Workspace ONE Express and Express+

VMware Workspace ONE UEM 2102

vmware®

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

https://docs.vmware.com/

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

Contents

Using Workspace ONE Express and Express+

1

Mobile devices provide access to internal content and resources. However, the diversity of mobile platforms, operating systems, and versions can make managing devices difficult. VMware Workspace ONE Express and Express+ powered by AirWatch solves this problem by enabling you to configure, secure, monitor, and manage the most popular types of mobile devices in the enterprise.

Workspace ONE Express provides an affordable solution to security concerns and accessibility inherent to enterprise mobility.

- Manage small-scale deployments (500 device maximum) from a single console.
- Enroll devices in your enterprise environment quickly and easily.
- Configure and update device settings over the air.
- Secure mobile access to corporate resources by regulating applications, email and connectivity, and security policies.
- Remotely lock, send messages, and enterprise wipe managed devices.

Workspace ONE Express+

Express+ is the result of a partnership with Dell. Where applicable, "Express+ only" appears in this documentation to identify exclusive features supported by this partnership.

Supported Browsers

The Workspace ONE Express console supports the latest stable builds of the following web browsers.

- Chrome
- Firefox
- Safari
- Internet Explorer 11

- Microsoft Edge

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

Upgrade your browser and guarantee the performance of the Workspace ONE Express console. Comprehensive platform testing has been performed to ensure functionality using these web browsers. If you run Workspace ONE Express in a non-certified browser, you might experience problems.

Supported Platforms

Workspace ONE Express supports the following devices and operating systems.

- Android Legacy 3.0+
- Android Enterprise 3.0+
- Apple iOS 7.0+
- Windows 10 Desktop devices
- Apple macOS 10.9+ (unsupported in Express+)

Upgrade from Workspace ONE Express

When your organization needs mobile device management features beyond what Workspace ONE Express offers, you can upgrade to the full product at any time.

Workspace ONE UEM

Select the Main Menu button **Learn More & Upgrade** and view helpful videos, live demos, and documentation of Workspace ONE UEM's full feature set, not to mention an easy upgrade path for when you make the switch.

Workspace ONE Express+

If you are interested in acquiring an Express+ license, contact your Dell Technologies Sales Representative.

What Happens to Features and Their Settings When You Upgrade

You retain all the configurations and device settings when you upgrade from Workspace ONE Express and Express+ to Workspace ONE UEM. The form those configurations and settings take may be slightly different. This table summarizes how those settings appear when you upgrade.

<table>
<tr><th>Feature</th><th>Original Bundle / Support</th><th>Implementation in Workspace ONE UEM</th></tr>
<tr><td>Settings
APNs for MDM
Android EMM Registration
Apple Automated Enrollment
Apple Device Enrollment Program
Cloud Connector
Directory Services
SMS
VPP Managed Distribution</td><td>Express, Express+</td><td>These settings and integrations configured in Express and Express+ remain configured as before and are found on the same pages.
Navigate to...
Groups & Settings > All Settings
or
Groups & Settings > Configurations
...to find these pages.
In the case of Android EMM Registration, there are more customizable options available on the settings page in Workspace ONE UEM.</td></tr>
<tr><td>Devices</td><td>Express, Express+</td><td>All devices remain enrolled and are seen in Devices List View.</td></tr>
<tr><td>Denylisted/ Allowlisted Devices</td><td>Express, Express+</td><td>All denylisted and allowlisted device configurations are configured as before.</td></tr>
<tr><td>User & Admin Accounts</td><td>Express, Express+</td><td>All basic and directory user and admin accounts exist after you upgrade.</td></tr>
<tr><td>User Groups</td><td>Express, Express+</td><td>All user groups exist after you upgrade.</td></tr>
<tr><td>Introduction Survey & Wizard</td><td>Express, Express+</td><td>The Introduction Survey and wizard are only available in Express and Express +. The settings you configure through this feature are found on the respective Settings pages, detailed below.</td></tr>
<tr><td>Introduction Survey - Location Question</td><td>Express, Express+</td><td>The Introduction Survey is only available in Express and Express+.
You can now enable/disable Location on the following pages.<table><tr><th>Platform</th><th>Page</th><th>Setting</th></tr><tr><td>Android</td><td>Groups & Settings > All Settings > Devices & Users > Android > Intelligent Hub Settings</td><td>Collect Location Data
Force GPS On</td></tr><tr><td>Apple iOS</td><td>Groups & Settings > All Settings > Devices & Users > Apple > Apple iOS > Intelligent Hub Settings</td><td>Collect Location Data</td></tr><tr><td>Apple macOS</td><td>Groups & Settings > All Settings > Devices & Users > Apple > macOS > Intelligent Hub Settings</td><td>Request to collect Location Data</td></tr></table></td></tr>
</table>

