Managing Devices

VMware Workspace ONE UEM 1903

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Managing Devices

1

Manage devices in your fleet and perform functions on a particular set of devices using many different screens in the Workspace ONE UEM console.

You can examine the data flow with the **Monitor** and take a closer look at your fleet with **Device Dashboard**. You can group devices together and create customized lists with the **Device List View**.

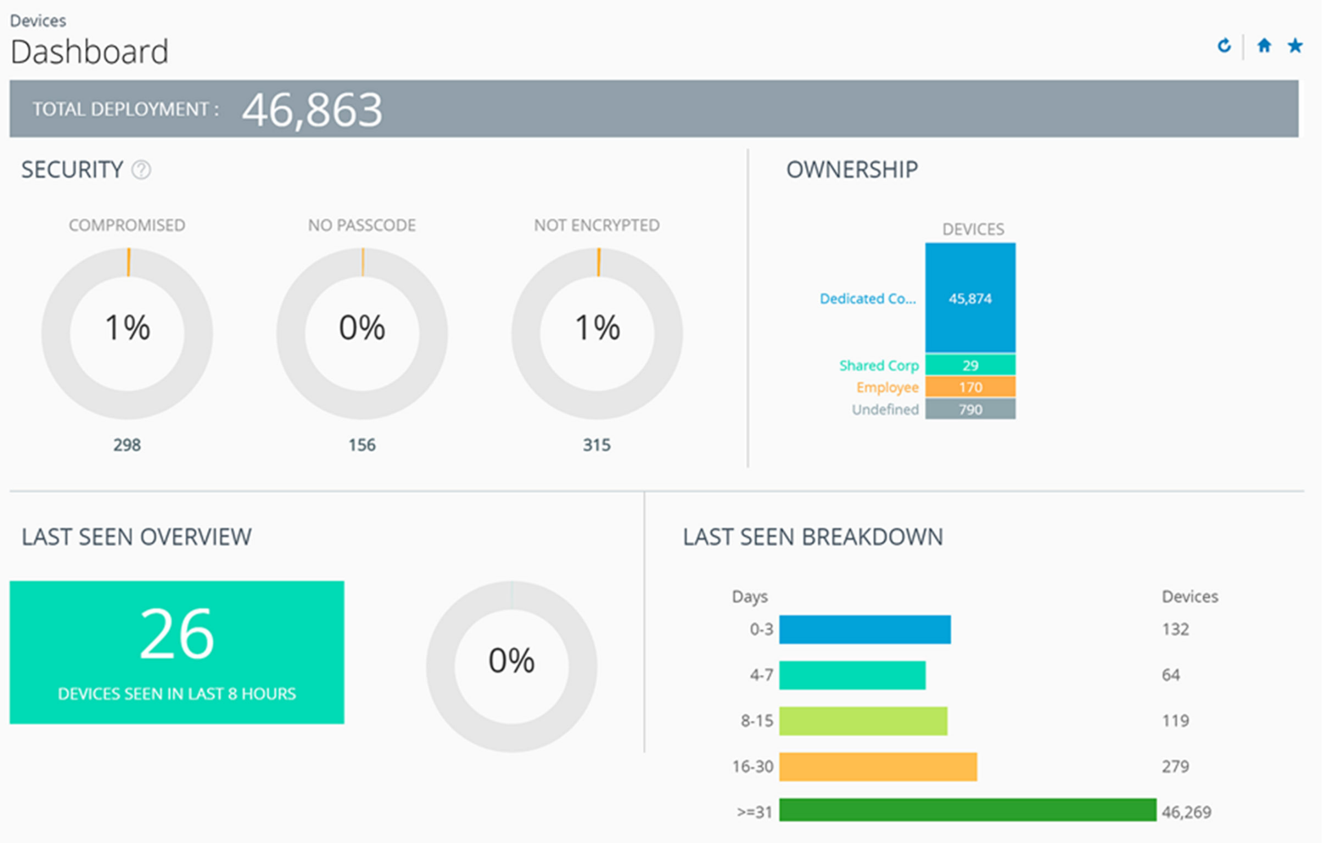
You can also generate **Reports** and use **Tags** to easily identify devices. You can even set up the **Self-Service Portal (SSP)** to enable end users to manage their own devices and reduce the strain on Help Desk personnel.

This chapter includes the following topics:

Device Dashboard

As devices are enrolled, you can manage them from the Workspace ONE UEM **Device Dashboard**.

The **Device Dashboard** provides a high-level view of your entire fleet and allows you to act on individual devices quickly.



You can view graphical representations of relevant device information for your fleet, such as device ownership type, compliance statistics, and platform and OS breakdowns. You can access each set of devices in the presented categories by selecting any of the available data views from the **Device Dashboard**.

From the **List View**, you can take administrative action: send messages, lock devices, delete devices, and change groups associated with the device.

- **Security** – View the top causes of security issues in your device fleet. Selecting any of the doughnut charts displays a filtered **Device List** view comprised of devices affected by the selected security issue. If supported by the platform, you can configure a compliance policy to act on these devices.
  - **Compromised** – The number and percentage of compromised devices (jailbroken or rooted) in your deployment.
  - **No Passcode** – The number and percentage of devices without a passcode configured for security.
  - **No Encryption** – The number and percentage of devices that are not encrypted for security. This reported figure excludes Android SD Card encryption. Only those Android devices lacking disc encryption are reported in the donut graph.

  Ownership – View the total number of devices in each ownership category. Selecting any of the bar graph segments displays a filtered **Device List** view comprised of devices affected by the selected ownership type.

- **Last Seen Overview/Breakdown** – View the number and percentage of devices that have recently communicated with the Workspace ONE UEM MDM server. For example, if several devices have not been seen in over 30 days, select the corresponding bar graph to display only those devices. You can then select all these filtered devices and send them a message requesting that they check in.
- **Platforms** – View the total number of devices in each device platform category. Selecting any of the graphs displays a filtered **Device List** view comprised of devices under the selected platform.
- **Enrollment** – View the total number of devices in each enrollment category. Selecting any of the graphs displays a filtered **Device List** view comprised of devices with the selected enrollment status.
- **Operating System Breakdown** – View devices in your fleet based on operating system. There are separate charts for Apple iOS, Android, Windows Phone, and Windows Rugged. Selecting any of the graphs displays a filtered **Device List** view comprised of devices running the selected OS version.

Device List View

Use the UEM console's Device List View to see a full listing of all devices in the currently selected organization group.

For information about a specific device, see the Device Details.

The **Last Seen** column displays an indicator showing the number of minutes elapsed since the device has checked-in. The indicator is red or green, depending on the number of minutes defined in **Device Inactivity Timeout (min)**. This indicator can be set by navigating to **Groups & Settings > All Settings > Devices & Users > General > Advanced**.

Select a device in the **General Info** column at any time to open the details page for that device.

Sort by columns and configure information filters to review device activity based on specific information. For example, sort by the **Compliance Status** column to view only devices that are currently out-of-compliance and target only those devices. Search all devices for a friendly name or user name to isolate one device or user.

Customize Device List View Layout

Display the full listing of visible columns in the **Device List** view by selecting the **Layout** button and select the **Custom** option. This view enables you to display or hide Device List columns per your preferences.

There is also an option to apply your customized column view to all administrators at or below the current organization group (OG). For instance, you can hide 'Asset Number' from the **Device List** views of the current OG and of all the OGs underneath.

Once all your customizations are complete, select the **Accept** button to save your column preferences and apply this new column view. You can return to the **Layout** button settings at any time to tweak your column display preferences.

Search in Device List View

You can search for a single device for quick access to its information and take remote action on the device.

To run a search, navigate to **Devices > List View**, select the **Search List** bar and enter a user name, device friendly name, or other device-identifying element. This action initiates a search across all devices, using your search parameter, within the current organization group and all child groups.

Hover-Over Pop-Up in Device List View

Each device in the **General Info** column features a tool tip icon in the shape of a folder located in the upper-right corner next to the device friendly name. When this icon is tapped (mobile touch device) or hovered-over with a mouse pointer (PC or Mac), it displays a Hover-Over pop-up. This pop-up screen contains information such as **Friendly Name**, **Organization Group**, **Group ID**, **Management**, and **Ownership**.

Similar tool tip icons are found in the **Enrollment** and **Compliance Status** columns in the Device List view. These tool tip icons feature Hover-Over Pop-Ups displaying **Enrollment Date** and **Compliance Violations** respectively.

Filtering Devices in List View

You can apply filters to view only the devices you are interested in. Select the **Filter** button to enable one or more of the following filters to view only those devices that fit the categories you select.

Setting	Description
Management	Display devices that have **App Level** management or devices managed by **Catalog**, **Container**, or **MDM**. Display devices managed by an **Unknown** method, are **Offline**, or **All** management methods.
Ownership	Display devices that have the ownership levels **Corporate - Dedicated**, **Corporate - Shared**, **Employee Owned**, or **Unassigned**. You can filter one or more ownership level at a time.
Smart Groups	Display devices that are part of the Smart Group that you choose. Click the **Search** text box and select from the list of Smart Groups that appear. Scroll down to view the alphabetical listing of Smart Groups.
User Groups	Display devices that are part of the User Groups that you choose. Click the **Search** text box and select from the list of User Groups that appear. Scroll down to view the alphabetical listing of User Groups.
Device Type	
Platform	Select from among the full listing of device platforms. You can filter more than one platform at a time.
OS Version	You must select at least one platform before you can select an OS version. When you select multiple platforms, a list of OS versions displays grouped by each selected platform.
Security	
Compromised	Select from among **Compromised**, **Not Compromised**, **Unknown**, or **All** of the above. A compromised device is a device that has been 'jailbroken' (for iOS devices) or 'rooted' (for Android devices).
Encryption	Select from among **Encrypted**, **Not Encrypted**, **Unknown**, or **All** of the above.
Passcode	Select from among **Passcode**, **No Passcode**, **Unknown**, or **All** passcode options.
Status	
Enrollment Status	Select from among **Enrolled**, **Enterprise Wipe Pending**, **Device Wipe Pending**, **Unenrolled**, or **All** of the above.

Setting	Description
Last Seen	Display devices based upon how long ago they checked in. Use the minimum and maximum text boxes in the **Last Seen (days)** option to display devices last seen within a range of days. Entered numbers are inclusive: an entry of 1 displays all devices last seen more than 1 day but less than 2 days ago. An entry of 2 displays all devices last seen more than 2 days but less than 3 days ago, and so on. An entry of zero displays devices last seen more than 0 days but less than 1 day (24 hours) ago. To display devices last seen more than (or equal to) the maximum entered number of days, leave the minimum text box blank. To display devices last seen less than (or equal to) the minimum entered number of days, leave the maximum text box blank.
Compliance	Select from among **Compliant**, **Non-Compliant**, **Pending Compliance Check**, **Not Available**, **Unknown**, or **All** of the above.
Enrollment History	Select enrollment dates from among **Past Day**, **Past Week**, **Past Month**, or **All** enrollment dates.
Advanced	
MAC Address	Filter by the media access control address of a device.
IP Range	Filter devices by their currently-assigned internet protocol address. Enter IP addresses in the **IP Range Start** and **IP Range End** text boxes to display devices that fall within that range. The current IP address can be one of many associated IP addresses of a device, most of which can be found on the Network tab of Device Details. Since a device can report multiple and different IP addresses, the IP address used in the filter may not always match the IP address shown on the Device List View grid.
Tags	View devices by their assigned tags for which you can search and select from a drop-down menu.
Tunnel	Select between showing all devices, showing devices connected to the tunnel, and devices not connected to the tunnel.
Content Compliance	Select between showing all devices, showing only those devices missing required docs, and only those devices lacking the latest version of required content.
Lost Mode	View all devices or only devices with Lost Mode enabled. Applicable to iOS devices only.

After selecting multiple filters, you can glance at the circled number badge to the right of the **Filters** button to see exactly how many filters are applied to produce the listing.

You can clear all selected filters and return to the full device listing by selecting the 'X' next to the **Filter** button.

Add a Device from List View

You can add or register a device including user assignment, custom attributes, and tagging.

Procedure

1 Navigate to **Devices > List View** or **Devices > Lifecycle > Enrollment Status**.

2 Select the **Add Device** button. The **Add Device** page displays. Complete the following in the **User** tab.

Setting	Description
User	
Search Text	Each device must be assigned to a user. Search for a user with this text box by entering search parameters and select the **Search User** button. You can select a user from among the search results or select the link **Create New User**.
Create New User	
Security Type	Select between **Basic** and **Directory** users. For more information, see Basic User Authentication and Active Directory with LDAP Authentication.
User name	Enter the user name by which your user is identified in your Workspace ONE UEM environment.
Password, **Confirm Password**	Enter and confirm the password that corresponds to the user name.
Email Address	Enter the email address for the user account.
Enrollment Organization Group	The organization group (OG) that serves as the enrollment OG for the device enrollment.
Show advanced user details	Display all the advanced user details, including comprehensive information covering user name, user phone number, and manager name. Also included are optional identification settings such as department, employee ID, and cost center. Select the default **User Role** for the user you are adding which determines which permissions the user has while using a connected device. For more information, see User Roles.
Device	
Expected Friendly Name	Enter the name of the device that appears in the device list view. You can also incorporate lookup values. For details, see Lookup Values.
Organization Group	Select the organization group from the drop-down menu with which the device is to be associated.
Ownership	Select the device ownership from the drop-down menu. Select between **None**, **Corporate - Dedicated**, **Corporate - Shared**, and **Employee-Owned**.
Platform	Select the platform of the device from the drop-down menu.
Show advanced deviceinformation options	Display all the advanced device information settings.
Advanced Device Information Settings	
Model	Select the device model from the drop-down listing. The contents of this drop-down menu depend upon the selection made in the **Platform** drop-down menu.
OS	Select the device's operating system from the drop-down listing. The contents of this drop-down menu depend upon the selection made in the **Platform** drop-down menu.
UDID	Enter the device's Unique Device Identifier.
Serial Number	Enter the device's serial number.
IMEI	Enter the device's 15-digit International Mobile Station Equipment Identity.
SIM	Enter the device's SIM card specifications.

Setting	Description
Asset Number	Enter the asset number for the device. This number is created internally from within your organization and this setting is provided to hold this data point.
Messaging	
Message Type	Select the type of message you want to send (**None**, **SMS**, or **Email**) to the device upon a successful enrollment to the Workspace ONE UEM environment.
Email Address	Enter the email address to which you want the enrollment message sent. This text box is only available when Email is selected as the **Message Type**.
Email Message Template	Select the email template from the drop-down menu. There is a link you can use to open the Message Template page where you can create an email message template.
Phone Number	Enter the phone number to which you want the SMS text message sent. This text box is only available when SMS is selected as the **Message Type**.
SMS Message Template	Select the SMS template from the drop-down menu. There is a link you can use to open the Message Template page where you can create an SMS message template.

3. (Optional) Assign **Custom Attributes** to the device. Select the **Add** button and supply an **Attribute** and its **Value**.
4. (Optional) Assign **Tags** to the device. Select the **Add** button and select a tag from the drop-down menu for each tag you want to assign.
5. Select **Save**.

Unenrolled Devices

Unenrolled devices can be viewed in the Workspace ONE UEM console provided they were registered or held an enrolled status in the past. You can also get access to troubleshooting logs made before a device's unenrollment from the UEM console.

Unenrolled Status

An unenrolled device is a device in one of three possible scenarios.

1. The device is new to Workspace ONE UEM and is not registered, not enrolled, and therefore not managed. A device in this scenario cannot be seen in the UEM console.
2. The new device has begun the Workspace ONE enrollment process and is registered with the UEM console but not yet fully enrolled. This scenario normally occurs during a wave of new enrollments where devices are registered as a way of restricting enrollment. The mechanism that allows registered devices to enroll is a device whitelist. A device in this state can be seen by the UEM console with the status 'unenrolled'. Given that a registered device is traditionally a part of the enrollment process, a device does not remain in this scenario for long.
3. The device was fully enrolled in the Workspace ONE UEM console at one time but it was deleted from the UEM console. This action removes it from all device management functions and features. In this scenario, the device is still registered with the UEM console and remains on the whitelist. The device can also be seen by the UEM console with the status 'unenrolled' and therefore can be re-enrolled easily. A device can remain in this scenario indefinitely.

You can retain up to approximately 150,000 devices on this whitelist. Contact support if your needs exceed this amount.

You can remove the registration record of any whitelisted device at any time, which makes the device unseen and unknown by the UEM console (scenario 1 preceding). A device in this scenario can be enrolled at a future date.

Alternately, you can remove the device from the whitelist and add the device to a blacklist, preventing future enrollment and effectively banning the device from your fleet.

Access Troubleshooting Logs Made Before Unenrollment

You can access Troubleshooting/Commands logs made before the device was unenrolled. These logs can be useful to get a full picture of the device's history. Take the following steps to view the Troubleshooting/Commands logs.

Procedure

1. Navigate to **Devices > List View**.
2. Select a device you know to have been unenrolled in the past.

   You can optionally **Filter** the list view to show only devices with a **Status** of **Unenrolled**.

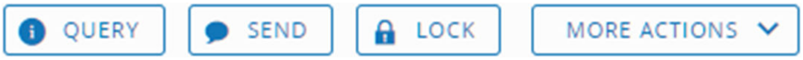
   When you select a device, the **Details View** displays.
3. Select the **More** tab drop-down, then select **Troubleshooting**, followed by the **Commands** tab.

What to do next

If you do not intend to re-enroll a previously unenrolled device to the same customer organization group again, consider deleting the device record permanently so the device history is clear upon re-enrollment. Contact Workspace ONE Support to make this arrangement.

Bulk Actions in Device List View

Once you filter a subset of devices, you can perform bulk actions to multiple devices by selecting devices and then selecting from the action button cluster.



For more information, see Selecting Devices in Device List View.

Bulk actions are only available in the Device List View if they are enabled in the system settings (**Groups & Settings > All Settings > System > Security > Restricted Actions**). Password Protect Actions require a PIN to perform.

With devices selected in the **List View**, the number of devices selected is displayed next to the action buttons. This number includes filtered devices that are selected as well.

Bulk Management Limit in Device List View

You can set a maximum number of devices that can receive a bulk action command to ensure smooth operations when managing a large device fleet.

Change these limits by navigating to **Groups & Settings > All Settings > Devices & Users > Advanced > Bulk Management**.

When a bulk management limit is in place and multiple devices are selected, a link appears next to the 'number of items selected' message which reads: **Some actions disabled due to bulk limits**.

Queued Bulk Action Warning in Device List View

Bulk actions take time to process. When you initiate a new bulk action while the Workspace ONE ™ UEM console is processing an existing bulk action, a warning message displays.

```
Your previous bulk actions requested are still being processed. This request is run once the previous
actions are complete. Do you want to continue with the current request?
```

Select **Yes** to add the new bulk action to the queue. Select **No** to cancel the new bulk action.

Selecting Devices in Device List View

You can select individual devices on a page by ticking individual check boxes to the left of each device. You can also select a block of devices across multiple pages. You can even select all devices in your entire fleet, which might trigger the restricted actions warning.

Selecting a Block of Devices

You can select a contiguous block of devices, even across multiple pages, by selecting the device check box at the beginning of the block. Next, hold down the shift key, then select the device check box at the end of the block. This action is similar to the block-selection in the Windows and Mac environments and it allows you to apply bulk actions to those selected devices.

Selecting All Devices

The Global check box, located to the left of the **Last Seen** column header, can be used to select or deselect all devices in the listing. If your **List View** contains a filtered listing of devices, the Global check box can be used to select or deselect all filtered devices.

When the Global check box features a green minus sign (⊟), it means at least one but not all devices are selected. Select this icon again and it changes to a check mark sign (☑), indicating that all devices in the listing (either filtered or unfiltered) have been selected. Select it a third time and it changes again to an empty check box (☐), indicating that no devices in the listing are currently selected.

Restricted Action Warning on All Devices Selected

When you initiate an action with all devices in your fleet selected, a warning message is displayed.

You are attempting to act on [number of selected] devices. This action may not apply to all devices. Certain limitations of this action include enrollment status, management type, device platform, model, or OS.

This warning is an acknowledgment of the diverse nature of a large device fleet featuring a multitude of different manufacturers, operating systems, and capabilities. It is unrelated to the **Bulk Management Limit** and any warnings it might generate. If you have a **Bulk Management Limit** in place, then this **Restricted Action Warning** message does not display.

Device Details

Use the Device Details page to track detailed information for a single device and to access user and device management actions quickly.

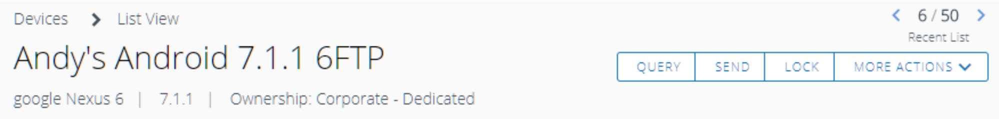
Access Device Details by selecting a device friendly name from one of the available Dashboards, or by using the available search tools in the Workspace ONE UEM console.

The main page features several major sections.

- **Notification Badges** – Displays the Compromised State, Compliance Violations, Enrollment Date, time Last Seen for the selected device, and GPS/Location Service Availability (for Android devices only).
- **Security** – Displays security settings such as which management software is being used, passcode status, and data protections.
- **User Info** – Displays basic user information including full name and email.
- **Device Info** – Displays device details such as organization group, location, smart groups, serial number, UDID, asset number, power status including battery health (for Zebra Android devices only), storage capacity, physical memory, and warranty information.
- **Profiles** – Displays all profiles such as installed (active), assigned (inactive), and unmanaged (sideloaded).
- **Apps** – Displays all installed apps, both automatic apps and on-demand apps.
- **Content** – Displays content marked as 'Required' by the administrator in the Workspace ONE UEM Managed Repository as well as in the admin repository.
- **Certifications** – Displays all installed certificates, including certifications near their expiration date.
- **Admin Applications** – Displays the installed Workspace ONE Intelligent Hub information including version number.
- **Zebra Battery Information** (for Zebra Android devices only) – Displays detailed battery information including battery health, manufacture date, serial number, and part number.

Device Details Dashboard

The dashboard displays basic device information such as the device type, device model, OS version number, ownership type, device action button cluster, and Recent List indicator.

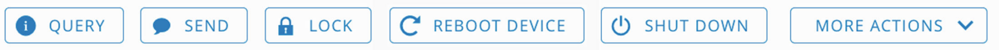


Andy's Android 7.1.1 6FTP

google Nexus 6 | 7.1.1 | Ownership: Corporate - Dedicated

Selecting the arrow buttons in the **Recent List** indicator changes the selected device based on its position in the filtered **List View**.

Device Details Action Button Cluster



Perform common device actions with the action button cluster including Query, Send [Message], Lock, and other actions accessed through the **More Actions** button.

Available Device Actions vary by platform, device manufacturer and model, and enrollment status, and the specific configuration of your Workspace ONE UEM console. For a full listing of remote actions an admin can invoke using the console, see Device Actions by Platform.

Device Details Menu Tabs

You can use the **Menu Tabs** to access specific device information, which varies depending on the selected device platform.

Menu Tab	Description
Summary	View general statistics such as enrollment status, compliance, last seen, GPS availability, platform/model/OS, organization group, serial number, power status, storage capacity, physical memory, and virtual memory.
Compliance	Display the status, policy name, date of the previous and forthcoming compliance check and the actions already taken on the device. The **Compliance** tab includes advanced troubleshooting and convenience features. ■ Non-Compliant devices, and devices in pending compliance status, have troubleshooting functions available. You can reevaluate compliance on a per-device basis (⇄) or get detailed information about the compliance status on the device (i). ■ Users with Read-Only privileges can view the specific compliance policy directly from the **Compliance** tab while Administrators can make edits to the compliance policy.
Profiles	View all profiles currently assigned, installed, and unmanaged on a device.
Apps	View all apps currently assigned and installed on the device. The **App Compliance** column identifies SDK-built applications that are non-compliant with SDK App Compliance settings. Find these settings in **Groups & Settings > All Settings > Settings and Policies > SDK App Compliance**.
Content	View the status, type, name, version, priority, deployment, last update, date, time of views, and content on the device marked 'Required' by the administrator in the Workspace ONE UEM Managed Repository. This tab also provides a toolbar for administrative action (install or delete).
Location	View current location or location history of a device. Select the **Period** or length of time you are looking back in **Search** of location data points. The Custom Period enables you to select a range of dates and times in 5-minute increments. You can also review latitude and longitude coordinates of these data points by moving the pointer over location markers on the map. Enable the collection of location data by navigating to **Groups & Settings > All Settings > Devices & Users** and selecting the platform-specific **Hub Settings** page. For more information about location data as it relates to privacy, see GPS Coordinates for Privacy Best Practices. Edit the number of location data points collected and the minimum distance between locations by navigating to **Groups & Settings > All Settings > Installation > Maps**.
User	Access details about the user of a device and the status of the other devices enrolled to this user.

Menu Tab	Description
More	These additional menu tabs vary based on the device platform. ■ **Network** – View current network information (Cellular, Wi-Fi, Bluetooth, IMEI) of a device. ■ **Security** – View current security status of a device based on security settings. ■ **Telecom** – View amounts of calls, data, and messages sent and received. ■ **Notes** – View and add notes regarding the device. For example, note the shipping status or if the device is in repair and out of commission. ■ **Certificates** – Identify device certificates by name and issuant. This tab also provides certificate expiration dates. ■ **Products** – View complete history and status of all product packages provisioned to the device and any provisioning errors. You can also Force Reprocess (redeploy) a product. ■ **Terms of Use** – View a list of End-User License Agreements (EULAs) which have been accepted during enrollment.
More,cont.	■ **Alerts** – View all alerts associated with the device. ■ **Shared Device Log** – View the history of the shared device including past check-ins and check-outs and status. ■ **Status History** – View history of device in relation to enrollment status. ■ **Targeted Logging** – View the logs for the Console, Catalog, Device Services, Device Management, and Self Service Portal. You must enable Targeted Logging in settings and a link is provided for this purpose. You must then select the **Create New Log** button and select a length of time the log is collected. ■ **Troubleshooting** – View **Event Log** and **Commands** logging information. This page features export and search functions, enabling you to perform targets searches and analysis. ■ **Event Log** – View detailed debug information and server check-ins, including a **Filter** by **Event Group Type**, **Date Range**, **Severity**, **Module**, and **Category**. In the **Event Log** listing, the **Event Data** column may display hypertext links that open a separate screen with even more detail surrounding the specific event. This information enables you to perform advanced troubleshooting such as determining why a profile fails to install. ■ **Commands** – View detailed listing of pending, queued, and completed commands sent to the device. Includes a **Filter** enabling you to filter commands by **Category**, **Status**, and specific **Command**. ■ **Attachments** – Use this storage space on the server for screenshots, documents, and links for troubleshooting and other purposes without taking up space on the device itself.

Device Actions by Platform

As a Workspace ONE UEM administrator, you can run commands remotely to individual (or bulk) devices in your fleet and different platforms offer different actions. Each of these platform-specific device actions and definitions represents remote commands an admin can invoke from the UEM console.

For more information, see Device Action Descriptions.

Action	Android	Apple iOS	Apple macOS	Apple TV	Chrome OS	QNX	Windows Rugged	Win 7	Windows Phone	Windows Desktop
Add Tag	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Workspace ONE Intelligent Hub (Query)	✓	✓						✓ (*)		
App Remote View	✓	✓					✓			

Action	Android	Apple iOS	Apple macOS	Apple TV	Chrome OS	QNX	Windows Rugged	Win 7	Windows Phone	Windows Desktop
Apps (Query)		✓	✓				✓	✓ (*)	✓	✓
Books (Query)		✓								
Cancel Log Request	✓									
Certificates (Query)		✓	✓	✓			✓	✓ (*)	✓	✓
Change Device Passcode	✓								✓	✓
Change Organization Group	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Change Ownership	✓	✓	✓	✓	✓	✓	✓	✓		✓
Clear Activation Lock		✓								
Clear Passcode (Device)	✓	✓					✓		✓	
Clear Passcode (Container)	✓									
Clear Passcode (Restrictions Setting)		✓								
Delete Device	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Device Information (Query)	✓	✓	✓	✓	✓		✓	✓ (*)	✓	✓
Device Wipe	✓	✓	✓	✓			✓		✓	✓
Edit Device	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Enable/Disable Lost Mode		✓								
Enroll	✓	✓	✓	✓					✓	✓
Enterprise Reset	✓						✓			
Enterprise Wipe	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
File Manager	✓						✓			
Find Device	✓	✓							✓	
iOS Update		✓								
Location	✓	✓	✓		✓		✓			✓
Lock Device	✓	✓	✓					✓	✓	✓
Lock SSO	✓	✓								

Action	Android	Apple iOS	Apple macOS	Apple TV	Chrome OS	QNX	Windows Rugged	Win 7	Windows Phone	Windows Desktop
Managed Settings		✓	✓							
Mark Do Not Disturb	✓	✓								
Override Job Log Level	✓									
Profiles (Query)		✓	✓	✓	✓			✓ (*)		
Provision Now						✓	✓			
Query All	✓	✓	✓	✓	✓		✓	✓	✓	✓
Reboot Device	✓									
Registry Manager							✓			
Remote Control	✓				✓		✓			
Remote Management	✓		✓			✓	✓	✓		✓
Remote View		✓								
Rename Device									✓	
Request Debug Log	✓									
Request Device Check-In		✓		✓	✓		✓			
Request Device Location		✓								
Restart Workspace ONE Intelligent Hub							✓			
Security (Query)		✓	✓	✓				✓ (*)	✓	✓
Send Message	✓	✓	✓		✓	✓	✓	✓	✓	✓
Start AirPlay		✓	✓							
Start AWCM	✓						✓			
Stop AWCM	✓						✓			
Sync Device	✓	✓		✓						
Task Manager							✓			
View Manifest							✓			
Warm Boot						✓	✓			

(*) This Windows 7 action is satisfied by running a Query All command, which returns all the same information as if each Query command were run separately.

Device Action Descriptions

View a detailed description of each action that can be run on a device, remotely from the console.

- **Add Tag** – Assign a customizable tag to a device, which can be used to identify a special device in your fleet.
- **Workspace ONE Intelligent Hub Query** – Send a query command to theWorkspace ONE Intelligent Hub on the device to ensure it has been installed and is functioning normally.
- **App Remote View** – Take a series of screenshots of an installed application and send them to the Remote View screen in the UEM console. You may choose the number of screenshots and the length of the gap, in seconds, between the screenshots.

Android and iOS devices require VMware Content Locker to be installed on the device to execute **App Remote View**.

- **Apps (Query)** – Send an MDM query command to the device to return a list of installed apps.
- **Books (Query)** – Send a query command to the device to return a list of installed books.
- **Certificates (Query)** – Send an MDM query command to the device to return a list of installed certificates.
- **Change Device Passcode** – Replace any existing device passcode used to access the selected device with a new passcode.
- **Change Organization Group** – Change the device's home organization group to another pre-existing OG. Includes an option to select a static or dynamic OG.
- **Change Ownership** – Change the Ownership setting for a device, where applicable. Choices include Corporate-Dedicated, Corporate-Shared, Employee Owned and Undefined.
- **Clear Activation Lock** – Clear the Activation Lock on an iOS device. With the Activation Lock enabled, the user requires an Apple ID and password prior to taking the following actions: disabling Find My iPhone, factory wipe, and reactivate to use the device.
- **Clear Passcode (Container)** – Clear the container-specific passcode. To be used in situations where the user has forgotten their device's container passcode.
- **Clear Passcode (Device)** – Clear the device passcode. To be used in situations where the user has forgotten their device's passcode.
- **Clear Passcode (Restrictions Setting)** – Clear the passcode that restricts device features such as app installation, Safari use, camera use and more.
- **Delete Device** – Delete and unenroll a device from the console. Sends the enterprise wipe command to the device that gets wiped on the next check-in and marks the device as **Delete In Progress** on the console. If the wipe protection is turned off on the device, the issued command immediately performs an enterprise wipe and removes the device representation in the console.
- **Device Information (Query)** – Send an MDM query command to the device to return basic information on the device such as friendly name, platform, model, organization group, operating system version and ownership status.
- **Device Wipe** – Send an MDM command to wipe a device clear of all data and operating system. This puts the device in a state where recovery partition will be needed to reinstall the OS. This action cannot be undone.
  - iOS Device Wipe Considerations
    - For iOS 11 and below devices, the device wipe command would also wipe the Apple SIM data associated with the devices.
    - For iOS 11+ devices, you have the option to preserve the Apple SIM data plan (if existed on the devices). To do this, select the **Preserve Data Plan** checkbox on the Device Wipe page before sending the device wipe command.

  - For iOS 11.3+ devices, you have an additional option to enable or disable to skip the **Proximity Setup** screen while sending down the device wipe command. When the option is enabled, the Proximity Setup screen will be skipped in the Setup Assistant and thus preventing the device user from seeing the Proximity Setup option.

- For Windows Desktop Devices, you can choose the type of device wipe.
  - **Wipe** - This option wipes the device of all content.
  - **Wipe Protected** - This option is similar a normal device wipe, but this option cannot be circumvented by the user. The Wipe Protected command keeps trying to reset the device until it is successful. In some device configurations, this command can leave the device unable to boot.

    - **Wipe and Persist Provisioning Data** - This option wipes the device but specifies that provisioning data should be backed up to a persistent location. After the wipe executes, the provisioning data is restored and applied to the device. The provisioning folder is saved. You can find the folder by navigating on the device to `%ProgramData%\Microsoft\Provisioning` .

- **Edit Device** – Edit device information such as **Friendly Name**, **Asset Number**, **Device Ownership**, **Device Group** and **Device Category**.
- **Enable/Disable Lost Mode** – Use this to lock a device and send a message, phone number or text to the lock screen. Lost Mode cannot be disabled by the user. When Lost Mode is disabled by an administrator, the device returns to normal functionality. Users are sent a message that tells them that the location of the device was shared. (iOS 9.3 + Supervised)
  - **Request Device Location** – Query a device when in Lost Mode and then use the Location tab to find the device. (iOS 9.3 + Supervised)
- **Enroll** – Send a message to the device user to enroll their device. You may optionally use a message template that may include enrollment information such as step-by-step instructions and helpful links. This action is only available on unenrolled devices.
- **Enterprise Reset** – Enterprise Reset a device to factory settings, keeping only the Workspace ONE UEM enrollment.
- **Enterprise Wipe** – Enterprise Wipe a device to unenroll and remove all managed enterprise resources including applications and profiles. This action cannot be undone and re-enrollment will be required for Workspace ONE UEM to manage this device again. Includes options to prevent future re-enrollment and a **Note Description** field for you to add any noteworthy details about the action.
  - Enterprise Wipe is not supported for cloud domain-joined devices.
- **File Manager** – Launch a File Manager within the UEM console that enables you to remotely view a device's content, add folders, conduct searches and upload files.
- **Find Device** – Send a text message to the applicable Workspace ONE UEM application together with an audible sound (with options to repeat the sound a configurable number of times and the length of the gap, in seconds, between sounds). This audible sound should help the user locate a misplaced device.
- **iOS Update** – Push an operating system update to one or more iOS devices. Applicable only to supervised, DEP-enrolled devices with iOS version 9 or greater.
- **Location** – Reveal a device's location by showing it on a map using its GPS capability enabled via the macOS Workspace ONE Intelligent Hub. Also requires user approval to enable the functionality in macOS System Preferences.
- **Lock Device** – Send an MDM command to lock a selected device, rendering it unusable until it is unlocked.
- **Lock SSO** – Lock the device user out of Workspace ONE UEM Container and all participating apps.
- **Managed Settings** – Enable or disable voice roaming, data roaming, and personal hotspots.

- **Mark Do Not Disturb** – Mark the device not to be disturbed, preventing it from receiving messages, emails, profiles, and any other type of incoming interaction. Only those devices that are actively Marked Do Not Disturb have the action **Clear Do Not Disturb** available, which removes the restrictions.
- **Override Job Log Level** – Override the currently-specified level of job event logging on the selected device. This action sets the logging verbosity of Jobs pushed through Product Provisioning and overrides the current log level configured in Android Hub Settings. Job Log Level Override can be cleared by selecting the drop-down menu item **Reset to Default** on the action screen, or by changing the Job Log Level under the Product Provisioning category in Android Hub Settings.
- **Profiles (Query)** – Send an MDM query command to the device to return a list of installed device profiles.
- **Provision Now** – Provision products to a device. Provisioning is the ability to create an ordered installation of files, actions, profiles and applications into a single product that can be pushed to devices.
- **Query All** – Send a query command to the device to return a list of installed apps (including Workspace ONE Intelligent Hub, where applicable), books, certificates, device information, profiles and security measures.
- **Reboot Device** – Reboot a device remotely, reproducing the effect of powering it off and on again.
- **Registry Manager** – Launch a Registry Manager within the UEM console that enables you to remotely view a device's OS registry, add keys, conduct searches and add properties.
- **Remote Control** – Take control of a supported device remotely using this action, which launches a console application that enables you to perform support and troubleshooting on the device. Android devices require Remote Control Service to be installed on the device.
- **Remote Management** – Take control of a supported device remotely using this action, which launches a console application that enables you to perform support and troubleshoot on the device. Android devices require Remote Control Service to be installed on the device.
- **Remote View** – Enable an active stream of the device's output to a destination of your choosing (including IP address, port, audio port, password and scan time), allowing you to see what the user sees as they operate the device.
- **Rename Device** – Change the device friendly name within the UEM console.
- **Request Device Log** – Request the debug log on the selected device, after which you may view the log by selecting the **More** tab and choosing **Attachments > Documents**. You cannot view the log within the Workspace ONE UEM consoleThe log is delivered as a ZIP file that can be used to troubleshoot and provide support.

When you request a log you can choose to receive the logs from the **System** or the **Hub**. **System** provides system-level logs. **Hub** provides logs from the multiple agents running on the device.

- **Request Device Check-In** – Request that the selected device check itself in to the UEM console. This action updates the **Last Seen** column status.
- **Restart Workspace ONE Intelligent Hub** – Restart the Workspace ONE Intelligent Hub. To be used during troubleshooting for when the enrollment process or submodule installation process is interrupted.
- **Security (Query)** – Send an MDM query command to the device to return the list of active security measures (device manager, encryption, passcode, certificates, etc.).
- **Send Message** – Send a message to the user of the selected device. Choose between **Email**, **Push Notification** (through AirWatch Cloud Messaging), and **SMS**.
- **Start AirPlay** – Stream audiovisual content from the device to an AirPlay mirror destination. The MAC address (format "xx:xx:xx:xx:xx:xx" with no case-sensitive) of the destination is required. A passcode can also be specified if required. Scan Time defines the number of seconds (10-300) to spend searching for the destination. Requires macOS 10.10 or greater.
- **Start/Stop AWCM** – Start/Stop the Cloud Messaging service for the selected device. VMware AirWatch Cloud Messaging (AWCM) streamlines the delivery of messages and commands from the Admin Console by eliminating the need for end users to access the public Internet or utilize consumer accounts, such as Google IDs.
- **Sync Device** – Synchronize the selected device with the UEM console, aligning its **Last Seen** status.
- **Task Manager** – Launch a Task Manager within the UEM console that enables you to remotely view a device's currently-running tasks, including task **Name**, **Process ID** and applicable **Actions** you may take.
- **View Manifest** – View the device's **Package Manifest** in XML format from the UEM console. The manifest on Windows Rugged devices lists metadata for widgets and apps.
- **Warm Boot** – Initiate a restart of the operating system without performing a power-on self-test (POST).

Enrollment Status

Use the **Enrollment Status** page to assess enrollment status on a per-device basis, import and register devices in bulk, whitelist/blacklist devices, and revoke/reset device tokens.

Select **Devices > Lifecycle > Enrollment Status** to see a full list of all devices by enrollment status in the currently selected organization group.

Sort by columns and configure information filters to review device activity based on specific information. For example, sort by the **Token Status** column to view only devices whose registration is not applicable and act only on those specific devices. Search all devices for a friendly name or user name to isolate one device or user.

Setting	Description
Filters	You can filter out entire device categories by using filters which enable you to see only those devices that you are interested in. ■ **Enrollment Status** ■ **Platform** ■ **Ownership** ■ **Token Status** ■ **Token Type** ■ **Source** ■ **First Seen**
Add	■ **Register Device** – You can register or **Add** a single device to be enrolled. ■ **Whitelist or Blacklist Devices** – You can allow only those devices to enroll that you have identified or whitelisted. Alternatively, you can restrict devices from an enrollment by blacklisting devices. ■ **Batch Import** – Import multiple devices or multiple users with the Batch Import screen. For more information, see Add a Device from List View, Add a Blacklisted or Whitelisted Device, and Batch Import Users or Devices.
Resend Message	Resend the original message sent to a user, including Self-Service Portal URL, Group ID, and login credentials.
More Actions	
Change Organization Group	Move the selected device to the organization group of your choosing.
Change Ownership	Change the type of ownership for the selected device.
Delete	Permanently delete the registration information for selected devices. This action forces the user to re-register to enroll. Where applicable, you must first revoke the token before deleting a device registration.
Reset Token	Reset the status of a token if it has been revoked or is expired.
Revoke Token	Force the registration token status of selected devices to expire, essentially blocking access for unwanted users or devices. For the **Reset Token** and **Revoke Token** actions, you can select to disable the **Notify Users** setting which prevents the default email notification from being sent.
Selecting Multiple Devices	Act on individual devices or multiple devices by selecting the check box next to each device and using the action buttons. Once you have applied a filter to show a specific set of devices, you can perform bulk actions to multiple selected devices. Perform this action by selecting the devices and selecting an action from the **Resend Message** and **More Actions** buttons. You can select individual check boxes. You can also select the entire set of filtered devices by selecting the global check box located atop the check box column. When you select an action for one or more devices, a confirmation screen displays allowing you to **Save** or **Cancel** the action.
Layout	Display the full listing of visible columns or choose to display or hide columns per your preferences by selecting the **Custom** option. There is also an option to apply your customized column view to all administrators at or below the current organization group. You can return to the **Layout** button settings at any time to modify your column display preferences.

Enrollment Status Details View

Select a device friendly name in the **General Info** column at any time to open the **Details View** for that device.

From the **Details View**, you can resend the enrollment message by selecting the **Resend Message** button. You can also edit a device registration info by selecting the **Edit Registration** button and completing the **Advanced Device Information** section.

The **Details View** displays a series of tabs, each containing relevant enrollment information about the device.

- **Summary** – View the registration date, time elapsed since the device was first seen, basic device and user info.
- **User** – View detailed user info.
- **Message** – View the outgoing Device Activation email message including credential information and QR code. There is a resource available, called "User Registration Message," that allows the Workspace ONE UEM administrator to hide the **Message** tab after the device has successfully enrolled.
- **Custom Attributes** – View the Custom Attributes associated with the device..
- **Tags** – View the tags currently associated with the device.
- **Offline Enrollment** – If available, this tab allows you to enroll the device while it is offline. This feature is useful for when you want to make the most of scheduled time for a device in an unavailable state (for example, while traveling).

Wipe Protection

Remotely wiping a device of privileged corporate content, called an Enterprise Wipe, is a step undertaken when a device becomes lost or stolen. It is meant as a safeguard against the threat of corporate content coming into contact with competitors.

However, there are circumstances when scheduled processes such as the Compliance Engine and other automated directives wipe multiple devices. As an administrator, you may want to be informed when such a directive is scheduled and be given the chance to intervene.

Configure wipe protection settings by defining a wipe threshold, which is a minimum number of devices wiped within a certain amount of time. For example, if more than 10 devices are wiped within 20 minutes, you can place future wipes on hold until after you validate the wipe commands.

You can review wipe logs to see when devices were wiped and for what reason. After reviewing the information, you can accept or reject the on-hold wipe commands and unlock the system to reset the wipe threshold counter.

Configure Wipe Protection Settings for Managed Devices

Set a wipe threshold for managed devices and notify administrators through email when the threshold is met. You can only configure these settings at the Global or Customer level organization group.

Procedure

1 Navigate to **Devices > Lifecycle > Settings > Managed Device Wipe Protection**.

2 Configure the following settings.

Setting	Description
Wiped Devices	Enter the number of **Wiped Devices** that acts as your threshold for triggering wipe protection.
Within (minutes)	Enter the value for **Within (minutes)** which is the amount of time the wipes must occur to trigger wipe protection.
Email	Select a message template to email to administrators. Create a message template for wipe protection by navigating to **Groups & Settings > All Settings > Devices & Users > General > Message Templates** and select **Add**, Next, select **Device Lifecycle** as the **Category** and **Wipe Protection Notification** as the **Type**. You can use the following lookup values as part of your message template. ■ {EnterpriseWipeInterval} – The value of **Within (minutes)** on the settings page. ■ {WipeLogConsolePage} – A link to the Wipe Log page.
To	Enter the email addresses of administrators who must be notified. These administrators must have access to the Wipe Log page.

For details, see Lookup Values.

3 Select **Save**.

View Wipe Logs

You can view the **Wipe Log** page to see when devices were wiped and for what reason. After reviewing the information, you can accept or reject any on-hold wipe commands and unlock the system to reset the wipe threshold counter.

If the system is locked, then you see a banner at the top of the page indicating this status.

Procedure

1 Navigate to **Devices > Lifecycle > Wipe Log**.

The **Report Device Wipe Log** resource manages access to the Wipe Log page, and is available by default for system admins, SaaS admins, and Workspace ONE UEM admins. You can add this resource to any custom admin role using the **Create Admin Role** page.

For more information, see Create Administrator Role.

2 **Filter** the Wipe Log by the following parameters.

- Date Range
- Wipe Type
- Status
- Source
- Ownership

3 View the list of devices and determine whether the presented devices are valid wipes.

Device pending actions have a status of "On Hold." Devices wiped before the threshold limit is reached display as "Processed".

a If they are valid wipes, then select each device and then select **Approve wipes** from the command list. The status changes to Approved.

b If they are not valid wipes, then select each device and then select **Reject wipes** from the command list. The status changes to Rejected.

4 Reset the device threshold counter and allow wipe commands to go through by selecting **Unlock System**.

What to do next

The system allows future automated wipe commands until the threshold limit is exceeded again.

You can only perform this action at a Global or Customer level organization group.

Shared Devices

Shared Device/Multi-User Device functionality ensures that security and authentication are in place for every unique end user. And if applicable, shared devices allow only specific end users to access sensitive information.

Issuing a device to every employee in certain organizations can be expensive. Workspace ONE UEM lets you share a mobile device among end users in two ways: using a single fixed configuration for all end users, or using a unique configuration setting for individual end users.

When administering shared devices, you must first provision the devices with applicable settings and restrictions before deploying them to end users. Once deployed, Workspace ONE UEM uses a simple login or log-out process for shared devices in which end users simply enter their directory services or dedicated credentials to log in. The end-user role determines their level of access to corporate resources such as content, features, and applications. This role ensures the automatic configuration of features and resources that are available after the user logs in.

The login or log-out functions are self-contained within the Workspace ONE Intelligent Hub. Self-containment ensures that the enrollment status is never affected, and that the device is managed whether it is in use or not.

Shared Devices Capabilities

There are basic capabilities surrounding the functionality and security of devices that are shared across multiple users. These capabilities offer compelling reasons to consider shared devices as a cost-effective solution to making the most of enterprise mobility.

Functionality

- Personalize each end-user experience without losing corporate settings.

- Logging in a device configures it with corporate access and specific settings, applications, and content based on the end-user role and organization group (OG).
- Allow for a log in/log out process that is self-contained in the Workspace ONE Intelligent Hub or VMware Identity Manager.
- After the end user logs out of the device, the configuration settings of that session are wiped. The device is then ready for login by another end user.

Security

- Provision devices with the shared device settings before providing devices to end users.
- Log in and log out devices without affecting an enrollment in Workspace ONE UEM.
- Authenticate end users during a login with directory services or dedicated Workspace ONE UEM credentials.
- Authenticate end users using VMware Identity Manager.
- Manage devices even when a device is not logged in.

Platforms that Support Shared Devices

The following devices support shared device/multi-user device functionality.

- Android 4.3+
- iOS devices with Workspace ONE Intelligent Hub v4.2+,
- MacOS devices with Workspace ONE Intelligent Hub v2.1+.

Define the Shared Device Hierarchy

While strictly optional, making an organization group (OG) specific to shared devices offers many benefits due to multi-tenancy and inherited device settings.

If you have a large number of shared devices in your fleet and you want to manage them apart from single user devices, you can make a shared device-specific OG. Making a shared device hierarchy in your OG structure is optional. Features like smart groups and user groups mean you do not have to rely strictly on OG hierarchy design to simplify device management.

However, having a shared device OG (or nested OGs) simplifies device management by enabling you to standardize device functionality through profiles, policies, and device inheritance without the processing overhead required by a smart group or a user group.

Procedure

1. Navigate to **Groups & Settings > Groups > Organization Groups > Organization Group Details**.

   Here, you can see an OG representing your company.

2. Ensure the **Organization Group Details** displayed are accurate, and then use the available settings to make modifications, if necessary. If you make changes, select **Save**.

3 Select **Add Child Organization Group**.

4 Enter the following information for the first OG underneath the top-level OG.

Setting	Description
Name	Enter a name for the child organization group (OG) to be displayed. Use alphanumeric characters only. Do not use odd characters.
Group ID	Enter an identifier for the OG for the end users to use during the device login. Group IDs are used during the enrollment of group devices to the appropriate OG. Ensure that users sharing devices receive the **Group ID** as it might be required for the device to log in depending on your Shared Device configuration. If you are not in an on-premises environment, the Group ID identifies your organization group across the entire shared SaaS environment. For this reason, all Group IDs must be uniquely named.
Type	Select the preconfigured OG type that reflects the category for the child OG.
Country	Select the country where the OG is based.
Locale	Select the language classification for the selected country.
Customer Industry	This setting is only available when **Type** is Customer. Select from the list of Customer Industries.
Time Zone	Select the time zone for the OG's location.

5 Select **Save**.

Configure Shared Devices

Similar to single-user device staging, multi-user staging (a "shared device") allows an IT administrator to provision devices to be used by more than one user.

Procedure

- Complete the **Security** section, as applicable.

Setting	Description
Require Shared Device Passcode.	Require users to create a Shared Device passcode in the Self-Service Portal to check out devices. This passcode is different from a Single Sign On passcode or a device-level passcode.
Require Special Characters.	Require special characters in the shared device passcode, which includes characters such as @, %, &, and so forth.
Shared Device Passcode Minimum Length	Set the minimum character length of the shared passcode.
Shared Device Passcode Expiration Time (days)	Set the length of time (in days) the shared passcode expires.
Keep Shared device Passcode for minimum time (days)	Set the minimum amount of time (in days) the shared device passcode must be changed.
Passcode History	Set the number of passcodes that are remembered by the system, providing a more secure environment by preventing the user from reusing old passcodes.
Auto Log out Enabled	Configure an automatic log out after a specific time period.

Setting	Description
Auto Log out After	Set the length of time that must elapse before the **Auto Log out** function activates in **Minutes**, **Hours**, or **Days**.
Enable Single App Mode.	Select this check box to configure Single App Mode, which locks the device into a single application when an end user logs in to the device. To check out an iOS device in Single App Mode, end users log in using their credentials. When the device is checked in again, it returns to Single App Mode. Enabling Single App Mode also disables the Home button on the device. **Note** Single App Mode applies only to Supervised iOS devices.
Clear Device Passcode on Logout (Android Only)	This setting controls whether the current device passcode is cleared when the user logs out (checks in) a multi-user shared device.
Clear App Data on Logout (Android Only)	Clear the app data when the user logs out of a shared device (checks it in).
Reinstall Apps on Logout (Android Work Managed Device and Android (Legacy) Only)	Use the drop-down to select whether to Always reinstall app between users or never reinstall app between users. For Android (Legacy) deployments, you can opt to reinstall app if the Hub cannot clear app data between users.

Log In and Log Out of Shared Android Devices

To use shared device functionality on Android devices, enroll the device using the Workspace ONE Intelligent Hub and set the VMware Workspace ONE Launcher as the default home screen. The Workspace ONE Launcher is automatically downloaded during enrollment.

Once the application is installed and set as the default home screen, the device is in a checked-in state. While in this state, the end user is unable to navigate away from this page and the device prompts the user to check out. To remove the profile and make the entire device accessible again, perform an Enterprise Wipe on the staging user device from the Workspace ONE UEM console.

Procedure

1. From the Workspace ONE Launcher log in page, users must enter their Group ID, user name, and password. If **Prompt User for Organization Group** is enabled on the console, end users are required to enter a **Group ID** to log in.
2. Select **Login** and accept the terms of use, if applicable.

   The device is configured. Once logged in, user profiles are pushed down based on the smart group and user group associations.

What to do next

To log out of an Android device, select the **Settings** button and select **log out**.

Log In and Log Out of Shared iOS Devices

You can log in to and out of an iOS device that is shared across multiple users.

What to do next

Tap **Log out** under the **Shared Device** section.

Note When the shared device is logged out, both the device passcode and Single Sign On passcode are cleared without any warning or notification. The device in this state allows the next user to configure another passcode.

Log In and log out of Shared macOS Devices

Multiple users can log in to and out of a macOS shared device, activating the automatic push of device profiles.

Log In to a macOS Device - Using assigned Network credentials, log in to a macOS device that has been staged and you receive the profiles assigned to your account in Workspace ONE UEM.

Log out of a macOS Device - The standard macOS log-out procedure also logs the device out of your assigned Workspace ONE UEM user profile.

Check In a Shared Device From the UEM Console

You can check in a device straight from the Workspace ONE UEM console, bypassing the need for the end user to check in the device using the installed Workspace ONE Intelligent Hub

When you check in a device using the UEM console, you effectively reset the enrollment to the multi staging user with the prescribed organization group, profiles, apps, and so on. On the device side, the Workspace ONE Intelligent Hub is restarted and the check-out screen displays.

This feature applies currently to iOS devices only. Devices that enrolled using a method other than the Workspace ONE Intelligent Hub (for example, Direct Enrollment, Workspace ONE, or Container) are not supported. Checking in devices in bulk from the console is not supported.

Procedure

1. Navigate to **Devices > List View** and locate the shared iOS device you want to check in.
2. Select the **Friendly Name** of the device to display **Device Details**.
3. Select the **More Actions** button in the upper-right corner of the screen.
4. Under the **Management** section, select **Check In Device**.

Enabling Directory Service-Based Enrollment

Directory service enrollment refers to the process of integrating Workspace ONE UEM with your organization's directory service infrastructure. Integrating your directory service in this manner means you can import users automatically and, optionally, user groups such as security groups and distribution lists.

When integrating with a directory service such as Active Directory (AD), you have options for how you import users.

- **Allow all directory users to enroll** – You can allow all your directory service users to enroll. Also, you can set up your environment to auto discover users based on their email. Then create a Workspace ONE UEM user account for them when they perform an enrollment.
- **Add users one by one** – After integrating with a directory service, you can add users individually in the same manner as creating basic Workspace ONE UEM user accounts. The only difference is you must enter their user name and select **Check User** to auto populate remaining information from your directory service.
- **Batch upload a CSV file** – Using this option, you can import a list of directory services accounts in a CSV (comma-separated values) template file. This file has specific columns, some of which cannot be left blank.
- **Integrate with user groups (Optional)** – With this method, you can use your existing user group memberships to assign profiles, apps, compliance policies, and so on.

Note For information about how to integrate your Workspace ONE UEM environment with your directory service, refer to the **VMware AirWatch Directory Services Guide**. If you are considering integrating Workspace ONE UEM with a SAML provider, refer to the **VMware AirWatch SAML Integration Guide**, both available on docs.vmware.com.

Lookup Values

A lookup value is a variable that represents a particular data element of a device, user, or admin account. Lookup values can be invaluable in completing a process or a form.

In several different text boxes in the Workspace ONE UEM console, you can add lookup values in place of manually entered or static values. In most cases, lookup values function as a stand-in for a piece of information you do not know or do not have access to.

For example, the **Add Device** screen is used to add a device to your fleet. One of the text boxes on this screen that can be completed with lookup values is the **Expected Friendly Name**.

The friendly name represents the device on many different screens in the UEM console including the **Device List View** and the **Details View**. And while you can enter a static friendly name manually, you can instead use lookup values to standardize the friendly name and make it a valuable identifier.

A common friendly name format can be constructed with the following lookup values.

{EnrollmentUser} {DeviceModel} {DeviceOperatingSystem} {DeviceSerialNumberLastFour}

If you enter the above in the **Expected Friendly Name** text box, it produces a friendly name that looks like this on the **Device List View**.

jsmith iPad iOS GHKD

This friendly name instantly provides you with at least three useful pieces of information. And with the last four digits of the device serial number at the end, it is virtually guaranteed to be unique.

Data Overhead

When used, lookup values do not add to the device's memory with an extra load. Lookup values are a construct of the UEM console itself, not something that is transferred to the device.

Static Strings Versus Lookup Values

Lookup values cannot be applied once a static string has been entered in a text box.

For example, assume that you have 100 devices to enroll. You add the first 50 devices using a manually entered static string for **Expected Friendly Name**. For the next 50 devices, you opt to use a lookup value for **Expected Friendly Name** instead. Those 100 devices, half with static friendly names and the other half with lookup values, can coexist perfectly well. There is no issue with mixing and matching static strings and lookup values.

However, you cannot return to the first 50 devices and replace the static string friendly name with a lookup value.

Custom Lookup Values

You can use the Custom Attributes feature to make your own lookup values. You can then use these custom lookup values in the same manner as ordinary lookup values. For details, see Create Custom Attributes.

Lookup Values Listing

To reference a full listing of lookup values including the locations in Workspace ONE UEM from which they are accessed, see https://support.workspaceone.com/articles/115001663908.

Device Enrollment

2

Enrolling a device is required before the device can be managed by the Workspace ONE UEM console. There are multiple enrollment paths, each path with options.

Enrolling Devices at Global

The Global organization group (OG) is designed to house Customer and other types of OGs. Given the way inheritance works, if you add devices to Global and configure Global with settings intended to affect those devices, you are also affecting all the Customer OGs underneath. This undermines the benefits of multitenancy and inheritance.

For more information, see Reasons You Should Not Enroll Devices in Global.

This chapter includes the following topics:

Enroll a Device with Workspace ONE Intelligent Hub

Enrolling a device with the Workspace ONE Intelligent Hub is the main option for Android, iOS, and Windows devices.

Procedure

1 Navigate to AWAgent.com from the native browser on the device that you are enrolling.

Workspace ONE UEM auto-detects if the Workspace ONE Intelligent Hub is already installed and redirects to the appropriate mobile app store to download the Workspace ONE Intelligent Hub if needed.

Downloading the Workspace ONE Intelligent Hub from public application stores requires either an Apple ID or a Google Account.

2 Run the Workspace ONE Intelligent Hub upon the completion of the download or return to your browser session.

Important To ensure a successful installation and running of the Workspace ONE Intelligent Hub on your Android device, it must have a minimum of 60 MB of space available. CPU and Run Time Memory are allocated per app on the Android platform. If an app uses more than allocated, Android devices optimize themselves by killing the app.

3 Enter your email address. Workspace ONE UEM checks if your address has been previously added to the environment. In which case, you are already configured as an end user and your organization group is already assigned.

If Workspace ONE UEM cannot identify you as an end user based on your email address, you are prompted to enter your **Environment URL**, **Group ID**, and **Credentials**. If your environment URL and Group ID are needed, your Workspace ONE UEM Administrator can provide it.

4 Finalize the enrollment by following all remaining prompts. You can use your email address in place of user name. If two users have the same email, the enrollment will fail.

Additional Enrollment Workflows

In some unique cases, the enrollment process must be adjusted for specific organizations and deployments. For each of the additional enrollment options, end users need the credentials detailed in the Required Information section of this guide.

- **Multi-Domain Environments** – Enrollment login in single and multi-domain environments is supported provided they are made in the following format. **domain\username**.
- **Kiosk Mode and Kiosk Designer** – Windows desktop end users can configure their desktop devices in kiosk mode. Users can also use the kiosk designer in the Workspace ONE UEM console to create a multi-app kiosk.
- **Notification-Prompt Enrollment** – The end user receives a notification (email and SMS) with the Enrollment URL, and enters their Group ID and login credentials. When the end user accepts the Terms of Use (TOU), the device automatically enrolls and outfits with all MDM features and content. This acceptance includes selected apps and features from the Workspace ONE UEM server.

- **Single-Click Enrollment** – In this workflow, which applies to web-based enrollments, an administrator sends a Workspace ONE UEM-generated token to the user with an enrollment link URL. The user merely selects the provided link to authenticate and enroll the device, making it the easiest and fastest enrollment process for the end user. This method can also be secured by setting expiration times.
  - **Web Enrollment** – There is an optional welcome screen that an administrator can invoke for Web enrollments by appending "/enroll/welcome" to the active environment. For example, by supplying the URL **https://<custenvironment > /enroll/welcome** to users participating in Web Enrollment, they see a Welcome to Workspace ONE UEM screen. This screen includes options to enroll with an Email Address or Group ID. The Web Enrollment option is applicable for Workspace ONE UEM version 8.0 and above.
- **Dual-Factor Authentication** – In this workflow, an administrator sends the same enrollment token generated by Workspace ONE UEM, but the user must also enter their login credentials. This method is just as easy to run as the Single-Click Enrollment but adds one additional level of security. The additional security measure is requiring the user to enter their unique credentials.
- **End-User Registration** – The user logs in to the Self-Service Portal (SSP) and registers their own device. Once registration is complete, the system sends an email to the end user that includes the enrollment URL and login credentials. This workflow assumes that administrators have not already performed device registration for a corporate device fleet. It also assumes that you require corporate devices to be registered so administrators can track enrollment status. Also, end-user registration means that corporate devices can be used together with user-purchased devices.
- **Single-User Device Staging** – The administrator enrolls devices on behalf of an end user. This method is useful for administrators who set up multiple devices for an entire team or single members of a team. Such a method saves the end users the time and effort of enrolling their own devices. The admin can also configure and enroll a device and mail it directly to a user who is off-site.
- **Multi-User Device Staging** – The administrator enrolls devices that are used by multiple users. Each device is enrolled and provisioned with a specific set of features that users access only after they log in with unique credentials.

For more information, see the following topics.

Enable Registration Tokens and Create a Default Message.

End-User Device Registration.

Device Registration.

Stage a Single-User Device.

Stage a Multi-User Device.

Workspace ONE Direct Enrollment

Direct Enrollment using VMware Workspace ONE ™ represents the smoothest way to get started with devices that are corporate-owned and personally enabled (COPE).

The COPE model offers businesses a way to strike a balance between the consumerization of devices and the security and control that IT needs. As an administrator, you can configure an optional prompt, restrict by device type, limit by user group, and defer the installation of apps to the user.

Supported Enrollment Options in Workspace ONE

Most of the existing enrollment options are supported in Direct Enrollment with Workspace ONE. Of the options not yet supported, most are due to be added in a future Workspace ONE UEM release.

For more information, see Workspace ONE Direct Enrollment Supported Options.

Enable Direct Enrollment in Workspace ONE

Since the Direct Enrollment with Workspace ONE option is disabled on every organization group by default, you must actively enable it. Parent inheritance and child override options apply for maximum tenancy solutions.

For more information, see Enable Direct Enrollment for Workspace ONE.

Enroll Your Device with Workspace ONE Direct Enrollment

With Workspace ONE Direct Enrollment enabled, logging into the enrollment organization group using a qualifying device with the Workspace ONE app means that you are immediately enrolled.

For more information, see Enroll Your Device with Workspace ONE Direct Enrollment.

Workspace ONE Direct Enrollment Supported Options

The Workspace ONE Direct Enrollment feature works with many of the existing enrollment options and platforms available before the feature's development.

Direct enrollment with Workspace ONE ™ supports the following platforms and enrollment options.

Supported Platforms

- iOS.
- Android Legacy.
- Android Enterprise.

Navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment**, select each applicable tab, and make your selections based on compatibility with Workspace ONE Direct Enrollment.

Authentication

The following authentication options are compatible with Workspace ONE Direct Enrollment.

- Directory Users.
- SAML plus Active Directory Users are supported "on-the-fly". SAML without LDAP users is supported so long as the user record pre-exists in Workspace ONE UEM at the time of initial login.

Basic Users, Staging Users, SAML without Directory Users, and Authentication Proxy users are not currently supported.

- Open Enrollment.
- Workspace ONE does not audit the Require Workspace ONE Intelligent Hub for iOS or macOS settings, which are used to block web enrollment on their respective platforms.

Terms of Use

All terms of use options are compatible with Workspace ONE Direct Enrollment.

Grouping

All grouping options are compatible with Workspace ONE Direct Enrollment.

Restrictions

The following restrictions options are compatible with Workspace ONE Direct Enrollment.

- Known Users and Configured Groups.
- Maximum Enrolled Device Limit.
- Policy settings are partially supported.
  - Allowed Ownership Types – Workspace ONE only prompts for employee-owned and Corporate Dedicated. If you do not want either, disable optional prompt and use the default ownership type.
  - Allowed Enrollment Types are not supported.
- Device Platform, Device Model, and OS Restrictions are supported.
- User Group Restrictions.

Optional Prompts

The following optional prompts options are compatible with Workspace ONE Direct Enrollment.

- Prompt for Device Ownership.
- Prompt for Asset Number (supported only when Prompt for Device Ownership is enabled).
- All other optional prompts are not supported.

Customization

The following customization options are compatible with Workspace ONE Direct Enrollment.

- Use specific Message Template for each Platform.
- Post-Enrollment Landing URL (iOS only).
- MDM Profile Message (iOS only).
- Use Custom MDM Applications.
- Enrollment Support Email and Enrollment Support Phone are not supported.

Staging

Device staging through Workspace ONE Direct Enrollment is not supported. If you must stage a device, whether for single or multiple users, you must enroll the device using Workspace ONE Intelligent Hub instead of Workspace ONE Direct Enrollment.

Enable Direct Enrollment for Workspace ONE

You can enable Workspace ONE ™ Direct Enrollment on the organization group (OG) of your preference. Once enabled, all qualified devices logging in for the first time to Workspace ONE UEM are directly enrolled. Unqualified devices that fall outside the criteria you define are enrolled in an unmanaged or container state.

Direct Enrollment is disabled by default. To enable Workspace ONE Direct Enrollment, take the following steps.

Procedure

1 Switch to the organization group for which you want to enable Direct Enrollment for Workspace ONE.

2 Navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment** and select the **Restrictions** tab.

3 If necessary, select to Override the parent OG's settings.

4 Scroll down to the **Management Requirements for Workspace ONE** and select your configuration options.

Setting	Description
Require MDM for Workspace ONE	Prompt qualified devices and users to be enrolled immediately upon login to Workspace ONE. Devices outside the defined criteria are allowed to enroll in an unmanaged state and can come under management later (Adaptive Management).
Assigned User Group	This setting specifies the user group you want to include in the direct enrollment process. You can also select **All Users** which are the default selection when you enable **Require MDM for Workspace ONE**.
iOS	Enable this setting to include iOS devices. Disabled makes iOS devices not eligible for direct enrollment, though they can still enroll into Workspace ONE UEM in an unmanaged state.
Android Legacy	Enable this option to include legacy Android devices. Disabled makes legacy Android devices not eligible for direct enrollment, though they can still enroll into Workspace ONE UEM in an unmanaged state.
Android Enterprise	Enable this setting to include Android Enterprise devices. Disabled makes Android Enterprise devices not eligible for direct enrollment, though they can still enroll into Workspace ONE UEM in an unmanaged state.

5 Select **Save**.

Results

Only supported options configured on the other enrollment tabs apply to your saved direct enrollment configuration.

What to do next

Once Workspace ONE Direct Enrollment has been enabled, the next step is to Enroll Your Device with Workspace ONE Direct Enrollment. For more information about Direct Enrollment for Workspace ONE Options and Enrollment Options in general, see Workspace ONE Direct Enrollment Supported Options and Configure Enrollment Options.

Enroll Your Device with Workspace ONE Direct Enrollment

With Workspace ONE ™ Direct Enrollment enabled, logging into the enrollment organization group using a qualifying device and user with the Workspace ONE app means that you are immediately enrolled.

Your users are also given the chance to install apps immediately which your company finds useful. Alternately, they can skip this step in favor of app installation later. To enroll a device with Workspace ONE Direct Enrollment, the end user takes the following steps.

Procedure

1. Download, install, and run the Workspace ONE app from the platform-specific app store or repository.
2. Enter the server URL or email address.
3. Enter your directory services user name and password.
4. Select affirmative steps specific to your platform to install or enable **Workspace Services**.
   a. **iOS** – allow the server to open Settings, enter your device passcode, install an unsigned device profile, and open a screen in Workspace.
   b. **Android Legacy** – Install Workspace ONE Intelligent Hub, allow it to make and manage phone calls, select ownership for your device with an option to enter the device asset number, activate the device admin application, then sign into Workspace ONE.
   c. **Android Enterprise** – Accept (or decline) the terms of use agreement, set up the work profile, and create the Workspace ONE passcode.
5. When Workspace ONE finishes the install routine, you can **Continue to install apps**.
6. You can install individual apps selected from a list, **Install all**, or **Skip** this step entirely.

Basic vs. Directory Services Enrollment

If you have a directory services infrastructure such as Active Directory (AD), Lotus Domino, and Novell e-Directory, you can apply existing users and groups in Workspace ONE UEM. If you do not have an existing directory services infrastructure or you choose not to integrate with it, you must perform Basic Enrollment. Basic enrollment means manually creating user accounts in the UEM console.

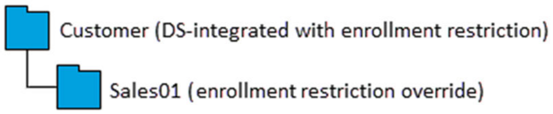
Note While Workspace ONE UEM supports a mix of both Basic and Directory-based users, you typically use one or the other for the initial enrollment of users and devices.

Pros and Cons

	Pros	Cons
Basic Enrollment	■ Can be used for any deployment method. ■ Requires no technical integration. ■ Requires no enterprise infrastructure. ■ Can enroll into potentially multiple organization groups.	■ Credentials only exist in Workspace ONE UEM and do not necessarily match existing corporate credentials. ■ Offers no federated security. ■ Single sign on not supported. ■ Workspace ONE UEM stores all user names and passwords. ■ Cannot be used for Workspace ONE Direct Enrollment.
Directory Service Enrollment	■ End users authenticate with existing corporate credentials. ■ Can automatically detect and sync changes from the directory system into Workspace ONE UEM. ■ Secure method of integrating with your existing directory service. ■ Standard integration practice. ■ Can be used for Workspace ONE Direct Enrollment. ■ SaaS deployments using the VMware Enterprise Systems Connector require no firewall changes and offers a secure configuration to other infrastructures, such as Microsoft ADCS, SCEP, and SMTP servers.	■ Requires an existing directory service infrastructure. ■ SaaS deployments require additional configuration due to the VMware Enterprise Systems Connector being installed behind the firewall or in a DMZ.

Directory Service Integration and Enrollment Restrictions

When directory service integration is configured on Workspace ONE UEM, directory service accounts inherit enrollment settings from the organization group (OG) from which the directory service is configured. Basic accounts, however, abide by local settings including overrides.


Customer (DS-integrated with enrollment restriction)
Sales01 (enrollment restriction override)

For example, assume the option **Enterprise Wipe devices of users that are removed from configured groups** is enabled on the Customer OG.

Given this scenario, **directory** enrollment users in Sales01 who leave a configured group see their devices wiped despite the enrollment restriction override configured in that OG. This is true even if those accounts have devices enrolled on a different OG because enrollment settings are user-centric, not device centric.

However, in this same scenario, devices belonging to **basic** enrollment users of Sales01 OG who leave a configured group are not wiped. This is because basic enrollment users in Sales01 are not a part of the directory service-integrated OG and therefore recognize and abide by the overridden enrollment restriction.

Enrollment Considerations, Basic Versus Directory

When considering end-user enrollment, in addition to the existing pros and cons of Basic versus Directory users, there are other questions to consider.

For the pros & cons of basic users vs directory users, see Basic vs. Directory Services Enrollment.

Consideration #1: Who Can Enroll?

In answering this question, consider the following.

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

  You can allow all users to enroll during the initial deployment rollout and then afterward, restrict the enrollment to prevent unknown users from enrolling. As your organization adds new employees or members to existing user groups, these changes are synced and merged.

- Are there certain users or groups who are not to be included in MDM? If so, you must either add users one at a time or batch import a CSV (comma-separated value) file of only eligible users.

If you want to restrict certain users and groups, see Configure Enrollment Restriction Settings.

Consideration #2: Where Will Users Be Assigned?

Another consideration to make when integrating your Workspace ONE UEM environment with directory services is how you assign directory users to organization groups during an enrollment. In answering this question, consider the following.

- Have you created an organization group structure that logically maps to your directory service groups? You must complete this task before you can edit user group assignments.
- If your users are enrolling their own devices, the option to select a Group ID from a list is simple. Human error is a factor in this simplicity and can lead to incorrect group assignments.

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

If you want to configure Group ID options, see Configure Enrollment Options on Grouping Tab.

* The base DN, or distinguished name, is the point from which a server searches for users. A distinguished name is a name that uniquely identifies an entry in the directory. Every entry in the directory has a DN.

Enabling Basic Enrollment

Basic Enrollment refers to the process of manually creating user accounts and user groups for each of your organization's users. If your organization is not integrating Workspace ONE UEM with a directory service, basic enrollment is how you create user accounts.

If you have a few basic accounts to create, then create them one at a time as described in Create Basic User Accounts.

For basic enrollments involving larger end-user numbers, you can save time by filling out and uploading CSV (comma-separated values) template files. These files contain all user information through the batch import feature. For more information, see Batch Import Users or Devices.

Bring Your Own Device (BYOD) Enrollment

A major challenge in managing users' personal devices is recognizing and distinguishing between employee-owned and corporate-owned devices and then limiting enrollment to only approved devices.

Workspace ONE UEM enables you to configure many options that customize the end-user experience of enrolling a personal device. Before you begin, you must consider how you plan to identify employee-owned devices in your deployment and whether to enforce enrollment restrictions for employee-owned devices.

Enrollment Considerations, BYOD

Assuming you are allowing employees to enroll their personal devices in your Workspace ONE UEM environment, there are many considerations you must make before you proceed.

Consideration #1: Will BYOD Users Enroll with VMware Workspace ONE or the Workspace ONE Intelligent Hub?

VMware Workspace ONE is a secure enterprise platform that delivers and manages any app on any device. It begins with self-service, single-sign on access to cloud, mobile, and Windows apps and includes powerfully integrated email, calendar, file, and collaboration tools.

With Workspace ONE, users do not need to enroll their personal devices to get access to services. The Workspace ONE app itself can be downloaded from the Apple App Store, Google Play, or Microsoft Store and installed. A user then logs in and gains access to applications based on the established policies. The Workspace ONE app configures an MDM management profile during its installation that enrolls the device automatically.

Workspace ONE Intelligent Hub represents the legacy enrollment option for mobile devices. For details, see Enroll a Device with Workspace ONE Intelligent Hub.

Consideration #2: How Will You Specify Ownership Type?

Every device enrolled into Workspace ONE UEM has an assigned device ownership type: Corporate Dedicated, Corporate Shared, or Employee Owned. Employees' personal devices are categorized as an Employee Owned type and subject to the specific privacy settings and restrictions you configure for that type.

In answering the question of specifying an ownership type, consider the following.

- Do you have access to a master list of corporate devices that you can bulk upload into the UEM console? If so, you might consider uploading this list and setting the default ownership type to Employee Owned.

- Have you considered the legal implications of allowing users to select an ownership type from a list? For example, if a user enrolls a personal device but incorrectly selects corporate owned as the ownership type. What are the ramifications when that user violates a policy and has their personal device fully wiped?

For your BYOD program, you can configure Workspace ONE UEM to apply a default ownership type during enrollment or allow users to select the appropriate ownership type themselves.

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

When answering this question, consider the following.

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

You can set up additional enrollment restrictions to further control who can enroll and which device types are allowed. For example, you can opt to support only those Android devices that feature built-in enterprise management functionality. After your organization evaluates and determines which kinds of employee-owned devices they want to use in your work environment, you can configure these settings.

For more information, see Additional Enrollment Restrictions.

Identify Corporate Devices and Specify Default Device Ownership

Preparing a list of devices can be useful if you have a mix of corporate-owned devices and employee-owned devices which employees enroll themselves. As enrollment commences, devices you identified as Corporate-Owned have their ownership type configured automatically based on what you selected. Then you can configure all employee-owned devices – which are not in the list – to enroll with an ownership type as Employee-Owned.

The following procedure explains how to import a list of pre-approved corporate devices. You can apply the Corporate-Owned ownership type after enrollment automatically, even if you have a restriction that automatically applies the Employee-Owned ownership type.

Restrictions for an open enrollment, by contrast, explicitly allow or block the enrollment for devices matching parameters you identify including platform, model, and operating system.

Procedure

1. Navigate to **Devices > Lifecycle > Enrollment Status** and select **Add**, then **Batch Import** which displays the **Batch Import** screen.

   Alternatively, you can select **Add** then **Whitelisted Devices** to enter up to 30 whitelisted devices at a time by IMEI, UDID, or Serial Number. You can also select either Corporate Owned or Corporate Shared as the **Ownership Type**.

2. Enter a **Batch Name** and **Batch Description**, then select **Add Whitelisted Device** as the **Batch Type**.

3 Select the link entitled, "Download template with an example for whitelisted devices" and save this comma-separated values (CSV) template to a location you have access to. Edit this CSV file with Excel to add all the devices you want to whitelist, then save the file.

4 Select **Choose File** and select your saved CSV file.

5 Select **Import** to import this device information to your whitelist.

6 Set the **Default Device Ownership** type to Employee Owned for all open enrollment.

   a Navigate to **Devices > Devices Settings > Devices & Users > General > Enrollment** and select the **Grouping** tab.

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

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

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

   e Select **Save**.

Prompt Users to Identify Ownership Type

If your deployment has organization groups with multiple ownership types, you can prompt users to identify their ownership type during enrollment. Careful consideration should be used before allowing users to choose their own ownership type.

You can always update the ownership type on individual devices later but it is safer and more secure to make a list of corporate devices. Then enroll the corporate-owned devices separately and later, set the default ownership type to Employee Owned.

Prerequisites

While simple, this approach assumes that every user correctly selects the appropriate ownership type applicable to their device. If a personal device user selects the Corporate-Owned type in error, their device is now subject to policies and profiles that normally do not apply to personal devices. This erroneous selection can have serious legal implications regarding user privacy.

Procedure

1 Navigate to **Devices > Device Settings > Devices & Users > General > Enrollment** and select the **Optional Prompt** tab.

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

3 Select **Save**.

Self-Enrollment Versus Device Staging

Workspace ONE UEM supports two methods for enrolling corporate devices. You can let users enroll their own devices or administrators can enroll devices on users' behalf in a process called **device staging**.

In device staging, an administrator enrolls devices before assigning them and distributing them to end users. This method is useful for administrators who must set up devices shared by multiple users across an organization.

Also, device staging works well for newly provisioned devices, since it happens before an employee receives the device. If your end users already have corporate devices, then allowing them to self-enroll makes the most sense. Letting users enroll their own devices is also beneficial when the total number of devices makes it impractical for administrators to perform device staging.

Device staging can be performed for Android, Windows Phone, iOS, and macOS devices.

Note Windows Phone currently only supports single user device staging.

Device staging through Workspace ONE Direct Enrollment is not supported. If you must stage a device, whether for single or multiple users, you must enroll the device using Workspace ONE Intelligent Hub instead of Workspace ONE Direct Enrollment.

For more information, see Workspace ONE Direct Enrollment.

Enrollment Considerations, Self-Enrollment

If you want to save time by allowing your end users to self enroll, consider the following questions.

Consideration #1: Device Ownership

- Do your end users already have assigned corporate devices? In this case, it may not be practical to collect each device and have it staged and instead have users enroll themselves.
- Are your end users sharing devices or do they have their own dedicated devices? If end users are not sharing devices, then you can make it the responsibility of that device's single owner to enroll themselves.

Consideration #2: Auto Discovery

Are you associating your organization's email domain with your Workspace ONE UEM environment? This process, known as an **auto discovery**, means that end users need only enter email address and credentials. The enrollment URL and Group ID are automatically entered.

See also Configure Autodiscovery Enrollment from a Child Organization Group and Configure Autodiscovery Enrollment from a Parent Organization Group.

Consideration #3: Workspace ONE Direct Enrollment

Workspace ONE Direct Enrollment is a feature that fits well with self-enrollment. Once enabled, all qualified devices that log into the enrollment organization group are immediately enrolled. And once fully installed, the end user can agree to install apps selected by the company or to opt out of installing apps.

For more information, see Workspace ONE Direct Enrollment.

Self-Enrollment Process

Self-enrollment can require that end users know their appropriate Group ID and login credentials. If you have integrated with directory services, these credentials are the same as the user's directory service credentials.

You can also associate your organization's email domain with your Workspace ONE UEM environment in a process known as auto discovery. With auto discovery enabled, devices of supported platforms prompt end users to enter their email address. These devices automatically complete enrollment if their email domain (the text after @) matches – without the need to enter a Group ID or enrollment URL. For more information, see Autodiscovery Enrollment.

Procedure

1. End users navigate to AWAgent.com, which automatically detects whether the Workspace ONE Intelligent Hub is installed.

   If Workspace ONE Intelligent Hub is not installed, the Website redirects to the appropriate mobile app store.

2. AirWatch Container users download the AirWatch Container app from the app store.

3. After launching the Workspace ONE Intelligent Hub or Container app, users enter their credentials – in addition to either an email address or URL/Group ID – and proceed with enrollment.

What to do next

Enrollment Considerations, Device Staging

Administrators can enroll devices on behalf of users in a process called **device staging**. Staging devices serves to streamline the process of registration and to enroll iOS devices shared by multiple users. You can also stage devices to provision an entire device fleet quickly with Apple Configurator.

Consideration #1: Use of Device Staging

Unless you are using Apple Configurator, administrators must stage devices one-by-one. For large deployments, consider the time and staffing this effort requires.

Whereas administrators can stage new devices easily, employees already using corporate-owned devices must ship devices in or collect them on-site to have devices staged.

If you have thousands of devices to pre-enroll, device staging can take time. Therefore it works best when you have a new batch of devices being provisioned, since you can gain access to the devices before employees receive them.

Device staging can be performed for Android, Windows Phone, and iOS devices in following ways.

- **Single User (Standard)** – Used when you are staging a device which any user can enroll.

  Note As indicated, this enrollment flow is intended for unattended devices. If you are using this flow for zero touch user enrollment, you are responsible for ensuring that staged devices are delivered to the intended user.

- **Single User (Advanced)** – Used when you are staging and enrolling a device for a particular user.

  Note The staging user/administrator must ensure that the device is checked out to the registered user.

- **Multi User** – Used when you are staging a device to be shared among multiple users.

Note Windows Phone currently only supports single user device staging.

Consideration #2: Are You Participating in Apple's Device Enrollment Program?

To maximize the benefits of Apple devices enrolled in Mobile Device Management (MDM), Apple has introduced the Device Enrollment Program (DEP). With DEP, you can perform the following.

- Install a non-removable MDM profile on a device, preventing end users from deleting it.
- Provision devices in Supervised mode (iOS only). Devices in Supervised mode can access additional security and configuration settings.
- Enforce an enrollment for all end users.
- Meet your organization's needs by customizing and streamline the enrollment process.
- Prevent iCloud back up by disabling users from signing in with their Apple ID when generating a DEP profile.
- Force OS updates for all end users.

Consideration #3: Use of Apple Configurator

Apple Configurator enables IT administrators to deploy and manage Apple iOS devices effectively. Organizations such as retail stores, classrooms, and hospitals find it especially useful to pre-enroll devices for multiple end users to share.

Using Configurator to enroll pre-registered devices meant for a single user is supported by adding serial number/IMEI information to a user's registered device in the Console. A major benefit of Apple Configurator is that you can use a USB hub or iOS device cart to provision multiple devices in minutes.

Consideration #4: Use of Workspace ONE Direct Enrollment

Device staging through Workspace ONE Direct Enrollment is not supported. If you must stage a device, whether for single or multiple users, you must enroll the device using Workspace ONE Intelligent Hub instead of Workspace ONE Direct Enrollment.

For more information, see Workspace ONE Direct Enrollment.

Consideration #5: Single User Staging or Registration?

If you are considering staging devices for a single user, registration might be preferred. The difference between staging for a single user and registering a device is subtle but important.

Registration – When you register a device, you do so for an individual, named user. This procedure means that the device expects the first user who logs in to be the same user to whom it was registered. If another user attempts to log in to a registered device, security purposes dictate that the device is locked out and cannot be enrolled.

Single User Staging – When you stage a device, you do so for any user qualified to enroll in Workspace ONE UEM. In theory, you might hand a staged device to any qualified user, and that user might successfully log in to the device and enroll in Workspace ONE UEM.

The staging workflow allows you to prepare the device and then start the Workspace ONE Intelligent Hub, where any qualified enrollment user can log in. Workspace ONE UEM then performs a one-time reassignment to associate the device to that user.

Supervised Mode

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

Benefits

Once a device is supervised and enrolled in Workspace ONE UEM, the administrator has the following enhanced features available for configuration when compared to normal devices.

- **Elevated Restrictions over MDM**
  - Prevent User from Removing Applications. Removing applications can also be restricted locally on the device using restrictions under System Configuration.
  - Prevent AirDrop.
  - Prevent users from modifying iCloud and Mail account settings which prevents account modification.
  - Disable iMessage.
  - Set iBookstore Content rating restrictions.
  - Disable Game Center and iBookstore.
- **Enhanced Security**
  - Prevent end users from visiting websites with adult content in Safari.
  - Restrict which devices can connect to specified AirPlay destinations, such as Apple TVs.
  - Prevent the installation of certificates or unmanaged configuration profiles.
  - Force all device network traffic through a global HTTP proxy.

- **Kiosk Mode**
  - Lock down devices to one app with single app mode and disable the home button.
- **Customize Wallpaper and Text on Device**
- **Enable or Clear Activation Lock**

Limitations

- USB Access to supervised devices is restricted to the supervising Mac.
- Cannot copy data to and from the device using iTunes unless the Apple Configurator identity certificate is installed on the device.
  - Media such as photos and videos cannot be copied from the device to a PC or Mac. To transfer this type of data, use the VMware Content Locker to sync the content with the user's Personal Documents section. Alternatively, a file sharing application can be used to transfer the data over WLAN/WWAN to a server.
- Supervised mode prevents access to device-side logs using the iPhone Configuration Utility (IPCU).
  - This mode makes it harder to troubleshoot any application or device issues. The reason for this difficulty is the logs from the device can only be obtained if the device is connected to the supervising Mac. To remediate some of the challenges, use the Workspace ONE SDK to send logs and logistics from the applications to the UEM console.
- Devices cannot be reset with factory settings easily.
  - Once a device is factory reset, it must be brought back to the supervising Mac to restore it back to supervised mode. This procedure may be problematic if the Mac is not near the device.

In deciding whether or not to enable Supervised Mode, consider the following. While it enables additional features that enhance security on the device, the USB limitations must be considered.

The proximity of the device to the supervising Mac plays an important role in the decisions. Since the USB limitation prevents access to device-side logs, a device experiencing issues must be shipped back to a depot and restaged to restore functionality.

Deciding on supervision in advance is important because the process to supervise or “unsupervise” requires the shipping of the device to an IT location or depot.

Stage a Single-User Device

Single-User Device Staging on the Workspace ONE UEM console allows a single administrator to outfit devices for other users on their behalf, which can be useful for IT administrators provisioning a fleet of devices.

Device staging through Workspace ONE Direct Enrollment is not supported. If you must stage a device, whether for single or multiple users, you must enroll the device using Workspace ONE Intelligent Hub instead of Workspace ONE Direct Enrollment.

Important The ability to create staging users is an elevated admin privilege. Permission to create a staging user should be limited only to specific, trusted administrators. Also, treat staging user credentials as you would any other admin privilege and do not disclose the user credentials.

Currently, any administrator with the permission to create a user can also create a staging user. Limit this ability by editing the roles assigned to your administrators. Navigate to **Accounts > Administrators > Roles**. Identify only those roles you want to limit and then **Edit** (✎) each of these roles in the category path **All > Accounts > Users > Accounts** by clearing the **Edit** check box from the "Add/Edit" permission.

Note LDAP binding is required when staging devices. To create this payload, see Binding a Device to the Directory Service in this guide.

Procedure

1 Navigate to **Accounts > Users > List View** and select **Edit** for the user account for which you want to enable device staging.

2 In the **Add / Edit User** page, select the **Advanced** tab.

   a Scroll down to the **Staging** section.

   b Select **Enable Device Staging**.

   c Select the staging settings that apply to this staging user.

   Single User Devices stages devices for a single user.

3 Toggle the type of single user device staging mode to either **Standard** or **Advanced**.

   Standard staging requires an end user to enter login information after staging, while Advanced means that the staging user can enroll the device on behalf of another user.

4 Ensure that **Multi User Devices** is set to **Disabled**.

5 Enroll the device.

   - Enroll using the Workspace ONE Intelligent Hub by entering a server URL and Group ID.
   - Open the device's Internet browser, navigate to the enrollment URL, and enter the proper Group ID.

6 Enter your staging user's credentials during enrollment.

   a If necessary, specify that you are staging for **Single User Devices**.

   You will only have to do this if multi-user device staging is also enabled for the staging user.

7 Complete enrollment for either Advanced or Standard staging.

   a If you are performing Advanced staging, you are prompted to enter the user name of the end-user device owner who is going to use the device. Proceed with enrollment by installing the Mobile Device Management (MDM) profile and accepting all prompts and messages.

   b If you are performing Standard staging, then when the end user completes the enrollment, they are prompted to enter their own credentials in the login window.

Results

The device is now staged and ready for use by the new user. If an enrollment terms of use agreement is in place, the staging single-user will not see this TOU agreement prompt until they log into their SSP account.

Stage a Multi-User Device

Multi-user device/shared device staging allows an IT administrator to provision devices intended to be used by more than one user. Multi-User staging allows the device to change its assigned user dynamically as the different network users log into that device.

Device staging through Workspace ONE Direct Enrollment is not supported. If you must stage a device, whether for single or multiple users, you must enroll the device using Workspace ONE Intelligent Hub instead of Workspace ONE Direct Enrollment.

Procedure

1 Navigate to **Accounts > Users > List View** and select **Edit** for the user account for which you want to enable device staging.

2 In the **Add / Edit User** page, select the **Advanced** tab.

   a Scroll down to the **Staging** section.

   b Select **Enable Device Staging**.

   c Select the staging settings that apply to this staging user.

   Single User Devices stages devices for a single user.

3 Toggle the type of single user device staging mode to either **Standard** or **Advanced**.

   Standard staging requires an end user to enter login information after staging, while Advanced means that the staging user can enroll the device on behalf of another user.

4 Ensure that **Multi User Devices** is set to **Enabled**.

5 Enroll the device using one of the two following methods.

   - Enroll using the Workspace ONE Intelligent Hub by entering a server URL and Group ID.
   - Open the device's Internet browser, navigate to the enrollment URL, and enter the proper Group ID.

6 Enter your staging user's credentials during enrollment. If necessary, specify that you are staging for **Single User Devices**.

   You only must do this if multi-user device staging is also enabled for the staging user.

7 Complete enrollment for either Advanced or Standard staging.

   - If you are performing Advanced staging, you are prompted to enter the user name of the end-user device owner who is going to use the device. Proceed with enrollment by installing the Mobile Device Management (MDM) profile and accepting all prompts and messages.
   - If you are performing Standard staging, then when the end user completes the enrollment, they are prompted to enter their own credentials in the login window.

Results

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

Device Registration

Registering corporate devices before they are enrolled is optional and the main benefit of this option is to restrict the enrollment to registered devices only.

Another benefit is tracking enrollment statuses, which let you know which of your users have enrolled and which have yet to enroll. You can then notify those users who have not yet enrolled.

Workspace ONE UEM can successfully register devices even when device identifiers are missing during the data entry phase, by users or administrators.

A third advantage to registering devices before enrollment is security. A registered device expects the user logging in for the first time to be the same individual it was registered to. If a different user attempts to log in to a registered device, the device is locked out and unable to enroll.

Enrollment Considerations, Registration

If you want to proceed with registering devices before enrollment, consider the following.

Who Will Register Devices?

An important consideration when registering devices is deciding who performs the actual device registration.

- What is the total number of devices in your deployment? In large deployments of thousands of devices, you can add this information to a CSV (comma-separated values) file. You then upload this file before devices are provisioned. You can also pass on the act of device registration onto the end user.
- Do you support a BYOD program where employees can use their personal devices? If you opt to restrict enrollment to only registered devices, you must give employees instructions on how to register their devices.

End-User Device Registration Through the SSP

You can direct end users to register their own devices before enrolling into Workspace ONE UEM if you are supporting BYOD. You can also require users with corporate owned devices to register if you want to track enrollment or use registration tokens. In either case, you must notify your end users of the process they need to follow.

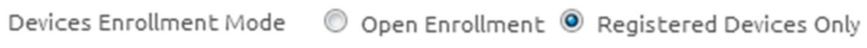
The following instructions assume that the end user has Workspace ONE UEM credentials, either from their existing directory service credentials or from a previously activated User Account. If you opted for enrolling with directory services without manually adding users, you will not have any user accounts already created.

In this case, if you want end users to register devices, you must send an email or intranet notification to each user group outside of Workspace ONE UEM with the registration instructions.

If you enabled registration tokens for enrollment authentication, they are sent to the user using the selected message type.

Restricting Enrollment to Registered Devices Only

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



Devices Enrollment Mode ○ Open Enrollment ● Registered Devices Only

Tracking Enrollment Status

Once devices are registered, you can track enrollment statuses by navigating to the **Device Dashboard** page and selecting the **Enrollment** chart, which lets you filter based on enrollment status. You can also access the Monitor, which lists devices recently enrolled.

- **Register Individual Devices** – Enter important device and asset information such as friendly name for easy recognition in the UEM console, model, operating system, serial number, Unique Device Identifier (UDID), and asset number. This process can also be the final step when adding a single user by selecting **Save and Add Device** rather than **Save**.
- **Register Multiple Devices** – Similar to adding users in bulk, this process streamlines the device registration process when adding multiple devices at a time. It can be included with the **Bulk User Account Creation** process.
- **End User Device Registration** – You can direct end users to register their own devices before enrolling into Workspace ONE UEM if you are supporting BYOD in your deployment. This arrangement is compatible with requiring devices to be registered before users can enroll.

For more information, see Enable Registration Tokens and Create a Default Message.

User Group Synchronization During Enrollment

If you intend to organize your application assignments, device profile assignments, compliance policy assignments, or user mappings around user groups, then consider keeping the User Group Sync setting enabled which is its default setting. This setting causes Workspace ONE to make a real-time call to the authentication server each time a device record is created.

For more information, see the **User Group Sync** section in Configure Enrollment Options on Grouping Tab.

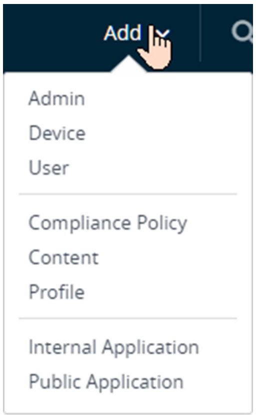
Register an Individual Device

While the Batch Import option makes registering hundreds or even dozens of devices convenient, when you have a small number of devices to register, you can register devices individually.

Procedure

1 Select the **Add** button, which can be found in the top-right quadrant of almost any screen in the Workspace ONE UEM console.

When selected, the button displays a drop-down menu with multiple options.



2 Select **Device**.

The **Add Device** page displays.

3 Complete the options according to your needs, starting with the **User** tab.

Setting	Description
User Section	
Search Text	Search for the user by entering a search parameter and select the **Search User** button. On a successful search, select the user account for whom you are registering the device. Several pre-populated text boxes display including Security Type, User Name, Password, and Email Address. You can edit these text boxes by displaying advanced user details.
Device Section	
Expected Friendly Name	Enter the Friendly Name of the device. This text box accepts **Lookup Values** which you can insert by selecting the plus sign. For details, see Lookup Values.
Organization Group	Select the Organization Group to which the device belongs.

Setting	Description
Ownership	Select the ownership level of the device.
Platform	Select the platform of the device.
Show advanced device information options	Display advanced device information settings.
Model	Select the device model. This drop-down menu option depends upon the **Platform** selection.
OS	Select the device operating system. This drop-down menu option depends upon the **Platform** selection.
UDID*	Enter the device unique device identifier.
Serial Number* § ‡	Enter the serial number of the device.
IMEI* §	Enter the device international mobile station equipment identity number.
SIM*	Enter the subscriber identity module for the device.
Asset Number*	Enter the device asset number.
Messaging Section	
Message Type	The type of notification sent to the user once the device is added. Select from **None**, **Email**, or **SMS**. The Email option requires a valid email address. You must also select an Email Message Template. The SMS option requires a phone number including country code and area code. SMS charges may apply. You must also select an SMS Message Template.
Email Address	Required for the Email Message Type.
Email Message Template	Required for the Email Message Type. Select a template from the drop-down menu. View the Email message with the **Message Preview** button.
Phone Number	Required for the SMS Message Type.
SMS Message Template	Required for the SMS Message Type. Select a template from the drop-down listing. View the SMS message with the **Message Preview** button.

* Among these denoted settings, at least one is required to register a device.

§ To register a Windows Phone device, you must enter either the IMEI or serial number of the device.

‡ To register a Windows Desktop device, you must enter the serial number of the device.

4 (Optional) Complete the **Custom Attributes** tab.

Setting	Description
Add	Add a custom **Attribute** and its corresponding **Application** and **Value** by selecting this button. In order to use the custom attribute feature while adding a device, you must have a custom attribute already created. Accomplish this by visiting Chapter 14 Custom Attributes.
Application	Select the application that gathers the attribute.
Attributes	Select the custom attribute from the drop-down menu.
Value	Select the value of the custom attribute from the drop-down menu.

5 (Optional) Complete the **Tags** tab.

Setting	Description
Add	Add a **Tag** to the device.
Tag	Select the Tag from the drop-down menu of existing Tags.

6 Select **Save** to complete the device registration process.

Results

The device is now registered to the selected Workspace ONE UEM user account specified in step 3.

What to do next

Deliver this device to this user so they can log in and complete the enrollment process. If another user attempts to log into this device before the registered user, the device is locked out and unable to enroll.

Missing Device Identifiers During Registration

If no device identifier is specified during registration (such as UDID, IMEI, and Serial Number), Workspace ONE UEM uses these attributes to match an enrolled device to its registration record automatically.

When inadequate registration information is provided, the following ranking allows Workspace ONE UEM to register devices successfully.

1 User to whom the device is registered.

2 Platform (if specified).

3 Model (if specified).

4 Ownership type (if specified).

5 Date of the oldest-matching registration record.

Register Multiple Devices

While Individual Device Registration works best when you have just a few devices you want to add, if you have hundreds or even dozens of devices to register, the Batch Import process is the way to go.

Procedure

1 Navigate to **Accounts > Users > List View** or **Devices > Lifecycle > Enrollment Status**.

a Select **Add** and then **Batch Import** to display the **Batch Import** screen.

2 Complete each of the required options: **Batch Name**, **Batch Description**, and **Batch Type**.

Within the **Batch File (.csv)** option is a list of task-based templates you can use to load users and their devices in bulk.

3 Select the appropriate download template and save the comma-separated values (CSV) file to somewhere accessible.

4 Locate the saved CSV file, open it with Excel, and enter all the relevant information for each of the devices that you want to import.

   Each template is pre-populated with sample entries demonstrating the type of information (and its format) intended to be placed in each column. Fields in the CSV file denoted with an asterisk (*) are required.

5 Save the completed template as a CSV file. In the UEM console, select the **Choose File** button from the **Batch Import** screen, navigate to the path where you saved the completed CSV file and select it.

6 Select **Save** to complete registration for all listed users and corresponding devices.

End-User Device Registration

Directing end users to register their own devices might be preferable if you are unsure of the device details during setup. Alternately, if you have a bring-your-own-device (BYOD) deployment in effect, such a directive might be prudent.

If you are supporting BYOD in your deployment, then direct end users to register their own devices before enrolling into Workspace ONE UEM. You can take this step and still require devices to be registered before users enroll. If you want to track enrollment or use registration tokens, then require users with corporate owned devices to register. In either case, you must notify your end users of the process.

The following instructions assume that the end user has Workspace ONE UEM credentials, either from their existing directory service credentials or from a previously activated User Account. If you opted to enroll with directory services without manually adding users, you must not have any user accounts already created.

If you want end users to register devices, you must send an email or notification to each user group outside of Workspace ONE UEM with registration instructions.

If you enabled registration tokens for enrollment authentication, the token is sent to the user in the selected message.

- Send an email or intranet notification to users outside of Workspace ONE UEM with the registration instructions. Ensure that enrollment authentication is enabled for Active Directory or Authentication Proxy by navigating to **Devices > Device Settings > Devices & Users > General > Enrollment > Authentication**.

  Verify that the setting **Deny Unknown Users** is deselected by navigating to **Devices > Device Settings > Devices & Users > General > Enrollment > Restrictions**.

- Create user accounts that allow all end users to register their devices, and then send user account activation messages to each user containing the registration instructions.

Both options require you to provide basic information to end users.

- **Where to Register** – End users can register by navigating to the Self-Service Portal URL. This URL follows the structure of **https://<AirWatchEnvironment > /MyDevice** where **<AirWatchEnvironment >** is the enrollment URL. For more information, see Direct Users to Self-Register.

- **How to Authenticate into the Self-Service Portal** – End users need the Group ID, user name, and password to log in to the Self-Service Portal (SSP).

Direct Users to Self-Register

Once the end user receives the registration message, they can register their own devices to save time.

Include these instructions in the registration message you send to end-users, and they will be given what they need to register their own devices.

Procedure

1 Navigate to the Self-Service Portal (SSP) URL: **https://<AirWatchEnvironment > /MyDevice**, where <AirWatchEnvironment> is the enrollment URL for your environment.

2 Log in by entering the **Group ID** and credentials (either an email address or user name and password).

These credentials can match the directory service credentials for directory users.

3 Select **Add Device** to open the **Register Device** form.

4 Enter the device information by completing the required text boxes in the **Register Device** form.

5 Select **Save** to submit and register the device.

Tracking Device Enrollment Status

Occasionally, you might need to troubleshoot device registration, or track the stage of the overall enrollment process. End users might accidentally delete the message containing registration instructions, or they might not redeem an authentication within the allotted expiration time.

Manage enrollment status by accessing the Enrollment Status page at **Devices > Lifecycle > Enrollment Status**. Track the enrollment status of devices by sorting the **Enrollment Status** column in the listing or by filtering the list view by **Enrollment Status**.

Using the Enrollment Status page, you can produce a custom list of registered (but unenrolled) devices, select all devices in this custom list, and resend the enrollment instructions. If enough time elapses and a device fails to enroll, you can opt to reset (or even revoke) their registration token.

For more information, see Enrollment Status.

Enable Registration Tokens and Create a Default Message

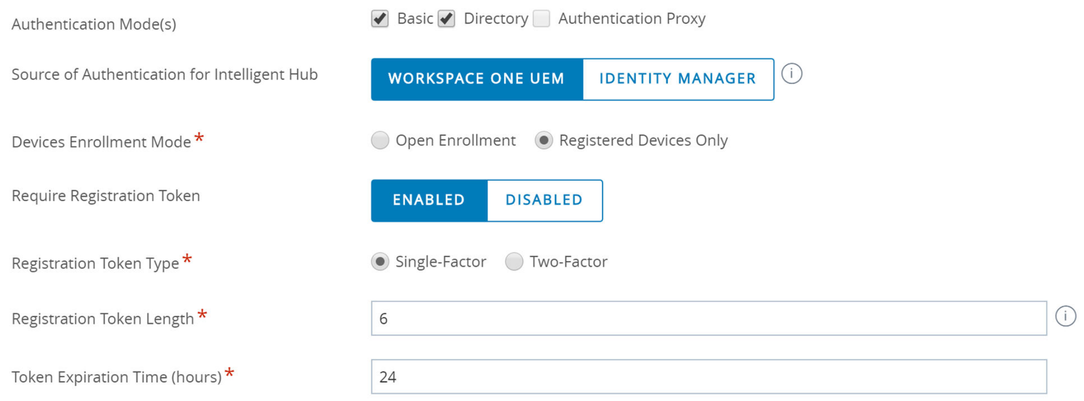
If you restrict an enrollment to registered devices only, you also have the option of requiring a registration token. This option increases security by confirming that a particular user is authorized to enroll.

You can also send an email or SMS message with the enrollment token attached to users with Workspace ONE ™ UEM accounts.

Procedure

1. Enable a token-based enrollment by selecting the appropriate organization group. Navigate to **Devices > Device Settings > Devices & Users > General > Enrollment** and ensure that the **Authentication** tab is selected.
2. Scroll down past the **Getting Started** section and select **Registered Devices Only** as the **Devices Enrollment Mode**.

   A toggle labeled **Require Registration Token** appears. Enabling this option restricts enrollment to only token-registered devices.



Authentication Mode(s) ☑ Basic ☑ Directory ☐ Authentication Proxy

Source of Authentication for Intelligent Hub [✓ WORKSPACE ONE UEM] IDENTITY MANAGER

Devices Enrollment Mode* ○ Open Enrollment ● Registered Devices Only

Require Registration Token [✓ ENABLED] DISABLED

Registration Token Type* ● Single-Factor ○ Two-Factor

Registration Token Length* 6

Token Expiration Time (hours)* 24

3. Select a **Registration Token Type**.
   - **Single-Factor** – The token is all that is required to enroll.
   - **Two-Factor** – A token and login with user credentials are required to enroll.
4. Set the **Registration Token Length**.

   This required setting denotes how complex the Registration Token is and must contain a value between 6–20 alphanumeric characters in length.
5. Set the **Token Expiration Time** (in hours).

   This required setting is the amount of time an end user must select a link and enroll. Once it expires, you must send another link.

Generate a Token with the UEM Console

You can use the UEM Console to generate and send a registration token, which is a highly secure method of enrolling a mobile device.

Procedure

1. Navigate to **Accounts > Users > List View** and select **Edit User** for a user.

   This process also works with creating users.

   The Add / Edit User page displays.

2 Scroll down and select a **Message Type.**

   - **Email** for directory users
   - **SMS** for basic user accounts

3 Select a **Message Template**. Next, select **Save and Add Device**.

   You can use the default template or create a template by selecting the link underneath that opens the **Message Template** page in a new tab.

   The **Add Device** screen displays.

4 Review **General** information about the device and confirming information about the **Message** itself. Once finished, select **Save** to send the token to the user using the selected message type.

Results

Note The token is not accessible through the UEM console for security.

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

You can use the Self Service Portal to generate and send a registration token, which can then be used to securely enroll a device.

Procedure

1 Log in to the Self-Service Portal.

   If you are using single sign-on or smartcards for authentication, you can log in from a device or a computer. Directory users can log in using their directory service credentials.

2 Select **Add Device**.

3 Enter the device information (friendly name and platform) and any other details by completing the settings in the **Register Device** form. Ensure that the email address and phone number are present and accurate as they might not automatically populate.

4 Select **Save** to send the enrollment token to the user using the selected message type.

Results

Note The token is not shown on this page and only appears in the message that is sent.

As a security feature, the following changes have been made for accounts that have enrolled with a token.

- Email Address and Phone Number on both the **Add Device** screen and **Account** screen have been made read-only.
- The View Enrollment Message action has been removed.

Perform Enrollment with a Registration Token

You can use a registration token to enroll a device which is a highly secure authentication method.

Procedure

1. Open the SMS or email message on the device and select the link that contains the enrollment token. If an enrollment page prompts for a Group ID or token, enter the token directly.
2. Enter a user name or password if two-factor authentication is used.
3. Continue with your enrollment as usual.

   Once complete, the device is associated with the user for which the token was created.

What to do next

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

Configure Enrollment Options

Customize your enrollment workflow by incorporating advanced options available in the Workspace ONE UEM console. Access more enrollment options by navigating to **Devices > Devices Settings > Devices & Users > General > Enrollment**.

Getting Started

Setting	Description
Add Email Domain	This button is used for setting up the Auto-Discovery Service to register email domains to your environment.
Authentication Mode(s)	Select the allowed authentication types, which include: ■ **Basic** – Basic user accounts (ones you create manually in the UEM console) can enroll. ■ **Directory** – Directory user accounts (ones that you have imported or allowed using directory service integration) can enroll. Workspace ONE Direct Enrollment supports Directory users with or without SAML. ■ **Authentication Proxy** – Allows users to enroll using Authentication Proxy user accounts. Users authenticate to a web endpoint. ■ Enter **Authentication Proxy URL**, **Authentication Proxy URL Backup**, and **Authentication Method Type** (choose between HTTP Basic and Exchange ActiveSync).
Source of Authentication for Intelligent Hub	Select the system the Intelligent Hub service uses as its source for users and authentication policies. ■ **Workspace ONE UEM** - Select this setting if you want Hub Services to use Workspace ONE UEM as the source. When you configured the **Hub Configuration** page for Hub Services, you entered the Hub Services tenant URL. ■ **Identity Manager** - Select this setting if you want Hub Services to use VMware Identity Manager as the source. When you configured the **Hub Configuration** page for Hub Services, you entered the VMware Identity Manager tenant URL.

Setting	Description
Devices Enrollment Mode	Select the preferred device enrollment mode, which includes: ■ **Open Enrollment** – Essentially allows anyone meeting the other enrollment criteria (authentication mode, restrictions, and so on) to enroll. Workspace ONE Direct Enrollment supports open enrollment. ■ **Registered Devices Only** – Only allowed users to enroll using devices you or they have registered. Device registration is the process of adding corporate devices to the UEM console before they are enrolled. For more information on registering devices, refer to the Enrollment section of the **VMware Workspace ONE UEM Mobile Device Management Guide**. Workspace ONE Direct Enrollment supports allowing only registered devices to enroll but only if registration tokens are not required.
Require Registration Token	Visible only when **Registered Devices Only** is selected. If you restrict enrollment to registered devices only, you also have the option of requiring a registration token to be used for enrollment. This increases security by confirming that a particular user is authorized to enroll. You can send an email or SMS message with the enrollment token attached to users with Workspace ONE UEM accounts.
Require Intelligent Hub Enrollment for iOS	Select this check box to require iOS device users to download and install the Workspace ONE Intelligent Hub before they can enroll. If disabled, Web Enrollment is available.
Require Intelligent Hub Enrollment for macOS	Select this check box to require macOS device users to download and install the Workspace ONE Intelligent Hub before they can enroll. If disabled, Web Enrollment is available.

In addition to the Authentication and Terms of Use tabs, you may optionally complete the following enrollment tabs.

1. Configure Enrollment Options on Grouping Tab.
2. Configure Enrollment Restriction Settings.
3. Configure Enrollment Options on Optional Prompt Tab.
4. Configure Enrollment Options on Customization Tab.

Configure Enrollment Options on Terms of Use

The Terms of Use tab allows you to add and review terms of use as it pertains to enrollment. The Terms of Use tab can be found by navigating to **Devices > Device Settings > Devices & Users > General > Enrollment.**

Setting	Description
Require Enrollment Terms of Use Acceptance	Enable this setting to require the acceptance of a terms of use agreement at enrollment time.
Add New Enrollment Terms of Use	Select to initiate the addition of a terms of use agreement for enrollment purposes.

Important If you enable **Require Enrollment Terms of Use Acceptance**, you must create a Terms of Use or Windows Desktop devices may fail to enroll.

Configure Enrollment Options on Grouping Tab

The Grouping tab allows you to view and specify basic information regarding organization groups and Group IDs for end users. Enable **Group ID Assignment Mode** to select how the Workspace ONE UEM environment assigns Group IDs to users.

The Grouping tab can be found by navigating to **Devices > Device Settings > Devices & Users > General > Enrollment**.

Setting	Description
Group ID Assignment Mode	Workspace ONE Direct Enrollment supports all assignment modes. ■ **Default** - Select this option if users are provided with Group IDs for enrollment. The Group ID used determines what organization group the user is assigned to. ■ **Prompt User to Select Group ID** - Enable this option to allow directory service users to select a Group ID from a list upon enrollment. The **Group ID Assignment** section lists available organization groups and their associated Group IDs. This listing does not require you to perform group assignment mapping, but does mean users have the potential to select an incorrect Group ID. ■ **Automatically Select Based on User Group** - This option only applies if you are integrating with user groups. Enable this option to ensure that users are automatically assigned to organization groups based on their directory service group assignments. The **Group Assignment Settings** section lists all the organization groups for the environment and their associated directory service user groups. Select the **Edit Group Assignment** button to modify the organization group/user group associations and set the rank of precedence each group has. For example, you have three groups, Executive, Sales, and Global, which are ranked in order of job role. Everyone is a member of Global, so if you were to rank that user group first, it puts all your users into a single organization group. Instead, if you rank Executives first, you ensure the small number of people belonging to that group are placed in their own organization group. Then rank Sales second, and you ensure that all Sales employees are placed in an organization group specific to sales. Rank Global last and anyone not already assigned to a group is placed in a separate organization group.

Table 2-1. Default

Setting	Description
Default Device Ownership	Select the default Device Ownership of devices enrollment into the current organization group. Workspace ONE Direct Enrollment supports setting a default device ownership.
Default Role	Select the default roles assigned to users at the current organization group, which can affect access to the Self-Service Portal. 1 **Full Access** - Grants users with access to higher SSP functions such as install/remove profiles and apps, reset passcodes, send device messages, and write-access to content. 2 **Basic Access** - Grants users with a low impact access. They can register their own device, view-only (but not install) profiles and apps, view their own account, and query and find their own device. 3 **External Access** - Users with External Access have all the abilities as basic access users but they also have read-only access to content on the SSP that is explicitly shared with them. Workspace ONE Direct Enrollment supports setting a default role.
Default Action for Inactive Users	Select the default action that impacts Active Directory users if their devices become inactive. Workspace ONE Direct Enrollment supports setting a default action for inactive users.

Table 2-2. User Group Sync

Setting	Description
Sync User Groups in Real Time for Workspace ONE	Workspace ONE can sync user groups for a given user as they register with the UEM console. Enabled by default, this feature is most effective when user groups are being used with great frequency for app assignment, profile assignment, policy assignment, or user mapping. This feature is CPU-intensive so unless your use case is similar to the above, disable this setting for improved performance and to prevent latency issues while launching the Workspace ONE application.

Table 2-3. User Role Mapping

Setting	Description
Enable Directory Group-Based Mapping	Select this box to enable ranked assignments that link a directory user group to a specific Workspace ONE UEM role. Users belonging to a particular group are assigned the associated roles. If they belong to more than one group, they take the highest ranked pairing. You can edit the order in which role-infused user groups are ranked by selecting the **Edit assignment** button. Workspace ONE Direct Enrollment supports directory group-based mapping.

Configure Enrollment Options on Optional Prompt Tab

On the **Optional Prompt** tab, you can decide to request extra device information, or present optional messages regarding enrollment and MDM information to the user.

The Optional Prompt tab can be found by navigating to **Devices > Device Settings > Devices & Users > General > Enrollment**.

Setting	Description
Prompt for Device Ownership Type	You can prompt the end user to select their device ownership type. Otherwise, configure a default device ownership type for the current organization group. Workspace ONE Direct Enrollment supports prompting for device ownership type.
Display Welcome Message	You can display a welcome message for your users early in the device enrollment process. You can configure both the header and the body of this welcome message by navigating to **System > Localization > Localization Editor**. Next, select the labels 'EnrollmentWelcomeMessageHeader' and 'EnrollmentWelcomeMessageBody' respectively.
Display MDM Installation Message	You can display a message for your users during the device enrollment process. You can configure both the header and the body of this MDM installation message by navigating to **System > Localization > Localization Editor**. Next, select the labels 'EnrollmentMdmInstallationMessageHeader' and 'EnrollmentMdmInstallationMessageBody' respectively. If you opt to customize your own header and body messages using the Localization Editor, you must opt to 'Override' in the **Current Setting** option. Doing so ensures that your customizations are used instead of the default messages. In addition to making one-off localization changes, you can also make localization changes in bulk by uploading an edited comma-separated values (CSV) file. Download this localization template CSV file by navigating to **System > Localization > Localization Editor** and select the **Modify** button. Edit the file per your preferences to affect bulk localization changes and upload it using the same screen.

Setting	Description
Enable Enrollment Email Prompt	You can prompt the user to enter their email credentials during enrollment. The Enrollment Email Prompt requests the email address from the end user to populate that option in the user record automatically. This data is beneficial to organizations deploying email to devices using the {EmailAddress} lookup value.
Enable Device Asset Number Prompt	You can prompt the user to enter the device asset number during enrollment. Workspace ONE Direct Enrollment supports enrollment email prompts but only when **Prompt for Device Ownership Type** is enabled and only for Corporate Owned devices.
Display Enrollment Transition Messages (Android Only)	You can display or hide enrollment messages on Android devices.
Enable TLS Mutual Auth for Windows	You can force Windows Phone and Windows Devices to use endpoints secured by TLS Mutual Authentication which requires an extra setup and configuration. Contact Support for assistance.

Create a Custom Enrollment Message

You can customize messages related to enrollment of a device and any future Mobile Device Management (MDM) prompts sent to a device.

While strictly optional, customized messages are often preferred over the default messages. It reduces confusion among your users because it shows a specific organization name in notifications rather than an environment URL or simply "Workspace ONE UEM".

Procedure

1. Navigate to **Devices > Device Settings > General > Enrollment** and select the **Customization** tab.
2. Select **Use specific Message Template for each Platform** and select a device activation message template from the drop-down for each platform.

   See Create Message Templates.
3. For iOS devices, optionally configure the following.
   a. Enter a **post-enrollment landing URL** for iOS devices.
   b. Enter an **MDM Profile message** for iOS devices, which is the message displayed in the install prompt for the MDM profile upon enrollment.
4. Select **Save**.

Create Message Templates

You can create your own library of message templates customized by platform to cover the variety of scenarios you might encounter including enrollment.

Procedure

1. Navigate to **Devices > Device Settings > General > Message Templates** and select **Add**.

2 Set the **Category** drop-down menu to match the category of your template. Options include **Administrator**, **Application**, **Compliance**, **Content**, **Device Lifecycle**, **Enrollment**, and **Terms of Use**.

3 Set the **Type** that best corresponds to the subcategory.

   The **Type** drop-down menu's options depend upon the **Category** setting.

4 Set the **Select Language** drop-down menu. Select the **Add** button to add languages.

5 Select the **Default** check box if you want the template to be the default template for the selected **Category**.

6 Select the **Message Type** for the template.

   The options are **Email**, **SMS**, and **Push** notification.

7 Compose your **Email** message by entering text to the **Message Body** text box.

   - The **Plain Text** option features only a monospaced serif font (Courier) with no formatting options.
   - The **HTML** option enables a **Rich Text** editing environment including fonts, formatting, heading levels, bullets, indentation, paragraph justification, subscript, superscript, image, and hyperlink capability. The HTML environment supports basic HTML coding using the **Show Source** button which you can use to toggle between the **Rich Text** and source views.

8 Save your template by selecting the **Save** button.

Configure Lifecycle Notifications

Lifecycle Notifications enable you to deliver customized messages after specific events during the lifecycle of a device, including enrollment and unenrollment.

This optional setting can be configured by navigating to **Devices > Lifecycle > Settings > Notifications** and entering the following options for the following sections.

- **Device Unenrolled** - Send an email notification when a device unenrolls.
- **Device Enrolled Successfully** - Send an email notification when a device enrolls successfully.
- **Device Blocked by Enrollment Restriction** - Send an email notification if an enrollment restriction blocks a device. You can configure this behavior by navigating to **Groups & Settings > All Settings > Devices & Users > General > Enrollment** and selecting the **Restrictions** tab.

Setting	Description
Send Email To.	■ **None** - Send no confirmation email upon a successful device block, enrollment, or unenrollment. ■ **User** - Send a confirmation email to the device user informing them of the successful device block, enrollment, or unenrollment. ■ **CC** - Send the same confirmation email to a single email address or multiple, comma-separated email addresses. ■ **Message Template**- Select the desired message template from the drop-down listing. You can add a new message template or edit an existing template by selecting the "Click here..." hyperlink that takes you to the **Devices & Users > General > Message Templates** settings page. ■ **Administrator** - Send a confirmation email to the Workspace ONE UEM administrator informing them of the successful device block, enrollment, or unenrollment. ■ **To** - Send the same confirmation email to a single email address or multiple, comma-separated email addresses.

Configure Enrollment Options on Customization Tab

You can provide an extra level of end-user support, including email and phone number, by configuring the **Customization** tab. Such a support level is valuable when users are unable to enroll their device for any reason.

The Customization tab can be found by navigating to **Devices > Device Settings > Devices & Users > General > Enrollment**.

Setting	Description
Use specific Message Template for each Platform	If enabled, you can select a unique message template for each platform. The provided link displays the Message Template page, allowing you to begin creating templates immediately. Workspace ONE ™ Direct Enrollment supports platform-specific message templates.
Enrollment Support Email	Enter the support email address.
Enrollment Support Phone	Enter the support phone number.
Post-Enrollment Landing URL (iOS only)	You can provide a post-enrollment landing URL that the end user is brought to upon a successful enrollment. This URL can be a company resource, such as a company website or login screen leading to more resources. Workspace ONE Direct Enrollment supports post-enrollment landing URLs.
MDM Profile Message (iOS only)	For iOS devices only, this text box is for a message that appears during enrollment. You can specify a message with a maximum of 255 characters. Workspace ONE Direct Enrollment supports iOS-only MDM profile messages.
Use Custom MDM Applications	Displays a link which opens the App Groups Listing page. This link is labeled **Application Groups**. Workspace ONE Direct Enrollment supports custom MDM apps.

Blacklisting and Whitelisting Device Registration

A blacklist is an explicit listing of devices or apps that are not allowed. A whitelist is a listing of devices or apps that are only allowed. Apply this concept to registration and you can control which devices are allowed to enroll in Workspace ONE UEM powered by AirWatch.

For example, in a deployment of only corporate-owned devices, you can create a whitelist of approved iOS devices. You can base this list of devices by International Mobile Equipment Identity (IMEI), Serial Number, or Unique Device Identifier (UDID). This way, enrollment is restricted to only those devices you have identified and enrollment by employee personal devices can be prohibited.

In addition, if a device is lost or stolen, you can add its IMEI, Serial Number, or UDID information to a list of blacklisted devices. Blacklisting a device unenrolls the device, removes all MDM profiles, and prevents enrollment until you remove the blacklist.

A user's registration record is updated with the device information after enrollment. When the device is unenrolled, any other user trying to enroll the same device is blocked from enrollment until the registration record for the previous user is deleted.

Note Current Microsoft functionality dictates that you cannot blacklist Windows Phone devices by IMEI or UDID.

Add a Blacklisted or Whitelisted Device

You can add a blacklisted (device restricted from enrollment) or whitelisted (device cleared for enrollment) based on various device attributes.

Procedure

1 Navigate to **Devices > Lifecycle > Enrollment Status** and select **Add**.

2 Select **Blacklisted Devices** or **Whitelisted Devices** from the **Add** drop-down menu and complete the settings.

Setting	Description
Blacklisted/Whitelisted Devices	Enter the list of whitelisted or blacklisted devices (by the Device Attribute selection), up to 30 at a time.
Device Attribute	Select the corresponding device attribute type. Select IMEI, Serial Number, or UDID.
Organization Group	Confirm to which Organization Group the devices are blacklisted or whitelisted.
Ownership	You can allow devices only with the selected ownership type. This option is only available while Whitelisting devices.
Additional Information	Allows you to select a platform to apply your whitelist or blacklist.
Platform	You can blacklist or whitelist all devices belonging to an entire platform. This option is only available when the **Additional Information** check box is enabled.

3 Select **Save** to confirm the settings.

Additional Enrollment Restrictions

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

You can also determine the maximum number of enrolled devices per organization group. Once you configure enrollment restrictions, you can even save those restrictions as a policy.

Enrollment Considerations, Additional Restrictions

Enrollment restrictions let you fine-tune the enrollment parameters you want to apply to your deployment. When deciding which enrollment restrictions you might use, consider the following.

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

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

Your organization must evaluate the number and kinds of devices your employees own. They must also determine which ones they want to use in your work environment. After this work is complete, you can save these enrollment restrictions as a policy.

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

Additional registration options provide control of the devices that end users are allowed to enroll. Useful to accommodate BYOD deployments, you can prevent the enrollment of blacklisted devices or restrict the enrollment to only whitelisted devices. You can whitelist devices by type, platform, or specific device IDs and serial numbers. For more information, see Add a Blacklisted or Whitelisted Device.

Consideration #3: Will You Restrict the Number of Enrolled Devices Per Organization Group?

You can apply a limit on the number of enrolled devices to an organization group (OG). Imposing such a limit helps you manage your deployment by preventing you from exceeding the number of valid enrollments. For more information, see Enrolled Device Limit Per Organization Group.

Configure Enrollment Restriction Settings

When integrating Workspace ONE UEM with directory services, you can determine which users can enroll devices into your corporate deployment.

You can restrict enrollment to only known users or to configured groups. Known users are users that exist in the UEM console. Configured groups are users associated to directory service groups if you opt to integrate with user groups. You can also limit the number of devices enrolled per organization group and save restrictions as a reusable policy.

These options are available by navigating to **Groups & Settings > All Settings > Devices & Users > General > Enrollment** and selecting the **Restrictions** tab. The Restrictions tab allows you to customize enrollment restriction policies by organization group and user group roles.

- Create and assign existing enrollment Restrictions policies using the Policy Settings.
- Assign the policy to a user group under the Group Assignment Settings area.
- Blacklist or whitelist devices by platform, operating system, UDID, IMEI, and so on.

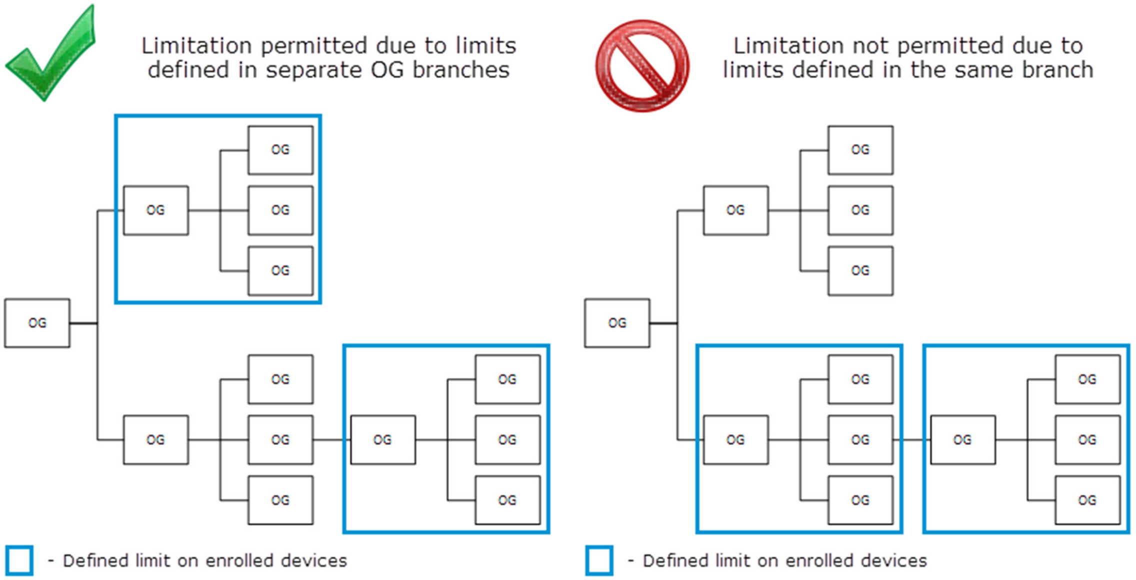
Setting	Description
User Access Control	Workspace ONE Direct Enrollment supports all user access control options. **Restrict Enrollment to Known Users** – Enable to restrict enrollment only to users that exist in the UEM console. This restriction applies to directory users you manually added to the UEM console one by one or through batch import. It can also be used to lock down enrollment after an initial deployment that allowed anyone to enroll. This option enables you to be selective about who can enroll. You can allow all directory users who do not have accounts in the UEM console to enroll into Workspace ONE UEM by disabling this option. User accounts are automatically created during enrollment. **Restrict Enrollment to Configured Groups** – Enable to restrict enrollment and only allow users belonging to All Groups or Selected Groups (if you have integrated with user groups) to enroll devices. Do not select this option if you have not integrated with your directory services user groups. You can create Workspace ONE UEM user accounts during enrollment by disabling the option to allow all directory users to enroll. Select **Enterprise Wipe devices of users that are removed from configured groups** to automatically enterprise wipe devices. If **All Groups** is selected, devices not belonging to any user group are removed. If **Selected Groups** is selected, then devices not belonging to a particular user group are removed. One option for integrating with user groups is to create an "MDM Approved" directory service group and import it to Workspace ONE UEM. After this import step, you can add existing directory service user groups to the "MDM Approved" group as they become eligible for Workspace ONE UEM.
Set limit for maximum enrolled devices at this OG and below	Enable and **Enter Device Limit** to limit the number of devices allowed to enroll in the current organization group (OG). Workspace ONE Direct Enrollment supports this option.

Note Restrictions do not apply for iOS devices enrolled through Apple's Device Enrollment Program (DEP), because the required device information is only received after the device has been enrolled.

Enrolled Device Limit Per Organization Group

You can apply a limit on the number of enrolled devices to an organization group (OG). Imposing such a limit helps you manage your deployment by preventing you from exceeding the number of valid enrollments.

This device limit can be placed on any type of OG (global, customer, partner). Once a limit is set at one OG, you are unable to set another limit anywhere in the same OG branch. You can set another enrolled device limit but only if you are setting it in a separate OG branch.


Limitation permitted due to limits defined in separate OG branches
Limitation not permitted due to limits defined in the same branch
OG
□ - Defined limit on enrolled devices
□ - Defined limit on enrolled devices

Limit the Number of Enrolled Devices Per Organization Group

Limiting the number of enrolled devices per organization group can be an effective way of managing the number of licenses in a per-device licensing environment.

If this option is unavailable, check the parent OG (higher than the current OG) or a child OG (lower than the current OG). It is likely that an existing limit has already been defined above or below your current OG.

Procedure

1 Navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment** and select the **Restrictions** tab.

2 Enable the limit under **Set a limit for maximum enrolled devices at this Organization Group and below**.

Create an Enrollment Restriction Policy

Your organization must evaluate the number and kinds of devices your employees own. They must also determine which devices to use in your work environment. After this work is complete, you can save these enrollment restrictions as a policy.

Procedure

1 Navigate to **Devices > Device Settings > Devices & Users > General > Enrollment**.

2 Select the **Restrictions** tab and then select **Add Policy** located in the **Policy Settings** section.

3 In the **Add/Edit Enrollment Restriction Policy** screen, add an enrollment restriction policy.

Setting	Description
Enrollment Restriction Policy Name	Enter a name for your enrollment restriction policy.
OrganizationGroup	Select an organization group from the drop-down menu. This is the OG to which your new enrollment restriction policy applies.
Policy Type	Select the type of enrollment restriction policy, which can be either **Organization Group Default** to apply to the selected organization group, or **User Group Policy** for specific User Groups through Group Assignment Settings on the **Restrictions** tab.
AllowedOwnership Types	Select whether to permit or prevent **Corporate - Dedicated**, **Corporate - Shared**, and **Employee Owned** devices. Workspace ONE Direct Enrollment only supports the ownership types Corporate Dedicated and Employee Owned.
AllowedEnrollment Types	Select whether to permit or prevent the enrollment of devices using **MDM** (Workspace ONE Intelligent Hub) and AirWatch **Container** (for iOS/Android) apps.
Device Limit per User	Select **Unlimited** to allow users to enroll as many devices as they want. Workspace ONE Direct Enrollment supports setting a device limit per user. Deselect this box to enter values for the **Device Limit Per User** section, to define the maximum number of devices per ownership type. ■ **Maximum Devices Per User** ■ **Corporate Max Devices** ■ **Shared Max Devices** ■ **Employee Owned Max Devices**
Allowed DeviceTypes	Select the **Limit enrollment to specific platforms, models or operating systems** check box to add additional device-specific restrictions. This option is supported by Workspace ONE Direct Enrollment. **Note** Current Microsoft functionality dictates that you cannot blacklist Windows Phone devices by IMEI or UDID.
Device Level Restrictions Mode	This option is only available if **Limit enrollment to specific platforms, models or operating systems** is selected in the **Allowed Device Types** option. Determine the kind of device limitations you should have. ■ **Only allow listed device types (Whitelist)** – Select this option to explicitly allow only devices matching the parameters you enter and to block everything else. ■ **Block listed device types (Blacklist)** – Select this option to explicitly block devices matching the parameters you enter and to allow everything else. For either device-level restrictions mode, select **Add Device Restriction** to choose a **Platform**, **Model**, **Manufacturer** (specific to Android devices), or **Operating System**. You may also add a **Device Limit** per defined device restriction. You may add multiple device restrictions. You can also block specific devices based on their IMEI, Serial Number or UDID by navigating to **Devices > Lifecycle > Enrollment Status** and selecting **Add**. This is an effective way to block a single device and prevent it from re-enrolling without affecting other users' devices. Preventing re-enrollment is also available as an option when performing an Enterprise Wipe. This option is supported by Workspace ONE Direct Enrollment.

4 Select **Save** to save your changes and navigate back to the **Devices & Users / General / Enrollment** screen.

Reasons You Should Not Enroll Devices in Global

There are several reasons enrolling devices directly to the top-level organization group (OG), commonly known as Global, is not a good idea. These reasons are multitenancy, inheritance, and functionality.

Multitenancy

You can make as many child organization groups as you need and you configure each one independently from the others. Settings you apply to a child OG do not impact other siblings.

Inheritance

Changes made to a parent level OG apply to the children. Conversely, changes made to a child level OG do not apply to the parent or siblings.

Functionality

There are settings and functionality that are only configurable to Customer type organization groups. These include wipe protection, telecom, and personal content. Devices added directly to the top-level Global OG are excluded from these settings and functionality.

The Global organization group (OG) is designed to house Customer and other types of OGs. Given the way inheritance works, if you add devices to Global and configure Global with settings intended to affect those devices, you are also affecting all the Customer OGs underneath. This undermines the benefits of multitenancy and inheritance.

Autodiscovery Enrollment

Workspace ONE UEM makes the enrollment process simple, using an autodiscovery system to enroll devices to environments and organization groups (OG) using user email addresses. Autodiscovery can also be used to allow end users to authenticate into the Self-Service Portal (SSP) using their email address.

Note To enable an autodiscovery for on-premises environments, ensure that your environment can communicate with the Workspace ONE UEM Autodiscovery servers.

Registration for Autodiscovery Enrollment

The server checks for an email domain uniqueness, only allowing a domain to be registered at one organization group in one environment. Because of this server check, register your domain at your highest-level organization group.

Autodiscovery is configured automatically for new Software as a Service (SaaS) customers.

Configure Autodiscovery Enrollment from a Parent Organization Group

Autodiscovery Enrollment simplifies the enrollment process enrolling devices to intended environments and organization groups (OG) using end-user email addresses.

Configure an autodiscovery enrollment from a parent OG by taking the following steps.

Procedure

1. Navigate to **Groups & Settings > All Settings > Admin > Cloud Services** and enable the **Auto Discovery** setting. Enter your login email address in **Auto Discovery AirWatch ID** and select **Set Identity**.
   a. If necessary, navigate to https://my.workspaceone.com/set-discovery-password to set the password for Auto Discovery service. Once you have registered and selected **Set Identity**, the **HMAC Token** auto-populates. Click **Test Connection** to ensure that the connection is functional.
2. Enable the **Auto Discovery Certificate Pinning** option to upload your own certificate and pin it to the auto discovery function. You can review the validity dates and other information for existing certificates, and also can **Replace** and **Clear** these existing certificates.
3. Select **Add a certificate** and the settings **Name** and **Certificate** display. Enter the name of the certificate you want to upload, select the **Upload** button, and select the cert on your device.
4. Select **Save** to complete an autodiscovery setup.

What to do next

Instruct end users who enroll themselves to select the email address option for authentication, instead of entering an environment URL and Group ID. When users enroll devices with an email address, they enroll into the same group listed in the **Enrollment Organization Group** of the associated user account.

Configure Autodiscovery Enrollment from a Child Organization Group

You can configure Autodiscovery Enrollment from a child organization group below the enrollment organization group. To enable an autodiscovery enrollment in this way, you must require users to select a Group ID during enrollment.

Force users to select a Group ID during enrollments.

Procedure

1. Navigate to **Devices > Device Settings > General > Enrollment** and select the **Grouping** tab.
2. Select **Prompt User to Select Group ID**.
3. Select **Save**.

User and Admin Accounts

3

You must create and integrate user accounts for devices to enroll into Workspace ONE UEM. Likewise, administrator accounts must be created and assigned so Admins can easily manage users and devices.

The UEM console allows you to establish a complete user and admin infrastructure. It provides configuration options for authentication, enterprise integration, and ongoing maintenance.

This chapter includes the following topics:

User Authentication Types

Before any devices can be enrolled, each device user must have an authentic user account recognized by Workspace ONE UEM. The type of user authentication you select depends upon the needs of your organization.

Basic Authentication

This type of user authentication is independent from any corporate user account system currently available such as Novell, Lotus Domino, or Microsoft Active Directory. As such, credentials only exist within the Workspace ONE UEM architecture. For more information, see Basic User Authentication.

Active Directory LDAP Authentication

Microsoft's Active Directory (AD) Lightweight Directory Access Protocol (LDAP) Authentication is the most commonly used account system. This type of user authentication harnesses and aligns with AD, making it easy for the end user since they only need their corporate login and password.

For more information, see Active Directory with LDAP Authentication and Active Directory with LDAP Authentication and VMware Enterprise Systems Connector.

Additional Authentication Types

There are other types of authentication methods including the use of an authentication proxy, Security Assertion Markup Language (SAML), and the secure and user-friendly token-based authentication.

For more information, see Authentication Proxy, SAML 2.0 Authentication, and Token-Based Authentication.

Enable Security Types for Enrollment

After you have selected the user authentication type, you must enable the authentication mode in the enrollment settings. For more information, see Enable Security Types for Enrollment.

Basic User Authentication

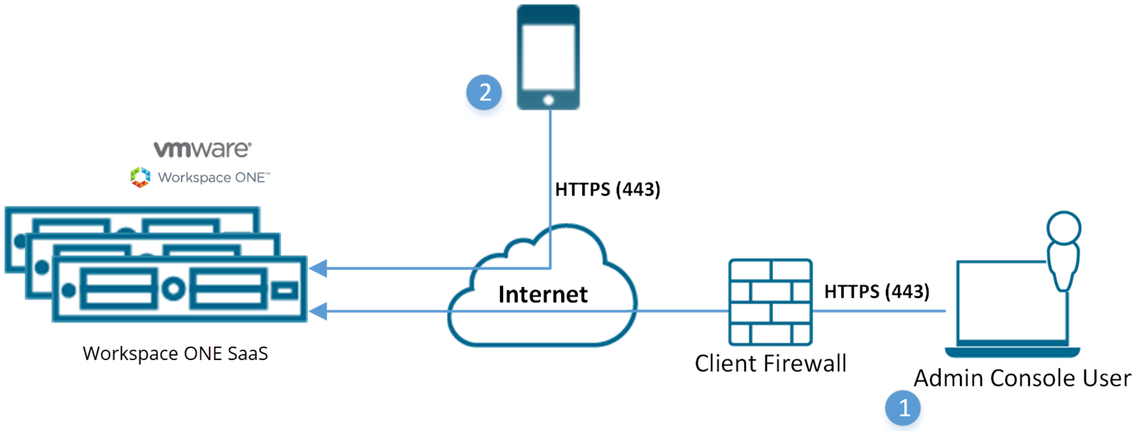
You can use Basic Authentication to identify users in the Workspace ONE UEM architecture but this method offers no integration to existing corporate user accounts.

Pros

- Can be used for any deployment method.
- Requires no technical integration.
- Requires no enterprise infrastructure.

Cons

- Cannot be used with Auto Discovery.
- Credentials only exist in Workspace ONE UEM and do not necessarily match existing corporate credentials.
- Offers no federated security or single sign-on.
- Workspace ONE UEM stores all user name and passwords.
- Cannot be used for Workspace ONE Direct Enrollment.



1 Console user logs in to Workspace ONE UEM SaaS using local account for authentication (Basic Authentication).

   - Credentials are encrypted during transport.
   - (for example, user name: jdoe@air-watch.com, password: abcd).

2 Device user enrolls device using local Workspace ONE UEM account (Basic Authentication) credentials.

   - Credentials are encrypted during transport.
   - (for example, user name: jdoe2, password 2557).

For more information, see Workspace ONE Direct Enrollment.

Active Directory with LDAP Authentication

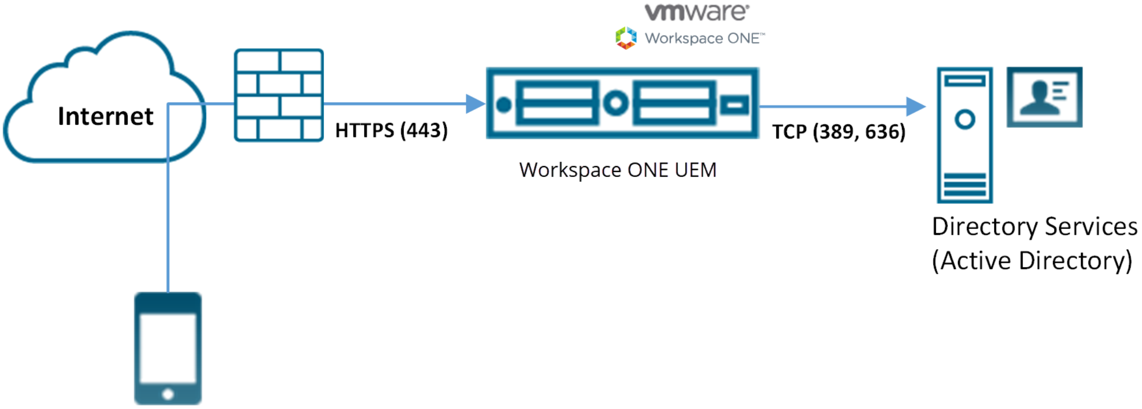
Active Directory (AD) with Lightweight Directory Access Protocol (LDAP) authentication is used to integrate user and admin accounts of Workspace ONE UEM with existing corporate accounts.

Pros

- End users now authenticate with existing corporate credentials.
- Secure method of integrating with LDAP / AD.
- Standard integration practice.
- Can be used for Workspace ONE Direct Enrollment.

Cons

- Requires an AD or other LDAP server.



1 Device connects to Workspace ONE UEM to enroll device. User enters their directory services user name and password.

   - User name and password are encrypted during transport.
   - Workspace ONE UEM does not store the user's directory services password.

2 Workspace ONE UEM queries the client's directory services through a secure LDAP protocol over the Internet using a service account for authentication.

3 The user's credentials are validated against the corporate directory service.

4 If the user credentials are valid, the Workspace ONE UEM server allows the device to complete a device enrollment.

For more information, see Workspace ONE Direct Enrollment.

Active Directory with LDAP Authentication and VMware Enterprise Systems Connector

The Active Directory with LDAP authentication and VMware Enterprise Systems Connector provides the same functionality as traditional AD & LDAP authentication. This model functions across the cloud for Software as a Service (SaaS) deployments.

Pros

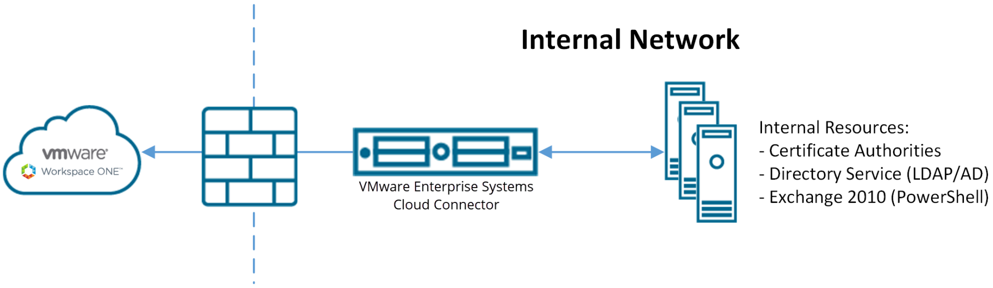
- End users authenticate with existing corporate credentials.
- Requires no firewall changes, as communication is initiated from the VMware Enterprise Systems Connector within your network.
- Transmission of credentials is encrypted and secure.
- Offers secure configuration to other infrastructure such as BES, Microsoft ADCS, SCEP, and SMTP servers.
- Can be used for Workspace ONE ™ Direct Enrollment.

Cons

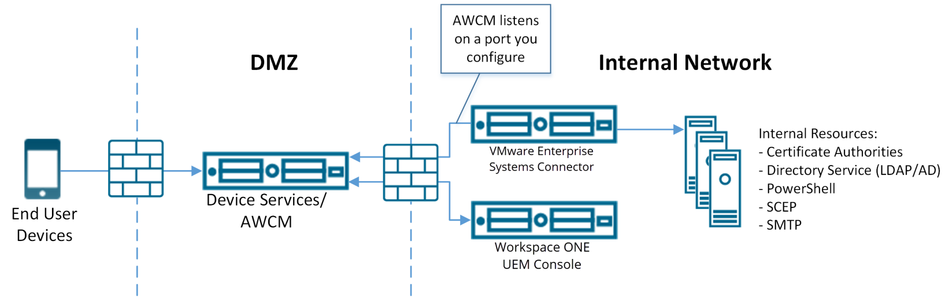
- Requires VMware Enterprise Systems Connector to be installed behind the firewall or in a DMZ.

- Requires extra configuration.

SaaS Deployment Model


Internal Network
vmware Workspace ONE
VMware Enterprise Systems Cloud Connector
Internal Resources:
- Certificate Authorities
- Directory Service (LDAP/AD)
- Exchange 2010 (PowerShell)

On-premises Deployment Model


AWCM listens on a port you configure
DMZ
Internal Network
End User Devices
Device Services/ AWCM
VMware Enterprise Systems Connector
Workspace ONE UEM Console
Internal Resources:
- Certificate Authorities
- Directory Service (LDAP/AD)
- PowerShell
- SCEP
- SMTP

For more information, see Workspace ONE Direct Enrollment.

Authentication Proxy

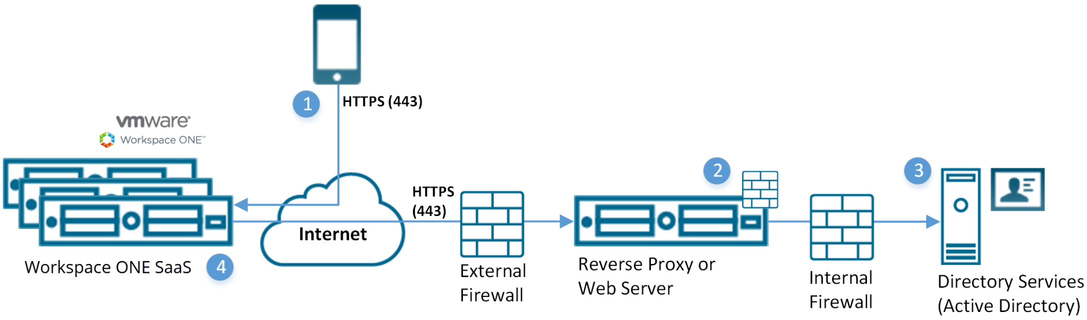
The authentication proxy delivers directory services integration across the cloud or across hardened internal networks. In this model, the Workspace ONE UEM server communicates with a publicly facing Web server or an Exchange ActiveSync Server. This arrangement authenticates users against the domain controller.

Pros

- Offers a secure method to proxy integration with AD/LDAP across the cloud.
- End users can authenticate with existing corporate credentials.
- Lightweight module that requires minimal configuration.

Cons

- Requires a public facing Web server or an Exchange ActiveSync server which ties into an AD/LDAP server.
- Only feasible for specific architecture layouts.
- Much less robust solution than VMware Enterprise Systems Connector.
- Cannot be used for Workspace ONE Direct Enrollment.



1 Device connects to Workspace ONE UEM to enroll device. User enters their directory services user name and password.

   - User name and password are encrypted during transport.
   - Workspace ONE UEM does not store the user's directory services password.

2 Workspace ONE UEM relays the user name and password to a configured Authentication Proxy endpoint that requires authentication (for example, Basic Authentication).

3 The user's credentials are validated against the corporate directory services.

4 If the user credentials are valid, the Workspace ONE UEM server allows the device to complete a device enrollment.

For more information, see Workspace ONE Direct Enrollment.

SAML 2.0 Authentication

The Security Assertion Markup Language (SAML) 2.0 Authentication offers single sign-on support and federated authentication. Workspace ONE UEM never receives any corporate credentials.

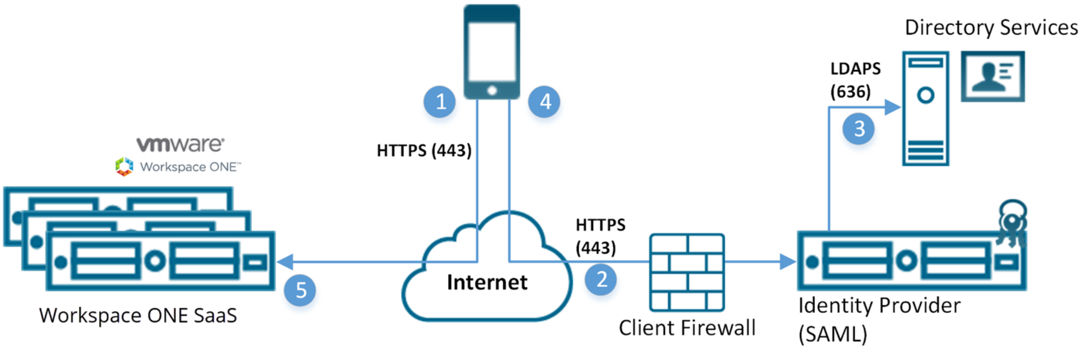
If an organization has a SAML Identity Provider server, use SAML 2.0 integration.

Pros

- Offers single sign-on capabilities.
- Authentication with existing corporate credentials.
- Workspace ONE UEM never receives corporate credentials in plain-text.
- Can be used for Workspace ONE Direct Enrollment when paired with a SAML Directory User.

Cons

- Requires corporate SAML Identity Provider infrastructure.
- Cannot be used for Workspace ONE Direct Enrollment when paired with a SAML Basic User.
- Multi-domain environment is not supported.



1 Device connects to Workspace ONE UEM for enrollment. The UEM server then redirects the device to the client specified identity provider.

2 Device securely connects through HTTPS to client provided identity provider and user enters credentials.

- Credentials are encrypted during transport directly between the device and SAML endpoint.

3 Credentials are validated against directory services.

4 The identity provider returns a signed SAML response with the authenticated user name.

5 The device responds back to the Workspace ONE UEM server and presents the signed SAML message. The user is authenticated.

.

Token-Based Authentication

The Token-based authentication offers the easiest way for a user to enroll their device. With this enrollment setting, Workspace ONE UEM generates a token, which is placed within the enrollment URL.

For **single-token authentication**, the user accesses the link from the device to complete an enrollment and the Workspace ONE UEM server references the token provided to the user.

For added security, set an expiration time (in hours) for each token. Setting an expiration minimizes the potential for another user to gain access to any information and features available to that device.

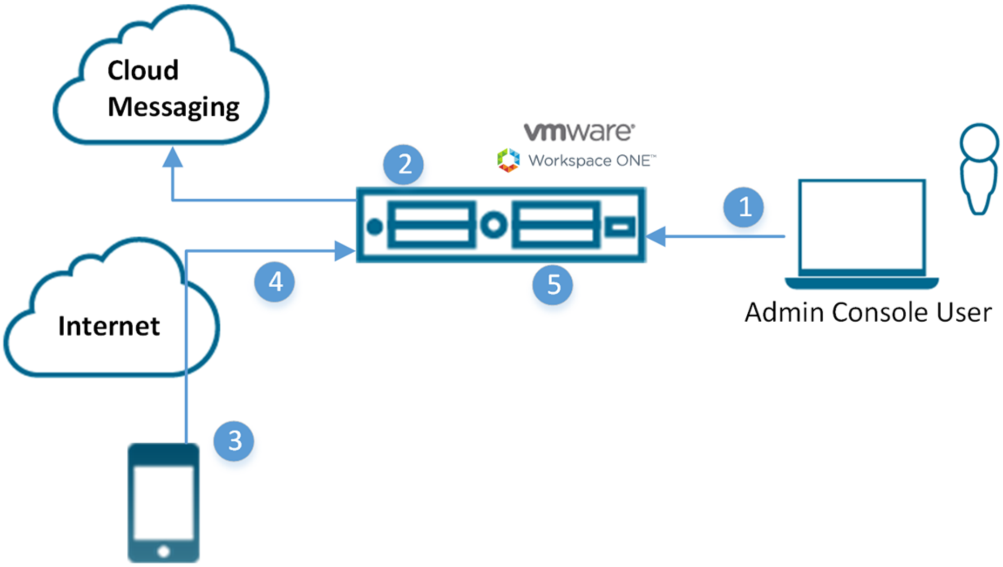
You can also decide to implement two factor authentication to take end-user identity verification a step further. With this authentication setting, the user must enter their user name and password upon accessing the enrollment link with the provided token.

Pros

- Minimal work for an end user to enroll and authenticate their device.
- Secure token use by setting expiration.
- User does not need credentials for single-token authentication.

Cons

- Requires either Simple Mail Transfer Protocol (SMTP) or Short Message Service (SMS) integration to send tokens to device.



1 Administrator authorizes user device registration.

2 Single use token generated and sent to user from Workspace ONE UEM.

3 User receives a token and navigates to enrollment URL. User is prompted for token and optionally two-factor authentication.

4 Device enrollment process.

5 Workspace ONE UEM marks token as expired.

Note SMTP is included with SaaS deployments.

Enable Security Types for Enrollment

Once Workspace ONE UEM is integrated with a selected user security type and before enrollment, enable each authentication mode you plan to allow.

Procedure

1 Navigate to **Devices > Device Settings > Devices & Users > General > Enrollment** in the **Authentication** tab.

2 Select the appropriate check boxes for the **Authentication Mode** setting.

Setting	Description
Add Email Domain	This button is used for setting up the Auto-Discovery Service to register email domains to your environment.
Authentication Mode(s)	Select the allowed authentication types, which include: - **Basic** – Basic user accounts (ones you create manually in the UEM console) can enroll. - **Directory** – Directory user accounts (ones that you have imported or allowed using directory service integration) can enroll. Workspace ONE Direct Enrollment supports Directory users with or without SAML. - **Authentication Proxy** – Allows users to enroll using Authentication Proxy user accounts. Users authenticate to a web endpoint. - Enter **Authentication Proxy URL**, **Authentication Proxy URL Backup**, and **Authentication Method Type** (choose between HTTP Basic and Exchange ActiveSync).
Source of Authentication for Intelligent Hub	Select the system the Intelligent Hub service uses as its source for users and authentication policies. - **Workspace ONE UEM** - Select this setting if you want Hub Services to use Workspace ONE UEM as the source. When you configured the **Hub Configuration** page for Hub Services, you entered the Hub Services tenant URL. - **Identity Manager** - Select this setting if you want Hub Services to use VMware Identity Manager as the source. When you configured the **Hub Configuration** page for Hub Services, you entered the VMware Identity Manager tenant URL.
Devices Enrollment Mode	Select the preferred device enrollment mode, which includes: - **Open Enrollment** – Essentially allows anyone meeting the other enrollment criteria (authentication mode, restrictions, and so on) to enroll. Workspace ONE Direct Enrollment supports open enrollment. - **Registered Devices Only** – Only allowed users to enroll using devices you or they have registered. Device registration is the process of adding corporate devices to the UEM console before they are enrolled. For more information on registering devices, refer to the Enrollment section of the **VMware Workspace ONE UEM Mobile Device Management Guide**. Workspace ONE Direct Enrollment supports allowing only registered devices to enroll but only if registration tokens are not required.
Require Registration Token	Visible only when **Registered Devices Only** is selected. If you restrict enrollment to registered devices only, you also have the option of requiring a registration token to be used for enrollment. This increases security by confirming that a particular user is authorized to enroll. You can send an email or SMS message with the enrollment token attached to users with Workspace ONE UEM accounts.
Require Intelligent Hub Enrollment for iOS	Select this check box to require iOS device users to download and install the Workspace ONE Intelligent Hub before they can enroll. If disabled, Web Enrollment is available.
Require Intelligent Hub Enrollment for macOS	Select this check box to require macOS device users to download and install the Workspace ONE Intelligent Hub before they can enroll. If disabled, Web Enrollment is available.

3 Select **Save**.

Basic User Accounts

Create basic user accounts in Workspace ONE UEM for your end users if you are not integrating with a directory service. Basic user accounts are also useful for testing purposes: they can be created quickly and disposed of afterward.

For more information, see Basic vs. Directory Services Enrollment.

Pros

- Can be used for any deployment method.
- Requires no technical integration.
- Requires no enterprise infrastructure.
- Can enroll into potentially multiple organization groups.

Cons

- Credentials only exist in Workspace ONE UEM and do not necessarily match existing corporate credentials.
- Offers no federated security.
- Single sign on not supported.
- Workspace ONE UEM stores all user names and passwords.
- Cannot be used for Workspace ONE Direct Enrollment.

Create Basic User Accounts

You can create basic user accounts for each user to authenticate and log in to the Workspace ONE UEM system. You can then send basic users a notification with instructions on activating their account including a password reset link that expires in 24 hours.

This topic details creating user accounts one at a time. To create user accounts in bulk, see Batch Import Users or Devices.

Procedure

1 Navigate to **Accounts > Users > List View**, select **Add** then **Add User**. The **Add / Edit User** page displays.

2 In the **General** tab, complete the following settings to add a basic user.

Setting	Description
Security Type	Select **Basic** to add a basic user.
User name	Enter a user name with which the new user is identified.
Password	Enter a password that the user can use to log in.
Confirm Password	Confirm the password.

Setting	Description
Full Name	Complete the **First Name**, **Middle Name**, and **Last Name** of the user.
Display Name	Represent the user in the UEM console by entering a name.
Email Address	Enter or edit the user's email address.
Email user name	Enter or edit the user's email user name.
Domain	Select the email domain from the drop-down setting.
Phone Number	Enter the user's phone number including plus sign, country code, and area code. This option is required if you intend to use SMS to send notifications.
Enrollment	
Enrollment Organization Group	Select the organization group into which the user enrolls.
Allow the user to enroll into additional Organization Groups	You can allow the user to enroll into more than one organization group. If you Enable this option but leave **Additional Organization Groups** blank, then any child OG created under the **Enrollment Organization Group** can be used as a point of enrollment.
Additional Organization Groups	This setting only appears when the option to allow the user to enroll into additional OGs is **Enabled**. This setting allows you to add additional organization groups from which your basic user can enroll.
User Role	Select the role for the user you are adding from this drop-down setting.
Notification	
Message Type	Select the type of message you want to send to the user, **Email**, **SMS**, or **None**. Selecting SMS requires a valid entry in the **Phone Number** option.
Message Template	The basic user activates their account with this notification. For security reasons, this notification does not include the user's password. Instead, a password reset link is included in the notification. The basic user selects this link to define another password. This password reset link expires in 24 hours automatically. Select the template for email or SMS messages by selecting one from this drop-down setting. Optionally, select **Message Preview** to preview the template and select the **Configure Message Template** to create a template.

3 You can optionally select the **Advanced** tab and complete the following settings.

Setting	Description
Advanced Info Section	
Email Password	Enter the email password of the user you are adding.
Confirm Email Password	Confirm the email password of the user you are adding.
User Principal Name	Enter the principal name of the basic user. This setting is optional.
Category	Select the User Category for the user being added.
Department	Enter the user's department for administrative purposes.
Employee ID	Enter the user's employee ID for administrative purposes.
Cost Center	Enter the user's cost center for administrative purposes.
Certificates Section	

Setting	Description
Use S/MIME	Enable or Disable Secure Multipurpose Internet Mail Extensions (S/MIME). If enabled, you must have an S/MIME-enabled profile and you must upload an S/MIME certificate by selecting **Upload**.
Separate Encryption Certificate	Enable or Disable encryption certificate. If enabled, you must upload an encryption certificate using **Upload**. Generally, the same S/MIME certificate is used for signing and encryption, unless a different certificate is expressly being used.
Old Encryption Certificate	Enable or disable a legacy version encryption certificate. If enabled, you must **Upload** an encryption certificate.
Staging Section	
Enable Device Staging	Enable or disable the staging of devices. If enabled, you must select between **Single User Devices** and **Multi User Devices**. If **Single User Devices**, you must select between **Standard**, where users themselves log in and **Advanced**, where a device is enrolled on behalf of another user.

4 Select **Save** to save only the new user or select **Save and Add Device** to save the new user and proceed to the **Add Device** page.

Directory-Based User Accounts

Integrating with an existing directory service enables you to pull in users automatically. It eliminates the need of having to add users manually to the Workspace ONE UEM console.

Every directory user you want to manage through Workspace ONE UEM must have a corresponding user account in the UEM console. For more information, see Basic vs. Directory Services Enrollment.

You can directly add your existing directory services users to Workspace ONE UEM using one of the following methods.

- Batch upload a file containing all your directory services users. The act of batch importing automatically creates a user account.
- Create user accounts one at a time by entering the directory user name and selecting **Check User** to auto-populate remaining details.
- Do not import in bulk nor manually create user accounts and instead allow all directory users to self-enroll at enrollment time.

Pros

- End users authenticate with existing corporate credentials.
- Can automatically detect and sync changes from the directory system into Workspace ONE UEM.
- Secure method of integrating with your existing directory service.
- Standard integration practice.
- Can be used for Workspace ONE Direct Enrollment.

- SaaS deployments using the VMware Enterprise Systems Connector require no firewall changes and offers a secure configuration to other infrastructures, such as Microsoft ADCS, SCEP, and SMTP servers.

Cons

- Requires an existing directory service infrastructure.
- SaaS deployments require additional configuration due to the VMware Enterprise Systems Connector being installed behind the firewall or in a DMZ.

Create a Directory-Based User Account

You must create accounts for each user in the Workspace ONE UEM system and directory users authenticate using your existing corporate credentials.

This topic details creating user accounts one at a time. To create user accounts in bulk, see Batch Import Users or Devices.

Procedure

1. Navigate to **Accounts > Users > List View** and select **Add** and then **Add User**. The **Add / Edit User** page displays.
2. In the **General** tab, complete the following settings to add a directory user.

Setting	Description
Security Type	Add an Active Directory user by choosing **Directory** as the Security Type.
Directory Name	This pre-populated setting identifies the Active Directory name.
Domain	Choose the domain name from the drop-down menu.
User name	Enter the user's directory user name and select **Check User**. If the system finds a match, the user's information is automatically populated. The remaining settings in this section are only available after you have successfully located an active directory user with the **Check User** button.
Full Name	Use **Edit Attributes** to allow any option that syncs a blank value from the directory to be edited. Edit Attributes also enables you to populate matching user's information automatically. If a setting syncs an actual value from the directory, then that setting must be edited in the directory itself. The change takes effect on the next directory sync. Complete any blank option returned from the directory in **Full Name** and select **Edit Attributes** to save the addition.
Display Name	Enter the name that displays in the admin console.
Email Address	Enter or edit the user's email address.
Email user name	Enter or edit the user's email user name.
Domain (email)	Select the email domain from the drop-down menu.
Phone Number	Enter the user's phone number including plus sign, country code, and area code. If you intend to use SMS to send notifications, the phone number is required.
Enrollment	
Enrollment Organization Group	Select the organization group into which the user enrolls.

Setting	Description
Allow the user to enroll into additional Organization Groups	Choose whether or not to allow the user to enroll into more than one organization group. If you select **Enabled**, then complete the **Additional Organization Groups**.
User Role	Select the role for the user you are adding from this drop-down menu.
Notification	
Message Type	Choose the type of message you may send to the user, **Email**, **SMS**, or **None**. Selecting SMS requires a valid entry in the **Phone Number** text box.
Message Template	Choose the template for email or SMS messages from this drop-down setting. Optionally, select the **Message Preview** to preview the template and select the **Configure Message Templates** link to create a template.

3 You may optionally select the **Advanced** tab and complete the following settings.

Setting	Description
Advanced Info Section	
Email Password	Enter the email password of the user you are adding.
Confirm Email Password	Confirm the email password of the user you are adding.
Distinguished Name	For directory users recognized by Workspace ONE UEM, this text box is pre-populated with the distinguished name of the user. Distinguished Name is a string representing the user name and all authorization codes associated with an Active Directory user.
Manager Distinguished Name	Enter the distinguished name of the user's manager. This text box is optional.
Category	Choose the user category for the user being added.
Department	Enter the user's department for your company's administrative purposes.
Employee ID	Enter the user's employee ID for your company's administrative purposes.
Cost Center	Enter the user's cost center for your company's administrative purposes.
Custom Attribute 1–5 (for Directory users only)	Enter your previously configured custom attributes, where applicable. You may define these custom attributes by navigating to **Groups & Settings > All Settings > Devices & Users > Advanced > Custom Attributes**. **Note** Custom attributes can be configured only at Customer organization groups.
Certificates Section	
Use S/MIME	Enable or disable the use of Secure/Multipurpose Internet Mail Extensions (S/MIME). If enabled, you must have an S/MIME-enabled profile and you must upload an S/MIME certificate by selecting **Upload**.
Separate Encryption Certificate	Enable or disable the use of a separate encryption certificate. If enabled, you must upload an encryption certificate using **Upload**. Generally, the same S/MIME certificate is used for signing and encryption, unless a different certificate is expressly being used.
Old Encryption Certificate	Enable or disable a legacy version encryption certificate. If enabled, you must **Upload** an encryption certificate.

Setting	Description
Staging Section	
Enable Device Staging	Enable or disable the staging of devices. If enabled, you must choose between **Single User Devices** and **Multi User Devices**. If **Single User Devices**, you must select between **Standard**, where users themselves log in and **Advanced**, where a device is enrolled on behalf of another user.

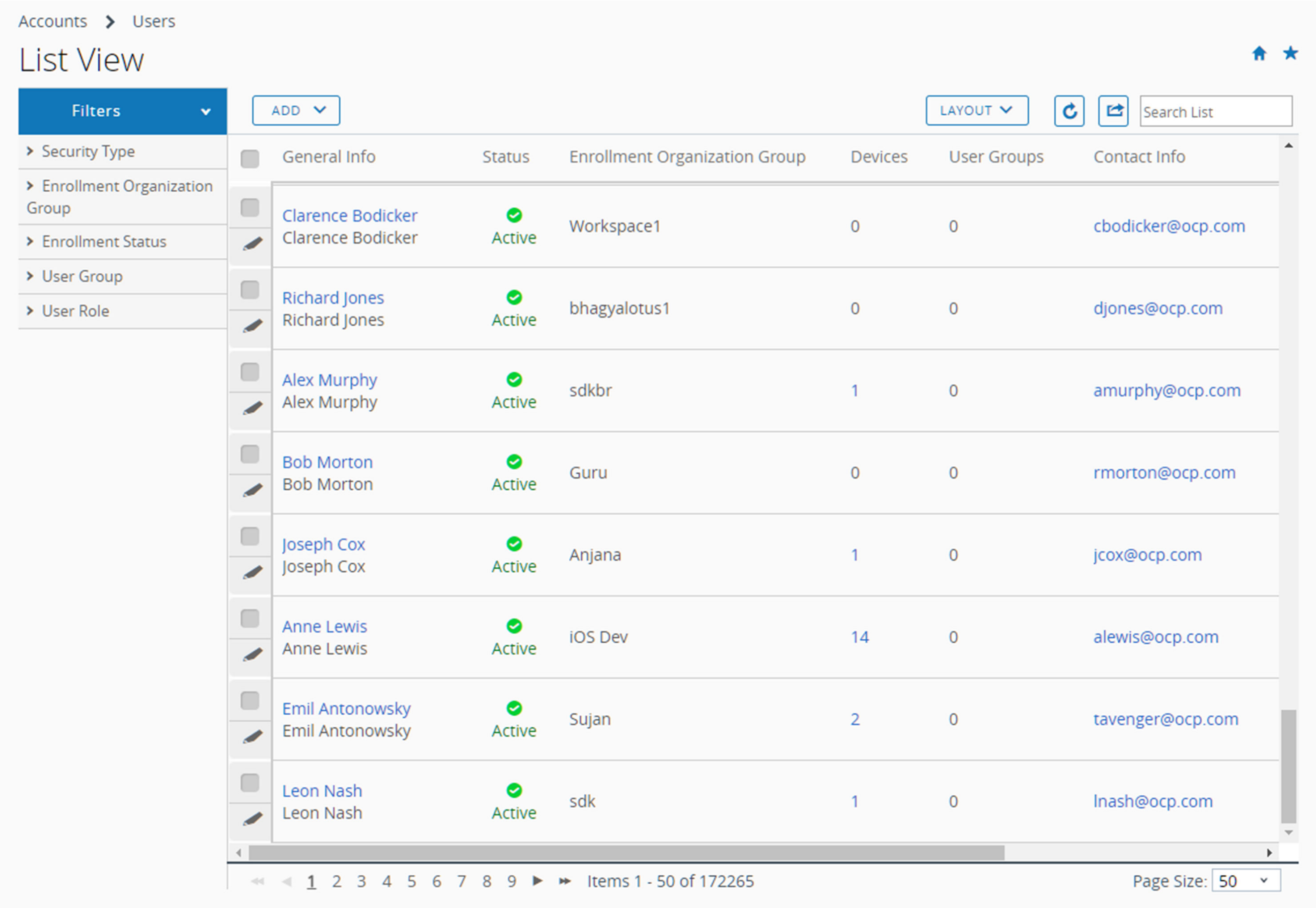
4 Select **Save** to save only the new user or select **Save and Add Device** to save the new user and proceed to the **Add Device** page.

What to do next

For more information about adding directory users to Workspace ONE UEM, see **Add Individual Directory Users One at a Time** and **Batch Import Directory Users**. from the **VMware Workspace ONE UEM Directory Services Documentation** on docs.vmware.com.

User Accounts List View

The **List View** page, which you can find by navigating to **Accounts > Users > List View**, provides useful tools for common user account maintenance and upkeep.



General Info	Status	Enrollment Organization Group	Devices	User Groups	Contact Info
Clarence Bodicker Clarence Bodicker	✓ Active	Workspace1	0	0	cbodicker@ocp.com
Richard Jones Richard Jones	✓ Active	bhagyalotus1	0	0	djones@ocp.com
Alex Murphy Alex Murphy	✓ Active	sdkbr	1	0	amurphy@ocp.com
Bob Morton Bob Morton	✓ Active	Guru	0	0	rmorton@ocp.com
Joseph Cox Joseph Cox	✓ Active	Anjana	1	0	jcox@ocp.com
Anne Lewis Anne Lewis	✓ Active	iOS Dev	14	0	alewis@ocp.com
Emil Antonowsky Emil Antonowsky	✓ Active	Sujan	2	0	tavenger@ocp.com
Leon Nash Leon Nash	✓ Active	sdk	1	0	lnash@ocp.com

1 2 3 4 5 6 7 8 9 Items 1 - 50 of 172265 Page Size: 50

Customize List View

You can use the User Accounts List View to create customized lists of users immediately. You can also customize the screen layout based on criteria that is most important to you. You can export this customized list for later analysis and add new users individually or in bulk.

Action	Description
Filters	View only the desired users by using the following filters. ■ Security Type ■ Enrollment Organization Group ■ Enrollment Status ■ User Group ■ User Role
Add	■ **Add User** – Perform a one-off addition of a basic user account. Add an employee or a newly promoted employee that needs access to MDM capabilities. For more information, see Create Basic User Accounts. ■ **Batch Import** – Add multiple users into Workspace ONE ™ UEM by importing a comma-separated values (CSV) file. Enter a unique name and description to group and organize multiple users at a time. For more information, see Batch Import Users or Devices.
Layout	Enables you to customize the column layout. ■ **Summary** – View the **List View** with the default columns and view settings. ■ **Custom** – Select only the columns in the **List View** you want to see. You can also apply selected columns to all administrators at or below the current organization group.
Sorting	Most columns in the **List View** (in both **Summary** and **Custom** Layout) are sortable including **Devices**, **User Groups**, and **Enrollment Organization Group**.
Export	Save a comma-separated values (CSV) file of the entire List View that can be viewed and analyzed in Excel.

Interact with User Accounts

The list view also features a check box to the left of each user account. View user details by selecting the hypertext user name in the General Info column.

The **Edit** icon ✎ enables you to make basic changes to the user account. Selecting a single check box causes three action buttons to appear, **Send Message**, **Add Device**, and **More Actions**.

You can select multiple user accounts using the check box, which, in turn, modifies the available actions.

Action	Description
Send Message.	Provide immediate support to a single user or group of users. Send a User Activation (user template) email to a user notifying them of their enrollment credentials.
Add Device.	Add a device for the selected user. Only available for single user selections.
More Actions	Display the following options.
Add to User Group.	Add selected users to new or existing user group for simplified user management. For more information, see User Groups List View and Edit User Group Permissions.
Remove from User Group.	Remove selected users from the existing user group.

Action	Description
Change Organization Group	Manually move the user to a different organization group. Update the available content, permissions, and restrictions of a user if they change positions, get a promotion, or change office locations.
Delete	If a member of your organization permanently terminates employment, you can quickly and completely delete a user account. Deleting account information is the equivalent of the account never having existed in the first place. A deleted account cannot be reactivated. If a deleted account owner returns, a new account must be created for them.
Activate	Activate a previously deactivated account if a user returns to an organization or must be reinstated in the company.
Deactivate	Deactivation is a security measure. Deactivate is used when a user is missing in action, their device is out-of-compliance, or their device is lost or stolen. All the information about a deactivated account is kept, such as name, email address, password, enrollment organization group, and so forth. A deactivated account simply means no one with these account credentials will be able to log in to Workspace ONE UEM console while the account is deactivated. Once the security issue is resolved (user is located, device becomes compliant, the device is recovered) then you can Activate the account.

Batch Import Feature

If you have several dozen or more users to add to Workspace ONE UEM, you can batch-create users and user groups or batch-import them from your directory service.

Making a batch import means taking a supplied template in a comma-separated values format. Then filling it out with your own data and uploading the completed template.

Changes in External LDAP and AD User Directories

Once your user and user group batch list are uploaded, changes to your external LDAP/AD user directories are not updated in Workspace ONE UEM. These user and user group changes must be updated manually or uploaded as a new batch.

Users and Devices

Choose from four different batch import templates: Blacklisted devices, Whitelisted devices, Simple device/user, and Advanced device/user. For more information, see Batch Import Users or Devices.

User Groups

You can batch import user groups in much the same way as individual users, by completing a Workspace ONE UEM supplied template and uploading it. For more information, see Batch Import User Groups.

Editing Basic Users

You can edit and move users in groups rather than one at a time by changing certain columns in the CSV file you upload as part of a batch import procedure. Such column manipulation is only applicable to two kinds of user authentication: basic user authentication and authentication proxy. For more information, see Editing Basic Users with Batch Import.

Move Users Between Organization Groups

Batch import can also be used to move multiple users to a different organization group. For more information, see Move Users with Batch Import.

Batch Import Users or Devices

To save time, you can batch import multiple users and devices into the UEM console. Users can be basic (stored on the database), directory-based (LDAP), or authentication proxy.

Procedure

1. Navigate to **Accounts > Users > Batch Status** or **Devices > Lifecycle > Enrollment Status > Add** and select **Batch Import**.
2. Enter the basic information including a **Batch Name** and **Batch Description** in the Workspace ONE UEM console.
3. Select the applicable batch type from the **Batch Type** drop-down menu.
4. Select and download the template that best matches the kind of batch import you are making.

   - **Blacklisted Devices**

     Import a list of known, non-compliant devices by IMEI, Serial Number, or UDID. Blacklisted devices are not allowed to enroll. If a blacklisted device attempts to enroll, it is automatically blocked.

   - **Whitelisted Devices**

     Import pre-approved devices by IMEI, Serial Number, or UDID. Use this template to import a list of known, trusted devices. The ownership and group ID associated to this device is automatically applied during enrollment.

   - **User and/or Device**

     Select between a **Simple** and an **Advanced** CSV template. The simple template features only the most often-used options while the advanced template features the full, unabridged compliment of import options.

   - **Change Organization Group**

     Move users to a different organization group.

5. Open the CSV file. Confirm whether or not users are part of the enrollment organization group (OG).

   The CSV file features several columns corresponding to the options on the **Add / Edit User** page. When you open the CSV template, notice that sample data has been added to each column in the template. The sample data is presented to inform you what kind of data is required and what format it must be in.

   Note A CSV file (comma-separated values) is simply a text file whose extension has been changed from "TXT" to "CSV". It stores tabular data (text and numbers) in plain text. Each line of the file is a data record. Each record consists of one or more fields, separated by commas. It can be opened and edited with any text editor. It can also be opened and edited with Microsoft Excel.

   a. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment** and select the **Grouping** tab.

      For a directory-based enrollment, the **Security Type** for each user must be **Directory**.

      If the **Group ID Assignment Mode** is set to **Default**, your users are part of the enrollment OG.

6. Enter data for your organization's users, including device information (if applicable) and save the file.
7. Return to the Batch Import page and select **Choose File** to locate and upload the CSV file that you had previously downloaded and filled out.
8. Select **Save**.

Batch Import User Groups

To save time, you can import multiple Lightweight Directory Access Protocol (LDAP)/Active Directory (AD) user groups into the Workspace ONE UEM console.

Procedure

1. Navigate to **Accounts > User Groups > List View** and select **Add**.
2. Select **Batch Import**.
3. Enter the basic information including **Batch Name** and **Batch Description** in the Workspace ONE UEM console.
4. Under **Batch File (.csv)**, select the **Choose File** button to locate and upload the completed CSV file.
5. Alternately, select the link **Download template for this batch type** and save the comma-separated values (CSV) file and use it to prepare a new importation file.
   - Open the CSV file, which has several columns corresponding to the settings that display on the **Add User Group** page. Columns with an asterisk are required and must be entered with data. Save the file.
   - The last column heading in the CSV file template is labeled "GroupID/Manage (Edit and Delete)/Manage(Users and Enrollment)/UG assignment/Admin Inheritance." This column heading corresponds to the settings and abides by the logic of the **Permissions** tab of the **Edit User Group** page. For details, see Edit User Group Permissions.

6. Select **Import**.
7. If the Batch Import does not complete successfully, view and troubleshoot errors by selecting **Accounts > Batch Status**. You can view specific batch import errors by clicking the **Errors** hyperlink.

Editing Basic Users with Batch Import

The Batch Import feature lets you edit and move users in groups rather than one at a time. The users must exist in Workspace ONE UEM for such a procedure to work. Edit the following settings in the CSV file and use Batch Import to upload this file.

- Password (Basic only).
- First Name.
- Middle Name.
- Last Name.
- Email Address.
- Phone Number.
- Mobile Number.
- Department.
- Email user name.
- Email Password.
- Authorized organization groups (at and below the given Group ID only).
- Enrollment user category (this category is accessible to the user, otherwise, defaulted to 0).
- Enrollment user role (this role is accessible to the user, otherwise, it assumes the default role of the organization group).

Such basic user editing applies only to Basic User Authentication and Authentication Proxy.

Move Users with Batch Import

You can use the Batch Import feature to move sets of users to a different organization group.

Procedure

1. From the Batch Import screen, enter the basic information including a Batch Name and a Batch Description in the Workspace ONE UEM console.
2. Choose **Change Organization Group** from the list of templates and save the CSV file somewhere accessible.
3. Enter the applicable **Group ID** of the user's existing organization group, **user name** to be moved, and **Target Group ID** of the user's new organization group.
4. Return to the Batch Import screen, select **Choose File** to locate and upload the saved CSV file and select **Open**.
5. Select **Save**.

Admin Accounts

Administrator Accounts enable you to maintain Mobile Device Management (MDM) settings, push, or revoke features and content, and much more from the UEM Console.

Also, a **Temporary Admin Account** enables a remote assistance feature within the Unified Endpoint Management Console. These Temporary Admin Accounts, which have a configurable expiration, can be used to access areas normally reserved for permanent admin account-holders.

Create an Admin Account

You can create as many administrator accounts, each with a unique set of permissions or roles, that you may need to manage your device fleet. For more information, see Create an Admin Account.

Create a Temporary Admin Account

Because of their configurable expiration date, temporary admin accounts are ideal for recruiting help from the larger group of users for troubleshooting, testing, and training exercises. For more information, see Create a Temporary Admin Account.

Add, Edit, and Delete Admin Accounts

As the number of administrator accounts expand, you can perform housekeeping duties to reassign permissions or roles, reset a password, or deactivate and delete admin accounts. For more information, see Managing Admin Accounts.

Create an Admin Account

You can add Admin Accounts from the **Administrators List View** page, providing access to advanced features of the Workspace ONE UEM console. Each admin that maintains and supervises the console must have an individual account.

Procedure

1. Navigate to **Accounts > Administrators > List View**, select **Add**, then **Add Admin**. The **Add/Edit Admin** page displays.
2. Under the **Basic** tab, for the **User Type** setting, select either **Basic** or **Directory**.
   - If you select **Basic**, then fill in all required settings on the **Basic** tab, including user name, password, First Name, and Last Name.
   - You can enable **Two-Factor Authentication** where you select between Email and SMS as a delivery method and the token expiration time in minutes.
   - You can also select a **Notification** option, choosing between None, Email, and SMS. The Admin receives an auto-generated response.
   - If you select **Directory**, then enter the **Domain** and **user name** of the admin user.
3. Select the **Details** tab and enter additional information, if necessary.
4. Select the **Roles** tab and then select the **Organization Group** followed by the **Role** you want to assign to the new admin. Add new roles by using **Add Role**.
5. Select the **API** tab and choose the **Authentication** type.
6. Select the **Notes** tab and enter additional **Notes** for the admin user.
7. Select **Save** to create the admin account with the assigned role.

Create a Temporary Admin Account

You can grant temporary administrative access to your environment for support, demonstrations, and other time limited use cases.

Procedure

1 Navigate to **Accounts > Administrators > List View**, select **Add**. Select the **Add Temporary Admin** option.

Alternatively, you can select the **Help** button from the header bar that appears at the top-right corner of almost every page of Workspace ONE UEM and select **Add Temporary Admin**.

2 In the **Basic** tab, select to add a temporary admin account based on **Email Address** or **user name** and complete the following settings.

Setting	Description
Email Address	Enter the email address on which the temporary admin account is based. Available only when Email Address radio button is selected.
User name	Enter the user name on which the temporary admin account is based. Available only when the user name radio button is selected.
Password / **Confirm Password**	Enter and confirm the password that is associated with the Email Address or user name.
Expiration Period	Select an **Expiration Period** which defaults to 6 hours. You can also set this drop-down menu to **Inactive** to create the account now and activate it later.
Ticket Number	Optionally, you can add the Ask Ticket Number from ZenDesk as a reference marker.

3 In the **Roles** tab, you can add, edit, and delete roles applicable to the temporary admin account.

- Add a role by selecting the **Add Role** button and then select the organization group and role for which the temporary admin account applies.
- Edit an existing role by selecting the edit icon (✏) and select a different organization group and role.
- Delete a role by selecting the delete icon (✖).

4 Select **Save**.

Managing Admin Accounts

You can implement key management functions for ongoing maintenance and upkeep of admin accounts by navigating to **Accounts > Administrators > List View**.

Display the **Add/Edit Admin** page by selecting the hypertext link in the **user name** column. This link enables you to update current roles assigned quickly or change roles within your organization quickly to keep their privileges up-to-date. You can also alter general admin information and reset a password.

You can **Filter** the list of administrators to include all roles or limit the listing to only a specific role you want to see.

Display the action buttons applicable to that admin by selecting the radio button next to the administrator user name.

- **View History** – Track when admins log in and out of the Workspace ONE UEM console.
- **Deactivate** – Change the status of an admin account from active to inactive. This feature allows you to suspend the management functions and privileges temporarily. At the same time, this feature enables you to keep the defined roles of the admin account for later use.
- **Activate** – Change the status of an admin account from inactive to active.
- **Delete** – Remove the admin account from the UEM console. Such an action is useful for when an administrator ends employment.
- **Reset Password** – Available to basic administrators only. Sends an email to the basic admin's email address on record. The email contains a link that expires in 48 hours. To reset the password, the basic admin must select the link and answer the password recovery question. This enables the basic admin to change their own password.

  Directory-based administrators must reset their passwords using the active directory system.

  Temporary administrators cannot reset their password. Another admin must delete then re-create the temporary admin account.

Role-Based Access

4

You can make roles that grant specific kinds of access to the Workspace ONE UEM console. You define roles for individual users and groups based on UEM console access levels you find useful.

For example, help desk administrators within your enterprise might have limited access within the console, while the IT Manager has a greater range of permissions.

To enable role-based access control, you must first set up the administrator and user roles within the UEM console. Specific resources, also known as permissions, define these roles which enable and disable access to various features within the UEM console. Roles can also be created for end users who need access to the Self-Service Portal.

Since roles (and specifically resources or permissions) determine what users and admins can and cannot do in the UEM console, care must be taken to grant the correct resources or permissions. For example, if you require admins enter a note before a device can be enterprise wiped, the role must not only have the permissions to enterprise wipe a device but also add a note.

Roles are important to maintain the security of your device fleet. An example of this is the creation of staging users, which is an elevated level administrator privilege. Treat staging user credentials the same as administrator privileges and do not disclose the user credentials.

Compare Two Admin Roles

You can compare the permissions of one administrator role with another for the sake of accuracy or to confirm deliberate permissions differences. For more information, see Compare Admin Roles.

This chapter includes the following topics:

Default and Custom Roles

There are several default roles already provided by Workspace ONE UEM from which you can select. These default roles are available with every upgrade and help quickly assign roles to new users. If you require further customization, you can create custom roles to tailor the user privileges and permissions further.

Unlike default roles, custom roles require manual updates with every Workspace ONE UEM upgrade.

Each type of role includes inherent advantages and disadvantages. **Default Roles** save time in configuring a brand new role from scratch, logically suit various administrative privileges, and automatically update alongside new features and settings. However, Default Roles might not be a precise fit for your organization or MDM deployment, which is why Custom Roles were created.

Default End-User Roles

Roles are available by default to end users in the Unified Endpoint Management Console.

- **Full Access Role** – Provides full permission to perform all the tasks on the Self-Service Portal.
- **Basic Access Role** – Provides all permissions except MDM commands from the Self-Service Portal.

Custom Roles allow you to customize as many unique roles as you require, and to tweak large or small changes across different users and administrators. However, Custom Roles must be manually maintained over time and updated with new features.

Edit a Default End-User Role to Create a Custom User Role

If none of the available default roles provide the proper fit for your organization, consider modifying an existing user role and creating a custom user role.

Create a custom end-user role by editing a default role that comes with the UEM console.

Procedure

1. Ensure that you are currently in the organization group you want the new role to be associated with.
2. Navigate to **Accounts > Users > Roles**.
3. Determine which role from the list best fits the role you want to create. Then edit that role by selecting the edit icon (✎) to the far right. The **Add/Edit Role** page displays.
4. Edit the **Name**, **Description**, and **Initial Landing Page** text boxes as necessary. Review each of the check boxes. These options represent the various permissions, selecting and deselecting those options as necessary.
5. Select **Save** to save your changes, overwriting the prior settings of the role in favor of the new settings.

Default Administrator Roles

The following roles are available by default to administrators in the Workspace ONE UEM console.

Use the Admin Role Compare tool to compare the specific permissions of two admin roles. For more information, see Compare Admin Roles.

Role	Description
System Administrator	The System Administrator role provides complete access to a Workspace ONE UEM environment. This role includes access to the Password and Security settings, Session Management, and UEM console audit information. This information is located the **Administration** tab under **System Configuration**. This role is limited to environment managers, for example, SaaS Operations teams for all SaaS environments hosted by VMware.
AirWatch Administrator	The AirWatch Administrator role allows comprehensive access to the Workspace ONE UEM environment. However, this access excludes the **Administration** tab under **System Configuration**, because that tab manages top-level UEM console settings. This role is limited to VMware employees with access to environments for troubleshooting, installation, and configuration purposes.
Console Administrator	The Console Administrator role is the default admin role for shared SaaS environments. The role features limited functionality surrounding compliance policy attributes, report authoring, and organization group selection.
Device Manager	The Device Manager role grants users significant access to the UEM console. However, this role is not designed to configure most System Configurations. These configurations include Active Directory (AD)/ Lightweight Directory Access Protocol (LDAP), Simple Mail Transfer Protocol (SMTP), Agents, and so on. For these tasks, use a top-tier role like the AirWatch Administrator or System Administrator.
Report Viewer	The Report Viewer role allows viewing of the data captured through Mobile Device Management (MDM). This role limits its users to generating, viewing, exporting, and subscribing to reports from the UEM console.
Content Management	The Content Management role only includes access to VMware Content Locker management. Use this role for specialized administrators responsible for uploading and managing a device content.
Application Management	The Application Management role allows admins with this access to deploy and manage the device fleet's internal and public apps. Use this role for an application management administrator.
Help Desk	The Help Desk role provides the tools necessary for most Level 1 IT Help Desk functions. The primary tool available in this role is the ability to see and respond to device info with remote actions. However, this role also contains report viewing and device searching abilities.
App Catalog Only Administrator	The App Catalog Only Admin role has much the same permissions as Application Management. Added to these permissions are abilities to add and maintain admin and user accounts, admin and user groups, device details, and tags.
Read Only	The Read Only role provides access to most of the UEM console, but limits access to read-only status. Use this role to audit or record the settings in a Workspace ONE UEM environment. This role is not useful for system operators or administrators.
Horizon Administrator	The Horizon Administrator role is a specially designed set of permissions for complementing a Workspace ONE UEM configuration integrated with VMware Horizon View.
NSX Administrator	The NSX Administrator role is a specially designed set of permissions intended to complement VMware NSX integrated with Workspace ONE UEM. This role offers the full complement of system and certificate management permissions, allowing administrators to bridge endpoint security with data center security.
Privacy Officer	The Privacy Officer role provides read access to Monitor Overview, Device List View, View system settings, and full edit permissions for privacy settings.

Edit a Default Admin Role to Create a Custom Admin Role

If the available default roles provide no proper fit for admin resources in your organization, consider modifying an existing default role into a custom admin role.

Create a custom administrator role by editing a default role that comes with the UEM console.

Procedure

1 Ensure that you are currently in the organization group with which you want the new role to be associated.

2 Navigate to **Accounts > Administrators > Roles**.

3 Determine which role from the list best fits the role you want to create. Select the check box for that role.

4 Select **Copy** from the actions menu above the listing. The **Copy Role** page displays.

5 Edit specific settings of the copy in the resulting **Copy Role** page. Create a unique **Name** and **Description** for the customized role.

6 Select **Save**.

What to do next

For more information, see Create Administrator Role.

User Roles

User roles allow you to enable or disable specific actions that logged-in users can perform. These actions include controlling access to a device wipe, device query, and managing personal content. You can also customize initial landing pages and restrict access to the Self-Service portal.

Creating multiple user roles is a time saving measure. You can make comprehensive configurations across different organization groups or change the user role for a specific user at any time.

Create a New User Role

In addition to the preset Basic Access and Full Access roles, you can create customized roles. Having multiple user roles available fosters flexibility and can potentially save time when assigning roles to new users.

Procedure

1 Navigate to **Accounts > Users > Roles** and select **Add Role**. The **Add/Edit Role** page displays.

2 Enter a **Name** and **Description**, and select the **Initial Landing Page** of the SSP for users with this new role.

   For existing user roles, the default **Initial Landing Page** is the **My Devices** page.

3 Select from a list of options the level of access and control end users of this assigned role have in the SSP.

   - Click **Select None** to clear all check boxes on the page.
   - Select all the check boxes on the page by selecting **Select All**.

4 **Save** the changes to the role. The added user role now appears in the list on the Roles page.

What to do next

From the Roles page, you can view, edit, or delete roles.

Configure a Default Role

A default role is the baseline role from which all user roles are based. Configuring a default role enables you to set the permissions and privileges users automatically receive upon enrollment.

Procedure

1 Navigate to **Devices > Device Settings > Devices & Users > General > Enrollment** and select the **Grouping** tab.

2 Configure a default level of access for end users in the Self-Service Portal (SSP) by selecting a Default Role.

   These role settings are customizable by organization group.

   - **Full Access** - Grants users with access to higher SSP functions such as install/remove profiles and apps, reset passcodes, send device messages, and write-access to content.
   - **Basic Access** - Grants users with a low impact access. They can register their own device, view-only (but not install) profiles and apps, view their own account, and query and find their own device.
   - **External Access** - Users with External Access have all the abilities as basic access users but they also have read-only access to content on the SSP that is explicitly shared with them.

3 Select **Save**.

Assign or Edit the Role of an Existing User

You can edit the role for a specific user, for example, to grant or restrict access to Workspace ONE UEM functions.

Procedure

1 Select the appropriate organization group.

2 Navigate to **Accounts > Users > List View**.

3 Search for the specific user that you want to edit from the list. Once you have identified the user, select the Edit icon under the check box. The **Add/Edit User** screen displays.

4 In the **General** tab, scroll to the **Enrollment** section and select a **User Role** from this drop-down menu to change the role for this specific user.

5 Select **Save**.

Admin Roles

Admin roles allow you to enable or disable permissions for every available setting and resource in the UEM Console. These settings grant or restrict console abilities for each member of your admin team, enabling you to craft a hierarchy of administrators specific to your needs.

Creating multiple admin roles is a time saving measure. Making comprehensive configurations across different organization groups means you can change the permissions for a specific administrator at any time.

Administrator Roles List View

The administrator roles list view enables you to add, edit, compare, and maintain your library of roles for your entire admin base.

The Administrator Roles List View can be found by navigating to **Accounts > Administrators > List View**.

Add Role

Make a new admin role from scratch by selecting the **Add Role** button. For more information, see Create Administrator Role.

Import Role and Export Role

You can import a role exported from another environment. You can also export a role saved as an XML file to a location on your device, suitable to be imported later. Select the role you want to export and select the **Export** button. For more information, see the following topics.

- Import Admin Roles
- Export Admin Roles
- Versioning Issues When Importing and Exporting Admin Roles

Copy Role

You can save time by making a copy of an existing role, including it's permissions. For more information, see Copy Role

View Users

The **View Users** button enables you to see the Administrators List View, displaying a listing of all admins. Enable the check box to the left of the role name and then select the **View Users** button.

Delete Role

You can delete an unused role from your library of administrator roles. You cannot delete a role that is assigned to an admin. Select an unassigned role you want to delete and select the **Delete** button.

Rename a Role

If you are importing an admin role named the same as an existing admin role, you can rename the existing role first. For more information, see Rename an Admin Role.

View the Resources of an Admin Role

You can view all the resources, or permissions, of any administrator role, including custom and default roles. This view can help you determine what an admin can, and cannot, do in the UEM console. For more information, see View the Resources of an Admin Role.

Edit Role

You can edit an existing role's name, description, and specific permissions. Select the pencil icon to the left of the role name from the listing and the **Edit Role** screen displays, enabling you to make changes.

Compare Two Roles

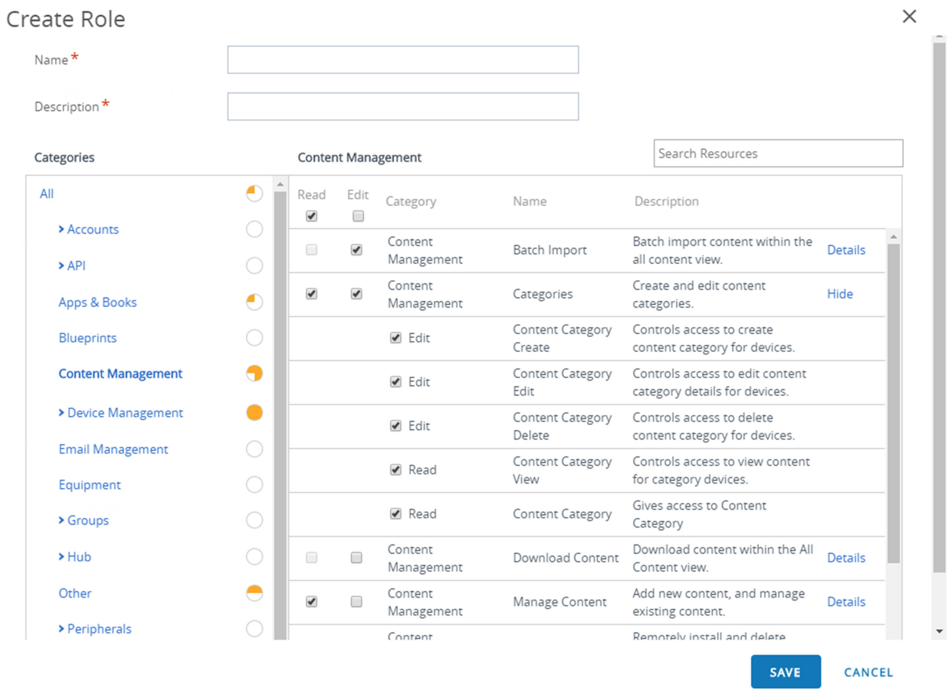
You can also compare the individual permissions settings between two roles. For more information, see Compare Admin Roles.

Create Administrator Role

You can create administrator roles which define specific tasks that can be performed in Workspace ONE UEM. You then assign these roles to individual admins.

Procedure

1 Navigate to **Accounts > Administrators > Roles** and select **Add Role** in the UEM console.



Create Role

Name *

Description *

Categories

- All ◔
- › Accounts ○
- › API ○
- Apps & Books ◔
- Blueprints ○
- Content Management ◑
- › Device Management ●
- Email Management ○
- Equipment ○
- › Groups ○
- › Hub ○
- Other ◓
- › Peripherals ○

Content Management

Search Resources

Read ☑	Edit ☐	Category	Name	Description	
☐	☑	Content Management	Batch Import	Batch import content within the all content view.	Details
☑	☑	Content Management	Categories	Create and edit content categories.	Hide
		☑ Edit	Content Category Create	Controls access to create content category for devices.	
		☑ Edit	Content Category Edit	Controls access to edit content category details for devices.	
		☑ Edit	Content Category Delete	Controls access to delete content category for devices.	
		☑ Read	Content Category View	Controls access to view content for category devices.	
		☑ Read	Content Category	Gives access to Content Category	
☐	☐	Content Management	Download Content	Download content within the All Content view.	Details
☑	☐	Content Management	Manage Content	Add new content, and manage existing content.	Details
		Content		Remotely install and delete	

2 In the **Create Role**, enter the **Name** and **Description** of the role.

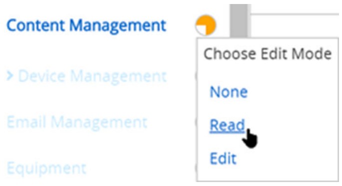
3 Select from the list of **Categories**.

The **Categories** section organizes top-level categories such as **Device Management** under which are located subcategories including **Applications**, **Browser**, and **Bulk Management** among others. This category subdivision enables an easy and quick role creation process. Each subcategory setting in the right panel has a **Read** and **Edit** check box.

When you select from the **Categories** section, its subcategorized contents (individual settings) populate in the right panel. Each individual setting features its own **Read** and **Edit** check box and a "select all" style **Read** and **Edit** check box in the column heading. This arrangement allows for a flexible level of control and customization while creating roles.

Use the **Search Resources** text box to narrow down the number of resources from which you can select. Resources are generally labeled the same way as they are referred to in the UEM console itself. For example, if you want to limit an admin role to editing App Logs, then enter "App Logs" in the **Search Resources** box and a listing of all resources that contain the string "App Logs" displays.

4 Select the appropriate **Read** and **Edit** check box in the corresponding resource options. You can also choose to clear any of the selected resources.



5 To make blanket category selections, select **None**, **Read**, or **Edit** directly from the **Categories** section without ever populating the right panel. Select the circular icon to the right of the Category label, which is a drop-down menu. Use this selection method when you are certain you want to select none, read-only, or edit capabilities for the entire category setting.

6 Select **Save** to finish creating the Custom Role. You can now view the added role in the list on the **Roles** page. From here, you can also edit the role details or delete the role.

What to do next

You must update the custom role after each Workspace ONE UEM version update to account for the new permissions in the latest release.

Import Admin Roles

You can import administrator roles saved from another environment as an XML file, making admin roles a portable resource, which can save time.

Procedure

1 Navigate to **Accounts > Administrators > Roles** and select **Import Role**.

2 In the Import Role page, select **Browse** and locate the previously saved XML file. Select **Upload** to upload the admin role to the Category listing for validation.

3 Workspace ONE UEM performs a series of validation checks including an XML file check, importing role permission check, duplicate role name check, and blank name and description check.

4 Check the resource settings and verify their imported role specifications by selecting specific **Categories** in the left pane.

5 You can also edit the resources and the **Name** and **Description** of the imported role based on your needs. If you want to keep both the existing role and the imported role, then rename the existing admin role before importing the new role.

   a If the role you are importing is named the same as an existing role in your environment, then a message displays. "A role with this name exists in this environment. Would you Like to override the existing role?"

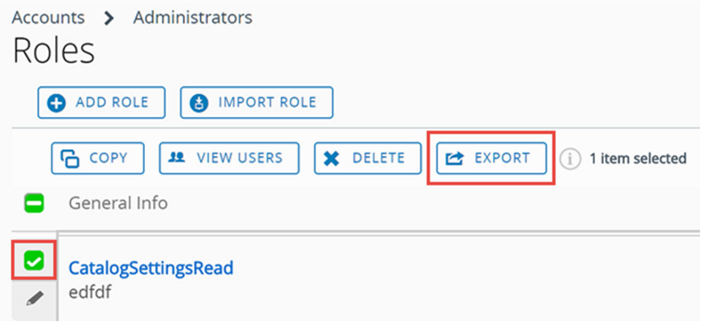
   b If you select No, then the existing role in your environment remains untouched and the role import is canceled.

   c If you select Yes, then you are prompted for the security PIN, which if entered correctly, replaces the existing role with the imported role.

6 Select **Save** to apply the imported role to the new environment.

Export Admin Roles

You can export administrator roles as an XML file and import those files into another environment, making admin roles a portable resource which can save time.



Procedure

1 Navigate to **Accounts > Administrators > Roles**.

2 Select the check box next to the administrator role that you want to export. Doing so displays actions buttons above the role listing. If you select more than one admin role, the Export action is not available.

3 Select **Export** and save the XML file to a location on your device.

Copy Role

You can save time by making a copy of an existing role. You can also change the permissions of the copy and save it under a different name.

Procedure

1 Select the check box next to the role you want to copy.

2 Select the **Copy** button. The **Copy Role** page displays.

3 Make your changes to the **Categories**, **Name**, and **Description**.

4 When finished, select **Save**.

Rename an Admin Role

If you are importing an admin role named the same as an existing admin role, you might find it useful to rename the existing role first. Renaming a role enables you to keep both the old and the new role in the same environment.

Procedure

1 Navigate to **Accounts > Administrators > Roles** and select the **Edit** icon (✎) of the role you want to rename. The **Edit Role** page displays.

2 Edit the **Name** of the role and optionally, the **Description**.

3 Select **Save**.

Versioning Issues When Importing and Exporting Admin Roles

There can be cases where an exported role is imported into an environment running an earlier version of Workspace ONE UEM. This earlier version might not have the same resources and permissions that comprise the imported role.

In these cases, Workspace ONE UEM notifies you with the following message.

There are some permissions in this environment that are not found in your imported file. Review and correct the highlighted permissions before saving.

Use the category listing page to deselect the highlighted permissions. This action allows you to save the role to the new environment.

Read/Edit Indicator in Categories for Admin Roles

There is a visual indicator in the **Categories** section that reflects the current selection of read-only, edit, or a combination of each. This indicator reports what the setting is without requiring you to open and examine the individual subcategory settings.

The indicator features a circular icon located to the right side of the Category listing that reports the following.

●	All options in this category have the edit capability (which by definition means that they also have read-only capability).
◕	Most category settings have the edit capability enabled, but edits are disabled for at least one subcategory.
◓	All category settings have read-only enabled (edit disabled).
◔	Most category settings are read-only, but edits are enabled for at least one subcategory.

Assign or Edit the Role of an Admin

You can assign roles to an admin which expand the capabilities of an Admin in the Workspace ONE UEM console. You can also edit existing roles, potentially limiting or expanding their capabilities.

Procedure

1. Navigate to **Accounts > Administrators > List View**, locate the admin account, and select the Edit icon in the Action button cluster. The **Add/Edit Admin** page displays.
2. Select the **Roles** tab. Then select **Add Role**.
3. Enter the **Organization Group** and **Role** details for each role that is added.
4. Select **Save**.

View the Resources of an Admin Role

Viewing the list of resources (or permissions) can help you make admin roles, which determine what an admin can and cannot do in the UEM console. You can use the Administrator Roles List View to review all the resources of any administrator role, including custom and default roles.

Prerequisites

Roles are comprised of hundreds of resources, or permissions, which serve as access (read only or edit) to a specific function within the UEM console. To view the resources of an admin role, take the following steps.

Procedure

1. Navigate to **Accounts > Administrators > Roles**.
2. Locate the admin role you would like to see the permissions for. If you have a large library of admin roles, use the **Search List** bar in the upper-right corner to narrow the listing.
3. Select the name of the role, which is a link, and the **View Role** screen displays containing all the permissions associated with the role.
   - Role Categories are listed in the left panel. There may be role subcategories which you can expand to view.
   - For more information about the orange-colored read/edit visual indicators seen on this screen, see Read/Edit Indicator in Categories for Admin Roles.
   - Select a specific category in the left panel and the category, name, and description of each resource displays on the right panel. The **Details** link to the far right reveals each specific read-only and edit function within the UEM console.
   - You can use the **Search Resources** box to locate a specific function by name. For example, if you want to make an admin role that can only add a tag to a device, enter the word "tag" in the **Search Resources** box and hit the enter key. Every resource that contains the string "tag" appears in the right panel. This makes it easy to locate the specific tag-related function and assign it to a role.

4 When finished auditing administrator roles, select **Close**.

What to do next

You can apply these steps to making your own roles by visiting Create Administrator Role.

Admin Roles Compare Tool

When creating an administrator role, it is often easier to modify an existing role than it is to create an admin role from scratch. The Compare Roles tool makes this process easy.

The Compare Roles Tool allows you to see only the differences between two admin roles, which makes the comparison process fairly simple. Alternately, you can compare two admin roles to confirm and verify all the known similarities, which can be equally important.

Compare Admin Roles

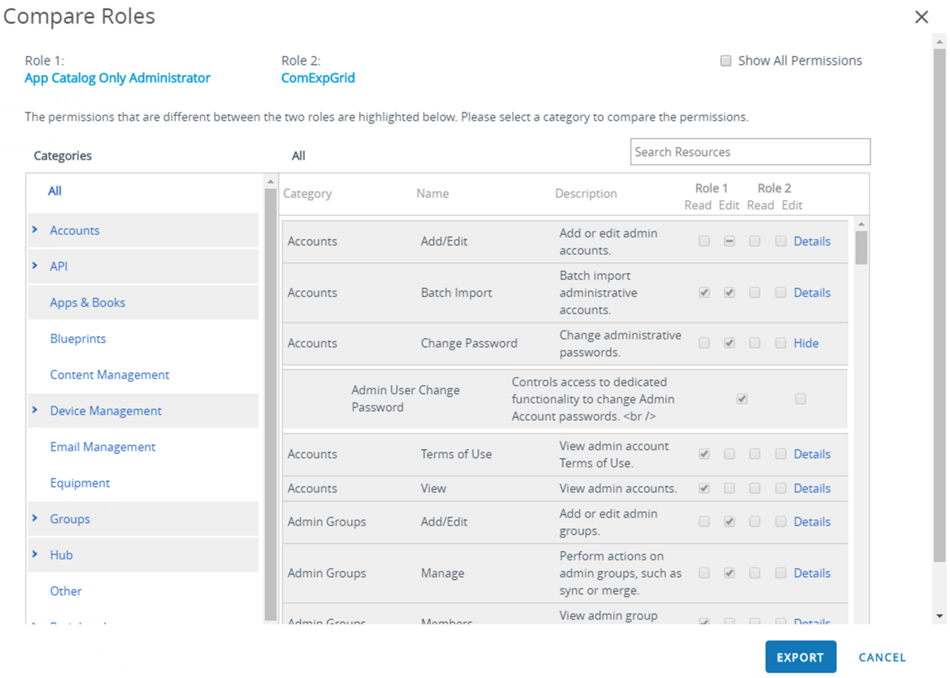
You can compare the permissions settings of any two administrator roles for the sake of accuracy or to confirm your deliberate settings differences.

Procedure

1 Navigate to **Accounts > Administrators > Roles**.

2 Locate any two listed roles, including roles that appear on different pages, and select those roles.

3 Select **Compare**. The **Compare Roles** page displays featuring a list of categories. Selecting a specific category on the left populates all the details of that category on the right.



Compare Roles

Role 1: App Catalog Only Administrator

Role 2: ComExpGrid

□ Show All Permissions

The permissions that are different between the two roles are highlighted below. Please select a category to compare the permissions.

Categories: All

Search Resources

Category	Name	Description	Role 1 Read	Role 1 Edit	Role 2 Read	Role 2 Edit	
Accounts	Add/Edit	Add or edit admin accounts.	□	⊟	□	□	Details
Accounts	Batch Import	Batch import administrative accounts.	✓	✓	□	□	Details
Accounts	Change Password	Change administrative passwords.	□	✓	□	□	Hide
	Admin User Change Password	Controls access to dedicated functionality to change Admin Account passwords. <br />		✓		□	
Accounts	Terms of Use	View admin account Terms of Use.	✓	□	□	□	Details
Accounts	View	View admin accounts.	✓	□	□	□	Details
Admin Groups	Add/Edit	Add or edit admin groups.	□	✓	□	□	Details
Admin Groups	Manage	Perform actions on admin groups, such as sync or merge.	□	✓	□	□	Details
Admin Groups	Members	View admin group	✓	□	□	□	Details

- If you have fewer than two or more than two roles selected, the **Compare** button does not display.

- Role subcategories can be viewed in the right panel by selecting the **Details** link to the far-right side. Collapse the role subcategory by selecting the **Hide** link.
- There is an **All** category in the left panel that, when selected, displays all the parent categories on the **Compare Roles** page. When you enter a search parameter in the **Search Resources** bar, the right panel only displays matching category and resources (also known as permissions) listings.
- The search function is persistent. This persistence means that if you have a parameter in the **Search Resources** bar, selecting the **All** category displays only the matching categories and resources. The search function is persistent even after you select specific resources and make **Read** and **Edit** selections.
- By default, only those categories and subcategories whose settings are different are displayed. You can display all the permissions including those settings that are identical across the two selected roles by enabling the **Show All Permissions** check box.
- If you select two roles that have identical permissions across the board, the console displays this message at the top of the **Compare Roles** page.

  "There are no differences in permissions between the two roles.".

What to do next

You can optionally select **Export** to create an Excel-viewable CSV file (comma-separated values). This CSV file contains all settings for Role 1 and Role 2, enabling you to analyze the differences between them.

Groups

5

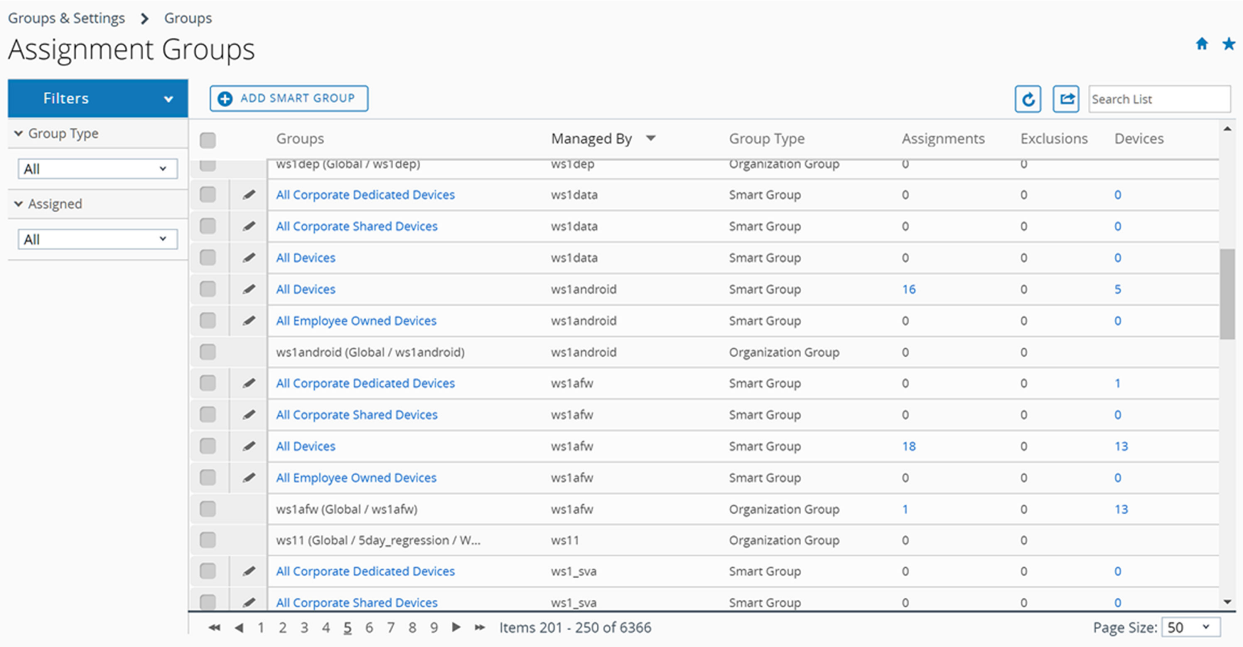
Workspace ONE UEM uses several different types of groups to manage users, devices, apps, content, and more.

This chapter includes the following topics:

Assignment Groups

Assignment Groups is an umbrella term used to categorize certain management grouping structures within Workspace ONE UEM. Organization Groups, Smart Groups, and User Groups each have full feature sets and properties and are distinct from each other. One element they have in common is the way they can be used to assign content to user devices easily. Assignment Groups enables an administrator to manage these three grouping structures from a single location.

Navigate to **Groups & Settings > Groups > Assignment Groups**.



Groups	Managed By	Group Type	Assignments	Exclusions	Devices
ws1dep (Global / ws1dep)	ws1dep	Organization Group	0	0	
All Corporate Dedicated Devices	ws1data	Smart Group	0	0	0
All Corporate Shared Devices	ws1data	Smart Group	0	0	0
All Devices	ws1data	Smart Group	0	0	0
All Devices	ws1android	Smart Group	16	0	5
All Employee Owned Devices	ws1android	Smart Group	0	0	0
ws1android (Global / ws1android)	ws1android	Organization Group	0	0	
All Corporate Dedicated Devices	ws1afw	Smart Group	0	0	1
All Corporate Shared Devices	ws1afw	Smart Group	0	0	0
All Devices	ws1afw	Smart Group	18	0	13
All Employee Owned Devices	ws1afw	Smart Group	0	0	0
ws1afw (Global / ws1afw)	ws1afw	Organization Group	1	0	13
ws11 (Global / 5day_regression / W...	ws11	Organization Group	0	0	
All Corporate Dedicated Devices	ws1_sva	Smart Group	0	0	0
All Corporate Shared Devices	ws1_sva	Smart Group	0	0	0

You can use the list view to assign multiple organization groups, smart groups, and user groups to one or more profiles, public applications, and policies.

Assignment Group List View

The Assignment Groups List View organizes three kinds of groups that have the function of assigning content to devices: organization groups, smart groups, and user groups. You can create a listing of only those groups you are interested in seeing.

Navigate to **Groups & Settings > Groups > Assignment Groups** and the Assignment Groups List View displays. The only assignment groups listed for viewing are those managed by the OG that the administrator is currently in.

Sort by Columns

You can sort the listing of groups by individual columns by selecting the column header.

Filter Groups

You can filter groups by **Group Type** (Smart Groups, Organization Groups, and User Groups). You can also filter by how or whether they have been **Assigned** (Assignments, Exclusions, All, and None).

Select Links in the Assignment Groups Listing

Four columns in the Assignment Groups Listing page serve a specific function and require a special mention.

- The **Groups** column features a link for each **Smart Group**. You can select this link to edit the smart group.

- If you select non-zero values in the **Assignments** column, the View Assignments page displays, even for assigned organization groups and user groups. This function allows you to view and confirm assignments to profiles, public applications, and compliance policies. For more information, see View Assignments.
- If you select non-zero values in the **Exclusions** column, the View Assignments page displays, even for excluded organization groups and user groups. The View Assignments page allows you to view and confirm exclusions from profiles, public applications, and compliance policies.
- If you select the **Devices** column number, the Devices List View page displays. The Device List View contains the listing of all devices in the selected organization group, smart group, or user group. For more information, see the Workspace ONE UEM Managing Devices Documentation.

Assign One or More Assignment Groups

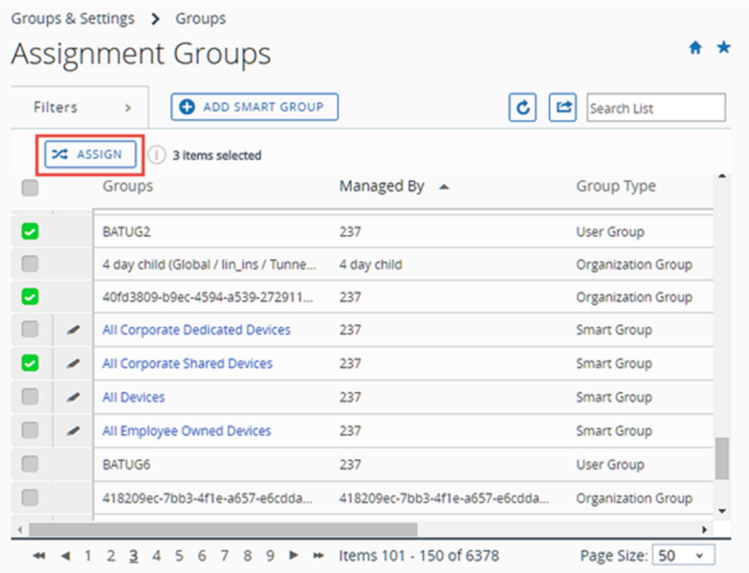
You can assign groups to device profiles, public applications, and compliance policies. You can also assign multiple groups of each individual type (organization, smart, or user) in a single sitting.

To assign public applications, you can configure different app policies for different groups of users. For more information, see **Use Flexible Deployment to Assign Applications** in the **VMware Workspace ONE UEM Mobile Application Management Guide**, which can be found on docs.vmware.com.

Procedure

1 Navigate to **Groups & Settings > Groups > Assignment Groups**.

2 Select one or more groups in the listing and select **Assign** above the column header.



☐		Groups	Managed By	Group Type
☑		BATUG2	237	User Group
☐		4 day child (Global / lin_ins / Tunne...	4 day child	Organization Group
☑		40fd3809-b9ec-4594-a539-272911...	237	Organization Group
☐	✎	All Corporate Dedicated Devices	237	Smart Group
☑	✎	All Corporate Shared Devices	237	Smart Group
☐	✎	All Devices	237	Smart Group
☐	✎	All Employee Owned Devices	237	Smart Group
☐		BATUG6	237	User Group
☐		418209ec-7bb3-4f1e-a657-e6cdda...	418209ec-7bb3-4f1e-a657-e6cdda...	Organization Group

3 The **Assign** page displays the **Organization Groups**, **Smart Groups**, and **User Groups** you selected.

4 Assign them by initiating a search for a **Profile**, a **Public Application**, and **Compliance Policy**. You may choose up to 10 profiles, up to 10 public applications, and a single compliance policy.

   You can only choose multiple entities of a single type per session. For example, you may assign multiple groups to up to 10 different profiles in a single command. However, you may not, in a single command, assign multiple groups to 10 profiles, 10 apps, **and** a compliance policy. If you have multiple entities of multiple types, you must undertake separate assignment sessions for each type (profiles, apps, and policies).

5 Select **Next** to display the **View Device Assignment** page which you can use to confirm the groups assignment.

6 Select **Save & Publish** to finalize the assignment.

Organization Groups

Think of organization groups as individual branches on a family tree, with each leaf as a device user. Workspace ONE UEM identifies each leaf and establishes its standing in the family tree using organization groups (OG). Most customers make OG trees look like their corporate hierarchy: Executives, Management, Operations, Sales, and so forth.

You can also establish OGs based on Workspace ONE UEM features and content.

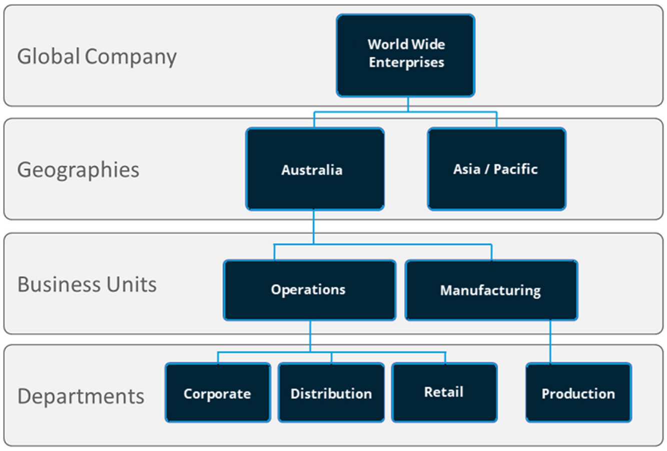
You can access organization groups by navigating to **Groups & Settings > Groups > Organization Groups > List View** or through the organization group drop-down menu.

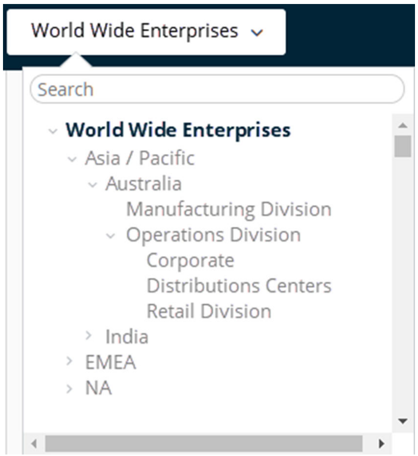
- Build groups for entities within your organization (Management, Salaried, Hourly, Sales, Retail, HR, Exec, and so on).
- Customize hierarchies with parent and child levels (for example, 'Salaried' and 'Hourly' as children under 'Management').
- Integrate with multiple internal infrastructures at the tier level.
- Delegate role-based access and management based on a multi-tenant structure.

Characteristics of Organization Groups

Organization groups can accommodate functional, geographic, and organization entities and enable a multi-tenancy solution.

- **Scalability** – Flexible support for exponential growth.
- **Multi-tenancy** – Create groups that function as independent environments.
- **Inheritance** – Streamline the setup process by setting child groups to inherit parent configurations.





- World Wide Enterprises
  - Asia / Pacific
    - Australia
      - Manufacturing Division
      - Operations Division
        - Corporate
        - Distributions Centers
        - Retail Division
    - India
  - EMEA
  - NA

Using the example of the organization group drop-down menu, profiles, features, applications, and other MDM settings can be set at the 'World Wide Enterprises' level.

Settings are inherited down to child organization groups, such as **Asia/Pacific** and **EMEA** or even further down to grand-child **Australia > Manufacturing Division** or even great grand-child **Australia > Operations Division > Corporate**.

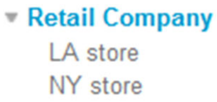
Settings between sibling organization groups such as **Asia/Pacific** and **EMEA** take advantage of the multi-tenant nature of OGs, by keeping these settings separate from one another. However, these two sibling OGs do inherit settings from their parent OG, **World Wide Enterprises**.

Alternatively, you can opt to override settings at a lower level and alter only the settings that you want to change or keep. These settings can be altered or carried down at any level.

Considerations for Setting Up Organization Groups

Before setting up your organization group (OG) hierarchy in the Workspace ONE UEM console, first decide on the group structure. The group structure allows you to make the best use of settings, applications, and resources.

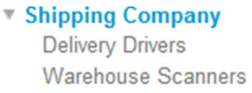
- **Delegated Administration** – You can delegate administration of subgroups to lower-level administrators by restricting their visibility to a lower organization group.



- Retail Company
  - LA store
  - NY store

- **Corporate administrators** can access and view everything in the environment.
- **LA manager** has access to the LA OG and can manage only those devices.
- **NY manager** has access to the NY OG and can manage only those devices.

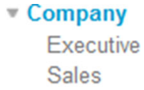
- **System Settings** – Settings can be applied at different levels in the organization group tree and inherited down. They can also be overridden at any level. Settings include device enrollment options, authentication methods, privacy setting, and branding.



Shipping Company
Delivery Drivers
Warehouse Scanners

- **Overall company** establishes an enrollment against the company Active Directory server.
- **Driver devices** override the parent authentication and allow a token-based enrollment.
- **Warehouse devices** inherit the AD settings from the parent group.

- **Device Use Case** – A profile can be assigned to one or several organization groups. Devices in those groups can then receive that profile. Refer to the Profiles section for more information. Consider configuring devices using profile, application, and content settings according to attributes such as device make, model, ownership type, or user groups before creating organization groups.



Company
Executive
Sales

- **Executive** devices cannot install applications and have access to the Wi-Fi sales network.
- **Sales** devices are allowed to install applications and have VPN access.

Override Versus Inherit Setting for Organization Groups

The hierarchy of the organization group (OG) structure you make determines which OGs are children and which are parents. Child OGs inherit settings from their parent OGs but you can elect to override this inheritance.

Each system settings page applies its settings according to two types of inheritance / override options where organization group hierarchy is concerned: 1) Current Setting and 2) Child Permission. The OG it applies settings to is the OG you are currently in.

For example, the **Branding** settings page found by navigating to **Groups & Settings > All Settings > System > Branding** control all the custom background images, logos, and color schemes for the OG on display in the organization group drop down.

Change OGs and you now have the option to import a new background image, new logo, a different color scheme, all specific to that OG. This option is enabled by changing the inheritance of the OGs on the settings page.

Child Permission

Think of the Child Permission setting as the parent OG's attitude toward the child OG. There are three different settings for Child Permission: **Inherit or Override**, **Inherit Only**, and **Override Only**.

The **Inherit or Override** setting simply means that the parent has no preference for the child's permissions. When a parent's Child Permission setting is **Inherit or Override**, the Current Setting of the child OG determines whether they override or inherit settings. Child Permissions are set to **Inherit or Override** by default.

A Child Permission setting of **Inherit Only** on the parent forces inheritance on all children. This means all children have the same settings as the parent. A Child Permission setting of **Override Only** removes the inheritance effect on all child OGs, requiring you to configure settings specific to that child OG.

Child Permission settings affect only the children one level down. Such settings have no impact on grandchildren or lower OGs.

Current Setting

If Child Permission is the parent's attitude toward the child, then the Current Setting of an OG is the child's attitude toward the parent. An OG's Current Setting can only be **Inherit** or **Override**.

A Current Setting of **Inherit** means the child OG accepts all the settings of the parent OG. Select a Current Setting of **Override**, and the child rejects the parent and is on its own. This means you can make new settings for the child.

You can only change an OG's Current Setting provided the parent OG's Child Permission setting is **Inherit or Override**.

Changing Permission Settings

You cannot change the Current Setting of a child if its parent's Child Permission setting doesn't allow it. For example, if MomandDadOG's Child Permission setting is **Override Only**, you cannot change the Current Setting of JuniorOG to **Inherit**. In short, the parent OG's Child Permission settings take precedence.

When you change the Current Settings of a child from **Override** to **Inherit**, changing the Child Permission setting of its parent to **Inherit Only** has the effect of locking the child OG's Child Permission setting such that you cannot change it. This behavior does not apply if the child OG setting is never overridden.

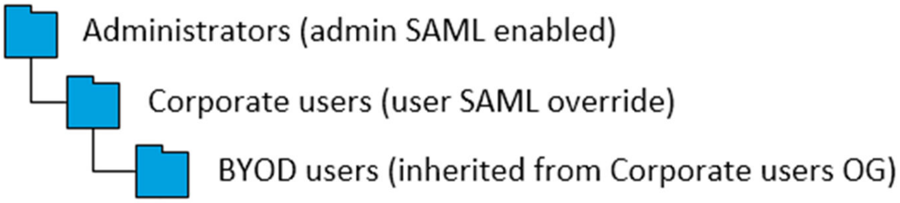
The work-around to this behavior is that you must change the Child Permission settings on the parent OG back to **Inherit or Override**, unlocking the Child Permission setting of the child OG.

The larger strategy is to plan in advance, configuring inheritance and override settings to the OG levels that make sense given the hierarchy structure you want.

Inheritance, Multi-Tenancy, and Authentication

The concept of overriding settings on a per-organization group basis, when combined with organization group (OG) characteristics such as inheritance and multi-tenancy, can be further combined with authentication. This combination provides for flexible configurations.

The following organization group model illustrates this flexibility.


Administrators (admin SAML enabled)
Corporate users (user SAML override)
BYOD users (inherited from Corporate users OG)

In this model, **Administrators**, generally in possession of greater permissions and functionality, are positioned at the top of this OG branch. These administrators log into their OG using SAML that is specific to admins.

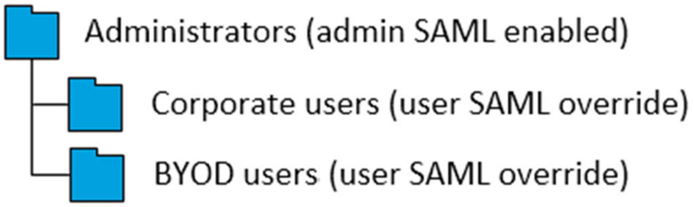
Corporate users are subservient to administrators so their OG is arranged as its child. Being users and not administrators, their SAML login setting cannot inherit the administrator setting. Therefore, the Corporate users' SAML setting is overridden.

BYOD users differ from Corporate users. Devices used by BYOD users belong to the users themselves and likely contain more personal information. So these device profiles might require slightly different settings. BYOD users might have a different terms of use agreement. BYOD devices might need different enterprise wipe parameters. For all these reasons and more, it might make sense for BYOD users to log into a separate OG.

And while not subservient to Corporate users in a corporate hierarchy sense, placing BYOD users as a child of Corporate users has advantages. This arrangement means that BYOD users inherit settings applicable to ALL corporate user devices simply by applying them to the Corporate users OG.

Inheritance also applies to SAML authentication settings. Since BYOD users is a child of Corporate users, BYOD users inherit their SAML for users' authentication settings.

An alternate model is to make BYOD users a sibling of Corporate users.


Administrators (admin SAML enabled)
Corporate users (user SAML override)
BYOD users (user SAML override)

Under this alternate model, the following is true.

- All device profiles meant to apply globally to ALL devices, including compliance policies, and other globally applicable device settings are applied to two organization groups instead of one. The reason for this duplication need is because inheritance from Corporate users to BYOD users is no longer a factor in this model. Corporate users and BYOD users are peers and therefore there is no inheritance.
- Another SAML override must be applied to BYOD users. This override is necessary because the system assumes it is inheriting SAML settings from its parent, Administrators. Such an assumption is a mistake because BYOD users are not administrators and do not have the same access and permissions.
- BYOD users continue to be handled separately from Corporate users. This alternate model means that they continue to enjoy their own device profile settings.

What factor determines which model is the best? Compare the number of globally applicable device settings with the number of group-specific device settings. Basically, if you want to treat all devices in generally the same way, then consider making BYOD users a child of Corporate users. If maintaining separate settings is more important, then consider making BYOD users a sibling of Corporate users.

For more information, see and Enterprise Wipe for BYOD Devices.

For a detailed example of OG inheritance involving enrollment, see Directory Service Integration and Enrollment Restrictions.

Create Organization Groups

You must create an organization group (OG) for each business entity where devices are deployed. Understand that the OG you are currently in is the parent of the child OG you are about to create.

Procedure

1. Navigate to **Groups & Settings > Groups > Organization Groups > Details**.
2. Select the **Add Child Organization Group** tab and complete the following settings.

Setting	Description
Name	Enter a name for the child organization group (OG) to be displayed. Use alphanumeric characters only. Do not use odd characters.
Group ID	Enter an identifier for the OG for the end users to use during the device login. Group IDs are used during the enrollment of group devices to the appropriate OG. Ensure that users sharing devices receive the **Group ID** as it might be required for the device to log in depending on your Shared Device configuration. If you are not in an on-premises environment, the Group ID identifies your organization group across the entire shared SaaS environment. For this reason, all Group IDs must be uniquely named.
Type	Select the preconfigured OG type that reflects the category for the child OG.
Country	Select the country where the OG is based.
Locale	Select the language classification for the selected country.
Customer Industry	This setting is only available when **Type** is Customer. Select from the list of Customer Industries.
Time Zone	Select the time zone for the OG's location.

3. Select **Save**.

Organization Group Type Functions

The type of an organization group can have an impact on what settings an admin can configure.

- **Global** – The top-most organization group. Usually, this group is called Global and has type Global.
  - For hosted SaaS environments, you are not able to access this group.
  - On-premises customers can turn on Verbose logging at this level.
- **Partner** – Top-level organization group for partners (third-party resellers of Workspace ONE UEM).
- **Customer** – The top-level organization group for each customer.
  - A customer organization group cannot have any children/parent organization groups that are of the customer type.
  - Some settings can only be configured at a Customer group. These settings filter down to lower organizations. Some examples of such settings include autodiscovery email domains, Volume Purchase Program settings, Device Enrollment Program settings (before AirWatch 8.0), and personal content.

- **Container** – The default organization group type.
  - All organization groups beneath a customer organization group must be of the container type. You can have containers between Partner and Customer groups.
- **Prospect** – Potential customers. Similar to a customer organization group. Might have less functionality than a true customer group.

There are additional Organization Group types such as Division, Region, and the ability to define your own Organization Group type. These types do not have any special characteristics and function identically to the Container Organization Group type.

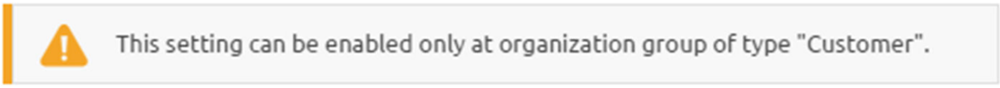
Adding Devices at Global

The Global organization group (OG) is designed to house Customer and other types of OGs. Given the way inheritance works, if you add devices to Global and configure Global with settings intended to affect those devices, you are also affecting all the Customer OGs underneath. This undermines the benefits of multitenancy and inheritance.

For more information, see Reasons You Should Not Enroll Devices in Global.

Organization Group Restrictions

If you attempt to configure an organization group (OG)-limited setting, the settings pages under **Groups & Settings > All Settings** notify you of the limitation.



This setting can be enabled only at organization group of type "Customer".

The following restrictions apply to creating Customer-level organization groups.

- Whether you are in a software-as-a-service (SaaS) or on-premises environment, you cannot create nested customer OGs.

Organization Groups Settings Comparison

As an Administrator, you might find it useful to compare the settings of one organization group (OG) to another.

The following are available when you compare OG settings.

- Upload XML files containing the OG settings from different Workspace ONE UEM software versions.
- Eliminate the possibility of a difference in configuration causing problems during version migration.
- Filter the comparison results, allowing you to display only the settings you are interested in comparing.
- Search for a single setting by name with the search function.

The Organization Group Compare feature is only available for on-premises customers.

Compare Two Organization Groups

You can compare the settings of one organization group to another to mitigate version migration issues.

An example of a version migration scenario is when a User Acceptance Testing (UAT) server has been upgraded, configured, and tested, you can compare the UAT settings to the production settings directly.

Procedure

1 Navigate to **Groups & Settings > All Settings > Admin > Settings Management > Settings Comparison**.

2 Select an OG in your environment from the left drop-down menu (labeled with the numeral **1**). Alternatively, upload the XML settings file by selecting the **Upload** button and selecting an exported OG setting XML file.

3 Select the comparison OG on the right drop-down menu (labeled with the numeral **2**).

4 Display a list of all settings for both selected organization groups by selecting the **Update** button.

   - Differences between the two sets of OG settings are automatically highlighted.
   - You can optionally enable the **Show Differences Only** check box. This check box displays only those settings that apply to one OG but not the other.
   - Individual settings that are empty (or not specified) display in the comparison listing as 'NULL'.

Smart Groups

Smart groups are customizable groups that determine which platforms, devices, and users receive an assigned application, book, compliance policy, device profile, or provision.

When you create organization groups, you typically base them on the internal corporate structure: geographical location, business unit, and department. For example, "North Sales," "South HR." Smart groups, however, offer the flexibility to deliver content and settings by device platform, model, operating system, device tag, or user group. You can even deliver content to individual users across multiple organization groups.

You can create smart groups when you upload content and define settings. However, their modular nature means you can also create them at any time, so they are available to be assigned later.

The main benefit of smart groups is their reusability. It might be intuitive to make a new assignment every time you add content or define a profile or policy. Instead, if you define assignees to smart groups only once, you can simply include those smart groups in your definition of content.

Create and Assign a Smart Group

You can create a smart group defined by platform, ownership, user group, OS version, model, device tag, enterprise OEM, and even individual devices by friendly name.

For example, you can make a smart group containing all employee-owned iPhone Touch devices with iOS version earlier than 9.0.2. Add to this same smart group all Android devices by HTC version 2.0 with OS version 4.1 or greater. Out of this group, you can exclude devices in the user group "full time." To this highly customized pool of *devices, you can assign 10 device profiles, 10 applications, or a compliance policy.

*Some restrictions might apply due to the multiplatform nature of this customized device pool. For example, there might be apps you want to assign that do not offer an Android version.

You can assign a smart group two ways. First, from the Assignment Groups List View after the smart group has been saved. Second, from the Assignment Groups setting which is found on multiple device product creation screens.

Create a Smart Group

Before you can assign a smart group to an application, book, compliance policy, device profile, or product provision, you must first create one.

Procedure

1. Select the applicable **Organization Group** (OG) to which your new smart group applies and from which it can be managed. Selecting an OG is optional.
2. Navigate to **Groups & Settings > Groups > Assignment Groups** and then select **Add Smart Group**.
3. Enter a **Name** for the smart group.
4. Optionally, you can enable the **Device Preview** to see which devices are included in the smart group you have designed. This device preview is disabled by default to improve performance.
5. Configure the smart group type.

   - **Criteria**

     The **Criteria** option works best for groups with large numbers of devices (more than 500) that receive general updates. This method works best because the inherent details of these groups can reach all endpoints of your mobile fleet.

   - **Devices or Users**

     The **Devices or Users** option works best for groups with smaller numbers of devices (500 or fewer) that receive sporadic, although important, updates. This method works best because of the granular level at which you can select group members.

Switching between **Criteria** and **Devices or Users** erases any entries and selections you might have made.

a In the **Criteria** type, select qualifying parameters to add in the smart group. If no selection is made in any setting, then that filtering is not applied toward the criteria.

Setting	Description
Organization Group	This criteria option filters devices by organization groups selected. You can select more than one OG.
User Group	This criteria option filters devices by user groups selected. You can select more than one user group.
Ownership	This criteria option filters devices by ownership type selected.
Tags	This criteria option filters devices according to the way they are tagged. You can select more than one tag.
Platform and Operating System	This criteria option filters devices by platform and OS selected. You can select multiple combinations of each. While Platform is a criterion within a smart group, the platform configured in the device profile or compliance policy always takes precedence over the smart group's platform. For instance, if a device profile is created for the iOS platform, the profile is only assigned to iOS devices even if the smart group includes Android devices.
Model	This criteria option filters devices by device model. Individual models displayed are based on the selections made in **Platform and Operating System**. You can select (or exclude) from this list of models.
Enterprise OEM Version	This criteria option filters devices by their original equipment manufacturer version. You can select more than one OEM.
Management Type	Filter devices according to the way the device is managed.
Enrollment Category	Filter devices according to the way the device is enrolled.
Additions	This criteria option adds individual devices and users that are not included in the filtering criteria. You can select more than one device and more than one user.
Exclusions	This criteria option excludes individual devices, individual users, and user groups that are included in the filtering criteria. You can exclude more than one device, more than one user, and more than one user group.

b Use the **Devices or Users** type to assign content and settings to special cases outside of the general enterprise mobility criteria. Enter the device friendly name in **Devices** and user name (first name or last name) in **Users**. You must **Add** at least one device or user or you cannot save the smart group.

Setting	Description
Devices	Add a device to this Smart Group by entering the device friendly name. You can add more than one device using this method.
Users	Add users to this smart group by entering the user name, first name, or last name. You can add more than one user using this method.

6 Select **Save** when complete.

Smart Group Assignment

Once you have created the smart group representing users and their devices and before it can take effect, you must assign it to at least one device product. You can assign it to an application, book, compliance policy, device profile, or product provision.

There are two methods to assign a smart group: assigning a smart group while creating the device product and assigning a smart group while managing the smart group itself.

Assign Smart Group While Creating Device Product

You can assign a smart group when you add or create an application, book, compliance policy, device profile, or product provision.

Procedure

1 Complete the **Assigned Groups** drop-down menu.

2 Select a smart group from the drop-down menu. Smart groups available are managed only within the organization group (OG) to which the resource is being added, or to a child OG below it.

3 If no smart group matches the desired assignment criteria, then select the **Create a Smart Group** option. You can assign more than one smart group per application, book, compliance policy, device profile, or product provision.

4 Select **Save** to include the assignment.

Assign Smart Group While Managing the Smart Group

You can also assign a smart group during the process of managing the smart group itself.

Procedure

1 View the entire list of smart groups by navigating to **Groups & Settings > Groups > Assignment Groups**.

2 Select one or more smart groups you want to assign and select **Assign**. The **Assign** page displays. Select the Groups link at the top of the **Assign** page to display the **Groups** page. On this page, the organization groups that manage the smart groups are displayed. Return to the Assign page by selecting the **Close** button.

3 On the **Assign** page, use the search box to view the list of eligible products and assign it to the selected smart groups.

4 Select **Next** to display the **View Device Assignment** page and confirm the assignment status.

5 Select **Save & Publish**.

Exclude Groups in Profiles and Policies

You can exclude groups from the assignment of device profiles and compliance policies with as much ease as assigning groups to these device products.

Prerequisites

You must have the groups defined before you initiate this task. At a minimum, you must be able to make a smart group comprised of the users you want to exclude. This task allows you to make a new smart group on the fly but if you prefer to exclude an organization group or user group, then see Create Organization Groups, Add User Groups with Directory Integration, or Add User Groups Without Directory Integration, Custom respectively.

Procedure

1 While adding a device profile or compliance policy, select **Yes** next to the **Exclusions** setting to display the **Excluded Groups** option.

2 In the **Excluded Groups** setting, select groups that you want to exclude from the assignment of this profile or policy.

- You can enter the first few letters of the group by name and the auto-search function shows you all the groups whose name corresponds to the string you entered.
- You can select one or more organization groups, user groups, or smart groups.
- You can make a new smart group by selecting the **Create Smart Group** button.

3 Select **Save and Publish** (for device profiles) or **Next** (for compliance policies) and continue the process for those tasks.

Results

If you select the same group in both the **Assigned Groups** and **Excluded Groups** settings, then the profile or policy fails to save.

Example

You want a compliance policy to apply to all device users except executives.

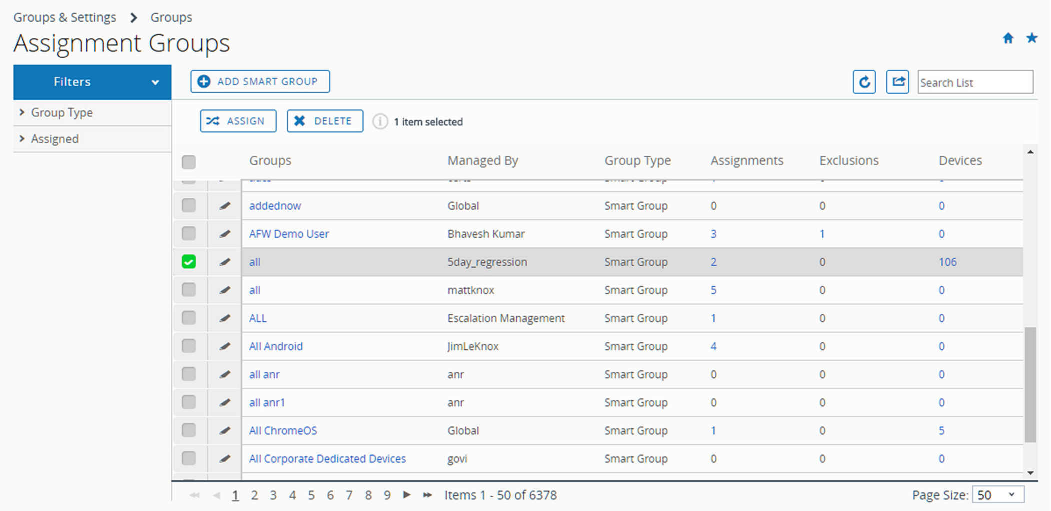
What to do next

Preview the affected devices by selecting **View Device Assignment**.

Smart Group List View

Manage your smart groups by editing, assigning, unassigning, excluding, and deleting them with the Workspace ONE UEM console.

View the entire list of smart groups by navigating to **Groups & Settings > Groups > Assignment Groups**. Admins can only see groups which they can manage based on their permissions settings.



Groups & Settings > Groups

Assignment Groups

1 item selected

☐		Groups	Managed By	Group Type	Assignments	Exclusions	Devices
☐	✎	addednow	Global	Smart Group	0	0	0
☐	✎	AFW Demo User	Bhavesh Kumar	Smart Group	3	1	0
☑	✎	all	5day_regression	Smart Group	2	0	106
☐	✎	all	mattknox	Smart Group	5	0	0
☐	✎	ALL	Escalation Management	Smart Group	1	0	0
☐	✎	All Android	JimLeKnox	Smart Group	4	0	0
☐	✎	all anr	anr	Smart Group	0	0	0
☐	✎	all anr1	anr	Smart Group	0	0	0
☐	✎	All ChromeOS	Global	Smart Group	1	0	5
☐	✎	All Corporate Dedicated Devices	govi	Smart Group	0	0	0

1 2 3 4 5 6 7 8 9 Items 1 - 50 of 6378 Page Size: 50

The columns **Groups**, **Assignments**, **Exclusions**, and **Devices** each feature links which you can select to view detailed information.

- Selecting links in the **Assignments** or **Exclusions** columns display the **View Smart Group Assignments** screen.
- Selecting a link in the **Devices** column displays the **Devices > List View** showing only those devices included in the smart group.
- You can **Filter** your collection of groups by **Group Type** (Smart, Organization, User, or all) or by **Assigned** status. Assigned status shows whether the group is assigned, is excluded, both, or neither.
- You can **Assign** a smart group directly from the listing.

Edit a Smart Group

You can edit an established smart group. Any edits that you apply to a smart group affects all policies and profiles to which that smart group is assigned.

Procedure

1 Navigate to **Groups & Settings > Groups > Assignment Groups**.

2. Select the **Edit** icon (✎) located to the left of the listed smart group that you want to edit. You can also select the smart group name in the **Group** column. The **Edit Smart Group** page displays with its existing settings.
3. In the **Edit Smart Group** page, alter **Criteria** or **Devices and Users** (depending upon which type the smart group was saved with) and then select **Next**.
4. In the **View Assignments** page, you can review which profiles, apps, books, provisions, and policies can be added or removed from the devices as a result.
5. Select **Publish** to save your smart group edits. All profiles, apps, books, provisions, and policies tied to this smart group update their device assignments based on this edit.

Results

The **Console Event** logger tracks changes made to smart groups, including the author of changes, devices added, and devices removed.

Example

Here is an example of a typical need to edit a smart group. Assume a smart group for executives is assigned to a compliance policy, device profile, and two internal apps. If you want to exclude some of the executives from one or more of the assigned content items, then simply edit the smart group by specifying **Exclusions**. This action prevents not only the two internal apps from being installed on the excluded executives' devices but also the compliance policy and device profile.

Delete a Smart Group

When you have no further use for a smart group, you can delete it.

You can only delete one smart group at a time. Selecting more than one smart group causes the **Delete** button to be unavailable.

Prerequisites

The smart group cannot be assigned to any device product. If a smart group is assigned, you are not permitted to delete it. See Unassign a Smart Group.

Procedure

1. Navigate to **Groups & Settings > Groups > Assignment Groups** and locate the smart group you want to delete from the listing.
2. Select the check box to the left of the smart group you want to delete.
3. Select **Delete** from the actions menu that displays.

Results

The unassigned smart group has been removed.

Unassign a Smart Group

You can unassign a smart group from an application, book, channel, policy, profile, or product. This action removes the associated content from all devices in the smart group.

Procedure

1 To unassign smart groups from applications, books, compliance policies, device profiles, or product provisions. Follow the navigation paths shown.

- **Applications** – Navigate to **Apps & Books > Applications > List View** and select the **Public**, or **Internal** tab.
- **Books** – Navigate to **Apps & Books > Books > List View** and select the **Public**, **Internal**, or **Web** tab.
- **Channels** – Navigate to **Content > Video > Channels**.
- **Compliance Policy** – Navigate to **Devices > Compliance Policies > List View**.
- **Device Profile** – Navigate to **Devices > Profiles & Resources > Profiles**.
- **Product Provision** – Navigate to **Devices > Provisioning > Products > List View**.

2 Locate the content or setting from the listing and select the **Edit** icon ✎ from the actions menu.

3 Select the **Assignment** tab or locate the **Assigned Smart Groups** text box.

4 Select Delete (**X**) next to the smart group that you want to unassign. This action does not delete the smart group. It simply removes the smart group assignment from the saved setting.

5 Follow the required steps to **Save** your changes.

Research Smart Group Events Using Console Event Logger

You can track the changes to smart groups, and when they were made and by whom, by using the **Console Event** logger. Such tracking can be useful when troubleshooting devices.

Procedure

1 Navigate to **Monitor > Reports & Analytics > Events > Console Events**.

2 Select **Smart Groups** from the **Module** drop-down filter at the top of the **Console Event** listing.

3 Apply more filters as you might require including **Date Range**, **Severity**, and **Category**.

4 Where applicable, select the hypertext link in the **Event Data** column which contains extra detail that can assist your research efforts.

User Groups

You can group sets of users into user groups which, like organization groups, act as filters for assigning profiles and applications. When configuring your MDM environment, align user groups with security groups and business roles within your organization.

You can assign profiles, compliance policies, content, and applications to users and devices with user groups. You can add your existing directory service groups into Workspace ONE UEM or create user groups from scratch.

As an alternative to user groups, you can also manage content by assigning devices according to a preconfigured range of network IP address or custom attributes.

User Groups Without Directory Integration, Custom

Creating a user group outside of your existing Active Directory structure allows you to create specialized groups of users at any time. Customize user groups according to your deployment by specifically designing access to features and content.

For instance, you can create a temporary user group for a specific project requiring specialized apps, device profiles, and compliance policies.

For more information about adding user groups in bulk, see Batch Import User Groups.

Add User Groups Without Directory Integration, Custom

You can establish a custom user group outside of your corporate structure, which might be preferred depending upon the kind of user group you need. Custom user groups can only be added at a customer level organization group.

Procedure

1 Navigate to **Accounts > User Groups > List View** and select **Add** and then **Add User Group**.

2 Change the user group **Type** option to **Custom**.

3 Enter the **Group Name** and **Description** used to identify the user group in the Workspace ONE UEM console.

4 Confirm the organization group that manages the user group and select **Save**.

5 You can then add users to this new user group by navigating to **Accounts > Users > List View**.

   Add multiple users by selecting check boxes to the far-left of each listed **user name**. Next, select the **Management** button above the column headings and select **Add to User Group**.

User Groups with Directory Integration

An alternative to custom user groups without active directory integration is through user group integration that applies your existing active directory structure, providing many benefits.

Once you import existing directory service user groups as Workspace ONE UEM user groups, you can perform the following.

- **User Management** - Reference your existing directory service groups (such as security groups or distribution lists) and align user management in Workspace ONE UEM with the existing organizational systems.
- **Profiles and Policies** - Assign profiles, applications, and policies across a Workspace ONE UEM deployment to groups of users.

- **Integrated Updates** - Automatically update user group assignments based on group membership changes.
- **Management Permissions** - Set management permissions to allow only approved administrators to change policy and profile assignments for certain user groups.
- **Enrollment** - Allow users to enroll with existing credentials and automatically assign an organization group.

The administrator must designate an existing organization group as the primary root location from which the administrator manages devices and users. Directory services must be enabled at this root organization group.

You can add your existing directory service groups into Workspace ONE UEM. While integration does not immediately create user accounts for each of your directory service accounts, it ensures that Workspace ONE UEM recognizes them as user groups. You can use this group to restrict who can enroll.

For more information about adding directory user groups in bulk, see Batch Import User Groups.

Add User Groups with Directory Integration

Making user groups with directory integration fosters an aligned approach to device management: device enrollment plus subsequent updates, administrative overview, and user management are each in lockstep with your existing directory service structure.

Prerequisites

Ensure that the user group **Type** is **Directory**.

Procedure

1 Navigate to **Accounts > User Groups > List View**, select **Add** then **Add User Group**.

Setting	Description
Type	Select the type of User Group. ■ **Directory** – Create a user group that is aligned with your existing active directory structure. ■ **Custom** – Create a user group outside of your organization's existing Active Directory structure. This user group type grants access to features and content for basic and directory users to customize user groups according to your deployment. Custom user groups can only be added at a customer level organization group.
External Type	Select the external type of group you are adding. ■ **Group** – Refers to the group object class on which your user group is based. Customize this class by navigating to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services > Group**. ■ **Organizational Unit** – Refers to the organizational unit object class on which your user group is based. Customize this class by navigating to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services > Group**. ■ **Custom Query** – You can also create a user group containing users you locate by running a custom query. Selecting this external type replaces the Search Text function but displays the Custom Query section.

Setting	Description
Search Text	Identify the name of a user group in your directory by entering the search criteria and selecting **Search** to search for it. If a directory group contains your search text, a list of group names displays. This option is unavailable when **External Type** is set to **Custom Query**.
Directory Name	Read-only setting displaying the address of your directory services server.
Domain and **Group Base DN**	This information automatically populates based on the directory services server information you enter on the **Directory Services** page (**Groups & Settings > System > Enterprise Integration > Directory Services**). Select the **Fetch DN** plus sign (+) next to the **Group Base DN** setting, which displays a list of distinguished name elements from which you can select.
Custom Object Class	Identifies the object class under which your query runs. The default object class is 'person' but you can supply a custom object class to identify your users with a greater success and accuracy. This option is available only when **Custom Query** is selected as **External Type**.
Group Name	Select a **Group Name** from your **Search Text** results list. Selecting a group name automatically alters the value in the Distinguished Name setting. This option is available only after you have completed a successful search with the **Search Text** setting.
Distinguished Name	This read-only setting displays the full distinguished name of the group you are creating. This option is available only when **Group** or **Organizational Unit** is selected as **External Type**.
Custom Base DN	Identifies the base distinguished name which serves as the starting point of your query. The default base distinguished name is 'AirWatch' and 'sso'. However, if you want to run the query with a different starting point, you can supply a custom base distinguished name. This option is available only when **Custom Query** is selected as **External Type**.
Organization Group Assignment	This optional setting enables you to assign the user group you are creating to a specific organization group. This option is available only when **Group** or **Organizational Unit** is selected as **External Type**.
User Group Settings	Select between **Apply default settings** and **Use Custom settings for this user group**. See the **Custom Settings** section for additional setting descriptions. You can configure this option from the permission settings after the group is created. This option is available only when **Group** or **Organizational Unit** is selected as **External Type**.
Custom Query	
Query	This setting displays the currently loaded query that runs when you select the **Test Query** button and when you select the **Continue** button. Changes you make to the **Custom Logic** setting or the **Custom Object Class** setting are reflected here.
Custom Logic	Add your custom query logic here, such as user name or admin name. For example, "cn=jsmith". You can include as much or as little of the distinguished name as you like. The **Test Query** button allows you to see if the syntax of your query is correct before selecting the **Continue** button.
Custom Settings	
Management Permissions	You can allow or disallow all administrators to manage the user group you are creating.
Default Role	Select a default role for the user group from the drop-down menu.
Default Enrollment Policy	Select a default enrollment policy from the drop-down menu.

Setting	Description
Auto Sync with Directory	This option enables the directory sync, which detects user membership from the directory server and stores it in a temporary table. Administrators approve changes to the console unless the Auto Merge option is selected. If you want to prevent user groups from automatically syncing during a scheduled sync, this setting must be disabled.
Auto Merge Changes	Enable this option to apply sync changes automatically from the database without administrative approval.
Maximum Allowable Changes	Use this setting to set a threshold for the number of automatic user group sync changes that can occur before approval must be given. Changes more than the threshold need admin approval and a notification is sent to this effect. For more information, see the **VMware AirWatch Mobile Device Management Guide**. This option is available only when **Auto Merge Changes** is enabled.
Add Group Members Automatically	Enable this setting to add users to the user group automatically. If you want to prevent user groups from automatically syncing during a scheduled sync, this setting must be disabled.
Send Email to User when Adding Missing Users	Enable to send an email to users when missing users are being added to the user group. Adding missing users means combining the temporary user group table with the Active Directory table.
Message Template	This option is available only when **Send Email to User when Adding Missing Users** is enabled. Select a message template to be used for the email notification during the addition of missing users to the user group. When adding active directory users new to the Workspace ONE UEM console, the message template availability depends upon the enrollment mode as configured in **Groups & Settings > All Settings > Devices & Users > General > Enrollment** selecting **Authentication**, and making a choice in the **Devices Enrollment Mode** option. When **Open Enrollment** is selected as the **Devices Enrollment Mode**, a User Activation email template is available in the **Message Template** drop-down. This email message enables the new AD user to enroll. When **Registered Devices Only** is selected as the **Devices Enrollment Mode**, a Device Activation email template is available in the **Message Template** drop-down. This email message enables the new AD user to enroll their devices. If **Require Registration Token** is enabled, the device can be registered with the token embedded in the message.

For more information on Distinguished Name, search for Microsoft's TechNet article entitled "Object Naming" at https://technet.microsoft.com/.

2 Select **Save**.

Edit User Group Permissions

Fine-tuning user group permissions allows you to reconsider who inside your organization can edit certain groups. For example, if your organization has a user group for company executives, you might not want lower-level administrators to have management permissions for that user group.

Use the **Permissions** page to control who can manage certain user groups and who can assign profiles, compliance policies, and applications to user groups.

Procedure

1. Navigate to **Accounts > User Groups > List View**.
2. Select the **Edit** icon of an existing user group row.
3. Select the **Permissions** tab, then select **Add**.
4. Select the **Organization Group** you want to define permissions for.
5. Select the **Permissions** you want to enable.
   - **Manage Group (Edit/Delete)** – Activate the ability to edit and delete user groups.
   - **Manage Users Within Group and Allow Enrollment** – Manage users within the user group and to allow a device enrollment in the organization group (OG). This setting can only be enabled when Manage Group (Edit/Delete) is also enabled. If Manage Group (Edit/Delete) is disabled, then this setting is also disabled.
   - **Use Group For Assignment** – Use the group to assign security policies and enterprise resources to devices. This setting can only be changed if Manage Group (Edit/Delete) is disabled. If Manage Group (Edit/Delete) is enabled, then this setting becomes locked and uneditable.
     - This setting is disabled when the user group is managed by a parent OG and you want to assign the group from one of its children OGs.
6. Select the **Scope** of these permissions, that is, which groups of administrators are allowed to manage or use this user group. Only **one** of the following options may be active.
   - **Administrator Only** – The permissions affect only those administrators at the parent organization group.
   - **All Administrators at or below this Organization Group** – The permissions affect the administrators in the organization group and all administrators in all child organization groups underneath.
7. Select **Save**.

Exception to Use Group For Assignment

In a certain use case, the **Use Group For Assignment** option in **Edit User Group Permissions** is unavailable. This means you are not able to use this user group as an assignment group.

You cannot select the **Use Group For Assignment** option (and therefore it cannot be used as an assignment group or smart group) in the following use case.

- When the user group is managed by a parent OG and you want to assign the group from one of its children OGs.

Accessing User Details

Once your users and user groups are in place, you can view all user information regarding user details, associated devices, and interactions.

Access user information from any location in the Workspace ONE UEM console where the user name is displayed, including each of the following pages in the console.

- User Group Members (**Accounts > User Groups > Details View > More > View Users**)
- Users List View (**Accounts > Users > List View**)
- Administrators List View (**Accounts > Administrators > List View**).

The User Details page is a single-page view.

- All associated user groups.
- All Devices associated with the user over time and a link to all enrolled devices.
- All devices a user has checked-out in a Shared Device Environment and a link to complete check-in/check-out device history.
- All device- and user-specific event logs.
- All assigned, accepted, and declined Terms of Use.

Encrypt Personal Details

You can encrypt personally identifiable information including first name, last name, email address, and phone number.

Procedure

1. Navigate to **Groups & Settings > All Settings > System > Security > Data Security** from the Global or Customer-level organization group for which you want to configure encryption.
2. Enable the **Encrypt User Information** setting, then select individual user data settings to activate encryption. Doing so disables the search, sort, and filter functionality.
3. Click **Save** to encrypt user data so it is not accessible in the database. Doing so limits some features in the Workspace ONE UEM console, such as search, sort, and filter.

User Groups List View

The User Groups List View page features useful tools for common user group maintenance and upkeep, including viewing, merging, deleting user groups, and adding missing users.

Navigate to **Accounts > User Groups > List View**.

You can use the User Groups List View to create lists of user groups immediately, based on criteria that is most important to you. You can also add new user groups individually or in bulk.

Action	Description
Filters	Display only the desired user groups by using the following filters. ■ User Group Type. ■ Sync Status. ■ Merge Status.
Add	

Action	Description
Add User Group.	Perform a one-off addition of either a Directory-Based User Group or a Custom User Group.
Batch Import	Import new user groups in bulk by using a comma-separated values (CSV) file. You can organize multiple user groups at a time by entering a unique name and description.
Sorting and Resizing Columns	Columns in the List View that are sortable are Group Name, Last Sync On, Users, and Merge Status. Columns that can be resized are Group Name and Last Sync On.
Details View	View basic user group information in the Details View by selecting the link in the **Group Name** column. This information includes group name, group type, external type, manager, and number of users. Details View also includes a link to the group mapping settings in **All Settings > Devices & Users > General > Enrollment** in the **Grouping** tab.
Export (↗)	Save a comma-separated values (CSV) file of the entire unfiltered or filtered List View that can be viewed and analyzed in Excel.

The **User Groups List View** also features a selection check box and **Edit** icon to the left of the user. Selecting the **Edit** icon (✎) enables you to make basic changes to the user group. You can make bulk actions on user groups by selecting one or more groups which reveals the action buttons for the listing.

More Actions for User Groups

You can select more than one user group by selecting as many check boxes as you like. Doing so modifies the available action buttons and also makes the available actions apply to multiple groups and their respective users.

Action	Description
Sync	Copy recently added user group users to the temporary table, manually, ahead of the scheduled, automated Active Directory sync by Workspace ONE UEM.
View Users	Displays the **User Group Members** screen, enabling you to review the user names of all the members in the selected user group.
More Actions	
View and Merge	View, Add, and Remove users recently added to the temporary user group table. User group users that appear in this table await the automated Workspace ONE UEM user group sync.
Add Missing Users	Combine the temporary user group table with the Active Directory table, making the addition of these new users in the user group official.
Delete	Delete a user group.

Add Users to User Groups

You can add users to user groups as the need arises.

When you have a new user to add to one or more user groups, follow these steps.

Procedure

1 Navigate to **Accounts > Users > List View**.

2 Select one or more users in the listing by inserting a check mark in the check box to the left.

3 Select the **More Actions** button and then select **Add To User Group**. The **Add Selected Users Into Custom User Group** page displays.

4 You can add users to an **Existing User Group** or create a **New User Group**.

5 Select the **Group Name**.

6 Select **Save**.

7 Navigate to **Accounts > User Groups > List View**.

   a The Active Directory (AD) synchronization (which is an automated, scheduled process) copies these pending user group users to a temporary table. Then these user group users are reviewed, added, or removed.

   b If you do not want to wait for the automated AD sync, you can synchronize manually. Start a manual synchronization by selecting the user group to which you added users, then select the **Sync** button.

8 You can optionally select **More > View and Merge** to perform maintenance tasks such as review, add, and remove pending user group users.

9 Combine the temporary table of pending user group users with the Active Directory user group users by selecting **More > Add Missing Users**.

Admin Groups

Admin groups enable you to assemble subsets of administrator accounts for assigning roles and permissions beyond the permissions that come from having an admin account.

Admin groups can be used to assign roles and permissions granting access to the console that is specific to a special project. You can add your existing directory service administrators into admin groups or create admin groups from scratch using custom queries.

For example, if you have a new business directive, you might need to assign special admin access to a group of training facilitators. You might create an admin group, run a custom query for training facilitators, and assign a role that is specific to the new business effort. For more information, see Admin Accounts.

Admin Groups List View

The Admin Groups List View page features useful tools for common user group maintenance and upkeep. Such upkeep includes adding, viewing, merging, and deleting user groups and missing users.

View this page by navigating to **Accounts > Administrators > Admin Groups**.

Display the **Edit Admin Group** page by selecting the hypertext name in the **Group Name** column of the list view. Use this page to change the name of the admin group. You can also add and remove roles that are applicable to group members. For more information, see Admin Roles.

Display the **Admin Group Members** listing by selecting the hypertext link number in the **Admin** column. This listing shows you the names of all the administrators in the admin group.

Access the following actions and maintenance functions by selecting the radio button next to the group name.

Action	Description
Sync	Copy recently added admin group users to the temporary table, manually, ahead of the scheduled, automated Active Directory sync by Workspace ONE UEM.
More Actions	
View and Merge	View, Add, and Remove users recently added to the temporary admin group table. Admin group administrators that appear in this table await the automated Workspace ONE UEM admin group sync.
Delete	Delete an admin group.
Top, Up, Down, Bottom	You can edit the ranking of each admin group as it appears in the listing. Moving the groups in this way is useful for when you have more admin groups than a single page can display.
Add Missing Users.	Combine the temporary admin group table with the Active Directory table, making the addition of these new admins in the group official.

Add Admin Groups

You can add admin groups to assign additional roles and permissions to your admins for special projects by taking the following steps.

Procedure

1 Navigate to **Accounts > Administrators > Admin Groups** and select **Add**. Complete the applicable settings.

Setting	Description
External Type	Select the external type of admin group you are adding. ■ **Group** – Refers to the group object class on which your admin group is based. Customize this class by navigating to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services > Group**. ■ **Organizational Unit** – Refers to the organizational unit object class on which your admin group is based. Customize this object class by navigating to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services > Group**. ■ **Custom Query** – You can also create an admin group containing administrators you locate by running a custom query. Selecting this external type replaces the Search Text function but displays the Custom Query section.
Directory Name	Read-only setting displaying the address of your directory services server.
Domain and **Group Base DN**	This information automatically populates based on the directory services server information you enter on the **Directory Services** page (**Accounts > User Groups > Settings > Directory Services**). Select the **Fetch DN** plus sign (+) next to the **Group Base DN** setting, which displays a list of Base Domain Names from which you can select.
Search Text	Enter the search criteria to identify the name of an admin group in your directory and select **Search** to search for it. If a directory group contains your search text, a list of group names displays. Also, you can apply default roles to the admin group you are creating. After a successful search is run, select the **Roles** tab and then select the **Add** button to add a new role. Or edit an existing role by changing the **Organization Group** and **Role** selection. This setting is available only when **Group** or **Organizational Unit** is selected as the **External Type**.

Setting	Description
Custom Object Class	Identifies the object class under which your query runs. The default object class is 'person' but you can supply a custom object class to identify your admins with greater accuracy. This setting is available only when **Custom Query** is selected as **External Type**.
Custom Base DN	Identifies the base distinguished name which serves as the starting point of your query. The default is 'airwatch' and 'sso' but you can supply a custom base distinguished name if you want to run the query from a different starting point. This setting is available only when **Custom Query** is selected as **External Type**.
Group Name	Select a **Group Name** from your **Search Text** results list. Selecting a group name automatically alters the value in the Distinguished Name setting. This setting is available only after you have completed a successful search with the **Search Text** setting.
Distinguished Name	Read-only setting that displays the full distinguished name of the admin group you are creating. This setting is available only after you have completed a successful search with the **Search Text** setting.
Rank	Read-only setting that displays the rank of the admin group once it is created. You can change an admin group's rank by navigating to **Groups & Settings > Groups > Admin Groups** and moving its relative position using the More action button ▼ to the right of the admin group listing.
Auto Sync	This option enables the directory sync, which detects user membership from the directory server and stores it in a temporary table. An administrator approves all changes to the console unless the **Auto Merge** option is enabled.
Auto Merge	Enable this option to apply sync changes automatically from the database without administrative approval.
Maximum Allowable Changes	Use this setting to set a threshold for the number of automatic admin group sync changes that can occur before approval must be given. This option is available only when **Auto Merge** is enabled.
Add Group Members Automatically	Enable this option to add administrators automatically to the admin group.
Time Zone	Enter the time zone associated with the admin group. This required setting impacts when the scheduled, automated Active Directory sync runs.
Locale	Select the localization setting (language) associated with the admin group. This setting is required.
Initial Landing Page	Enter the initial landing page for administrators in the admin group. The default setting for this required setting is the Device Dashboard but you can set it to any page of your choice.
Custom Query	
Query	This setting displays the currently loaded query that runs when you select the **Test Query** button and when you select the **Continue** button. Changes you make to the **Custom Logic** option or the **Custom Object Class** setting are reflected here.
Custom Logic	Add your custom query logic here, such as an admin name. For example, "cn=jsmith". You can include as much or as little of the distinguished name as you like. The **Test Query** button allows you to see if the syntax of your query results in a successful search before selecting the **Continue** button.

For more information on Distinguished Name, search for Microsoft's TechNet article entitled "Object Naming" at https://technet.microsoft.com/.

2 Select **Save**.

View Assignments

As a convenience, you can confirm the profiles, apps, books, channels, and compliance policies that are included in (and excluded from) the assigned group.

Procedure

1 Navigate to the group listing in **Groups & Settings > Groups > Assignment Groups** and locate a group that has been assigned to at least one entity.

2 In the **Assignments** column, select the hyperlinked number to open the **View Assignments** page. This page displays only those categories that contain **Assignments** or **Exclusions** in the group.

What to do next

Above the header row in the **View Assignments** screen, you can use the **Refresh** button, the **Export** button, and the **Search List** text box to help you locate and confirm that the specific profile, app, book, channel, and compliance policy has been assigned.

Device Assignments

6

Device Assignments enable you to move devices across organization groups (OG) and user names based on the network Internet protocol (IP) address range or custom attributes. It is an alternative to organizing the content (for example, profiles, apps, policies, and products) by user groups.

Instead of admins manually moving devices between OGs, you can direct the console to move devices automatically when it connects to Wi-Fi that you define. You can also move devices based on custom attribute rules that you define.

A typical use case for device assignments is a user who regularly changes roles and requires specialized profiles and applications for each role.

You must choose between implementing **User Groups** and **Device Assignments** to move devices since Workspace ONE UEM does not support both functions on the same device.

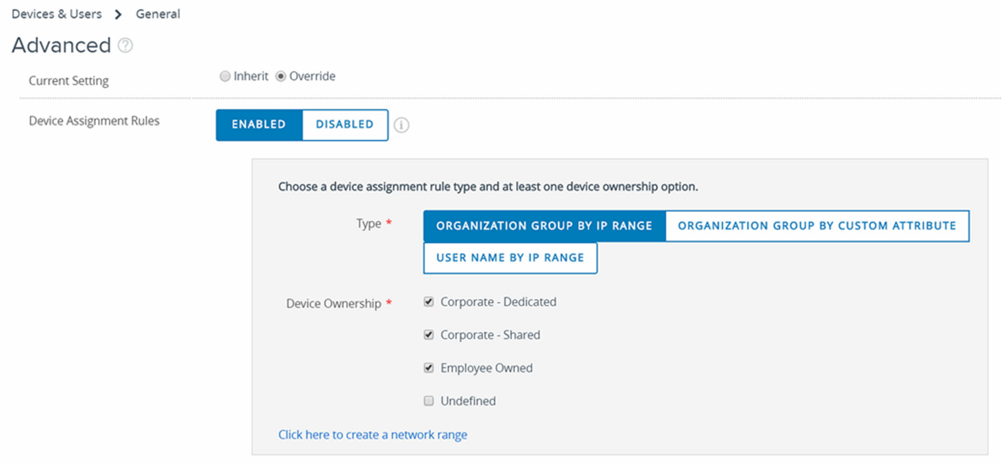
This chapter includes the following topics:

Enable Device Assignments

Before you can move devices across organization groups (OG) and user names based on an Internet protocol (IP) or custom attribute, you must enable device assignments. Device assignments can only be configured at a child organization group.

Procedure

1. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Advanced** and select **Override** or **Inherit** for the **Current Setting** according to your needs.



Devices & Users > General

Advanced

Current Setting ○ Inherit ● Override

Device Assignment Rules **ENABLED** DISABLED

Choose a device assignment rule type and at least one device ownership option.

Type * **ORGANIZATION GROUP BY IP RANGE** ORGANIZATION GROUP BY CUSTOM ATTRIBUTE USER NAME BY IP RANGE

Device Ownership *
☑ Corporate - Dedicated
☑ Corporate - Shared
☑ Employee Owned
☐ Undefined

Click here to create a network range

2. Select **Enabled** in the **Device Assignment Rules** setting.
3. Choose the management **Type**.

   - **Organization Group By IP Range** – Moves the device to a specified OG when the device leaves one Wi-Fi network range and enters another. This move triggers the automatic push of profiles, apps, policies, and products.
   - **Organization Group By Custom Attribute** – Moves the device to an organization group based on custom attributes.

     Custom attributes enable administrators to extract specific values from a managed device and return it to the Workspace ONE UEM console. You can also assign the attribute value to devices for use in product provisioning or device lookup values.

     - When **Organization Group By Custom Attribute** is enabled, a link appears entitled **Click Here To Create Custom Attribute Based Assignment Rule**. When selected, this link opens another tab in your browser. This tab displays the **Custom Attribute Assignment Rules** page, enabling you to create your own attribute assignment rules. For more information, see Assign Organization Groups Using Custom Attributes.

- **User name By IP Range** – When a device exits one network and enters another, the device changes user names instead of moving to another OG. This user name change triggers the same push of profiles, apps, policies, and products as an OG change does. This option is for customers with a limited ability to create organization groups, providing an alternate way to take advantage of the device assignment feature.

  Important If you want to change the assignment **Type** on an existing assignment configuration, you must delete all existing defined ranges. Remove IP Range assignments by navigating to **Groups & Settings > Groups > Organization Groups > Network Ranges**. Remove custom attribute assignments by navigating to **Devices > Provisioning > Custom Attributes > Custom Attribute Assignment Rules**.

4. Choose the **Device Ownership** options. Only devices with the selected ownership types are assigned.

   - Corporate – Dedicated
   - Corporate – Shared
   - Employee Owned
   - Undefined

5. You can add a network range by selecting the link, **Click here to create a network range**.

   You can alternatively visit this page by navigating to **Groups & Settings > Groups > Organization Groups > Network Ranges**. The Network Ranges settings selection is only visible if **Device Assignments** has been enabled for the Organization Group you are in when you visit this location. For more information, see Define Device Assignment Rule or Network Range.

   When selected, the **Network Ranges** page is displayed.

6. Select **Save** once all the options are set.

Define Device Assignment Rule or Network Range

When your device connects to Wi-Fi, the device authenticates and automatically installs profiles, apps, policies, and product provisions specific to the OG that you select.

You can also define rules based on custom attributes. When a device enrolls with an assigned attribute, the rule assigns the device to the configured organization group. The device can also be assigned in the case where the device receives a product provision containing a qualifying custom attribute.

Device assignments can only be configured at a child organization group.

Procedure

1. Navigate to **Groups & Settings > Groups > Organization Groups > Network Ranges**.

   The Network Ranges option is not visible until you enable device assignments. So if you cannot find 'Network Ranges' in the Organization Groups navigation path, see Enable Device Assignments.

2 To add a single Internet protocol (IP) address range, select **Add Network Range**. In the **Add/Edit Network Range** page, complete the following settings and then select **Save**.

Table 6-1. Add Network Range

Setting	Description
Start IP Address	Enter the top end of the network range.
End IP Address	Enter the bottom end of the network range.
Organization Group Name	Enter the OG name to which devices move when the network range is entered. This setting is only visible if the network assignment **Type** is 'Organization Group By IP Range.'
User name	Enter the user name to whom devices register when the network range is entered. This setting is only visible if the network assignment **Type** is 'User name by IP Range.'
Description	Optionally, add a helpful description of the network range.

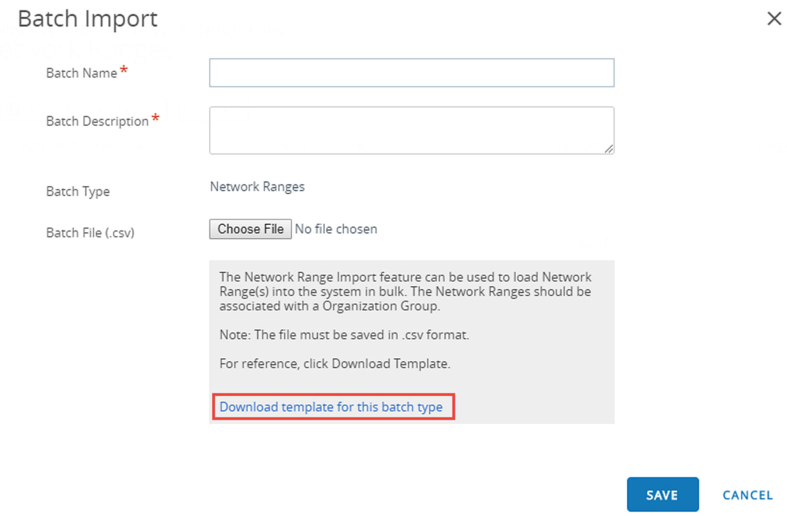
Overlapping network ranges results in the message, "Save Failed, Network Range exists."

3 If you have several network ranges to add, you can optionally select **Batch Import** to save time.

a On the Batch Import page, select the **Download template for this batch type** link to view and download the bulk import template.

b Complete this template, import it using the **Batch Import** page.

c Select **Save**.



Batch Import

Batch Name*	
Batch Description*	
Batch Type	Network Ranges
Batch File (.csv)	Choose File No file chosen

The Network Range Import feature can be used to load Network Range(s) into the system in bulk. The Network Ranges should be associated with a Organization Group.

Note: The file must be saved in .csv format.

For reference, click Download Template.

Device Profiles

7

Device Profiles are the primary means by which you can manage devices. They represent the settings that, when combined with compliance policies, help you enforce corporate rules and procedures.

Create profiles for each platform type then configure a payload, which consists of the individual settings you configure for each platform type.

The process for creating a profile consists of first specifying the **General** settings followed by the **Payload** settings.

- The **General** settings determine how the profile is deployed and who receives it.
- The **Payload** for the profile is the actual restriction itself and other settings as applied to the device when the profile is installed.

This chapter includes the following topics:

Profile Processing

Device profiles provide a standardized foundation for device management. Together with compliance policies, device profiles are the mechanism by which device management becomes such a valuable tool.

The processing and publishing of device profiles represents a significant server strain and must be governed to relieve this strain. The Workspace ONE UEM console uses a batching logic for the most processor-intensive types of device profiles. This batching logic can be adjusted by navigating to **Groups & Settings > All Settings > Installation > Performance Tuning**.

Add General Profile Settings

The following profile settings and options apply to most platforms and can be used as a general reference. However, some platforms can offer different selections. These steps and settings apply to any profile.

Procedure

1 Navigate to **Devices > Profiles & Resources > Profiles > ADD**.

You can select from among the following options to add a profile.

- **Add Profile** – Perform a one-off addition of a new device profile.
- **Upload Profile** – Upload a signed profile on your device.
- **Batch Import** – Import new device profiles in bulk by using a comma-separated values (CSV) file. Enter a unique name and description to group and organize multiple profiles at a time.

2 Select **Add Profile**.

3 Select the appropriate platform for the profile you want to deploy.

Depending on the platform, the payload settings vary.

4 Complete the **General** tab by completing the following settings.

Setting	Description
Name	Name of the profile to be displayed in the Workspace ONE UEM console.
Version	Read-only text box that reports the current version of the profile as determined by the **Add Version**.
Description	A brief description of the profile that indicates its purpose.
Deployment	Determines if the profile is automatically removed upon unenrollment (does not apply to Android profiles). ■ **Managed** – The profile is removed. ■ **Manual** – The profile remains installed until removed by the end user.
Assignment Type	Determines how the profile is deployed to devices. ■ **Auto** – The profile is deployed to all devices. ■ **Optional** – An end user can optionally install the profile from the Self-Service Portal (SSP), or it can be deployed to individual devices at the administrator's discretion. End users can also install profiles representing Web applications, using a Web Clip or a Bookmark payload. And if you configure the payload to show in the App Catalog, then you can install it from the App Catalog. ■ **Interactive** – **(Does not apply to iOS or Android)**. This profile is of a unique type that end users install with the Self Service Portal. When installed, these special types of profiles interact with external systems to generate data meant to be sent to the device. This option is only available if enabled in **Groups & Settings > All Settings > Devices & Users > Advanced > Profile Options**. ■ **Compliance** – The profile is applied to the device by the Compliance Engine when the user fails to take corrective action toward making their device compliant. For more information, see Compliance Profiles.

Setting	Description
Allow Removal	■ **Always** – The end user can manually remove the profile at any time. ■ **With Authorization** – The end user can remove the profile with the authorization of the administrator. Selecting this option adds an account **Password** text box. ■ **Never** – The end user cannot remove the profile from the device.
Managed By	The organization group with administrative access to the profile.
Assigned Groups	Refers to the group to which you want the device profile added. Includes an option to create a new smart group which can be configured with specs for minimum OS, device models, ownership categories, organization groups and more. For more information, see Assignment Groups. While Platform is a criterion within a smart group, the platform configured in the device profile or compliance policy always takes precedence over the smart group's platform. For instance, if a device profile is created for the iOS platform, the profile is only assigned to iOS devices even if the smart group includes Android devices.
Exclusions	If **Yes** is selected, a new text box **Excluded Groups** displays. This text box enables you to select those groups you want to exclude from the assignment of the device profile. See Exclude Groups in Profiles and Policies for details.
View Device Assignment	After you make an **Assigned Group** selection, you can preview a list of all assigned devices, taking the smart group assignments and exclusions into account.
Additional Assignment Criteria	These check boxes enable additional restrictions for the profile. ■ **Install only on devices inside selected areas.** – Enter an address anywhere in the world and a radius in kilometers or miles to make a 'perimeter of profile installation'. For more information, see Geofence Areas. ■ **Enable Scheduling and install only during selected time periods** – Specify a configured time schedule in which devices receive the profile only within that time-frame. Selecting this option adds a required text box **Assigned Schedules**. For more information, please see Time Schedules.
Removal Date	The date when the profile is removed from the device. Must be a future date formatted as MM/DD/YYYY.

5 Configure a **Payload** for the device platform.

For step-by-step instructions on configuring a specific **Payload** for a particular platform, refer to the applicable **Platform Guide**, available on docs.vmware.com.

6 Select **Save & Publish**.

Device Profiles List View

After you create and assign profiles, you need a way to manage these settings one at a time and remotely from a single source. The **Devices > Profiles & Resources > Profiles** provides a centralized way to organize and target profiles.

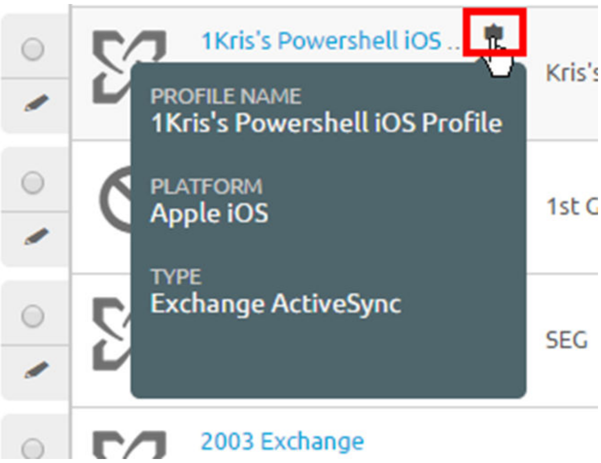
You can create tailor-made lists of device profiles based on the criteria you specify by using **Filters**, **Layout**, and **Column Sorting**. You can also export these lists to a CSV file suitable for viewing with Excel and see the status of the device profile.

Setting	Description
Filters	View only the desired profiles by using the following filters. - **Status** – Filter devices to view Active, Inactive, and All devices. - **Platform** – Filter devices by 13 types of platforms or all platforms. - **Smart Group** – Filter devices by selecting a smart group from the drop-down menu.
Layout	Enables you to customize the column layout of the listing. - **Summary** – View the **List View** with the default columns and view settings. - **Custom** – Select only the columns in the **List View** you want to see. You can also apply selected columns to all administrators at or below the current organization group.
Export ↗	Save a CSV file (comma-separated values) of the entire **List View** that can be viewed and analyzed in Excel. If you have a filter applied to the **List View**, the exported listing reflects the filtered results.
Column Sorting	Select the column heading to toggle the sorting of the list.
Profile Details	In both the **Summary** and **Custom** views, the **Profile Details** column, each profile features an icon representing the payload type. ✉ – Single payload types feature a unique icon for that individual payload type. 📶 8 – Profiles featuring multiple payloads of the same type feature a number badge in the upper-right corner of the icon. ⚙ 2 – Profiles featuring multiple payloads of differing types feature a generic icon with a number badge.
Installed Status	This column shows the status of a profile installation by displaying three icon indicators, each with a hypertext number link. Selecting this link displays the **View Devices** page, which is a listing of affected devices in the selected category. - **Installed** (✓) – This indicator displays the number of devices on which the profile is assigned and successfully installed. - **Not Installed** (⊖) – This indicator displays the number of devices to which the profile is assigned but not installed. - **Assigned** (👤) – This indicator displays the total number of assigned profiles whether they are installed or not.
Radio button and **Edit Icon**	The **List View** features a selection radio button and **Edit** icon, each to the left of the profile. Selecting the **Edit** icon (✎) enables you to make basic changes to the profile configuration. Selecting a single radio button causes the **Devices** button, the **XML** button, and **More Actions** button to appear above the listing. - **Devices** – View devices that are available for that profile and whether the profile is installed and if not, see the reason why. Survey which devices are in your fleet and manually push profiles if necessary. - **</ > XML** – Display the XML code that Workspace ONE UEM generates after profile creation. View and save the XML code to reuse or alter outside of the Console. - **More Actions** - **Copy** – Make a copy of an existing profile and tweak the configuration of the copy to get started with device profiles. - **Activate/Deactivate** – Toggle between making a device profile active and inactive. - **Delete** – Maintain your roster of profiles by removing unnecessary profiles.

Device Profile Hover-Over Pop-Up

Each device profile in the **Profile Details** column features a tool tip icon in the upper-right corner. When this icon is tapped (mobile touch device) or hovered-over with a mouse pointer (PC or Mac), it displays a hover-over pop-up.

This pop-up contains profile information such as **Profile Name**, the **Platform**, and the included payload **Type**.



1Kris's Powershell iOS ..

Kris's

PROFILE NAME
1Kris's Powershell iOS Profile

PLATFORM
Apple iOS

TYPE
Exchange ActiveSync

1st C

SEG

2003 Exchange

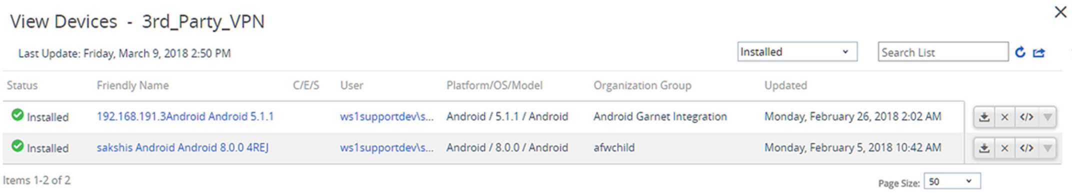
A similar tooltip icon is found in the **Assigned Groups** column in the **Profiles List** view, featuring hover-over pop-ups displaying **Assigned Smart Groups** and **Deployment Type**.

Confirm Device Profile Installation

During those infrequent cases in which profiles do not install on targeted devices, the **View Devices** screen enables you to see the specific reason why.

Procedure

1 Navigate to **Devices > Profiles & Resources > Profiles** and select the number links to the right of the **Installed Status** column to open the **View Devices** screen.



View Devices - 3rd_Party_VPN

Last Update: Friday, March 9, 2018 2:50 PM

Installed

Search List

Status	Friendly Name	C/E/S	User	Platform/OS/Model	Organization Group	Updated
✓ Installed	192.168.191.3Android Android 5.1.1		ws1supportdev\s...	Android / 5.1.1 / Android	Android Garnet Integration	Monday, February 26, 2018 2:02 AM
✓ Installed	sakshis Android Android 8.0.0 4REJ		ws1supportdev\s...	Android / 8.0.0 / Android	afwchild	Monday, February 5, 2018 10:42 AM

Items 1-2 of 2

Page Size: 50

2 (Optional) Produce a comma-separated value (CSV) file of the entire **View Devices** page by selecting the **Export** icon (↗).

Excel can be used to read and analyze the CSV file.

3 (Optional) Customize which columns in the **View Devices** page you want to be visible by selecting the **Available Columns** icon (⚒).

View Devices Command Status Column

iOS devices feature a **Command Status** column on the **View Devices** screen which includes useful installation statuses as they relate to the selected iOS device.

The following statuses appear in the Command Status column.

- **Error** – Displays as a link that, when selected, shows the specific error code applicable to the device.
- **Held** – Displays when the device is included in a certificate batch process that is underway.
- **Not Applicable** – Displays when the profile assignment does not impact the device but is nonetheless part of the smart group or deployment. For example, when the profile type is unmanaged.
- **Not Now** – Displays when the device is locked or otherwise occupied.
- **Pending** – Displays when the installation is queued and is on schedule to be completed.
- **Success** – Displays when the profile is successfully installed.

Device Profiles Read-Only View

Device Profiles created in and managed by one organization group (OG) are in a read-only state when accessed by a logged-in administrator with lower-level privileges. The profile window reflects this read-only state by adding a special comment, “this profile is being managed at a higher organization group and cannot be edited.”.

This read-only limitation applies to smart group assignments as well. When a profile is created at a parent OG and is assigned to a smart group, a child OG admin can see but not edit it.

Such behavior maintains a hierarchy-based security and fosters communication among admins.

Device Profile Editing

Using the Workspace ONE UEM console, you can edit a device profile that has already been installed to devices in your fleet. There are two types of changes you can make to any device profile.

- **General** – General profile settings serve to manage the profile distribution: how the profile is assigned, by which organization group it is managed, to/from which smart group it is assigned/excluded.
- **Payload** – Payload profile settings affect the device itself: passcode requirement, device restrictions such as camera use or screen capture, Wi-Fi configurations, VPN among others.

Since the operation of the device itself is not impacted, **General** changes can usually be made without republishing the profile. Saving such changes results in the profile only being pushed to devices that were not already assigned to the profile.

Payload changes, however, must always be republished to all devices, new and existing, since the operation of the device itself is affected.

Edit General Device Profile Settings

General profile settings include changes that manage its distribution only. This distribution includes how the profile is assigned, by which organization group (OG) it is managed, and to/from which assignment group it is assigned/excluded.

For more information, see Add General Profile Settings and View Device Assignment.

Procedure

1. Navigate to **Devices > Profiles & Resources > Profiles** and select the **Edit** icon (✎) from the actions menu of the profile you want to edit.

   The only profiles that are editable are those profiles that an organization group (or a child organization group underneath) manages.

2. Make any changes you like in the **General** category.

3. After completing **General** changes, you may select **Save & Publish** to apply the profile to any new devices you may have added or removed.

Results

Devices already assigned with the profile do receive the republished profile again. The **View Device Assignment** screen appears, confirming the list of currently assigned devices.

Edit Payload Device Profile Settings

Payload profile settings include changes that affect the device itself: passcode requirement, device restrictions such as camera use or screen capture, Wi-Fi configurations, VPN among others.

The **Add Version** button enables you to create an increment version of the profile where settings in the **Payload** can be modified.

Procedure

1. Enable **Payload** editing that impacts the operation of the device by selecting the **Add Version** button.

   Selecting the **Add Version** button and saving your changes means republishing the device profile to all devices to which it is assigned. This republishing includes devices that already have the profile.

   For step-by-step instructions on configuring a specific **Payload**, refer to the applicable **Platform Guide**, available on docs.vmware.com.

2. After completing **Payload** changes, select **Save & Publish** to apply the profile to all assigned devices.

Results

The **View Device Assignment** screen appears, enabling you to confirm the list of currently assigned devices.

Compliance Profiles

To understand Compliance Profiles, you must have a full understanding of device profiles and compliance policies. Device profiles serve as the foundation for device management and security while compliance policies act as a security gate protecting corporate content.

Device profiles grant you control over a wide range of device settings. These settings include passcode complexity, Geofencing, time schedules, device hardware functionality, Wi-Fi, VPN, Email, Certificates, and many more.

The compliance engine monitors rules, enforces actions, and applies escalations (all of which you define). Compliance profiles, however, seek to provide the compliance engine with all the options and settings ordinarily available only to device profiles. For more information, see Chapter 9 Compliance Policies.

For example, you can make a special device profile that is identical to your normal device profile, only with more restrictive settings. You can then apply this special device profile in the Actions tab when you define your compliance policy. With such an arrangement, if the user fails to make their device compliant, you can apply the more restrictive compliance profile.

Add a Compliance Profile

You can add a compliance profile, which is a hybrid of a compliance policy and a device profile, joining the best of these two features together. Adding a compliance profile is a two part process: 1) make a device profile and 2) assign it as an 'action' in a compliance policy.

Compliance profiles are created and saved in the same manner as Auto and Optional device profiles.

Procedure

1. Navigate to **Devices > Profiles & Resources > Profiles**, then select **Add**, then **Add Profile**, then select a platform.
2. Select a **Name** for your compliance profile that you can recognize later.
3. In the **General** profile tab, select 'Compliance' in the **Assignment Type** drop-down setting.
4. Complete the remaining General and Payload settings.
5. When finished, select **Save & Publish**.
6. Select this profile in your compliance policy.
7. Navigate to **Devices > Compliance Policies > List View** and select **Add**, then select a platform.
8. Define the **Rules** and select **Next**.
9. In the **Actions** tab, make the following selections.
   a. Set the first drop-down menu to 'Profile'.
   b. Set the second drop-down menu to 'Install Compliance Profile'.
   c. Set the third drop-down menu to the device profile you named.
10. Select **Next** and proceed configuring the remaining settings including Assignment and Summary tabs.

11 Save the compliance policy by selecting **Finish** or **Finish and Activate**.

What to do next

For step-by-step instructions on completing a device profile, see Add General Profile Settings.

For step-by-step instructions on completing a compliance policy, see Add a Compliance Policy.

Geofence Areas

Workspace ONE UEM enables you to define your profile with a Geofencing Area. A geofence area limits the use of the device to specific areas including corporate offices, school buildings, and retail department stores. You can think of a geofence area as a virtual perimeter for a real-world geographic area.

For example, a geofence area with a 1-mile radius can apply to your office, while a much larger geofence area can apply approximately to an entire state. Once you have defined a geofence area you can apply it to profiles, SDK applications, and Workspace ONE UEM apps such as the VMware Content Locker, and more.

- Enabling a Geofence Area is a two-step process.
  a Add Geofencing Area.
  b Apply a Geofence to a Profile.
- Geofencing is available for Android and iOS devices.
- Remember that while Geofencing is combined with another payload to enable security profiles based on location, consider having only one payload per profile.

For more information about how Workspace ONE UEM tracks GPS location, see the following VMware Knowledge Base article: https://support.workspaceone.com/articles/115001663108.

Geofencing Support on iOS Devices

Geofencing for apps only works on iOS devices that have **Location Services** running. In order for location services to function, the device must be connected to either a cellular network or a Wi-Fi hotspot. Otherwise, the device must have integrated GPS capabilities.

For Wi-Fi only devices, GPS data is reported when the device is on, unlocked, and the Workspace ONE Intelligent Hub is open and being used. For cellular devices, GPS data is reported when the device changes cell towers. VMware Browser and Content Locker reports GPS data (using Workspace ONE Intelligent Hub) when the end user opens and uses them.

Devices in an "airplane mode" result in location services (and therefore Geofencing) being deactivated.

Device	Wi-Fi	Cellular Network	Built-In GPS
iPhone	✓	✓	✓
iPad Wi-Fi + 3G/4G	✓	✓	✓
iPad Wi-Fi	✓		
iPod Touch	✓		

The following requirements must all be met for the GPS location to be updated.

- The device must have the Workspace ONE Intelligent Hub running.
- Privacy settings must allow GPS location data to be collected (**Groups & Settings > All Settings > Devices & Users > General > Privacy**).
- The settings for Workspace ONE Intelligent Hub for Apple iOS must enable “Collect Location Data” (**Groups & Settings > All Settings > Devices & Users > Apple > Apple iOS > Hub Settings**).

  Set the Workspace ONE Intelligent Hub SDK settings to the Default SDK settings instead of "None".

Add Geofencing Area

You must define a Geofencing area before you can apply one to a device.

Procedure

1. Access the Area settings page by navigating to **Devices > Profiles & Resources > Profile Settings > Areas**. Select **Add** followed by **Geofencing Area**.
2. Enter an **Address** and the **Radius** of the geofence in kilometers or miles.

   You can double-click any area on the map to set the central location.
3. Select **Click to Search** to view on a map roughly where you want to apply the geofence.

   Note Integration with Bing maps requires that "insecure content" is loaded on this page. If a location search does not load as expected, you might need to allow "Show all Content" for your browser.
4. Enter the **Area Name** (how it appears in the Workspace ONE UEM console) and select **Save**.

What to do next

Next, you must apply a geofence to a profile. For more information, see Apply a Geofence to a Profile.

Apply a Geofence to a Profile

Once you have added a Geofencing area, you can apply it to a profile and combine it with other payloads to create more robust profiles.

If a user manually disables location services on their iOS device, Workspace ONE UEM can no longer collect location updates. Workspace ONE UEM considers the device to be in the location where services were disabled.

Procedure

1. Navigate to **Devices > Profiles & Resources > Profiles > ADD** and select a platform.
2. Select **Install only on devices inside selected areas** on the **General** tab.

   An **Assigned Geofence Areas** box displays. If no Geofence Area has been defined, the menu directs you back to the Geofence Area creation menu.
3. Enter one or multiple Geofencing areas to this profile.

4 Configure a payload such as Passcode, Restrictions, or Wi-Fi that you want to apply only while devices are inside the selected Geofencing areas.

5 Select **Save & Publish**.

Example

For example, you can define geofence areas around each of your offices. Then add a Restrictions payload that disallows access to the Game Center, multiplayer gaming, YouTube content, and other settings. Once activated, employees of the organization group to whom the profile is applied no longer have access to these functions while in the office.

iBeacons

iBeacon is a bluetooth-based proximity sensing protocol developed by Apple. As such, it is exclusive to certain Apple products.

iBeacon is specific to iOS and is used to manage location awareness. For more information, please see the **VMware AirWatch iOS Platform Guide**, available on docs.vmware.com.

Time Schedules

Time Schedules enable you to control when each device profile is active. The profile dictates how restrictive or permissive the device usability is. The time schedule simply puts the profile installation on a schedule.

Enabling a Time Schedule is a two-step process.

1 Define a Time Schedule.

For more information, see Define a Time Schedule

2 Apply a Time Schedule to a Profile.

For more information, see Apply a Time Schedule to a Profile

Define a Time Schedule

You must define a time schedule before applying it to a device profile.

Procedure

1 Navigate to **Devices > Profiles & Resources > Profiles Settings > Time Schedules**.

2 Select **Add Schedule** above the **Schedule Name** column.

3 Select **Add Schedule** located under the **Day of the Week** column, then complete the following settings.

Setting	Description
Schedule Name	Enter the name of the time schedule that appears in the listing.
Time Zone	Select the time zone of the organization group under which the device is managed.

Setting	Description
Day of the Week	Apply a scheduled profile installation by choosing a day of the week.
All Day	Make the profile install at midnight on the selected **Day of the Week**. Selecting this check box removes the **Start Time** and **End Time** columns.
Start Time	Select the time of day you want the profile to be installed.
End Time	Select the time of day you want the profile to be uninstalled.
Actions	Remove the day's schedule by clicking the **X**.

4 Select **Save**.

Apply a Time Schedule to a Profile

Once you have defined a time schedule, you can apply it to a new profile and combine it with other payloads to create more robust profiles. For instance, you can define time schedules for normal work hours and add a Restrictions payload that denies access to YouTube, multiplayer gaming, and other apps.

Once activated, the organization group users to whom the profile was applied no longer have access to these functions during the specified times.

Procedure

1 Navigate to **Devices > Profiles & Resources > Profiles > ADD** and select your platform.

2 Select **Enable Scheduling and install only during selected time periods** on the **General** tab.

3 In the **Assigned Schedules** box, enter one or more Time Schedules to this profile.

4 Configure a payload, such as Passcode, Restrictions, or Wi-Fi that you want to apply only while devices are inside the time frames.

5 Select **Save & Publish**.

Apply a Time Schedule to an Existing Profile

You can apply a previously defined time schedule to an existing profile, causing that profile to adhere to the time restrictions you design.

Procedure

1 Navigate to **Devices > Profiles & Resources > Profiles** and select the profile from the listing for editing. Select the pencil icon (✏) or click the profile name.

2 In the **General** tab of the profile page, enable the setting **Enable Scheduling and install only during selected time periods**.

3 In the **Assigned Schedule** setting that appears, select from the drop-down menu the previously saved time schedule.

4 Select **Save & Publish**.

Delete a Time Schedule

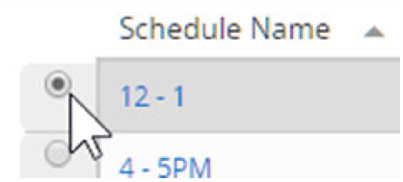
Keep your collection clear of unused time schedules by deleting them. You cannot delete a time schedule that is assigned to a profile. Unassign the schedule from the profile before deleting.

Prerequisites

Navigate to **Devices > Profiles & Resources > Profiles Settings > Time Schedules**.

Procedure

1 Select the radio button next to the time schedule you want to delete.



	Schedule Name ▲
●	12 - 1
○	4 - 5PM

2 Select the **Delete** button.

View Device Assignment

Selecting the **Save & Publish** button upon configuring a device profile displays the **View Device Assignment** page and serves as a preview of affected (or unaffected) devices.

Depending upon which kind of change you make to the device profile, the **Assignment Status** column reflects various states.

- **Added** – The profile is added and published to the device.
- **Removed** – The profile is removed from the device.
- **Unchanged** – Indicates that the profile is not scheduled to be republished to the device.
- **Updated** – Indicates that the profile is republished to a device that already has the profile assigned.

Select **Publish** to finalize the changes and, if necessary, republish any required profile.

Resources

8

Resources simplify the provisioning of Wi-Fi, VPN, and Exchange payloads for Workspace ONE UEM deployments that support multiple device platforms, such as iOS, Android, and Windows.

Create a resource for any of these payloads and define the general settings each device platform receives. You can then optionally configure platform-specific settings that apply only to those devices.

Resources are defined, managed, and deployed separately from device profiles. Deploy resources alongside device profiles to provide deep and broad device management for all supported platforms in your deployment.

You do not have to use resources to deploy Wi-Fi, VPN, or Exchange settings. If you choose, you can still create separate device profiles for these payloads for each platform. Consider deploying resources when you expect the Wi-Fi, VPN, or Exchange settings to be identical or similar across platforms. Then, create additional device profiles as usual to manage functionality further for each platform.

This chapter includes the following topics:

Resources List View

Use the Resources List View to add and manage your collection of device resources which includes viewing, deleting, and editing individual resource configurations.

Add a Resource

You can add a resource to provision your multi-platform device fleet with the same Exchange, wi-fi, and VPN settings.

Navigate to **Devices > Profiles & Resources > Resources** and select **Add Resource**. You must select from the following options to add a resource.

- **Exchange** – Configure email settings so you can keep in touch with your Exchange email server.
- **Wi-Fi** – Configure Wi-Fi connectivity settings so you can maintain network connectivity.

- **VPN** – Configure virtual private network settings so you can maintain a secure connection.

Each resource requires three distinct configuration steps. Create a device resource by specifying the **Resource Details**, the applicable **Platforms**, and the **Assignment** of the resource to devices.

- The **Resource Details** contain the resource name, description, server dependencies, and other critical settings that determine how the resource operates.
- The **Platforms** define on which devices the resource runs.
- The **Assignment** determines how the resource is deployed, including organization groups, user groups, and smart groups.

Manage Resources

Once you have amassed a collection of resources, you can manage them by navigating to **Devices > Profiles & Resources > Resources** and Filter, View, Edit, and Delete resources.

- **Filter** the Resource List View to show Active, Inactive, or All resources.
- View the different platforms which your resource includes by selecting the hyperlink numeral in the **Platforms** column.
  - Open **Advanced Settings** for the resource by selecting the hyperlink platform name.
  - Open the **View Devices** page by selecting the hyperlink numerals in the **Installed/Assigned** column of the Platforms page. This page displays the list of devices assigned to the resource.
  - View and Export the XML code and upload a certificate by clicking the **View** hyperlink in the XML column of the Platforms page.
- Edit a resource by selecting the name link of the resource which displays the **Resource Details** section of the **Edit Resource** page.
  - Edit the resource details by clicking the edit pencil (✎) to the left of the resource listing. You may proceed making edits to the other sections of the **Edit Resource** page by selecting the **Next** button.
- Edit the assignment of the resource by selecting the radio button to the left of the Resource listing and then clicking the **Edit Assignment** button.
- Delete a resource by selecting the radio button to the left of the resource listing and clicking the **Delete** button. Deleting a resource sets the resource to inactive until it is removed from all devices.

Add an Exchange Resource

You can add a resource dedicated to providing devices with the means to send and receive secure email communications.

For an overview, see Chapter 8 Resources.

Procedure

1 Navigate to **Devices > Profiles & Resources > Resources** and select **Add Resource** followed by **Exchange** and complete the following settings.

Setting	Description
Resource Details	
Resource Name	Name of the profile to be displayed in the Workspace ONE UEM console.
Description	A brief description of the profile that indicates its purpose.
Connection Info	
Mail Client	Select the email client you want to use with the resource.
Exchange Host	Enter the Exchange Host for the email account to be included in the resource.
Use SSL	Enable a secure socket layer for this mail client.
Advanced	
Domain*	Enter a lookup value for the email domain.
User name*	Enter a lookup value for the email user name.
Email Address*	Enter a lookup value for the email address.
Password	Enter the password for the email account. Enable the **Show Characters** check box to display the unredacted password.
Identity Certificate	Upload and attach a certificate authority to the email account by selecting the **Add A Certificate** button.
Past Days of Mail to Sync	Select the length of email history you want to synchronize. Choose from **3 Days**, **1 Week**, **2 Weeks**, **1 Month**, and **Unlimited**.
Sync Calendar	Choose to synchronize your device calendar with the exchange calendar. This setting is enabled by default on iOS and macOS devices.
Sync Contacts	Choose to synchronize your device contacts with the exchange contacts. This setting is enabled by default on iOS and macOS devices.

* For details, see Lookup Values.

2 Click **Next** to proceed to the **Platforms** selection. Choose among the following supported platforms, opting for either the default settings or **Advanced Settings**.

- Configure Advanced Settings for iOS Exchange.
- Configure Advanced Settings for macOS Exchange.
- Configure Advanced Settings for Android Exchange.
- Configure Advanced Settings for Windows Phone Exchange.
- Configure Advanced Settings for Windows Desktop Exchange.

3 Click **Next** to proceed to the **Assignment** section.

4 Assign the resource to devices by completing the following settings.

Setting	Description
Assignment Type	Determines how the resource is deployed to devices. ■ **Auto** – The resource is deployed to all devices automatically. ■ **Optional** – An end user can optionally install the resource from the Self-Service Portal (SSP), or it can be deployed to individual devices at the discretion of the administrator.
Managed By	The organization group with administrative access to the resource.
Assigned Groups	Refers to the group to which you want the device resource added. Includes an option to create a new smart group which can be configured with specs for minimum OS, device models, ownership categories, organization groups and more.
Exclusions	If **Yes** is selected, a new text box **Excluded Groups** displays which enables you to select those groups you want to exclude from the assignment of this resource.
View Device Assignment	After you have made a selection in the **Assigned Group** text box, you may select this button to preview a list of all devices to which this resource is assigned, taking the smart group assignments and exclusions into account.

Configure Advanced Settings for iOS Exchange

Advanced Exchange settings for iOS consist of S/MIME and Security configuration options, providing user-specific, certificate-based encryption of email.

Setting	Description
Use S/MIME.	Use Secure Multipurpose Internet Mail Extensions, a public key encryption and signing standard.
S/MIME Certificate	Only available when **Use S/MIME** is enabled. Add a signing certificate to emails by selecting **Add A Certificate**.
S/MIME Encryption Certificate	Only available when **Use S/MIME** is enabled. Add a certificate that encrypts and digitally signs email by selecting **Add A Certificate**.
Enable Per-Message Switch.	Only available when **Use S/MIME** is enabled. Allow end users to choose which individual email messages to sign and encrypt using the native iOS mail client (iOS 8+ supervised only).
Settings and Security	
Prevent moving messages.	Prevent moving mail from an Exchange mailbox to another mailbox on the device.
Prevent use in third-party apps.	Prevent other apps from using the Exchange mailbox to send messages.
Prevent Recent Address syncing.	Prevent suggestions for contacts when sending mail in Exchange.
Prevent Mail Drop.	Prevent Apple's Mail Drop feature from being used.

Configure Advanced Settings for macOS Exchange

Enable your macOS devices to retrieve exchange email by configuring advanced settings.

Setting	Description
Internal Exchange Host	The name of the secure server for EAS use. This option and following appear when **Native Mail Client** is selected.
Port	Enter the number of the port assigned for communication with the Internal Exchange Host.
Internal Server Path	The location of the secure server for EAS use.
Use SSL For Internal Exchange Host.	Communicate with the Internal Exchange Host by enabling the Secure Socket Layer (SSL).
External Exchange Host.	The name of the external server for EAS use.
Port	Enter the number of the port assigned for communication with the External Exchange Host.
External Server Path	The location of the external server for EAS use.
Use SSL For External Exchange Host.	Communicate with the External Exchange Host by enabling the Secure Socket Layer (SSL).

Configure Advanced Settings for Android Exchange

Advanced Exchange settings for Android consist of historical syncing, restrictions, sync scheduling, and S/MIME. Configure these options to deliver email to your Android devices.

Setting	Description
Settings	
Past Days of Calendar to Sync	Synchronize a selected number of past days on the device calendar.
Allow Sync Tasks	Allow tasks to sync with device.
Maximum Email Truncation Size (KB)	Specify the size (in kilobytes) beyond which email messages are truncated when they are synced to the devices.
Email Signature	Enter the email signature to be displayed on outgoing emails.
Ignore SSL Errors	Allow devices to ignore SSL errors for Agent processes.
Restrictions	
Allow Attachments	Allow attachments with email.
Maximum Attachment Size	Specify the maximum attachment size in MB.
Allow Email Forwarding	Allow the forwarding of email.
Allow HTML Format	Specify whether email synchronized to the device can be in HTML format. If this setting is disabled, all email is converted to text.
Disable screenshots	Disallow screenshot to be taken on the device.
Sync Interval	Enter the number of minutes between syncs.
Peak Days for Sync Schedule	

Setting	Description
	■ Schedule the peak weekdays for syncing and the **Start Time** and **End Time** on selected days. ■ Set the frequency of **Sync Schedule Peak** and **Sync Schedule Off Peak**. ■ Selecting **Automatic** syncs email whenever updates occur. ■ Selecting **Manual** only syncs email when selected. ■ Selecting a time value syncs the email on a set schedule. ■ Enable **Use SSL**, **Use TLS**, and **Default Account**.
S/MIME Settings	
	Select **Use S/MIME** From here you can select an S/MIME certificate you associate as a **User Certificate** on the **Credentials** payload. ■ **S/MIME Certificate** – Select the certificate to be used. ■ **Require Encrypted S/MIME Messages** – Require encryption of S/MIME messages. ■ **Require Signed S/MIME Messages** – Require all S/MIME messages be digitally signed. Provide a **Migration Host** if you are using S/MIME certificates for encryption.

Configure Advanced Settings for Windows Phone Exchange

Advanced Exchange settings for Windows Phone consist of sync scheduling and data protection settings. Configure these settings to deliver exchange email to your devices securely.

Settings	Descriptions
Settings	
Next Sync Interval (Min)	Enter the number of minutes between syncs.
Diagnostic Logging	Select the type of diagnostic logging you want to gather.
Content Type	
Require Data Protection Under Lock	Protect data when a device is pin locked. When the device is configured to use a pin lock, the protected data is encrypted using a separate enterprise key. If someone gains access to the device pin lock, your organization's email and data is protected by a separate key.
Protected Domains	Available only when **Require Data Protection Under Lock** is enabled. Enter the lookup values of the exchange domains that you want to protect. For details, see Lookup Values.
Allow Email Sync	Allow the syncing of email. Disabling this setting removes access to email through Exchange Active Sync.

Configure Advanced Settings for Windows Desktop Exchange

Advanced Exchange settings for Windows Desktop consist of sync scheduling and data protection settings. Configure these settings to deliver exchange email to your devices securely.

Settings	Descriptions
Settings	
Next Sync Interval (Min)	Select the frequency, in minutes, that the device syncs with the EAS server.
Diagnostic Logging	Log information for troubleshooting purposes.

Settings	Descriptions
Content Type	
Allow Email Sync	Allow the syncing of email messages.

Add a Wi-Fi Resource

You can add a resource dedicated to providing devices with the means to connect to a wireless network, allowing them to send and receive data securely.

Procedure

1 Navigate to **Devices > Profiles & Resources > Resources** and select **Add Resource** followed by **Wi-Fi** and complete the following settings.

Setting	Description
Resource Details	
Resource Name	Name of the profile to be displayed in the Workspace ONE UEM console.
Description	A brief description of the profile that indicates its purpose.
Connection Info	
Service Set Identifier	Enter an identifier that is associated with the name (SSID) of the desired Wi-Fi network.
Hidden Network	Enable if the network is not open to broadcast.
Auto-Join	Setting that directs the device to join the network automatically.
Encryption	Use the drop-down menu to specify if data transmitted using the Wi-Fi connection is encrypted. Displays based on the **Security Type**.
Password	Enter the password for the email account. Enable the **Show Characters** check box to display the unredacted password.

2 Click **Next** to proceed to the **Platforms** selection. Choose among the following supported platforms, opting for either the default settings or **Advanced Settings**.

- Configure Advanced Settings for Wi-Fi Proxy.
- Configure Advanced Settings for macOS Wi-Fi.
- Configure Advanced Settings for Android Wi-Fi.
- Configure Advanced Settings for Windows Wi-Fi.

3 Click **Next** to proceed to the **Assignment** section.

4 Assign the resource to devices by completing the following settings.

Setting	Description
Assignment Type	Determines how the resource is deployed to devices. ■ **Auto** – The resource is deployed to all devices automatically. ■ **Optional** – An end user can optionally install the resource from the Self-Service Portal (SSP), or it can be deployed to individual devices at the discretion of the administrator.
Managed By	The organization group with administrative access to the resource.
Assigned Groups	Refers to the group to which you want the device resource added. Includes an option to create a new smart group which can be configured with specs for minimum OS, device models, ownership categories, organization groups and more.
Exclusions	If **Yes** is selected, a new text box **Excluded Groups** displays which enables you to select those groups you want to exclude from the assignment of this resource.
View Device Assignment	After you have made a selection in the **Assigned Group** text box, you may select this button to preview a list of all devices to which this resource is assigned, taking the smart group assignments and exclusions into account.

Configure Advanced Settings for Wi-Fi Proxy

Configure advanced Wi-Fi settings to connect devices to Workspace ONE UEM using a proxy.

Setting	Description
Proxy Type	Choose between **None**, **Manual**, and **Auto**.
Proxy URL	Available only when **Proxy Type** is **Auto**. Enter the URL of the Wi-Fi proxy that the device uses to connect.
Allow a direct connection if PAC is unreachable	Available only when **Proxy Type** is **Auto**. Enable if you want to allow the device to connect during times when the proxy auto config file is not accessible.
Proxy Server	Available only when **Proxy Type** is **Manual**. Enter the name of the proxy server to which your devices connect.
Proxy Server Port	Available only when **Proxy Type** is **Manual**. Include the port number of the proxy server through which the device connects to the proxy server.
Proxy user name	Available only when **Proxy Type** is **Manual**. Enter a user name recognized by the proxy server.
Proxy Password	Available only when **Proxy Type** is **Manual**. Enter the password that corresponds to the user name entered.

Configure Advanced Settings for macOS Wi-Fi

Configure advanced Wi-Fi settings to connect your devices to Workspace ONE UEM using a proxy.

Setting	Description
Profile	Choose the target of the proxy settings configuration. **Device** – Limit the proxy settings to the specific macOS device **User** – Apply the proxy settings to the user of the macOS device. Apply proxy settings to both targets by inserting a check in both boxes.
Proxy	

Setting	Description
Proxy Type	Choose between **None**, **Manual**, and **Auto**.
Proxy URL	Available only when **Proxy Type** is **Auto**. Enter the URL of the Wi-Fi proxy that the device uses to connect.
Allow a direct connection if PAC is unreachable	Available only when **Proxy Type** is **Auto**. Enable if you want to allow the device to connect during times when the proxy auto config file is not accessible.
Proxy Server	Available only when **Proxy Type** is **Manual**. Enter the name of the proxy server to which your devices connect.
Proxy Server Port	Available only when **Proxy Type** is **Manual**. Include the port number of the proxy server through which the device connects to the proxy server.
Proxy user name	Available only when **Proxy Type** is **Manual**. Enter a user name recognized by the proxy server.
Proxy Password	Available only when **Proxy Type** is **Manual**. Enter the password that corresponds to the user name entered.

Configure Advanced Settings for Android Wi-Fi

Advanced Wi-Fi settings for Android consist of Fusion and Proxy settings. These settings allow you to specify wireless configurations for radio frequencies, spectral masks, and proxy server settings.

Setting	Description
Fusion	
Include Fusion Settings	Display the main settings for the Fusion feature.
Set Fusion 802.11d / **Enable 802.11d**	Use an 802.11d wireless specification for operation in additional regulatory domains.
Set Country Code / **Country Code**	Set the Country Code for use in the 802.11d specifications.
Set RF Band	Display all the Radio Frequency specification options including 2.4 GHz and 5-GHz channel masking.
Set 2.4 GHz / **Enable 2.4 GHz**	Use the 2.4-GHz wireless frequency.
2.4 GHz Channel Mask	Reduce adjacent channel interference by applying a channel or spectral mask around the 2.4-GHz frequency.
Set 5 GHz / **Enable 5 GHz**	Use the 5-GHz wireless frequency.
5 GHz Channel Mask	Reduce adjacent channel interference by applying a channel or spectral mask around the 5-GHz frequency.
Proxy	
Enable Manual Proxy	Display the proxy server settings.
Proxy Server	Enter the proxy domain name.
Proxy Server Port	Enter the port number to be used by the proxy server.
Exclusion List	Enter hostnames that are not routed through the proxy. Use an asterisk as a wildcard for the domain. For example, *.air-watch.com.

Configure Advanced Settings for Windows Wi-Fi

Configure advanced Wi-Fi settings to connect your Windows devices (desktop and phone) to Workspace ONE UEM using a proxy.

Setting	Description
Proxy	Enable the use of a proxy to connect your Windows devices to Workspace ONE UEM.
URL	Available only when **Proxy** is enabled. Enter the URL of the Wi-Fi proxy that the device uses to connect.
Port	Available only when **Proxy** is enabled. Include the port number of the proxy server through which the device connects to the proxy server.

Add a VPN Resource

You can add a resource dedicated to providing a virtual private network (VPN). A VPN enables users to send and receive data across public networks as though they were connected directly to a private network.

Procedure

1. Navigate to **Devices > Profiles & Resources > Resources** and select **Add Resource** followed by **VPN** and complete the following settings.

Setting	Description
Resource Details	
Resource Name	Name of the profile to be displayed in the Workspace ONE UEM console.
Description	A brief description of the profile that indicates its purpose.
Connection Info	
Connection Type	Select the type of secure connection from the drop-down listing.
Server	Enter the server URL.

2. Click **Next** to proceed to the **Platforms** selection. Choose among the following supported platforms, opting for either the default settings or **Advanced Settings**.

   - Configure Advanced Settings for iOS VPN
   - Configure Advanced Settings for Android VPN
   - Configure Advanced Settings for Windows Phone VPN

3. Click **Next** to proceed to the **Assignment** section.

4 Assign the resource to devices by completing the following settings.

Setting	Description
Assignment Type	Determines how the resource is deployed to devices. ■ **Auto** – The resource is deployed to all devices automatically. ■ **Optional** – An end user can optionally install the resource from the Self-Service Portal (SSP), or it can be deployed to individual devices at the discretion of the administrator.
Managed By	The organization group with administrative access to the resource.
Assigned Groups	Refers to the group to which you want the device resource added. Includes an option to create a new smart group which can be configured with specs for minimum OS, device models, ownership categories, organization groups and more.
Exclusions	If **Yes** is selected, a new text box **Excluded Groups** displays which enables you to select those groups you want to exclude from the assignment of this resource.
View Device Assignment	After you have made a selection in the **Assigned Group** text box, you may select this button to preview a list of all devices to which this resource is assigned, taking the smart group assignments and exclusions into account.

Configure Advanced Settings for iOS VPN

Advanced VPN settings for iOS consist of connection and authentication settings, proxy, and vendor configurations. Enable these settings as necessary to configure VPN for iOS.

Settings	Description
Connection Info	
Account	Enter the name of the VPN account.
Disconnect on Idle (min).	Allow the VPN to auto-disconnect after a specific amount of time. Support for this value depends on the VPN provider.
Send All Traffic.	Select to force all traffic through the specified network.
Per App VPN Rules	Select to enable and configure Per App VPN rules.
Connect Automatically.	Select to allow the VPN to connect automatically to Safari Domains. This option appears when the **Per App VPN Rules** check box is selected.
Provider Type	Select the type of Per-App VPN provider. Determine how to tunnel traffic, either through an application layer or IP layer by selecting between AppProxy and PacketTunnel. This option appears when the **Per App VPN Rules** check box is selected.
Safari Domains	Enter each domain to which you want the Per-App VPN to connect automatically. These domains are internal sites that trigger an automatic VPN connection. This option appears when the **Per App VPN Rules** check box is selected.
Authentication	
User Authentication	Authenticate end users by either uploading a **Certificate** or by requiring a **Password** for VPN access.
Group Name	Enter the Workspace ONE UEM group name.
Password	Available only when **User Authentication** is set to Password. Enter the password for the Workspace ONE UEM Group Name.

Settings	Description
Identity Certificate	This setting is only available when **User Authentication** is set to Certificate. Select **Add A Certificate** to either name and upload a certificate file or select an existing certificate authority using a certificate template.
Enable VPN On Demand.	This setting is only available when **User Authentication** is set to Certificate. Enable VPN On Demand to use certificates to establish VPN connections automatically.
Use new On-Demand keys.	This setting is only available when **User Authentication** is set to Certificate. Enable the option to activate a VPN connection when end users access any of the specified domains.
Match Domain or Host.	This setting is only available when **User Authentication** is set to Certificate. Enter a domain or hostname that, when accessed by an end user, triggers the activation of a VPN connection.
On-Demand Action	This setting is only available when **User Authentication** is set to Certificate. Select the domain-specific on-demand action that takes place when end users activate a VPN connection. Select among Always Establish, Never Establish, and Establish if Needed.
Proxy	
Proxy	Select among **None**, **Manual**, and **Auto**.
Proxy Server Auto Config URL	Available only when **Proxy** is **Auto**. Enter the URL of the Wi-Fi proxy that the device uses to connect.
Server	Available only when **Proxy** is **Manual**. Enter the name of the proxy server to which your devices connect.
Port	Available only when **Proxy** is **Manual**. Include the port number of the proxy server through which the device connects to the proxy server.
User name	Available only when **Proxy** is **Manual**. Enter a user name recognized by the proxy server.
Password	Available only when **Proxy** is **Manual**. Enter the password that corresponds to the user name entered.
Vendor Configurations	
Vendor Keys	Create custom keys using the vendor config dictionary.
Key	Enter the specific key provided by the vendor.
Value	Enter the VPN value for each key.

Configure Advanced Settings for Android VPN

Advanced VPN settings for Android consist of authentication and VPN on demand, which you must configure to establish VPN for Android devices.

Setting	Description
Authentication	
Identify Certificate.	Enter the certificate credentials used to authenticate the connection by selecting **Add a Certificate**.
Credential Source	Select the source of the credentials. Select between Upload, Defined Certificate Authority, and User Certificate.
Credential Name	Available when **Credential Source** is set to Upload. Enter the name of the uploaded credential.
Certificate	Available when **Credential Source** is set to Upload. Click Upload to select a certificate file from your device.

Setting	Description
Certificate Authority	Available when **Credential Source** is set to Defined Certificate Authority. Select the certificate authority from a drop-down listing.
Certificate Template	Available when **Credential Source** is set to Defined Certificate Authority. This setting auto-populates based on your selection in the Certificate Authority setting.
S/MIME	Available when **Credential Source** is set to User Certificate. Select between the user-centric S/MIME Signing certificate or S/MIME Encryption certificate.
Enable VPN On Demand	
Enable VPN On Demand.	Enable VPN On Demand to use certificates to establish VPN connections automatically. Enable VPN by entering the name of the app and selecting the plus sign to the left of the magnifying glass icon. You can enter more than one application.

Configure Advanced Settings for Windows Phone VPN

Configure device VPN settings to access corporate infrastructure remotely and securely. You can also limit traffic through the VPN by configuring Per-app VPN connections. Then set the VPN to connect automatically whenever the specified application is launched.

Settings	Descriptions
Connection Info	
Advanced Connection Settings	Configure advanced routing rules for device VPN connections.
Routing Addresses	Select **Add** to enter the IP Addresses and Subnet Prefix Size for the VPN connection. You can add additional routing addresses as needed. Available when **Advanced Connection Settings** is enabled.
DNS Routing Rules	Select **Add** to enter the **Domain Name** on which the VPN server is hosted. Enter the **Domain Name**, **DNS Servers**, and **Web Proxy Servers** for each specific domain. Available when **Advanced Connection Settings** is enabled.
Routing Policy	Allow traffic to use the local network connection by selecting **Allow Direct Access to External Resources**. Conversely, select **Force All Traffic Through VPN** to send all traffic through the VPN. Available when **Advanced Connection Settings** is enabled.
Proxy	Select **Auto Detect** to detect any proxy servers used by the VPN automatically. Select **Manual** to configure the proxy server. Available when **Advanced Connection Settings** is enabled.
Proxy Auto Config URL	Enter the URL for the proxy auto config. Available only when **Proxy** is set to Auto Detect.
Server	Enter the URL for the proxy server configuration settings. Displays when **Proxy** is set to Manual
Port	Enter the port number used to access the proxy server. Displays when **Proxy** is set to Manual.
Bypass proxy for local	Bypass the proxy server when the device detects it is on the local network.
Authentication	

Settings	Descriptions
Authentication Type	Select the authentication protocol for the VPN. ■ EAP – Allows for various authentication methods. ■ Machine Certificate – Detects a client certificate in the device certificate store to use for authentication.
Protocols	Select the type of EAP authentication. ■ EAP-TLS – Smart Card or client certificate authentication. ■ EAP-MSCHAPv2 – User name and Password.
Credential Type	Select **Use Certificate** to use a client certificate. Select **Use Smart Card** to use a Smart Card to authenticate. Displays when the **Protocols** option is set to **EAP-TLS**.
Simple Certificate Selection	Simplify the list of certificates from which the user selects. The most recently issued certificate is presented and the entity for which the certificate was issued groups the certificates. Displays when the **Protocols** option is set to **EAP-TLS**.
Use Windows login Credentials	Use the same credentials as the Windows device. Displays when the **Protocols** option is set to **EAP-MSCHAPv2**.
VPN Traffic Rules	
App Identifier	Specify the App to which the traffic rules apply by entering the application package family name. ■ Package Family Name, for example: WorkspaceONE.MDMAgent_htcwkw4rx2gx4
VPN On Demand	Automatically connect using VPN when the application is launched.
Routing Policy	Select the routing policy for the app. ■ **Allow Direct Access to External Resources** allows for both VPN traffic and traffic through the local network connection. ■ **Force All Traffic Through VPN** forces all traffic through the VPN.
VPN Traffic Filters	Add traffic filters for specific Legacy and Modern applications. Select **Add New Filter** to add **Filter Types** and **Filter Values** for the routing rules. Only traffic from the specified app that matches these rules can be sent through the VPN. ■ **IP Protocol** – Numeric value 0–255 representing the IP protocol to allow. For example, TCP = 6 and UDP = 17. ■ **IP Address** – A list of comma-separated values specifying remote IP address ranges to allow. ■ **Ports** – A list of comma-separated values specifying remote port ranges to allow. For example, 100–120, 200, 300–320. Ports are only valid when the protocol is set to TCP or UDP. ■ **LocalPorts** – A list of comma-separated values specifying local port ranges through which traffic is allowed. ■ **LocalAddress** – A list of comma-separated values specifying local IP addresses through which traffic is allowed.
Device Wide VPN Rules	Select **Add** to add traffic rules for the entire device. Select **Add** to add **Filter Types** and **Filter Values** for the routing rules. Only traffic that matches these rules can be sent through the VPN.
Policies	
Remember Credentials	Remember the end user's login credentials.
Always On	Force the VPN connection on, which activates the VPN connection when the network connection disconnects and reconnects.

Settings	Descriptions
VPN Lockdown	Force the VPN on, disable any network access if the VPN is not connected, and prevent a connection or modification to other VPN profiles.
Trusted Network	Enter trusted network addresses separated by commas. The VPN does not connect when a trusted network connection is detected.
Split Tunnel	Allow end users to use a split tunnel VPN. This text box applies to Windows Phone 8.1 devices only.
Bypass for Local	Bypass the VPN connection for local intranet traffic. For example, you do not use the VPN connection if you are also connected to your work network connection at the office. This text box applies to Windows Phone 8.1 devices only.
Trusted Network Detection	Use Trusted Network Detection when connecting to the VPN. This text box applies to Windows Phone 8.1 devices only.
Connection Type	Select the connection type you want to allow. Always ON leaves the VPN connection running always. This text box applies to Windows Phone 8.1 devices only.
Idle Disconnection Time	Set the maximum amount of time that can pass without connectivity requests before automatically disconnecting the VPN. This text box applies to Windows Phone 8.1 devices only.
VPN On Demand	
Allows Apps	Select **Add** to define apps to have all their traffic secured over the VPN. You can add as many apps as you like.
Allowed Networks	Select **Add** to define networks. All traffic over configured networks is secured over the VPN. You can add as many networks as you like.
Excluded Apps	Select **Add** to define excluded apps. All traffic to these apps is NOT secured over the VPN. You can add as many excluded apps as you like.
Excluded Networks	Select **Add** to define excluded networks. All traffic over excluded networks is NOT secured over the VPN. You can add as many excluded networks as you like.
DNS Suffix Search List	Select **Add** to define the DNS Suffix Search List. DNS suffixes are appended to shortened URLs for DNS resolution and connectivity. You can add as many DNS suffixes as you like.

Compliance Policies

9

The compliance engine is an automated tool by Workspace ONE UEM that ensures all devices abide by your policies. These policies can include basic security settings such as requiring a passcode and having a minimum device lock period. For certain platforms, you can also decide to set and enforce certain precautions. These precautions include setting password strength, blacklisting certain apps, and requiring device check-in intervals to ensure that devices are safe and in-contact with Workspace ONE UEM.

Once devices are determined to be out of compliance, the compliance engine warns users to address compliance errors to prevent disciplinary action on the device. For example, the compliance engine can trigger a message to notify the user that their device is out of compliance.

In addition, devices not in compliance cannot have device profiles assigned to it and cannot have apps installed on the device. If corrections are not made in the amount of time specified, the device loses access to certain content and functions that you define. The available compliance policies and actions vary by platform.

You can automate escalations when corrections are not made, for example, locking down the device and notifying the user to contact you to unlock the device. These escalation steps, disciplinary actions, grace periods, and messages are all customizable with the Unified Endpoint Management Console.

There are two methods by which compliance is measured.

- Real Time Compliance (RTC)

  Unscheduled samples received from the device are used to determine whether or not the device is compliant. The samples are requested on demand by the admin.

- Engine Compliance

  The compliance engine, a software algorithm that receives and measures scheduled samples, primarily determines the compliance of a device. The time intervals for the running of the scheduler are defined in the console by the admin.

Enforcing mobile security policies is represented by this general overview.

1 Choose your platform.

  Determine on which platform you want to enforce compliance. After you select a platform, you are never shown an option that does not apply to that platform.

2 Build your policies.

Customize your policy to cover everything from an application list, compromised status, encryption, manufacturer, model and OS version, passcode and roaming.

3 Define escalation.

   Configure time-based actions in hours or days and take a tiered approach to those actions.

4 Specify actions.

   Send SMS, email, or push notifications to the user device or send an email only to an Administrator. Request device check-in, remove or block specific profiles, install compliance profiles, remove, or block apps and perform an enterprise wipe.

5 Configure assignments.

   Assign your compliance policy by organization group or smart group then confirm the assignment by device.

Confirm the Health of Windows Devices

Windows devices enable you to configure and scan the health of the device at startup to ensure that your corporate resources are secure. For more information, see the topic **Compromised Device Detection with Health Attestation** found in the **Windows Desktop Device Management** documentation on docs.vmware.com.

This chapter includes the following topics:

- Compliance Policies List View
- Compliance Policy Rules by Platform
- Add a Compliance Policy
- Compromised Device Detection with Health Attestation

Compliance Policies List View

The Compliance Policies List View enables you to see all the active and inactive compliance policies and their configurations. Devices are placed in a **Pending** compliance status during an initial enrollment. Creating, saving, and assigning a policy to an enrolled device causes the device compliance status to either be **Compliant** or **NonCompliant**.

Similarly, changes to **Smart Group** assignments only cause a device compliance policy to be **Pending** when the device is new to the smart group. Devices already assigned to the smart group cannot see their compliance status change simply because the smart group expands (or contracts) its assignment.

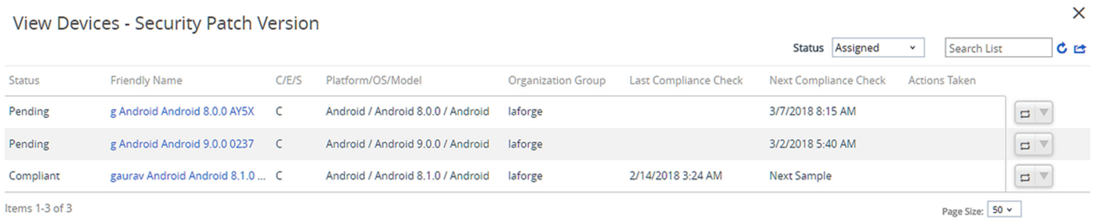
View the Compliance Policy List view by navigating to **Devices > Compliance Policies > List View**.

Setting	Description
Status	Filter the listing between **All**, **Active** and **Inactive** statuses.
Actions Menu	View and edit individual policies, view devices to which the policy has been assigned, and delete policies you no longer want to keep.
Compliant / NonCompliant / Pending / Assigned	The digits in this column feature hypertext links that, when selected, display the **View Devices** page for the specific status on the selected compliance policy. The **Assigned** status is the sum of **Compliant**, **NonCompliant**, and **Pending** devices. For more information, see View Devices Page.

View Devices Page

The **View Devices** page is used to view compliance details for each device that is assigned to the selected policy. It is displayed when you select one of the hyperlink text digits in the Compliance Policy List View column titled **Compliant / NonCompliant / Pending / Assigned**.

Filter the listing among these four statuses by selecting from the **Status** drop-down menu. The **Assigned** status is the sum of **Compliant**, **Non-Compliant**, and **Pending** statuses.



View Devices - Security Patch Version

Status: Assigned

Search List

Status	Friendly Name	C/E/S	Platform/OS/Model	Organization Group	Last Compliance Check	Next Compliance Check	Actions Taken
Pending	g Android Android 8.0.0 AY5X	C	Android / Android 8.0.0 / Android	laforge		3/7/2018 8:15 AM	
Pending	g Android Android 9.0.0 0237	C	Android / Android 9.0.0 / Android	laforge		3/2/2018 5:40 AM	
Compliant	gaurav Android Android 8.1.0 ...	C	Android / Android 8.1.0 / Android	laforge	2/14/2018 3:24 AM	Next Sample	

Items 1-3 of 3

Page Size: 50

There are three listed device statuses in the **Status** column.

- **Compliant** – The assigned compliance policy has determined that the device is compliant.
- **Non-Compliant** – The assigned compliance policy has determined that the device is non-compliant.
- **Pending** – The compliance policy is scheduled to be assigned to the newly enrolled device.

You can also confirm the **C/E/S** (ownership) of the device, the **Platform/OS/Model**, **Organization Group**, **Last Compliance Check**, **Next Compliance Check**, and **Actions Taken**. The Actions Taken column lists the actions that have been taken to address non-compliant devices.

You may also choose to reevaluate the compliance for a specific device. Engage the compliance engine and re-report compliance status on the device by selecting **Re-Evaluate Compliance** ( ).

Compliance Policy Rules by Platform

Not all compliance policy rules apply to all platforms. The **Add a Compliance Policy** page is platform-based so you see only the compliance policy rules and actions that apply to your device.

Use the following table to determine which rules are available to deploy to your devices.

Compliance Policy	Android and Android Legacy	Apple iOS	Apple macOS	Chrome OS	QNX	Windows Rugged	Windows 7	Windows Phone	Windows Desktop
Application List	✓	✓	✓						
Antivirus Status									✓
Cell Data Usage	✓	✓							
Cell Message Usage	✓								
Cell Voice Usage	✓								
Compliance Attribute									✓
Compromised Status	✓	✓							✓
Device Last Seen	✓	✓	✓	✓	✓	✓	✓	✓	✓
Device Manufacturer	✓								
Encryption	✓	✓	✓				✓	✓	✓
Firewall Status			✓						✓
Free Disk Space		✓							
iBeacon Area		✓							
Interactive Certificate Profile Expiry	✓	✓							
Last Compromised Scan	✓	✓							
MDM Terms of Use Acceptance	✓	✓	✓			✓	✓	✓	✓
Model	✓	✓	✓					✓	
OS Version	✓	✓	✓	✓			✓	✓	✓
Passcode	✓	✓					✓	✓	✓
Roaming *	✓	✓							✓
Roaming Cell Data Usage *	✓	✓							
Security Patch Version	✓								
SIM Card Change *	✓	✓						✓	
System Integrity Protection			✓						

Compliance Policy	Android and Android Legacy	Apple iOS	Apple macOS	Chrome OS	QNX	Windows Rugged	Windows 7	Windows Phone	Windows Desktop
Windows Automatic Update Status									✓
Windows Copy Genuine Validation							✓		

Note * Only available for Telecom Advanced Users.

Compliance Policy Rules Descriptions

Compliance policy rules enable you to construct a solid foundation for your policy as the component parts of a policy. The actions, escalations, and assignments that follow are all built upon these rules.

Setting	Description
Application List	Detect specific blacklisted apps that are installed on a device, or detect all apps that are not whitelisted. You can prohibit certain apps (such as social media apps) and vendor-blacklisted apps, or permit only the apps you specify. You can also specify a minimum version number for an app.
Antivirus Status	Detect whether or not an antivirus app is running. The compliance policy engine checks the Action Center on the device for an antivirus solution. If your third-party solution does not display in the action center, it reports as not monitored.
Cell Data/Message/Voice Use	Detect when end-user devices exceed a particular threshold of their assigned telecom plan. For this policy to take effect Telecom must be configured.
Compliance Attribute	Compare attribute keys in the device against third-party endpoint security, which returns a Boolean value representing device compliance. Only available for Windows Desktop devices.
Compromised Status	Detect if the device is compromised. Prohibit the use of jailbroken or rooted devices that are enrolled with Workspace ONE UEM. Jailbroken and rooted devices strip away integral security settings and can introduce malware in your network and provide access to your enterprise resources. Monitoring for compromised device status is especially important in BYOD environments where employees have various versions of devices and operating systems.
Device Last Seen	Detect if the device fails to check in within an allotted time window.
Device Manufacturer	Detect the device manufacturer allowing you to identify certain Android devices. You can specifically prohibit certain manufacturers or permit only the manufacturers you specify.
Encryption	Detect whether or not encryption is enabled on the device.
Firewall Status	Detect whether or not a firewall app is running. The compliance policy engine checks the Action Center on the device for a firewall solution. If your third-party solution does not display in the action center, it reports as not monitored.
Free Disk Space	Detect the available storage space on the device.
iBeacon Area	Detect whether your iOS device is within the area of an iBeacon Group.
Interactive Certificate Profile Expiry	Detect when an installed profile on the device expires within the specified length of time.

Setting	Description
Last Compromised Scan	Detect if the device has not reported its compromised status within the specified schedule.
MDM Terms of Use Acceptance	Detect if the end user has not accepted the current MDM Terms of Use within a specified length of time.
Model	Detect the device model. You can specifically prohibit certain models or permit only the models you specify.
OS Version	Detect the device OS version. You can prohibit certain OS versions or permit only the operating systems and versions you specify.
Passcode	Detect whether a passcode is present on the device.
Roaming*	Detect if the device is roaming.
Roaming Cell Data Use*	Detect roaming cell data use against a static amount of data measured in MB or GB.
Security Patch Version	Detect the date of the Android device's most recent security patch from Google. Applicable only to Android version 6.0 and later.
SIM Card Change*	Detect if the SIM card has been replaced.
System Integrity Protection	Detect the status of macOS's proprietary protection of system-owned files and directories against modifications by processes without a specific "entitlement", even when executed by the root user or a user with root privileges.
Windows Automatic Update Status	Detect whether Windows Automatic Update has been activated. The compliance policy engine checks the Action Center on the device for an Update solution. If your third-party solution does not display in the action center, it reports as not monitored.
Windows Copy Genuine Validation	Detect whether the copy of Windows currently running on the device is genuine.

* Only available for Telecom Advanced Users.

Compliance Policies Actions by Platform

The supported actions by platform, enforced by compliance policies, are as follows.

Compliance Policy Action	Android and Android Legacy	Apple iOS	Apple macOS	Chrome OS	QNX	Windows Rugged	Windows 7	Windows Phone	Windows Desktop
Application									
Block/Remove Managed App	✓	✓	✓						
Block/Remove All Apps	✓	✓	✓						
Command									
Change Roaming Settings.		✓(iOS 5+)							
Enterprise Wipe	✓	✓	✓		✓		✓	✓	✓
Enterprise Reset	✓					✓			

Compliance Policy Action	**Android and Android Legacy**	**Apple iOS**	**Apple macOS**	**Chrome OS**	**QNX**	**Windows Rugged**	**Windows 7**	**Windows Phone**	**Windows Desktop**
OS Updates		✓ (DEP only)							
Request Device Check-In		✓						✓	✓
Revoke Azure Tokens*.	✓	✓							
Email									
Block Email	✓	✓							
Notify									
Send Email to User**.	✓	✓	✓	✓		✓	✓	✓	✓
Send SMS to Device.	✓	✓						✓	✓
Send Push Notification to Device.	✓	✓	✓	✓			✓	✓	✓
Send Email to Administrator.	✓	✓	✓		✓	✓	✓	✓	✓
Profile									
Install Compliance Profiles	✓	✓	✓					✓	✓
Block/Remove Profile	✓	✓	✓					✓	✓
Block/Remove Profile Type	✓	✓	✓						
Block/Remove All Profiles	✓	✓	✓					✓	✓

* Requires 'Use Azure AD For Identity Services' enablement in **Settings > System > Enterprise Integration > Directory Services > Advanced**. Affects all devices for a given user, disabling any app that relies upon the Azure token.

** Includes option to CC the user's manager.

Add a Compliance Policy

Adding a compliance policy is a process comprising of four segments: Rules, Actions, Assignment, and Summary. Not all features and options presented in this guide are available for all platforms. The

Workspace ONE UEM console bases all available options on the initial platform choice, so the console never presents an option that your device cannot use.

Note Windows Rugged compliance is only supported on Motorola devices (Enterprise Reset action enforces compliance).

Configure the compliance engine with profiles and automated escalations by completing the Compliance Policy tabs.

Procedure

1 Navigate to **Devices > Compliance Policies > List View** and select **Add**.

2 Select a platform from the **Add Compliance Policy** page on which to base your compliance policy.

3 Detect conditions by configuring the **Rules** tab by first matching **Any** or **All** of the rules.

- **Add Rule** – Select to add additional rules and parameters. For more information, see Compliance Policy Rules by Platform and Compliance Policy Rules Descriptions.
- **Previous** and **Next** – Select to go back to the previous step or advance to the next step, Actions, respectively.

4 Define the consequences of noncompliance within of your policy by completing the **Actions** tab.

Available actions are platform-dependent. For more information, see Compliance Policies Actions by Platform.

5 Specify **Actions** and **Escalations** that occur.

An **Escalation** is simply an automatic action taken when the prior **Action** does not cause the user to take corrective steps to make their device compliant.

Select the options and types of actions to perform.

Setting	Description
Actions and Escalations	
Mark as Not Compliant check box	Enables you to perform actions on a device without marking it as non-compliant. The compliance engine accomplishes this task by observing the following rules. ■ The Mark as Not Compliant check box is enabled (checked) by default for each newly added Action. ■ If one action has the Mark as Not Compliant option enabled (checked), then all subsequent actions and escalations are also marked as not compliant (checked). These subsequent check boxes cannot be edited. ■ If an action has the Mark as Not Compliant option disabled (not checked), then the next action/escalation has the option enabled by default (checked). This check box can be edited. ■ If an action/escalation has the Mark as Not Compliant option disabled and the device does not pass the compliance rule, the device is officially 'compliant'. The prescribed action is then run. ■ A device's status remains 'compliant' unless it encounters an action/escalation with the Mark as Not Compliant check box enabled. Only then is the device considered non-compliant.
Application	Block or remove a managed application. You can enforce application compliance by establishing a whitelist, blacklist, or required list of applications.

Setting	Description
Command	Initiate a device check-in or run an enterprise wipe.
Email	Block the user from email. If you are using Mobile Email Management together with the Email compliance engine, then the 'Block Email' action applies. Access this option by navigating to **Email > Compliance Policies > Email Policies**. This action lets you use Device Compliance policies such as blacklisted apps with any Email compliance engine policies you configure. With this Action selected, email compliance is triggered with a single device policy update if the device falls out of compliance.
Notify	Notify someone about the compliance violation. You have the following options to send a notification. ■ Send Email to User. ■ Send SMS to Device. ■ Send Push Notification to Device. ■ Send Email to Administrator. Multiple emails can be inserted into the accompanying **CC** text box provided they are separated by commas. You can also CC the user's manager by inserting a lookup value; click the plus sign next to the CC text box and choose {UsersManager} from the drop-down menu. For details, see Lookup Values. For all Notify actions, you have the option of using a message template. Use this option by deselecting the **Default Template** check box, which displays a drop-down menu enabling you to select a message template. There is also a link that, when selected, displays the **Message Template** page in a new window. This page enables you to create your own message template.
Profile	Install, Remove, or Block a specific Device Profile, Device Profile type, or Compliance Profile. Compliance profiles are created and saved in the same manner as Auto and Optional device profiles. Navigate to **Devices > Profiles & Resources > Profiles**, then select **Add**, then **Add Profile**. Select a platform, and in the **General** profile tab, select 'Compliance' in the **Assignment Type** drop-down setting. Compliance profiles are applied in the **Actions** tab of the **Add a Compliance Policy** page to be used when an end user violates a compliance policy. Select **Install Compliance Profile** from the drop-down and then select the previously saved compliance profile.
Escalations Only	
Add Escalation button	Creates an escalation. When adding escalations, it is a best practice to increase the security of actions with each additional escalation.
After time Interval...	You can delay the escalation by minutes, hours, or days.
...**Perform the following actions**	**Repeat** – Enable this check box to repeat the escalation a selected number of times before the next scheduled action begins.

For macOS, you can only perform the following actions:

- Device Wipe
- Send Email to Administrator
- Enterprise Wipe
- Block/Remove Profile
- Send Email to User

- Block/Remove Profile Type
- Send Push Notification to Device
- Block/Remove All Profiles

6 Determine which devices are subjected to (and excluded from) the compliance policy by completing the **Assignment** and **Summary** tabs of the Add Compliance Policy page.Name, finalize, and activate the policy with the Summary tab.

Setting	Description
Managed By	Select the organization group by which this compliance policy is managed.
Assigned Groups	Assign to this policy one or more groups. For more information, see Assignment Groups.
Exclusions	If you want to exclude groups, select **Yes**. Next, select from the available listing of groups in the **Excluded Groups** text box. See Exclude Groups in Profiles and Policies.
View Device Assignment button	See a listing of devices affected by this compliance policy assignment.

While Platform is a criterion within a smart group, the platform configured in the device profile or compliance policy always takes precedence over the smart group's platform. For instance, if a device profile is created for the iOS platform, the profile is only assigned to iOS devices even if the smart group includes Android devices.

7 After you determine the Assignment of this policy, select **Next**.

The **Summary** tab displays.

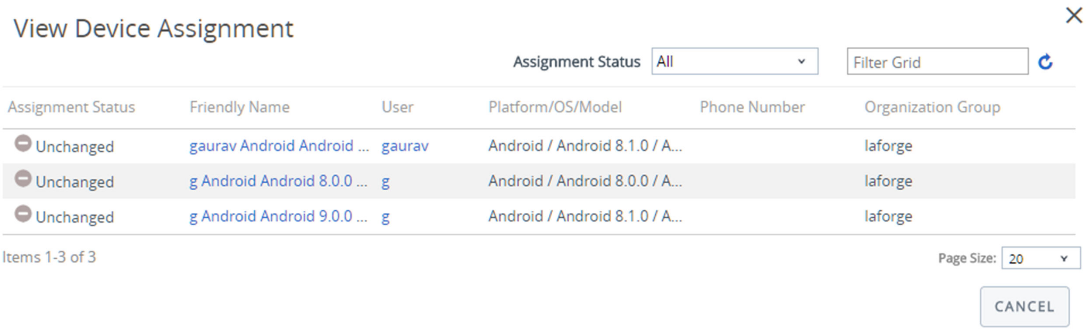
8 Provide a **Name** and a useful **Description** of the compliance policy.

9 Select one of the following options.

- **Finish** – Save your compliance policy without activating it to the assigned devices.
- **Finish and Activate** – Save and apply the policy to all affected devices.

View Device Assignment

Select **View Device Assignment** on the **Assignment** tab while configuring a compliance policy to display the **View Device Assignment** page. This page confirms affected (or unaffected) devices.



View Device Assignment

Assignment Status: All

Filter Grid

Assignment Status	Friendly Name	User	Platform/OS/Model	Phone Number	Organization Group
Unchanged	gaurav Android Android ...	gaurav	Android / Android 8.1.0 / A...		laforge
Unchanged	g Android Android 8.0.0 ...	g	Android / Android 8.0.0 / A...		laforge
Unchanged	g Android Android 9.0.0 ...	g	Android / Android 8.1.0 / A...		laforge

Items 1-3 of 3

Page Size: 20

The **Assignment Status** column displays the following entries for the devices that appear in the listing.

- **Added** – The compliance policy has been added to the listed device.
- **Removed** – The compliance policy has been removed from the device.
- **Unchanged** – The device remains unaffected by the changes made to the compliance policy.

Select **Publish** to finalize the changes and, if necessary, republish any compliance policy.

Compromised Device Detection with Health Attestation

Health Attestation scans devices during startup for failures in device integrity. Use Health Attestation to detect compromised Windows Desktop devices.

In both BYOD and Corporate-Owned device deployments, it is important to know that devices are healthy when accessing corporate resources. The Windows Health Attestation Service accesses device boot information from the cloud through secure communications. This information is measured and checked against related data points to ensure that the device booted up as intended and is not victim to security vulnerabilities or threat. Measurements include Secure Boot, Code Integrity, BitLocker, and Boot Manager.

Workspace ONE UEM enables you to configure the Windows Health Attestation service to ensure device compliance. If any of the enabled checks fail, the Workspace ONE UEM compliance policy engine applies security measures based on the configured compliance policy. This functionality allows you to keep your enterprise data secure from compromised devices. Since Workspace ONE UEM pulls the necessary information from the device hardware and not the OS, compromised devices are detected even when the OS kernel is compromised.

Configure the Health Attestation for Windows Desktop Compliance Policies

Keep your devices secured by using Windows Health Attestation Service for compromised device detection. This service allows Workspace ONE UEM to check the device integrity during startup and take corrective actions.

Procedure

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Desktop > Windows Health Attestation**.
2. (Optional) Select **Use Custom Server** if you are using a custom on-premesis server running Health Attestation. Enter the **Server URL**.

3 Configure the Health Attestation settings:

Settings	Descriptions
Compromised Status Definition	
Use Custom Server	Select to configure a custom server for Health Attestation. This option requires a server running Windows Server 2016 or newer. Enabling this option displays the **Server URL** field.
Server URL	Enter the URL for your custom Health Attestation server.
Secure Boot Disabled	Enable to flag compromised device status when Secure Boot is disabled on the device. Secure Boot forces the system to boot to a factory trusted state. When Secure Boot is enabled, the core components used to boot the machine must have the correct cryptographic signatures that the OEM trusts. The UEFI firmware verifies the trust before it allows the machine to start. Secure boot prevents the startup if any it detects any tampered files.
Attestation Identity Key (AIK) Not Present	Enable to flag compromised device status when the AIK is not present on the device. Attestation Identity Key (AIK) is present on a device, it indicates that the device has an endorsement key (EK) certificate. It can be trusted more than a device that does not have an EK certificate.
Data Execution Prevention (DEP) Policy Disabled	Enable to flag compromised device status when the DEP is disabled on the device. The Data Execution Prevention (DEP) Policy is a memory protection feature built into the system level of the OS. The policy prevents running code from data pages such as the default heap, stacks, and memory pools. DEP is enforced by both hardware and software.
BitLocker Disabled	Enable to flag compromised device status when BitLocker encryption is disabled on the device.
Code Integrity Check Disabled	Enable to flag compromised device status when the code integrity check is disabled on the device. Code integrity is a feature that validates the integrity of a driver or system file each time it is loaded into memory. Code integrity checks for unsigned drivers or system files before they load into the kernel. The check also scans for users with administrative privileges running system files modified by malicious software.
Early Launch Anti-Malware Disabled	Enable to flag compromised device status when the early launch anti-malware is disabled on the device. Early launch anti-malware (ELAM) provides protection for the computers in your network when they start up and before third-party drivers initialize.
Code Integrity Version Check	Enable to flag compromised device status when the code integrity version check fails.
Boot Manager Version Check	Enable to flag compromised device status when the boot manager version check fails.
Boot App Security Version Number Check	Enable to flag compromised device status when the boot app security version number does not meet the entered number.
Boot Manager Security Version Number Check	Enable to flag compromised device status when the boot manager security version number does not meet the entered number.
Advanced Settings	Enable to configure advance settings in the Software Version Identifiers section.
Software Version Identifiers	
Code Integrity Policy Hash Check	Enable to define a whitelist of known, valid hash values for the **Code Integrity** software. If the hash is not a whitelisted value, health attestation compliance fails.

Settings	Descriptions
Secure Boot Config Policy Hash Check	Enable to define a whitelist of known, valid hash values for the **Secure Boot Config** software. If the hash is not a whitelisted value, health attestation compliance fails.
PCR0 Check	Enable to define a whitelist of known, valid measurements for the **PRC0 Check** software. This measurement checks the BIOS trusted code to ensure that it has not been compromised. If the measurement is not a whitelisted value, health attestation compliance fails.

4 Select **Save**.

Configure Health Attestation for Windows Phone Compliance Policies

Keep your devices secured by using Windows Health Attestation Service for compromised device detection. This service allows AirWatch to check the device integrity during boot and take corrective actions.

Compromised status compliance policy is applicable to Windows 10 Mobile devices with a Trusted Platform Module (TPM) 1.2 or higher.

Procedure

1 Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Phone > Windows Health Attestation**.

2 (Optional) Select **Use Custom Server** if you are using a custom on-premesis server running Health Attestation. Enter the **Server URL**.

3 Configure the Health Attestation settings:

Settings	Descriptions
Compromised Status Definition	
Use Custom Server	Select to configure a custom server for Health Attestation. This option requires a server running Windows Server 2016 or newer. Enabling this option displays the **Server URL** field.
Server URL	Enter the URL for your custom Health Attestation server.
Secure Boot Disabled	Enable to flag compromised device status when Secure Boot is disabled on the device. Secure Boot forces the system to boot to a factory trusted state. When Secure Boot is enabled, the core components used to boot the machine must have the correct cryptographic signatures that the OEM trusts. The UEFI firmware verifies the trust before it allows the machine to start. Secure boot prevents the startup if any it detects any tampered files.
Attestation Identity Key (AIK) Not Present	Enable to flag compromised device status when the AIK is not present on the device. Attestation Identity Key (AIK) is present on a device, it indicates that the device has an endorsement key (EK) certificate. It can be trusted more than a device that does not have an EK certificate.
Data Execution Prevention (DEP) Policy Disabled	Enable to flag compromised device status when the DEP is disabled on the device. The Data Execution Prevention (DEP) Policy is a memory protection feature built into the system level of the OS. The policy prevents running code from data pages such as the default heap, stacks, and memory pools. DEP is enforced by both hardware and software.

Settings	Descriptions
BitLocker Disabled	Enable to flag compromised device status when BitLocker encryption is disabled on the device.
Code Integrity Check Disabled	Enable to flag compromised device status when the code integrity check is disabled on the device. Code integrity is a feature that validates the integrity of a driver or system file each time it is loaded into memory. Code integrity checks for unsigned drivers or system files before they load into the kernel. The check also scans for users with administrative privileges running system files modified by malicious software.
Early Launch Anti-Malware Disabled	Enable to flag compromised device status when the early launch anti-malware is disabled on the device. Early launch anti-malware (ELAM) provides protection for the computers in your network when they start up and before third-party drivers initialize.
Code Integrity Version Check	Enable to flag compromised device status when the code integrity version check fails.
Boot Manager Version Check	Enable to flag compromised device status when the boot manager version check fails.
Boot App Security Version Number Check	Enable to flag compromised device status when the boot app security version number does not meet the entered number.
Boot Manager Security Version Number Check	Enable to flag compromised device status when the boot manager security version number does not meet the entered number.
Advanced Settings	Enable to configure advance settings in the Software Version Identifiers section.
Software Version Identifiers	
Code Integrity Policy Hash Check	Enable to define a whitelist of known, valid hash values for the **Code Integrity** software. If the hash is not a whitelisted value, health attestation compliance fails.
Secure Boot Config Policy Hash Check	Enable to define a whitelist of known, valid hash values for the **Secure Boot Config** software. If the hash is not a whitelisted value, health attestation compliance fails.
PCR0 Check	Enable to define a whitelist of known, valid measurements for the **PRC0 Check** software. This measurement checks the BIOS trusted code to ensure that it has not been compromised. If the measurement is not a whitelisted value, health attestation compliance fails.

What to do next

For more information, see the Microsoft TechNet article on Health Attestation.

Privacy for BYOD Deployments 10

One of the biggest concerns for BYOD end users is the privacy of the personal content on their devices. Your organization must assure employees that their personal data is not subject to corporate oversight.

With Workspace ONE UEM MDM, you can ensure the privacy of personal data by creating customized privacy policies that do not collect personal data based on the device ownership type. In addition, you can define granular privacy settings to disable the collection of the personally identifiable information and disallow certain remote actions to employee-owned devices to ensure employee privacy.

You must inform your end users about how their data is collected and stored when they enroll into Workspace ONE UEM.

Important Countries and jurisdictions have differing regulations governing the data that can be collected from end users. Your organization must thoroughly research the applicable laws before you configure your BYOD and privacy policies.

This chapter includes the following topics:

Security and Privacy in Workspace ONE UEM

Workspace ONE UEM provides customized levels of device and application management to help you balance corporate security and end-user privacy in a BYOD scenario.

Each management type provides a different balance of privacy and device management. You should work with your legal team and IT teams to determine which balance is best for your BYOD users. Use the following comparison to help make the most practical choice.

Table 10-1. Privacy Versus Security

	Minimal Management	Adaptive Management	Required Management
	<-	--	->
Devices	■ No MDM profile - devices cannot be managed by the enterprise. ■ No Profiles for Wi-Fi, VPN, Native Email, restrictions, etc. ■ No Device passcode complexity enforcement. ■ Factory wipe and remote device lock not allowed.	■ Flexible - end users choose whether their devices are managed by Workspace Services. ■ Configuration profiles for Wi-Fi, VPN, Native Email, restrictions, etc. are available after users enable Adaptive Management through Workspace Services. ■ Device passcode and complexity requirement enforced. ■ Factory wipe and remote device lock not allowed.	■ MDM profile - devices are fully managed by the enterprise using the Workspace ONE Intelligent Hub. ■ Configuration profiles for Wi-Fi, VPN, Native Email, restrictions, etc. ■ Device passcode and complexity requirement enforced. ■ Factory wipe and remote device lock enabled.
Applications	■ User manage application installation and permissions 　■ Users must trust unknown sources (Android) or Trust Developer (iOS) to install internal, SDK, or wrapped applications. 　■ Admins cannot deploy AppConfig & Per-App VPN or push applications. ■ Users access VMware Email, Content, and Browsing applications through VMware Workspace ONE.	■ Users are prompted to Enable Workspace Services when they initially access an application where management is required. 　■ With Workspace Services enabled, all **Required Management - Applications** functionality is enabled. 　■ With Workspace Services disabled, all **Minimal Management - Applications** functionality is enabled.	■ Admins push and pull public, internal, SDL, and wrapped applications to devices using MDM actions. ■ Admins monitor blacklisted applications and take compliance actions on devices. ■ Admins configure SSO and Per-App VPN. ■ Admins manage applications with AppConfig.
Privacy	■ User-centric privacy model 　■ Minimal device and user information collected in applications. 　■ Users configure privacy options for each application installed. 　■ GPS location not tracked.	■ Balanced privacy model 　■ Workspace Services profile optimizes functionality and minimizes privacy infringement. 　■ Customized privacy notice communicates IT policies and collected data to end users. 　■ GPS location not tracked.	■ Enterprise-centric privacy model 　■ Corporate data protected at device and application level. 　■ Workspace Services available. 　■ GPS location tracking and geofencing available.

Configure Privacy Settings

End-user privacy is a major concern for you and your users. Workspace ONE UEM provides granular control over what data is collected from users and what collected data is viewable by admins. Configure the privacy settings to serve both your users and your business needs.

Procedure

1. Navigate to **Devices > Device Settings > Devices & Users > General > Privacy**.
2. Select the appropriate setting for **GPS**, **Telecom**, **Applications**, **Profiles**, and **Network** data collection.

   ● **Collect and Display** – User data is collected and displayed in the UEM console.

   ◐ **Collect Do Not Display** – User data is collected for use in reports but is not displayed it in the UEM console.

   ○ **Do Not Collect** – User data is not collected and therefore it is not displayed.

3. Select the appropriate setting for the **Commands** that can be performed on devices. Consider disabling all remote commands for employee-owned devices, especially full wipe. This disablement prevents inadvertent deletion or wiping of an end user's personal content. If you disable the wipe function for select iOS ownership types, users do not see the "Erase all content and settings" permission during enrollment.

   ● **Allow** – The command is made on devices without permission from the user.

   ◐ **Allow With User Permission** – The command is made on devices but only with the permission of the user.

   ○ **Prevent** – The command does not run on devices.

4. If you are going to allow remote control, file manager, or registry manager access for Android/ Windows Rugged devices, consider using the **Allow With User Permission** option. This option requires the end user to consent to admin access on their device through a message prompt before the action is performed. If you opt to allow use of any commands, explicitly mention these commands in your terms of use agreement.
5. For **User Information**, select **Display** or **Do Not Display** in the Console for the **First Name**, **Last Name**, **Phone Number**, **Email Accounts**, and **user name** data.
6. If an option other than **user name** is set to **Do Not Display**, that data displays as "Private" wherever it appears in the UEM console. Options you set to **Do Not Display** are not searchable in the console. When a user name is set to **Do Not Display**, the user name displays as "Private" only on the Device List View and Device Details pages. All other pages in the UEM console show the user name of the enrolled user.

7 You can encrypt personally identifiable information, including first name, last name, email address, and telephone number. Navigate to **Groups & Settings > All Settings > System > Security > Data Security** from the Global or Customer-level organization group you want to configure encryption for. Enabling encryption, selecting which user data to encrypt, and selecting **Save** encrypts user data. Doing so limits some features in the UEM console, such as search, sort, and filter.

8 Select whether to **Enable** or **Disable** the **Do Not Disturb Mode** on the device. This setting lets user devices ignore MDM commands for a specified period. When Enabled, you can select a grace period or activation time in minutes, hours, or days, after which the **Do Not Disturb Mode** expires.

9 Select to **Enable** or **Disable** the **User-Friendly Privacy Notice** on the device.

10 When **Enabled**, you may choose **Yes** (display a privacy notice) or **No** (do not display a privacy notice) for each ownership level: **Employee Owned**, **Corporate - Dedicated**, **Corporate - Shared**, and **Unknown**.

11 Click **Save**. Privacy settings is a restricted action so you must enter your four digit console PIN to continue.

Privacy Notices for BYOD End Users

A privacy notice informs your end users about what data you collect from their devices based on their device type, deployment type, and ownership type.

Privacy Notice Configuration

Privacy notices are automatically delivered based on the organization group and device ownership of the device connecting. You may choose to display a privacy notice for each ownership type: **Employee Owned**, **Corporate - Dedicated**, **Corporate - Shared**, and **Unknown**.

Privacy Notice Deployment

When you assign an ownership type to receive privacy notices, all users in the selected ownership type receive the privacy notification immediately as a Web clip. If you inserted the privacy notice lookup value `PrivacyNotificationUrl` in your message template, then the message includes a URL where the user can read the privacy notice.

Users receive the privacy notice automatically if:

- They enroll a new device and they are of an ownership type for which the privacy notice is enabled.
- They currently use an enrolled device and their ownership is changed post-enrollment to a type that is assigned the Web clip.

To learn how to deploy a privacy notice as part of a device activation, see Register an Individual Device.

Privacy Settings

Privacy settings enable you to define how device and user information are handled in the Workspace ONE UEM console. This information is useful in Bring Your Own Device (BYOD) deployments.

- Review and adjust privacy policies according to device ownership, which lets you align with data privacy laws in other countries or legally defined restrictions.
- Ensure that certain IT checks and balances are in place, preventing overload of servers and systems.

Important Each jurisdiction has its own regulations governing what data can be collected from end users. Research these regulations thoroughly before Configure Privacy Settings.

Create a Privacy Notice for BYOD Users

Inform your users about what data your company collects from their enrolled devices with a customized privacy notification. Work with your legal department to determine what message about data collection you communicate to your end users.

Procedure

1. Navigate to **Groups and Settings > All Settings > Devices and Users > General > Message Templates**.
2. Select **Add** to create a template. If you have already created a privacy notification template, select it from the list of available templates to use or edit it.
3. Complete the **Add/Edit Message Template** settings.

Setting	Description
Name	Enter a name for the notification template.
Description	Enter a description of the template you are creating.
Category	Select **Enrollment**.
Type	Select **MDM Device Activation**.
Select Language	Select the default language for your template. Use the **Add** button to add more default languages for a multi-language delivery.
Default	Assigns this template as the default message template.
Message Type	Select one or more message types: **Email**, **SMS**, or **Push** message.

4. Create the notification content. The message types that you selected in the **Message Type** selection determine which messages appear for you to configure.

Element	Description
Email	
Email Content Formatting	Choose whether your email notification is delivered as **Plain Text** or **HTML**.
Subject	Enter the subject line for your email notification.

Element	Description
Message Body	Compose the email message to send to your users. The editing and formatting tools that appear in this text box depend on which format you chose in the **Email Content Formatting** selection. If you have enabled the Visual Privacy Notice, include the lookup value `PrivacyNotificationUrl` in the message body.
SMS	
Message Body	Compose the SMS message to send to your users. If you have enabled the Visual Privacy Notice, include the lookup value `PrivacyNotificationUrl` in your message body.
Push	
Message Body	Compose the Push notification to send to your users. If you have enabled the Visual Privacy Notice, include the lookup value `PrivacyNotificationUrl` in your message body.

5 Select **Save**.

Privacy Best Practices

Striking a balance between your business needs and the privacy concerns of your employees can be challenging. There are a few simple practices that can manage Privacy Settings to strike the best balance.

Important Every deployment is different. Tailor these settings and policies that fit your organization in the best way by consulting with your own legal, human resource, and management teams.

User Information for Privacy Best Practices

In general, you display user information such as the first name, last name, phone number, and email address for both employee-owned and corporate-owned devices.

Application Information for Privacy Best Practices

In general, it is appropriate to set the collection of application information to either **do not collect** or **collect and do not display** for employee-owned devices. This setting is important because public apps installed on a device, if viewed, can be considered personally identifiable information. For corporate-owned devices, Workspace ONE UEM records all installed applications on the device.

If Do Not Collect is selected, only personal application information is not collected. Workspace ONE UEM collects all managed applications, whether public, internal, or purchased.

Remote Commands for Privacy Best Practices

Consider disabling all remote commands for employee-owned devices. However, if you allow remote actions or commands, explicitly mention these remote actions and commands in your terms of use agreement.

GPS Coordinates for Privacy Best Practices

The collection of GPS coordinates relates to privacy concerns in a fundamental way. While it is not appropriate to collect GPS data for employee-owned devices, the following notes apply to all devices enrolled in Workspace ONE UEM.

- Only the Workspace ONE Intelligent Hub relays device GPS location data back to the UEM console.
  - Other apps that use the Workspace ONE SDK such as VMware Browser, Content Locker, Boxer, and so forth, do not report GPS data back to the UEM console.
  - GPS is typically used for lost or stolen devices. It is also used when knowing the location of a device is inherently part of the Workspace ONE UEM console function such as Geofencing.
  - When GPS data is reported, Workspace ONE UEM defines a 1-kilometer region around this location. It then reports location information whenever the device moves outside the region or whenever the user opens a Workspace ONE UEM or internal application. No new GPS data is reported unless one of these actions occurs.

Telecom Data for Privacy Best Practices

It is only appropriate to collect telecom data for employee-owned devices if they are a part of a stipend where cellphone expenses are subsidized. In this case, or for corporate-owned devices, consider the following about data you can collect.

- **Carrier/Country Code** – Carrier and Country Code are recorded and can be used for telecom tracking purposes. Telecom plans can be set up and devices can be assigned to the appropriate plan based on their carrier and country. This information can also be used to track devices by home carrier and home country or by current country and current carrier.
- **Roaming Status** – This status can be used to track which devices are in a 'Roaming' or 'Not Roaming' state. Compliance policies can be set up to disable voice and data use while the device is roaming or you can also apply other compliance actions. Also, if the device is assigned to a telecom plan, Workspace ONE UEM can track data use while roaming. Collecting and monitoring roaming status can be helpful in preventing large carrier charges due to roaming.
- **Cellular Data Use** – The data use in terms of total bytes sent and received. This data can be collected for each cellular device. If the device is assigned to a telecom plan, you can monitor data use based on a percentage of total data amount per billing cycle. This feature allows you to create compliance policies based on the percentage of data used and is helpful in preventing large carrier overage charges.
- **Cell Use** – The voice minutes that can be collected for each cellular device. Similar to data, if the device is assigned to a telecom plan, you can monitor use based on a percentage of minutes per billing cycle. This method allows you to create compliance policies based on the percentage of minutes used and can be helpful in preventing large carrier overage charges.

- **SMS Use** – The short message service (SMS) data that can be collected for each cellular device. Similar to data, if the device is assigned to a telecom plan, you can monitor SMS use based on a percentage of messages per billing cycle. This method allows you to create compliance policies based on the percentage of messages used. Monitoring SMS use is helpful in preventing large carrier overage charges.

User Data Collection from BYOD End Users

The Workspace ONE UEM infrastructure collects and stores many types of user-generated data. The following matrix matches each data type to the platforms and operating systems from which the data can be collected.

Use this matrix to determine which data collection is necessary for your deployment. Workspace ONE UEM also defines optional data that you can collect, such as Bluetooth MAC. You can configure these options and assign privacy settings by ownership type: dedicated corporate, shared corporate and employee owned.

	Android	Apple iOS	macOS	Windows Rugged	Windows Phone	Windows 7	Windows Desktop
Application Tracking							
View installed internal apps	✓	✓	✓	X	✓	✓	✓
View app versions	✓	✓	✓	X	✓	✓	✓
Capture app status	✓	X	✓	X	✓	X	✓
Certificates							
View list of installed certificates	✓	✓	✓	X	✓	X	✓*
Asset Tracking							
Device Name	✓	✓	✓	✓	✓	✓	✓
Device UDID	✓	✓	✓	✓	✓	✓	✓
Phone Number	✓	✓	X	✓	✓	X	✓
IMEI/MEID Number	✓	✓	X	✓	✓	X	✓
Device serial number	✓	✓	✓	✓	✓	✓	✓
IMSI number	✓	X	X	✓	✓	X	✓
Device model	✓	✓	✓	✓	✓	X	X
Device model name (Friendly)	X	✓	✓	✓	✓	X	X
Manufacturer	✓	✓	✓	✓	X	X	✓
OS Version	✓	✓	✓	✓	✓	✓	✓
OS Build	✓	X	✓	✓	✓	✓	✓
Firmware/kernel version	X	X	✓	X	X	X	X

	Android	Apple iOS	macOS	Windows Rugged	Windows Phone	Windows 7	Windows Desktop
Track device errors	X	X	✓	✓	✓	✓	✓
Device Status							
Battery available	✓	✓	✓	✓	✓	✓	✓
Battery capacity	✓	✓	✓	✓	✓	X	X
Memory available	✓	✓	✓	✓	X	✓	X
Memory capacity	✓	✓	✓	✓	X	✓	X
Location							
GPS tracking	✓	✓**	✓	✓	✓	X	✓
Network							
Wi-fi IP Address	✓	✓	✓	✓	✓	✓	✓
Wi-fi MAC	✓	✓	✓	✓	✓	✓	✓
Wi-fi signal strength	X	X	✓	✓	X	✓	✓
Carrier Settings version	✓	✓	X	X	X	X	X
Cell signal strength	✓	X	X	X	X	X	X
Cell technology (none, GSM, CDMA)	✓	✓	X	X	X	X	X
Current MCC	✓	✓	X	X	X	X	X
Current MNC	✓	✓	X	X	X	X	X
SIM card number	✓	✓	X	X	✓	X	✓
SIM carrier network	✓	✓	X	X	X	X	X
Subscriber MNC	✓	✓	X	X	X	X	X
Bluetooth MAC	✓	✓	✓	X	✓	✓	X
Show IP addresses	✓	✓	✓	X	✓	✓	X
Show LAN adapters	X	X	✓	X	X	✓	X
Show MAC address	✓	✓	✓	X	✓	✓	X
Roaming							
Detect roaming status	✓	✓	X	X	✓	X	X
Disable Push notifications when roaming	X	✓	X	X	X	X	X
Voice roaming enabled (allowed)	X	✓	X	X	X	X	X
Data Usage							
Track data usage through cell network	✓	✓	X	X	X	X	X

	Android	Apple iOS	macOS	Windows Rugged	Windows Phone	Windows 7	Windows Desktop
Track data usage through Wi-fi network	X	X	X	X	X	X	X
Calls							
Track call history	✓	X	X	X	X	X	X
Messages							
Track SMS history	✓	X	X	X	X	X	X
Cellular Status							
Current Carrier network	✓	✓	X	X	✓	X	X
Current network status	✓	✓	X	X	X	X	X
Remote View							
Remotely control device	✓	X	✓	✓	X	✓	✓
Screen capture (save, email, print, etc.)	✓	X	✓	✓	X	✓	✓
Screen sharing (remote view within apps)	✓	✓	X	✓	X	✓	✓
File Manager							
Access device file manager	✓	X	✓	✓	X	✓	✓
Access device registry manager	X	X	X	✓	X	✓	✓
Copy files	✓	X	✓	✓	X	✓	✓
Create folders	✓	X	✓	✓	X	✓	✓
Download files from device	✓	X	✓	✓	X	✓	✓
Move files	✓	X	✓	✓	X	✓	✓
Rename folders and files	✓	X	✓	✓	X	✓	✓
Upload files to device	✓	X	✓	✓	X	✓	✓

✓ - Can be collected

X - Cannot be collected

✓* - Can be collected on Workspace ONE Intelligent Hub deployments

✓** - Can be collected on Workspace ONE Intelligent Hub or iOS 9.3+Supervised Mode deployments

Terms of Use for BYOD End Users

For liability reasons, you must inform employees about the data that is captured and the actions that are allowed on devices enrolled in Workspace ONE UEM. To help communicate your strategy, create Terms of Use agreements in the Workspace ONE UEM console.

Users are prompted to read and accept the terms of use you configure before they can enable MDM on their personal devices. By assigning Terms of Use agreements based on the ownership type, you can create and distribute different agreements for corporate and BYOD users.

After your organization has written its Terms of Use agreement, consider giving it to end users in a one to two-page white paper that omits unnecessary legal language. This white paper is not the official Terms of Use to which end users agree, but instead serves to communicate your corporate policies. Ideally, end users do not see the terms of use for employee-owned devices for the first time when they enroll their device. Be upfront about what end-user information you collect and how your BYOD policies affect them.

Restrictions for BYOD Devices

Workspace ONE UEM permits you to deploy different security policies and restrictions to employee-owned and corporate-dedicated devices.

Using restriction profiles, you can set tight restrictions for corporate-dedicated devices, and looser restrictions for employee-owned devices. For example, restrictions to apps like YouTube or native App Stores are not typically deployed to employee-owned devices. Instead, you can create security profiles and restrictions that increase the level of device security without having a negative impact on functionality.

Device-Agnostic Restrictions

Workspace ONE UEM makes the following restrictions available for every device and platform:

- **Encrypted backups** - Protect all backups with data encryption for BYOD devices with access to corporate content.
- **Force fraud warning in supported browsers** - Require users to acknowledge all warnings issued by the browser when it detects a suspicious site.
- **Disable moving emails** - Prohibit the exposure of sensitive corporate data by disabling the ability to forward a corporate email to a personal account, or open it in third-party applications.

Platform-Specific Restrictions

Each platform has its own set of enforceable restrictions. Evaluate these restrictions individually to determine their value to your deployment. Some, like iOS restrictions limited to supervised devices, do not apply, because employee-owned devices must not be enrolled with Apple Configurator.

- You can create security profiles and restrictions by navigating to **Devices > Profiles > List View** and selecting **Add**, then selecting the appropriate platform.
- If you create profiles specifically for employee-owned devices, only assign them to Smart Groups based on Ownership Type: Employee-Owned.

Enterprise Wipe for BYOD Devices

An essential aspect of your BYOD deployment is removing corporate content when an employee leaves, or when a device is lost or stolen. Workspace ONE UEM allows you to perform an Enterprise Wipe on devices to remove all corporate content and access, but leave personal files and settings untouched.

Workspace ONE UEM lets you decide how an Enterprise Wipe applies to public and purchased VPP applications that sit in a gray area between corporate and employee-owned devices. An Enterprise Wipe also unenrolls the device from Workspace ONE UEM and strips it of all content enabled through MDM. This content includes email accounts, VPN settings, Wi-Fi profiles, secure content, and enterprise applications.

If you used Apple Volume Purchase Plan redemption codes for devices running iOS 6 and earlier, you cannot reclaim any redeemed licenses for that application. When installed, the application is associated to the user App Store account. This association cannot be undone. However, you can redeem license codes used for iOS 7 and later.

Perform an Enterprise Wipe for a BYOD Device

An enterprise wipe unenrolls the device from Workspace ONE UEM and strips it of all enterprise content, including email accounts, VPN settings, profiles, and applications.

Procedure

1. In the Admin Console, select the appropriate organization group.
2. Navigate to **Devices > List View** and select a device or multiple devices from the list.
3. The Device Details view displays a list of actions you can perform under the **More** drop-down in the top right. Select **Enterprise Wipe**.
4. In the confirmation dialog box, select **Prevent Re-Enrollment** to prevent this device from enrolling again.
5. Enter a Security PIN if applicable, and then select **Enterprise Wipe** to finish the action.

Disable Full Wipe for BYOD Devices

For security and privacy reasons, you can disable the ability to perform a full wipe on a BYOD Device.

If you disable full wipe for select iOS ownership types, then users enrolling under that ownership type do not see "Erase all content and settings" permissions during profile installation.

Procedure

1. Navigate to **Devices > Device Settings > Devices & Users > General > Privacy**.
2. Scroll down to the **Commands** section and find the **Employee Owned** column.
3. Set the **Full Wipe** option to **Prevent** and select **Save**.

Device Tags

11

Device tags allow you to identify a specific device without requiring a device profile, smart group, or compliance policy and without creating a note.

For example, if a device has a defective battery or a broken screen, you can use tags to identify these devices from the Workspace ONE UEM console. Another use is to identify hardware variants in a more visible way rather than relying on the model number or description to tell devices apart.

For instance, two PCs can have the same model number, but their CPUs might be slightly different, or the amount of memory might have been customized. Tagging enhanced hardware enables easy identification of these devices.

Tags and Smart Groups

The tag feature is integrated with smart groups, meaning tags can be used to define a smart group.

For instance, if you have tagged all the devices in your fleet with cosmetic damage then you can make a smart group out of these devices. You can then exclude this smart group from the pool of devices you temporarily assign to site visitors.

Another example is tagging low-performing devices. Creating a smart group of these tagged devices and excluding them from being used in mission-critical assignments.

Device Tags and Role Permissions

All activities related to the device tag feature require permissions on the role you assign to your administrators. If you want your admins to own the responsibility of creating tags, you must add that permission (also called resource) to the role you assign to that administrator. The same is true of viewing tags, editing tags, deleting tags, assigning tags, even the ability to search for tags. For details about auditing permissions as they pertain to admin accounts, see View the Resources of an Admin Role.

This chapter includes the following topics:

- Edit an Existing Device Tag
- Delete an Existing Device Tag

Filter Devices by Tag

You can use the filter feature in the Device List View to show only devices with specific tags.

Procedure

1. Navigate to **Devices > List View**, select **Filters** to display the **Filters** column s to the left of the device list.
2. Select **Advanced** from the list of Filter Categories and select **Tags**.
3. Click anywhere in the Search text box and select from the list of device tags that display.

Results

Devices with deselected tags are filtered out of the resulting list. The **Device List View** immediately refreshes itself when the first tag is selected.

Create a New Tag from System Settings

You can create a new device tag for use in the Workspace ONE UEM console. Tags allow you to easily identify a specific device at a glance without requiring a device profile, smart group, or compliance policy and without requiring the creation of a note.

Prerequisites

You must have the correct permissions to create a tag. You can check on these permissions by viewing all the assigned resources (or permissions) of an admin role, modify the role with the 'Create Tag' permission and if not already assigned, then assign the modified role to your admin account. For details, see View the Resources of an Admin Role.

Procedure

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Advanced > Tags**.
2. Select the **Create Tag** button.

   The **Create Tag** screen displays.
3. Enter the **Name** of the tag. The selection of the tag name is what makes the tag useful or not. Select a name that can be used to identify a device at a glance.
4. Select the **Type** of tag you want: **Device**, **General**, or **Video**.
5. Select the **Color code** that is associated with the tag. After you assign this tag to a device, tags of the configured color are visible in the **Device List View**, making them easy to see.
6. Select **Save**.

Results

The device tag is now available to be assigned to a device.

What to do next

Navigate to **Devices > List View** and select one or more devices to assign this tag to.

Assign Tags to a Single Device

When you have to make a quick one-off adjustment of a device's tags, you can assign one or more tags to a single device easily.

You can assign tags to a device to identify it without using notes, profiles, policies, or giving the device a special friendly name.

Are you looking for granting permissions as part of an admin role that includes (or excludes) the ability to assign a tag to a device? See View the Resources of an Admin Role.

Procedure

1 Navigate to **Devices > List View** and select the device you want to tag.

- Display the **Details View** by selecting the device friendly name from the listing.
- Select the check box above the pencil icon, next to the device.

2 Select the **More Actions** button and then select **Assign Tag**.

The **Tag Assignment** screen displays with a listing of tags available to apply to your selected device.

3 Select each of the tags you want to assign to the device.

You can select more than one tag. If you selected **Assign Tag** from the device **Details View**, you also have a **Manage Tags** link which, when selected, opens the Tags System Settings page, enabling you to create a new tag. For more information, see Create a New Tag from System Settings.

4 Select **Save**.

Assign Tags to Multiple Devices

You can assign a tag (or multiple tags) to one or more devices allowing you to identify them without using notes, profiles, policies, or giving the devices special friendly names. Assigning multiple tags to multiple devices saves time.

Prerequisites

You must have the correct permissions to assign a tag to multiple devices. You can check on these permissions by viewing all the assigned resources (or permissions) of an admin role, modify the role with the 'Device Bulk Management assign Tags' permission and if not already assigned, then assign the modified role to your admin account. For details, see View the Resources of an Admin Role.

Procedure

1. Navigate to **Devices > List View**.
2. Select the check box of each device you want to assign a tag to.
3. Select **More Actions** and then select **Assign Tag**.

   The **Tag Assignment** page displays with a listing of tags available to apply to your selected devices.
4. Select the tags you want to assign to all the selected devices.

   You can select more than one tag.
5. Select **Save**.

Edit an Existing Device Tag

You can edit an existing device tag for use in the Workspace ONE UEM console. Tags allow you to easily identify a specific device at a glance without requiring a device profile, smart group, or compliance policy and without requiring the creation of a note.

Prerequisites

You must have the correct permissions to edit a tag. You can check on these permissions by viewing all the assigned resources (or permissions) of an admin role, modify the role with the 'Edit Tag' permission and if not already assigned, then assign the modified role to your admin account. For details, see View the Resources of an Admin Role.

Procedure

1. Navigate to **Groups & Settings > Devices & Users > Advanced > Tags**.
2. Identify the tag you want to edit from the listing.
3. Select the pencil icon (✏) next to the tag you want to edit.

   The Edit Tag screen displays.
4. You can edit the **Name** of the tag, the tag's **Type**, and the **Color code** of the tag.
5. Select **Save**.

Results

The tag has been edited with a new Name, Type, and Color code. Devices that were assigned with the previous tag have been updated with the edited tag.

Delete an Existing Device Tag

So long as a tag is unassigned and you have no plans to use it again, you can delete it from the Workspace ONE UEM console.

Prerequisites

You must have the correct permissions to delete a tag. You can check on these permissions by viewing all the assigned resources (or permissions) of an admin role, modify the role with the 'Delete Tag' permission and if not already assigned, then assign the modified role to your admin account. For details, see View the Resources of an Admin Role.

Tags you want to delete must not be assigned to any device.

To unassign tags from devices, navigate to **Devices > List View** and search for the tag you want to delete. Open the device **Details View** on devices with the assigned tag. Unassign the tag from all devices to which it is assigned.

Procedure

1. Once the tag is completely unassigned, navigate to **Groups & Settings > Devices & Users > Advanced > Tags**.
2. Identify the tag you want to delete from the listing.
3. Select the radio button next to the tag you want to delete.

   The **Delete** button displays above the listing.
4. Select **Delete**.

   A confirmation appears asking "Permanently delete tag?"
5. Select **OK** on the confirmation.

   If the tag is assigned to a device, you are not allowed to delete it. See the instructions above to unassign tags from devices.

Results

If the tag is not assigned to any device when you delete it, it is now removed from the Workspace ONE UEM console.

Introduction to Reports

12

Workspace ONE UEM Reports provide access to reports on various sections of your Workspace ONE UEM solution. Use these reports to analyze patterns from the UEM console.

Custom Reports

Custom reports have moved locations. Navigate to **Monitor > Intelligence**.

For more information, see Reports for Workspace ONE Intelligence.

Workspace ONE UEM Reports

The reports functionality allows you to access detailed information about the devices, users, and applications in your Workspace ONE UEM solution. The exports of these reports are in CSV format.

For more information, see Workspace ONE UEM Reports Overview.

Reports Storage

Optimize the storage of your Workspace ONE UEM Reports through reports storage. This storage feature increases the performance of Workspace ONE UEM Reports. Consider enabling reports storage if you see a performance impact on your Workspace ONE UEM database when using reports.

For more information, see Reports Storage.

This chapter includes the following topics:

Reports for Workspace ONE Intelligence

Use Reports by Workspace ONE Intelligence to collate data in your Workspace ONE UEM deployment. Intelligence reporting uses a cloud-based report storage system to gather data and create the reports.

Reports Background

The Reports feature provides faster, easier access to critical business intelligence data than normal Workspace ONE UEM reports. Build reports using starter templates or customize canned reports. You can select from categories that include Apps, Devices, and OS Updates. These reports provide the latest data extracted from your Workspace ONE UEM environment.

Reports use a separate service to push data to a reports cloud service. This service captures data useful to administrators when trying to answer critical questions. The feature gathers an initial snapshot of your deployment and continues to capture ongoing changes.

Install the Workspace ONE Intelligence Connector Service

Before using Workspace ONE Intelligence features, you must install the Workspace ONE Intelligence Connector service (also known as the ETL installer) onto a separate server in your Workspace ONE UEM environment.

Each feature uses the Workspace ONE Intelligence Connector Service installed from the Workspace ONE Intelligence Connector Installer. The Workspace ONE Intelligence Connector service gathers the data from your Workspace ONE UEM console server and pushes it to the reports cloud service.

For more information, see Workspace ONE Intelligence Requirements and Install the Workspace ONE Intelligence Connector Service for On-Premises.

Reports Wizard

The Reports wizard can create a customized report using a starter template or a new report. The wizard guides you through each step.

Reports use filters you can customize to gather data from apps and devices based on key attributes. Include as many filters as necessary to narrow the results of the report. Each filter added uses the "AND" operator. You then select the value for the value and the operator for each attribute.

For more information, see Run the Reports Wizard.

Manage Reports

After creating a report, manage your reports from the Reports List View. From this screen, you can run reports, schedule reports to run, copy reports, and delete reports.

For more information, see Reports Management

Workspace ONE Intelligence Requirements

Before you can use Workspace ONE Intelligence features, you must turn on reports powered by Workspace ONE Intelligence (different from Workspace ONE UEM reporting). You must then install the Workspace ONE Intelligence Connector service (also known as the ETL installer).

How to Access Reports

- **Shared SaaS** customers work with their account representatives to access reports powered by Workspace ONE Intelligence. These deployments do not need to install their own Workspace ONE Intelligence Connector server.
- **Dedicated SaaS** customers work with their account representatives to access reports powered by Workspace ONE Intelligence. These deployments do not need to install their own Workspace ONE Intelligence Connector server.
- **On-premises** customers work with their account representative to access reports powered by Workspace ONE Intelligence. These deployments must install their own Workspace ONE Intelligence Connector server.

Required Workspace ONE UEM Console Version

Workspace ONE Intelligence requires Workspace ONE UEM console v9.6+.

Required Database Permissions

To install the Workspace ONE Intelligence Connector, the person installing needs permissions for the following roles for the console and directory services servers.

- DBOwner for the Workspace ONE UEM database
- DBDatareader for the MSDB
- SQLAgentUserRole for the MSDB

Workspace ONE Intelligence Connector Server Requirements for On-Premises

You must install the Workspace ONE Intelligence Connector service on its own server before you can use Workspace ONE Intelligence features.

Table 12-1. Hardware Requirments by Number of Devices

Component	5000 Devices	25,000 Devices	50,000 Devices	100,000 Devices
Server	1	1	1	1
CPUs	2 (2 GHz Intel processor)	2 (2 GHz Intel processor)	2 (2 GHz Intel processor)	2 (2 GHz Intel processor)
Memory	4 GB	8 GB	8 GB	8 GB
Storage	25 GB	25 GB	25 GB	25 GB

Table 12-2. Software Requirements

Component	Requirement
Java	Java 8
OS	Windows Server 2012 R2 or later

Table 12-3. Network Requirements

Component	Requirement
Outbound traffic from the Workspace ONE Intelligence Connector service	Port 443
Protocol for outbound traffic from the Workspace ONE Intelligence Connector service	HTTPS
Internal network access to the Workspace ONE UEM Database	The port used is based on your Workspace ONE UEM deployment.

Whitelist Regions of the Cloud Service for On-Premises

On the server for the Workspace ONE Intelligence Connector, whitelist specific URL destinations so that the connector installer can call the endpoints for a list of all supported regions. Also, whitelist other URL destinations depending on your region.

For the list, see the topic *URLs to Whitelist for On-Premises by Region* in the **VMware Workspace ONE Intelligence Guide**.

For an outline of what region resides in what part of the world, see the topic *Workspace ONE UEM SaaS Environment Location Mapped to a Workspace ONE Intelligence Region* in the **VMware Workspace ONE Intelligence Guide**.

Proxy

If you use a proxy server and want to use it with the Workspace ONE Intelligence Connector, make sure you have whitelisted specific destinations. If you do not whitelist the listed destinations, the installation can fail.

For more information, see the topic *URLs to Whitelist for the Use of a Proxy Server in On-Premises Deployments* in the **VMware Workspace ONE Intelligence Guide**.

Install the Workspace ONE Intelligence Connector Service for On-Premises

The Workspace ONE Intelligence Connector service collects data from your Workspace ONE UEM database and pushes it to the cloud-based report service.

Find the connector at https://resources.workspaceone.com/view/88ymmbfft3zt9jbnc3gt/en.

You must install it on its own server. For additional information about the installation process of other Workspace ONE UEM application servers, refer to the **VMware Workspace ONE UEM Installation Guide** on https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/.

Important If you upgrade the Workspace ONE UEM database as part of the upgrade process, you must stop the Workspace ONE Intelligence Connector Service during the Workspace ONE UEM Database upgrade. You must then restart the service after finishing the upgrade process.

Important If you must change the setting for **Deployment Region**, do not run the installer again.

Prerequisites

Ensure you have whitelisted the applicable URLs so the connector installation process can communicate with the correct cloud-based reports service. For the list of URLs, see the topic **URLs to Whitelist for On-Premises by Region**in the **Workspace ONE Intelligence User Guide**.

If you use a proxy server and want to use it with the Workspace ONE Intelligence Connector, make sure you have whitelisted specific destinations. If you do not whitelist the listed destinations, the installation can fail. See the topic URLs to Whitelist for the Use of a Proxy Server in On-Premises Deployments in the **Workspace ONE Intelligence User Guide**.

Procedure

1 Ensure you have met the hardware, software, and network requirements outlined in the **Workspace ONE Intelligence User Guide**.

2 Download the Workspace ONE Intelligence Connector installer on to the server you configured for the service.

3 Run the installer and select **Next**.

4 Accept the Terms of Use and select **Next**.

5 Ensure that the Workspace ONE Intelligence Connector Service is selected as a feature to install. Select **Next**.

The installer detects the version of Java installed on the application server. If the installer does not detect the required version, the required version installs.

6 Enter the Database server settings.

Setting	Description
Database server that you are installing to	Select **Browse** next to the **Database server** text box and select your Workspace ONE UEM database from the list. If you are using a custom port, do not select **Browse**. Instead, use the following syntax: **DBHostName,<customPortNumber > ,** then select **Browse** to select the database server.For example: db.acme.com, 8043
Connect using	Select one of the following authentication methods. ■ **Windows Authentication** uses a service account on the Windows server to authenticate. You are prompted to enter the service account that you want to use. This service account is used to run all the application pools and Workspace ONE UEM-related services. The service account must have Workspace ONE UEM Database access. ■ **SQL Server Authentication** uses the SQL server authentication method. You are prompted to enter the user name and password.
Name of database catalog	Enter the name of the Workspace ONE UEM database or browse the SQL server and select it from a list.

7 Select the Destination Folder in which to install the Workspace ONE Intelligence Connector service.

8 Configure the Workspace ONE Intelligence Connector Service settings.

   a Select the deployment region for your cloud service. Ensure that the right region is selected.

      Do not run the installer again if you must change this region in the future.

      If you upgrade your Workspace ONE Intelligence Connector Service from a previous version, this screen does not display because you cannot change your region during an upgrade.

   b Enter your Workspace ONE UEM Installation Token.

      This token is created as part of the Workspace ONE UEM Installation process.

9 (Optional) Enter proxy information.

   Find this information in the Workspace ONE UEM console in **Groups & Settings > All Settings > Installation > Proxy > Console Proxy Settings**.

10 Select **Install** to install the Workspace ONE Intelligence Connector Service. After the installation finishes, select **Finish**.

Run the Reports Wizard

The reports wizard guides you through creating a customized report on your Workspace ONE UEM environment. The wizard has blank templates that you can use as a base for your reports, or you can customize canned reports.

For information about accessing the Workspace ONE Intelligence UI, see Access Workspace ONE Intelligence.

Procedure

1 Access the Workspace ONE Intelligence UI.

2 Go to **Reporting > Reports** and then select **Add Report**.

3 Select the report category: **Apps**, **Devices**, or **OS Updates**.

4 Select a template and select **Next**.

   - Apps Templates

Setting	Description
Apps Starter Template	Select to create a report from a blank template.
Managed Apps	Select to create a report that shows a list of all managed apps on your devices.
All Apps	Select to create a report that lists all apps, managed or unmanaged, on your devices.
Workspace ONE UEM iOS and Android Agents	Select to create a report that lists all Workspace ONE Intelligent Hub app details on your iOS and Android devices.

- Devices Templates

Setting	Description
Enrolled devices	Select to create a report that lists all enrolled devices and their details.
Non-Compliant Devices	Select to create a report that lists all devices that violate your compliance policies.
Device Starter Template	Select to create a report from a blank template.

- OS Updates Templates

Table 12-4. OS Updates Templates

Setting	Description
All Windows OS Updates	Create a report on all (or filtered) updates to the Windows OS.
Critical Update Status	Create a report containing all (or filtered) critical updates to the OS.
Security Update Status	Create a report focused on security updates to the OS.
Service Pack Update Status	Create a report about service pack updates to the OS.
OS Updates Starter Template	Select to create a report based on a blank template.

5 On the Customize screen, select the add filter icon (+) to add filters to your blank template or customize a starter template further.

Each filter requires the following settings.

Setting	Description
Filter	Select an attribute that corresponds to the data you are trying to gather. For example, the Enrolled Devices template uses the **Enrollment Status** attribute to narrow results.
Selectors	Select an operator that applies to the value of the attribute. For example, if you are using the **Device Organization Group GUID** attribute, select the **Includes** selector to include all devices in the OG that match the value.
Value	Enter a value on which you want to receive data. For some selectors, you can select the value from a drop-down menu whereas others require an explicit entry. For example, if you are using the **Enrollment Status** attribute and the **Includes** selector, select **Enrolled** to receive a report on all enrolled devices. Conversely, if you are filtering devices by the **Country** attribute and the **Include** selector, you must enter in the name of the country you want to include in the report. You must **Add Filter** for each country you want to filter.

6 Under **Report Preview**, select **Edit Columns**.

The **Edit Columns** screen displays.

7 Find the column that corresponds to the filter you have selected to see a preview of the report.

8 Select **Save** to return to the **Add Report** screen and select **Next**.

9 Enter a name and a description for the report.

10 Select **Run report now** if you want to run the report after saving the customized report.

11 (Optional) Select **Run report now** or create a schedule for the report at another time.

12 Select **Save** to save the report.

Access Workspace ONE Intelligence

Access the Workspace ONE Intelligence interface from the Workspace ONE UEM console. From the Workspace ONE Intelligence interface, you can use dashboards, automation, and reports (formerly custom reports).

To access the Workspace ONE Intelligence interface, you must enter your credentials and opt-In to the service.

Access the reports by navigating to **Monitor > Intelligence**, select **Opt-in**, and select **Launch** after installing the Workspace ONE Intelligence Connector service.

To return to the Workspace ONE UEM console, follow the required steps.

Procedure

1 Select the square menu for VMware Services in the top right corner of the UI.

2 Select **Workspace ONE UEM** from the VMware Services menu.

Reports Management

After creating a report, you can manage your reports from the Reports List View. You can run reports, schedule reports to run, copy reports, and delete reports. Select a single report and use the management actions, the scheduler, and the audit logs.

List View

The list view for Reports, **Reporting > Reports**, lets you select multiple reports and take actions with one selection.

- **Add Report** - Opens the Reports wizard to create a new report.
- **Edit** - Edits the filters of a report.
- **Run** - Runs the report immediately. After the report finishes, you receive an email with a link directing you to your report.
- **Share**- Sends the report to a single administrator or multiple administrators. They can then access the report through the link sent.
- **Schedule** - Schedules a report to run and to send an email containing a link to the report after it is finished. To access the report, users must have an admin account on the Workspace ONE UEM console to log in and authenticate before downloading.

- **Copy** - Creates a copy of the report. Use this action when you want different schedules for the same report. Copy also helps when you want to create a report that is based on an existing report without starting from the beginning.
- **Delete** - Deletes a report and removes it and any associated subscriptions permanently.

Single Report View

Select a report to access the **Overview**, **Schedules**, and **Audit Log** tabs.

- **Overview** - The **Overview** tab for a report contains management actions.
  - Edit
  - Run
  - Share
  - Delete
- **Schedules** - The **Schedules** tab contains management actions for scheduling reports.

  Select to add, edit, or delete a report. Add a report and configure the wizard settings. After the report runs, the system sends an email to the contacts configured in the wizard. The email contains a download link to the report. To access the report, users must have an admin account on the Workspace ONE UEM console to log in and authenticate before downloading.

  In the **Schedule** wizard, configure the following settings to schedule a report.

Table 12-5. Settings to Schedule Reports

Setting	Description
Schedule Name	Enter a name for the schedule.
Recurrence	Select from the drop-down menu the frequency the report runs. - Hourly - Daily - Weekly - Monthly The **Recurrence** value affects the available time settings.
Hourly - Every	Select the number of hours that must pass before the report runs again.
Hourly - Starts At	Select the time of day the report runs.
Daily - Time of the day	Select the time of day you want the report to run.
Weekly - Days of the week	Select the days of the week and the time of day you want the report to run.
Weekly - Starts At	Select the time of day the report runs.
Monthly - Day of month	Set the day of the month and the time of day you want the report to run. This setting displays when **Recurrence** is set to **Monthly**.
Monthly - Starts At	Select the time of day the report runs.
All Recurrence Settings - **Ends**	If you want to stop the recurrence of a report, set the end date.
Send To	Enter each recipient email address.

Table 12-5. Settings to Schedule Reports (continued)

Setting	Description
Subject	Enter a subject for the email sent after the report finishes. The email contains the link to access the report.
Message	Enter a message for the email sent after the report finishes.

You can view scheduled reports and their frequency by navigating to **Reporting > Scheduled Reports**. The Scheduled Reports page has **Edit** and **Delete** actions to manage schedules.

- **Audit Log** - The **Audit Log** tab lists events for a report. Find out when an event occurred, who caused it, and what happened. The log lists the following data.
  - Date and time
  - Admin account
  - Event name
  - Action

Workspace ONE UEM Reports Overview

The reports functionality allows you to access detailed information about the devices, users, and applications in your Workspace ONE UEM solution.

Use this information to troubleshoot your deployment and make informed decisions on what actions to take. The exports of these reports are in comma-separated values (CSV) format.

- More intuitive interface.
- Improved report generation reliability.
- Easier filter selection.
- Faster download times.
- Enhanced export status tracing capability.
- Streamlined reports subscription functionality.

The storage of your reports depends on the storage solution you use. By default, Workspace ONE UEM stores the reports in the database. The reports remain in the database until they expire. Once expired, the reports are automatically deleted. Depending on the size of your deployment, consider using a storage solution as an extension to your database to improve performance.

Extend your database with File Storage and Reports Storage.

- File Storage stores reports, content, and application in a separate file storage server.
- Reports Storage stores Workspace ONE UEM Reports in a dedicated file store separate from all other content.

To improve performance, consider enabling the reports storage. This storage uses a dedicated server to store all Workspace ONE UEM Reports and increase performance. For more information, see Reports Storage.

Important If you are using version 9.0.2 or 9.0.3, you must enable File Storage to use Workspace ONE UEM Reports. For more information, see File Storage

New Reports

The **New** tag in front of the report name in the UEM console identifies new reports. These reports combine multiple deprecated reports.

To see the new reports, navigate to **Monitor > Reports & Analytics > Reports > List View**. To see the exported new reports, navigate to **Monitor > Reports & Analytics > Exports**.

Workspace ONE UEM offers 20 new reports. The following table shows the available columns for each of these new reports.

Admin Login History	
Name	Browser
Core User	Platform
Login Date	Failure Reason
Source IP	Status
Admin User Roles	
Organization Group ID	Role
Organization Group Name	Role Description
User name	Last Login Date
Email	User Type
First Name	Primary
Last Name	
Application Details By Device	
Organization Group ID	Installed Version
Organization Group Name	Bundle Size (KB)
Friendly Name	Dynamic Size (KB)
Serial Number	Total Size
App Name	Install Status
App Identifier	Install Status Reason
Deployed By Workspace ONE UEM	App First Seen
Managed App	App Updated Date
Assigned Version	Device ID
Device Type	Device Model

OS Version	Ownership Type
Device Last Seen	User name
Email address	
Blacklist or Non-Whitelist Application Details By Device	
Organization Group ID	Device Model
Organization Group Name	OS Version
Device ID	Ownership
User name	Phone Number
Email Address	App Name
Serial Number	App Identifier
IMEI	App Version
Device Platform	App First Seen
Certificate Near Expiration	
Certificate Name	Profile Name
Issued To	Friendly Name
Issued By	Organization Group Name
CA Name	Effective Date
Status	Days until Expires
Content Details by Device	
Organization Group ID	Content Type
Organization Group Name	Content Installed
Device ID	Content Priority
Friendly Name	Content Importance
User name	Content Category
Email Address	Status
Serial Number	Content Version
IMEI	Content Size in KB
Device Platform	Effective Date
Device Model	Expiration Date
OS Version	Last Modified Date
Ownership	Last Seen
Content Name	Days Offline
Count of Active Devices	
Organization Group Name	Total Number of Inactive Devices
Total Number of Active Devices	Total Number of Devices
Count of Active Devices by Users	

Organization Group ID	Total Number of Inactive Devices
User name	Total Number of Devices
Total Number of Active Devices	
Device Battery Log	
Device ID	Battery Flag
Friendly Name	Battery Life Percent
Organization Group ID	Battery Voltage
Organization Name	Battery Current
Device Model	Battery Temperature
Device Platform	Battery mAh Consumed
OS Version	Battery Average Interval
Owner	Battery Average Current
AC Line Status	Backup Battery Lifetime
Sample Time	Backup Battery Full Life Time
Transmit Time	Backup Battery Life Percent
Battery Life Time	Backup Battery Flag
Battery Full Time	Backup Battery Voltage
Device Inventory	
Organization Group ID	Current Carrier
Organization Group Name	Device Roaming
Device ID	Roaming Start date
Friendly Name	Roaming End Date
User name	MAC Address
Email Address	Wi-Fi IP Address
First Name	IMEI
Last Name	Sim Card Number
Display Name	GPRS Connection
Serial Number	Device Capacity(GB)
Device Platform	Available Capacity(GB)
Device Model	Available Physical Memory (MB)
Phone Number	Total Physical Memory (MB)
Ownership	Battery Life Percent
OS Version	AC Power Sample Time
Enrollment Date	Device On AC Power
Compliance Status	Payload Removal Disallowed
Enrollment Status	Is Supervised

Unenrollment Date	EAS DeviceID
Managed By	Is Cloud Backup Enabled
Last Seen	Last iCloud Backup Date
Asset Number	Is Activation Lock Enabled
Is Compromised	Purchase Country
Find My iPhone	Estimated Purchase Date
Country	Warranty Status
MDM Managed	Registration Date
Device Identifier	Coverage Start Date
Home Carrier	Coverage End Date
Device Location Log	
Organization Group Name	Email Address
Organization Group ID	Sample Time
Friendly Name	Latitude
Device ID	Longitude
User name	Elevation
Device Security Posture	
Organization Group ID	IMEI
Organization Group Name	Data protection is enabled
Device ID	Block level encryption is enabled
Friendly Name	File level encryption is enabled
Serial Number	Passcode is present.
Device Model	Passcode Compliant Y/N
Phone Number	Pending Installs
Ownership	All assigned profiles are installed
OS Version	Passcode Compliant With Profiles
Last Seen	Encryption is compliant
Is Compromised	Internal storage encryption is enabled
MAC Address	SD Card encryption is enabled
Wi-Fi IP Address	Offline Days
Enrollment User Name	Device Group
Email Address	
Device Usage Detail	
Organization Group ID	Roaming Data Usage
Organization Group Name	Data Usage (MB)

Device ID	Plan Name
Friendly Name	Cell Card Identifier
Ownership	Record Date
Device Platform	Daily Peak Voice
Device Model	Daily Off Peak Voice
OS Version	Daily Message
User name	Message Limit
Email Address	Daily Data Usage
Serial Number	Billing Cycle
IMEI	Monthly Peak Voice
Phone Number	Monthly Voice Percent Utilization
Last Seen	Monthly Off Peak Voice
Sim Card Number	Monthly message
Sample Time	Monthly Message Percent Utilization
Home Carrier	Monthly Data Usage
Current Carrier	Monthly Data Percent Utilization
Country	Call Start Date Time
Network IP Address	Call Duration Minutes
Cellular IP Address	Call Direction
Device Roaming	Call Answered State
Roaming Start date	Call End State
Roaming End Date	Call Connection State
Data Received (KB)	Call Roaming
Data Sent (KB)	Contact Name
Total KB	
Device Wipe Log	
Device ID or MAC Address	Organization Group ID
Friendly Name	Organization Group Name
Serial Number	User name
Device Type	Email Address
Device Model	Wipe Issued By
OS Version	Wipe Type
Ownership	Event Time
Device Platform	
Devices with User Details	

Organization Group ID	User Status
Organization Group Name	Device Platform
Friendly Name	Device Model
Device ID	OS Version
User name	Ownership
User Id	Serial Number
First Name	IMEI
Last Name	Enrollment Status
Email Address	Compliance Status
User Phone Number	Date Enrolled
Domain Type	Date Unenrolled
Profile Configuration Settings	
Organization Group	Device Model
Profile Name	Minimum Operating System Name
Profile Group Type	Maximum Operating System Name
Device Platform	Profile Setting Name
Description	Value
Assignment Type	Location Group Path
Profile Details by Device	
Organization Group ID	Model
Organization Group Name	OS Version
Friendly Name	C/E/S
User name	Profile
Email User name	Installed Version
Email Address	Latest Version
Serial Number	Installed Date
MAC Address	Installed
SDK Analytics	
Device ID	App Identifier
Friendly Name	Application Name
Organization Group ID	Application Version
Organization Group Name	Event Name
User name	Event Data
Sample Time	
Shared Device History	

Organization Group ID	Last Name
Organization Group Name	Email Address
Device ID	Check-in Date
Device Name	Checkout Date
First Name	
Terms of Use Acceptance Detail	
Organization Group Name	Phone Number
Organization Group ID	Terms of Use Name
User name	Version
First Name	Accepted Version
Last Name	Accepted
Email Address	Accepted On

Subscribe to a New Report

Subscribe to a new report to receive alerts from the **Monitor** page of the UEM console. Subscription enables you to access important information regarding usage and other technical parameters.

For security reasons, the subscription email for new reports does not contain the report as a file attachment. The email provides a link to download the report. This link requires authentication to download. Only admins with valid credentials can access the reports.

Important Administrators with the appropriate role permissions and organization group access can view and edit other administrator's subscriptions.

Procedure

1 Navigate to **Monitor > Reports & Analytics > Reports > List View > All Reports**.

2 Select a desired new report and select the **Report Subscriptions** icon.

3 On the **Parameters** tab, configure applicable settings to set criteria for the scope of the report.

These settings vary depending on the report.

4 On the **Schedule** tab, configure the following settings.

Setting	Description
From	Specifies from whom the subscription is sent.
To	Specifies who receives the subscription.
Recurrence	Defines when the UEM console sends the subscription. Available options are once, daily, weekly, and monthly. You can also set the time of day for the report and the end of recurrence. If the recurrence is set to specific days of the month such as the 31st day of a month when the month only has 30 days, you do not receive a report for that month.

Setting	Description
Date/Time	Specifies when to start sending subscriptions.
Subject	Specifies a subject to help identify the subscription when the UEM console delivers it.
Message	Defines the message to explain the subscription when the UEM console delivers it.

Generate Reports

The Workspace ONE UEM reports and analytics solution includes the ability to export data from many sections in the UEM console. From the **Exports** page on the UEM console, you can download the generated reports – once reports are successfully generated, links to download are available in the **Export** grid.

Procedure

1 Navigate to **Monitor > Reports & Analytics > Reports > List View** and select the desired report.

2 On the report screen, complete the applicable settings.

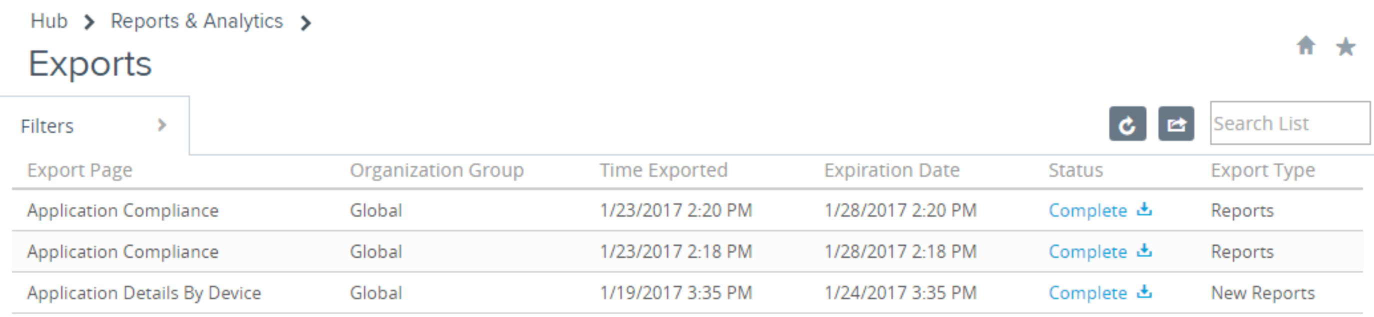
These settings vary depending on the report.

3 Click **Download** to export the report to the **Exports** page.

4 Navigate to **Monitor > Reports & Analytics > Exports** and select the desired report. Click **Complete** available under **Status** column against the selected report to download it.

Results

Note The exported new reports are mentioned as **New Reports** and the existing reports are mentioned as **Reports** under **Export Type** column.



Export Page	Organization Group	Time Exported	Expiration Date	Status	Export Type
Application Compliance	Global	1/23/2017 2:20 PM	1/28/2017 2:20 PM	Complete	Reports
Application Compliance	Global	1/23/2017 2:18 PM	1/28/2017 2:18 PM	Complete	Reports
Application Details By Device	Global	1/19/2017 3:35 PM	1/24/2017 3:35 PM	Complete	New Reports

What to do next

Note From v9.0, the reports (in a comma-separated values (CSV) structure) are available for download in zipped format.

Subscribe to an Old Report

Subscribe to a report to receive alerts from the **Monitor** page of the UEM console. Subscription enables you to access important information regarding usage and other technical parameters.

Important Any subscriptions associated with a deprecated report should function as it is. Instead, they are marked as deprecated. Consider using new reports and creating subscriptions to use them.

Procedure

1 Navigate to **Monitor > Reports & Analytics > Reports > List View > All Reports**.

2 Select a desired report and select the **Report Subscriptions** icon.

3 On the **General** tab, configure the following settings.

Setting	Description
Description	Defines a descriptive name for the subscription.
Render Format	Defines the format for the report. The default file format is comma-separated values (CSV).
Reply To	Specifies who receives the subscription.
Subject	Specifies a subject to help identify the subscription when the UEM console delivers it.
Message Body	Defines the message to explain the subscription when the UEM console delivers it.

4 On the **Parameters** tab, configure applicable settings to set criteria for the scope of the report.

These settings vary depending on the report.

5 On the **Execution** tab, configure the following settings.

Setting	Description
Once	Select this option to subscribe to this report a single time.
Daily	Select this option to receive the report every time a set number of days pass.
Weekly	Select this option to receive the report on specific days of the week.
Monthly	Select this option to receive the report on a specific day of the month. You can also set the schedule to First, Second, Third, Fourth, or Last weekday of the month. If the recurrence is set to a day that does not occur in the month, you do not receive a report. For example, if you set recurrence to the Fourth Friday of a month, and the month only has 3 Fridays, you do not receive a report for that month. This also applies to specific days of the month such as the 31st day of a month when the month only has 30 days.
Date/Time	Set the specific day and time to receive the report.
Range	Set the end date for the subscription to the report.

6 On the **Distribution List** tab, use one or all the parameters to make a distribution list to receive the subscription.

Setting	Description
Choose Role	Select a role from the menu and click **Add to List** to add it to the distribution list.
Choose User	Select individual users and click **Add to List** to add them to the distribution list.
Enter Email Address	Enter the addresses of subscription recipients manually, if you know the address and click **Add to List** to add them to the distribution list.
Search List	Enter text to search the distribution list to find individual entries and to delete entries from the distribution list.
Distribution List	Define to whom Workspace ONE UEM sends the subscription. Create this list using the role, user, and email address entries.

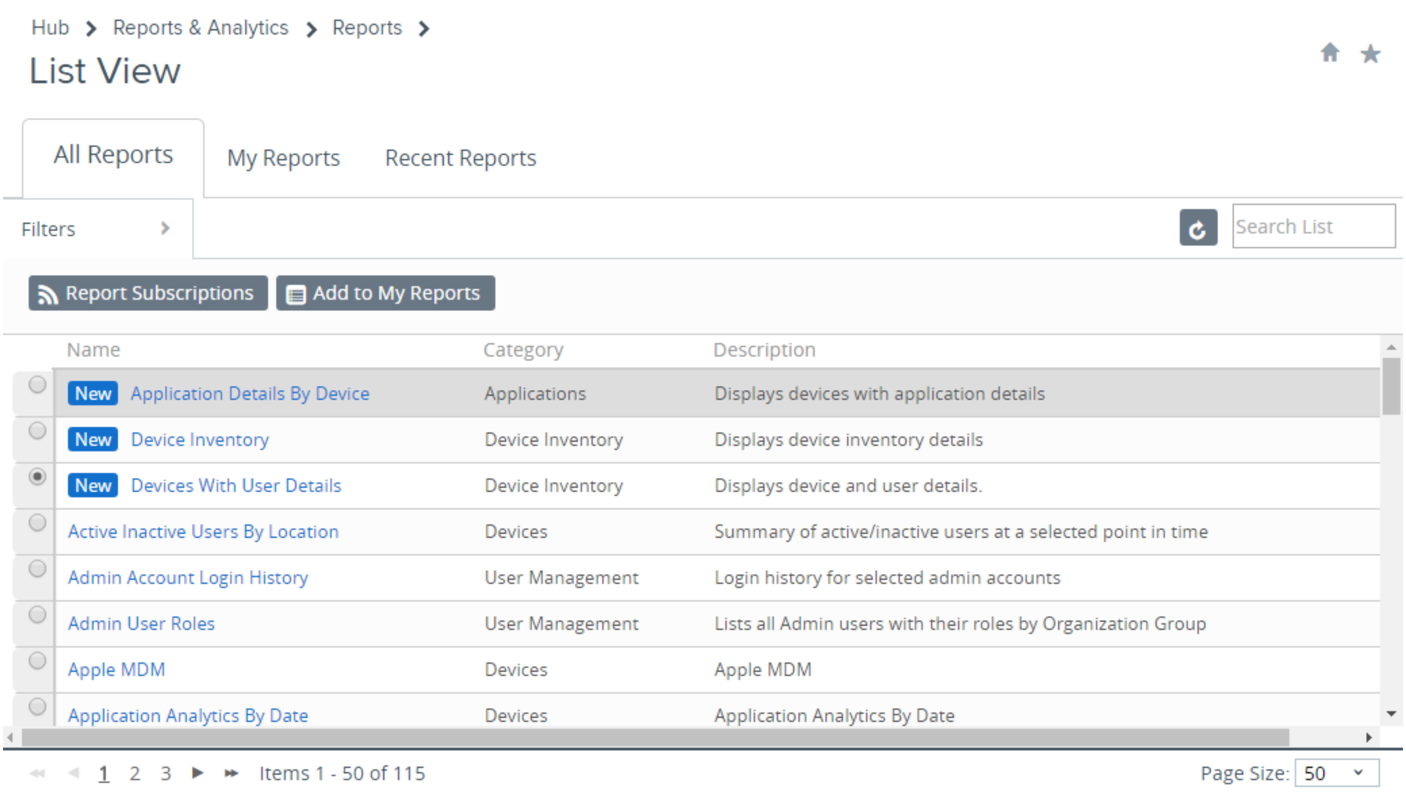
Note Admins can edit failed or inactive subscriptions and can save them again to fix the error.

Manage Reports

You can navigate to **Monitor > Reports & Analytics > Reports > List View** page to view reports in the UEM console. You can export data in various formats and perform the following actions.

Report Subscriptions – Configure a report to run on a specified interval with defined parameters.

Add to My Reports – Add reports to the **My Reports** tab for quick access.



	Name	Category	Description
○	New Application Details By Device	Applications	Displays devices with application details
○	New Device Inventory	Device Inventory	Displays device inventory details
●	New Devices With User Details	Device Inventory	Displays device and user details.
○	Active Inactive Users By Location	Devices	Summary of active/inactive users at a selected point in time
○	Admin Account Login History	User Management	Login history for selected admin accounts
○	Admin User Roles	User Management	Lists all Admin users with their roles by Organization Group
○	Apple MDM	Devices	Apple MDM
○	Application Analytics By Date	Devices	Application Analytics By Date

Troubleshooting Reports

If you are having issues with the Reports feature, consider troubleshooting your issue before calling support. These troubleshooting steps address the most common issues with the Reports feature.

Problem

Reports do not initiate.

Cause

The background processing service is not running.

Solution

Follow the instructions in Enable Background Processing Service.

Problem

Errors occasionally occur during report processing.

Cause

Various causes.

Solution

Refer to the following logs.

- Web Console Logs – For troubleshooting purpose, refer to web console logs when any console error occurs. These logs can be referred for both new and existing reports. Logs can be found here:

  ```
   \AirWatch\Logs\WebConsole\WebConsoleLog.txt
  ```

- Detailed error logs about new reports – Refer to logs found here:

  ```
  \AirWatch\Logs\Services\BackgroundProcessorServiceLogFile.txt
  ```

- Detailed error logs about old reports – Refer to the reports server logs found here:

  ```
  \Microsoft SQL Server\MSRS12.ABC\Reporting Services\LogFiles
  ```

Enable Background Processing Service

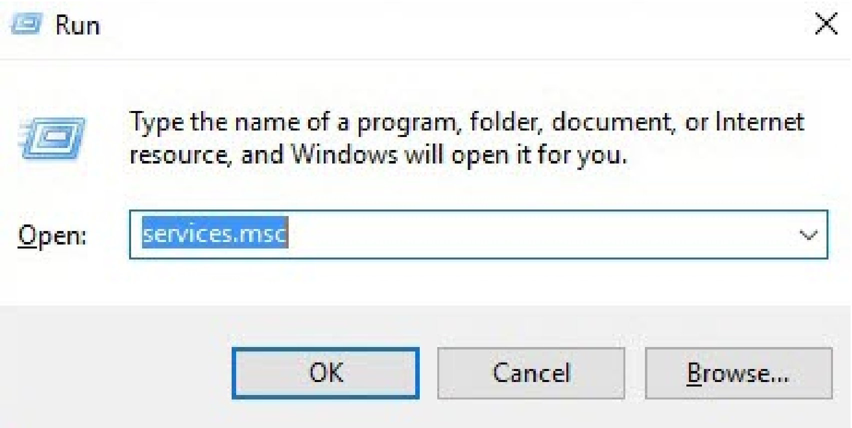
Workspace ONE UEM Reports require the background processing service running on the UEM console server. The installation process enables this process but if it is not running, you must enable it to use Workspace ONE UEM Reports.

Each UEM console server requires the background processing service. Each server processes reports and writes them to their respective queue before sending them to the database, file storage, or reports storage.

Procedure

1 Press **Windows key + R** on the console server box.

2 Run the command "services.msc".



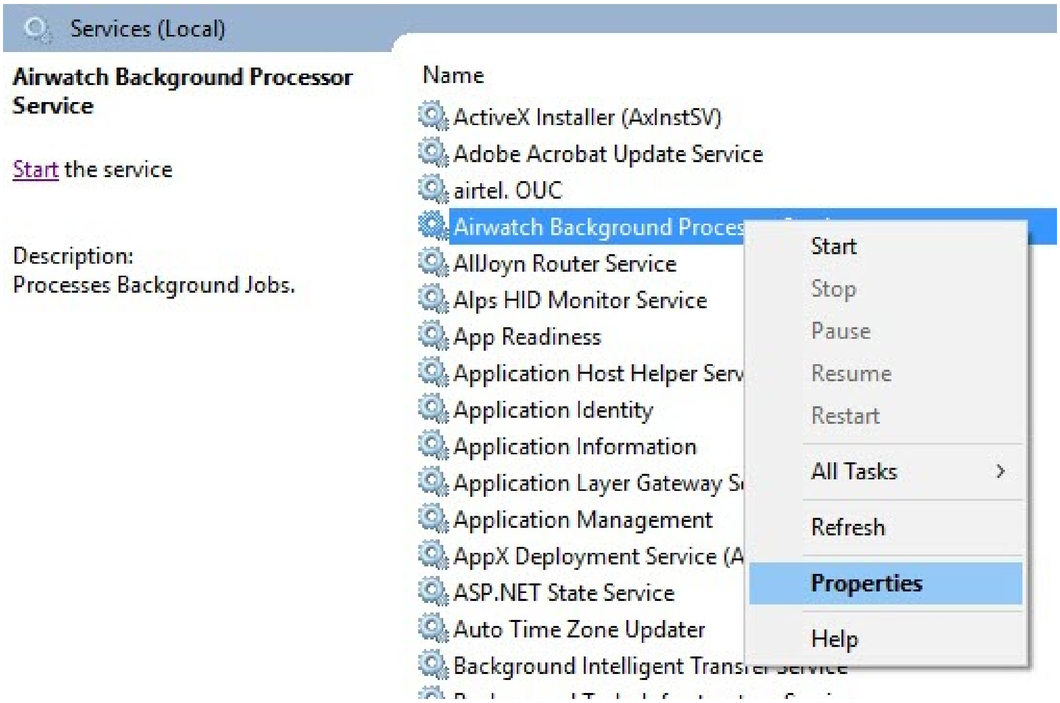
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: services.msc

A screen appears listing all services running on the Console Server box.

3 Locate **Airwatch Background Processor Service** and select **Properties**.



Services (Local)

Airwatch Background Processor Service

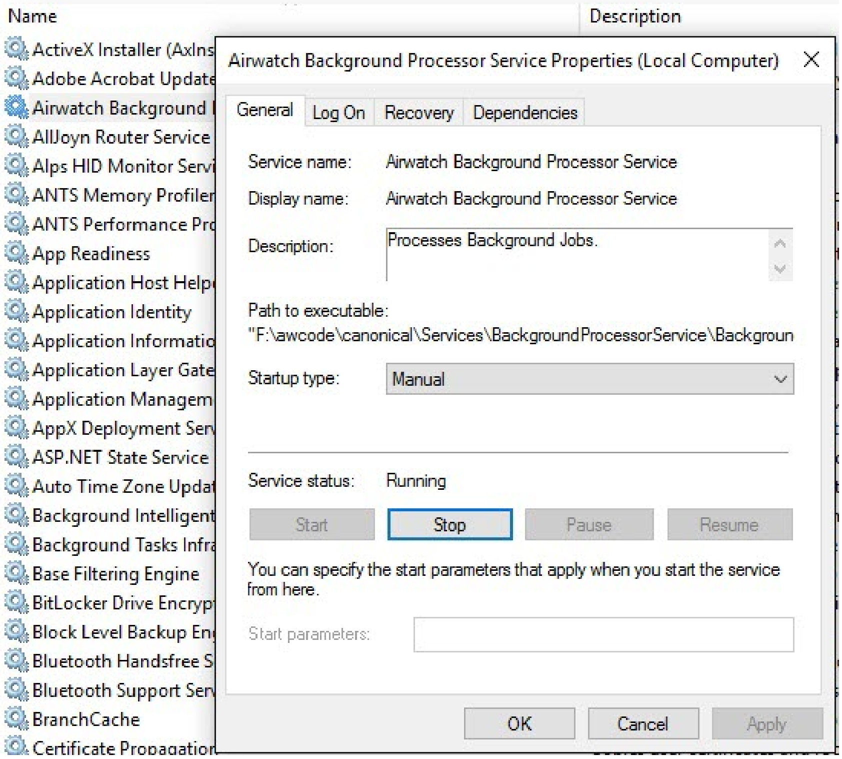
Start the service

Description:
Processes Background Jobs.

Name
ActiveX Installer (AxInstSV)
Adobe Acrobat Update Service
airtel. OUC
Airwatch Background Proces
AllJoyn Router Service
Alps HID Monitor Service
App Readiness
Application Host Helper Serv
Application Identity
Application Information
Application Layer Gateway S
Application Management
AppX Deployment Service (A
ASP.NET State Service
Auto Time Zone Updater
Background Intelligent Trans

A screen appears showing if the service status.

4 Make sure that status of this service is **Running**. If status is **Stopped**, ensure to **Start** the service.



Airwatch Background Processor Service Properties (Local Computer)

Service name: Airwatch Background Processor Service

Display name: Airwatch Background Processor Service

Description: Processes Background Jobs.

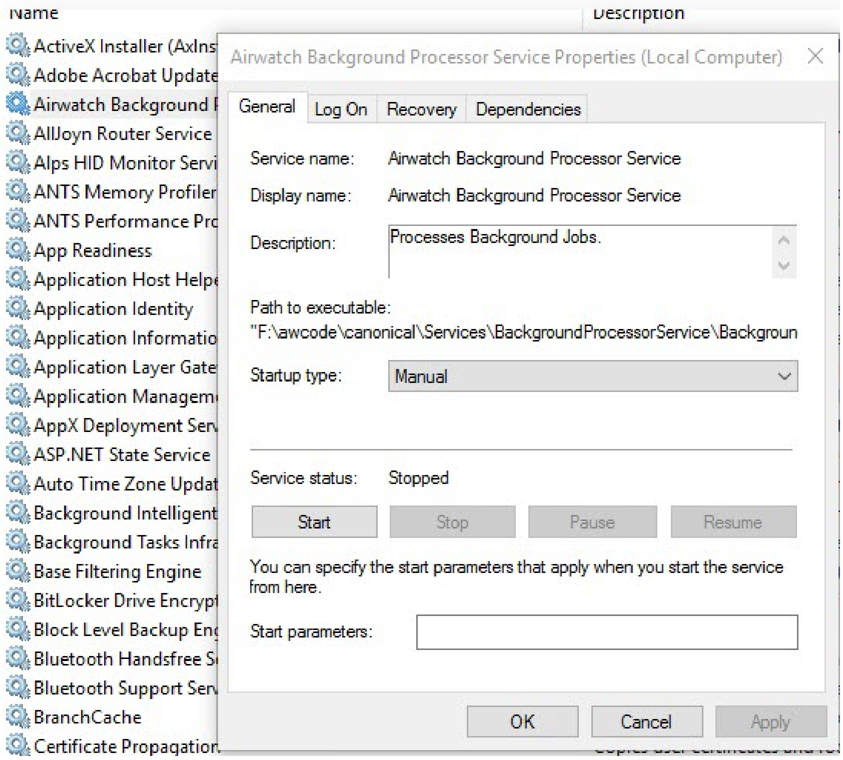
Path to executable:
"F:\awcode\canonical\Services\BackgroundProcessorService\Backgroun

Startup type: Manual

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:



Airwatch Background Processor Service Properties (Local Computer)

Service name: Airwatch Background Processor Service

Display name: Airwatch Background Processor Service

Description: Processes Background Jobs.

Path to executable:
"F:\awcode\canonical\Services\BackgroundProcessorService\Backgroun

Startup type: Manual

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

File Storage

Certain Workspace ONE UEM functionality uses a dedicated file storage service to handle processing and downloads, which reduces the overall burden on your Workspace ONE UEM database and increases its performance. Configuring file storage manually is only applicable to on-premises customers. It is automatically configured for SaaS customers.

It also includes certain Workspace ONE UEM reports, internal application deployment, and Workspace ONE UEM-managed content. When you enable file storage for any of these functionalities, it is applied to the others automatically. Setting up file storage causes all reports, all internal applications, and all managed content to be stored there.

Workspace ONE UEM Reports

As of console version 9.0.2, three new reports were added that appear the same as existing reports but use a revamped back-end framework. This new framework generates reports with greater reliability and faster download times. To take advantage of these benefits, you must set up file storage.

Internal Applications

When file storage is enabled, all internal application packages that you upload through the UEM console are stored in a file storage location.

File storage is required to deploy Win32 applications (IPA, PAK, APPX, MSI, EXE, and so on) and macOS applications (.dmg, .pkg, .mpkg, and so on) from the Apps & Books area of the UEM console. This feature is called software distribution.

Workspace ONE UEM Managed Content

You can separate the managed content from the Workspace ONE UEM database by storing it in a dedicated file storage location. Uploading large amounts of managed content might cause issues with database performance. In this case, on-premises customers can free up space in the database by moving the managed content to an integrated local file storage solution.

Personal content also moves to the file storage solution is enabled. By default, personal content is stored in the SQL database. If you have a Remote File Storage enabled, personal content is stored in the RFS and not in the file storage or SQL database.

File Storage Requirements

Separate the managed content from the Workspace ONE UEM database by storing it in a dedicated File Storage. To set up a file storage, you must determine the location and storage capacity for your file storage, configure the network requirements, and create an impersonation account.

Important File Storage is required for Windows 10 Software Distribution.

Create the Shared Folder on a Server in Your Internal Network

- File storage can reside on a separate server or the same server as one of the other Workspace ONE UEM application servers in your internal network. It is only accessible to components that require access to it, such as the Console and Device Services servers.
- If the Device Services server, Console server, and the server hosting the shared folder are not in the same domain, then supply the domain during service account configuration in the format <domain\username>. Domain Trust can also be established to avoid authentication failure.

Configure the Network Requirements

- **If using Samba/SMB** – TCP: 445, 137, 139. UDP: 137, 138
- **If using NFS** – TCP and UDP: 111 and 2049

Allocate Sufficient Hard Disk Capacity

Your specific storage requirements may vary depending on how you plan to use file storage. The file storage location should have enough space to accommodate the internal apps, managed content, or reports you intend to use. Take into the account the following considerations.

- If you enable caching for internal apps or content, then a best practice is to size the Device Services server for 120 percent of the cumulative size of all the apps/content you need to publish.
- For storing reports, your storage requirements depend on the number of devices, the daily amount of reports, and the frequency with which you purge them. As a starting point, you should plan to allocate at least 50 GB for deployment sizes up to 250,000 devices running about 200 daily reports. Adjust these numbers based on the actual amount you observe in your deployment. Apply this sizing to your Console server as well if you enable caching.

Create a Service Account with Correct Permissions

- Create an account in the domain of the shared storage directory.
- Give the local user read/write/modify permissions to the file share that is being used for the File Storage Path.
- Configure File Storage Impersonation User in Workspace ONE UEM with the domain account in the format <domain\username>.
- If the shared storage directory is not on a domain, create an identical local user and password on the server being used for File Storage, Console, and Device Services server. In this case, supply the local user account in the format <username>.

You can also use a domain service account instead of a local user account.

Configure File Storage at the Global Organization Group

Configure file storage settings at the Global organization group level in the UEM Console.

Enable File Storage for Reports

Before you can enjoy the benefits of reports file storage, you must enable and configure file storage.

Procedure

1 At the Global organization group level, navigate to **Groups & Settings > All Settings > Installation > File Path** and scroll to the bottom of the page.

2 Select the **File Storage Enabled** slider and configure the settings.

When file storage is enabled, you can configure an external repository in which files are stored. A disabled setting means that files are stored as binary large objects in the database.

Setting	Description
File Storage Path	Enter the path files are to be stored in the following format: \\{Server Name}\{Folder Name}, where Folder Name is the name of the shared folder you create on the server.
File Storage Caching Enabled	If you enable caching, consider accommodating for the amount of space needed on the server.
File Storage Impersonation Enabled	Select to add a service account with the correct permissions.
File Storage Impersonation Username	Provide a valid service account user name to obtain both read and write permissions to the shared storage directory.
Password	Provide a valid service account password to obtain both read and write permissions to the shared storage directory.

3 Select the **Test Connection** button to test the configuration.

Reports Storage

Optimize the storage of your Workspace ONE UEM Reports through reports storage. This storage feature increases the performance of Workspace ONE UEM Reports.

This storage is different than file storage used by reports, internal applications, and content. If you already use file storage, you do not need to enable reports storage. Consider enabling reports storage if you see a performance impact on your Workspace ONE UEM database when using reports. Reports storage applies to reports only, helping increase overall reports performance, and reducing the burden on your Workspace ONE UEM database.

If you enable both file storage and reports storage, reports storage overrides file storage when storing reports.

Report storage requires a dedicated server to host the service and storage of the reports.

Reports Storage Requirements

To deploy the reports storage solution, ensure that your server meets the requirements.

Note If you are already using File Storage, then Report Storage is available, but not required to run your deployment. If you configure Reports Storage alongside File Storage, the report files will prioritize report storage over file storage.

Create the Shared Folder on a Server in Your Internal Network

- Report storage can reside on a separate server or the same server as one of the other Workspace ONE UEM application servers in your internal network. Ensure only the components that require access to the server can access the report storage server, such as the Console and Device Services servers.
- If the Device Services server, Console server, and the server hosting the shared folder are not in the same domain, then establish Domain Trust between the domains to avoid an authentication failure. If the Device Services or Console servers are not joined to any domain, then supplying the domain during service account configuration is sufficient.

Configure Reports Storage at the Global Organization Group

Configure reports storage settings at the Global organization group level in the UEM console.**Create a Service Account with Correct Permissions**

- Create an account with read and write permissions to the shared storage directory.
- Create the same local user and password on the Console, Device Services, and the server that is being used for report storage.
- Give the local user read/write/modify permissions to the file share that is being used for the Report Storage Path.

  If you give the user modify permission, Workspace ONE UEM deletes old reports from the storage. If you do not give the user modify permissions, consider monitoring report storage to prevent running out of space.
- Configure the Report Storage Impersonation User in Workspace ONE UEM with the local user.

You can also use a domain service account instead of a local user account.

Allocate Sufficient Hard Disk Capacity

Your specific storage requirements can vary depending on how you plan to use reports storage. Ensure that the reports storage location has enough space to accommodate the reports you intend to use.

For storing reports, your storage requirements depend on the number of devices, the daily number of reports, and the frequency with which you purge them. As a starting point, plan to allocate at least 50 GB for deployment sizes up to 250,000 devices running about 200 daily reports. Adjust these numbers based on the actual amount you observe in your deployment. Also apply this sizing to your Console server if you enable caching.

Enable Reports Storage

Enable reports storage to store your reports on a dedicated server and improve performance.

Procedure

1 Navigate to **Groups & Settings > All Settings > Installation > Reports**.

2 Set **Report Storage Enabled** to **Enabled**.

3 Configure the report storage settings.

Settings	Description
Report Storage File Path	Enter the path reports are to be stored in the following format: \\{Server Name}\{Folder Name}, where Folder Name is the name of the shared folder you created on the server.
Report Storage Caching Enabled	When enabled, files are cached locally on the DS server when accessed for the first time. Subsequent requests are served using the file cached on the DS server instead of streaming from the file storage location. If you enable caching, consider accommodating for the amount of space needed on the server. For more information, see Reports Storage Requirements.
Report Storage Impersonation Enabled	Enabling this option adds a service account with the correct permissions.
Report Storage Impersonation user name	Enter the user name of a valid service account with both read, write, and modify permissions to the shared storage directory. Displays when **Report Storage Impersonation Enabled** is enabled.
Report Storage Impersonation Password	Enter the password of a valid service account with both read, write, and modify permissions to the shared storage directory. Displays when **Report Storage Impersonation Enabled** is enabled.

4 Select the **Test Connection** button to test the configuration.

Certificate Management

13

As the mobility of sensitive corporate content becomes the norm, the probability of unauthorized access and malicious threats increases. Even if you protect your corporate email, Wi-Fi, and virtual private network (VPN) using strong passwords, your infrastructure remains vulnerable. Your infrastructure is vulnerable to brute force attacks, dictionary attacks, and employee error.

For much greater protection, consider implementing digital certificates for securing your corporate assets. Certificates offer a level of stability, security, and authentication with which passwords cannot compete. Mobile Certificate Management by Workspace ONE UEM solves this problem by ensuring security throughout the lifecycle of a device.

Revoke and Renew Digital Certificates

You can revoke and renew certificates individually or in bulk by using the Renew or Revoke Digital Certificates.

This chapter includes the following topics:

Renew or Revoke Digital Certificates

Once issued, Workspace ONE UEM enables you to manage deployed digital certificates using the **Certificate List View** in the Workspace ONE UEM console. Administrators can view and sort certificates by device, authority, user, profile, issued date, and so on. Navigate to **Devices > Certificates > List View**.

The Certificate List View provides a summary of deployed certificates and the ability to renew or revoke certificates individually or in bulk. Locate and revoke all digital certificates from a deactivated user/device or even renew/rotate all Wi-Fi authentication certs before a compliance driven expiration date.

Procedure

1 Initiate the process by navigating to **Devices > Certificates > List View**.

2 Identify and select the digital certificates you want to renew or revoke by inserting one or more check marks in the empty check boxes.

3 Select the action button that you want to apply the action to the selected certificates.

- **Renew**
- **Revoke**

Certificate Integration Resources

You can find each of the certificate documents by name on docs.vmware.com.

- **VMware AirWatch Certificate EOBO with ADCS via DCOM** – Set up the Enrollment Agent Signing Certificate using ADCS over the DCOM protocol and take advantage of Microsoft’s Certificate Enroll On Behalf Of Others function.
- **VMware AirWatch Certificate Authentication for Cisco AnyConnect** – Set up your Cisco ASA Firewall with Workspace ONE UEM to automatically deploy and configure AnyConnect VPN with External CA Authentication.
- **VMware AirWatch Certificate Authentication for Cisco IPSec VPN** – Set up your Cisco ASA Firewall and Workspace ONE UEM to automatically deploy and configure IPSec VPN with External CA Authentication.
- **VMware AirWatch Certificate Authentication for EAS with ADCS** – Establish trust between your directory services, certificate authority, and an email server other than CAS.
- **VMware AirWatch Certificate Authentication for EAS with NDES-MSCEP** – Set up the Microsoft Exchange Client Access Server (CAS) and Workspace ONE UEM to allow a device to connect to Microsoft Exchange ActiveSync (EAS) using a certificate for authentication.
- **VMware AirWatch Certificate Authentication for EAS with SEG** – Set up Kerberos Delegation to enable EAS certificate authentication with the Secure Email Gateway.
- **VMware Workspace ONE UEM Integration with Entrust IdentityGuard** – Integrate with Entrust IdentityGuard service.
- **VMware Workspace ONE UEM Integration with Global Sign Guide** – Integrate with GlobalSign's services to issue certificates.
- **VMware Workspace ONE UEM Integration with JCCH Guide** – Integrate with JCCH's services to issue certificates.
- **VMware Workspace ONE UEM Integration with Microsoft ADCS via DCOM** – Set up the MS certificate authority for direct CA over the DCOM protocol. Take advantage of digital certificates by automating the issuing, renewal, and revocation process to mobile devices.
- **VMware Workspace ONE UEM Integration with Microsoft NDES via SCEP** – Set up the Microsoft certificate authority for direct CA integration with Workspace ONE UEM over the NDES/SCEP/MSECP protocol.
- **VMware Workspace ONE UEM Integration with OpenTrust CMS Mobile 2** – Integrate with OpenTrust CMS Mobile services.

- **VMware Workspace ONE UEM Integration with RSA PKI Guide** – Integrate with RSA PKI to issue certificates.
- **VMware Workspace ONE UEM Integration with SCEP** – Use SCEP to leverage certificates as part of your Workspace ONE UEM deployment.
- **VMware Workspace ONE UEM Integration with SecureAuth PKI Guide** – Integrate with SecureAuth PKI services to issue certificates.
- **VMware Workspace ONE UEM Integration with Symantec MPKI Guide** – Integrate with Symantec's MPKI services.
- **VMware AirWatch Certificate Authentication for EAS with SEG and TMG** – Discusses two configurations – TMG to EAS server and TMG to SEG to EAS server and defines the configurations required in order to setup certificate authentication.
- **VMware Workspace ONE UEMSecuring Mobile Devices with Certificates** – Learn more about why, in the mobile landscape, digital certificates do more than act as a security safeguard for internal content.
- **VMware Workspace ONE UEM Selecting Microsoft CA Deployment Models Overview** – Provides you with an overview of the different Microsoft CA Deployment Model and helps you in selecting the right deployment model for your enterprise.

Custom Attributes

14

Custom attributes enable you to extract specific values from a managed device and return it to the Workspace ONE UEM console. You can also assign the attribute value for device lookup values.

Note Custom attributes (and the rules generator) are only configurable and useable at Customer-level organization groups.

Custom Attributes Database

Custom attributes are stored either as XML files on the device or in the custom attribute database on the Workspace ONE UEM console server. When using the database, custom attributes are sent as samples to Workspace ONE UEM periodically for asset tracking of key/value pairs. If a record in the device database is configured with 'Create Attribute' = TRUE, then the Workspace ONE Intelligent Hub automatically retrieves the Name and Value sent with the custom attributes sample. The key/value pair displays in the Device Details page for the device in the Custom Attributes tab.

Note Custom Attribute values cannot return the following special characters: **/ \ " * : ; < > ? |**. If a script returns a value which contains these characters, the value is not reported on the console. Trim these characters from the script's output.

This chapter includes the following topics:

Create Custom Attributes

Create a custom attribute and values to push to devices. These attributes and values control how product rules work. Custom Attributes also function as lookup values for certain devices.

Procedure

1 Navigate to **Devices > Provisioning > Custom Attributes > List View**.

2 Select **Add** and then select **Add Attribute**.

3 Under the **Settings** tab, enter an **Attribute Name**.

4 Enter the optional **Description** of what the attribute identifies.

5 Enter the name of the **Application** that gathers the attribute.

6 Select **Collect Value for Rule Generator** to make the values of the attribute available in the drop-down menu of the rule generator.

7 Select **Use in Rule Generator** if you want to use the attribute in the rule generator.

8 Select **Persist** to prevent the removal of the custom attribute from the Workspace ONE UEM console unless an Admin or an API call explicitly removes it.

Otherwise, the attribute is removed as normal. If you delete a custom attribute reported from a device to the UEM console, a persisted custom attribute remains in the UEM console. Custom attribute persistence is only available to Android and Windows Rugged devices.

9 Select **Use as Lookup Value** to use the custom attribute as a lookup value anywhere in the UEM console.

You can use custom attributes as part of a device friendly name to simplify device naming.

10 Select the **Values** tab.

11 Select **Add Value** to add values to the custom attribute and then select **Save**.

Custom Attributes Importing

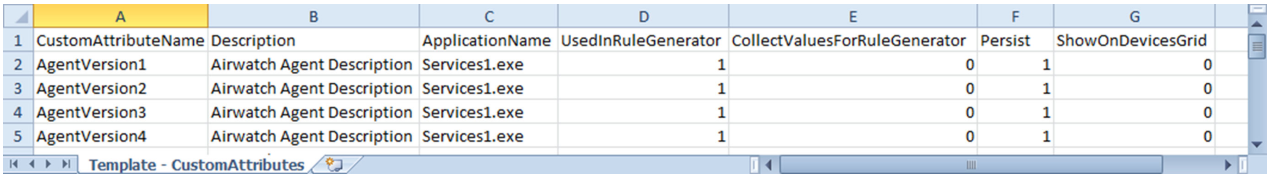
The custom attribute batch import feature allows you to load custom attributes and corresponding values into the system in bulk. In the templates provided, each column corresponds to one custom attribute and each row corresponds to their different parameters.

With the templates, you can import custom attributes in different ways and with different information.

Caution The syntax of the first column of each template must be replicated exactly. Failure to use the proper syntax can cause database issues and result in loss of data.

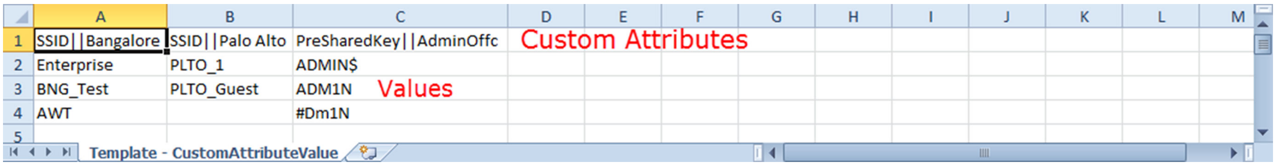
Template Types

- Custom Attributes Template – Allows you to define a custom attribute and its settings.



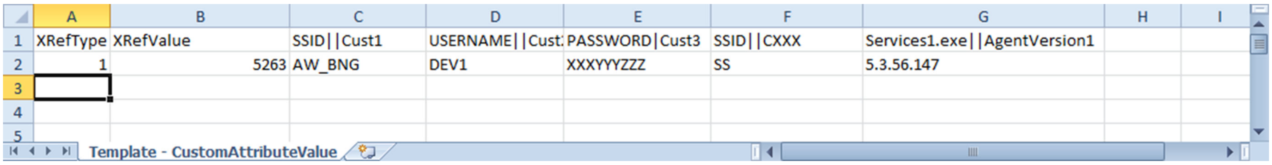
	A	B	C	D	E	F	G
1	CustomAttributeName	Description	ApplicationName	UsedInRuleGenerator	CollectValuesForRuleGenerator	Persist	ShowOnDevicesGrid
2	AgentVersion1	Airwatch Agent Description	Services1.exe	1	0	1	0
3	AgentVersion2	Airwatch Agent Description	Services1.exe	1	0	1	0
4	AgentVersion3	Airwatch Agent Description	Services1.exe	1	0	1	0
5	AgentVersion4	Airwatch Agent Description	Services1.exe	1	0	1	0

- Custom Attribute Values Template – Allows you to define the values of predefined custom attributes.



	A	B	C
1	SSID||Bangalore	SSID||Palo Alto	PreSharedKey||AdminOffc
2	Enterprise	PLTO_1	ADMIN$
3	BNG_Test	PLTO_Guest	ADM1N
4	AWT		#Dm1N
5			

- Device Custom Attribute Values – Allows you to define the values of predefined custom attributes for individual devices based on the cross reference (Xref) value. The Xref values determine the individual devices receiving the value for each custom attribute.



<table>
<tr><th></th><th>A</th><th>B</th><th>C</th><th>D</th><th>E</th><th>F</th><th>G</th><th>H</th><th>I</th></tr>
<tr><td>1</td><td>XRefType</td><td>XRefValue</td><td>SSID||Cust1</td><td>USERNAME||Cust</td><td>PASSWORD|Cust3</td><td>SSID||CXXX</td><td>Services1.exe||AgentVersion1</td><td></td><td></td></tr>
<tr><td>2</td><td>1</td><td>5263</td><td>AW_BNG</td><td>DEV1</td><td>XXXYYYZZZ</td><td>SS</td><td>5.3.56.147</td><td></td><td></td></tr>
<tr><td>3</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>4</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>5</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

a DeviceID (Workspace ONE UEM assigned DeviceID when the device enrolls)

b Serial Number

c UDID

d MAC Address

e IMEI Number

Save the file as a .csv before you import it.

Assign Organization Groups Using Custom Attributes

Configure rules that control how devices are assigned to organization groups following enrollment. You can only create one custom attribute assignment rule for each organization group you run.

Procedure

1. Ensure that you are currently in a customer type organization group.
2. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Advanced**.
3. Set **Device Assignment Rules** to **Enabled**.
4. Set the **Type** to **Organization Group by Custom Attribute**.
5. Select **Save**.
6. Navigate to **Devices > Provisioning > Custom Attributes > List View > Add > Add Attribute** and create a custom attribute if you have not already done so.

   See Create Custom Attributes for more information.
7. Navigate to **Devices > Provisioning > Custom Attributes > Custom Attributes Assignment Rules > Add Rule**.
8. Select the **Organization Group** to which the rule assigns devices.

9 Select **Add Rule** to configure the logic of the rule.

Setting	Description
Attribute/ Application	This custom attribute determines device assignment.
Operator	This operator compares the **Attribute** to the **Value** to determine if the device qualifies for the product. When using more than one Operator in a rule, you must include a **Logical Operator** between each **Operator**. **Note** There is a limitation on the less than (<) and greater than (>) operators. This limitation includes "less than or equal to" and "greater than or equal to" variants. These operators are mathematical in nature, which means they are effective at comparing numbers including integers. They cannot be used to compare non-numeric text strings. And while it is common for software versions to be represented with numbers indicating a graded versioning system (for example, 6.14.2), such representations are not numbers because they have more than one decimal point. These representations are actually text strings. Therefore, any assignment rule that compares software version numbers with multiple decimal points using greater than or less than operators (and their variants) can result in an error message.
Value	All values from all applicable devices are listed here for the **Attribute** selected for the rule.
Add Logical Operator	Select to display a drop-down menu of logical operators such as AND, OR, NOT, and parentheses. Allows for more complex rules.

10 Select **Save** after configuring the logic of the rule.

Results

When a device enrolls with an assigned attribute, the rule assigns the device to the configured organization group.