Console Basics

VMware Workspace ONE UEM 1907

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

Working in the UEM Console 1

The Workspace ONE UEM powered by AirWatch allows you to view and manage every aspect of your 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, sending feedback, and global search.

Send Feedback

You can provide feedback by completing an optional survey about your experience with the Workspace ONE UEM console. Your feedback is used to make improvements to our software. Start the survey yourself by selecting your user name in the upper-right corner and then select **Send Feedback**. You can also opt into the popup window that appears after the 25th login within a 30-day period. If you opt out of this popup window, you will not be prompted again.

Together with the data collected at the time you created your admin account, VMware processes these survey responses with third-party assistance to facilitate a closed loop feedback system. This system helps us understand our users better and allows us to improve our products based on your needs.

For more information about how VMware handles information collected through Workspace ONE UEM, such as analytics, see the VMware Privacy Policy at https://www.vmware.com/help/privacy.html.

This chapter includes the following topics:

- UEM Console Notifications

Logging In to the UEM Console

Before you are able to do anything in Workspace ONE UEM powered by AirWatch, you must first log in to the console.

Before you can log in to the Workspace ONE 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.<YourCompany>.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.

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.

1 Enter your **User name**.
   - The Workspace ONE UEM console saves the user name and the type of user (SAML or non-SAML) in the browser cache.
     - If SAML user, admin is directed to SAML login.
     - If non-SAML user, admin must enter a password.
   - If the **Remember** check box is enabled, then the **User name** text box is pre-populated with the last logged-in user the next time you visit your Environment URL.

2 Enter your **Password**.
   - If you are logging in for the first time, you are prompted for the login password. Enter it to proceed.
   - If you have logged in before and you are allowing your default browser to remember user names and passwords, then the **Password** text box auto-completes with the password saved in the browser cache.

3 Select the **Log In** button.
   - Your default home screen (which is customizable) opens upon login. Learn how to customize your home screen by visiting Header Menu.

Session Timeouts and Logouts

There are two basic scenarios under which you can be logged out of the Workspace ONE UEM console.

1 Explicit Logout (this includes closing the browser window and inactivity logouts.)

- If you have configured your default browser to remember your user name and password, then upon the next login, the browser pre-populates the user name text box with the last user to successfully log in.
- If you have configured your browser to forget user names and passwords, then the user name and type of user (SAML / non-SAML) are wiped from the browser cache.

2 Session Invalidation (this includes load balancer issues and sessions timeouts due to admin setting.)

- Non-SAML users log back in using a saved user name and selecting the **Log In** button.
- SAML users can log back into the console without any clicks.

Login Lockouts

System Administrators and AirWatch Administrators can configure the maximum number of invalid login attempts before admins are locked out of the console by navigating to **Groups & Settings > All Settings > Admin > Console Security > Passwords**.

You are locked out from the UEM console in two scenarios: 1) when you make failed login attempts greater than the maximum number of invalid login attempts and 2) when you answer your password recovery question incorrectly three times while trying to reset your password.

When this happens, you must either reset your password using the troubleshooting link on the login page or you must get assistance from an admin to unlock your account using the Admin List View. You receive an email notification when your account is locked and again when it becomes unlocked. For more information, see Research Account Lockout Console Events.

Password Expiration

Basic administrators are notified by email 5 days before their password expires with another email notification the day before. On-premises administrators can change this default 5 day period by navigating to **Groups & Settings > All Settings > Admin > Console Security > Passwords** while in the Global organization group. Dedicated SaaS administrators must contact support to make changes to this setting.

You can make a custom password expiration notification for your admins by navigating to **Groups & Settings > All Settings > Devices & Users > General > Message Template** and select 'Administrator' as the **Category** and 'Admin Password Expiry Notification' as the **Type**.

For information about Enrollment User Password Settings, which are managed separately from Admin Console Passwords, see the system settings page by navigating to **Groups & Settings > All Settings > Devices & Users > General > Passwords**.

Research Account Lockout Console Events

When Basic Administrator accounts are locked out or unlocked, a console event is generated. Both events generate a logging level 5 (warning) event. In addition to reviewing the basic login history directly from **Account Settings**, you can research Admin account lockouts or unlock console events by taking the following steps.

Procedure

1. Navigate to **Monitor > Reports & Analytics > Events > Console Events**.
2. Select "Warning and above" from the **Severity** drop-down filter at the top of the **Console Event** listing.
3. Select "Login" from the **Category** drop-down filter.
4. Select "Administration" from the **Module** drop-down filter.
5. Apply more filters as you might require including **Date Range**.

Results

Where applicable, select the hypertext link in the **Event Data** column which contains extra detail that can assist your research efforts.

Using the Getting Started Wizard

The Getting Started Wizard serves as a checklist that walks you through the Workspace ONE UEM powered by AirWatch 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 VMware Workspace ONE Documentation.

- **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 Monitor.

- **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

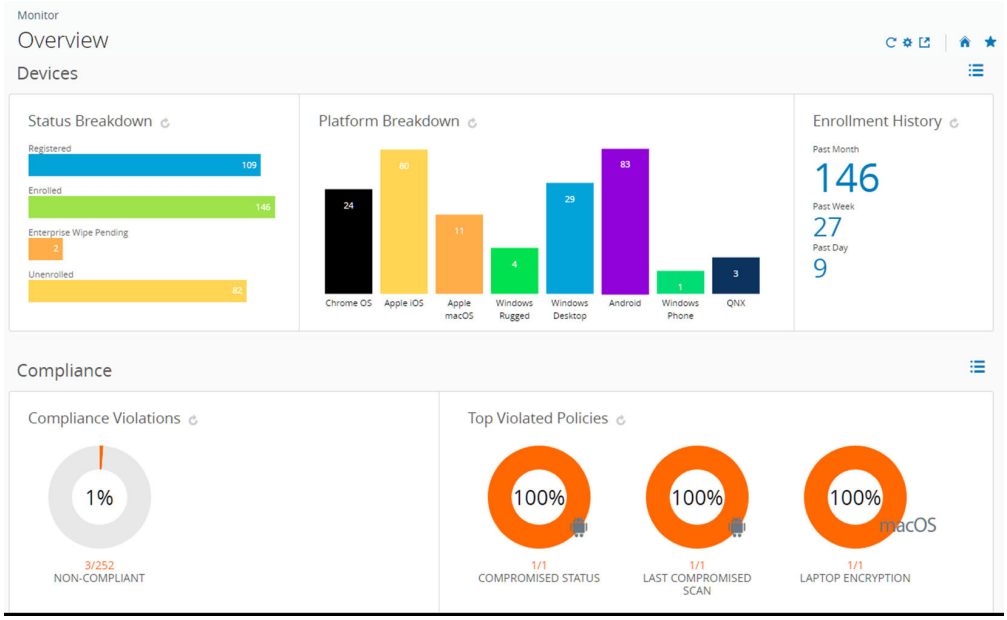
Each of the four submodules displays a list of sections representing features that you can configure or ignore, according to the needs of your organization. Features not configured display an empty **Incomplete** check box while configured features display a green **Complete** check mark.

- 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.

UEM Console Monitor Overview

The Workspace ONE UEM powered by AirWatch Monitor Overview is your central portal for fast access to critical information. With its colorful bar and donut graphs, 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 **Monitor > Overview** page 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 () and **Chart View** icon (). 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 Monitor by selecting the **Available Sections** icon (). Select or deselect check boxes representing available sections (Devices, Compliance, Profiles, and so on) and select **Save** to craft the Monitor Overview.

You can export Monitor data in PDF format by selecting the **Export** icon (). 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 that you are in a customer type organization group, then navigate to **Monitor > Intelligence**, select the **Next** button to see how Intelligence works, and opt-in to take advantage of the service.

You can opt out of Intelligence custom reporting at any time.

For more information, see the **Workspace ONE Intelligence User 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 **Monitor > Admin Panel**. The Admin Panel can only be accessed from a Customer organization group. For more information, see Organization Group Type Functions.

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.

Tracking and Monitoring Application Deployment

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.

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 1-1. Descriptions of Deployment Statuses in the App and Profile Monitor

Status	Description
Done	Devices report the Done status when the app or profile installs successfully.
Pending	Devices report the Pending Status when an app or profile reports the following statuses. **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. ■ Command Acknowledged.
Incomplete	Device reports the Incomplete Status when an app or profile reports the following statuses. **Profiles** ■ Pending Information. **Apps** ■ User Removed. ■ Install Rejected. ■ Install Failed. ■ License Not Available. ■ Rejected. ■ Management Rejected. ■ Download Failed. ■ Criteria Missing. ■ Command Failed. 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 application 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.

Procedure

1. Navigate to **Monitor > 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**.

Results

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

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. For more information, see **Industry Templates Overview** in **VMware Workspace ONE UEM iOS Platform Documentation** on docs.vmware.com.

Manage Account Settings

You can manage your account settings in Workspace ONE UEM powered by AirWatch, 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, select how to receive alerts, and change the email to which it sends alerts. For more information, see Configure Notifications Settings.

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 user name 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.

You are locked out from the login page when you answer a Password Recovery Question incorrectly more than three times. When this happens, you must reset your password using the troubleshooting link on the login page. Alternatively, you can get assistance from an admin to unlock your account using the Admin List View. You receive an email notification when your account is locked and again when it becomes unlocked.

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.

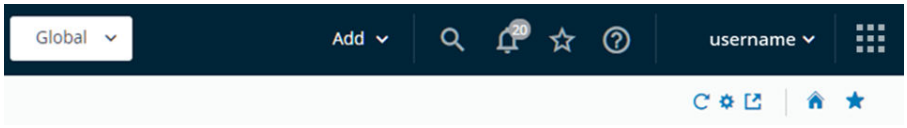
When you first log in to the UEM console, you are required to establish a Security PIN.

Reset your security PIN every so often to minimize security risks.

For more information about the login process, see Logging In to the UEM Console.

Header Menu

The **Header Menu** appears at the top of nearly every page of the Workspace ONE UEM powered by AirWatch, 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.
- **My Services Selector** – () Use this bento menu button to select between all Workspace ONE services that are available to you.
- **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 Monitor Overview by selecting only the sections you want to see. Available only on the Monitor screen.
- **Export** – () Produces a full (or filtered, if filtering is used) listing of users, devices, profiles, apps, books, or policies to an XLSX or CSV (comma-separated values) file, both of which you can view and analyze with MS 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.

Main Menu

The **Main Menu** allows you to navigate to all the features available to your role and Mobile Device Management (MDM) deployment within Workspace ONE UEM powered by AirWatch.

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 UEM console deployment that you are interested in. Getting Started produces an on-boarding experience that is more tailored to your actual configuration.
Monitor	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. Access **Configurations**, which is a categorized and curated list of links that lead directly to the settings pages you need.

Configurations

Configurations are a curated list of settings pages that are categorized, searchable, and logically organized making them easy to use. Configurations enable you to identify and jump directly to essential settings pages in Workspace ONE UEM powered by AirWatch and Workspace ONE Express. Get started by navigating to **Groups & Settings > Configurations**.

Each Configuration can be inspected by selecting the 'greater than' left arrow to expand the row and reading the description. Once expanded, you can also read the official documentation on the Configuration by selecting the **Learn More** button.

Searchable

You can search for Configurations and categories by making entries in the search bar located above the listing.

Categorized

All the Configurations are categorized by attributes and use cases so you can quickly locate the ones you need the most. Clicking on categories acts like a filter, eliminating Configurations from view that are not part of the selected category. To clear out selected categories and reset the view, click the 'x' next to the category name or select the Reset button above the search bar.

Portable Categories

You can share Configuration categories with other administrators that include category combinations. For example, if you select **Platform Setup**, **Apple**, and **Enrollment**, you can share this combination of categories by copying the URL in the address bar of your browser.

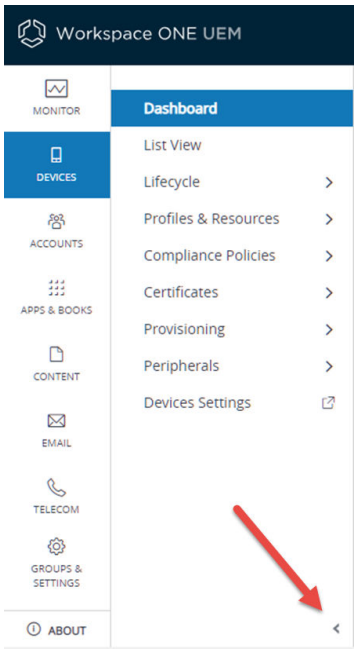
Collapse and Expand the Submenu

You can collapse the left panel submenu of the Workspace ONE UEM powered by AirWatch to create more screen space for device information. You can also expand or reopen a collapsed submenu.

Procedure

- To temporarily collapse the submenu, select the "less-than" arrow shown here.

Example



What to do next

To expand or reopen the collapsed submenu, select the "greater-than" arrow at the bottom-left of the screen, next to the "About" icon.

Global Search

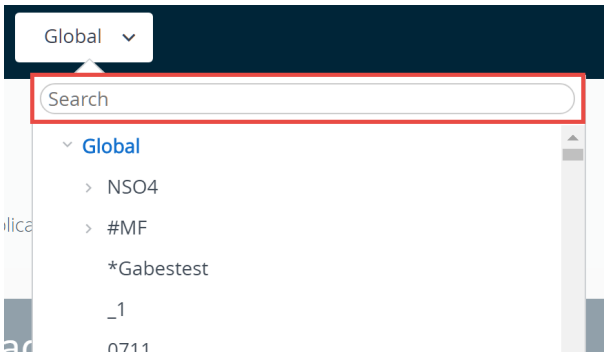
Using a modular design with a tabbed interface, Global Search runs searches across your entire deployment. Global Search applies your search string to a single tab at a time, which produces faster results. Apply the same string to another area of the Workspace ONE UEM powered by AirWatch by selecting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

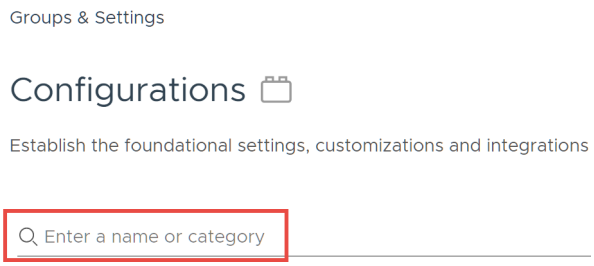
Organization Group Searches

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.



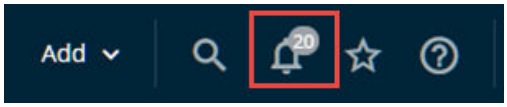
Settings Searches

You can search for settings by initiating a search from the Configurations page. Navigate to **Groups & Settings > Configurations** and enter your keyword in the search text box.



UEM Console Notifications

Notifications are a communication tool designed to keep you informed about Workspace ONE UEM powered by AirWatch 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. Purge your logs or increase the limit by contacting your support representative. 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.

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.
- **Dismiss All** – Close all active alerts and send them to the Dismissed alert listing.
- **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.

Procedure

1. Select the **Account** drop-down, which is accessible from almost every page on the Workspace ONE 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.

Setting	Description
MDM APNs Expiring	This notification helps you avoid the hassles involved with expired certificates and keeps your devices in contact with Workspace ONE UEM.
List View Export	You can trigger an alert when the exportation of a User List View or Device List View is complete.
User Group Merge	You can trigger an alert when the Active Directory database changes sync with Workspace ONE UEM and you have Auto Merge Changes disabled.
VPP App Auto Update	You can trigger an alert when an app installed with Apple Volume Purchase Program has an updated version you can install.
Application APNs Certificate Expiration	This notification helps you avoid the hassles involved with expired certificates and keeps the apps functional on your devices.

Setting	Description
Provisioning Profile Expiration	You are notified when a provisioning profile containing applications expires, requiring you to regenerate the provisioning profile and update it.
API Utilization	You are notified when the number of API (Application Programming Interface) calls reaches 50%, 75%, 90%, and 100% of the daily API limit.

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.

Environment Setup

2

The virtual space that encompasses your managed device fleet and the management of the Workspace ONE UEM powered by AirWatch is called the Environment. There are many ways to configure this environment to your liking.