Introduction Survey - App Catalog Question	Express, Express+	The Introduction Survey is only available in Express and Express+. Express/Express+ uses the legacy catalog. You can now enable/disable the legacy catalog on the following page. **Groups & Settings > All Settings > Apps > Workspace ONE > AirWatch Catalog > General > Publishing** Settings ■ Legacy Catalog (iOS) ■ Legacy Catalog (Android) ■ Legacy Catalog (Windows Desktop) ■ Legacy Catalog (macOS)
Blueprints - Public Apps	Express, Express+	Blueprints are only available in Express and Express+. Any store apps added in a Blueprint can be found by navigating to **Apps & Books > Applications > Native > Public**.
Blueprints - Web Apps	Express, Express+	Blueprints are only available in Express and Express+. Any web apps added in a Blueprint can be found by navigating to **Apps & Books > Applications > Web > Web Links**.
Blueprints - Purchased Apps	Express, Express+	Blueprints are only available in Express and Express+. Any store apps added in a Blueprint can be found by navigating to **Apps & Books > Applications > Native > Purchased**.
Blueprints - Resources - Email	Express, Express+	Blueprints are only available in Express and Express+. Any Email Resource configured in a Blueprint can be found by navigating to **Devices > Profiles & Resources > Profiles**.
Blueprints - Resources - Wi-Fi	Express, Express+	Blueprints are only available in Express and Express+. Any Wi-Fi Resource configured in a Blueprint can be found by navigating to **Devices > Profiles & Resources > Profiles**.
Blueprints - Policies - Passcode	Express, Express+	Blueprints are only available in Express and Express+. Any Passcode Policy configured in a Blueprint can be found by navigating to **Devices > Profiles & Resources > Profiles**. A separate profile of payload type 'Passcode' is created for each platform. Each profile must now be managed separately.
Blueprints - Policies - Other Policies	Express, Express+	Blueprints are only available in Express and Express+. Any Other Policies configured in a Blueprint is found by navigating to **Devices > Profiles & Resources > Profiles**. A separate profile of payload type 'Restrictions' is created for each platform. Each profile must now be managed separately.
Blueprints - Configurations - Personalization	Express+ only	Blueprints are only available in Express and Express+. Any Personalization Configuration configured in a Blueprint is found by navigating to **Devices > Profiles & Resources > Profiles**. A device profile of payload type ‘Personalization’ is created for the Windows platform.
Blueprints - Configurations - Windows Updates	Express+ only	Blueprints are only available in Express and Express+. Any Windows Updates Configuration configured in a Blueprint is found by navigating to **Devices > Profiles & Resources > Profiles**. A device profile of payload type ‘Windows Updates’ is created for the Windows platform.

Blueprints - Security - Password	Express+ only	Blueprints are only available in Express and Express+. Any Password Security settings configured in a Blueprint is found by navigating to **Devices > Profiles & Resources > Profiles**. A device profile of payload type 'Password' is created for the Windows platform.
Blueprints - Security - Restrictions	Express+ only	Blueprints are only available in Express and Express+. Any Security Restrictions configured in a Blueprint are found by navigating to **Devices > Profiles & Resources > Profiles**. A device profile of payload type 'Restrictions' is created for the Windows platform.
Blueprints - Security - Encryption	Express+ only	Blueprints are only available in Express and Express+. Any Encryption Security settings configured in a Blueprint are found by navigating to **Devices > Profiles & Resources > Profiles**. A device profile of payload type 'Encryption' is created for the Windows platform.
Blueprints - Security - Firewall	Express+ only	Blueprints are only available in Express and Express+. Any Firewall Security settings configured in a Blueprint are found by navigating to **Devices > Profiles & Resources > Profiles**. A device profile of payload type 'Firewall' is created for the Windows platform.
Blueprints - Security - Defender	Express+ only	Blueprints are only available in Express and Express+. Any Defender Security settings configured in a Blueprint are found by navigating to **Devices > Profiles & Resources > Profiles**. A device profile of payload type 'Defender Exploit Guard' created for the Windows platform.
Blueprints - Security - BIOS	Express+ only	Blueprints are only available in Express and Express+. Any BIOS Security settings configured in a Blueprint are found by navigating to **Devices > Profiles & Resources > Profiles**. A device profile of payload type 'BIOS' is created for the Windows platform.
Users/User Group Assignments	Express, Express+	All users and user groups assigned to Blueprints become Smart Groups that include the users/groups from each Blueprint. These are found by navigating to **Groups & Settings > Groups > Assignment Groups**.
Console Notification Settings	Express, Express+	All console notification settings remain the same after you upgrade.

Privacy

It is important that you inform your end users about how their data is collected, stored, and displayed when they enroll into Workspace ONE Express. The device ownership level prescribes how data is collected and you can customize this configuration by contacting Workspace ONE Support.

Default Privacy and Data Collection Settings

User Information	Displayed in Console
First Name	Yes
Last Name	Yes
Phone Number	Yes
Email Accounts	Yes
User name	Yes

Privacy settings in Workspace ONE Express are dependent upon the ownership level of the enrolled device.

Privacy Setting	Corporate-Dedicated	Employee-Owned
GPS Data Collection	On	Off
Personal Apps Install Data Collection	On	Off
Prevention of Unmanaged Profile Installation	On	On
Enterprise Wipe Functionality	On	Off
Lock Device Functionality	On	Off

If you want to customize the privacy settings beyond what the device ownership level prescribes, contact Workspace ONE Support.

Workspace ONE Express and Express+ customers can configure location settings at various points in time.

Configure Location Settings During Express Setup

During the Express Setup process, one of the questions asked is **Do you want to collect device Location data?**

If you respond No, then no location data is collected for any device that enrolls into Workspace ONE Express or Express+.

If you respond Yes, then at enrollment time, the device end user is prompted whether they want location data collected. If the user declines, then no location data is collected. If the user accepts, then location data is collected but only for corporate-owned devices. **Location data is never collected for employee-owned devices.**

Configure Location Settings After Express Setup

You can configure location settings after the Express Setup process by reentering the Express Setup page. Follow these steps.

1 Navigate to **Getting Started > Setup**.

2 If not already selected, select the **Survey** tab. You are not required to rerun the entire setup.

3 Scroll down to the **Location data** question and make your new selection: From Yes to No or from No to Yes.

4 Select **Save & Continue**.

Any changes you make to the location settings take effect immediately. The one exception to this immediate effect is the following scenario.

- During Express Setup, assume you set your preference not to collect Location Data and subsequently, many iOS devices are enrolled. Later, you decide to change this setting to Collect Location Data; any iOS devices currently enrolled must re-enroll after the settings change for the collection of location data to take effect.

  This scenario impacts iOS devices only.

Terms of Use

Ensure that all users with managed devices agree to the policy by defining and enforcing terms of use. You can optionally make the acceptance of the terms of use a requirement for enrolling, installing apps, or accessing the Workspace ONE Express Admin Console.

Contact Workspace ONE Support to implement terms of use for your device deployment.

Express Setup

2

Setting up Workspace ONE Express is as easy as logging in to the website. Upon the initial login, a step-by-step wizard guides you through the process of configuring the software.

The Setup Wizard runs when you log in to Workspace ONE Express for the first time. If you stop and log out at any point during setup, the wizard saves your place. The next time you log in, the wizard returns you to the same spot.

Introduction and Survey

The Introduction and Survey page briefly acquaints you with Workspace ONE Express and asks you several questions about your deployment.

1 **Do you use Active Directory?**

   Active Directory is Microsoft's directory service developed for Windows domain networks and is by far the most popular directory service. Workspace ONE Express also supports other directory services such as Lotus Domino and Novell e-Directory.

2 **Will your employees be using Apple devices?**

   If you plan on enrolling Apple devices in the future, you can set up the APNs certificate from the Configuration menu later.

3 **Will your employees be using Android devices?**

   Workspace ONE Express supports all Android devices, Legacy and Enterprise. If you plan on enrolling Android devices, you can register with Android EMM using this Wizard or from the Configurations page later.

4 **Do you plan to use an Apple Volume Purchase Program (VPP) to add apps?**

   While you can supply apps to your devices without participating in Apple's Volume Purchase Program, the program affords some advantages that may be of value: you can purchase apps & books in volume, get access to custom B2B apps, and buy content with purchase orders.

5 **Do you want to collect device Location data?**

Privacy is important to our customers. Selecting **Yes** here prompts the user on their device whether they want location data collected. If the user declines, then no location data is collected. If the user accepts, then location data is collected but only for corporate-owned devices. Location data is never collected for employee-owned devices.

After completing Setup, Express and Express+ customers can change the location setting by returning to this Express Setup page at any time.

6 **Do you want to distribute an app catalog to your devices?**

The app catalog is a bookmark that will be added to the home screen of enrolled devices. You can choose to distribute the app catalog to devices if you have on-demand applications that you want to provide to your end users to download.

You can revisit the survey questionnaire to change any of your selections, making sure you select **Save and Continue** when finished.

Apple Push Notification Service

If you plan to have Apple devices in your device fleet, you must establish connectivity between Apple and Workspace ONE Express before those devices can be managed.

1 Navigate to **Groups & Settings > Devices & Users > Apple > APNs for MDM**.

2 Download a Certificate Request.

a Download the Workspace ONE Express-generated certificate request file (PLIST) by selecting the **MDM_APNsRequest.plist** link and saving the file to your device.

b Select **Save** to proceed.

3 Create an Apple Certificate.

a Enter your corporate Apple ID. If you do not have a corporate Apple ID, you can create one from this setup page.

b Next, select the **Apple Push Certificates Portal** to sign in with your corporate Apple ID and download the PEM file. You need this PEM file for the following step.

4 Upload the Apple Certificate.

a Upload the AirWatch MDM certificate file (PEM) you received from Apple.

b Select **Save** to proceed.

Android EMM Registration

You can configure your Android registration as Enterprise or Legacy but not both. To start managing Android Enterprise devices, you must register Workspace ONE Express as your Enterprise Mobility Manager (EMM) provider with Google.

1 Select the **Register With Google** button to launch Google Play's Bring Android to Work registration screen.

2 Answer the presented questions and select **Complete Registration** when done.

3 You are taken back to the **Android EMM Registration** page in Workspace ONE Express, where the EMM registration results are displayed.

4 Select **Save** to apply the registration of Workspace ONE Express as the Android Enterprise Mobility Manager with Google.

Set Up AirWatch Cloud Connector

The AirWatch Cloud Connector (ACC) Setup screen prompts you to download and run the ACC Installer.

Installing the AirWatch Cloud Connector is a three-step process.

1 Initiate the InstallShield Wizard including the certificate password.

2 Configure a proxy server, as necessary.

3 Complete the installation and select whether you want to show the Windows Installer log.

Once installed, it also prompts you to test the connection to the AirWatch Cloud Connector server.

Set Up Active Directory

The Workspace ONE Express Active Directory Setup screen prompts you to enter the settings for your existing active directory service, including server information and binding authentication information.

Once completed, Workspace ONE Express integrates with your existing directory service making user and device integration much easier. For more information about individual settings, see Set Up Directory Services Manually.

Set Up Apple's Volume Purchase Program

While you can supply apps to your devices without participating in Apple's Volume Purchase Program, it may be of value to your organization. You can purchase apps & books in volume, get access to custom B2B apps, and use purchase orders.

If you do not yet have a VPP account, the setup page enables you to create one. You can then upload the VPP token and Sync all your purchased apps, making them available to add to Blueprints.

For more information, see Add Applications to a Blueprint.

Blueprints

3

Blueprints ensure that Workspace ONE Express users have the apps they need, email and Wi-Fi configurations to stay in touch, and security settings to keep the corporate content safe.

Blueprints are saveable, editable, reusable device configurations for your organization.

Create a Blueprint

You can create Workspace ONE Express blueprints quickly and easily by following the step-by-step blueprint wizard. You can opt out of the blueprint creation process at any time. The wizard saves your progress, allowing you to pick up where you left off later.

1 From the main menu, navigate to **Blueprints > List View** and select the **Add Blueprint** button.
   - Select between **Mobile (iOS/Android)** and **Window**. Express+ Only.
2 Complete the **Name** text box, which is the label that appears in the Blueprint listing.
3 Add Applications to a Blueprint.
4 Add Resources to a Blueprint.
5 Adding Policies to a Blueprint. Available in Express+ but for Mobile Blueprints only.
6 Add a Configuration, Express+. Express+ Only.
7 Add Blueprint Security, Express+. Express+ Only.
8 Add Users and User Groups to a Blueprint.
9 Review.

This chapter includes the following topics:

- How Do You Migrate Blueprints for Android Enterprise

Add Applications to a Blueprint

After you have named the blueprint, include apps so that when it is assigned to devices, your Workspace ONE Express users have access to the apps they need.

This step is optional and you can skip ahead by selecting **Continue to Resources**. You can select the **discard apps selection** at any time to return to **Create a Blueprint**. You can also close the entire blueprint creation session by selecting the **X**. Your progress is automatically saved.

Procedure

1. Select **Add App**.
2. Select the Type of App to add: **Add Public App**, **Add Web App**, and **Configure Office 365** (Express+ Only).
   - **Add Public App**

     Add an app available in any of the major app stores to your blueprint. Select among **Android**, **Apple**, and **Windows Desktop**.
   - **Add Web App**

     Add an app that links to a specific website, such as email, wiki, or online auction house.
     - You must supply the **URL**, **Name**, and **App Delivery** method, described in step 4.
     - When adding an application using a Google Play Store URL, additional information such as name and application icons cannot be retrieved.
     - Optionally, you can **Upload Icon** representing the Web app manually. Express+ users are limited to uploading icons for Android and iOS Web Apps only.
     - Android Enterprise devices must be running Android 8.0 (Oreo) or later to use Web Apps.
   - **Configure Office 365** (Express+ Only)

     You must upload the XML file that contains the Office 365 configuration settings for your Windows 10 devices (Express+ Only). You can visit config.office.com to generate an XML file that configures Office 365 to your needs.
3. Select the **Platforms** and **Country** in which the app is used.

   This selection determines where Workspace ONE Express searches for the app.

4 Search the applicable app stores for the apps you want to add. For Android apps from the Google Play Store, you must copy and paste the URL into the **App URL** field.

   - Apps from the Google Play Store for Android Enterprise must be approved before they can be added to a Blueprint.

   a Select the green **Approve** button in the app listing of the Google Play Store.

   A separate popup window displays containing a list of elements the app has access to.

   b Review this access list and select **Approve** again to proceed and add the app to the Blueprint. Alternatively, select **Cancel** to deny the app from your Blueprint.

   c If you approved the app for your Blueprint, another popup window displays containing **Approval Settings** and **Notifications**. Select the settings and notification options you want to enable and select **Save** to apply these settings to the app.

5 Once you have located and approved the app, you must select how you want the app to be delivered.

   - **On Demand: users download**

     The app must be downloaded to the device by the user. This option reduces the time it takes to push the blueprint to devices. However, it also means that the user can opt out of installing the app.

   - **Automatic: system push**

     The app is installed when the blueprint gets pushed to devices. This option increases the time it takes to push the blueprint to devices but it means that the app is installed automatically.

     Only Android and Apple offer these options. Users must download apps from the Windows Store.

6 Select **Continue** to save your settings and proceed to the next step.

   You can alternatively go back and add another app type from step 2.

Add Resources to a Blueprint

After you have added applications, you can include email and Wi-Fi configuration settings in your Workspace ONE Express blueprints, enabling users to receive email and connect to network resources. This step is optional. Select **Continue** to skip this section.

Procedure

1 Select **Configure** to complete the **Email** settings.

Setting	Description
Account Name	Enter the unique name of the email account, for example, Secure Corporate Email.
Exchange ActiveSync Host	Enter the domain name of the Exchange ActiveSync Host that your devices connect with to send and receive email.
Use SSL	Select to enable Secure Socket Layer for your email configuration.
Domain	Enter the login domain by which the user email is recognized. The default is the **{EmailDomain}**, entered as a lookup value. A lookup value is a variable that represents the user or the device. In this case, the domain the blueprint uses to log the user in is the email domain. The advantage to using a lookup value over entering a static text domain is that users do not necessarily all have the same email domain. No matter what email domain each user uses to retrieve their email, the lookup value represents that user (or device) accurately.
User name	Enter the login user name. The default is **{EmailUserName}** lookup value.
Email Address	Enter the login email address. The default is **{EmailAddress}** lookup value.

2 Select **Configure** to complete the **Wi-Fi** settings.

Setting	Description
Service Set Identifier (SSID)	Enter a unique identifier for the wireless access point.
Hidden Network	Select whether you want the network access point to be visible in the Wi-Fi listing.
Auto-Join	Select whether you want authenticated devices to be automatically joined upon return to the Wi-Fi hot spot.
Security Type	Select the type of wireless network encryption: **None**, **WEP** (unsupported in Express+), **WPA**, and **WPA2**.
Password	Enter the wireless network password. Select the **Show Characters** check box to replace the redacted password entry and view the password as entered. This setting is only available when a **Security Type** selection is made.

3 When finished configuring the settings, select **Continue** to save your settings and move to the next step, Policies.

Adding Policies to a Blueprint

Workspace ONE Express Blueprints can contain Device Feature, Application, and Data Loss Prevention policies, which, together with platform eligibility, determine which permissions are available for the device in question.

Device Feature Policies

- **Allow use of camera**.
- **Allow use of Bluetooth**.
- **Allow use of AirDrop/Near Field Communication (NFC)**.
- **Allow use of Siri or Cortana**.
- **Allow Device Wipe**.
- **Allow use of Google/iCloud Backup**.

Application Policies

- **Allow access to the App store**.
- **Allow use of YouTube** – Grant access to YouTube. For Apple devices, applicable only to iOS 5.0 and earlier.
- **Allow use of Game Center** – Grant your users to access Apple's social gaming network.
- **Allow untrusted applications** – Enable your users to install apps that are not obtained from an official repository of apps (App Store, Microsoft Store, Google Play).
- **Allow Native Browser**.

Data Loss Prevention Policies

- **Allow screen capture**.
- **Allow copy/paste between applications**.
- **Allow SD Card**.
- **Allow unmanaged use of managed document** – Managed documents refers to corporate assets. Enable this setting to allow your users to open and edit corporate content with unmanaged apps. For example, opening a Word Document using Google Docs instead of MS Word).
- **Do Not require device encryption** – Remove the requirement for device encryption, a secure data storage methodology.

Add Passcode Policy to a Blueprint

After you have added resources to the blueprint, you can define how the device is used while being managed. This definition includes a passcode requirement, length, and complexity of the passcode. This step is optional.

1 Complete each of the policy settings that reflect your security concerns and operating norms.

  Not all options are applicable to all platforms. Consult the charts on this page in the section entitled **Android Policy Support**.

2 Insert check marks to enable each applicable policy setting.

Setting	Description
Require Passcode	Select whether or not to require a passcode for the device.
Minimum Passcode Length	Select the minimum passcode length from 4 to 16 characters.
Auto-Lock (in min)	Select the time in minutes that the device automatically locks.
Maximum Number of Failed Attempts	Select the number of times the user is allowed to fail to authenticate before locking the device.
Password Complexity	Select the complexity of the password, between **Simple** and **Alphanumeric** characters.
Maximum Password Age (days)	Select the number of days before the user is required to change their password.

3 After completing each of the sections, select **Continue** to proceed to the next step, adding users and user groups.

Android Policy Support

Given the divergent nature of the Android platform, Workspace ONE Express support for resources and policies sometimes depends upon a device-specific application programming interface (API). The original equipment manufacturer (OEM) authors this API.

Table 3-1. Email

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Pana-sonic	Amazon	Nook	Sony	Intel	ASUS	Blue-bird
Native Email Configuration		v1.0+	v1.0+		v1.0+					v5.0+			

Table 3-2. Device Functionality

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Pana-sonic	Amazon	Nook	Sony	Intel	ASUS	Blue-bird
Allow Camera.	v4.0+	v2.0+		v1.0+		MX v1.3+					v1.0+		v1.0
Allow Screen Capture.		v2.0+	v1.0+						v1.0+	v5.0+	v1.0+		
Allow NFC.			v2.0+		v2.0+					v7.0			
Enterprise Wipe	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Allow Email Account Addition.		v5.0+								v6.0+			

Table 3-3. Encryption

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Pana-sonic	Amazon	Nook	Sony	Intel	ASUS	Blue-bird
Require Storage Encryption.	v3.0+	v2.0+	v1.0+	v1.0+	v1.0+	MX v1.3+							

Table 3-4. Sync and Storage

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Pana-sonic	Amazon	Nook	Sony	Intel	ASUS	Blue-bird
Allow Google Backup.		v2.0+	v2.2+										
Allow SD Card Access.		v2.0+	v1.0+	v1.0+	v2.0+	MX v1.3+			v1.0+	v2.0+	v1.0+		

Table 3-5. Applications

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Pana-sonic	Amazon	Nook	Sony	Intel	ASUS	Blue-bird
Allow Google Play.		v2.0+	v1.0+								v1.0+		
Allow YouTube.		v2.0+	v1.0+								v1.0+		
Allow Copy & Paste Between Applications.		v4.0+									v1.0+		
Allow Untrusted applications.		v2.0+	v1.0+	v1.0+	v2.0+	MX v1.3+		v1.0+		v5.0			v1.0

Table 3-6. Bluetooth

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Pana-sonic	Amazon	Nook	Sony	Intel	ASUS	Blue-bird
Allow Bluetooth.		v2.0+	v1.0+	v1.0+	v2.0+	MX v1.3+		v1.0+		v2.0+			v1.0

Table 3-7. Browser

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Pana-sonic	Amazon	Nook	Sony	Intel	ASUS	Blue-bird
Allow Native Android Browser.		v2.0+	v1.0+							v2.0+			

Add a Configuration, Express+

Configurations are a Blueprint component exclusive to Workspace ONE Express+. Furthermore, they are specific to the Windows 10 variety Blueprints, comprised of settings for image personalization and Windows update settings.

If you are interested in a Workspace ONE Express+ license, see Upgrade from Workspace ONE Express.

Personalization

This section of the Blueprint configuration enables you to customize the background and lock screen image as well as personalizing the start layout.

1 Select the **Configure** button under Personalization.

2 Configure the **Images** settings.

Setting	Description
Desktop Image	Select **Upload** to add an image to use as the desktop background.
Lock Screen Image	Select **Upload** to add an image to use as the lock screen background.

3 Configure the **Start Layout** settings.

Upload a start layout XML. This XML file overrides the default start menu layout and prevents users from changing the layout. You can configure the layout of tiles, the number of groups, and the apps in each group. You must create this XML yourself. For more information on creating a start layout XML, see https://docs.microsoft.com/en-us/windows/configuration/customize-and-export-start-layout.

Windows Update

This section of the Blueprint configuration enables you to direct how your Windows 10 device updates itself.

1 Select the **Configure** button under Windows Updates.

2 Configure the **Branching and Deferral** settings.

Setting	Description
Update Branch	Select the update branch to follow for updates. ■ Windows Insider Branch - Slow ■ Windows Insider Branch - Fast ■ Release Windows Insider Build ■ Semi-Annual Channel (Targeted) ■ Device receives all applicable feature updates immediately after the release of a new Windows version. