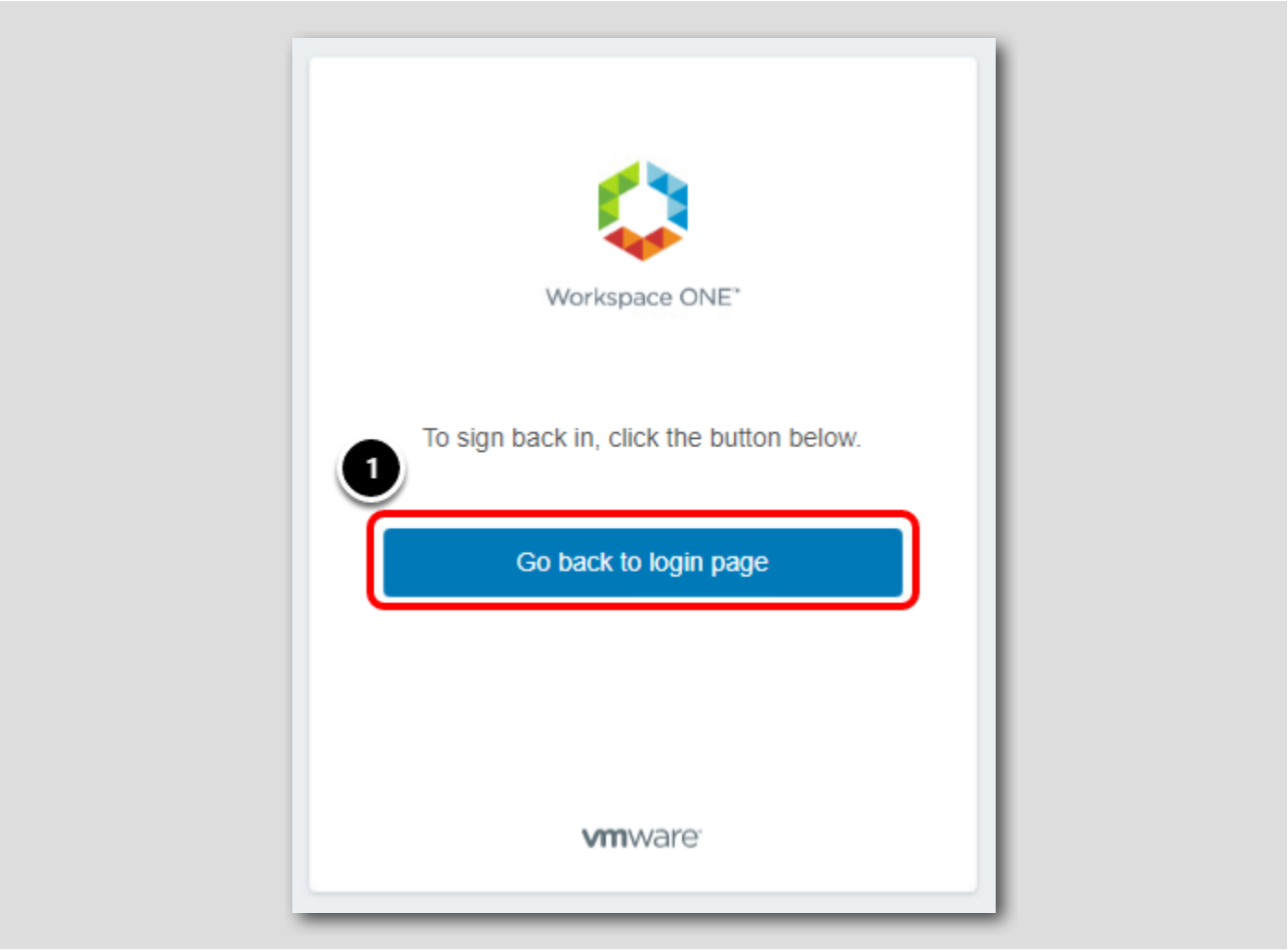


To view the App Catalog, Branding and Custom Tab changes we made earlier, we need to log out of Intelligent Hub and log back in.

1. Click the User dropdown circle at the top right of the Intelligent Hub.
2. Click Sign out to log out of Intelligent Hub.

Go Back to Intelligent Hub Login Page

[489]



1. Click the Go back to login page button.

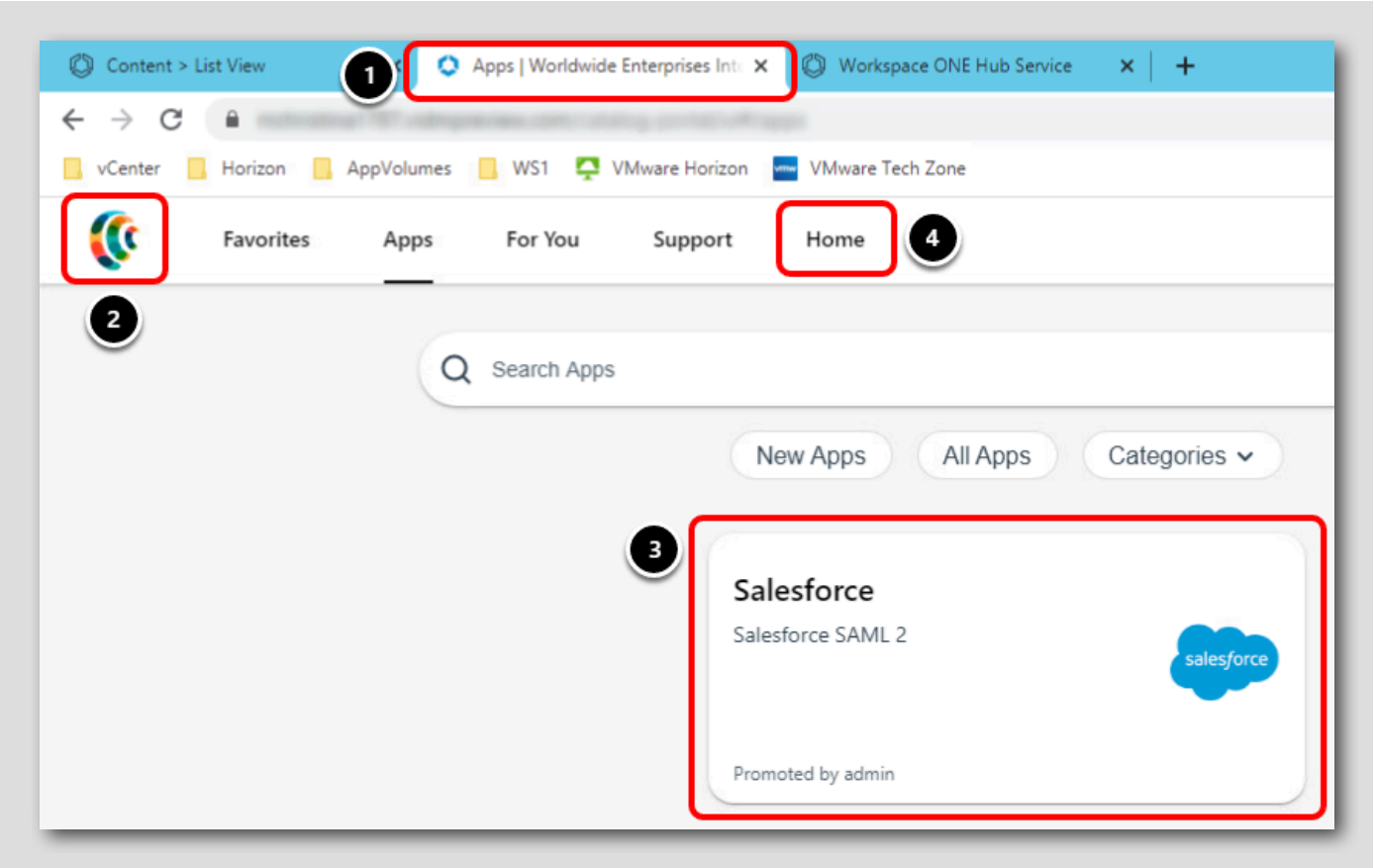
Log Back Into Intelligent Hub

[490]

1. Enter **administrator** for Username.
2. Enter **VMware1!** for Password.
3. Click the **Sign in** button.

Confirm Branding, App Catalog and Custom Tab Changes

[491]



1. Notice the Company Name in the browser tab has changed to Worldwide Enterprises.
2. Notice the company logo has changed to the logo we uploaded.
3. Notice the Salesforce app is now promoted at the top of the App Catalog.
4. **Click** the **Home tab** and notice a new browser tab opens to the URL we entered earlier.

Summary

[492]

Congratulations! You have completed the Workspace ONE Intelligent Hub and Hub Services module! In this module, you learned how to:

- Configure Workspace ONE Hub Services and view customizations within Intelligent Hub
- Add a SaaS app to the Intelligent Hub catalog
- Create different versions of Intelligent Hub settings and assign to a Hub Template
- Customize the Intelligent Hub app catalog layout

- Customize branding for the Workspace ONE Intelligent Hub app
- Create a Custom Tab for Intelligent Hub
- Create and send Custom Notifications to the Intelligent Hub app

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

[493]

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*!


Your Personal journey from zero to IT Superhero
How the products work – beginner to expert
Quick start for your first proof of concept
TECH ZONE
Hands on Labs, Tools and Best Practices
Guide to production deployments & operations
Latest product information

Module 6- Workspace ONE Intelligence - Introduction to Dashboards, Automation, and Reports (45 minutes) Beginner

Introduction

[495]

With so much data available to IT admins managing modern, mobile work styles and no single tool to make sense of it, IT is faced with a huge challenge to manage the digital workspace. The lack of unified visibility across devices, applications and users makes it particularly hard to make data-driven decisions. As a result, manual processes become the norm, and IT is cornered into being reactive to employee demands and external events instead of being proactive.

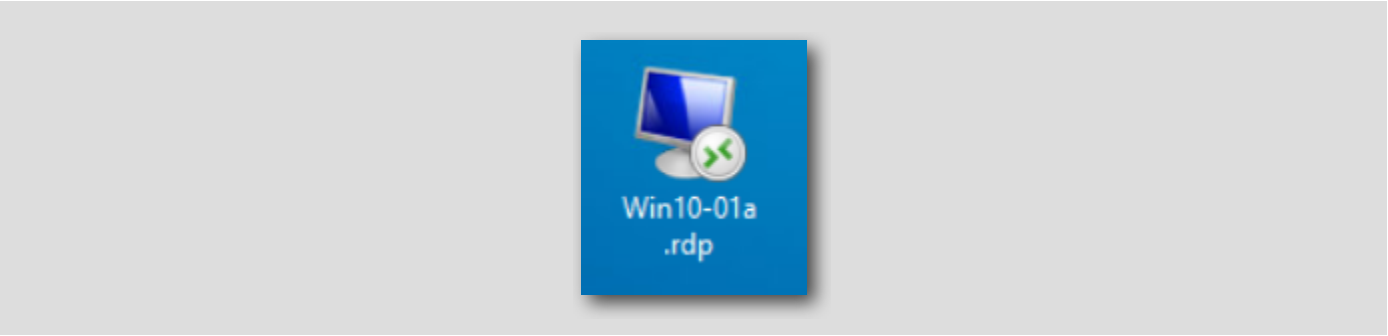
Deep insights empower IT admins to better plan and optimize their app and policy deployments based on network performance, resource entitlement and deployment risk. And with the ability to automate processes, IT admins can proactively increase their level of security hygiene and meet compliance requirements, while improving user experiences.

With the *automation engine* at the heart of Workspace ONE Intelligence, IT admins can automate workflows across their environments by defining rules that take actions based on a rich set of parameters. This allows IT to create *contextual workflows* that take automated remediation actions based on security threats, and meet compliance requirements through automated access control. In addition, the Experience Management solution within Intelligence monitors digital employee experience and automated actions can be triggered when a poor experience is detected. And because Workspace ONE Intelligence provides *extensibility* with an API layer for third parties, IT admins can build workflows that leverage their unique environment to meet their needs.

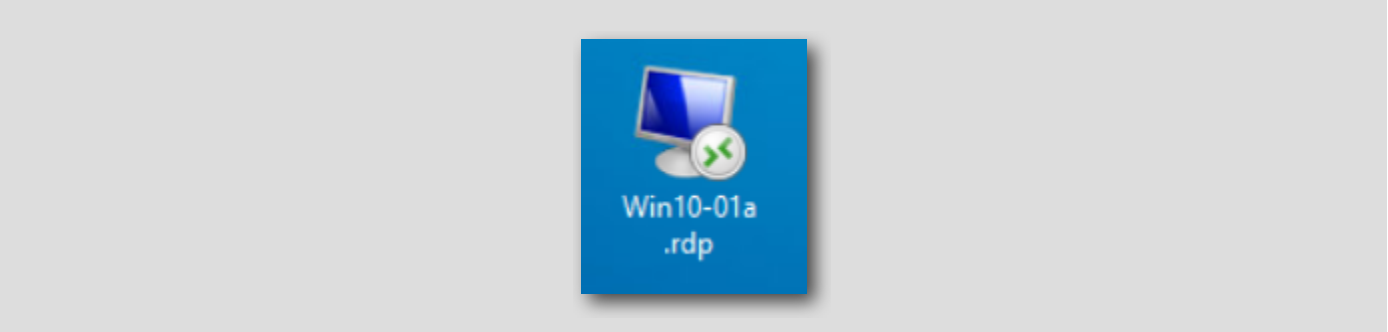
With automation, Workspace ONE Intelligence helps IT meet employee experience targets and increase security through automated remediation.

Connect to the Windows 10 Virtual Machine

[496]



Double-click the **Win10-01a.rdp** shortcut located on the Main Console Desktop to connect to the Windows 10 virtual machine.



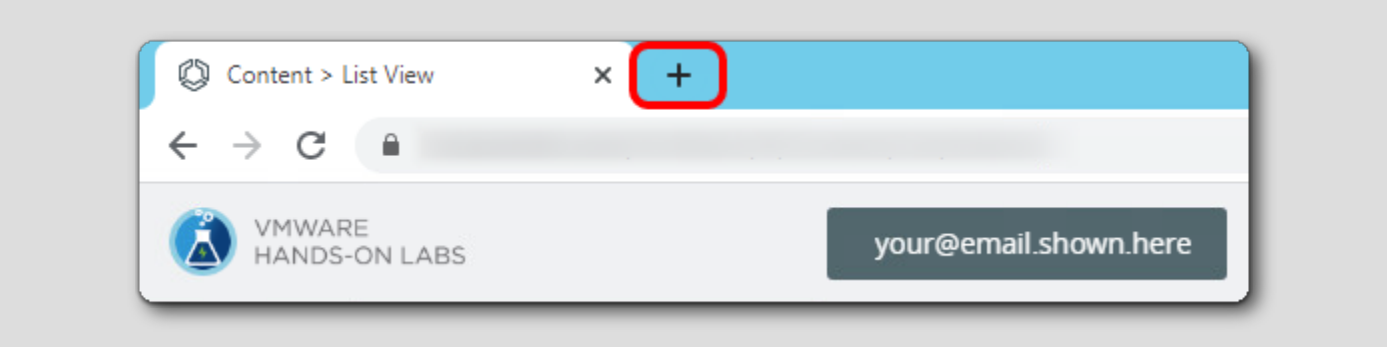
Log into Workspace ONE Access Admin Console

[497]

In this section, we login to the Workspace ONE Access admin console and access the Hub Services admin console.

Open a New Browser Tab

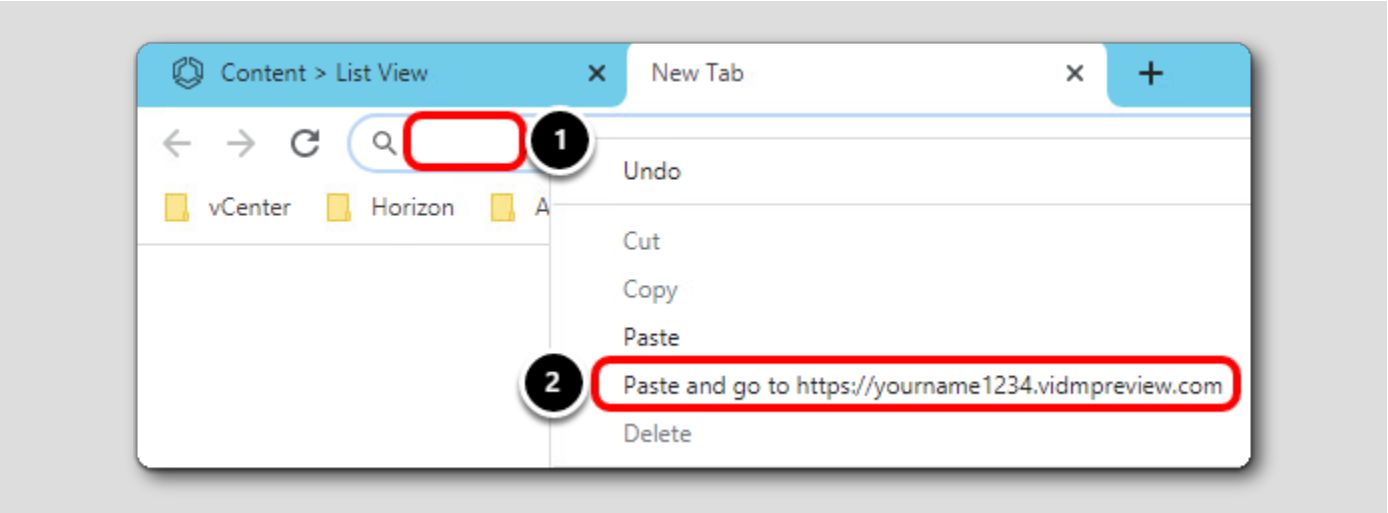
[498]



Click the Add **Tab button** in the browser to open a new tab.

Navigate to Your Workspace ONE Access Tenant URL

[499]

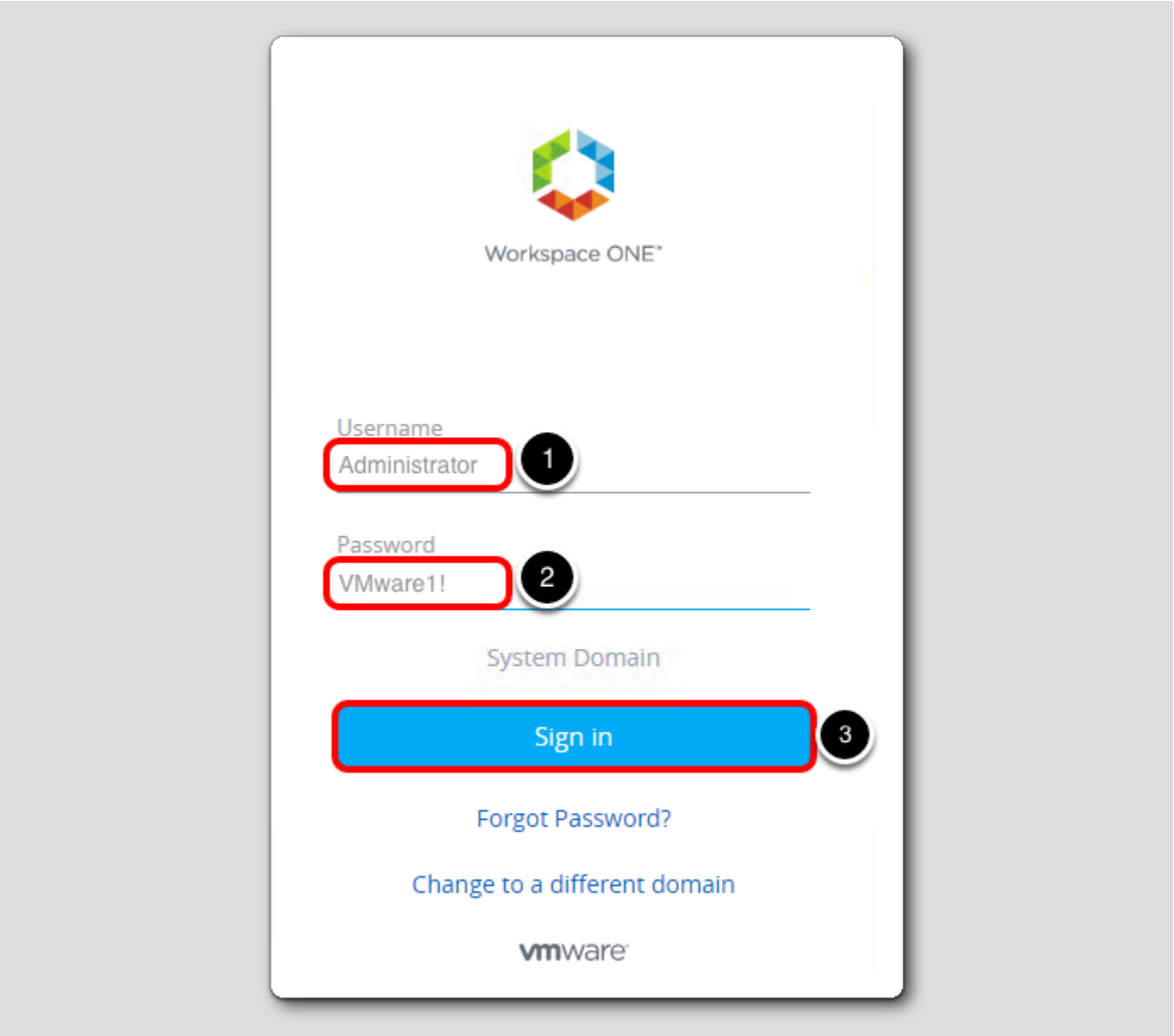


1. Right-click **inside the address bar** in the new tab.
2. Click **Paste and go to** the URL.

NOTE: This is the Workspace ONE Access tenant URL you received from the previous steps. If you did not copy or note this information from the previous step, return to those previous steps and note your Workspace ONE Access tenant URL.

Login to Your Workspace ONE Access Tenant

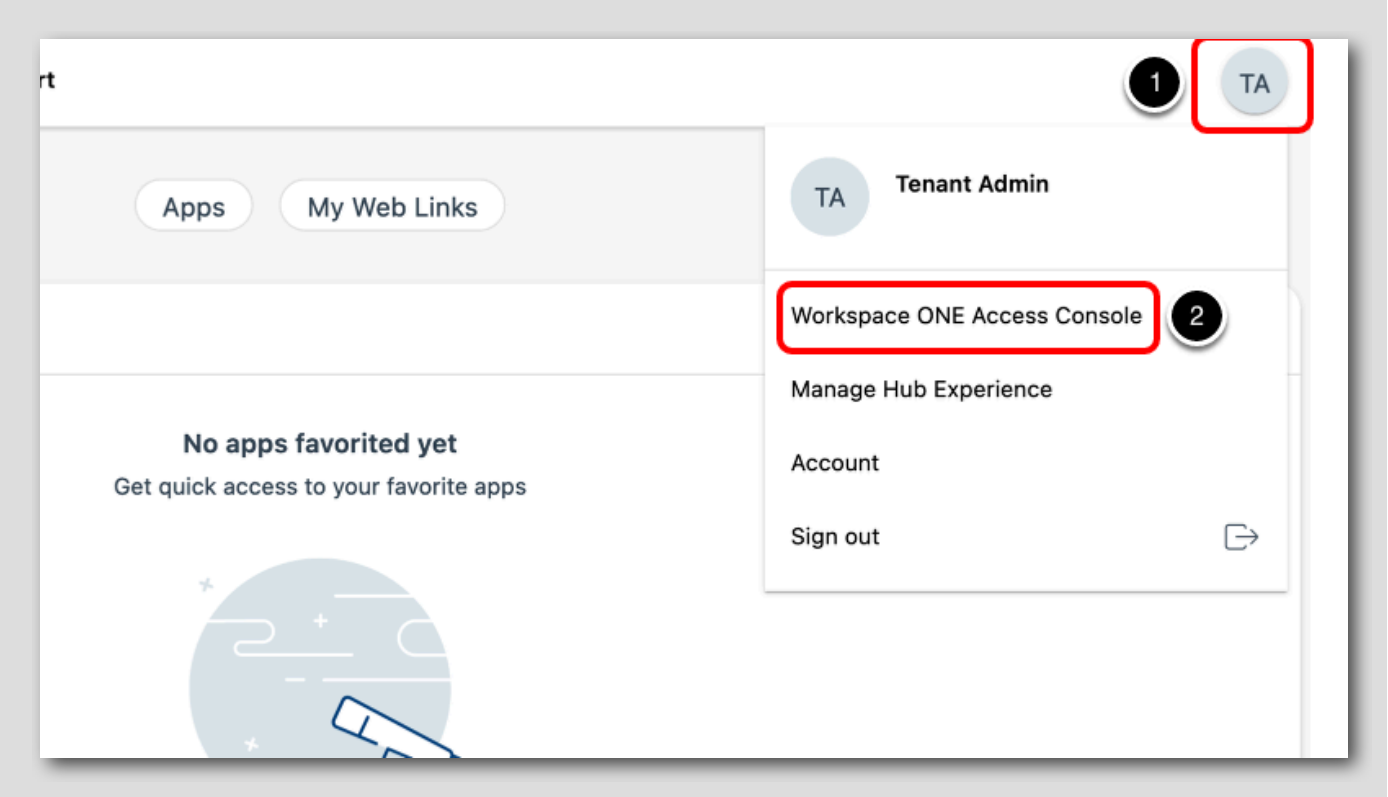
[500]



1. Enter **`Administrator`** for the Username
2. Enter **`VMware1!`** for the Password
3. Click **Sign In**

Navigate to the Administrator Console

[501]



After logging in, you will see the Intelligent Hub User Portal as pictured above. You will need to navigate to the Administrator Console.

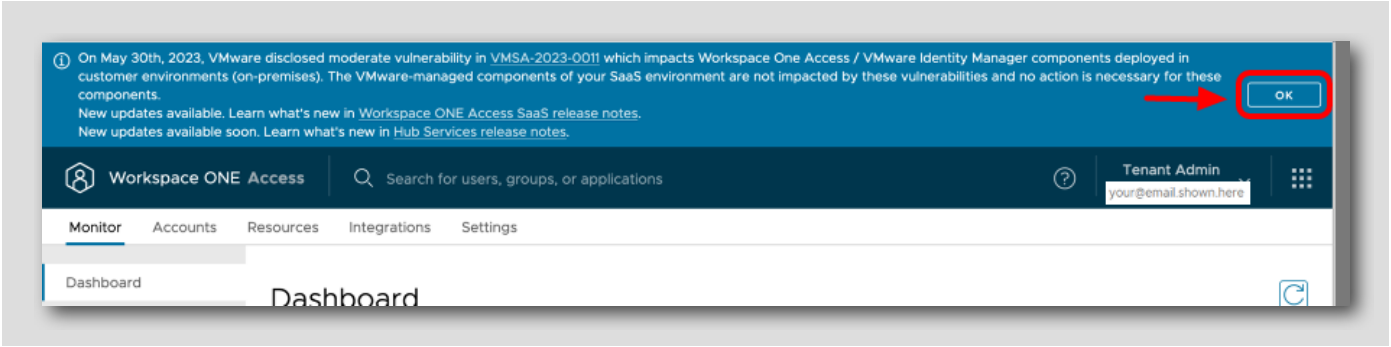
1. Click the **User dropdown circle** in the top-right corner.
2. Click **Workspace ONE Access Console.**

This will open the Administration Console in a separate tab in your browser.

NOTE: If you do not see the above view, you are already in the Administration Console and can skip this step.

(Optional)Dismiss the Release Notes Banner

[502]



If you see a banner about Security Updates or Release Notes details, click **OK** on the far right to dismiss it.

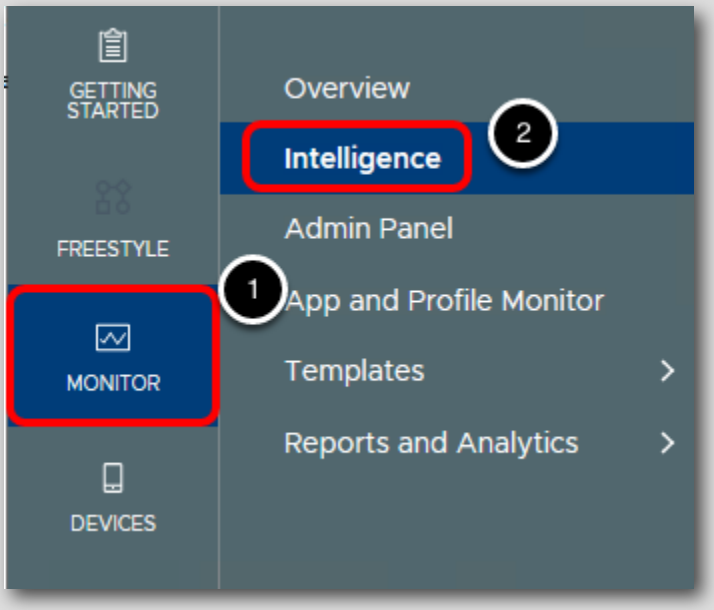
Intelligence Opt-In Process

[503]

The first step to start using Workspace ONE Intelligence is to authorize the data synchronization between Workspace ONE UEM and Intelligence Cloud Service. This is done through the Opt-In Process that needs to be performed by someone with administrator privileges to the Workspace ONE UEM console.

Access to Intelligence

[504]

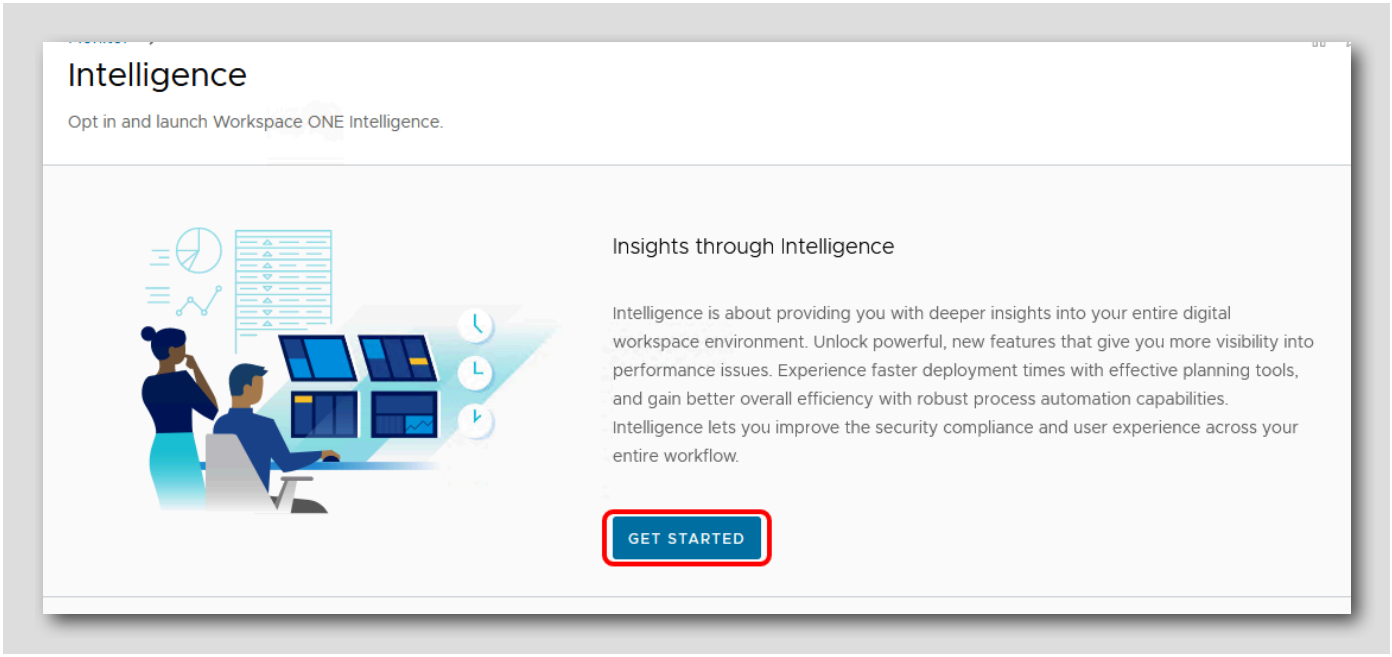


In the Workspace ONE UEM Console:

1. Click **Monitor**.
2. Click **Intelligence**.

Getting Started

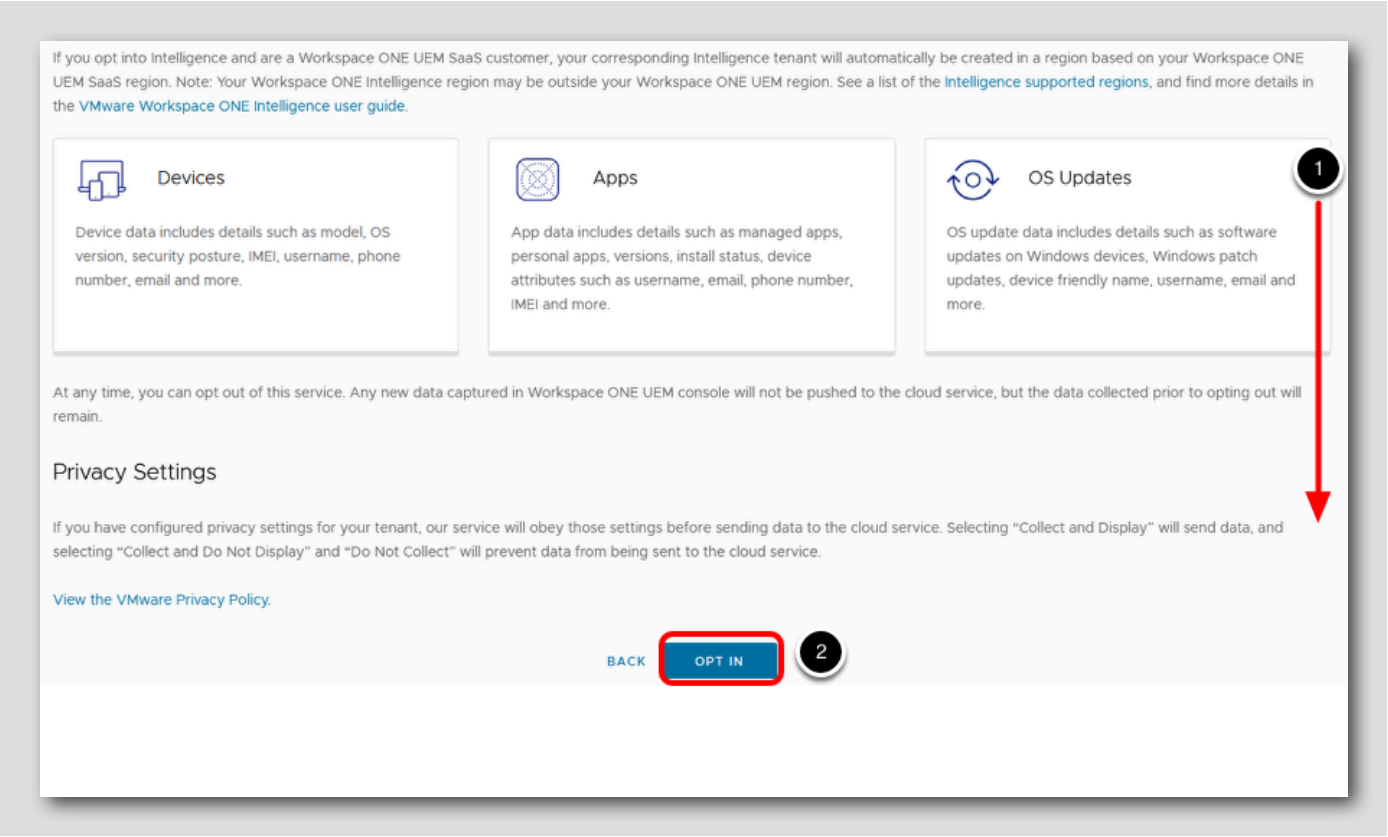
[505]



Click **GET STARTED** to initiate the Opt-in process

Authorizing Intelligence to collect and replicate the data (Opt-In)

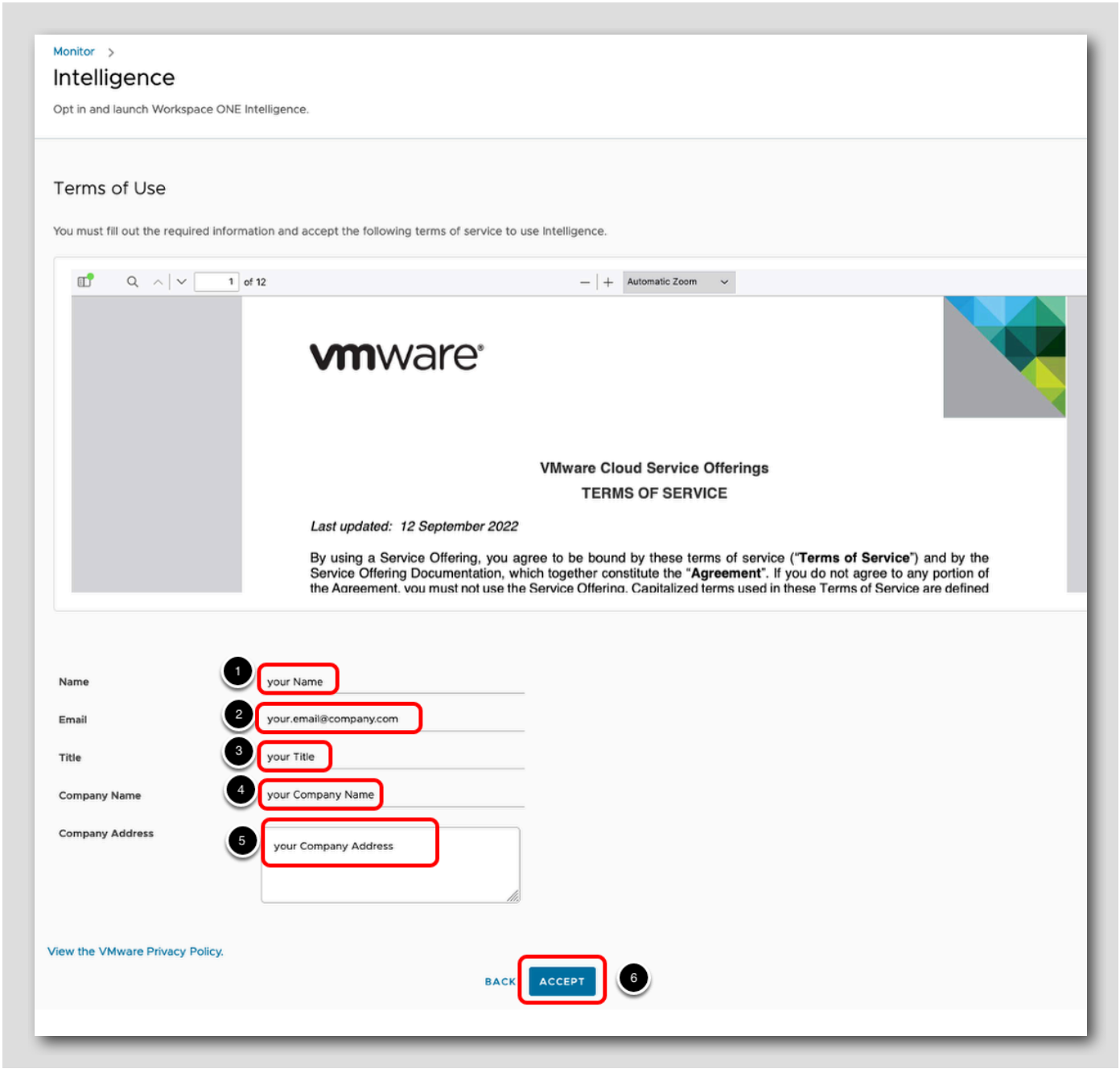
[506]



1. Scroll down to find the **OPT IN** box.
2. **Select** the **OPT IN** box.

Complete the Terms of Service

[507]



This is the final step on the opt-in Process, where you will be providing your information and accept the VMware Cloud Services Terms of Service.

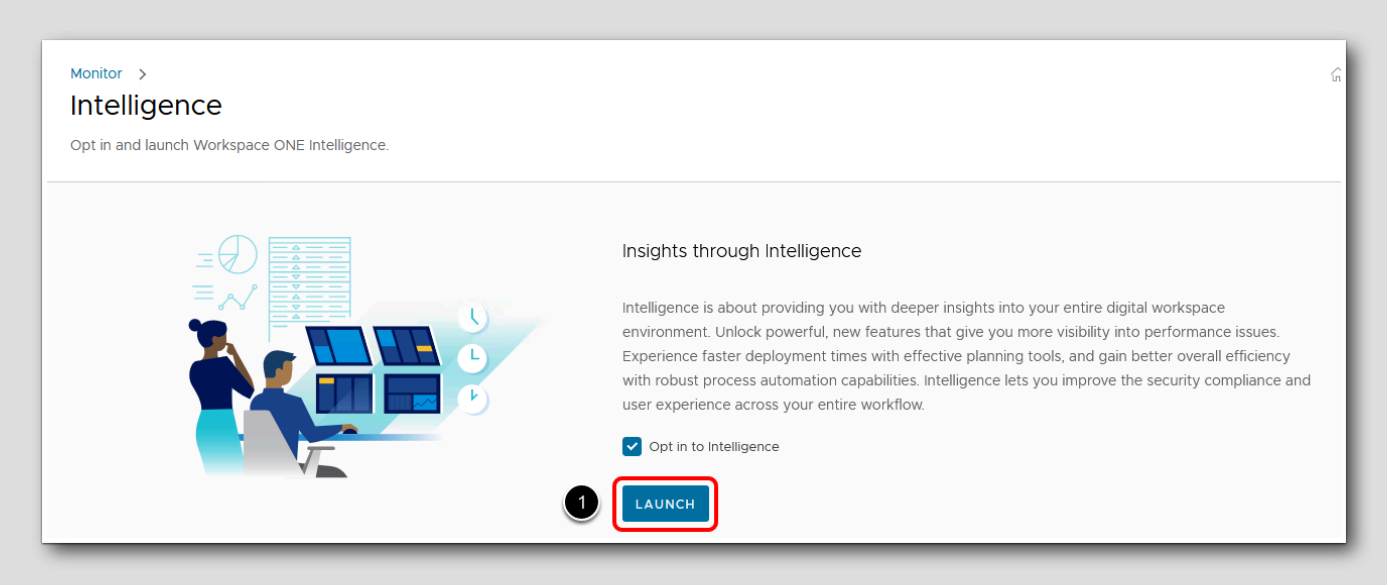
1. Enter **your Name**.
2. Enter **your Email Address**.
3. Enter **your Title**.
4. Enter **your Company Name**.
5. Enter **your Company Address**.
6. Click **Accept**.

After accepting, you will be redirected to the Workspace ONE Intelligence Console.

Note: Due to the lab environment the terms of service may not be displayed, please continue to the next step.

Launch Intelligence

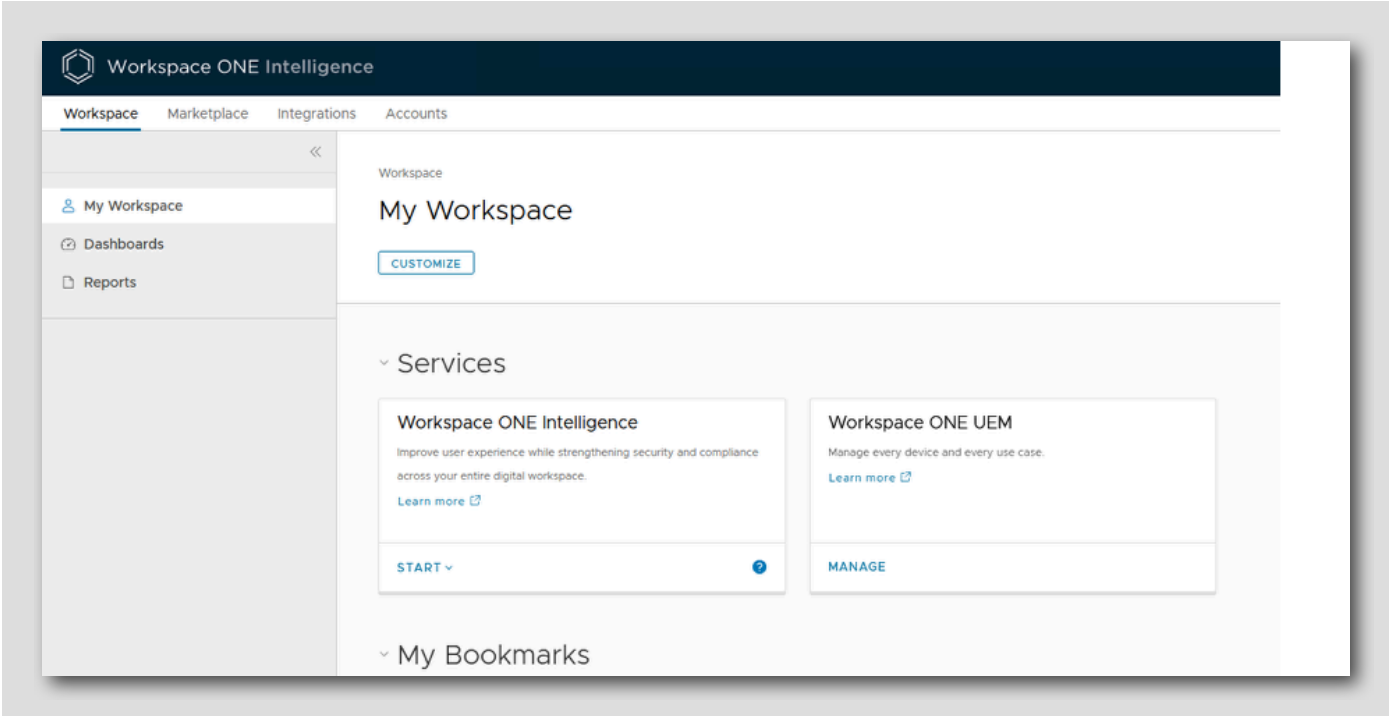
[508]



1. Click **Launch** top open Intelligence

Confirm Intelligence Activation

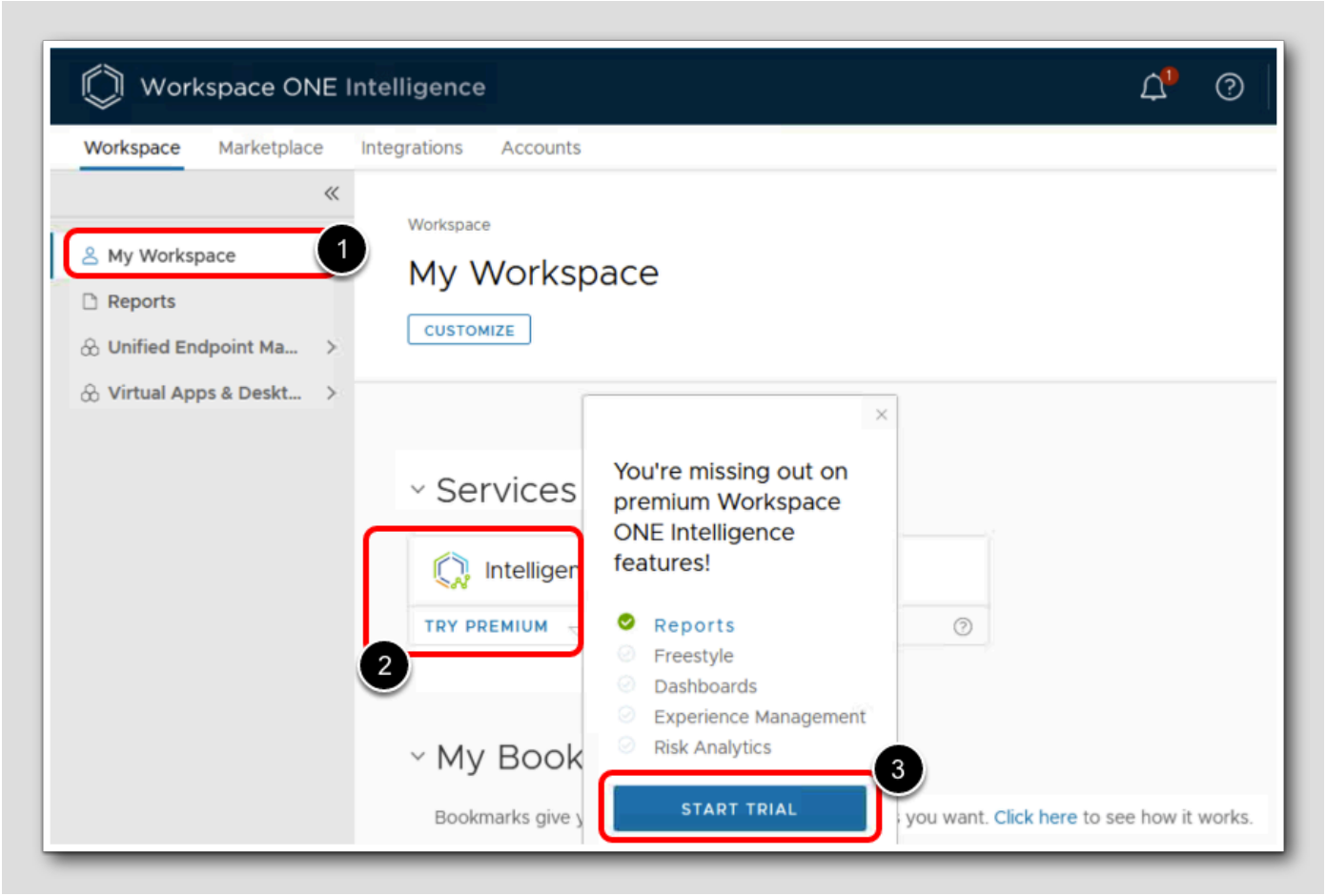
[509]



1. Verify the Intelligence website opens

Activate 30 Day Trial

[510]



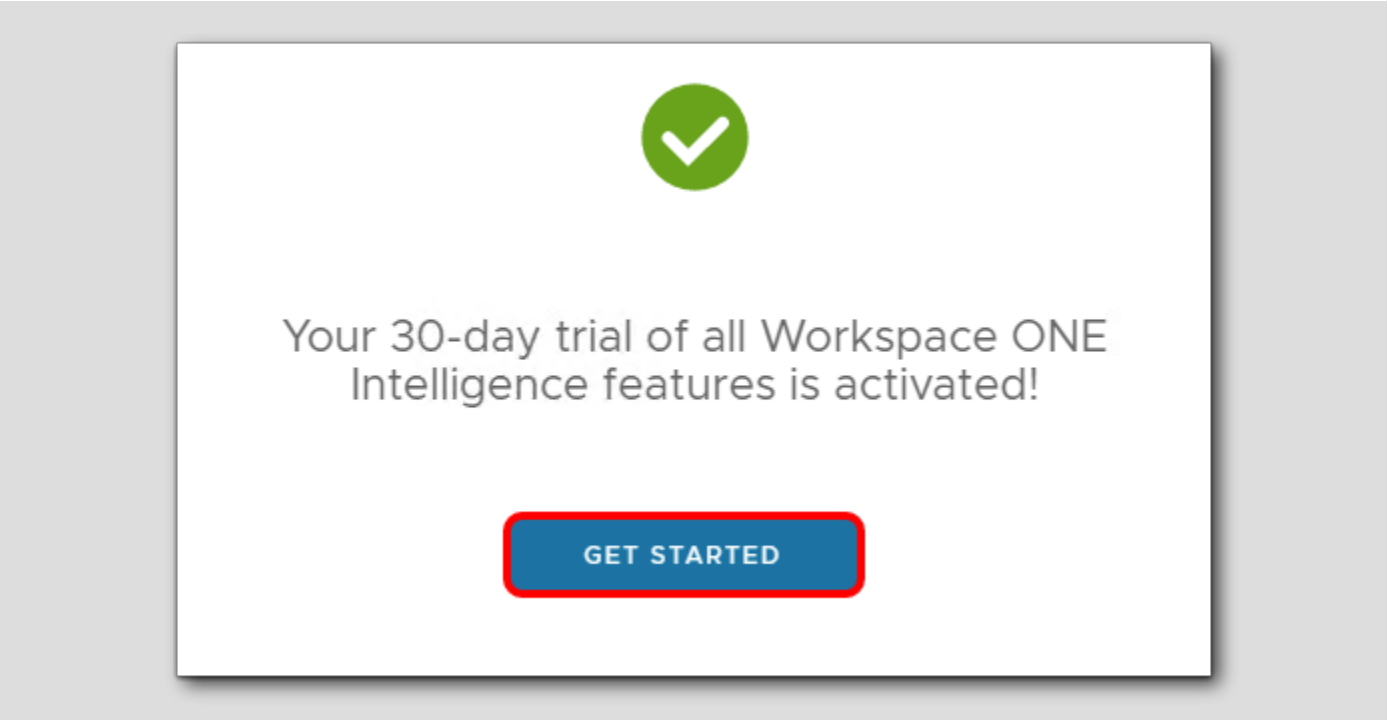
1. Click **My Workspace**
2. Click **Try Premium** under **Intelligence**
3. Click **Start Trial**

Enter the details for 30 Day trial [511]

1. Enter your First Name.
2. Enter your Last Name.
3. Enter your Email Address.
4. Enter your Job Title.
5. Enter your Company Name.
6. Enter your Company City.
7. Enter your Zip/Postal Code.
8. Enter your Company Country.
9. Enter your Phone Number.
10. Click Accept.

Confirm Trial Activation

[512]

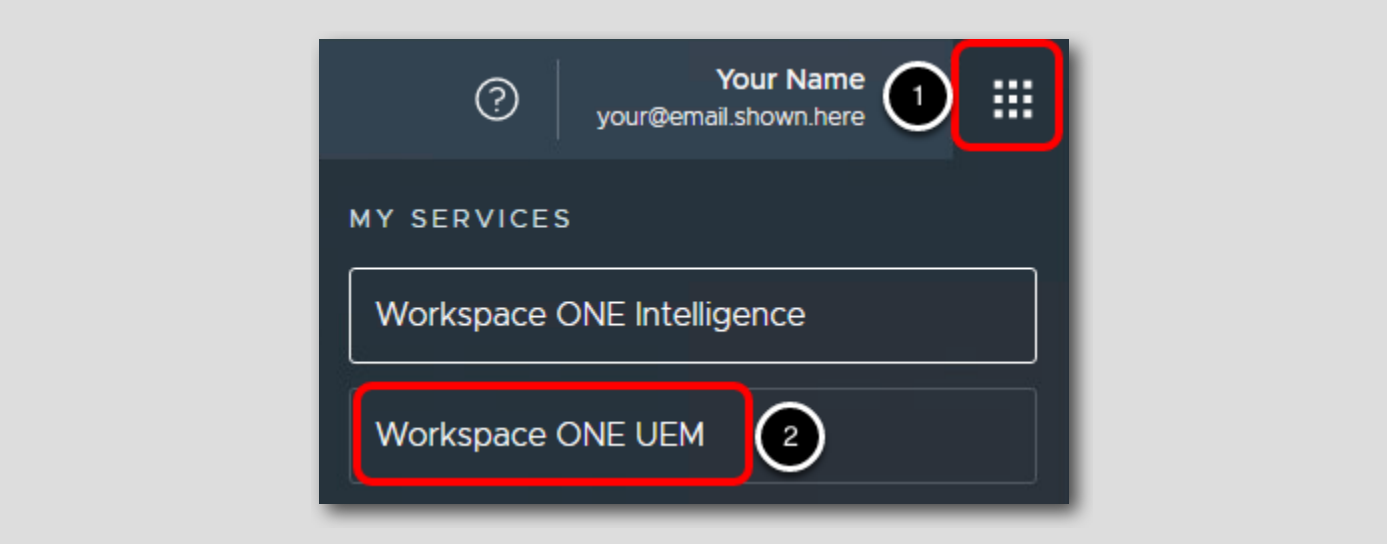


Click **Get Started**.

Returning to Workspace ONE UEM Console

[513]

You will now enroll the provided Windows 10 virtual machine into Workspace ONE UEM. You will use this Windows 10 virtual machine throughout the lab to see how you can interact with the device in both Workspace ONE UEM and Workspace ONE Intelligence.



1. Click the **Services** button.
2. Click **Workspace ONE UEM**.

DO NOT Enroll Personal Windows 10 Devices [514]

IMPORTANT: You SHOULD NOT enroll a personal Windows 10 device for the upcoming exercise! Personal devices may be enrolled into other EMM providers which can cause undesired conflicts and issues.

Please follow the upcoming steps to enroll and use the provided **Win10-01a virtual machine** for this Hands-on Lab.

IMPORTANT: You SHOULD NOT enroll any personal device(s) for the upcoming exercise!

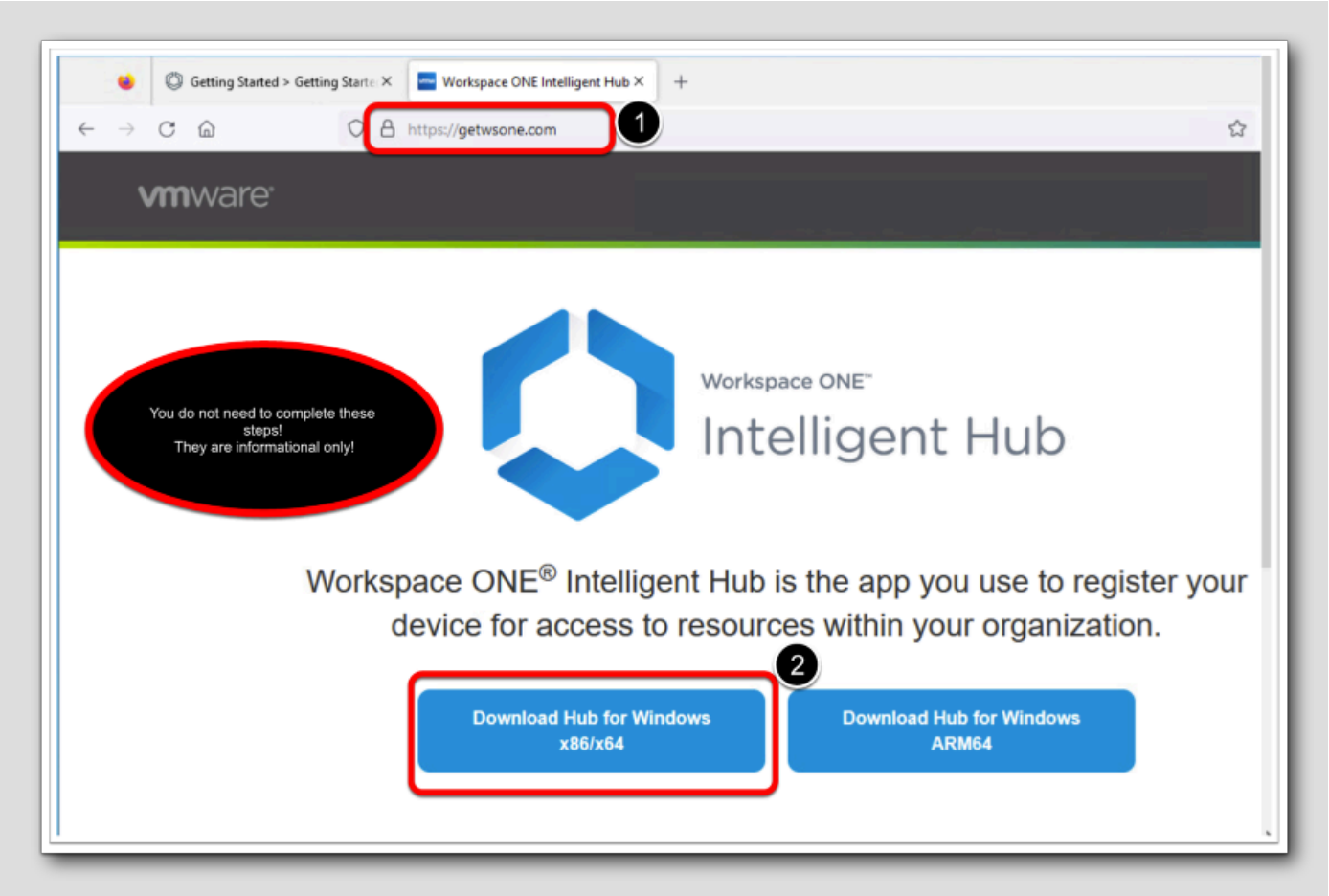
Personal devices may be enrolled into other UEM providers which can cause undesired conflicts and issues. - We want to avoid this!

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

Enrolling Your Windows 10 Device with a Basic Account [515]

You will now enroll the Windows 10 device in Workspace ONE UEM by using the Workspace ONE Intelligent Hub app.

Downloading the Workspace ONE Intelligent Hub app. [516]



NOTE: You do NOT need to complete these steps, the Workspace ONE Intelligent Hub has already been downloaded for you! This step is purely informative.

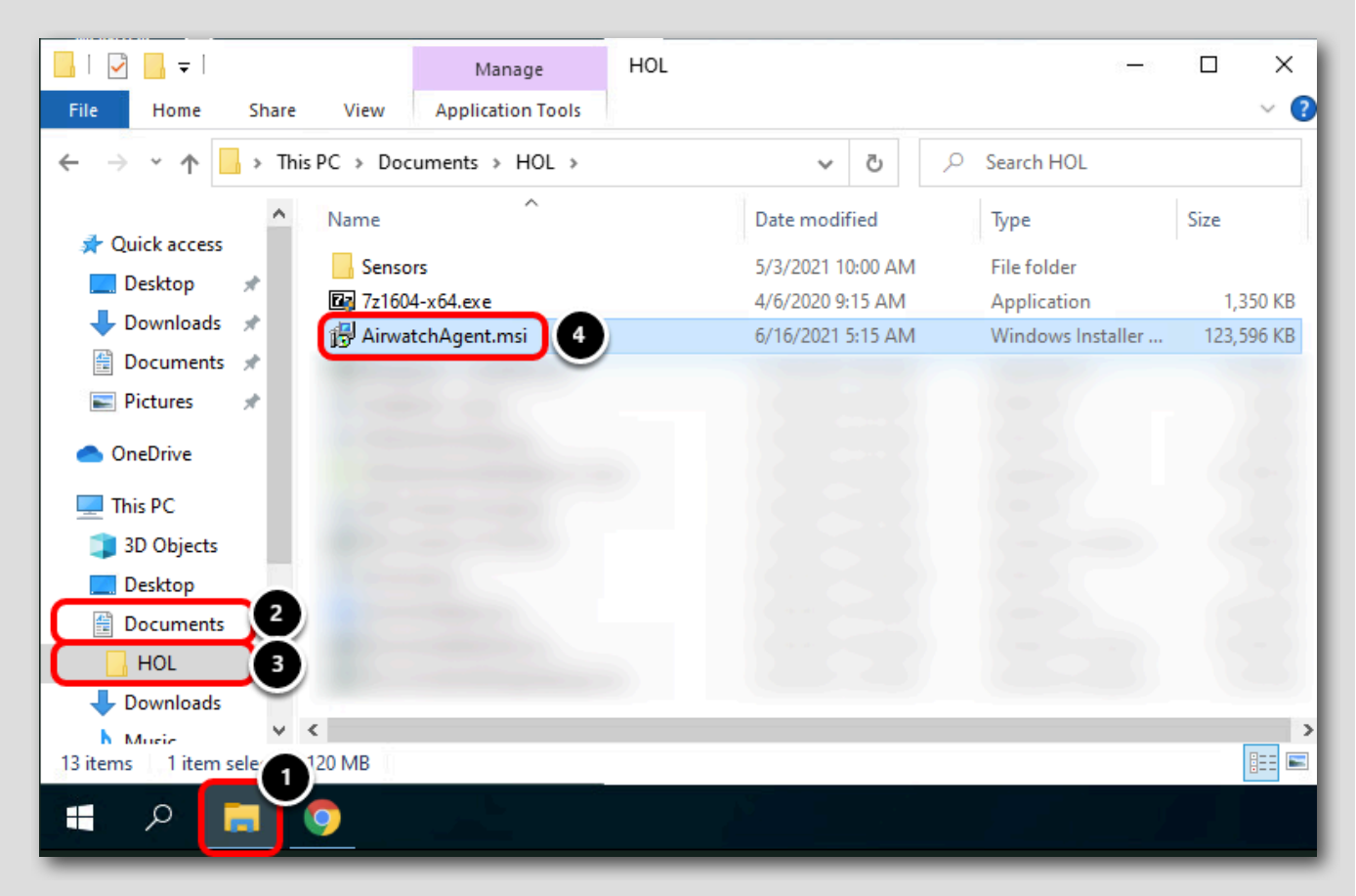
You can download the latest Workspace ONE Intelligent Hub app for your current platform by following the below steps:

1. Navigate to **`https://www.getwsone.com`** in your browser.
2. Click **Download Hub for Windows 10**.
3. Click **Keep** when warned about the AirWatchAgent.msi download.

For expediency, the Workspace ONE Intelligent Hub app has already been downloaded for you. Continue to the next step to start the installer.

Launch the Workspace ONE Intelligent Hub Installer

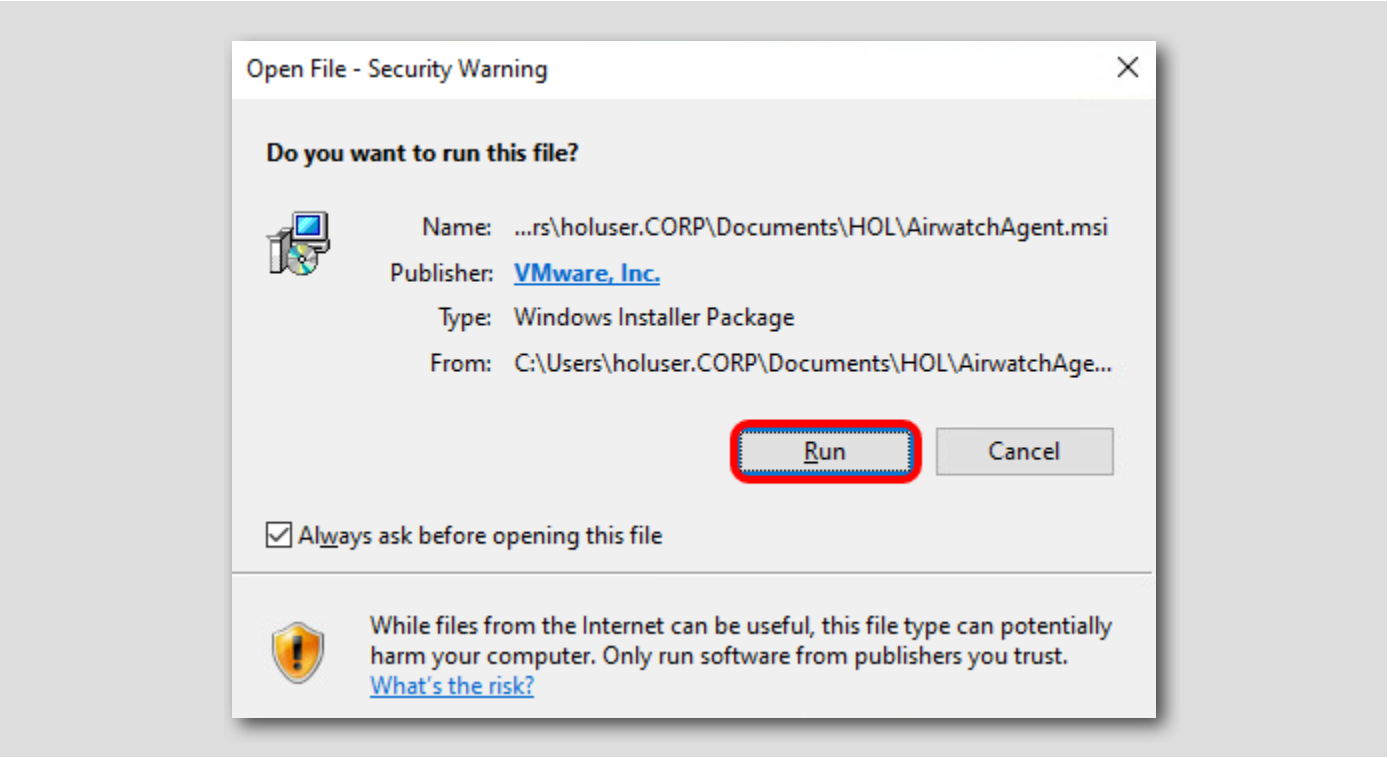
[517]



1. Click the **File Explorer** icon from the taskbar.
2. Click **Documents**.
3. Click **HOL**.
4. Double-click the **AirwatchAgent.msi** file to start the installer.

NOTE: The installer may take a few seconds to launch, please be patient after clicking the AirwatchAgent.msi file.

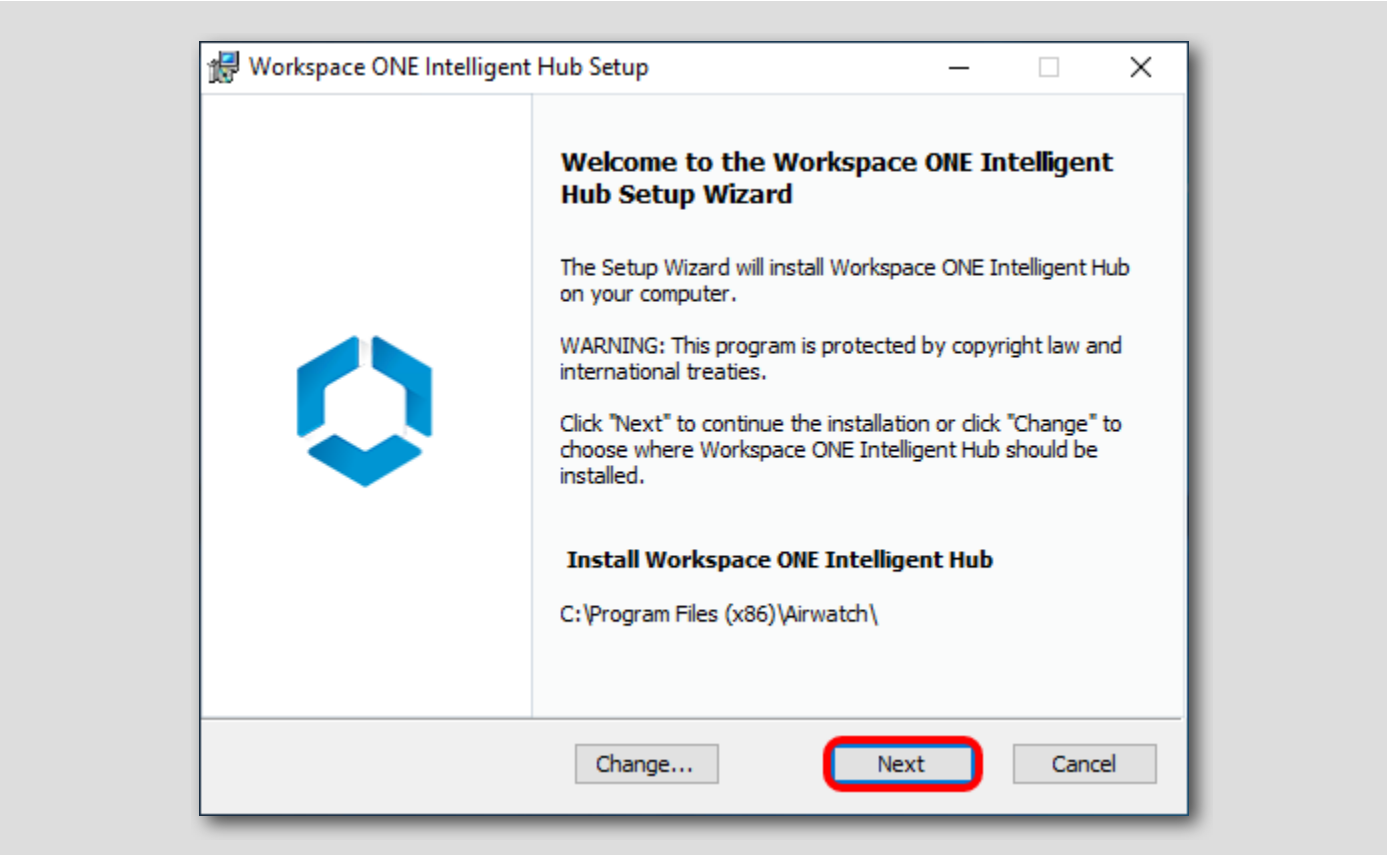
Click Run [518]



Click **Run** to proceed with the installation.

Accept the Default Install Location

[519]

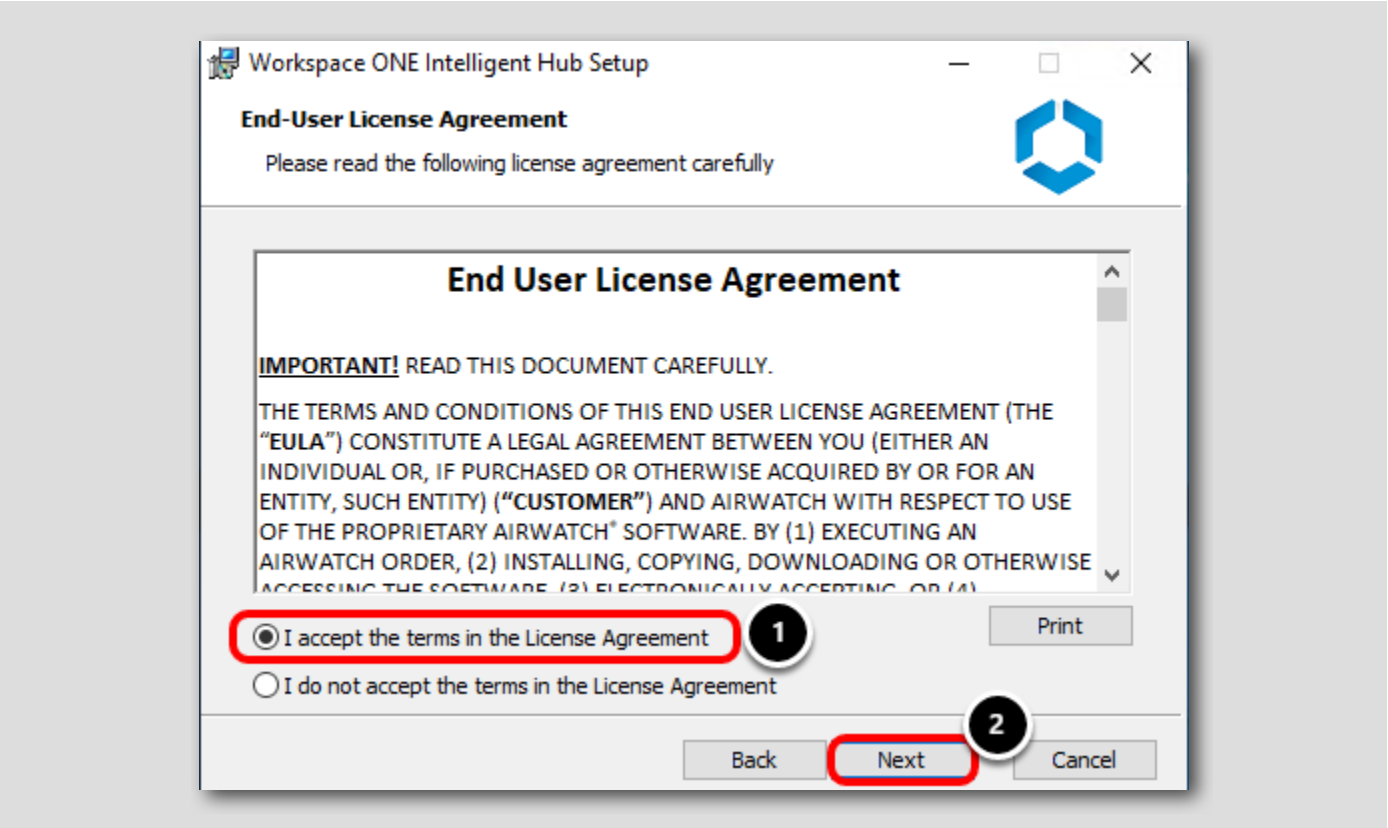


Leave the default install location and click **Next**.

NOTE: The Next button may take several seconds to enable while the required additional features are installed.

Accept the License Agreement

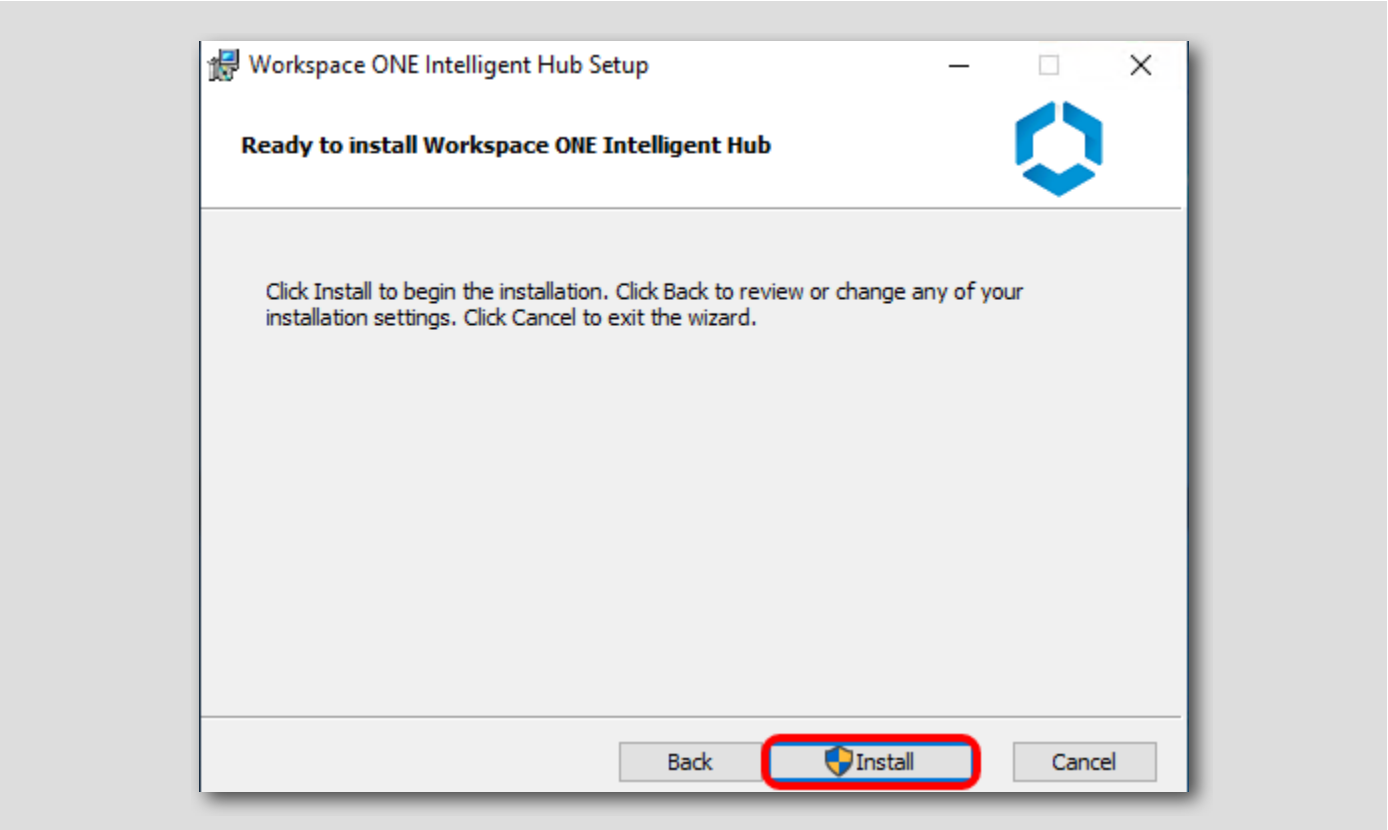
[520]



1. Select I accept the terms of the License Agreement.
2. Click **Next**.

Start the Workspace ONE Intelligent Hub Install

[521]

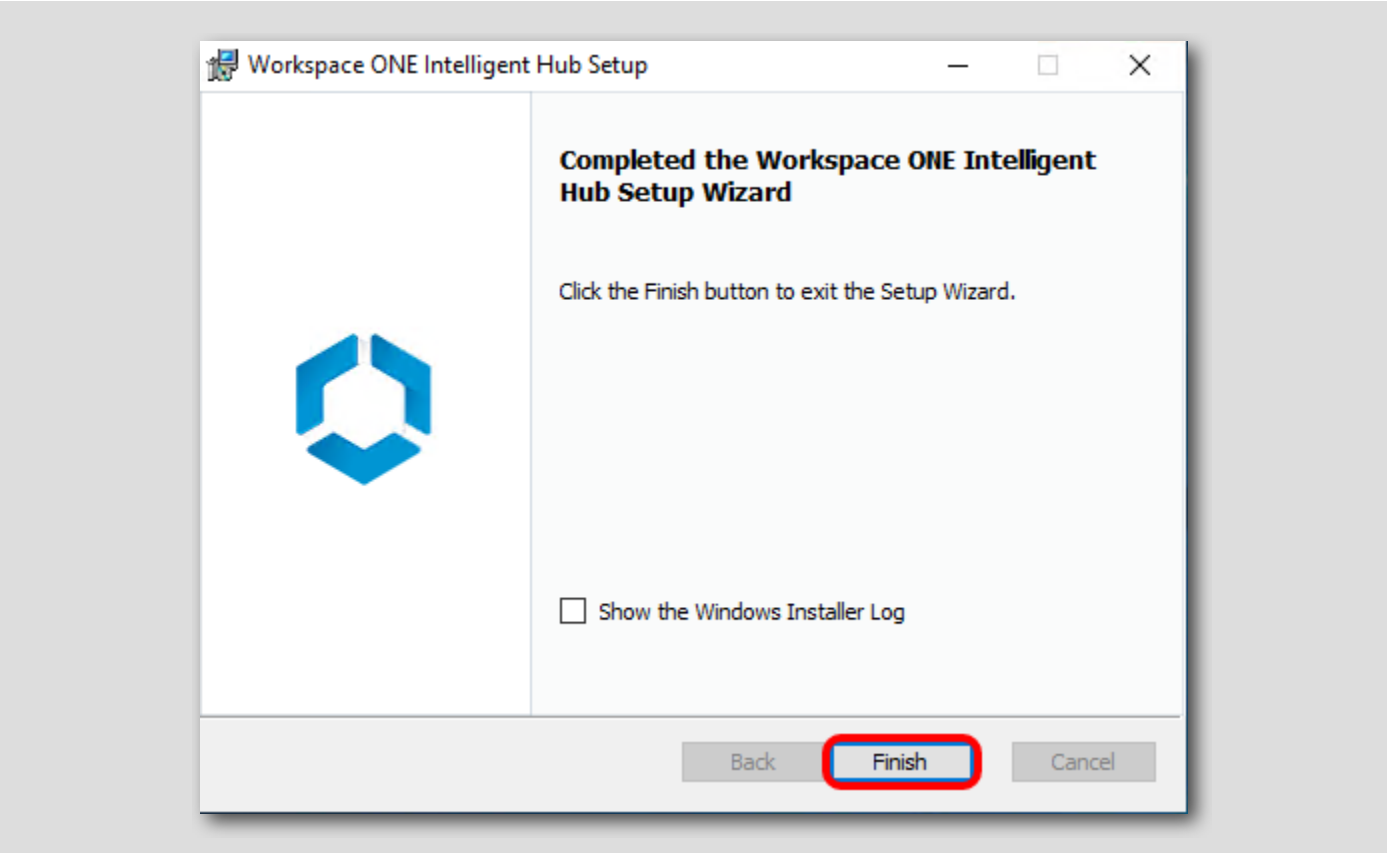


Click **Install** to start the installer.

NOTE: The Workspace ONE Intelligent Hub install may take several minutes to complete, do not interrupt the installer!

Complete the Workspace ONE Intelligent Hub Installer

[522]



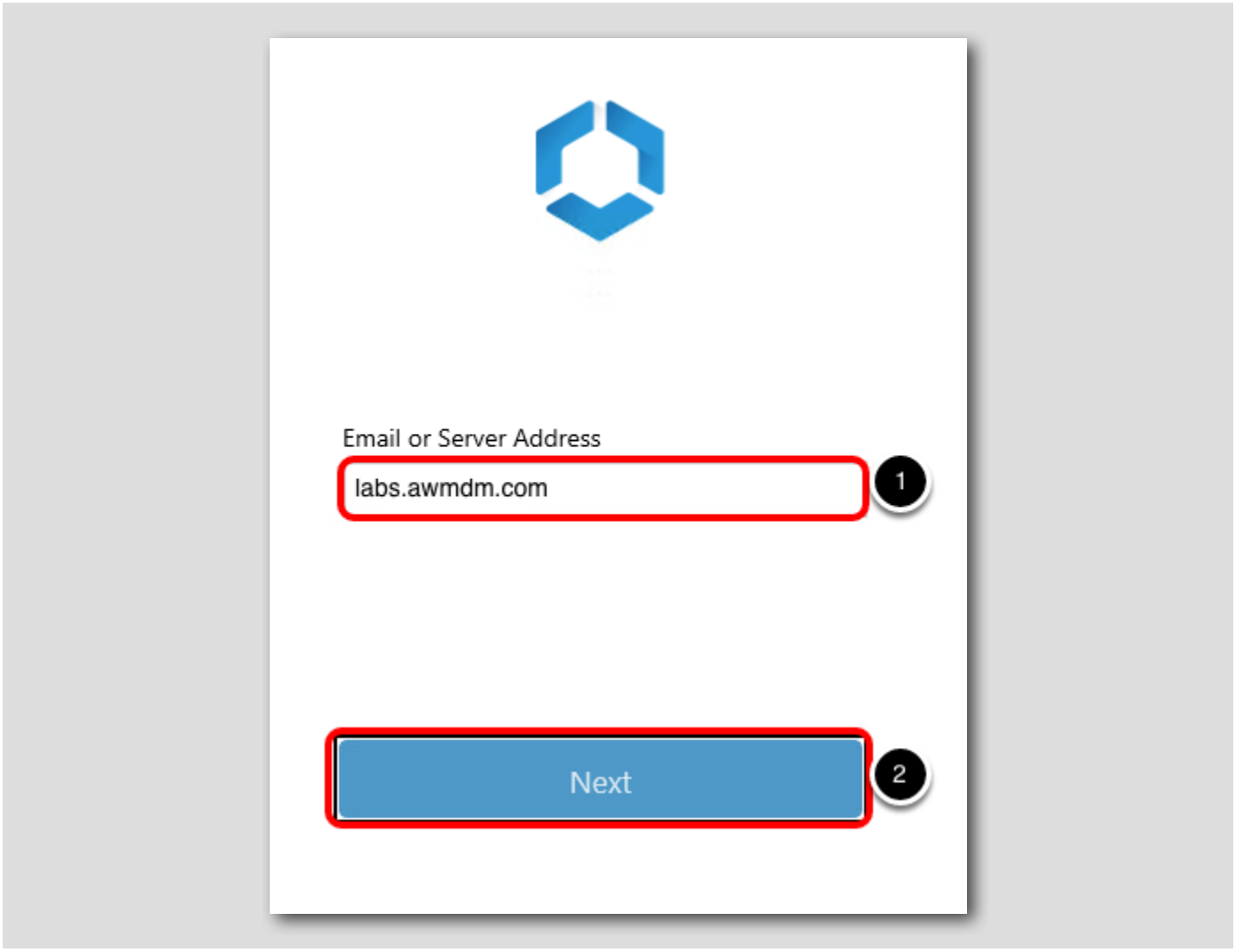
NOTE: The installer may take several minutes to complete. Please wait until you see the completed install screen before continuing.

Click **Finish** to complete the Workspace ONE Intelligent Hub installer.

NOTE: After clicking finish, the Native Enrollment application will launch to guide you through enrolling into Workspace ONE UEM. It will take 2-3 minutes to launch the Intelligent Hub.

Enroll Your Windows 10 Device using the Workspace ONE Intelligent Hub

[523]

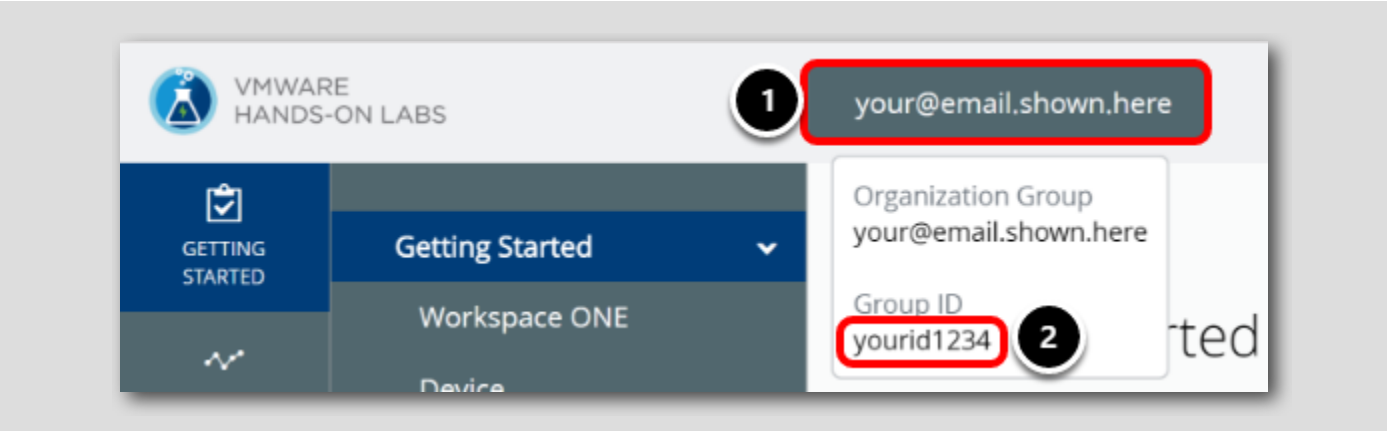


NOTE: The above screen may take 2-3 minutes to display after clicking Finish from the previous step!

1. Enter **`labs.awmdm.com`** for the Server Address.
2. Click **Next**.

Locate your Group ID from Workspace ONE UEM Console

[524]

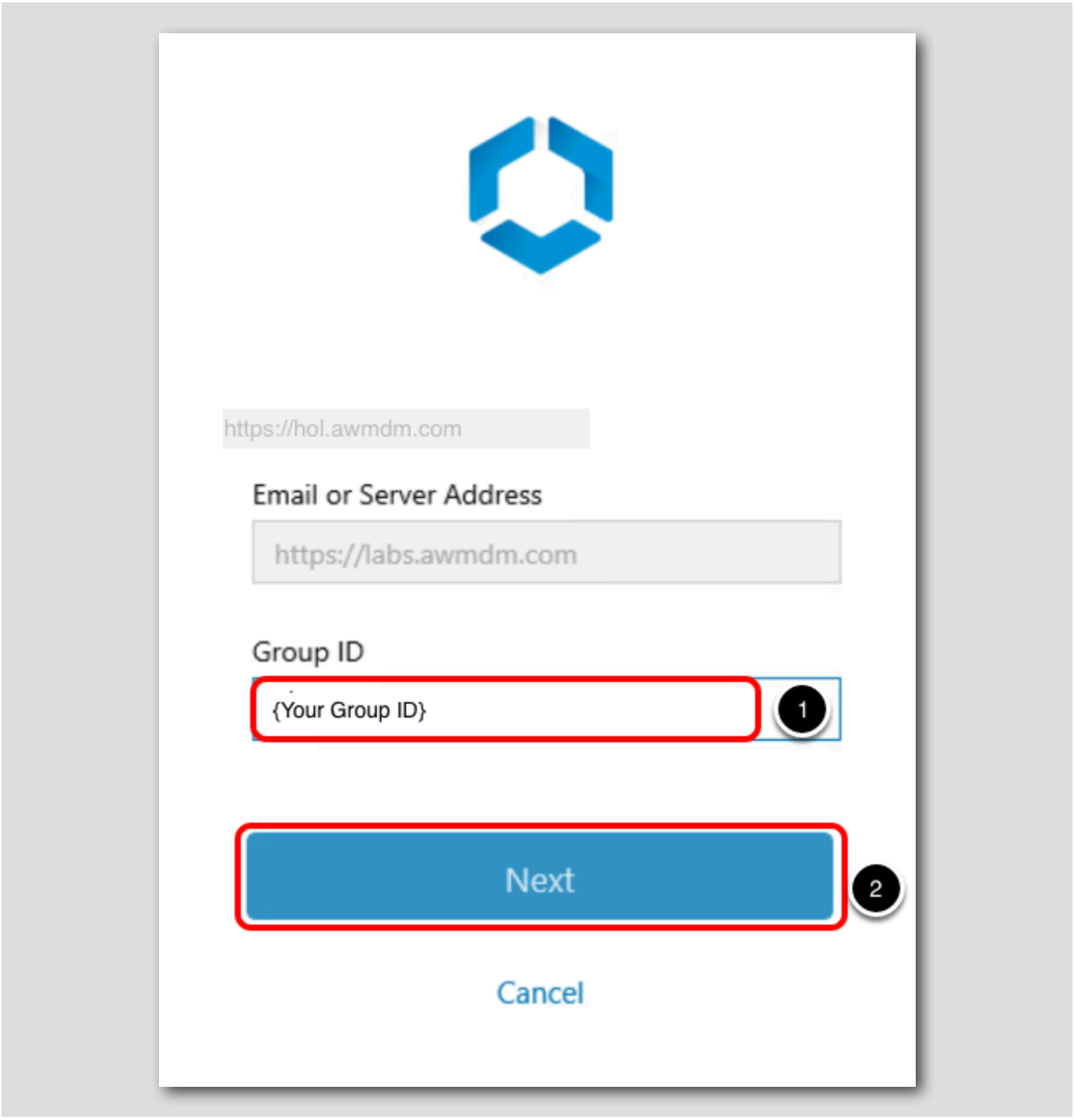


The next step is to retrieve your **Organization Group ID**.

1. To find the Group ID, Go back to the Workspace ONE UEM Administration Console and 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. Copy this value.

Enter Your Group ID

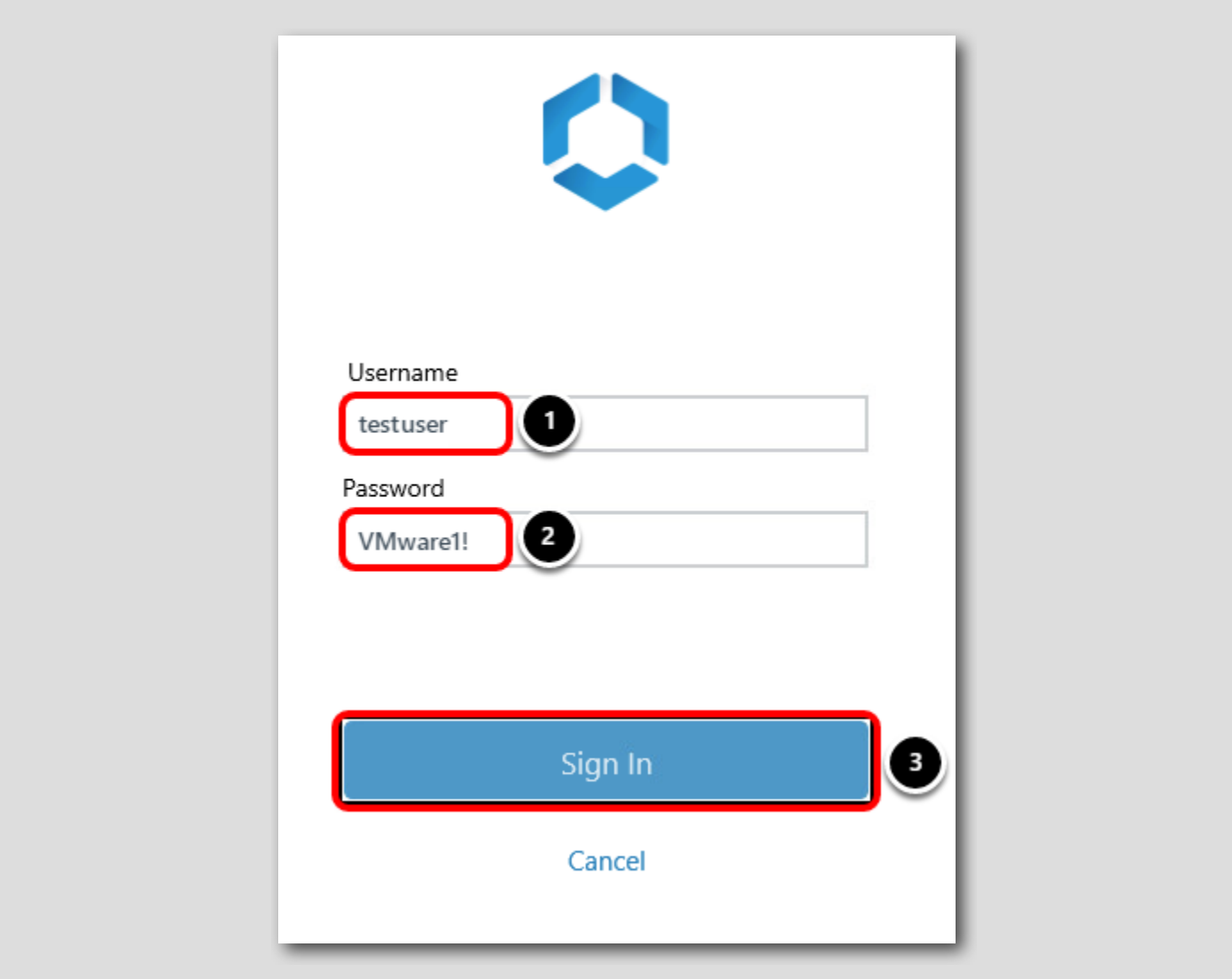
[525]



1. Enter **Your Group ID** in the **Group ID** field. If you forgot your Group ID, check the previous steps on how to retrieve it.
2. Click **Next**.

Enter Your User Credentials

[526]

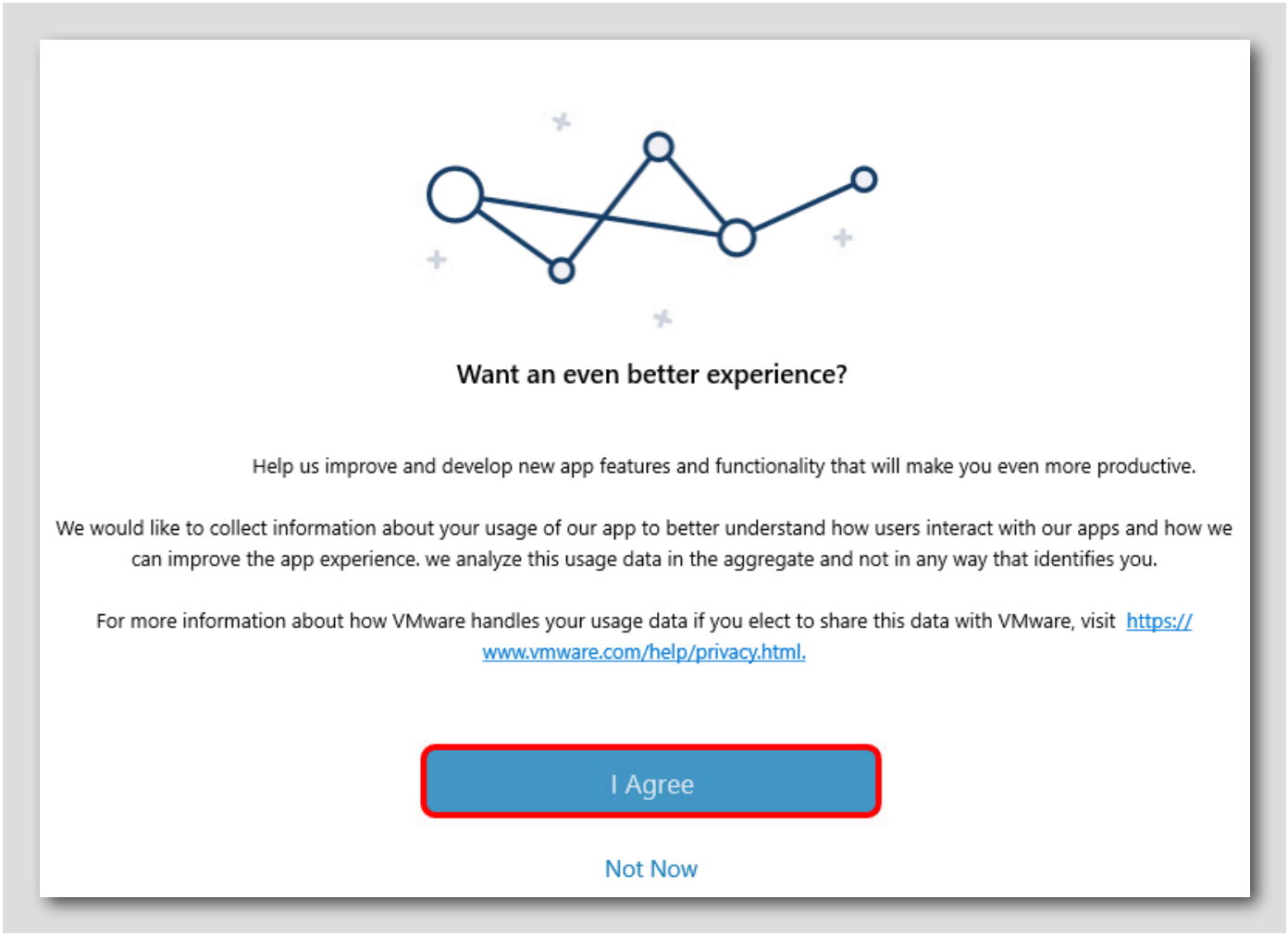


1. Enter **`testuser`** in the **Username** field.
2. Enter **`VMware1!`** in the **Password** field.
3. Click **Sign In**.

NOTE: Wait while the server checks your enrollment details. This may take a few minutes.