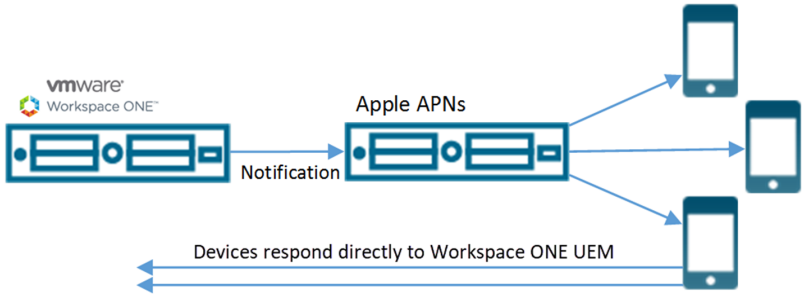
This Environment can accommodate certain settings such as the URL, admin login credentials, certificates for managing platforms, configuring Telecom, privacy and security settings, branding the console with your company colors, and more.

This chapter includes the following topics:

APNs Certificates

To manage iOS devices, you must first obtain an Apple Push Notification Service (APNs) certificate. An APNs certificate allows Workspace ONE UEM powered by AirWatch 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.



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.

Generate a New APNs Certificate

Before you can manage iOS devices with Workspace ONE UEM, you must first generate an APNs Certificate to enable and maintain secure communications between your iOS devices and the Workspace ONE UEM console.

You can follow the steps outlined in the Using the Getting Started Wizard or generate a new APNs certificate manually by taking the following steps.

Procedure

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > APNs for MDM**.
2. Select the **Generate New Certificate** button.

   You are taken to Step 1 Sign Request.
3. Select the link 'MDM_APNsRequest.plist' and choose a location in which to save the PLIST file, which you must upload to Apple the next step.
4. 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.
5. You need two items to continue:
   a. The Workspace ONE UEM Certificate Request, which is the PLIST file that you saved to your device.
   b. A corporate Apple ID that should be dedicated to MDM for your company. Select the link provided ('Click here') to proceed with the creation of the Apple ID. Doing so opens a new tab in your browser.
6. 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).
7. Select **Save**.

Results

Your APNs certificate has been generated.

What to do next

Check the connectivity of your APNs certificate over the HTTP/2 protocol, which is a major revision of the existing hypertext transfer protocol. For more information, see Check APNs Connectivity over HTTP/2.

Renew an APNs Certificate

You must occasionally renew APNs Certificates to enable and maintain secure communications between your iOS devices and Workspace ONE UEM.

You can follow the steps outlined in the Using the Getting Started Wizard or renew expired APNs certificates manually by taking the following steps.

Procedure

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > APNs for MDM**.
2. If the **Valid To** date has passed, select the **Renew** button and follow the on-screen instructions.
3. Select the link 'MDM_APNsRequest.plist' and choose a location in which to save the PLIST file, which you must upload to Apple the next step.
4. 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.
5. You need two items to continue:
   a. The Workspace ONE UEM Certificate Request, which is the PLIST file that you saved to your device.
   b. The Apple ID that you originally used to create the certificate, which is displayed in item 2 of the Step 1 Sign Request.
6. 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).
7. Select **Save**.

Results

Your APNs certificate has been renewed.

What to do next

Check the connectivity of your APNs certificate over the HTTP/2 protocol, which is a major revision of the existing hypertext transfer protocol. For more information, see Check APNs Connectivity over HTTP/2.

Check APNs Connectivity over HTTP/2

You can check the connectivity between Workspace ONE UEM powered by AirWatch and the Apple HTTP/2 API endpoint. This check allows you to ensure APNs functionality over an HTTP/2 connection after generating a new certificate or following a certificate renewal.

Prerequisites

This connectivity test is only for testing APNs over HTTP/2 which is not enabled by default. Any connectivity failures from this test do not impact APNs functionality over a legacy connection.

Procedure

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > APNs for MDM**.
2. Select the **Test Connection** button.

   The Workspace ONE UEM console conducts an internal test to determine whether connectivity over the new HTTP/2 protocol is functional.

Results

Because this test only centers on the HTTP/2 protocol, test failures here do not affect current APNs communication. If the HTTP/2 connectivity test fails, the steps you take depend upon the cause of the failure.

1. **Expired Certificate** - The certificate you are using for the test has expired. Request a renewal by viewing Renew an APNs Certificate.
2. **Invalid Certificate** - The certificate you are using for the test, while not expired, is invalid for another reason. You can request a certificate renewal or wait a few minutes and test the connection again.
3. **Unknown Error** - Typically occurs during a temporary loss of internet access. Wait a few minutes and test the connection again.
4. **APNs Client Deactivated** - While rare, this means that Apple has returned an internal error or that the APNs service is unavailable. Wait a few minutes and test the connection again.

Terms of Use

You can enforce terms of use (TOU) on all managed devices within Workspace ONE UEM powered by AirWatch.

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.

You can make TOU agreements specific to an organization group. Ensure that your current active organization group is correct for the TOU you are creating.

Procedure

1. Navigate to **Devices > Device Settings > Devices & Users > General > Enrollment** and select the **Terms of Use** tab.
2. Select the **Add New Enrollment Terms of Use** button and complete the following options.

Setting	Description
Name	Enter a unique name for the new TOU.
Type	This option is pre-populated as **Enrollment**.
Version	This option is automatically tracked and populated accordingly.
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.

3. 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.
4. Select **Save**.

Results

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 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.

Procedure

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.

Procedure

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.

Prerequisites

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 XLSX or CSV format, both viewable with MS Excel.

Procedure

1 Navigate to **Monitor > 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.

Results

VMware Workspace ONE UEM does not provide legally binding sample text. Your company legal team must review any text examples provided.

Customize the UI with Branding

Workspace ONE UEM powered by AirWatch allows extensive customization options. These options allow you to brand your 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.

Procedure

1. Select the organization group you want to brand and then navigate to **Groups & Settings > All Settings > System > Branding**.
2. Configure logo and background settings on the **Branding** tab.
3. Upload a Company Logo by uploading a file saved on your computer. The suggested resolution of the uploaded image is 800x300.
4. Upload a background for the login page by uploading a file saved on your computer. The suggested resolution of the uploaded image is 1024x768.
5. Upload a background for the Self-Service Portal (SSP) login page by uploading a file saved on your computer. The suggested resolution of the uploaded image is 1024x768.
6. Configure customizations to the **Colors** section in the **Branding** tab.
7. Configure the settings on the **Custom CSS** tab. Enter customized CSS code for advanced branding.
8. Select **Save**.

Restrict UEM Console Actions

Given a scenario when the Workspace ONE UEM powered by AirWatch 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.

Procedure

1. Navigate to **Groups & Settings > All Settings > System > Security > Restricted Actions**.
2. Configure the **Send Message to All** setting. 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.
3. You can require that certain UEM console actions require admins to enter a PIN. Configure the **Password Protect Actions** by enabling or disabling the following actions.

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

Setting	Description
Admin Account Delete	Prevents the deletion of an admin user account in **Accounts > Administrators > List View**.
***Regenerate VMware Enterprise Systems Connector Certificate**	Prevents the regeneration of the VMware Enterprise Systems Connector certificate in **Groups & Settings > All Settings > System > Enterprise Integration > VMware Enterprise Systems Connector**.
***APNs Certificate Change**	Prevents the disabling of APNs for MDM in **Groups & Settings > All Settings > Devices & Users > Apple > APNs For MDM**.
Application Delete/ Deactivate/Retire	Prevents the deletion, deactivation, or retirement of an application in **Apps & Books > Applications > List View**.

Setting	Description
Content Delete/ Deactivate	Prevents the deletion or deactivation of a content file in **Content > List View**.
***Data Encryption Toggle**	Prevents the Encryption of user information setting in **Groups & Settings > All Settings > System > Security > Data Security**.
Device Delete	Prevents the deletion of a device in **Devices > List View**. Admin security PIN is still required for bulk actions even when this setting is disabled.
***Device Wipe**	Prevents any attempt to perform a device wipe from the Device List View or Device Details screens.
Enterprise Reset	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.
Enterprise Wipe	Prevents any attempt to perform an enterprise wipe on a device from the **Devices Details** page of a device.
Enterprise Wipe (Based on User Group Membership Toggle)	Prevents any attempt to perform an enterprise wipe on a device when it is removed from a user group. This setting is an optional setting that you can configure under **Groups & Settings > All Settings > Devices & Users > General > 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.
***Organization Group Delete**	Prevents any attempt to delete the current organization group from **Groups & Settings > Groups > Organization Groups > Organization Group Details**.
Profile Delete/Deactivate	Prevents any attempt to delete or deactivate a profile from **Devices > Profiles & Resources > Profiles**.
Provisioning Product Delete	Prevents any attempt to delete a provisioning product from **Devices > Provisioning > Products List View**.
Revoke Certificate	Prevents any attempt to revoke a certificate from **Devices > Certificates > List View**.
***Secure Channel Certificate Clear**	Protects from any attempt to clear an existing secure channel certificate from **Groups & Settings > All Settings > System > Advanced > Secure Channel Certificate**.
User Account Delete	Prevents any attempt to delete a user account from **Accounts > Users > List View**.
Change in Privacy Settings	Prevents any attempt to alter the privacy settings in **Groups & Settings > All Settings > Devices & Users > General > Privacy**.
Delete Telecom Plan	Prevents the deletion of a telecom plan in **Telecom > Plan List**.
Override Job Log Level	Prevents attempts to override the currently selected job log level from **Groups & Settings > Admin > Diagnostics > 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.
***App Scan Vendor Reset/Toggle**	Prevents the resetting (and subsequent wiping) of your app scan integration settings. This action is performed in **Groups & Settings > All Settings > Apps > App Scan**.
Shut Down	Prevents any attempt to shut down the device in **Devices > List View > Device Details**.
Maximum invalid PIN attempts	Defines the maximum number of invalid attempts at entering a PIN before the console locks down. This setting must be between 1 and 5.

Select Password Protect Actions

Restricted Console Actions provide an added layer of protection against malicious actions that are potentially destructive.

Procedure

1 Configure settings for restricted actions by navigating to **Groups & Settings > All Settings > System > Security > Restricted Actions**.

2 For each action you choose to protect by requiring admins to enter a PIN, 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 * following.

3 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 must log into the Workspace ONE UEM console and set a new security PIN.

Setting	Description
Admin Account Delete	Prevents the deletion of an admin user account in **Accounts > Administrators > List View**.
Regenerate VMware Enterprise Systems Connector Certificate	Prevents the regeneration of the VMware Enterprise Systems Connector certificate in **Groups & Settings > All Settings > System > Enterprise Integration > VMware Enterprise Systems Connector**.
***APNs Certificate Change**	Prevents the disabling of APNs for MDM in **Groups & Settings > All Settings > Devices & Users > Apple > APNs For MDM**.
Application Delete/Deactivate/Retire	Prevents the deletion, deactivation, or retirement of an application in **Apps & Books > Applications > List View**.
Content Delete/Deactivate	Prevents the deletion or deactivation of a content file in **Content > List View**.
***Data Encryption Toggle**	Prevents the Encryption of user information setting in **Groups & Settings > All Settings > System > Security > Data Security**.
Device Delete	Prevents the deletion of a device in **Devices > List View**. Admin security PIN is still required for bulk actions even when this setting is disabled.
***Device Wipe**	Prevents any attempt to perform a device wipe from the Device List View or Device Details screens.
Enterprise Reset	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.
>Enterprise Wipe	Prevents any attempt to perform an enterprise wipe on a device from the **Devices Details** page of a device.

Setting	Description
Enterprise Wipe (Based on User Group Membership Toggle)	Prevents any attempt to perform an enterprise wipe on a device when it is removed from a user group. This setting is an optional setting that you can configure under **Groups & Settings > All Settings > Devices & Users > General > 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.
***Organization Group Delete**	Prevents any attempt to delete the current organization group from **Groups & Settings > Groups > Organization Groups > Organization Group Details**.
Profile Delete/Deactivate	Prevents any attempt to delete or deactivate a profile from **Devices > Profiles & Resources > Profiles**.
Provisioning Product Delete	Prevents any attempt to delete a provisioning product from **Devices > Provisioning > Products List View**.
Revoke Certificate	Prevents any attempt to revoke a certificate from **Devices > Certificates > List View**.
***Secure Channel Certificate Clear**	Protects from any attempt to clear an existing secure channel certificate from **Groups & Settings > All Settings > System > Advanced > Secure Channel Certificate**.
User Account Delete	Prevents any attempt to delete a user account from **Accounts > Users > List View**.
Change in Privacy Settings	Prevents any attempt to alter the privacy settings in **Groups & Settings > All Settings > Devices & Users > General > Privacy**.
Delete Telecom Plan	Prevents the deletion of a telecom plan in **Telecom > Plan List**.
Override Job Log Level	Prevents attempts to override the currently selected job log level from **Groups & Settings > Admin > Diagnostics > 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.
***App Scan Vendor Reset/Toggle**	Prevents the resetting (and subsequent wiping) of your app scan integration settings. This action is performed in **Groups & Settings > All Settings > Apps > App Scan**.
Shut Down	Prevents any attempt to shut down the device in **Devices > List View > Device Details**.
Maximum invalid PIN attempts	Defines the maximum number of invalid attempts at entering a PIN before the console locks down. This setting must be between 1 and 5.

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.

Procedure

1 Navigate to **Groups & Settings > All Settings > System > Security > Restricted Actions**.

2 If you require that your admins enter a note before taking any of these actions, make sure that you modify the role with the **Add Note** resource (permission).

For more information, see Create Administrator Role.

Setting	Description
Lock Device	Require a note for any attempt to lock a device from **Device List View** or **Device Details**.
Lock SSO	Require a note for any attempt to lock an SSO session from **Device List View** or **Device Details**.
Device Wipe	Require a note for any attempt to perform a device wipe from **Device List View** or **Device Details**.
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 powered by AirWatch 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 Identity Manager Documentation**. See also **VMware Tunnel Admin Guide**, the **AirWatch Logging Guide**, and the **AirWatch Installation Guide**, each available on docs.vmware.com. You can also search for these topics on docs.vmware.com.

User and Admin Accounts 3

In order to enroll devices, you must create and integrate user accounts. Likewise, administrator accounts must be created and assigned so Admins can easily manage users and devices.

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

This chapter includes the following topics:

User Authentication Types

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

Basic Authentication

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

Active Directory LDAP Authentication

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

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

Additional Authentication Types

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

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

Enable Security Types for Enrollment

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

Basic User Authentication

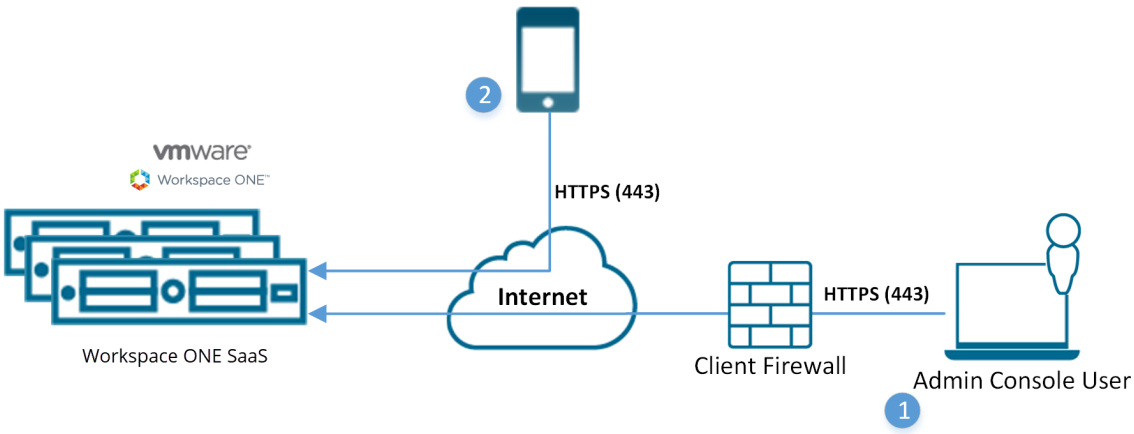
You can use Basic Authentication to identify users in the Workspace ONE UEM architecture but this method offers no integration to existing corporate user accounts.

Pros

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

Cons

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



1 Console user logs in to Workspace ONE UEM SaaS using local account for authentication (Basic Authentication).
   - Credentials are encrypted during transport.
   - (for example, user name: jdoe@air-watch.com, password: abcd).
2 Device user enrolls device using local Workspace ONE UEM account (Basic Authentication) credentials.
   - Credentials are encrypted during transport.
   - (for example, user name: jdoe2, password 2557).

Active Directory with LDAP Authentication

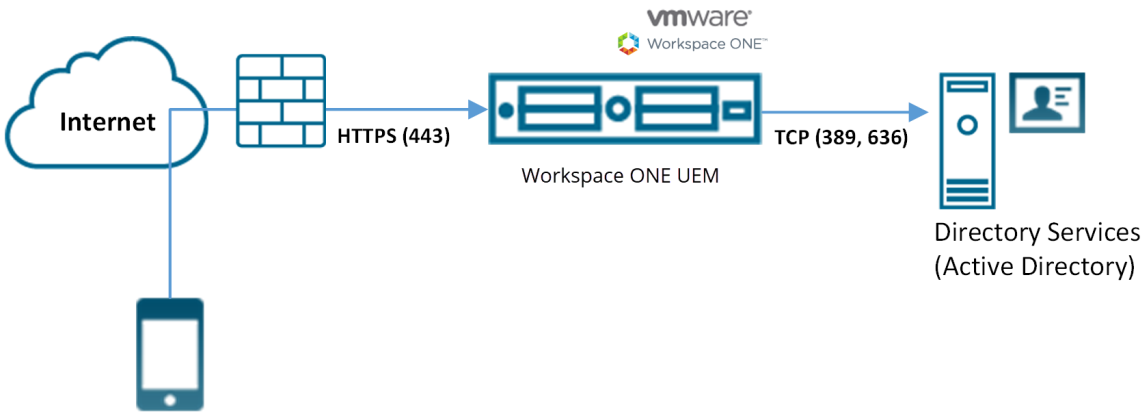
Active Directory (AD) with Lightweight Directory Access Protocol (LDAP) authentication is used to integrate user and admin accounts of Workspace ONE UEM with existing corporate accounts.

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.

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.

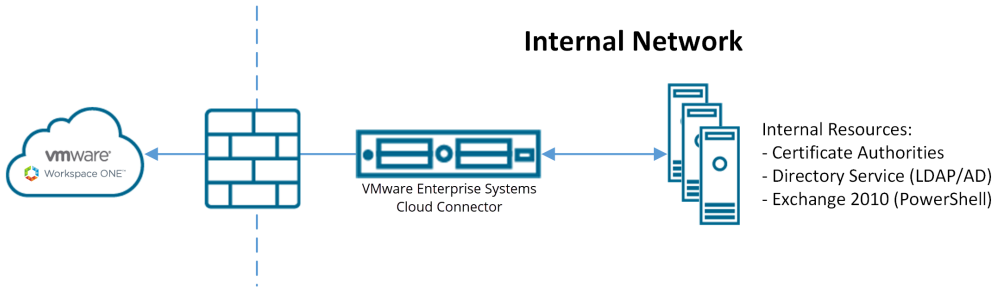
Pros

- 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.

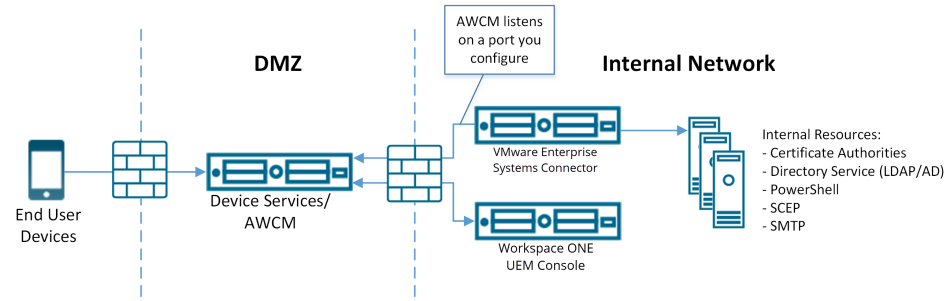
Cons

- 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



Authentication Proxy

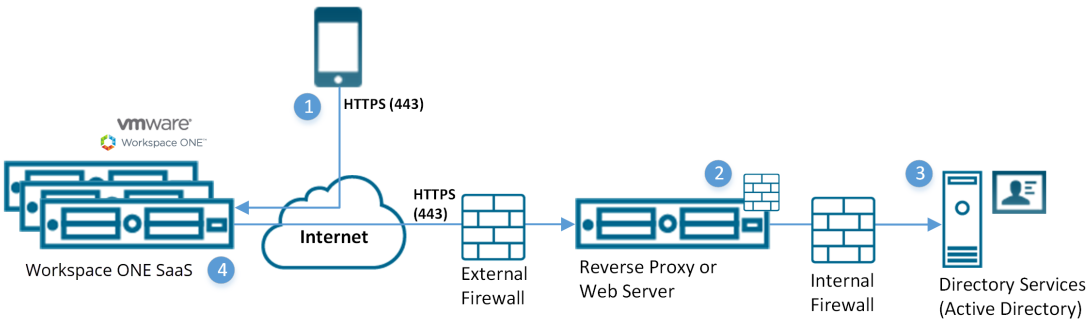
The authentication proxy delivers directory services integration across the cloud or across hardened internal networks. In this model, the Workspace ONE UEM server communicates with a publicly facing Web server or an Exchange ActiveSync Server. This arrangement authenticates users against the domain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

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.

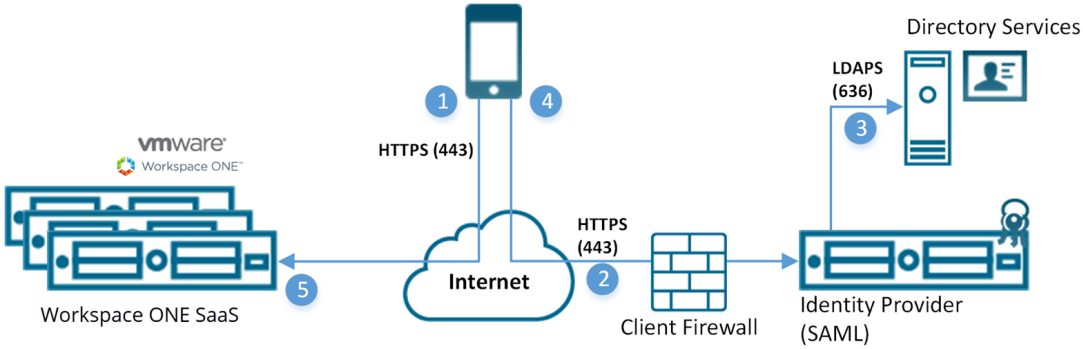
If an organization has a SAML Identity Provider server, use SAML 2.0 integration. Ensure that the Identity Provider returns the `objectGUID` attribute as part of the SAML response.

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.
- Multi-domain environments are supported for Administrators only.

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 the VMware AirWatch SAML Integration Guide.

Token-Based Authentication

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

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

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

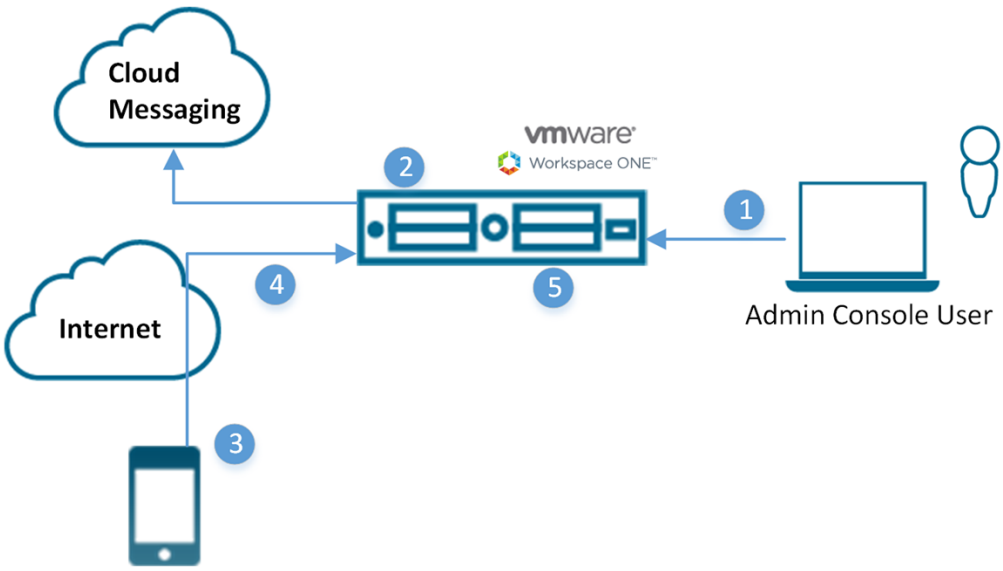
You can also decide to implement two factor authentication to take end-user identity verification a step further. With this authentication setting, the user must enter their user name and password upon accessing the enrollment link with the provided token.

Pros

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

Cons

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



1 Administrator authorizes user device registration.

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

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

4 Device enrollment process.

5 Workspace ONE UEM marks token as expired.

Note SMTP is included with SaaS deployments.

Enable Security Types for Enrollment

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

Procedure

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

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

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

3 Select **Save**.

Basic User Accounts

Create basic user accounts in Workspace ONE UEM powered by AirWatch 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.

Pros

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

Cons

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

Create Basic User Accounts

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

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

Procedure

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

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

Setting	Description
Security Type	Select **Basic** to add a basic user.
User name	Enter a user name with which the new user is identified.
Password	Enter a password that the user can use to log in.
Confirm Password	Confirm the password.
Full Name	Complete the **First Name**, **Middle Name**, and **Last Name** of the user.

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

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

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

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

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

Directory-Based User Accounts

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

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.
- Detects and syncs changes from the directory system into Workspace ONE UEM automatically. For instance, when you disable users in AD, the corresponding user account in Workspace ONE UEM console is marked inactive.
- Secure method of integrating with your existing directory service.

- Standard integration practice.
- Can be used for Workspace ONE Direct Enrollment.
- SaaS deployments using the AirWatch Cloud Connector require no firewall changes and offers a secure configuration to other infrastructures, such as Microsoft ADCS, SCEP, and SMTP servers.

For more information regarding syncing of account statuses, see Directory User Status Syncing.

Cons

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

Directory User Status Syncing

When you make users inactive in your directory service, it impacts the corresponding Workspace ONE UEM account in a similar way but only assuming these prerequisite conditions.

- Syncing of removed users works with Active Directory only.
- The user name you entered in the **Bind User Name** option must have Active Directory administrator privileges.
  - Check on this name by navigating to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services** in the **Server** tab and look for the **Bind User Name** option.
- You can allow non administrators in Active Directory access to the deleted objects container provided you follow the steps outlined in the following Microsoft Support article. https://support.microsoft.com/en-in/help/892806/how-to-let-non-administrators-view-the-active-directory-deleted-object.
- The recycle bin must be enabled using the Active Directory Administrative Center.
  a Open the **Active Directory Administrative Center**.
  b Select the domain, then right-click the domain.
  c Select **Enable Recycle Bin**. Once enabled, the recycle bin cannot be disabled.

Create a Directory-Based User Account

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

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

Procedure

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

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

Setting	Description
Security Type	Add an Active Directory user by choosing **Directory** as the Security Type.
Directory Name	This pre-populated setting identifies the Active Directory name.
Domain	Choose the domain name from the drop-down menu.
User name	Enter the user's directory user name and select **Check User**. If the system finds a match, the user's information is automatically populated. The remaining settings in this section are only available after you have successfully located an active directory user with the **Check User** button.
Full Name	Use **Edit Attributes** to allow any option that syncs a blank value from the directory to be edited. Edit Attributes also enables you to populate matching user's information automatically. If a setting syncs an actual value from the directory, then that setting must be edited in the directory itself. The change takes effect on the next directory sync. Complete any blank option returned from the directory in **Full Name** and select **Edit Attributes** to save the addition.
Display Name	Enter the name that displays in the admin console.
Email Address	Enter or edit the user's email address.
Email user name	Enter or edit the user's email user name.
Domain (email)	Select the email domain from the drop-down menu.
Phone Number	Enter the user's phone number including plus sign, country code, and area code. If you intend to use SMS to send notifications, the phone number is required.
Enrollment	
Enrollment Organization Group	Select the organization group into which the user enrolls.
Allow the user to enroll into additional Organization Groups	Choose whether or not to allow the user to enroll into more than one organization group. If you select **Enabled**, then complete the **Additional Organization Groups**.
User Role	Select the role for the user you are adding from this drop-down menu.
Notification	
Message Type	Choose the type of message you may send to the user, **Email**, **SMS**, or **None**. Selecting SMS requires a valid entry in the **Phone Number** text box.
Message Template	Choose the template for email or SMS messages from this drop-down setting. Optionally, select the **Message Preview** to preview the template and select the **Configure Message Templates** link to create a template.

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

Setting	Description
Advanced Info Section	
Email Password	Enter the email password of the user you are adding.
Confirm Email Password	Confirm the email password of the user you are adding.
Distinguished Name	For directory users recognized by Workspace ONE UEM, this text box is pre-populated with the distinguished name of the user. Distinguished Name is a string representing the user name and all authorization codes associated with an Active Directory user.

Setting	Description
Manager Distinguished Name	Enter the distinguished name of the user's manager. This text box is optional.
Category	Choose the user category for the user being added.
Department	Enter the user's department for your company's administrative purposes.
Employee ID	Enter the user's employee ID for your company's administrative purposes.
Cost Center	Enter the user's cost center for your company's administrative purposes.
Custom Attribute 1–5 (for Directory users only)	Enter your previously configured custom attributes, where applicable. You may define these custom attributes by navigating to **Groups & Settings > All Settings > Devices & Users > Advanced > Custom Attributes**. **Note** Custom attributes can be configured only at Customer organization groups.
Certificates Section	
Use S/MIME	Enable or disable the use of Secure/Multipurpose Internet Mail Extensions (S/MIME). If enabled, you must have an S/MIME-enabled profile and you must upload an S/MIME certificate by selecting **Upload**.
Separate Encryption Certificate	Enable or disable the use of a separate encryption certificate. If enabled, you must upload an encryption certificate using **Upload**. Generally, the same S/MIME certificate is used for signing and encryption, unless a different certificate is expressly being used.
Old Encryption Certificate	Enable or disable a legacy version encryption certificate. If enabled, you must **Upload** an encryption certificate.
Staging Section	
Enable Device Staging	Enable or disable the staging of devices. If enabled, you must choose between **Single User Devices** and **Multi User Devices**. If **Single User Devices**, you must select between **Standard**, where users themselves log in and **Advanced**, where a device is enrolled on behalf of another user.

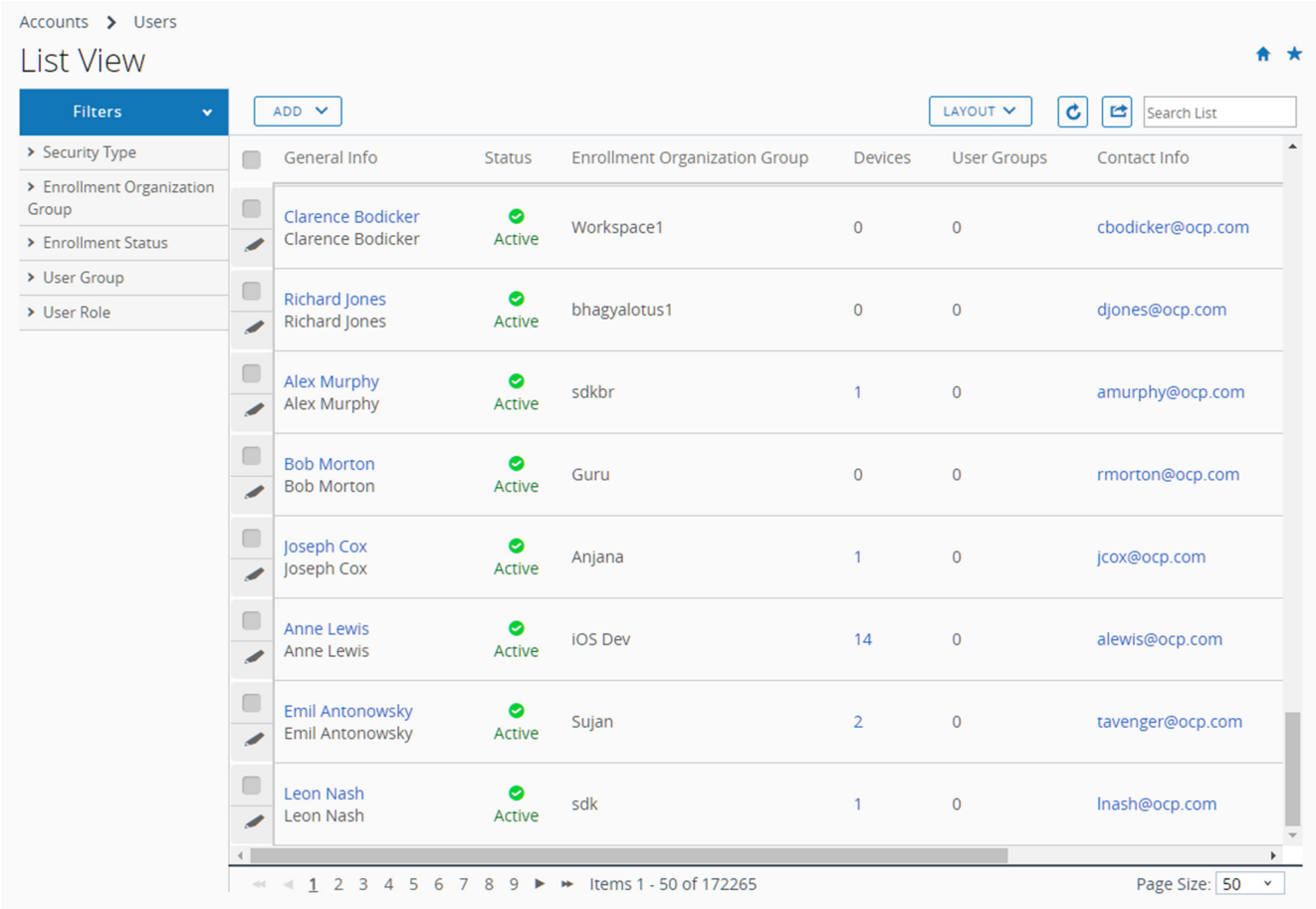
4 Select **Save** to save only the new user or select **Save and Add Device** to save the new user and proceed to the **Add Device** page.

What to do next

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

User Accounts List View

The **List View** page, which you can find by navigating to **Accounts > Users > List View**, provides useful tools for common user account maintenance and upkeep within Workspace ONE Express and Workspace ONE UEM powered by AirWatch.



Customize List View

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

Action	Description
Filters	View only the desired users by using the following filters. ■ Security Type ■ Enrollment Organization Group ■ Enrollment Status ■ User Group ■ User Role
Add	■ **Add User** – Perform a one-off addition of a basic user account. Add an employee or a newly promoted employee that needs access to MDM capabilities. For more information, see Create Basic User Accounts. ■ **Batch Import** – Add multiple users into Workspace ONE 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.

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 an XLSX or CSV (comma-separated values) file of the entire List View. Both file formats can be viewed and analyzed with MS Excel.

Interact with User Accounts

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

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

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

Action	Description
Send Message.	Provide immediate support to a single user or group of users. Send a User Activation (user template) email to a user notifying them of their enrollment credentials.
Add Device.	Add a device for the selected user. Only available for single user selections.
More Actions	Display the following options.
Add to User Group.	Add selected users to new or existing user group for simplified user management. For more information, see User Groups List View and Edit User Group Permissions.
Remove from User Group.	Remove selected users from the existing user group.
Change Organization Group	Manually move the user to a different organization group. Update the available content, permissions, and restrictions of a user if they change positions, get a promotion, or change office locations.
Delete	If a member of your organization permanently terminates employment, you can quickly and completely delete a user account. Deleting account information is the equivalent of the account never having existed in the first place. A deleted account cannot be reactivated. If a deleted account owner returns, a new account must be created for them.
Activate	Activate a previously deactivated account if a user returns to an organization or must be reinstated in the company.
Deactivate	Deactivation is a security measure. Deactivate is used when a user is missing in action, their device is out-of-compliance, or their device is lost or stolen. All the information about a deactivated account is kept, such as name, email address, password, enrollment organization group, and so forth. A deactivated account simply means no one with these account credentials will be able to log in while the account is deactivated. Once the security issue is resolved (user is located, device becomes compliant, the device is recovered) then you can Activate the account.

Batch Import Feature

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

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

Changes in External LDAP and AD User Directories

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

Users and Devices

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

User Groups

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

Editing Basic Users

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

Move Users Between Organization Groups

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

Batch Import Users or Devices

You can batch import multiple users and devices into the console. You can also visit the Batch Status page to check on the status of a batch job. Navigate to **Accounts > Users > Batch Status**.

The Batch Status screen displays a list of all batch import jobs you have requested, including the job's status.

To begin the process of batch importing users or devices, take the following steps.

Procedure

1 Navigate to **Accounts > Users > Batch Status** or **Devices > Lifecycle > Enrollment Status > Add** and select **Batch Import**.

2 Enter the basic information including a **Batch Name** and **Batch Description**.

3 Select the applicable batch type from the **Batch Type** drop-down menu.

4 Select and download the template that best matches the kind of batch import you are making.

- **Blacklisted Devices**

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

- **Whitelisted Devices**

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

- **User and/or Device**

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

- **Change Organization Group**

  Move users to a different organization group.

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

The CSV file features several columns corresponding to the options on the **Add / Edit User** page. When you open the CSV template, notice that sample data has been added to each column in the template. The sample data is presented to inform you what kind of data is required and what format it must be in. Do not stray from the format presented by the sample data.

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

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

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

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

6 Enter data for your organization's users, including device information (if applicable) and save the file.

7 Return to the Batch Import page and select **Choose File** to locate and upload the CSV file that you had previously downloaded and filled out.

8 Select **Save**.

Batch Import User Groups

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

Procedure

1. Navigate to **Accounts > User Groups > List View** and select **Add**.
2. Select **Batch Import**.
3. Enter the basic information including **Batch Name** and **Batch Description** in the Workspace ONE UEM console.
4. Under **Batch File (.csv)**, select the **Choose File** button to locate and upload the completed CSV file.
5. Alternately, select the link **Download template for this batch type** and save the comma-separated values (CSV) file and use it to prepare a new importation file.
   - Open the CSV file, which has several columns corresponding to the settings that display on the **Add User Group** page. Columns with an asterisk are required and must be entered with data. Save the file.
   - The last column heading in the CSV file template is labeled "GroupID/Manage (Edit and Delete)/ Manage(Users and Enrollment)/UG assignment/Admin Inheritance." This column heading corresponds to the settings and abides by the logic of the **Permissions** tab of the **Edit User Group** page. For details, see Edit User Group Permissions.
6. Select **Import**.
7. If the Batch Import does not complete successfully, view and troubleshoot errors by selecting **Accounts > Batch Status**. You can view specific batch import errors by clicking the **Errors** hyperlink.

Editing Basic Users with Batch Import

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

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

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

Move Users with Batch Import

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

Procedure

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

Admin Accounts

Administrator Accounts enable you to maintain settings, push, or revoke features and content, and much more with Workspace ONE UEM powered by AirWatch and Workspace ONE Express.

Create an Admin Account

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

Add, Edit, and Delete Admin Accounts

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

Temporary Admin Account

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

Create a Temporary Admin Account

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

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 and Workspace ONE Express. Each admin that maintains and supervises the console must have an individual account.

Procedure

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

Create a Temporary Admin Account

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

Procedure

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

   Alternatively, you can select the **Help** button from the header bar that appears at the top-right corner of almost every page of Workspace ONE UEM and Workspace ONE Express and select **Add Temporary Admin**.
2. In the **Basic** tab, select to add a temporary admin account based on **Email Address** or **user name** and complete the following settings.

Setting	Description
Email Address	Enter the email address on which the temporary admin account is based. Available only when Email Address radio button is selected.
User name	Enter the user name on which the temporary admin account is based. Available only when the user name radio button is selected.
Password / **Confirm Password**	Enter and confirm the password that is associated with the Email Address or user name.

Setting	Description
Expiration Period	Select an **Expiration Period** which defaults to 6 hours. You can also set this drop-down menu to **Inactive** to create the account now and activate it later.
Ticket Number	Optionally, you can add the Ask Ticket Number from ZenDesk as a reference marker.

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

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

4 Select **Save**.

Managing Admin Accounts

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

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

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

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

- **View History** – Track when admins log in and out of the Workspace ONE UEM console or Workspace ONE Express.
- **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 console. Such an action is useful for when an administrator ends employment.
- **Reset Password** – Available to basic administrators only. Sends an email to the basic admin's email address on record. The email contains a link that expires in 48 hours. To reset the password, the basic admin must select the link and answer the password recovery question. This enables the basic admin to change their own password.

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

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

For more information regarding syncing of account statuses, see Directory User Status Syncing.

Role-Based Access

4

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

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

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

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

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

Compare Two Admin Roles

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

This chapter includes the following topics:

Default and Custom Roles

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

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

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

Default End-User Roles

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

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

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

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

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

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

Procedure

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

Default Administrator Roles

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

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

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

Edit a Default Admin Role to Create a Custom Admin Role

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

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

Procedure

1. Ensure that you are currently in the organization group with which you want the new role to be associated.
2. Navigate to **Accounts > Administrators > Roles**.
3. Determine which role from the list best fits the role you want to create. Select the check box for that role.
4. Select **Copy** from the actions menu above the listing. The **Copy Role** page displays.
5. Edit specific settings of the copy in the resulting **Copy Role** page. Create a unique **Name** and **Description** for the customized role.
6. Select **Save**.

What to do next

For more information, see Create Administrator Role.

User Roles

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

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

Create a New User Role

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

Procedure

1. Navigate to **Accounts > Users > Roles** and select **Add Role**. The **Add/Edit Role** page displays.
2. Enter a **Name** and **Description**, and select the **Initial Landing Page** of the SSP for users with this new role.

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

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

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

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

What to do next

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

Configure a Default Role

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

Procedure

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

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

These role settings are customizable by organization group.

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

3 Select **Save**.

Assign or Edit the Role of an Existing User

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

Procedure

1 Select the appropriate organization group.

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

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

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

5 Select **Save**.

Admin Roles

Admin roles allow you to enable or disable permissions for every available setting and resource in the Workspace ONE UEM powered by AirWatch. 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**.

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.

View the Resources of an Admin Role

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

Edit Role

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

Compare Two Roles

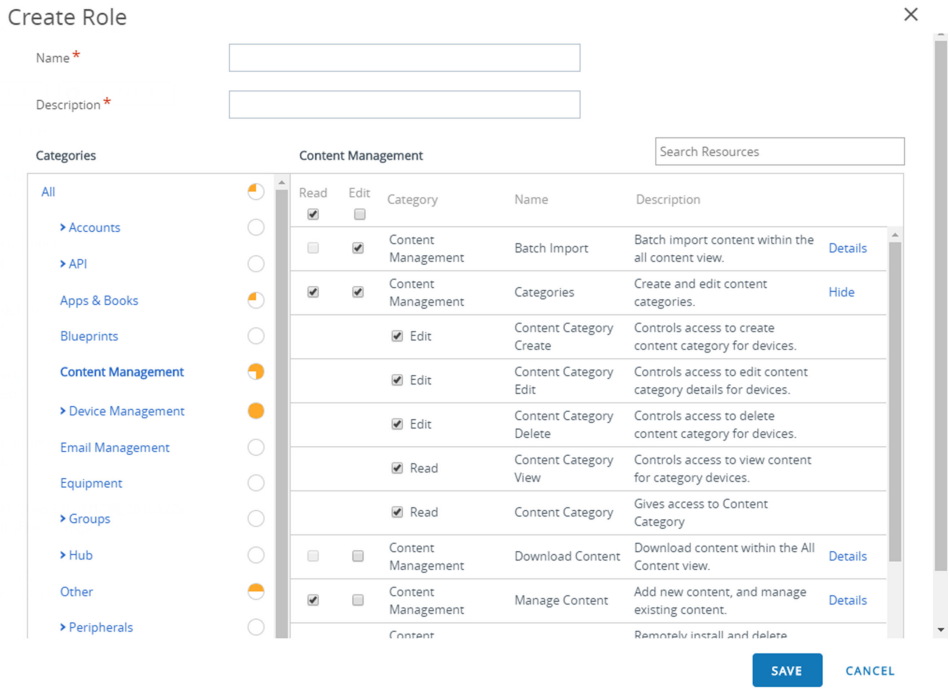
You can also compare the individual permissions settings between two roles. For more information, see Compare Admin Roles.

Create Administrator Role

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

Procedure

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



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

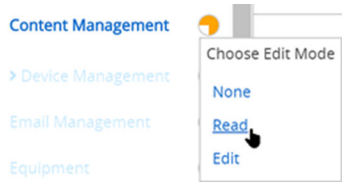
3 Select from the list of **Categories**.

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

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

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

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



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

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

What to do next

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

Import Admin Roles

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

Procedure

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

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

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

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

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

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

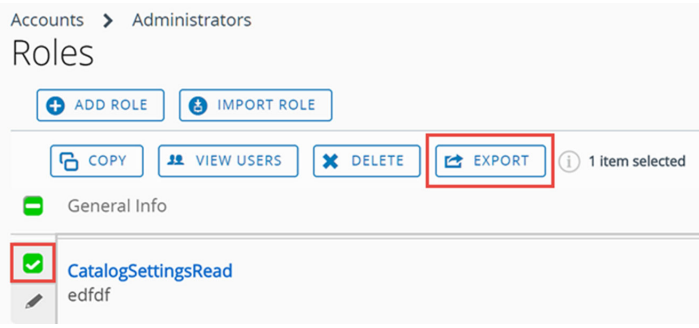
   b If you select No, then the existing role in your environment remains untouched and the role import is canceled.

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

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

Export Admin Roles

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



Procedure

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

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

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

Copy Role

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

Procedure

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

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

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

4 When finished, select **Save**.

Rename an Admin Role

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

Procedure

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

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

3 Select **Save**.

Versioning Issues When Importing and Exporting Admin Roles

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

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

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

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

Read/Edit Indicator in Categories for Admin Roles

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

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

All options in this category have the edit capability (which by definition means that they also have read-only capability).

Most category settings have the edit capability enabled, but edits are disabled for at least one subcategory.

All category settings have read-only enabled (edit disabled).

Most category settings are read-only, but edits are enabled for at least one subcategory.

Assign or Edit the Role of an Admin

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

Procedure

1 Navigate to **Accounts > Administrators > List View**, locate the admin account, and select the Edit icon in the Action button cluster. The **Add/Edit Admin** page displays.

2 Select the **Roles** tab. Then select **Add Role**.

3 Enter the **Organization Group** and **Role** details for each role that is added.

4 Select **Save**.

View the Resources of an Admin Role

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

Prerequisites

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

Procedure

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

What to do next

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

Admin Roles Compare Tool

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

The Compare Roles Tool allows you to see only the differences between two admin roles, which makes the comparison process fairly simple. Alternately, you can compare two admin roles to confirm and verify all the known similarities, which can be equally important.

Compare Admin Roles

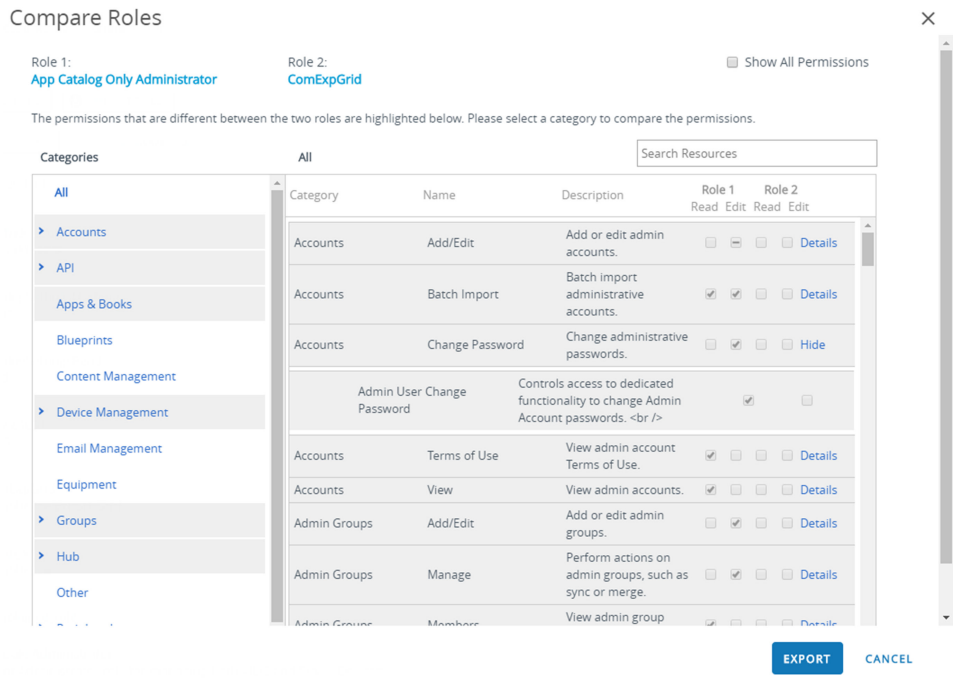
You can compare the permissions settings of any two administrator roles for the sake of accuracy or to confirm your deliberate settings differences.

Procedure

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

2 Locate any two listed roles, including roles that appear on different pages, and select those roles.

3 Select **Compare**. The **Compare Roles** page displays featuring a list of categories. Selecting a specific category on the left populates all the details of that category on the right.



- If you have fewer than two or more than two roles selected, the **Compare** button does not display.
- Role subcategories can be viewed in the right panel by selecting the **Details** link to the far-right side. Collapse the role subcategory by selecting the **Hide** link.
- There is an **All** category in the left panel that, when selected, displays all the parent categories on the **Compare Roles** page. When you enter a search parameter in the **Search Resources** bar, the right panel only displays matching category and resources (also known as permissions) listings.
- The search function is persistent. This persistence means that if you have a parameter in the **Search Resources** bar, selecting the **All** category displays only the matching categories and resources. The search function is persistent even after you select specific resources and make **Read** and **Edit** selections.

- By default, only those categories and subcategories whose settings are different are displayed. You can display all the permissions including those settings that are identical across the two selected roles by enabling the **Show All Permissions** check box.
- If you select two roles that have identical permissions across the board, the console displays this message at the top of the **Compare Roles** page.

  "There are no differences in permissions between the two roles.".

What to do next

You can optionally select **Export** to create an Excel-viewable XLSX or CSV file (comma-separated values). The export file contains all settings for Role 1 and Role 2, enabling you to analyze the differences between them.

How Do You Create a Restrictive Help Desk Admin and Add a Role Giving it Specific Functions?

You can make a custom role that allows a help desk admin to do only the things you allow them to do. Follow this use case to learn how accounts, roles, and programmable permissions all work together to get you where you need to go.

Use Case: You have a need for dedicated help desk resources to shoulder the task of adding users and devices without impacting your other administrators. These admins must also be able to whitelist and blacklist devices. At the same time, limiting the points of access to higher console abilities is crucial. You want to add a handful of admin accounts and give these accounts the ability to add users and devices, whitelist and blacklist devices, and nothing else.

The role being made in this use case is outfitted with just a handful of console functions: adding users and devices, and whitelisting and blacklisting devices. All other Workspace ONE UEM functions are prohibited by this role.

Prerequisites

You must have an existing administrator account. This use case makes a custom role based on the "help desk" role, which comes with Workspace ONE UEM powered by AirWatch, and assigns it to your admin account.

Procedure

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

  The full listing of Administrator Roles displays.

2 Enter the keyword 'help' in the search text box in the upper-right corner of the screen.

  All roles containing the text string 'help' display in the listing.

3 Choose the **Help Desk** role by selecting the check box to the left of the role name.

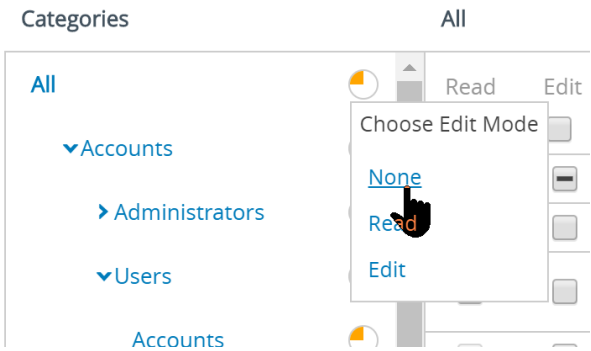
  A new button cluster appears under the main button cluster.

4 Select the **Copy** button.

The **Copy Role** screen displays.

5 Enter the **Name** and **Description** for your custom help desk role.

6 Select the orange pie chart to the right of the **All** category on the left side of the **Copy Role** screen. Select **None** from the **Choose Edit Mode** popup that displays.



This action removes all permissions from this custom help desk role, giving you a clean slate. So the only permissions these admins have going forward are the ones you give them here.

7 Enable the following 9 permissions. You can find the location of each permission check box by following the category, subcategory, and permission name from the table.

Category > Subcategories	Permission Name (check box)
Accounts > Users > Accounts	User Accounts Add (Edit)
Accounts > Users > Accounts	User Registration Edit (Edit)
Accounts > Users > Accounts	User Accounts Edit (Edit)
Accounts > Users > Accounts	User Accounts Add (Edit)
Accounts > Users > Accounts	User Registration (Read)
Device Management > Devices List View	Device List View Access (Read)
Device Management > Devices List View	Devices (Read)
Settings > Devices & Users > General	Add Blacklisted Device (Edit)
Settings > Devices & Users > General	Add Whitelisted Device (Edit)

Starting at the top of the table, let's walk-through the first row as an example. The permission we need (called User Accounts Add) can be found in the **Copy Role** screen by selecting the "Account" category from the left panel.

In the same left panel, select the "Users" subcategory and lastly, select "Accounts" which is under Users. You can now see all the permissions in the right panel of the **Copy Role** screen.

In this "Users > Accounts" subcategory, there are 5 check boxes we are interested in. Enable those check boxes as indicated in the table. "User Account Add" gets the Edit check box, "User Registration Edit" gets the Edit check box, and so forth. Follow the same process for the remaining 4 permissions.

8 Select **Save** to finalize the custom help desk role definition.

9 Assign this custom role to your existing administrator account by navigating to **Accounts > Administrators > List View** and locate your administrator account from the listing.

10 Select the Edit icon ( ) to the left of your admin account.

The **Add/Edit Admin** screen displays.

11 Select the **Roles** tab.

12 Assign the custom help desk role to the administrator account.

While this use case dictates that only nine UEM Console functions be assigned to your administrator role, you can add this custom help desk role and other roles to your admin account, even if your admin account already has one or more roles assigned to it.

13 Select **Save** to finalize the role assignment.

Results

When administrators with only this custom help desk role log into your Workspace ONE UEM environment, the only functions they have access to is the **Add** button, from which they can only select from two choices: Device and User. They also have access to the **Devices** main menu button which includes **List View** and **Lifecycle > Enrollment Status**, which is where you add whitelisted and blacklisted devices.

Groups

5

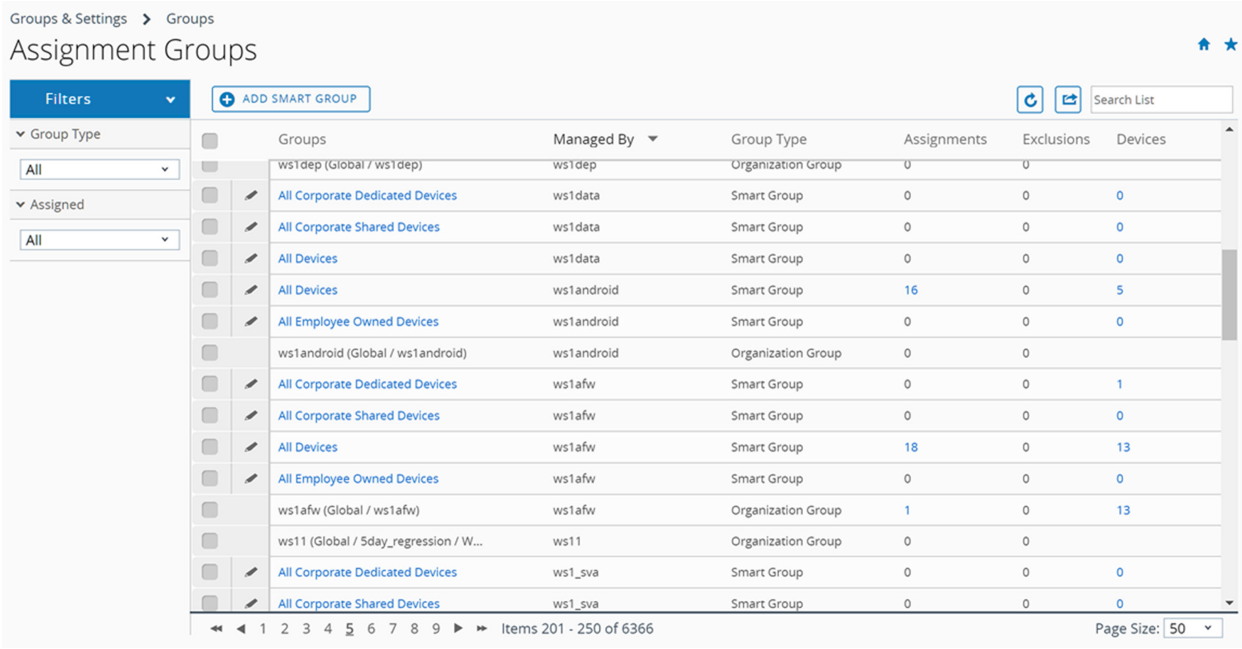
Workspace ONE UEM powered by AirWatch uses several different types of groups to manage users, devices, apps, content, and more.

This chapter includes the following topics:

Assignment Groups

Assignment Groups is an umbrella term used to categorize certain management grouping structures within Workspace ONE UEM powered by AirWatch. Organization Groups, Smart Groups, and User Groups each have full feature sets and properties and are distinct from each other. One element they have in common is the way they can be used to assign content to user devices easily. Assignment Groups enables an administrator to manage these three grouping structures from a single location.

Navigate to **Groups & Settings > Groups > Assignment Groups**.



You can use the list view to assign multiple organization groups, smart groups, and user groups to one or more profiles, public applications, and policies.

Assignment Group List View

The Assignment Groups List View organizes three kinds of groups that have the function of assigning content to devices: organization groups, smart groups, and user groups. You can create a listing of only those groups you are interested in seeing.

Navigate to **Groups & Settings > Groups > Assignment Groups** and the Assignment Groups List View displays. The only assignment groups listed for viewing are those managed by the OG that the administrator is currently in.

Sort by Columns

You can sort the listing of groups by individual columns by selecting the column header.

Filter Groups

You can filter groups by **Group Type** (Smart Groups, Organization Groups, and User Groups). You can also filter by how or whether they have been **Assigned** (Assignments, Exclusions, All, and None).

Select Links in the Assignment Groups Listing

Four columns in the Assignment Groups Listing page serve a specific function and require a special mention.

- The **Groups** column features a link for each **Smart Group**. You can select this link to edit the smart group.

- If you select non-zero values in the **Assignments** column, the View Assignments page displays, even for assigned organization groups and user groups. This function allows you to view and confirm assignments to profiles, public applications, and compliance policies. For more information, see View Assignments.
- If you select non-zero values in the **Exclusions** column, the View Assignments page displays, even for excluded organization groups and user groups. The View Assignments page allows you to view and confirm exclusions from profiles, public applications, and compliance policies.
- If you select the **Devices** column number, the Devices List View page displays. The Device List View contains the listing of all devices in the selected organization group, smart group, or user group. For more information, see the Workspace ONE UEM Managing Devices Documentation.

Assign One or More Assignment Groups

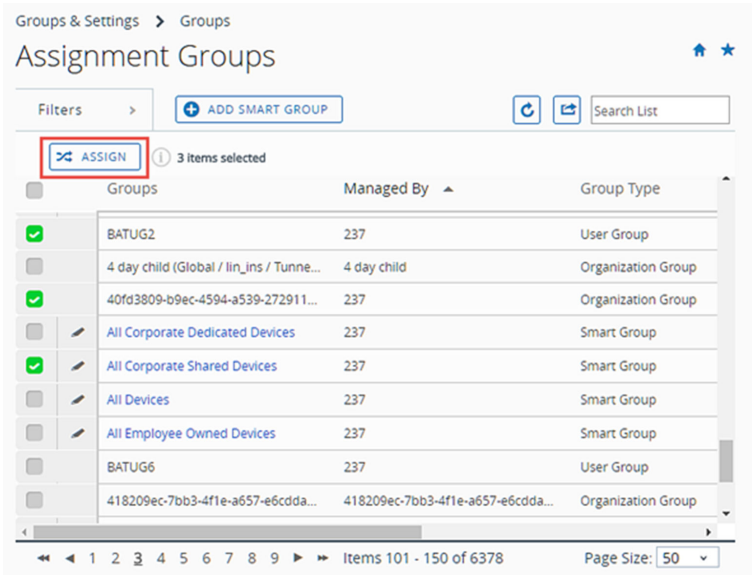
You can assign groups to device profiles, public applications, and compliance policies. You can also assign multiple groups of each individual type (organization, smart, or user) in a single sitting.

To assign public applications, you can configure different app policies for different groups of users. For more information, see **Use Flexible Deployment to Assign Applications** in the **VMware Workspace ONE UEM Mobile Application Management Guide**, which can be found on docs.vmware.com.

Procedure

1 Navigate to **Groups & Settings > Groups > Assignment Groups**.

2 Select one or more groups in the listing and select **Assign** above the column header.



3 The **Assign** page displays the **Organization Groups**, **Smart Groups**, and **User Groups** you selected.

4 Assign them by initiating a search for a **Profile**, a **Public Application**, and **Compliance Policy**. You may choose up to 10 profiles, up to 10 public applications, and a single compliance policy.

   You can only choose multiple entities of a single type per session. For example, you may assign multiple groups to up to 10 different profiles in a single command. However, you may not, in a single command, assign multiple groups to 10 profiles, 10 apps, **and** a compliance policy. If you have multiple entities of multiple types, you must undertake separate assignment sessions for each type (profiles, apps, and policies).

5 Select **Next** to display the **View Device Assignment** page which you can use to confirm the groups assignment.

6 Select **Save & Publish** to finalize the assignment.

Organization Groups

Think of organization groups as individual branches on a family tree, with each leaf as a device user. Workspace ONE UEM powered by AirWatch identifies each leaf and establishes its standing in the family tree using organization groups (OG). Most customers make OG trees look like their corporate hierarchy: Executives, Management, Operations, Sales, and so forth.

You can also establish OGs based on Workspace ONE UEM features and content.

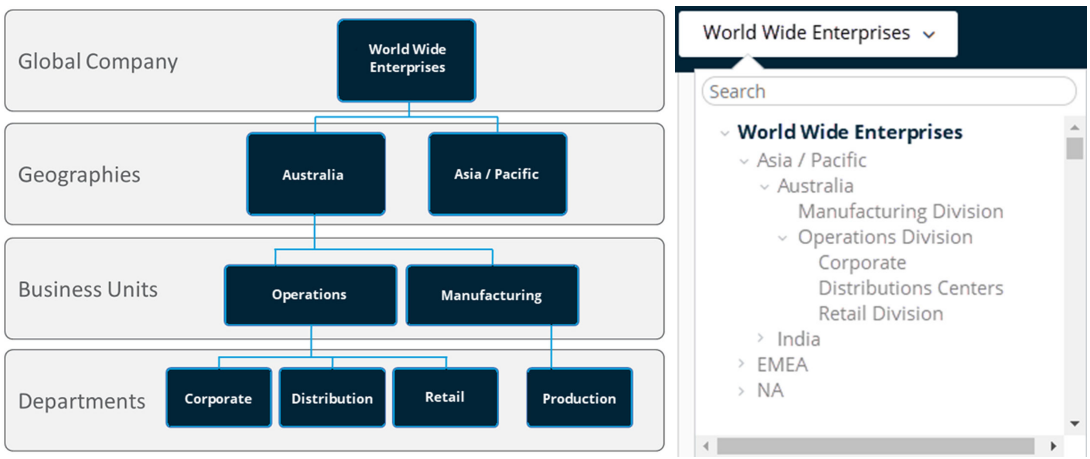
You can access organization groups by navigating to **Groups & Settings > Groups > Organization Groups > List View** or through the organization group drop-down menu.

- Build groups for entities within your organization (Management, Salaried, Hourly, Sales, Retail, HR, Exec, and so on).
- Customize hierarchies with parent and child levels (for example, 'Salaried' and 'Hourly' as children under 'Management').
- Integrate with multiple internal infrastructures at the tier level.
- Delegate role-based access and management based on a multi-tenant structure.

Characteristics of Organization Groups

Organization groups can accommodate functional, geographic, and organization entities and enable a multi-tenancy solution.

- **Scalability** – Flexible support for exponential growth.
- **Multi-tenancy** – Create groups that function as independent environments.
- **Inheritance** – Streamline the setup process by setting child groups to inherit parent configurations.



Using the example of the organization group drop-down menu, profiles, features, applications, and other MDM settings can be set at the 'World Wide Enterprises' level.

Settings are inherited down to child organization groups, such as **Asia/Pacific** and **EMEA** or even further down to grand-child **Australia > Manufacturing Division** or even great grand-child **Australia > Operations Division > Corporate**.

Settings between sibling organization groups such as **Asia/Pacific** and **EMEA** take advantage of the multi-tenant nature of OGs, by keeping these settings separate from one another. However, these two sibling OGs do inherit settings from their parent OG, **World Wide Enterprises**.

Alternatively, you can opt to override settings at a lower level and alter only the settings that you want to change or keep. These settings can be altered or carried down at any level.

Considerations for Setting Up Organization Groups

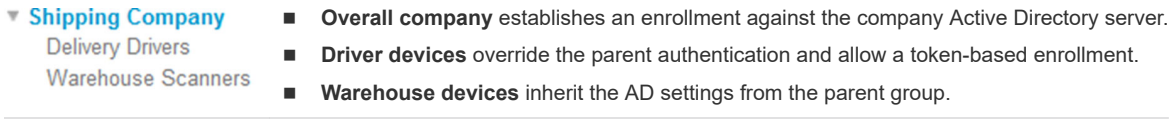
Before setting up your organization group (OG) hierarchy in the Workspace ONE UEM console, first decide on the group structure. The group structure allows you to make the best use of settings, applications, and resources.

- **Delegated Administration** – You can delegate administration of subgroups to lower-level administrators by restricting their visibility to a lower organization group.

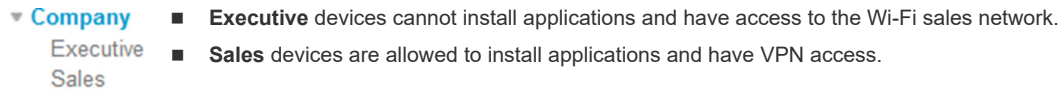
Retail Company
LA store
NY store

- **Corporate administrators** can access and view everything in the environment.
- **LA manager** has access to the LA OG and can manage only those devices.
- **NY manager** has access to the NY OG and can manage only those devices.

- **System Settings** – Settings can be applied at different levels in the organization group tree and inherited down. They can also be overridden at any level. Settings include device enrollment options, authentication methods, privacy setting, and branding.



- **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.



Override Versus Inherit Setting for Organization Groups

The hierarchy of the organization group (OG) structure you make determines which OGs are children and which are parents. Child OGs inherit settings from their parent OGs but you can elect to override this inheritance.

Each system settings page applies its settings according to two types of inheritance / override options where organization group hierarchy is concerned: 1) Current Setting and 2) Child Permission. The OG it applies settings to is the OG you are currently in.

For example, the **Branding** settings page found by navigating to **Groups & Settings > All Settings > System > Branding** control all the custom background images, logos, and color schemes for the OG on display in the organization group drop down.

Change OGs and you now have the option to import a new background image, new logo, a different color scheme, all specific to that OG. This option is enabled by changing the inheritance of the OGs on the settings page.

Child Permission

Think of the Child Permission setting as the parent OG's attitude toward the child OG. There are three different settings for Child Permission: **Inherit or Override**, **Inherit Only**, and **Override Only**.

The **Inherit or Override** setting simply means that the parent has no preference for the child's permissions. When a parent's Child Permission setting is **Inherit or Override**, the Current Setting of the child OG determines whether they override or inherit settings. Child Permissions are set to **Inherit or Override** by default.

A Child Permission setting of **Inherit Only** on the parent forces inheritance on all children. This means all children have the same settings as the parent. A Child Permission setting of **Override Only** removes the inheritance effect on all child OGs, requiring you to configure settings specific to that child OG.

Child Permission settings affect only the children one level down. Such settings have no impact on grandchildren or lower OGs.

Current Setting

If Child Permission is the parent's attitude toward the child, then the Current Setting of an OG is the child's attitude toward the parent. An OG's Current Setting can only be **Inherit** or **Override**.

A Current Setting of **Inherit** means the child OG accepts all the settings of the parent OG. Select a Current Setting of **Override**, and the child rejects the parent and is on its own. This means you can make new settings for the child.

You can only change an OG's Current Setting provided the parent OG's Child Permission setting is **Inherit or Override**.

Changing Permission Settings

You cannot change the Current Setting of a child if its parent's Child Permission setting doesn't allow it. For example, if MomandDadOG's Child Permission setting is **Override Only**, you cannot change the Current Setting of JuniorOG to **Inherit**. In short, the parent OG's Child Permission settings take precedence.

When you change the Current Settings of a child from **Override** to **Inherit**, changing the Child Permission setting of its parent to **Inherit Only** has the effect of locking the child OG's Child Permission setting such that you cannot change it. This behavior does not apply if the child OG setting is never overridden.

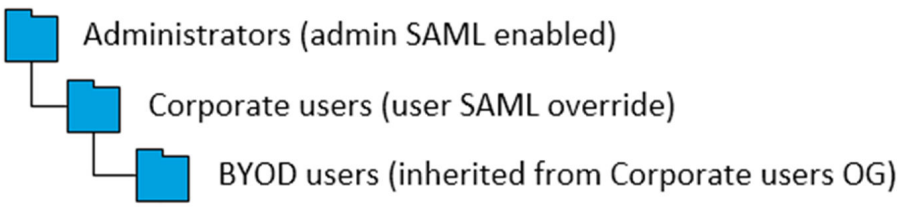
The work-around to this behavior is that you must change the Child Permission settings on the parent OG back to **Inherit or Override**, unlocking the Child Permission setting of the child OG.

The larger strategy is to plan in advance, configuring inheritance and override settings to the OG levels that make sense given the hierarchy structure you want.

Inheritance, Multi-Tenancy, and Authentication

The concept of overriding settings on a per-organization group basis, when combined with organization group (OG) characteristics such as inheritance and multi-tenancy, can be further combined with authentication. This combination provides for flexible configurations.

The following organization group model illustrates this flexibility.



In this model, **Administrators**, generally in possession of greater permissions and functionality, are positioned at the top of this OG branch. These administrators log into their OG using SAML that is specific to admins.

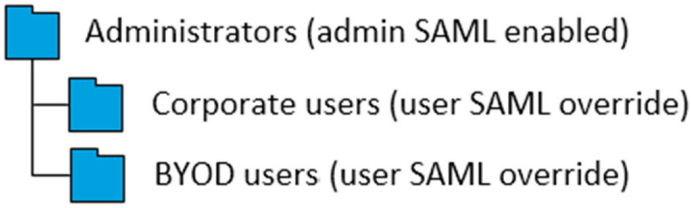
Corporate users are subservient to administrators so their OG is arranged as its child. Being users and not administrators, their SAML login setting cannot inherit the administrator setting. Therefore, the Corporate users' SAML setting is overridden.

BYOD users differ from Corporate users. Devices used by BYOD users belong to the users themselves and likely contain more personal information. So these device profiles might require slightly different settings. BYOD users might have a different terms of use agreement. BYOD devices might need different enterprise wipe parameters. For all these reasons and more, it might make sense for BYOD users to log into a separate OG.

And while not subservient to Corporate users in a corporate hierarchy sense, placing BYOD users as a child of Corporate users has advantages. This arrangement means that BYOD users inherit settings applicable to ALL corporate user devices simply by applying them to the Corporate users OG.

Inheritance also applies to SAML authentication settings. Since BYOD users is a child of Corporate users, BYOD users inherit their SAML for users' authentication settings.

An alternate model is to make BYOD users a sibling of Corporate users.



Under this alternate model, the following is true.

- All device profiles meant to apply globally to ALL devices, including compliance policies, and other globally applicable device settings are applied to two organization groups instead of one. The reason for this duplication need is because inheritance from Corporate users to BYOD users is no longer a factor in this model. Corporate users and BYOD users are peers and therefore there is no inheritance.
- Another SAML override must be applied to BYOD users. This override is necessary because the system assumes it is inheriting SAML settings from its parent, Administrators. Such an assumption is a mistake because BYOD users are not administrators and do not have the same access and permissions.
- BYOD users continue to be handled separately from Corporate users. This alternate model means that they continue to enjoy their own device profile settings.

What factor determines which model is the best? Compare the number of globally applicable device settings with the number of group-specific device settings. Basically, if you want to treat all devices in generally the same way, then consider making BYOD users a child of Corporate users. If maintaining separate settings is more important, then consider making BYOD users a sibling of Corporate users.

Create Organization Groups

You must create an organization group (OG) for each business entity where devices are deployed. Understand that the OG you are currently in is the parent of the child OG you are about to create.

Procedure

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

2 Select the **Add Child Organization Group** tab and complete the following settings.

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

3 Select **Save**.

Organization Group Type Functions

The type of an organization group can have an impact on what settings an admin can configure.

- **Global** – The top-most organization group. Usually, this group is called Global and has type Global.
  - For hosted SaaS environments, you are not able to access this group.
  - On-premises customers can turn on Verbose logging at this level.
- **Partner** – Top-level organization group for partners (third-party resellers of Workspace ONE UEM).
- **Customer** – The top-level organization group for each customer.
  - A customer organization group cannot have any children/parent organization groups that are of the customer type.
  - Some settings can only be configured at a Customer group. These settings filter down to lower organizations. Some examples of such settings include autodiscovery email domains, Volume Purchase Program settings, Device Enrollment Program settings (before AirWatch 8.0), and personal content.
- **Container** – The default organization group type.
  - All organization groups beneath a customer organization group must be of the container type. You can have containers between Partner and Customer groups.

- **Prospect** – Potential customers. Similar to a customer organization group. Might have less functionality than a true customer group.

There are additional Organization Group types such as Division, Region, and the ability to define your own Organization Group type. These types do not have any special characteristics and function identically to the Container Organization Group type.

Adding Devices at Global

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

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

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.

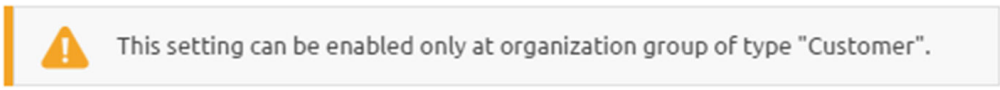
Functionality

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.

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.



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

- Whether you are in a software-as-a-service (SaaS) or on-premises environment, you cannot create nested customer OGs.

Organization Groups Settings Comparison

As an Administrator, you might find it useful to compare the settings of one organization group (OG) to another.

The following are available when you compare OG settings.

- Upload XML files containing the OG settings from different Workspace ONE UEM software versions.
- Eliminate the possibility of a difference in configuration causing problems during version migration.
- Filter the comparison results, allowing you to display only the settings you are interested in comparing.
- Search for a single setting by name with the search function.

The Organization Group Compare feature is only available for on-premises customers.

Compare Two Organization Groups

You can compare the settings of one organization group to another to mitigate version migration issues.

An example of a version migration scenario is when a User Acceptance Testing (UAT) server has been upgraded, configured, and tested, you can compare the UAT settings to the production settings directly.

Procedure

1. Navigate to **Groups & Settings > All Settings > Admin > Settings Management > Settings Comparison**.
2. Select an OG in your environment from the left drop-down menu (labeled with the numeral **1**). Alternatively, upload the XML settings file by selecting the **Upload** button and selecting an exported OG setting XML file.
3. Select the comparison OG on the right drop-down menu (labeled with the numeral **2**).
4. Display a list of all settings for both selected organization groups by selecting the **Update** button.
   - Differences between the two sets of OG settings are automatically highlighted.
   - You can optionally enable the **Show Differences Only** check box. This check box displays only those settings that apply to one OG but not the other.
   - Individual settings that are empty (or not specified) display in the comparison listing as 'NULL'.

Smart Groups

Smart groups are customizable groups within Workspace ONE UEM powered by AirWatch that determine which platforms, devices, and users receive an assigned application, book, compliance policy, device profile, or provision.

When you create organization groups, you typically base them on the internal corporate structure: geographical location, business unit, and department. For example, "North Sales," "South HR." Smart groups, however, offer the flexibility to deliver content and settings by device platform, model, operating system, device tag, or user group. You can even deliver content to individual users across multiple organization groups.

You can create smart groups when you upload content and define settings. However, their modular nature means you can also create them at any time, so they are available to be assigned later.

The main benefit of smart groups is their reusability. It might be intuitive to make a new assignment every time you add content or define a profile or policy. Instead, if you define assignees to smart groups only once, you can simply include those smart groups in your definition of content.

Create and Assign a Smart Group

You can create a smart group defined by platform, ownership, user group, OS version, model, device tag, enterprise OEM, and even individual devices by friendly name.

For example, you can make a smart group containing all employee-owned iPhone Touch devices with iOS version earlier than 9.0.2. Add to this same smart group all Android devices by HTC version 2.0 with OS version 4.1 or greater. Out of this group, you can exclude devices in the user group "full time." To this highly customized pool of *devices, you can assign 10 device profiles, 10 applications, or a compliance policy.

*Some restrictions might apply due to the multiplatform nature of this customized device pool. For example, there might be apps you want to assign that do not offer an Android version.

You can assign a smart group two ways. First, from the Assignment Groups List View after the smart group has been saved. Second, from the Assignment Groups setting which is found on multiple device product creation screens.

Create a Smart Group

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

Procedure

1. Select the applicable **Organization Group** (OG) to which your new smart group applies and from which it can be managed. Selecting an OG is optional.
2. Navigate to **Groups & Settings > Groups > Assignment Groups** and then select **Add Smart Group**.
3. Enter a **Name** for the smart group.
4. Optionally, you can enable the **Device Preview** to see which devices are included in the smart group you have designed. This device preview is disabled by default to improve performance.
5. Configure the smart group type.
   - **Criteria**

The **Criteria** option works best for groups with large numbers of devices (more than 500) that receive general updates. This method works best because the inherent details of these groups can reach all endpoints of your mobile fleet.

- **Devices or Users**

  The **Devices or Users** option works best for groups with smaller numbers of devices (500 or fewer) that receive sporadic, although important, updates. This method works best because of the granular level at which you can select group members.

Switching between **Criteria** and **Devices or Users** erases any entries and selections you might have made.

a In the **Criteria** type, select qualifying parameters to add in the smart group. If no selection is made in any setting, then that filtering is not applied toward the criteria.

Setting	Description
Organization Group	This criteria option filters devices by organization groups selected. You can select more than one OG.
User Group	This criteria option filters devices by user groups selected. You can select more than one user group.
Ownership	This criteria option filters devices by ownership type selected.
Tags	This criteria option filters devices according to the way they are tagged. You can select more than one tag.
Platform and Operating System	This criteria option filters devices by platform and OS selected. You can select multiple combinations of each. While Platform is a criterion within a smart group, the platform configured in the device profile or compliance policy always takes precedence over the smart group's platform. For instance, if a device profile is created for the iOS platform, the profile is only assigned to iOS devices even if the smart group includes Android devices.
Model	This criteria option filters devices by device model. Individual models displayed are based on the selections made in **Platform and Operating System**. You can select (or exclude) from this list of models.
Enterprise OEM Version	This criteria option filters devices by their original equipment manufacturer version. You can select more than one OEM.
Management Type	Filter devices according to the way the device is managed.
Enrollment Category	Filter devices according to the way the device is enrolled.
Additions	This criteria option adds individual devices and users that are not included in the filtering criteria. You can select more than one device and more than one user.
Exclusions	This criteria option excludes individual devices, individual users, and user groups that are included in the filtering criteria. You can exclude more than one device, more than one user, and more than one user group.

b Use the **Devices or Users** type to assign content and settings to special cases outside of the general enterprise mobility criteria. Enter the device friendly name in **Devices** and user name (first name or last name) in **Users**. You must **Add** at least one device or user or you cannot save the smart group.

Setting	Description
Devices	Add a device to this Smart Group by entering the device friendly name. You can add more than one device using this method.
Users	Add users to this smart group by entering the user name, first name, or last name. You can add more than one user using this method.

6 Select **Save** when complete.

Smart Group Assignment

Once you have created the smart group representing users and their devices and before it can take effect, you must assign it to at least one device product. You can assign it to an application, book, compliance policy, device profile, or product provision.

There are two methods to assign a smart group: assigning a smart group while creating the device product and assigning a smart group while managing the smart group itself.

Assign Smart Group While Creating Device Product

You can assign a smart group when you add or create an application, book, compliance policy, device profile, or product provision.

Procedure

1 Complete the **Assigned Groups** drop-down menu.

2 Select a smart group from the drop-down menu. Smart groups available are managed only within the organization group (OG) to which the resource is being added, or to a child OG below it.

3 If no smart group matches the desired assignment criteria, then select the **Create a Smart Group** option. You can assign more than one smart group per application, book, compliance policy, device profile, or product provision.

4 Select **Save** to include the assignment.

Assign Smart Group While Managing the Smart Group

You can also assign a smart group during the process of managing the smart group itself.

Procedure

1 View the entire list of smart groups by navigating to **Groups & Settings > Groups > Assignment Groups**.

2 Select one or more smart groups you want to assign and select **Assign**. The **Assign** page displays. Select the Groups link at the top of the **Assign** page to display the **Groups** page. On this page, the organization groups that manage the smart groups are displayed. Return to the Assign page by selecting the **Close** button.

3 On the **Assign** page, use the search box to view the list of eligible products and assign it to the selected smart groups.

4 Select **Next** to display the **View Device Assignment** page and confirm the assignment status.

5 Select **Save & Publish**.

Exclude Groups in Profiles and Policies

You can exclude groups from the assignment of device profiles and compliance policies with as much ease as assigning groups to these device products.

Prerequisites

You must have the groups defined before you initiate this task. At a minimum, you must be able to make a smart group comprised of the users you want to exclude. This task allows you to make a new smart group on the fly but if you prefer to exclude an organization group or user group, then see Create Organization Groups, Add User Groups with Directory Integration, or Add User Groups Without Directory Integration, Custom respectively.

Procedure

1 While adding a device profile or compliance policy, select **Yes** next to the **Exclusions** setting to display the **Excluded Groups** option.

2 In the **Excluded Groups** setting, select groups that you want to exclude from the assignment of this profile or policy.

- You can enter the first few letters of the group by name and the auto-search function shows you all the groups whose name corresponds to the string you entered.
- You can select one or more organization groups, user groups, or smart groups.
- You can make a new smart group by selecting the **Create Smart Group** button.

3 Select **Save and Publish** (for device profiles) or **Next** (for compliance policies) and continue the process for those tasks.

Results

If you select the same group in both the **Assigned Groups** and **Excluded Groups** settings, then the profile or policy fails to save.

Example

You want a compliance policy to apply to all device users except executives.

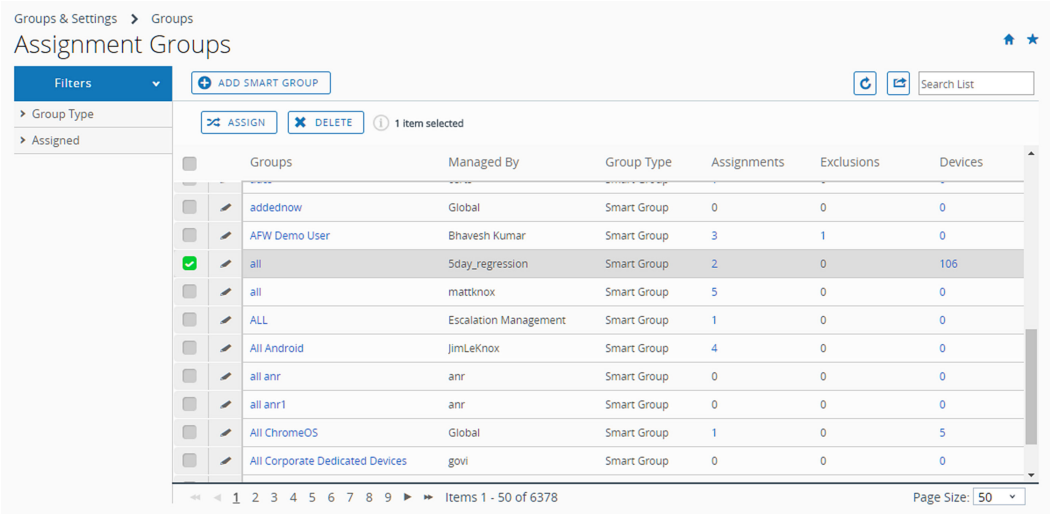
What to do next

Preview the affected devices by selecting **View Device Assignment**.

Smart Group List View

Manage your smart groups by editing, assigning, unassigning, excluding, and deleting them with the Workspace ONE UEM console.

View the entire list of smart groups by navigating to **Groups & Settings > Groups > Assignment Groups**. Admins can only see groups which they can manage based on their permissions settings.



The columns **Groups**, **Assignments**, **Exclusions**, and **Devices** each feature links which you can select to view detailed information.

- Selecting links in the **Assignments** or **Exclusions** columns display the **View Smart Group Assignments** screen.
- Selecting a link in the **Devices** column displays the **Devices > List View** showing only those devices included in the smart group.
- You can **Filter** your collection of groups by **Group Type** (Smart, Organization, User, or all) or by **Assigned** status. Assigned status shows whether the group is assigned, is excluded, both, or neither.
- You can **Assign** a smart group directly from the listing.

Edit a Smart Group

You can edit an established smart group. Any edits that you apply to a smart group affects all policies and profiles to which that smart group is assigned.

Procedure

1 Navigate to **Groups & Settings > Groups > Assignment Groups**.

2 Select the **Edit** icon ( ) located to the left of the listed smart group that you want to edit. You can also select the smart group name in the **Group** column. The **Edit Smart Group** page displays with its existing settings.

3 In the **Edit Smart Group** page, alter **Criteria** or **Devices and Users** (depending upon which type the smart group was saved with) and then select **Next**.

4 In the **View Assignments** page, you can review which profiles, apps, books, provisions, and policies can be added or removed from the devices as a result.

5 Select **Publish** to save your smart group edits. All profiles, apps, books, provisions, and policies tied to this smart group update their device assignments based on this edit.

Results

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

Example

Here is an example of a typical need to edit a smart group. Assume a smart group for executives is assigned to a compliance policy, device profile, and two internal apps. If you want to exclude some of the executives from one or more of the assigned content items, then simply edit the smart group by specifying **Exclusions**. This action prevents not only the two internal apps from being installed on the excluded executives' devices but also the compliance policy and device profile.

Delete a Smart Group

When you have no further use for a smart group, you can delete it.

You can only delete one smart group at a time. Selecting more than one smart group causes the **Delete** button to be unavailable.

Prerequisites

The smart group cannot be assigned to any device product. If a smart group is assigned, you are not permitted to delete it. See Unassign a Smart Group.

Procedure

1 Navigate to **Groups & Settings > Groups > Assignment Groups** and locate the smart group you want to delete from the listing.

2 Select the check box to the left of the smart group you want to delete.

3 Select **Delete** from the actions menu that displays.

Results

The unassigned smart group has been removed.

Unassign a Smart Group

You can unassign a smart group from an application, book, channel, policy, profile, or product. This action removes the associated content from all devices in the smart group.

Procedure

1. To unassign smart groups from applications, books, compliance policies, device profiles, or product provisions. Follow the navigation paths shown.
   - **Applications** – Navigate to **Apps & Books > Applications > List View** and select the **Public**, or **Internal** tab.
   - **Books** – Navigate to **Apps & Books > Books > List View** and select the **Public**, **Internal**, or **Web** tab.
   - **Channels** – Navigate to **Content > Video > Channels**.
   - **Compliance Policy** – Navigate to **Devices > Compliance Policies > List View**.
   - **Device Profile** – Navigate to **Devices > Profiles & Resources > Profiles**.
   - **Product Provision** – Navigate to **Devices > Provisioning > Products > List View**.
2. Locate the content or setting from the listing and select the **Edit** icon from the actions menu.
3. Select the **Assignment** tab or locate the **Assigned Smart Groups** text box.
4. Select Delete (**X**) next to the smart group that you want to unassign. This action does not delete the smart group. It simply removes the smart group assignment from the saved setting.
5. Follow the required steps to **Save** your changes.

Research Smart Group Events Using Console Event Logger

You can track the changes to smart groups, and when they were made and by whom, by using the **Console Event** logger. Such tracking can be useful when troubleshooting devices.

Procedure

1. Navigate to **Monitor > Reports & Analytics > Events > Console Events**.
2. Select **Smart Groups** from the **Module** drop-down filter at the top of the **Console Event** listing.
3. Apply more filters as you might require including **Date Range**, **Severity**, and **Category**.
4. Where applicable, select the hypertext link in the **Event Data** column which contains extra detail that can assist your research efforts.

User Groups

You can group sets of users into user groups which, like organization groups, act as filters for assigning profiles and applications. When configuring your environment in Workspace ONE UEM powered by AirWatch, align user groups with security groups and business roles within your organization.

You can assign profiles, compliance policies, content, and applications to users and devices with user groups. You can add your existing directory service groups into Workspace ONE UEM or create user groups from scratch.

As an alternative to user groups, you can also manage content by assigning devices according to a preconfigured range of network IP address or custom attributes.

User Groups Without Directory Integration, Custom

Creating a user group outside of your existing Active Directory structure allows you to create specialized groups of users at any time. Customize user groups according to your deployment by specifically designing access to features and content.

For instance, you can create a temporary user group for a specific project requiring specialized apps, device profiles, and compliance policies.

For more information about adding user groups in bulk, see Batch Import User Groups.

Add User Groups Without Directory Integration, Custom

You can establish a custom user group outside of your corporate structure, which might be preferred depending upon the kind of user group you need. Custom user groups can only be added at a customer level organization group.

Procedure

1. Navigate to **Accounts > User Groups > List View** and select **Add** and then **Add User Group**.
2. Change the user group **Type** option to **Custom**.
3. Enter the **Group Name** and **Description** used to identify the user group in the Workspace ONE UEM console.
4. Confirm the organization group that manages the user group and select **Save**.
5. You can then add users to this new user group by navigating to **Accounts > Users > List View**.

   Add multiple users by selecting check boxes to the far-left of each listed **user name**. Next, select the **Management** button above the column headings and select **Add to User Group**.

User Groups with Directory Integration

An alternative to custom user groups without active directory integration is through user group integration that applies your existing active directory structure, providing many benefits.

Once you import existing directory service user groups as Workspace ONE UEM user groups, you can perform the following.

- **User Management** - Reference your existing directory service groups (such as security groups or distribution lists) and align user management in Workspace ONE UEM with the existing organizational systems.
- **Profiles and Policies** - Assign profiles, applications, and policies across a Workspace ONE UEM deployment to groups of users.

- **Integrated Updates** - Automatically update user group assignments based on group membership changes.
- **Management Permissions** - Set management permissions to allow only approved administrators to change policy and profile assignments for certain user groups.
- **Enrollment** - Allow users to enroll with existing credentials and automatically assign an organization group.

The administrator must designate an existing organization group as the primary root location from which the administrator manages devices and users. Directory services must be enabled at this root organization group.

You can add your existing directory service groups into Workspace ONE UEM. While integration does not immediately create user accounts for each of your directory service accounts, it ensures that Workspace ONE UEM recognizes them as user groups. You can use this group to restrict who can enroll.

For more information about adding directory user groups in bulk, see Batch Import User Groups.

Add User Groups with Directory Integration

Making user groups with directory integration fosters an aligned approach to device management: device enrollment plus subsequent updates, administrative overview, and user management are each in lockstep with your existing directory service structure.

Prerequisites

Ensure that the user group **Type** is **Directory**.

Procedure

1 Navigate to **Accounts > User Groups > List View**, select **Add** then **Add User Group**.

Setting	Description
Type	Select the type of User Group. ■ **Directory** – Create a user group that is aligned with your existing active directory structure. ■ **Custom** – Create a user group outside of your organization's existing Active Directory structure. This user group type grants access to features and content for basic and directory users to customize user groups according to your deployment. Custom user groups can only be added at a customer level organization group.
External Type	Select the external type of group you are adding. ■ **Group** – Refers to the group object class on which your user group is based. Customize this class by navigating to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services > Group**. ■ **Organizational Unit** – Refers to the organizational unit object class on which your user group is based. Customize this class by navigating to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services > Group**. ■ **Custom Query** – You can also create a user group containing users you locate by running a custom query. Selecting this external type replaces the Search Text function but displays the Custom Query section.

Setting	Description
Search Text	Identify the name of a user group in your directory by entering the search criteria and selecting **Search** to search for it. If a directory group contains your search text, a list of group names displays. This option is unavailable when **External Type** is set to **Custom Query**.
Directory Name	Read-only setting displaying the address of your directory services server.
Domain and **Group Base DN**	This information automatically populates based on the directory services server information you enter on the **Directory Services** page (**Groups & Settings > System > Enterprise Integration > Directory Services**). Select the **Fetch DN** plus sign (+) next to the **Group Base DN** setting, which displays a list of distinguished name elements from which you can select.
Custom Object Class	Identifies the object class under which your query runs. The default object class is 'person' but you can supply a custom object class to identify your users with a greater success and accuracy. This option is available only when **Custom Query** is selected as **External Type**.
Group Name	Select a **Group Name** from your **Search Text** results list. Selecting a group name automatically alters the value in the Distinguished Name setting. This option is available only after you have completed a successful search with the **Search Text** setting.
Distinguished Name	This read-only setting displays the full distinguished name of the group you are creating. This option is available only when **Group** or **Organizational Unit** is selected as **External Type**.
Custom Base DN	Identifies the base distinguished name which serves as the starting point of your query. The default base distinguished name is 'AirWatch' and 'sso'. However, if you want to run the query with a different starting point, you can supply a custom base distinguished name. This option is available only when **Custom Query** is selected as **External Type**.
Organization Group Assignment	This optional setting enables you to assign the user group you are creating to a specific organization group. This option is available only when **Group** or **Organizational Unit** is selected as **External Type**.
User Group Settings	Select between **Apply default settings** and **Use Custom settings for this user group**. See the **Custom Settings** section for additional setting descriptions. You can configure this option from the permission settings after the group is created. This option is available only when **Group** or **Organizational Unit** is selected as **External Type**.
Custom Query - **Query**	This setting displays the currently loaded query that runs when you select the **Test Query** button and when you select the **Continue** button. Changes you make to the **Custom Logic** setting or the **Custom Object Class** setting are reflected here.
Custom Logic	Add your custom query logic here, such as user name or admin name. For example, "cn=jsmith". You can include as much or as little of the distinguished name as you like. The **Test Query** button allows you to see if the syntax of your query is correct before selecting the **Continue** button.
Custom Settings - **Management Permissions**	You can allow or disallow all administrators to manage the user group you are creating.
Default Role	Select a default role for the user group from the drop-down menu.
Default Enrollment Policy	Select a default enrollment policy from the drop-down menu.

Setting	Description
Auto Sync with Directory	This option enables the directory sync, which detects user membership from the directory server and stores it in a temporary table. Administrators approve changes to the console unless the Auto Merge option is selected. If you want to prevent user groups from automatically syncing during a scheduled sync, this setting must be disabled.
Auto Merge Changes	Enable this option to apply sync changes automatically from the database without administrative approval.
Maximum Allowable Changes	Use this setting to set a threshold for the number of automatic user group sync changes that can occur before approval must be given. Changes more than the threshold need admin approval and a notification is sent to this effect. This option is available only when **Auto Merge Changes** is enabled.
Add Group Members Automatically	Enable this setting to add users to the user group automatically. If you want to prevent user groups from automatically syncing during a scheduled sync, this setting must be disabled.
Send Email to User when Adding Missing Users	Enable to send an email to users when missing users are being added to the user group. Adding missing users means combining the temporary user group table with the Active Directory table.
Message Template	This option is available only when **Send Email to User when Adding Missing Users** is enabled. Select a message template to be used for the email notification during the addition of missing users to the user group. When adding active directory users new to the Workspace ONE UEM console, the message template availability depends upon the enrollment mode as configured in **Groups & Settings > All Settings > Devices & Users > General > Enrollment** selecting **Authentication**, and making a choice in the **Devices Enrollment Mode** option. When **Open Enrollment** is selected as the **Devices Enrollment Mode**, a User Activation email template is available in the **Message Template** drop-down. This email message enables the new AD user to enroll. When **Registered Devices Only** is selected as the **Devices Enrollment Mode**, a Device Activation email template is available in the **Message Template** drop-down. This email message enables the new AD user to enroll their devices. If **Require Registration Token** is enabled, the device can be registered with the token embedded in the message.

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

2 Select **Save**.

Edit User Group Permissions

Fine-tuning user group permissions allows you to reconsider who inside your organization can edit certain groups. For example, if your organization has a user group for company executives, you might not want lower-level administrators to have management permissions for that user group.

Use the **Permissions** page to control who can manage certain user groups and who can assign profiles, compliance policies, and applications to user groups.

Procedure

1. Navigate to **Accounts > User Groups > List View**.
2. Select the **Edit** icon of an existing user group row.
3. Select the **Permissions** tab, then select **Add**.
4. Select the **Organization Group** you want to define permissions for.

   You must select an organization group (OG) that is within the root OG hierarchy of the user group.
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 OG. This setting can only be enabled when Manage Group (Edit/Delete) is also enabled. If Manage Group (Edit/Delete) is disabled, then this setting is also disabled.
   - **Use Group For Assignment** – Use the group to assign security policies and enterprise resources to devices. This setting can only be changed if Manage Group (Edit/Delete) is disabled. If Manage Group (Edit/Delete) is enabled, then this setting becomes locked and uneditable.
     - This setting is disabled when the user group is managed by a parent OG and you want to assign the group from one of its children OGs.
6. Select the **Scope** of these permissions, that is, which groups of administrators are allowed to manage or use this user group. Only **one** of the following options may be active.
   - **Administrator Only** – The permissions affect only those administrators at the parent OG.
   - **All Administrators at or below this Organization Group** – The permissions affect the administrators in the OG and all administrators in all child OGs underneath.
7. Select **Save**.

Accessing User Details

Once your users and user groups are in place, you can view all user information regarding user details, associated devices, and interactions.

Access user information from any location in the Workspace ONE UEM console where the user name is displayed, including each of the following pages in the console.

- User Group Members (**Accounts > User Groups > Details View > More > View Users**)
- Users List View (**Accounts > Users > List View**)
- Administrators List View (**Accounts > Administrators > List View**).

The User Details page is a single-page view.

- All associated user groups.
- All Devices associated with the user over time and a link to all enrolled devices.

- All devices a user has checked-out in a Shared Device Environment and a link to complete check-in/check-out device history.
- All device- and user-specific event logs.
- All assigned, accepted, and declined Terms of Use.

Encrypt Personal Details

You can encrypt personally identifiable information including first name, last name, email address, and phone number.

Procedure

1. Navigate to **Groups & Settings > All Settings > System > Security > Data Security** from the Global or Customer-level organization group for which you want to configure encryption.
2. Enable the **Encrypt User Information** setting, then select individual user data settings to activate encryption. Doing so disables the search, sort, and filter functionality.
3. Click **Save** to encrypt user data so it is not accessible in the database. Doing so limits some features in the Workspace ONE UEM console, such as search, sort, and filter.

User Groups List View

The User Groups List View page features useful tools for common user group maintenance and upkeep, including viewing, merging, deleting user groups, and adding missing users.

Navigate to **Accounts > User Groups > List View**.

You can use the User Groups List View to create lists of user groups immediately, based on criteria that is most important to you. You can also add new user groups individually or in bulk.

Action	Description
Filters	Display only the desired user groups by using the following filters. ■ User Group Type. ■ Sync Status. ■ Merge Status.
Add	
Add User Group	Perform a one-off addition of either a Directory-Based User Group or a Custom User Group.
Batch Import	Import new user groups in bulk by using a comma-separated values (CSV) file. You can organize multiple user groups at a time by entering a unique name and description.
Sorting and Resizing Columns	Columns in the List View that are sortable are Group Name, Last Sync On, Users, and Merge Status. Columns that can be resized are Group Name and Last Sync On.
Details View	View basic user group information in the Details View by selecting the link in the **Group Name** column. This information includes group name, group type, external type, manager, and number of users. Details View also includes a link to the group mapping settings in **All Settings > Devices & Users > General > Enrollment** in the **Grouping** tab.
Export ( )	Save an XLSX or CSV (comma-separated values) file of the entire unfiltered or filtered List View. Both file formats can be viewed and analyzed with MS Excel.

The **User Groups List View** also features a selection check box and **Edit** icon to the left of the user. Selecting the **Edit** icon () enables you to make basic changes to the user group. You can make bulk actions on user groups by selecting one or more groups which reveals the action buttons for the listing.

More Actions for User Groups

You can select more than one user group by selecting as many check boxes as you like. Doing so modifies the available action buttons and also makes the available actions apply to multiple groups and their respective users.

Action	Description
Sync	Copy recently added user group users to the temporary table, manually, ahead of the scheduled, automated Active Directory sync by Workspace ONE UEM and Workspace ONE Express.
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 user group sync in Workspace ONE UEM and Workspace ONE Express.
Add Missing Users	Combine the temporary user group table with the Active Directory table, making the addition of these new users in the user group official.
Delete	Delete a user group.

Add Users to User Groups

You can add users to user groups as the need arises.

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

Procedure

1. Navigate to **Accounts > Users > List View**.
2. Select one or more users in the listing by inserting a check mark in the check box to the left.
3. Select the **More Actions** button and then select **Add To User Group**. The **Add Selected Users Into Custom User Group** page displays.
4. You can add users to an **Existing User Group** or create a **New User Group**.
5. Select the **Group Name**.
6. Select **Save**.
7. Navigate to **Accounts > User Groups > List View**.
   a. The Active Directory (AD) synchronization (which is an automated, scheduled process) copies these pending user group users to a temporary table. Then these user group users are reviewed, added, or removed.

b If you do not want to wait for the automated AD sync, you can synchronize manually. Start a manual synchronization by selecting the user group to which you added users, then select the **Sync** button.

8 You can optionally select **More > View and Merge** to perform maintenance tasks such as review, add, and remove pending user group users.

9 Combine the temporary table of pending user group users with the Active Directory user group users by selecting **More > Add Missing Users**.

Admin Groups

Admin groups enable you to assemble subsets of administrator accounts for assigning roles and permissions beyond the permissions that come from having an admin account in Workspace ONE UEM powered by AirWatch.

Admin groups can be used to assign roles and permissions granting access to the console that is specific to a special project. You can add your existing directory service administrators into admin groups or create admin groups from scratch using custom queries.

For example, if you have a new business directive, you might need to assign special admin access to a group of training facilitators. You might create an admin group, run a custom query for training facilitators, and assign a role that is specific to the new business effort. For more information, see Admin Accounts.

Admin Groups List View

The Admin Groups List View page features useful tools for common user group maintenance and upkeep. Such upkeep includes adding, viewing, merging, and deleting user groups and missing users.

View this page by navigating to **Accounts > Administrators > Admin Groups**.

Display the **Edit Admin Group** page by selecting the hypertext name in the **Group Name** column of the list view. Use this page to change the name of the admin group. You can also add and remove roles that are applicable to group members. For more information, see Admin Roles.

Display the **Admin Group Members** listing by selecting the hypertext link number in the **Admin** column. This listing shows you the names of all the administrators in the admin group.

Access the following actions and maintenance functions by selecting the radio button next to the group name.

Action	Description
Sync	Copy recently added admin group users to the temporary table, manually, ahead of the scheduled, automated Active Directory sync by Workspace ONE UEM.
More Actions	
View and Merge	View, Add, and Remove users recently added to the temporary admin group table. Admin group administrators that appear in this table await the automated Workspace ONE UEM admin group sync.
Delete	Delete an admin group.

Action	Description
Top, Up, Down, Bottom	You can edit the ranking of each admin group as it appears in the listing. Moving the groups in this way is useful for when you have more admin groups than a single page can display.
Add Missing Users.	Combine the temporary admin group table with the Active Directory table, making the addition of these new admins in the group official.

Add Admin Groups

You can add admin groups to assign additional roles and permissions to your admins for special projects by taking the following steps.

Procedure

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

Setting	Description
External Type	Select the external type of admin group you are adding. ■ **Group** – Refers to the group object class on which your admin group is based. Customize this class by navigating to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services > Group**. ■ **Organizational Unit** – Refers to the organizational unit object class on which your admin group is based. Customize this object class by navigating to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services > Group**. ■ **Custom Query** – You can also create an admin group containing administrators you locate by running a custom query. Selecting this external type replaces the Search Text function but displays the Custom Query section.
Directory Name	Read-only setting displaying the address of your directory services server.
Domain and **Group Base DN**	This information automatically populates based on the directory services server information you enter on the **Directory Services** page (**Accounts > User Groups > Settings > Directory Services**). Select the **Fetch DN** plus sign (+) next to the **Group Base DN** setting, which displays a list of Base Domain Names from which you can select.
Search Text	Enter the search criteria to identify the name of an admin group in your directory and select **Search** to search for it. If a directory group contains your search text, a list of group names displays. Also, you can apply default roles to the admin group you are creating. After a successful search is run, select the **Roles** tab and then select the **Add** button to add a new role. Or edit an existing role by changing the **Organization Group** and **Role** selection. This setting is available only when **Group** or **Organizational Unit** is selected as the **External Type**.
Custom Object Class	Identifies the object class under which your query runs. The default object class is 'person' but you can supply a custom object class to identify your admins with greater accuracy. This setting is available only when **Custom Query** is selected as **External Type**.
Custom Base DN	Identifies the base distinguished name which serves as the starting point of your query. The default is 'airwatch' and 'sso' but you can supply a custom base distinguished name if you want to run the query from a different starting point. This setting is available only when **Custom Query** is selected as **External Type**.

Setting	Description
Group Name	Select a **Group Name** from your **Search Text** results list. Selecting a group name automatically alters the value in the Distinguished Name setting. This setting is available only after you have completed a successful search with the **Search Text** setting.
Distinguished Name	Read-only setting that displays the full distinguished name of the admin group you are creating. This setting is available only after you have completed a successful search with the **Search Text** setting.
Rank	Read-only setting that displays the rank of the admin group once it is created. You can change an admin group's rank by navigating to **Groups & Settings > Groups > Admin Groups** and moving its relative position using the More action button to the right of the admin group listing.
Auto Sync	This option enables the directory sync, which detects user membership from the directory server and stores it in a temporary table. An administrator approves all changes to the console unless the **Auto Merge** option is enabled.
Auto Merge	Enable this option to apply sync changes automatically from the database without administrative approval.
Maximum Allowable Changes	Use this setting to set a threshold for the number of automatic admin group sync changes that can occur before approval must be given. This option is available only when **Auto Merge** is enabled.
Add Group Members Automatically	Enable this option to add administrators automatically to the admin group.
Time Zone	Enter the time zone associated with the admin group. This required setting impacts when the scheduled, automated Active Directory sync runs.
Locale	Select the localization setting (language) associated with the admin group. This setting is required.
Initial Landing Page	Enter the initial landing page for administrators in the admin group. The default setting for this required setting is the Device Dashboard but you can set it to any page of your choice.
Custom Query	
Query	This setting displays the currently loaded query that runs when you select the **Test Query** button and when you select the **Continue** button. Changes you make to the **Custom Logic** option or the **Custom Object Class** setting are reflected here.
Custom Logic	Add your custom query logic here, such as an admin name. For example, "cn=jsmith". You can include as much or as little of the distinguished name as you like. The **Test Query** button allows you to see if the syntax of your query results in a successful search before selecting the **Continue** button.

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

2 Select **Save**.

View Assignments

As a convenience, you can confirm the profiles, apps, books, channels, and compliance policies that are included in (and excluded from) the assigned group within Workspace ONE UEM powered by AirWatch.

Procedure

1. Navigate to the group listing in **Groups & Settings > Groups > Assignment Groups** and locate a group that has been assigned to at least one entity.
2. In the **Assignments** column, select the hyperlinked number to open the **View Assignments** page. This page displays only those categories that contain **Assignments** or **Exclusions** in the group.

What to do next

Above the header row in the **View Assignments** screen, you can use the **Refresh** button, the **Export** button, and the **Search List** text box to help you locate and confirm that the specific profile, app, book, channel, and compliance policy has been assigned.

Self-Service Portal

6

The Self Service Portal (SSP) for Workspace ONE UEM powered by AirWatch 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/9yfkbk6r2pzldhjlhrz9.

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.

This chapter includes the following topics:

Configure the Default Login Page for the SSP

You can set the default authentication method displayed on the Self-Service Portal of Workspace ONE UEM powered by AirWatch 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 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 in Workspace ONE UEM powered by AirWatch.

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.

Procedure

1. Select **Add Device** on the **My Devices** page.
2. Complete the required text boxes: **Friendly Name**, **Platform**, **Device Ownership**, and **Message Type** as applicable.
3. Select **Save** to add the new device to the SSP account.

Results

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. For detailed instructions on limiting resources for user and admin roles, see Create a New User Role and Create Administrator Role.

- **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.
- **Security** – Shows general security information about a particular device enrolled under your user account.

Remote Actions in the SSP

The Self-Service Portal of Workspace ONE UEM powered by AirWatch provides a means for end users to use key MDM tools without IT involvement. Provided an administrator allows, end users can run the SSP in a web browser and access key MDM support tools.

Administrators have several remote actions and options for managed devices available to them. However, when devices are employee-owned, those employees might want to access similar management tools for their own use. The Self Service Portal (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.

End users can perform remote actions over-the-air to the selected device from within the Self Service Portal. 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.

Action	Description
Change Passcode	Set a new passcode for the selected device.
Clear Passcode	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.
Delete Device	Remove the device from the Self Service Portal.
Delete Registration	Delete any pending enrollment record from the Self Service Portal.
Device Query	Request the device to send a comprehensive set of MDM information to the Workspace ONE UEM Server.
Device Wipe	Wipe all data from the selected device, including all data, email, profiles, and MDM capabilities and returns the device to factory default settings.
Download Hub	Download and install the Workspace ONE Intelligent Hub to the device from which you are viewing the SSP.
Enterprise Wipe	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.
Locate Device	Activate the GPS feature to locate a lost or stolen device. This action is hidden when privacy settings are restrictive.
Lock Device/Screen	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.
Lock SSO	Lock the single sign-on passcode for apps on this device. The next SSO app opened will prompt for a passcode.
Make Noise	Rind a device by remotely causing it to ring.
Resend Enrollment Message	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.
Send Message	Send a message using email, phone notification or SMS to the device.
Set Roaming	Set whether roaming is enabled for this device.
Sync Device	Outfit devices with the latest company policies, content, and apps.
View Enrollment Message	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.

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.

Action	Description
Generate App Token	Generate a token that the device can use to access secure applications.
Manage Email	Manage devices connected to an email account.
Review Terms of Use	Review past terms of use for this account.
Revoke Token	Revokes the token for a selected application.
Upload S/MIME Certificate	Upload an S/MIME Certificate for a corporate email account.

Self-Service Portal Actions Matrix

Each of the major device platforms supports various basic and advanced SSP actions in Workspace ONE UEM powered by AirWatch.

Action	Android	iOS	Win Phone	macOS	Win Mobile	Win 7	Win Desktop
Basic Actions							
Change Passcode.	✓						
Clear (SSO) Passcode.	✓	✓	✓				✓
Delete Device.	✓	✓	✓	✓	✓	✓	✓
Delete Registration.	✓	✓			✓	✓	✓
Device Query	✓	✓		✓		✓	✓
Device Wipe	✓	✓	✓	✓	✓		
Download Hub.				✓		✓	
Enterprise Wipe	✓	✓	✓	✓	✓	✓	✓
Locate Device.	✓	✓	✓		✓		✓
Lock Device/Screen.	✓	✓		✓	✓	✓	
Lock SSO.		✓	✓				
Make Noise.	✓						
Resend Enrollment Message.	✓	✓			✓	✓	✓
Send Message.	✓	✓	✓	✓	✓	✓	✓
Set Roaming.		✓					
Sync Device.	✓	✓					
View Enrollment Message.*	✓	✓			✓	✓	✓
Advanced Actions							
Generate App Token.	✓	✓	✓	✓	✓	✓	✓

Action	Android	iOS	Win Phone	macOS	Win Mobile	Win 7	Win Desktop
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.