VMware AirWatch Mobile Device Management Guide
Managing your organization's mobile devices
# Table of Contents

**Chapter 1: Introduction to Mobile Device Management** ................................................. 6

Benefits of Mobile Device Management ................................................................. 6
Supported Browsers .............................................................................................. 7
Supported Platforms ........................................................................................... 7

**Chapter 2: Workspace ONE UEM Console** ............................................................ 8

Getting Started Wizard ....................................................................................... 8
Manage Account Settings ................................................................................... 10
Header Menu ......................................................................................................... 12
Main Menu ........................................................................................................... 13
Collapse and Expand the Submenu .................................................................. 14
Global Search ........................................................................................................ 14
UEM Console Notifications .................................................................................. 14
UEM Console Hub ............................................................................................... 17

**Chapter 3: Environment Setup** ........................................................................... 23

Log In to the UEM Console .................................................................................. 23
APNs Certificates ................................................................................................. 23
Privacy and Data Collection ............................................................................... 24
Terms of Use .......................................................................................................... 29
Console Branding ................................................................................................. 32
Restricted UEM Console Actions ...................................................................... 32
Other Enterprise Systems for Integration ......................................................... 35

**Chapter 4: User and Admin Accounts** ................................................................. 36

User Authentication Types .................................................................................. 36
Basic User Accounts ........................................................................................... 42
Directory-Based User Accounts ......................................................................... 45
User Accounts List View ...................................................................................... 48
Batch Import Feature .......................................................................................... 50
Admin Accounts .................................................................................................. 53
Chapter 5: Role-Based Access ................................................................. 56
  Default and Custom Roles .................................................................. 56
  User Roles ....................................................................................... 58
  Admin Roles ..................................................................................... 60

Chapter 6: Assignment Groups ............................................................. 67
  Create Custom Assignment Group List .............................................. 67
  Assign One or More Assignment Groups ......................................... 68
  Organization Groups ......................................................................... 69
  Smart Groups .................................................................................. 75
  User Groups ..................................................................................... 80
  Admin Groups .................................................................................. 87
  View Assignments ............................................................................ 90

Chapter 7: Device Enrollment ............................................................... 92
  Enroll a Device with AirWatch Agent ............................................... 92
  Additional Enrollment Workflows ................................................... 93
  Workspace ONE Direct Enrollment ............................................... 94
  Basic vs. Directory Services Enrollment ......................................... 97
  Bring Your Own Device (BYOD) Enrollment ................................. 99
  Self-Enrollment Versus Device Staging .......................................... 102
  Device Registration .......................................................................... 107
  Configure Enrollment Options ....................................................... 115
  Blacklisting and Whitelisting Device Registration ......................... 122
  Additional Enrollment Restrictions ............................................... 123
  Autodiscovery Enrollment ............................................................. 127

Chapter 8: Shared Devices .................................................................... 129
  Define the Shared Device Hierarchy ................................................. 130
  Log In and Log Out of Shared Android Devices .......................... 131
  Check-In a Shared Device From the UEM Console ....................... 131
  Enabling Directory Service-Based Enrollment .............................. 132

Chapter 9: Device Assignments ............................................................ 133
<table>
<thead>
<tr>
<th>Chapter 10: Device Profiles</th>
<th>137</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add General Profile Settings</td>
<td>137</td>
</tr>
<tr>
<td>Device Profiles List View</td>
<td>139</td>
</tr>
<tr>
<td>Device Profile Editing</td>
<td>142</td>
</tr>
<tr>
<td>Compliance Profiles</td>
<td>143</td>
</tr>
<tr>
<td>Geofence Areas</td>
<td>144</td>
</tr>
<tr>
<td>Time Schedules</td>
<td>146</td>
</tr>
<tr>
<td>View Device Assignment</td>
<td>148</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 11: Resources</th>
<th>149</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources List View</td>
<td>149</td>
</tr>
<tr>
<td>Add an Exchange Resource</td>
<td>150</td>
</tr>
<tr>
<td>Add a Wi-Fi Resource</td>
<td>155</td>
</tr>
<tr>
<td>Add a VPN Resource</td>
<td>158</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 12: Compliance Policies</th>
<th>166</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance Policies List View</td>
<td>167</td>
</tr>
<tr>
<td>Compliance Policy Rules by Platform</td>
<td>169</td>
</tr>
<tr>
<td>Add a Compliance Policy</td>
<td>173</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 13: Device Tags</th>
<th>177</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Devices by Tag</td>
<td>177</td>
</tr>
<tr>
<td>Create a New Tag</td>
<td>177</td>
</tr>
<tr>
<td>Add Tags</td>
<td>178</td>
</tr>
<tr>
<td>Manage Tags</td>
<td>179</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 14: Managing Devices</th>
<th>180</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Dashboard</td>
<td>180</td>
</tr>
<tr>
<td>Device List View</td>
<td>182</td>
</tr>
<tr>
<td>Device Details</td>
<td>189</td>
</tr>
<tr>
<td>Device Actions by Platform</td>
<td>192</td>
</tr>
</tbody>
</table>
Enrollment Status ........................................................................................................... 197
Wipe Protection .............................................................................................................. 199
Lookup Values ............................................................................................................... 201

Chapter 15: Certificate Management ............................................................................. 203
Digital Certificates List View ....................................................................................... 203
Certificate Integration Resources .................................................................................. 203

Chapter 16: Custom Attributes ...................................................................................... 205
Custom Attributes Database ......................................................................................... 205
Create Custom Attributes ............................................................................................. 205
Importing Custom Attributes ......................................................................................... 205
Platform-Specific Custom Attributes Provisioning ......................................................... 206
Create Custom Attributes ............................................................................................. 206
Custom Attributes Importing ......................................................................................... 206
Assign Organization Groups Using Custom Attributes .................................................. 207

Chapter 17: Self-Service Portal ....................................................................................... 209
Access the Self Service Portal on Devices ...................................................................... 209
Self Service Portal (SSP) Customizations ..................................................................... 209
Product Improvement Program Setting ......................................................................... 209
Token-Based Security Measures ..................................................................................... 209
Configure the Default Login Page for the SSP ............................................................... 210
My Devices Page of the SSP .......................................................................................... 210
Remote Actions in the SSP ............................................................................................. 212
Self-Service Portal Actions Matrix ................................................................................. 214
VMware Content Locker Options .................................................................................... 214
Chapter 1: Introduction to Mobile Device Management

Mobile devices are valuable enterprise tools. They allow employees to have immediate access to your internal content and resources. However, the diversity of mobile platforms, operating systems, and versions can make managing a set of devices difficult. Workspace ONE™ Unified Endpoint Manager Mobile Device Management (MDM) solves this problem by enabling you to configure, secure, monitor, and manage all types of mobile devices in the enterprise.

Benefits of Mobile Device Management

Mobile device management provides an elegant solution to security concerns and accessibility inherent to enterprise mobility.

- Manage large-scale deployments of mobile devices from a single console.
- Enroll devices in your enterprise environment quickly and easily.
- Configure and update device settings over the air.
- Enforce security and compliance policies.
- Secure mobile access to corporate resources.
- Remotely lock and wipe managed devices.

You can tailor your MDM environment to gain immediate access to device locations, current users, and content. You can also automate your MDM deployment to enforce security and compliance settings with rules and warnings that are unique to each user or organization group. Finally, you can restrict or enable content and features based on the geographic location of a device.

This guide outlines how to create, configure, and maintain your MDM deployment.
Supported Browsers

The Workspace ONE Unified Endpoint Management (UEM) console supports the latest stable builds of the following web browsers.

- Chrome
- Firefox
- Safari
- Internet Explorer 11
- Microsoft Edge

**Note:** If using IE to access the UEM console, navigate to Control Panel > Settings > Internet Options > Security and ensure you have a security level or custom security level that includes the Font Download option being set to Enabled.

If you are using a browser older than those listed above, upgrade your browser to guarantee the performance of the UEM console. Comprehensive platform testing has been performed to ensure functionality using these web browsers. The UEM console may experience minor issues if you choose to run it in a non-certified browser.

Supported Platforms

Workspace ONE UEM supports the following devices and operating systems.

- Android 4.0+
- Apple iOS 7.0+
- Apple macOS 10.9+
- Chrome OS (latest)
- QNX 6.5+
- Tizen 2.3+
- Windows Desktop (8/8.1/RT/10)
- Windows 7 (Windows 7 or later)
- Windows Phone (Windows Phone 8/ 8.1, Windows 10 Mobile)
- Windows Rugged (Mobile 5/6 and Windows CE 4/5/6)

Limited support might be available for other devices or operating systems. Workspace ONE Direct Enrollment is supported on iOS and Android devices only. For more information, see *Workspace ONE Direct Enrollment on page 94*.

Refer to each platform-specific guide by searching the online help, visiting docs.vmware.com, or contacting VMware Support for more information.
Chapter 2:
Workspace ONE UEM Console

The Workspace ONE™ Unified Endpoint Management (UEM) console allows you to view and manage every aspect of your Mobile Device Management (MDM) deployment. With this single, web-based resource, you can quickly and easily add new devices and users to your fleet, manage profiles, and configure system settings.

Acquaint yourself with security settings and interface features such as the Getting Started Wizard, menu icons, and global search.

Getting Started Wizard

The Getting Started Wizard serves as a checklist that walks you through the Workspace ONE™ Unified Endpoint Management (UEM) console settings step by step. It presents only those modules within your specific deployment which produces an on-boarding experience tailored to your configuration.

Navigate the Getting Started Wizard

The Getting Started Wizard main menu operates in a way that is most convenient to you. It not only tracks how far along you are in the configuration process, it can be started, paused, restarted later, and rewound to review and even change prior responses.

- Select Start Wizard to initiate the first step in a submodule. Here, you answer questions and access the exact pages within the UEM console to configure settings for each feature. As you complete each submodule, the percentage counter in the upper-right corner progresses and displays how far along you are in completing the submodule.

- If you stop a submodule before completing it, select Continue to return to where you left off.

- You can opt out of any submodule by selecting Skip Section, which temporarily disables the Continue button and inserts a Resume Section link. Enable the Continue button once more by selecting this link.

The Getting Started page is split into four submodules: Workspace ONE, Device, Content, and Application. Each submodule has its own set of steps. Steps that are shared among all submodules are tracked automatically so you never have to complete the same step twice.

- **Workspace ONE** – Representing unimpeded access from any employee or corporate owned device. Secure connectivity to enterprise productivity apps such as email, calendar, contacts, documents, and more. Instant, Single Sign-On (SSO) access to mobile, cloud, and Windows applications. Powerful data security that protects the enterprise...
and employees against compromised devices.

For more information about Workspace ONE, see the VMware Workspace ONE Quick Configuration Guide, available on docs.vmware.com.

- **Device** – Perform actions on MDM enrolled devices such as lock, notify, or enterprise wipe. Deploy profiles to configure email, restrictions, settings, and more. Configure compliance rules to ensure that security policies are being met in your device fleet. View how best to manage your devices from the Dashboard and Hub.

- **Content** – Deploy content & access it on the go within the Content Locker application. View & Manage your content with Content Dashboards, Reports, and Logs. Use Personal Content to share and collaborate with others. Integrate with existing repositories and deploy your content to mobile devices.

- **Application** – Deploy internally developed or publicly available free or purchased applications. Deploy a custom App Catalog to allow users to search and download applications. Integrate with compliance or app control profiles by making whitelist and blacklist of applications. Configure advanced application management options like app scanning.

**Navigate the Workspace ONE, Device, Content, and Application Wizards**

Each of the four submodules displays a list of sections representing features that you can configure or ignore, according to the needs of your organization. Features not configured display an empty *Incomplete* check box while configured features display a green *Complete* check mark.

- Select the **Configure** button to begin defining settings for the feature you are interested in.

- Review or change settings of a complete feature by selecting the **Edit** button.

- The percentage completed progress bar progresses as you complete each feature.

- Most features have a **Video** button next to the **Configure** or **Edit** button. This video lets you see the feature in action and aid your understanding of how it may be useful to your organization.

- Some features in the submodule can be skipped without penalty toward the percentage completed progress bar. Where available, select the **Skip This Step** button to remove the feature from your list. To display the feature once again, select the **Reactivate** button.

Some features and functions have prerequisites. For example, Mobile Single Sign-On requires that you have already configured Enterprise Connector, Active Directory, and VMware Identity Manager. Where possible, you are provided with a button to initiate the configuration of these required features.

**Enable the Getting Started Wizard Manually**

For a new Workspace ONE UEM implementation, access the Getting Started page from the main menu, located above the **Hub** icon in the left panel. However, you can manually enable the Getting Started Wizard at any time. Manually enabling the Getting Started Wizard restarts the walk-through.

1. Select any **Organization Group** other than the top-level group.

2. Navigate to **Groups & Settings > Groups > Organization Groups > Organization Group Details**. Ensure that you are currently at a customer-level organization group and **Save** your changes.

3. Navigate to **Groups & Settings > All Settings > System > Getting Started**.
4. Select **Enable** for each of the settings on this page:
   a. **Getting Started Workspace ONE Status**
   b. **Getting Started Device Status**
   c. **Getting Started Content Status**
   d. **Getting Started Application Status**

5. **Save** changes to the page.

For more information, see Organization Groups on page 69.

**Manage Account Settings**

You can manage your account settings including personal user information, notification preferences, login history, and security configuration.

**User**

Ensure you can be reached by entering your personal information in the **User** tab including email, up to four different phone numbers, time zone, and locale.

**Notifications**

Use the Notifications settings on the **Account Settings** page to enable or disable APNs Expiration alerts, choose how to receive alerts, and change the email to which it sends alerts. For more information, see Configure Notifications Settings on page 16.

**Logins**

Review your entire login history including login date and time, the source IP address, login type, source applications, browser make and version, OS platform, and login status.

**Security**

You can reset your login password, reset the password recovery questions, and reset your four-digit security PIN.

**Password**

The **Password** accompanies your account username when you log into the UEM console. You can **Reset** this password at any time.

**Password Recovery Questions**

The **Password Recovery Questions** are the method by which you reset your password. You must define this question together with its answer when you log in to the UEM console for the first time. You can select a new password recovery question by selecting the **Reset** button. This action logs out the user automatically. Upon logging back in, they are presented with the **Security Settings** screen where they are required to select from the list of Password Recovery Questions and supply the answer.
Admins who never selected a password recovery question and do not have a **Reset** button for Password Recovery Questions must have their accounts deleted and re-created. Upon logging in for the first time after their account is re-created, they are required to define a password recovery question and answer.

**Security PIN**

Establish security for the UEM console by creating a **Security PIN**. The PIN acts as a safeguard against accidentally wiping a device or deleting important aspects of your environment, such as users and organization groups. The Security PIN also works as a second layer of security. It presents an added point of authentication by blocking actions made by unapproved users.

When you first log in to the UEM console, you are required to establish a Security PIN.

**Reset** your security PIN every so often to minimize security risks.
Header Menu

The **Header Menu** appears at the top of nearly every page of the Workspace ONE™ Unified Endpoint Management (UEM) console, enabling you to access to the following functions and features.

- **Organization Group** – Select the Organization Group (the tab labeled Global) to which you want to apply changes.
- **Add** – Quickly create an admin, device, user, policy, content, profile, internal application, or public application.
- **Global Search** – (🔍) Search all aspects of your deployment within the UEM console, including devices, users, content, applications, configuration settings, admins, pages, and more.
- **Notifications** – (🔔) Stay informed about important console events with Notifications. The number badge on the Notifications bell icon indicates the number of alerts that require your attention.
- **Saved** – (⭐) Access your favorite and most-utilized pages within the UEM console.
- **Help** – (📚) Browse or search the available guides and UEM console documentation.
- **Account** – View your account information. Change the **Account Role** that you are assigned to within the current environment. Customize settings for contact information, language, **Notifications**, view history of **Logins**, and **Security** settings including PIN reset. You can also Log out of the UEM console and return to the Login screen.
- **Refresh** – (🔄) See updated stats and info without leaving the current view by refreshing the screen.
- **Available Sections** – (☯️) Customize the view of the Hub Overview by selecting only the sections you want to see. Available only on the Hub Overview.
- **Export** – (/csv) Produces a full (or filtered, if filtering is used) listing of users, devices, profiles, apps, books, or policies to a comma-separated values (CSV) file that you can view and analyze with Excel.
- **Home** – (🏠) Use this icon to assign any screen in the UEM console as your home page. The next time you open the UEM console, your selected screen displays as your home page.
- **Save** – (⭐️) Add the current page to the Saved page list for quick access to your favorite UEM console pages.

For more information, see the following topics.

- Organization Groups on page 69.
- Manage Account Settings on page 10.
- Role-Based Access on page 56.
- UEM Console Notifications on page 14.
- Workspace ONE UEM Console on page 8.
- UEM Console Hub on page 17.
Main Menu

The Main Menu allows you to navigate to all the features available to your role and Mobile Device Management (MDM) deployment.

**Getting Started**
Ensure that all aspects of a basic successful deployment are established. Getting Started is organized to reflect only those modules within a Workspace ONE™ Unified Endpoint Management (UEM) console deployment that you are interested in. Getting Started produces an on-boarding experience that is more tailored to your actual configuration.

**Hub**
View and manage MDM information that drives decisions you must make and access a quick overview of your device fleet. View information such as the most blacklisted apps that violate compliance. Track module licenses with the Admin Panel Dashboard and monitor all devices that are currently out of compliance. Select and run Industry Templates to streamline the onboarding process with industry-specific apps and policies for your iOS devices.

**Devices**
Access an overview of common aspects of devices in your fleet, including compliance status, ownership type breakdown, last seen, platform type, and enrollment type. Swap views according to your own preferences including full Dashboard, list view, and detail view. Access additional tabs, including all current profiles, enrollment status, Notification, Wipe Protection settings, compliance policies, certificates, product provisioning, and printer management.

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

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

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

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

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

**Groups & Settings**
Manage structures, types and statuses related to organization groups, smart groups, app groups, user groups, and Admin Groups. Configure entire system settings or access settings related to all Main Menu options.
Collapse and Expand the Submenu

You can collapse the submenu by selecting the arrow at the bottom of the Workspace ONE™ Unified Endpoint Management (UEM) console. This action creates more space on the screen for device information.

To expand or reopen the submenu, select the modified arrow.

Global Search

Using a modular design with a tabbed interface, Global Search runs searches across your entire deployment. Global Search applies your search string to a single tab at a time, which produces faster results. Apply the same string to another area of the Workspace ONE™ UEM console by selecting another tab.

After running a global search, select the following tabs to view the results.

- **Devices** – Returns matches to Device friendly name and Device Profile name searches.
- **Accounts** – Returns matches to user name and administrator name searches.
- **Applications** – Returns matches to internal, public, purchased, and Web application searches.
- **Content** – Returns matches to any content that appears on devices.
- **Settings** – Returns matches to individual field-level settings and console main page searches.

You can also perform a search for an organization group by selecting the organization group drop-down menu. The Search bar displays above the list.

UEM Console Notifications

Notifications are a communication tool designed to keep you informed about Workspace ONE™ Unified Endpoint Management (UEM) console events that may impact your operation. The Notifications button is located next to the Global Search button.
There are many different kinds of notifications.

- **MDM APNs Expiring** – You are notified 30 days before APNs for MDM certificates expire, which is a Critical Priority alert. After the APNs certificate expires, the Critical Priority alert is reduced to a High Priority alert. This notification helps you avoid the hassles involved with expired certificates and keeps your devices in contact with Workspace ONE UEM.

- **Application APNs Certificate Expiration** – You are notified 30 days before APNs for Applications expire, which is a Critical Priority alert. This notification helps you avoid the hassles involved with expired certificates and keeps the apps functional on your devices.

- **App Removal Protection** – This High Priority alert displays when the Application Removal threshold is crossed. You can act by selecting the Review App Removal link on the Notifications pop-up.

- **Device App Log Storage Alert** – This notification is a High Priority alert which displays when your storage log exceeds 75% of its capacity. Contact your support representative to purge your logs or increase the limit. This alert can be dismissed.

- **List View Export** – This notification appears when the Device or User list view export you requested has been completed and is ready for examination. This notification is an Info Priority level and can be dismissed.

- **Peer-to-Peer Server Update Required** – You are notified when a new version of the peer-to-peer server becomes available and that you can upgrade your server to avoid service disruptions.

- **Provisioning Profile Expiration** – You are notified when a provisioning profile containing applications expires, requiring you to regenerate the provisioning profile and update it. This notification is a Critical priority level and cannot be dismissed.

- **User Group Merge Pending** – This notification lets you know that the user group merge process is pending and in need of admin approval. Such notification happens in two scenarios:
  - You have the Auto Merge Changes setting disabled on your Directory-based User Group, which means all changes need approval.
  - You have the Auto Merge Changes enabled and the number of changes exceed the Maximum Allowable Changes threshold. The portion of changes above the threshold need admin approval.

- **VPP App Auto Update** – High priority alerts that notify you when an app installed with Apple Volume Purchase Program has an updated version you can install.

For information about Device Lifecycle Notifications, see Configure Lifecycle Notifications on page 120.

**Manage UEM Console Notifications**

When there are active notifications that require your attention, a numeral badge appears on the alert icon indicating the number of active alerts. Display the **Notifications** pop-up by selecting the bell-shaped Notifications icon.

You can manage the notifications you receive. This management includes viewing the list of active alerts, Renewing your APNs, Dismissing expired alerts, viewing the list of dismissed alerts, and Configuring Notification Settings.
Each alert displays the organization group under which the APNs for an MDM certificate is located. The alert also shows the expiration date of the certificate and a link to Renew your APNs.

- **View Active Alerts** – The default view displays the list of active alerts.

- **Renew your APNs** – Displays the Change Organization Group (OG) screen. This screen appears when the OG that manages the device with the impending license expiration is different than the OG you are currently in. Renew this APNs license by selecting Yes to change your OG automatically.

Renew the license and keep the device in contact with Workspace ONE™ UEM by following the instructions on the APNs For MDM settings page.

- **Dismiss Alert** – Close the expired alert and send it to the Dismissed alert listing by selecting the X button. You cannot close critical priority notifications.

- **View Dismissed Alerts** – View the listing of dismissed alerts by selecting the Dismissed tab at the top of the Notifications pop-up.

### Configure Notifications Settings

Use the Notifications settings on the **Account Settings** page to enable or disable APNs Expiration alerts, choose how to receive alerts, and change the email to which it sends alerts.

To configure notification settings, take the following steps.

1. Select the **Account** button, which is accessible from almost every page on the Workspace ONE™ Unified Endpoint Management (UEM) console, then select **Manage Account Settings** and select the **Notifications** tab.

   You can also access the notification settings page by selecting the gear icon located in the lower-right corner of the Notifications pop up screen.

2. Select how you want to be notified when each of the following events occurs.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDM APNs Expiring</td>
<td>This notification helps you avoid the hassles involved with expired certificates and keeps your devices in contact with Workspace ONE UEM.</td>
</tr>
<tr>
<td>List View Export</td>
<td>You can trigger an alert when the exportation of a User List View or Device List View is complete.</td>
</tr>
<tr>
<td>User Group Merge</td>
<td>You can trigger an alert when the Active Directory database changes sync with Workspace ONE UEM and you have Auto Merge Changes disabled.</td>
</tr>
<tr>
<td>VPP App Auto Update</td>
<td>You can trigger an alert when an app installed with Apple Volume Purchase Program has an updated version you can install.</td>
</tr>
<tr>
<td>Application APNs Certificate Expiration</td>
<td>This notification helps you avoid the hassles involved with expired certificates and keeps the apps functional on your devices.</td>
</tr>
<tr>
<td>Provisioning Profile Expiration</td>
<td>You are notified when a provisioning profile containing applications expires, requiring you to regenerate the provisioning profile and update it.</td>
</tr>
</tbody>
</table>
3. For each event, select between None, Console, Email, and Console and Email. Selections of Email and Console and Email require you entering at least one email address in the Send email(s) to: field. You can enter multiple email addresses separated by commas.

4. Save or Cancel your changes.

**UEM Console Hub**

The Workspace ONE™ United Endpoint Manager Hub is your central portal for fast access to critical information. You can quickly identify important issues and act from a single location in the UEM console.

Selecting any bar or donut graph on the page displays the **Device List View**. This list view contains all the devices specific to the metric you selected. You can then perform actions such as sending a message to those devices.

For example, select the Antivirus Status donut graph. Within seconds, the **Device List View** displays with a list of devices whose lack of antivirus software has triggered a policy violation. Select all the devices in this list by clicking the check box to the far left of each device. You can also select the "select all" check box below the **Add Device** button. The action button cluster displays above the listing. Select the **Send** button to send a message to the users of the selected devices. You can select an Email, a push notification, or an SMS text message.

The Hub provides summary graphs and detailed views.

- **Devices** – View the exact number of devices.
  - Status breakdown of all devices including registered, enrolled, enterprise wipe pending, device wipe pending and unenrolled.
  - Platform breakdown of devices enrolled in Workspace ONE UEM.
  - Enrollment history over the past day, past week, and past month.
• **Compliance** – View which devices are violating compliance policies.
  - All compliance policies currently violated by devices, including apps, security settings, geolocation, and more.
  - Top violated policies, covering all types of compliance policies established.
  - Blacklisted Apps, including all blacklisted apps installed on devices, ranked by order of instances of violation.
  - Devices lacking the apps that you want to be installed and ready for your users.

• **Profiles** – View which profiles are out of date.
  - Latest Profile Version, including devices with old versions of each profile.

• **Apps** – View which applications are associated with devices.
  - Latest Application Version, including devices with old versions of each application.
  - Most Installed Apps, ranked by devices that have the application currently installed.

• **Content** – View devices with content that is out of date.
  - Latest Content Version, including each file that is out of date ranked by order of instance.

• **Email** – View devices that are currently unable to receive email.
  - Devices Blocked from email, including devices blocked by default, blacklisted or unenrolled.

• **Certificates** – View which certificates are set to expire.
  - Certificates expiring within one month, one to three months, three to six months, six to 12 months and greater than 12 months. Also, view certificates that have already expired.

The set of devices shown varies depending on your current organization group, including all devices in child organization groups. Switch to lower organization groups and automatically update device results by using the organization group drop-down menu.

Toggle between views by selecting the **List View** icon (.rectangle) and **Chart View** icon (.circle). Select any metric to open the Device List View for that specific set of devices. You can then perform actions such as sending a message to those devices. Customize the Hub by selecting the **Available Sections** icon (ellipse). Select or deselect check boxes representing available sections (Devices, Compliance, Profiles, and so on) and select **Save** to craft the Hub’s overview.

You can export Hub data in PDF format by selecting the **Export** icon (paperclip). Exporting to PDF is useful for providing daily, weekly, or monthly reports of the current state of your mobile device deployment.

**Intelligence**

Intelligence custom reporting and analytics can provide you with deeper insights about your device fleet. Such insights include enhanced visibility on performance issues, highly effective planning tools, and faster deployment times.

Ensure you are in a customer type organization group, then navigate to **Hub** > **Intelligence**, select the **Next** button to see how Intelligence works, and opt-in to take advantage of the service.

You may opt-out of Intelligence custom reporting at any time.

For more information, see the VMware Workspace ONE™ **UEM Reports & Analytics Guide**, on docs.vmware.com.
Admin Panel Dashboard

The Admin Panel provides an overview of module license information and deployed Workspace ONE™ UEM components. The Admin Panel contains a summary of licenses condensed into two separate sections, Active Products and Deployed Components.

Access the Admin Panel by navigating to Hub > Admin Panel. The Admin Panel can only be accessed from a Customer organization group. For more information, see Organization Group Type Functions on page 73.

Active Products in the Admin Panel

The Active Products section confirms the license validity of features included in your deployment such as Browser, Container, Mobile Device Management, App Catalog, and more. For each feature you can see the total number of licenses, the license model, and the license type.

Deployed Components in the Admin Panel

The Deployed Components section features a panel for every enabled component at the customer organization group, each reporting the connectivity status.

- VMware Enterprise Systems Connector
- Secure Email Gateway
- VMware Tunnel

You can select the refresh button (⟳) to refresh the connectivity status of the individual enabled component.

You can also select the settings button (🔧) to display the systems setting page that corresponds to the enabled component.

Industry Templates for iOS

An Industry Template is a collection of mobile applications and device profiles that you can push to your devices, greatly expediting the deployment process. You can select templates in support of industries such as healthcare and retail and you can edit these templates to fit your needs.

App and Profile Monitor

The App and Profile Monitor provides a quick method for tracking the recent deployment of apps and profiles to your devices. The monitor displays historical data on the deployment process and the install status of the app or profile on devices.

The App and Profile Monitor tracks the status of app and profile deployments to your end-user devices. The monitor only tracks apps and profiles deployed in the past 15 days. This data allows you to see the status of your deployments and diagnose any issues.

When you search for an app or profile, a card containing the deployment data is added to the App and Profile Monitor view. You can only display five cards at a time. These cards remain added until you log out. Any cards must be added again when you log in again.
The Historical section only shows the past seven days of data. It shows the number of devices reporting the Done status for deployment. The Current Deployment section shows the device deployment status. For more information on the deployment statuses, see App and Profile Monitor Statuses on page 20. If you see an Incomplete status, select the number next to the status to see a Device List View of all devices reporting the status. This feature lets you examine devices with issues so you can troubleshoot your deployment.

The App and Profile Monitor only tracks deployments started after upgrading to Workspace ONE™ UEM v9.2.1+. If you deployed the app or profile before upgrading, the monitor does not track any data on the deployment.

### App and Profile Monitor Statuses

The App and Profile Monitor displays the current deployment status for devices during a deployment. The status combines different app and profile installation statuses into Done, Pending, or Incomplete.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Done</td>
<td>Devices report the Done status when the app or profile installs successfully.</td>
</tr>
<tr>
<td>Status</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Pending</td>
<td>Devices report the Pending Status when an app or profile reports the following statuses.</td>
</tr>
</tbody>
</table>

**Profiles**
- Pending Install.
- Pending Removal.
- Unconfirmed Removal.
- Confirmed Removal.

**Apps**
- Needs Redemption.
- Redeeming.
- Prompting.
- Installing.
- MDM Removal.
- MDM Removed.
- Unknown.
- Install Command Ready for Device.
- Awaiting Install on Device.
- Prompting for Login.
- Updating.
- Pending Release.
- Prompting for Management.
- Install Command Dispatched.
- Download in Progress.
- CommandAcknowledged.
<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incomplete</td>
<td>Device reports the Incomplete Status when an app or profile reports the following statuses.</td>
</tr>
<tr>
<td>Profiles</td>
<td>○ Pending Information.</td>
</tr>
</tbody>
</table>

If you see an Incomplete status, select the number next to the status to see a Device List View of all devices reporting the status. This feature lets you examine devices with issues so you can troubleshoot your deployment.

Track a Deployment with the App and Profile Monitor

Track a deployment of an application or profile to end-user devices with the App and Profile Monitor. This monitor provides at-a-glance information on the status of your deployments.

To track a deployment:

1. Navigate to Hub > App and Profile Monitor.
2. In the search field, enter the name of the app or profile. You must select the Enter key on your keyboard to start the search.
3. Select the app or profile from the drop-down menu and select Add.

The app or profile data displays on a card. You can only have five cards added at one time.

Reports and Analytics

Workspace ONE™ UEM has extensive reporting and event logging capabilities that provide administrators with actionable, result-driven statistics about device fleets.

You can use these pre-defined reports or create custom reports based on specific devices, user groups, date ranges, or file preferences. Reports can be viewed by navigating to the Reports page at Hub > Reports & Analytics > Reports > List View. Added reports are accessible from the My Reports tab at the top of the Reports page for quick access.
Chapter 3: Environment Setup

You can determine the environment URL and login credentials, generate certificates for managing platforms, configure telecom, privacy settings, customize the Workspace ONE™ Unified Endpoint Management (UEM) console, and more.

Log In to the UEM Console

Before you can log in to the Workspace ONE™ Unified Endpoint Management (UEM) console, you must have the Environment URL and log in credentials. How you obtain this information depends on your type of deployment.

- **SaaS Deployment** – Your Account Manager provides your Environment URL and user name/password. The URL is not customizable, and generally follows the format of awmdm.com.

- **On-premises** – The on-premises URL is customizable and follows the format awmdm.<MyCompany>.com.

Your Account Manager provides the initial setup credentials for your environment. Administrators who create more accounts to delegate management responsibility may also create and distribute credentials for their environment. See Create an Admin Account for details.

Once your browser has successfully loaded the UEM console Environment URL, you can log in using the user name and Password provided by your Workspace ONE UEM Administrator.

APNs Certificates

To manage iOS devices, you must first obtain an Apple Push Notification Service (APNs) certificate. An APNs certificate allows Workspace ONE UEM to communicate securely to Apple devices and report information back to the UEM console. Per Apple's Enterprise Developer Program, an APNs certificate is valid for one year and then must be renewed. The UEM console sends reminders through Notifications as the expiration date nears. Your current certificate is revoked when you renew from the Apple Development Portal, which prevents device management until you upload the new one. Plan to upload your certificate immediately after it is renewed. Consider using a different certificate for each environment if you use separate production and test environments.
For more information, please see the Generating and Renewing an APNs Certificate for Workspace ONE UEM KB article: https://support.air-watch.com/articles/115001662728.

APNs Certificate Expiration

The Notifications button in the header bar of the console alerts you when your APNs for MDM certificates are close to expiring. This notice allows you to act.
For more information, see UEM Console Notifications on page 14.

Generate an APNs Certificate

You must generate and occasionally renew APNs Certificates to enable and maintain secure communications between your iOS devices and Workspace ONE™ UEM. To generate an APNs certificate, you must choose between two methods.

1. Follow the steps outlined in the Getting Started Wizard on page 8.

OR

2. Generate APNs certificates manually by taking the following steps.

   a. Navigate to Groups & Settings > All Settings > Devices & Users > Apple > APNs for MDM.

   b. If the Valid To date has passed, select the Renew button and follow the on-screen instructions. There is an instructions link that shows you how to use the Apple Push Certificates Portal to upload a certificate request. Provided on this page is a convenient Go To Apple button that opens the Apple Push Certificates Portal in a new tab of your browser. You need two items to continue.

      i. Workspace ONE UEM Certificate Request, which is a file in the PLIST format that you can save to your device.

      ii. The Apple ID that you originally used to create the certificate.

   c. Click Next to advance to the next page where you must enter your Apple ID and upload the Apple-issued Workspace ONE UEM MDM certificate (PEM file).

   d. Select Save.

Privacy and Data Collection

It is important that you inform your end users about how their data is collected and stored when they enroll into Workspace ONE™ UEM. The UEM console allows you to create a customized privacy notification to inform users about
what data your company collects from enrolled devices. Work with your legal department to determine what message about the collection of data you communicate to your end users.

**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.

**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.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the notification template.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the template you are creating.</td>
</tr>
<tr>
<td>Category</td>
<td>Select Enrollment.</td>
</tr>
<tr>
<td>Type</td>
<td>Select MDM Device Activation.</td>
</tr>
<tr>
<td>Select Language</td>
<td>Select the default language for your template. Use the Add button to add more default languages for a multi-language delivery.</td>
</tr>
<tr>
<td>Default</td>
<td>Assigns this template as the default message template.</td>
</tr>
</tbody>
</table>
4. Create the notification content. The message types that you selected in the **Message Type** selection determine which messages appear for you to configure.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email</strong></td>
<td></td>
</tr>
<tr>
<td>Email Content Formatting</td>
<td>Choose whether your email notification is delivered as <strong>Plain Text</strong> or <strong>HTML</strong>.</td>
</tr>
<tr>
<td>Subject</td>
<td>Enter the subject line for your email notification.</td>
</tr>
<tr>
<td>Message Body</td>
<td>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 <strong>Email Content Formatting</strong> selection. If you have enabled the Visual Privacy Notice, include the lookup value <code>PrivacyNotificationUrl</code> in the message body.</td>
</tr>
<tr>
<td><strong>SMS</strong></td>
<td></td>
</tr>
<tr>
<td>Message Body</td>
<td>Compose the SMS message to send to your users. If you have enabled the Visual Privacy Notice, include the lookup value <code>PrivacyNotificationUrl</code> in your message body.</td>
</tr>
<tr>
<td><strong>Push</strong></td>
<td></td>
</tr>
<tr>
<td>Message Body</td>
<td>Compose the Push notification to send to your users. If you have enabled the Visual Privacy Notice, include the lookup value <code>PrivacyNotificationUrl</code> in your message body.</td>
</tr>
</tbody>
</table>

5. Select **Save**.

**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 on page 26.

**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.

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 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.
   - 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.

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.

**Note:** If you disable the wipe function for select iOS ownership types, users do not see the "Erase all content and settings" permission during enrollment.

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.

4. 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.

   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.

   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.

5. 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.
6. Select to Enable or Disable the User-Friendly Privacy Notice on the device.
   - 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.

7. Click Save. You must enter your PIN to save the changes. Click 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 AirWatch Agent relays device GPS location data back to the UEM console.
  - Other apps that use the Workspace ONE UEM 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.

**Terms of Use**

Ensure that all users with managed devices agree to the policy by defining and enforce terms of use (TOU). If necessary, users must accept the TOU before proceeding with enrollment, installing apps, or accessing the UEM console. The UEM console allows you to customize fully and assign a unique TOU to each organization group and child organization group. The TOU displays during each device enrollment. Get access to the following functions.

- Set version numbers.
- Set platforms to receive the TOU.
- Notify users by email with the TOU updates.
- Create language-specific copies of the TOU.
• Create multiple TOU agreements and assign them to organization groups based on platform or the type of ownership.

• Meet the liability requirements of specific groups by customizing TOU.

Create Enrollment Terms of Use

You can create an agreement about terms of use (TOU) specific to enrollment purposes. You can also limit devices allowed for enrollment by device platform, ownership type, and enrollment type.

1. Ensure that your current active organization group is correct for the TOU you are creating.

2. Navigate to Devices > Device Settings > Devices & Users > General > Enrollment and select the Terms of Use tab.

3. Select the Add New Enrollment Terms of Use button and complete the following options.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the new TOU.</td>
</tr>
<tr>
<td>Type</td>
<td>This option is pre-populated as Enrollment.</td>
</tr>
<tr>
<td>Version</td>
<td>This option is automatically tracked and populated accordingly.</td>
</tr>
</tbody>
</table>
| Platforms, Device Ownership, and Enrollment Type | If you do not want to make your TOU for any specific category of device, then keep the default selection of Any for these options. If you prefer to specify a platform, ownership, and enrollment, you can select one or more of these categories and define the limitations specific to your TOU.
  • If you select Selected Platform option, then choose your desired platforms from the list that appears. Your TOU applies to the device platforms you select, excluding all others.
  • If you select Selected Ownership Types option, then you must choose your desired ownership from the list that appears. Your TOU applies to the ownership types you select, excluding all others.
  • If you select Selected Enrollment Types option, then you must choose your desired enrollment from the list that appears. Your TOU applies to the types of enrollment you select, excluding all others. |
| Notification                                    | Send an email to users whenever the TOU is updated by selecting this check box. The notification email is sent when you select Save in step 5. |
| Select Language                                | Optionally, for localization purposes, you may enter a TOU agreement for each language applicable to your needs by making a choice in the Select Language drop-down. |

4. In the text box provided, enter your customized TOU.

   The editor provides a basic text entry tool to create a TOU or paste in an existing TOU. To paste text from an external source, right-click the text box and choose Paste as plain text to prevent any HTML or formatting errors.

5. Select Save.

You can enforce MDM terms of use acceptance by creating a compliance policy for MDM Terms of Use Acceptance.
Create Application or Console Terms of Use

You can also create application-based terms of use (TOU) to notify end users when a specific application collects data or when it imposes restrictions.

When users run these applications from your enterprise app catalog, they must accept the agreement to access the application. You can set TOU for app versions, make language-specific TOU, and remove apps if the TOU is not accepted.

Console TOU display when an administrator logs in to the Workspace ONE™ UEM console for the first time. For the UEM console, you can set TOU version numbers and create language-specific copies of the TOU.

For Applications, assign the TOU when adding or editing an application using the Terms of Use tab.

1. Navigate to Groups & Settings > All Settings > System > Terms of Use.

2. Select Add Terms of Use.

3. Enter a Name for the terms of use and select the Type, which can be Console or Application.

4. Configure settings such as a Version number and a Grace Period, depending on the Type you selected.

5. Enter your TOU in the text box provided. The editor provides a basic text entry tool to create a TOU or paste in an existing TOU. If you are pasting text from an external source, right-click the text box and choose Paste as plain text to prevent any HTML or formatting errors.

6. Select Save.

View Terms of Use Acceptance

While compliance policies can be configured to help enforce terms of use acceptance, you can also see who has and who has not accepted the agreement. Then, if necessary, you can contact those individuals directly.

1. Navigate to Groups & Settings > All Settings > System > Terms of Use.

2. Use the Type drop-down menu to filter based on the agreement type, for example, Enrollment. The Users / Devices column displays devices that have accepted/not accepted/been assigned the terms of use.

3. Select the appropriate number in the Devices column for the terms of use row to see device information pertaining to that agreement. Optionally, access the drop-down menu for the row and select one of the following.
   - View Devices or Users – Display all devices and their acceptance statuses. You can filter by organization group.
   - View Previous Versions – View previous iterations of the agreement.
   - View Terms of Use – View the terms of use agreement.

Track Terms of Use Acceptance with Reports

You can track user acceptance for terms of use, enabling you to take possible action.

View details regarding specific organization groups, console acceptances, and device enrollment acceptances. View the acceptances directly in the Workspace ONE™ UEM console or export the report in CSV format which is viewable in Excel.

1. Navigate to Hub > Reports & Analytics > Reports > List View.

2. Search for and generate the Terms of Use Acceptance Detail report by selecting the report title.

3. Select the Organization Groups.
4. Select the **Terms of Use Type**.

5. Select the **Report Format**.

6. Select **Download** to save the report.

---

**Important:** VMware Workspace ONE UEM does not provide legally binding sample text and any text examples provided must be reviewed by your own company or legal team.

---

**Console Branding**

The Workspace ONE ™ Unified Endpoint Management (UEM) console allows extensive customization options. These options allow you to brand aspects of your Workspace ONE UEM tools and resources according to the color scheme, logo, and overall aesthetic of your organization.

Branding can be configured in support of multi-tenancy, so different divisions of your enterprise can have their unique look and feel at their organization group level.

For more information, see [Organization Groups on page 69](#).

**Configure Console Branding**

You can align with the color scheme, logo, and overall aesthetic of your organization by customizing the console.

1. Select the organization group you want to brand and then navigate to **Groups & Settings > All Settings > System > Branding**.

2. Configure the settings on the **Branding** tab:
   - Upload a Company Logo by uploading a file saved on your computer. The suggested resolution of the uploaded image is 800x300.
   - Upload a background for the login page by uploading a file saved on your computer. The suggested resolution of the uploaded image is 1024x768.
   - Upload a background for the Self-Service Portal login page by uploading a file saved on your computer. The suggested resolution of the uploaded image is 1024x768.

3. Configure customizations to the **Colors** section in the **Branding** tab.

4. Configure the settings on the **Custom CSS** tab.
   - Enter customized CSS code for advanced branding.

5. Select **Save**.

---

**Restricted UEM Console Actions**

Given a scenario when the Workspace ONE ™ Unified Endpoint Management (UEM) console is left unattended, an extra safeguard is provided against malicious actions that are potentially destructive. You can place those actions out of reach of unauthorized users. Navigate to **Groups & Settings > All Settings > System > Security > Restricted Actions**.
Enable Send Message to All

Enable this setting to allow a system administrator to send a message to all devices in your deployment from the Device List View. It can also be used to send a message to a specific group.

For more information, see Device List View on page 182.

Select Password Protect Actions

Restricted Console Actions provides an added layer of protection against malicious actions that are potentially destructive. Configure settings for restricted actions by navigating to Groups & Settings > All Settings > System > Security > Restricted Actions.

You can require that certain actions require admins to enter a PIN. For each action you choose to protect, select the appropriate Password Protect Actions button for Enabled or Disabled as appropriate. This requirement provides you with granular control over which actions you want to make more secure.

Note: Some actions always require a PIN and as a result cannot be disabled. Denoted by * below.

You can set the maximum number of failed attempts the system accepts before automatically logging out the session. If you reach the set number of attempts, you need to log into the Workspace ONE UEM console and set a new security PIN.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Account Delete</td>
<td>Prevents the deletion of an admin user account in Accounts &gt; Administrators &gt; List View.</td>
</tr>
<tr>
<td>*APNs Certificate Change</td>
<td>Prevents the disabling of APNs for MDM in Groups &amp; Settings &gt; All Settings &gt; Devices &amp; Users &gt; Apple &gt; APNs For MDM.</td>
</tr>
<tr>
<td>Application Delete/Deactivate/Retire</td>
<td>Prevents the deletion, deactivation, or retirement of an application in Apps &amp; Books &gt; Applications &gt; List View.</td>
</tr>
<tr>
<td>Content Delete/Deactivate</td>
<td>Prevents the deletion or deactivation of a content file in Content &gt; List View.</td>
</tr>
<tr>
<td>*Data Encryption Toggle</td>
<td>Prevents the Encryption of user information setting in Groups &amp; Settings &gt; All Settings &gt; System &gt; Security &gt; Data Security.</td>
</tr>
<tr>
<td>Device Delete</td>
<td>Prevents the deletion of a device in Devices &gt; List View. Admin security PIN is still required for bulk actions even when this setting is disabled.</td>
</tr>
<tr>
<td>*Device Wipe</td>
<td>Prevents any attempt to perform a device wipe from the Device List View or Device Details screens.</td>
</tr>
<tr>
<td>Enterprise Reset</td>
<td>Prevents any attempt to perform an enterprise reset on a device from the Devices Details page of a Windows Rugged, Rugged Android, or QNX device.</td>
</tr>
<tr>
<td>Enterprise Wipe</td>
<td>Prevents any attempt to perform an enterprise wipe on a device from the Devices Details page of a device.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Enterprise Wipe (Based on User Group Membership Toggle)</strong></td>
<td>Prevents any attempt to perform an enterprise wipe on a device when it is removed from a user group. This is an optional setting that you can configure under Groups &amp; Settings &gt; All Settings &gt; Devices &amp; Users &gt; General &gt; Enrollment on the Restrictions tab. If you Restrict Enrollment to Configured Groups on this tab, you then have the added option of performing an enterprise wipe a device when it is removed from a group. For more information, see the Configure Enrollment Restriction Settings on page 124.</td>
</tr>
<tr>
<td><em>Organization Group Delete</em></td>
<td>Prevents any attempt to delete the current organization group from Groups &amp; Settings &gt; Groups &gt; Organization Groups &gt; Organization Group Details.</td>
</tr>
<tr>
<td>Profile Delete/Deactivate</td>
<td>Prevents any attempt to delete or deactivate a profile from Devices &gt; Profiles &amp; Resources &gt; Profiles.</td>
</tr>
<tr>
<td>Provisioning Product Delete</td>
<td>Prevents any attempt to delete a provisioning product from Devices &gt; Staging &amp; Provisioning &gt; Products List View.</td>
</tr>
<tr>
<td>Revoke Certificate</td>
<td>Prevents any attempt to revoke a certificate from Devices &gt; Certificates &gt; List View.</td>
</tr>
<tr>
<td><em>Secure Channel Certificate Clear</em></td>
<td>Protects from any attempt to clear an existing secure channel certificate from Groups &amp; Settings &gt; All Settings &gt; System &gt; Advanced &gt; Secure Channel Certificate.</td>
</tr>
<tr>
<td>User Account Delete</td>
<td>Prevents any attempt to delete a user account from Accounts &gt; Users &gt; List View.</td>
</tr>
<tr>
<td>Change in Privacy Settings</td>
<td>Prevents any attempt to alter the privacy settings in Groups &amp; Settings &gt; All Settings &gt; Devices &amp; Users &gt; General &gt; Privacy.</td>
</tr>
<tr>
<td>Delete Telecom Plan</td>
<td>Prevents the deletion of a telecom plan in Telecom &gt; Plan List.</td>
</tr>
<tr>
<td>Override Job Log Level</td>
<td>Prevents attempts to override the currently-selected job log level from Groups &amp; Settings &gt; Admin &gt; Diagnostics &gt; Logging. Overriding the Job Log Level is useful when a device or group of devices is having an issue. In this case, the admin can override those device settings by forcing an elevated log level to Verbose, which logs the maximum level of console activity, making it ideal for troubleshooting.</td>
</tr>
<tr>
<td><em>App Scan Vendor Reset/Toggle</em></td>
<td>Prevents the resetting (and subsequent wiping) of your app scan integration settings. This action is performed in Groups &amp; Settings &gt; All Settings &gt; Apps &gt; App Scan.</td>
</tr>
<tr>
<td>Shut Down</td>
<td>Prevents any attempt to shut down the device in Devices &gt; List View &gt; Device Details.</td>
</tr>
<tr>
<td>Maximum invalid PIN attempts</td>
<td>Defines the maximum number of invalid attempts at entering a PIN before the console locks down. This setting must be between 1 and 5.</td>
</tr>
</tbody>
</table>

**Configure Required Notes for Action**

You can also require admins to enter notes using the Require Notes check box and explain their reasoning when performing these actions. Navigate to Groups & Settings > All Settings > System > Security > Restricted Actions.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock Device</td>
<td>Require a note for any attempt to lock a device from Device List View or Device Details.</td>
</tr>
<tr>
<td>Lock SSO</td>
<td>Require a note for any attempt to lock an SSO session from Device List View or Device Details.</td>
</tr>
<tr>
<td>Device Wipe</td>
<td>Require a note for any attempt to perform a device wipe from Device List View or Device Details.</td>
</tr>
</tbody>
</table>
### Setting | Description
--- | ---
Enterprise Reset | Require a note for any attempt to enterprise reset a device from the Device Details page of a Windows Rugged or Rugged Android device.
Enterprise Wipe | Require a note for any attempt to perform an enterprise wipe from Device Details.
Override Job Log Level | Require a note before attempts to override the default job log level from Groups & Settings > Admin > Diagnostics > Logging.
Reboot Device | Require a note before a reboot attempt from Devices > List View > Device Details.
Shut Down | Require a note before a shut down attempt from Devices > List View > Device Details.

### Other Enterprise Systems for Integration

Take advantage of advanced MDM functionality by integrating your Workspace ONE™ UEM environment with existing enterprise infrastructures including email management with SMTP, directory services, and content management repositories.

- **Email Relay (SMTP)** – Provide security, visibility, and control for mobile email.
- **Directory Services (LDAP/AD)** – Take advantage of existing corporate groups to manage users and devices.
- **Microsoft Certificate Services** – Use existing Microsoft certificate infrastructure for a Workspace ONE UEM deployment.
- **Simple Certificate Enrollment Protocol (SCEP PKI)** – Configure certificates for Wi-Fi, VPN, Microsoft EAS and more.
- **Email Management Exchange 2010 (PowerShell)** – Securely connect Workspace ONE UEM to enforce policies with corporate email servers.
- **BlackBerry Enterprise Server (BES)** – Integrate with BES for streamlined BlackBerry management.
- **Third-party Certificate Services** – Import certificate management systems to be managed within the Console.
- **Lotus Domino Web Service (HTTPS)** – Access Lotus Domino content and features through your AW deployment.
- **Content Repositories** – Integrate with SharePoint, Google Drive, SkyDrive, file servers, and network shares.
- **Syslog (Event log data)** – Export event log data to be viewed across all integrated servers and systems.
- **Corporate Networks** – Configure Wi-Fi and VPN settings, provision device profiles with user credentials for access.
- **System Information and Event Management (SIEM)** – Record and compile device and console data to ensure security and compliance with regulations and corporate policies.

For more information on how to integrate Workspace ONE UEM with these infrastructures, see **VMware Enterprise Systems Connector Guide**, available at https://docs.vmware.com/en/VMware-Identity-Manager/index.html. See also **VMware Tunnel Admin Guide**, the **AirWatch Logging Guide**, and the **AirWatch Installation Guide**, each available on docs.vmware.com. You may also search for these topics on docs.vmware.com.
Chapter 4: User and Admin Accounts

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.

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 choose depends upon the needs of your organization.

**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

On-premises Deployment Model


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.
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.

For more information, see [Workspace ONE Direct Enrollment](#).

### 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 may 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.

Navigate to **Devices > Device Settings > Devices & Users > General > Enrollment** in the **Authentication** tab and select the appropriate check boxes for the **Authentication Mode** setting.

**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 on page 97**.

**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.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Type</td>
<td>Select <strong>Basic</strong> to add a basic user.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter a user name with which the new user is identified.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password that the user can use to log in.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password.</td>
</tr>
<tr>
<td>Full Name</td>
<td>Complete the <strong>First Name</strong>, <strong>Middle Name</strong>, and <strong>Last Name</strong> of the user.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Represent the user in the UEM console by entering a name.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Enter or edit the user's email address.</td>
</tr>
<tr>
<td>Email user name</td>
<td>Enter or edit the user's email user name.</td>
</tr>
<tr>
<td>Domain</td>
<td>Select the email domain from the drop-down setting.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>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.</td>
</tr>
</tbody>
</table>

<p>| Enrollment               | Select the organization group into which the user enrolls.                 |</p>
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow the user to enroll into additional</strong></td>
<td>You can allow the user to enroll into more than one organization group.</td>
</tr>
<tr>
<td><strong>Organization Groups</strong></td>
<td>If you Enable this option but leave <em>Additional Organization Groups</em> blank, then <em>any</em> child OG created under the <em>Enrollment Organization Group</em> can be used as a point of enrollment.</td>
</tr>
<tr>
<td><strong>Additional Organization Groups</strong></td>
<td>This setting only appears when the option to allow the user to enroll into additional OGs is Enabled.</td>
</tr>
<tr>
<td></td>
<td>This setting allows you to add additional organization groups from which your basic user can enroll.</td>
</tr>
<tr>
<td><strong>User Role</strong></td>
<td>Select the role for the user you are adding from this drop-down setting.</td>
</tr>
<tr>
<td><strong>Notification</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Message Type</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Message Template</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
3. You can optionally select the **Advanced** tab and complete the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advanced Info Section</strong></td>
<td></td>
</tr>
<tr>
<td>Email Password</td>
<td>Enter the email password of the user you are adding.</td>
</tr>
<tr>
<td>Confirm Email Password</td>
<td>Confirm the email password of the user you are adding.</td>
</tr>
<tr>
<td>User Principal Name</td>
<td>Enter the principal name of the basic user. This setting is optional.</td>
</tr>
<tr>
<td>Category</td>
<td>Select the User Category for the user being added.</td>
</tr>
<tr>
<td>Department</td>
<td>Enter the user’s department for administrative purposes.</td>
</tr>
<tr>
<td>Employee ID</td>
<td>Enter the user’s employee ID for administrative purposes.</td>
</tr>
<tr>
<td>Cost Center</td>
<td>Enter the user’s cost center for administrative purposes.</td>
</tr>
<tr>
<td><strong>Certificates Section</strong></td>
<td></td>
</tr>
<tr>
<td>Use S/MIME</td>
<td>Enable or Disable Secure Multipurpose Internet Mail Extensions (S/MIME).</td>
</tr>
<tr>
<td></td>
<td>If enabled, you must have an S/MIME-enabled profile and you must upload an S/MIME certificate by selecting <strong>Upload</strong>.</td>
</tr>
<tr>
<td>Separate Encryption Certificate</td>
<td>Enable or Disable encryption certificate.</td>
</tr>
<tr>
<td></td>
<td>If enabled, you must upload an encryption certificate using <strong>Upload</strong>. Generally, the same S/MIME certificate is used for signing and encryption, unless a different certificate is expressly being used.</td>
</tr>
<tr>
<td>Old Encryption Certificate</td>
<td>Enable or disable a legacy version encryption certificate.</td>
</tr>
<tr>
<td></td>
<td>If enabled, you must <strong>Upload</strong> an encryption certificate.</td>
</tr>
<tr>
<td><strong>Staging Section</strong></td>
<td></td>
</tr>
<tr>
<td>Enable Device Staging</td>
<td>Enable or disable the staging of devices.</td>
</tr>
<tr>
<td></td>
<td>If enabled, you must select between <strong>Single User Devices</strong> and <strong>Multi User Devices</strong>. If <strong>Single User Devices</strong>, you must select between <strong>Standard</strong>, where users themselves log in and <strong>Advanced</strong>, where a device is enrolled on behalf of another user. See <strong>Self-Enrollment Versus Device Staging on page 102</strong> for more information.</td>
</tr>
</tbody>
</table>

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. For more information, see **Basic vs. Directory Services Enrollment on page 97**.

Every directory user you want to manage through Workspace ONE UEM must have a corresponding user account in the UEM console.

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 AD DS, 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.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Type</strong></td>
<td>Add an Active Directory user by choosing <strong>Directory</strong> as the Security Type.</td>
</tr>
<tr>
<td><strong>Directory Name</strong></td>
<td>This pre-populated setting identifies the Active Directory name.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>Choose the domain name from the drop-down menu.</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>Enter the user's directory user name and select <strong>Check User</strong>. 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 <strong>Check User</strong> button.</td>
</tr>
</tbody>
</table>
### Setting | Description
--- | ---
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.

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
--- | ---
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.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distinguished Name</td>
<td>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.</td>
</tr>
<tr>
<td>Manager Distinguished Name</td>
<td>Enter the distinguished name of the user's manager. This text box is optional.</td>
</tr>
<tr>
<td>Category</td>
<td>Choose the user category for the user being added.</td>
</tr>
<tr>
<td>Department</td>
<td>Enter the user's department for your company's administrative purposes.</td>
</tr>
<tr>
<td>Employee ID</td>
<td>Enter the user's employee ID for your company's administrative purposes.</td>
</tr>
<tr>
<td>Cost Center</td>
<td>Enter the user's cost center for your company's administrative purposes.</td>
</tr>
<tr>
<td>Custom Attribute 1–5 (for Directory users only)</td>
<td>Enter your previously configured custom attributes, where applicable. You may define these custom attributes by navigating to Groups &amp; Settings &gt; All Settings &gt; Devices &amp; Users &gt; Advanced &gt; Custom Attributes.</td>
</tr>
</tbody>
</table>

**Note:** Custom attributes can be configured only at Customer organization groups.

### Certificates Section

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use S/MIME</td>
<td>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 <strong>Upload</strong>.</td>
</tr>
<tr>
<td>Separate Encryption Certificate</td>
<td>Enable or disable the use of a separate encryption certificate. If enabled, you must upload an encryption certificate using <strong>Upload</strong>. Generally, the same S/MIME certificate is used for signing and encryption, unless a different certificate is expressly being used.</td>
</tr>
<tr>
<td>Old Encryption Certificate</td>
<td>Enable or disable a legacy version encryption certificate. If enabled, you must <strong>Upload</strong> an encryption certificate.</td>
</tr>
</tbody>
</table>

### Staging Section

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Device Staging</td>
<td>Enable or disable the staging of devices. If enabled, you must choose between <strong>Single User Devices</strong> and <strong>Multi User Devices</strong>. If <strong>Single User Devices</strong>, you must select between <strong>Standard</strong>, where users themselves log in and <strong>Advanced</strong>, where a device is enrolled on behalf of another user.</td>
</tr>
</tbody>
</table>

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.

### 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.
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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filters</strong></td>
<td>View only the desired users by using the following filters.</td>
</tr>
<tr>
<td></td>
<td>• Security Type</td>
</tr>
<tr>
<td></td>
<td>• Enrollment Organization Group</td>
</tr>
<tr>
<td></td>
<td>• Enrollment Status</td>
</tr>
<tr>
<td></td>
<td>• User Group</td>
</tr>
<tr>
<td></td>
<td>• User Role</td>
</tr>
<tr>
<td><strong>Add</strong></td>
<td>• <strong>Add User</strong> – 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 on page 43.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Batch Import</strong> – 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 on page 51.</td>
</tr>
</tbody>
</table>
### Action | Description
--- | ---
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. For more information, see Access User Details on page 85.

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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Message</td>
<td>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.</td>
</tr>
<tr>
<td>Add Device</td>
<td>Add a device for the selected user. Only available for single user selections.</td>
</tr>
</tbody>
</table>
| 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 on page 85 and Edit User Group Permissions on page 84.  
- **Remove from User Group**: Remove selected users from the existing user group.  
- **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 resigns or is fired, you can quickly and completely delete a user account.  
- **Activate**: Activate the account if a user returns to an organization or must be reinstated in the company.  
- **Deactivate**: Deactivate a user if a user is missing in action, out-of-compliance, or if their device is lost or stolen. |

### 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 is 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.

**Batch Import Users or Devices**

To save time, you can batch import multiple Lightweight Directory Access Protocol (LDAP)/Active Directory (AD) users and devices into the Workspace ONE™ UEM console.

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. 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 with any text editor. It can also be opened with Microsoft Excel.

You can confirm whether or not users are part of the enrollment organization group (OG).

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

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

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

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.

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.
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 to **Basic User Authentication on page 36** and **Authentication Proxy on page 39** only.

**Move Users with Batch Import**

You may also use the Batch Import feature to move sets of users to a different organization group.
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 Unified Endpoint Management 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 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.

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

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

   OR

   Select the Help button from the header bar that appears at the top-right corner of almost every page of Workspace ONE UEM and choose Add Temporary Admin.

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

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

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

   a. Add a role by selecting the Add Role button and then select the organization group and role for which the temporary admin account applies.

   b. Edit an existing role by selecting the edit icon (-pencil) and choose a different organization group and role.

   c. Delete a role by selecting the delete icon (trash).

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, answer the password recovery question, allowing the basic admin to change their own password. For more information about Password Recovery Questions, see Manage Account Settings on page 10.

  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.
Chapter 5: Role-Based Access

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 may 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.

Default and Custom Roles

There are several default roles already provided by Workspace ONE™ UEM from which you may select. These default roles are available with every upgrade and help quickly assign roles to new users. If you require further customization, you may 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 may 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.

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 on page 65.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Administrator</td>
<td>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.</td>
</tr>
<tr>
<td>AirWatch Administrator</td>
<td>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.</td>
</tr>
<tr>
<td>Console Administrator</td>
<td>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.</td>
</tr>
<tr>
<td>Device Manager</td>
<td>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.</td>
</tr>
<tr>
<td>Report Viewer</td>
<td>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.</td>
</tr>
<tr>
<td>Content Management</td>
<td>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.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Application Management</td>
<td>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.</td>
</tr>
<tr>
<td>Help Desk</td>
<td>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.</td>
</tr>
<tr>
<td>App Catalog Only Admin</td>
<td>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.</td>
</tr>
<tr>
<td>Read Only</td>
<td>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.</td>
</tr>
<tr>
<td>Horizon Administrator</td>
<td>The Horizon Administrator role is a specially designed set of permissions for complementing a Workspace ONE UEM configuration integrated with VMware Horizon View.</td>
</tr>
<tr>
<td>NSX Administrator</td>
<td>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.</td>
</tr>
<tr>
<td>Privacy Officer</td>
<td>The Privacy Officer role provides read access to Hub Overview, Device List View, View system settings, and full edit permissions for privacy settings.</td>
</tr>
</tbody>
</table>

**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.

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.

For more information, see Create Administrator Role on page 61.

**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.

To create a user role:
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.

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.

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.
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.

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 on page 61.

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 on page 63
- Export Admin Roles on page 63
- Versioning Issues When Importing and Exporting Admin Roles on page 64
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.

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.

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 on page 64.

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 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 on page 65.

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. To create an administrator role, follow these steps.
1. Navigate to Accounts > Administrators > Roles and select Add Role in the UEM console.

![Create Role]

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

3. Make a selection 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 make a selection 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 may 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.

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.

To import a role into a separate Workspace ONE™ UEM environment.

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 may 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.
To initiate this process, take the following steps.

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.
3. Select Export and save the XML file to a location on your device.
   If you select more than one admin role, the Export action is not available.

**Rename an Admin Role**

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

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 may be cases where an exported role is imported into an environment running an earlier version of Workspace ONE™ UEM. This earlier version may 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.

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.

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. By showing you only the differences between two admin roles, the Compare Roles tool makes this process easy.

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. Compare two Admin Roles with the Compare Roles tool.

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.
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 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."

You can also 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.
Chapter 6: 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.

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.

Navigate to Groups & Settings > Groups > Assignment Groups.

Create Custom Assignment Group List

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.

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.

- 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 following topics.

View Assignments on page 90
Device List View on page 182

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 type (organization, smart, and user) at one time.

To assign public applications, you can configure different app policies for different groups of users.

1. Navigate to Groups & Settings > Groups > Assignment Groups.
2. Select one or more groups in the listing and select Assign above the column header.
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**

Workspace ONE™ UEM identifies users and establishes permissions using organization groups. While any organization method delivers content to devices, use organization groups (OG) to establish an MDM hierarchy identical to your organizational hierarchy. You may 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.

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 may choose 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.
  
  • Corporate administrators can access and view everything in the environment.
  
  • **Retail Company**
    
      - LA store 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.
• **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** 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 your structure determines which organization groups are children and which are parents. However, only with the addition of repositories and applications can you elect to override this native inheritance.

You can add repositories and applications to child groups that inherit parent group settings. Alternatively, if you choose, you may override inheritance at each group level.

**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.

---

**Shipping Company**

- **Delivery Drivers**
- **Warehouse Scanners**
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.

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 make BYOD users a child of Corporate users. If maintaining separate settings is more important, then make BYOD users a sibling of Corporate users.

For a detailed example of OG inheritance involving enrollment, see Directory Service Integration and Enrollment Restrictions on page 98.

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.

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

2. Select the Add Child Organization Group tab and complete the following settings.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the child organization group (OG) to be displayed. Use alphanumeric characters only. Do not use odd characters.</td>
</tr>
<tr>
<td>Group ID</td>
<td>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 may be required for the device to log in depending on your Shared Device configuration.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the preconfigured OG type that reflects the category for the child OG.</td>
</tr>
<tr>
<td>Country</td>
<td>Select the country where the OG is based.</td>
</tr>
<tr>
<td>Locale</td>
<td>Select the language classification for the selected country.</td>
</tr>
<tr>
<td>Customer Industry</td>
<td>This setting is only available when Type is Customer. Select from the list of Customer Industries.</td>
</tr>
</tbody>
</table>

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 type customer.
  - 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 type container. 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 on page 127.

**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.

![Warning](image)

This setting can be enabled only at organization group of type "Customer".

The following restrictions apply to creating Customer-level organization groups.

- In a software-as-a-service (SaaS) environment, you cannot create nested customer OGs.
- In an on-premises environment, you can create nested customer OGs, but only if your administrator role is System Administrator.

**Organization Groups Settings Comparison**

As an Administrator, you may 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.

For instance, once a User Acceptance Testing (UAT) server has been upgraded, configured, and tested, you can compare the UAT settings to the production settings directly.

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 choosing 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 may 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'.

---

**Chapter 6: Assignment Groups**

VMware AirWatch Mobile Device Management Guide | v.2018.09 | September 2018

Copyright © 2018 VMware, Inc. All rights reserved.
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 a Smart Group

Before you can assign a smart group to an application, book, compliance policy, device profile, video channel, or product provision, you must first create one.

1. Choose the applicable Organization Group to which your new smart group applies and from which it can be managed.

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. Choose between Select Criteria and Select Devices or Users. Switching between Select Criteria and Select Devices or Users erases any entries and selections you may have made.

The Select 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. In the Select 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Group</td>
<td>This criteria option filters devices by organization groups selected. You can select more than one OG.</td>
</tr>
<tr>
<td>User Group</td>
<td>This criteria option filters devices by user groups selected. You can select more than one user group.</td>
</tr>
<tr>
<td>Ownership</td>
<td>This criteria option filters devices by ownership type selected.</td>
</tr>
<tr>
<td>Tags</td>
<td>This criteria option filters devices according to the way they are tagged. You can select more than one tag.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Platform and Operating System</td>
<td>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.</td>
</tr>
<tr>
<td>Model</td>
<td>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.</td>
</tr>
<tr>
<td>Enterprise OEM Version</td>
<td>This criteria option filters devices by their original equipment manufacturer version. You can select more than one OEM.</td>
</tr>
<tr>
<td>Additions</td>
<td>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.</td>
</tr>
<tr>
<td>Exclusions</td>
<td>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.</td>
</tr>
</tbody>
</table>

The Select 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.

Use the Select 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.

There is a limit to the number of rules (500) that a smart group may be programmed with. This 500 rule limit is unrelated to the 500 device threshold determining whether your smart group is Select Criteria or Select Devices or Users-based.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices</td>
<td>Enter the device friendly name to add a device to this smart group. You can add more than one device using this method.</td>
</tr>
<tr>
<td>Users</td>
<td>Enter the username, first name, or last name to add users to this smart group. You can add more than one user using this method.</td>
</tr>
</tbody>
</table>

6. Select Save when complete.

**Assign a Smart Group**

Once you have created the smart group and before it can take effect, you must assign it. You can assign it to an application, book, compliance policy, device profile, video channel, or product provision. There are two methods to assign a smart group.
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, video channel, or product provision.

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, video channel, 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.

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**.

For more information, see **View Device Assignment on page 148**.

Exclude Groups in Profiles and Policies
In addition to apps, books, video channels, and products, smart groups apply to device profiles and compliance policies. This flexibility lets you exclude selected smart groups and user groups from profiles and policies.

For example, if you want a compliance policy for all users in the company except executives, take the following steps.

Exclude Another Smart Group
Make two smart groups, one consisting of all users and another containing executives. Create the Compliance Policy and assign it to the "all users" smart group then specify the "executives" smart group in the Exclusions option.

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 those groups that you want to exclude from the assignment of this profile or policy. You can alternatively make a new group by selecting the **Create Assignment Group** button.
   - If you select the same group in both the **Assigned Groups** and **Excluded Groups** settings, then the profile or policy fails to save.
3. 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.

![Smart Group List View](image)

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, Delete, and Unassign a Smart Group

Any edits that you apply to a smart group affects all policies and profiles to which that smart group is assigned.

For example, 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, then simply edit the smart group by specifying Exclusions. This action removes not only the two internal apps but also the compliance policy and device profile from those excluded devices.

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 may 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.

The **Console Event** logger track changes made to smart groups, including the author of changes, devices added, and devices removed.

**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. If a smart group is assigned, you are not permitted to delete it.

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 name and select **Delete** from the actions menu that displays.

**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.

1. 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 > Staging & 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.
1. Navigate to **Hub > 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 may require including **Date Range**, **Severity**, and **Category**.

4. Where applicable, select the hypertext link in the **Event Data** column which contains extra detail that may 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. For more information, see **Device Assignments on page 133**.

**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 on page 52**.

**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.

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 on page 52**.

### 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.

Before proceeding, ensure that the user group **Type** is **Directory**.
1. Navigate to **Accounts > User Groups > List View**, select **Add** then **Add User Group**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Select the type of User Group.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Directory</strong> – Create a user group that is aligned with your existing active directory structure.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Custom</strong> – 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.</td>
</tr>
<tr>
<td><strong>External Type</strong></td>
<td>Select the external type of group you are adding.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Group</strong> – Refers to the group object class on which your user group is based. Customize this class by navigating to <strong>Groups &amp; Settings &gt; All Settings &gt; System &gt; Enterprise Integration &gt; Directory Services &gt; Group</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Organizational Unit</strong> – Refers to the organizational unit object class on which your user group is based. Customize this class by navigating to <strong>Groups &amp; Settings &gt; All Settings &gt; System &gt; Enterprise Integration &gt; Directory Services &gt; Group</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Custom Query</strong> – 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.</td>
</tr>
<tr>
<td><strong>Search Text</strong></td>
<td>Identify the name of a user group in your directory by entering the search criteria and selecting <strong>Search</strong> to search for it. If a directory group contains your search text, a list of group names displays.</td>
</tr>
<tr>
<td></td>
<td>This option is unavailable when <strong>External Type</strong> is set to <strong>Custom Query</strong>.</td>
</tr>
<tr>
<td><strong>Directory Name</strong></td>
<td>Read-only setting displaying the address of your directory services server.</td>
</tr>
<tr>
<td><strong>Domain and Group Base DN</strong></td>
<td>This information automatically populates based on the directory services server information you enter on the <strong>Directory Services</strong> page (<strong>Groups &amp; Settings &gt; System &gt; Enterprise Integration &gt; Directory Services</strong>).</td>
</tr>
<tr>
<td></td>
<td>Select the <strong>Fetch DN</strong> plus sign (+) next to the <strong>Group Base DN</strong> setting, which displays a list of distinguished name elements from which you can select.</td>
</tr>
<tr>
<td><strong>Custom Object Class</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This option is available only when <strong>Custom Query</strong> is selected as <strong>External Type</strong>.</td>
</tr>
<tr>
<td><strong>Group Name</strong></td>
<td>Select a <strong>Group Name</strong> from your <strong>Search Text</strong> results list. Selecting a group name automatically alters the value in the Distinguished Name setting.</td>
</tr>
<tr>
<td></td>
<td>This option is available only after you have completed a successful search with the <strong>Search Text</strong> setting.</td>
</tr>
<tr>
<td><strong>Distinguished Name</strong></td>
<td>This read-only setting displays the full distinguished name of the group you are creating.</td>
</tr>
<tr>
<td></td>
<td>This option is available only when <strong>Group</strong> or <strong>Organizational Unit</strong> is selected as <strong>External Type</strong>.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Custom Base DN</td>
<td>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.</td>
</tr>
<tr>
<td>Organization Group Assignment</td>
<td>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.</td>
</tr>
<tr>
<td>User Group Settings</td>
<td>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.</td>
</tr>
<tr>
<td>Query</td>
<td>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.</td>
</tr>
<tr>
<td>Custom Logic</td>
<td>Add your custom query logic here, such as user name or admin name. For example, &quot;cn=jsmith&quot;. 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.</td>
</tr>
<tr>
<td>Management Permissions</td>
<td>You can allow or disallow all administrators to manage the user group you are creating.</td>
</tr>
<tr>
<td>Default Role</td>
<td>Select a default role for the user group from the drop-down menu.</td>
</tr>
<tr>
<td>Default Enrollment Policy</td>
<td>Select a default enrollment policy from the drop-down menu.</td>
</tr>
<tr>
<td>Auto Sync with Directory</td>
<td>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.</td>
</tr>
<tr>
<td>Auto Merge Changes</td>
<td>Enable this option to apply sync changes automatically from the database without administrative approval.</td>
</tr>
<tr>
<td>Maximum Allowable Changes</td>
<td>Use this setting to set a threshold for the number of automatic user group sync changes that are allowed to occur before approval must be given. Changes more than the threshold are in need of admin approval and a notification is sent to this effect. This option is available only when Auto Merge Changes is enabled.</td>
</tr>
</tbody>
</table>
## Setting | Description
---|---
**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** | You can send an email to users while adding missing users. Adding missing users means combining the temporary user group table with the Active Directory table.

**Message Template** | Select a message template to be used for the email notification during the addition of missing users to the user group.
This option is available only when **Send Email to User when Adding Missing Users** is enabled.

> For more information on Distinguished Name, search for Microsoft’s TechNet article entitled "Object Naming" at [https://technet.microsoft.com](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. Important logic restrictions are highlighted in red.

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. 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.
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**.

### Access 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.

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.

1. Enable the **Encrypt User Information** setting, then select individual user data settings to activate encryption. Doing so disables the search, sort, and filter functionality.

2. 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** |  
**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 (_csv)** | 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.

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.
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Missing Users</td>
<td>Combine the temporary user group table with the Active Directory table, making the addition of these new users in the user group official.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete a user group.</td>
</tr>
</tbody>
</table>

Add Users to User Groups

When you have a new user to add to one or more user groups, follow these steps.

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 may add users to an Existing User Group or create a New User Group.
5. Choose the Group Name.
6. Select Save.
   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 may synchronize manually. Start a manual synchronization by selecting the user group to which you added users, then select the Sync button.
8. You may 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 may 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 on page 53.
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' in the VMware Workspace ONE™ UEM Console Guide.

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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sync</td>
<td>Copy recently added admin group users to the temporary table, manually, ahead of the scheduled, automated Active Directory sync by Workspace ONE UEM.</td>
</tr>
<tr>
<td>More Actions</td>
<td></td>
</tr>
<tr>
<td>View and Merge</td>
<td>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.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete an admin group.</td>
</tr>
<tr>
<td>Top, Up, Down, Bottom</td>
<td>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.</td>
</tr>
<tr>
<td>Add Missing Users</td>
<td>Combine the temporary admin group table with the Active Directory table, making the addition of these new admins in the group official.</td>
</tr>
</tbody>
</table>

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.
1. Navigate to **Accounts > Administrators > Admin Groups** and select **Add**. Complete the applicable settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>External Type</strong></td>
<td>Select the external type of admin group you are adding.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Group</strong> – Refers to the group object class on which your admin group is based. Customize this class by navigating to <strong>Groups &amp; Settings &gt; All Settings &gt; System &gt; Enterprise Integration &gt; Directory Services &gt; Group</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Organizational Unit</strong> – Refers to the organizational unit object class on which your admin group is based. Customize this object class by navigating to <strong>Groups &amp; Settings &gt; All Settings &gt; System &gt; Enterprise Integration &gt; Directory Services &gt; Group</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Custom Query</strong> – 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.</td>
</tr>
<tr>
<td><strong>Directory Name</strong></td>
<td>Read-only setting displaying the address of your directory services server.</td>
</tr>
<tr>
<td><strong>Domain and Group Base DN</strong></td>
<td>This information automatically populates based on the directory services server information you enter on the Directory Services page (Accounts &gt; User Groups &gt; Settings &gt; 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.</td>
</tr>
<tr>
<td><strong>Search Text</strong></td>
<td>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 <strong>Group</strong> or <strong>Organizational Unit</strong> is selected as the External Type.</td>
</tr>
<tr>
<td><strong>Custom Object Class</strong></td>
<td>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 success and accuracy. This setting is available only when <strong>Custom Query</strong> is selected as External Type.</td>
</tr>
<tr>
<td><strong>Custom Base DN</strong></td>
<td>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 <strong>Custom Query</strong> is selected as External Type.</td>
</tr>
<tr>
<td><strong>Group Name</strong></td>
<td>Select a <strong>Group Name</strong> 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.</td>
</tr>
<tr>
<td><strong>Distinguished Name</strong></td>
<td>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.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Rank</td>
<td>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 &amp; Settings &gt; Groups &gt; Admin Groups and moving its relative position using the More action button to the right of the admin group listing.</td>
</tr>
<tr>
<td>Auto Sync</td>
<td>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.</td>
</tr>
<tr>
<td>Auto Merge</td>
<td>Enable this option to apply sync changes automatically from the database without administrative approval.</td>
</tr>
<tr>
<td>Maximum Allowable Changes</td>
<td>Use this setting to set a threshold for the number of automatic admin group sync changes that are allowed to occur before approval must be given. This option is available only when Auto Merge is enabled.</td>
</tr>
<tr>
<td>Add Group Members Automatically</td>
<td>Enable this option to add administrators automatically to the admin group.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Enter the time zone associated with the admin group. This required setting impacts when the scheduled, automated Active Directory sync runs.</td>
</tr>
<tr>
<td>Locale</td>
<td>Select the localization setting (language) associated with the admin group. This setting is required.</td>
</tr>
<tr>
<td>Initial Landing Page</td>
<td>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.</td>
</tr>
<tr>
<td>Custom Query</td>
<td></td>
</tr>
<tr>
<td>Query</td>
<td>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.</td>
</tr>
<tr>
<td>Custom Logic</td>
<td>Add your custom query logic here, such as an admin name. For example, &quot;cn=jsmith&quot;. 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.</td>
</tr>
</tbody>
</table>

💡 For more information on Distinguished Name, search for Microsoft's TechNet article entitled "Object Naming" at [https://technet.microsoft.com](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.
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.

Above the header row in the **View Assignments** screen, are three new tools to help you confirm the specific profile, app, book, channel, and compliance policy.
Chapter 7: Device Enrollment

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 on page 127.

Enroll a Device with AirWatch Agent

Enrolling a device with the AirWatch Agent is the main option for Android, iOS, and Windows devices.

1. Navigate to [AWAgent.com](file://) from the native browser on the device that you are enrolling.
   - Workspace ONE™ UEM auto-detects if the AirWatch Agent is already installed and redirects to the appropriate mobile app store to download the Agent if needed.
   - Downloading the Agent from public application stores requires either an Apple ID or a Google Account.
2. Run the Agent upon the completion of the download or return to your browser session.

   **Important:** To ensure a successful installation and running of the AirWatch Agent 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
Finalize the enrollment by following all remaining prompts.

**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.

- **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 on page 113.

End-User Device Registration on page 112.
Device Registration on page 107.
Stage a Single-User Device on page 106.
Stage a Multi-User Device on page 106.

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.

Workspace ONE Direct Enrollment Supported Options

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 Agent 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 AirWatch Agent instead of Workspace ONE Direct Enrollment.

Enable Direct Enrollment for Workspace ONE
You must 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.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require MDM for Workspace ONE</td>
<td>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).</td>
</tr>
<tr>
<td>Assigned User Group</td>
<td>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.</td>
</tr>
<tr>
<td>iOS</td>
<td>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.</td>
</tr>
<tr>
<td>Android Legacy</td>
<td>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.</td>
</tr>
<tr>
<td>Android Enterprise</td>
<td>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.</td>
</tr>
</tbody>
</table>

5. Select Save.

Only supported options configured on the other enrollment tabs apply to your saved direct enrollment configuration. Once Workspace ONE Direct Enrollment has been enabled, the next step is to Enroll Your Device with Workspace ONE Direct Enrollment on page 96.

For more information about Direct Enrollment for Workspace ONE Options and Enrollment Options in general, see Workspace ONE Direct Enrollment Supported Options on page 94 and Configure Enrollment Options on page 115.

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.

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 AirWatch Agent, allow Agent to make and manage phone calls, select the 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

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Enrollment</strong></td>
<td><strong>Can be used for any deployment method.</strong>&lt;br&gt;<strong>Requires no technical integration.</strong>&lt;br&gt;<strong>Requires no enterprise infrastructure.</strong>&lt;br&gt;<strong>Can enroll into potentially multiple organization groups.</strong></td>
</tr>
<tr>
<td>Directory Service Enrollment</td>
<td>Pros</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------</td>
</tr>
<tr>
<td></td>
<td>• End users authenticate with existing corporate credentials.</td>
</tr>
<tr>
<td></td>
<td>• Can automatically detect and sync changes from the directory system into Workspace ONE UEM.</td>
</tr>
<tr>
<td></td>
<td>• Secure method of integrating with your existing directory service.</td>
</tr>
<tr>
<td></td>
<td>• Standard integration practice.</td>
</tr>
<tr>
<td></td>
<td>• Can be used for Workspace ONE Direct Enrollment.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>

**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.

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 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 vs Directory users, consider also the following questions.

For the pros & cons of basic users vs directory users, see **Basic vs. Directory Services Enrollment on page 97**.

**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? 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 on page 124.

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 on page 117.

* 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 on page 43.

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 on page 51.

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 AirWatch Agent?**

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.

AirWatch Agent represents the legacy enrollment option for mobile devices. For details, see Enroll a Device with AirWatch Agent on page 92.

**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 on page 123.

**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.

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.

Now, set the Default Device Ownership type to Employee Owned for all open enrollment.

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

2. Select Employee Owned as the Default Device Ownership.

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

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

5. 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.

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.

Risks

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, 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.

While you can always update the ownership type later, 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.

**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 AirWatch Agent instead of Workspace ONE Direct Enrollment.

For more information, see **Workspace ONE Direct Enrollment on page 94.**

**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 themself.

**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 on page 128** and **Configure Autodiscovery Enrollment from a Parent Organization Group on page 128.**

**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 on page 94.

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 on page 127.

1. End users navigate to AWAgent.com, which automatically detects whether the AirWatch Agent is installed. If it is not, 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 Agent or Container app, users enter their credentials – in addition to either an email address or URL/Group ID – and proceed with enrollment.

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.
- **Single User (Advanced)** – Used when you are staging and enrolling a device for a particular 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 being able to delete 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 AirWatch Agent instead of Workspace ONE Direct Enrollment.

For more information, see Workspace ONE Direct Enrollment on page 94.

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 to log 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 AirWatch Agent, 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™ UEM 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 AirWatch Agent instead of Workspace ONE Direct Enrollment.

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.

3. **Single User Devices** stages devices for a single user. 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 using one of the two following methods.
   - Enroll using the AirWatch Agent 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 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.
   - 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.

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

**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 AirWatch Agent instead of Workspace ONE Direct Enrollment.

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.

3. Single User Devices stages devices for a single user. 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 AirWatch Agent 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 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.
   - 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.

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.

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 Hub, 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 opt to have end users register their own devices before enrolling into Workspace ONE UEM if you are supporting BYOD in your deployment and yet still require devices to be registered before they can enroll.

For more information, see Enable Registration Tokens and Create a Default Message on page 113.

**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 on page 117.

**Register an Individual Device**

To register an individual device, take the following steps.

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**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Section</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Search Text</strong></td>
<td>Search for the user by entering a search parameter and select the <strong>Search User</strong> button. If a successful search is performed, the user account for whom you are registering the device is displayed. 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.</td>
</tr>
<tr>
<td><strong>Device Section</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Expected Friendly Name</strong></td>
<td>Enter the Friendly Name of the device. This text box accepts <strong>Lookup Values</strong> which you can insert by selecting the plus sign. For details, see <strong>Lookup Values on page 201</strong>.</td>
</tr>
<tr>
<td><strong>Organization Group</strong></td>
<td>Select the Organization Group to which the device belongs.</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>Select the ownership level of the device.</td>
</tr>
<tr>
<td><strong>Platform</strong></td>
<td>Select the platform of the device.</td>
</tr>
<tr>
<td><strong>Show advanced device information options</strong></td>
<td>Display advanced device information settings.</td>
</tr>
<tr>
<td><strong>Model</strong></td>
<td>Select the device model. This drop-down menu option depends upon the <strong>Platform</strong> selection.</td>
</tr>
<tr>
<td><strong>OS</strong></td>
<td>Select the device operating system. This drop-down menu option depends upon the <strong>Platform</strong> selection.</td>
</tr>
<tr>
<td><strong>UDID</strong></td>
<td>Enter the device unique device identifier.</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>Enter the serial number of the device.</td>
</tr>
<tr>
<td><strong>IMEI</strong></td>
<td>Enter the device international mobile station equipment identity number.</td>
</tr>
<tr>
<td><strong>SIM</strong></td>
<td>Enter the subscriber identity module for the device.</td>
</tr>
<tr>
<td><strong>Asset Number</strong></td>
<td>Enter the device asset number.</td>
</tr>
<tr>
<td><strong>Messaging Section</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Message Type</strong></td>
<td>The type of notification sent to the user once the device is added. Select from <strong>None</strong>, <strong>Email</strong>, or <strong>SMS</strong>.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Email</strong> option requires a valid email address. You must also select an Email Message Template.</td>
</tr>
<tr>
<td></td>
<td>The <strong>SMS</strong> option requires a phone number including country code and area code. <strong>SMS</strong> charges may apply. You must also select an SMS Message Template.</td>
</tr>
<tr>
<td><strong>Email Address</strong></td>
<td>Required for the <strong>Email Message Type</strong>.</td>
</tr>
</tbody>
</table>
4. Complete the **Custom Attributes** tab (optional).

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add a custom <strong>Attribute</strong> and its corresponding <strong>Value</strong> by selecting this button. For more information, .</td>
</tr>
<tr>
<td>Attributes</td>
<td>Select the custom attribute from the drop-down menu.</td>
</tr>
<tr>
<td>Value</td>
<td>Select the value of the custom attribute from the drop-down menu.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add a <strong>Tag</strong> to the device.</td>
</tr>
<tr>
<td>Tag</td>
<td>Select the Tag from the drop-down menu of existing Tags.</td>
</tr>
</tbody>
</table>

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

The device is now registered to the selected Workspace ONE UEM user account specified in step 3. 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, in the following ranking. This ranking allows Workspace ONE UEM to register devices successfully for which inadequate information has been provided.

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

Registering devices before they are enrolled is optional and allows you to restrict an enrollment to registered devices only. Another benefit is tracking enrollment statuses.

You can register multiple devices using a batch import feature which saves time.

To register multiple devices:

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.

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

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

5. 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.

6. 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.

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

End-User Device Registration

Directing end users to register their own devices may 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 may 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](https://<AirWatchEnvironment>/MyDevice) where `<AirWatchEnvironment>` is the enrollment URL. For more information, see [Direct Users to Self-Register on page 113](#).

• **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 follow these steps to register their own devices to save time.

1. Navigate to the Self-Service Portal (SSP) URL: [https://<AirWatchEnvironment>/MyDevice](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 may need to troubleshoot device registration, or track the stage of the overall enrollment process. End users may 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 may choose to reset (or even revoke) their registration token.

For more information, see [Enrollment Status on page 197](#).

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

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.
Scrolled 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.

2. 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.

3. 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.

4. Set the Token Expiration Time (in hours). This required setting is the amount of time an end user has to select a link and enroll. Once it expires, you must send another link.

Generate a Token With the UEM Console

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 and SMS for basic user accounts.

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

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

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

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.

**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**

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.

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 > Device Settings > Devices & Users > General > Enrollment.

**Getting Started**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Email Domain</td>
<td>This button is used for setting up the Auto-Discovery Service to register email domains to your environment. For more information about the AutoDiscovery Service, see Autodiscovery Enrollment on page 127.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Authentication Mode(s)</td>
<td>Select the allowed authentication types, which include:</td>
</tr>
<tr>
<td></td>
<td>• Basic – Basic user accounts (ones you create manually in the UEM console) can enroll.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Authentication Proxy – Allows users to enroll using Authentication Proxy user accounts. Users authenticate to a web endpoint.</td>
</tr>
<tr>
<td>Devices Enrollment Mode</td>
<td>Select the preferred device enrollment mode, which includes:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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 <a href="https://www.vmware.com/support/ume/">VMware Workspace ONE UEM Mobile Device Management Guide</a>. Workspace ONE Direct Enrollment supports allowing only registered devices to enroll but only if registration tokens are not required.</td>
</tr>
<tr>
<td>Require Registration Token</td>
<td>Visible only when Registered Devices Only is selected.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Require Agent Enrollment for iOS</td>
<td>Select this check box to require iOS device users to download and install the Agent before they can enroll.</td>
</tr>
<tr>
<td>Require Agent Enrollment for macOS</td>
<td>Select this check box to require macOS device users to download and install the Agent before they can enroll.</td>
</tr>
</tbody>
</table>

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 on page 117.
2. Configure Enrollment Restriction Settings on page 124.
3. Configure Enrollment Options on Optional Prompt Tab on page 118.
4. Configure Enrollment Options on Customization Tab on page 121.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require Enrollment Terms of Use Acceptance</td>
<td>Enable this setting to require the acceptance of a terms of use agreement at enrollment time.</td>
</tr>
<tr>
<td>Add New Enrollment Terms of Use</td>
<td>Select to initiate the addition of a terms of use agreement for enrollment purposes. For details, see Create Enrollment Terms of Use on page 30.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ID Assignment Mode</td>
<td>Workspace ONE Direct Enrollment supports all assignment modes.</td>
</tr>
<tr>
<td>- <strong>Default</strong></td>
<td>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.</td>
</tr>
<tr>
<td>- <strong>Prompt User to Select Group ID</strong></td>
<td>Enable this option to allow directory service users to select a Group ID from a list upon enrollment. The <strong>Group ID Assignment</strong> 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.</td>
</tr>
<tr>
<td>- <strong>Automatically Select Based on User Group</strong></td>
<td>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 <strong>Group Assignment Settings</strong> section lists all the organization groups for the environment and their associated directory service user groups. Select the <strong>Edit Group Assignment</strong> 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.</td>
</tr>
</tbody>
</table>
### Default Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Device Ownership</td>
<td>Select the default Device Ownership of devices enrollment into the current organization group. Workspace ONE Direct Enrollment supports setting a default device ownership.</td>
</tr>
<tr>
<td>Default Role</td>
<td>Select the default roles assigned to users at the current organization group, which can affect access to the Self-Service Portal. Workspace ONE Direct Enrollment supports setting a default role.</td>
</tr>
<tr>
<td>Default Action for Inactive Users</td>
<td>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.</td>
</tr>
</tbody>
</table>

### User Group Sync Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sync User Groups in Real Time for Workspace ONE</td>
<td>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.</td>
</tr>
</tbody>
</table>

### User Role Mapping Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Directory Group-Based Mapping</td>
<td>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 <strong>Edit assignment</strong> button. Workspace ONE Direct Enrollment supports directory group-based mapping.</td>
</tr>
</tbody>
</table>

### Configure Enrollment Options on Optional Prompt Tab

On the **Optional Prompt** tab, you may 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**.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prompt for Device Ownership Type</td>
<td>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.</td>
</tr>
<tr>
<td>Display Welcome Message</td>
<td>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 <strong>System &gt; Localization &gt; Localization Editor</strong>. Next, select the labels 'EnrollmentWelcomeMessageHeader' and 'EnrollmentWelcomeMessageBody' respectively. If you opt to customize your own header and body messages using the Localization Editor, you must opt to 'Override' in the <strong>Current Setting</strong> 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 <strong>System &gt; Localization &gt; Localization Editor</strong> and select the <strong>Modify</strong> button. Edit the file per your preferences to affect bulk localization changes and upload it using the same screen.</td>
</tr>
<tr>
<td>Display MDM Installation Message</td>
<td>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 <strong>System &gt; Localization &gt; Localization Editor</strong>. Next, select the labels 'EnrollmentMdmInstallationMessageHeader' and 'EnrollmentMdmInstallationMessageBody' respectively.</td>
</tr>
<tr>
<td>Enable Enrollment Email Prompt</td>
<td>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. For details, see <strong>Lookup Values on page 201</strong>.</td>
</tr>
<tr>
<td>Enable Device Asset Number Prompt</td>
<td>You can prompt the user to enter the device asset number during enrollment. Workspace ONE Direct Enrollment supports enrollment email prompts but only when <strong>Prompt for Device Ownership Type</strong> is enabled and only for Corporate Owned devices.</td>
</tr>
<tr>
<td>Display Enrollment Transition Messages (Android Only)</td>
<td>You can display or hide enrollment messages on Android devices.</td>
</tr>
<tr>
<td>Enable TLS Mutual Auth for Windows</td>
<td>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.</td>
</tr>
</tbody>
</table>

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."

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 Enrollment Message Templates on page 120.

3. For iOS devices, optionally configure the following:
   - Enter a post-enrollment landing URL for iOS devices.
   - 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 Enrollment Message Templates

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

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. You can add languages by selecting the Add button.

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 message by entering text to the Message Body text box.
   You have two methods with which to compose the Email message template: Plain Text and HTML. 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, which can be configured by navigating to Groups & Settings > All Settings > Devices & Users > General > Enrollment and selecting the **Restrictions** tab.

### 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use specific Message Template for each Platform</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Enrollment Support Email</strong></td>
<td>Enter the support email address.</td>
</tr>
<tr>
<td><strong>Enrollment Support Phone</strong></td>
<td>Enter the support phone number.</td>
</tr>
<tr>
<td><strong>Post-Enrollment Landing URL (iOS only)</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
Blacklisting and Whitelisting Device Registration

A blacklist is an explicit listing of devices or apps that are not allowed. A whitelist is an explicit listing of devices or apps that are only allowed. This concept can be applied to registration to enable you to control which devices are allowed to enroll and which devices are not permitted to enroll.

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.

**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.

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.

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

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](page 122).

#### 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](page 125).
**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Access Control</td>
<td>All user access control options are supported by Workspace ONE Direct Enrollment.</td>
</tr>
<tr>
<td><strong>Restrict Enrollment to Known Users</strong></td>
<td>Enable to restrict enrollment only to users that already exist in the UEM console. This 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 enables you to selectively allow users to enroll. Disable this option to allow all directory users who do not already exist in the UEM console to enroll into Workspace ONE UEM. User accounts are automatically created during enrollment.</td>
</tr>
<tr>
<td><strong>Restrict Enrollment to Configured Groups</strong></td>
<td>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. You should not select this option if you have not integrated with your directory services user groups. Disable this option to allow all directory users to create new Workspace ONE UEM user accounts during enrollment. In addition, you can select the <strong>Enterprise Wipe devices of users that are removed from configured groups</strong> option to automatically enterprise wipe any devices <strong>not</strong> belonging to any user group (if <strong>All Groups</strong> is selected) or a particular user group (if <strong>Selected Groups</strong> is selected). One option for integrating with user groups is to create an &quot;MDM Approved&quot; directory service group, import it to Workspace ONE UEM, then add existing directory service user groups to the &quot;MDM Approved&quot; group as they become eligible for Workspace ONE UEM.</td>
</tr>
<tr>
<td>Set limit for maximum enrolled devices at this OG and below</td>
<td>Enable and <strong>Enter Device Limit</strong> to limit the number of devices allowed to enroll in the current organization group (OG). Setting a maximum enrolled devices is supported by Workspace ONE Direct Enrollment.</td>
</tr>
</tbody>
</table>

**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.

Limit the Number of Enrolled Devices Per Organization Group

To define an enrolled device limit on your current OG, take the following steps.

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.

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.

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.

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.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrollment Restriction Policy Name</td>
<td>Enter a name for your enrollment restriction policy.</td>
</tr>
<tr>
<td>Organization Group</td>
<td>Choose an organization group from the drop-down field. This is the OG to which your new enrollment restriction policy applies.</td>
</tr>
<tr>
<td>Policy Type</td>
<td>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.</td>
</tr>
<tr>
<td>Allowed Ownership Types</td>
<td>Choose 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.</td>
</tr>
<tr>
<td>Allowed Enrollment Types</td>
<td>Choose whether to permit or prevent the enrollment of devices using MDM (AirWatch Agent) and AirWatch Container (for iOS/Android) apps.</td>
</tr>
<tr>
<td>Device Limit per User</td>
<td>Select Unlimited to allow users to enroll as many devices as they want. Setting a device limit per user is supported by Workspace ONE Direct Enrollment. Uncheck this box to enter values for the Device Limit Per User section, to define the maximum number of devices per ownership type.</td>
</tr>
<tr>
<td></td>
<td>• Maximum Devices Per User</td>
</tr>
<tr>
<td></td>
<td>• Corporate Max Devices</td>
</tr>
<tr>
<td></td>
<td>• Shared Max Devices</td>
</tr>
<tr>
<td></td>
<td>• Employee Owned Max Devices</td>
</tr>
<tr>
<td>Allowed Device Types</td>
<td>Select the Limit enrollment to specific platforms, models or operating systems checkbox to add additional device-specific restrictions. This option is supported by Workspace ONE Direct Enrollment.</td>
</tr>
</tbody>
</table>

**Note:** Current Microsoft functionality dictates that you cannot blacklist Windows Phone devices by IMEI or UDID.
### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Device Level Restrictions Mode | This field is only available if **Limit enrollment to specific platforms, models or operating systems** is selected in the **Allowed Device Types** field. 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), **Operating System**, or **Enterprise Version**. 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.

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://myworkspaceone.com/set-discovery-password](https://myworkspaceone.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.
   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.

3. Select Save to complete an autodiscovery setup.

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.

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

2. Select Prompt User to Select Group ID.

3. Select Save.
Chapter 8: Shared Devices

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.

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.

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 AirWatch Agent. 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 AirWatch Agent.
  - 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.
- 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 AirWatch Agent v4.2+
- MacOS devices with AirWatch Agent v2.1+

Define the Shared Device Hierarchy
When you first log in to Workspace ONE™ UEM, you see a single organization group (OG) that has been created for you using the name of your organization. This group serves as your top-level OG. Below this top-level group you can create subgroups to build out your company hierarchical structure.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the child organization group (OG) to be displayed. Use alphanumeric characters only. Do not use odd characters.</td>
</tr>
<tr>
<td>Group ID</td>
<td>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 <strong>Group ID</strong> as it may be required for the device to log in depending on your Shared Device configuration.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the preconfigured OG type that reflects the category for the child OG.</td>
</tr>
<tr>
<td>Country</td>
<td>Select the country where the OG is based.</td>
</tr>
<tr>
<td>Locale</td>
<td>Select the language classification for the selected country.</td>
</tr>
<tr>
<td>Customer Industry</td>
<td>This setting is only available when <strong>Type</strong> is Customer. Select from the list of Customer Industries.</td>
</tr>
</tbody>
</table>

5. Select **Save**.
Log In and Log Out of Shared Android Devices

To use shared device functionality on Android devices, enroll the device using the AirWatch Agent and set the Android Launcher application as the default home screen. The Launcher application 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.

Log In to an Android Device

1. From the 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, then end users are required to enter a Group ID to log in.
2. Tap 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.

Log Out of an Android Device

1. Tap the Settings button.
2. Select log out.

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 agent.

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 agent is restarted and the check-out screen displays.

Restrictions

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

Task

Check-in an iOS device from the console by taking the following steps.

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.
Chapter 9: Device Assignments

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.

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.

1. Navigate to Groups & Settings > All Settings > Devices & Users > General > Advanced and select Override or Inherit for the Current Setting according to your needs.
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 on page 207.
   
   - **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.

   4. Choose the Device Ownership options. Only devices with the selected ownership types are assigned.
      
      - Corporate – Dedicated
      - Corporate – Shared

   **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 > Staging & Provisioning > Custom Attributes > Custom Attribute Assignment Rules.
5. You can add a network range by selecting the link, Click here to create a network range. When selected, the Network Ranges page is displayed. 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 on page 135.

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.

1. Navigate to Groups & Settings > Groups > Organization Groups > Network Ranges.

   This setting 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 on page 133.

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.

   - 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. On the Batch Import page, select the Download template for this batch type link to view and download the bulk import template.
Complete this template, import it using the **Batch Import** page, and select **Save**.
Chapter 10: Device Profiles

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.

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.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the profile to be displayed in the Workspace ONE™ UEM console.</td>
</tr>
<tr>
<td>Version</td>
<td>Read-only text box that reports the current version of the profile as determined by the Add Version.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the profile that indicates its purpose.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Deployment</td>
<td>Determines if the profile is automatically removed upon unenrollment (does not apply to Android profiles).</td>
</tr>
<tr>
<td></td>
<td>- Managed – The profile is removed.</td>
</tr>
<tr>
<td></td>
<td>- Manual – The profile remains installed until removed by the end user.</td>
</tr>
<tr>
<td>Assignment Type</td>
<td>Determines how the profile is deployed to devices.</td>
</tr>
<tr>
<td></td>
<td>- Auto – The profile is deployed to all devices.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 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 &amp; Settings &gt; All Settings &gt; Devices &amp; Users &gt; Advanced &gt; Profile Options.</td>
</tr>
<tr>
<td></td>
<td>- 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 on page 143.</td>
</tr>
<tr>
<td>Allow Removal</td>
<td>- Always – The end user can manually remove the profile at any time.</td>
</tr>
<tr>
<td></td>
<td>- With Authorization – The end user can remove the profile with the authorization of the administrator. Selecting this option adds an account Password text box.</td>
</tr>
<tr>
<td></td>
<td>- Never – The end user cannot remove the profile from the device.</td>
</tr>
<tr>
<td>Managed By</td>
<td>The organization group with administrative access to the profile.</td>
</tr>
<tr>
<td>Assigned Groups</td>
<td>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 on page 67.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Exclusions</td>
<td>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 on page 77 for details.</td>
</tr>
</tbody>
</table>
### Setting | Description
--- | ---
**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 on page 144.

- **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 on page 146.

**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 have created and assigned profiles, you will 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filters</strong></td>
<td>View only the desired profiles by using the following filters.</td>
</tr>
<tr>
<td></td>
<td><strong>Status</strong> – Filter devices to view Active, Inactive, and All devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Platform</strong> – Filter devices by 13 types of platforms or all platforms.</td>
</tr>
<tr>
<td></td>
<td><strong>Smart Group</strong> – Filter devices by selecting a smart group from the drop-down menu.</td>
</tr>
</tbody>
</table>

| **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. |

<p>| <strong>Export</strong> | Save a CSV file (comma-separated values) of the entire <strong>List View</strong> that can be viewed and analyzed in Excel. If you have a filter applied to the <strong>List View</strong>, the exported listing reflects the filtered results. |</p>
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column Sorting</td>
<td>Select the column heading to toggle the sorting of the list.</td>
</tr>
<tr>
<td>Profile Details</td>
<td>In both the Summary and Custom views, the Profile Details column, each profile features an icon representing the payload type.</td>
</tr>
<tr>
<td></td>
<td>– Single payload types feature a unique icon for that individual payload type.</td>
</tr>
<tr>
<td></td>
<td>– Profiles featuring multiple payloads of the same type feature a number badge in the upper-right corner of the icon.</td>
</tr>
<tr>
<td></td>
<td>– Profiles featuring multiple payloads of differing types feature a generic icon with a number badge.</td>
</tr>
<tr>
<td>Installed Status</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Installed (✔️) – This indicator displays the number of devices on which the profile is assigned and successfully installed.</td>
</tr>
<tr>
<td></td>
<td>• Not Installed (⛔️) – This indicator displays the number of devices to which the profile is assigned but not installed.</td>
</tr>
<tr>
<td></td>
<td>• Assigned (👨‍👩‍👧‍👦) – This indicator displays the total number of assigned profiles whether they are installed or not.</td>
</tr>
<tr>
<td>Radio button and Edit Icon</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• &lt;/&gt; 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.</td>
</tr>
<tr>
<td></td>
<td>• More Actions</td>
</tr>
<tr>
<td></td>
<td>○ Copy – Make a copy of an existing profile and tweak the configuration of the copy to get started with device profiles.</td>
</tr>
<tr>
<td></td>
<td>○ Activate/Deactivate – Toggle between making a device profile active and inactive.</td>
</tr>
<tr>
<td></td>
<td>○ Delete – Maintain your roster of profiles by removing unnecessary profiles.</td>
</tr>
</tbody>
</table>
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.

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. 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.

You can also 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.

You can also 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 the following installation statuses as they relate to the selected iOS device.

- 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.

1. Navigate to **Devices > Profiles & Resources > Profiles** and select the **Edit** icon (笔) 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. 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.

For more information, see the following topics.
Add General Profile Settings on page 137
View Device Assignment on page 148

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.

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. 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 Compliance Policies on page 166.

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

Compliance profiles are created and saved in the same manner as Auto and Optional device profiles.

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.

5. When finished, select **Save & Publish**.

For step-by-step instructions on completing a device profile, see *Add General Profile Settings on page 137*

Next, you must select this profile in your compliance policy.

6. Navigate to **Devices > Compliance Policies > List View** and select **Add**, then select a platform.

7. Define the **Rules** and select **Next**.

8. In the **Actions** tab, make the following selections.
   - Set the first drop-down menu to 'Profile'.
   - Set the second drop-down menu to 'Install Compliance Profile'.
   - Set the third drop-down menu to the device profile you named in step 2.

9. Select **Next** and proceed configuring the remaining settings including Assignment and Summary tabs.

10. Save the compliance policy by selecting **Finish** or **Finish and Activate**.

For step-by-step instructions on completing a compliance policy, see *Add a Compliance Policy on page 173*.

---

**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.
  1. **Add a Geofencing Area on page 145**.
  2. **Apply a Geofence to a Profile on page 146**.

- 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](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 agent 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 AirWatch Agent) when the end user opens and uses them.

Devices in an "airplane mode" result in location services (and therefore Geofencing) being deactivated.

<table>
<thead>
<tr>
<th>Device</th>
<th>Wi-Fi</th>
<th>Cellular Network</th>
<th>Built-In GPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>iPad Wi-Fi + 3G/4G</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>iPad Wi-Fi</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPod Touch</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

The following requirements must all be met for the GPS location to be updated.

- The device must have the AirWatch Agent running.
- Privacy settings must allow GPS location data to be collected (**Groups & Settings > All Settings > Devices & Users > General > Privacy**).
- The Apple iOS Agent settings must enable “Collect Location Data” (**Groups & Settings > All Settings > Devices & Users > Apple > Apple iOS > Agent Settings**).
  
  Set the Agent SDK settings to the Default SDK settings instead of "None".

**Add a Geofencing Area**

You must define a Geofencing area before you can apply one to a device.

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. Also, 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 may 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**.

Next, you must **Apply a Geofence to a Profile on page 146**.
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.

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.

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**.

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.

**iBeacons**

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](http://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.
2. Apply a Time Schedule to a Profile.

**Define a Time Schedule**

You must define a time schedule before applying it to a device profile.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Schedule Name</strong></td>
<td>Enter the name of the time schedule that appears in the listing.</td>
</tr>
<tr>
<td><strong>Time Zone</strong></td>
<td>Select the time zone of the organization group under which the device is managed.</td>
</tr>
<tr>
<td><strong>Day of the Week</strong></td>
<td>Apply a scheduled profile installation by choosing a day of the week.</td>
</tr>
<tr>
<td><strong>All Day</strong></td>
<td>Make the profile install at midnight on the selected <strong>Day of the Week</strong>. Selecting this check box removes the <strong>Start Time</strong> and <strong>End Time</strong> columns.</td>
</tr>
<tr>
<td><strong>Start Time</strong></td>
<td>Select the time of day you want the profile to be installed.</td>
</tr>
<tr>
<td><strong>End Time</strong></td>
<td>Select the time of day you want the profile to be uninstalled.</td>
</tr>
<tr>
<td><strong>Actions</strong></td>
<td>Remove the day's schedule by clicking the X.</td>
</tr>
</tbody>
</table>

4. Select **Save**.

**Apply a Time Schedule to a New 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.

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.

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.

1. Select the radio button next to the time schedule you want to delete.
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.
Chapter 11: Resources

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.

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 (-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 Resources on page 149.
1. Add an Exchange resource by completing the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resource Details</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Resource Name</strong></td>
<td>Name of the profile to be displayed in the Workspace ONE ™ UEM console.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>A brief description of the profile that indicates its purpose.</td>
</tr>
<tr>
<td><strong>Connection Info</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Mail Client</strong></td>
<td>Select the email client you want to use with the resource.</td>
</tr>
<tr>
<td><strong>Exchange Host</strong></td>
<td>Enter the Exchange Host for the email account to be included in the resource.</td>
</tr>
<tr>
<td><strong>Use SSL</strong></td>
<td>Enable a secure socket layer for this mail client.</td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>Enter a lookup value for the email domain.</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>Enter a lookup value for the email user name.</td>
</tr>
<tr>
<td><strong>Email Address</strong></td>
<td>Enter a lookup value for the email address.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password for the email account. Enable the Show Characters check box to display the unredacted password.</td>
</tr>
<tr>
<td><strong>Identity Certificate</strong></td>
<td>Upload and attach a certificate authority to the email account by selecting the Add A Certificate button.</td>
</tr>
<tr>
<td><strong>Past Days of Mail to Sync</strong></td>
<td>Select the length of email history you want to synchronize. Choose from 3 Days, 1 Week, 2 Weeks, 1 Month, and Unlimited.</td>
</tr>
<tr>
<td><strong>Sync Calendar</strong></td>
<td>Choose to synchronize your device calender with the exchange calendar. This setting is enabled by default on iOS and macOS devices.</td>
</tr>
<tr>
<td><strong>Sync Contacts</strong></td>
<td>Choose to synchronize your device contacts with the exchange contacts. This setting is enabled by default on iOS and macOS devices.</td>
</tr>
</tbody>
</table>

* For details, see Lookup Values on page 201.

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 on page 152.
   - Configure Advanced Settings for macOS Exchange on page 153.
   - Configure Advanced Settings for Android Exchange on page 153.
   - Configure Advanced Settings for Windows Phone Exchange on page 154.
   - Configure Advanced Settings for Windows Desktop Exchange on page 155.

3. Click Next to proceed to the Assignment section.

4. Assign the resource to devices by completing the following settings.
### 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use S/MIME</td>
<td>Use Secure Multipurpose Internet Mail Extensions, a public key encryption and signing standard.</td>
</tr>
<tr>
<td>S/MIME Certificate</td>
<td>Only available when Use S/MIME is enabled. Add a signing certificate to emails by selecting Add A Certificate.</td>
</tr>
<tr>
<td>S/MIME Encryption Certificate</td>
<td>Only available when Use S/MIME is enabled. Add a certificate that encrypts and digitally signs email by selecting Add A Certificate.</td>
</tr>
<tr>
<td>Enable Per-Message Switch</td>
<td>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).</td>
</tr>
</tbody>
</table>

### Settings and Security

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent moving messages</td>
<td>Prevent moving mail from an Exchange mailbox to another mailbox on the device.</td>
</tr>
<tr>
<td>Prevent use in third-party apps</td>
<td>Prevent other apps from using the Exchange mailbox to send messages.</td>
</tr>
<tr>
<td>Prevent Recent Address syncing</td>
<td>Prevent suggestions for contacts when sending mail in Exchange.</td>
</tr>
<tr>
<td>Prevent Mail Drop</td>
<td>Prevent Apple’s Mail Drop feature from being used.</td>
</tr>
</tbody>
</table>
**Configure Advanced Settings for macOS Exchange**

Enable your macOS devices to retrieve exchange email by configuring advanced settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Exchange Host</td>
<td>The name of the secure server for EAS use. This option and following appear when Native Mail Client is selected.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the number of the port assigned for communication with the Internal Exchange Host.</td>
</tr>
<tr>
<td>Internal Server Path</td>
<td>The location of the secure server for EAS use.</td>
</tr>
<tr>
<td>Use SSL For Internal Exchange Host</td>
<td>Communicate with the Internal Exchange Host by enabling the Secure Socket Layer (SSL).</td>
</tr>
<tr>
<td>External Exchange Host</td>
<td>The name of the external server for EAS use.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the number of the port assigned for communication with the External Exchange Host.</td>
</tr>
<tr>
<td>External Server Path</td>
<td>The location of the external server for EAS use.</td>
</tr>
<tr>
<td>Use SSL For External Exchange Host</td>
<td>Communicate with the External Exchange Host by enabling the Secure Socket Layer (SSL).</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Past Days of Calendar to Sync</td>
<td>Synchronize a selected number of past days on the device calendar.</td>
</tr>
<tr>
<td>Allow Sync Tasks</td>
<td>Allow tasks to sync with device.</td>
</tr>
<tr>
<td>Maximum Email Truncation Size (KB)</td>
<td>Specify the size (in kilobytes) beyond which email messages are truncated when they are synced to the devices.</td>
</tr>
<tr>
<td>Email Signature</td>
<td>Enter the email signature to be displayed on outgoing emails.</td>
</tr>
<tr>
<td>Ignore SSL Errors</td>
<td>Allow devices to ignore SSL errors for Agent processes.</td>
</tr>
</tbody>
</table>

**Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Attachments</td>
<td>Allow attachments with email.</td>
</tr>
<tr>
<td>Maximum Attachment Size</td>
<td>Specify the maximum attachment size in MB.</td>
</tr>
<tr>
<td>Allow Email Forwarding</td>
<td>Allow the forwarding of email.</td>
</tr>
</tbody>
</table>
### Setting Descriptions

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow HTML Format</td>
<td>Specify whether email synchronized to the device can be in HTML format. If this setting is disabled, all email is converted to text.</td>
</tr>
<tr>
<td>Disable screenshots</td>
<td>Disallow screenshot to be taken on the device.</td>
</tr>
<tr>
<td>Sync Interval</td>
<td>Enter the number of minutes between syncs.</td>
</tr>
</tbody>
</table>

#### Peak Days for Sync Schedule

- 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 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.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Next Sync Interval (Min)</strong></td>
<td>Enter the number of minutes between syncs.</td>
</tr>
<tr>
<td><strong>Diagnostic Logging</strong></td>
<td>Select the type of diagnostic logging you want to gather.</td>
</tr>
</tbody>
</table>
| **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. |
### Settings Descriptions

<table>
<thead>
<tr>
<th>Settings</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected Domains</td>
<td>Available only when <strong>Require Data Protection Under Lock</strong> is enabled. Enter the lookup values of the exchange domains that you want to protect. For details, see <strong>Lookup Values on page 201</strong>.</td>
</tr>
<tr>
<td>Allow Email Sync</td>
<td>Allow the syncing of email. Disabling this setting removes access to email through Exchange Active Sync.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Settings</strong></td>
</tr>
<tr>
<td>Next Sync Interval (Min)</td>
<td>Select the frequency, in minutes, that the device syncs with the EAS server.</td>
</tr>
<tr>
<td>Diagnostic Logging</td>
<td>Log information for troubleshooting purposes.</td>
</tr>
</tbody>
</table>

**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.

1. **Add a Wi-Fi resource** by completing the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resource Details</strong></td>
<td></td>
</tr>
<tr>
<td>Resource Name</td>
<td>Name of the profile to be displayed in the Workspace ONE™ UEM console.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the profile that indicates its purpose.</td>
</tr>
<tr>
<td><strong>Connection Info</strong></td>
<td></td>
</tr>
<tr>
<td>Service Set Identifier</td>
<td>Enter an identifier that is associated with the name (SSID) of the desired Wi-Fi network.</td>
</tr>
<tr>
<td>Hidden Network</td>
<td>Enable if the network is not open to broadcast.</td>
</tr>
<tr>
<td>Auto-Join</td>
<td>Setting that directs the device to join the network automatically.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Use the drop-down menu to specify if data transmitted using the Wi-Fi connection is encrypted. Displays based on the <strong>Security Type</strong>.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the email account. Enable the <strong>Show Characters</strong> check box to display the unredacted password.</td>
</tr>
</tbody>
</table>

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** on page 156.
- **Configure Advanced Settings for macOS Wi-Fi** on page 157.
- **Configure Advanced Settings for Android Wi-Fi** on page 157.
- **Configure Advanced Settings for Windows Wi-Fi** on page 158.

3. Click **Next** to proceed to the **Assignment** section.

4. Assign the resource to devices by completing the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assignment Type</strong></td>
<td>Determines how the resource is deployed to devices.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Auto</strong> – The resource is deployed to all devices automatically.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Optional</strong> – 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.</td>
</tr>
<tr>
<td><strong>Managed By</strong></td>
<td>The organization group with administrative access to the resource.</td>
</tr>
<tr>
<td><strong>Assigned Groups</strong></td>
<td>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. For more information, see Assignment Groups on page 67.</td>
</tr>
<tr>
<td><strong>Exclusions</strong></td>
<td>If <strong>Yes</strong> is selected, a new text box <strong>Excluded Groups</strong> displays which enables you to select those groups you want to exclude from the assignment of this resource. See Exclude Groups in Profiles and Policies on page 77 for details.</td>
</tr>
<tr>
<td><strong>View Device Assignment</strong></td>
<td>After you have made a selection in the <strong>Assigned Group</strong> 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.</td>
</tr>
</tbody>
</table>

**Configure Advanced Settings for Wi-Fi Proxy**

Configure advanced Wi-Fi settings to connect devices to Workspace ONE™ UEM using a proxy.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Proxy Type</strong></td>
<td>Choose between <strong>None</strong>, <strong>Manual</strong>, and <strong>Auto</strong>.</td>
</tr>
<tr>
<td><strong>Proxy URL</strong></td>
<td>Available only when <strong>Proxy Type</strong> is <strong>Auto</strong>. Enter the URL of the Wi-Fi proxy that the device uses to connect.</td>
</tr>
<tr>
<td><strong>Allow a direct connection if PAC is unreachable</strong></td>
<td>Available only when <strong>Proxy Type</strong> is <strong>Auto</strong>. Enable if you want to allow the device to connect during times when the proxy auto config file is not accessible.</td>
</tr>
<tr>
<td><strong>Proxy Server</strong></td>
<td>Available only when <strong>Proxy Type</strong> is <strong>Manual</strong>. Enter the name of the proxy server to which your devices connect.</td>
</tr>
</tbody>
</table>
### Configure Advanced Settings for macOS Wi-Fi

Configure advanced Wi-Fi settings to connect your devices to Workspace ONE™ UEM using a proxy.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Server Port</td>
<td>Available only when Proxy Type is Manual. Include the port number of the proxy server through which the device connects to the proxy server.</td>
</tr>
<tr>
<td>Proxy user name</td>
<td>Available only when Proxy Type is Manual. Enter a user name recognized by the proxy server.</td>
</tr>
<tr>
<td>Proxy Password</td>
<td>Available only when Proxy Type is Manual. Enter the password that corresponds to the user name entered.</td>
</tr>
<tr>
<td>Profile</td>
<td>Choose the target of the proxy settings configuration.</td>
</tr>
<tr>
<td>Device</td>
<td>Limit the proxy settings to the specific macOS device</td>
</tr>
<tr>
<td>User</td>
<td>Apply the proxy settings to the user of the macOS device.</td>
</tr>
<tr>
<td>Allow a direct connection if PAC is unreachable</td>
<td>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.</td>
</tr>
<tr>
<td>Proxy Server Port</td>
<td>Available only when Proxy Type is Manual. Include the port number of the proxy server through which the device connects to the proxy server.</td>
</tr>
<tr>
<td>Proxy user name</td>
<td>Available only when Proxy Type is Manual. Enter a user name recognized by the proxy server.</td>
</tr>
<tr>
<td>Proxy Password</td>
<td>Available only when Proxy Type is Manual. Enter the password that corresponds to the user name entered.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include Fusion Settings</td>
<td>Display the main settings for the Fusion feature.</td>
</tr>
</tbody>
</table>
### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Fusion 802.11d / Enable 802.11d</td>
<td>Use an 802.11d wireless specification for operation in additional regulatory domains.</td>
</tr>
<tr>
<td>Set RF Band</td>
<td>Display all the Radio Frequency specification options including 2.4 GHz and 5-GHz channel masking.</td>
</tr>
<tr>
<td>Set 2.4 GHz / Enable 2.4 GHz</td>
<td>Use the 2.4-GHz wireless frequency.</td>
</tr>
<tr>
<td>2.4 GHz Channel Mask</td>
<td>Reduce adjacent channel interference by applying a channel or spectral mask around the 2.4-GHz frequency.</td>
</tr>
<tr>
<td>Set 5 GHz / Enable 5 GHz</td>
<td>Use the 5-GHz wireless frequency.</td>
</tr>
<tr>
<td>5 GHz Channel Mask</td>
<td>Reduce adjacent channel interference by applying a channel or spectral mask around the 5-GHz frequency.</td>
</tr>
</tbody>
</table>

### Proxy

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Manual Proxy</td>
<td>Display the proxy server settings.</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>Enter the proxy domain name.</td>
</tr>
<tr>
<td>Proxy Server Port</td>
<td>Enter the port number to be used by the proxy server.</td>
</tr>
<tr>
<td>Exclusion List</td>
<td>Enter hostnames that are not routed through the proxy. Use an asterisk as a wildcard for the domain. For example, *.air-watch.com.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy</td>
<td>Enable the use of a proxy to connect your Windows devices to Workspace ONE UEM.</td>
</tr>
<tr>
<td>URL</td>
<td>Available only when Proxy is enabled. Enter the URL of the Wi-Fi proxy that the device uses to connect.</td>
</tr>
<tr>
<td>Port</td>
<td>Available only when Proxy is enabled. Include the port number of the proxy server through which the device connects to the proxy server.</td>
</tr>
</tbody>
</table>

### 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.
1. Add a **VPN** resource by completing the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resource Details</strong></td>
<td></td>
</tr>
<tr>
<td>Resource Name</td>
<td>Name of the profile to be displayed in the Workspace ONE™ UEM console.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the profile that indicates its purpose.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connection Info</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Type</td>
<td>Select the type of secure connection from the drop-down listing.</td>
</tr>
<tr>
<td>Server</td>
<td>Enter the server URL.</td>
</tr>
</tbody>
</table>

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 on page 159
   - Configure Advanced Settings for Android VPN on page 161
   - Configure Advanced Settings for Windows Phone VPN on page 162

3. Click **Next** to proceed to the **Assignment** section.

4. Assign the resource to devices by completing the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assignment Type</strong></td>
<td>Determines how the resource is deployed to devices.</td>
</tr>
<tr>
<td>Auto</td>
<td>The resource is deployed to all devices automatically.</td>
</tr>
<tr>
<td>Optional</td>
<td>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.</td>
</tr>
<tr>
<td>Managed By</td>
<td>The organization group with administrative access to the resource.</td>
</tr>
<tr>
<td>Assigned Groups</td>
<td>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. For more information, see Assignment Groups on page 67.</td>
</tr>
<tr>
<td>Exclusions</td>
<td>If <strong>Yes</strong> is selected, a new text box <strong>Excluded Groups</strong> displays which enables you to select those groups you want to exclude from the assignment of this resource. See Exclude Groups in Profiles and Policies on page 77 for details.</td>
</tr>
<tr>
<td>View Device Assignment</td>
<td>After you have made a selection in the <strong>Assigned Group</strong> 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.</td>
</tr>
</tbody>
</table>

### 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.
<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account</strong></td>
<td>Enter the name of the VPN account.</td>
</tr>
<tr>
<td><strong>Disconnect on Idle (min)</strong></td>
<td>Allow the VPN to auto-disconnect after a specific amount of time. Support for this value depends on the VPN provider.</td>
</tr>
<tr>
<td><strong>Send All Traffic</strong></td>
<td>Select to force all traffic through the specified network.</td>
</tr>
<tr>
<td><strong>Per App VPN Rules</strong></td>
<td>Select to enable and configure Per App VPN rules.</td>
</tr>
<tr>
<td><strong>Connect Automatically</strong></td>
<td>Select to allow the VPN to connect automatically to Safari Domains. This option appears when the Per App VPN Rules check box is selected.</td>
</tr>
<tr>
<td><strong>Provider Type</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Safari Domains</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>User Authentication</strong></td>
<td>Authenticate end users by either uploading a Certificate or by requiring a Password for VPN access.</td>
</tr>
<tr>
<td><strong>Group Name</strong></td>
<td>Enter the Workspace ONE™ UEM group name.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Available only when User Authentication is set to Password. Enter the password for the Workspace ONE UEM Group Name.</td>
</tr>
<tr>
<td><strong>Identity Certificate</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Enable VPN On Demand</strong></td>
<td>This setting is only available when User Authentication is set to Certificate. Enable VPN On Demand to use certificates to establish VPN connections automatically.</td>
</tr>
<tr>
<td><strong>Use new On-Demand keys</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Match Domain or Host</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>On-Demand Action</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Proxy</strong></td>
<td>Select among None, Manual, and Auto.</td>
</tr>
</tbody>
</table>
### Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Server</td>
<td>Available only when Proxy is Auto. Enter the URL of the Wi-Fi proxy that the device uses to connect.</td>
</tr>
<tr>
<td>Auto Config URL</td>
<td>Server Available only when Proxy is Manual. Enter the name of the proxy server to which your devices connect.</td>
</tr>
<tr>
<td>Port</td>
<td>Available only when Proxy is Manual. Include the port number of the proxy server through which the device connects to the proxy server.</td>
</tr>
<tr>
<td>User name</td>
<td>Available only when Proxy is Manual. Enter a user name recognized by the proxy server.</td>
</tr>
<tr>
<td>Password</td>
<td>Available only when Proxy is Manual. Enter the password that corresponds to the user name entered.</td>
</tr>
</tbody>
</table>

### Vendor Configurations

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Keys</td>
<td>Create custom keys using the vendor config dictionary.</td>
</tr>
<tr>
<td>Key</td>
<td>Enter the specific key provided by the vendor.</td>
</tr>
<tr>
<td>Value</td>
<td>Enter the VPN value for each key.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>Identify Certificate</td>
<td>Enter the certificate credentials used to authenticate the connection by selecting Add a Certificate.</td>
</tr>
<tr>
<td>Credential Source</td>
<td>Select the source of the credentials. Select between Upload, Defined Certificate Authority, and User Certificate.</td>
</tr>
<tr>
<td>Credential Name</td>
<td>Available when Credential Source is set to Upload. Enter the name of the uploaded credential.</td>
</tr>
<tr>
<td>Certificate</td>
<td>Available when Credential Source is set to Upload. Click Upload to select a certificate file from your device.</td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>Available when Credential Source is set to Defined Certificate Authority. Select the certificate authority from a drop-down listing.</td>
</tr>
<tr>
<td>Certificate Template</td>
<td>Available when Credential Source is set to Defined Certificate Authority. This setting auto-populates based on your selection in the Certificate Authority setting.</td>
</tr>
<tr>
<td>S/MIME</td>
<td>Available when Credential Source is set to User Certificate. Select between the user-centric S/MIME Signing certificate or S/MIME Encryption certificate.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Enable VPN On Demand</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable VPN On Demand</td>
<td>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.</td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection Info</strong></td>
<td></td>
</tr>
<tr>
<td>Advanced Connection Settings</td>
<td>Configure advanced routing rules for device VPN connections.</td>
</tr>
<tr>
<td>Routing Addresses</td>
<td>Select <strong>Add</strong> to enter the IP Addresses and Subnet Prefix Size for the VPN connection. You can add additional routing addresses as needed. Available when <strong>Advanced Connection Settings</strong> is enabled.</td>
</tr>
<tr>
<td>DNS Routing Rules</td>
<td>Select <strong>Add</strong> to enter the <strong>Domain Name</strong> on which the VPN server is hosted. Enter the <strong>Domain Name</strong>, <strong>DNS Servers</strong>, and <strong>Web Proxy Servers</strong> for each specific domain. Available when <strong>Advanced Connection Settings</strong> is enabled.</td>
</tr>
<tr>
<td>Routing Policy</td>
<td>Allow traffic to use the local network connection by selecting <strong>Allow Direct Access to External Resources</strong>. Conversely, select <strong>Force All Traffic Through VPN</strong> to send all traffic through the VPN. Available when <strong>Advanced Connection Settings</strong> is enabled.</td>
</tr>
<tr>
<td>Proxy</td>
<td>Select <strong>Auto Detect</strong> to detect any proxy servers used by the VPN automatically. Select <strong>Manual</strong> to configure the proxy server. Available when <strong>Advanced Connection Settings</strong> is enabled.</td>
</tr>
<tr>
<td>Proxy Auto Config URL</td>
<td>Enter the URL for the proxy auto config. Available only when <strong>Proxy</strong> is set to Auto Detect.</td>
</tr>
<tr>
<td>Server</td>
<td>Enter the URL for the proxy server configuration settings.</td>
</tr>
<tr>
<td></td>
<td>Displays when <strong>Proxy</strong> is set to Manual</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number used to access the proxy server.</td>
</tr>
<tr>
<td></td>
<td>Displays when <strong>Proxy</strong> is set to Manual</td>
</tr>
<tr>
<td>Bypass proxy for local</td>
<td>Bypass the proxy server when the device detects it is on the local network.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Select the authentication protocol for the VPN.</td>
</tr>
<tr>
<td></td>
<td>• EAP – Allows for various authentication methods.</td>
</tr>
<tr>
<td></td>
<td>• Machine Certificate – Detects a client certificate in the device certificate store to use for authentication.</td>
</tr>
<tr>
<td>Protocols</td>
<td>Select the type of EAP authentication.</td>
</tr>
<tr>
<td></td>
<td>• EAP-TLS – Smart Card or client certificate authentication.</td>
</tr>
<tr>
<td></td>
<td>• EAP-MSCHAPv2 – User name and Password.</td>
</tr>
<tr>
<td>Settings</td>
<td>Descriptions</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Credential Type</td>
<td>Select <strong>Use Certificate</strong> to use a client certificate. Select <strong>Use Smart Card</strong> to use a Smart Card to authenticate. Displays when the <strong>Protocols</strong> option is set to <strong>EAP-TLS</strong>.</td>
</tr>
<tr>
<td>Simple Certificate Selection</td>
<td>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 <strong>Protocols</strong> option is set to <strong>EAP-TLS</strong>.</td>
</tr>
<tr>
<td>Use Windows login Credentials</td>
<td>Use the same credentials as the Windows device. Displays when the <strong>Protocols</strong> option is set to <strong>EAP-MSCHAPv2</strong>.</td>
</tr>
<tr>
<td><strong>VPN Traffic Rules</strong></td>
<td></td>
</tr>
</tbody>
</table>
| 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_htcwk4rx2gx4 |
| 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. |
<table>
<thead>
<tr>
<th>Settings</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remember Credentials</strong></td>
<td>Remember the end user's login credentials.</td>
</tr>
<tr>
<td><strong>Always On</strong></td>
<td>Force the VPN connection on, which activates the VPN connection when the network connection disconnects and reconnects.</td>
</tr>
<tr>
<td><strong>VPN Lockdown</strong></td>
<td>Force the VPN on, disable any network access if the VPN is not connected, and prevent a connection or modification to other VPN profiles.</td>
</tr>
<tr>
<td><strong>Trusted Network</strong></td>
<td>Enter trusted network addresses separated by commas. The VPN does not connect when a trusted network connection is detected.</td>
</tr>
<tr>
<td><strong>Split Tunnel</strong></td>
<td>Allow end users to use a split tunnel VPN. This text box applies to Windows Phone 8.1 devices only.</td>
</tr>
<tr>
<td><strong>Bypass for Local</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Trusted Network Detection</strong></td>
<td>Use Trusted Network Detection when connecting to the VPN. This text box applies to Windows Phone 8.1 devices only.</td>
</tr>
<tr>
<td><strong>Connection Type</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Idle Disconnection Time</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

**VPN On Demand**

<p>| <strong>Allows Apps</strong> | Select <strong>Add</strong> to define apps to have all their traffic secured over the VPN. You can add as many apps as you like. |
| <strong>Allowed Networks</strong> | Select <strong>Add</strong> to define networks. All traffic over configured networks is secured over the VPN. You can add as many networks as you like. |
| <strong>Excluded Apps</strong> | Select <strong>Add</strong> 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. |
| <strong>Excluded Networks</strong> | Select <strong>Add</strong> 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. |</p>
<table>
<thead>
<tr>
<th>Settings</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Suffix Search List</td>
<td>Select <strong>Add</strong> to define the DNS Suffix Search List.</td>
</tr>
<tr>
<td></td>
<td>DNS suffixes are appended to shortened URLs for DNS resolution and connectivity.</td>
</tr>
<tr>
<td></td>
<td>You can add as many DNS suffixes as you like.</td>
</tr>
</tbody>
</table>
Chapter 12: Compliance Policies

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 involves a five-step procedure.

- **Choosing 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.

- **Building your policies** – Customize your policy to cover everything from an application list, compromised status, encryption, manufacturer, model and OS version, passcode and roaming.

- **Defining escalation** – Configure time-based actions in minutes, hours, or days and take a tiered approach to those actions.
• **Specifying 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.

• **Configuring assignments** – Assign your compliance policy by organization group or smart group then confirm the assignment by device.

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Filter the listing between All, Active and Inactive statuses.</td>
</tr>
<tr>
<td>Actions Menu</td>
<td>View and edit individual policies, view devices to which the policy has been assigned, and delete policies you no longer want to keep.</td>
</tr>
<tr>
<td>Compliant / NonCompliant / Pending / Assigned</td>
<td>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 on page 167.</td>
</tr>
</tbody>
</table>

**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.

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.

<table>
<thead>
<tr>
<th>Compliance Policy</th>
<th>Android</th>
<th>Apple</th>
<th>Apple macOS</th>
<th>Chrome OS</th>
<th>QNX</th>
<th>Windows Rugged</th>
<th>Windows 7</th>
<th>Windows Phone</th>
<th>Windows Desktop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application List</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antivirus Status</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cell Data Usage</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cell Message Usage</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cell Voice Usage</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance Attribute</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Compromised Status</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Last Seen</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Device Manufacturer</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Firewall Status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Free Disk Space</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iBeacon Area</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interactive Certificate Profile Expiry</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Compromised Scan</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDM Terms of Use Acceptance</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Model</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS Version</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Passcode</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Roaming *</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Roaming Cell Data Usage *</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Patch Version</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIM Card Change *</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Automatic Update Status</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Copy Genuine Validation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application List</td>
<td>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.</td>
</tr>
<tr>
<td>Antivirus Status</td>
<td>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.</td>
</tr>
<tr>
<td>Cell Data/Message/Voice Use</td>
<td>Detect when end-user devices exceed a particular threshold of their assigned telecom plan. For this policy to take effect Telecom must be configured.</td>
</tr>
<tr>
<td>Compliance Attribute***</td>
<td>Compare attribute keys in the device against third-party endpoint security, which returns a Boolean value representing device compliance.</td>
</tr>
<tr>
<td>Compromised Status</td>
<td>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.</td>
</tr>
<tr>
<td>Device Last Seen</td>
<td>Detect if the device fails to check in within an allotted time window.</td>
</tr>
<tr>
<td>Device Manufacturer</td>
<td>Detect the device manufacturer allowing you to identify certain Android devices. You can specifically prohibit certain manufacturers or permit only the manufacturers you specify.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Detect whether or not encryption is enabled on the device.</td>
</tr>
<tr>
<td>Firewall Status</td>
<td>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.</td>
</tr>
<tr>
<td>Free Disk Space</td>
<td>Detect the available storage space on the device.</td>
</tr>
<tr>
<td>iBeacon Area</td>
<td>Detect whether your iOS device is within the area of an iBeacon Group.</td>
</tr>
<tr>
<td>Interactive Certificate Profile Expiry</td>
<td>Detect when an installed profile on the device expires within the specified length of time.</td>
</tr>
</tbody>
</table>

💡 For more information about compromised device detection using VMware, see the following Knowledge Base articles: https://support.airwatch.com/articles/115001662748 and https://support.airwatch.com/articles/115001662508.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Compromised Scan</td>
<td>Detect if the device has not reported its compromised status within the specified schedule.</td>
</tr>
<tr>
<td>MDM Terms of Use Acceptance</td>
<td>Detect if the end user has not accepted the current MDM Terms of Use within a specified length of time.</td>
</tr>
<tr>
<td>Model</td>
<td>Detect the device model. You can specifically prohibit certain models or permit only the models you specify.</td>
</tr>
<tr>
<td>OS Version</td>
<td>Detect the device OS version. You can prohibit certain OS versions or permit only the operating systems and versions you specify.</td>
</tr>
<tr>
<td>Passcode</td>
<td>Detect whether a passcode is present on the device.</td>
</tr>
<tr>
<td>Roaming*</td>
<td>Detect if the device is roaming.</td>
</tr>
<tr>
<td>Roaming Cell Data Use*</td>
<td>Detect roaming cell data use against a static amount of data measured in MB or GB.</td>
</tr>
<tr>
<td>Security Patch Version**</td>
<td>Detect the date of the Android device's most recent security patch from Google.</td>
</tr>
<tr>
<td>SIM Card Change*</td>
<td>Detect if the SIM card has been replaced.</td>
</tr>
<tr>
<td>Windows Automatic Update Status</td>
<td>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.</td>
</tr>
<tr>
<td>Windows Copy Genuine Validation</td>
<td>Detect whether the copy of Windows currently running on the device is genuine.</td>
</tr>
</tbody>
</table>

* Only available for Telecom Advanced Users.

** Only available for Android version 6.0 and later.

*** Only available for Windows Desktop devices.
### Compliance Policies Actions by Platform

The supported actions by platform, enforced by compliance policies, are as follows.

<table>
<thead>
<tr>
<th>Compliance Policy Action</th>
<th>Android</th>
<th>Apple iOS</th>
<th>Apple macOS</th>
<th>Chrome OS</th>
<th>QNX</th>
<th>Windows Rugged</th>
<th>Windows 7</th>
<th>Windows Phone</th>
<th>Windows Desktop</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block/Remove Managed App</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block/Remove All Apps</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Command</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Roaming Settings</td>
<td>✓</td>
<td>(iOS 5+)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Wipe</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Enterprise Reset</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS Updates</td>
<td>✓</td>
<td>(DEP only)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request Device Check-In</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revoke Azure Tokens*</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block Email</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Notify</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send Email to User**</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Send SMS to Device</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send Push Notification to Device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send Email to Administrator</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Profile</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install Compliance Profile</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block/Remove Profile</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block/Remove Profile Type</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block/Remove All Profiles</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* 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.

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.
   - 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 on page 172.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mark as Not Compliant check box</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• The Mark as Not Compliant check box is enabled (checked) by default for each newly added Action.</td>
</tr>
<tr>
<td></td>
<td>• If one action has the Mark as Not Compliant option enabled (checked), then all subsequent actions and escalations are also marked as non compliant (checked). These subsequent check boxes cannot be edited.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td><strong>Application</strong></td>
<td>Block or remove a managed application. You can enforce application compliance by establishing a whitelist, blacklist, or required list of applications.</td>
</tr>
<tr>
<td><strong>Command</strong></td>
<td>Initiate a device check-in or run an enterprise wipe.</td>
</tr>
</tbody>
</table>

VMware AirWatch Mobile Device Management Guide | v.2018.09 | September 2018

Copyright © 2018 VMware, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>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 &gt; Compliance Policies &gt; 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.</td>
</tr>
<tr>
<td>Notify</td>
<td>Notify someone about the compliance violation. You have the following options to send a notification.</td>
</tr>
<tr>
<td></td>
<td>- Send Email to User.</td>
</tr>
<tr>
<td></td>
<td>- Send SMS to Device.</td>
</tr>
<tr>
<td></td>
<td>- Send Push Notification to Device.</td>
</tr>
<tr>
<td></td>
<td>- Send Email to Administrator.</td>
</tr>
<tr>
<td></td>
<td>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 on page 201.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Profile</td>
<td>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 &gt; Profiles &amp; Resources &gt; 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.</td>
</tr>
</tbody>
</table>

---

**Escalations Only**

<table>
<thead>
<tr>
<th>Add Escalation button</th>
<th>Creates an escalation. When adding escalations, it is a best practice to increase the security of actions with each additional escalation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>After time Interval...</td>
<td>You can delay the escalation by minutes, hours, or days.</td>
</tr>
<tr>
<td>...Perform the following actions</td>
<td>Repeat – Enable this check box to repeat the escalation a selected number of times before the next scheduled action begins.</td>
</tr>
</tbody>
</table>
For macOS, you can only perform the following actions:

**Tip:** Query non-compliant iOS 7+ devices to decrease the delay between when a user makes their device compliant and when Workspace ONE UEM detects that change. Set this sample by navigating to **Groups & Settings > Settings > Devices & Users > Apple > MDM Sample Schedule** and setting the **Non-Compliant Device Sample**.

<table>
<thead>
<tr>
<th>MDM Agent Sample</th>
<th>12</th>
<th>hour(s)</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Non-Compliant Device Sample</strong></td>
<td>2</td>
<td>hour(s)</td>
<td>1</td>
</tr>
</tbody>
</table>

VMware can query non-compliant device more frequently, to decrease the delay between when a user has taken actions to make their device compliant and when AirWatch detects that action. Please consider that lowering this setting can have a negative effect on the performance of your system, depending on the number of non-compliant devices in your environment.

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.

You can then name, finalize, and activate the policy with the Summary tab.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed By</td>
<td>Select the organization group by which this compliance policy is managed.</td>
</tr>
<tr>
<td>Assigned Groups</td>
<td>Assign to this policy one or more groups. For more information, see <strong>Assignment Groups on page 67</strong>.</td>
</tr>
<tr>
<td>Exclusions</td>
<td>If you want to exclude groups, select Yes. Next, select from the available listing of groups in the <strong>Excluded Groups</strong> text box. See <strong>Exclude Groups in Profiles and Policies on page 77</strong>.</td>
</tr>
<tr>
<td>View Device Assignment button</td>
<td>See a listing of devices affected by this compliance policy assignment.</td>
</tr>
</tbody>
</table>

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.
   - Provide a **Name** and a useful **Description** of the compliance policy.
   - Select one of the following:
     - **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.
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.
Chapter 13: Device Tags

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.

Filter Devices by Tag

You can use the filter feature in the Device List View to show only devices with specific tags.

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. 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

You can create tags to help identify a device in a more visible way than by friendly naming, device profiles, smart groups, or compliance policies. Create a tag in the Device List View.
1. Navigate to Devices > List View.

2. Select a device using the check box to the left of the device listing.

3. Select More and select Add Tag from the drop-down menu. The Tag Assignment page appears.

4. Select NEW TAG.

5. Enter the Name of the new tag and select a Color.

6. Select Add to save the tag.

Alternatively, you can create a tag by navigating to Groups & Settings.

1. Navigate to Groups & Settings > All Settings > Devices & Users > Advanced > Tags.

2. Select the Organization Group to which you want the tag to belong and then select Add.

3. In the Add Tag page, enter the Name of the tag.

4. Select the Type of tag you want to add. General or Device.

5. Select Save.

Add Tags

You can add tags to a device to identify it without using notes, profiles, policies, or giving the device a special friendly name.

Add Tags to a Single Device

For when you have to make a quick one-off adjustment of a device's tags, you can add one or more tags to a single device easily.

1. Navigate to Devices > List View and select the device you want to tag. You can select a single device in either of the two ways to display the Send and More Actions buttons.
   - Display the Details View by selecting the device from the listing.
   - Select the check box next to the device.

2. Select the More Actions button and then select Add 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.

4. Select Save to apply one or more tags to the device.

Add Tags to Multiple Devices

You can add a tag (or multiple tags) to one or more devices. Adding multiple tags to multiple devices saves time.
1. Navigate to Devices > List View.
2. Select the check box of each device you want to tag.
3. Select More Actions and then select Add 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 to apply one or more tags to the devices.

Are you looking for granting permissions as part of an admin role that includes (or excludes) the ability to add a tag to a device? See View the Resources of an Admin Role.

Manage Tags

Once you accrue several device tags, you can edit existing tags, remove tags from devices, and delete unused tags.

Edit a Tag

You can edit an existing tag for when you want to rename a tag or change its type and the color of its marker.

1. Navigate to Groups & Settings > All Settings > Devices & Users > Advanced > Tags and select the edit button or the name of the tag which you want to edit. Only the tags that are part of a child organization group and the organization group currently selected are editable.
2. Make your changes to the Name and Type settings per your preferences.
3. Select Save.

Remove a Tag

If an assigned tag no longer applies to the device, you can remove a tag from (or 'untag') a device.

1. Navigate to the device Details View.
2. Select the Summary tab and scroll to the bottom of the Device Info page, where you can find all the tags currently assigned to the device.
3. Select X next to each tag you want to remove.

**Important:** Removing a tag from a device (or 'untagging' a device) is not the same thing as deleting a tag.

Delete a Tag

If a tag is not assigned to any device and it no longer serves a purpose, you can delete it.

1. Navigate to Groups & Settings > All Settings > Devices & Users > Advanced > Tags.
2. Select X next to the tag you want to delete.
Chapter 14: Managing Devices

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 Hub 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.

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**

Select Devices > List View to see a full listing of all devices in the currently selected organization group.

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>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.</td>
</tr>
<tr>
<td>Ownership</td>
<td>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.</td>
</tr>
<tr>
<td>Smart Groups</td>
<td>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.</td>
</tr>
<tr>
<td>User Groups</td>
<td>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.</td>
</tr>
<tr>
<td>Device Type</td>
<td>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.</td>
</tr>
<tr>
<td>Security</td>
<td>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.</td>
</tr>
<tr>
<td>Status</td>
<td>Enrollment Status Select from among Enrolled, Enterprise Wipe Pending, Device Wipe Pending, Unenrolled, or All of the above. 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.</td>
</tr>
<tr>
<td>Advanced</td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Filter by the media access control address of a device.</td>
</tr>
<tr>
<td>IP Range</td>
<td>Filter devices by their currently-assigned internet protocol address. Enter IP addresses in the <strong>IP Range Start</strong> and <strong>IP Range End</strong> 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.</td>
</tr>
<tr>
<td>Tags</td>
<td>View devices by their assigned tags for which you can search and select from a drop-down menu.</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Select between showing all devices, showing devices connected to the tunnel, and devices not connected to the tunnel.</td>
</tr>
<tr>
<td>Content Compliance</td>
<td>Select between showing all devices, showing only those devices missing required docs, and only those devices lacking the latest version of required content.</td>
</tr>
<tr>
<td>Lost Mode</td>
<td>View all devices or only devices with Lost Mode enabled. Applicable to iOS devices only.</td>
</tr>
</tbody>
</table>

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. To add a device from **Devices > List View** or **Devices > Lifecycle > Enrollment Status**, take the following steps.
1. Select the **Add Device** button. The **Add Device** page displays. Complete the following in the **User** tab.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User</strong></td>
<td></td>
</tr>
<tr>
<td>Search Text</td>
<td>Each device must be assigned to a user. Search for a user with this text box by entering search parameters and select the <strong>Search User</strong> button. You can select a user from among the search results or select the link <strong>Create New User</strong>.</td>
</tr>
<tr>
<td><strong>Create New User</strong></td>
<td></td>
</tr>
<tr>
<td>Security Type</td>
<td>Select between <strong>Basic</strong> and <strong>Directory</strong> users. For more information, see <strong>Basic User Authentication</strong> on page 36 and <strong>Active Directory with LDAP Authentication</strong> on page 37.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name by which your user is identified in your Workspace ONE™ UEM environment.</td>
</tr>
<tr>
<td>Password, Confirm Password</td>
<td>Enter and confirm the password that corresponds to the user name.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Enter the email address for the user account.</td>
</tr>
<tr>
<td>Enrollment Organization Group</td>
<td>The organization group (OG) that serves as the enrollment OG for the device enrollment.</td>
</tr>
<tr>
<td>Show advanced user details</td>
<td>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 <strong>User Role</strong> for the user you are adding which determines which permissions the user has while using a connected device. For more information, see <strong>User Roles on page 58</strong>.</td>
</tr>
<tr>
<td><strong>Device</strong></td>
<td></td>
</tr>
<tr>
<td>Expected Friendly Name</td>
<td>Enter the name of the device that appears in the device list view. You can also incorporate lookup values. For details, see <strong>Lookup Values on page 201</strong>.</td>
</tr>
<tr>
<td>Organization Group</td>
<td>Select the organization group from the drop-down menu with which the device is to be associated.</td>
</tr>
<tr>
<td>Ownership</td>
<td>Select the device ownership from the drop-down menu. Select between <strong>None</strong>, <strong>Corporate - Dedicated</strong>, <strong>Corporate - Shared</strong>, and <strong>Employee-Owned</strong>.</td>
</tr>
<tr>
<td>Platform</td>
<td>Select the platform of the device from the drop-down menu.</td>
</tr>
<tr>
<td>Show advanced device information options</td>
<td>Display all the advanced device information settings.</td>
</tr>
<tr>
<td><strong>Advanced Device Information Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Model</td>
<td>Select the device model from the drop-down listing. The contents of this drop-down menu depend upon the selection made in the <strong>Platform</strong> drop-down menu.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OS</td>
<td>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 <strong>Platform</strong> drop-down menu.</td>
</tr>
<tr>
<td>UDID</td>
<td>Enter the device's Unique Device Identifier.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Enter the device's serial number.</td>
</tr>
<tr>
<td>IMEI</td>
<td>Enter the device's 15-digit International Mobile Station Equipment Identity.</td>
</tr>
<tr>
<td>SIM</td>
<td>Enter the device's SIM card specifications.</td>
</tr>
<tr>
<td>Asset Number</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Messaging**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Type</td>
<td>Select the type of message you want to send (<strong>None</strong>, <strong>SMS</strong>, or <strong>Email</strong>) to the device upon a successful enrollment to the Workspace ONE UEM environment.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Enter the email address to which you want the enrollment message sent. This text box is only available when Email is selected as the <strong>Message Type</strong>.</td>
</tr>
<tr>
<td>Email Message Template</td>
<td>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.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>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 <strong>Message Type</strong>.</td>
</tr>
<tr>
<td>SMS Message Template</td>
<td>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.</td>
</tr>
</tbody>
</table>

2. Optionally assign **Custom Attributes** to the device. Select the **Add** button and supply an **Attribute** and its **Value**.

3. Optionally 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.

4. 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.

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.

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.

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 on page 188.

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.

🔗 To watch a video about Selecting Devices and Bulk actions, go to [https://support.air-watch.com/articles/115001664748](https://support.air-watch.com/articles/115001664748).

**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.

- **Required Content** – Displays content marked as 'Required' by the administrator in the Workspace ONE UEM Managed Repository. Select **View Content Management Pages** for details.

- **Certifications** – Displays all installed certificates, including certifications near their expiration date.

- **Admin Applications** – Displays the installed AirWatch Agent 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.

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. See Device Actions by Platform on page 1 for a full listing of remote actions an admin can invoke using the Console.

Device Details Menu Tabs

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

<table>
<thead>
<tr>
<th>Menu Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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 (i) 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. |
<p>| Required 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). |</p>
<table>
<thead>
<tr>
<th>Menu Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Location</strong></td>
<td>View current location or location history of a device. Select the <strong>Period</strong> or length of time you are looking back in <strong>Search</strong> 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 <strong>Groups &amp; Settings &gt; All Settings &gt; Devices &amp; Users</strong> and selecting the platform-specific <strong>Agent Settings</strong> page. For more information about location data as it relates to privacy, see <strong>GPS Coordinates for Privacy Best Practices on page 28</strong>. Edit the number of location data points collected and the minimum distance between locations by navigating to <strong>Groups &amp; Settings &gt; All Settings &gt; Installation &gt; Maps</strong>.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>Access details about the user of a device and the status of the other devices enrolled to this user.</td>
</tr>
<tr>
<td><strong>More</strong></td>
<td>These additional menu tabs vary based on the device platform.</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>View current network information (Cellular, Wi-Fi, Bluetooth, IMEI) of a device.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>View current security status of a device based on security settings.</td>
</tr>
<tr>
<td><strong>Telecom</strong></td>
<td>View amounts of calls, data, and messages sent and received.</td>
</tr>
<tr>
<td><strong>Notes</strong></td>
<td>View and add notes regarding the device. For example, note the shipping status or if the device is in repair and out of commission.</td>
</tr>
<tr>
<td><strong>Certificates</strong></td>
<td>Identify device certificates by name and issuant. This tab also provides certificate expiration dates.</td>
</tr>
<tr>
<td><strong>Provisioning</strong></td>
<td>View complete history and status of all packages provisioned to the device and any provisioning errors.</td>
</tr>
<tr>
<td><strong>Terms of Use</strong></td>
<td>View a list of End-User License Agreements (EULAs) which have been accepted during enrollment.</td>
</tr>
</tbody>
</table>
Menu Tab | Description
--- | ---
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 on page 194**.

<table>
<thead>
<tr>
<th>Action</th>
<th>Android</th>
<th>Apple iOS</th>
<th>macOS</th>
<th>Apple TV</th>
<th>Chrome OS</th>
<th>QNX</th>
<th>Windows Rugged</th>
<th>Win 7</th>
<th>Windows Phone</th>
<th>Windows Desktop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Tag</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>AirWatch Agent (Query)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>(*)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>App Remote View</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Apps (Query)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>(*)</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Books (Query)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Cancel Log Request</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>(✓)</td>
</tr>
<tr>
<td>Certificates (Query)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>(✓)</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Android</td>
<td>Apple iOS</td>
<td>macOS</td>
<td>Apple TV</td>
<td>Chrome OS</td>
<td>QNX</td>
<td>Windows Rugged</td>
<td>Win 7</td>
<td>Windows Phone</td>
<td>Windows Desktop</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------</td>
<td>-----------</td>
<td>-------</td>
<td>----------</td>
<td>-----------</td>
<td>-----</td>
<td>----------------</td>
<td>-------</td>
<td>---------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Change Device Passcode</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Change Organization Group</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Change Ownership</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Clear Activation Lock</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Clear Passcode (Device)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Clear Passcode (Container)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Clear Passcode (Restrictions Setting)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Delete Device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Device Information (Query)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Device Wipe</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Edit Device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Enable/Disable Lost Mode</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Enroll</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Enterprise Reset</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Enterprise Wipe</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>File Manager</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Find Device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>iOS Update</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Location</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lock Device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lock SSO</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Managed Settings</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mark Do Not Disturb</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Override Job Log Level</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Profiles (Query)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Provision Now</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Query All</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Reboot Device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Registry Manager</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Remote Control</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Remote Management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Remote View</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Rename Device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Request Debug Log</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Request Device Check-In</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Request Device Location</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Restart AirWatch Agent</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
### 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.
- **AirWatch Agent (Query)** – Send a query command to the device's AirWatch Agent 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.
- **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.

(*) 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.

---

<table>
<thead>
<tr>
<th>Action</th>
<th>Android</th>
<th>Apple iOS</th>
<th>macOS</th>
<th>Apple TV</th>
<th>Chrome OS</th>
<th>QNX</th>
<th>Windows Rugged</th>
<th>Win 7</th>
<th>Windows Phone</th>
<th>Windows Desktop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security (Query)</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td>(*)</td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Send Message</td>
<td>✔ ✔</td>
<td>✔</td>
<td></td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td></td>
<td>✔</td>
<td>✔ ✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Start AirPlay</td>
<td></td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Start AWCM</td>
<td>✔ ✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Stop AWCM</td>
<td>✔ ✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Sync Device</td>
<td>✔ ✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Task Manager</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>View Manifest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Warm Boot</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
• **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 UEM console. This action performs an Enterprise Wipe and remove its representation in the UEM 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.
  - 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.

• **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 AirWatch Agent. 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 Agent 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 Agent 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 AirWatch Agent, 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.

• **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.

• **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**. The log is delivered as a text file that can be used to troubleshoot and provide support.

• **Request Device Check-In** – Request that the selected device check itself in to the UEM console. This action updates the **Last Seen** column status.
Chapter 14: Managing Devices

- **Restart AirWatch Agent** – Restart the AirWatch Agent. 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filters</td>
<td>You can filter out entire device categories by using filters which enable you to see only those devices that you are interested in.</td>
</tr>
<tr>
<td></td>
<td>• Enrollment Status</td>
</tr>
<tr>
<td></td>
<td>• Platform</td>
</tr>
<tr>
<td></td>
<td>• Ownership</td>
</tr>
<tr>
<td></td>
<td>• Token Status</td>
</tr>
<tr>
<td></td>
<td>• Token Type</td>
</tr>
<tr>
<td></td>
<td>• Source</td>
</tr>
<tr>
<td></td>
<td>• First Seen</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Add</td>
<td>• <strong>Register Device</strong> – You can register or Add a single device to be enrolled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Whitelist or Blacklist Devices</strong> – 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Batch Import</strong> – Import multiple devices or multiple users with the Batch Import screen.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <em>Add a Device from List View on page 184</em>, <em>Add a Blacklisted or Whitelisted Device on page 122</em>, and <em>Batch Import Users or Devices on page 51</em>.</td>
</tr>
<tr>
<td>Resend Message</td>
<td>Resend the original message sent to a user, including Self-Service Portal URL, Group ID, and login credentials.</td>
</tr>
<tr>
<td>More Actions</td>
<td></td>
</tr>
<tr>
<td>Change Organization</td>
<td>Move the selected device to the organization group of your choosing.</td>
</tr>
<tr>
<td>Group</td>
<td></td>
</tr>
<tr>
<td>Change Ownership</td>
<td>Change the type of ownership for the selected device.</td>
</tr>
<tr>
<td>Delete</td>
<td>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.</td>
</tr>
<tr>
<td>Reset Token</td>
<td>Reset the status of a token if it has been revoked or is expired.</td>
</tr>
<tr>
<td>Revoke Token</td>
<td>Force the registration token status of selected devices to expire, essentially blocking access for unwanted users or devices.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Selecting Multiple</td>
<td>Act on individual devices or multiple devices by selecting the check box next to each device and using the action buttons.</td>
</tr>
<tr>
<td>Devices</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>When you select an action for one or more devices, a confirmation screen displays allowing you to Save or Cancel the action.</td>
</tr>
<tr>
<td>Layout</td>
<td>Display the full listing of visible columns or choose to display or hide columns per your preferences by selecting the Custom option.</td>
</tr>
<tr>
<td></td>
<td>There is also an option to apply your customized column view to all administrators at or below the current organization group.</td>
</tr>
<tr>
<td></td>
<td>You can return to the Layout button settings at any time to modify your column display preferences.</td>
</tr>
</tbody>
</table>
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.

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.

  For more information, see [Lookup Values on page 201](#).

**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 on page 201](#).

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.

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 on page 61](#).

2. You can **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**. At this point, 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.

**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 on page 206.

**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](https://support.workspaceone.com/articles/115001663908).
Chapter 15: Certificate Management

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.

Digital Certificates List View

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.

Revoke or Renew a Digital Certificate

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.

Initiate the process by navigating to Devices > Certificates > List View.

1. Identify and select the digital certificates you want to renew or revoke by inserting one or more check marks in the empty check boxes.

2. Select the action button that you want to invoke: Renew or Revoke, to apply the action to the selected certificates.

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-MSECP – 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.
Chapter 16: 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. These attributes allow you to take advantage of the rules generator when creating products using Product Provisioning.

**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 AirWatch Agent 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.

**Create Custom Attributes**

Create a custom attribute and values to push to devices. You create the attributes and values associated with them. For more information, see Create Custom Attributes on page 206.

**Importing Custom Attributes**

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. For more information, see Custom Attributes Importing on page 206.
Platform-Specific Custom Attributes Provisioning

You can push custom attributes to a device using XML provisioning for use with advanced product provisioning functionality. The method for pushing the XML varies based on the device platform.

Create Custom Attributes

Create a custom attribute and values to push to devices. These attributes and values control how product rules work and function as lookup values for certain devices.

1. Navigate to Devices > Staging & 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.
   For example, 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.

- Custom Attribute Values Template – Allows you to define the values of predefined custom attributes.

- 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.

1. DeviceID (Workspace ONE™ UEM assigned DeviceID when the device enrolls)
2. Serial Number
3. UDID
4. MAC Address
5. 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.

1. Ensure that you are currently in a customer type organization group.
3. Set Device Assignment Rules to Enabled.
4. Set the Type to Organization Group by Custom Attribute.
5. Select Save.
6. Navigate to Devices > Staging & Provisioning > Custom Attributes > List View > Add > Add Attribute and create a custom attribute if you have not already done so. See Create Custom Attributes on page 206 for more information.


8. Select the Organization Group to which the rule assigns devices.

9. Select Add Rule to configure the logic of the rule.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute/Application</td>
<td>This custom attribute determines device assignment.</td>
</tr>
<tr>
<td>Operator</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> There is a limitation on the less than (&lt;) and greater than (&gt;) operators. This limitation includes &quot;less than or equal to&quot; and &quot;greater than or equal to&quot; 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.</td>
</tr>
<tr>
<td>Value</td>
<td>All values from all applicable devices are listed here for the Attribute selected for the rule.</td>
</tr>
<tr>
<td>Add Logical Operator</td>
<td>Select to display a drop-down menu of logical operators such as AND, OR, NOT, and parentheses. Allows for more complex rules.</td>
</tr>
</tbody>
</table>

10. Select Save after configuring the logic of the rule.

When a device enrolls with an assigned attribute, the rule assigns the device to the configured organization group.
Chapter 17: Self-Service Portal

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

Access the Self Service Portal on Devices

You can access the Self-Service Portal (SSP) from your workstations or devices by navigating to https://<AirWatchEnvironment>/MyDevice. If you have a device that supports Web Clips or Bookmarks, your administrator may have supplied these shortcuts enabling you to access the SSP directly.

Self Service Portal (SSP) Customizations

You can alter the default login page background by configuring Branding settings.

Navigate to Groups & Settings > All Settings > System > Branding and select the Upload button in the Self-Service Portal Login Page Background setting. Select a custom background image with a suggested size of 1024x768 pixels.

Product Improvement Program Setting

The Self Service Portal is included in VMware’s Product Improvement Program, which gives you the opportunity to impact the quality and effectiveness of our products. When enabled, this program tests only on usability data, which is essential to ensuring our customers’ real-world needs are being met.

You can opt in or opt out of the Product Improvement Program at any time by navigating to Groups & Settings > All Settings > Admin > Product Improvement Programs.

To learn more about this program, see https://resources.workspaceone.com/view/9yfkbk6r2pzldhj1hrz9.

Token-Based Security Measures

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.

Configure the Default Login Page for the SSP

You can set the default authentication method displayed on the Self-Service Portal depending on your organization’s and users’ needs.

**Note:** This setting is only accessible at the Global level for on-premises customers.

Configure this setting by navigating to Groups & Settings > All Settings > Installation > Advanced > Other and set the SSP Authentication Type to:

- **Email** – Prompts users for only their email address if you have set up auto discovery.
- **Legacy** – Prompts users for their Group ID and credentials (username/password).
- **Dedicated** – Prompts users for only their credentials (username/password). This option defaults a single Group ID for single-customer environments.

My Devices Page of the SSP

The My Devices page of the Self Service Portal provides access to detailed information about devices and enables users to perform a wide range of actions.

The viewable tabs and available actions varies based on device platform. See the applicable platform guide, available on docs.vmware.com.

Select a Language for the SSP

The Self-Service Portal automatically matches the browser default language. However, you can override this default setting by choosing from the Select Language drop-down on the login screen.

Log Into the SSP

Log in using the same credentials (Group ID, username and password) used to originally enroll in Workspace ONE UEM.

Change Your Password for the SSP

You may use the Account page to change the password associated with your Workspace ONE UEM account. This password will be used for device enrollment and logging into the SSP.

Change your password by selecting the Account button located at the top-right of the Self Service Portal screen. The User Account page displays allowing you to select the Change button next to the Current Password field.

Select a Device in the SSP

After logging in to the SSP, the My Devices page displays all the devices associated with the account. Each enrolled device appears in its own tab across the top of the Self Service Portal page. Select the tab representing the device you want to
view and manage.
The device status is listed under the name of the device on the tab. Those statuses include Discovered, Enrolled, Pending Enrollment, Unenrolled, and Enterprise Wipe Pending.

Add a Device in the SSP
You can add a device directly from the self-service portal.
1. Select Add Device on the My Devices page.
2. Complete the required text boxes: Friendly Name, Platform, Device Ownership, Message Type, and Email Address as applicable.
3. Select Save to add the new device to the SSP account.

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.

Note: The status of a newly added device sets to "Pending Enrollment" until it is fully enrolled.

Device Information in the SSP
When a user logs in to the SSP, their primary device appears in the main viewer. The main view page displays basic information such as Enrollment Date, the Last Seen date, and the device Status.
The Go to Details button displays tabs containing information about the selected device under the selected user account.
- Summary – Displays summarized information for Compliance, Profiles, Apps, Content, Friendly Name, Asset Number, UDID number, and Wi-Fi MAC Address.
  ○ A device's friendly name can be edited directly from the Summary tab view by selecting the edit icon to the right of the Friendly Name text box.

Note: The Device Summary User role resource controls the visibility of the Summary tab in the SSP. If specific pieces of information are restricted from a user role's view by way of a disabled resource such as Device Apps, Device Compliance, or Device Profiles, then corresponding information normally appearing on the Summary tab is also hidden.

Visit User Roles and Admin Roles for detailed instructions on limiting resources for user and admin roles.

- Compliance – Shows the compliance status of the device, including the name and level of all compliance policies that apply to the device.
- Profiles – Shows all the MDM profiles (including automatic profiles) that have been sent to the devices enrolled under your user account. This tab also shows the status of each profile.
-Apps – Displays all applications installed on the selected device and provides basic app information.
Remote Actions in the SSP

Workspace ONE UEM gives administrators several remote actions and options for managed devices. However, when devices are employee-owned, those employees might want to access similar management tools for their own use. The Workspace ONE UEM SSP provides a means for employees to use some key MDM tools without any IT involvement. If you enable it, end users can run the SSP in a web browser and access key MDM support tools. You can also enable or disable the displays of information and the ability to perform remote actions from the SSP.

Your administrator determines the selected device’s action permissions and available actions in the SSP, which vary based on platform. Allowed actions are split between Basic Actions and Advanced Actions on the main access page. The administrator determines action permissions, therefore device users might have limited actions available. See the applicable platform guide, available on docs.vmware.com. You can also search the online help for platform-specific options.

Basic Remote Actions in the SSP

Basic remote actions appear on the Basic Actions subtab of the selected device in the self-service portal. The actions available depend upon enrollment status, device platform, and action permissions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Passcode</td>
<td>Set a new passcode for the selected device.</td>
</tr>
<tr>
<td>Clear Passcode</td>
<td>Clear the passcode on the selected device and prompt for a new passcode. This action is useful if users forget their device passcode and are locked out of their device.</td>
</tr>
<tr>
<td>Delete Device</td>
<td>Remove the device from the Self Service Portal.</td>
</tr>
<tr>
<td>Delete Registration</td>
<td>Delete any pending enrollment record from the Self Service Portal.</td>
</tr>
<tr>
<td>Device Query</td>
<td>Request the device to send a comprehensive set of MDM information to the Workspace ONE UEM Server.</td>
</tr>
<tr>
<td>Device Wipe</td>
<td>Wipe all data from the selected device, including all data, email, profiles, and MDM capabilities and returns the device to factory default settings.</td>
</tr>
<tr>
<td>Download Agent</td>
<td>Download and install the AirWatch Agent to the device from which you are viewing the SSP.</td>
</tr>
<tr>
<td>Enterprise Wipe</td>
<td>Wipe all corporate data from the selected device and removes the device from Workspace ONE UEM. All the enterprise data contained on the device is removed, including MDM profiles, policies, and internal applications. The device returns to the state it was in before the installation of Workspace ONE UEM.</td>
</tr>
<tr>
<td>Locate Device</td>
<td>Activate the GPS feature to locate a lost or stolen device. This action is hidden when privacy settings are restrictive.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Lock Device/Screen</td>
<td>Locks the selected device so that an unauthorized user cannot access it, which is useful if the device is lost or stolen. End users can also use the GPS feature to locate the device.</td>
</tr>
<tr>
<td>Lock SSO</td>
<td>Lock the single sign-on passcode for apps on this device. The next SSO app opened will prompt for a passcode.</td>
</tr>
<tr>
<td>Make Noise</td>
<td>Rind a device by remotely causing it to ring.</td>
</tr>
<tr>
<td>Resend Enrollment Message</td>
<td>Send another copy of the initial enrollment email, SMS, or QR code to the device intended to register. As a security feature, the email address that appears in the resend enrollment message form is read-only for accounts that enrolled with a token.</td>
</tr>
<tr>
<td>Send Message</td>
<td>Send a message using email, phone notification or SMS to the device.</td>
</tr>
<tr>
<td>Set Roaming</td>
<td>Set whether roaming is enabled for this device.</td>
</tr>
<tr>
<td>Sync Device</td>
<td>Outfit devices with the latest company policies, content, and apps.</td>
</tr>
<tr>
<td>View Enrollment Message</td>
<td>See the actual email, SMS, or QR code that comprised the initial enrollment message. As a security feature, this action is not available for accounts that enrolled with a token.</td>
</tr>
</tbody>
</table>

**Note:** Registration and Enrollment actions only display in the SSP when the enrollment of a selected device is still pending.

### Advanced Remote Actions in the SSP

Advanced remote actions appear on the Advanced Actions subtab of the selected device in the self-service portal. The actions available depend upon enrollment status, device platform, and action permissions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate App Token</td>
<td>Generate a token that the device can use to access secure applications.</td>
</tr>
<tr>
<td>Manage Email</td>
<td>Manage devices connected to an email account.</td>
</tr>
<tr>
<td>Review Terms of Use</td>
<td>Review past terms of use for this account.</td>
</tr>
<tr>
<td>Revoke Token</td>
<td>Revokes the token for a selected application.</td>
</tr>
</tbody>
</table>
## Self-Service Portal Actions Matrix

Each of the major device platforms supports various basic and advanced SSP actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Android</th>
<th>iOS</th>
<th>Win Phone</th>
<th>macOS</th>
<th>Win Mobile</th>
<th>Win 7</th>
<th>Win Desktop</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Actions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Passcode</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Clear (SSO) Passcode</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Delete Device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Delete Registration</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Device Query</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Device Wipe</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Download Agent</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Enterprise Wipe</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Locate Device</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lock Device/Screen</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lock SSO</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Make Noise</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Resend Enrollment Message</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Send Message</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Set Roaming</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sync Device</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>View Enrollment Message *</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

| **Advanced Actions**          |         |     |           |       |            |       |             |
| Generate App Token            | ✓       | ✓   | ✓         | ✓     | ✓          | ✓     | ✓           |
| Manage Email                  |         | ✓   |           | ✓     | ✓          | ✓     | ✓           |
| Review Terms of Use           | ✓       | ✓   | ✓         | ✓     | ✓          | ✓     | ✓           |
| Revoke Token                  | ✓       | ✓   | ✓         | ✓     | ✓          | ✓     | ✓           |
| Upload S/MIME Certificate     | ✓       | ✓   | ✓         | ✓     | ✓          | ✓     | ✓           |

* As a security feature, this action is not available for accounts that enrolled with a token.

## VMware Content Locker Options

Workspace ONE UEM offers three end user facing features that facilitate your organization’s content management. In addition to the robust configurations and management options available within the Workspace ONE UEM console for content, you can also configure the behavior of these user facing features.
VMware Content Locker – Allows end users to access important content on their devices while simultaneously safeguarding those files. Any content accessed through the VMware Content Locker opens inside the application, ensuring that it cannot be copied, saved, or shared without approval.

Content Locker Sync – Allows end users to add files to a shared folder on their computers that syncs with their Personal Content repository. This folder gives them access to those files on their mobile device's VMware Content Locker application or from the Self-Service Portal.

**Note:** Downloading, installing, and using these features are user-dependent actions. See the VMware Content Locker End-User Guide in the appropriate platform for step by step instructions. See also the Content Apps for Desktop End-User Guide at [https://resources.air-watch.com/view/jshgwzqd2fdcby73ryhf/en](https://resources.air-watch.com/view/jshgwzqd2fdcby73ryhf/en).

These guides are available on docs.vmware.com or the myAirWatch documentation repository.

For details, contact your Workspace ONE UEM Administrator.