Accept Data Policy

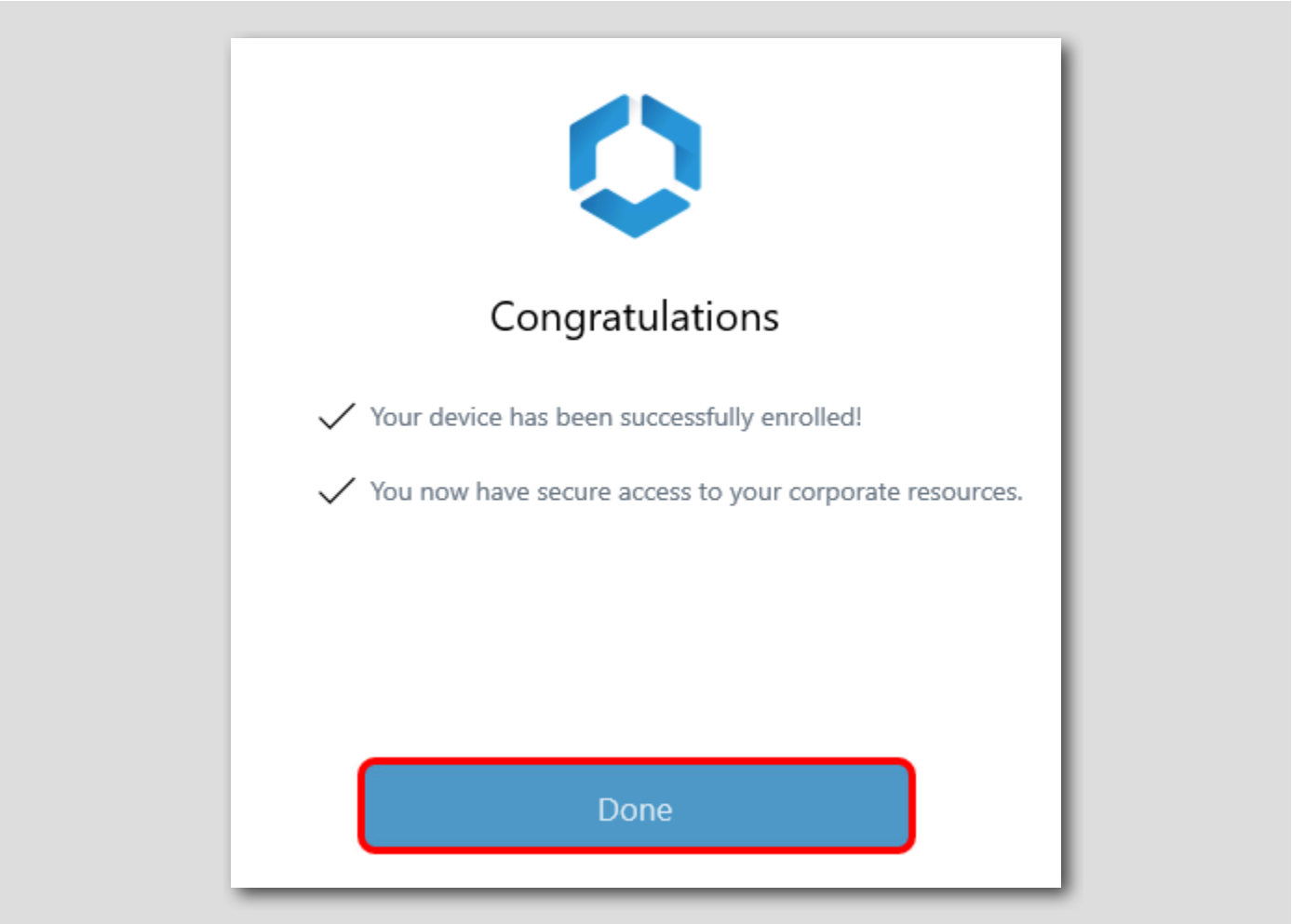
[527]



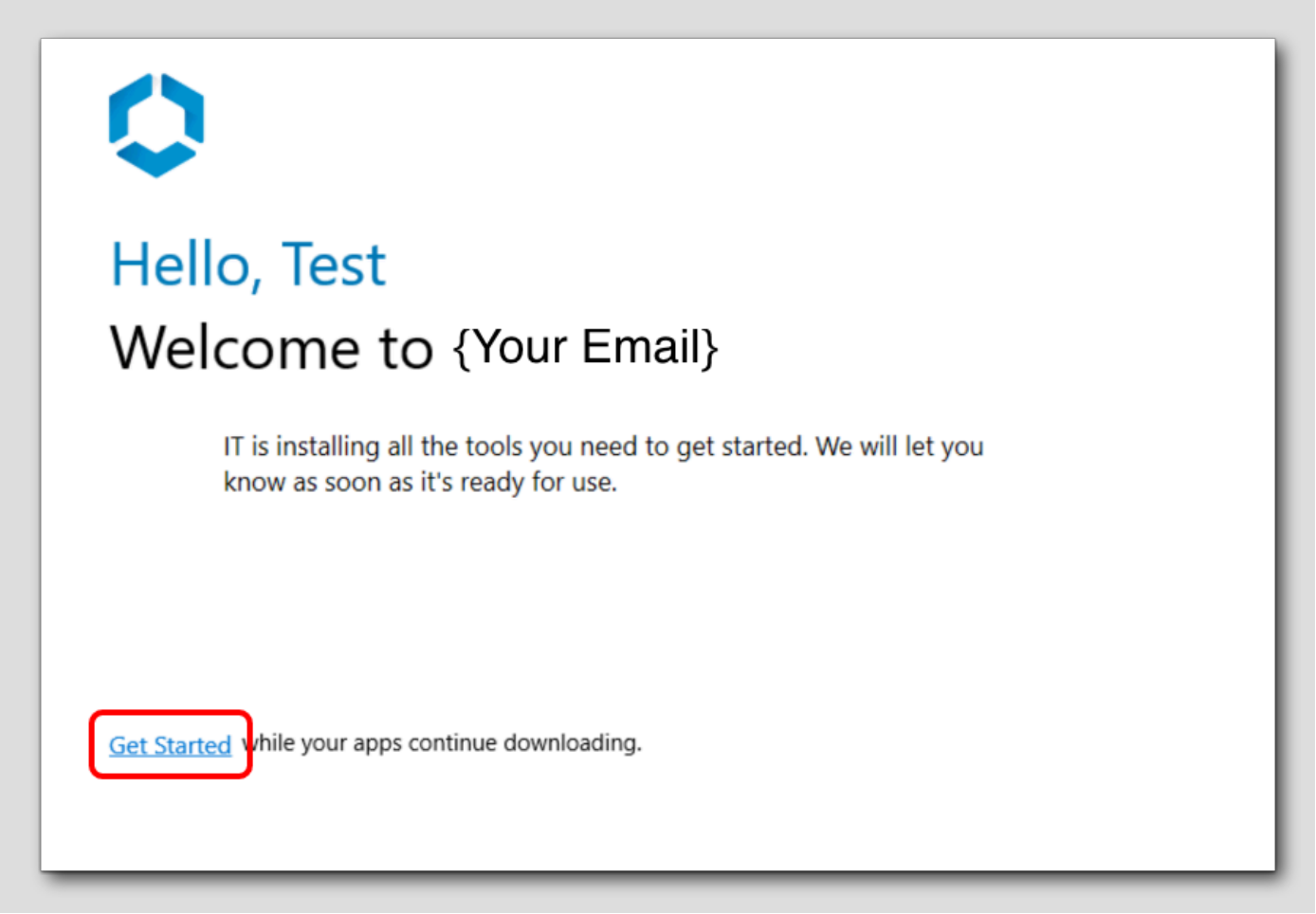
Click **I Agree**.

Finish the Workspace ONE UEM Enrollment Process

[528]



Click **Done** to end the Enrollment process.

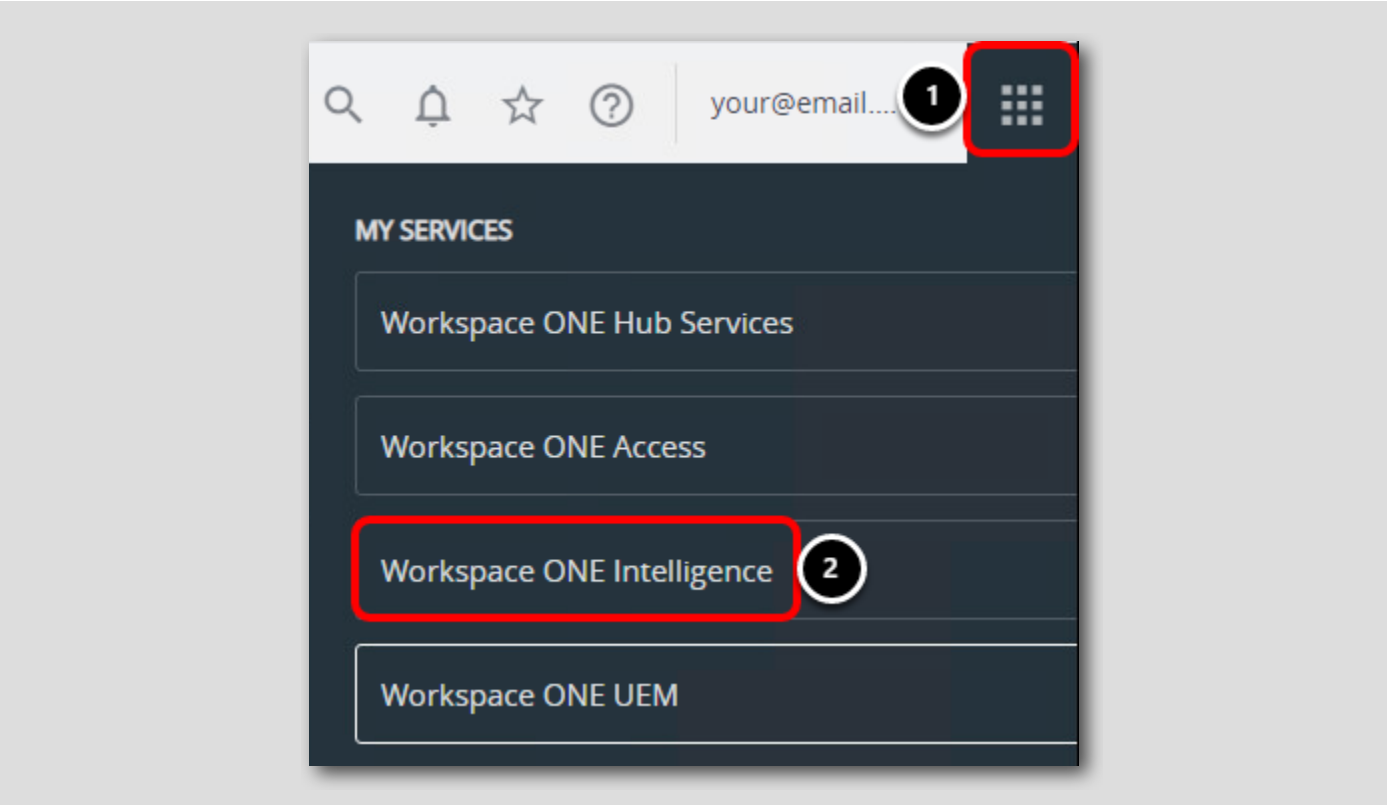


Click **Get Started** to close the onboarding welcome screen.

Your Windows 10 device is now successfully enrolled into Workspace ONE UEM!

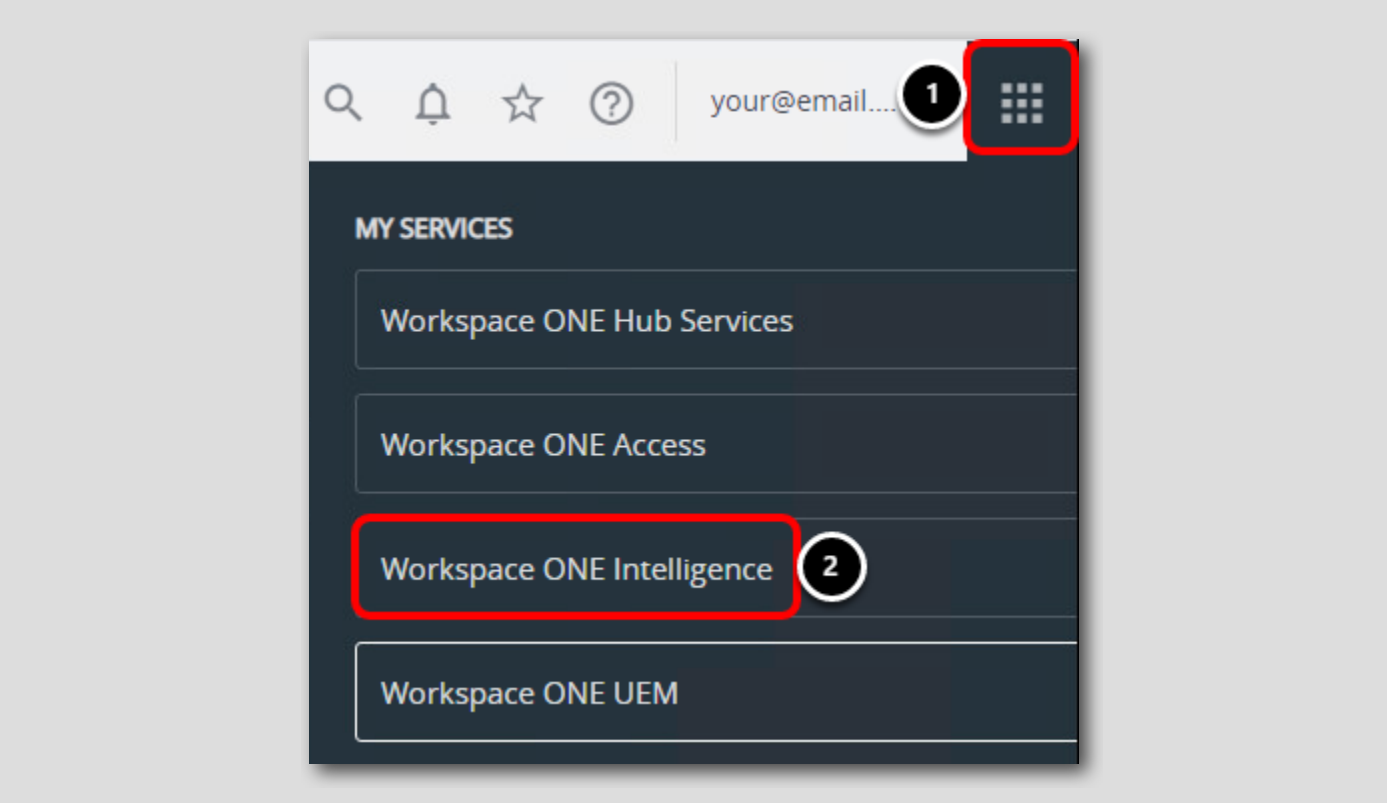
Return to the Workspace ONE Intelligence Console

[529]



Back in the Workspace ONE UEM Administration console in your browser,

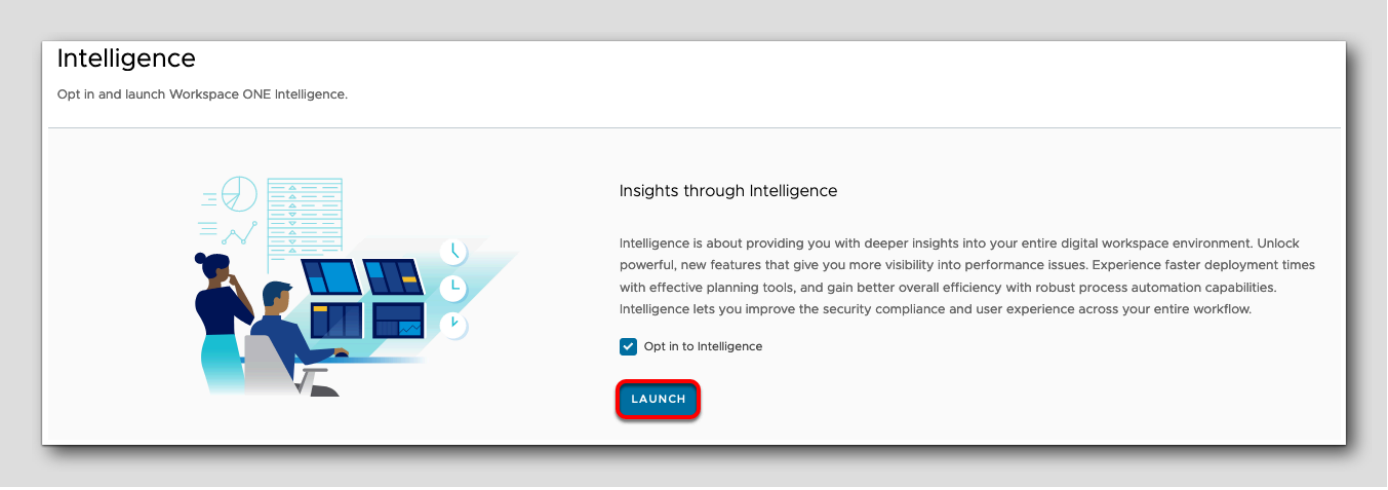
1. Click the **My Services** button in the top-right corner.
2. Click **Workspace ONE Intelligence**.



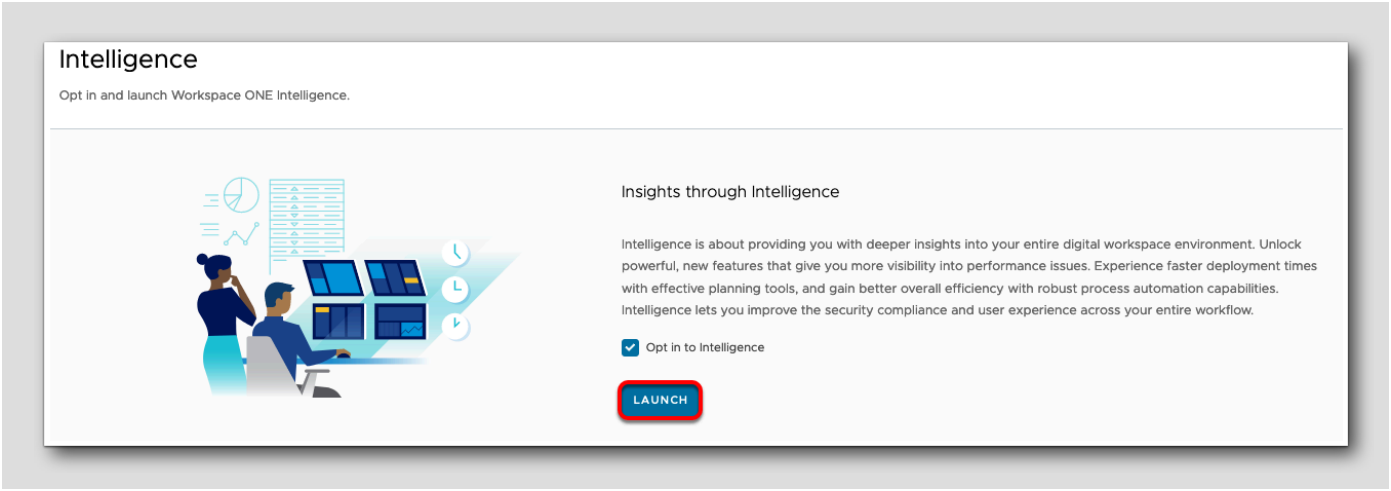
Creating Reports

[530]

In this activity, you explore reporting capabilities by creating a report for enrolled devices.

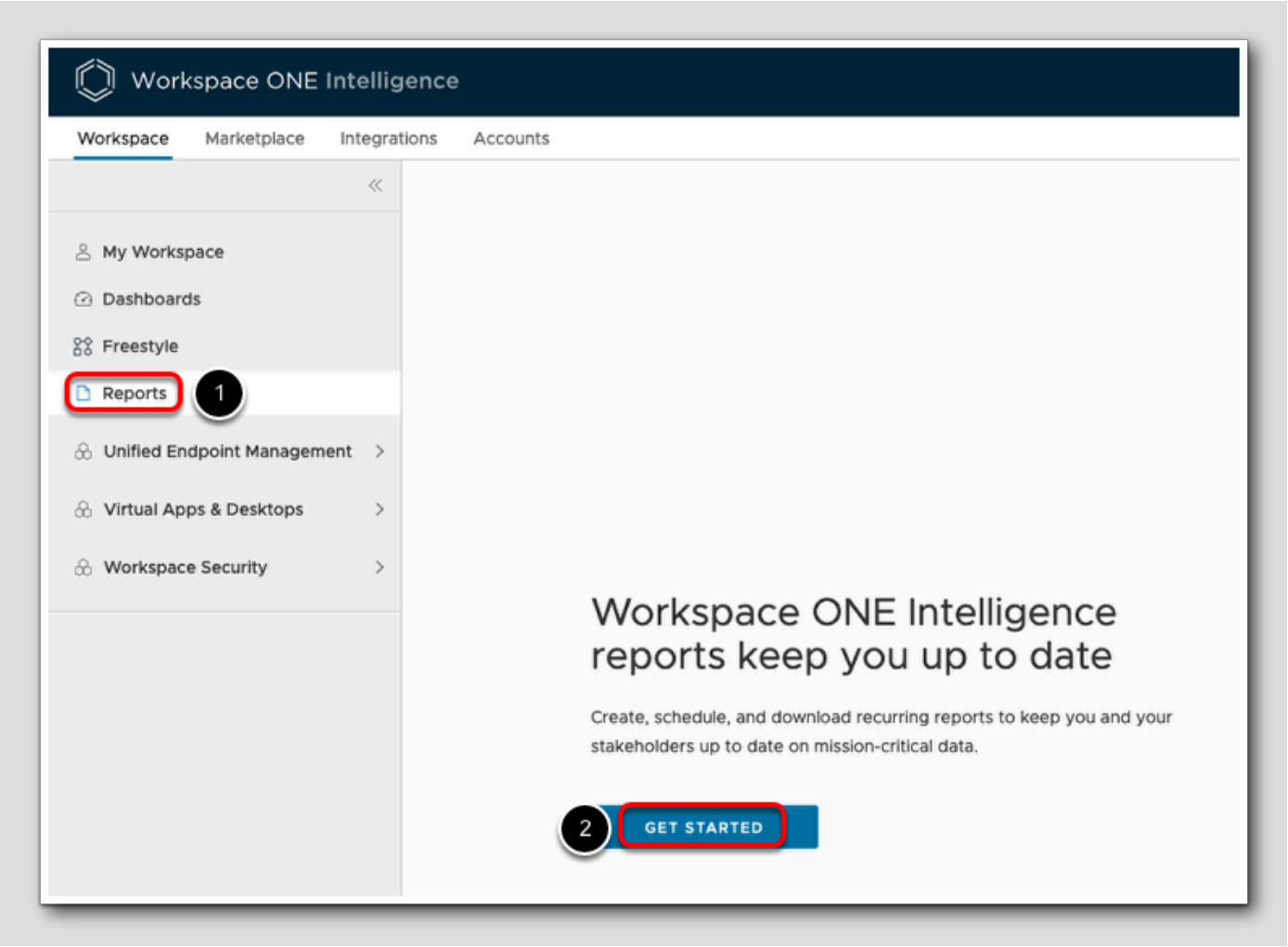


Select **Launch**


Intelligence
Opt in and launch Workspace ONE Intelligence.
Insights through Intelligence
Intelligence is about providing you with deeper insights into your entire digital workspace environment. Unlock powerful, new features that give you more visibility into performance issues. Experience faster deployment times with effective planning tools, and gain better overall efficiency with robust process automation capabilities. Intelligence lets you improve the security compliance and user experience across your entire workflow.
Opt in to Intelligence
LAUNCH

Open Report Settings

[531]

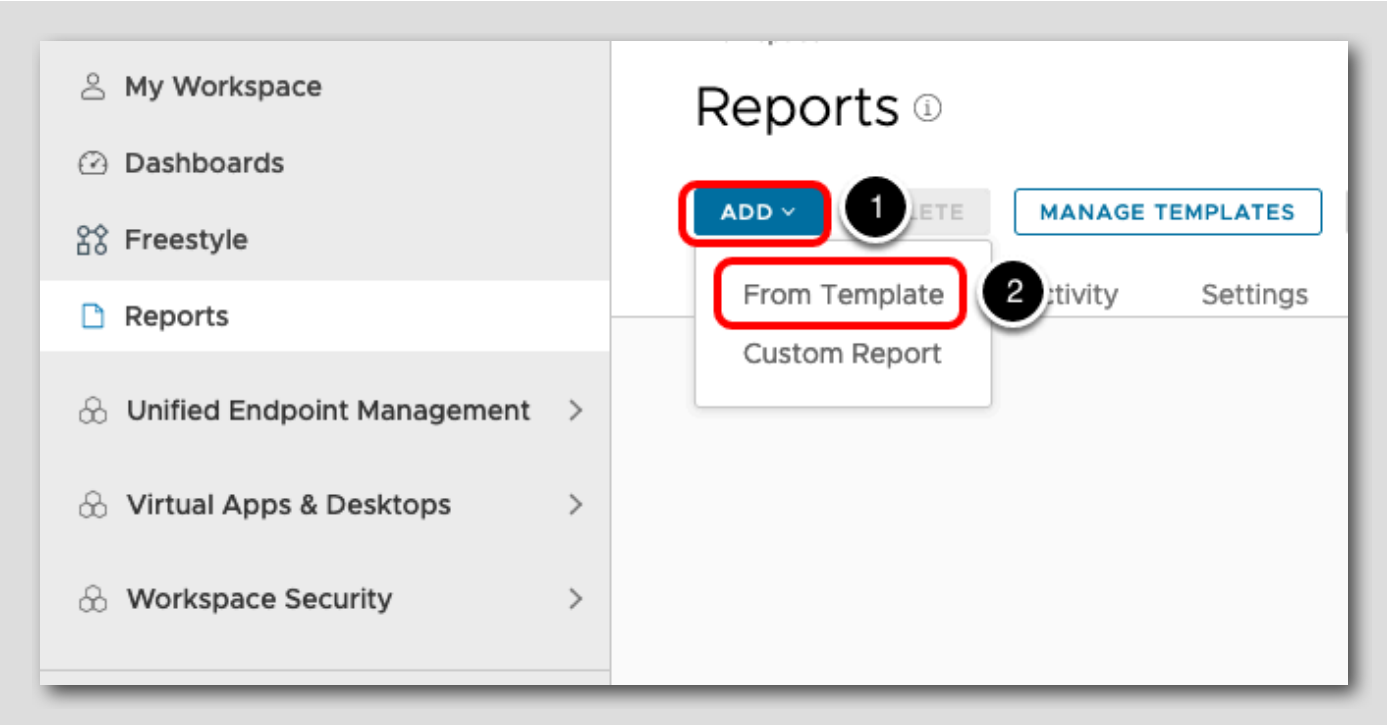


In the Workspace ONE Intelligence Console:

1. Click **Reports**.
2. A Get Started page is displayed if this is the first time accessing the Reports section. If displayed, click **Get Started**.

Add a Report

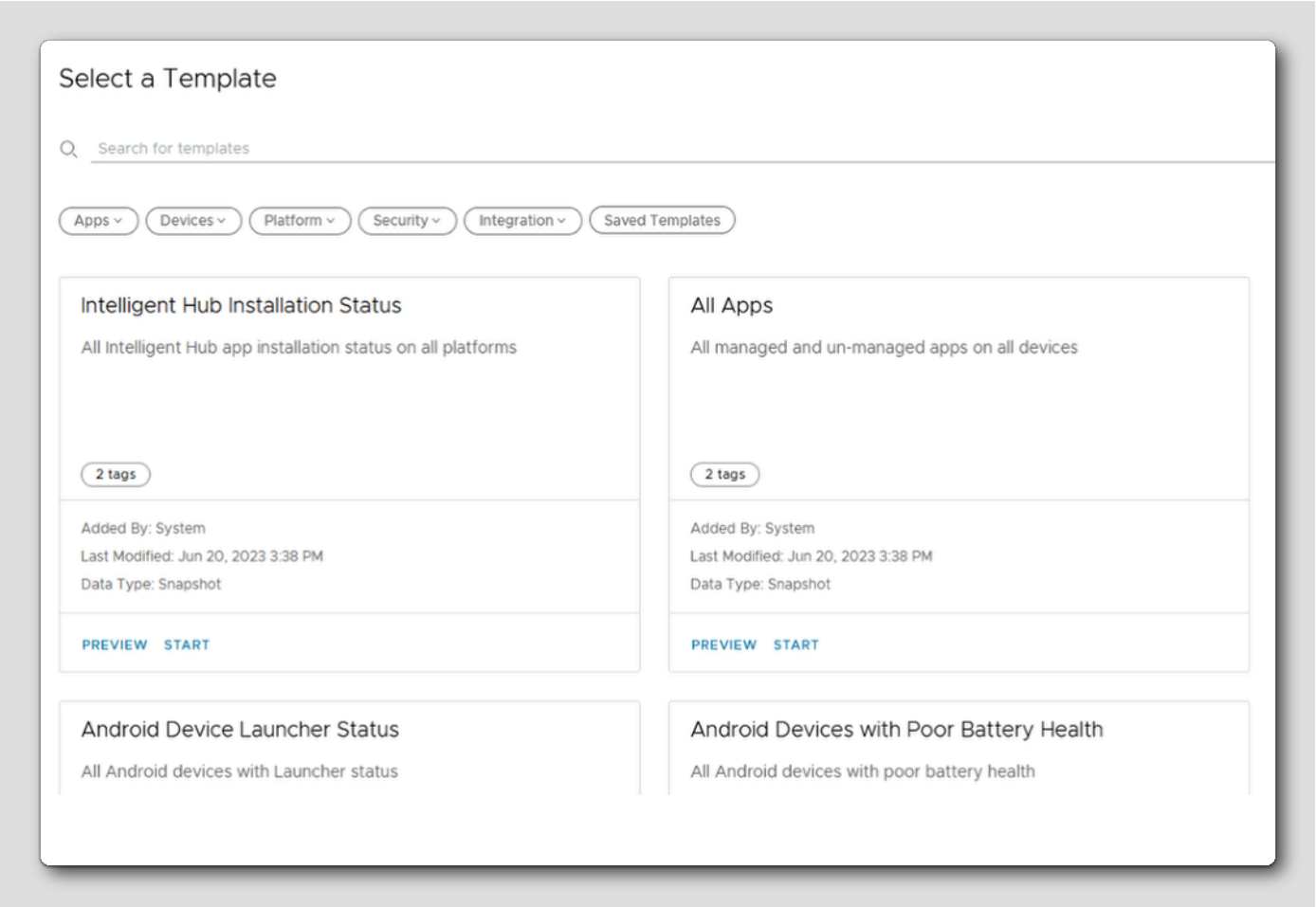
[532]



1. Click **Add**.
2. Click **From Template**.

Explore Report Categories and Templates

[533]



To begin creating a report, select the category of data you want to obtain. The available categories include:

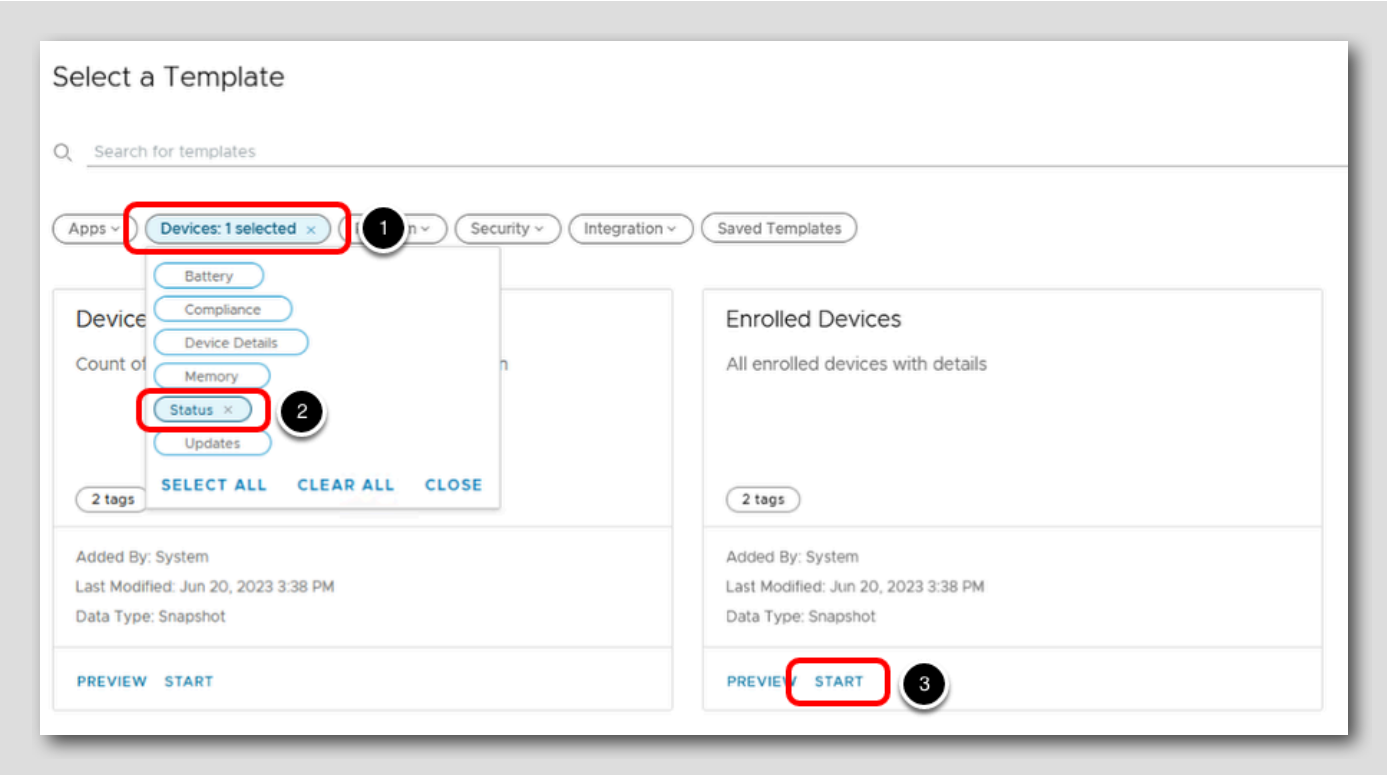
- Apps
- Devices
- Platform
- Security
- Integration

Then, use the tags on each category to filter the category's customizable templates to define the content your report collects. For complete control of the report's content, use the Custom Report template to define your own criteria.

Feel free to click on each category to see the templates available to each.

Select Enrolled Devices Template

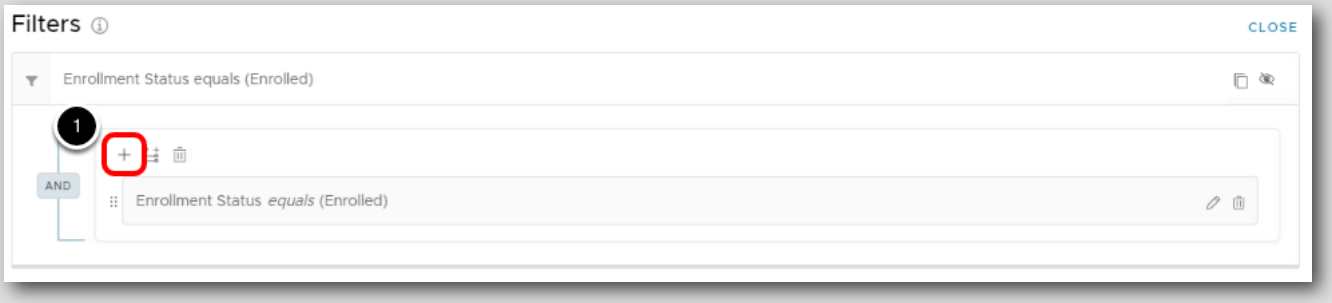
[534]

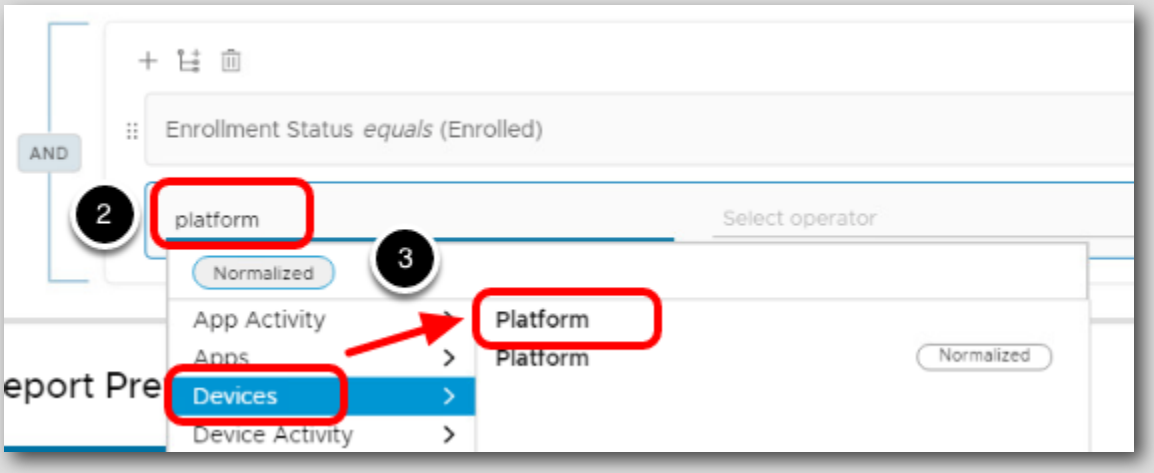


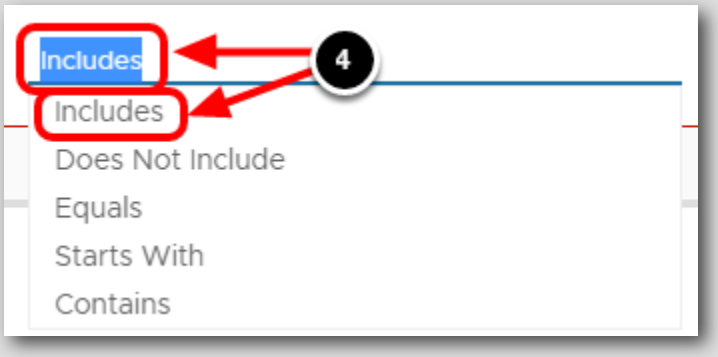
1. Select **Devices** category.
2. Select **Status** tag to filter the related templates.
3. Click **Start** for the Enrolled Devices template. Selecting this template creates a report about enrolled devices that displays data in pre-defined columns

Add Report Filters

[535]







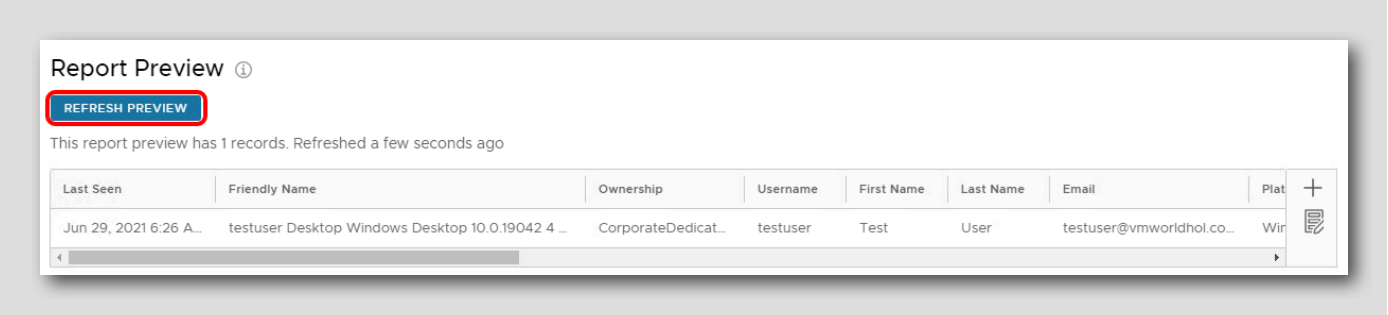
1. Under Filters, click the **+** icon to add a new filter.
2. Enter **`platform`** in the first search field.
3. Select **Platform** under Devices from the drop-down menu that appears.
4. Select **Includes** for the Select Operator field.
5. Select **Apple**, **Android**, and **WinRT** from the final drop-down menu.

   NOTE: If you do not see the above options in the drop-down menu, this means you do not have an enrolled device of that type in your organization. You can type each platform name manually and press **ENTER** after each to add them to the list.

NOTE: The platform list is based on devices available in your environment, so you may not see all three requested platforms on this activity.

Preview the Report

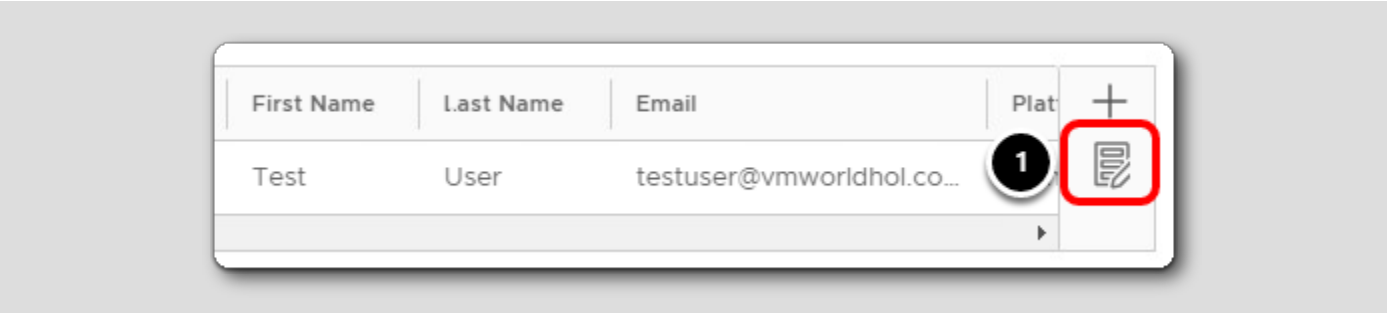
[536]

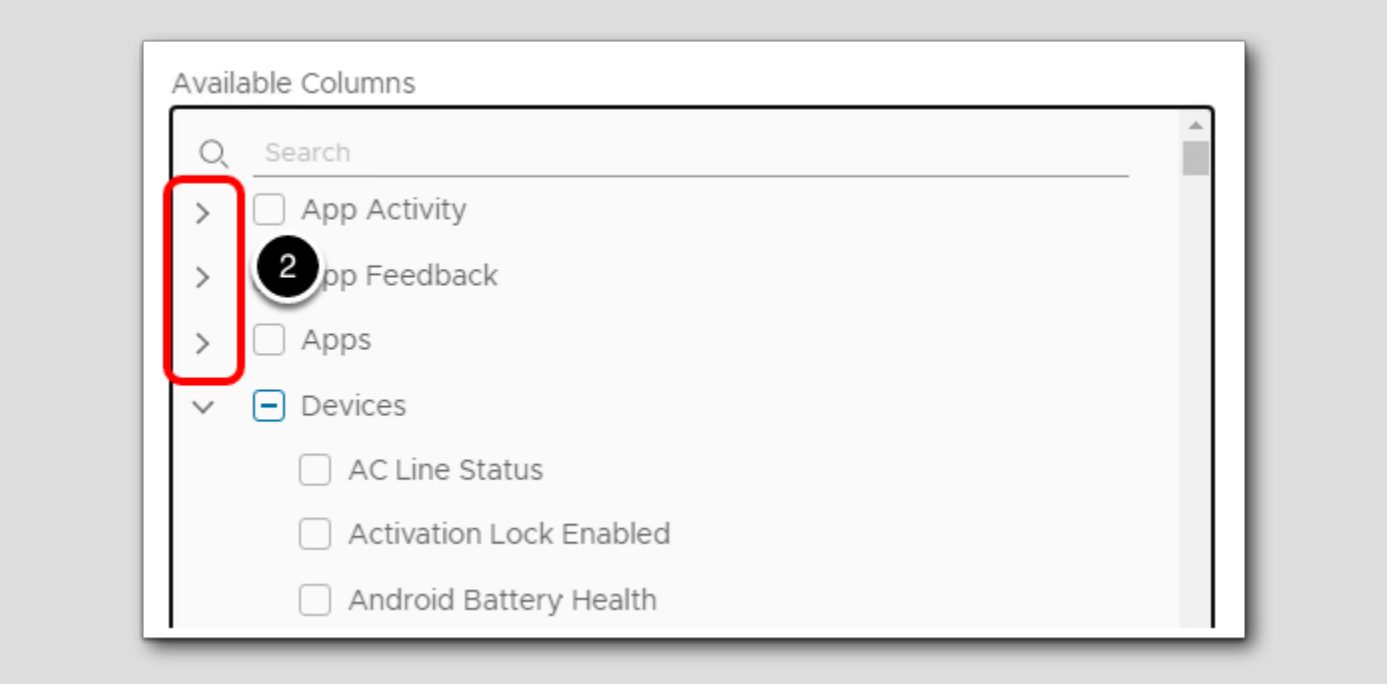


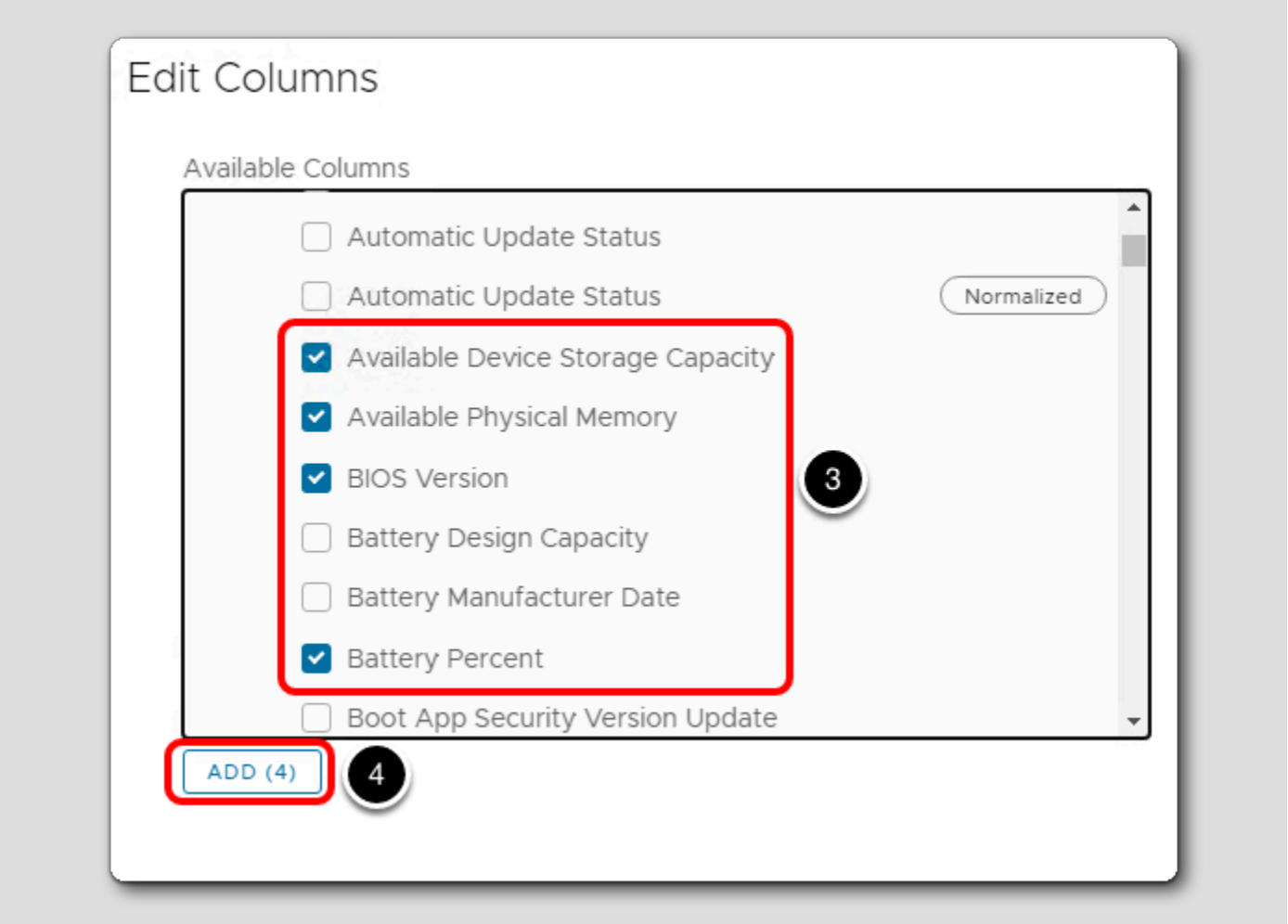
Scroll down to the Report Preview section and click **Refresh Preview**. Observe how your currently enrolled devices automatically populate in the preview.

Add Report Columns

[537]



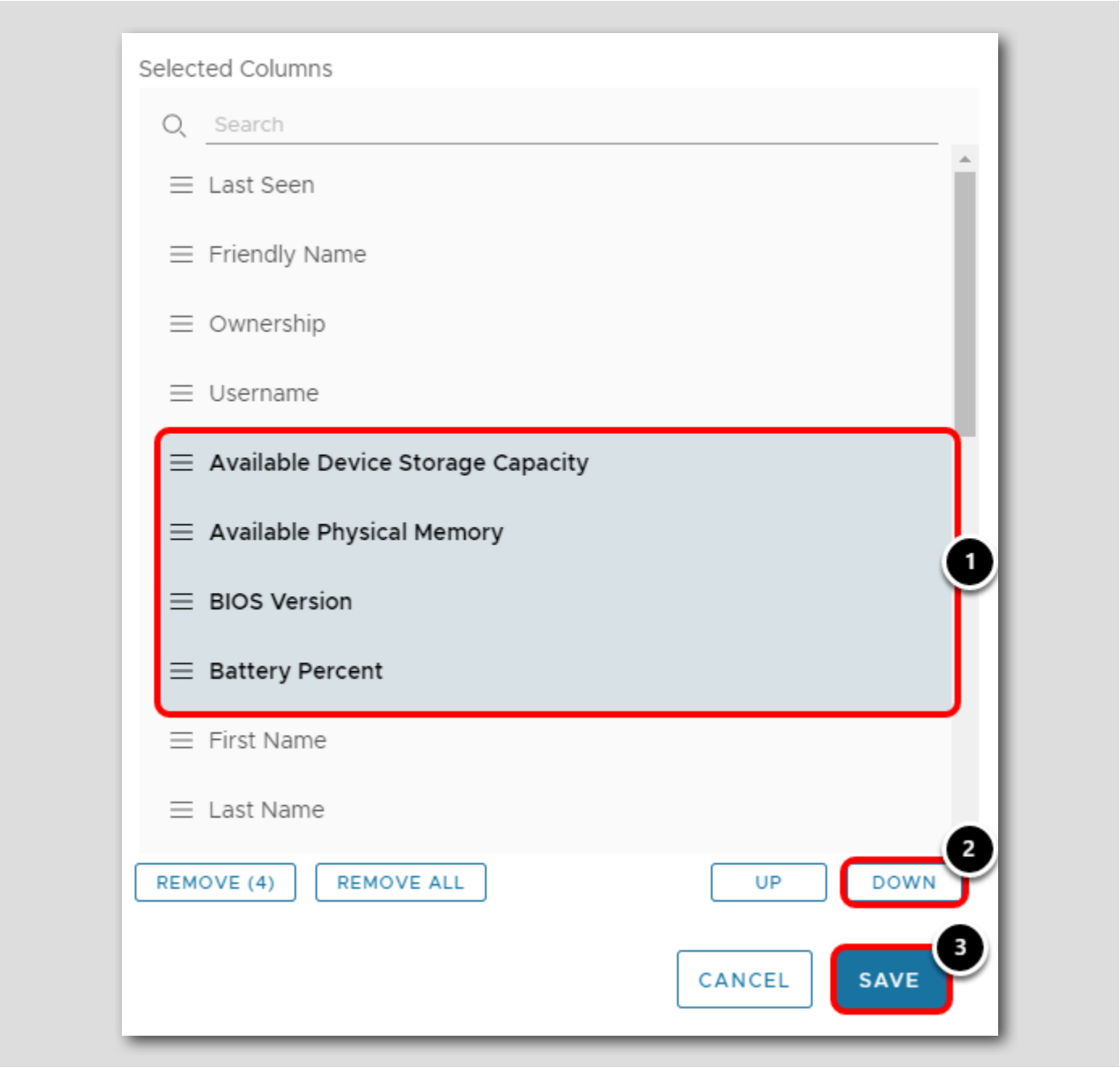




1. Under Report Preview, click the **Edit Columns** button.
2. Scroll down to find the Devices section. You can click the arrows next to **App Activity**, **App Feedback** and **Apps** to collapse these sections.
3. Under Available Columns, select the following:
    - **Available Device Storage Capacity**
    - **Available Physical Memory**
    - **BIOS Version**
    - **Battery Percent**
4. Click **Add**.

Change Column Order

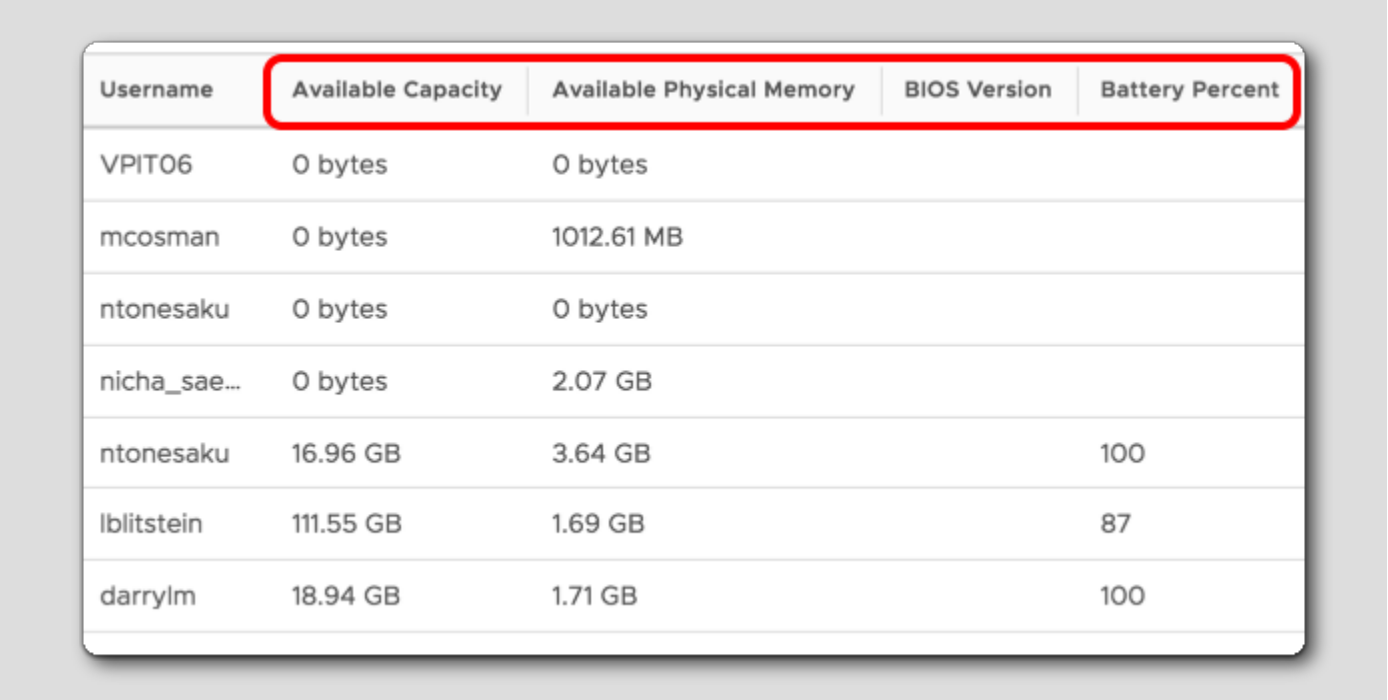
[538]



1. Under Selected Columns, select **Available Device Storage Capacity**, **Available Physical Memory**, **BIOS Version**, and **Battery Percent**. These newly added columns will be at the top of the list. You will need to **Shift + Click** each column to select multiple columns at once.
2. Click **Down** four times to re-order the columns. You can also drag and drop the selected items to move the values up and down.
3. Click **Save**.

Review New Columns

[539]



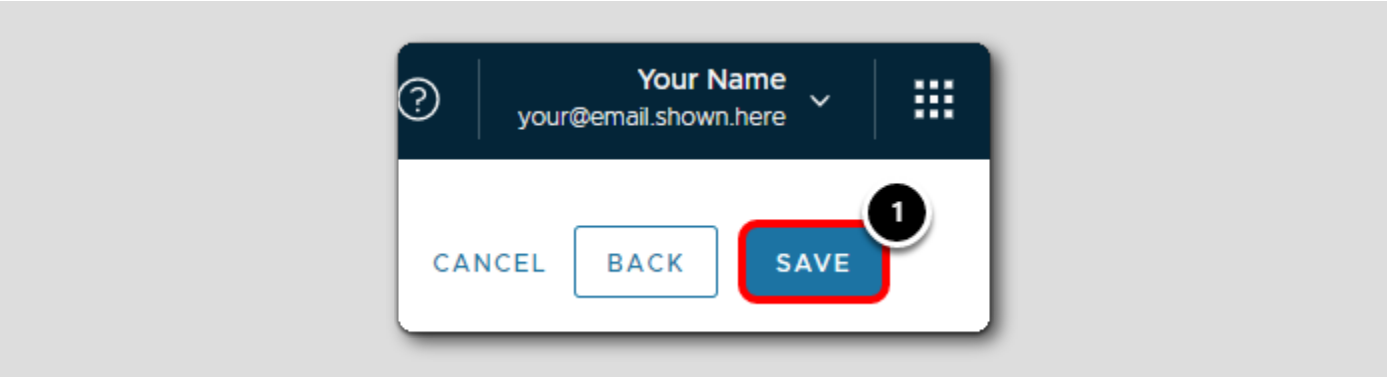
In the Report Preview, verify the new columns appear in the report.

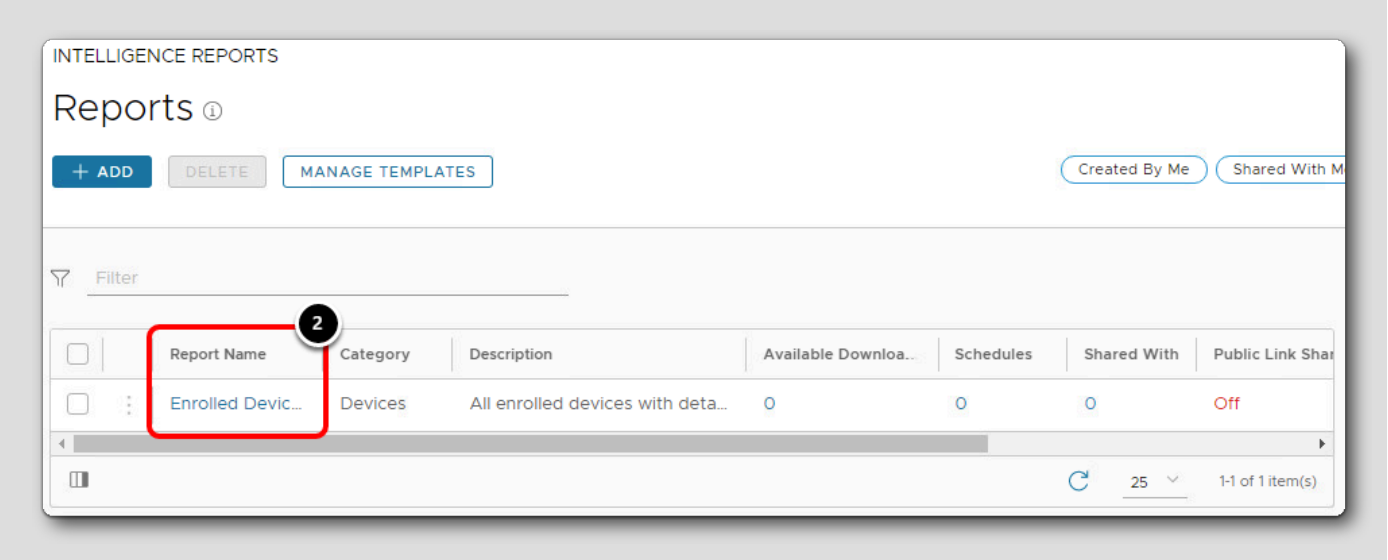
NOTE: If column data is empty, it is either because the device samples have not been retrieved yet or the column does not apply to the given device (i.e.: Battery Percent on a Desktop device).

NOTE: The above screenshot is from a demo environment with multiple devices to show an example. Your environment will look different.

Save the Report

[540]

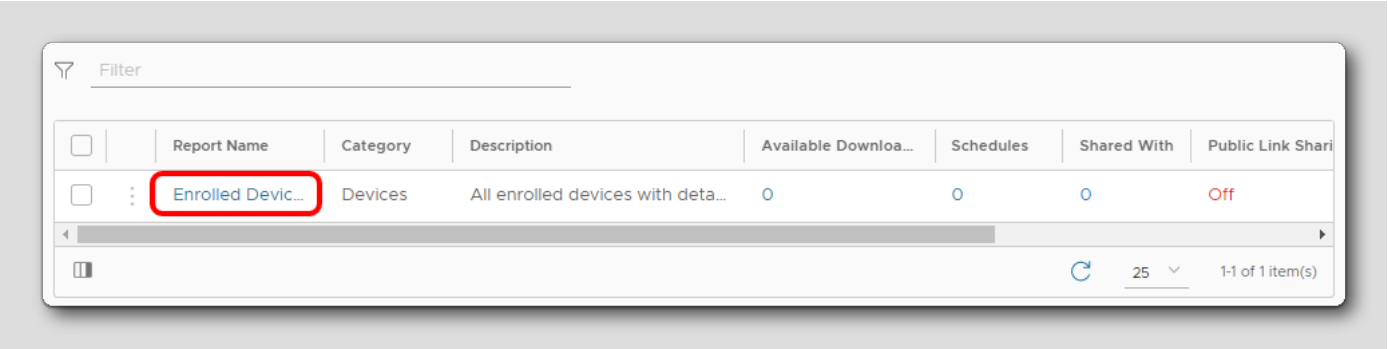




1. Click **Save** in the top right corner to save the report.
2. Confirm that the Enrolled Devices report saved successfully.

Manage the Report

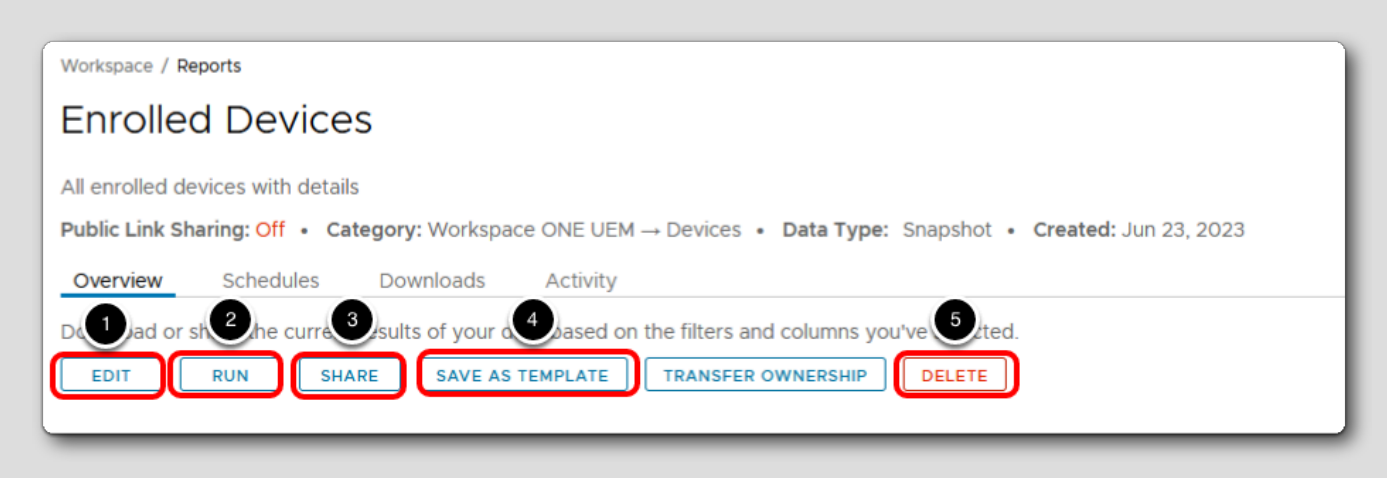
[541]



After the report saves, it is added to the list of available reports. Click the **Report Name (Enrolled Devices)** to manage the report.

Explore Report Overview

[542]



From this view, you can configure additional management settings:

NOTE: Do not click the following buttons, these details are informational only.

1. **Edit** allows you to alter the settings you configured when you made the report.
2. **Run** allows you to manually trigger a data sync.
3. **Share** allows you to email the report.
4. **Save As Template** allows you to create a template from this report.
5. **Delete** allows you to remove the report.

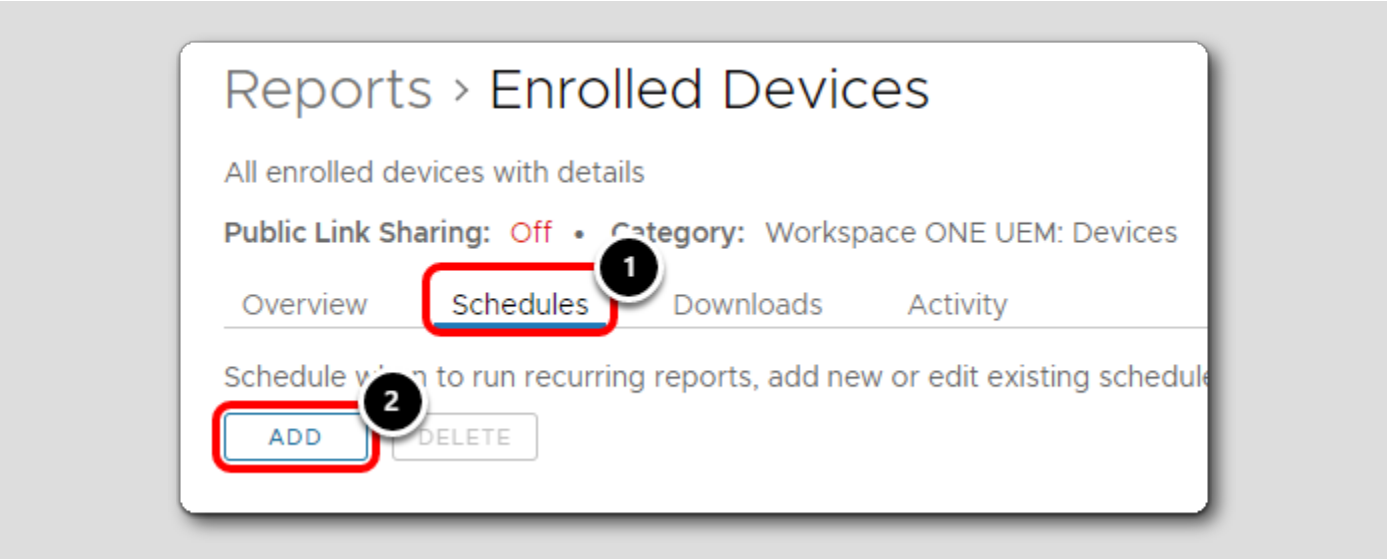
Scheduling Reports

[543]

After saving a report, you can use scheduling to automate data collection and collaboration. In this activity, you will schedule the *Enrolled Devices* report to run on a monthly basis.

Add a Report Schedule

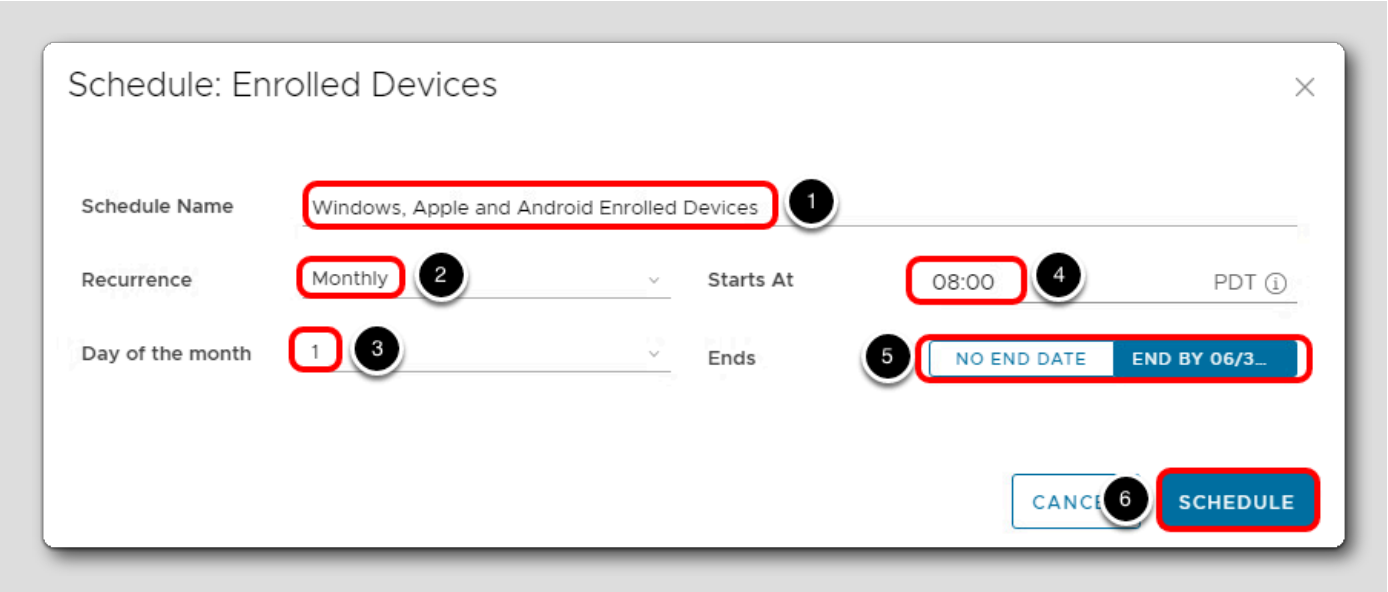
[544]



1. Click **Schedules**.
2. Click **Add**.

Configure the Report Schedule

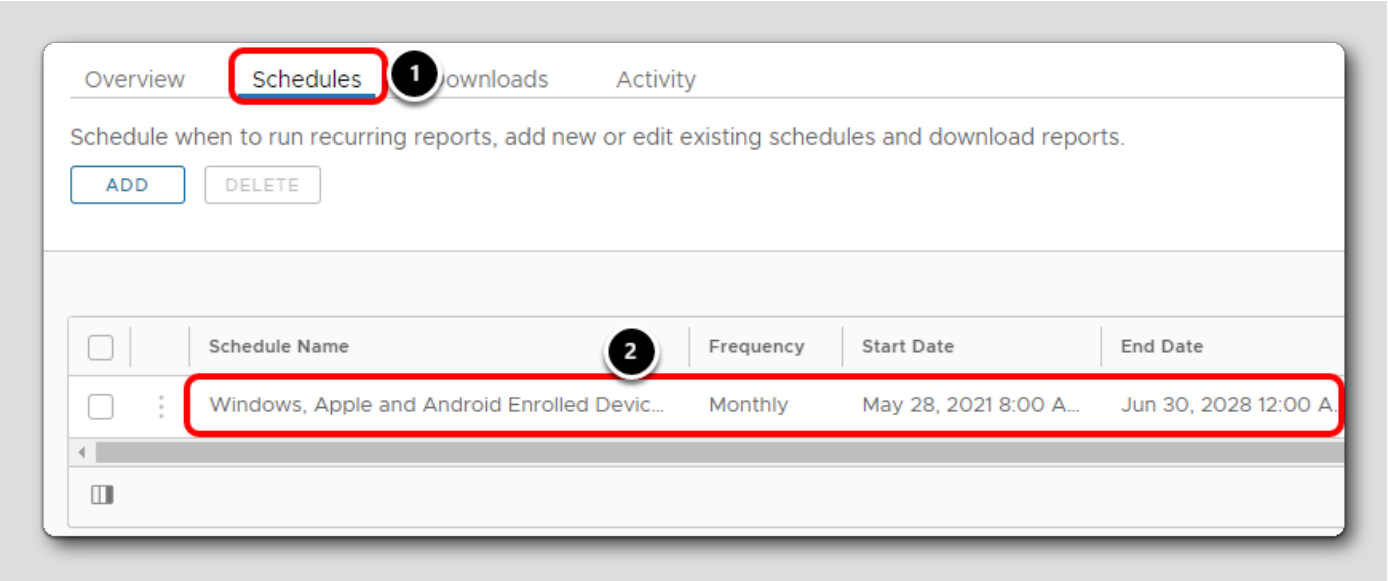
[545]



1. Enter a Schedule Name. For example, **`Windows, Apple and Android Enrolled Devices`**.
2. For Recurrence, select **Monthly**.
3. For Day of the Month, select **1**.
4. For Starts At, change the time to **08:00**.
5. For Ends, select a future date such as **06/30/2028**. You can click the dropdown arrow by the Year on the popout to change between the currently selected year.
6. Click **Schedule**.

Confirm Report Schedule

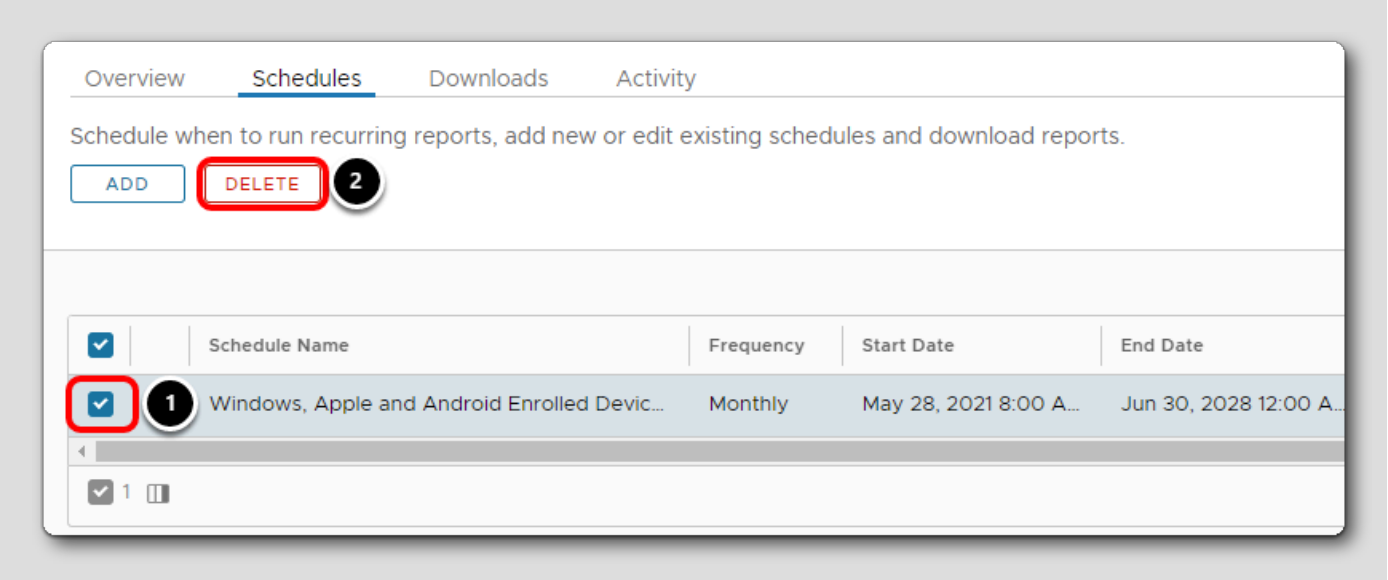
[546]

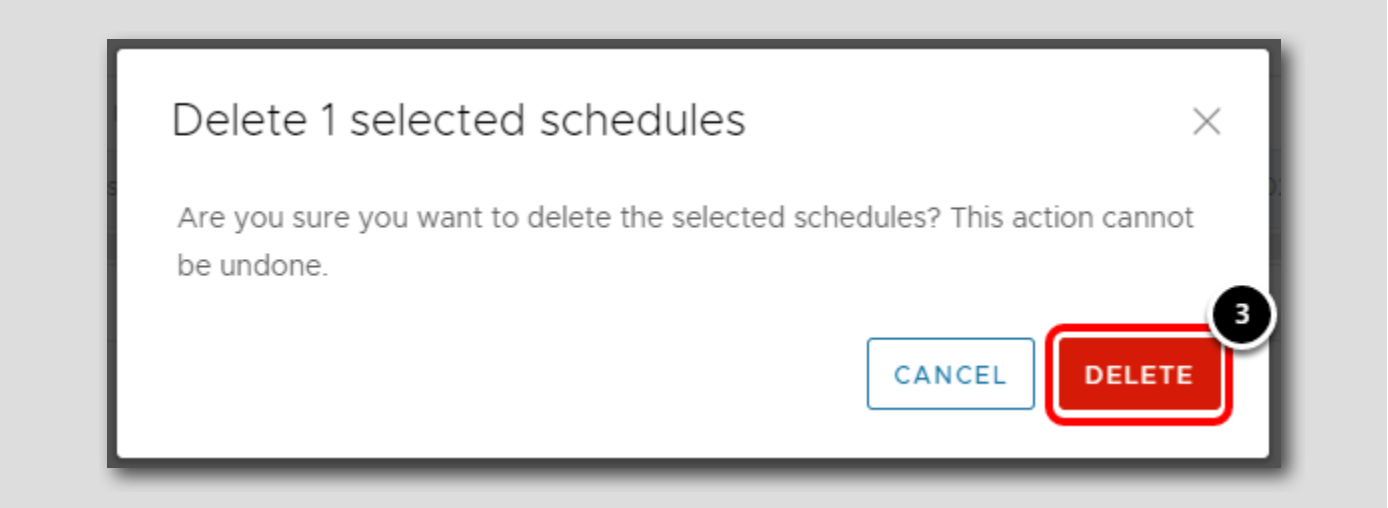


1. Click **Schedules**.
2. Confirm that the schedule matches the parameters you defined.

Delete Report Schedule

[547]





To delete a schedule report:

1. Select the report to be deleted. In this case, select the **Windows, Apple and Android Enrolled Devices** report you just created.
2. Click **Delete**.
3. Click **Delete** on the popup to confirm the action.

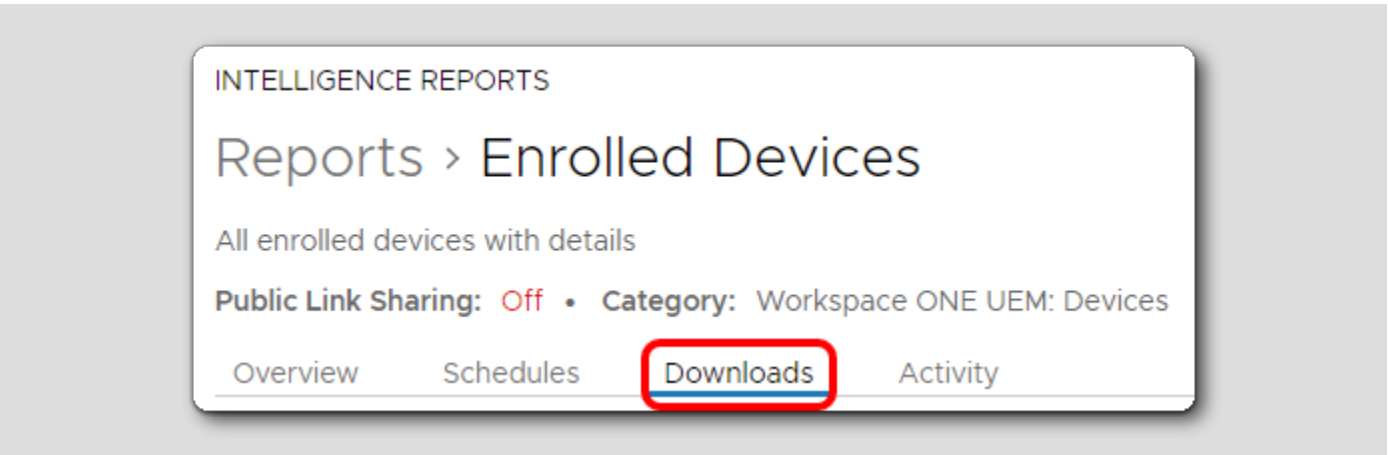
Downloading Reports

[548]

After saving a report, you can almost immediately download it as a CSV file. In this activity, you will download the CSV file for the *Enrolled Devices* report that you created.

Access Report Downloads

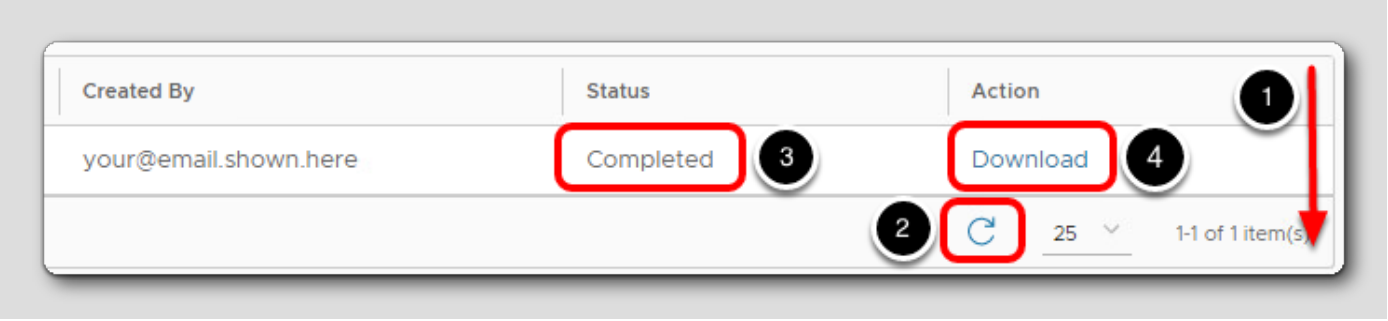
[549]

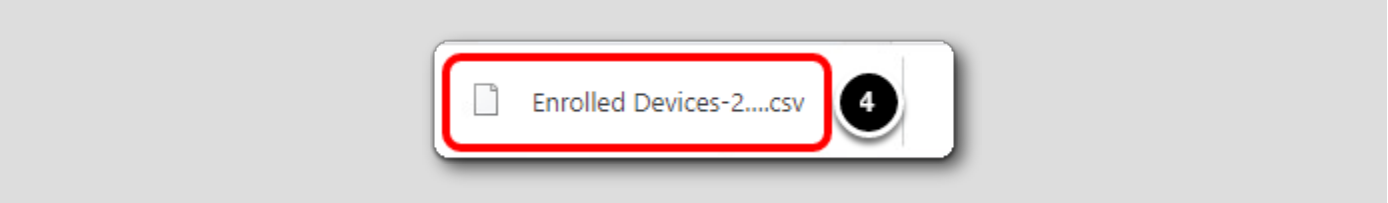


To access the report's available downloads, select the **Downloads** tab.

Download the Report

[550]



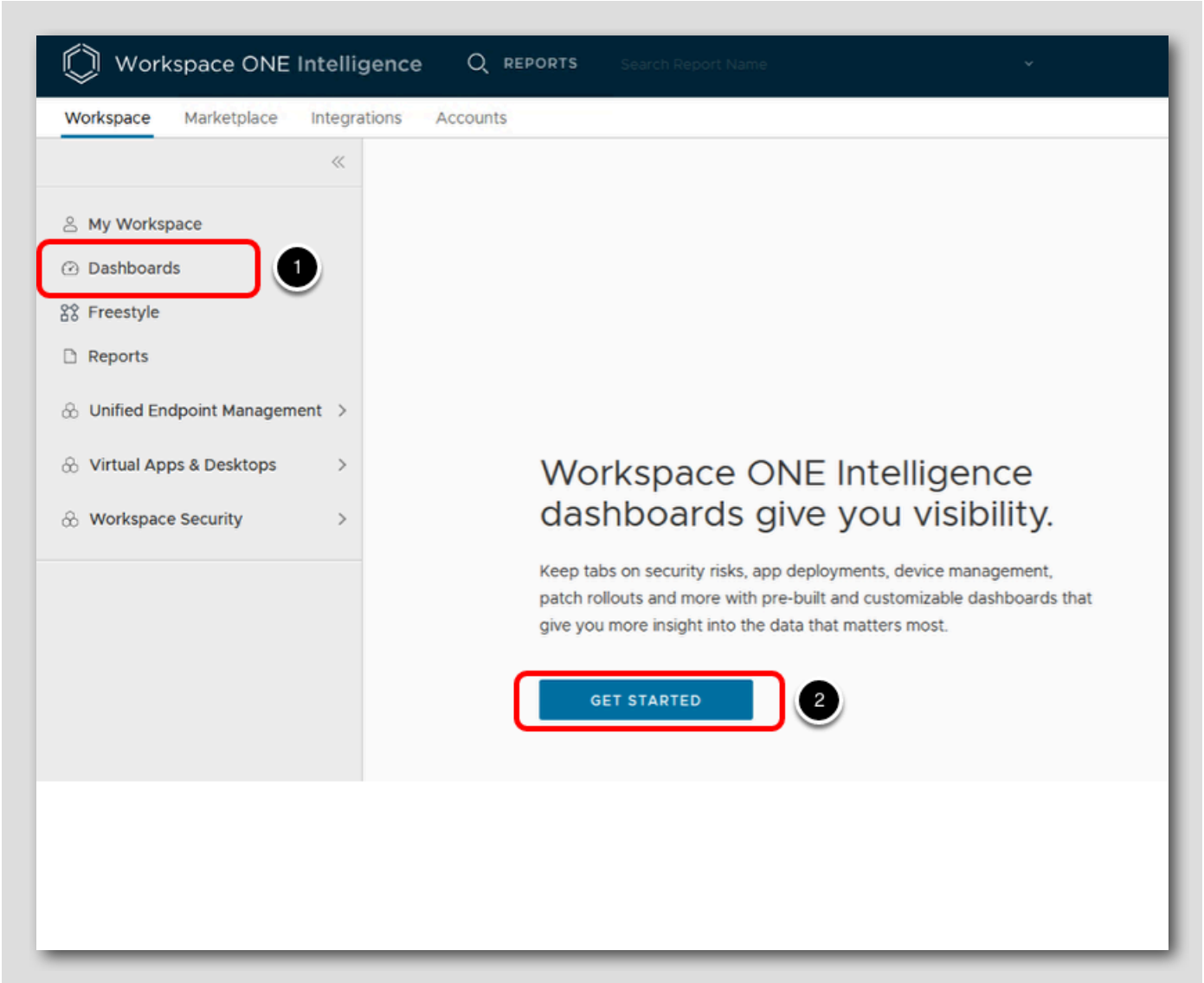


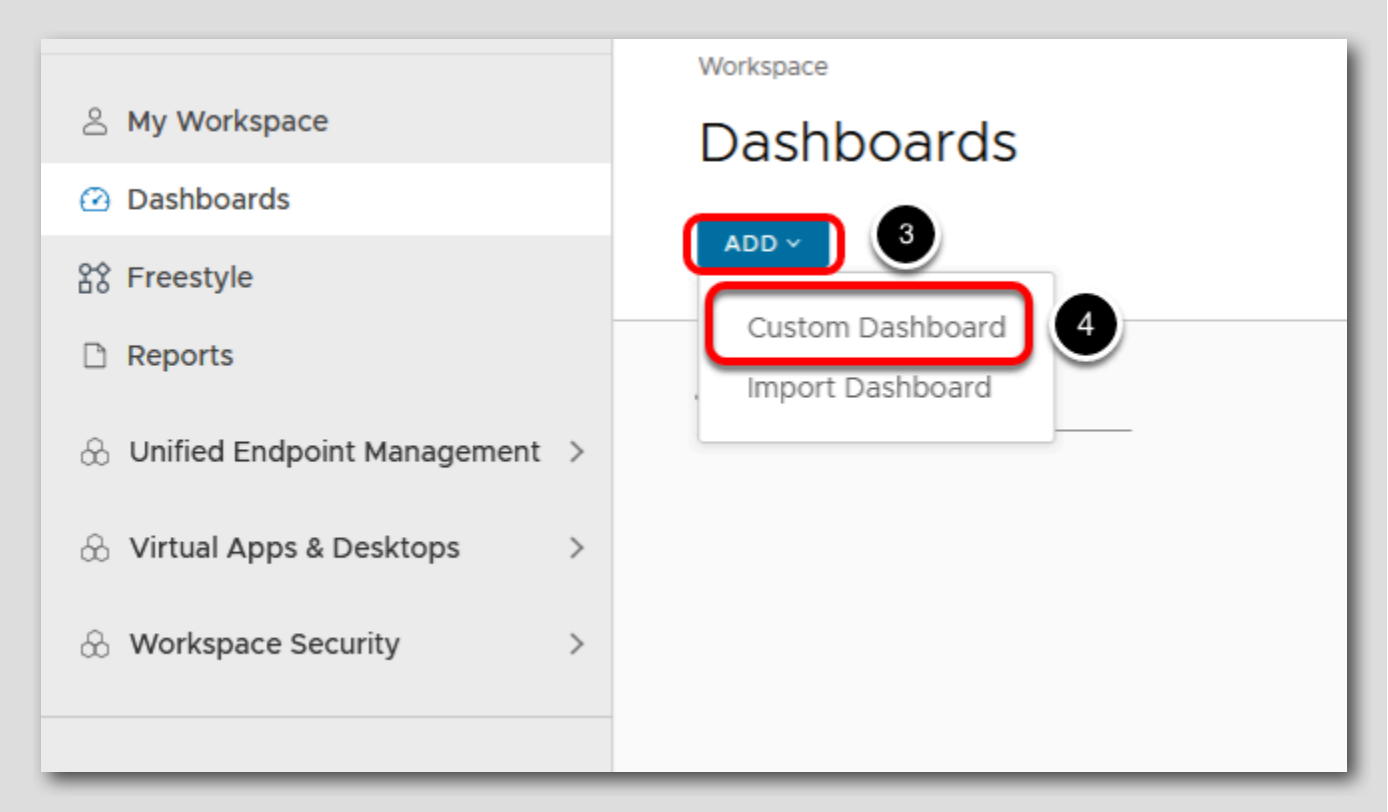
On the Downloads tab:

1. Scroll down to the reports list.
2. Click the **Refresh** icon if no reports are displayed to refresh the list.
3. Verify the status displays as **Completed**.
4. Click **Download**.
5. Validate that a CSV of the *Enrolled Devices* report downloads.

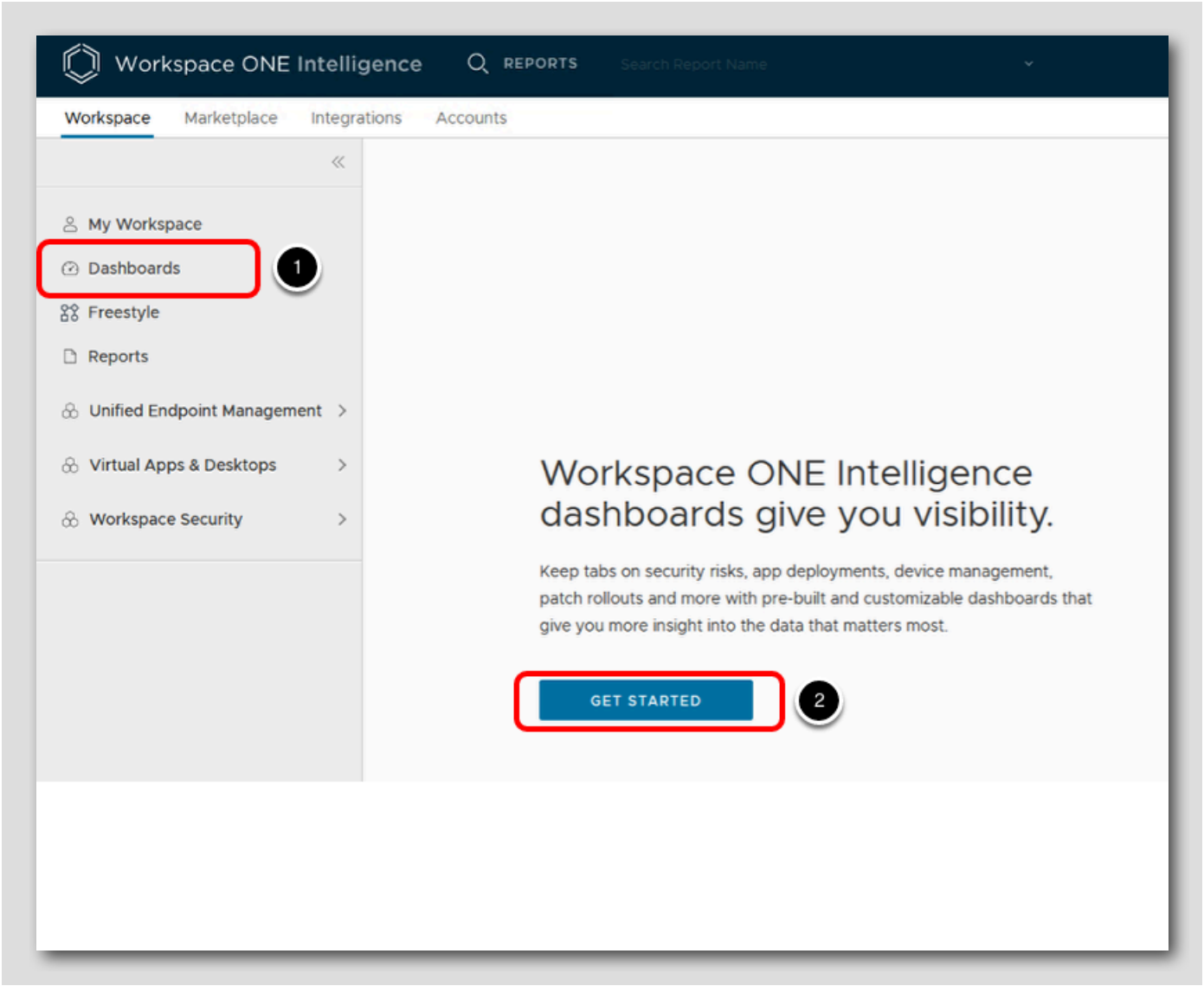
Customizing the Dashboard View

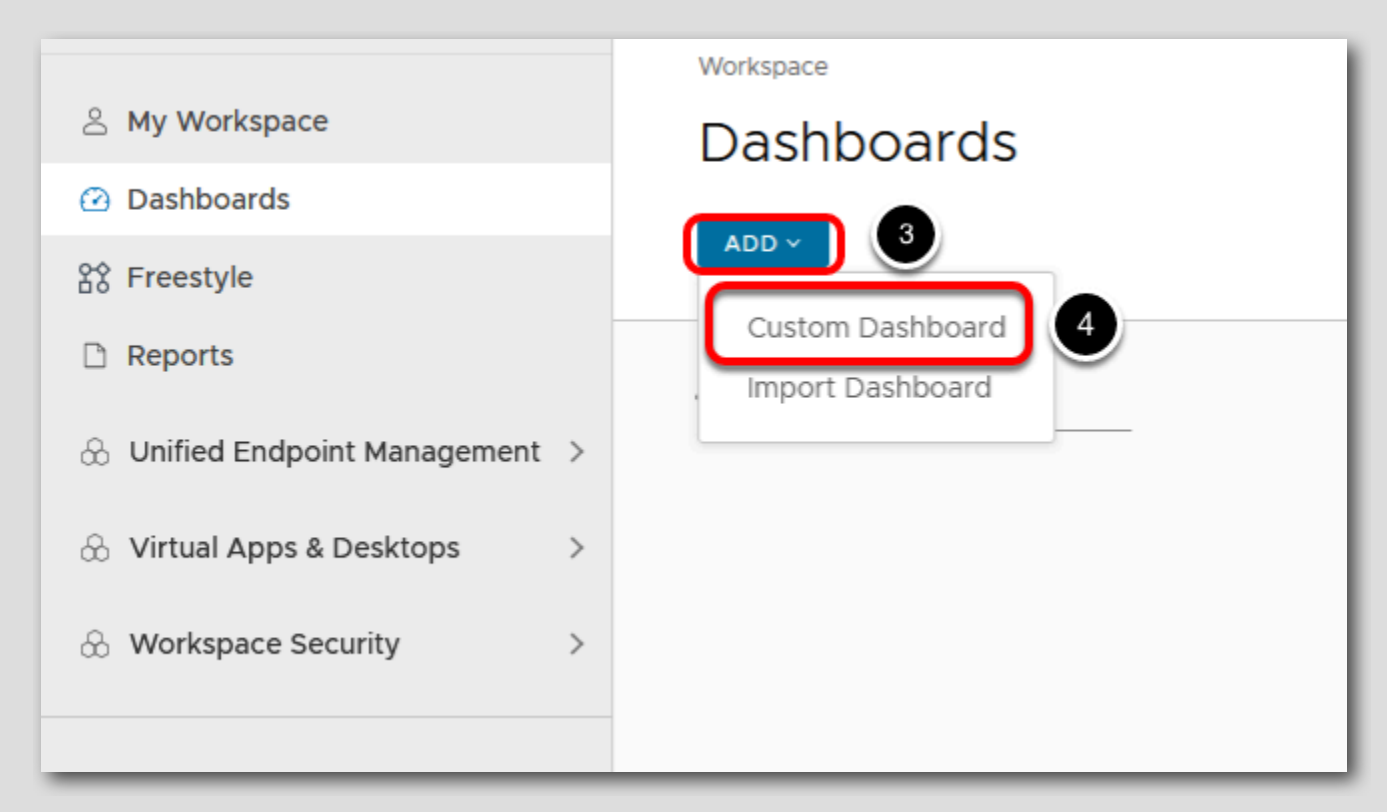
[551]



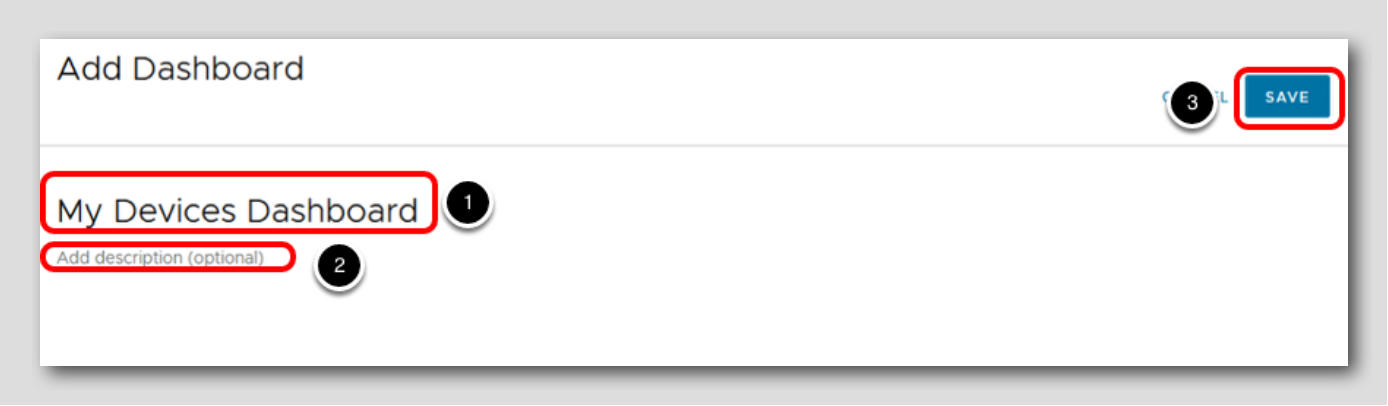


1. Click the **Dashboards** tab.
2. A Getting Started page is shown the first time you access the Dashboards page. If displayed, click **Get Started**.
3. Click **Add** to create a new Dashboard.
4. Click **Custom Dashboard**.


Workspace ONE Intelligence
REPORTS
Search Report Name
Workspace
Marketplace
Integrations
Accounts
My Workspace
Dashboards
1
Freestyle
Reports
Unified Endpoint Management
Virtual Apps & Desktops
Workspace Security
Workspace ONE Intelligence dashboards give you visibility.
Keep tabs on security risks, app deployments, device management, patch rollouts and more with pre-built and customizable dashboards that give you more insight into the data that matters most.
GET STARTED
2



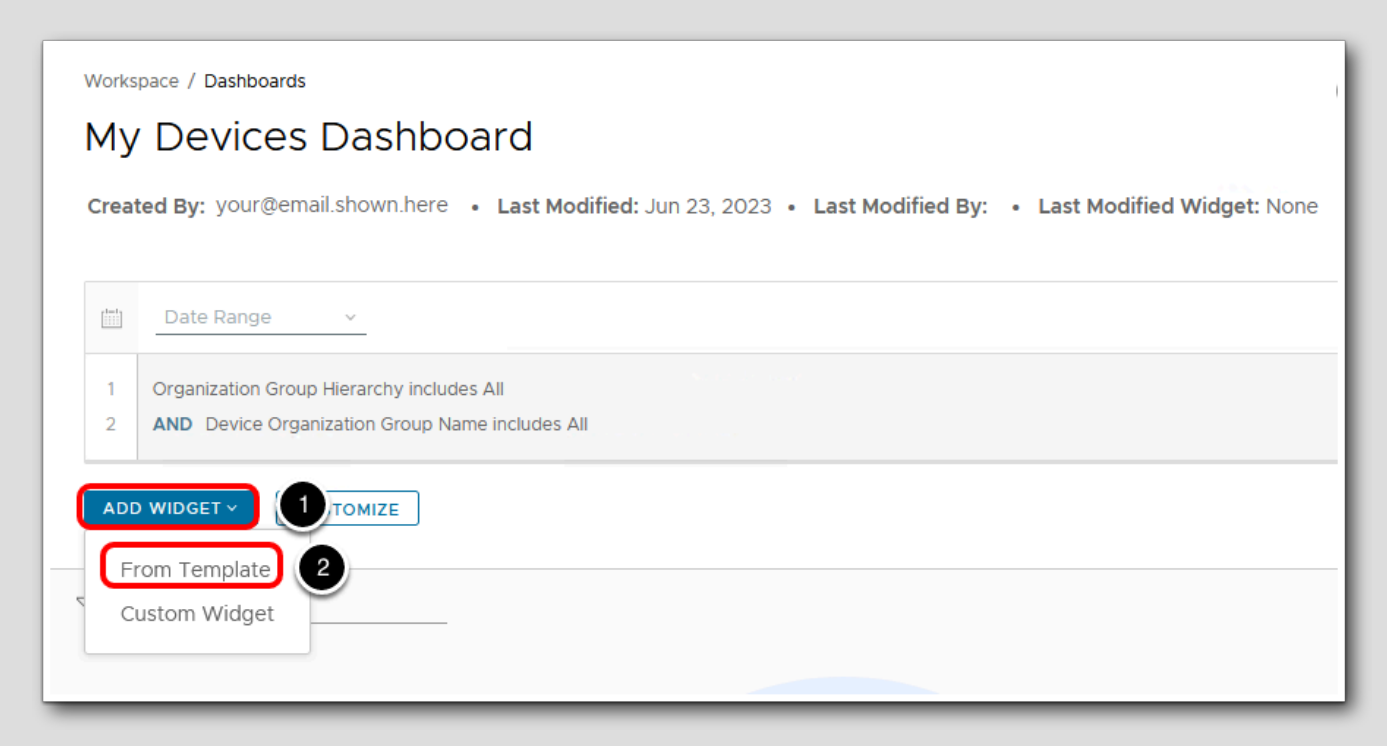
Add Dashboard [552]



1. Enter a dashboard name, such as **`My Devices Dashboard`**
2. Enter an optional description for the dashboard
3. Click **Save**

Add A Widget

[553]

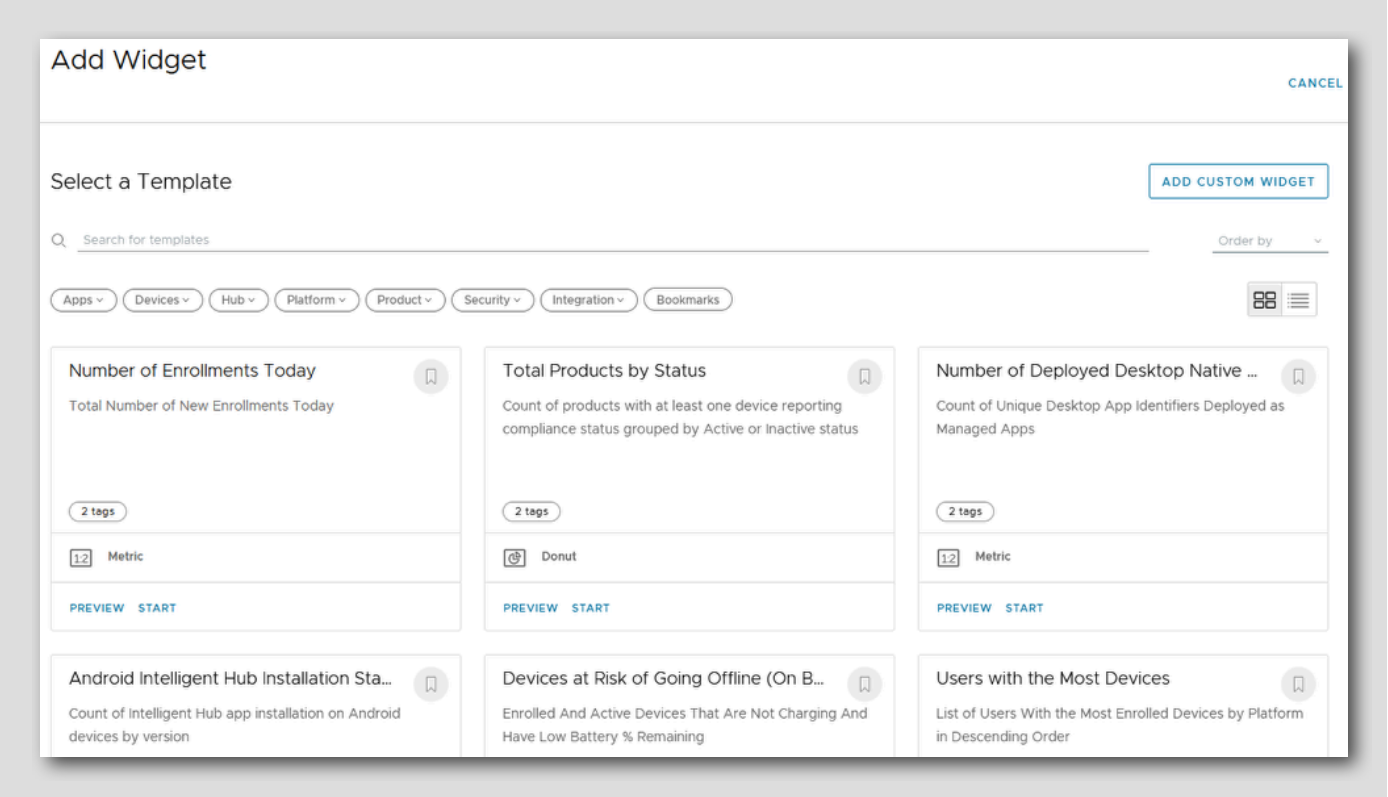


Newly created dashboards by default have no information on them. You can add widgets to them and create custom dashboards to meet your business needs.

1. Click **Add Widget**.
2. Click **From Template**.

Explore Widget Categories and Templates

[554]



To begin creating a widget, you can select Custom Widget or select one of built-in widgets by selecting the categories and tags. The list of categories will be based on the integrations configured within your Workspace ONE Intelligence tenant and may differ from the image you see in this activity.

The available categories can include:

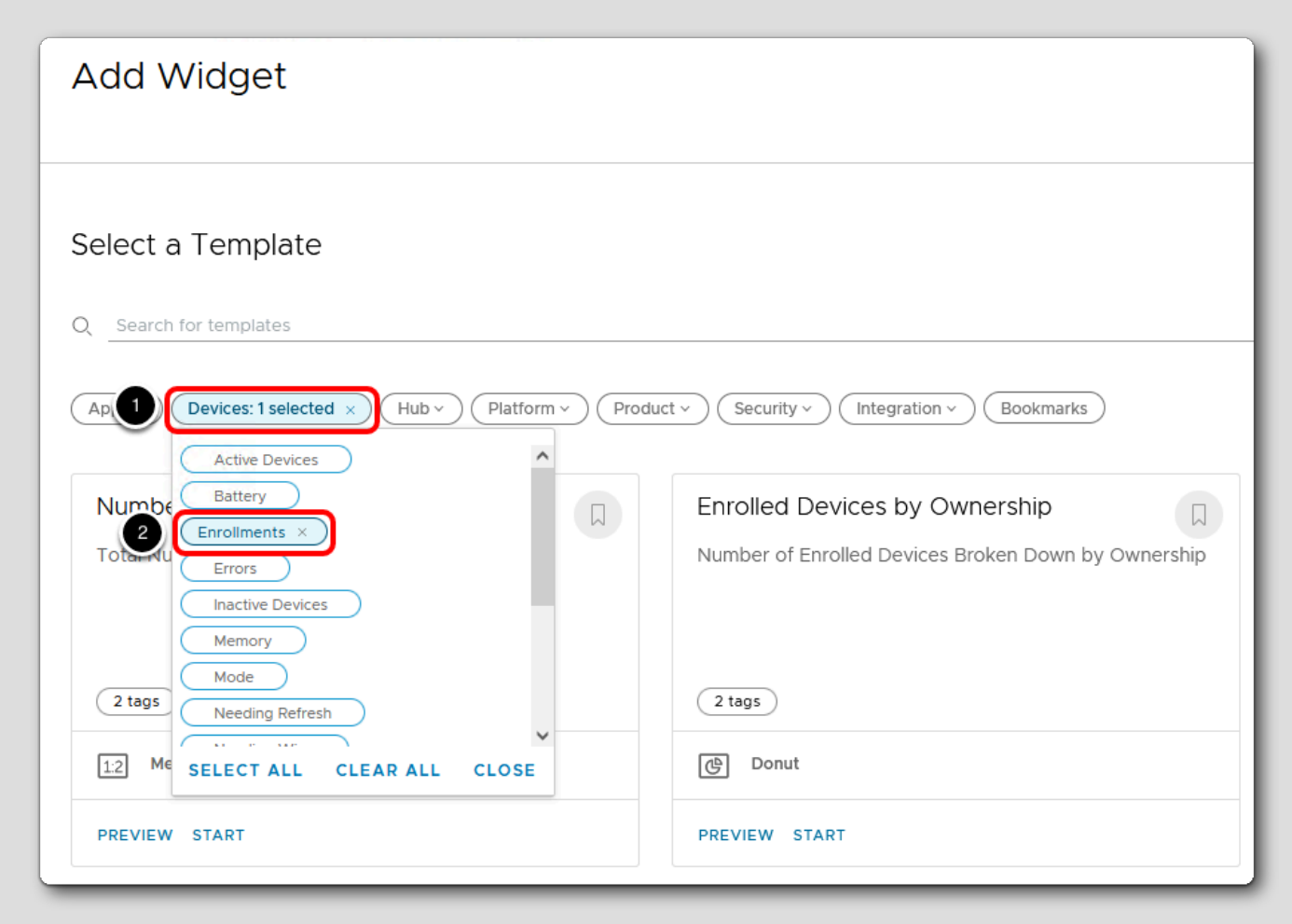
- Apps
- Devices
- Hub
- Platform
- Product
- Security
- Integration

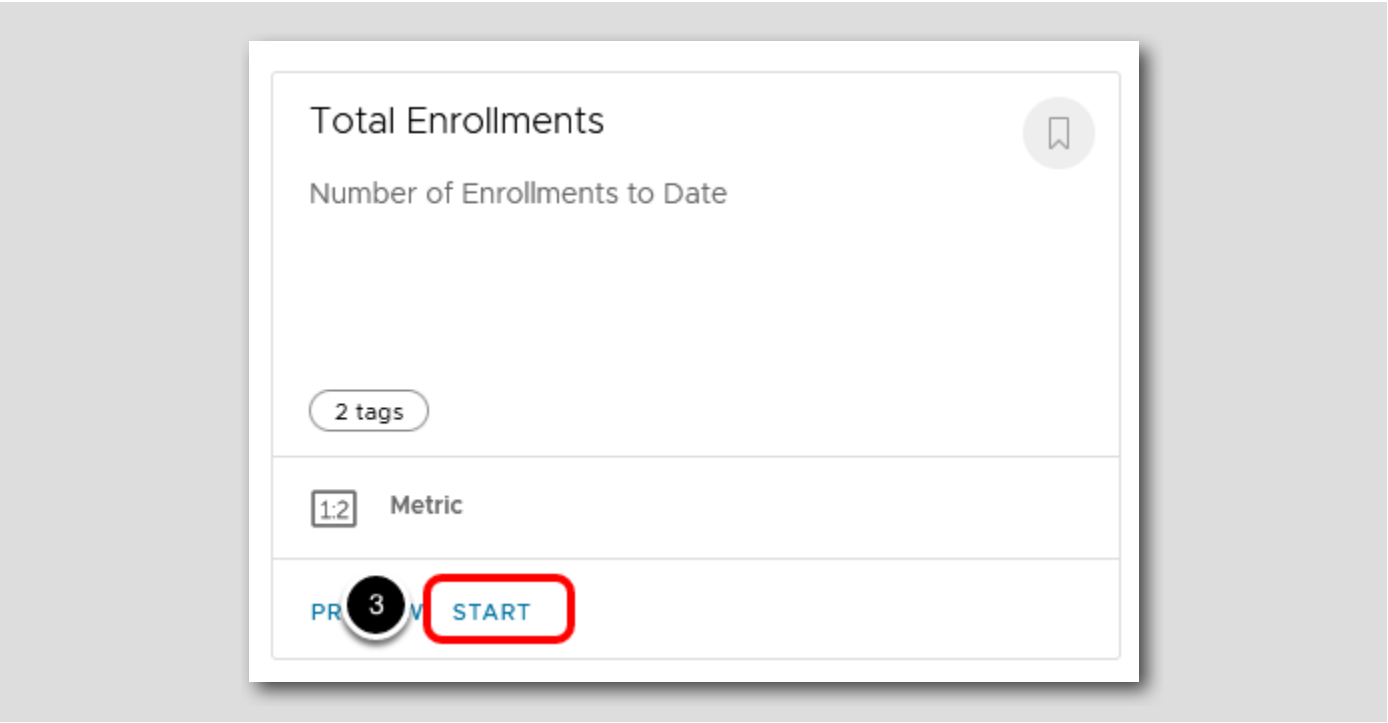
When you start with Workspace ONE Intelligence for the first time, you will see multiple categories.

Then, use the tag for each category to filter the customizable templates to define the content your widget displays. For complete control of the widget's content, use the Custom Widget template to define your own criteria.

Feel free to click on each category to see the templates available to each.

Select a Template [555]



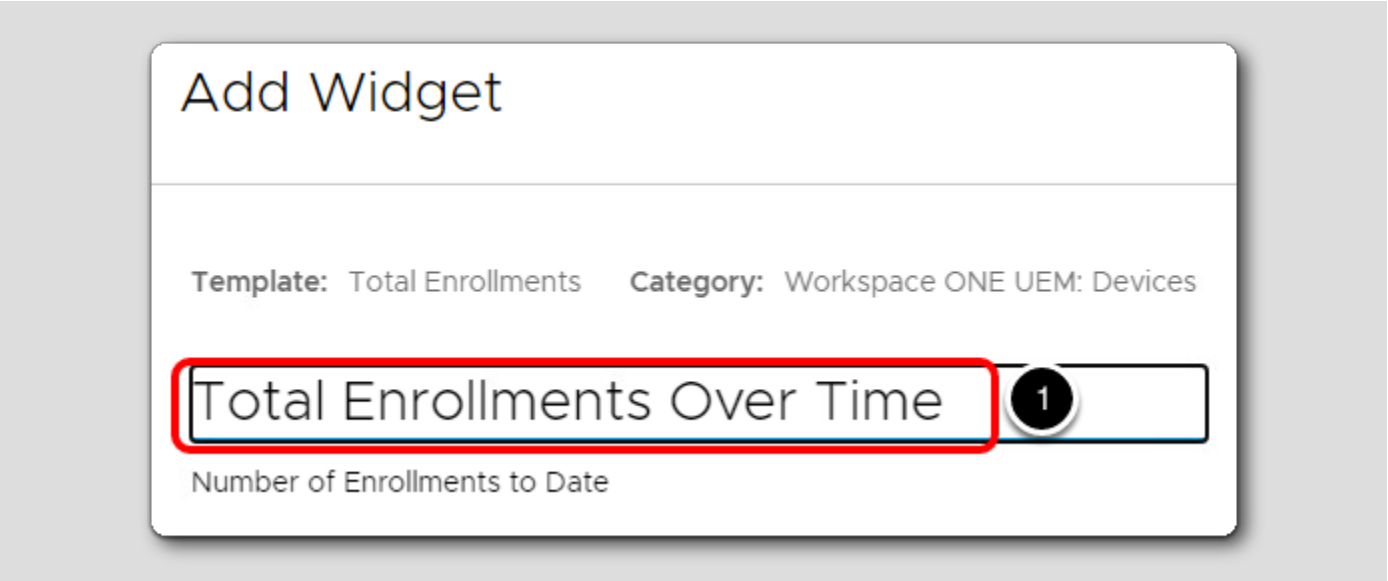


1. Select the **Devices Category**.

   NOTE: If the dropdown does not load when clicked, you may need to scroll down before clicking the Devices category or maximize the lab window. The list will not load if there is not enough UI space to draw the drop down on the smaller resolution.
2. Select the **Enrollments** tag.
3. Click **Start** for **Total Enrollments** template.

Name the Default Template

[556]

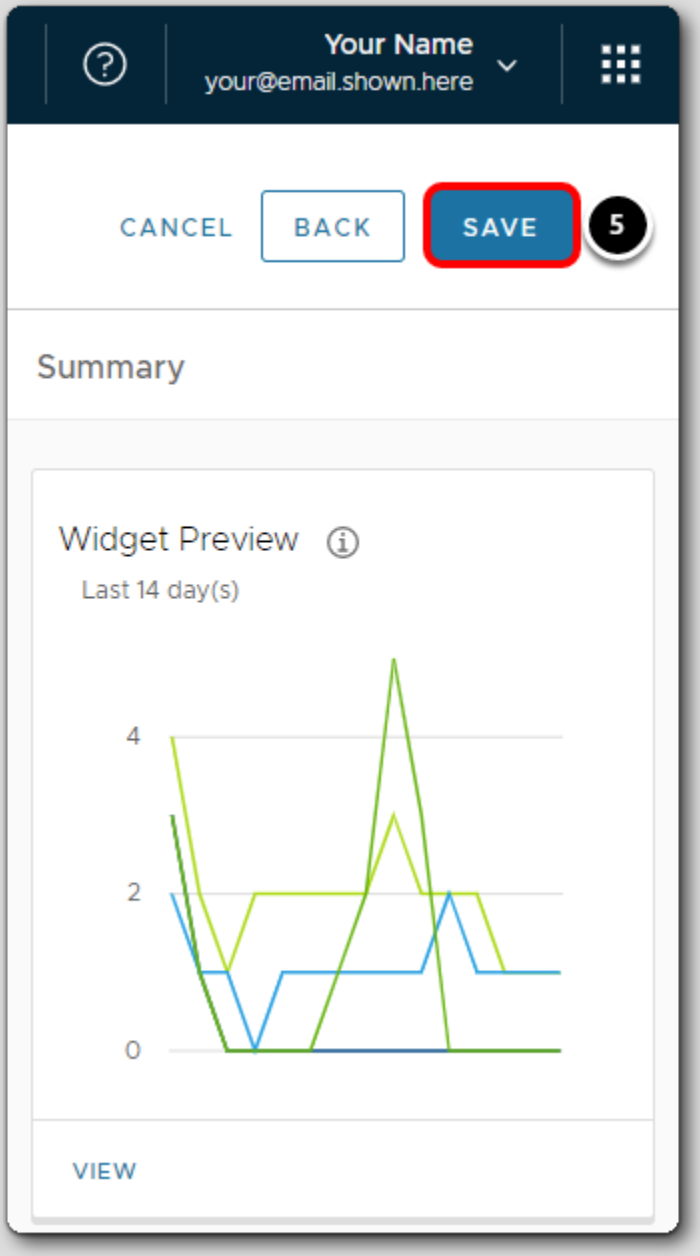


Under Data Visualization, review the default Total Enrollments template. The initial default settings provide a snapshot of current device enrollment. If you change the settings, the snapshot results change accordingly.

1. Change the name of the widget to **`Total Enrollments Over Time`**.

Configure the Template

[557]


Your Name
your@email.shown.here
CANCEL
BACK
SAVE
5
Summary
Widget Preview
Last 14 day(s)
4
2
0
VIEW

To create a snapshot of total enrollments over time, modify the default Total Enrollments template.

1. Select **Historical**.
2. For Chart Type, select **Line**.
3. For Group by, enter **`Platform`** and select the first result from the list.
4. Set the Date Range to **`Last 14 Days`**.
5. Click **Save** in the top right corner to save the widget.

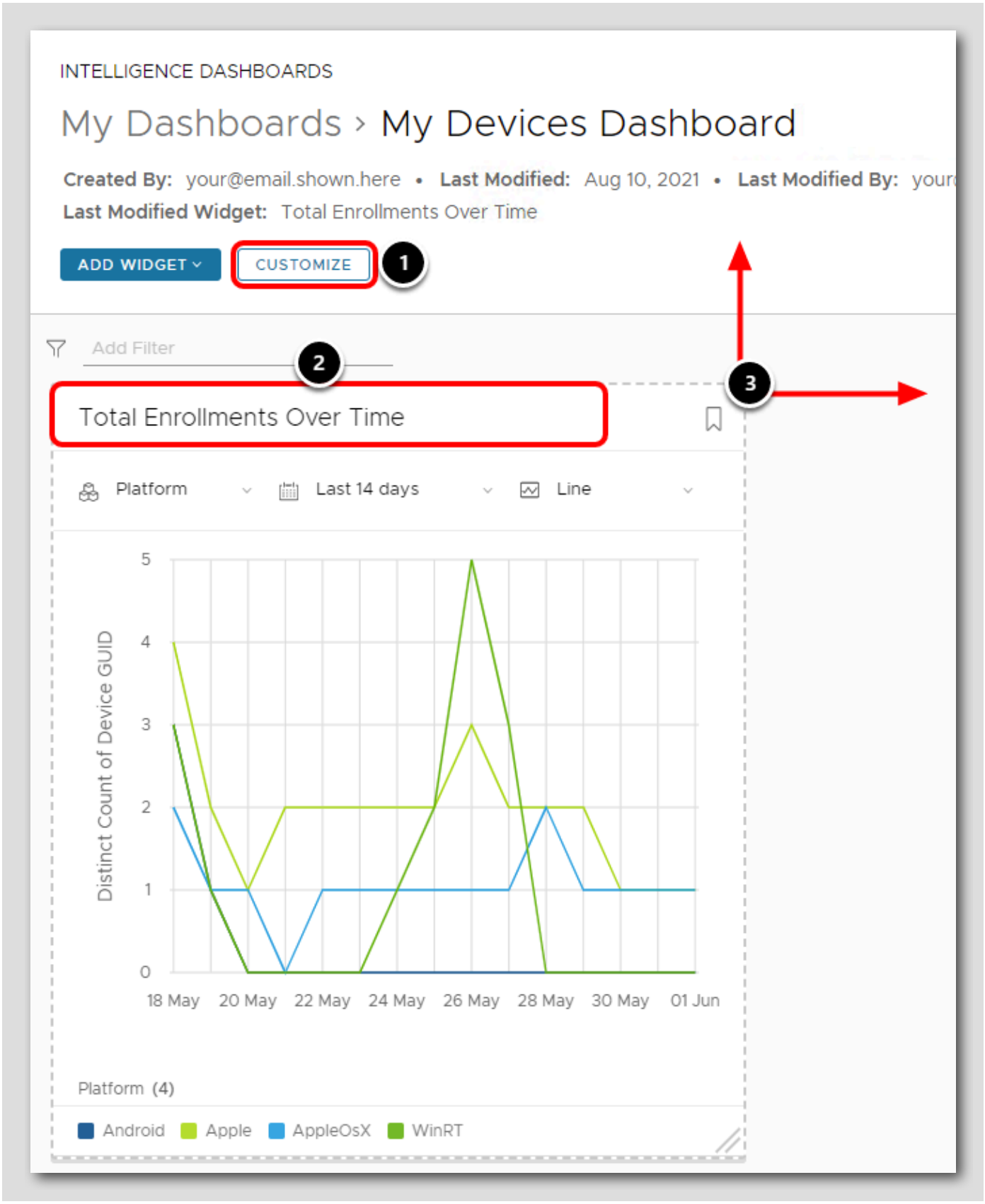
Note: The screenshot shown is from a test environment. Your preview is based on your environment, and will differ from the preview you see in the screenshot.

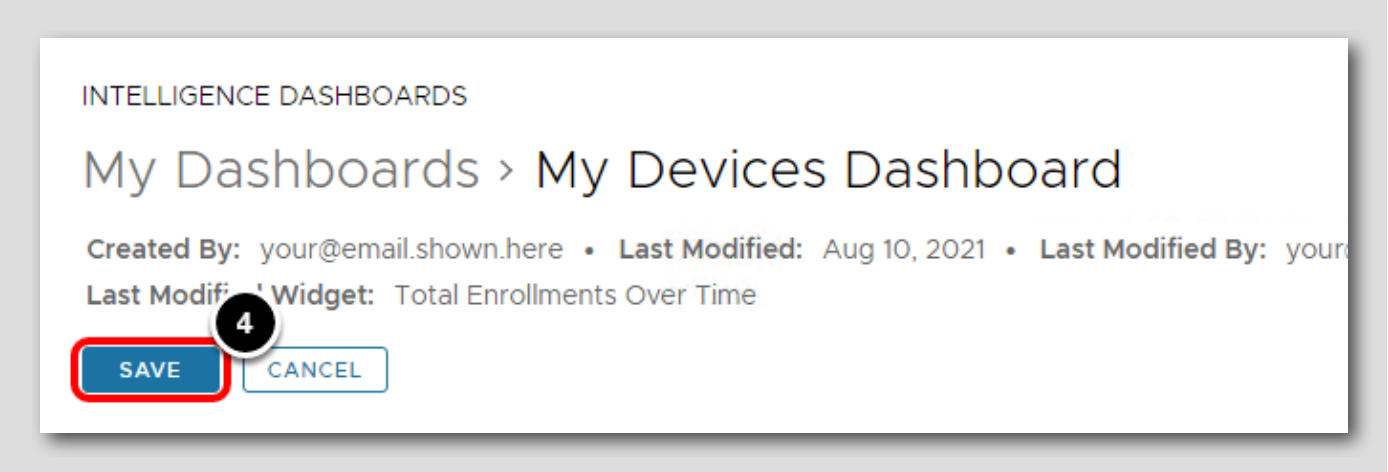
As a supplement to its reporting capabilities, the Workspace ONE Intelligence dashboard displays critical business data in an easy-to-consume visual summary. Within dashboards, the configurable widgets allow you to customize the data that displays.

After configuring the Total Enrollment Over Time widget, you can manage how it displays on your dashboard. In this activity, you will modify your dashboard view by repositioning and expanding the Total Enrollment Over Time widget.

Customize the Dashboard

[558]


INTELLIGENCE DASHBOARDS
My Dashboards › My Devices Dashboard
Created By: your@email.shown.here • Last Modified: Aug 10, 2021 • Last Modified By: your
Last Modified Widget: Total Enrollments Over Time
ADD WIDGET
CUSTOMIZE
1
Add Filter
2
3
Total Enrollments Over Time
Platform
Last 14 days
Line
Distinct Count of Device GUID
5
4
3
2
1
0
18 May
20 May
22 May
24 May
26 May
28 May
30 May
01 Jun
Platform (4)
Android
Apple
AppleOsX
WinRT

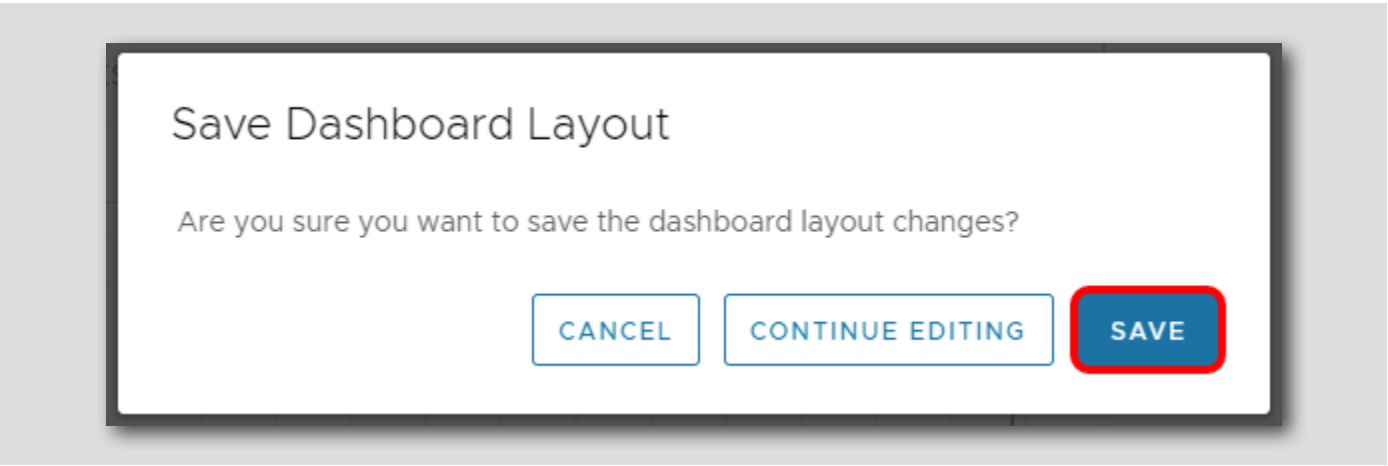


By default, the new widget appears at the bottom of your dashboard. Since this is the first widget on this dashboard, it will be at the top.

1. Click **Customize** the unlock the dashboard widgets.
2. You can click **Total Enrollments Over Time** (the chart title) and drag the widget to a new location on your dashboard.
3. You can click and drag the corners of the widget to change the width or height of the **Total Enrollments Over Time** widget.
4. After you are satisfied with the position and size of the widget, click **Save** at the top of the Dashboards page.

Save the Dashboard Layout

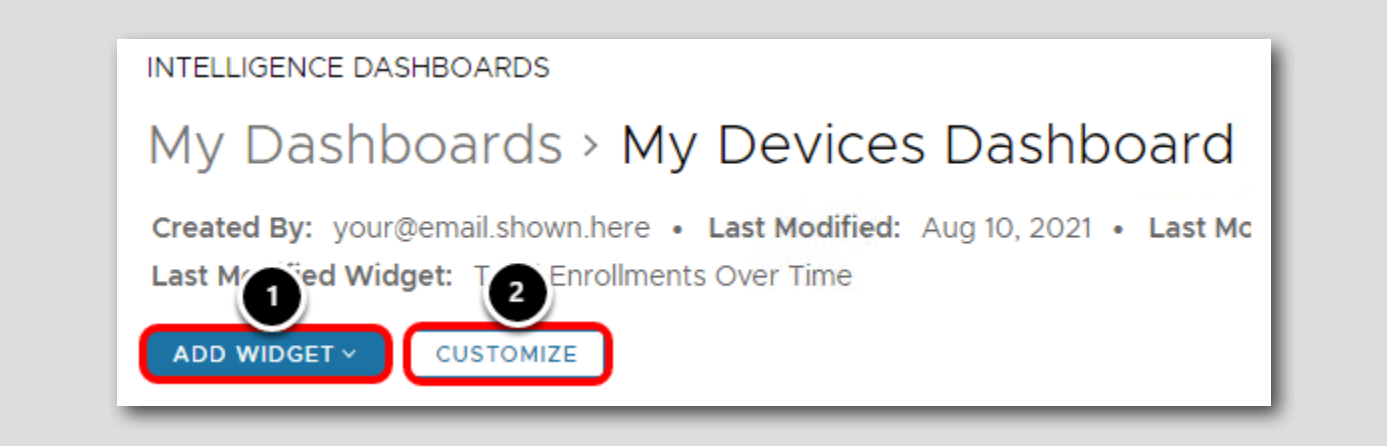
[559]



Click **Save** to save the dashboard layout.

Future Updates to the Dashboard

[560]



If you wish to modify the dashboard in the future, you can interact with the following:

1. **Add Widget** allows you to add additional widgets to the dashboard.
2. **Customize** allows you to change the layout of the existing widgets on the dashboard.

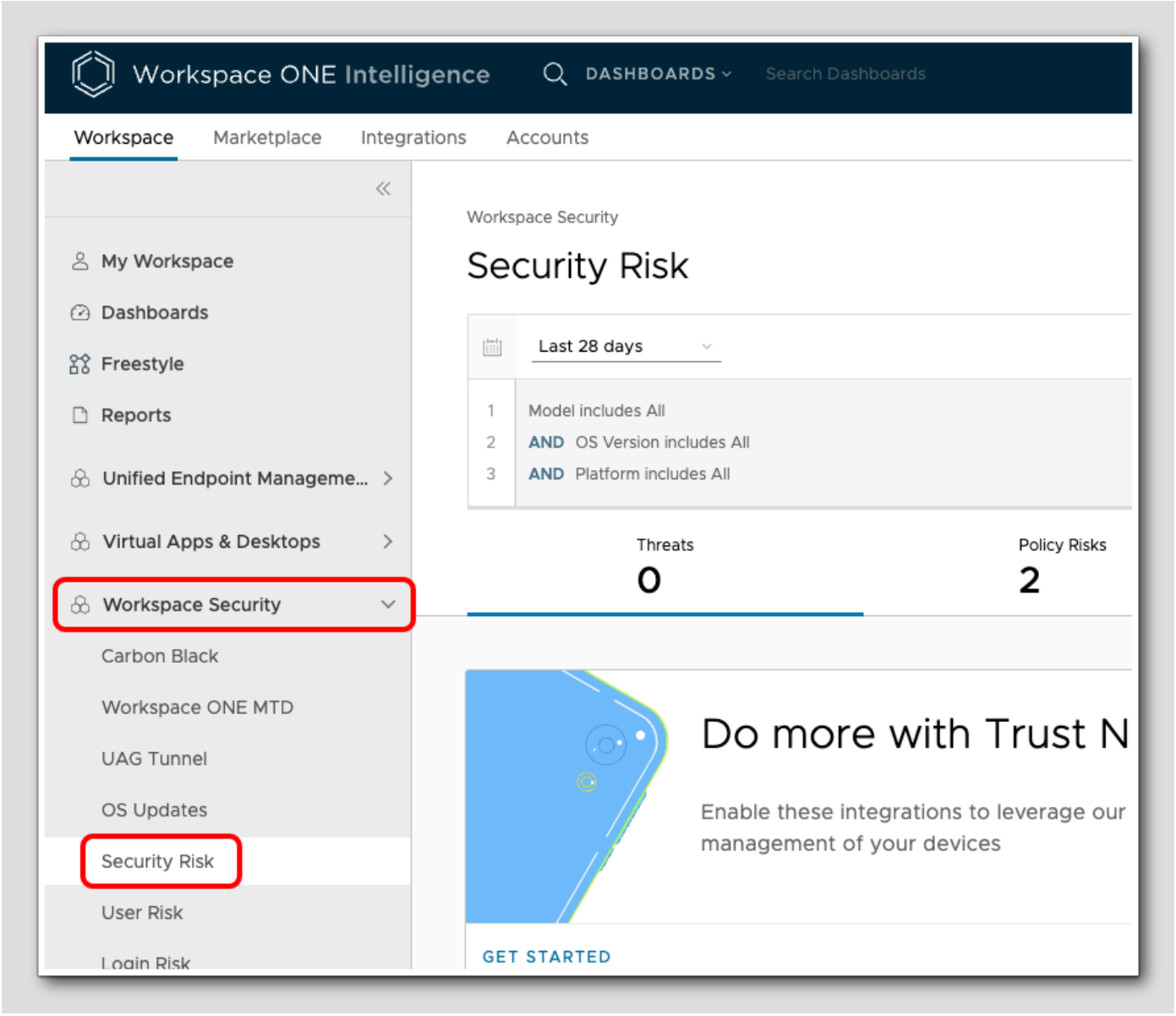
Increasing Compliance Across Devices

[561]

The Security Risk dashboards in Workspace ONE Intelligence gather reports on numerous device states and quickly identify high-risk devices. In this activity, you will explore the following Security Risk dashboards Workspace ONE Intelligence: Threats Summary, Compromised Devices, Policy Risks, and Vulnerabilities.

Access the Security Risk Dashboards

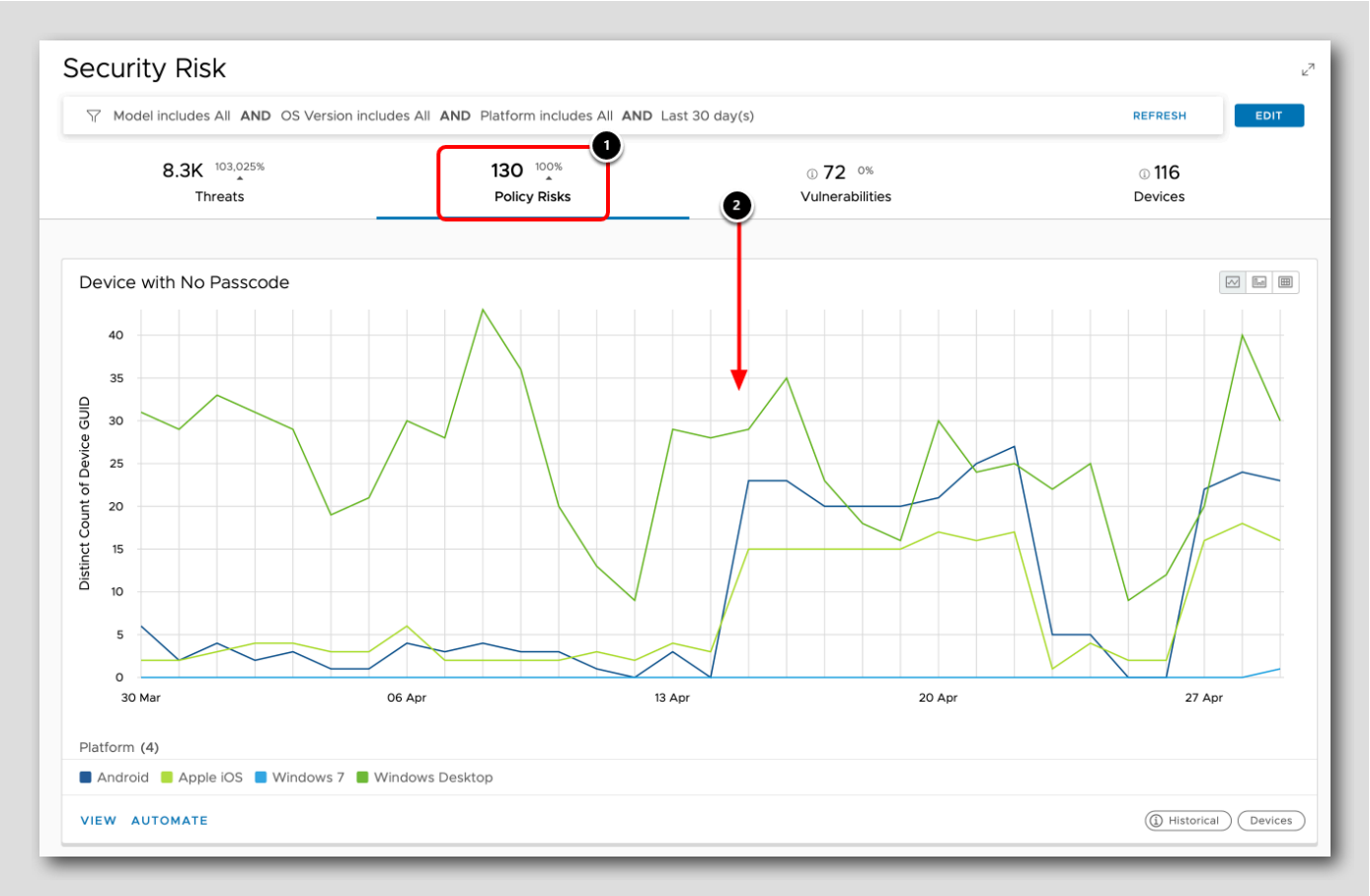
[562]



In the Workspace ONE Intelligence console, under Workspace Security, click **Security Risk**.

Identify Devices without Passcodes

[563]



NOTE: The screenshot was taken from a demo environment, so your view will not match the example above.

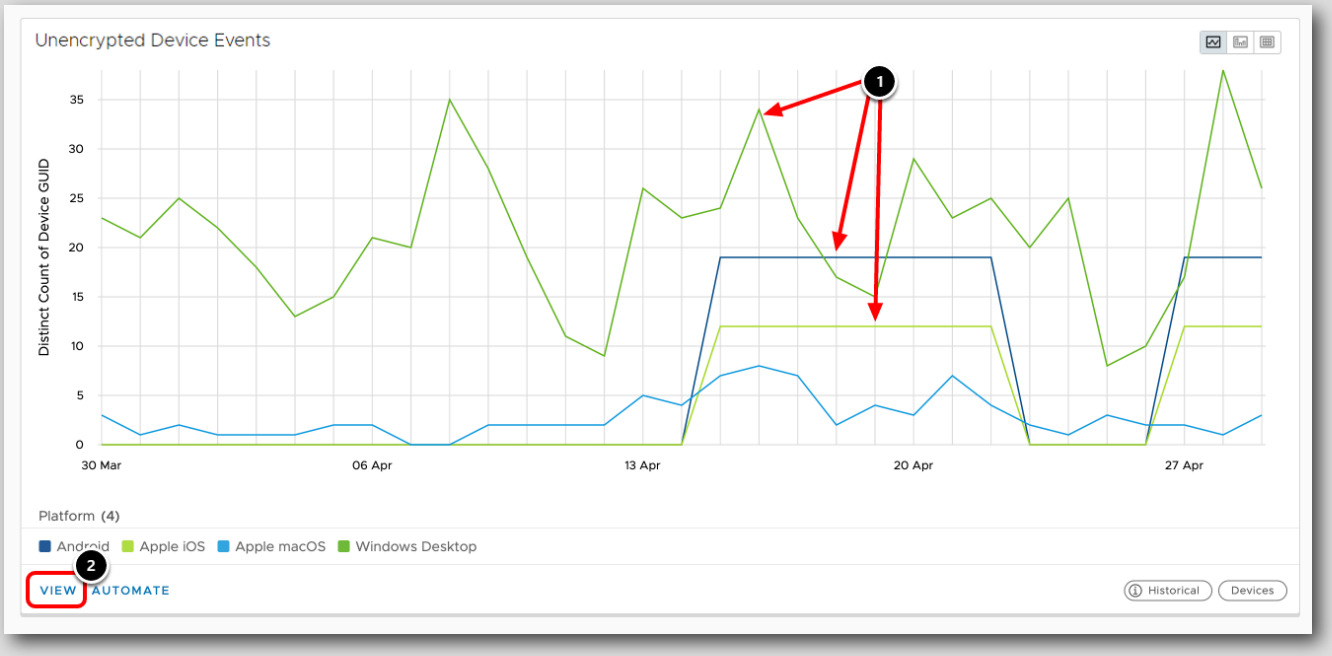
1. Select the **Policy Risks** tab to view the number of passcode-less devices detected in the past 30 days.

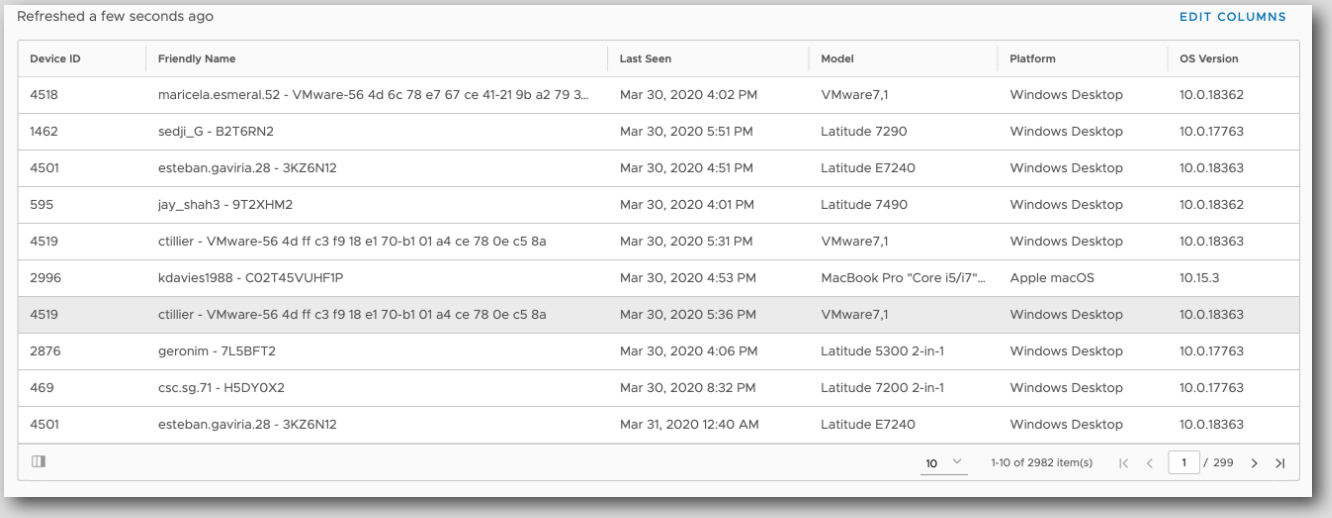
   Then, after you understand the scope of the issue, use automation to mitigate the risk. For example, you can create a rule to automatically move a passcode-less device to quarantine, or remove its access to corporate data.

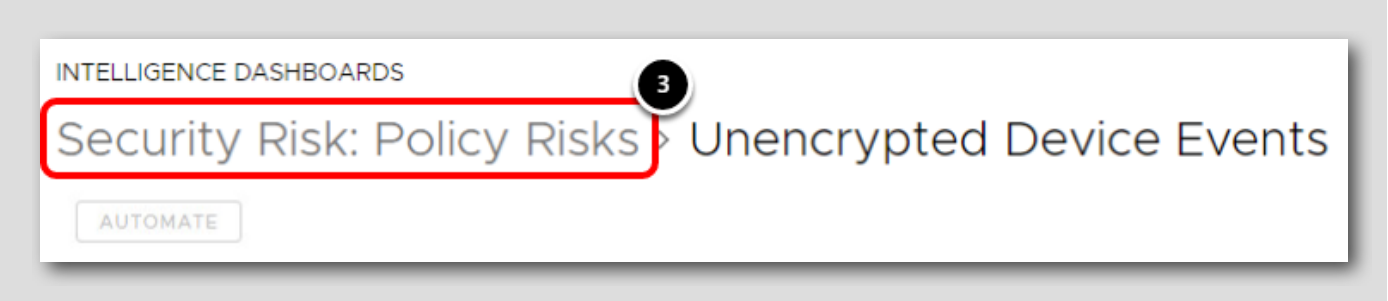
2. Scroll down.

Identify Unencrypted Devices

[564]







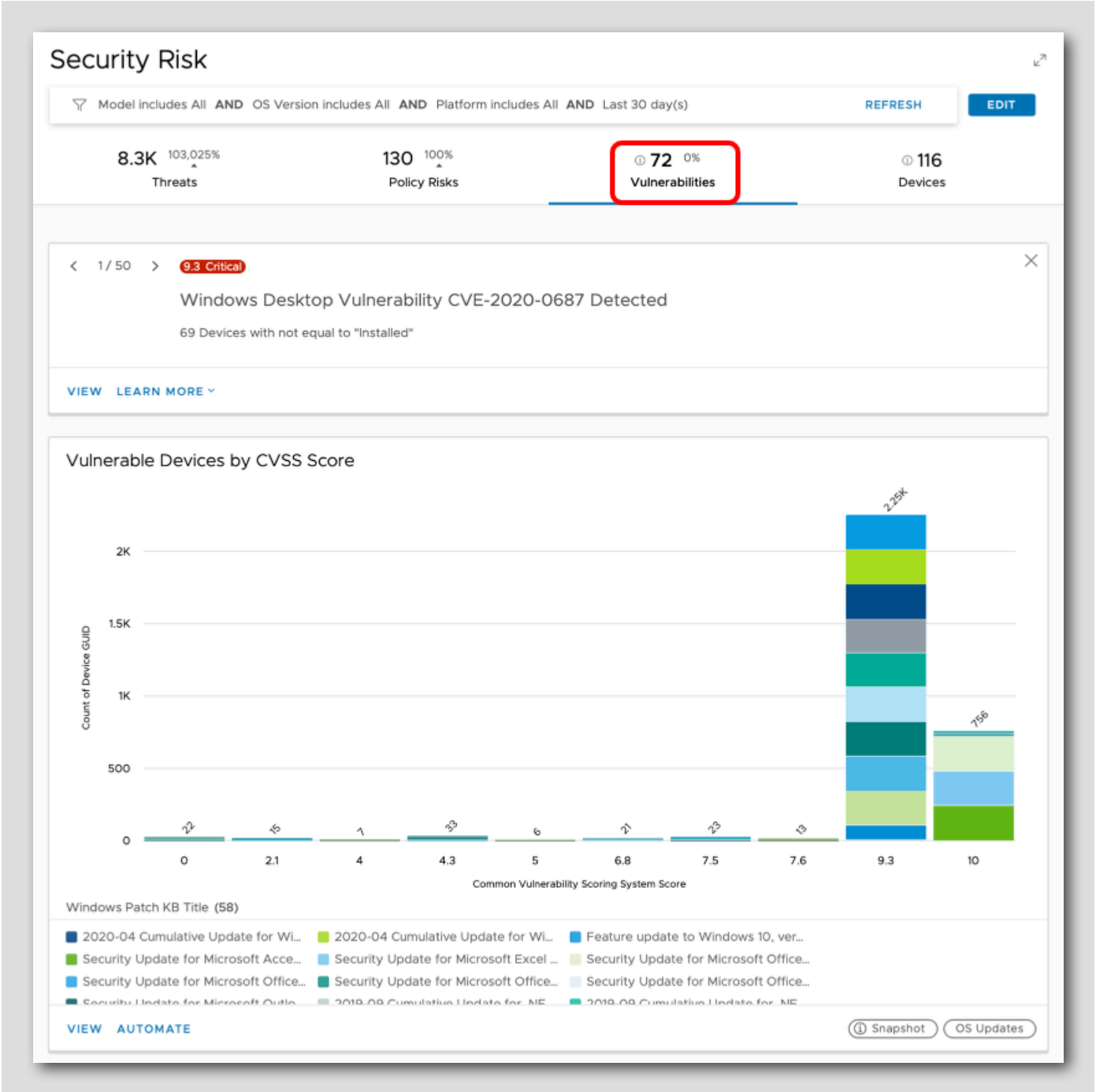
NOTE: The screenshot was taken from a demo environment, so your view will not match the example above.

Scroll down to find **Unencrypted Device Events** dashboard. This chart shows the total number of unencrypted devices identified on a daily basis by Workspace ONE Intelligence.

1. **Point to** the data points for additional details about the number of devices per platform.
2. Click **View** to obtain a detailed list of devices.
3. Click **Security Risk: Policy Risks** to return.

Identify Vulnerable Devices

[565]



NOTE: The screenshot was taken from a demo environment, so your view will not match the example above.

Select the **Vulnerabilities** tab to view the number of vulnerable devices identified in the last 30 days.

Without encryption, confidential information is unprotected, and can easily land in the wrong hands. To mitigate this risk, create policies to enforce device encryption. For example, you can create a policy to block corporate access until the device is encrypted through Workspace ONE UEM.

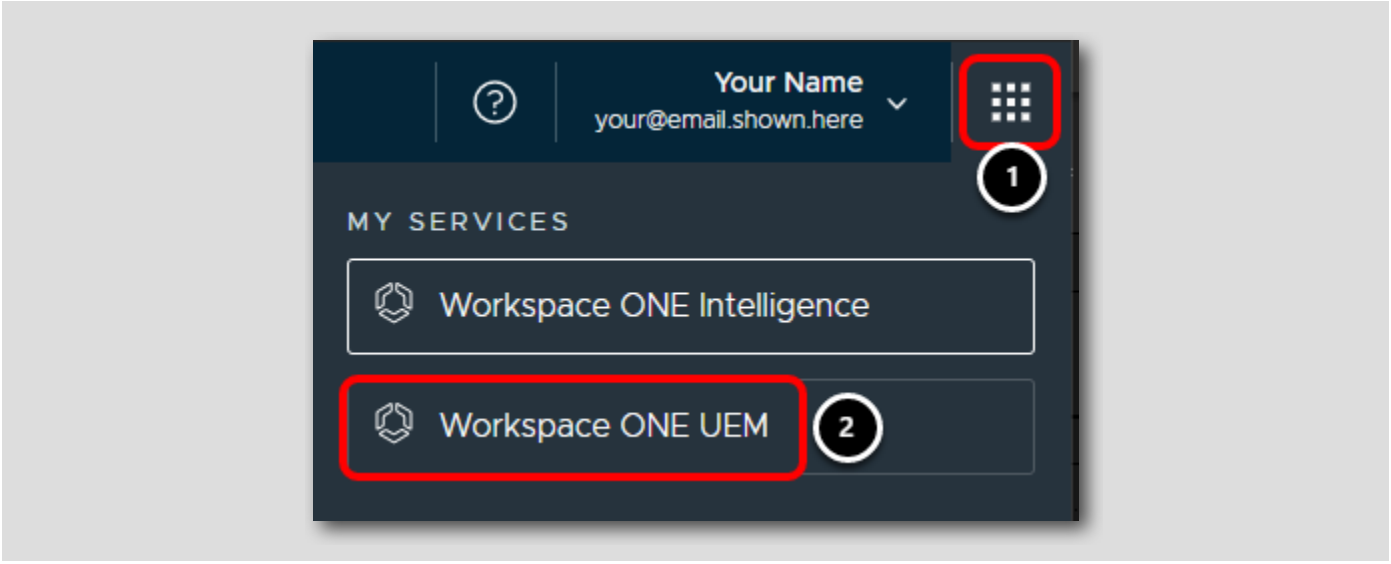
Configuring Workspace ONE Intelligence Automation Connectors [566]

To take full advantage of Workspace ONE Intelligence, you need to configure at least one Automation Connector to enable Automation Actions in your environment.

Among the multiple available Connectors, the Workspace ONE UEM connector is key, as it enables Intelligence Automation to take actions against your organization's devices, apps, device sensors and OS updates.

In this activity, you will configure the Workspace ONE UEM Connectors to allow API communication between Workspace ONE Intelligence and Workspace ONE UEM.

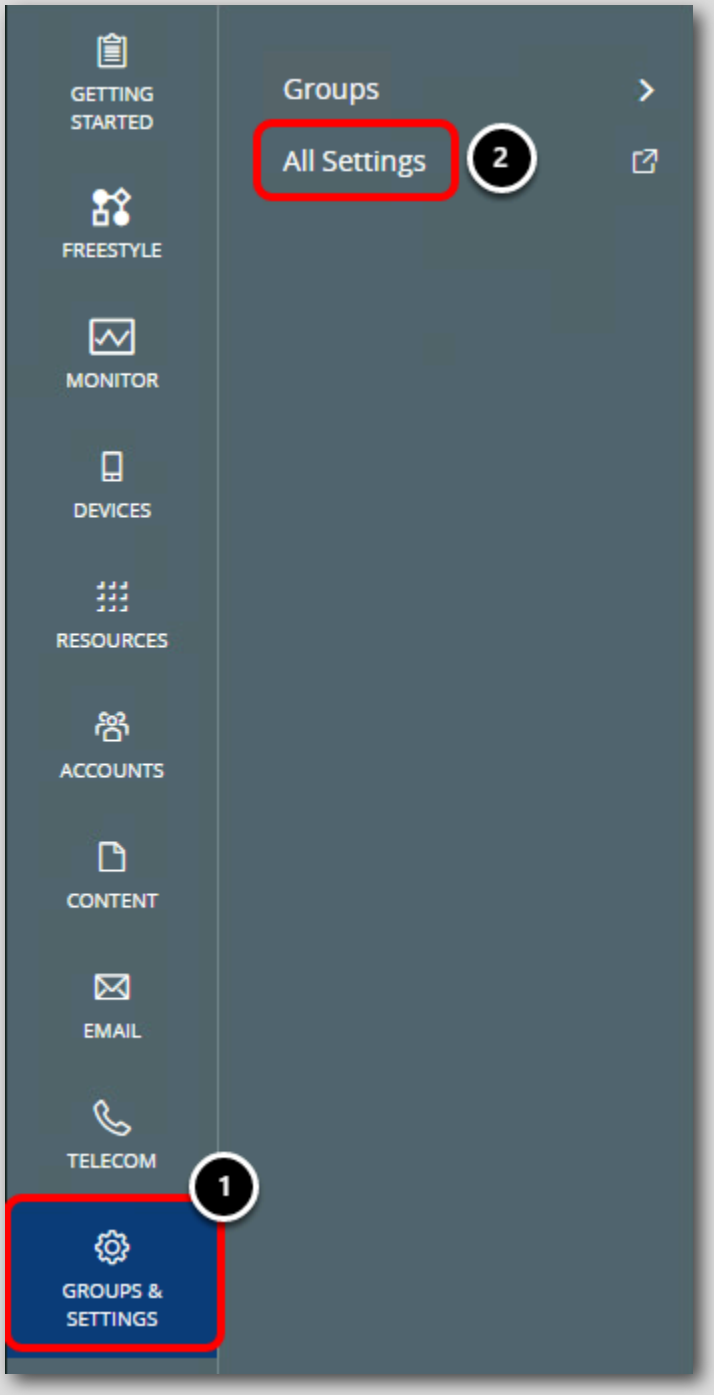
Switch to Workspace ONE UEM Console [567]



From the Workspace ONE Intelligence console:

1. Click the **Services** menu icon.
2. Select **Workspace ONE UEM**.

Navigate to All Settings [568]

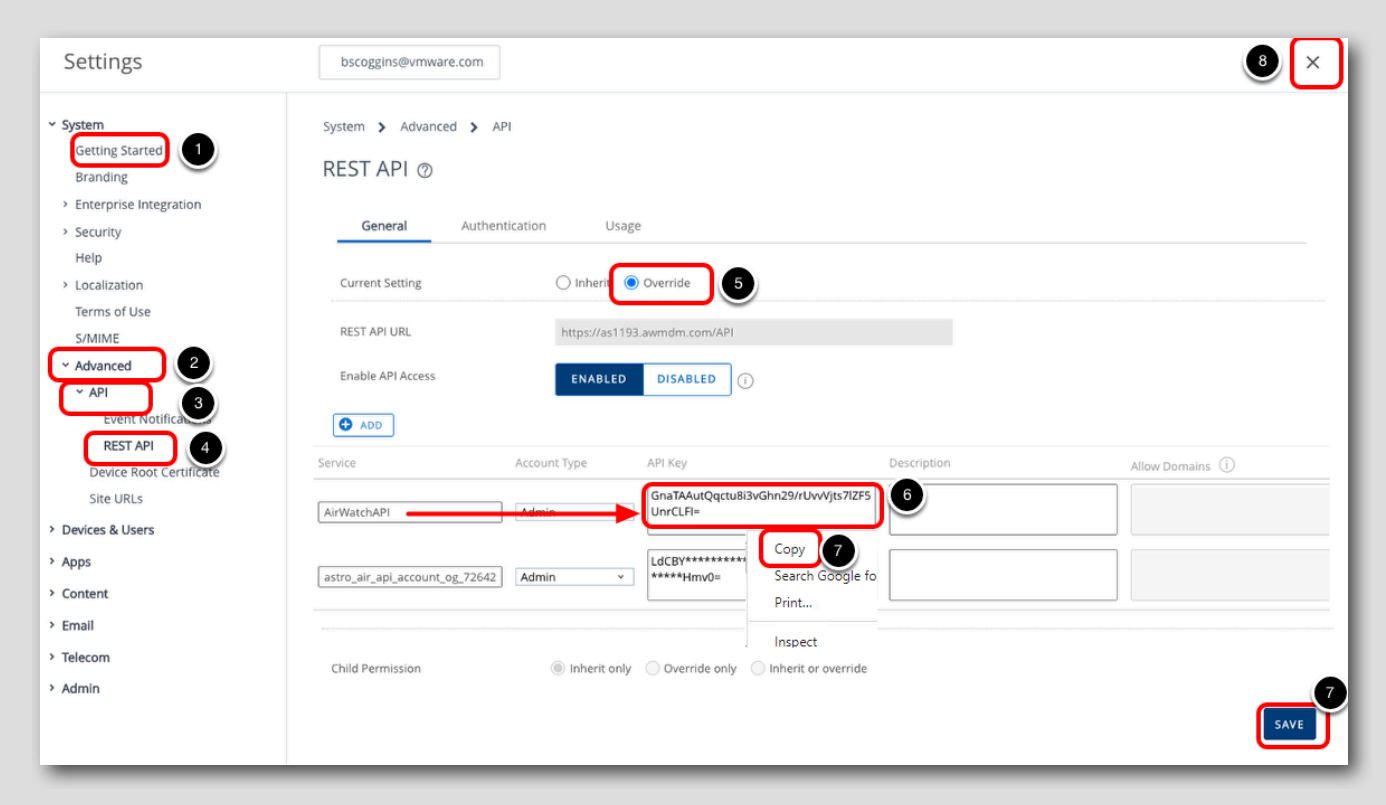


In the Workspace ONE UEM Administrator console:

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

Regenerate the API Key

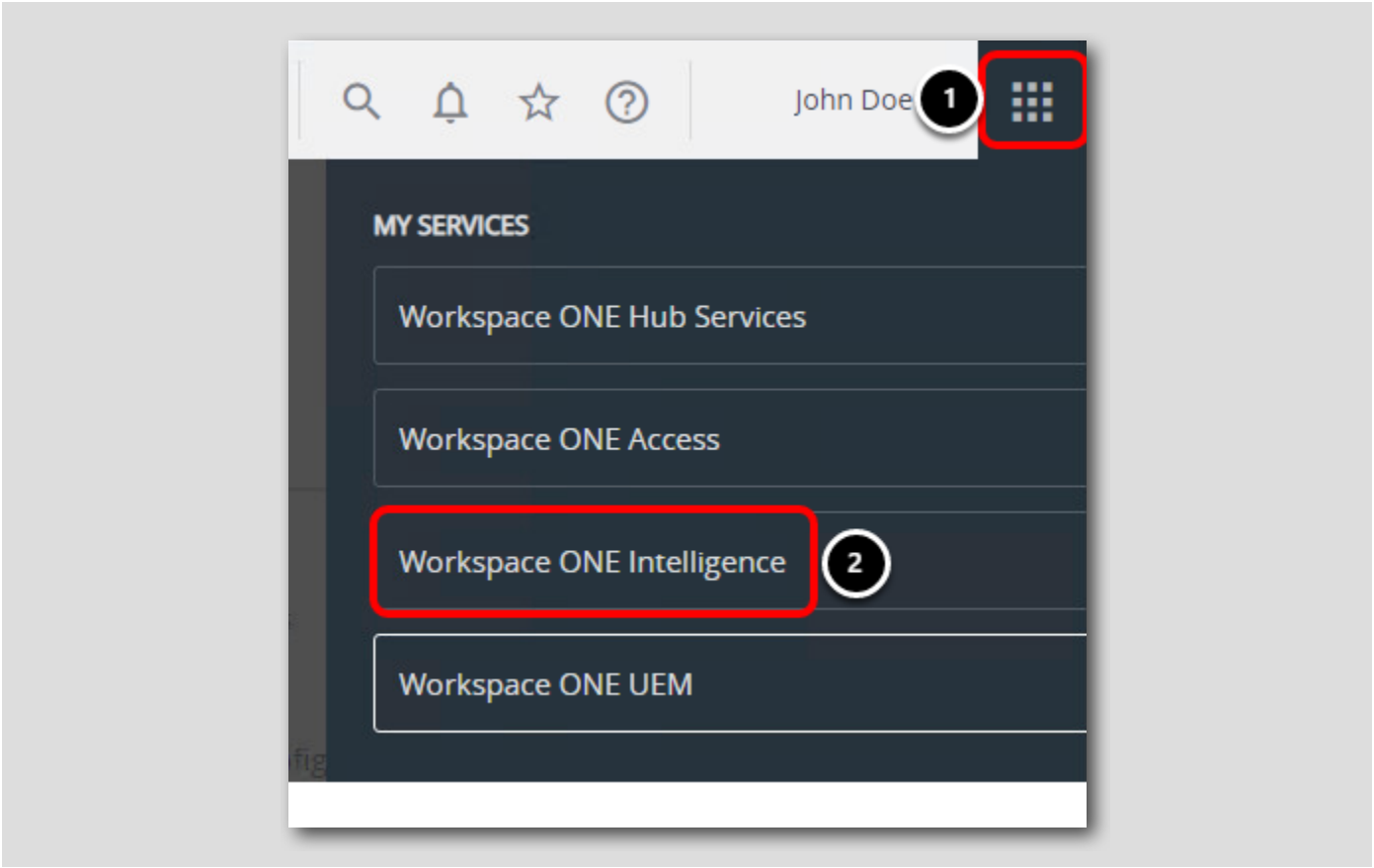
[569]



1. Click **System**.
2. Click **Advanced**.
3. Click **API**.
4. Click **REST API**.
5. Click **Override** to generate the new API Key used to integrate with Workspace ONE Intelligence.
6. For the **AirWatchAPI Service**, select the full API Key field and **right-click**.
7. Click **Copy** to save the API Key for an upcoming step.
8. Click **Save**.
9. Click **Close**.

Return to Workspace ONE Intelligence Console

[570]

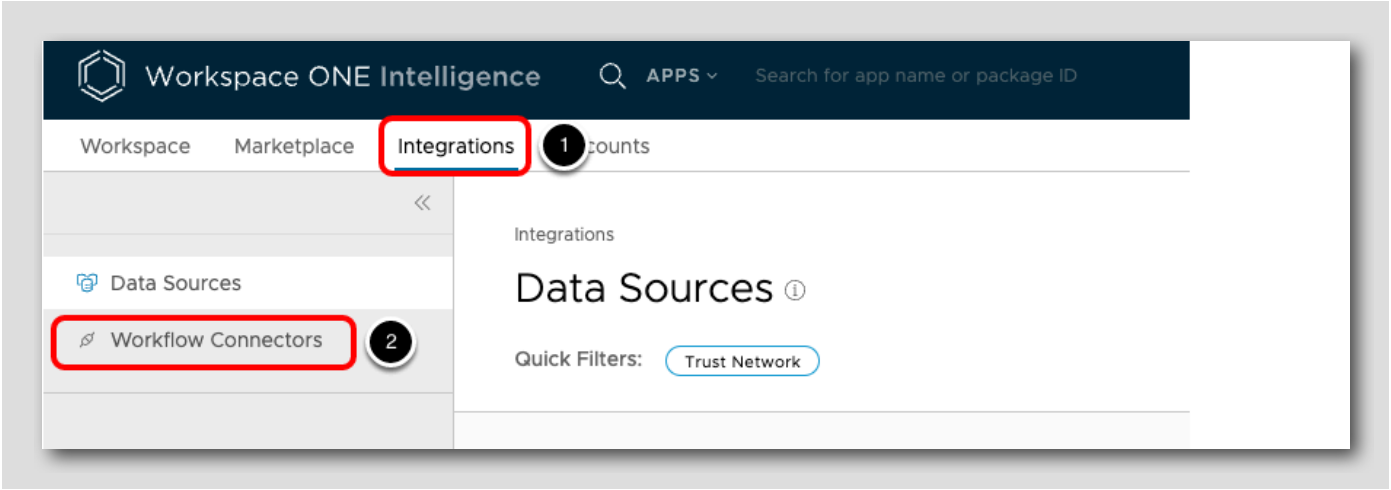


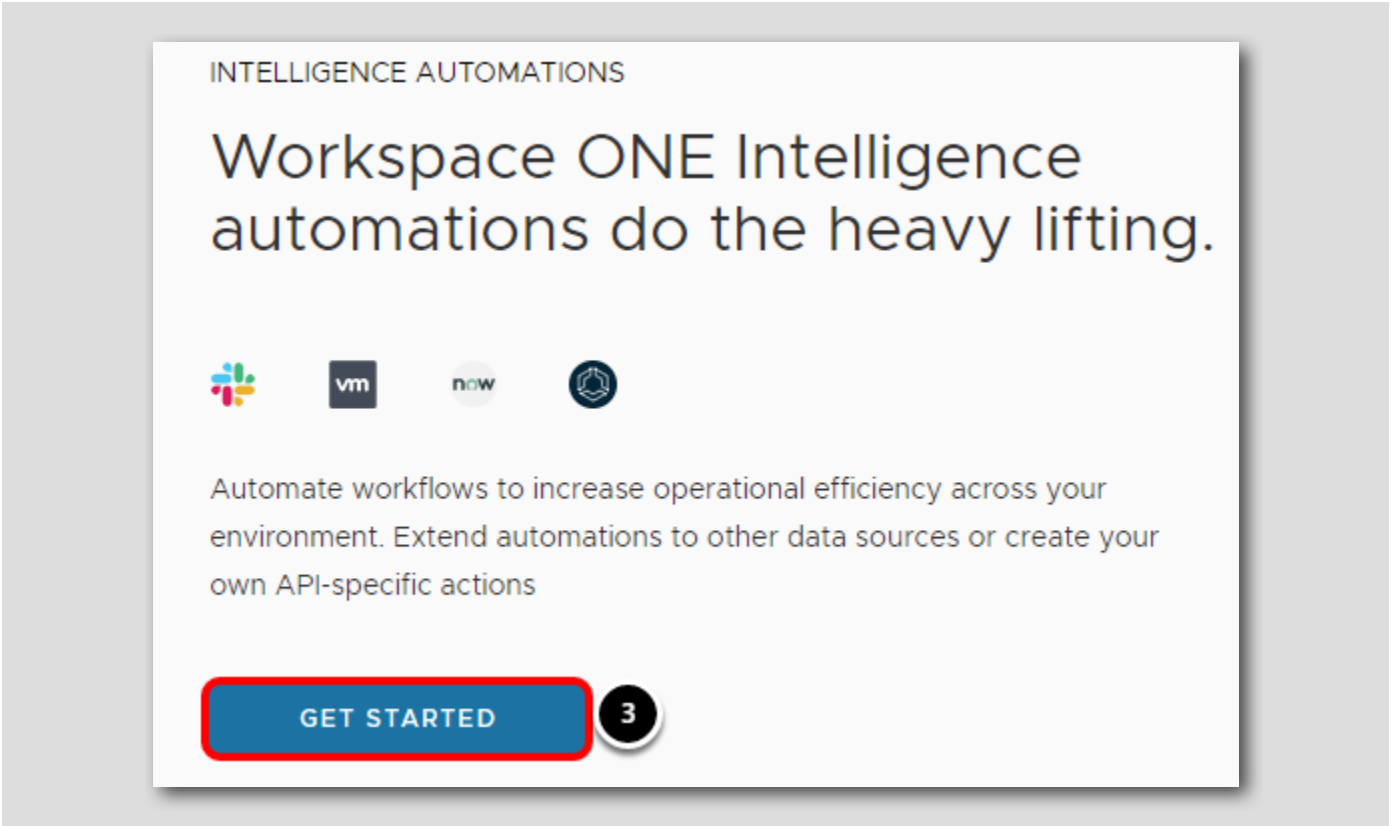
From the Workspace ONE UEM Administrator console:

1. Click the **Services** menu icon.
2. Select **Workspace ONE Intelligence**.

Open Automation Connections

[571]

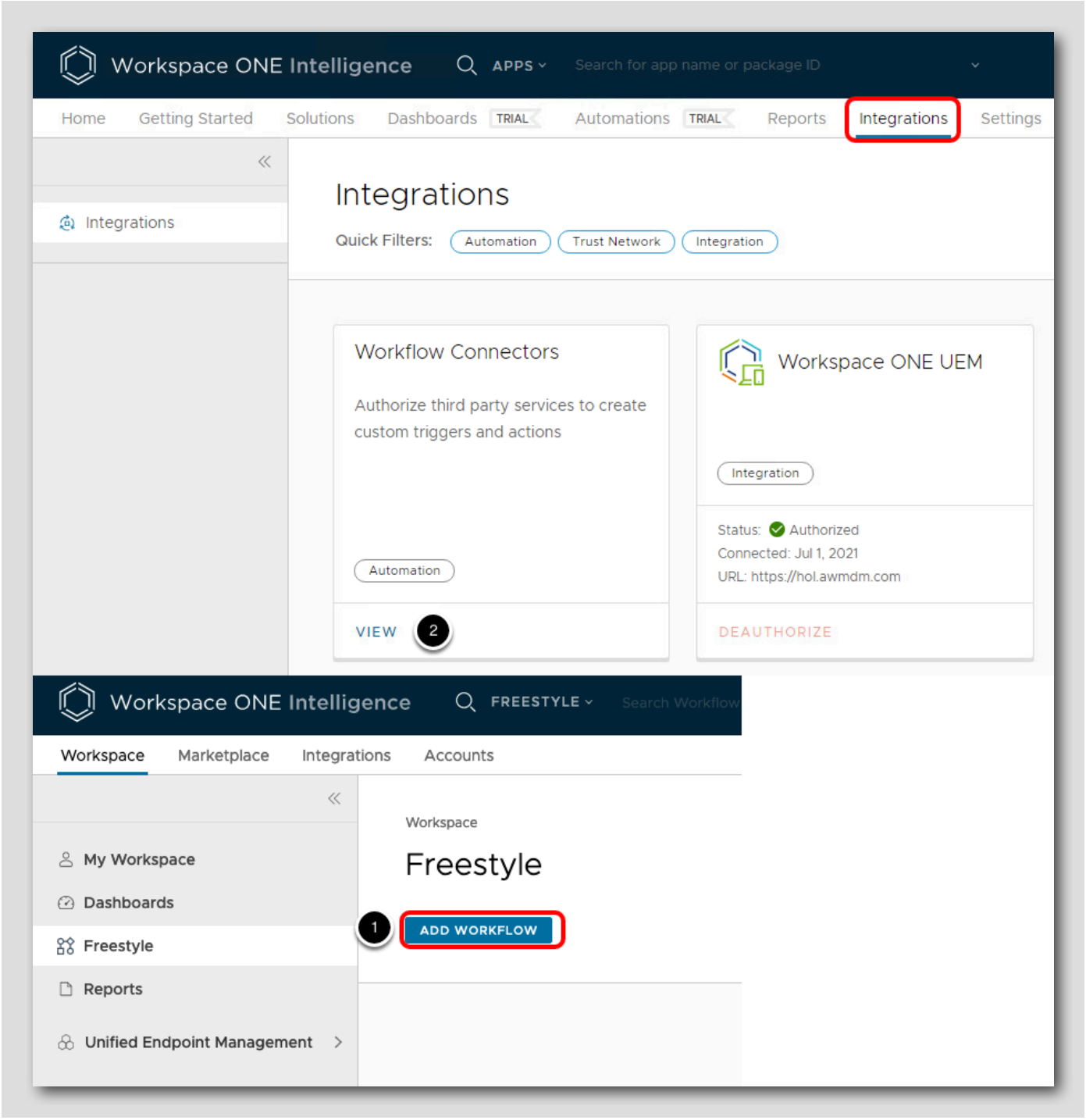


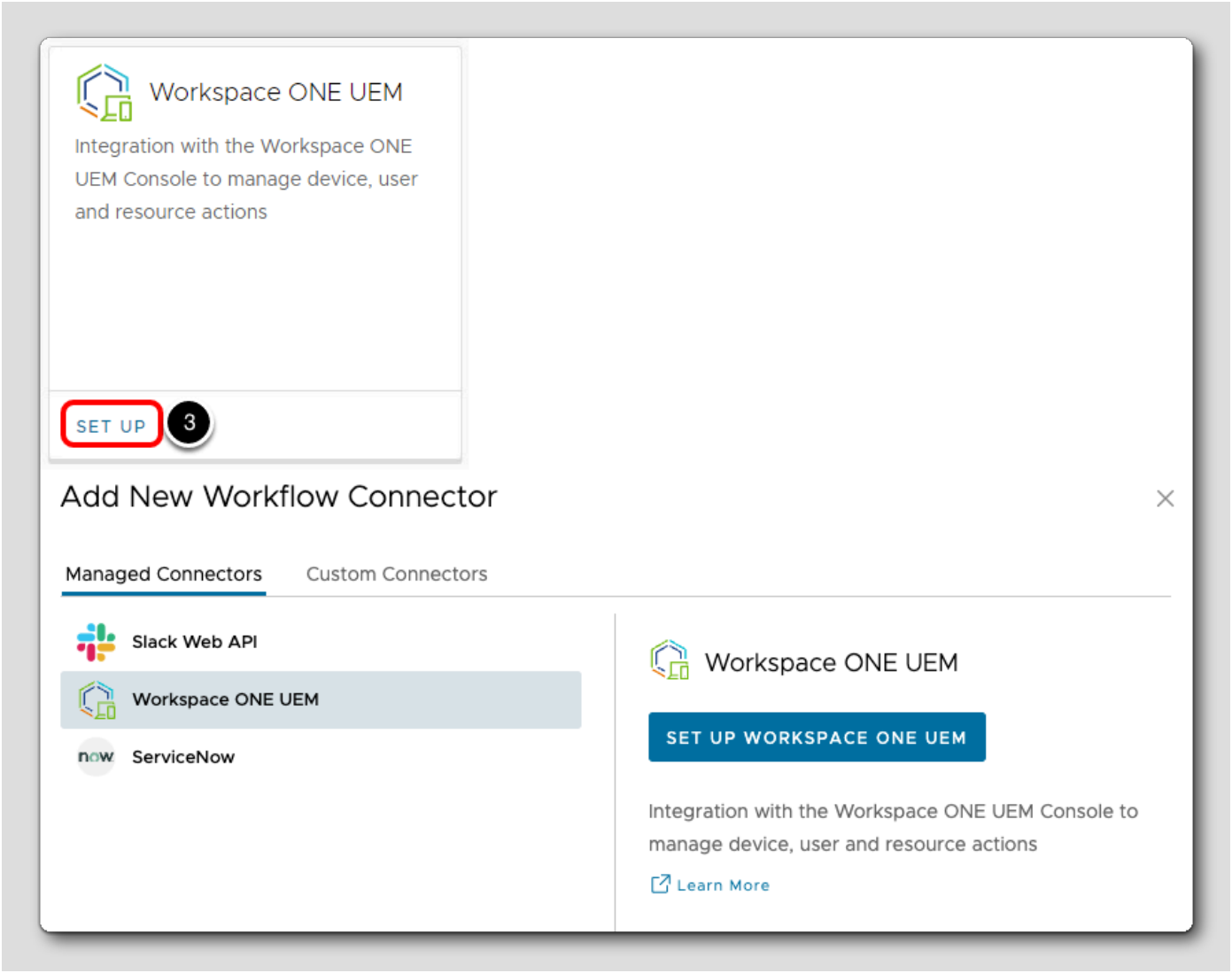


1. Click **Integrations**.
2. Click **Workflow Connectors**.
3. Click **Get Started**.

Setup Workspace ONE UEM Integration

[572]

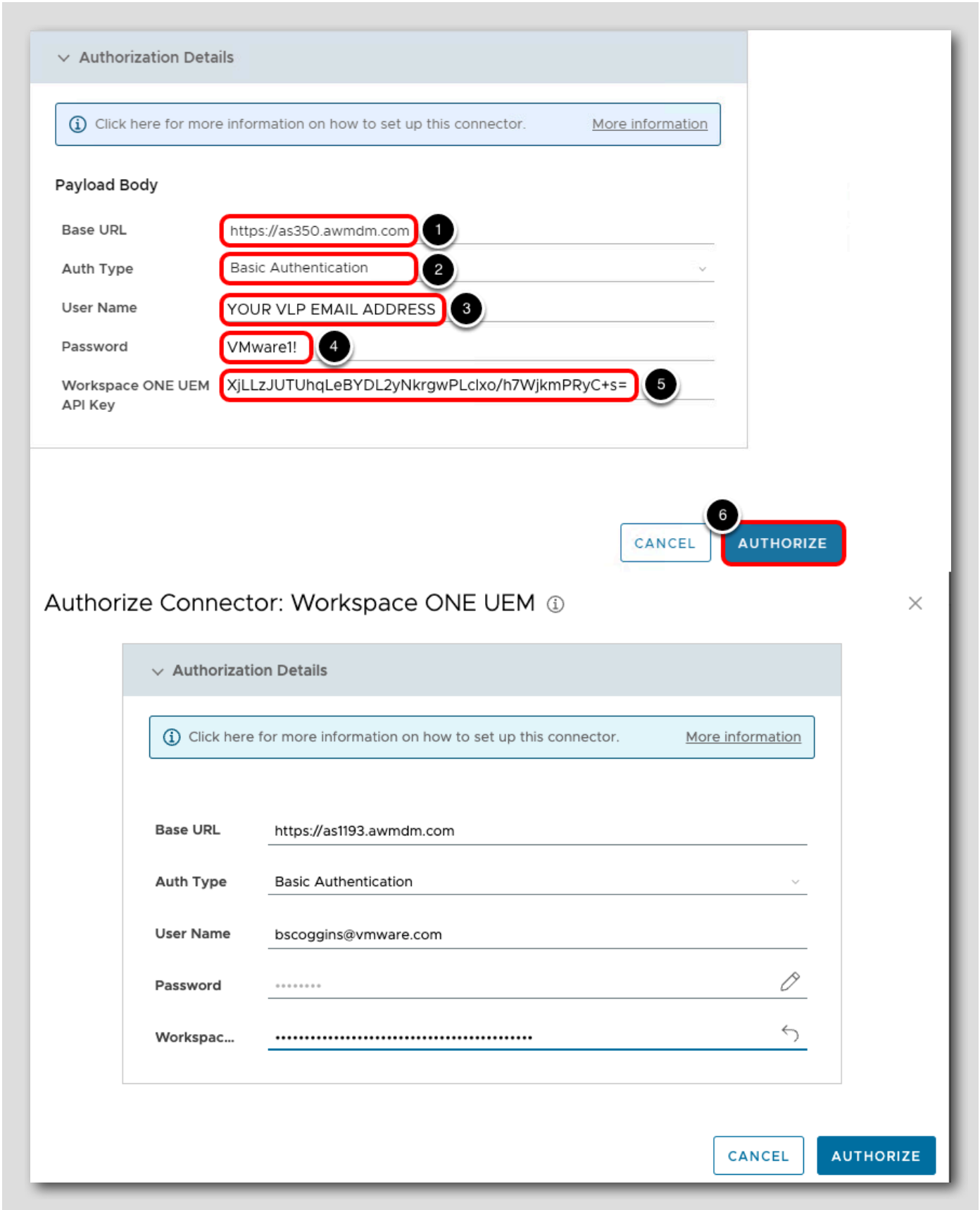




1. If you were taken away from the Integrations tab after clicking Get Started, click the **Integrations** tab again.
2. Click **View** for the Workflow Connections card.
3. Click **Setup** for the Workspace ONE UEM card.

On the Workspace ONE UEM card, click **Set Up**.

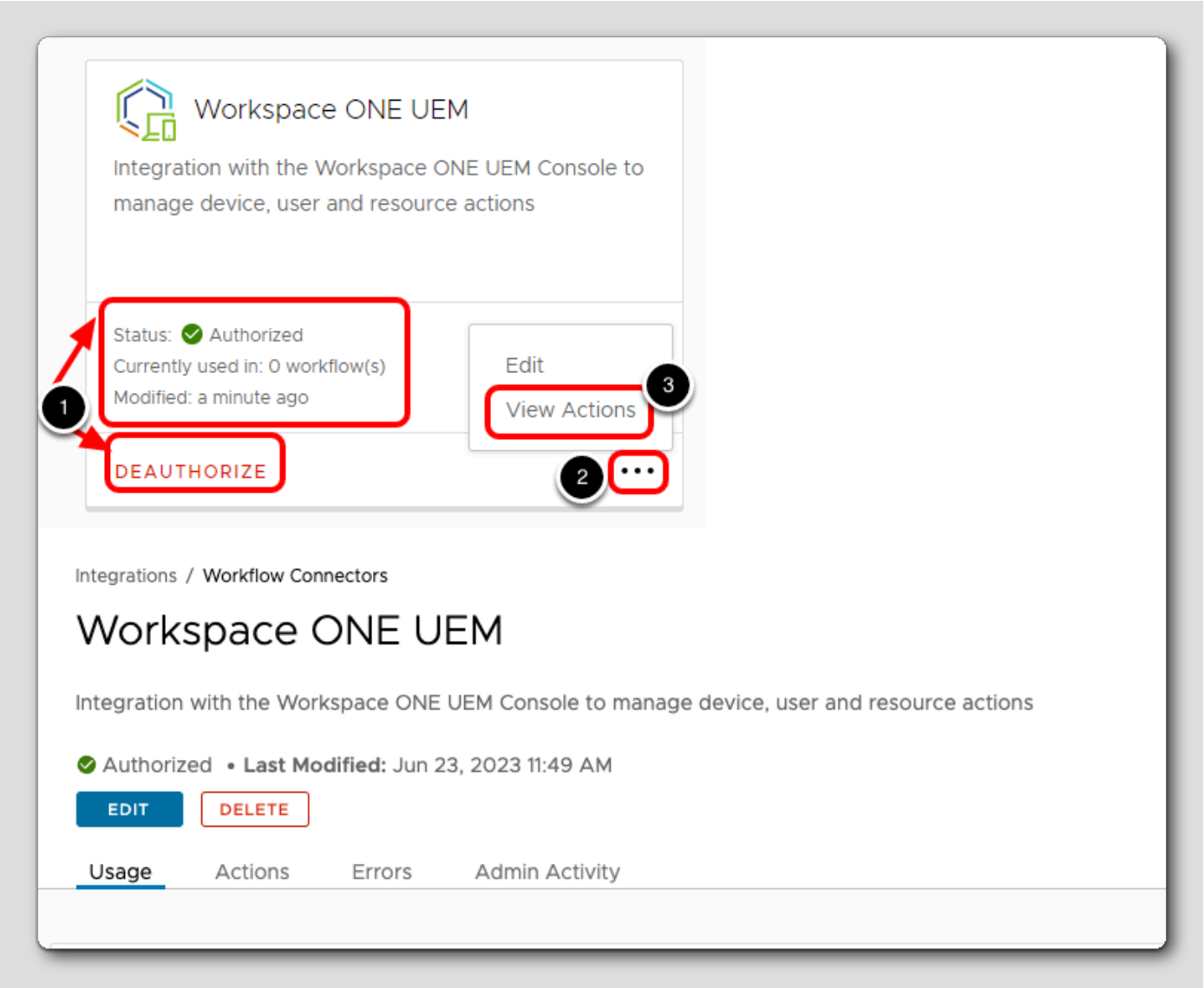
Configure Authorization


Authorization Details
Click here for more information on how to set up this connector.
More information
Payload Body
Base URL
https://as350.awmdm.com
1
Auth Type
Basic Authentication
2
User Name
YOUR VLP EMAIL ADDRESS
3
Password
VMware1!
4
Workspace ONE UEM API Key
XjLLzJUTUhqLeBYDL2yNkrgwPLclxo/h7WjkmPRyC+s=
5
CANCEL
6
AUTHORIZE
Authorize Connector: Workspace ONE UEM
Authorization Details
Click here for more information on how to set up this connector.
More information
Base URL
https://as1193.awmdm.com
Auth Type
Basic Authentication
User Name
bscoggins@vmware.com
Password
Workspac...
CANCEL
AUTHORIZE

1. Enter the Base URL for the Workspace ONE UEM environment. In this case, **`https://as1193.awmdm.com`**.
2. Choose **Basic Authentication** for the Auth Type.
3. Enter the API User Name for the Workspace ONE UEM administrator with access to the REST API Key you copied earlier. This will be **Your VLP E-Mail Address** that you used to sign into the Workspace ONE UEM Console.
4. Enter the API User Password **`VMware1!`**.
5. Paste the **Workspace ONE UEM API Key**. This is the AirWatchAPI Service Key that you copied from the Workspace ONE UEM console in the previous activity.
6. Click **Authorize**.

Validate Authorization

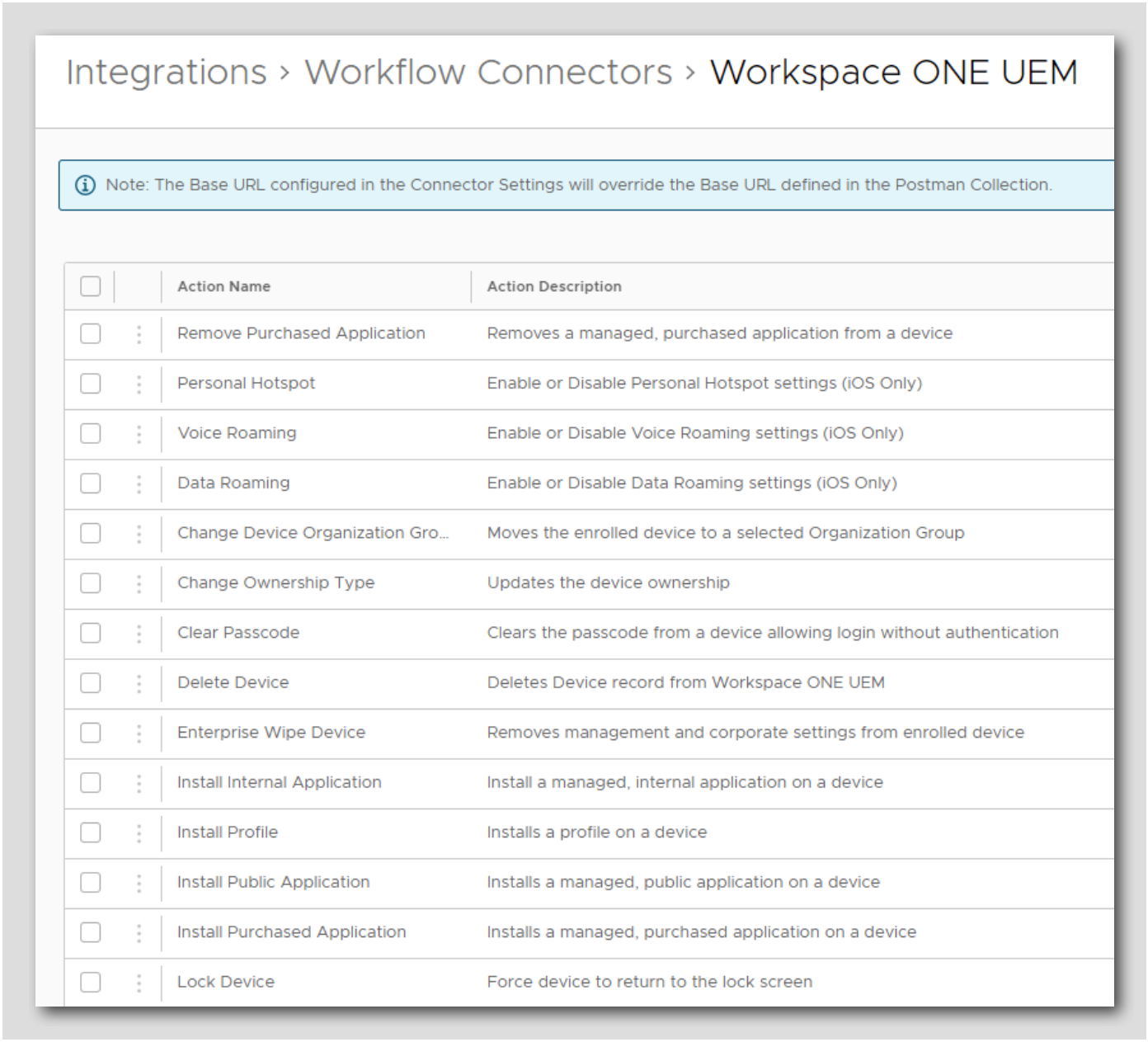
[574]



1. Verify the Workspace ONE UEM card now displays the Status as **Authorized** and the card action changes to **Deauthorize**. This indicates integration was successful.
2. Click the ... button.
3. Click **View Actions**.

Review Automation Actions against Workspace ONE UEM

[575]



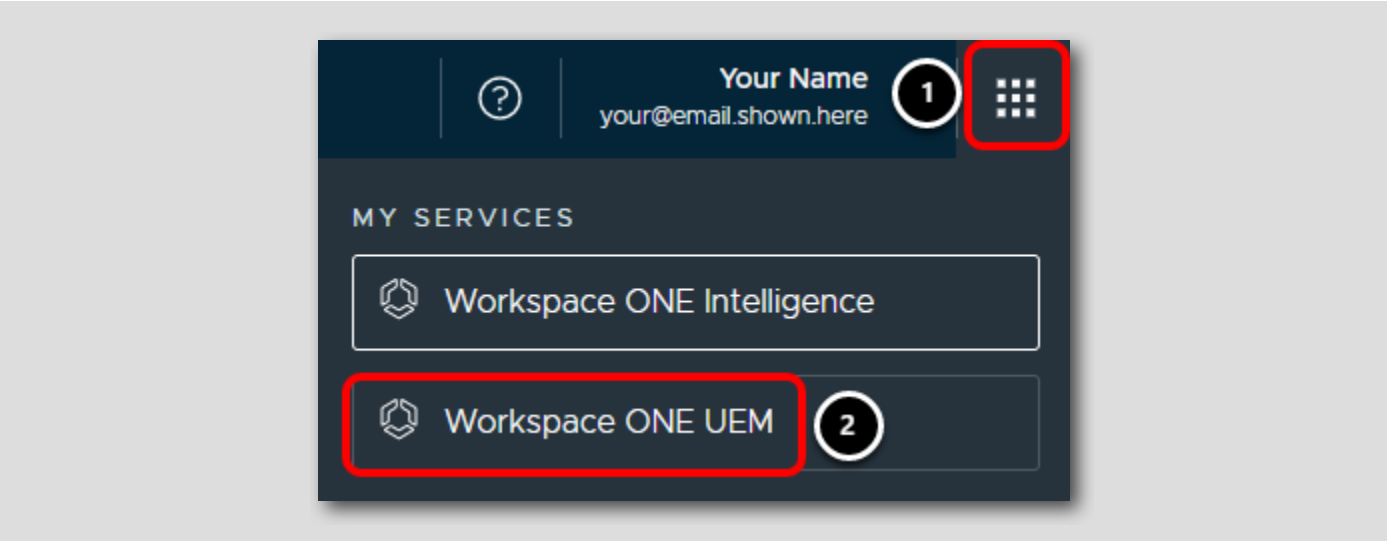
As a result, you are now able to define automated flows, which can take over 25+ different actions against your devices, apps, and OS updates. The screenshot shows some of the actions available against devices.

Continue to the next step.

Using Automation to Tag Low Battery Life Devices [576]

In this activity, you will use the automation capabilities in Workspace ONE Intelligence to tag low battery life devices in Workspace ONE UEM.

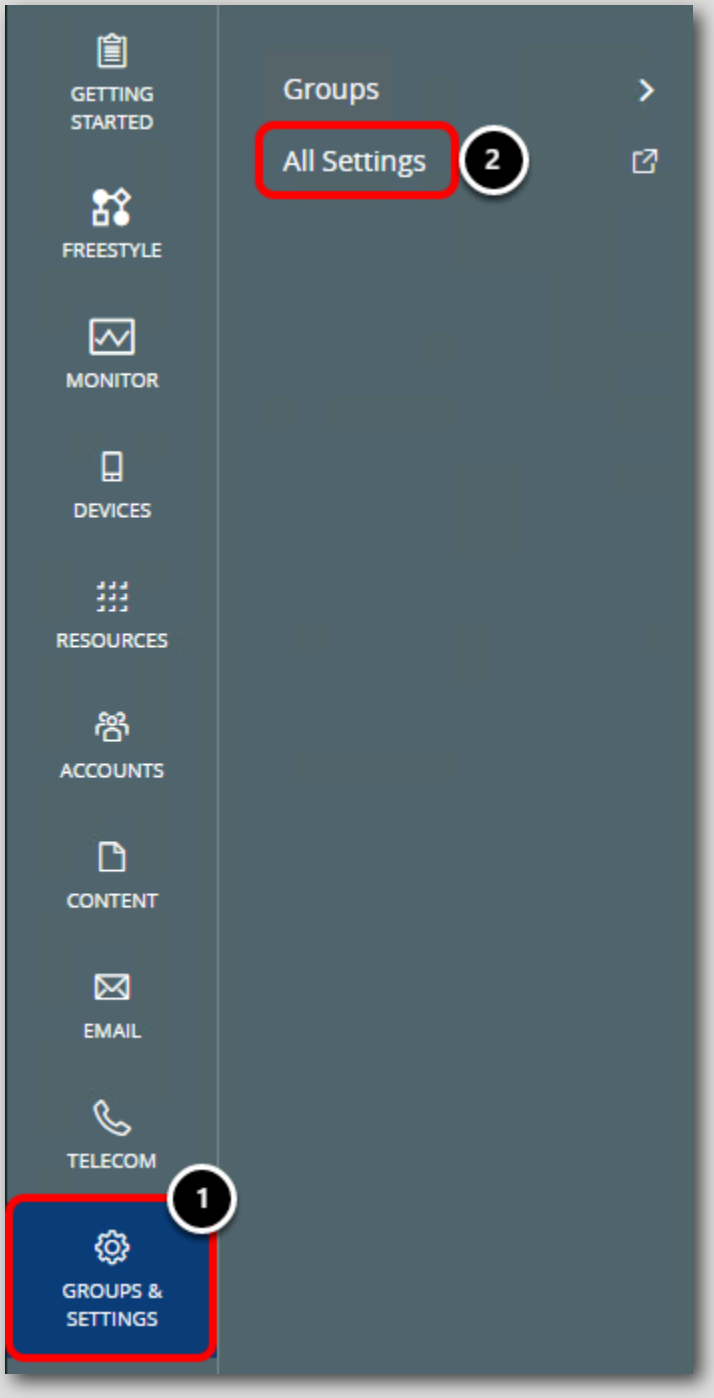
Return to the Workspace ONE UEM Console [577]



From the Workspace ONE Intelligence Console:

1. Click the **Services** menu.
2. Click **Workspace ONE UEM**.

Navigate to All Settings in Workspace ONE UEM Console [578]

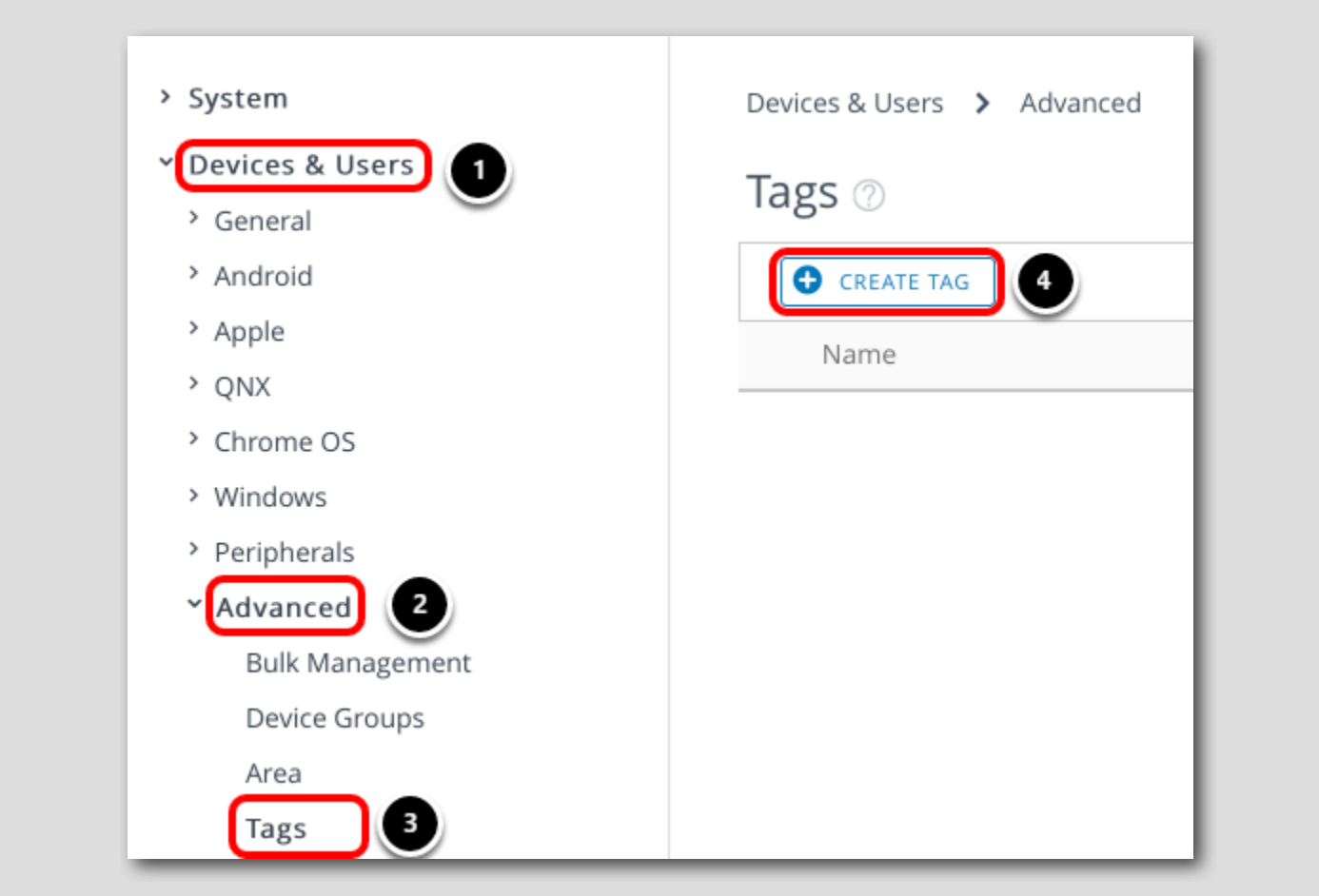


In the Workspace ONE UEM console:

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

Create the Low Battery Health Tag

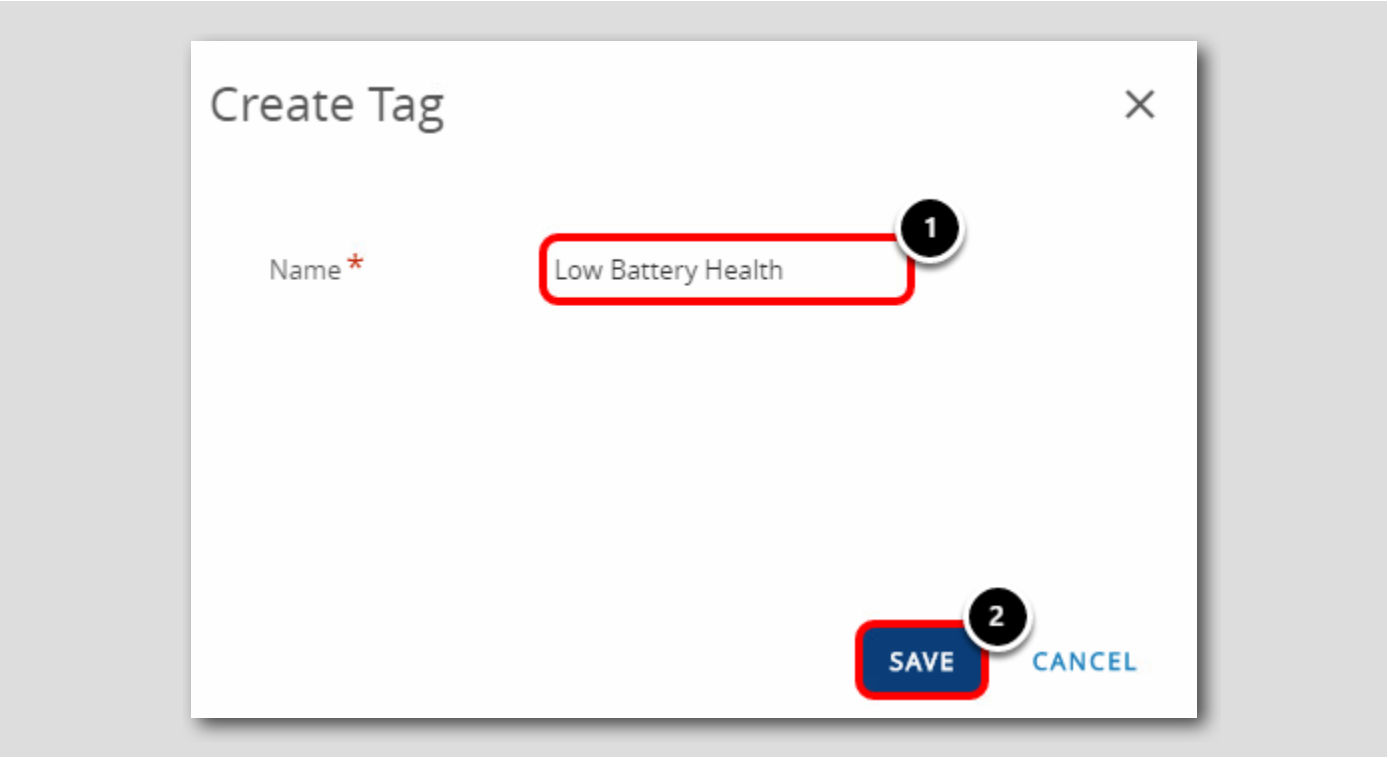
[579]



1. Click **Device & Users**.
2. Click **Advanced**.
3. Click **Tags**.
4. Click **Create Tag**.

Save Low Battery Health Tag

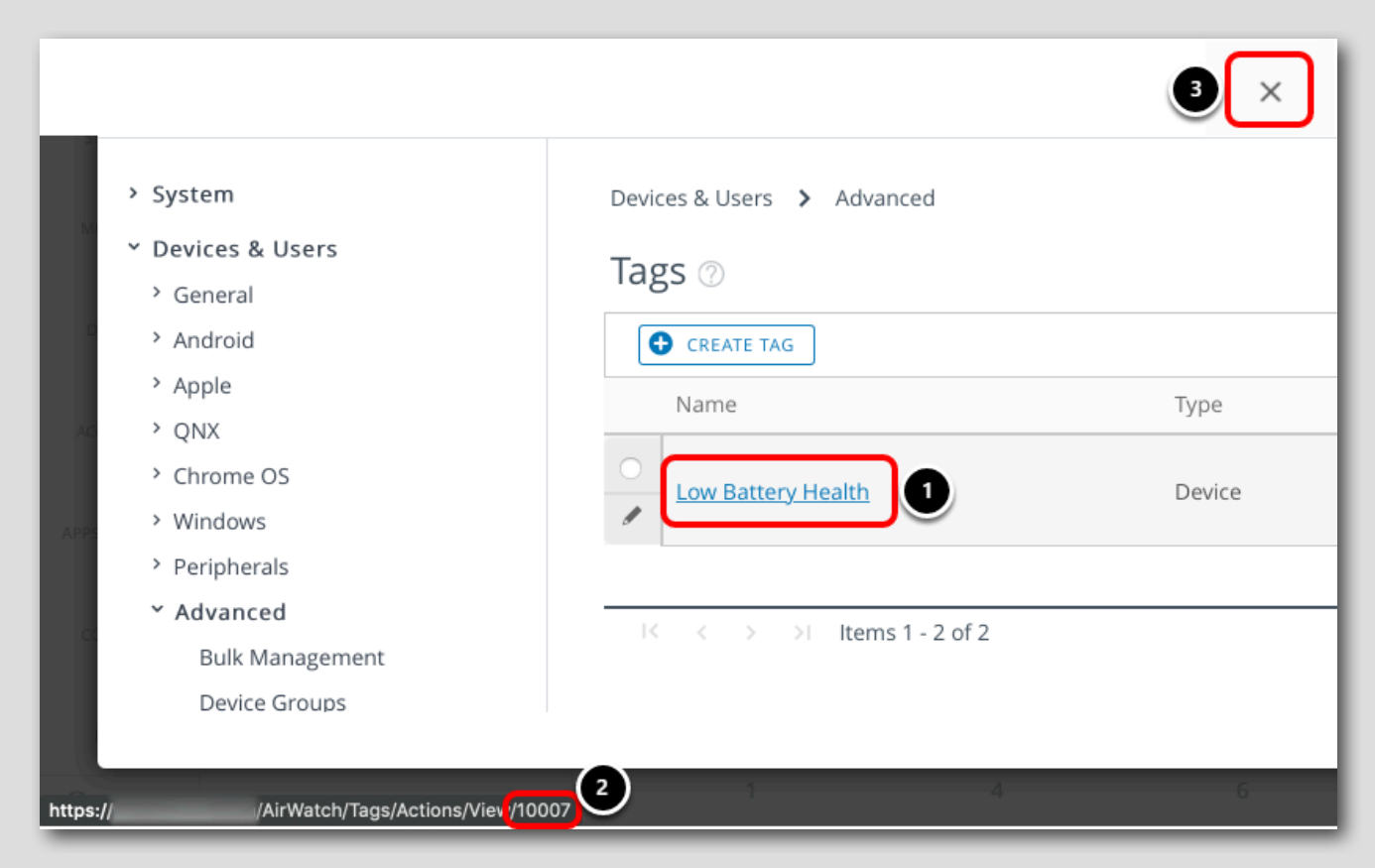
[580]



1. Enter **`Low Battery Health`** for the Tag Name.
2. Click **Save**.

Obtain Tag ID

[581]

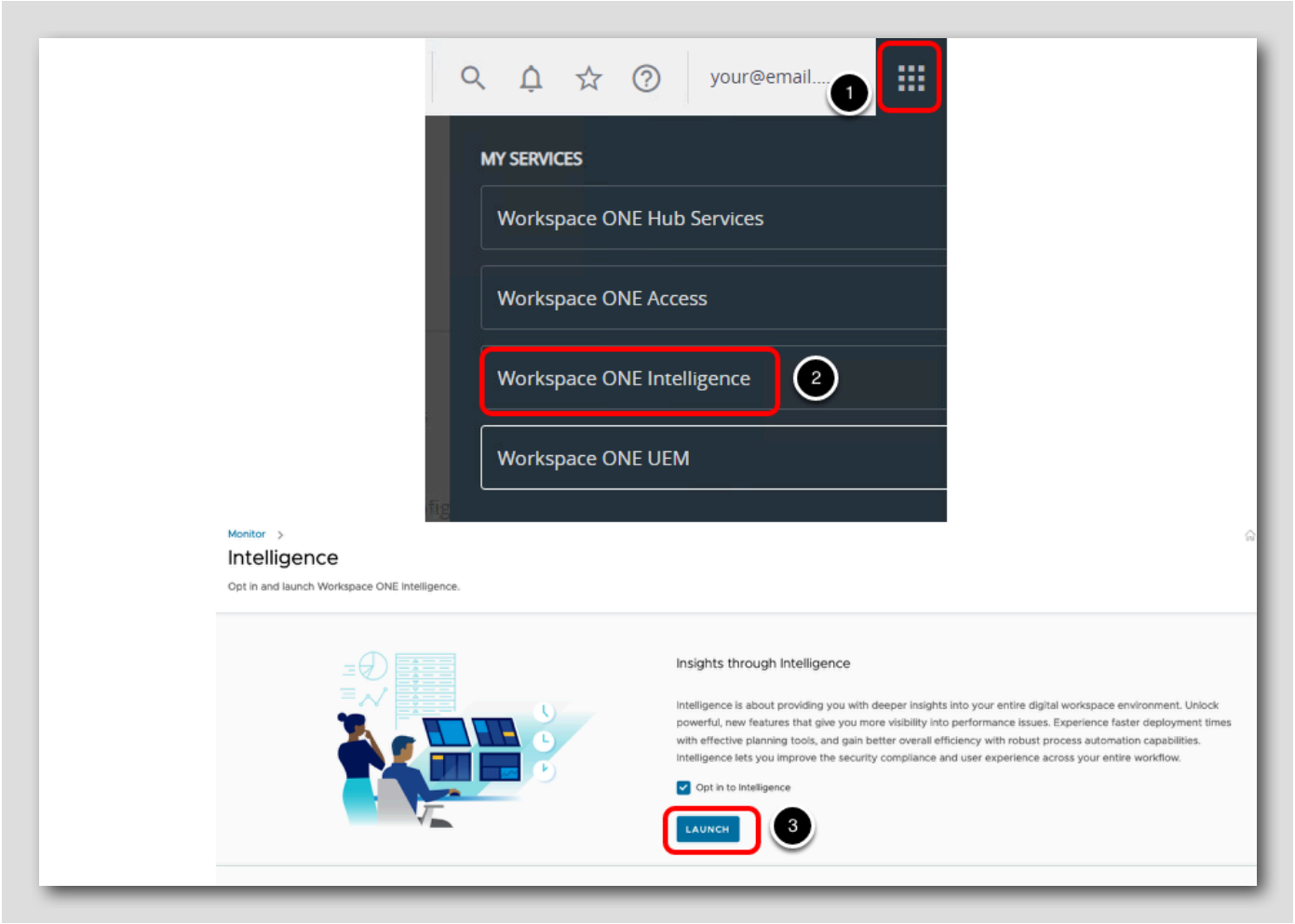


1. Hover the mouse over the **Low Battery Health** tag you just created.
2. The tag URL is displayed on the status bar of the browser—the tag ID is the **number** at the end of the URL. Manually enter the number into Notepad or copy it somewhere you can reference. This tag ID will be used as part of the automation action in the following steps.
3. Click **Close**.

Note: In the sample image, the tag ID is **10007** – your ID will differ.

Return to the Workspace ONE Intelligence Console

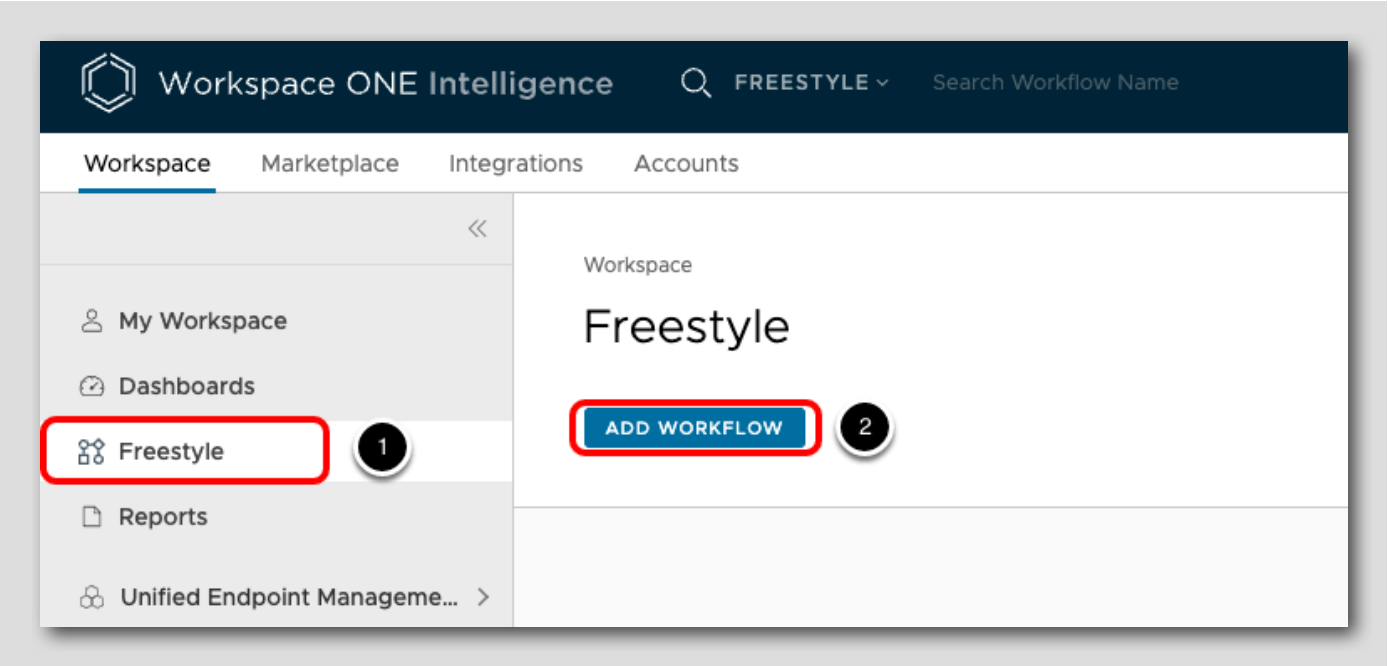
[582]



1. Click the **My Services** button.
2. Click **Workspace ONE Intelligence**.
3. Click **Launch**.

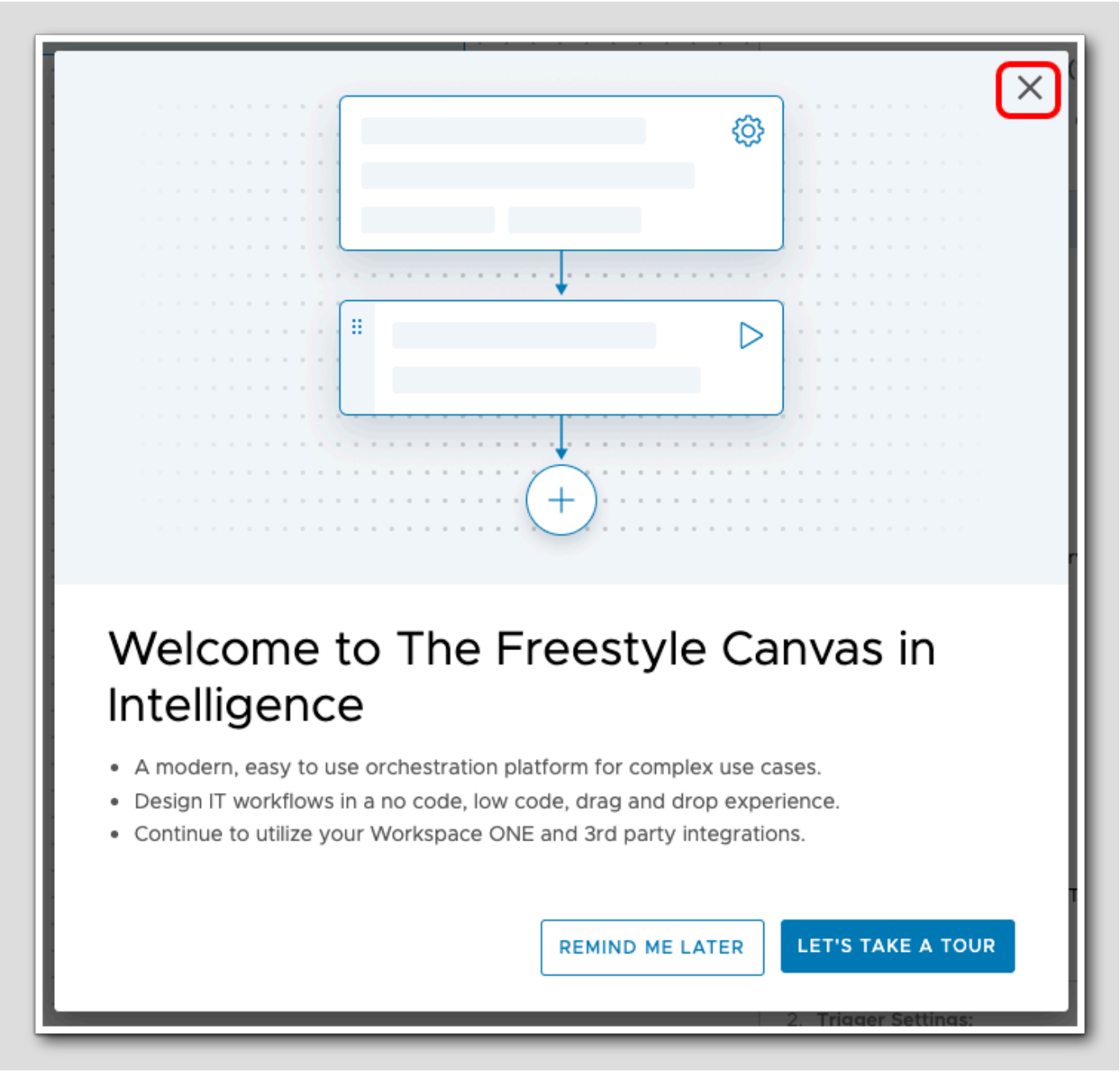
Open Freestyle Settings

[583]



In the Workspace ONE Intelligence console:

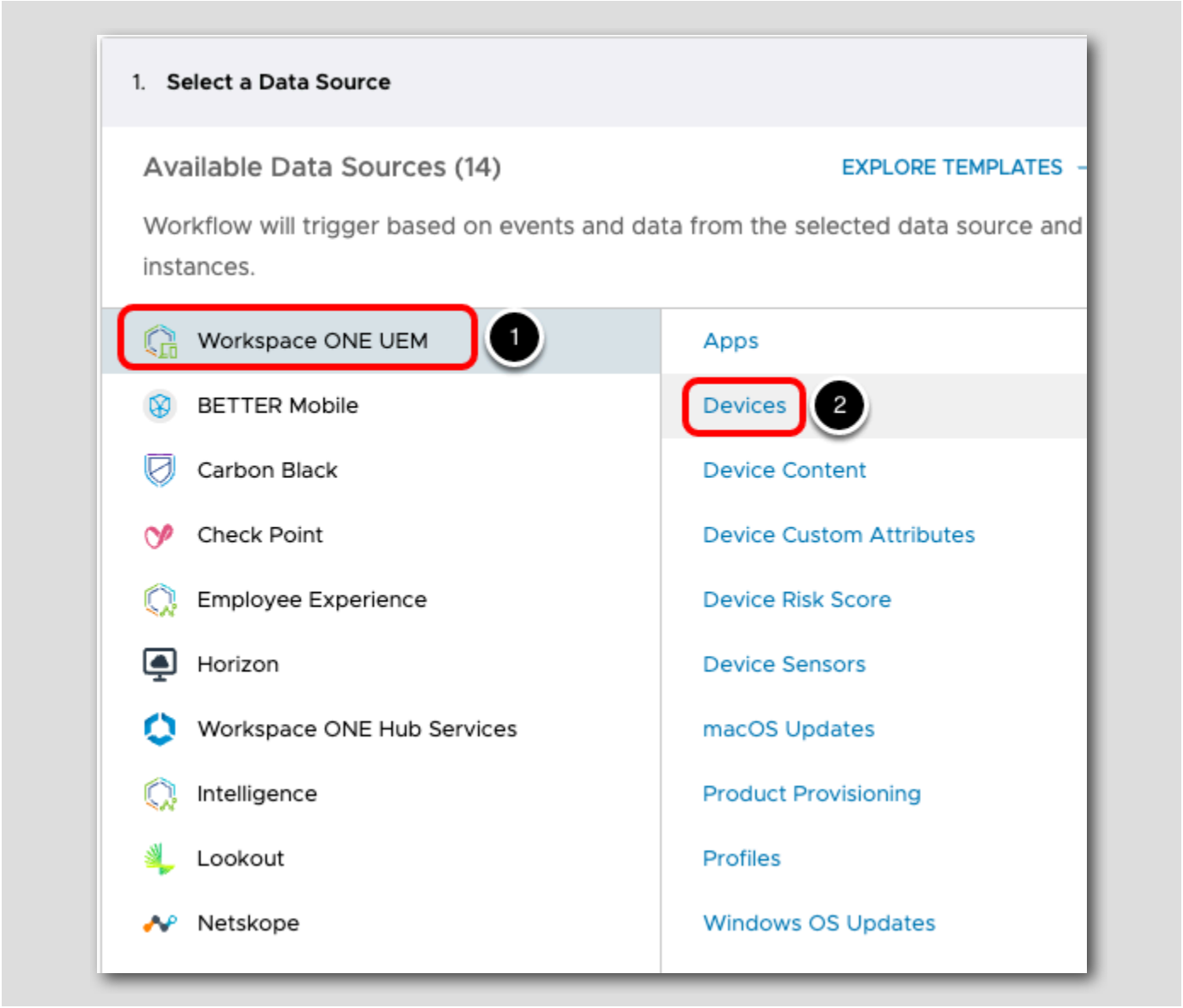
1. Click **Freestyle**.
2. Click **Add Workflow**.



1. Click the X in the upper right corner to close the Freestyle Canvas popup window.

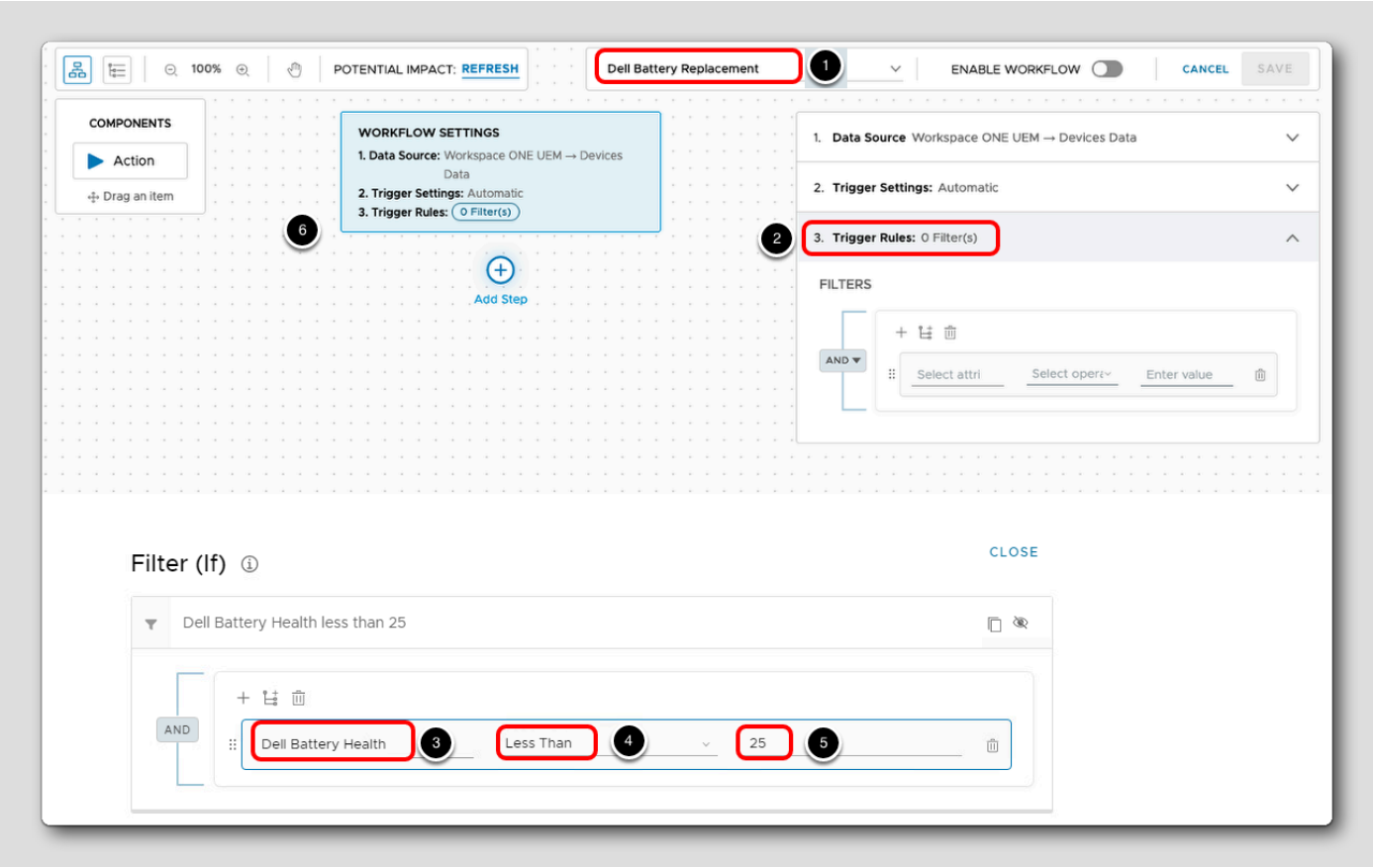
Select a Data Source

[584]



1. Navigate to **Workspace ONE UEM**.
2. Click **Devices**

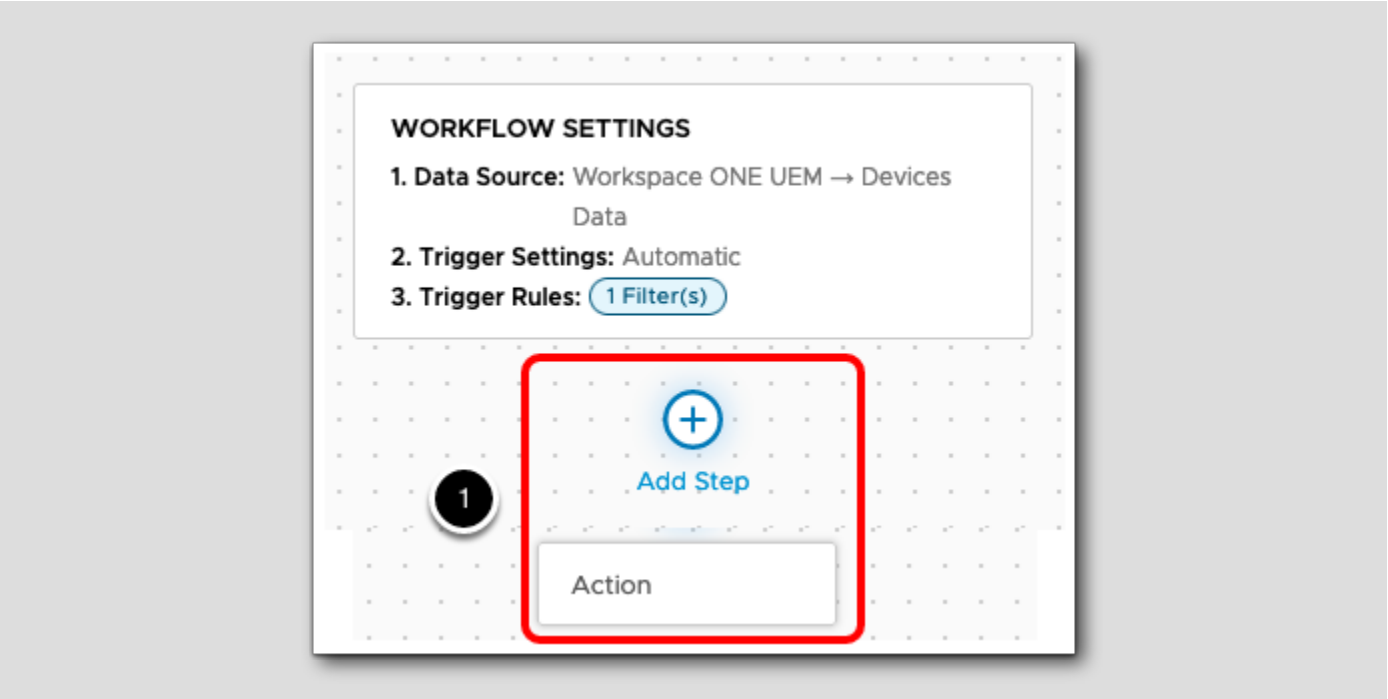
Define Automation Settings

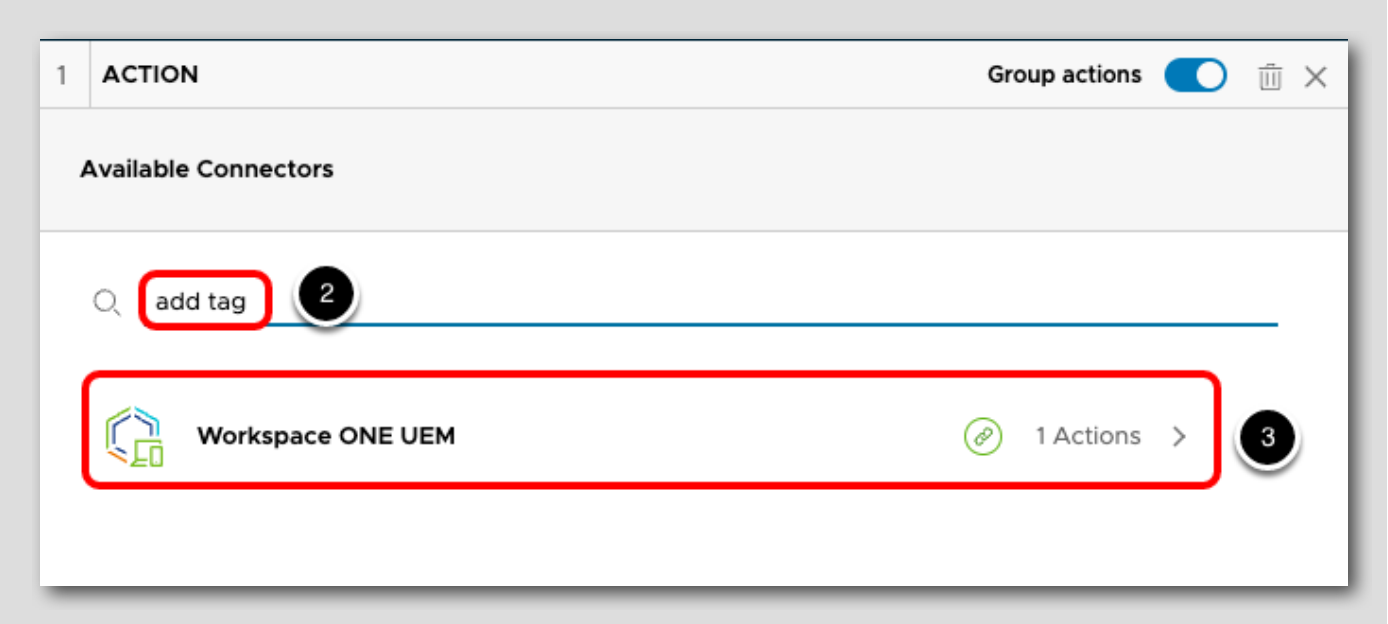


1. In the Name field, enter **`Dell Battery Replacement`**.
2. Select **Trigger Rules**.
3. Under **Filter**, select **Dell Battery Health**.
4. Select **Less Than**.
5. Enter **25**.

Add an Action

[586]

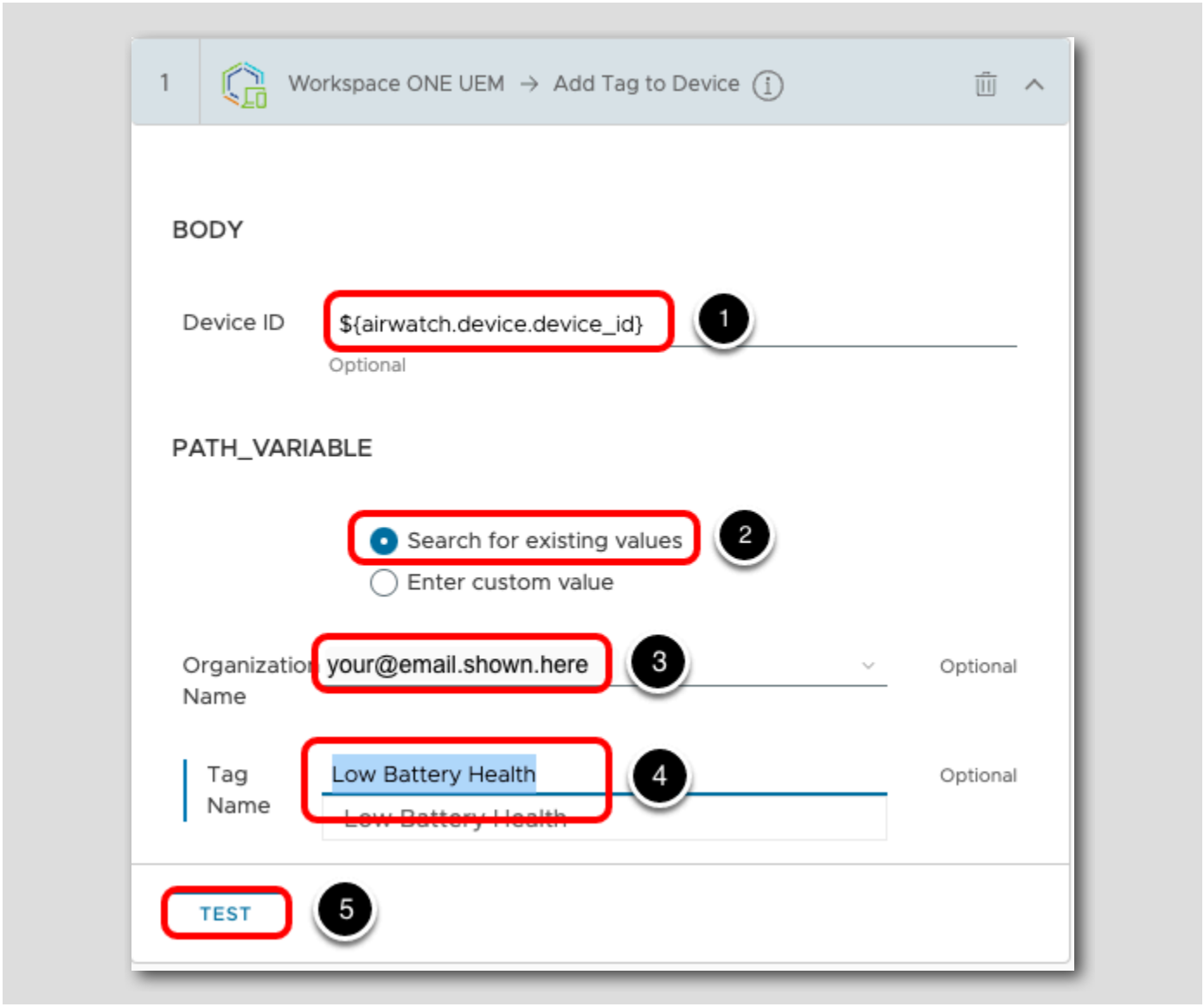




1. Select **Add Step** -> **Action**.
2. Enter **`add tag`** in the search field.
3. Select the **Workspace ONE UEM** -> **Add Tag to Device** result.

Configure Action Settings

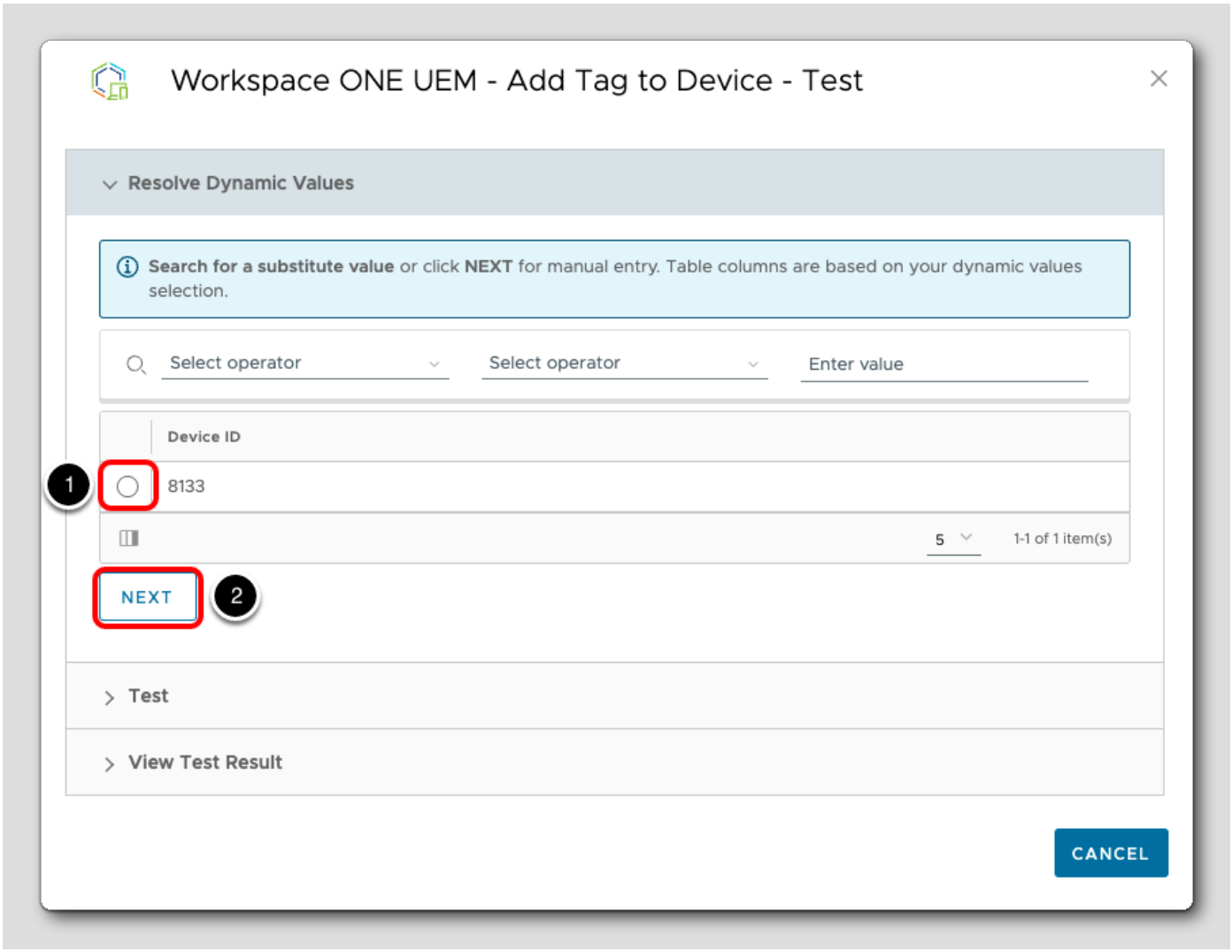
[587]



1. Leave the Device ID field as **`${device_id}`**
2. Change the Path Variables selection to **Search for existing values**.
3. Click the **Organization Name** field and select your organization name from the list. The organization name of your group will match your email address.
4. Click the **Tag Name** field and select the **Low Battery Health** tag from the list.
5. Click **Test**.

Test the Add Tag to Device Automation

[588]



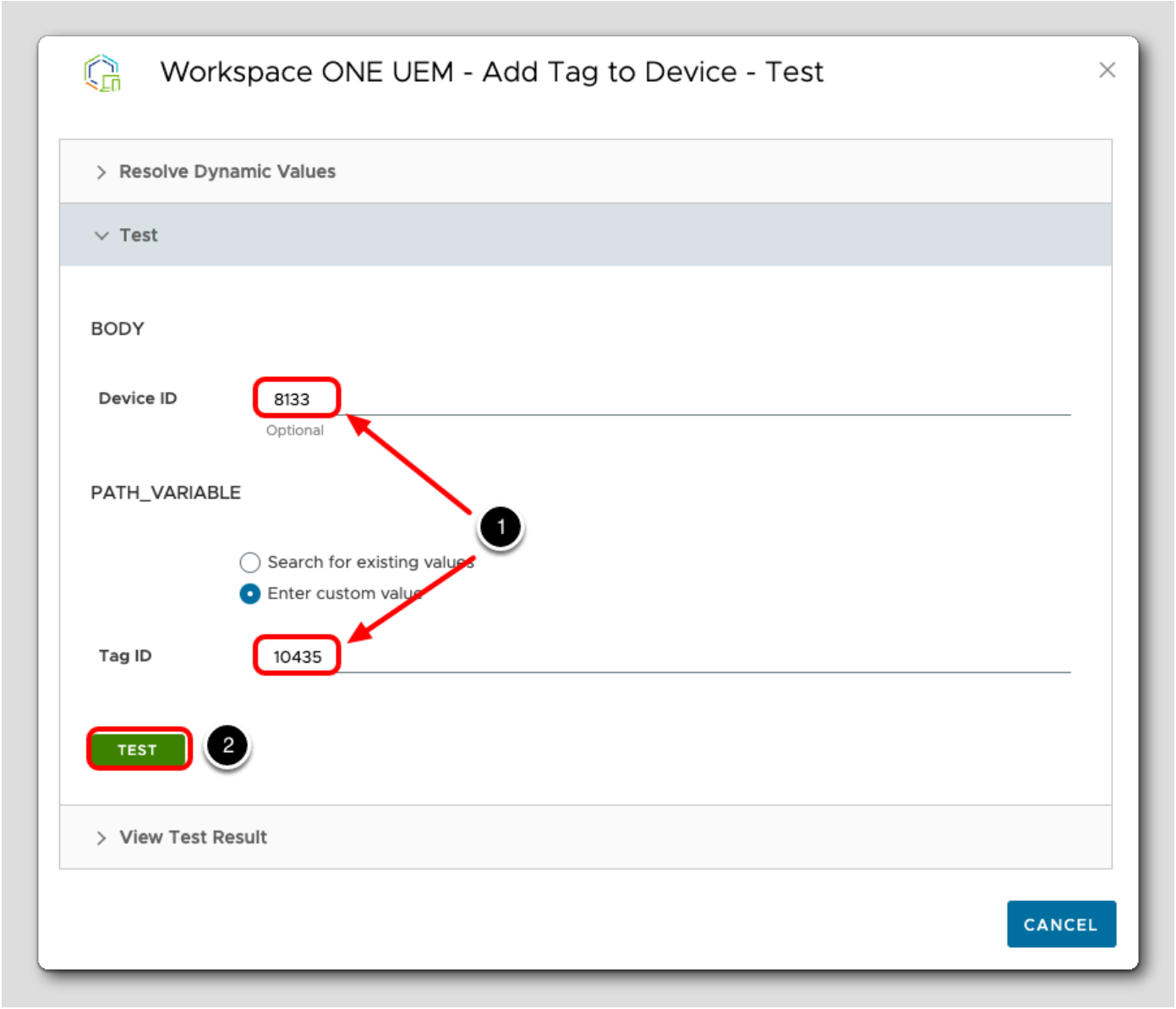
1. You will need to select a Device ID to substitute for the dynamic value **`${device_id}`** from the previous step. The single Device ID record correlates to the Windows 10 device you enrolled earlier, click to select it.

   NOTE: The Device ID shown here will differ from your environment.

2. Click **Next**.

Run the Test

[589]



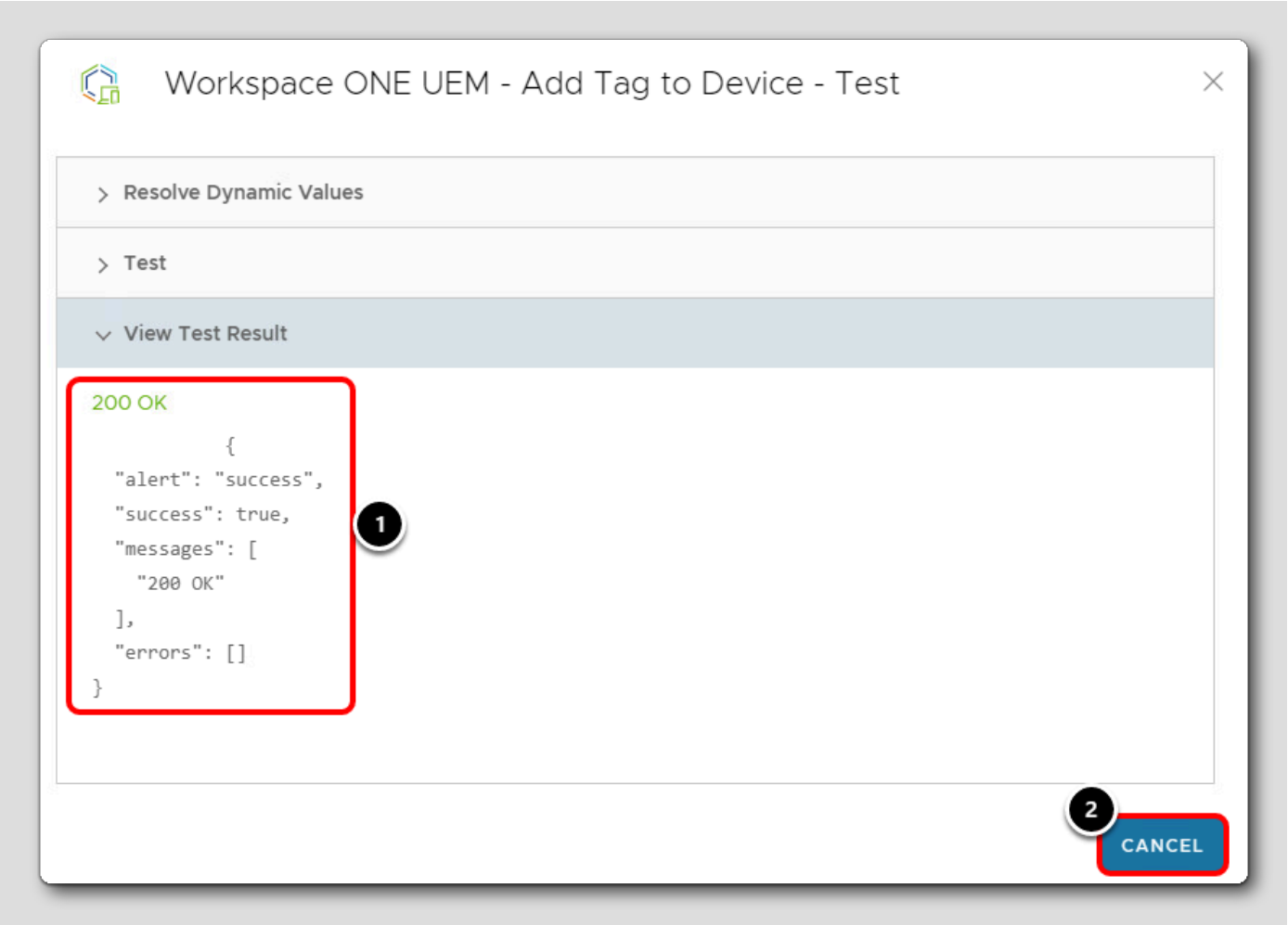
1. Notice that the Device ID and Tag ID values were replaced with the values from your Workspace ONE UEM environment.

   NOTE: The Device ID shown here will differ from your environment.

2. Click **Test**.

Confirm Test was Successful

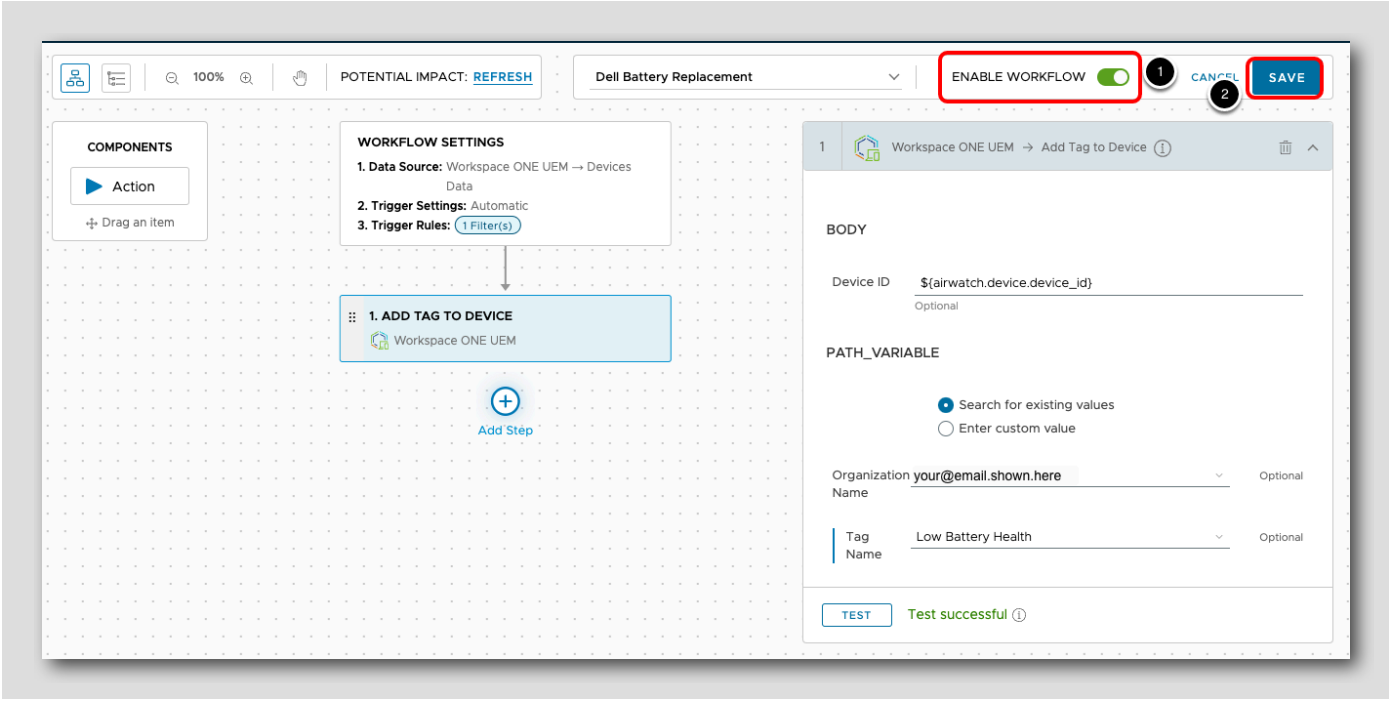
[590]



1. Confirm that the Test Results show **200 OK**.
2. Click **Cancel** to exit the automation test.

Save the Workflow

[591]

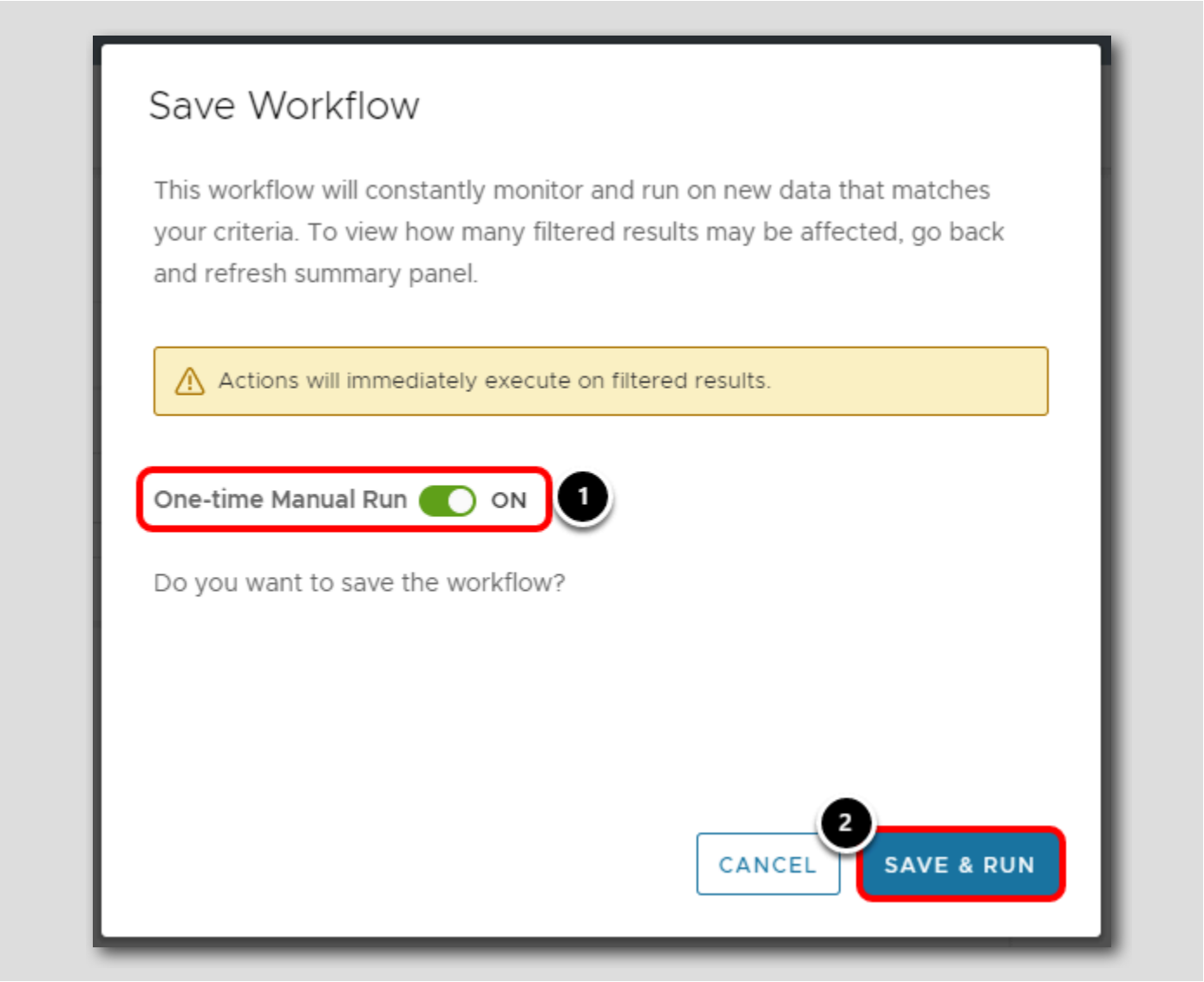


1. In the top right corner, toggle **Enable Workflow** on.
2. Click **Save**.

NOTE: This screenshot was taken from a sample environment. Your Filter Results will show 0 because the Dell Battery Health event does not apply to the Windows 10 virtual machine that was enrolled. When deploying the same automation to physical Dell devices, your affected devices would show here.

Save and Run Workflow

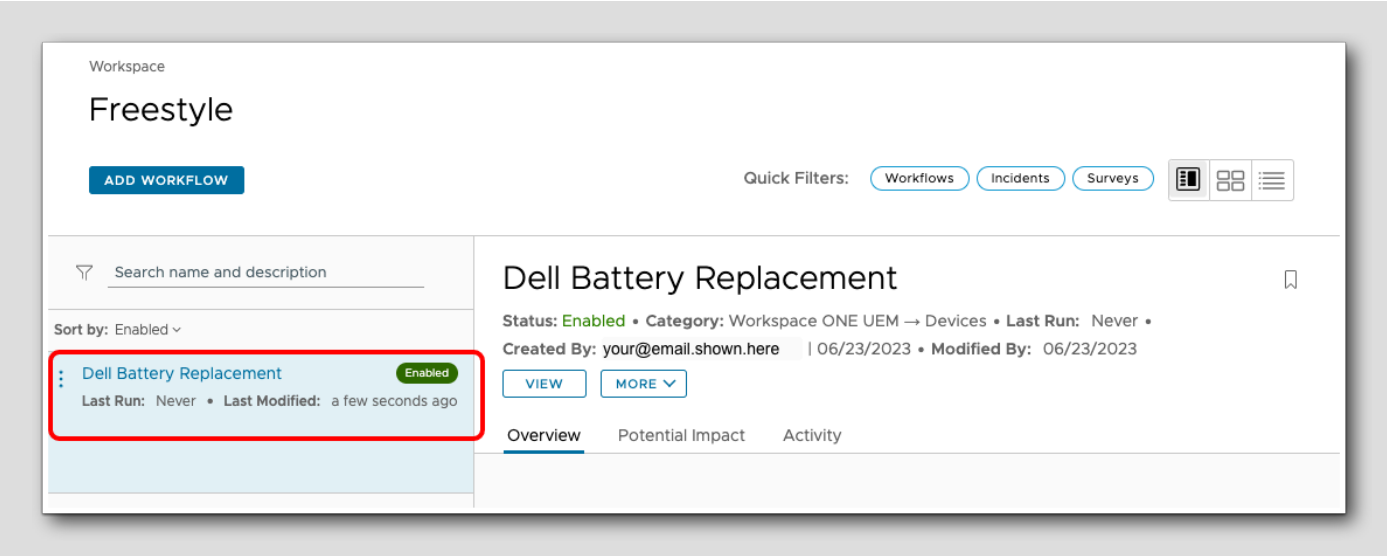
[592]



1. Toggle the **One-time Manual Run** option to on. This will immediately execute the workflow against the target devices.
2. Click **Save & Run**.

Confirm Automation is Created

[593]



Confirm that you can see the Dell Battery Replacement automation in the dashboard with a status of **Enabled**.

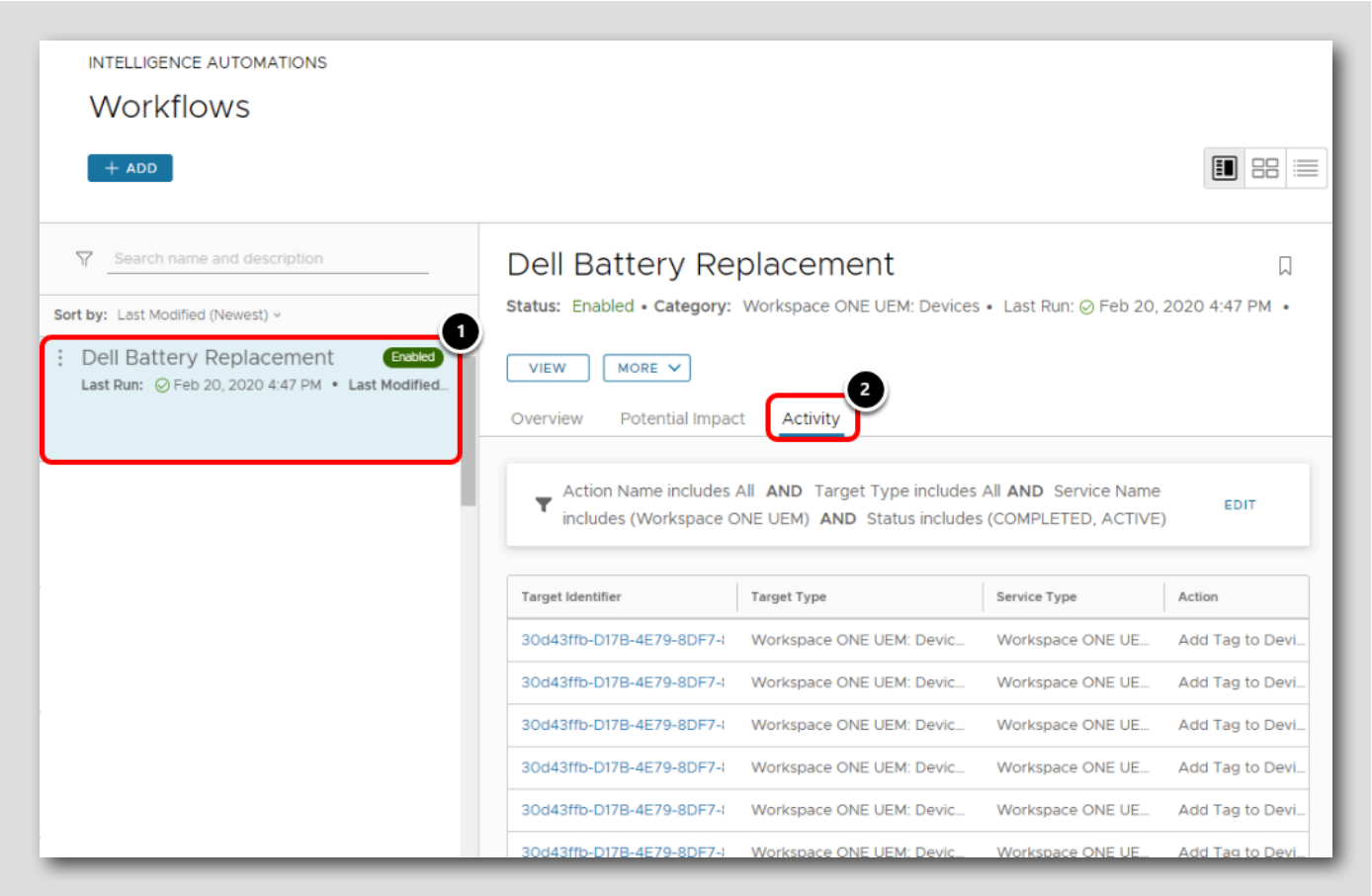
Reviewing Automation Events

[594]

After you have created an automation in the Workspace ONE Intelligence console, the configured actions begin to take effect and are recorded in the logs. In this activity, you will use the automation logs to review the automation events for Dell devices that need battery replacement.

Open the Log

[595]



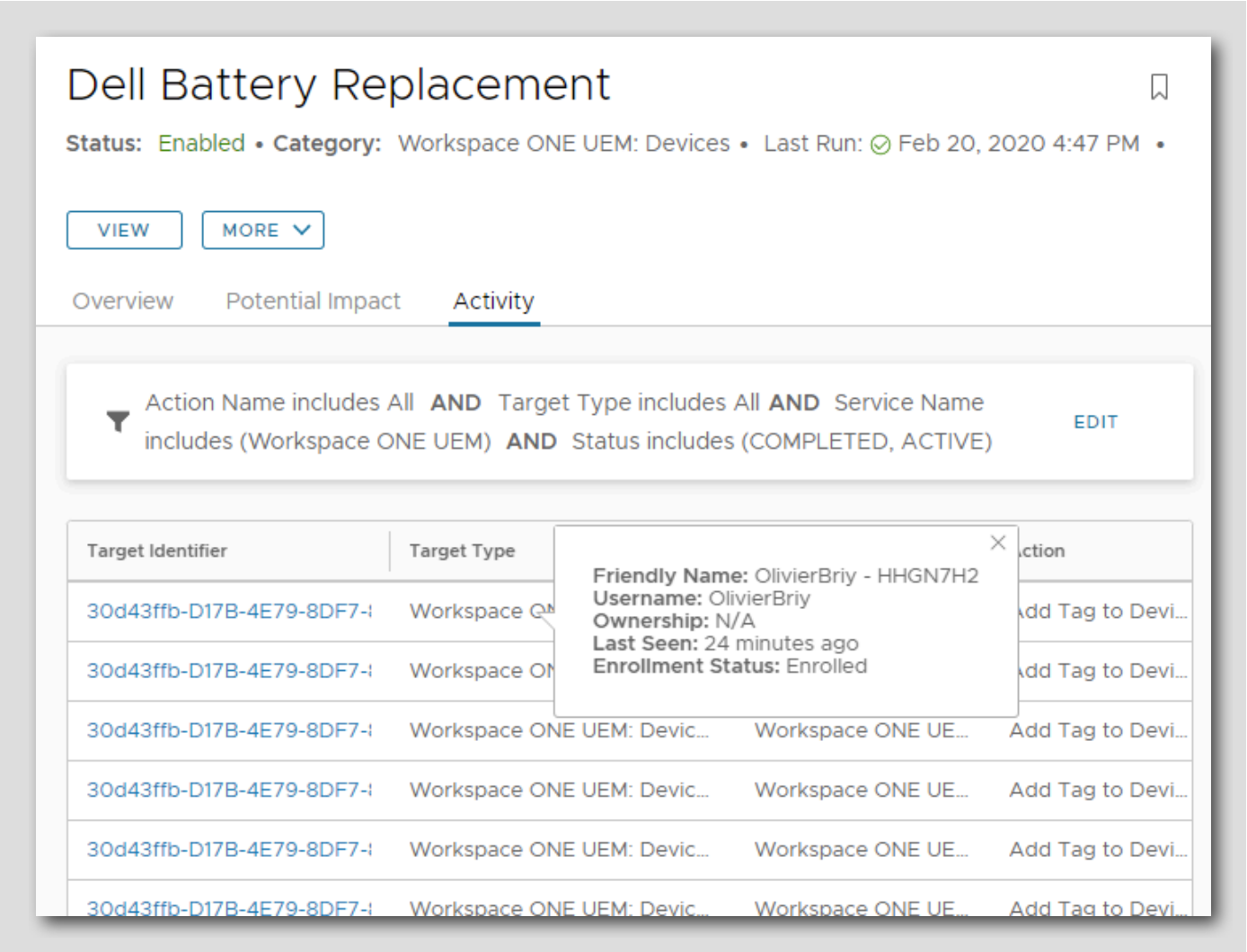
NOTE: The screenshot will differ from your environment because the Dell Battery Health event will not trigger for the Windows 10 virtual machine that was enrolled since it is not a physical Dell device. Refer to the screenshot for a sample of how this would appear in a real environment.

In the Automations Dashboard:

1. Click the **Dell Battery Replacement** workflow.
2. Select **Activity**.

Review the Log

[596]

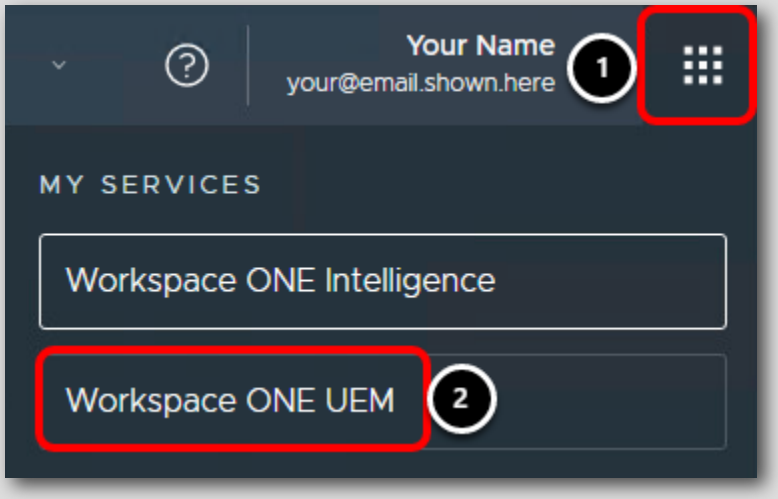


NOTE: The screenshot will differ from your environment because the Dell Battery Health event will not trigger for the Windows 10 virtual machine that was enrolled since it is not a physical Dell device. Refer to the screenshot for a sample of how this would appear in a real environment.

Depending on the battery health of the device you enrolled, the automation event you configured in this activity may or may not have been triggered. For this reason, the following screenshot is a sample from an unrelated log. It provides an example of multiple actions taken on different services.

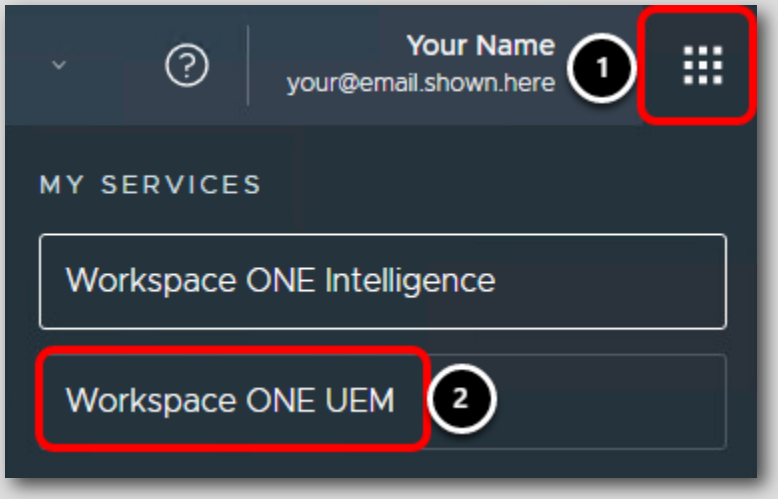
Return to the Workspace ONE UEM Console

[597]



In the top-right corner of the Workspace ONE Intelligence Console:

1. Click the **My Services** button
2. Click the **Workspace ONE UEM** button



Un-enrolling your Windows 10 Device

[598]

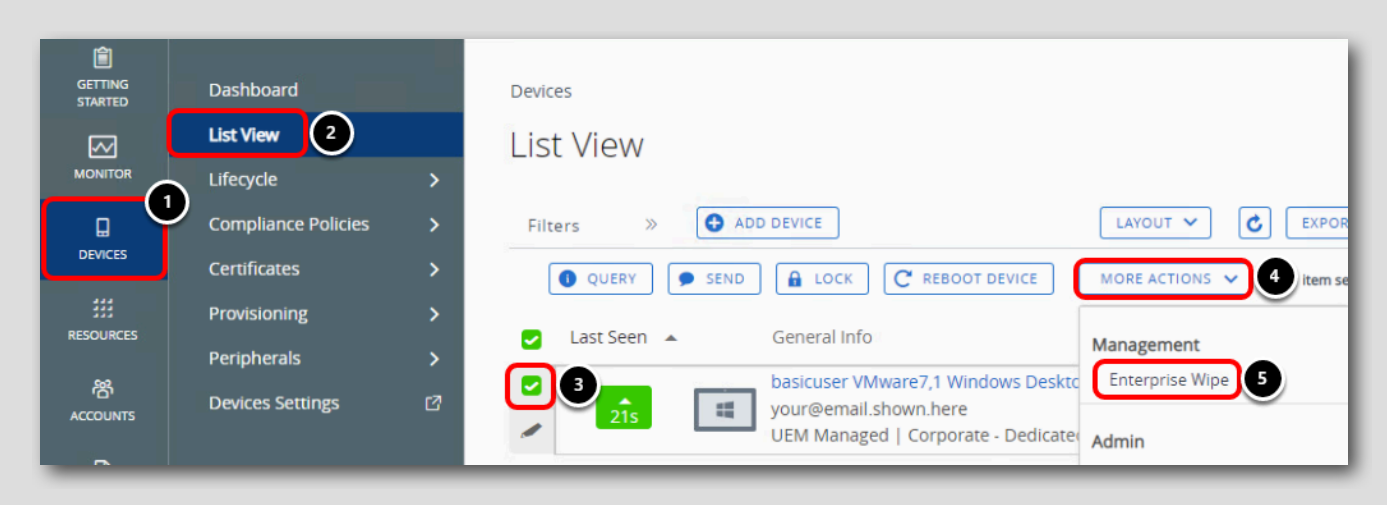
In this section, we are going to un-enroll our Windows 10 VM so that we can use it for other lab modules.

We will use the **Enterprise Wipe** wipe command to remove all of the managed content that was pushed to the device (such as profiles

and apps) by Workspace ONE while not modifying any personal content or data on the device.

Enterprise Wipe from Workspace ONE UEM Console

[599]

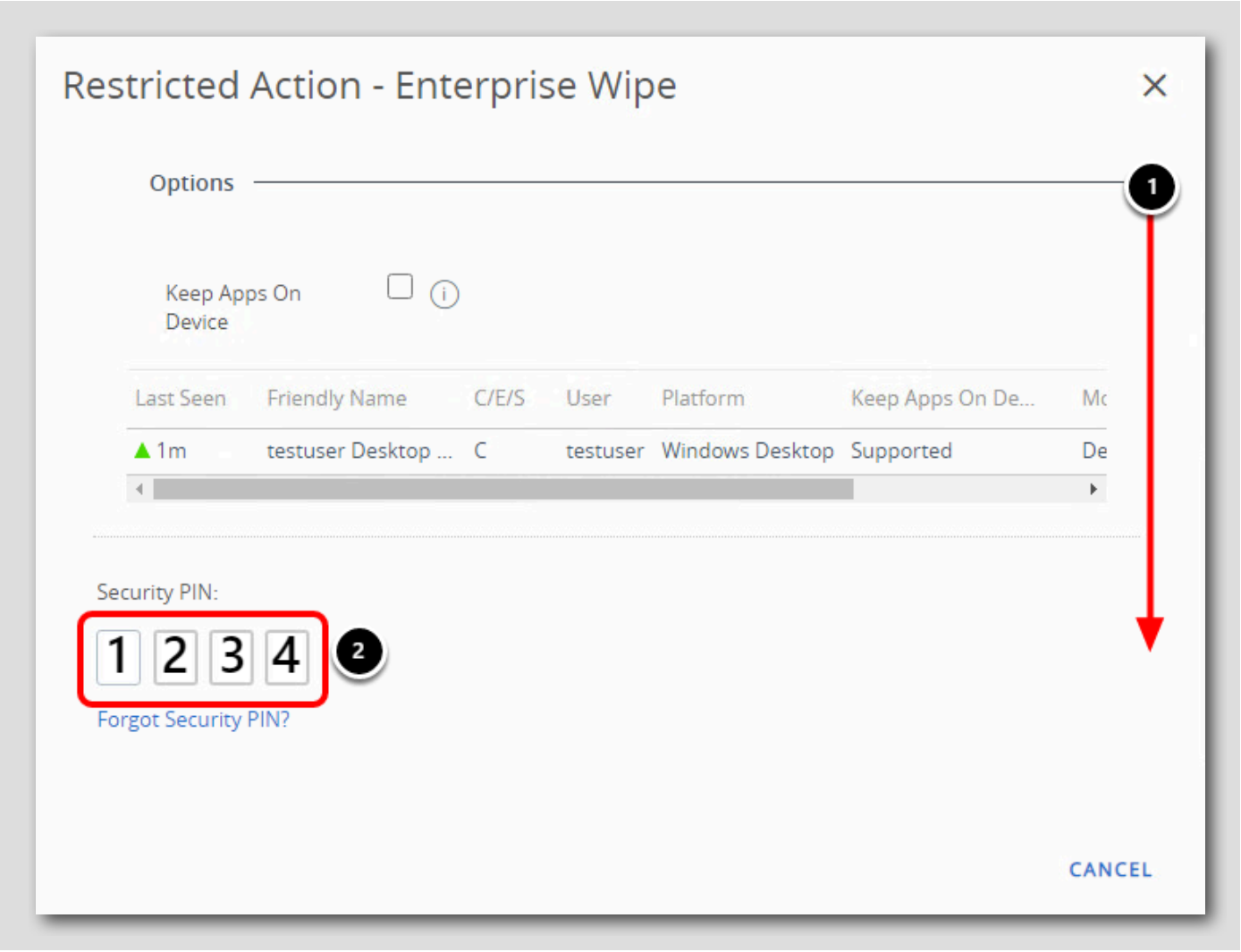


Return to the Workspace ONE UEM Administrator Console in Google Chrome,

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

Enter PIN and Enterprise Wipe Device

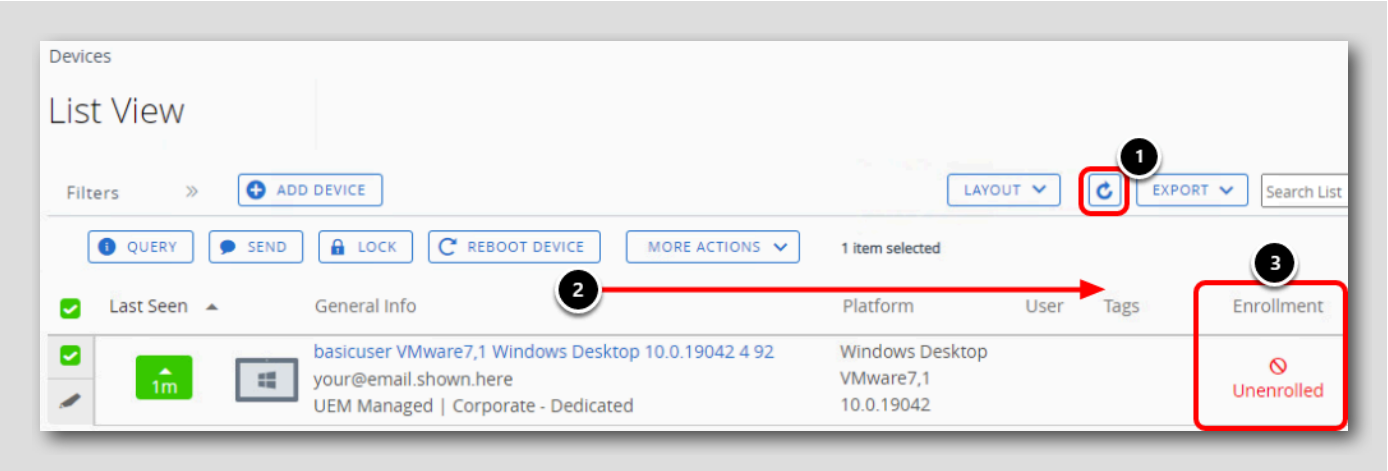
[600]



1. You may need to scroll down to find the Security PIN input
2. Enter the Security PIN that you created when you first logged into the Workspace ONE UEM administration console, which was **1234**. If you used a different PIN, enter that one instead.
3. Click **Delete**

Validate Enterprise Wipe

[601]

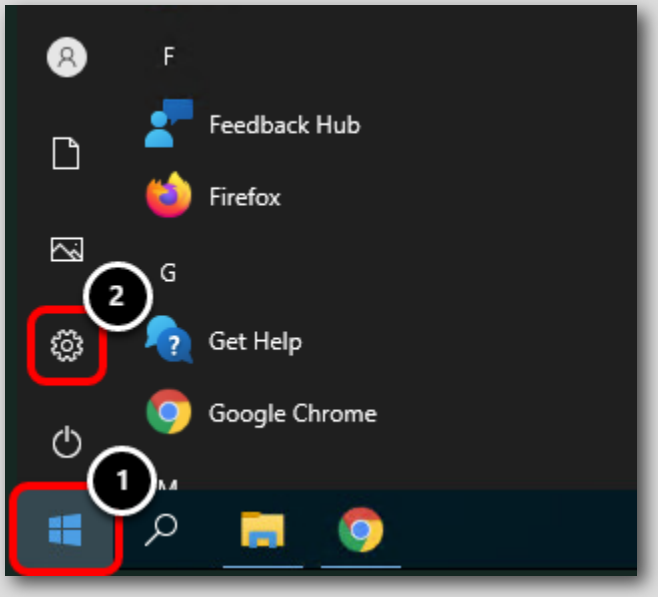


NOTE: The Enterprise Wipe may take several minutes to process.

1. Click the **Refresh** icon periodically to refresh the page to check if the Enterprise Wipe has processed
2. If needed, scroll to the right to find the Enrollment column
3. Notice that the Enrollment status for the device changes to **Unenrolled** once the Enterprise Wipe command is processed

Navigate to Windows 10 Settings

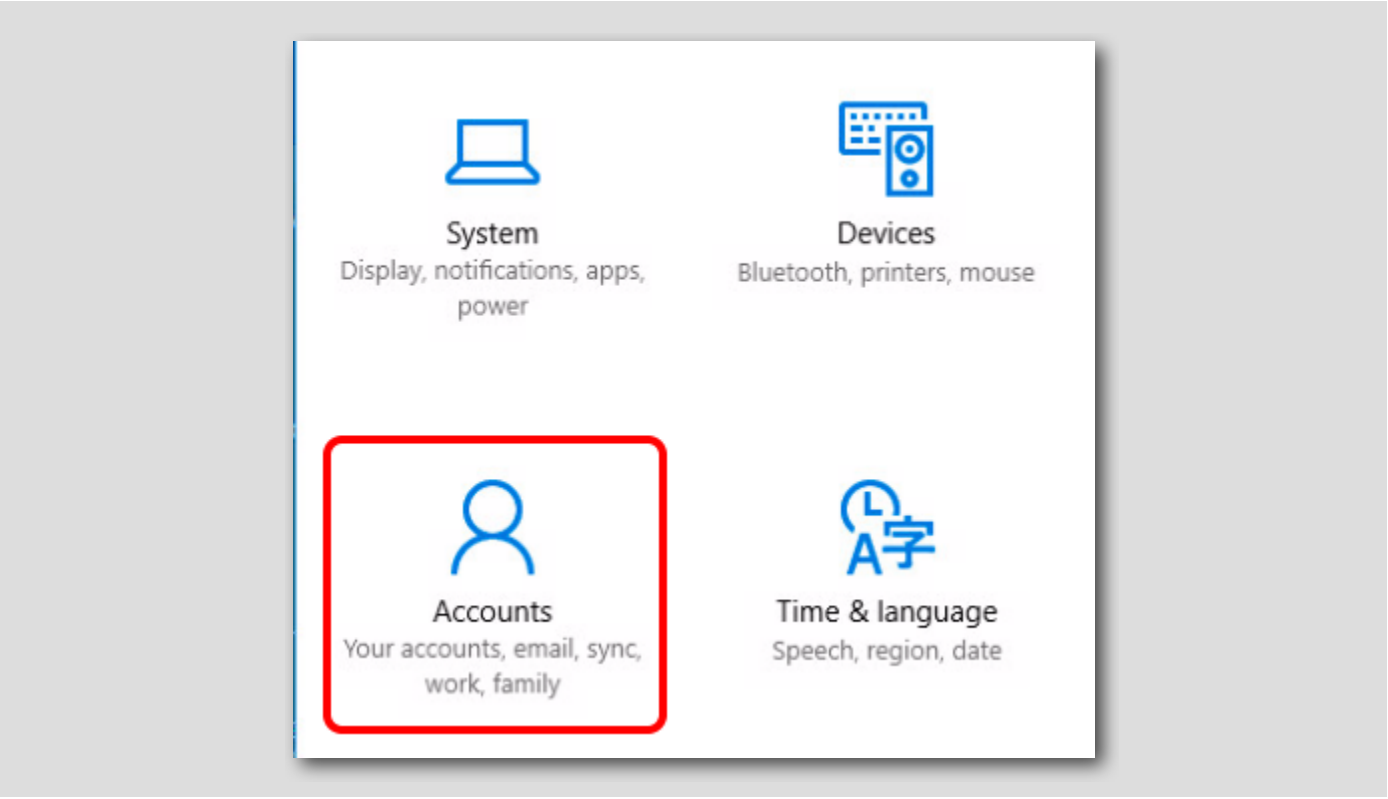
[602]



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

Access Accounts Settings

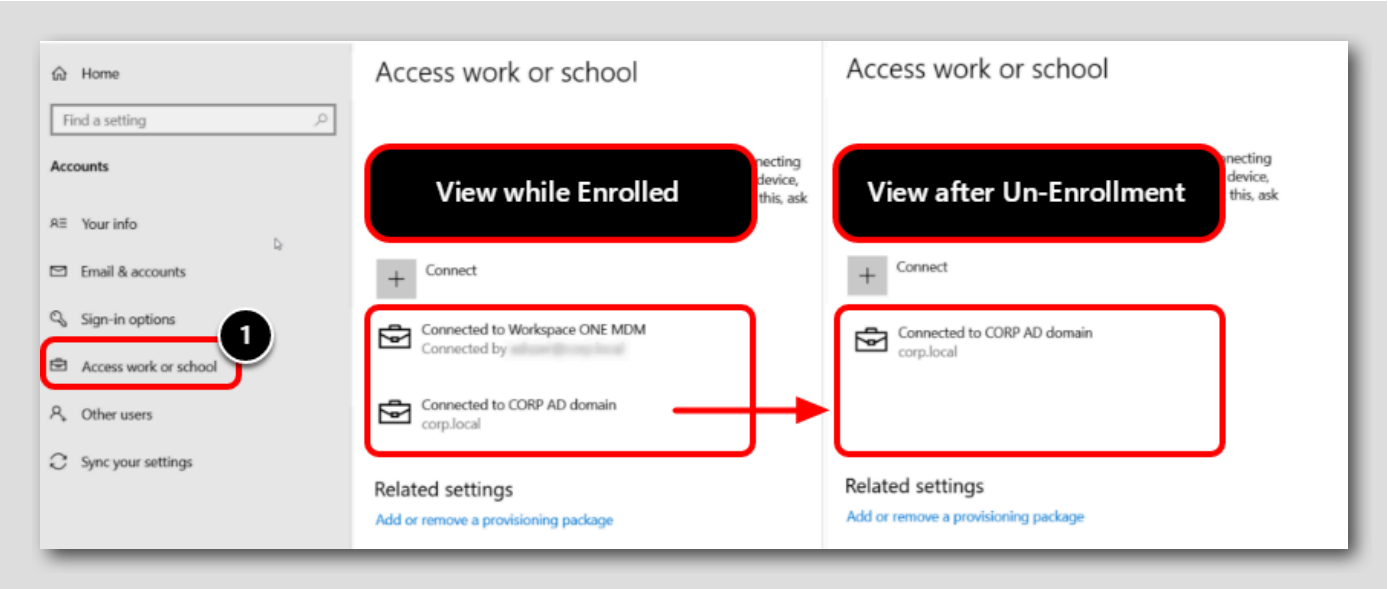
[603]



From the Settings Menu, access **Accounts**

Validate That No Management Account Exists

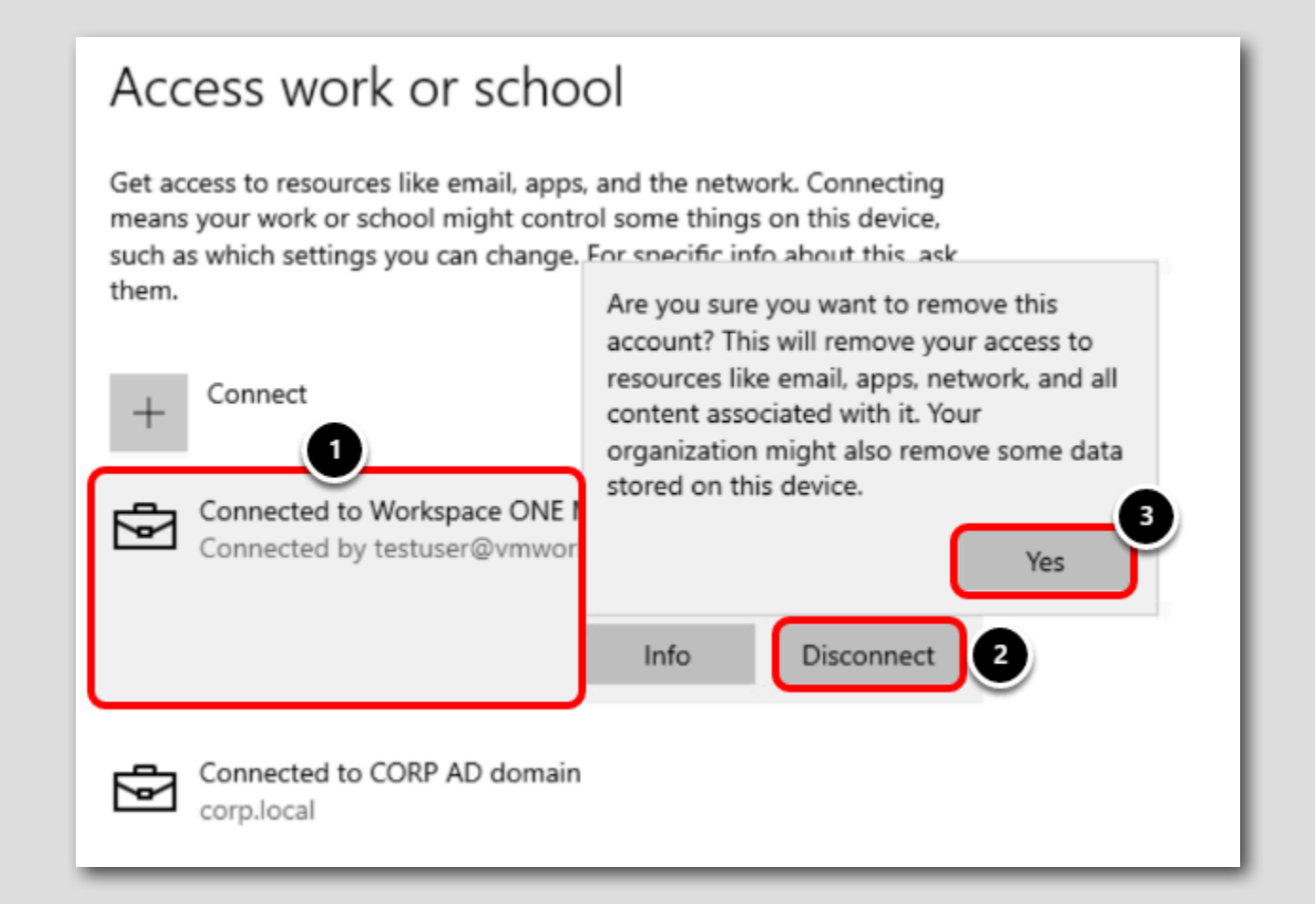
[604]



1. Click on Access work or school
2. Validate that you DO NOT see any account connected to Workspace ONE MDM.

NOTE: The CORP AD domain is the local domain in this lab and is not controlled by Workspace ONE UEM Enrollment, so you will see this connection when your device is enrolled or unenrolled.

NOTE: If the Access Work or School page was opened from earlier, you may need to refresh or navigate away from the page and return to see the changes.



1. Click the **Connected to Workspace ONE UEM** account
2. Click **Disconnect**
3. Click **Yes**

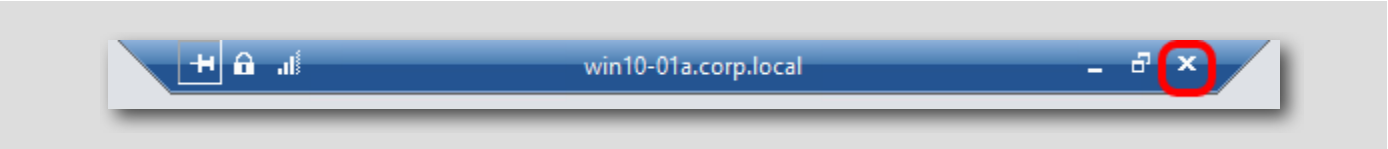
Return to the Main Console

[605]

Click **Close (X)** on the Remote Desktop Connection bar at the top of the screen to return to the Main Console to finish making configurations within the Workspace ONE UEM Console.

NOTE: If the Remote Desktop Connection bar is not visible, you may have unpinned it. Hover your mouse of the top of the screen to

display the Remote Desktop Connection bar again, then click close.



Summary

[606]

In this module, you've learned how to:

- Create automated reports that share relevant information to interested parties, and eliminate manual steps for the IT Team.
- Add Widgets to Dashboards that show Total Enrollments over time.
- Predict battery failures and automate replacement tagging for Windows 10 Dell devices.
- Leverage integration with 3rd party services, like ServiceNow, to trigger automated actions.

To learn more about additional use cases where you can leverage Workspace ONE Intelligence, please review the following resources:

- VMware Workspace ONE Digital Employee Experience (DEX) Solution Overview
- Digital Employee Experience Management Whitepaper
- Digital Employee Experience (DEX) Solution Architecture
- Workspace ONE Intelligence and VMware Carbon Black: Automating Device Quarantine - Feature Walk-through
- VMware Workspace ONE Intelligence: Connectors - Feature Walk-through
- Workspace ONE Intelligence: Understanding Risk Analytics - Deep Dive
- How VMware IT Uses Workspace ONE Intelligence - VMware on VMware

For additional resources and information on Workspace ONE Intelligence, be sure to check out the VMware Workspace ONE Intelligence pages:

https://www.vmware.com/products/workspace-one/intelligence.html

https://www.vmware.com/products/workspace-one/digital-employee-experience-management.html

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

[607]

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 7 - Introduction to Freestyle Orchestrator (30 minutes) Beginner

Introduction [609]

Device management is continuously evolving, and this rapid evolution has directly impacted the IT administrator experience. *VMware Workspace ONE® UEM* has been following every step of this journey, evolving and innovating with every release, allowing administrators to manage cross-platform devices to enable a true Digital Workspace experience. To continue that innovation journey, we are announcing **Freestyle Orchestrator**.

Freestyle Orchestrator enables Workspace ONE UEM administrators to create complex workflows that fit specific requirements with flexibility and speed. Freestyle workflows can be used to set up resources such as applications, profiles, sensors, and scripts. These workflows use conditions to apply resources to devices based on granular criteria.

What Problem Does Freestyle Orchestrator Solve? [610]

The current method to provision resources (profiles, applications, content, scripts, and so on) over-the-air based on MDM APIs started with mobile platforms and later extended to desktops, such as Windows 10, macOS, and Chrome OS. The management experience on each platform has specific needs; overall, administrators want to control the provisioning process, such as controlling the sequence in which resources are deployed on the device and defining conditions based on the current resource state and external conditions that require specialized scripts.

There is a lot of complexity behind the scenes to deliver the desired management experience on desktop platforms. The provisioning process requires knowledge across Workspace ONE and external tools, such as coding. Freestyle Orchestrator simplifies this process and allows administrators to define complex workflows in a very effective way visually.

Defining the Use Case

[611]

A better understanding of the use case and requirements will help to organize the resources in Workspace ONE UEM and define the workflow. The workflow becomes a logical way to achieve a goal, which can evolve as new use cases emerge from business needs.

Consider a Windows 10 device - Application use cases where you must provision applications in a specific order or conditions; where certain Applications must be deployed first, before other applications.

The business requirements look simple; however, when we translate them into technical requirements, they map to profiles with different types of payloads (restrictions, certificates, custom settings, and so on), applications, specialized scripts, conditions to validate the resource state, and more.

The use case in this example translates into the following functional requirements:

- Deploy Zoom Client for Meetings - Automatic for Users
- Deploy Zoom Plugin for Microsoft Outlook - Optional
- Deploy and configure Outlook plugins like Zoom Meetings only when Microsoft Office AND Zoom Client are installed.

You must configure the Profiles and Applications resources in advance and as per the following list to be used as part of the workflow:

- Set Applications to *on-demand* deployment. Resources set as *automatic* are provisioned outside the workflow.
- Application resources must contain at least one assignment rule for default policy. However, resources provisioned by the workflow use the smart group assigned to the workflow.

If a resource such as an application or a profile is assigned to a device and configured for automatic deployment, in addition to being assigned to the device as part of a workflow, the resource will be installed based on whichever command is processed by the device.

Administrators access the Freestyle Orchestrator Designer through the Workspace ONE UEM Console.

DO NOT Enroll Personal Windows 10 Devices

[612]

IMPORTANT: You SHOULD NOT enroll a personal Windows 10 device for the upcoming exercise! Personal devices may be enrolled into other EMM providers which can cause undesired conflicts and issues.

Please follow the upcoming steps to enroll and use the provided **Win10-01a virtual machine** for this Hands-on Lab.

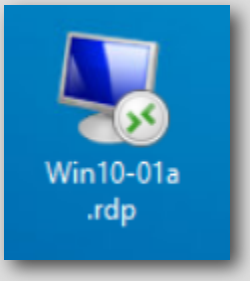
IMPORTANT: You SHOULD NOT enroll any personal device(s) for the upcoming exercise!

Personal devices may be enrolled into other UEM providers which can cause undesired conflicts and issues. - We want to avoid this!

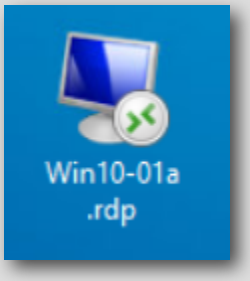
To complete this lab, we recommend you use a test device ONLY and avoid enrolling personal devices in the lab.

Connect to the Windows 10 Virtual Machine

[613]



Double-click the **Win10-01a.rdp** shortcut located on the Main Console Desktop to connect to the Windows 10 virtual machine.



Login to the Workspace ONE UEM Console

[614]

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

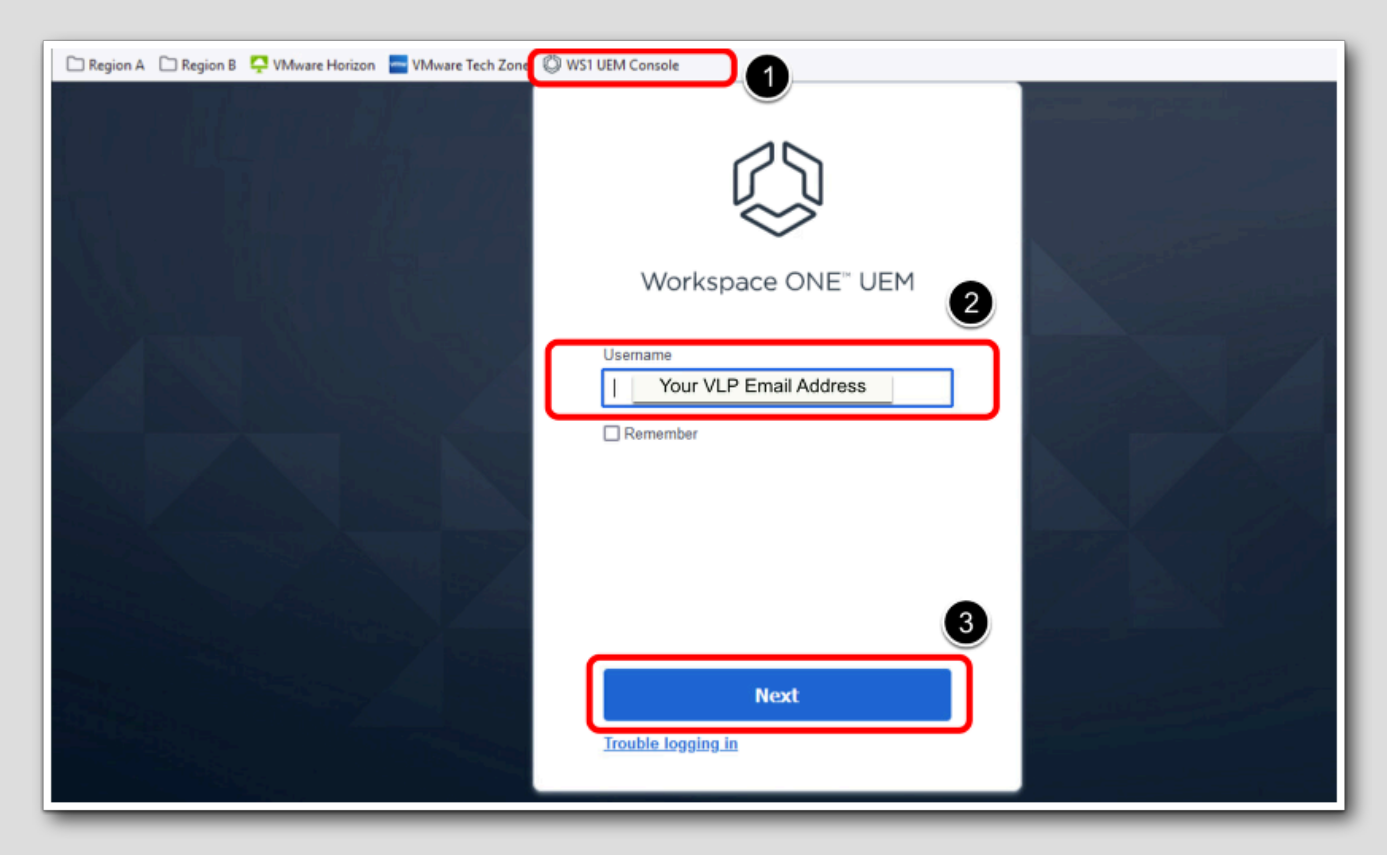
Launch Firefox Browser

[615]

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

[616]

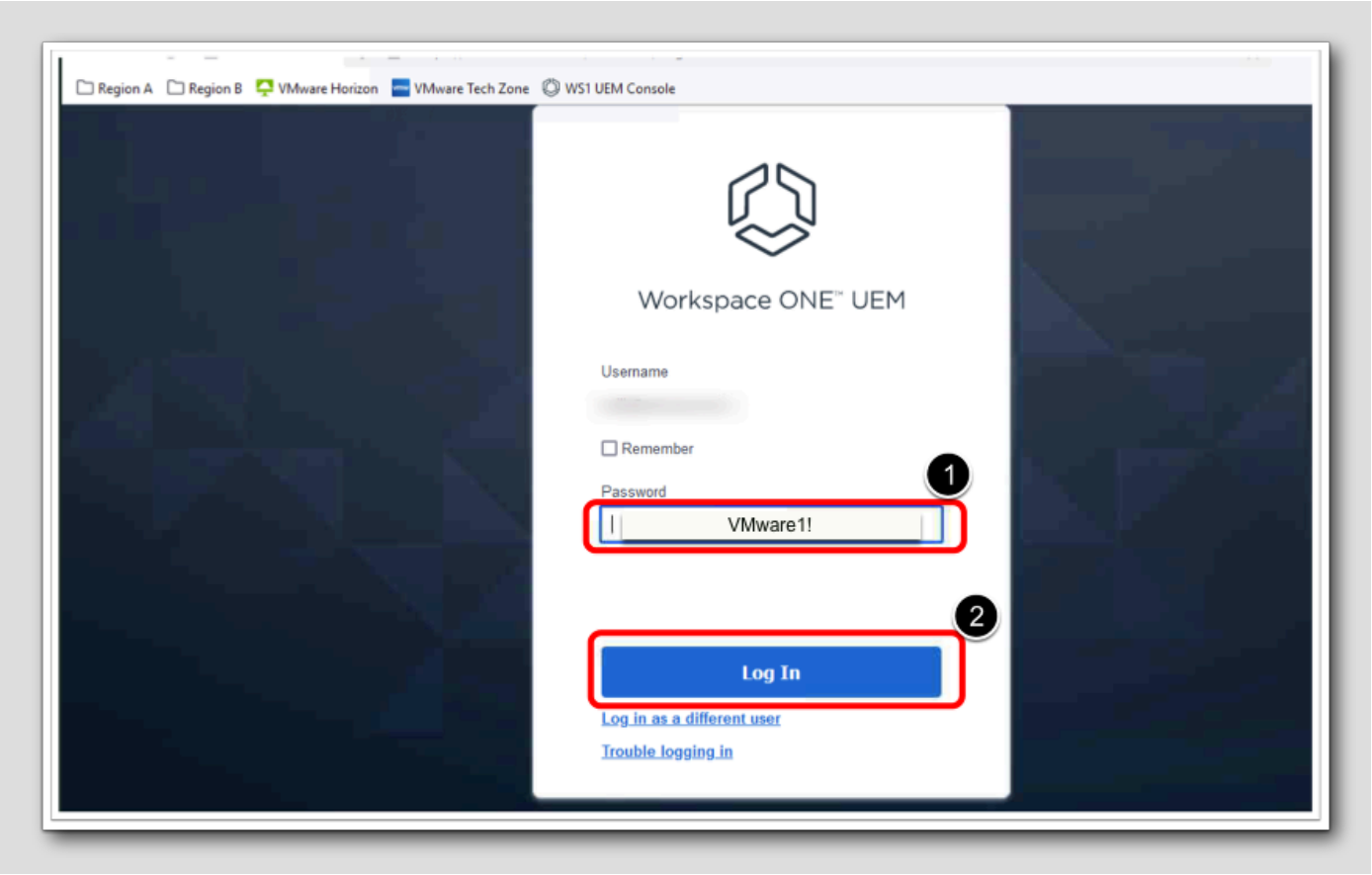


1. Select the **WS1 UEM Console** link from the Bookmark Toolbar
2. Enter your **Username**. This is the **email address** that you have associated with your **VMware Learning Platform (VLP)** account that you utilized to take Hands-on Labs.
3. Click **Next**, then advance to the next step of the lab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

[617]



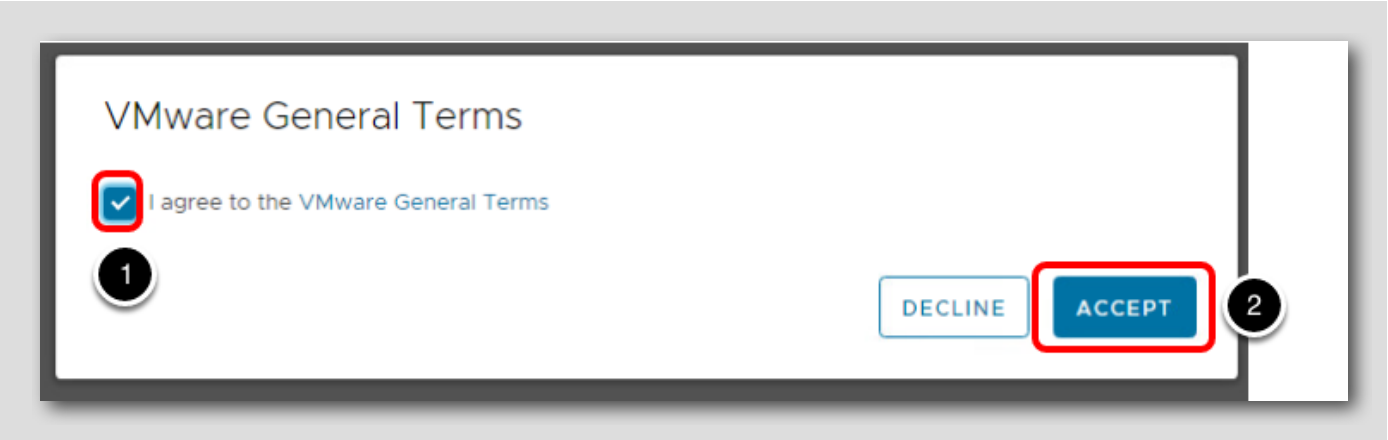
The password field will be displayed after entering your username.

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

[618]



You will be presented with the VMware General Terms.

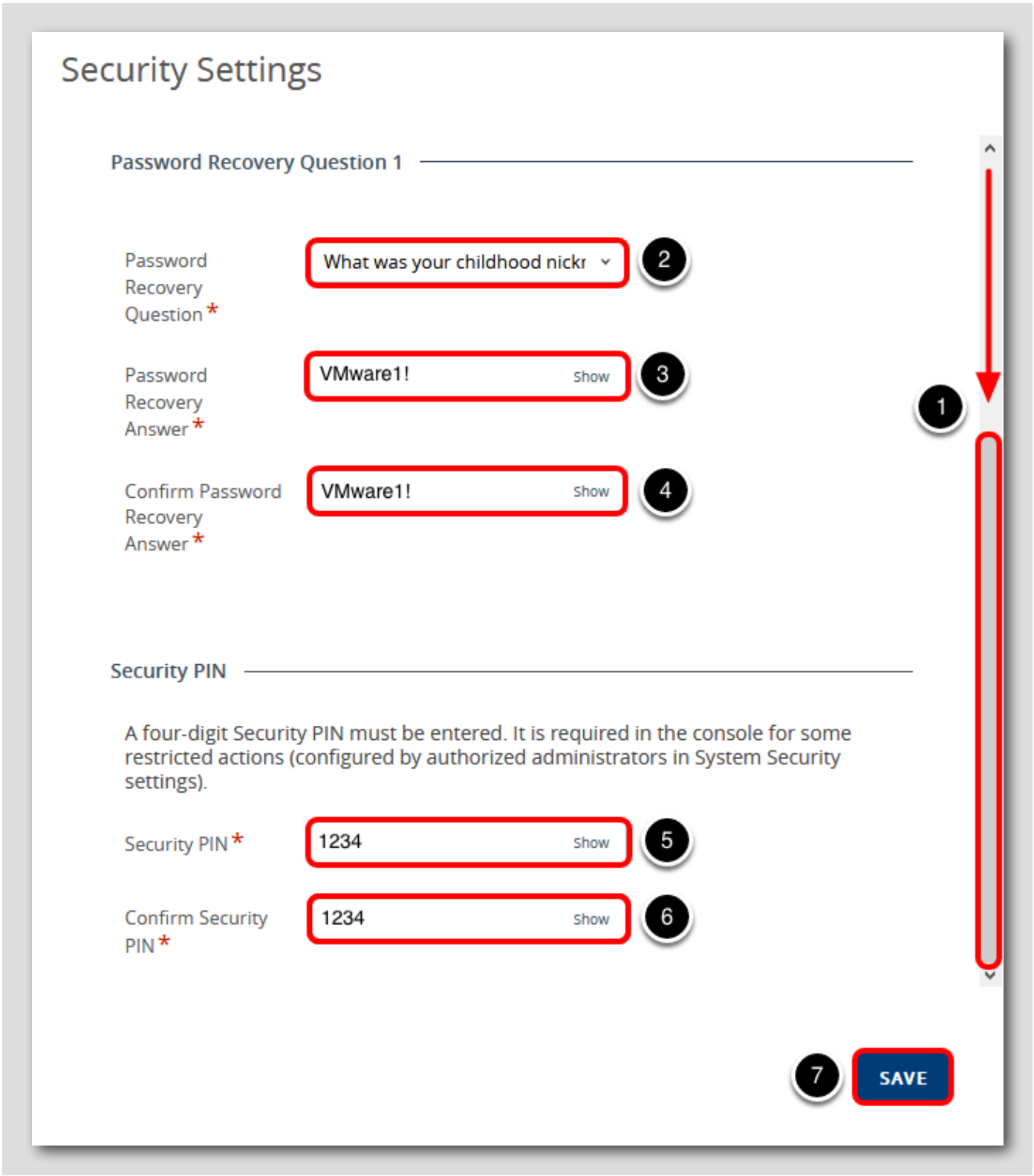
1. Select the box next to I Agree to the VMware General Terms.
2. Click the **Accept** button.

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

[619]

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

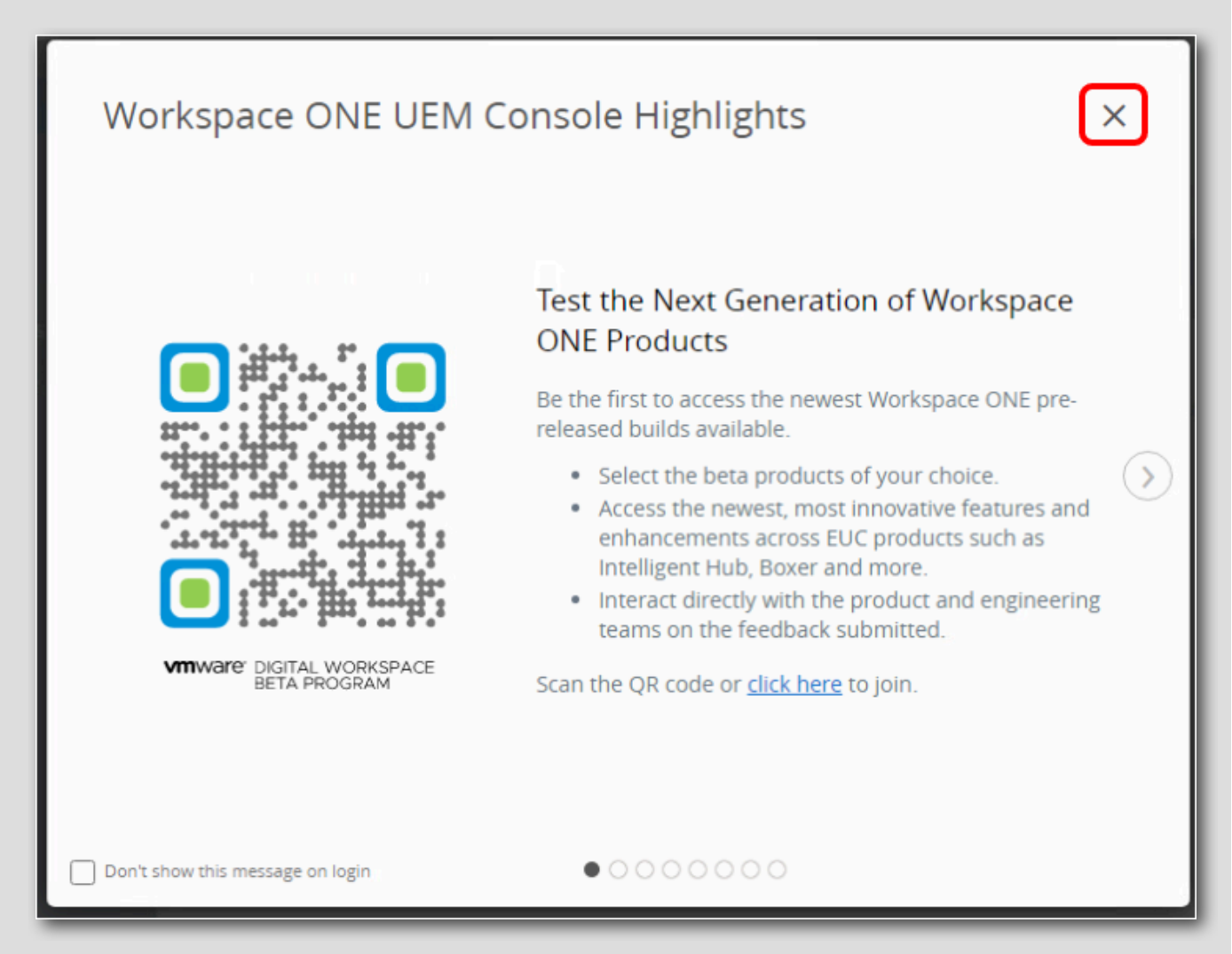

Security Settings
Password Recovery Question 1
Password Recovery Question *
What was your childhood nickr
2
Password Recovery Answer *
VMware1!
Show
3
1
Confirm Password Recovery Answer *
VMware1!
Show
4
Security PIN
A four-digit Security PIN must be entered. It is required in the console for some restricted 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

[620]



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.

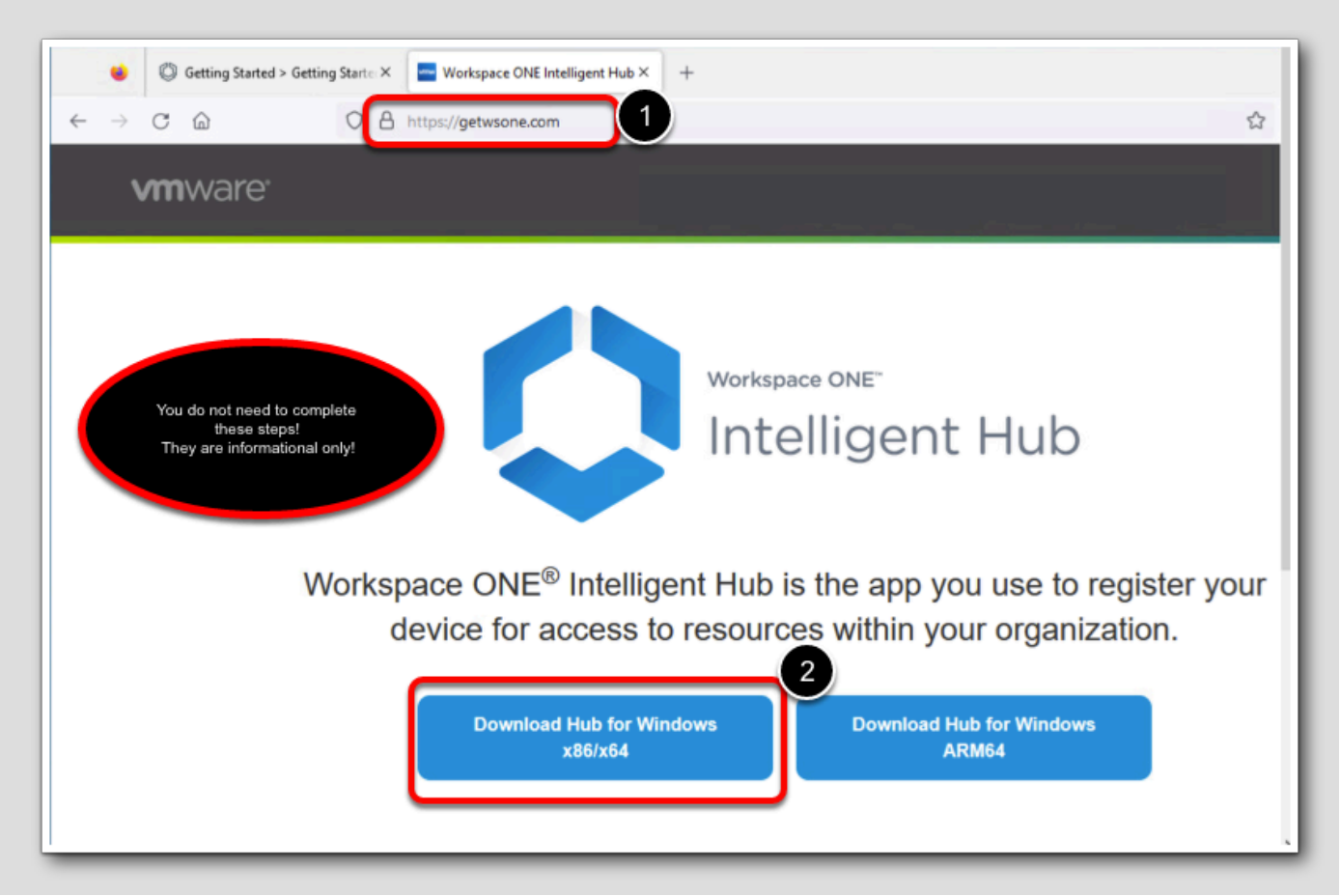
Enrolling Your Windows 10 Device with a Basic Account

[621]

You will now enroll the Windows 10 device in Workspace ONE UEM by using the Workspace ONE Intelligent Hub app.

Downloading the Workspace ONE Intelligent Hub app

[622]



NOTE: You do NOT need to complete these steps, the Workspace ONE Intelligent Hub has already been downloaded for you! This step is purely informative.

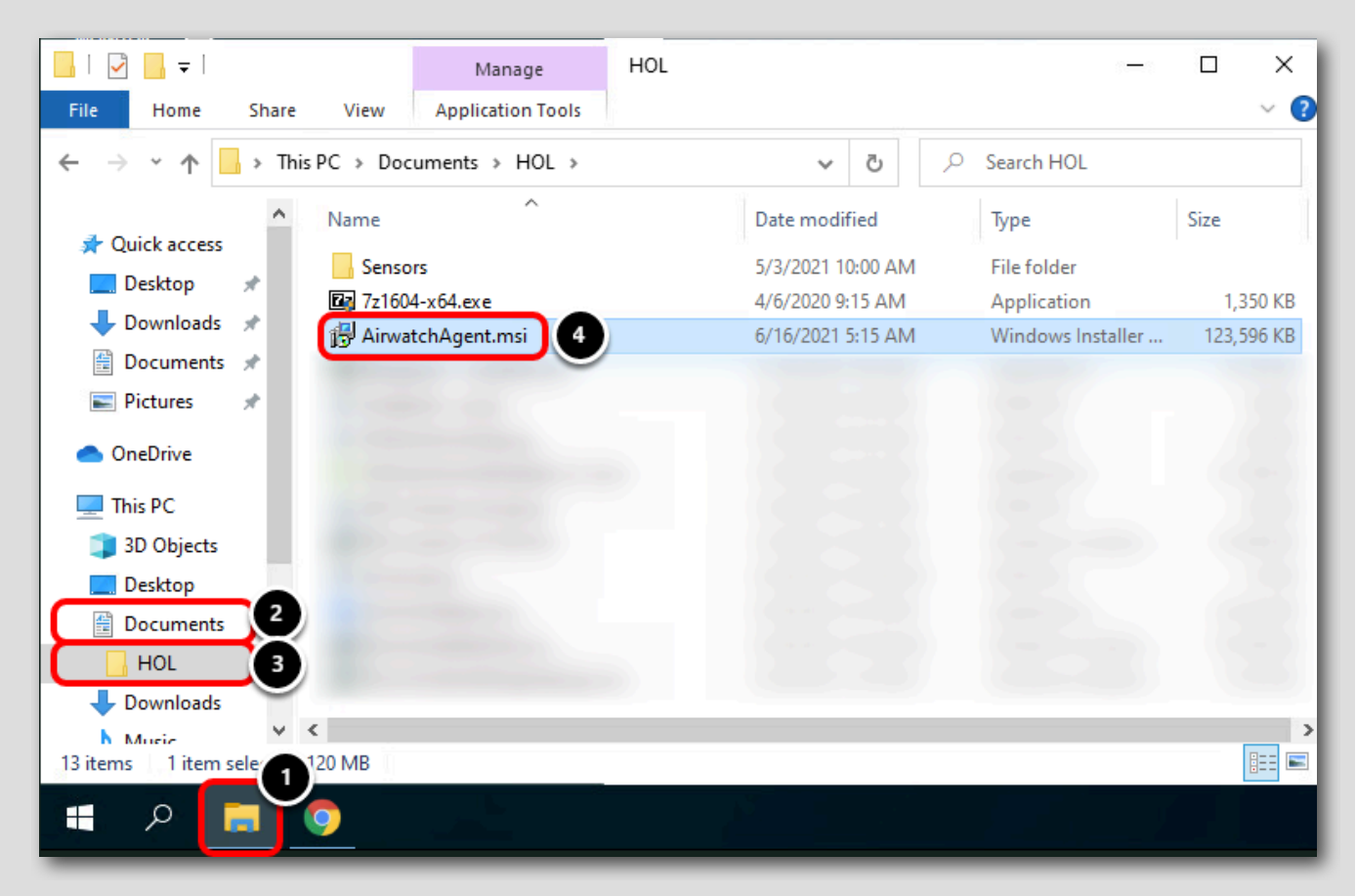
You can download the latest Workspace ONE Intelligent Hub app for your current platform by following the below steps:

1. Navigate to **`https://www.getwsone.com`** in your browser.
2. Click **Download Hub for Windows 10**.
3. Click **Keep** when warned about the AirWatchAgent.msi download.

For expediency, the Workspace ONE Intelligent Hub app has already been downloaded for you. Continue to the next step to start the installer.

Launch the Workspace ONE Intelligent Hub Installer

[623]

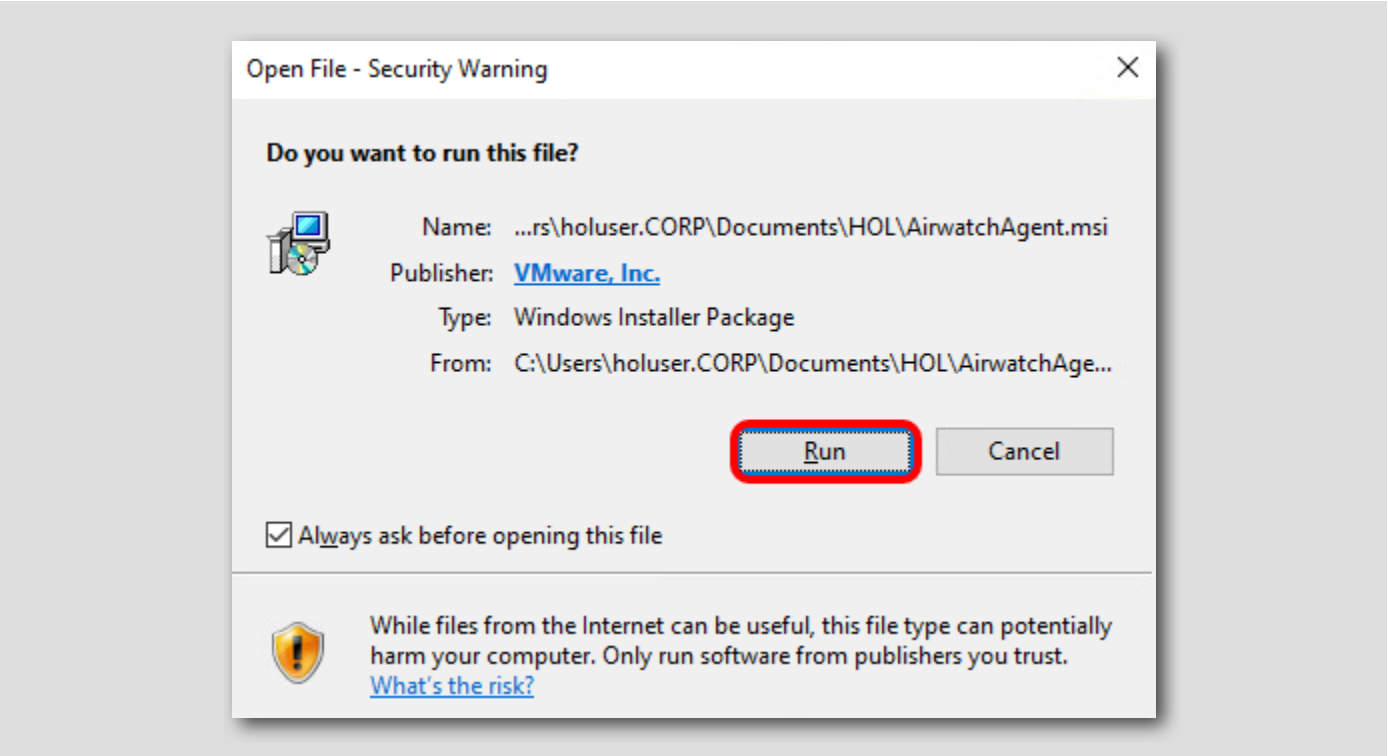


1. Click the **File Explorer** icon from the taskbar.
2. Click **Documents**.
3. Click **HOL**.
4. Double-click the **AirwatchAgent.msi** file to start the installer.

NOTE: The installer may take a few seconds to launch, please be patient after clicking the AirwatchAgent.msi file.

Click Run

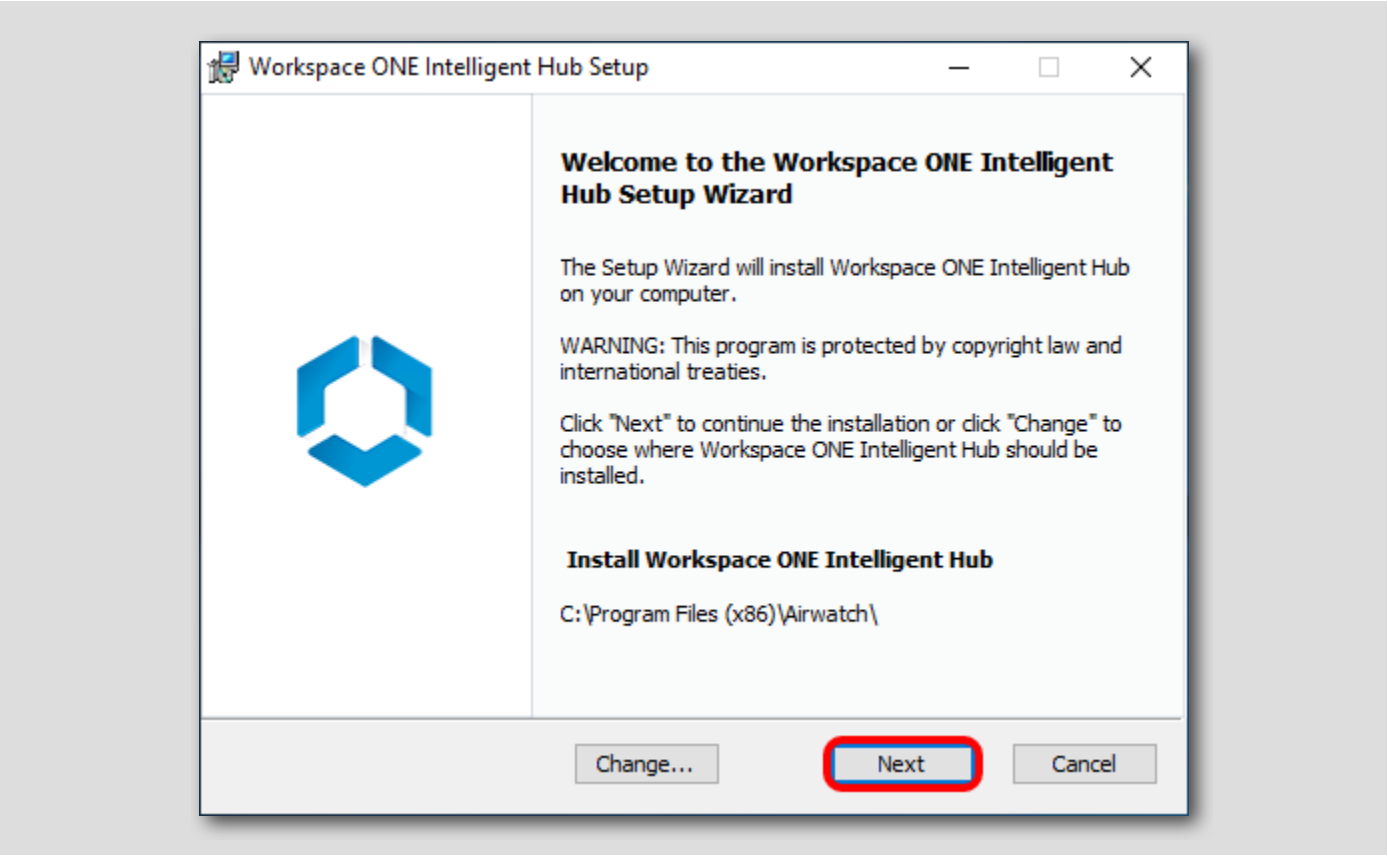
[624]



Click **Run** to proceed with the installation.

Accept the Default Install Location

[625]

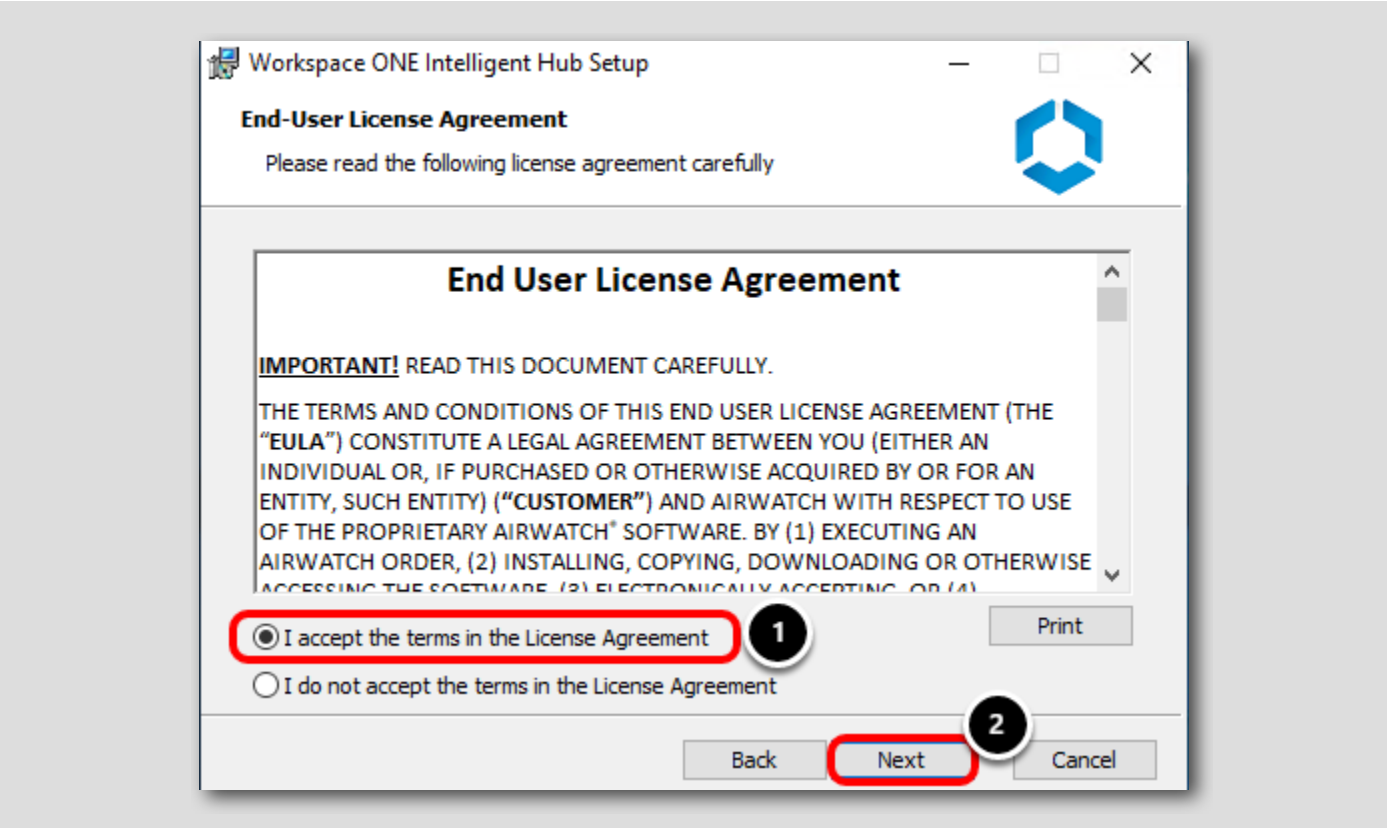


Leave the default install location and click **Next**.

NOTE: The Next button may take several seconds to enable while the required additional features are installed.

Accept the License Agreement

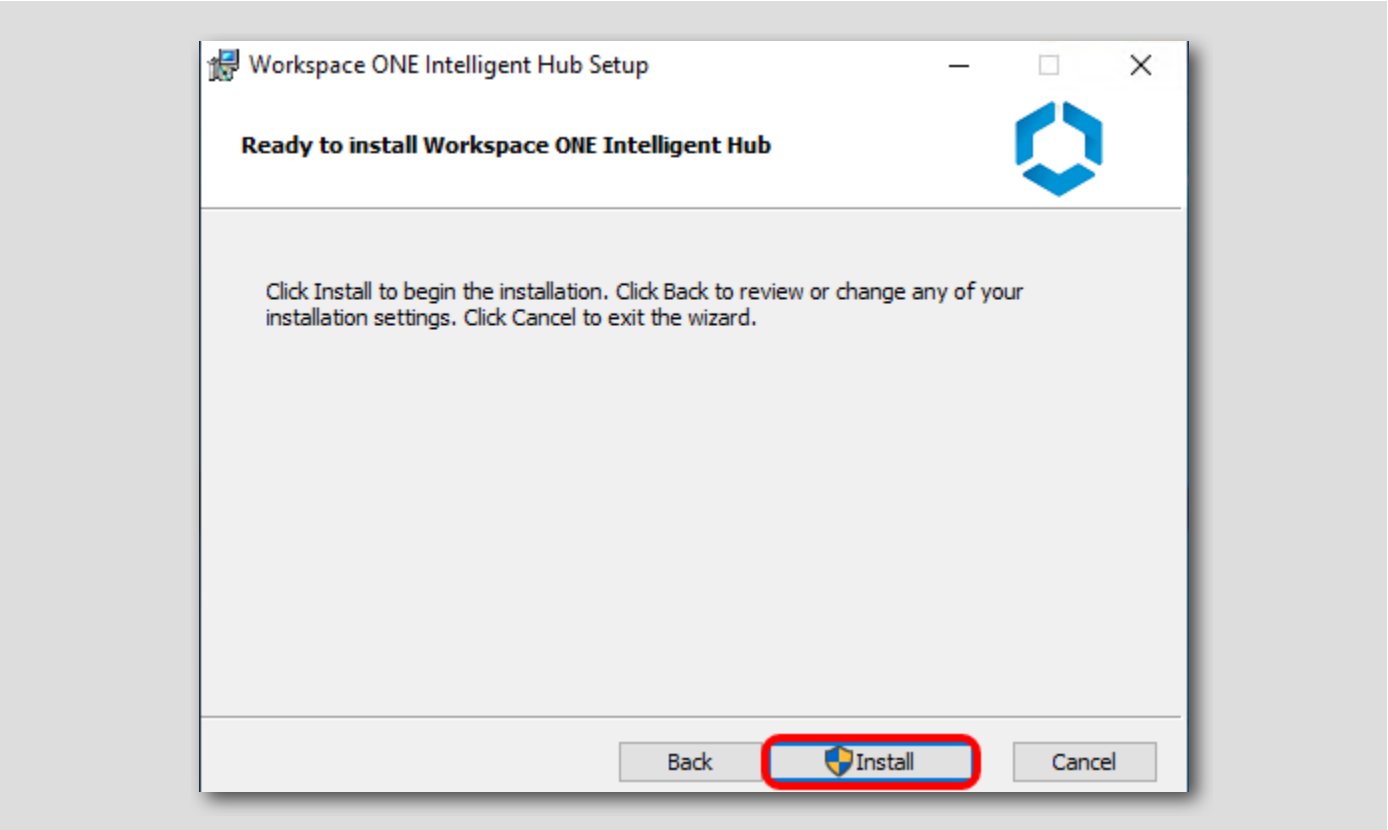
[626]



1. Select I accept the terms of the License Agreement.
2. Click **Next**.

Start the Workspace ONE Intelligent Hub Install

[627]

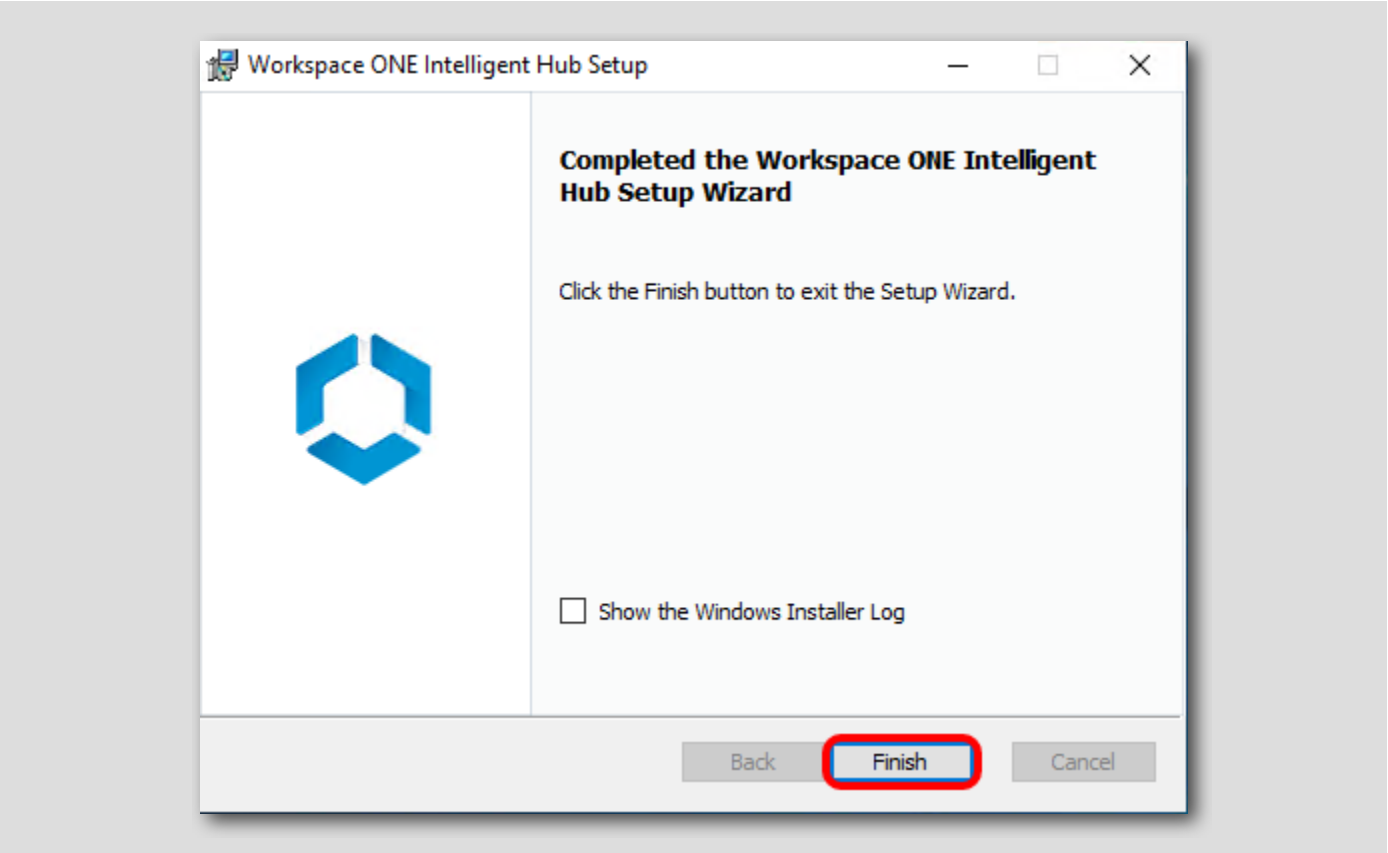


Click **Install** to start the installer.

NOTE: The Workspace ONE Intelligent Hub install may take several minutes to complete, do not interrupt the installer!

Complete the Workspace ONE Intelligent Hub Installer

[628]



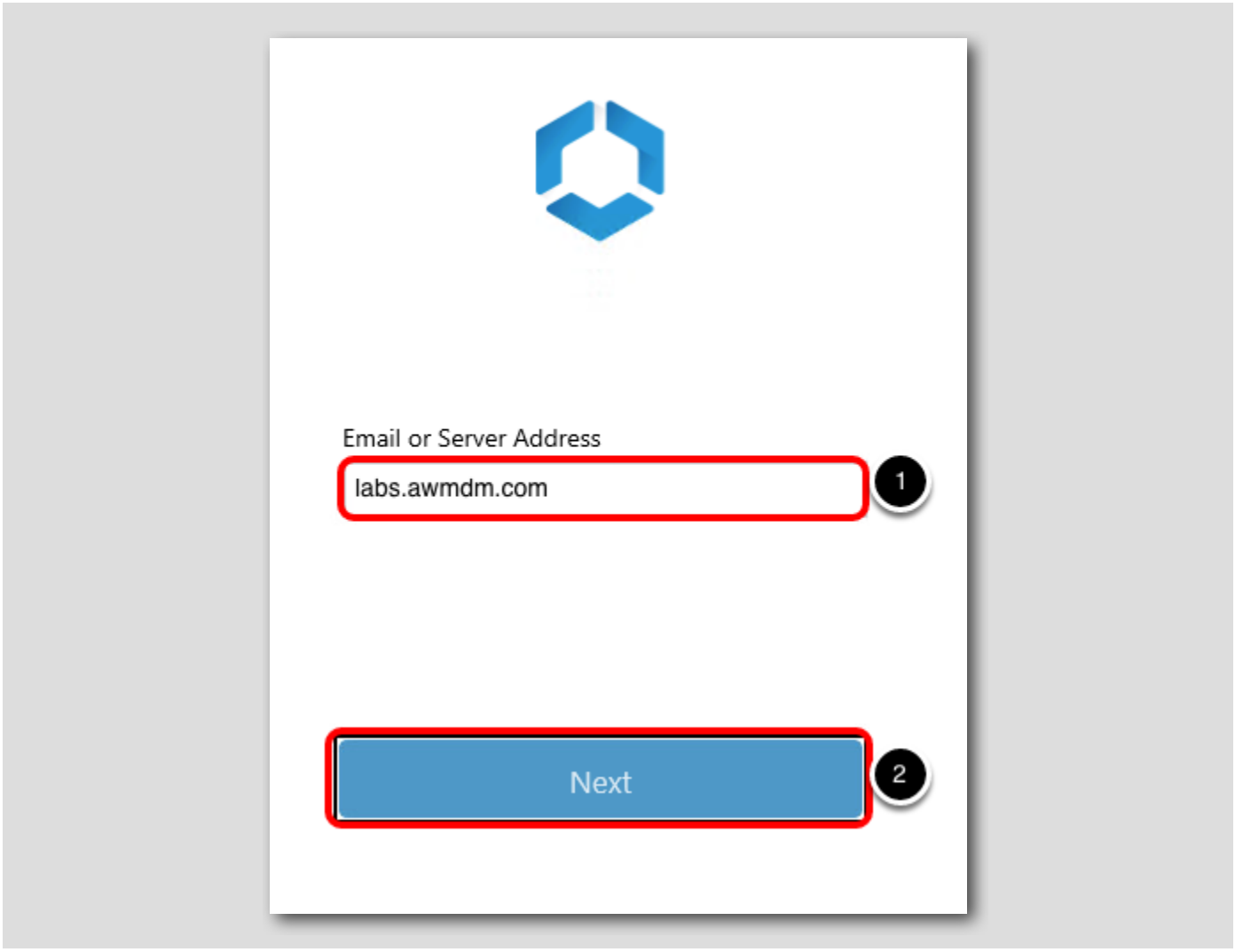
NOTE: The installer may take several minutes to complete. Please wait until you see the completed install screen before continuing.

Click **Finish** to complete the Workspace ONE Intelligent Hub installer.

NOTE: After clicking finish, the Native Enrollment application will launch to guide you through enrolling into Workspace ONE UEM. It will take 2-3 minutes to launch the Intelligent Hub.

Enroll Your Windows 10 Device using the Workspace ONE Intelligent Hub

[629]

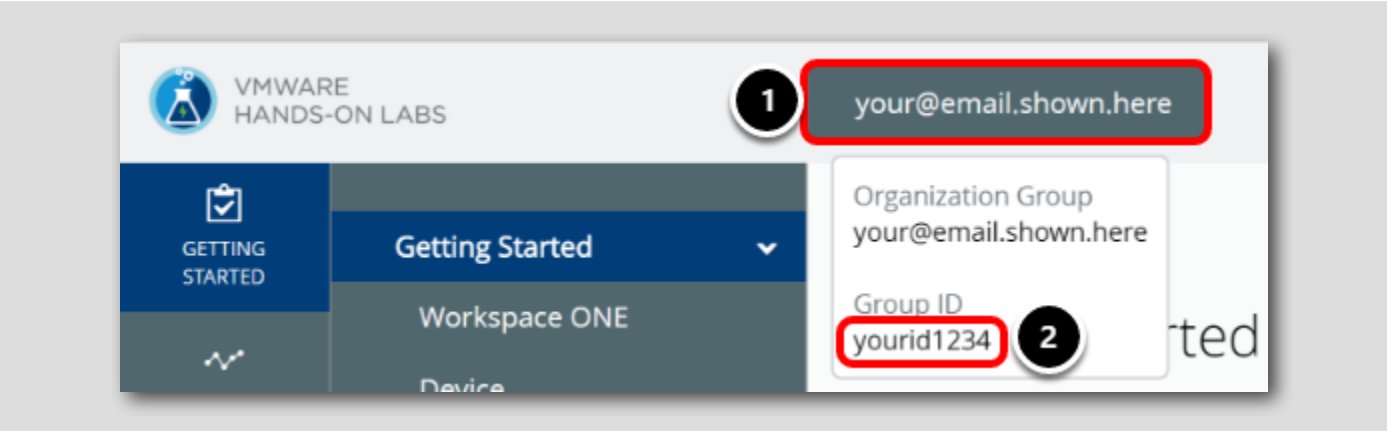


NOTE: The above screen may take 2-3 minutes to display after clicking Finish from the previous step!

1. Enter **`labs.awmdm.com`** for the Server Address.
2. Click **Next**.

Locate your Group ID from Workspace ONE UEM Console

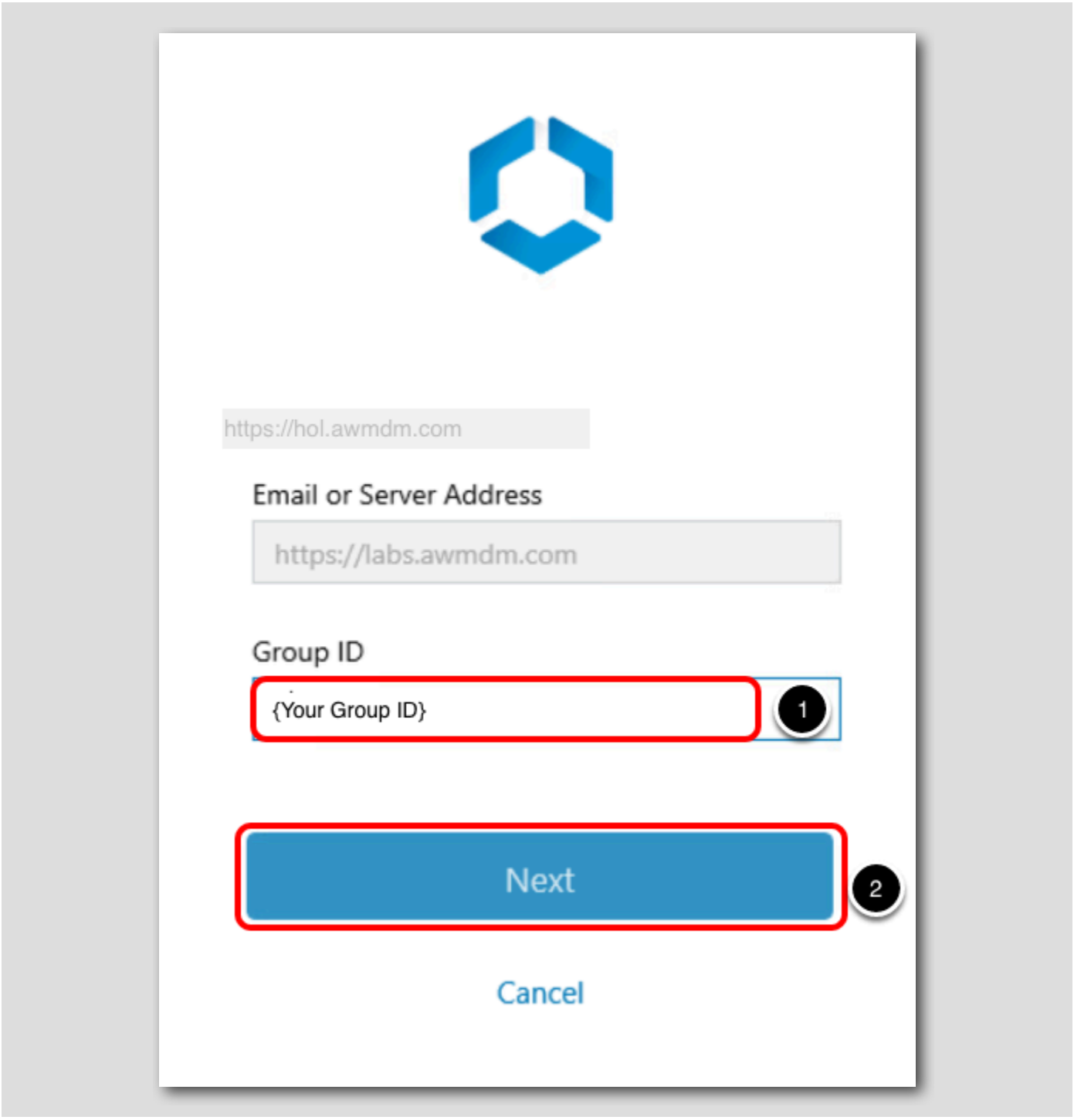
[630]



The next step is to retrieve your **Organization Group ID**.

1. To find the Group ID, Go back to the Workspace ONE UEM Administration Console and 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. Copy this value.

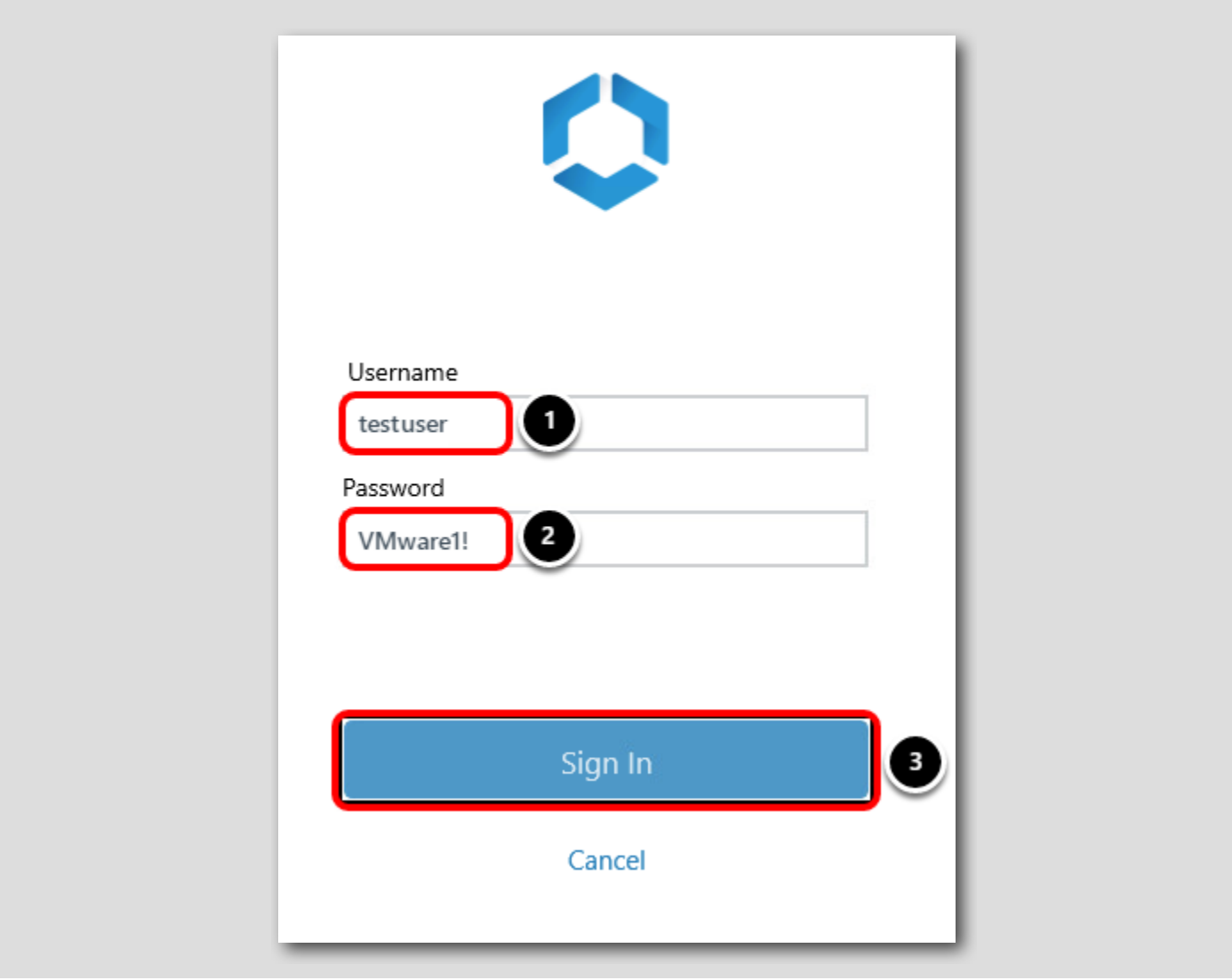
Enter Your Group ID [631]



1. Enter **Your Group ID** in the **Group ID** field. If you forgot your Group ID, check the previous steps on how to retrieve it.
2. Click **Next**.

Enter Your User Credentials

[632]

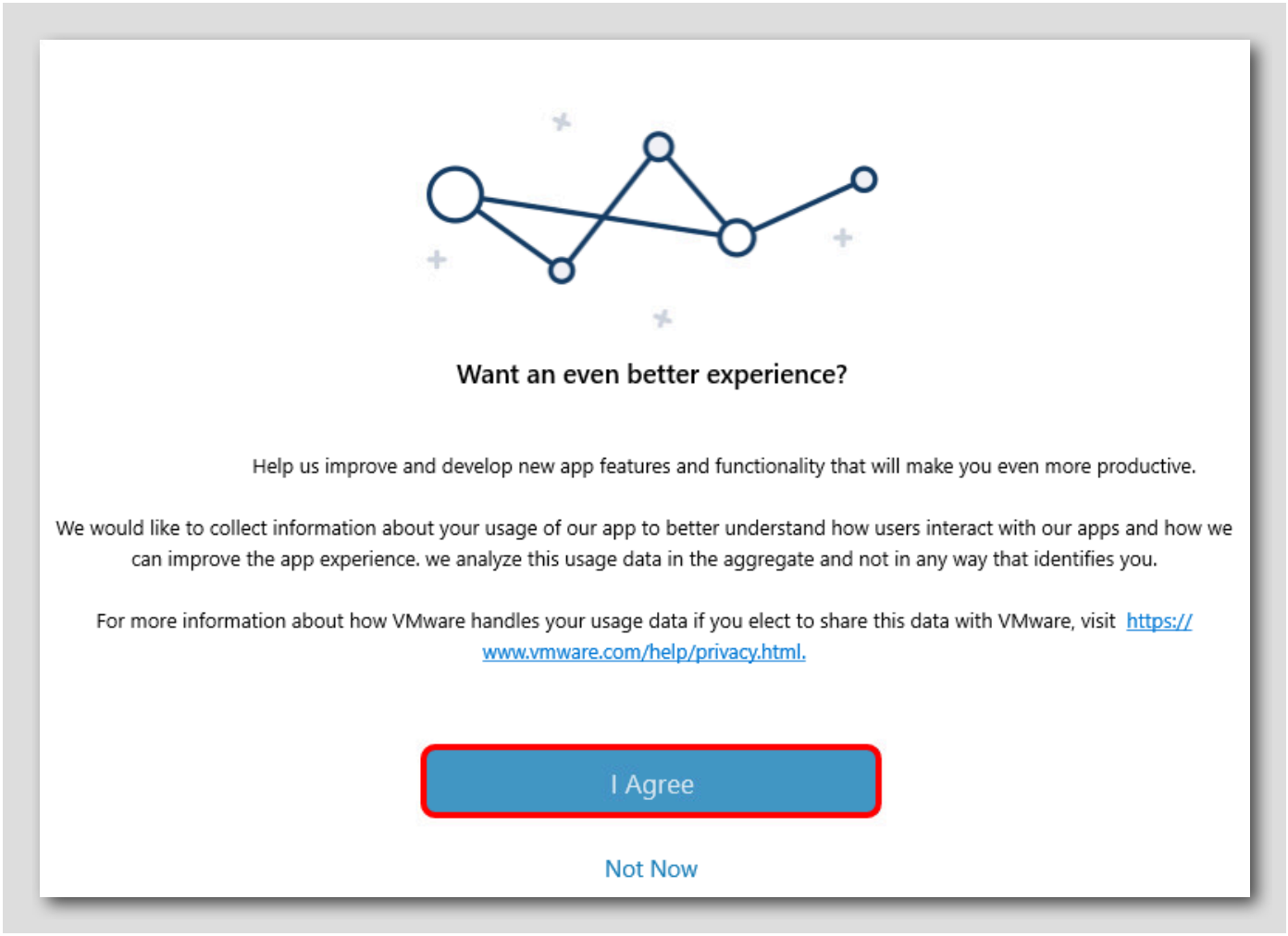


1. Enter **`testuser`** in the **Username** field.
2. Enter **`VMware1!`** in the **Password** field.
3. Click **Sign In**.

NOTE: Wait while the server checks your enrollment details. This may take a few minutes.

Accept Data Policy

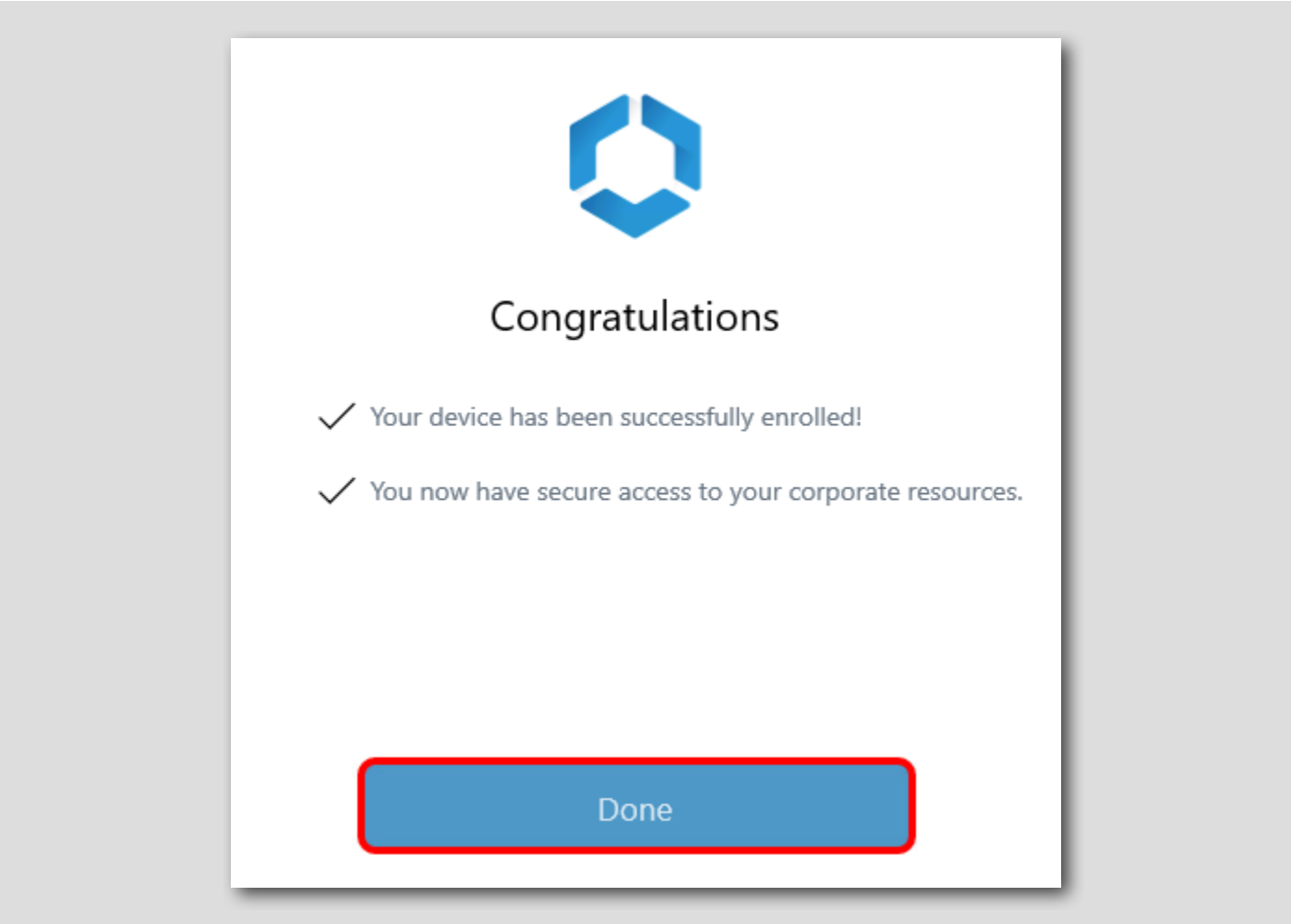
[633]



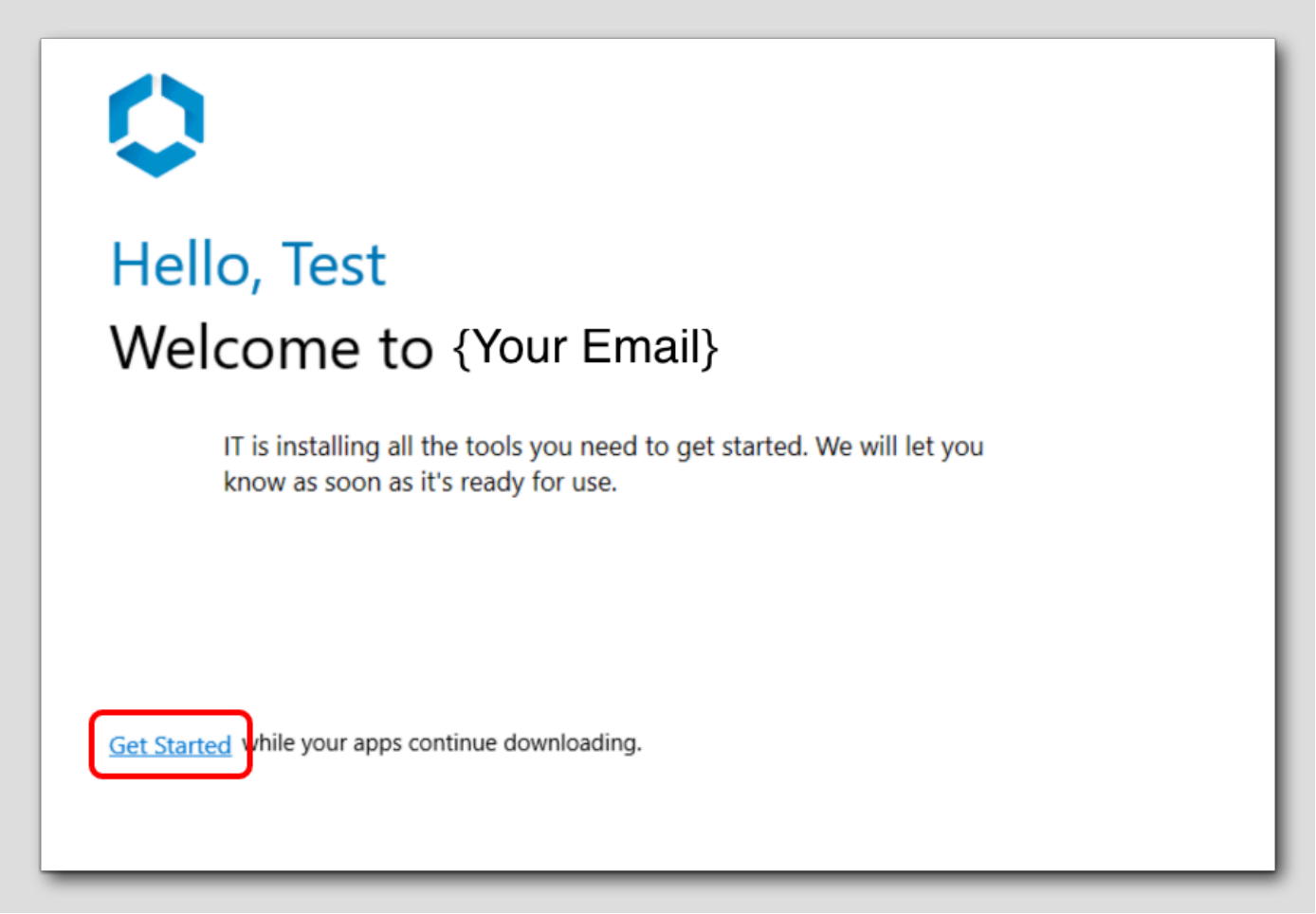
Click **I Agree**.

Finish the Workspace ONE UEM Enrollment Process

[634]



Click **Done** to end the Enrollment process.

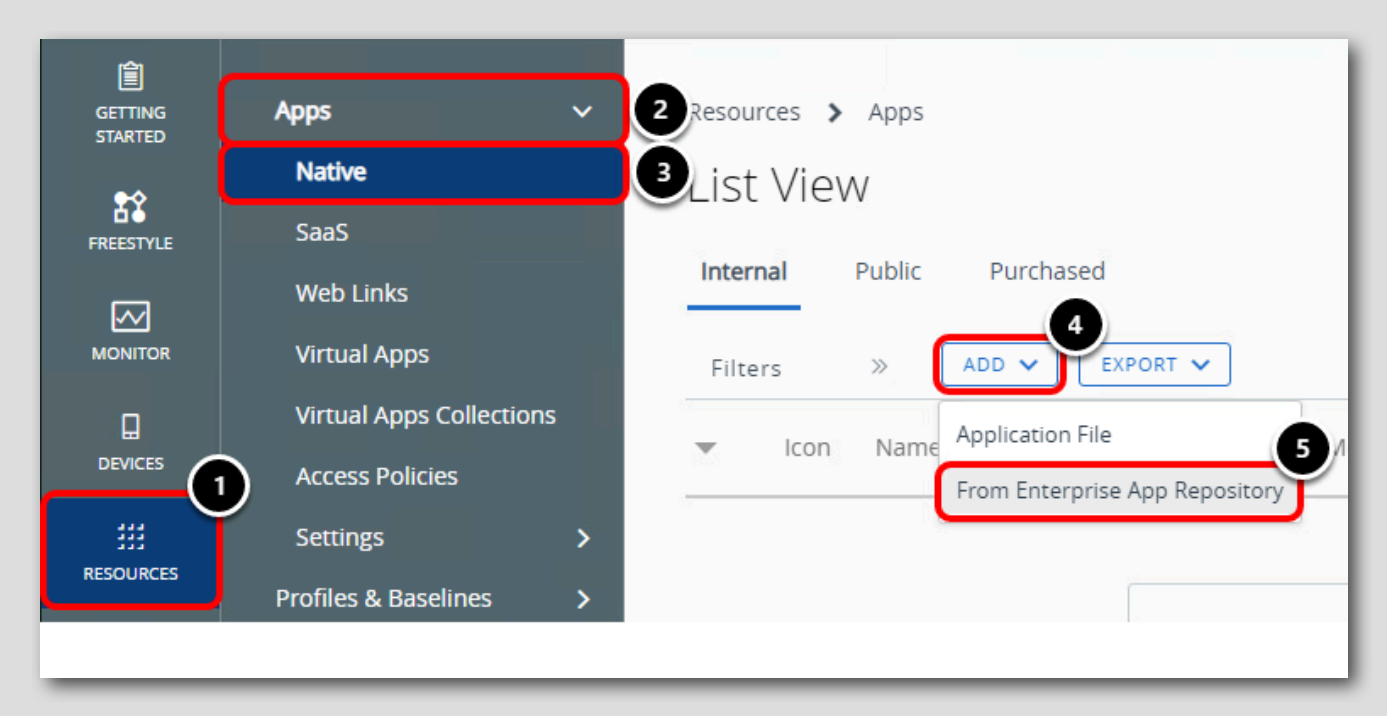


Click **Get Started** to close the onboarding welcome screen.

Your Windows 10 device is now successfully enrolled into Workspace ONE UEM!

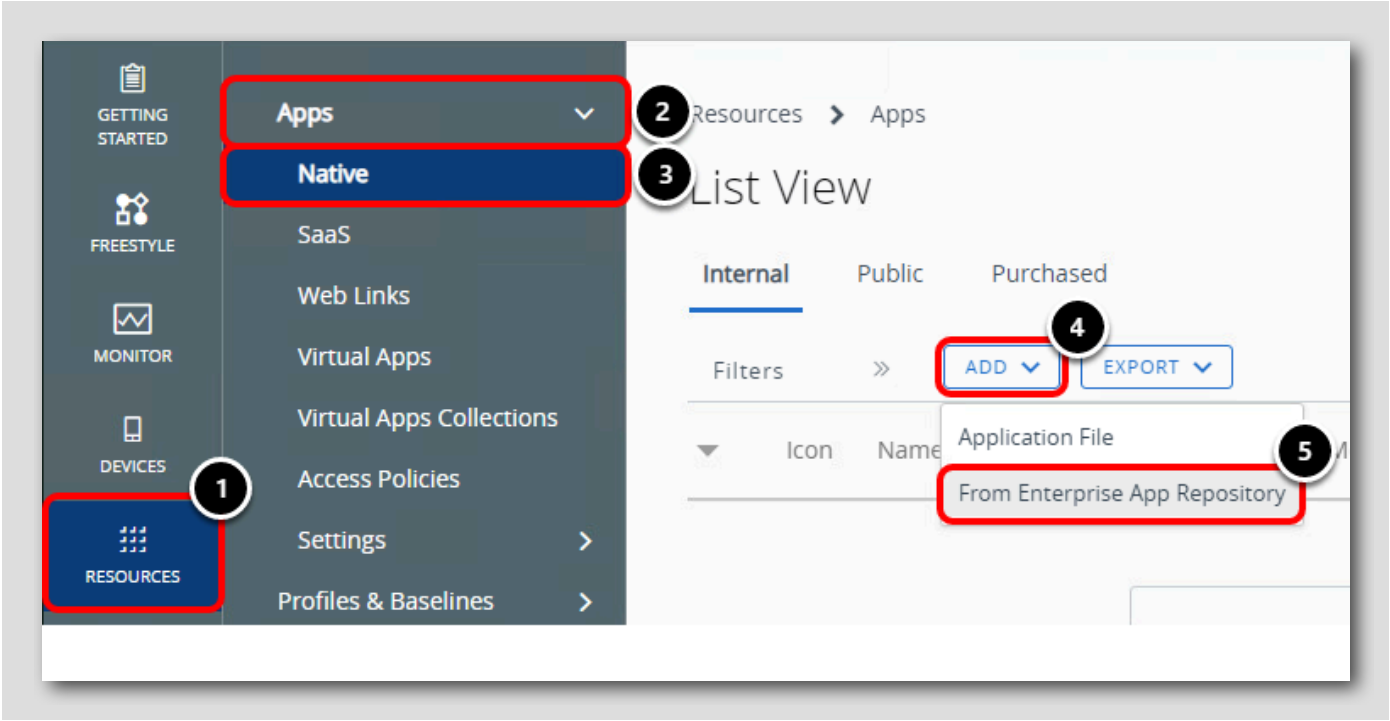
Configure Zoom Client for Meetings Application

[635]

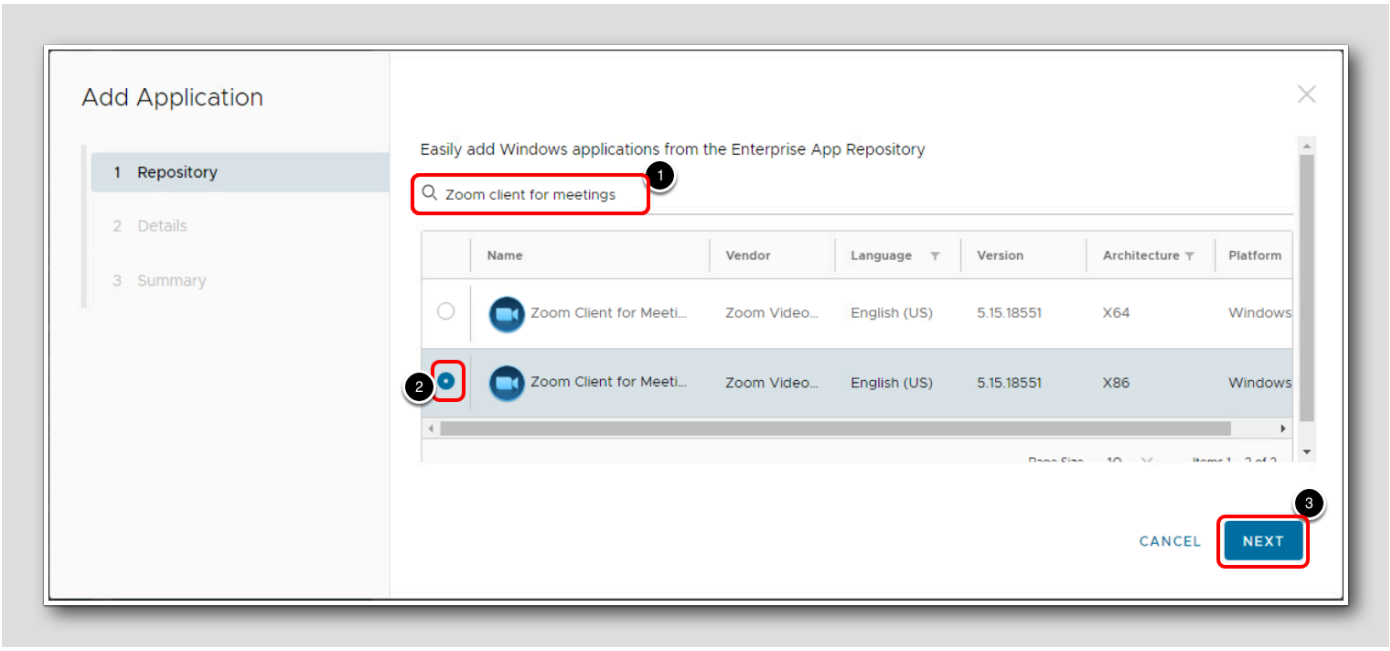


Return to the Workspace ONE UEM Administration Console in the web browser:

1. Click **Resources**
2. Expand **Apps**
3. Click **Native**
4. Click **Add**
5. Click **From Enterprise App Repository**



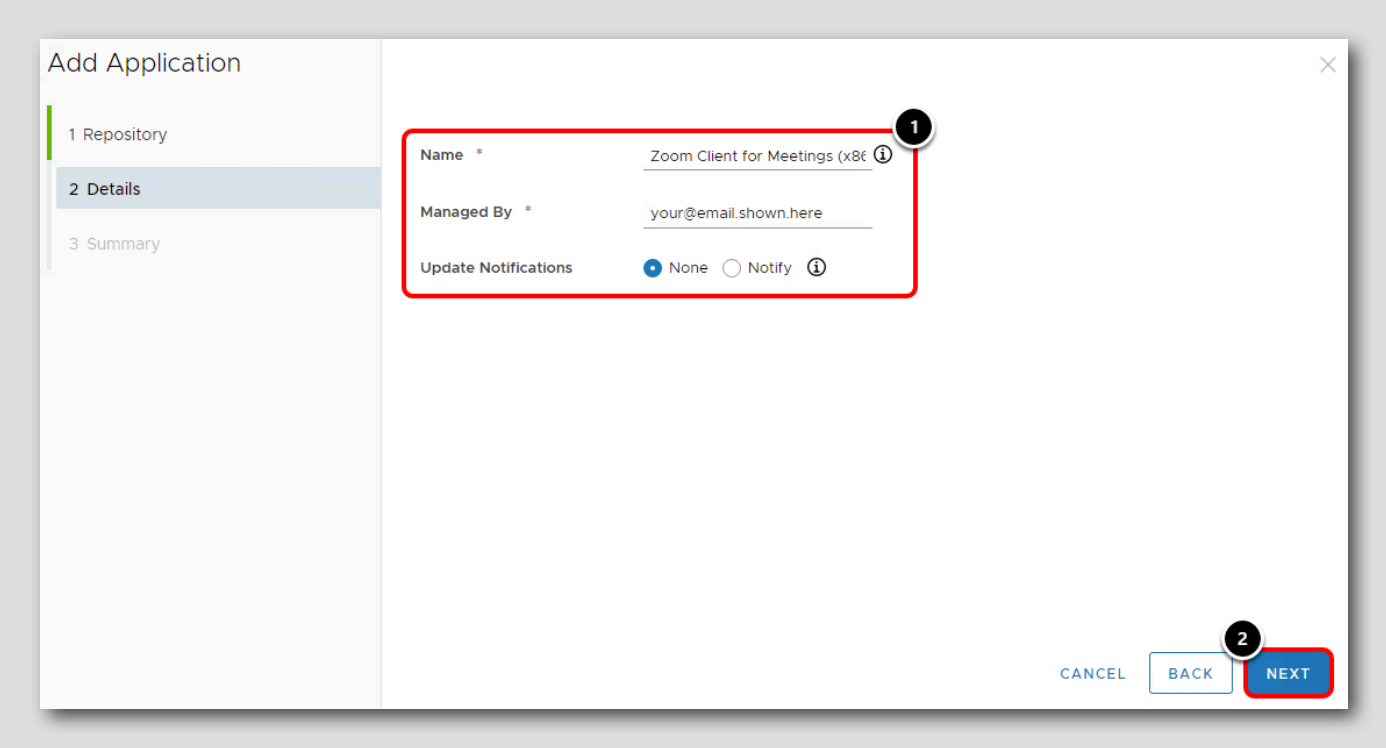
Search for Zoom Client for Meetings [636]



1. Search **Zoom Client for Meetings** and hit ENTER.
2. Select the **Zoom Client for Meetings (x86)** app. Ensure you are selecting the x86 version of the app (check the Name and Architecture columns).
3. Click **Next**.

Review Application Details

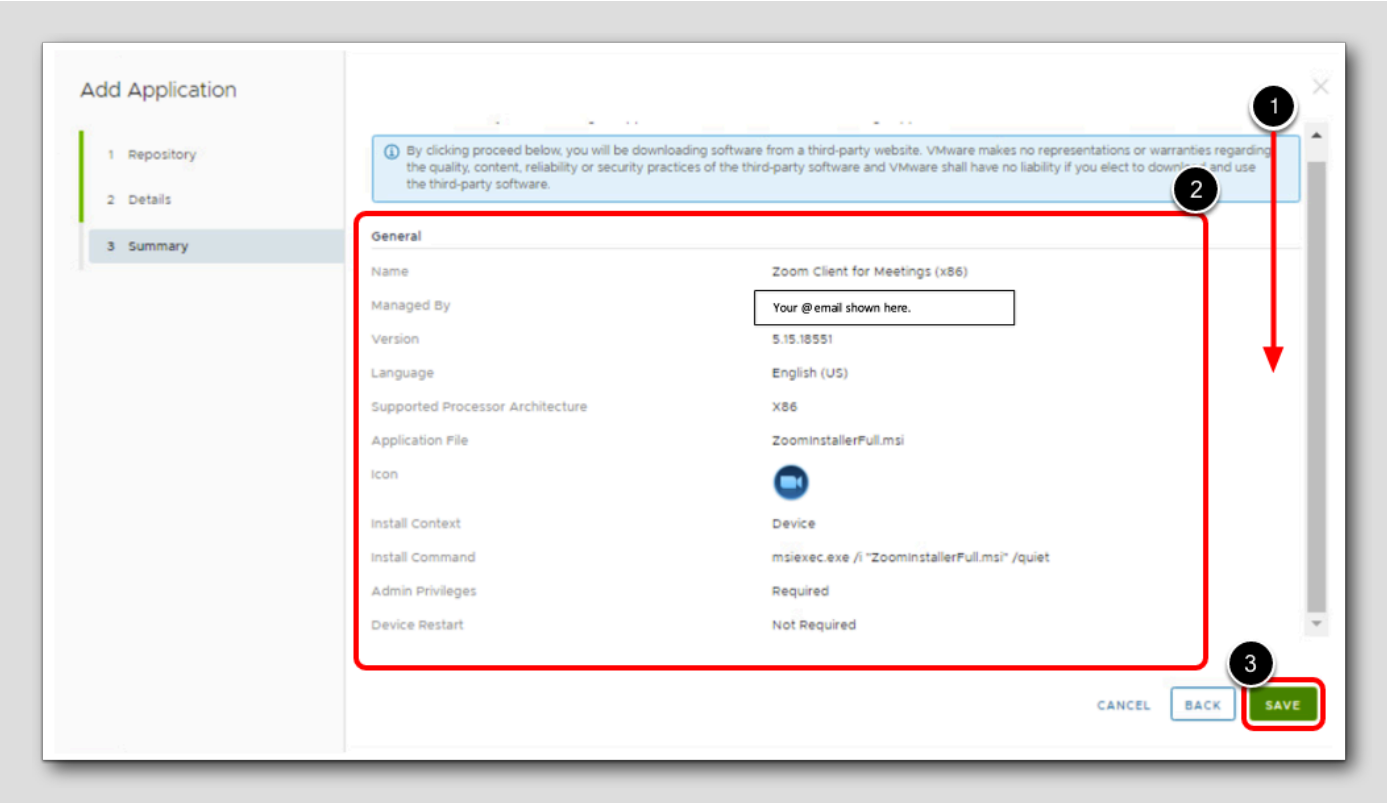
[637]



1. Review the Applications details. Keep all of the default values for this section.
2. Click **NEXT**.

Review Application Summary

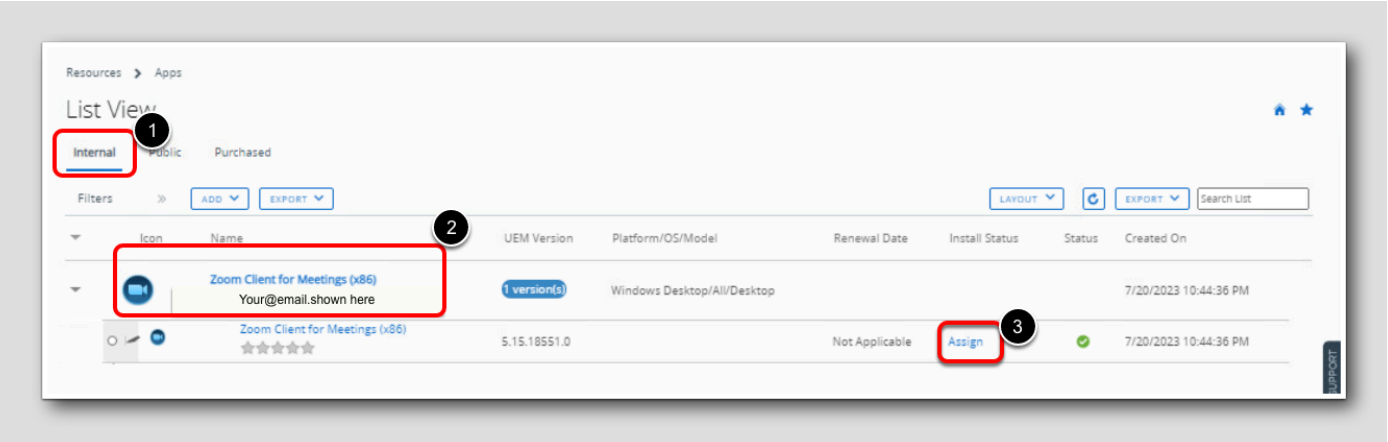
[638]



1. Scroll down to the bottom of the page.
2. **Review** the Applications Installation details. The Enterprise App Repository speeds up app delivery by pre-configuring the app installer, install command, and other configurations.
3. Click **SAVE**.

Create Application Assignment

[639]

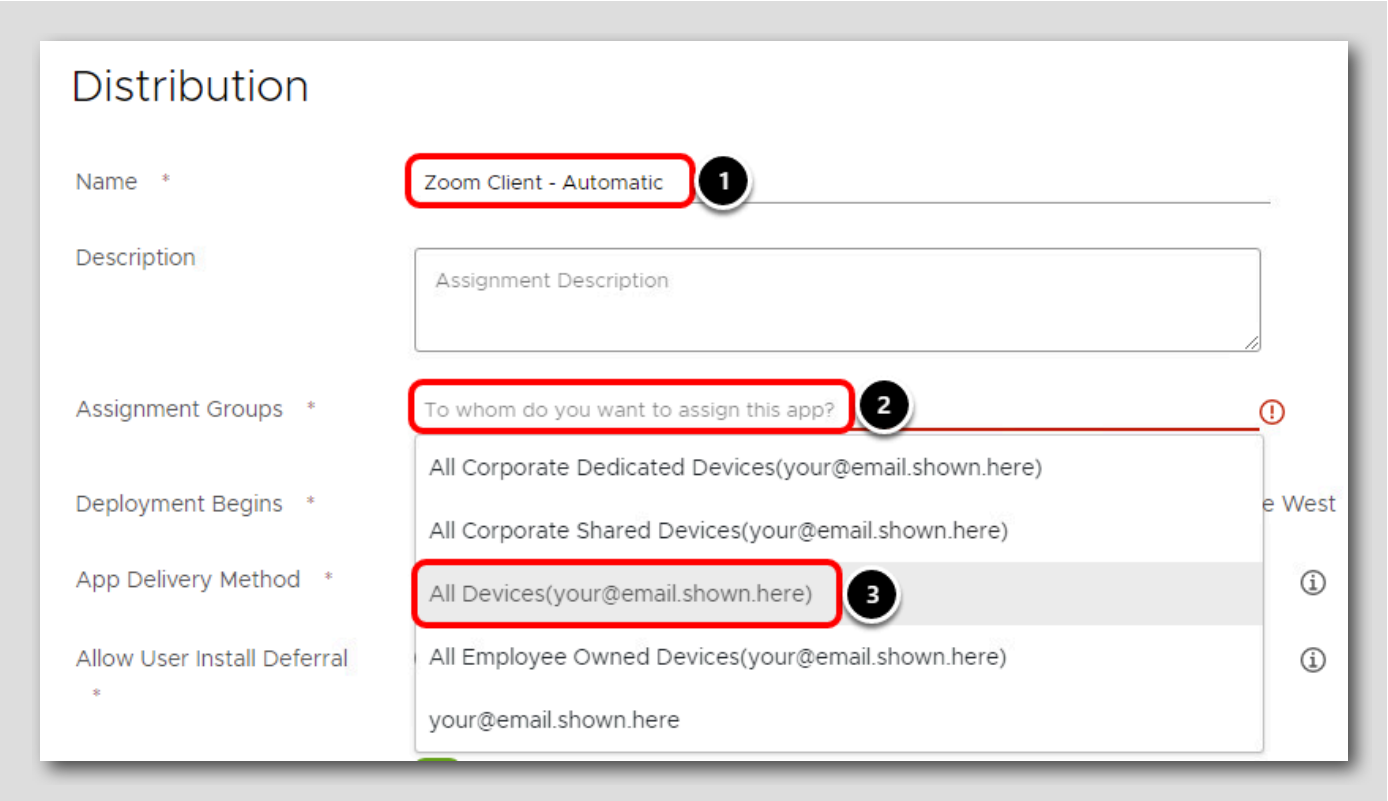


1. Ensure you are on the **Internal** tab.
2. Find the **Zoom Client for Meetings (x86)** app that you just added.
3. Click **Assign** under the Install Status column.

The application has been added to your organization group but is not assigned to any users or devices. The following steps will have you create an application assignment to determine which devices will receive the application.

Create Application Distribution

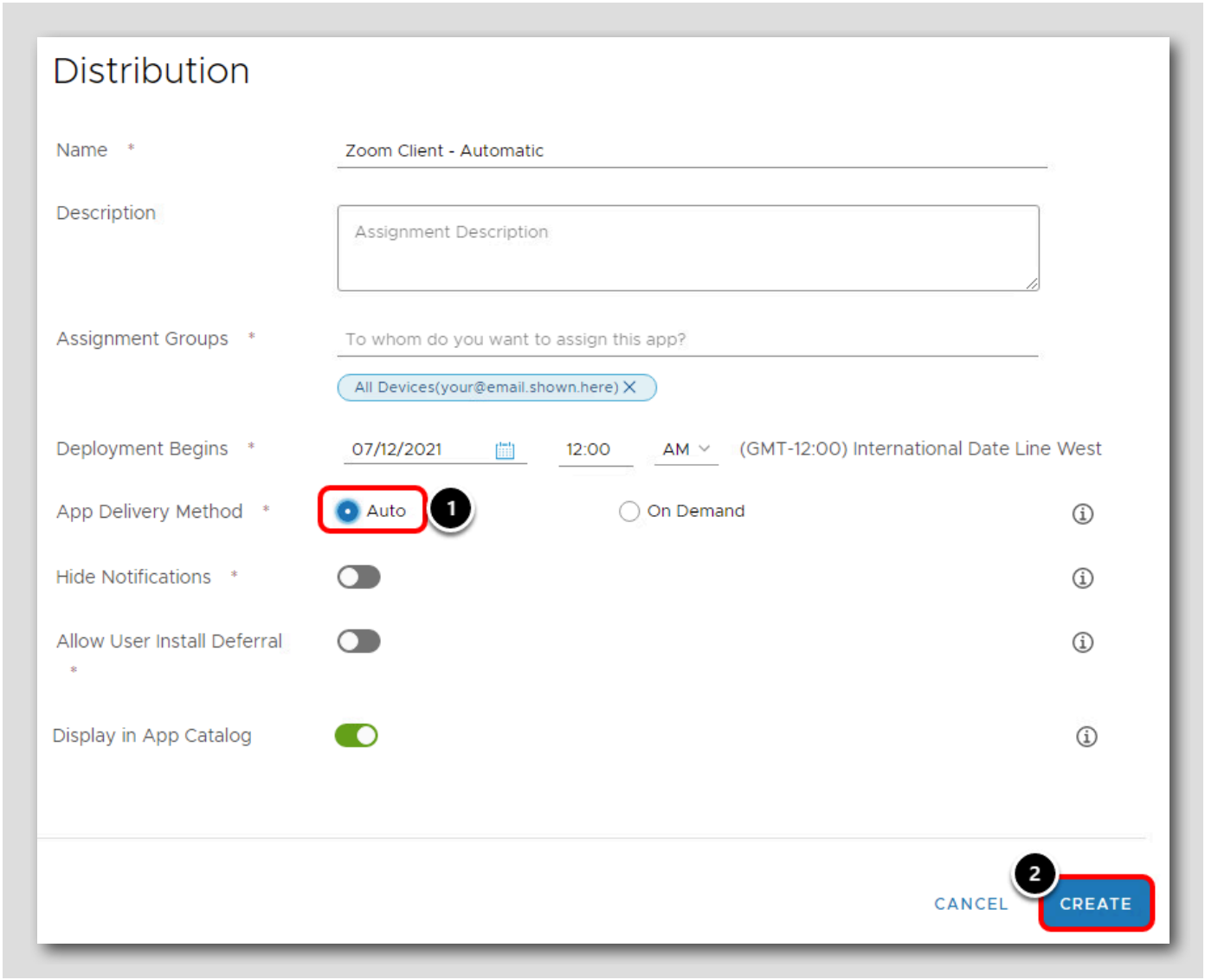
[640]



1. Enter **`Zoom Client - Automatic`** for the distribution name.
2. Click in the **Assignment Groups** field to see a list of eligible groups.
3. Select the **All Devices (your@email.shown.here)** group. This will assign the application to all Windows 10 devices enrolled in your organization.

Update App Delivery Method

[641]

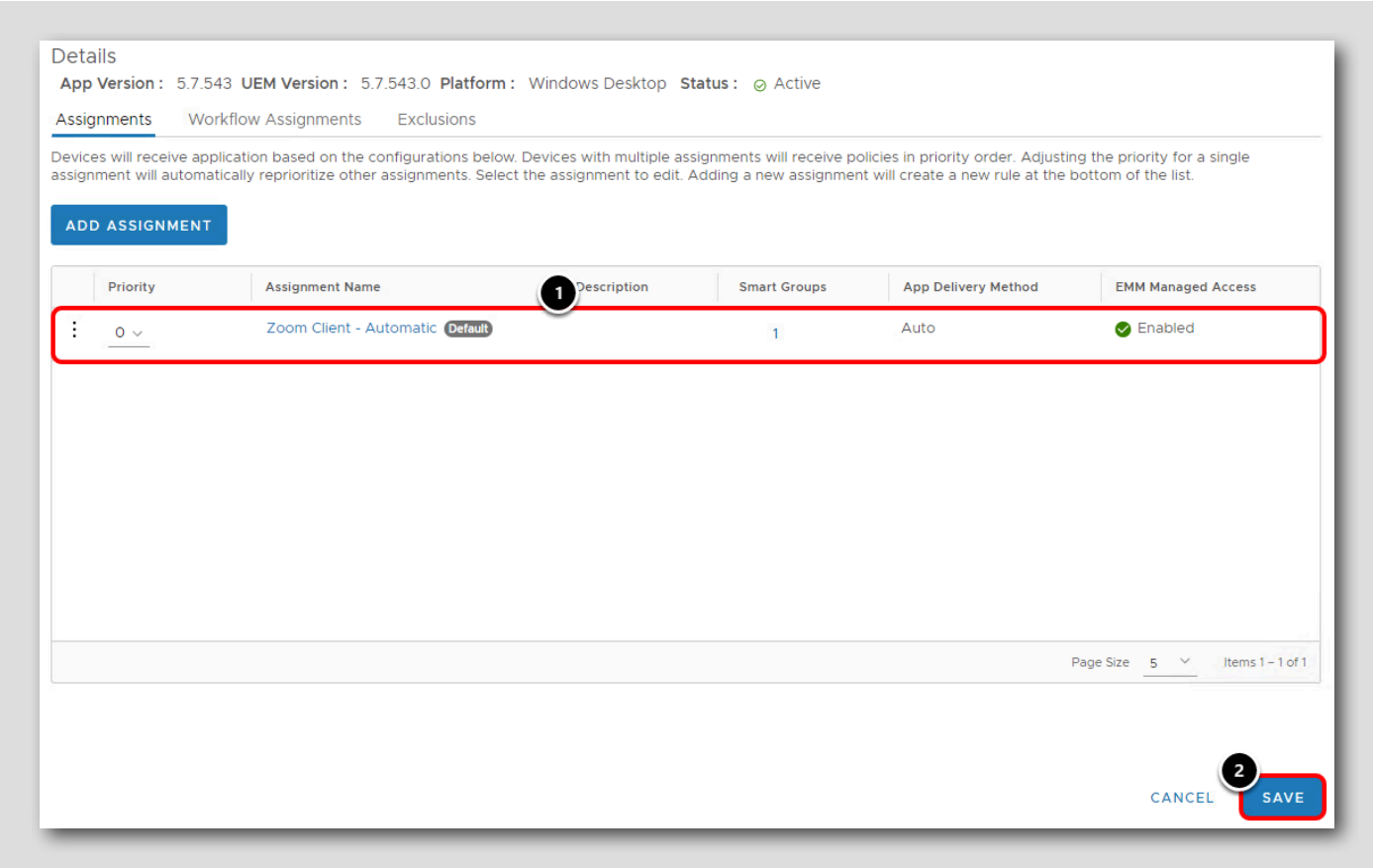


1. Change the App Delivery Method to **Auto**. Auto will automatically install the Zoom app on the assigned Windows 10 devices as they check-in to Workspace ONE UEM as opposed to On Demand which makes the app available in the catalog but does not automatically install the app.
2. Click **Create**.

Note: You now have the ability to choose if the app is displayed in the app catalog or not. This is helpful when deploying driver updates or scripted actions and don't want the end-user to see this in the catalog.

Review Application Distribution

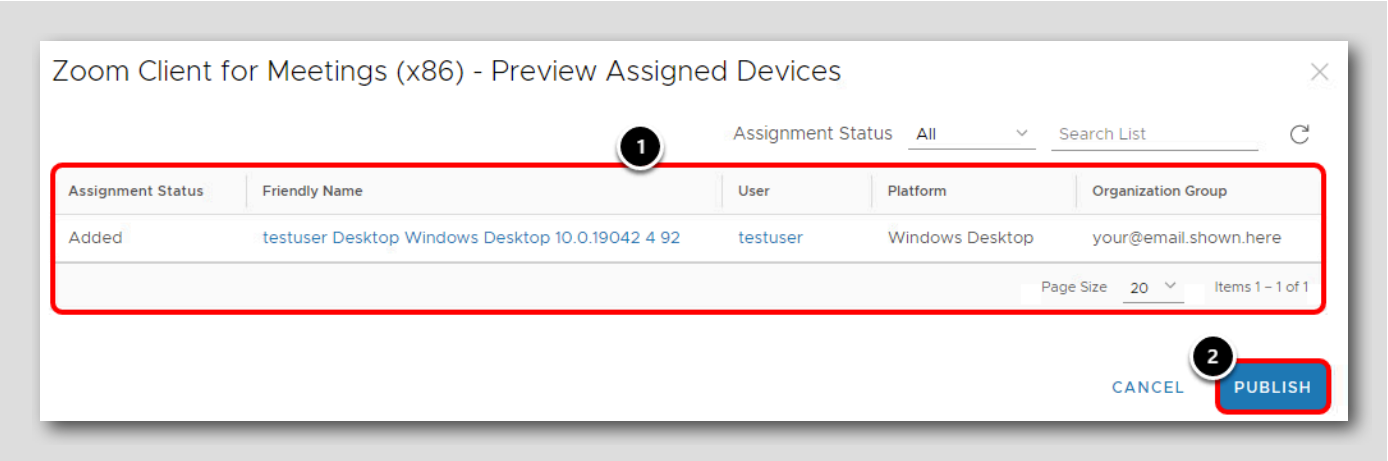
[642]



1. The list of assignments is displayed here. Confirm that the Zoom Client - Automatic assignment you created is displayed. You can return to this section to edit, add, or remove assignments as needed.
2. Click **Save**.

Preview Assigned Devices

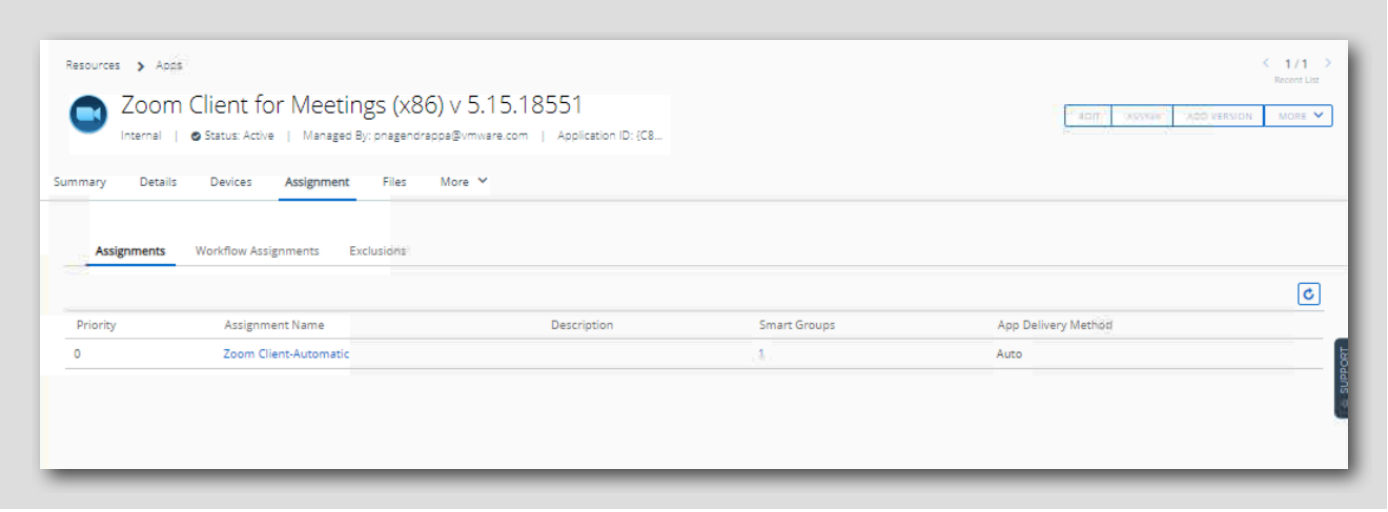
[643]



1. A preview of devices that will receive this app is displayed here. A single device record is shown as you have only enrolled one device in your organization.
2. Click **Publish**.

Confirm Device Assignment

[644]

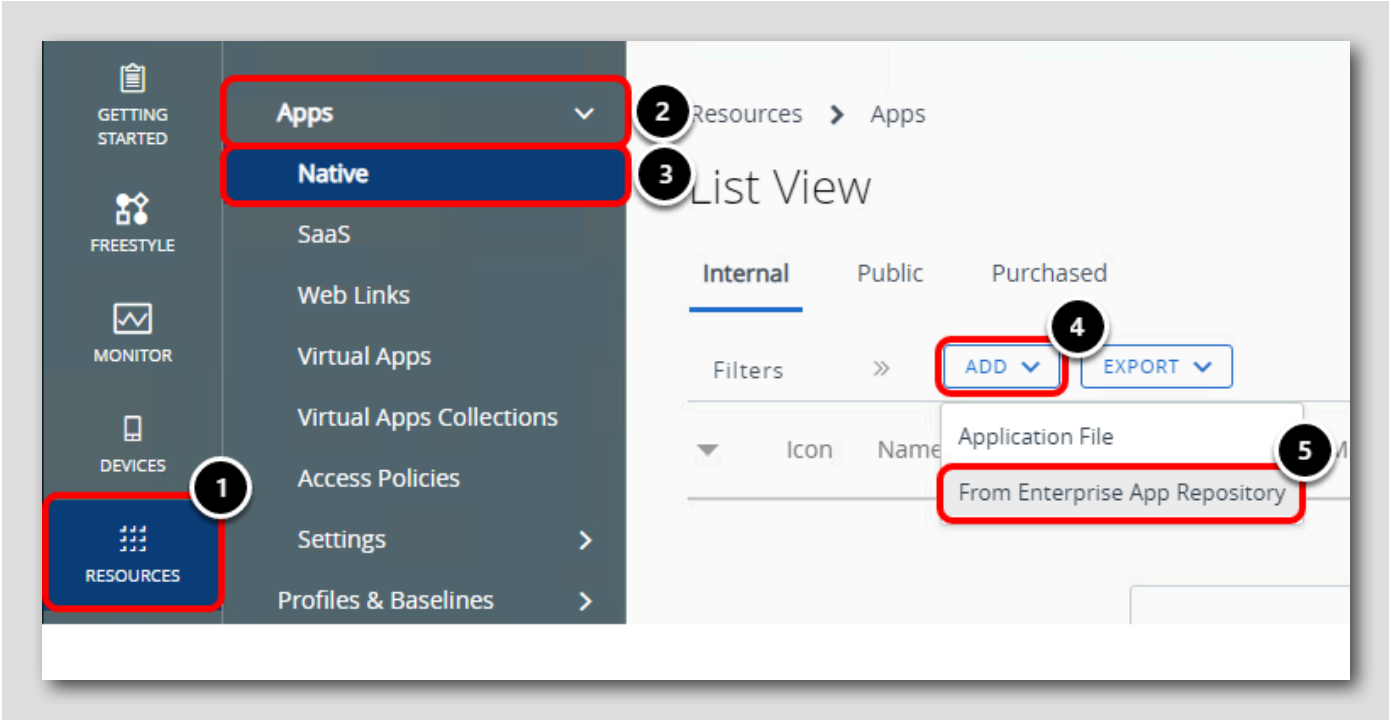


The **Zoom Client for Meetings (x86)** application has been created and assigned to the All Devices smart group with the Auto app delivery method, meaning all assigned devices will automatically install this application.

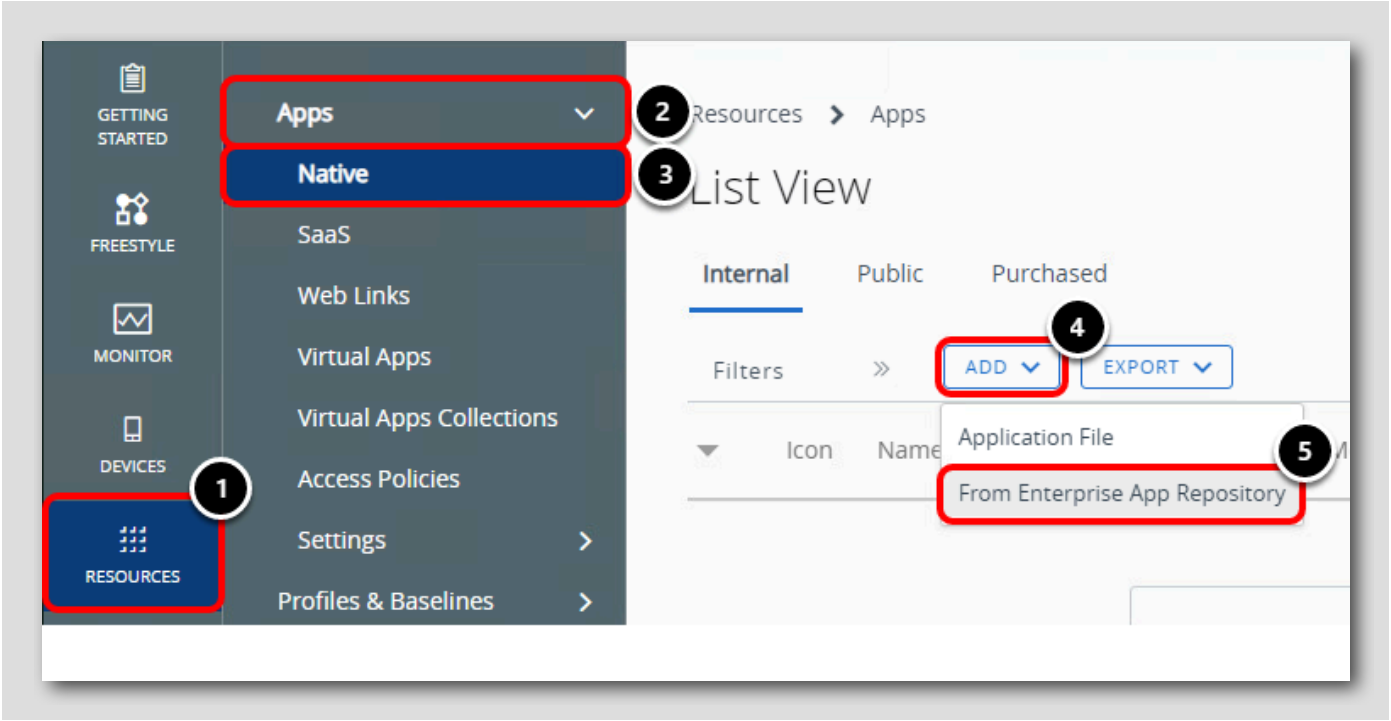
Continue to the next step.

Configure the Zoom Plugin for Microsoft Outlook Application

[645]

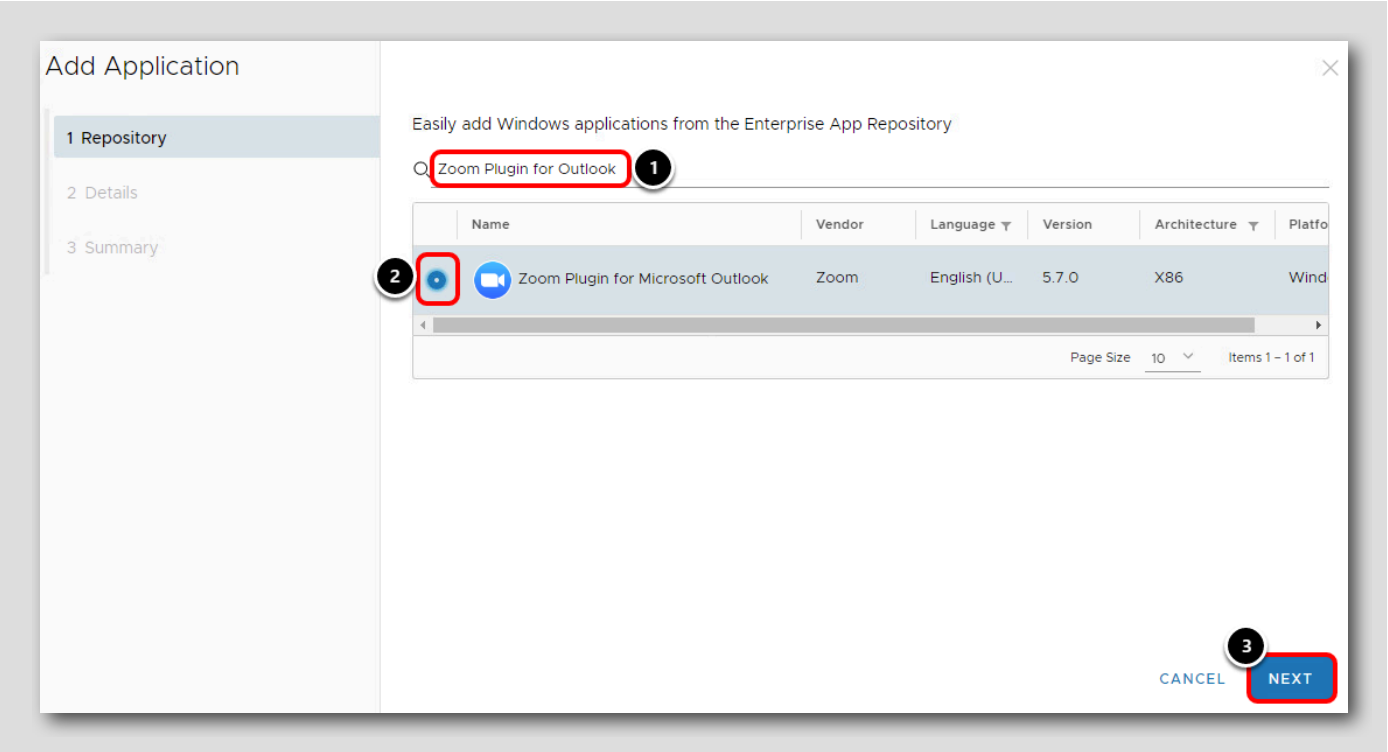


1. Click **Resources**
2. Expand **Apps**
3. Click **Native**
4. Click **Add**
5. Click **From Enterprise App Repository**


GETTING STARTED
FREESTYLE
MONITOR
DEVICES
RESOURCES
1
Apps
Native
SaaS
Web Links
Virtual Apps
Virtual Apps Collections
Access Policies
Settings
Profiles & Baselines
2
3
Resources > Apps
List View
Internal
Public
Purchased
4
Filters
ADD
EXPORT
Icon
Name
Application File
From Enterprise App Repository
5

Search for Zoom Plugin for Microsoft Outlook

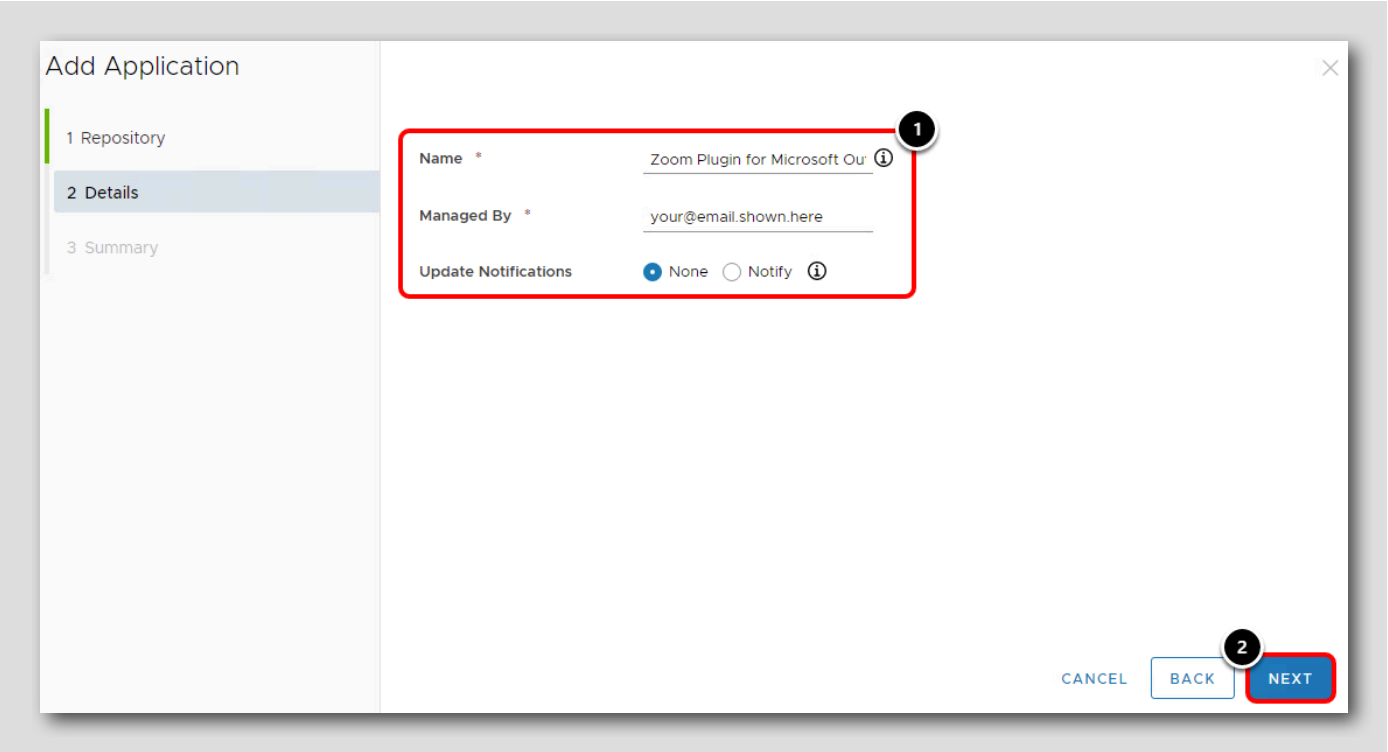
[646]



1. Search **`Zoom Plugin for Outlook`** and hit **`ENTER`**.
2. Select the **Zoom Plugin for Microsoft Outlook** app.
3. Click **Next**.

Review Application Details

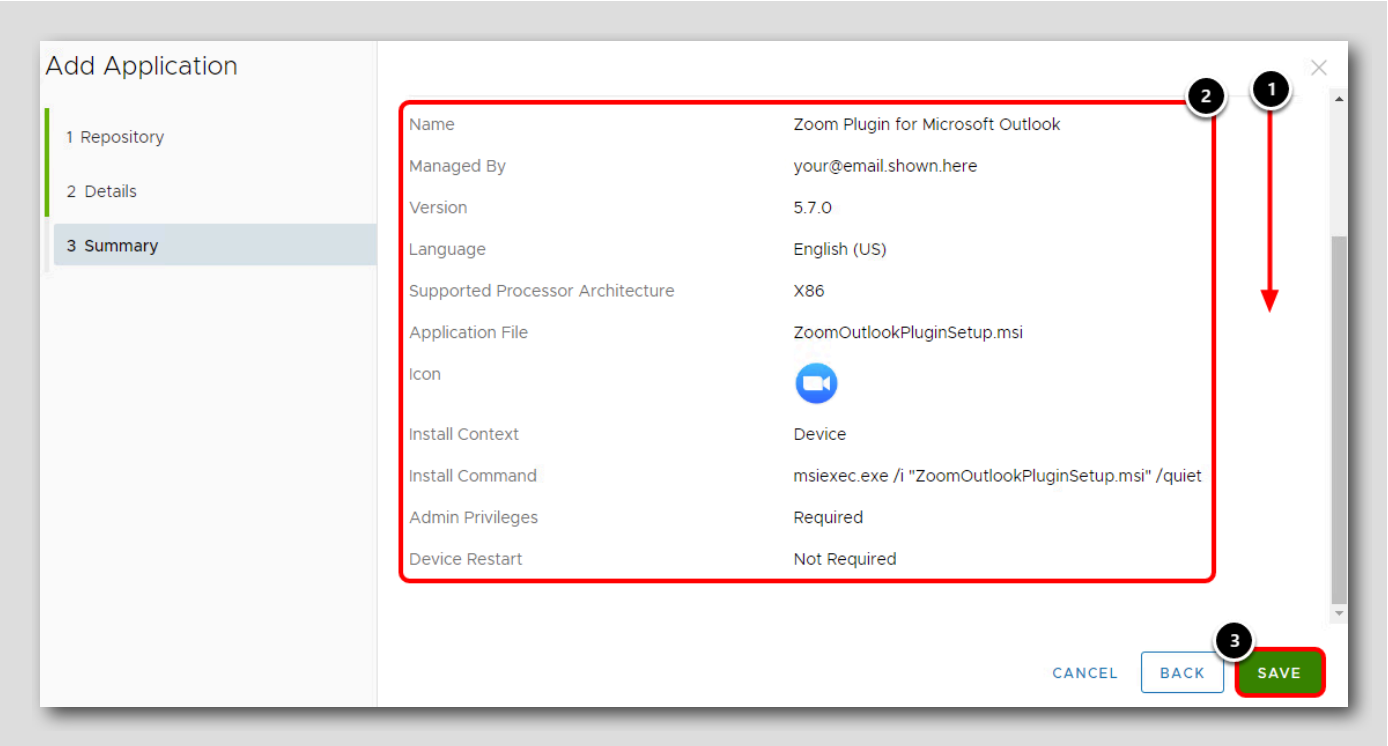
[647]



1. Review the Applications details. Keep all of the default values for this section.
2. Click **NEXT**.

Review Application Summary

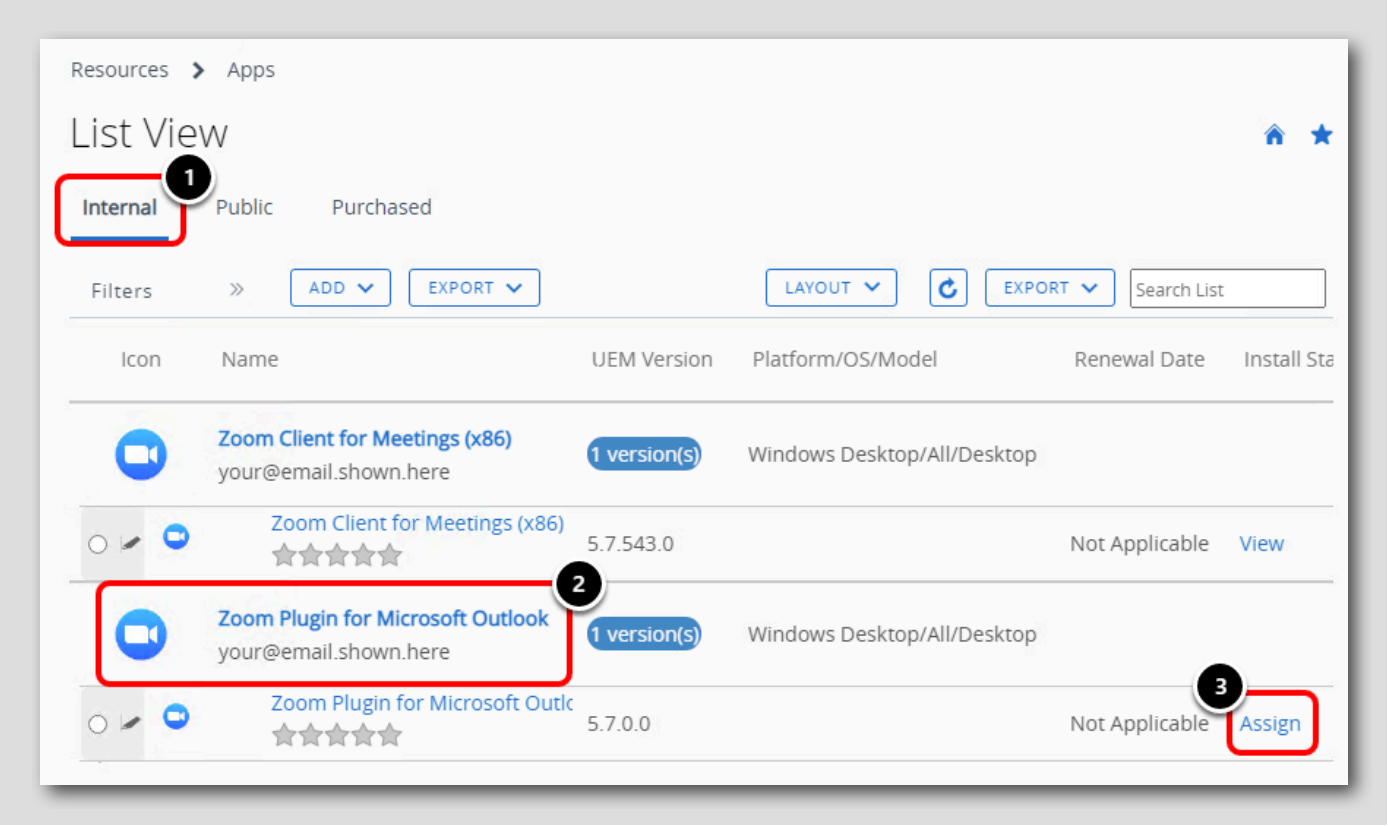
[648]



1. Scroll down to the bottom of the page.
2. **Review** the Applications Installation details. The Enterprise App Repository speeds up app delivery by pre-configuring the app installer, install command, and other configurations.
3. Click **SAVE**.

Create Application Assignment

[649]



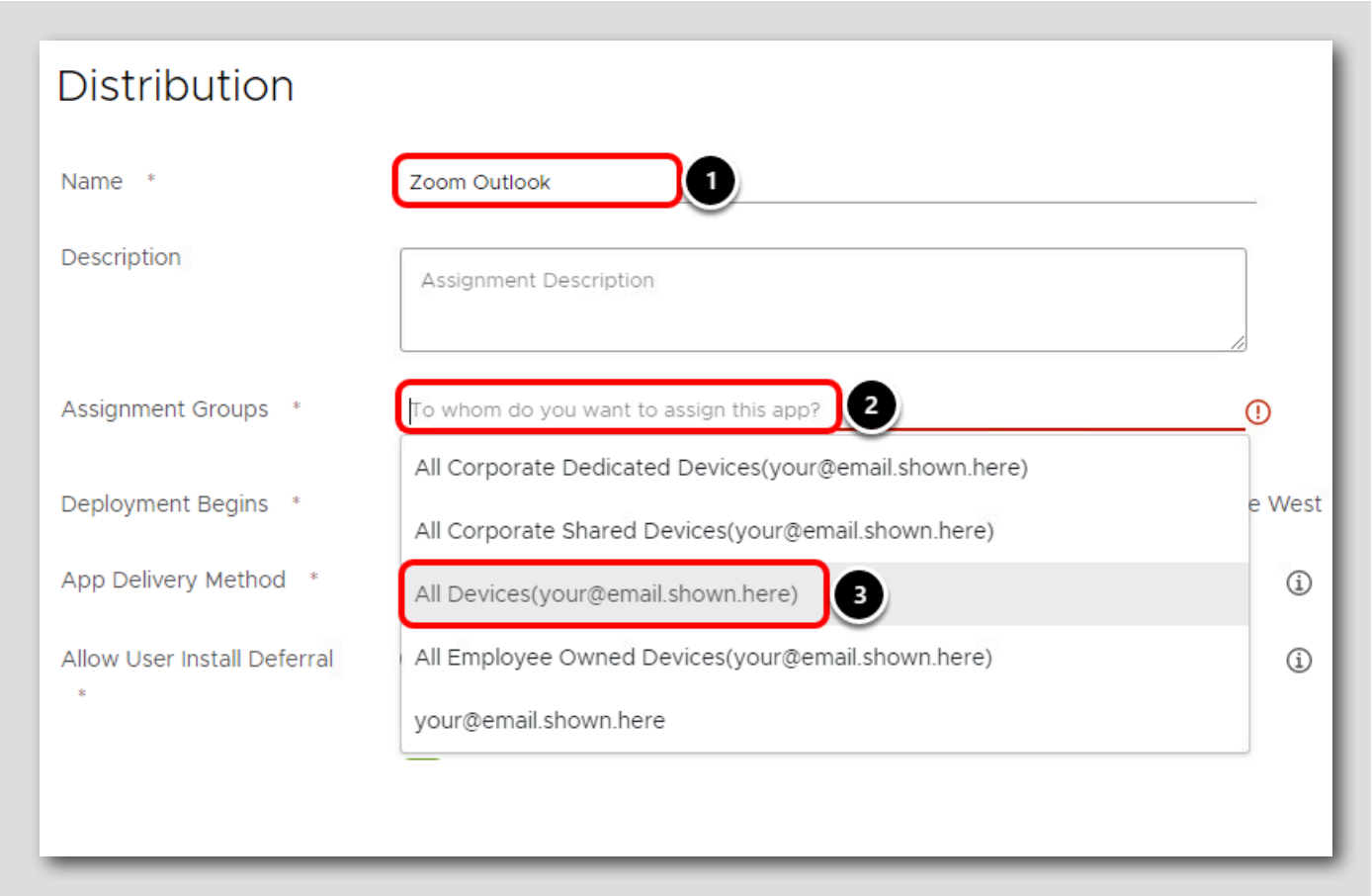
1. Ensure you are on the **Internal** tab.
2. Find the **Zoom Plugin for Microsoft Outlook** app that you just added.
3. Click **Assign** under the Install Status column.

   NOTE: You may need to scroll to the right to see the button.

The application has been added to your organization group but is not assigned to any users or devices. The following steps will have you create an application assignment to determine which devices will receive the application.

Create Application Distribution

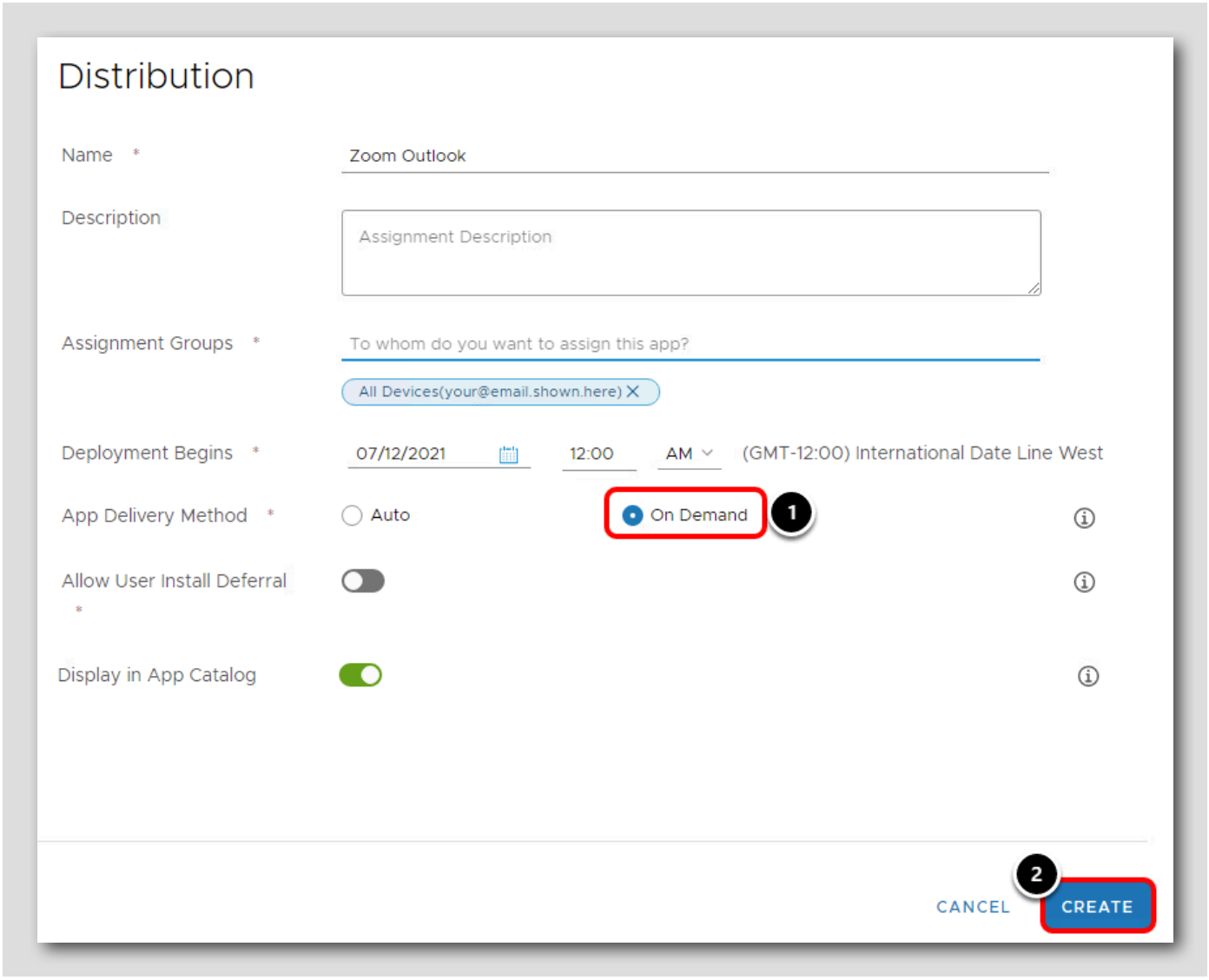
[650]



1. Enter **`Zoom Outlook`** for the distribution name.
2. Click in the **Assignment Groups** field to see a list of eligible groups.
3. Select the **All Devices (your@email.shown.here)** group. This will assign the application to all Windows 10 devices enrolled in your organization.

Create the Application Distribution

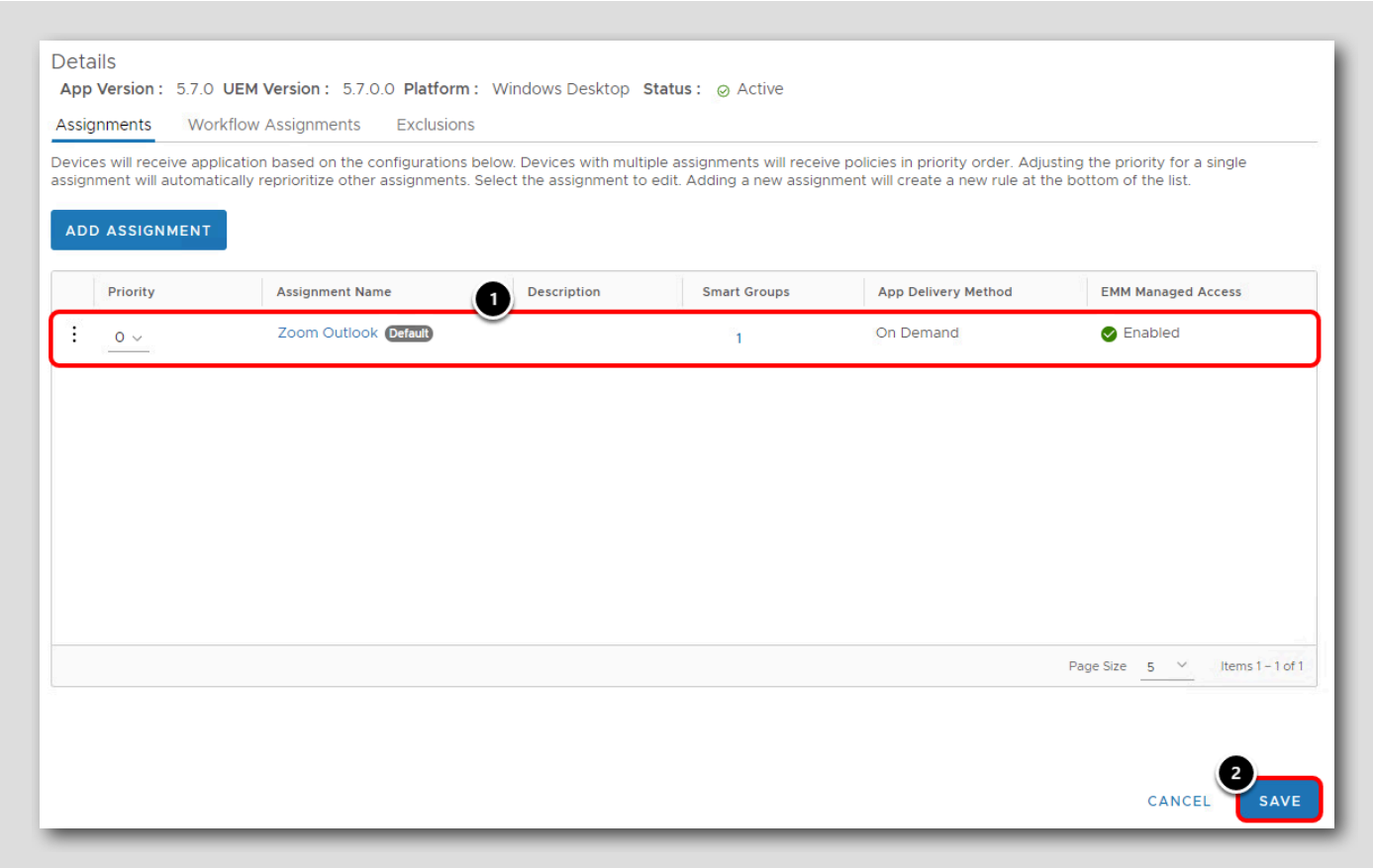
[651]



1. Leave the App Delivery Method as **On Demand**. Auto will automatically install the app on the assigned Windows 10 devices as they check-in to Workspace ONE UEM as opposed to On Demand which makes the app available in the catalog but does not automatically install the app. When you intend to distribute apps through Freestyle Orchestrator, apps should be left as On Demand, otherwise they will not install as specified in your workflows and will instead of be installed as soon as possible.
2. Click **Create**.

Review Application Distribution

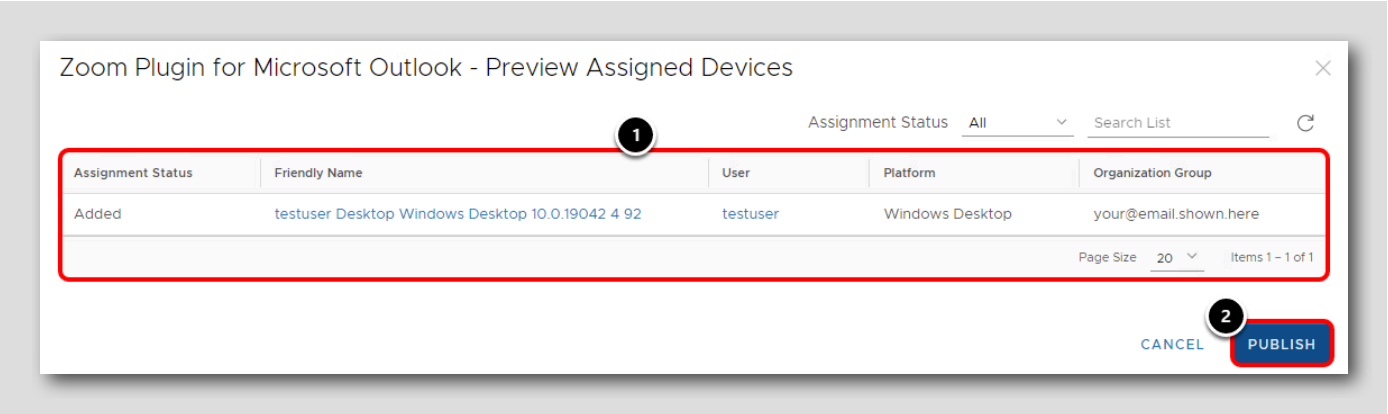
[652]



1. The list of assignments is displayed here. Confirm that the Zoom Outlook assignment you created is displayed. You can return to this section to edit, add, or remove assignments as needed.
2. Click **Save**.

Preview Assigned Devices

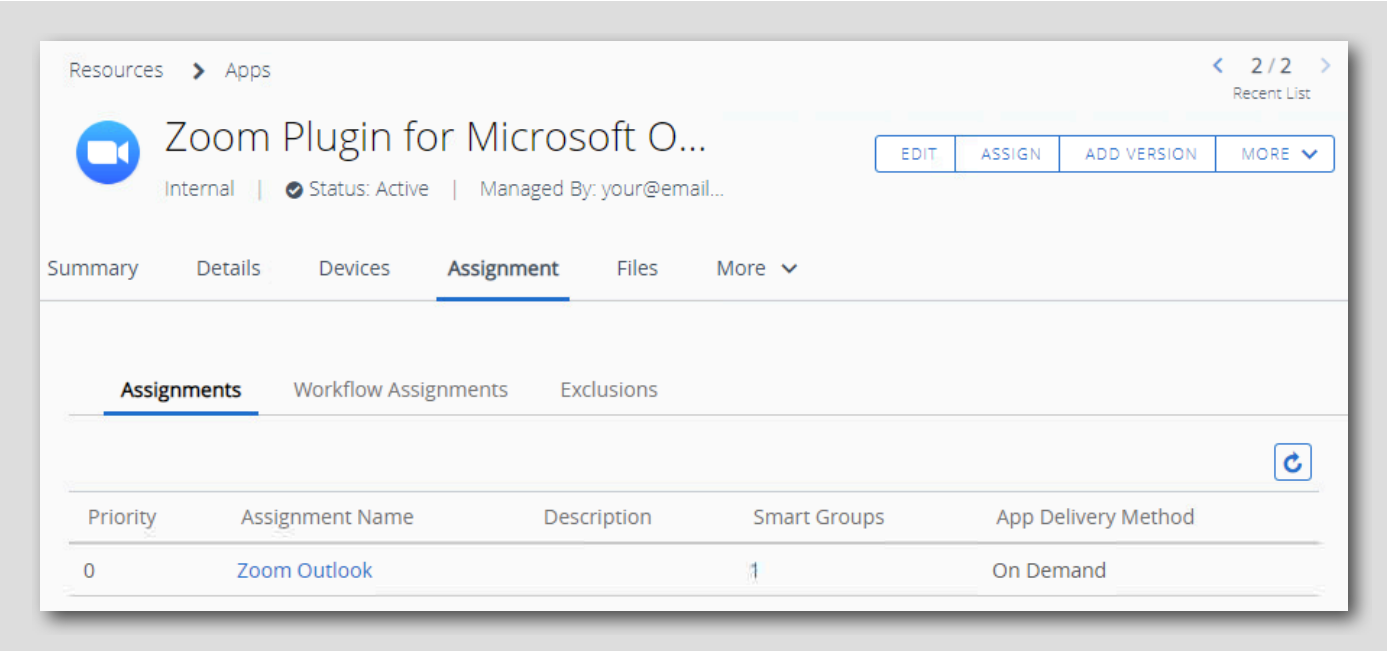
[653]



1. A preview of devices that will receive this app is displayed here. A single device record is shown as you have only enrolled one device in your organization.
2. Click **Publish**.

Confirm Device Assignment

[654]



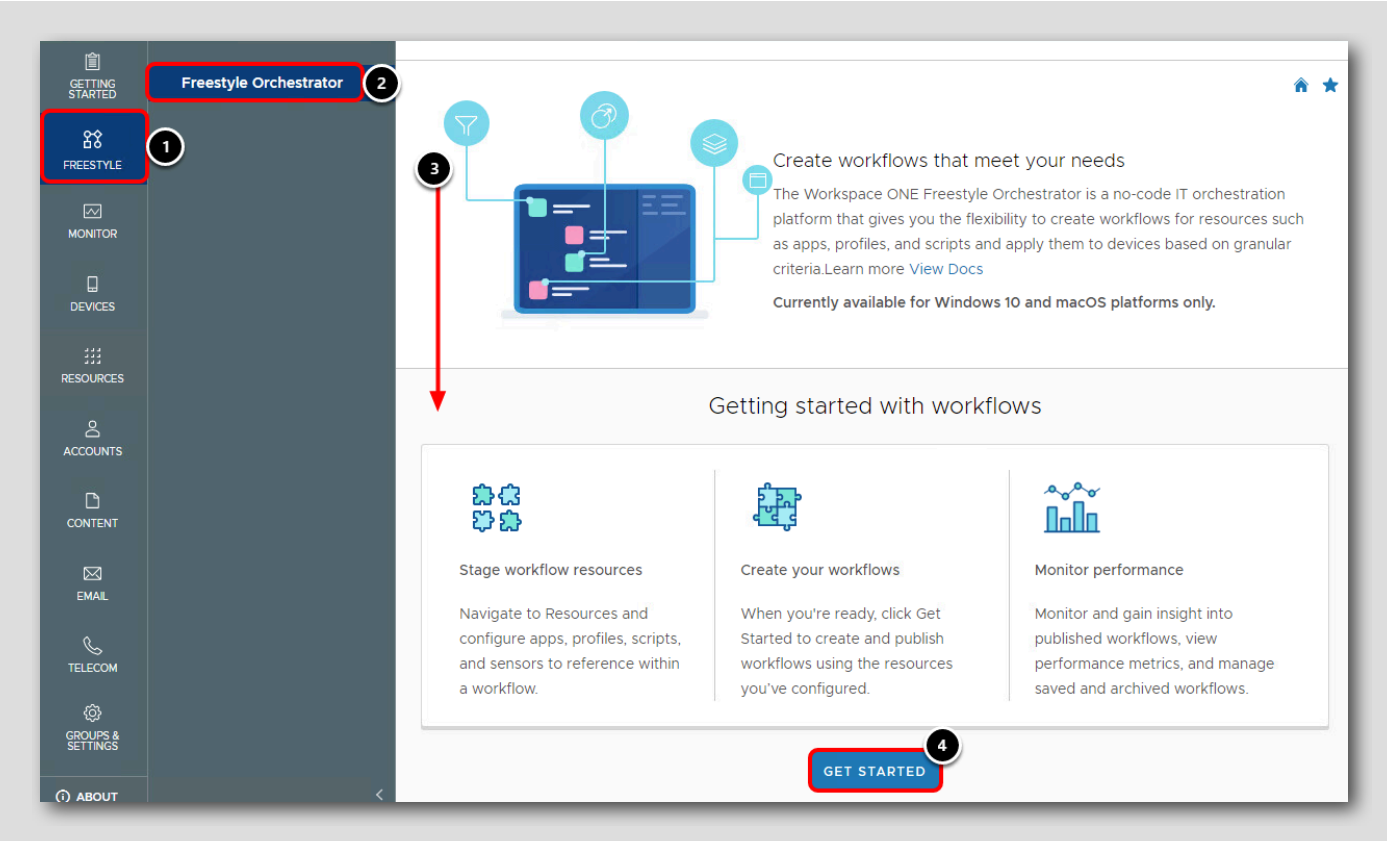
The **Zoom Plugin for Microsoft Office** application has been created and assigned to the All Devices smart group with the On Demand app delivery method, meaning all assigned devices can have the application delivered to them but it will not be done automatically when the devices enroll.

Remember that we chose to leave the app assignment as On Demand because we intend to deliver the Zoom Plugin for Microsoft Office through a Freestyle Orchestrator Workflow, so we want to allow the workflow to determine if and when the app is installed rather than automatically installing it after enrollment.

Continue to the next step.

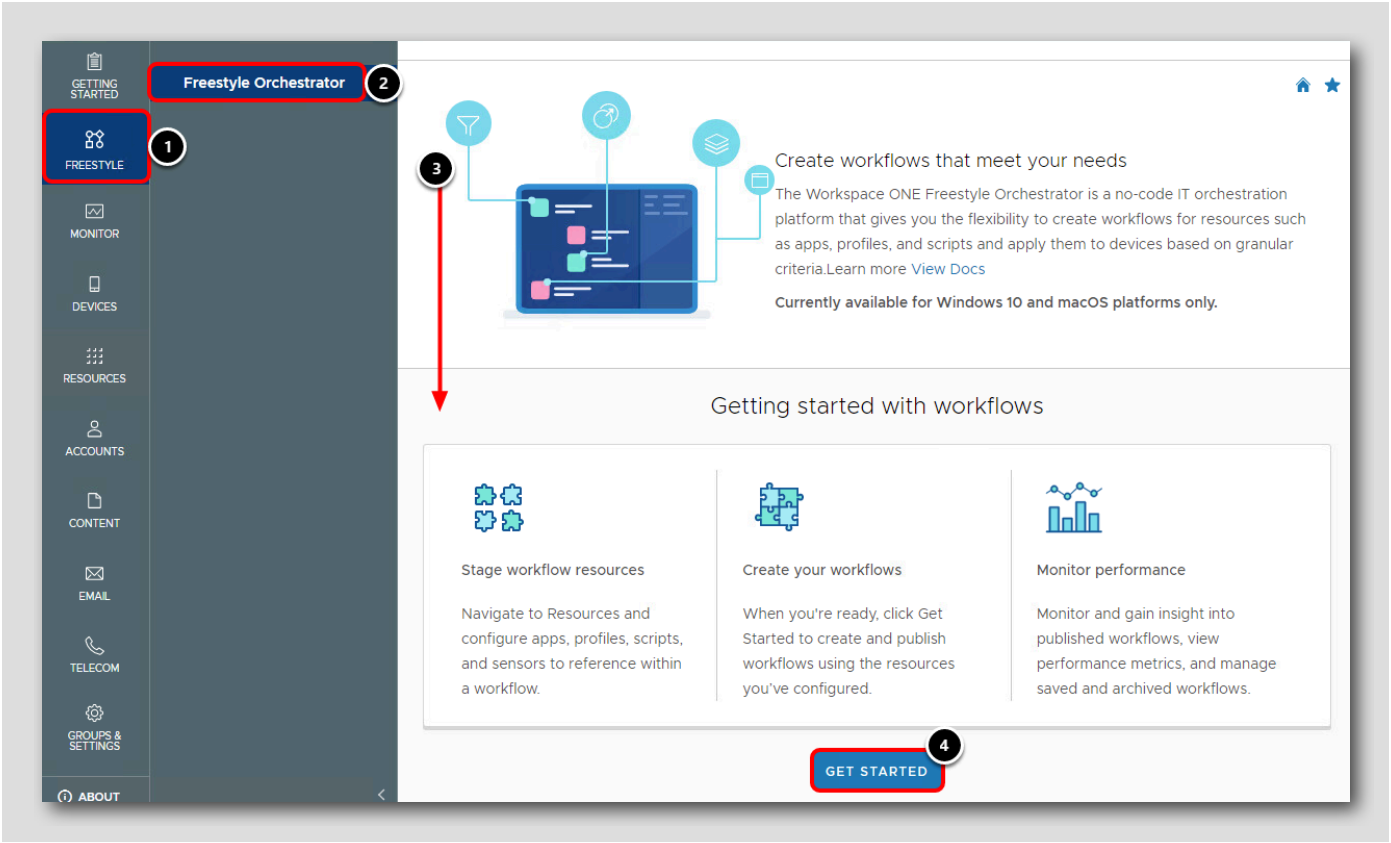
Create a Workflow with Freestyle Orchestrator

[655]



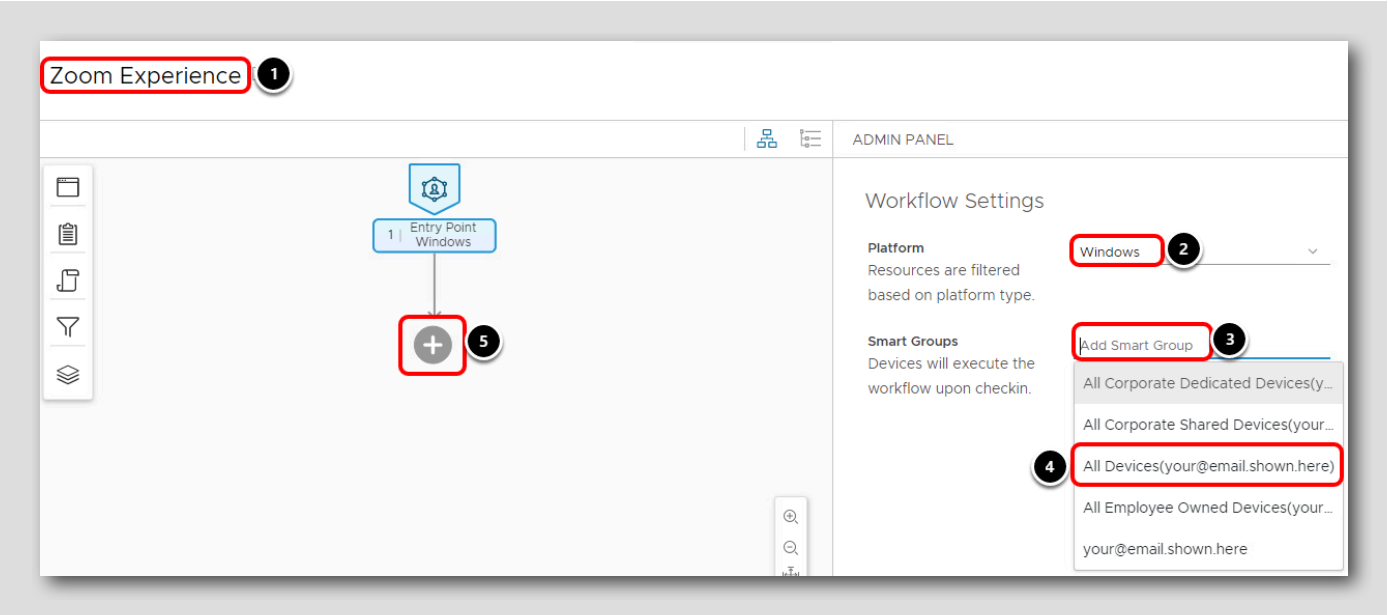
You will now build a workflow in Freestyle Orchestrator that will distribute the Zoom Plugin for Microsoft Outlook to your devices only if the required Zoom application is installed. The conditional checks and step logic of workflows allows you to intelligently distribute resources in the manner in which they are required.

1. Click **Freestyle**
2. Click **Freestyle Orchestrator**
3. Scroll down past the Freestyle Orchestrator Getting Started information
4. Click **Get Started**


GETTING STARTED
FREESTYLE
MONITOR
DEVICES
RESOURCES
ACCOUNTS
CONTENT
EMAIL
TELECOM
GROUPS & SETTINGS
ABOUT
Freestyle Orchestrator
1
2
3
4
Create workflows that meet your needs
The Workspace ONE Freestyle Orchestrator is a no-code IT orchestration platform that gives you the flexibility to create workflows for resources such as apps, profiles, and scripts and apply them to devices based on granular criteria.Learn more View Docs
Currently available for Windows 10 and macOS platforms only.
Getting started with workflows
Stage workflow resources
Navigate to Resources and configure apps, profiles, scripts, and sensors to reference within a workflow.
Create your workflows
When you're ready, click Get Started to create and publish workflows using the resources you've configured.
Monitor performance
Monitor and gain insight into published workflows, view performance metrics, and manage saved and archived workflows.
GET STARTED

Setup the Workflow

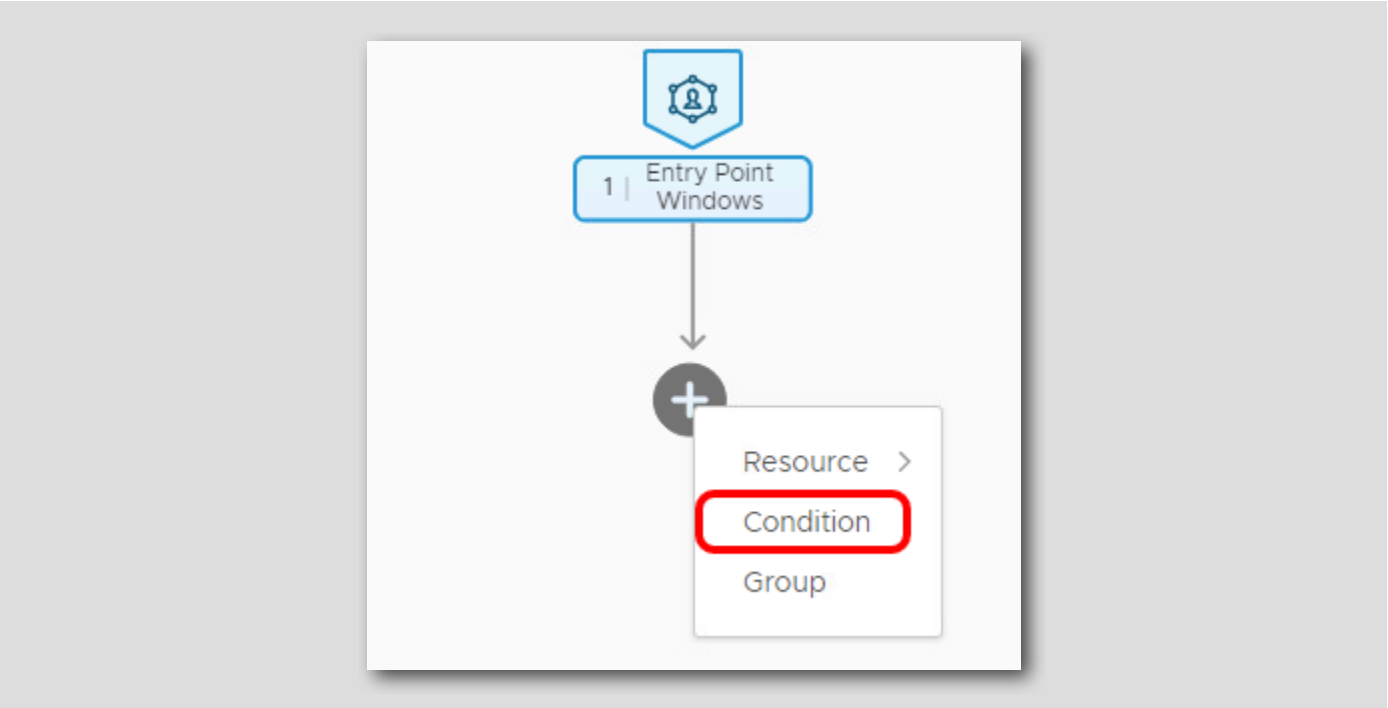
[656]



1. Give the Workflow the name **`Zoom Experience`**
2. Select **Windows** for the Platform
3. Click the **Smart Groups** field to see a list of eligible Smart Groups
4. Select **All Devices (your@email.shown.here)** from the list
5. Click the **+ Sign** button to build out the next step

Add Workflow Condition

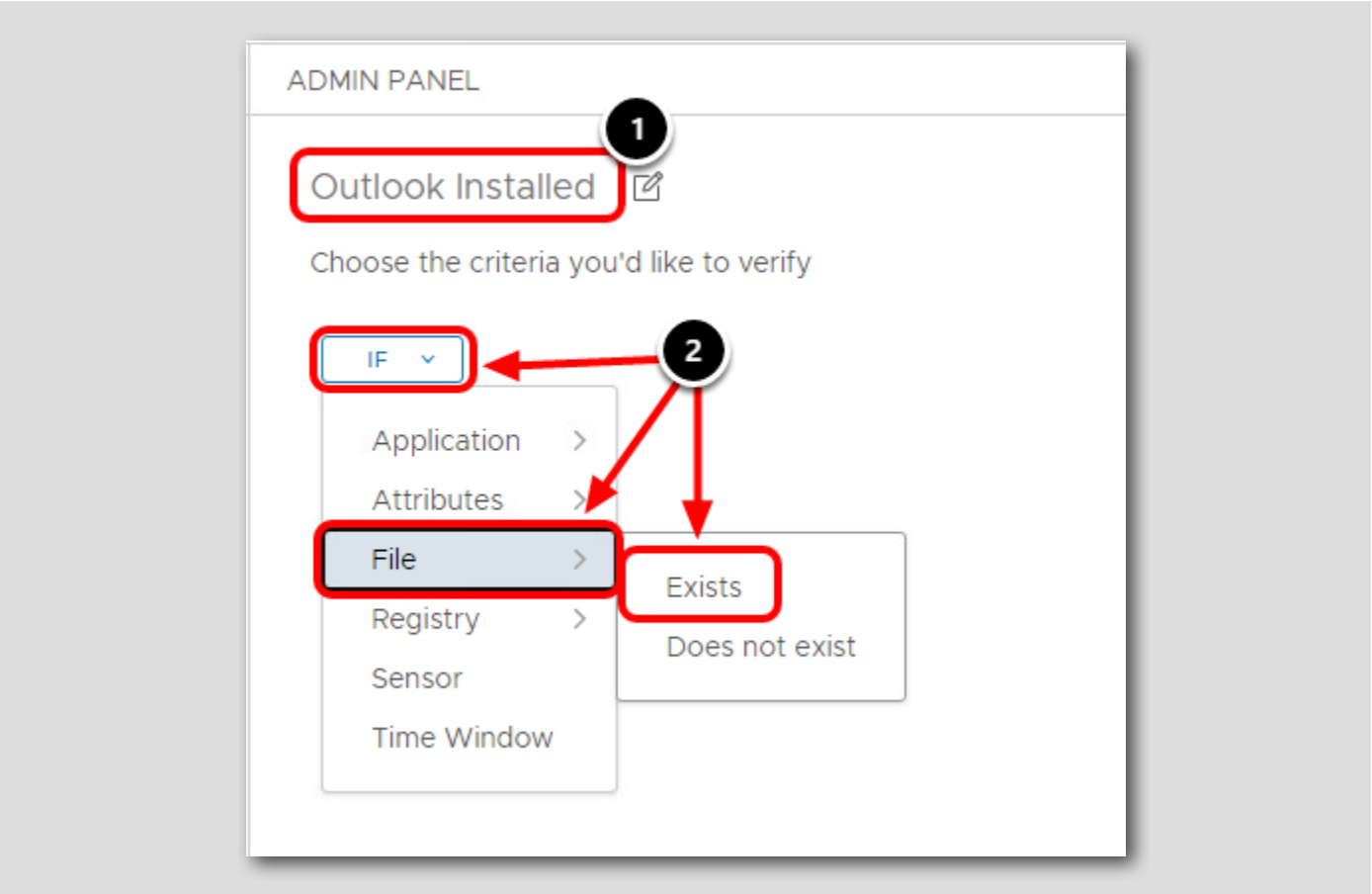
[657]



Click **Condition**. This will allow you to create and configure a Condition (If / Else) for your workflow.

Add File Exists Condition

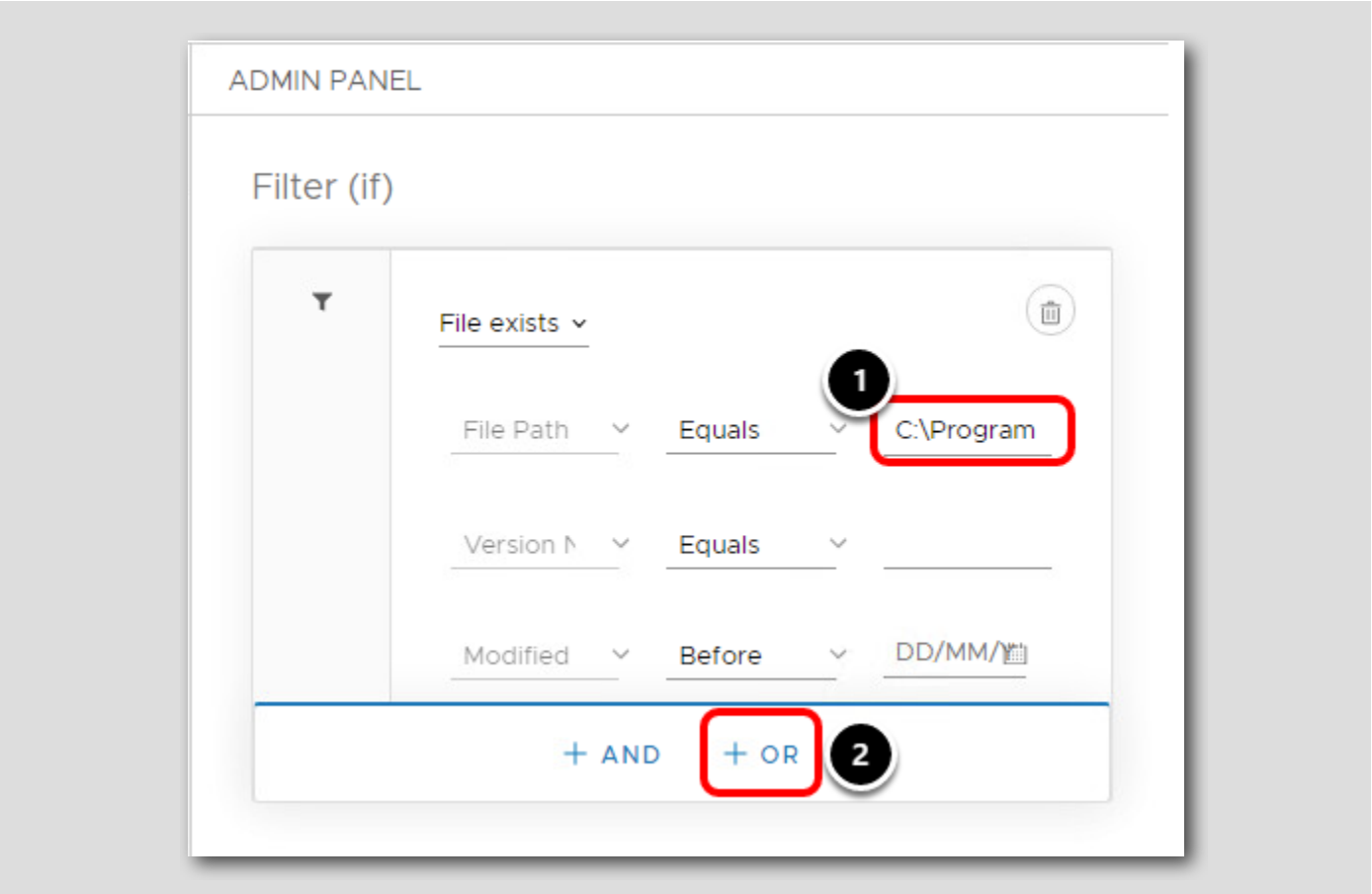
[658]



1. Give the condition the name **`Outlook Installed`**
2. Click the **IF** button to add a criteria, then select **File** then **Exists** from the dropdown list

Add File Condition Value

[659]



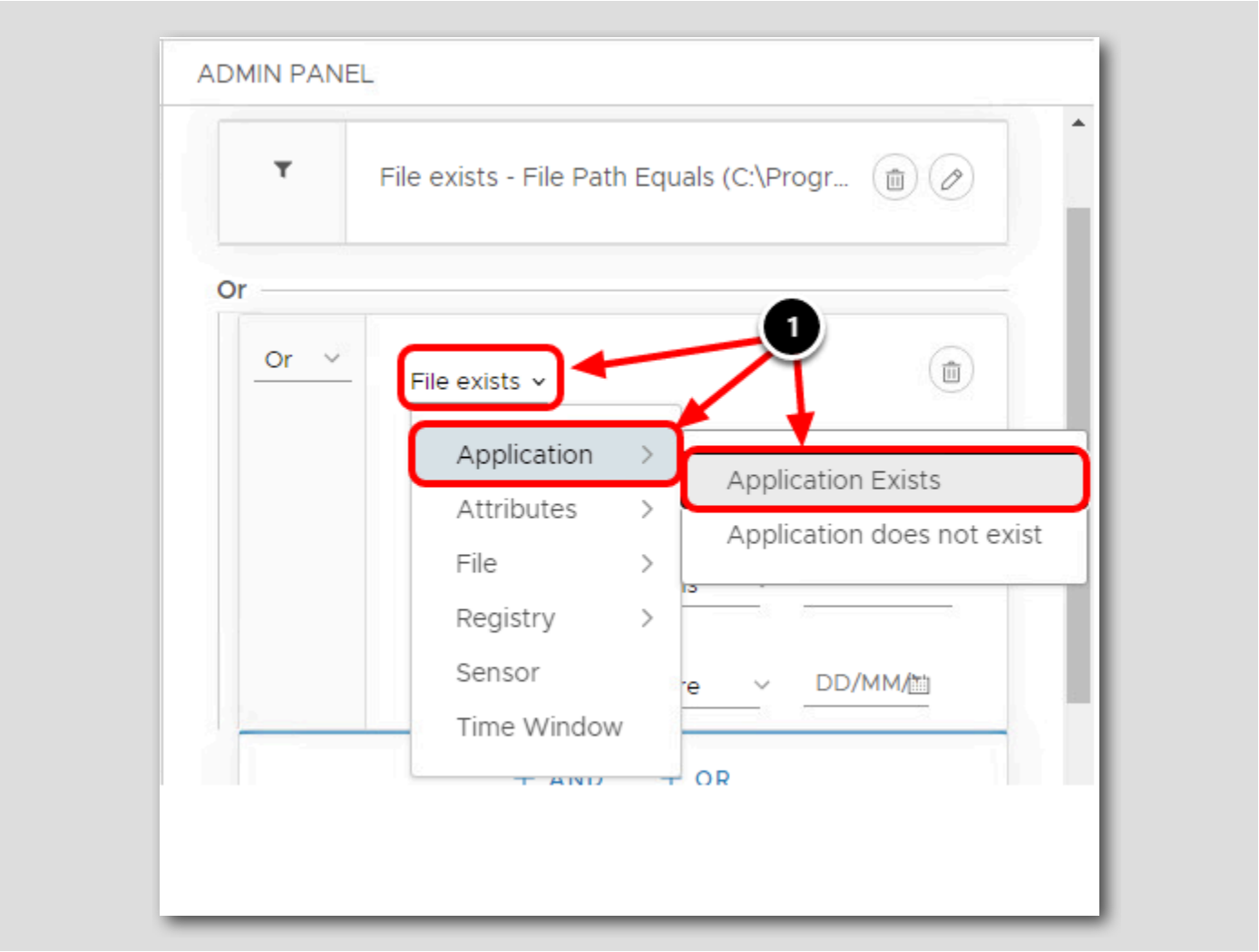
1. In the File Path equals section, enter in **`C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE`**.

   NOTE: Remember that you can copy-paste or click to highlight the text and drag-and-drop from the manual to avoid error!

2. Select OR

Add Application Exists Condition Value

[660]

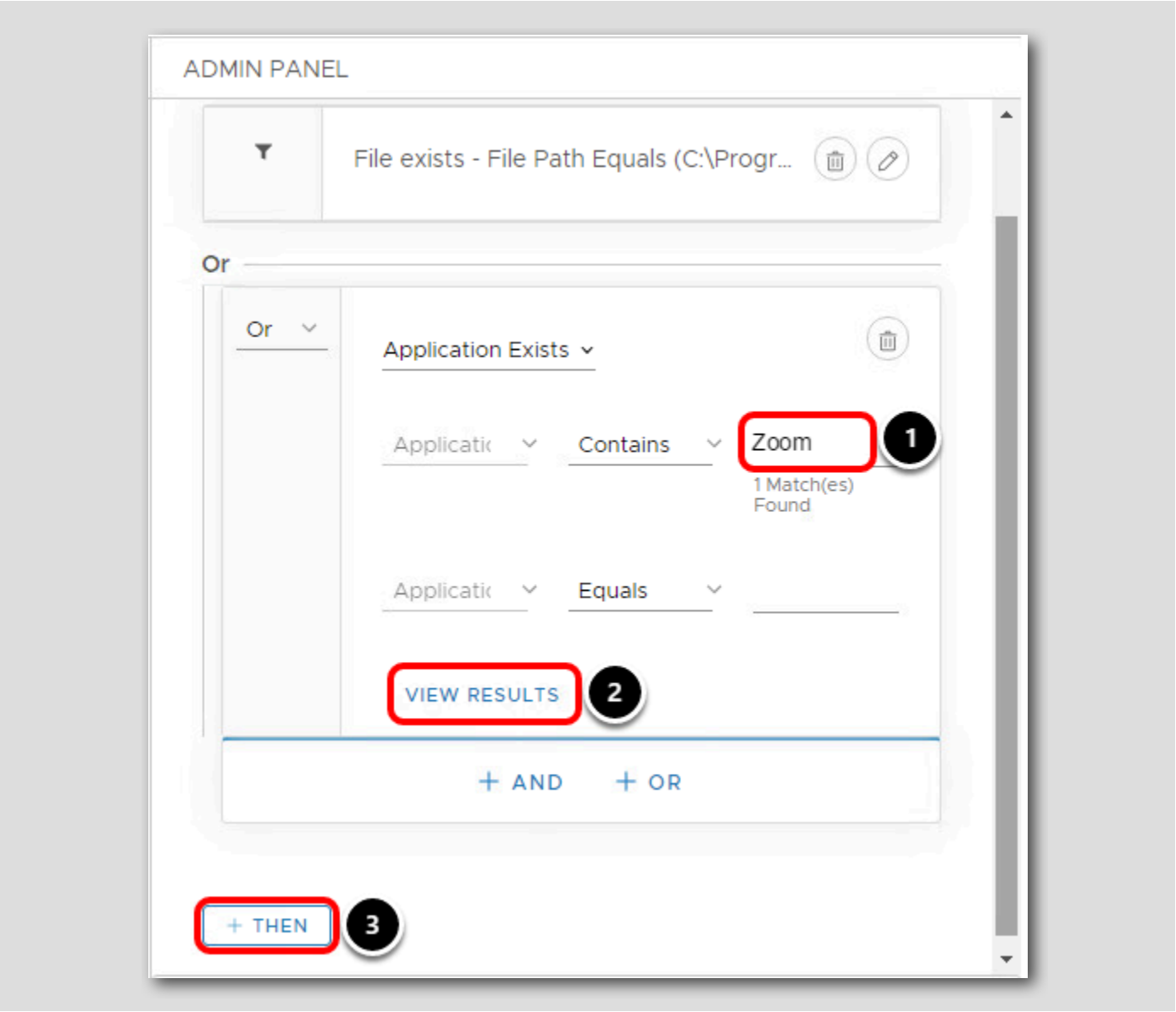


Under the new Or section:

1. Click the **File Exists** Condition, then select **Application > Application Exists**

Add the Or Condition

[661]



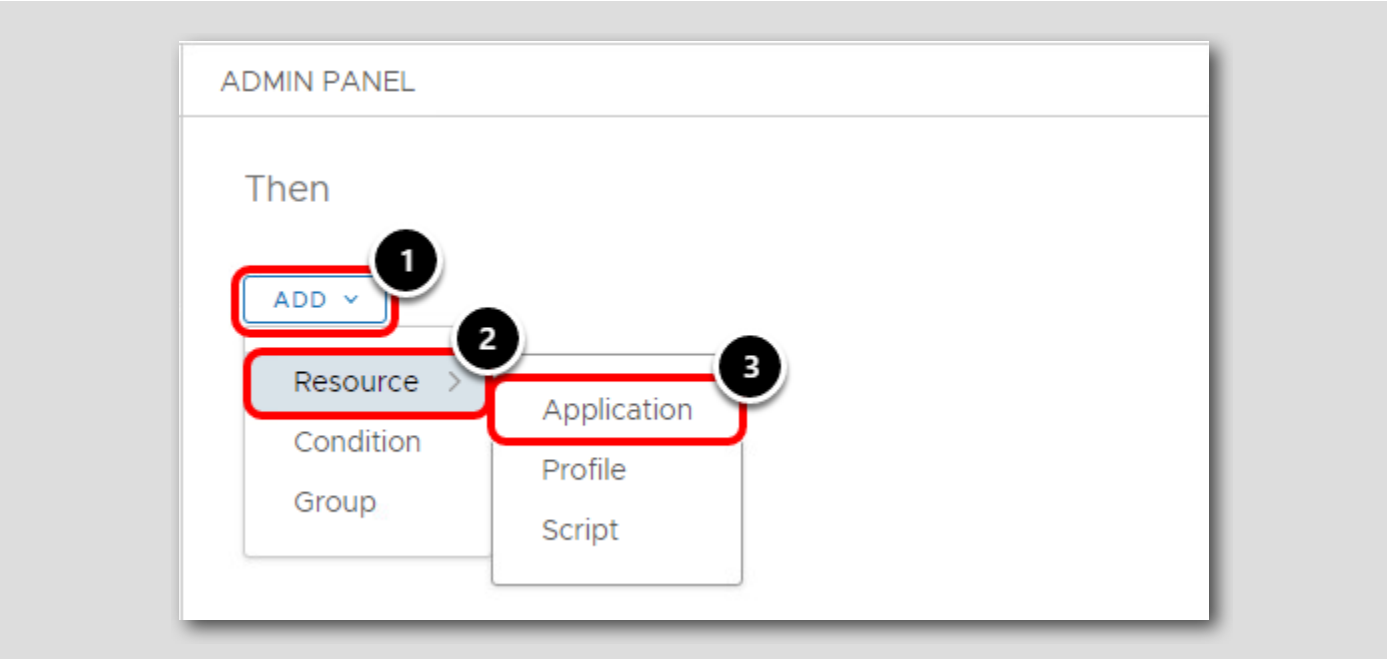
1. In the Application Name Contains field, enter **Zoom**. Notice the matched number of applications found underneath the field.

   NOTE: Ensure you use the exact capitalization as shown (**Zoom**) and confirm 1 Match(es) Found appears before continuing!

2. To see these results, click **View Results**. Click the **< Back** button on the page to return to configuring the **Or** action.
3. To configure an action for this If statement, select **Then**

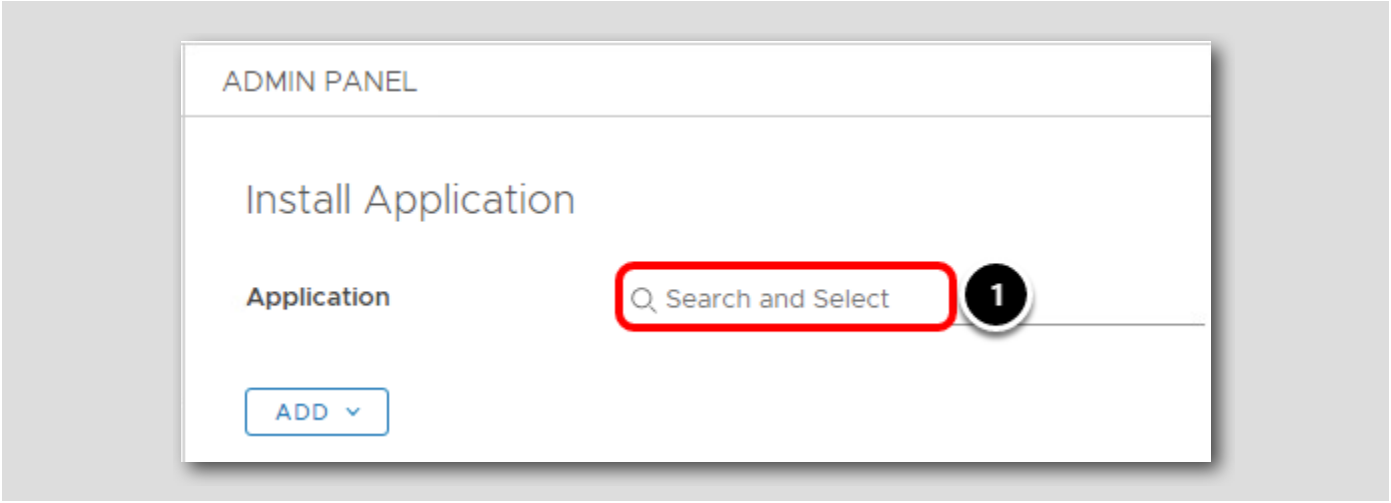
Then Action: Install Zoom Plugin for Microsoft Outlook

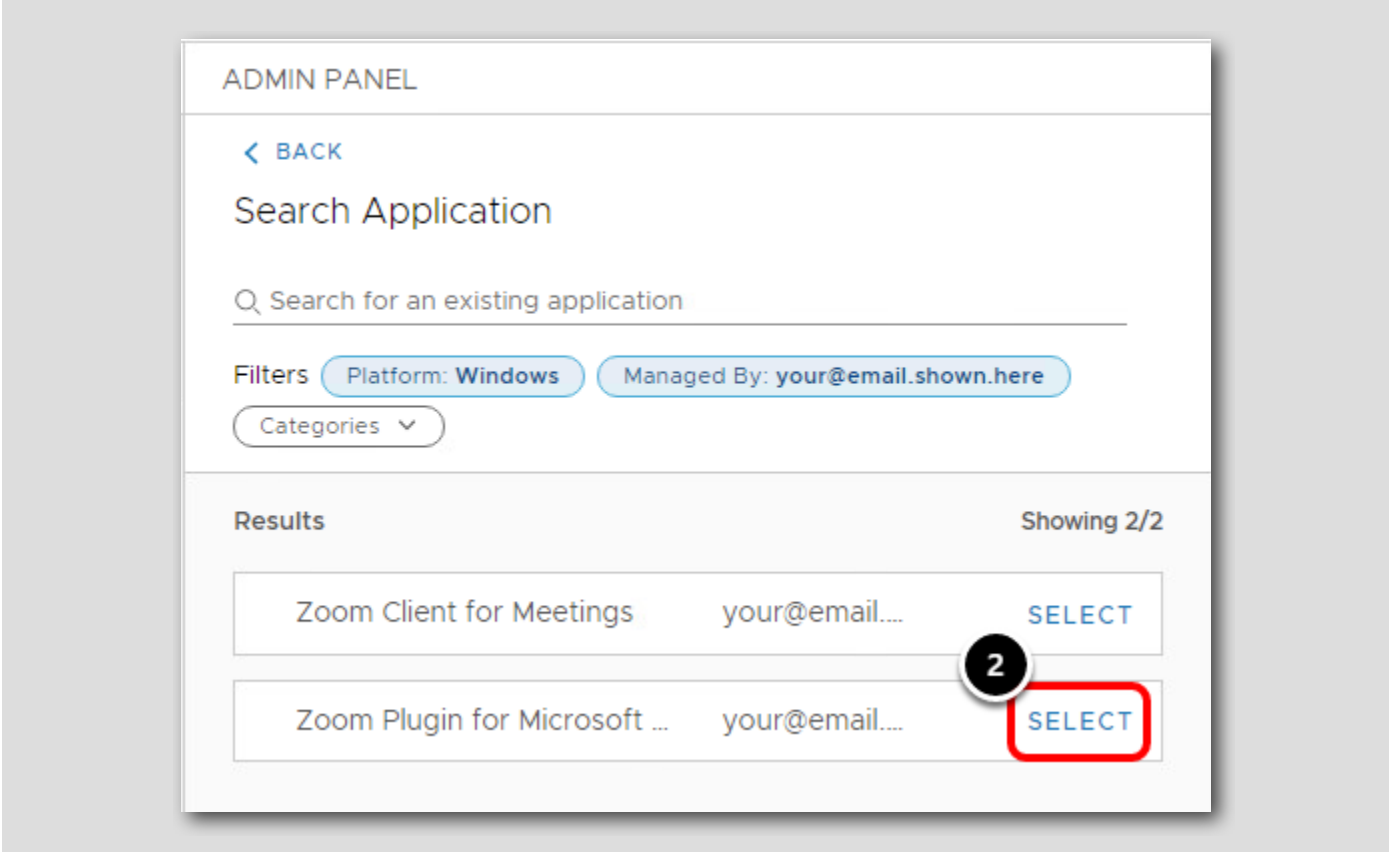
[662]



1. Click the **Add** dropdown
2. Select **Resource**
3. Click **Application**

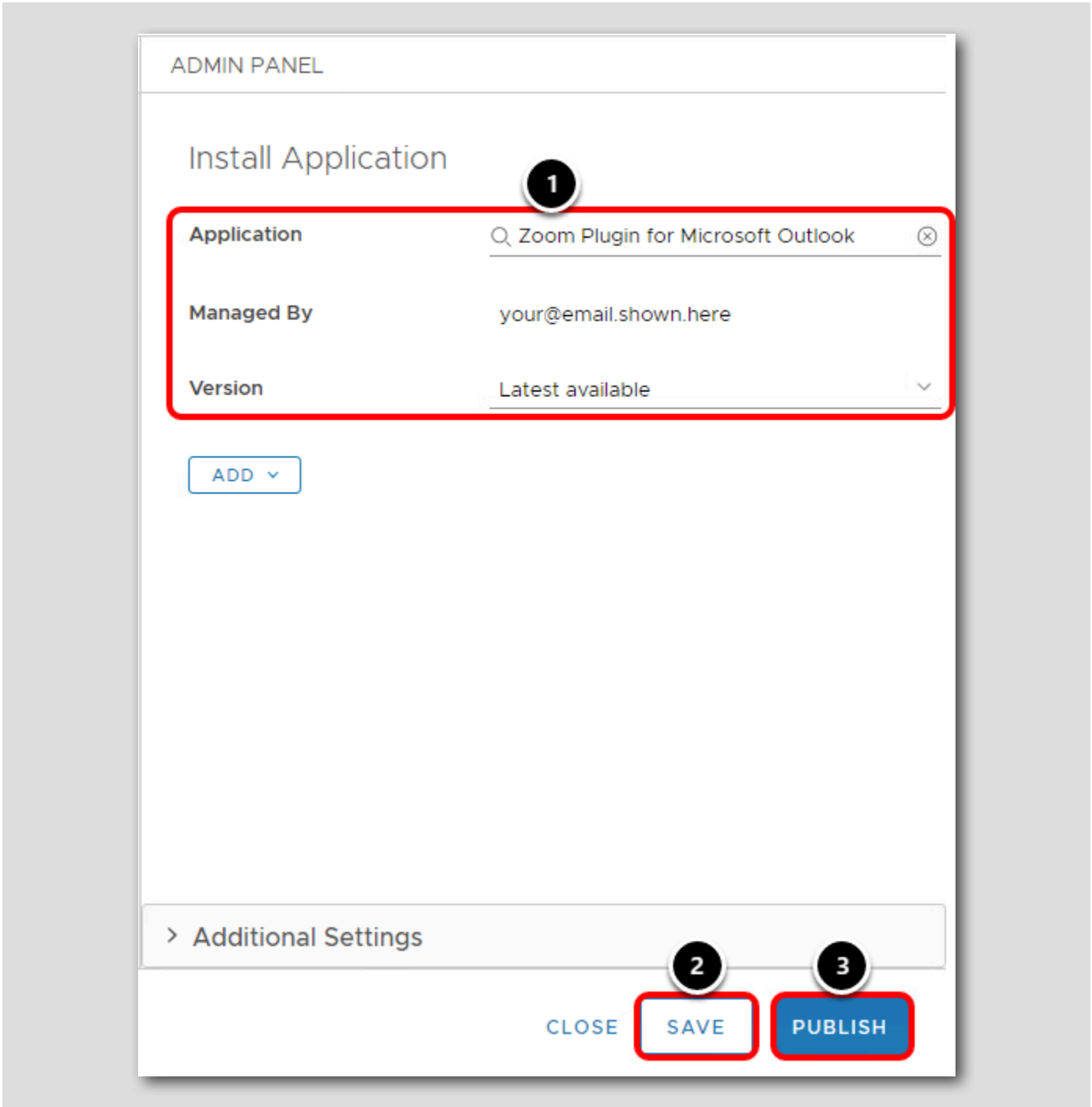
Select Zoom Plugin for Microsoft Outlook [663]





1. Click the Application search field
2. Select the **Zoom Plugin for Microsoft Outlook** app

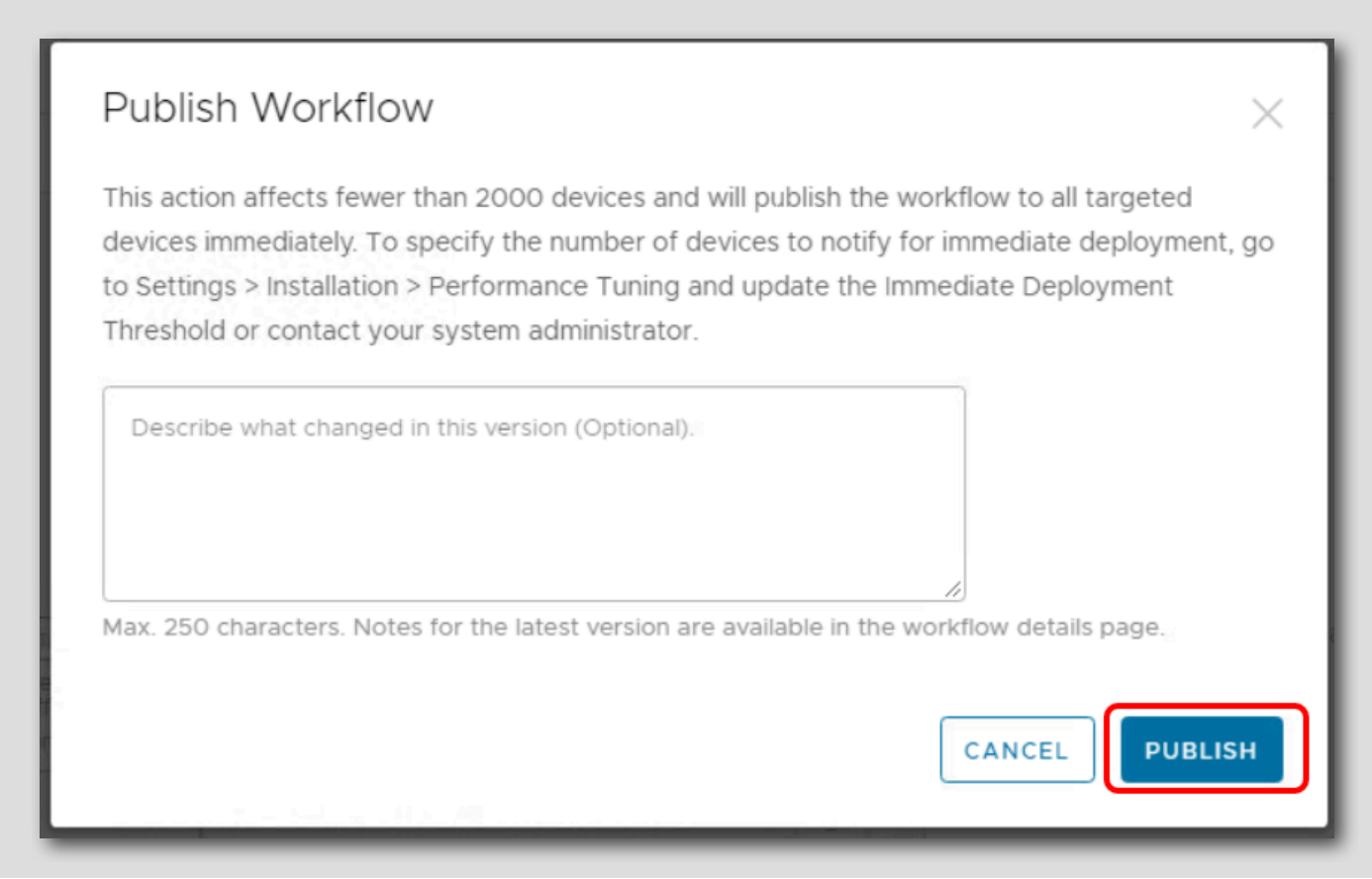
Review Application Install settings [664]



1. Review the application details. The Version is using Latest available, which means if multiple versions of the Zoom Plugin for Microsoft Outlook app are uploaded, the latest application will be used. You can also specify a version to use in this use case as well.
2. Click **Save**.
3. Click **Publish**.

Publish Workflow

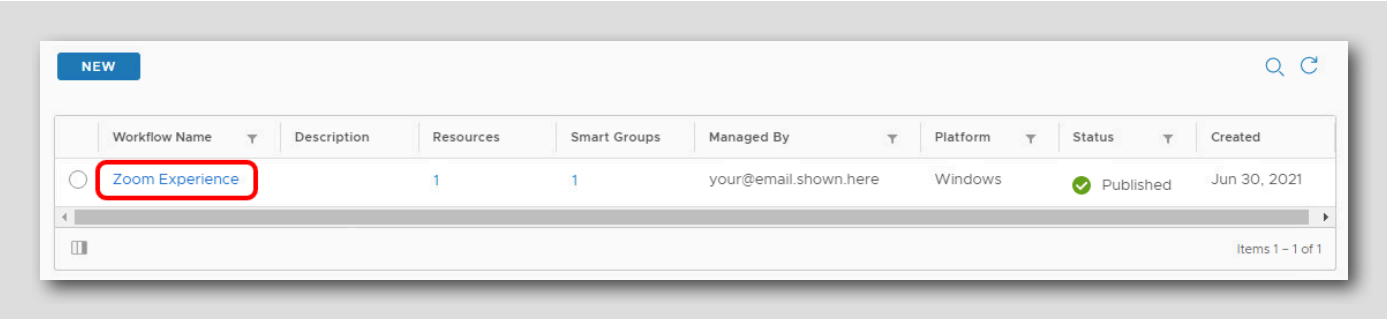
[665]



Select **Publish**.

Review the Workflow

[666]

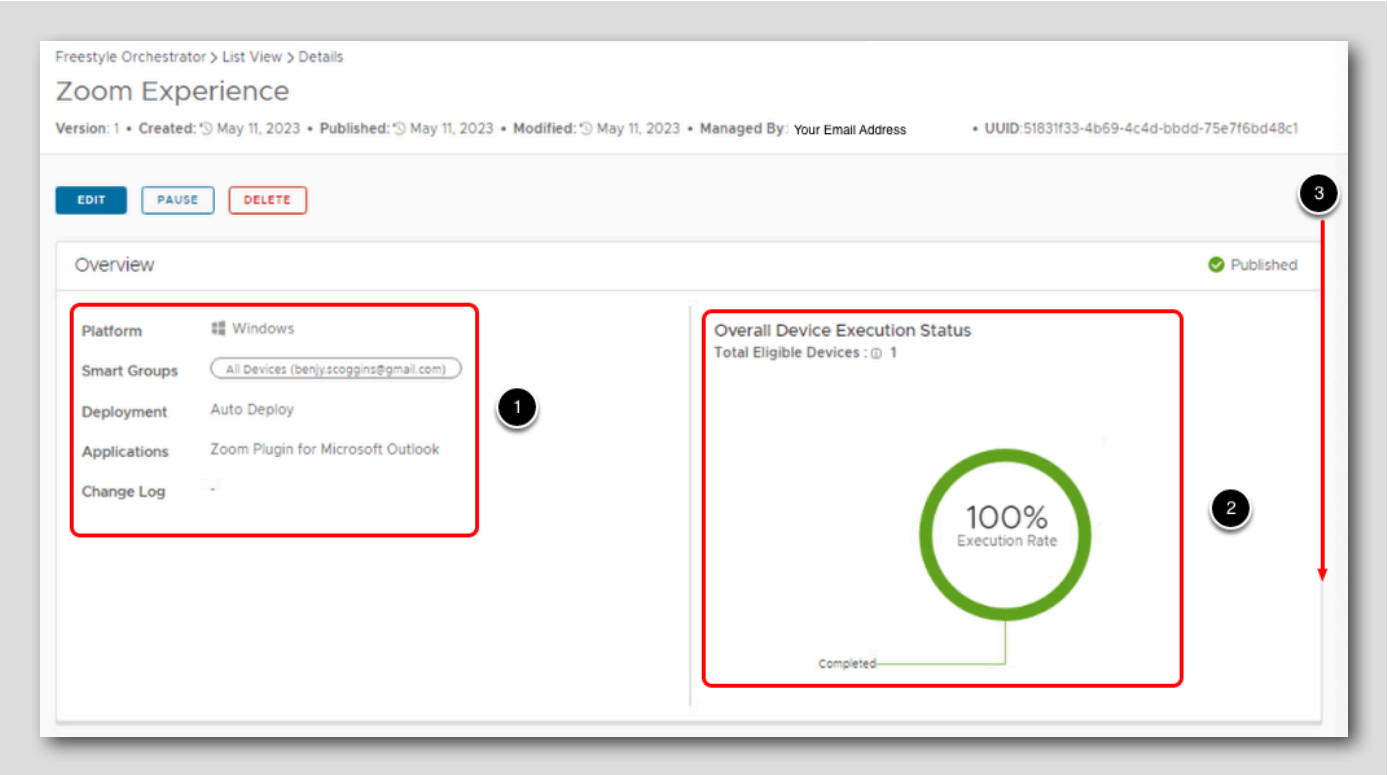


A list of workflows you create will be available on this page, which displays their name, resources, assigned smart groups, target platform, and their status.

Click the **Zoom Experience** workflow to select the workflow you just created.

Review Workflow Overview

[667]



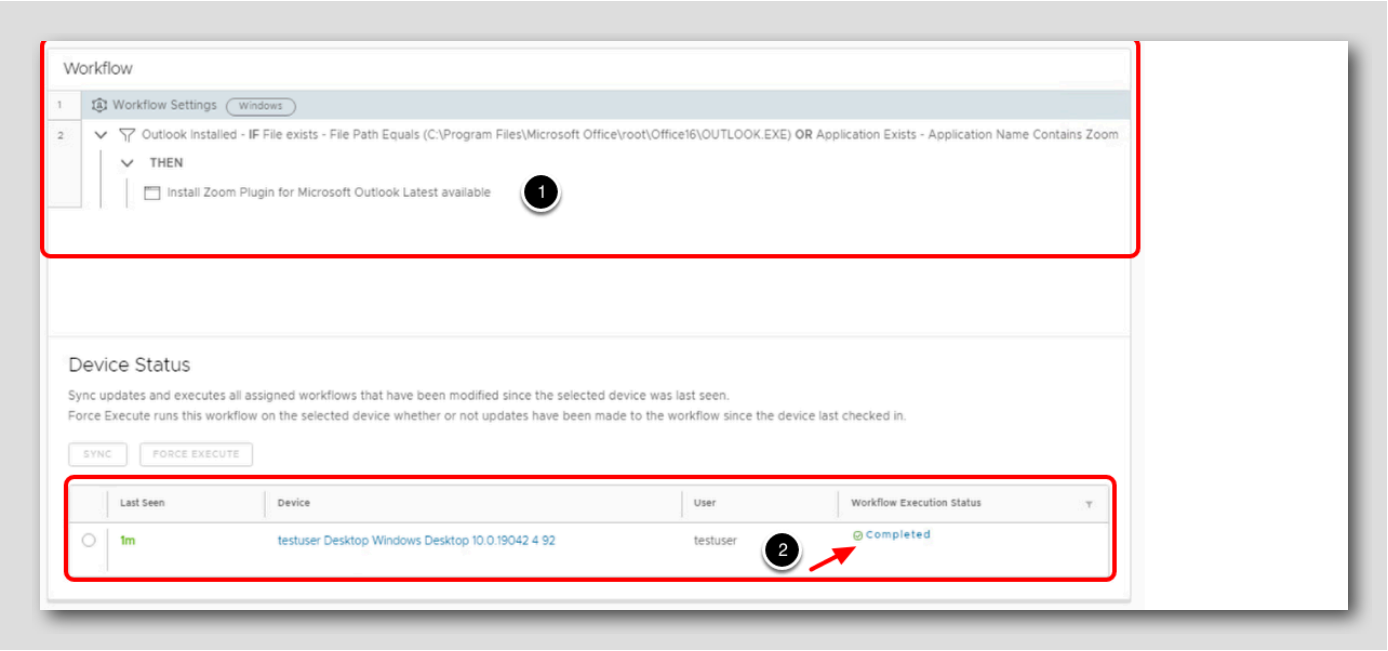
1. Review the Workflows Configurations, which displays the target platform, assigned smart groups, and applications that belong to this workflow.
2. Review the Workflow Device Execution Status, which displays the number of assigned devices and how many have received the workflow.

   NOTE: You may initially observe "Device distribution is unavailable" under the Overall Device Execution Status. You will address this in an upcoming step.

   NOTE: Data may take up to 4 hours to update based on when devices check-in. To force sync your workflow to devices, you can query workflows for a device through the Device Details page or force sync from hub / device.
3. Scroll down

Review the Workflow Details and Devices

[668]



1. Review the **Workflow details**
    - Review the Conditions you configured: If file exists OR App name contains Zoom, and the Install Zoom Plug in for Microsoft Outlook Command.
2. Review the **Device Status** of the Workflow.

   NOTE: The Device Status may show no devices if the workflow has not executed yet. You will address this in an upcoming step.

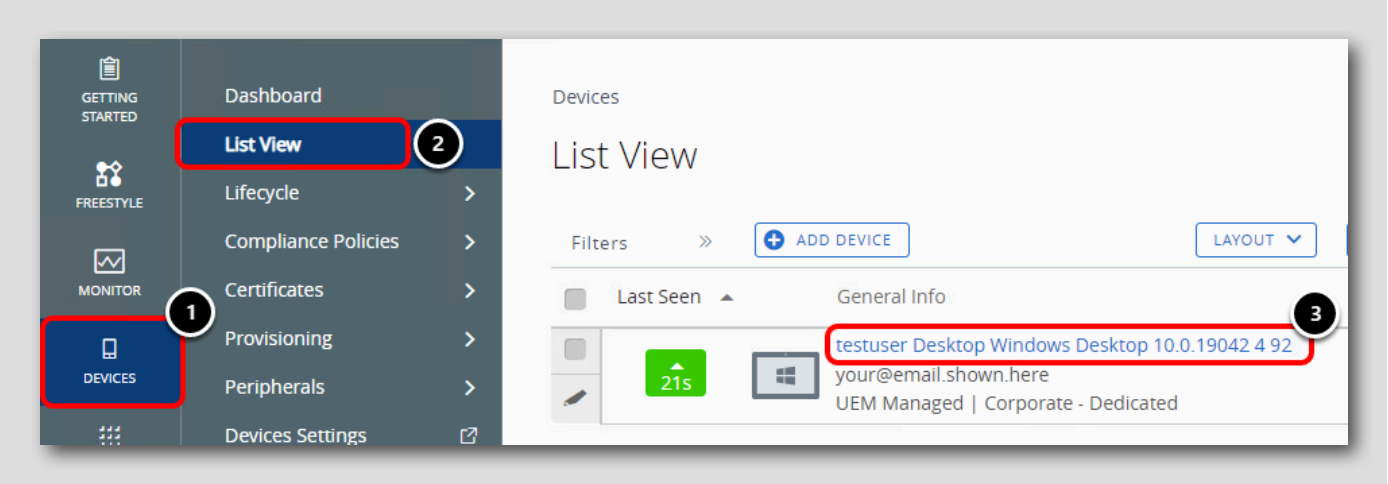
Verifying the Workflow Execution in Workspace ONE UEM

[669]

You will now verify the execution of the Workflow and force the execution if needed by querying the device from the Workspace ONE UEM administrator console. Workflows can take some time to execute and report data back to the console, so this will be used to speed up the execution.

Navigate to the device

[670]

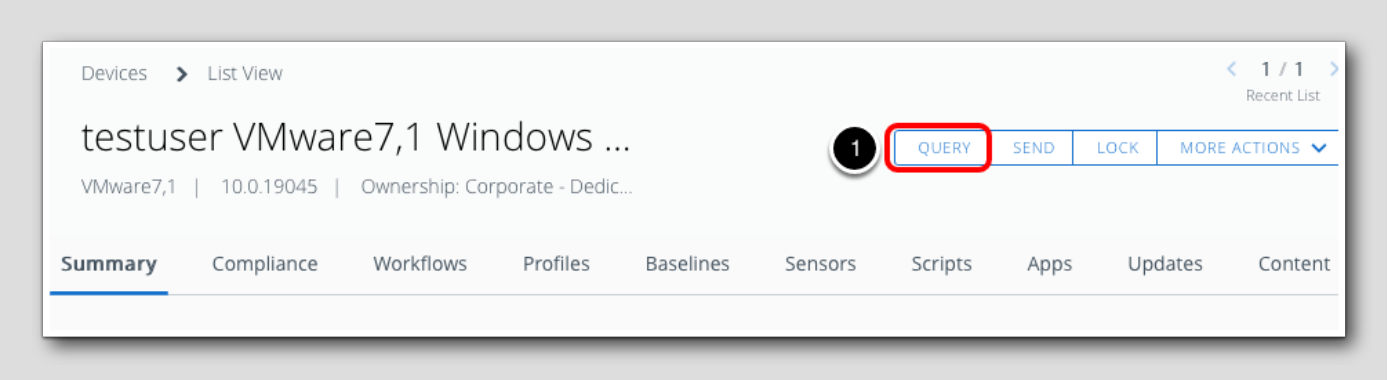


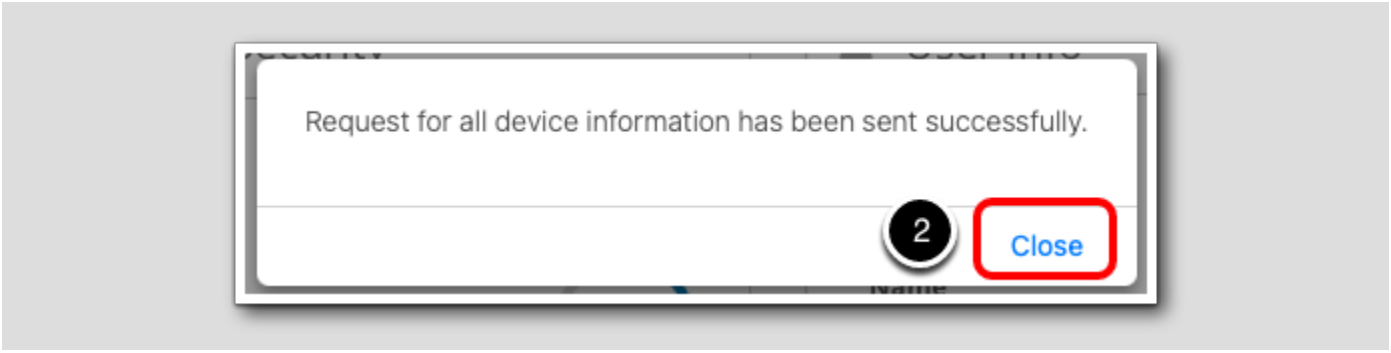
In the Workspace ONE UEM Administrator Console:

1. Click **Devices**
2. Click **List View**
3. Click the **enrolled device name** to see the device details.

Query Device Details

[671]

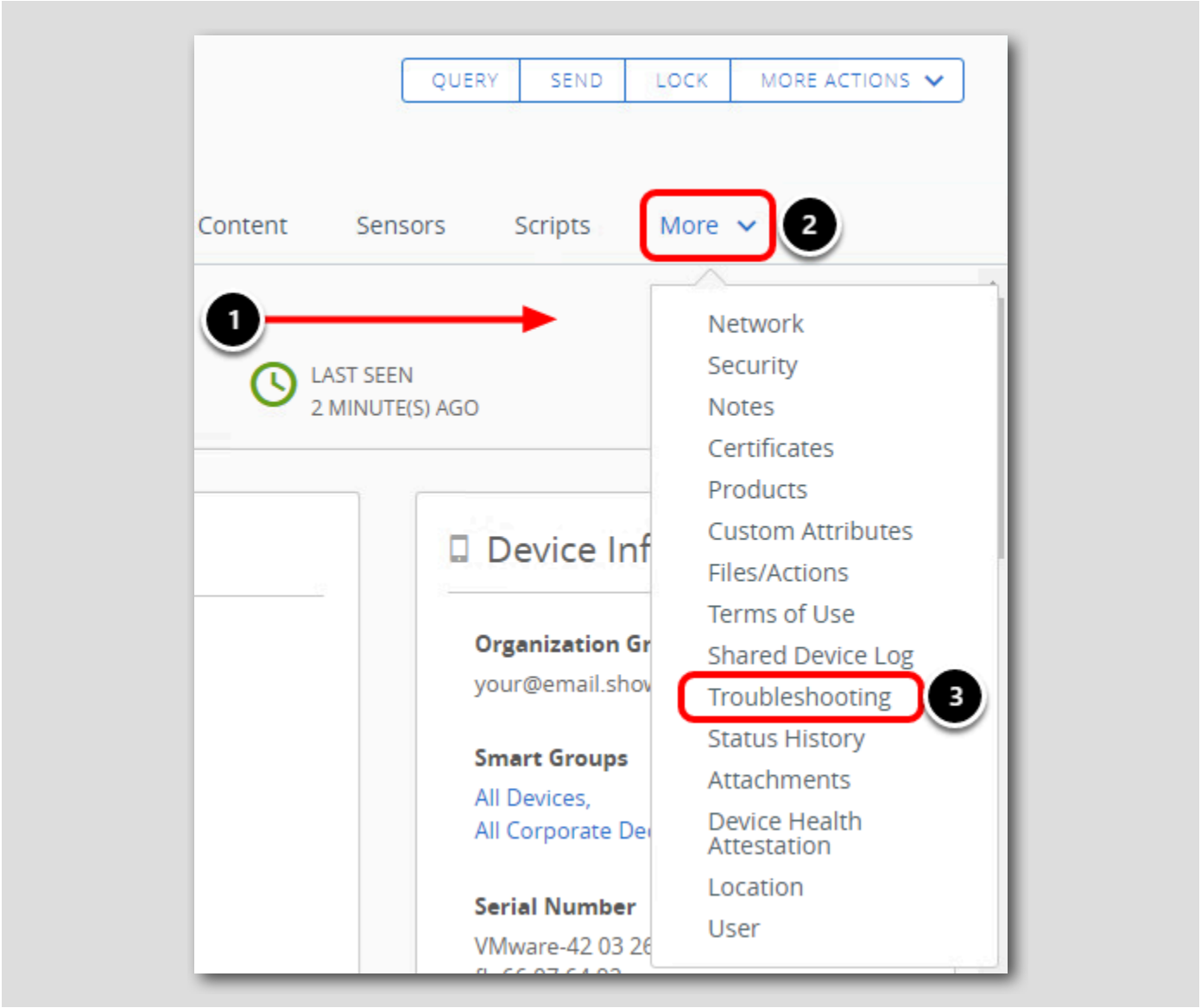




1. Click **Query** to run a full query on the device. This will trigger the Workflows query in addition to other queries (Device samples, apps, certificates, etc.) and will also cause the published workflow to process.
2. Click **Close** when prompted that the sync was successful.

Verifying the Device Queries

[672]

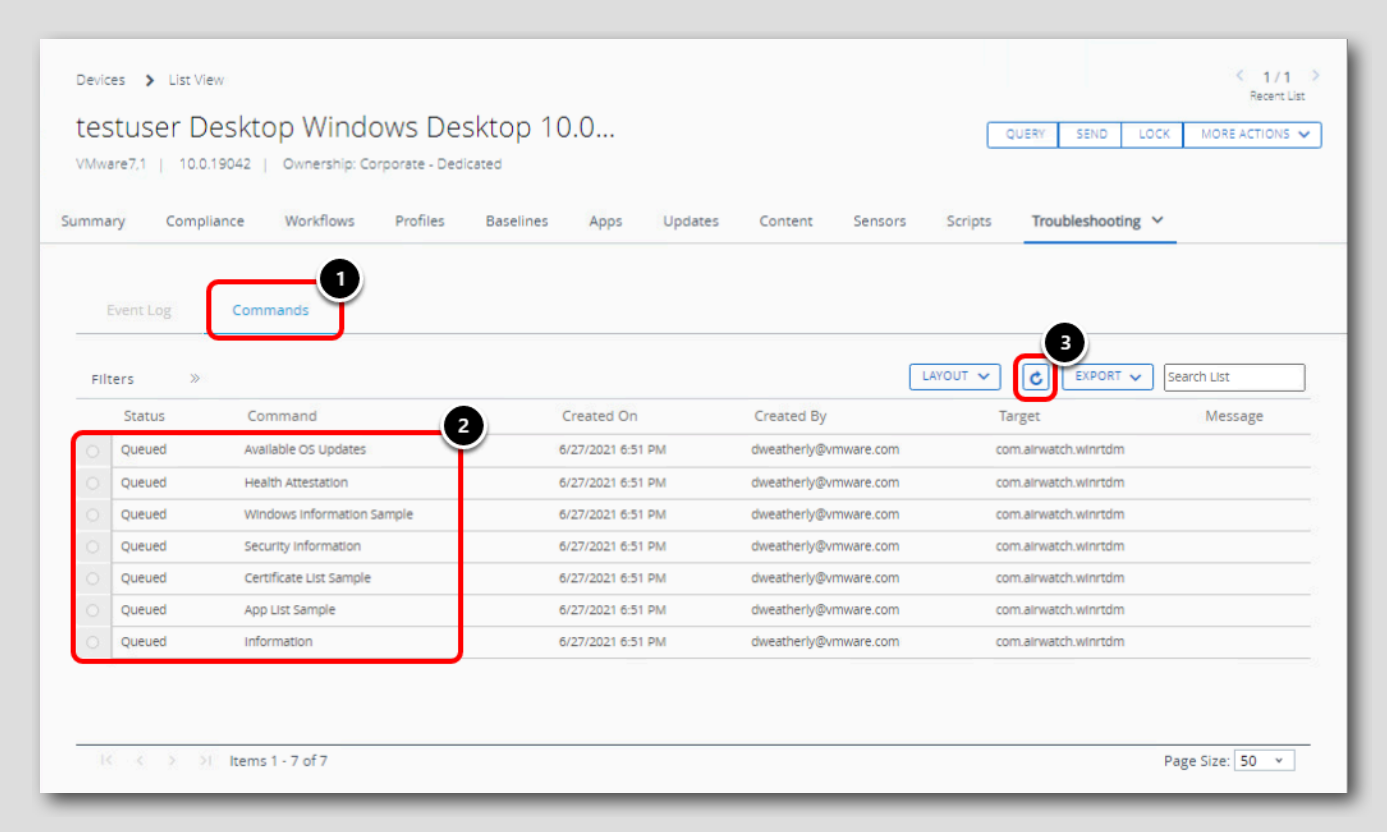


From the Device Details page:

1. Scroll to the right to find the More dropdown if needed
2. Select **More**
3. Click **Troubleshooting**

Verify the Command Queue

[673]



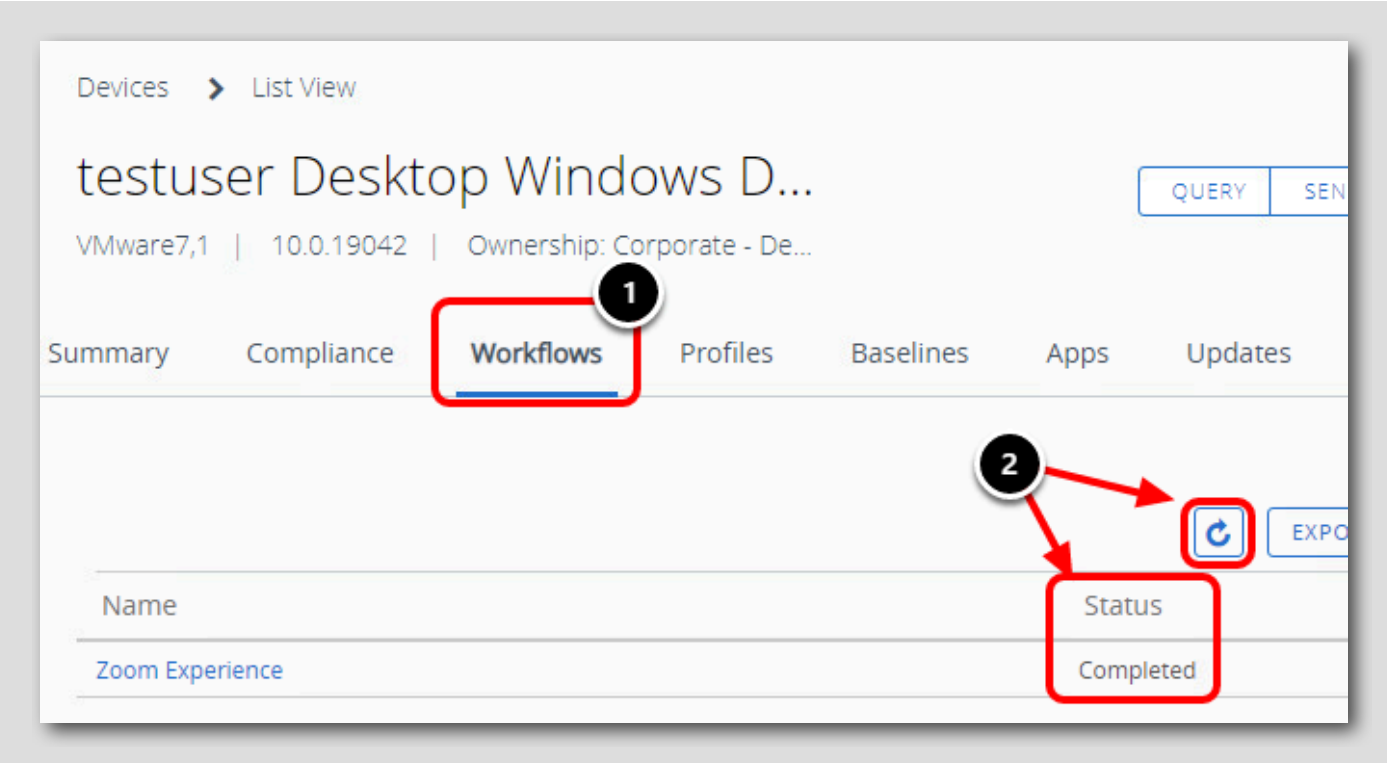
1. Select the **Commands** Tab
2. **Review Commands** that are in the queue
3. **Click** to Refresh page every couple of minutes or until commands are cleared.

NOTE: If you do not see any commands in the queue, they may have already processed.

Continue to the next step.

Verify Workflow Execution on Device

[674]



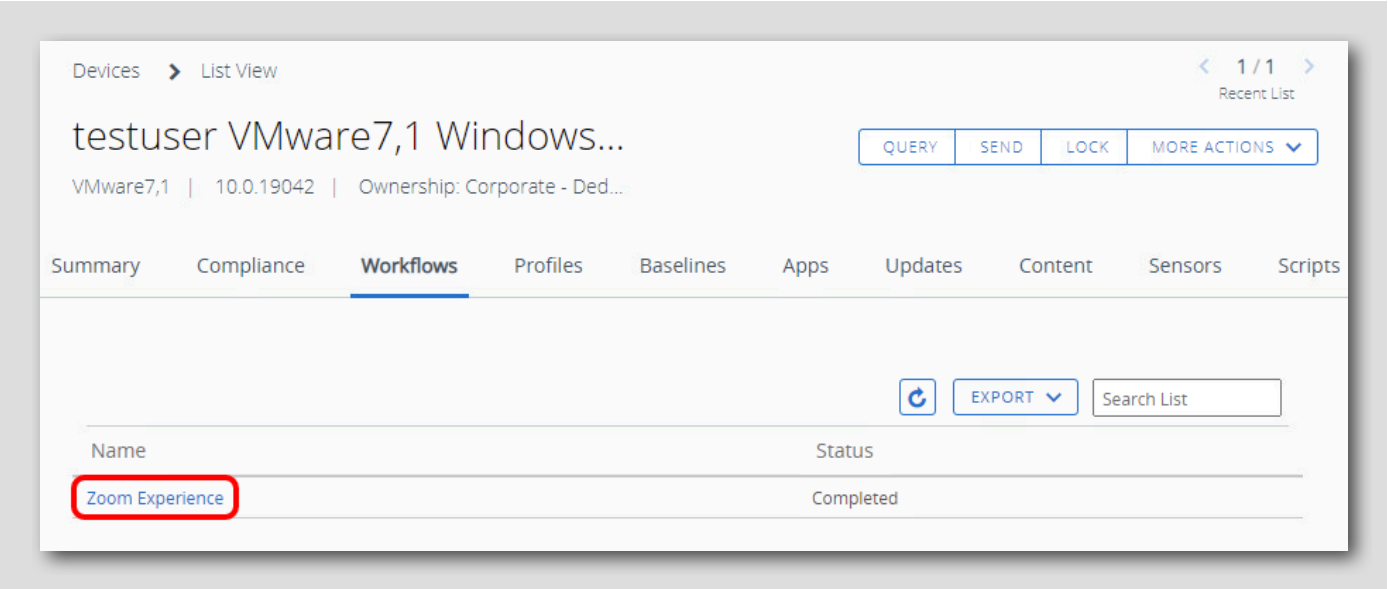
1. Click the **Workflows** Tab
2. Check if the Zoom Experience workflow status is **Completed**. If not, click the **Refresh** button periodically until the Status changes to Completed.

   NOTE: The workflow may take several minutes to complete and report as Completed.

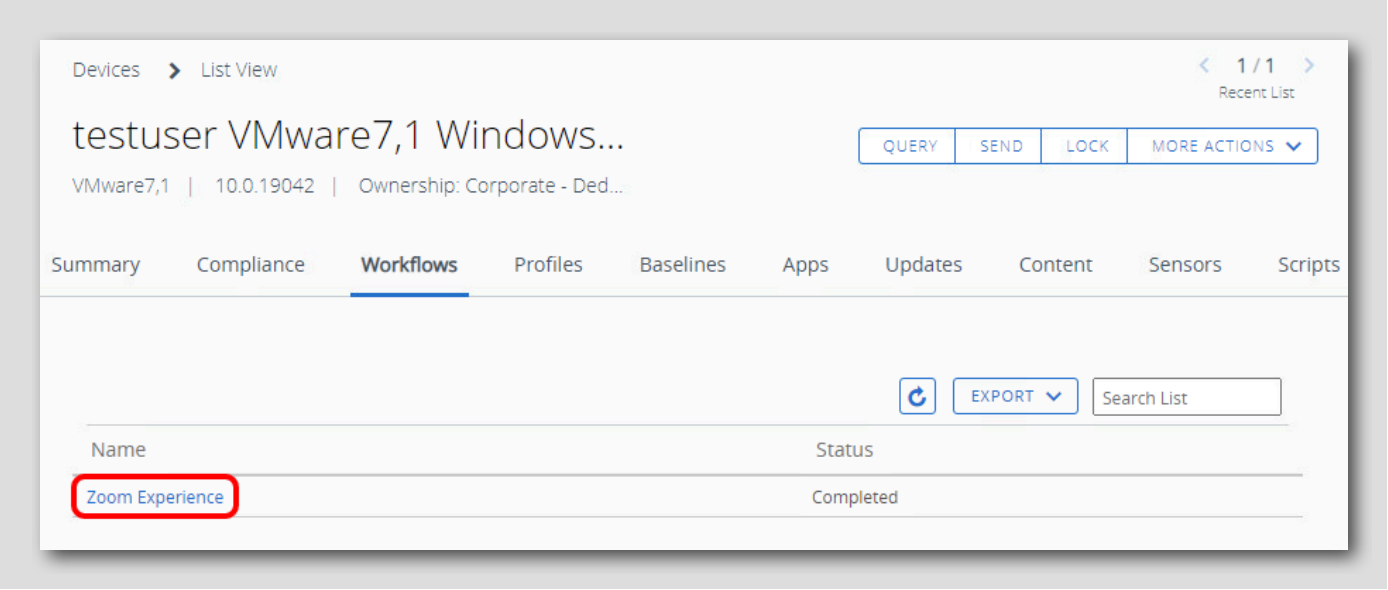
Continue to the next step once the workflow status is Completed.

Verifying the Workflow Execution on a Device

[675]

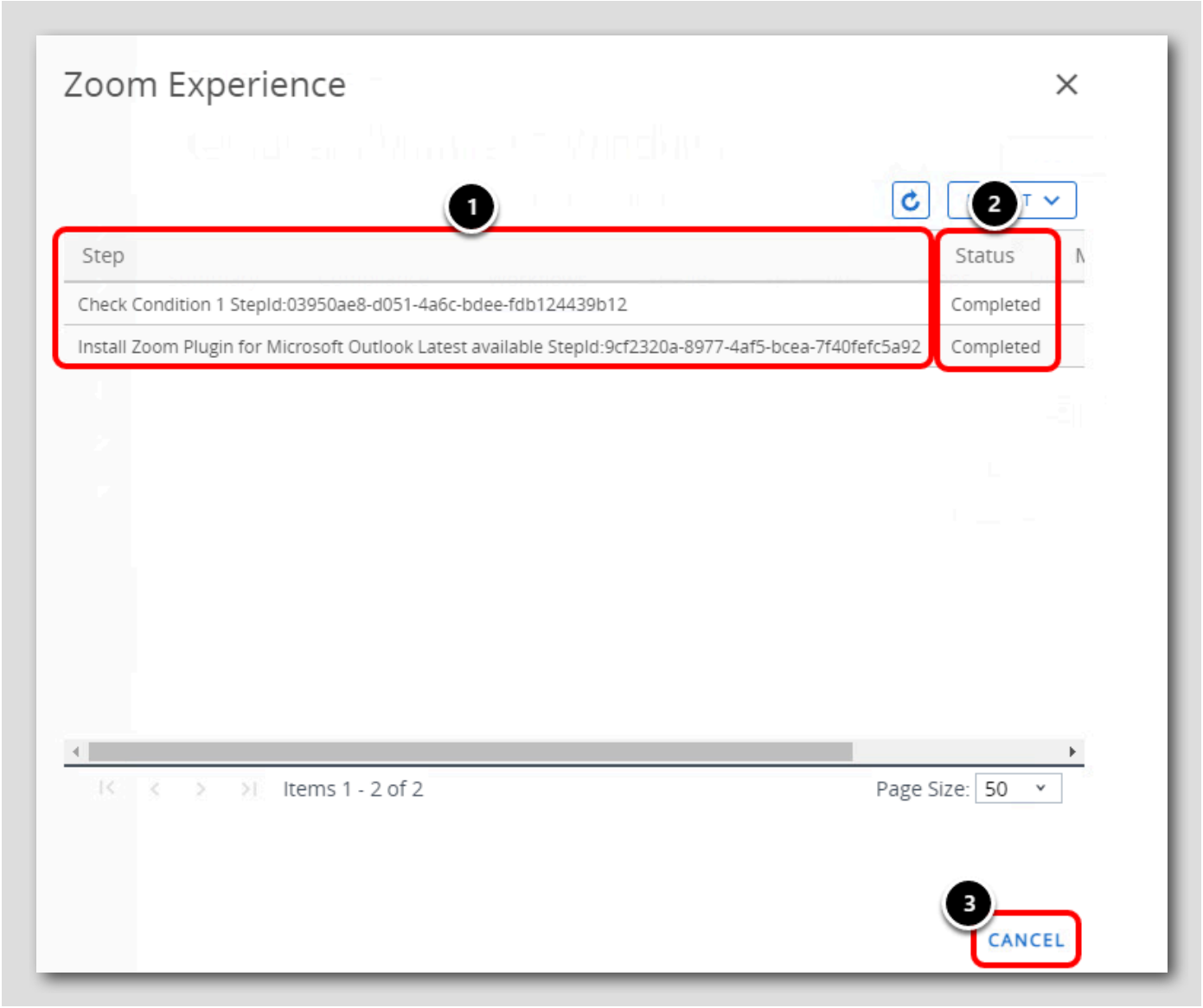


Click the **Zoom Experience** workflow.



Confirm the Workflow executed on Device

[676]



1. Review the **Workflow Steps** to see what actions occurred in the workflow
2. Review the **Workflow Status** to confirm each step is Completed
3. Click **Cancel** to close the workflow

Confirm Outlook Plug in Installed

[677]

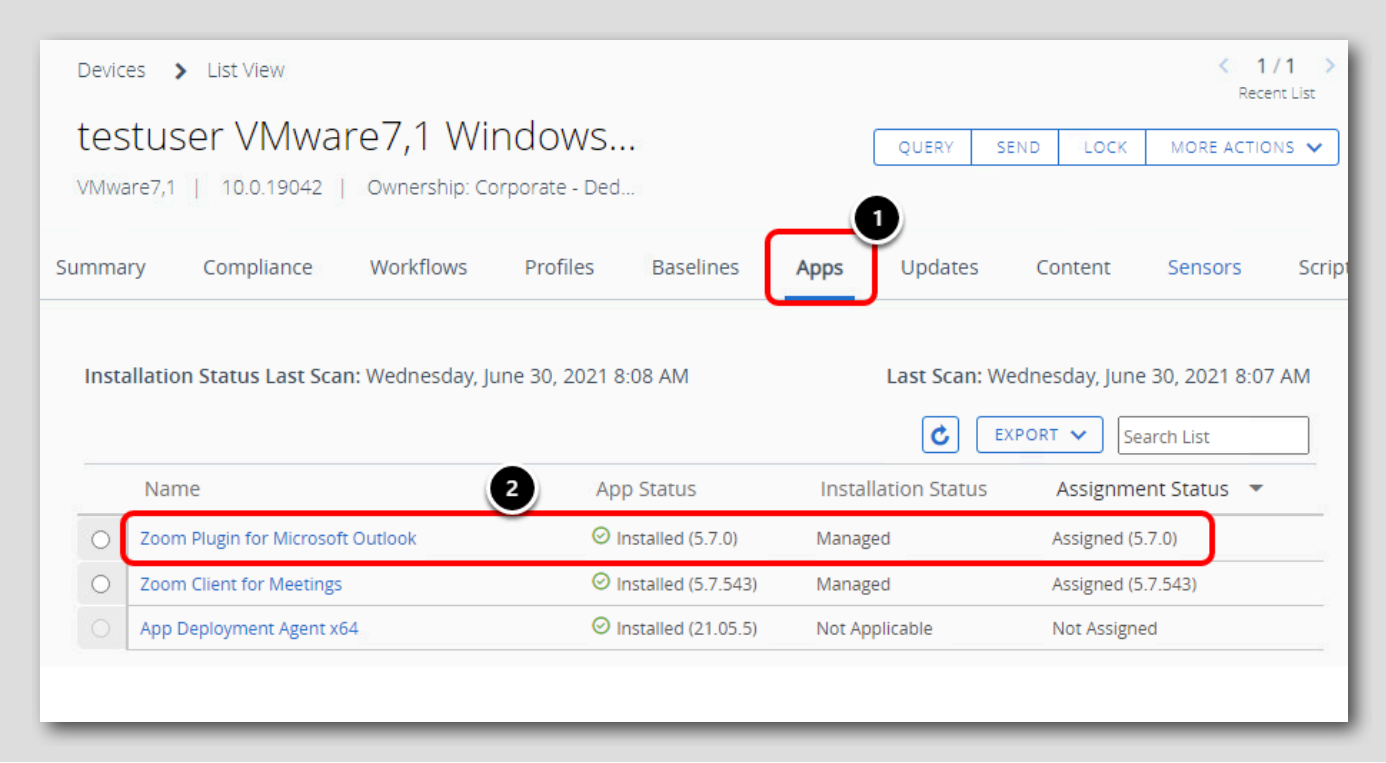
Finally, to verify the Workflow completed, we should see the Zoom Outlook Plugin Installed on the Device.

We can Check 2 different ways:

1. Confirm Zoom Outlook Plug In Installed using the Workspace ONE UEM Console
2. Confirm Zoom Outlook Plug In Installed Directly on the device.

Confirm Zoom Outlook Plug In Installed using the Workspace ONE UEM Console

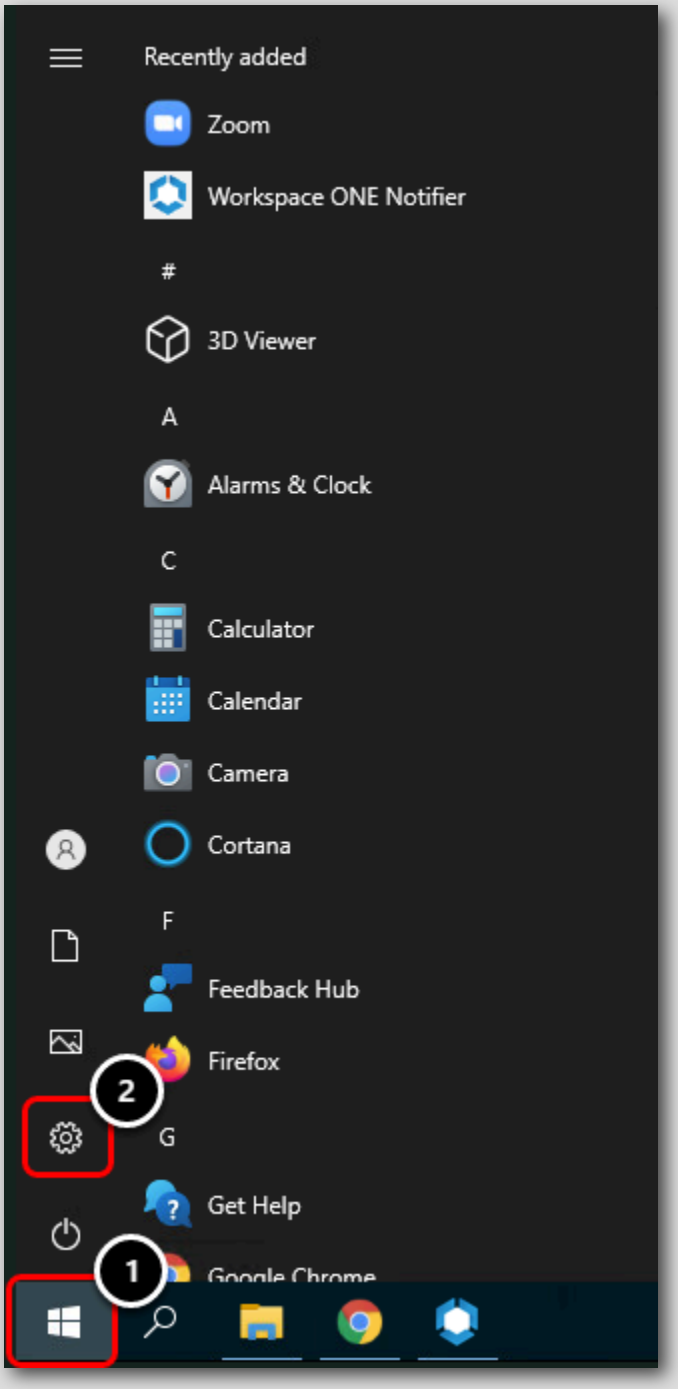
[678]



In the Workspace ONE UEM Console, ensure you are in the device details page.

1. Select the **Apps** tab
2. Confirm **Zoom Plugin for Microsoft Outlook** is showing an App Status of Installed

Confirm Zoom Outlook Plug In Installed Directly on the device. [679]

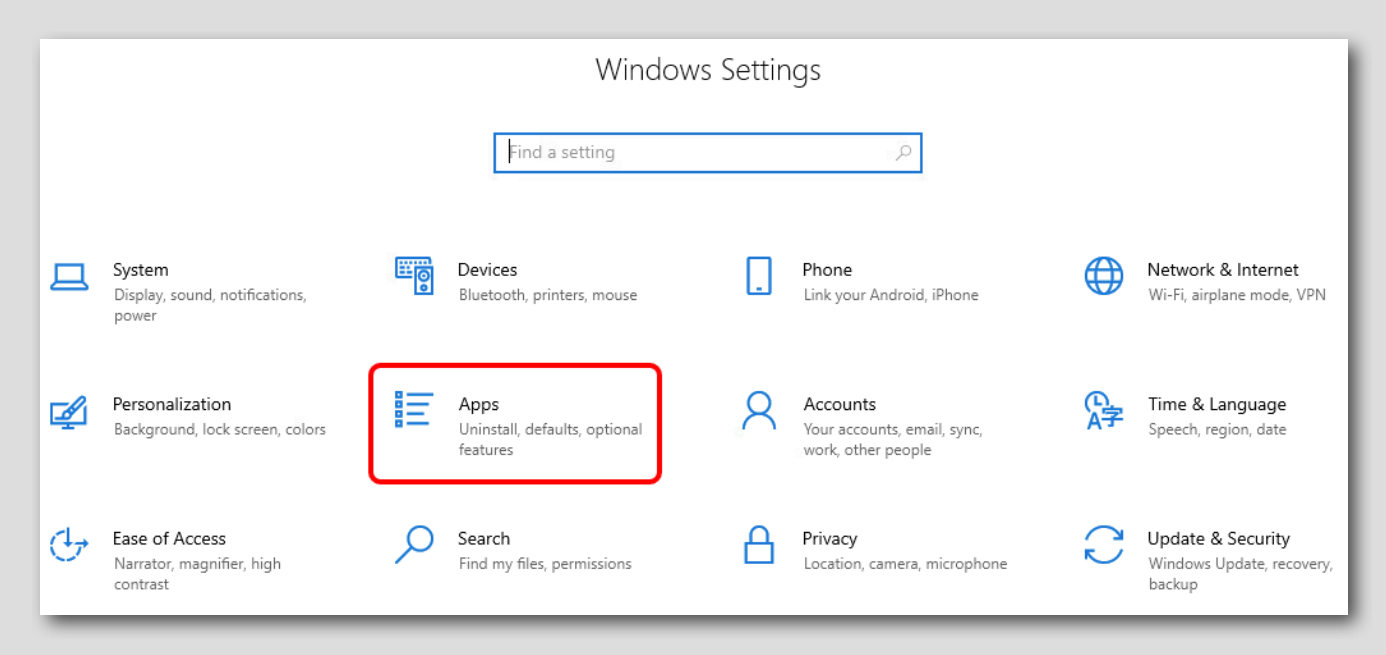


On the Win10-01a Virtual Machine that you are connected to via Remote Desktop:

1. Click **Windows**
2. Select **Settings**

Select Applications

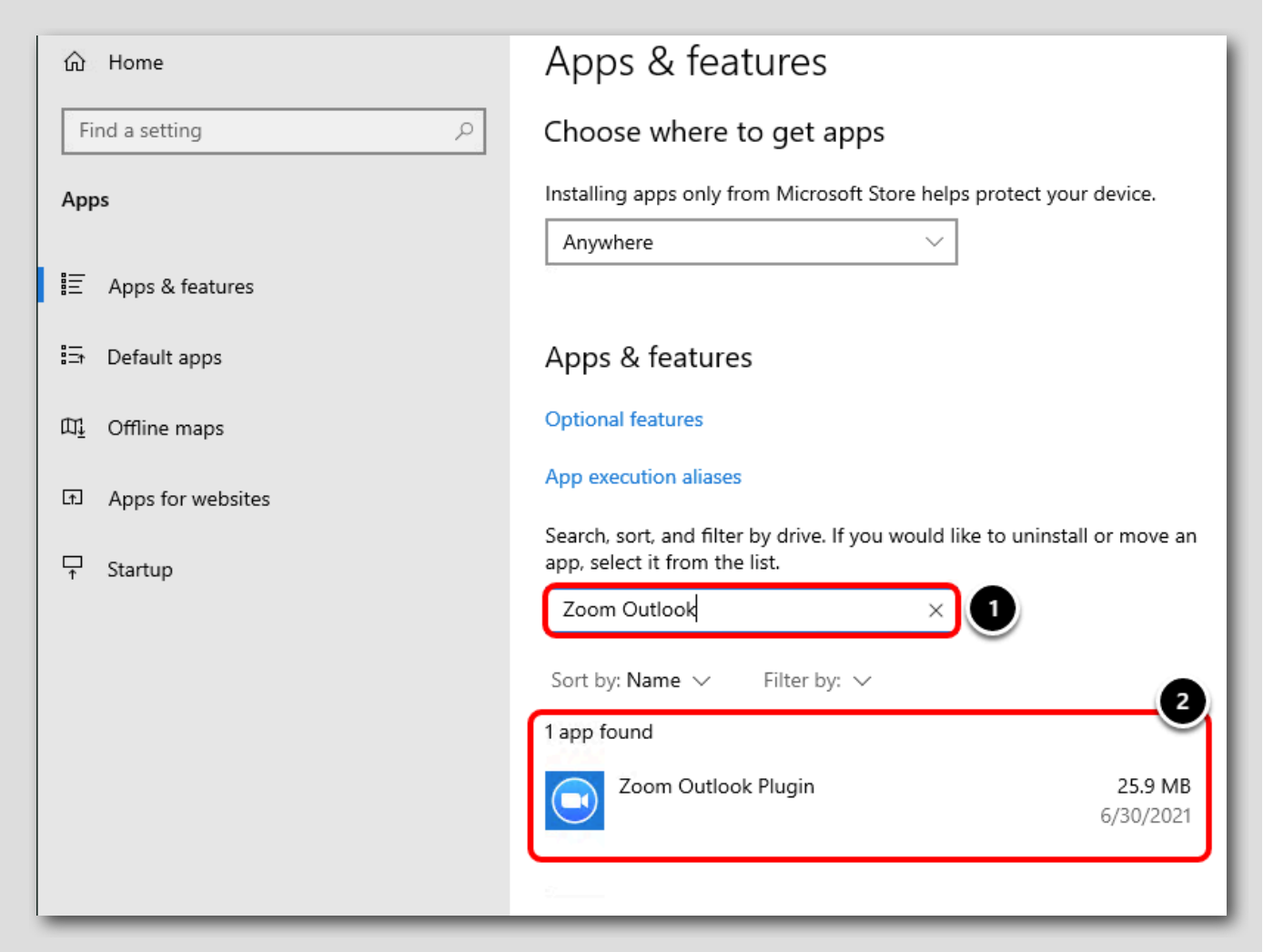
[680]



Click **Apps**.

Search Zoom Outlook

[681]



1. Enter **`Zoom Outlook`** in the search bar
2. Confirm that the **Zoom Outlook Plugin** appears in the installed app list

You have now Verified that the Zoom Outlook Plug In has been installed as part of a Workflow built by Freestyle Orchestrator. The Zoom Outlook Plugin was only installed after the Zoom app was confirmed to be installed on the application by checking the Zoom install path was populated and that the app existed on the device.

Un-enrolling your Windows 10 Device

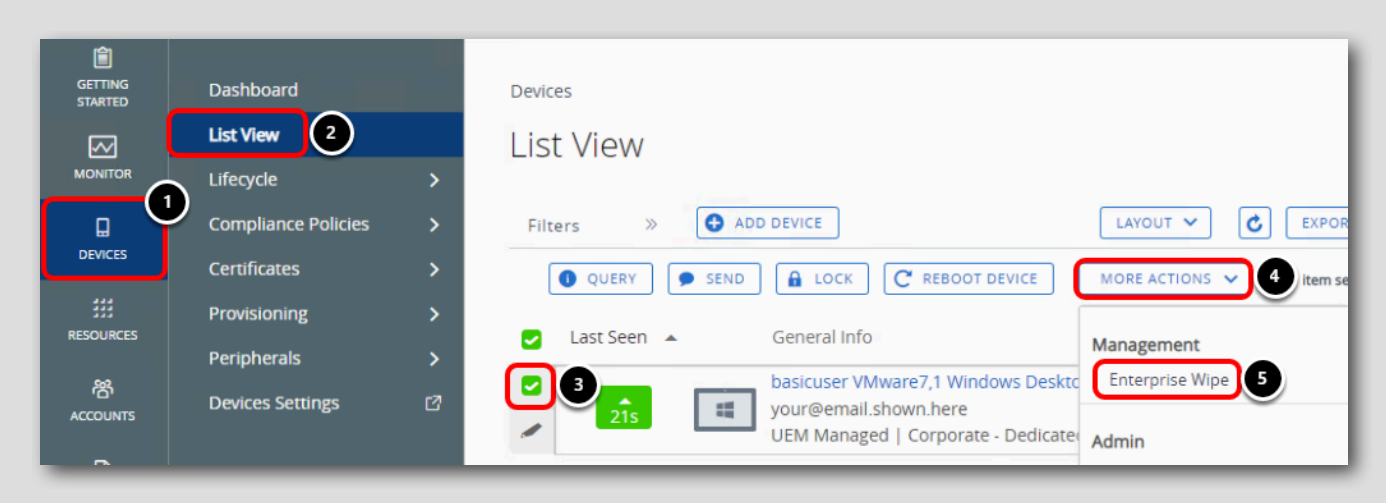
[682]

In this section, we are going to un-enroll our Windows 10 VM so that we can use it for other lab modules.

We will use the **Enterprise Wipe** wipe command to remove all of the managed content that was pushed to the device (such as profiles and apps) by Workspace ONE while not modifying any personal content or data on the device.

Enterprise Wipe from Workspace ONE UEM Console

[683]

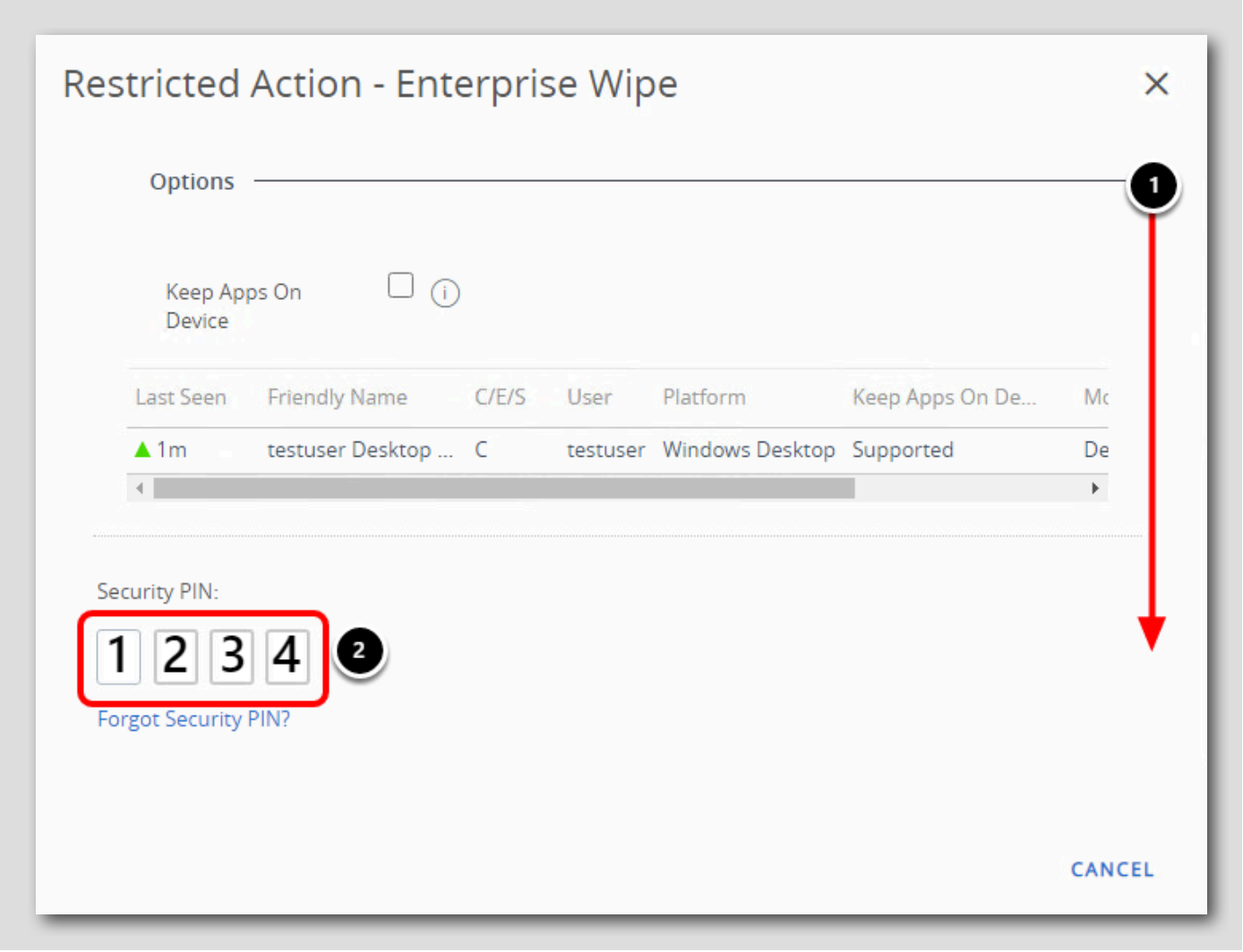


Return to the Workspace ONE UEM Administrator Console in Google Chrome,

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

Enter PIN and Enterprise Wipe Device

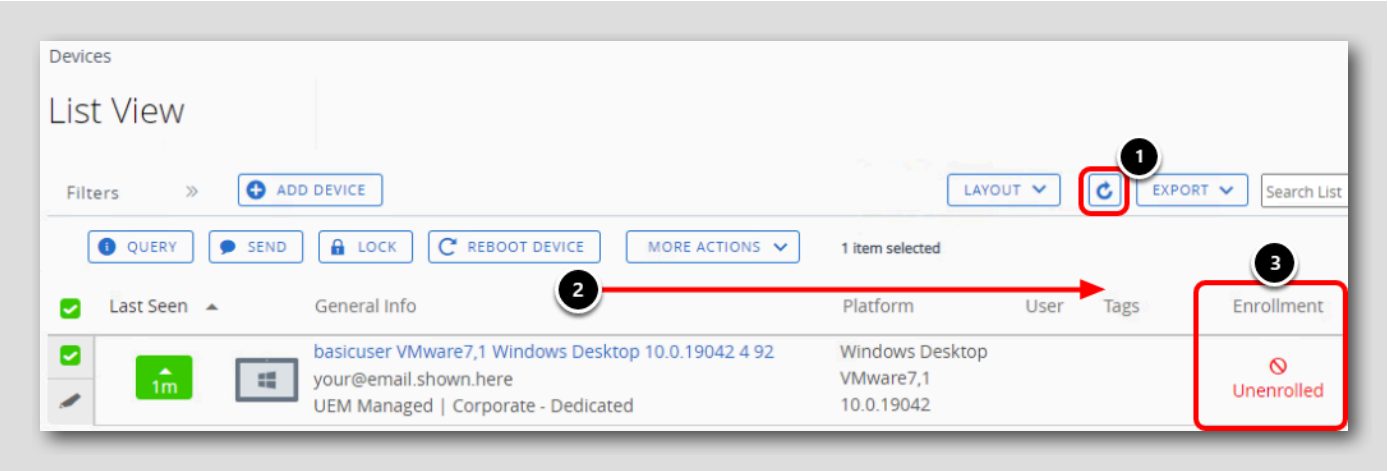
[684]



1. You may need to scroll down to find the Security PIN input
2. Enter the Security PIN that you created when you first logged into the Workspace ONE UEM administration console, which was **1234**. If you used a different PIN, enter that one instead.
3. Click **Delete**

Validate Enterprise Wipe

[685]

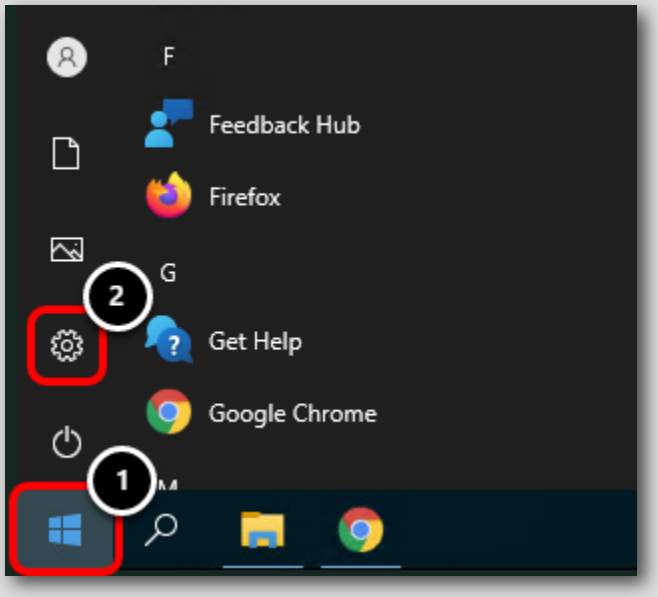


NOTE: The Enterprise Wipe may take several minutes to process.

1. Click the **Refresh** icon periodically to refresh the page to check if the Enterprise Wipe has processed
2. If needed, scroll to the right to find the Enrollment column
3. Notice that the Enrollment status for the device changes to **Unenrolled** once the Enterprise Wipe command is processed

Navigate to Windows 10 Settings

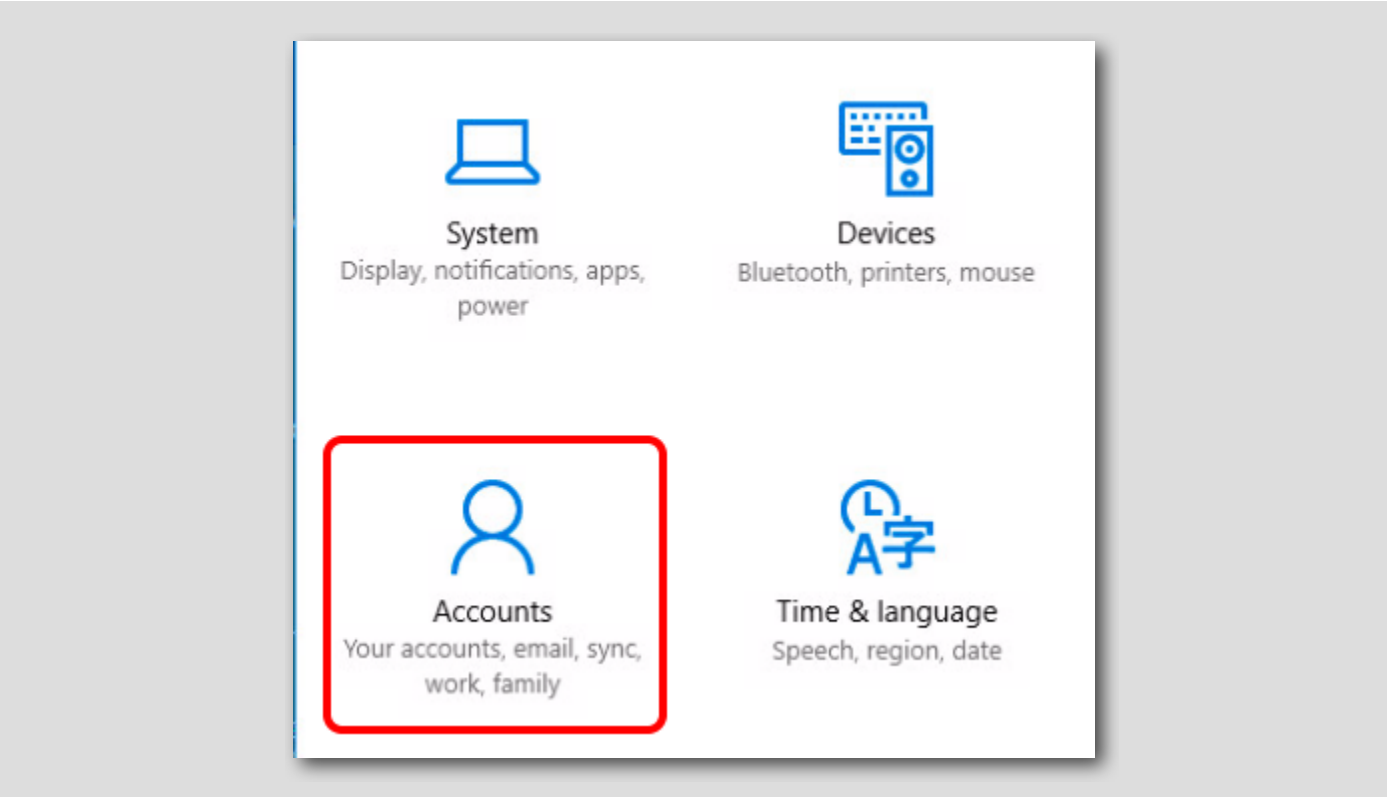
[686]



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

Access Accounts Settings

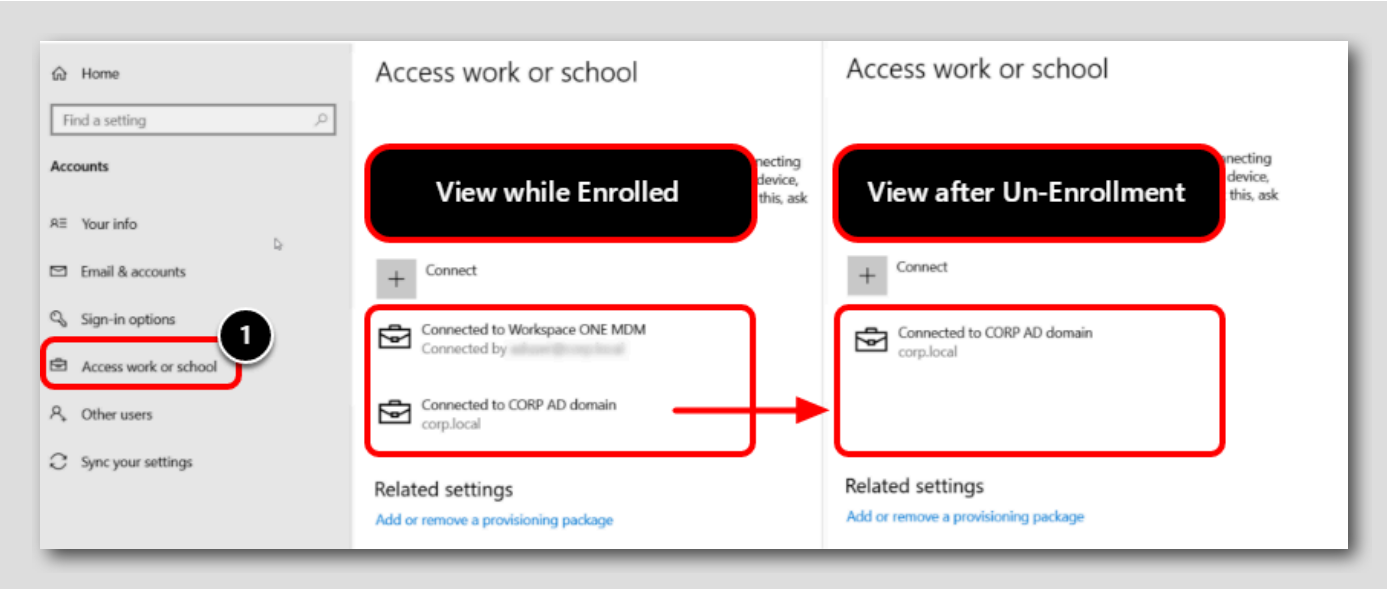
[687]



From the Settings Menu, access **Accounts**

Validate That No Management Account Exists

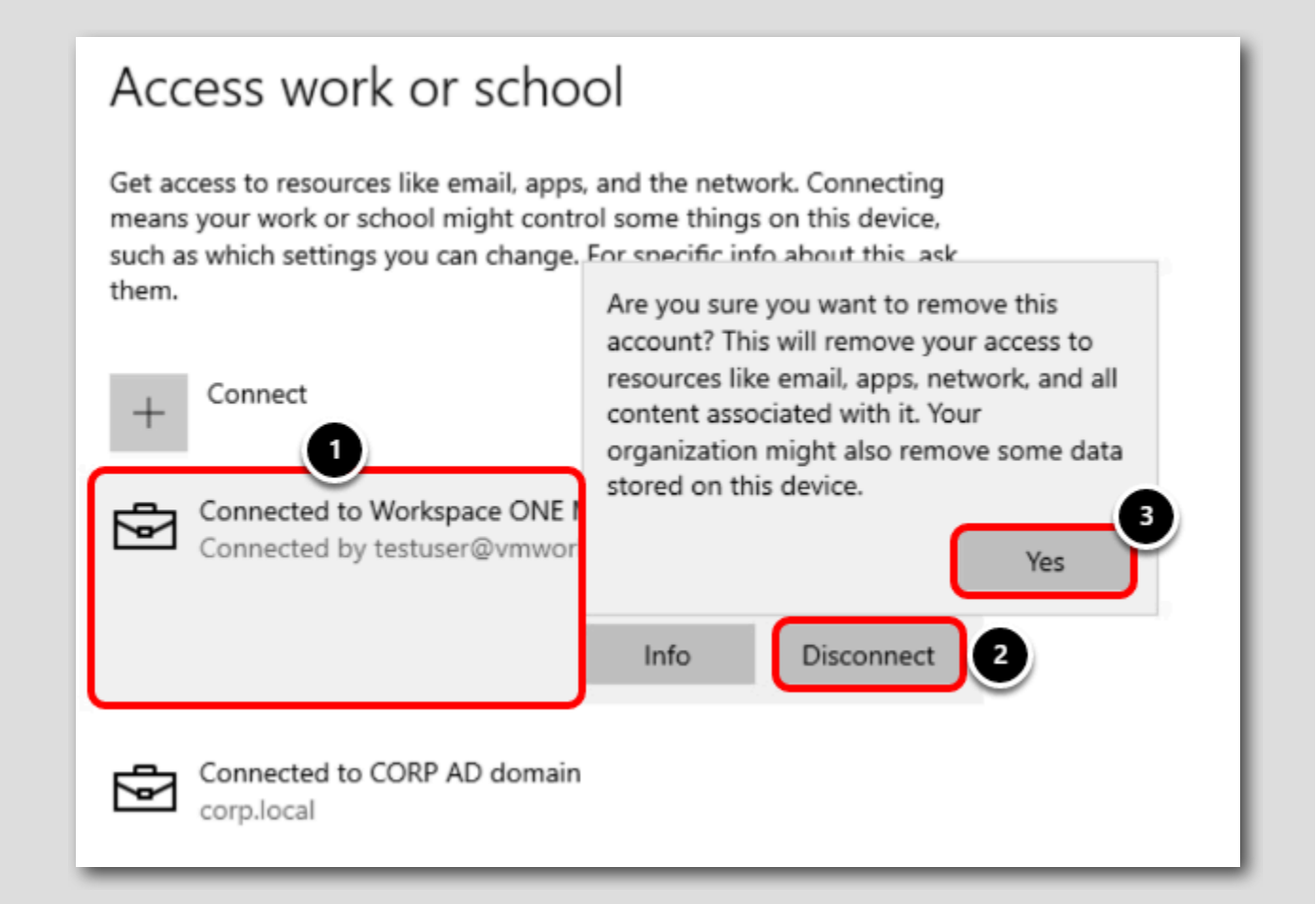
[688]



1. Click on Access work or school
2. Validate that you DO NOT see any account connected to Workspace ONE MDM.

NOTE: The CORP AD domain is the local domain in this lab and is not controlled by Workspace ONE UEM Enrollment, so you will see this connection when your device is enrolled or unenrolled.

NOTE: If the Access Work or School page was opened from earlier, you may need to refresh or navigate away from the page and return to see the changes.



1. Click the **Connected to Workspace ONE UEM** account
2. Click **Disconnect**
3. Click **Yes**

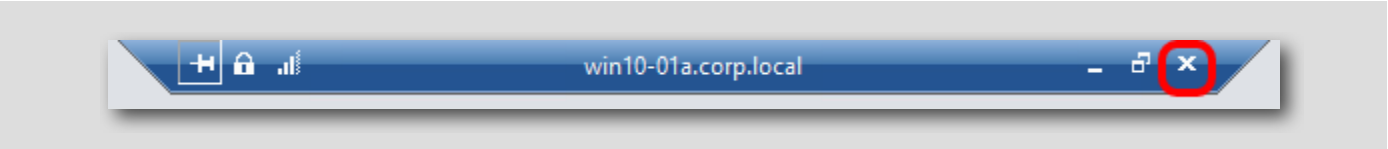
Return to the Main Console

[689]

Click **Close (X)** on the Remote Desktop Connection bar at the top of the screen to return to the Main Console to finish making configurations within the Workspace ONE UEM Console.

NOTE: If the Remote Desktop Connection bar is not visible, you may have unpinned it. Hover your mouse of the top of the screen to

display the Remote Desktop Connection bar again, then click close.



Summary

[690]

Congratulations! You have completed the Introduction to Freestyle Orchestrator module!

Together, we explored the Use-Case for Windows 10 devices, where you install applications based on conditions; where certain Applications OR Files must be existing first

In this module, you learned how to:

- Assign Applications through the Enterprise Application Repository
    - Configure Zoom Client for Meetings Application (Auto Installed)
    - Configure Zoom Plugin for Microsoft Outlook (Available On-Demand)
- Create a Workflow with Freestyle Orchestrator
- Verifying the Workflow Execution in Workspace ONE UEM
- Verifying the Workflow Execution on a Device

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

[691]

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 8 - Introduction to Linux Management (30 Minutes) Beginner

Introduction [693]

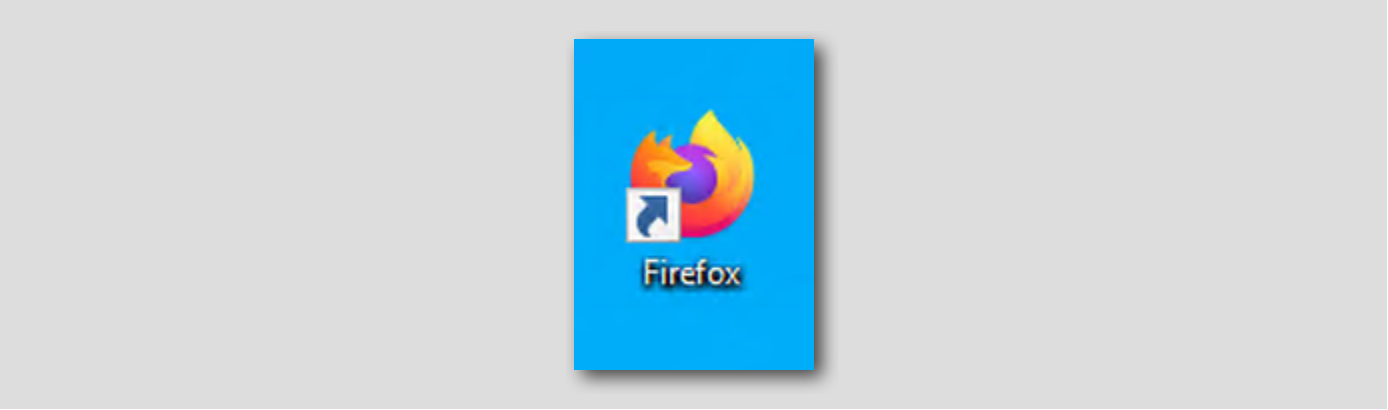
The flexibility of the Linux operating system makes it a preferred platform for a wide range of uses, including developer workstations, Raspberry Pi devices, and many IoT devices. With Workspace ONE UEM, you can build on the flexibility and ubiquity of Linux devices and manage them along-side your other enterprise devices in one central location with the tools and features to manage the entire lifecycle of Linux devices.

In this lab, we will explore some Workspace ONE administration features and concepts available for the Linux platform. This lab will give you a better understanding of how Linux devices are enrolled, how to troubleshoot enrollment issues and validating successful enrollments.

Login to the Workspace ONE UEM Console [694]

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

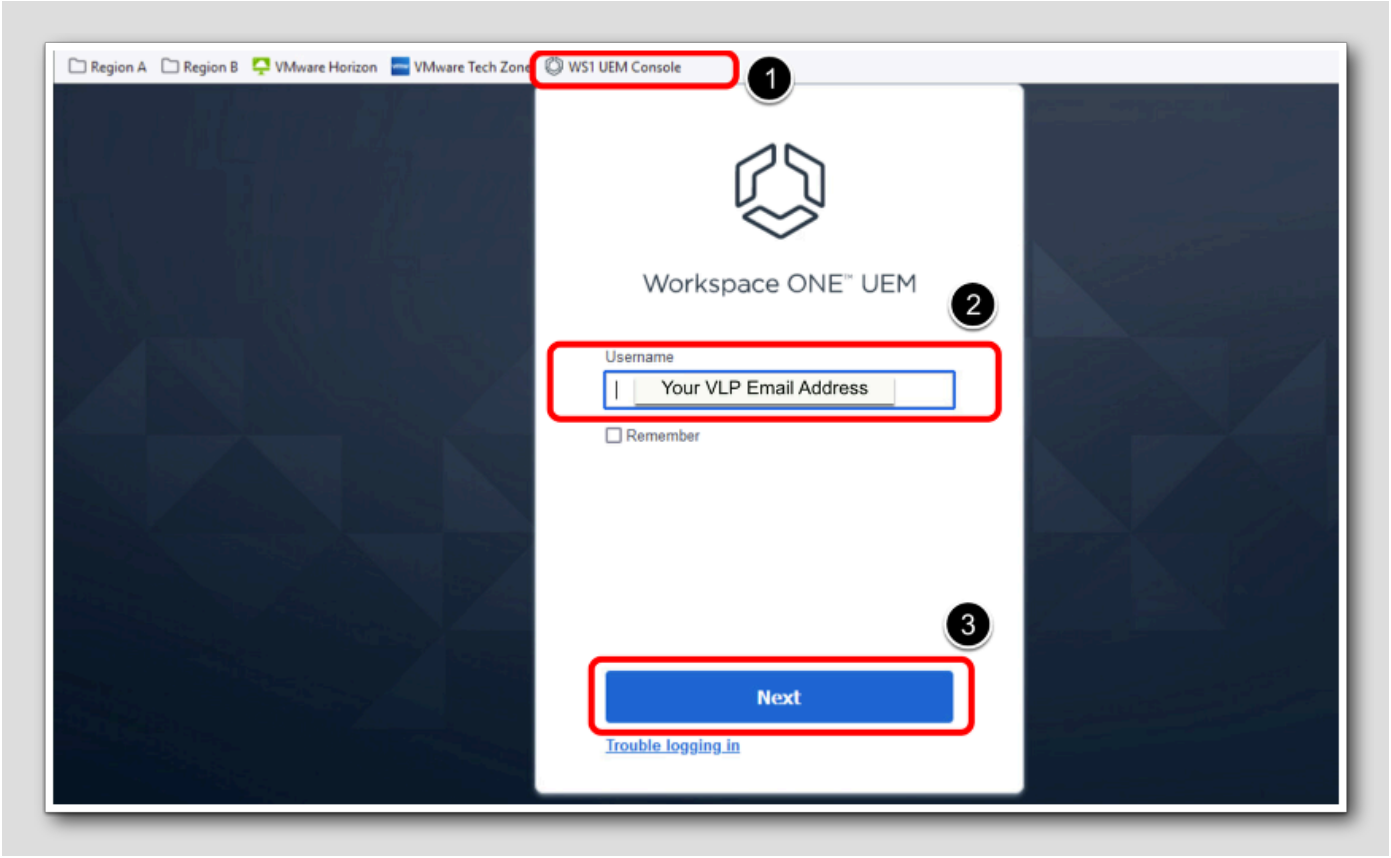
Launch Firefox Browser [695]



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

[696]

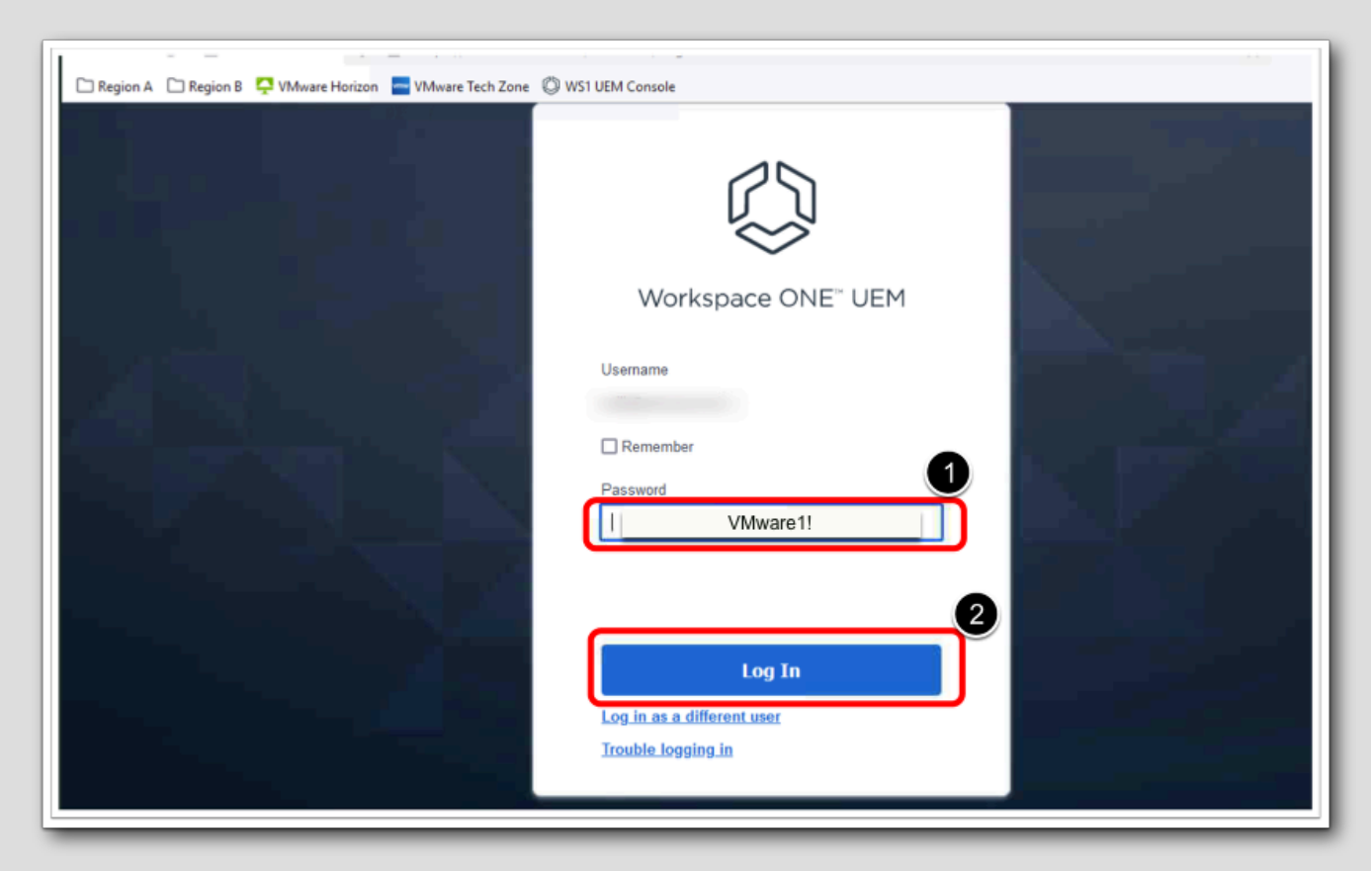


1. Select the **WS1 UEM Console** link from the Bookmark Toolbar
2. Enter your **Username**. This is the **email address** that you have associated with your **VMware Learning Platform (VLP)** account that you utilized to take Hands-on Labs.
3. Click **Next**, then advance to the next step of the lab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

[697]



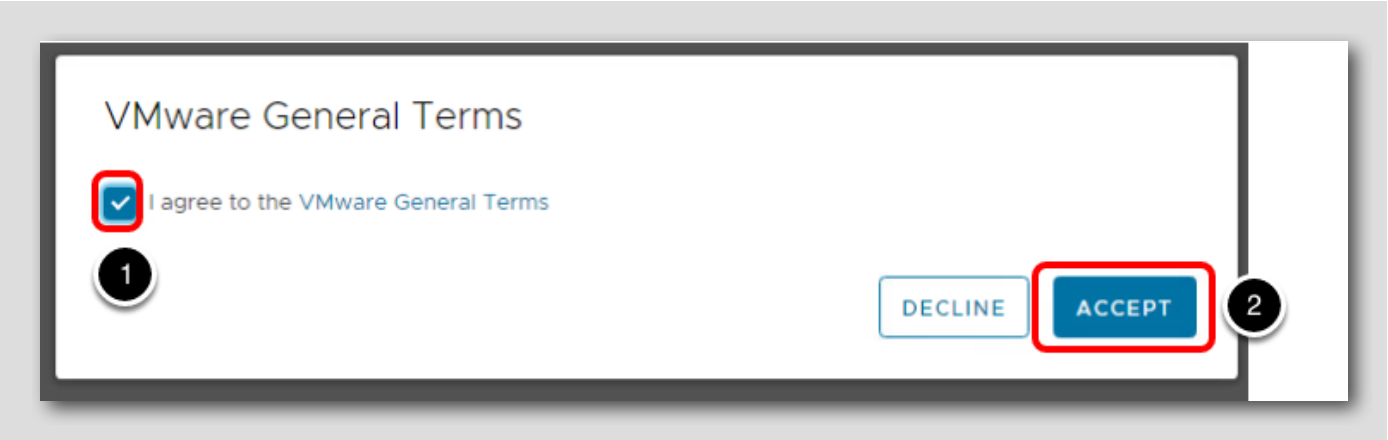
The password field will be displayed after entering your username.

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

[698]



You will be presented with the VMware General Terms.

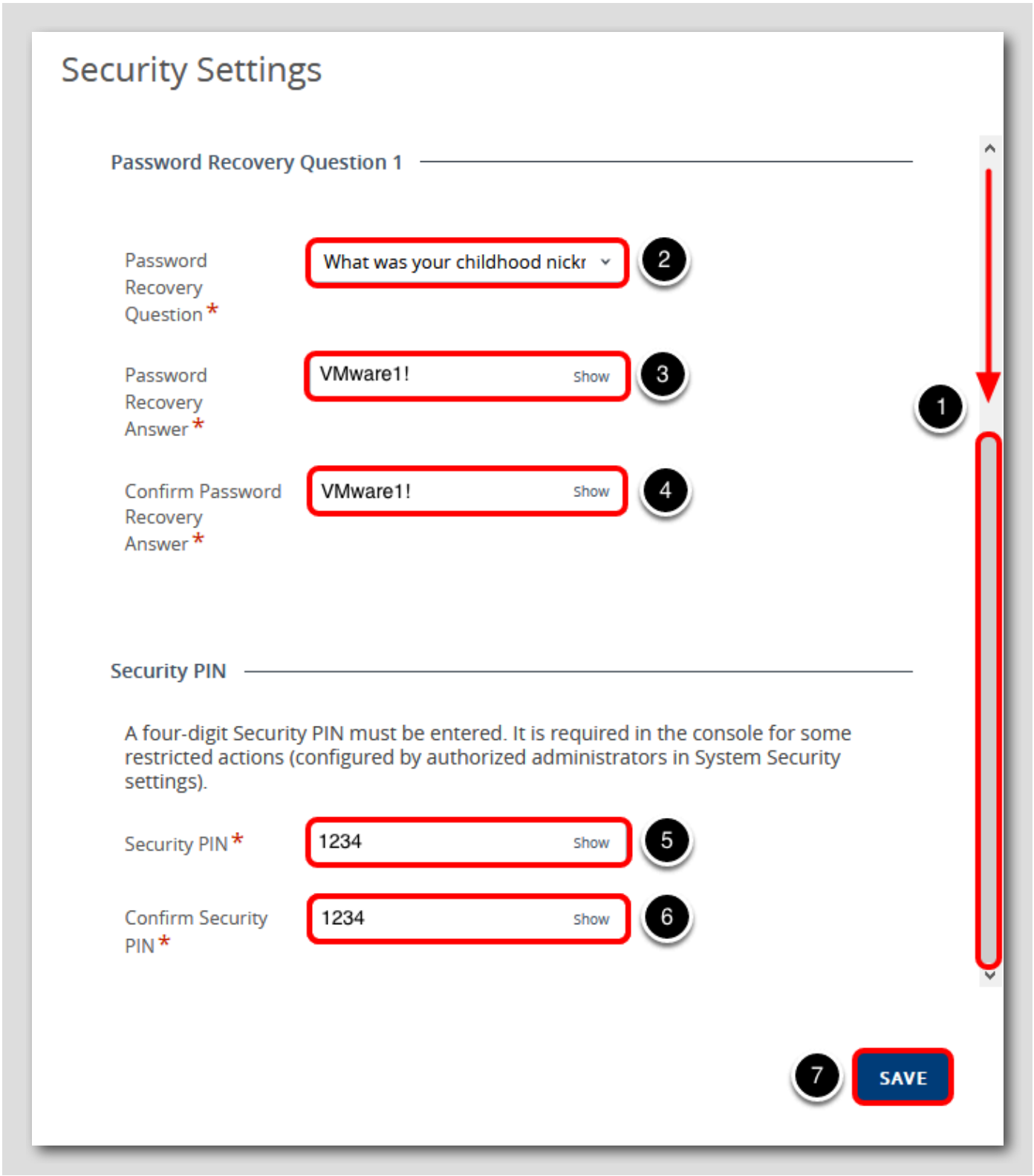
1. Select the box next to I Agree to the VMware General Terms.
2. Click the **Accept** button.

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

[699]

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

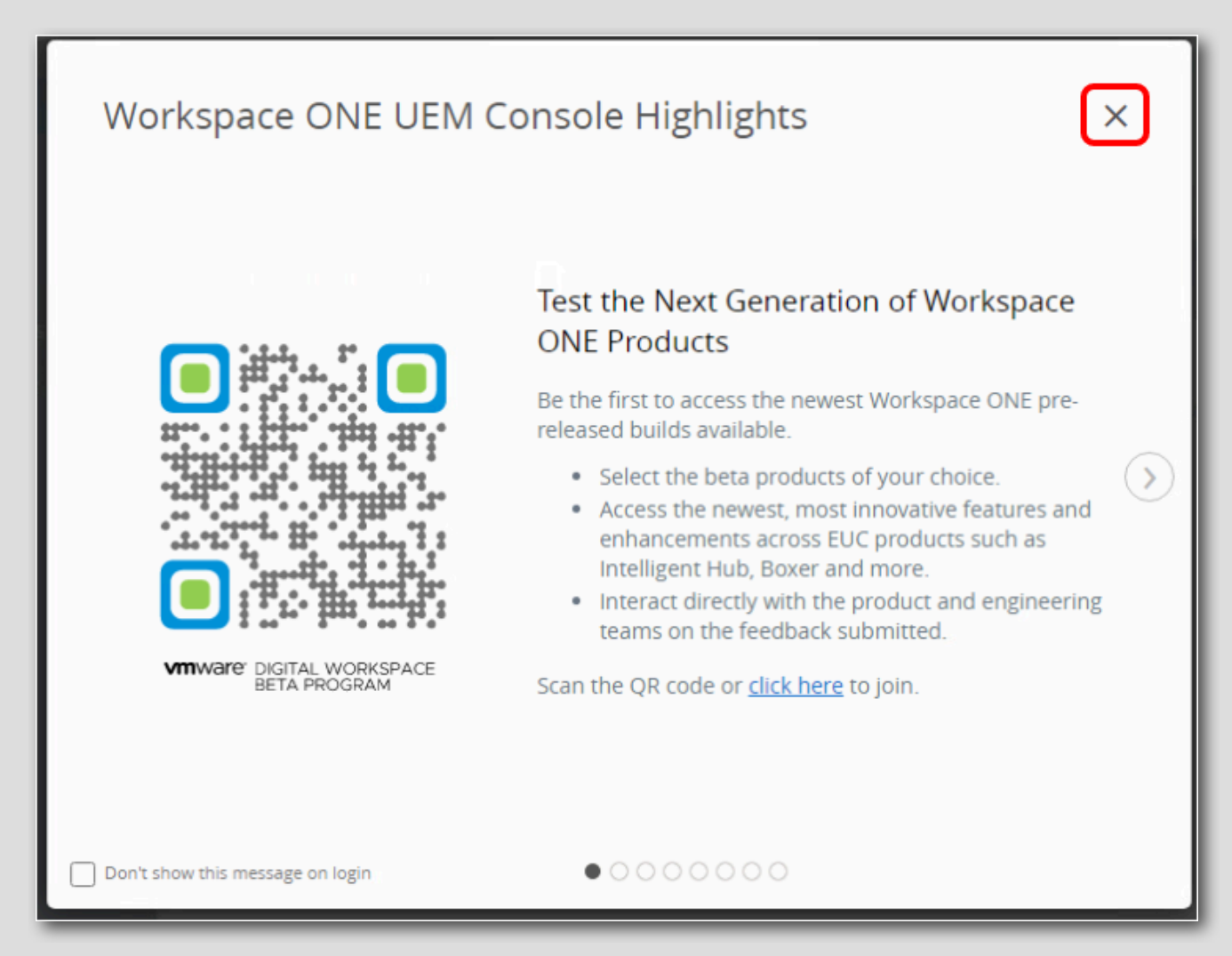

Security Settings
Password Recovery Question 1
Password Recovery Question *
What was your childhood nickr
2
Password Recovery Answer *
VMware1!
Show
3
1
Confirm Password Recovery Answer *
VMware1!
Show
4
Security PIN
A four-digit Security PIN must be entered. It is required in the console for some restricted 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

[700]

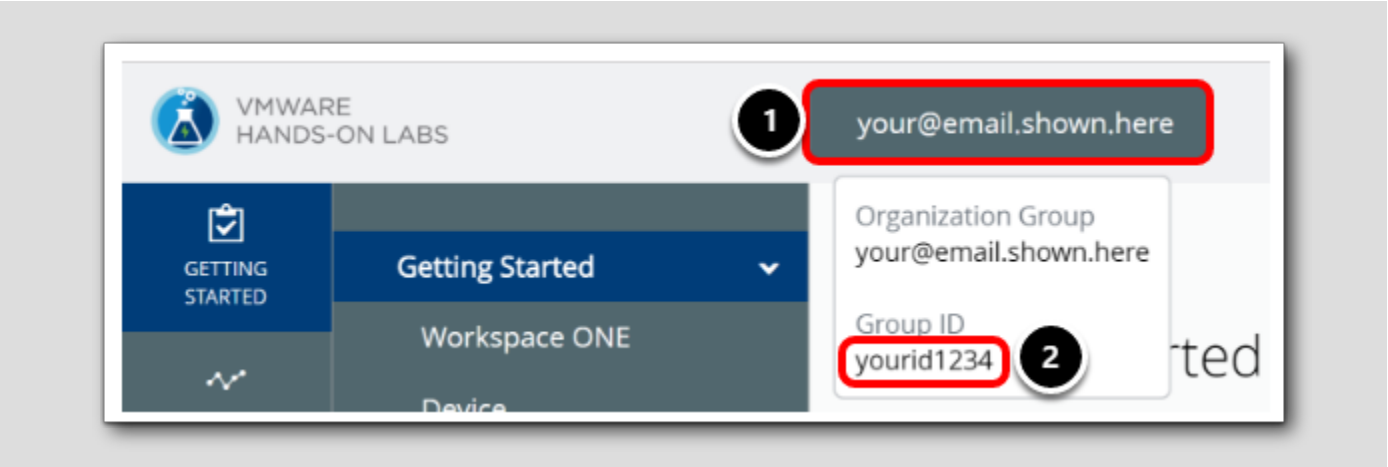


A popup window will appear after you complete your security questions.

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

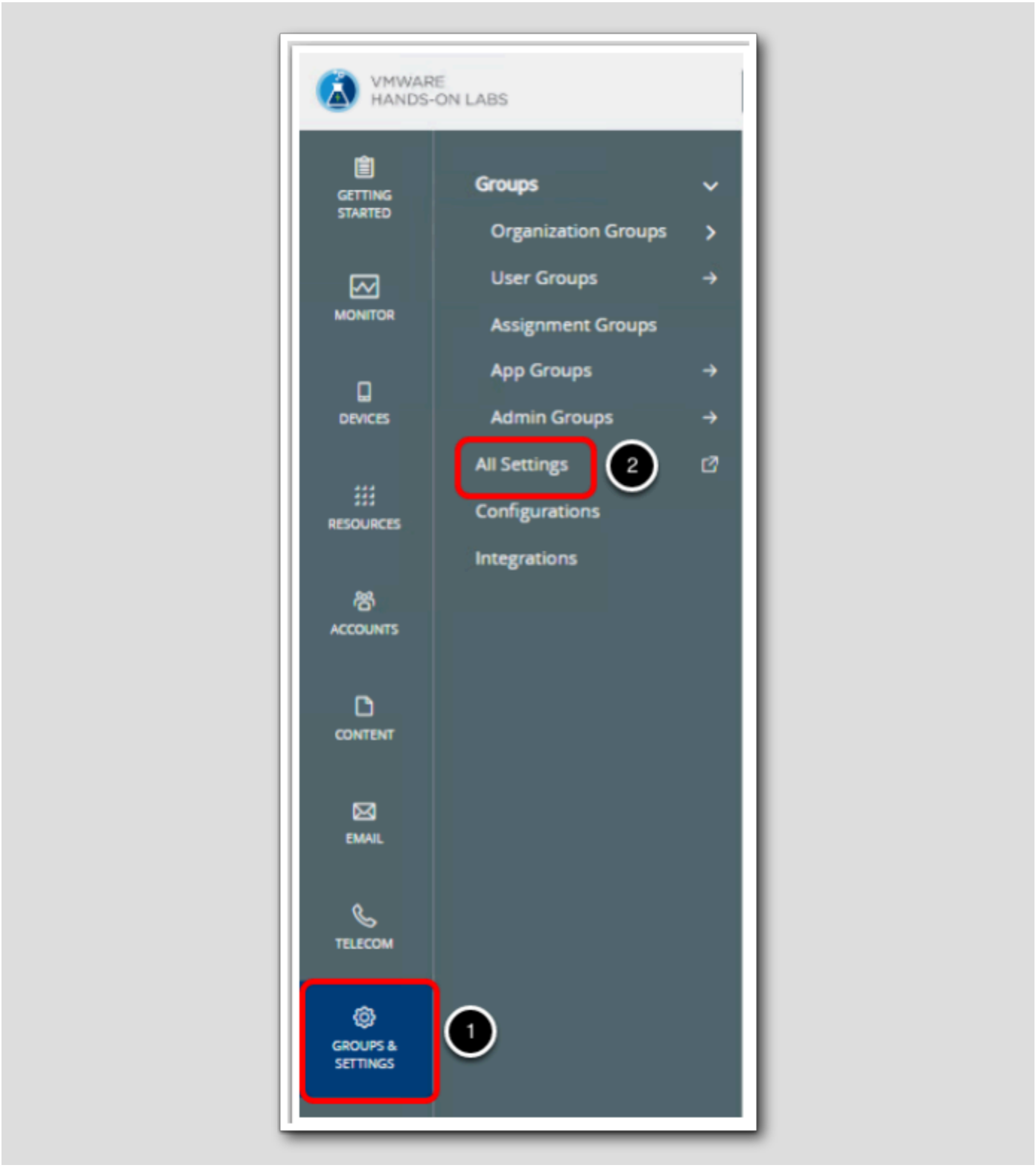
UEM Console Configuration

[701]



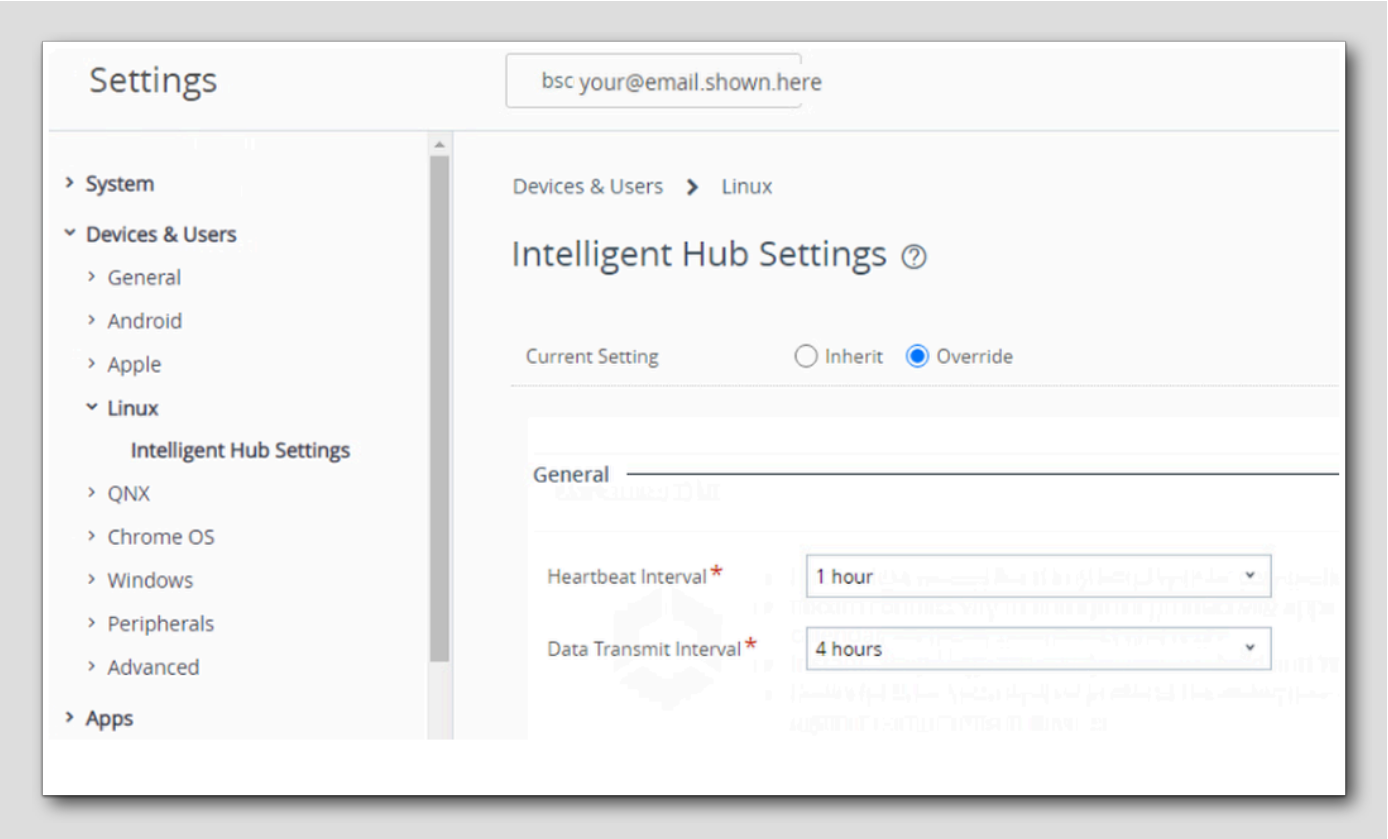
The next step is to retrieve your **Organization Group ID**.

1. To find the Group ID, Go back to the Workspace ONE UEM Administration Console and 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. Copy this value, we will use this when we enroll our Linux device.



1. From the menu on the left Select **Groups & Settings**

2. Select **All Settings**



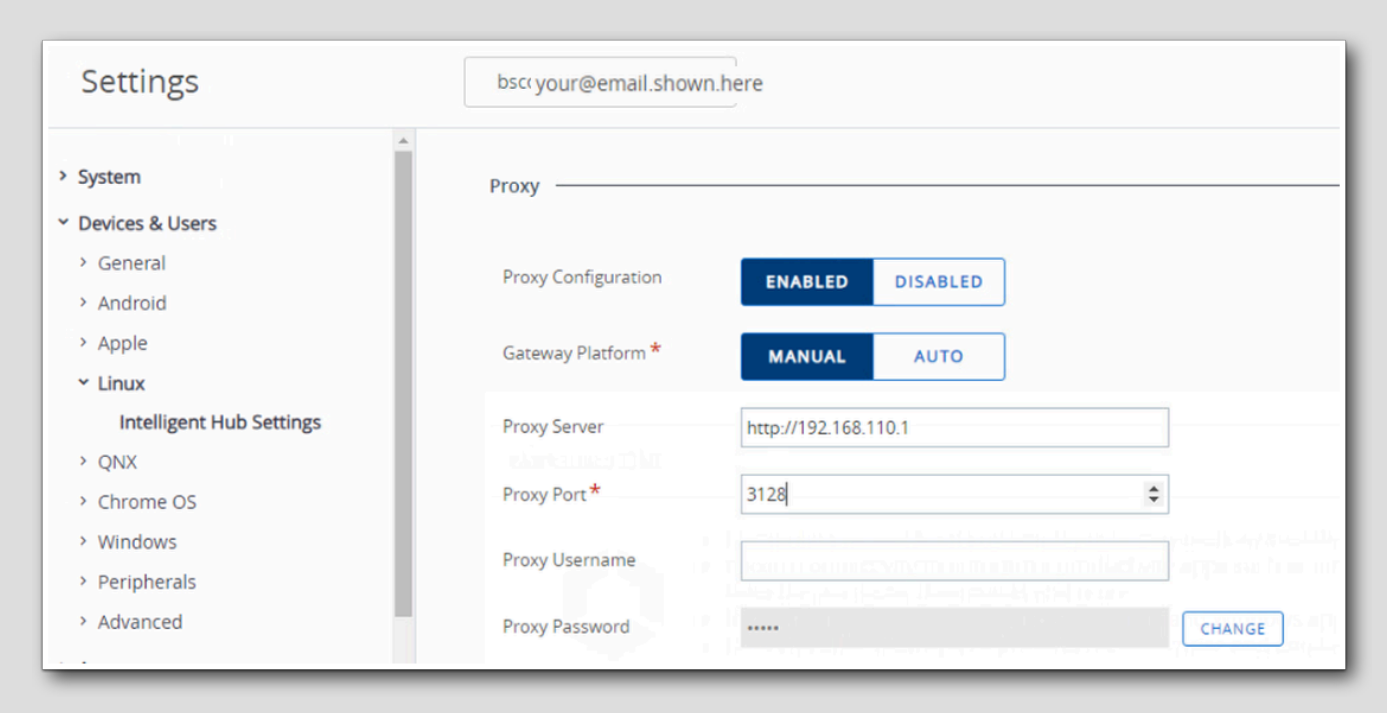
From within the Settings menu,

1. Expand **Devices & Users** in the left column

2. Expand **Linux**

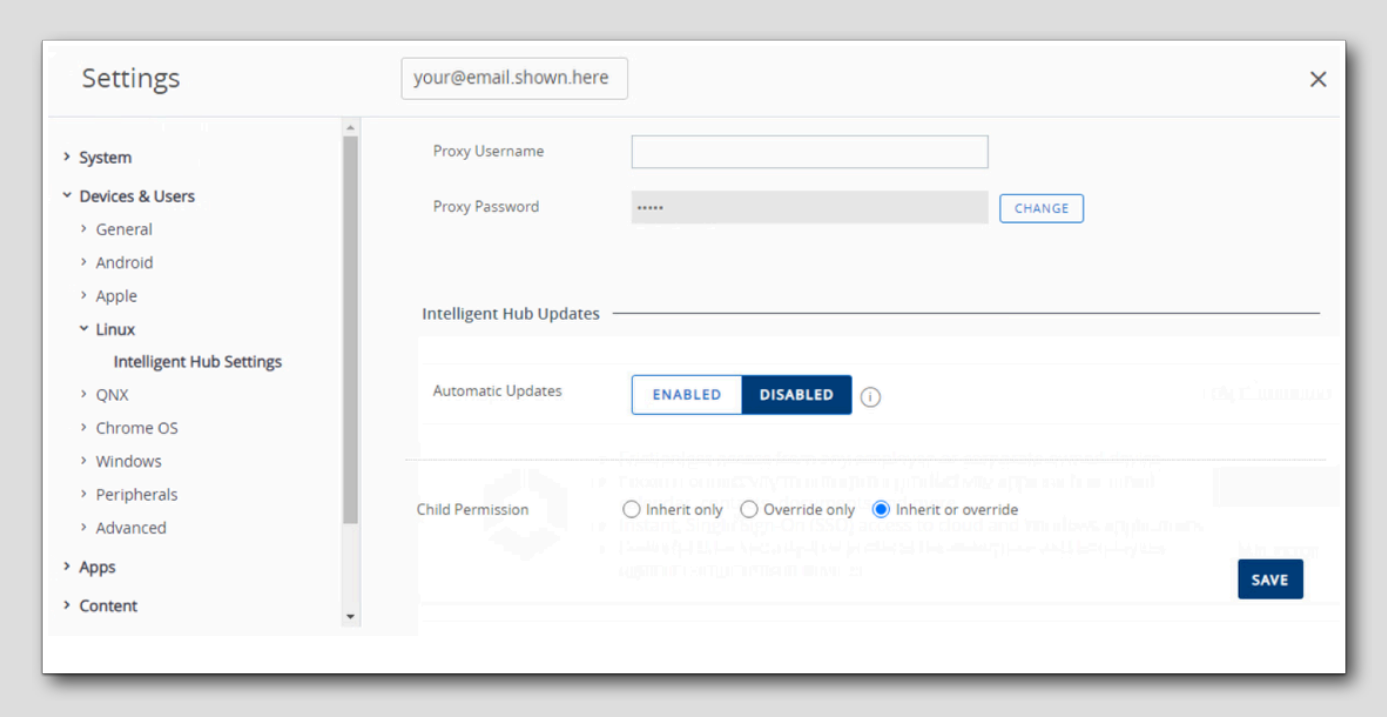
3. Click **Intelligent Hub Settings**

4. Select **Override** for the Current Setting



1. Scroll down to the bottom of the page
2. Select **Enabled** for the Proxy Configuration
3. Select **Manual** for the Gateway Platform
4. Enter **http://192.168.110.1** for the Proxy Server
5. Enter **3128** for the Proxy Port

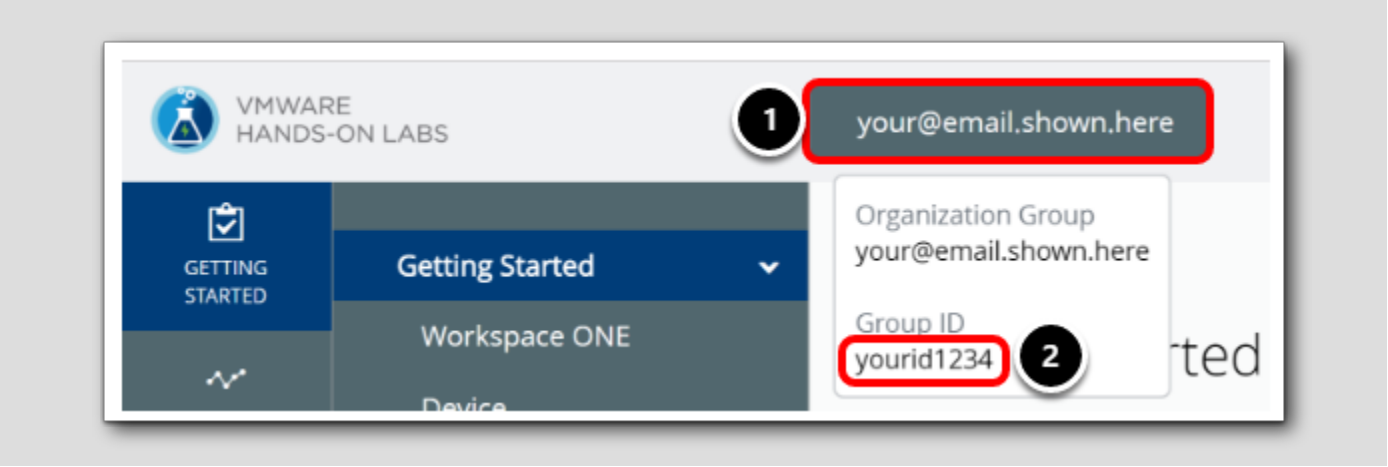
Note: In the lab we do not require a Proxy Username or Password and will leave these values at their defaults.

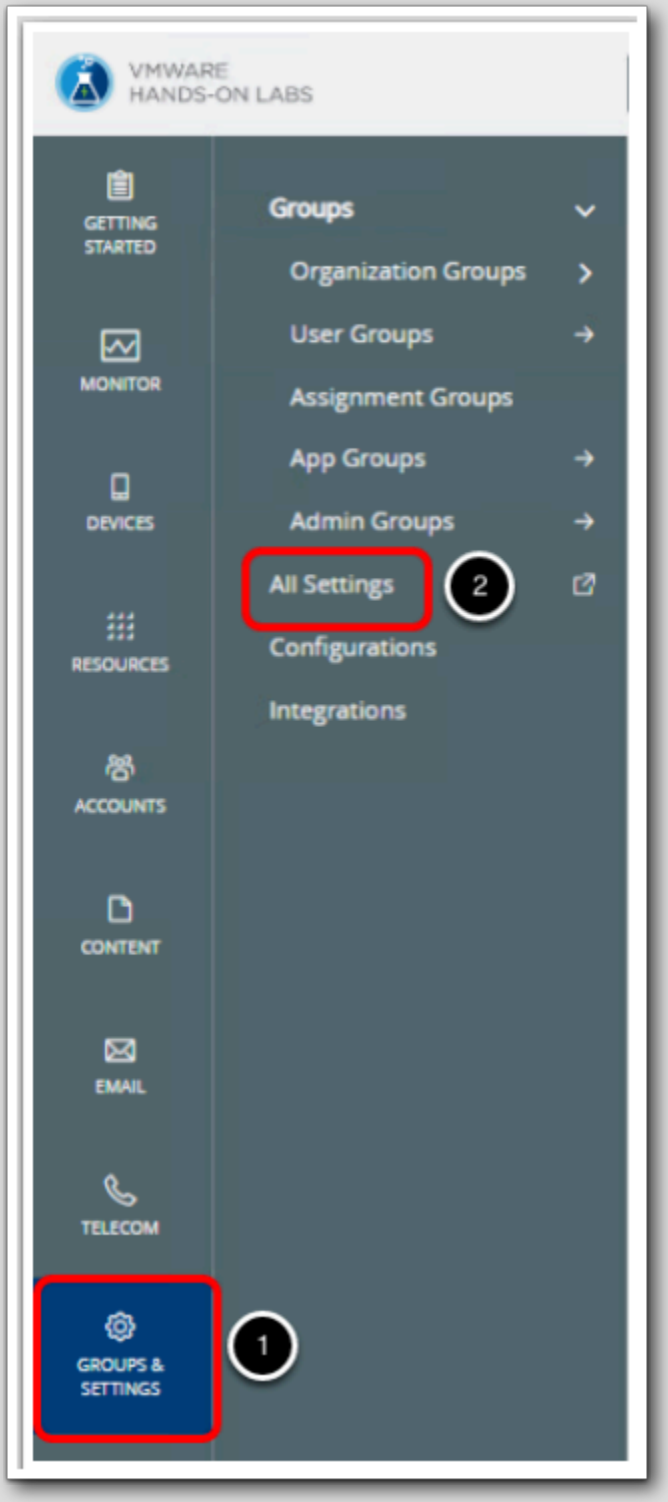


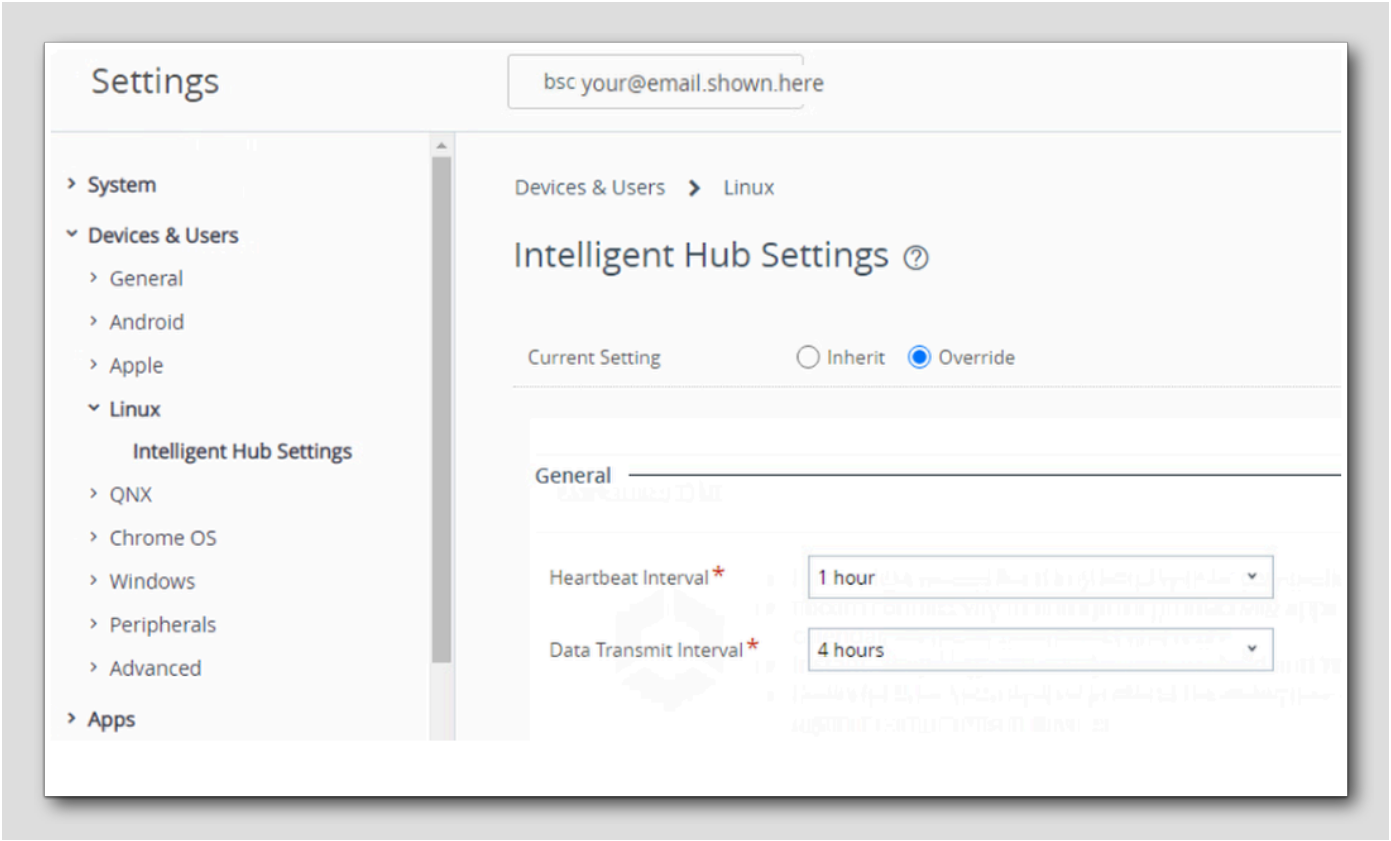
1. Scroll down to the bottom of the page

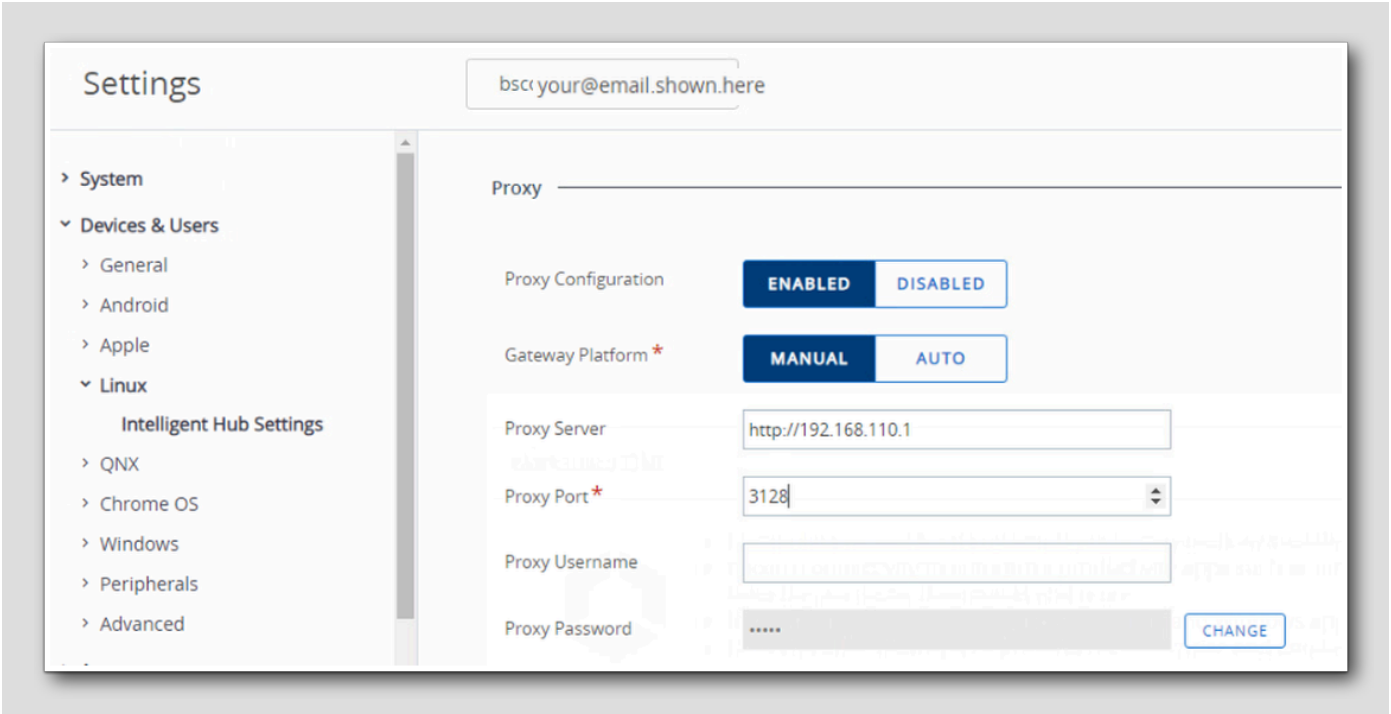
2. Click **Save**

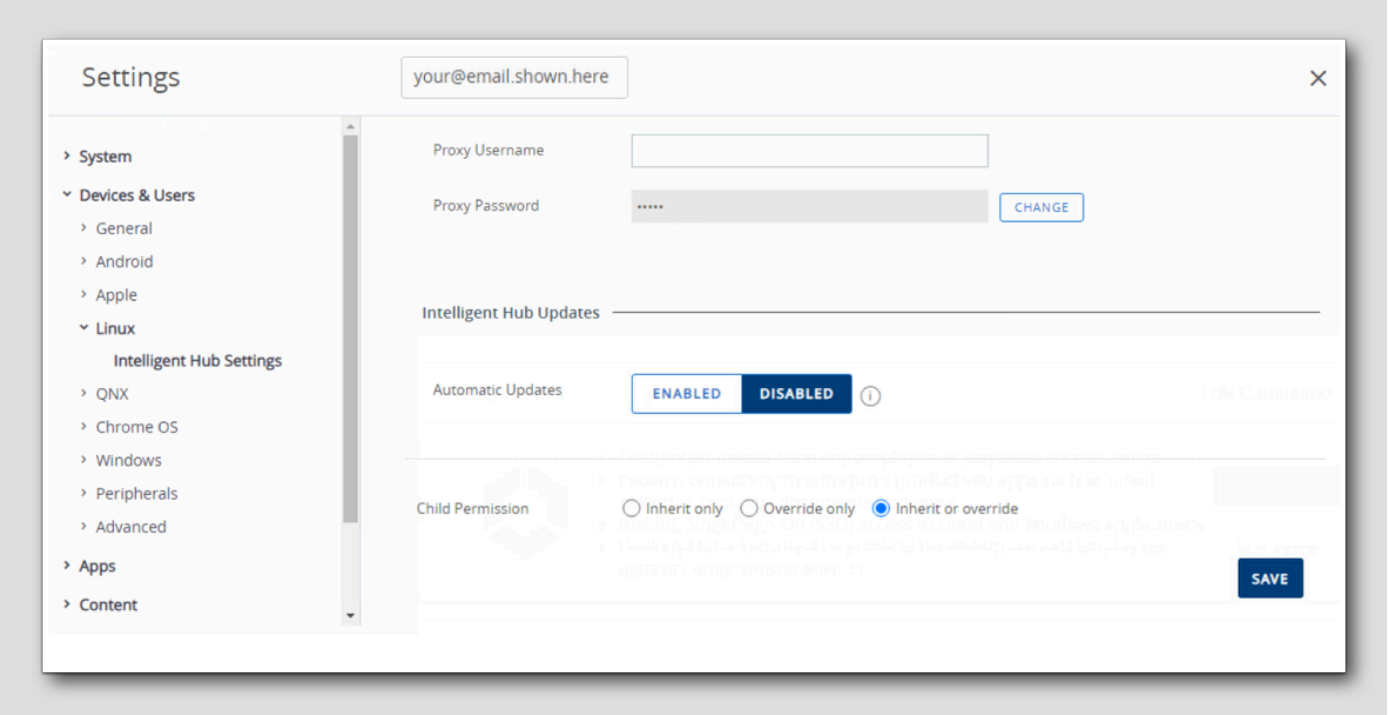
3. Click **Close**




VMWARE
HANDS-ON LABS
GETTING STARTED
MONITOR
DEVICES
RESOURCES
ACCOUNTS
CONTENT
EMAIL
TELECOM
GROUPS & SETTINGS
1
Groups
Organization Groups
User Groups
Assignment Groups
App Groups
Admin Groups
All Settings
2
Configurations
Integrations


Settings
bsc your@email.shown.here
System
Devices & Users
General
Android
Apple
Linux
Intelligent Hub Settings
QNX
Chrome OS
Windows
Peripherals
Advanced
Apps
Devices & Users > Linux
Intelligent Hub Settings
Current Setting
Inherit
Override
General
Heartbeat Interval *
1 hour
Data Transmit Interval *
4 hours


Settings
bsc your@email.shown.here
System
Devices & Users
General
Android
Apple
Linux
Intelligent Hub Settings
QNX
Chrome OS
Windows
Peripherals
Advanced
Proxy
Proxy Configuration
ENABLED
DISABLED
Gateway Platform *
MANUAL
AUTO
Proxy Server
http://192.168.110.1
Proxy Port *
3128
Proxy Username
Proxy Password
CHANGE

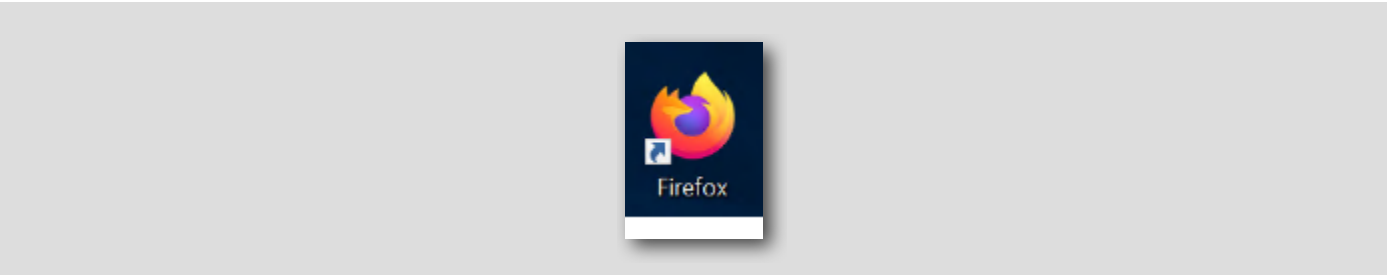


Locate your Group ID from Workspace ONE UEM Console [702]

Configure Linux Intelligent Hub Settings [703]

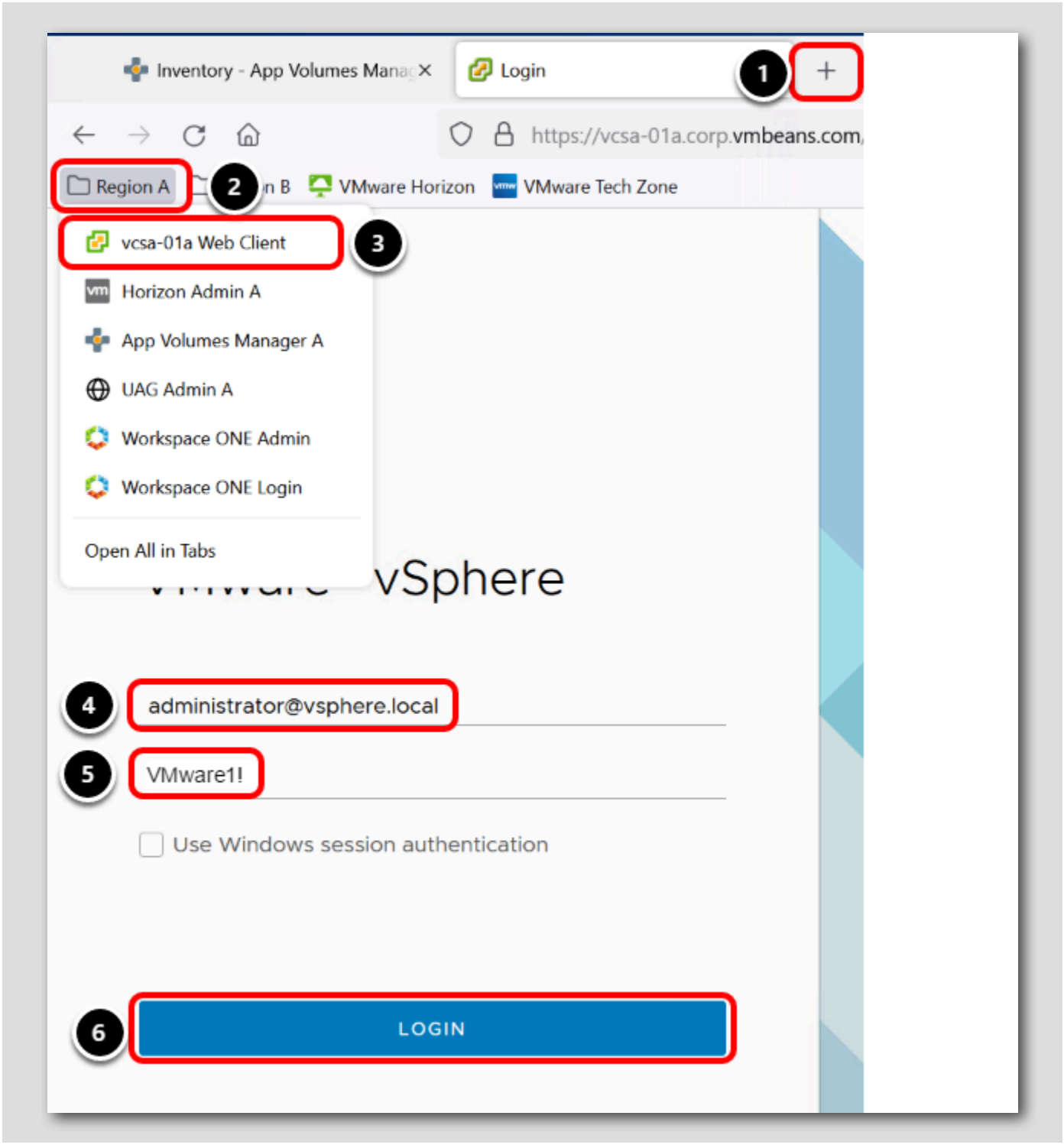
Log into vCenter [704]

Launch Firefox [705]



On the Main Console desktop, launch the **Firefox** browser

Log in to vCenter [706]

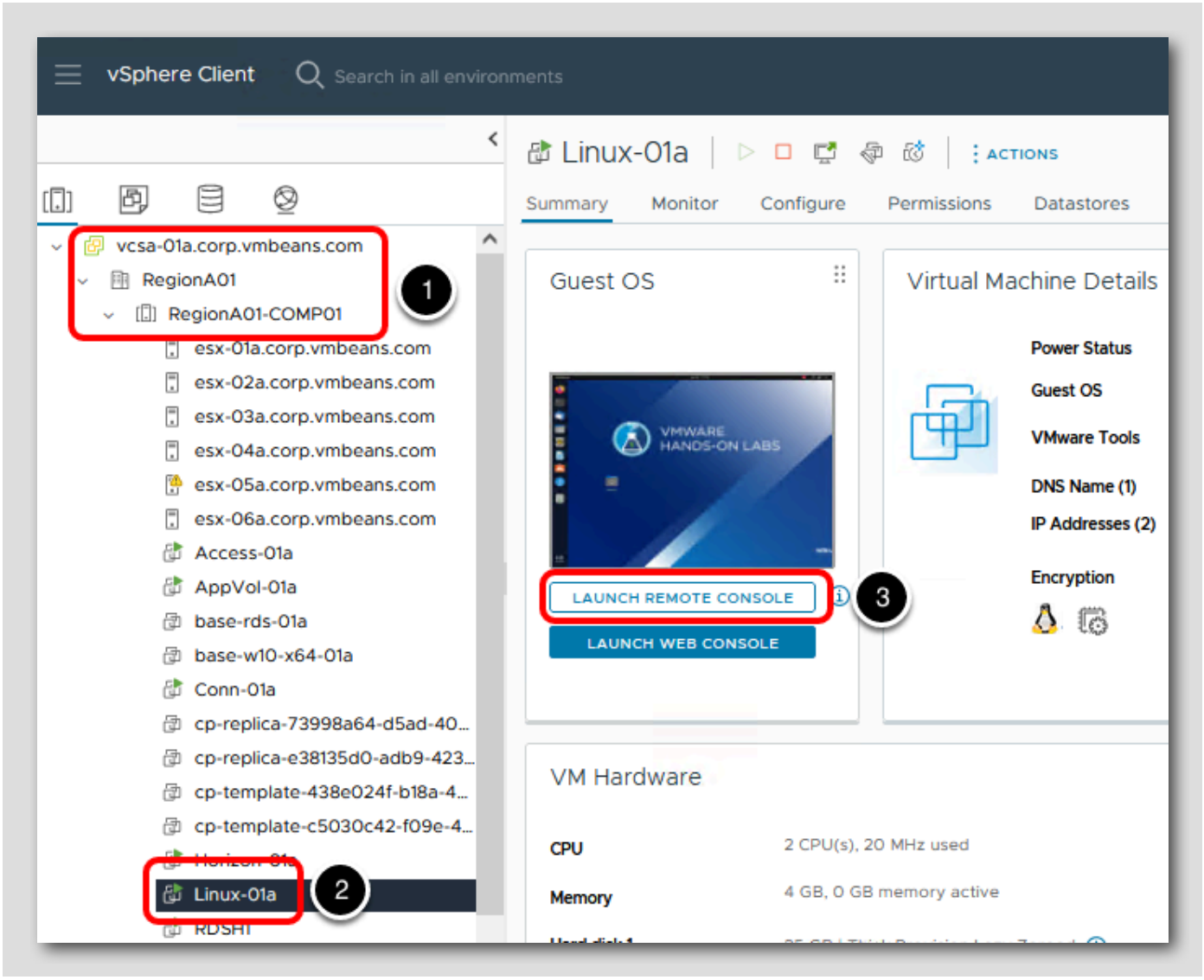


To log in to vCenter:

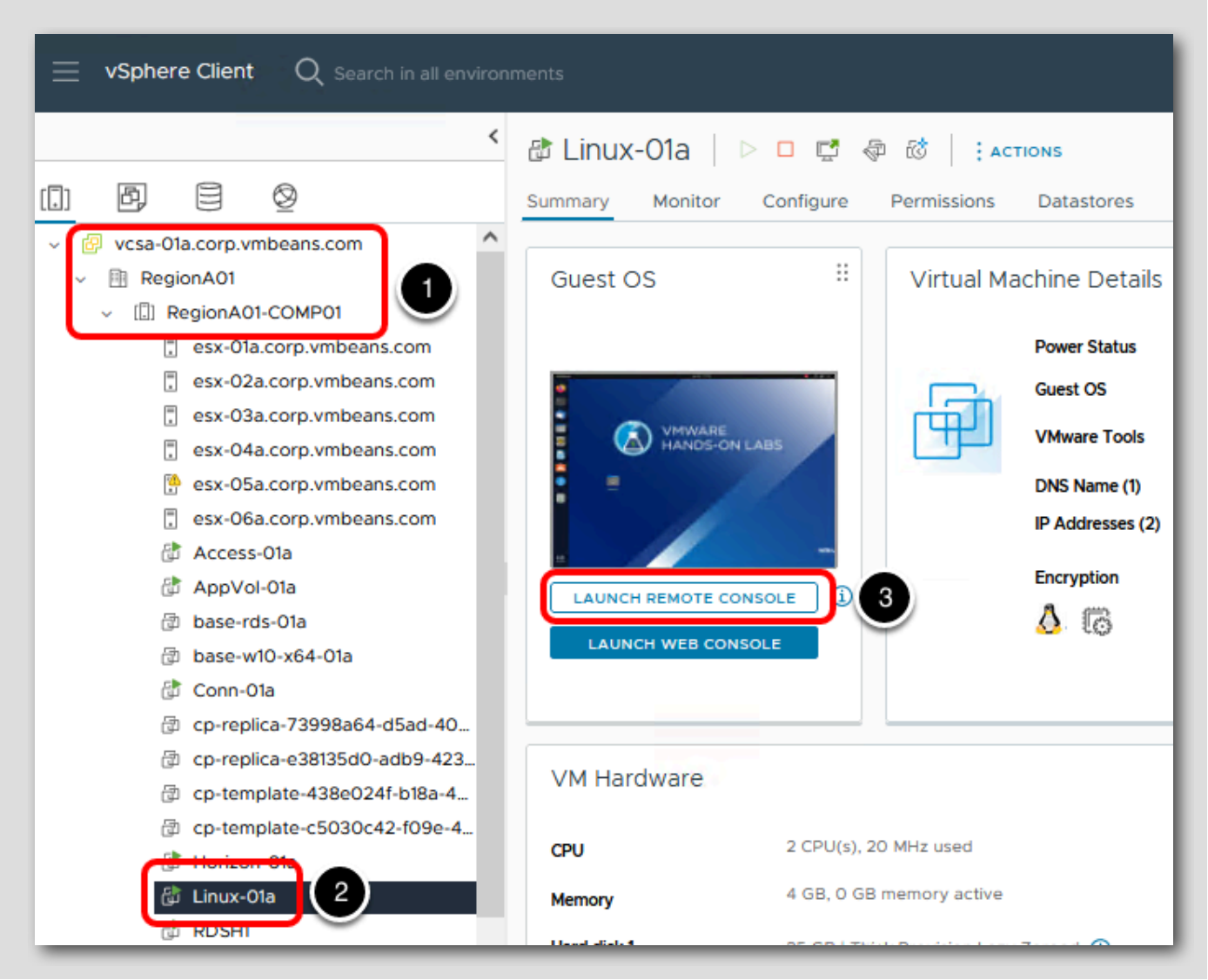
1. Click the + icon to open a new tab in the Firefox browser
2. Click the **Region A** bookmarks folder
3. Click **vcsa-01a Web Client** to open vCenter
4. Enter Username: **administrator@vsphere.local**
5. Enter Password: **VMware1!**
6. Click **Login**

Enroll Linux Machine

[707]



1. Expand **vcsa-01a.corp.vmbeans.com** -> **RegionA01** -> **RegionA01-COMP01**
2. Click the **Linux-01a** virtual machine
3. Click **LAUNCH REMOTE CONSOLE**

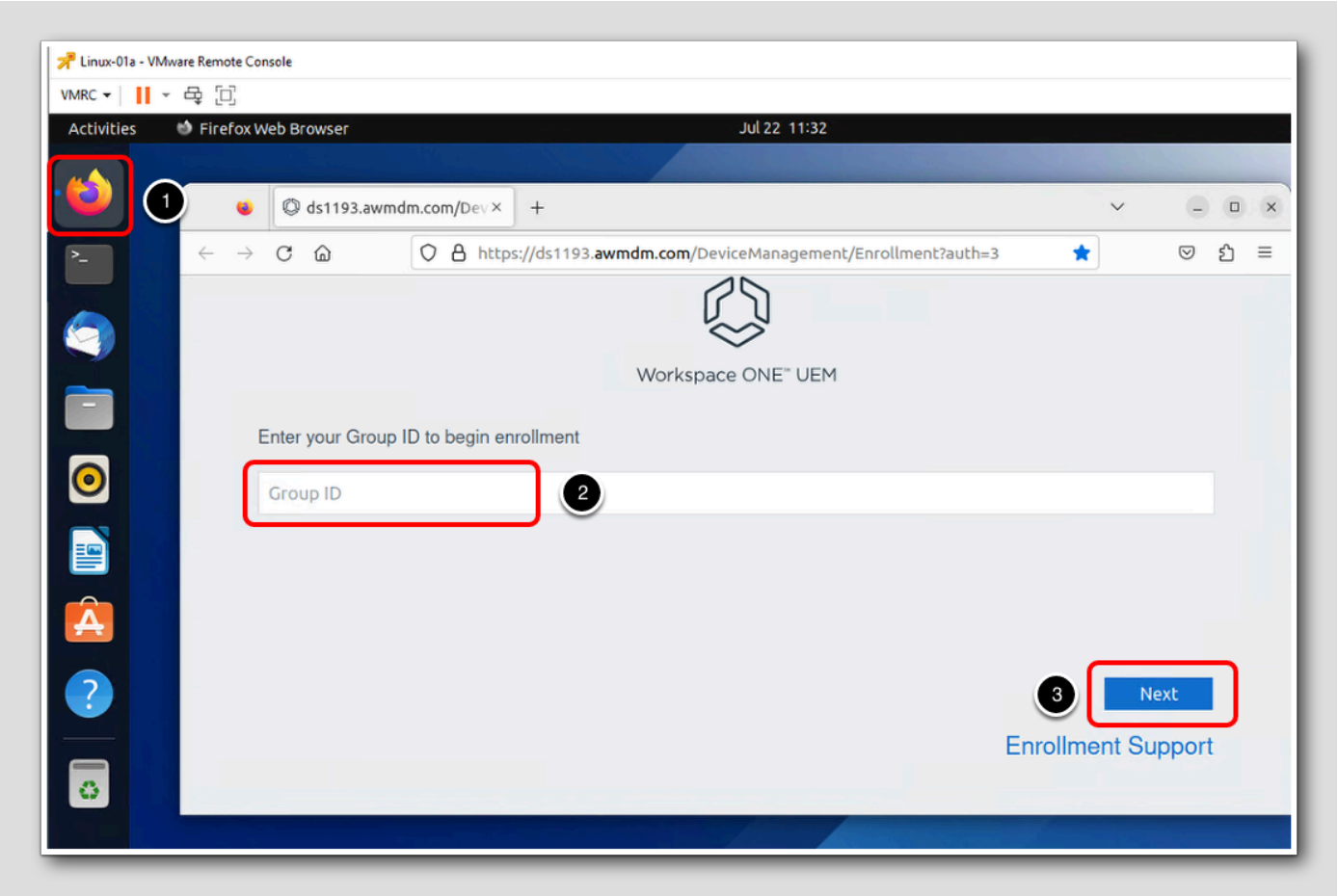


Launch Remote Console for Linux Virtual Machine

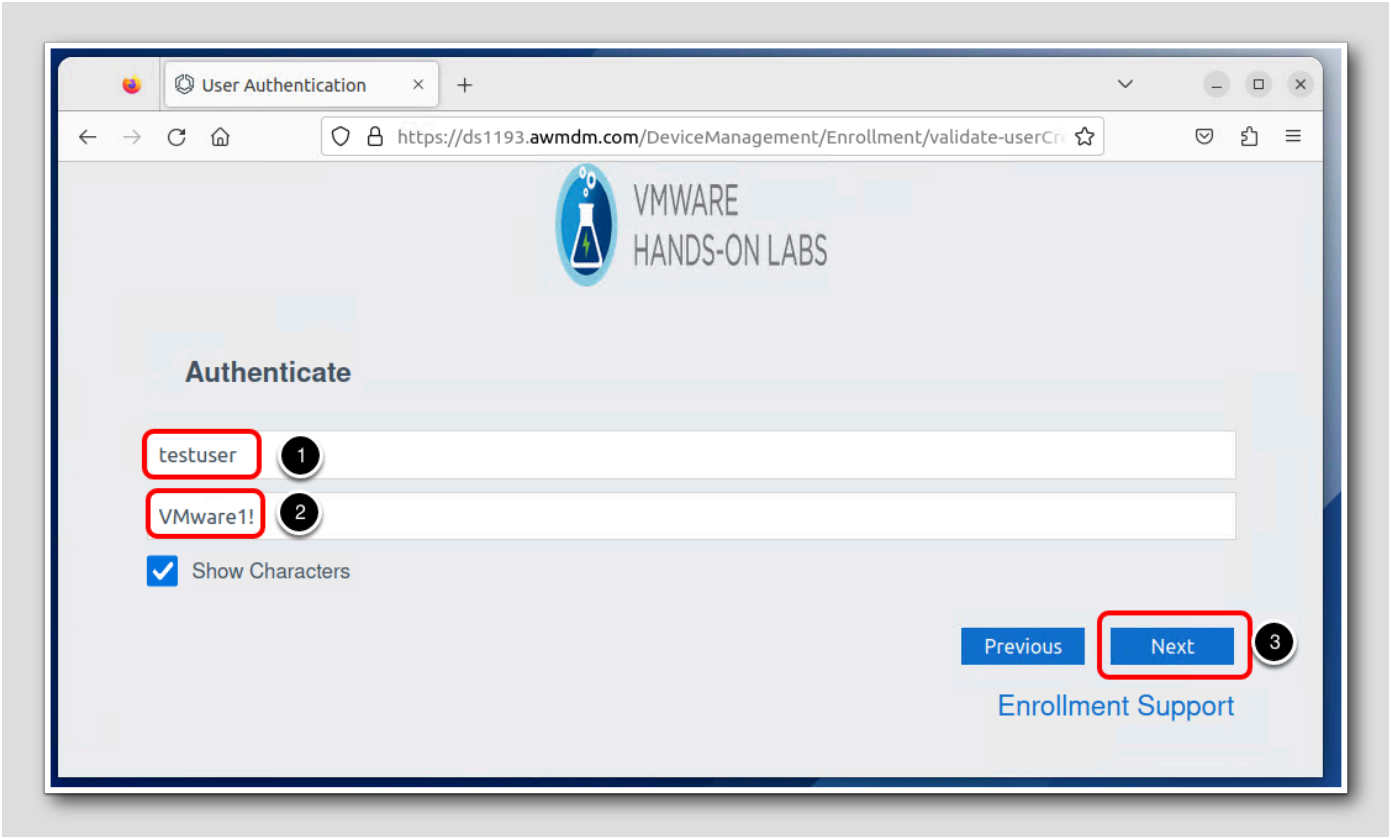
[708]

Download Intelligent Hub

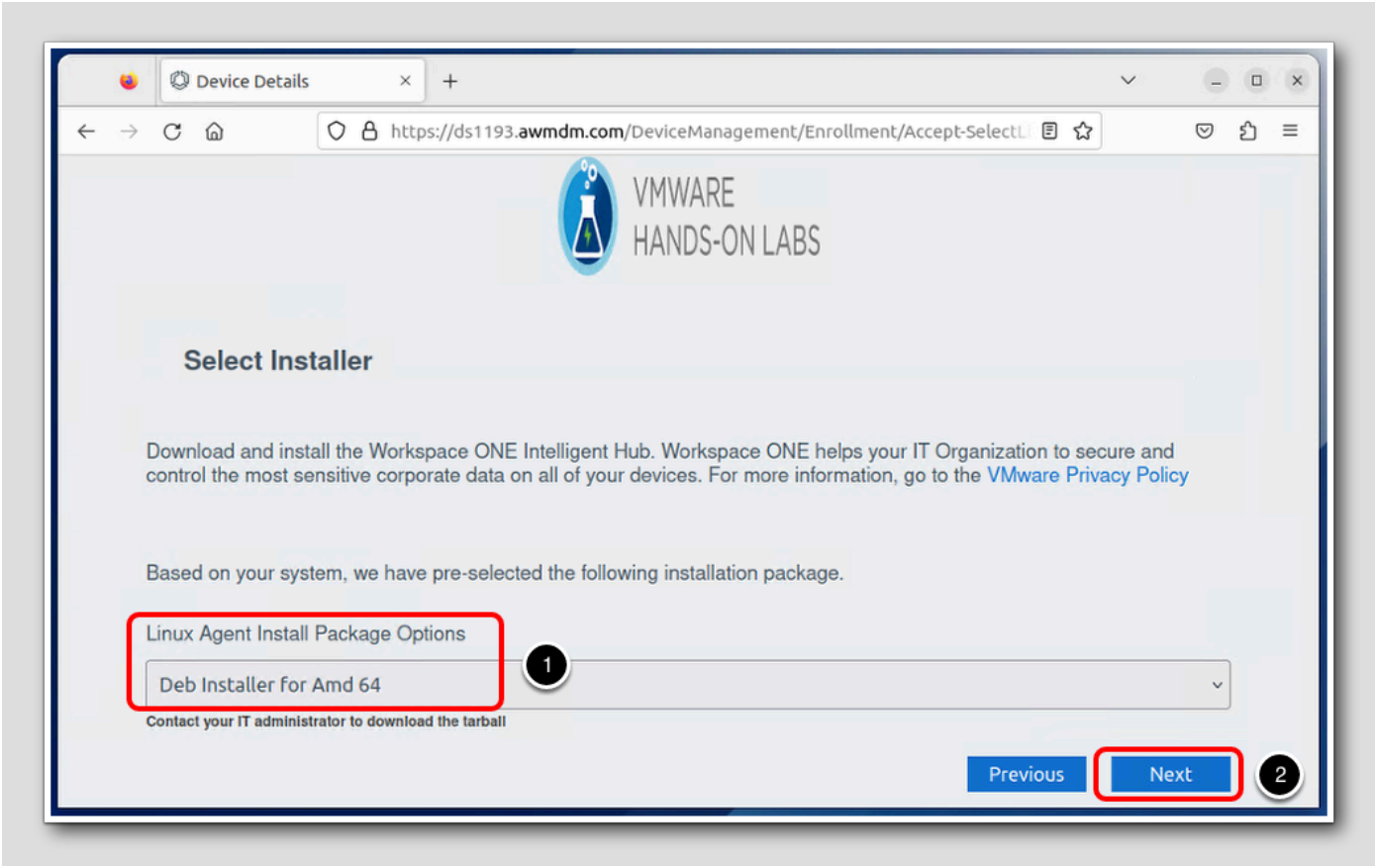
[709]



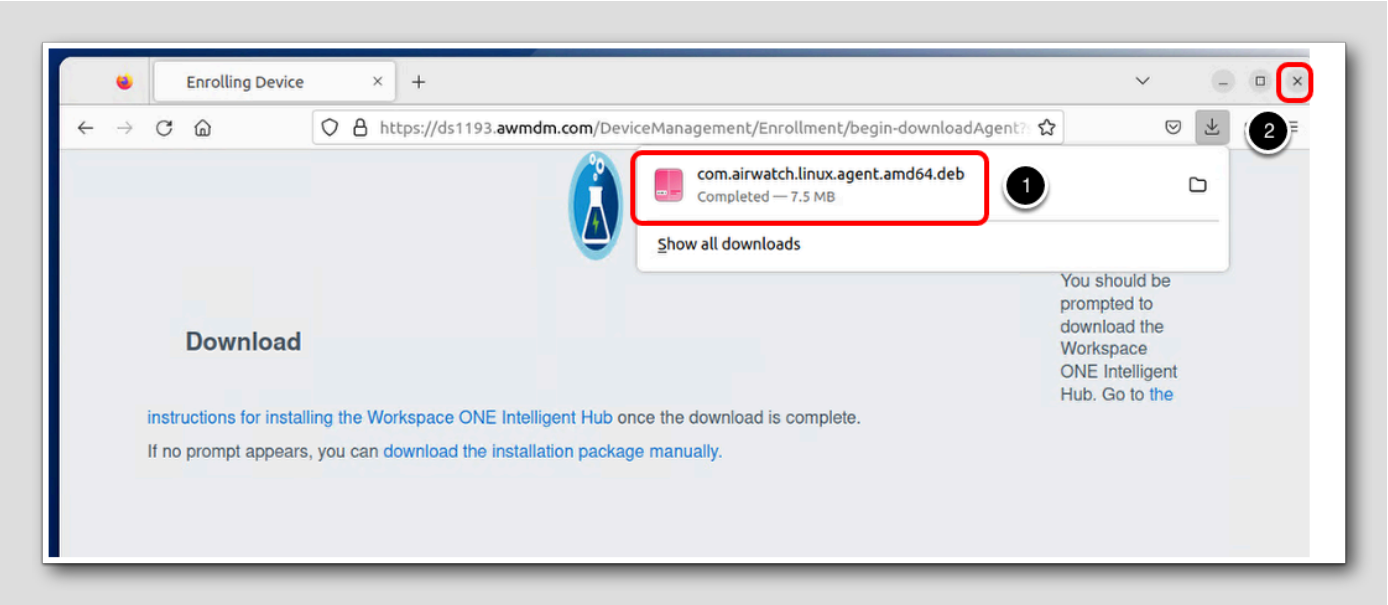
1. Click **Firefox**
2. Enter your **Group ID** that was copied from the UEM console earlier in the module
3. Click **Next**



1. Enter **testuser** for Username
2. Enter **VMware1!** for Password
3. Click **Next**



1. Leave the default selection for the Linux Agent Installer - Deb Installer for AMD 64
    - Note: If we were using a different version of Linux we could change this to download the appropriate installer
2. Click **Next**



The download will begin automatically

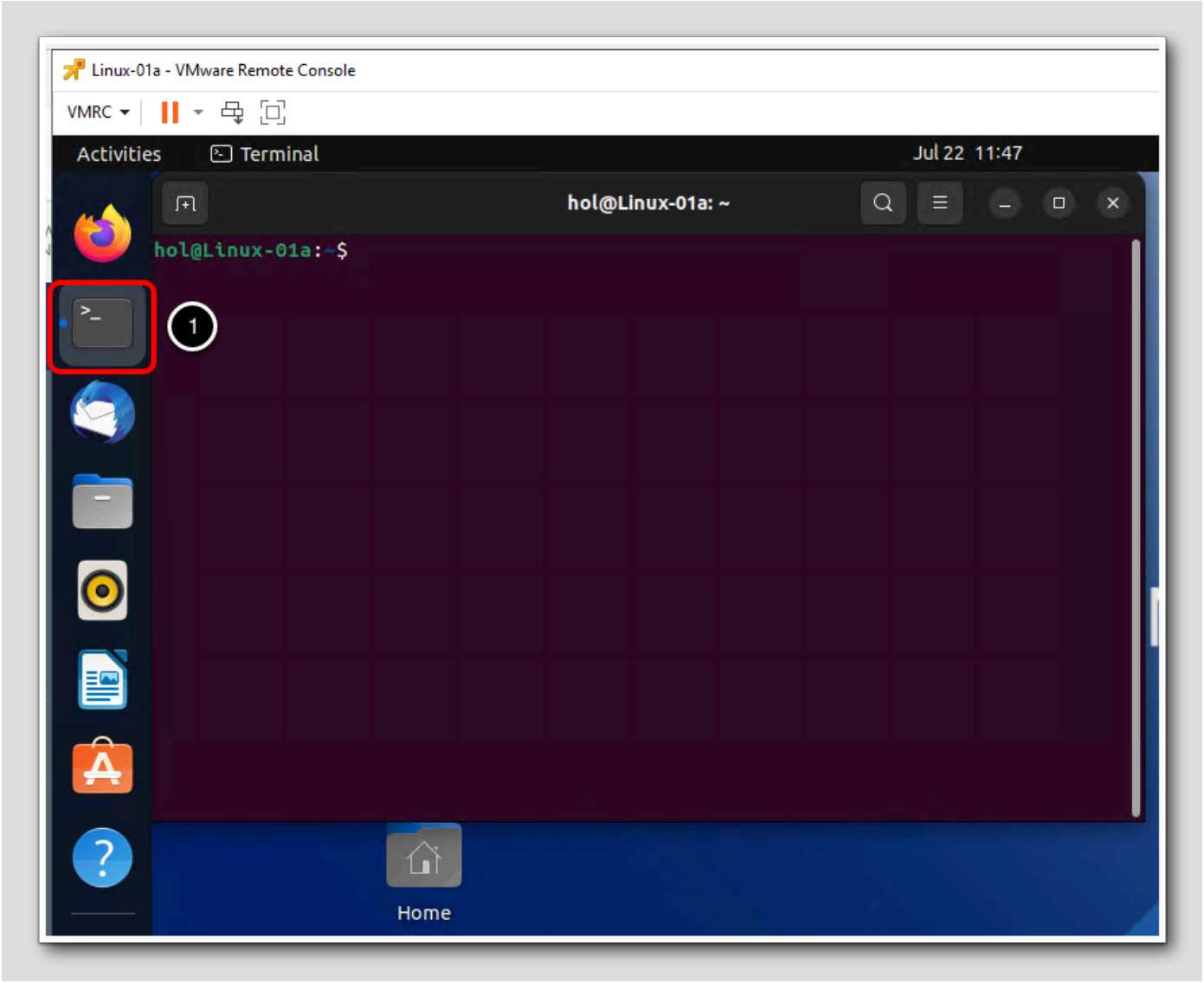
1. Verify the Agent downloaded successfully
2. Close **Firefox**

After the Agent has been downloaded it is installed using the Terminal. For more information about installing the Intelligent Hub please refer to the following *documentation*.

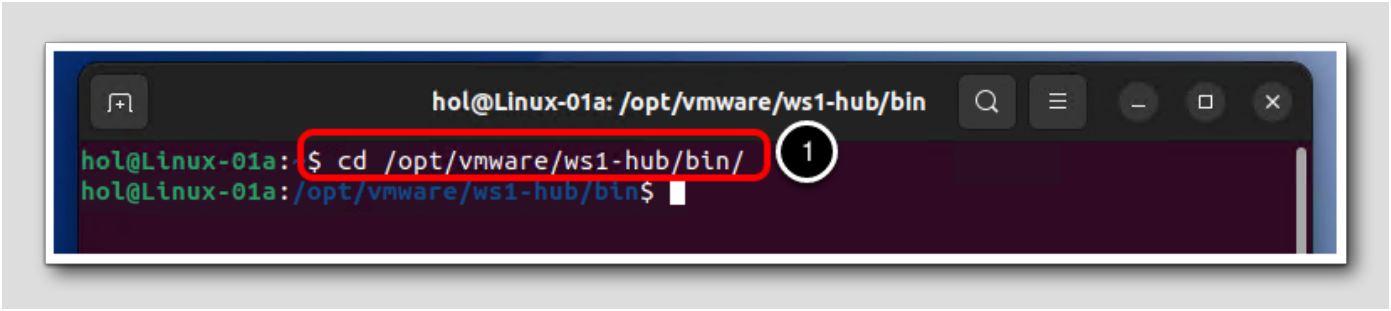
Note: In the lab we have already installed the Linux agent for you, please proceed to the next step and Enroll the Linux Machine.

Enroll the Linux Machine

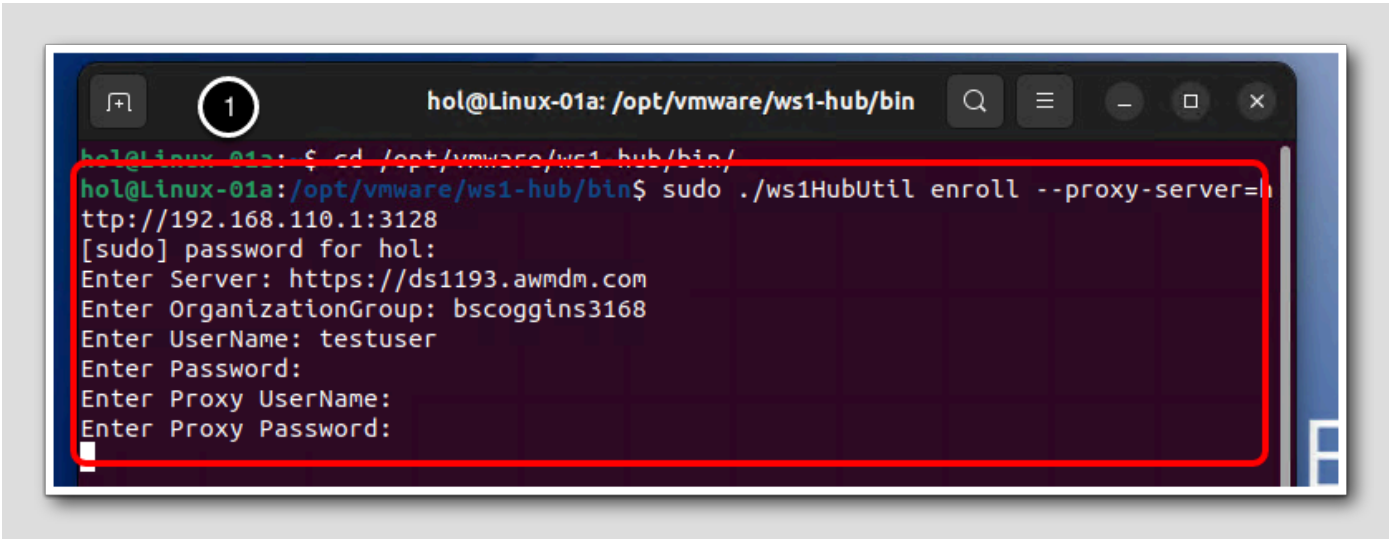
[710]



1. Click **Terminal**

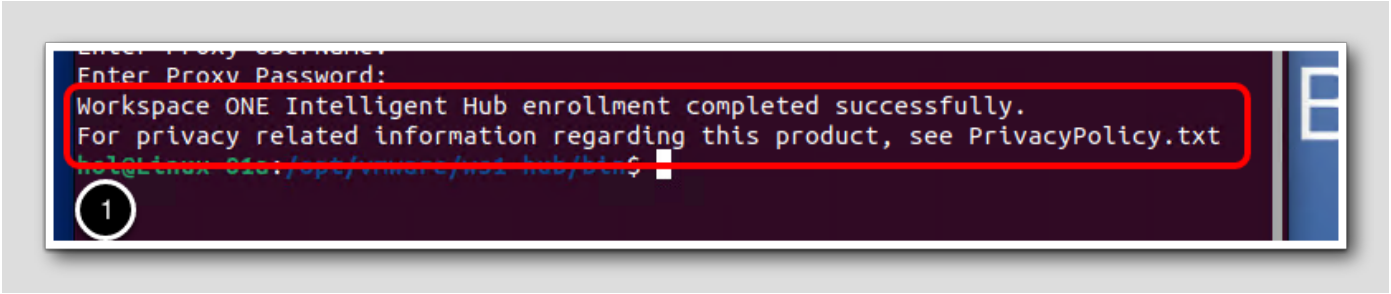


1. Type the following command `cd /opt/vmware/ws1-hub/bin` and press Enter



1. Type the following command to begin the enrollment process `sudo ./ws1HubUtil enroll --proxy-server=htttp://192.168.110.1:3128` and press **enter**
    - Enter `VMware1!` for hol password and press **enter**
    - Enter `https://ds1193.awmdm.com` for Server and press **enter**
    - Enter your `Group ID` for OrganizationGroup and press **enter**
    - Enter `testuser` for UserName and press **enter**
    - Enter `VMware1!` for UserName and press **enter**
    - Leave Proxy UserName blank and press **enter**
    - Leave Proxy Password blank and press **enter**

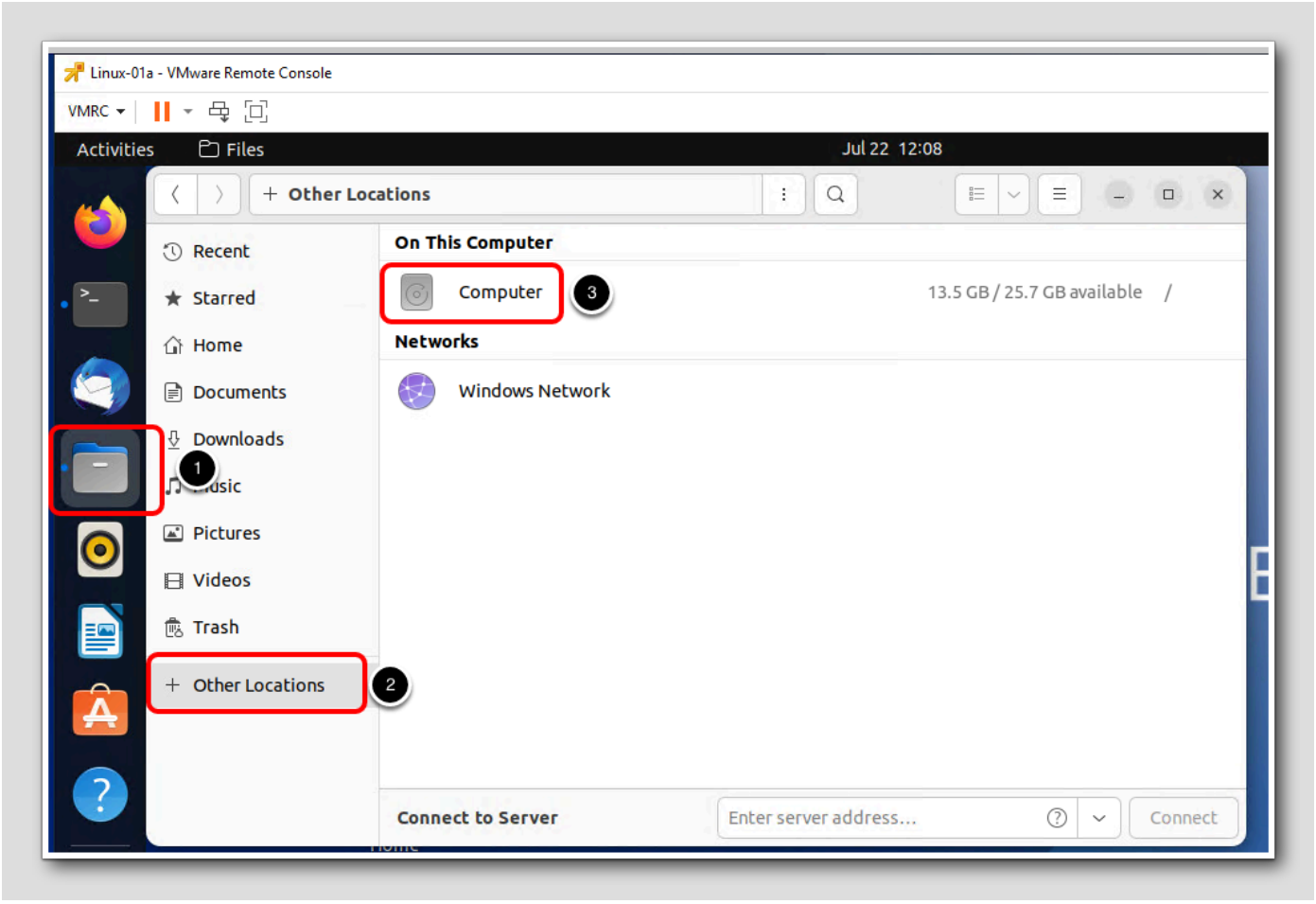
Note: The enrollment process may take several minutes to complete and you can proceed to the next steps



1. Once the enrollment process finishes you should see the following message

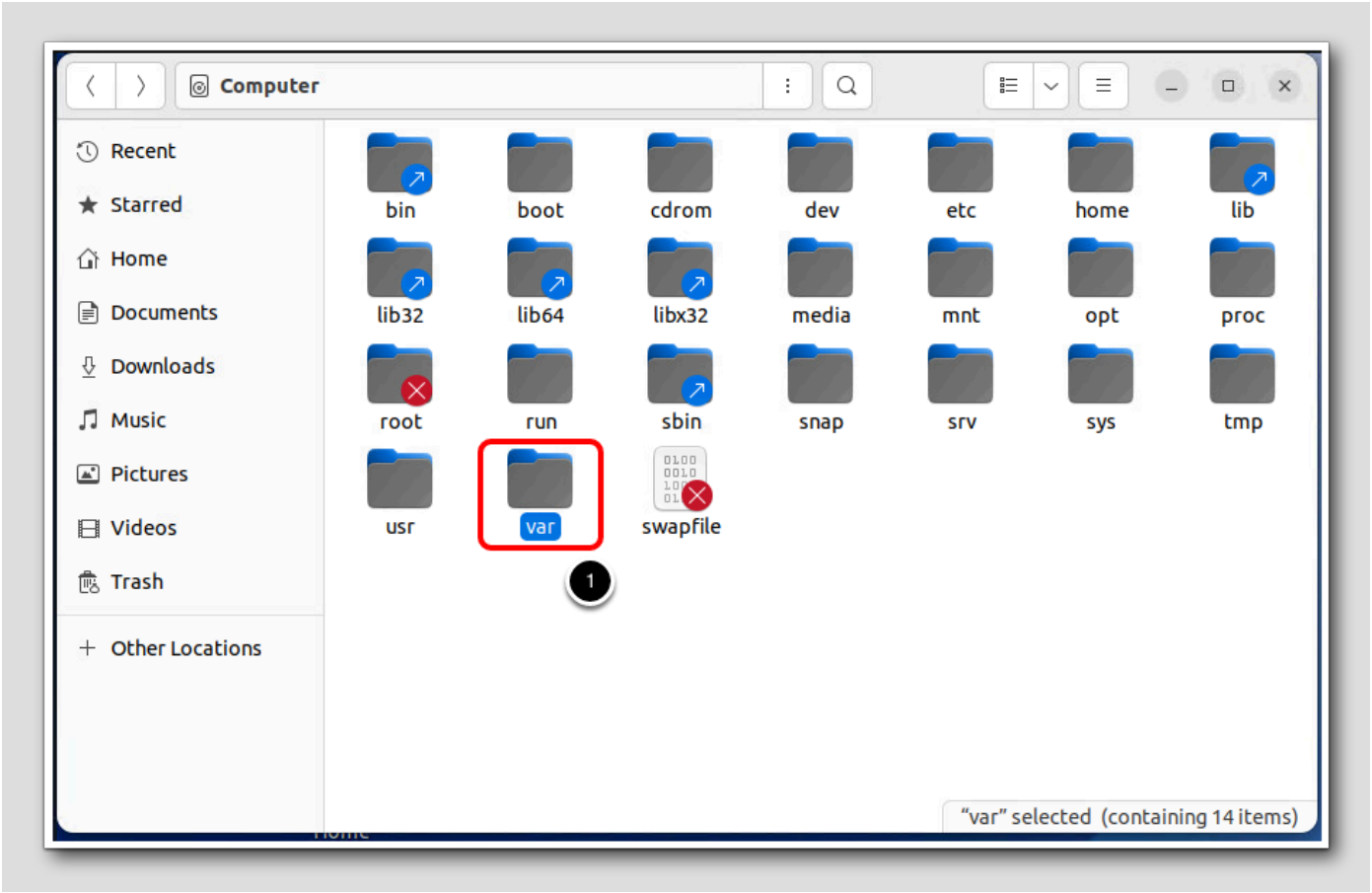
Troubleshooting Enrollment Issues

[711]

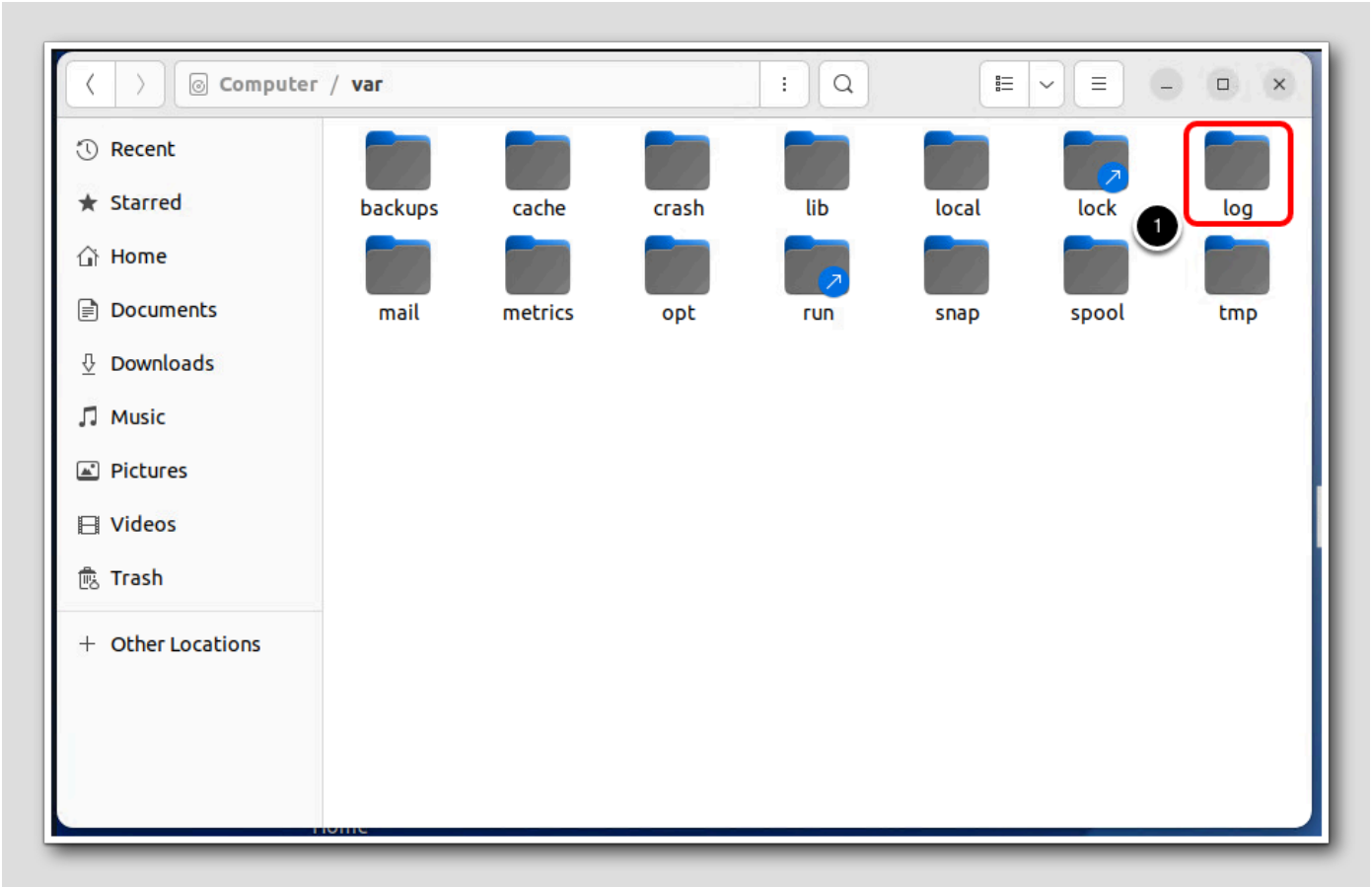


1. Click **Files**

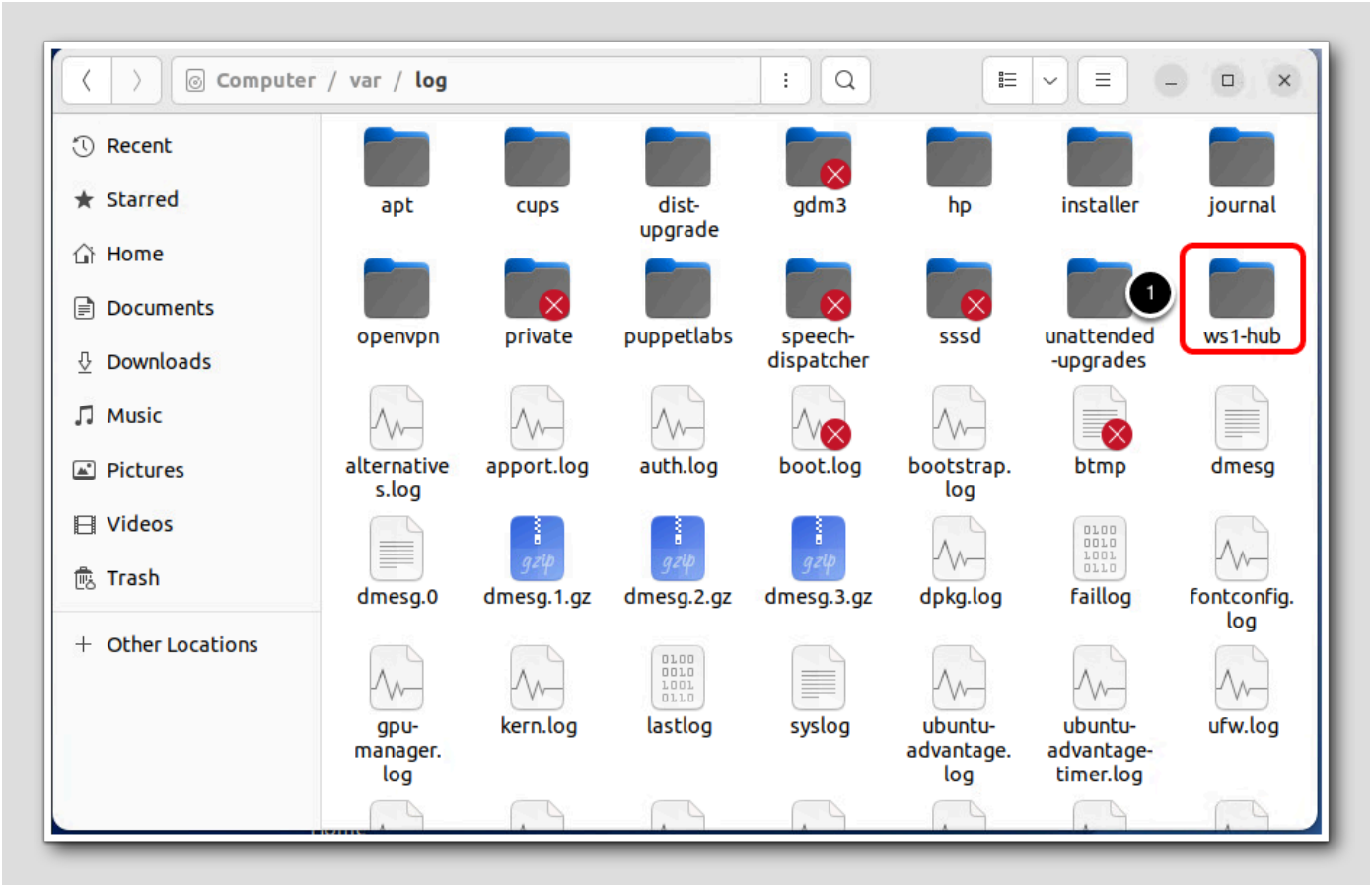
2. Click **Other Locations**
3. Click **Computer**



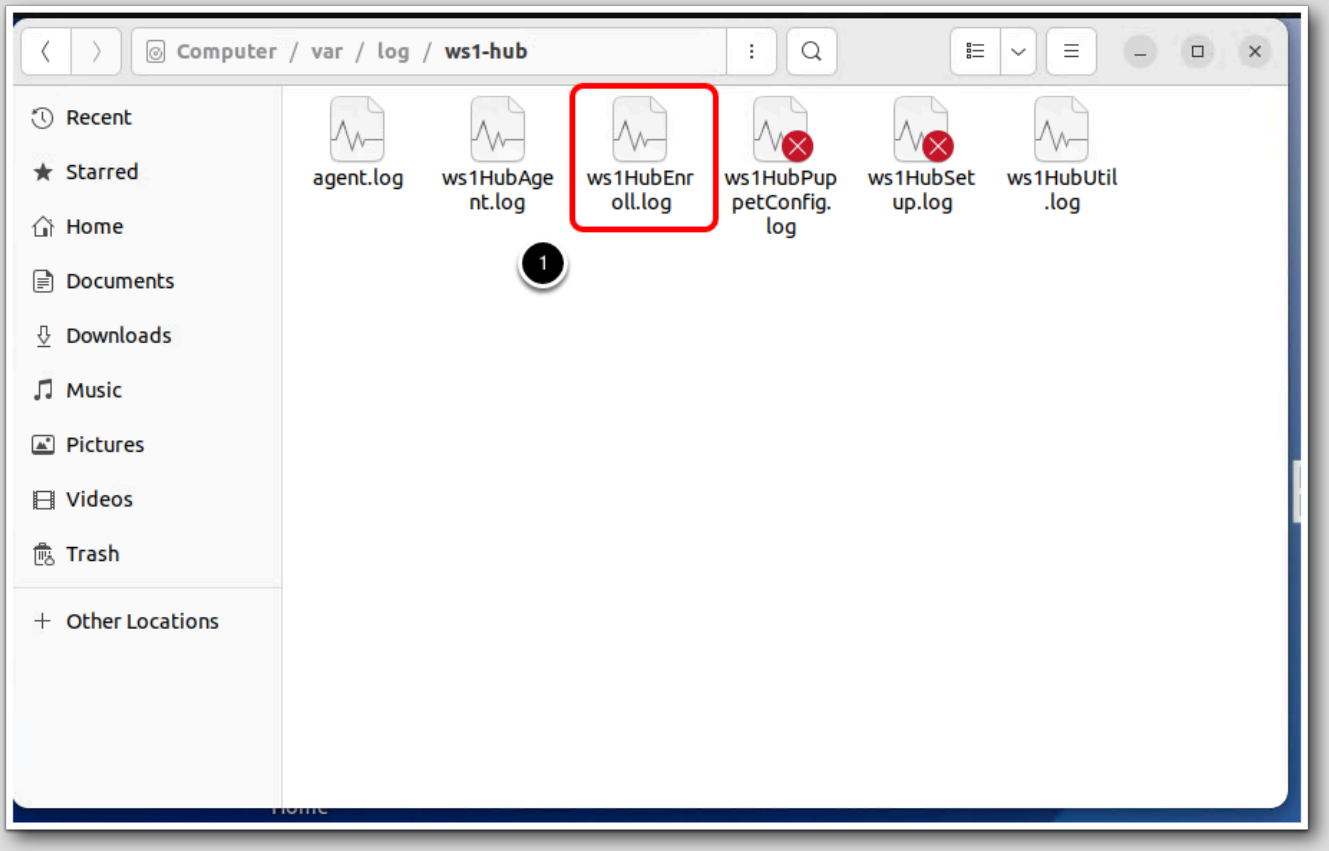
1. Click **var**


Computer / var
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
backups
cache
crash
lib
local
lock
log
mail
metrics
opt
run
snap
spool
tmp
1

1. Click **log**

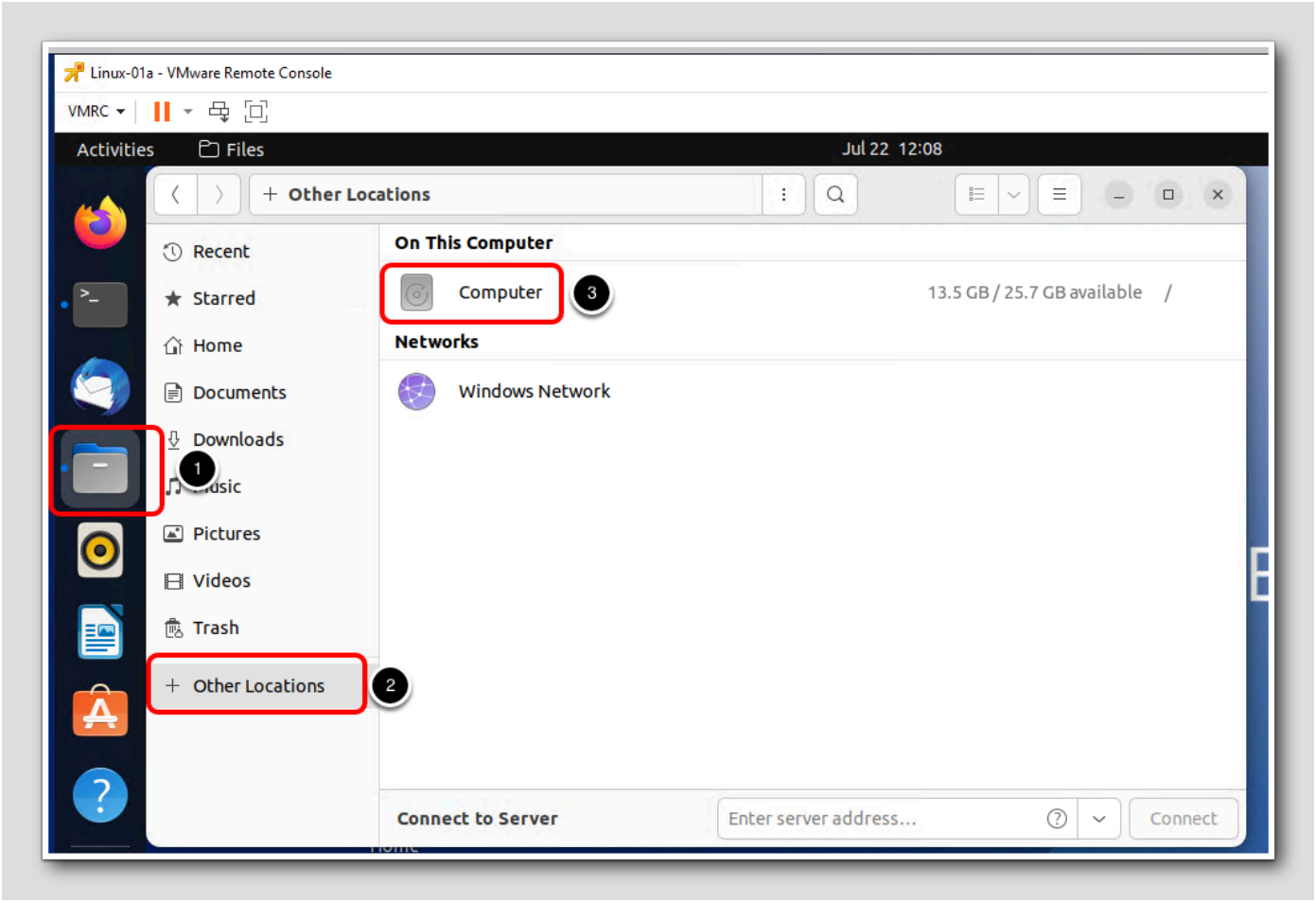


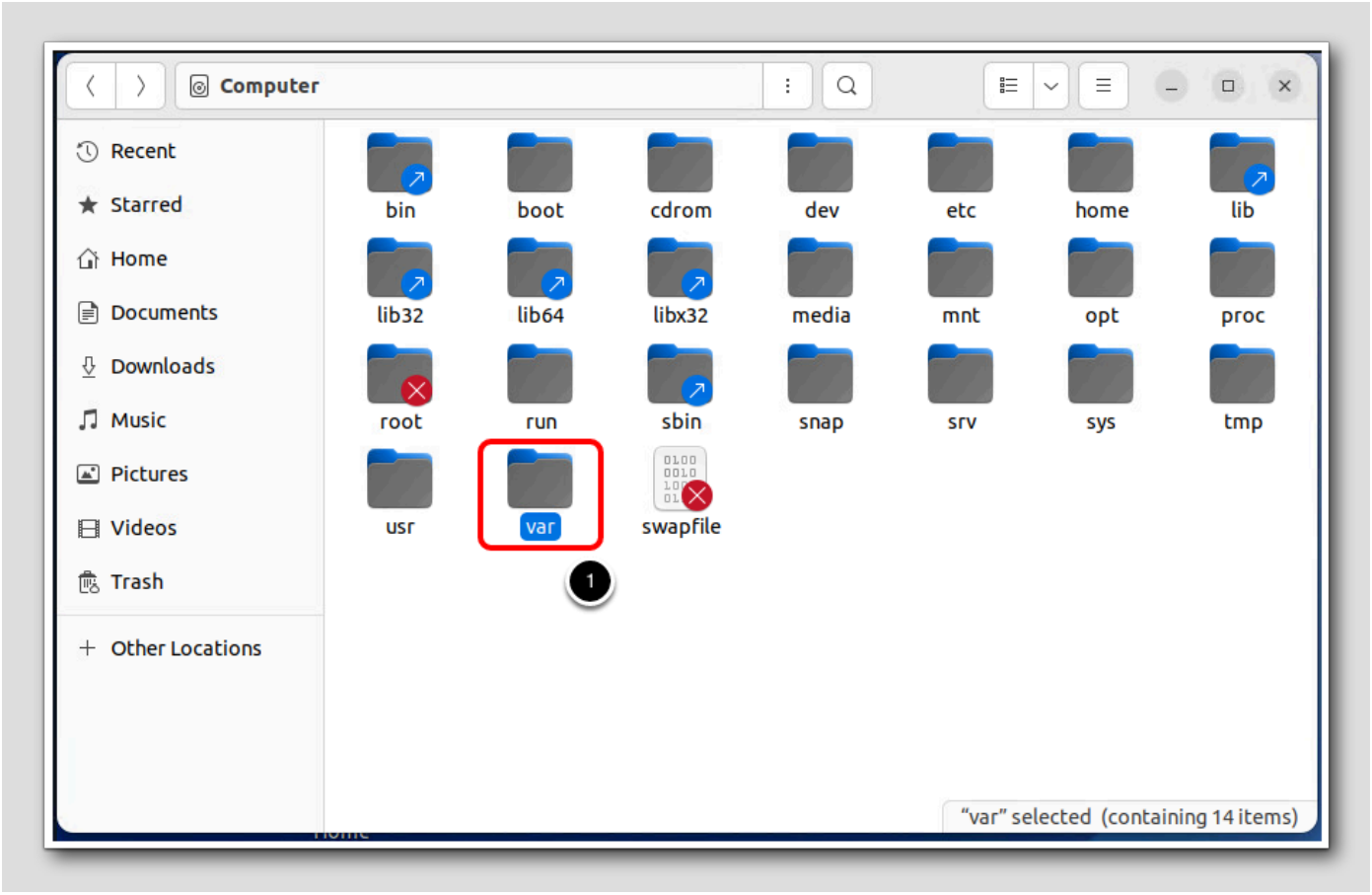
1. Click **ws1-hub**

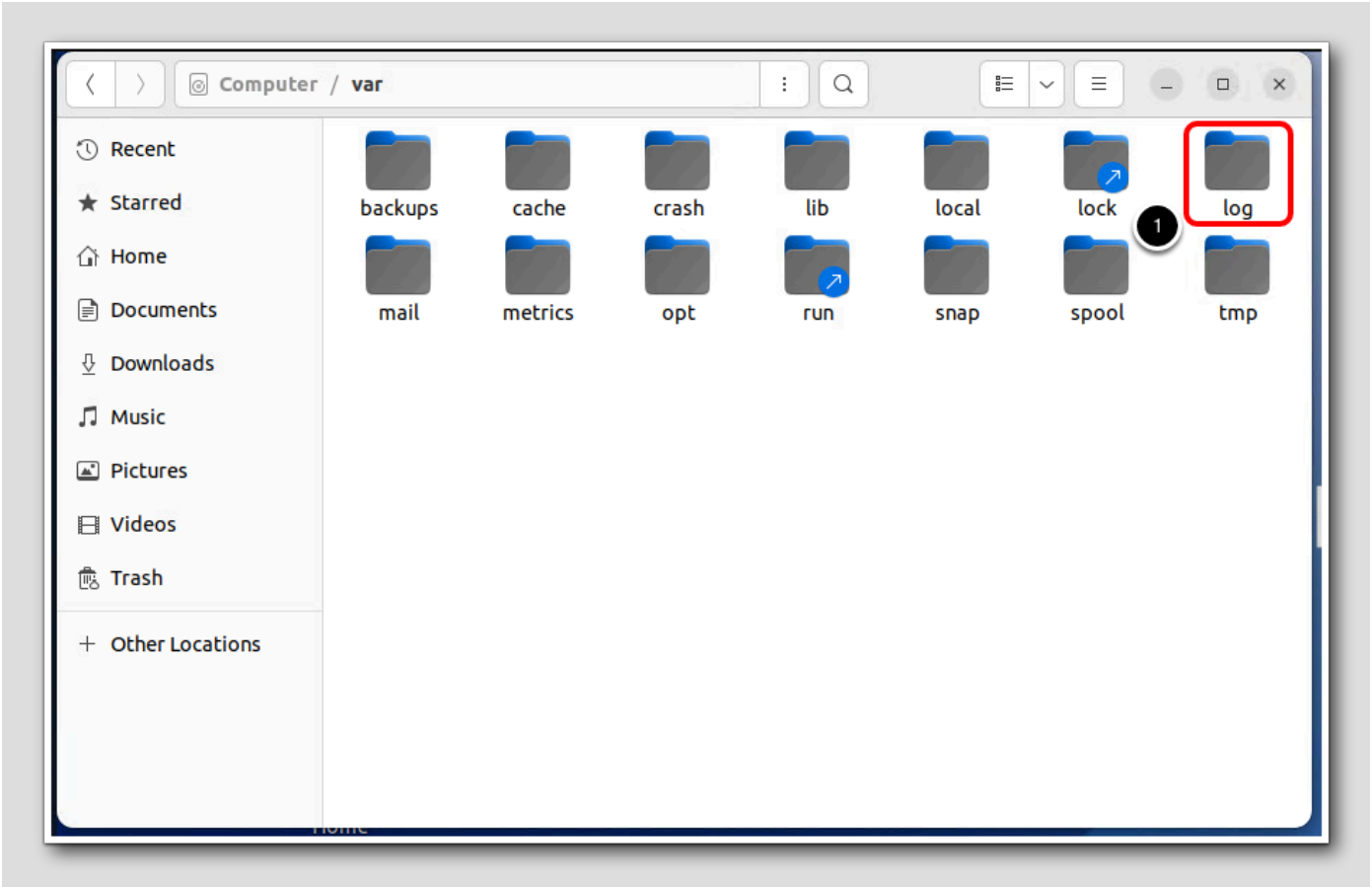


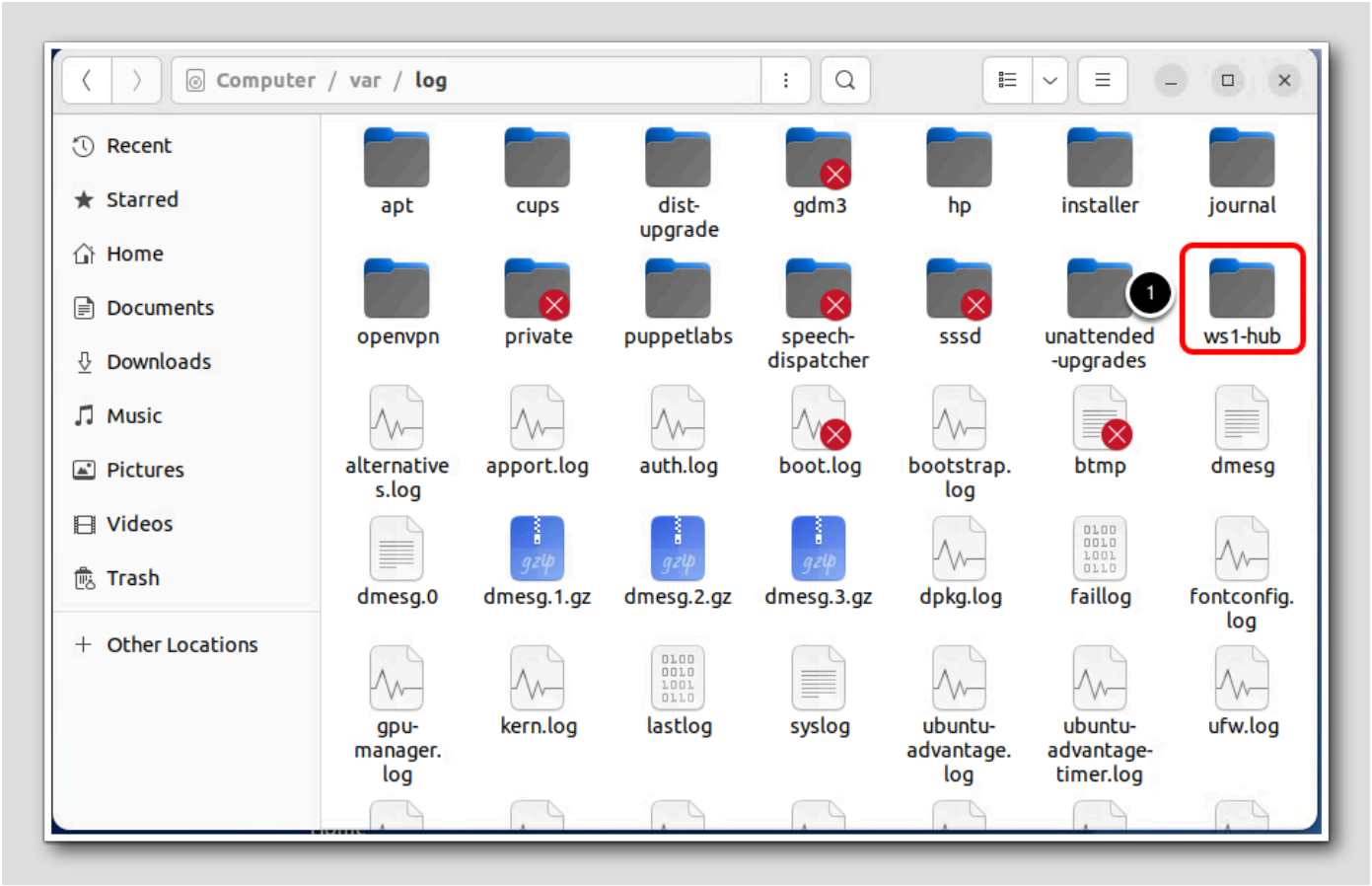
1. Double Click the **ws1HubEnroll.log** file

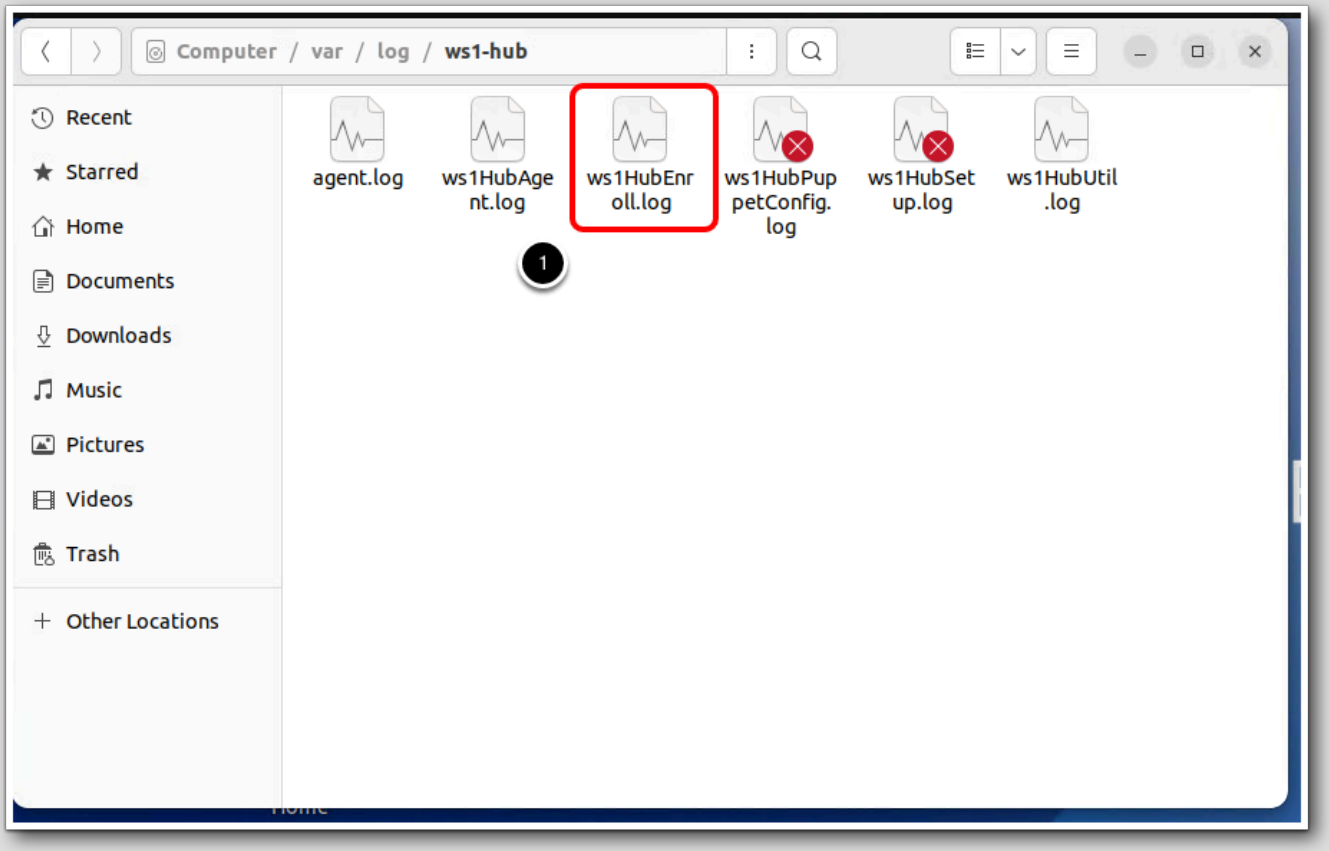
The ws1HubEnroll.log file can be used to help troubleshoot enrollment issues if required.

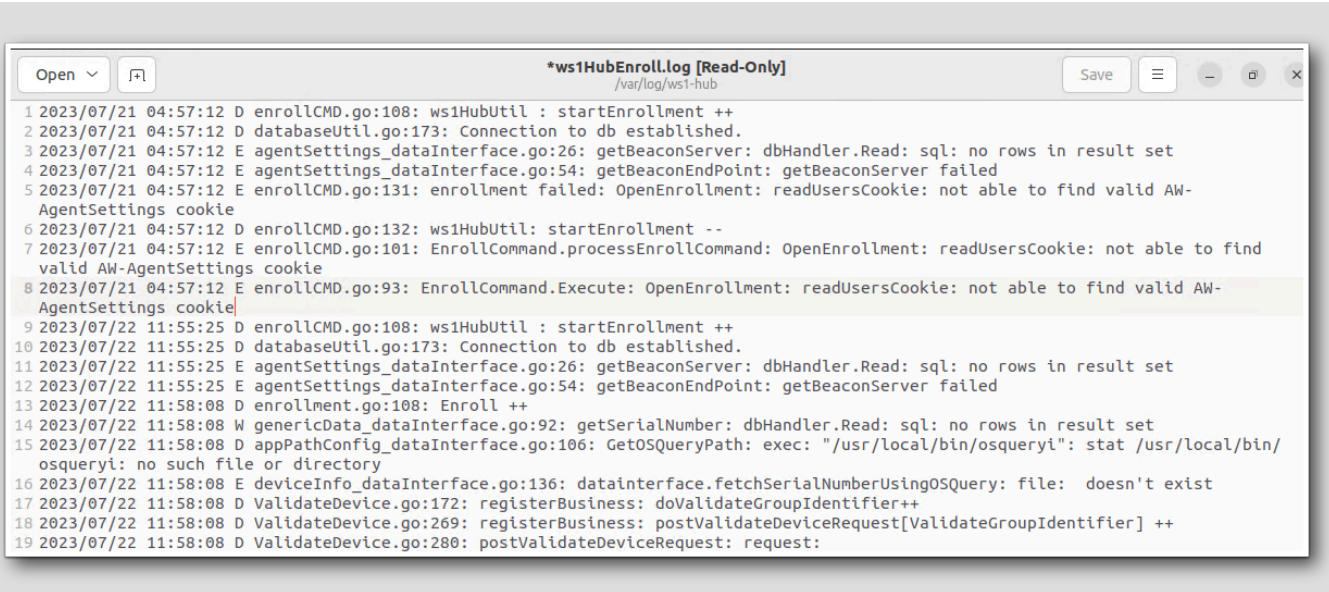



Computer
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
bin
boot
cdrom
dev
etc
home
lib
lib32
lib64
libx32
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
swapfile
1
"var" selected (containing 14 items)


Computer / var
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
backups
cache
crash
lib
local
lock
log
mail
metrics
opt
run
snap
spool
tmp
1


Computer / var / log
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
apt
cups
dist-upgrade
gdm3
hp
installer
journal
openvpn
private
puppetlabs
speech-dispatcher
sssd
unattended-upgrades
1
ws1-hub
alternatives.log
apport.log
auth.log
boot.log
bootstrap.log
btmp
dmesg
dmesg.0
dmesg.1.gz
dmesg.2.gz
dmesg.3.gz
dpkg.log
faillog
fontconfig.log
gpu-manager.log
kern.log
lastlog
syslog
ubuntu-advantage.log
ubuntu-advantage-timer.log
ufw.log


Computer / var / log / ws1-hub
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
agent.log
ws1HubAgent.log
ws1HubEnroll.log
ws1HubPuppetConfig.log
ws1HubSetup.log
ws1HubUtil.log
1


Open
*ws1HubEnroll.log [Read-Only]
/var/log/ws1-hub
Save
1 2023/07/21 04:57:12 D enrollCMD.go:108: ws1HubUtil : startEnrollment ++
2 2023/07/21 04:57:12 D databaseUtil.go:173: Connection to db established.
3 2023/07/21 04:57:12 E agentSettings_dataInterface.go:26: getBeaconServer: dbHandler.Read: sql: no rows in result set
4 2023/07/21 04:57:12 E agentSettings_dataInterface.go:54: getBeaconEndPoint: getBeaconServer failed
5 2023/07/21 04:57:12 E enrollCMD.go:131: enrollment failed: OpenEnrollment: readUsersCookie: not able to find valid AW-AgentSettings cookie
6 2023/07/21 04:57:12 D enrollCMD.go:132: ws1HubUtil: startEnrollment --
7 2023/07/21 04:57:12 E enrollCMD.go:101: EnrollCommand.processEnrollCommand: OpenEnrollment: readUsersCookie: not able to find valid AW-AgentSettings cookie
8 2023/07/21 04:57:12 E enrollCMD.go:93: EnrollCommand.Execute: OpenEnrollment: readUsersCookie: not able to find valid AW-AgentSettings cookie
9 2023/07/22 11:55:25 D enrollCMD.go:108: ws1HubUtil : startEnrollment ++
10 2023/07/22 11:55:25 D databaseUtil.go:173: Connection to db established.
11 2023/07/22 11:55:25 E agentSettings_dataInterface.go:26: getBeaconServer: dbHandler.Read: sql: no rows in result set
12 2023/07/22 11:55:25 E agentSettings_dataInterface.go:54: getBeaconEndPoint: getBeaconServer failed
13 2023/07/22 11:58:08 D enrollment.go:108: Enroll ++
14 2023/07/22 11:58:08 W genericData_dataInterface.go:92: getSerialNumber: dbHandler.Read: sql: no rows in result set
15 2023/07/22 11:58:08 D appPathConfig_dataInterface.go:106: GetOSQueryPath: exec: "/usr/local/bin/osqueryi": stat /usr/local/bin/osqueryi: no such file or directory
16 2023/07/22 11:58:08 E deviceInfo_dataInterface.go:136: datainterface.fetchSerialNumberUsingOSQuery: file: doesn't exist
17 2023/07/22 11:58:08 D ValidateDevice.go:172: registerBusiness: doValidateGroupIdentifier++
18 2023/07/22 11:58:08 D ValidateDevice.go:269: registerBusiness: postValidateDeviceRequest[ValidateGroupIdentifier] ++
19 2023/07/22 11:58:08 D ValidateDevice.go:280: postValidateDeviceRequest: request:

View Enrollment Log Files

[712]

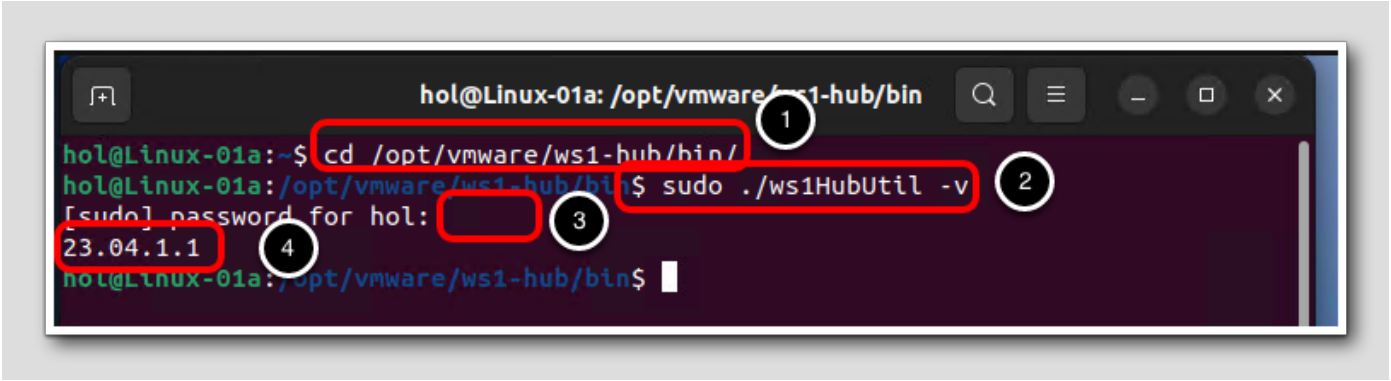
Using command line utilities

[713]

Use these command-line utilities to expedite the deployment of Workspace ONE Intelligent Hub on your Linux devices. The `ws1HubUtil` application is located at the agent binary directory under the installation directory: /opt/vmware/ws1-hub/bin.

The `ws1HubUtil` installed on the Linux device includes the following commands:

- Version
- Enroll
- Beacon
- Sample
- Sensor
- Service
- Upgrade
- Unenroll

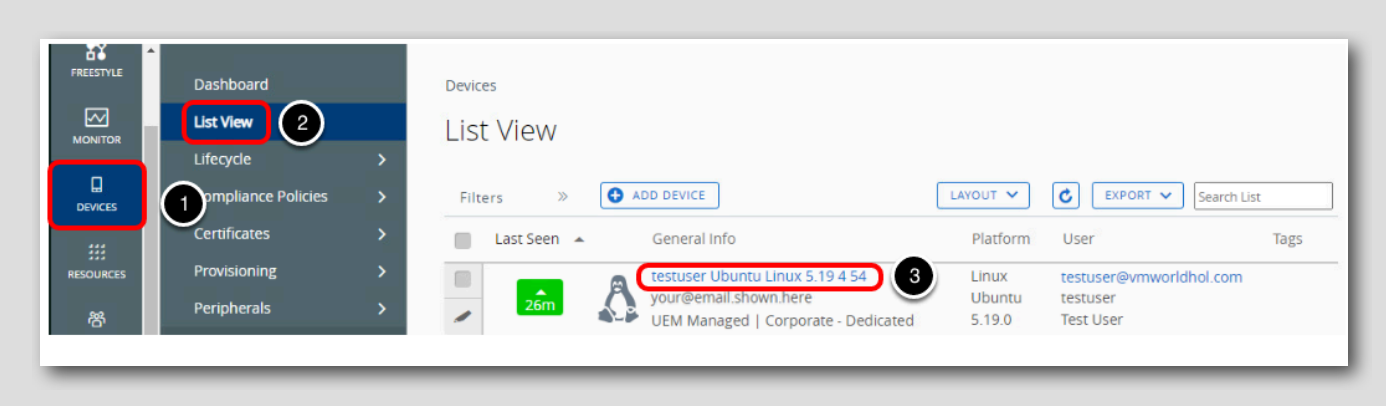


In the following example we will use ws1HubUtil to determine the version that is installed

1. Open terminal and change to the following directory `cd /opt/vmware/ws1-hub/bin` and press **Enter**
2. Type `sudo ./ws1HubUtil -v` and press **enter**
3. Enter `VMware1!` for hol user password and press **enter**
4. The Hub version that is installed is returned

Validate Enrollment on Linux Device [714]

Validate the Device Enrollment [715]

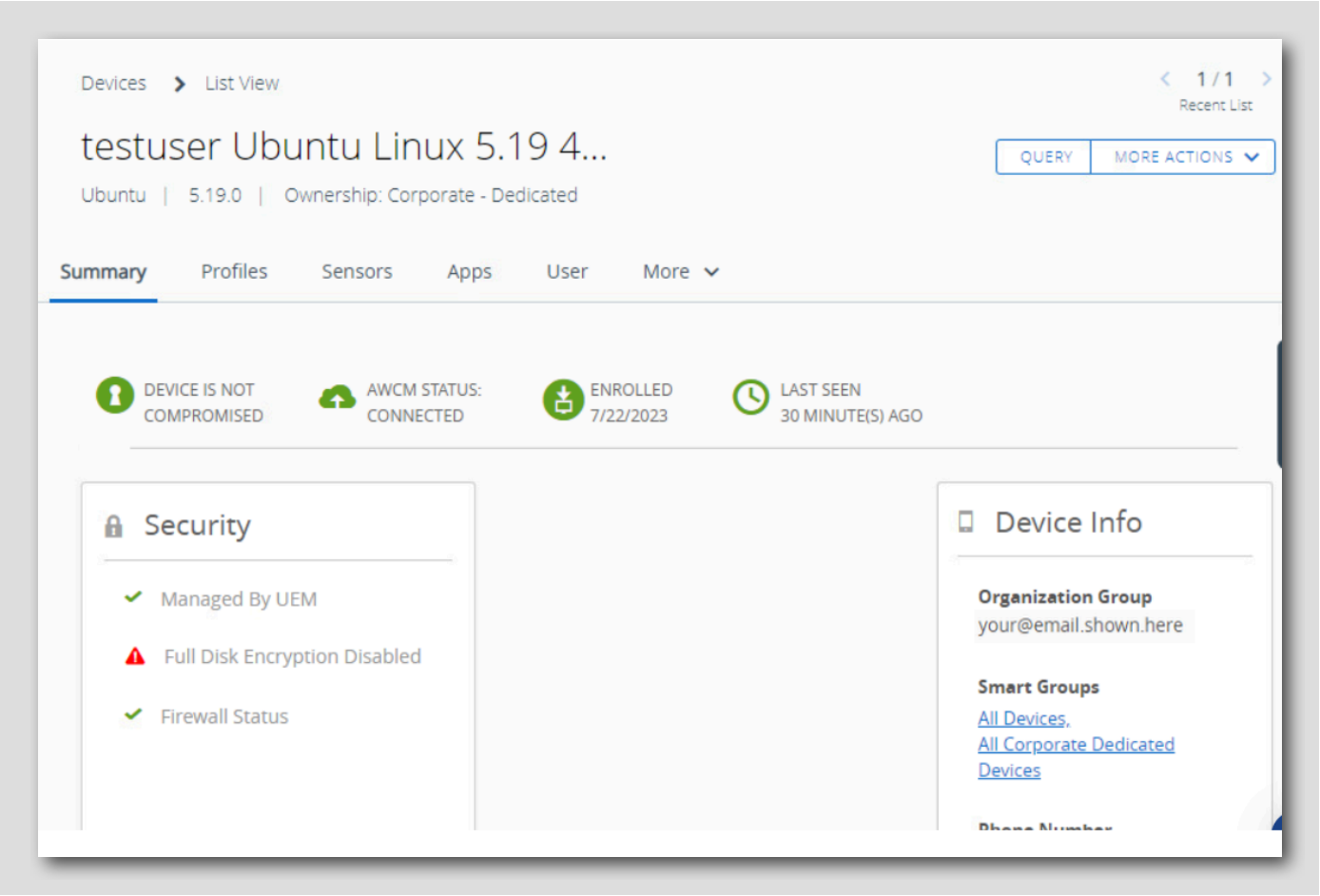


Return to the Workspace ONE UEM administrator console:

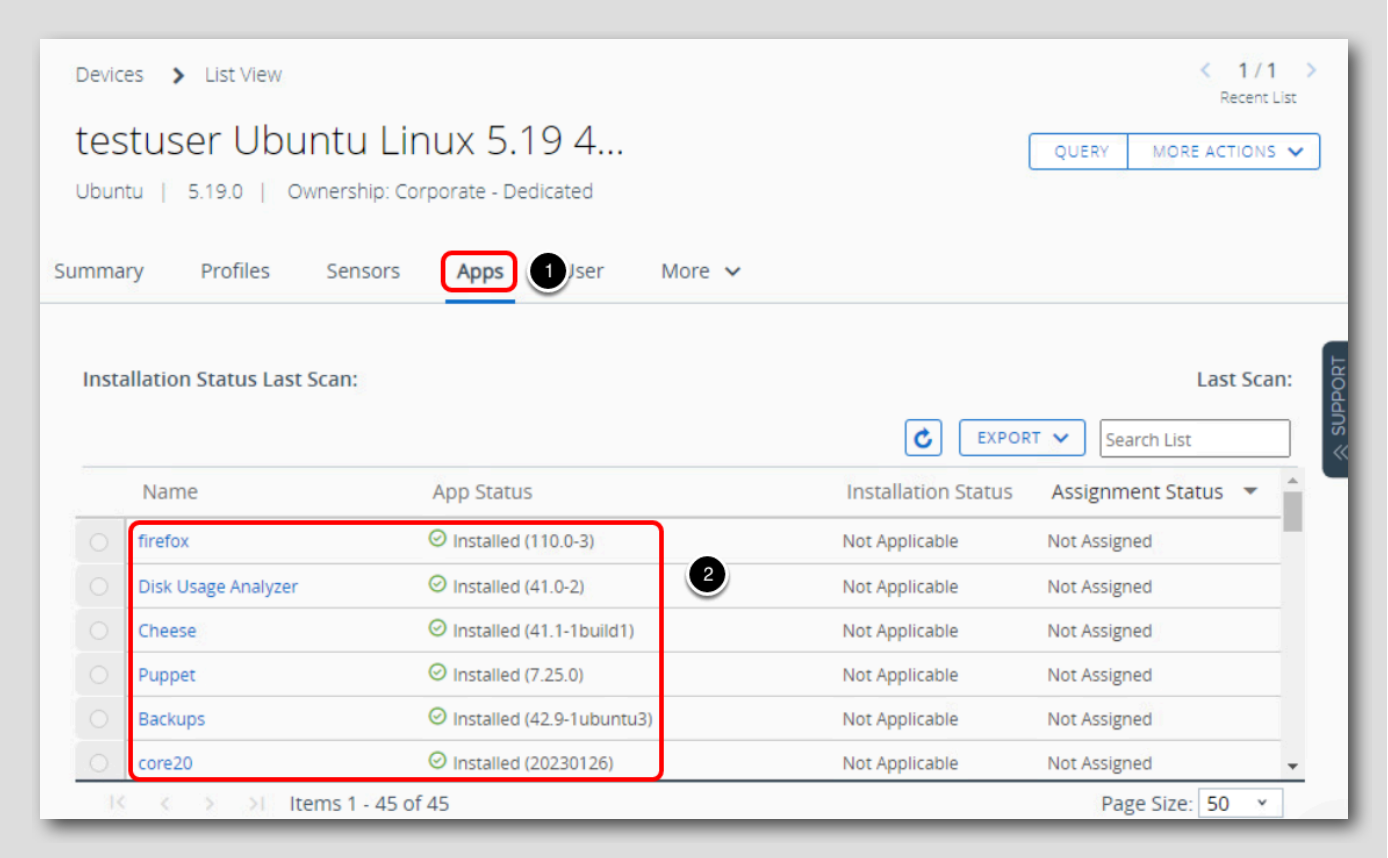
1. Click **Devices**
2. Click **List View**
3. Click the **enrolled Linux device** to view the Device Details page

View the Device Status

[716]



The Details View shows the device Security status, if the device is enrolled, the last time the device was seen and other information about the device.



1. Click Apps
2. Review inventory of installed applications and their versions.

Summary

[717]

In addition to managing mobile devices, Workspace ONE UEM can also manage your Linux devices. This quick look into Linux management should provide a clearer picture of how you can enroll and troubleshoot enrollment issues for your Linux devices.

This concludes the Introduction to Linux Management module.

For additional information on managing Linux devices with Workspace ONE UEM please refer to the following resources

Workspace ONE for Linux Endpint Management

Vmware Digital Workspace Tech Zone - Linux Management has Arrived!

Appendix

Hands-on Labs Interface (Windows Main Console)

[719]

Welcome to Hands-on Labs! This overview of the interface and features will help you to get started quickly. Click next in the manual to explore the Main Console or use the Table of Contents to return to the Lab Overview page or another module.

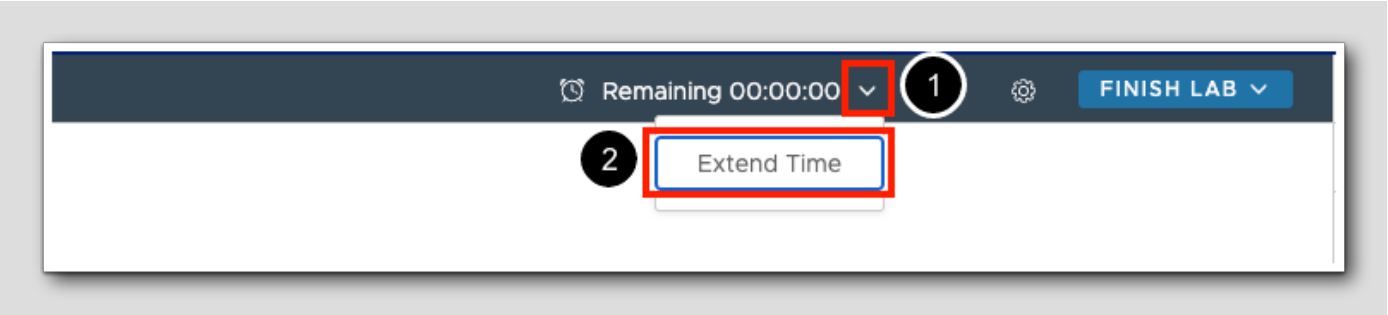
Location of the Main Console

[720]

1. The area in the large RED box contains the Main Console. The Lab Manual is on the tab to the right of the Main Console.

Extend Time

[721]



1. Your lab starts with a timer. The lab cannot be saved and will end when the timer expires. Click the drop down arrow next to the remaining time
2. Select **Extend Time**to increase the time allowed. The amount of time you can extend will depend on the lab.

Alternate Methods of Keyboard Data Entry

[722]

In this lab you will input text into the Main Console. Besides directly typing in the console, two alternate methods make it easier to enter complex data.

Click and Drag Lab Manual Content Into Console Active Window

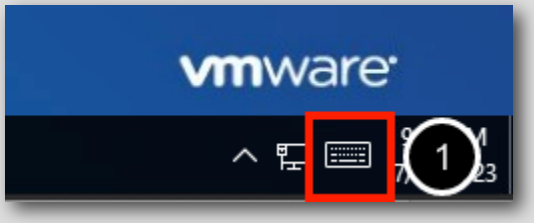
[723]

https://www.youtube.com/watch?v=xS07n6GzGuo

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

Accessing the Online International Keyboard

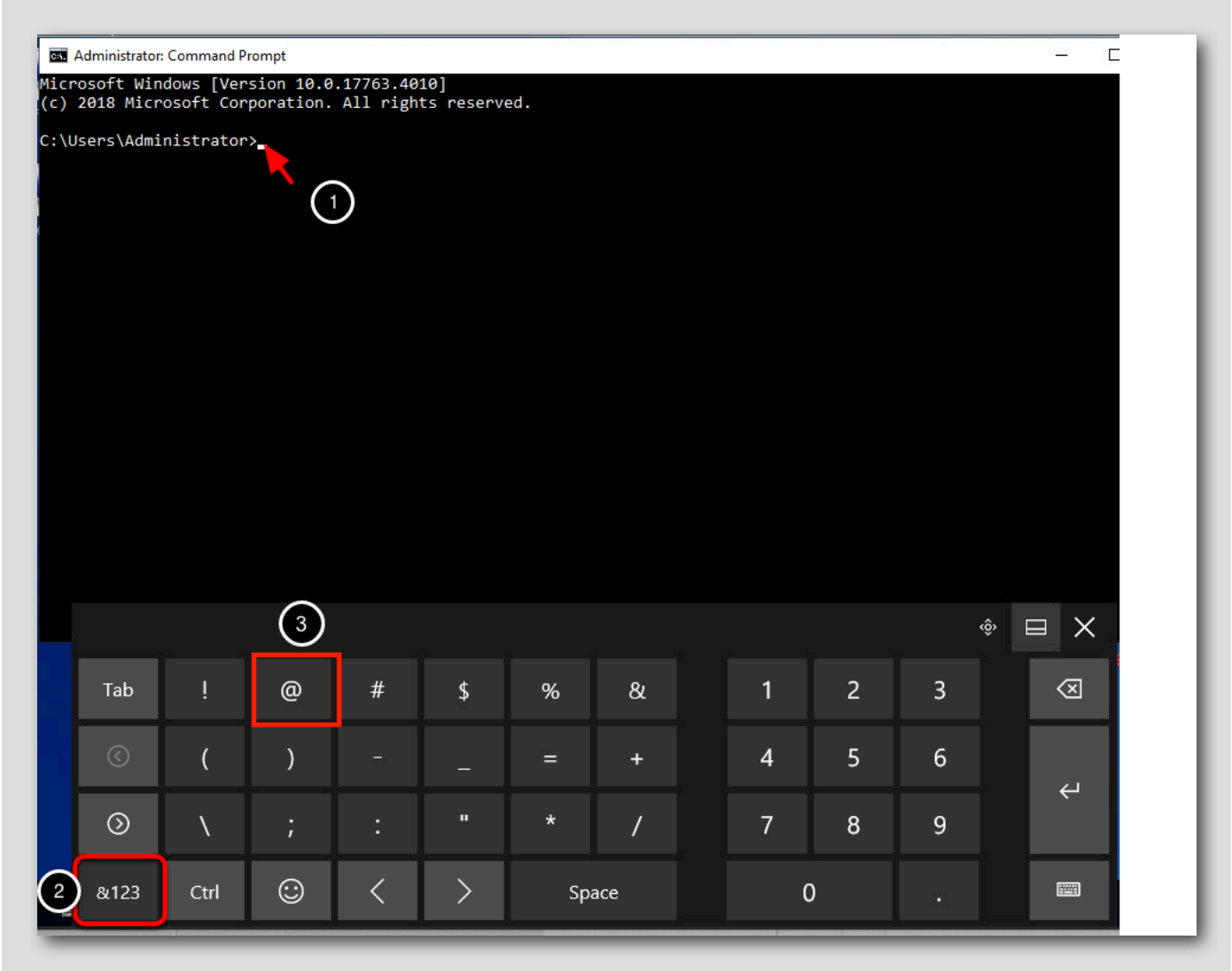
[724]



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

1. Click on the **keyboard icon** found on the Windows Quick Launch Task Bar.

Click once in active console window [725]



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

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

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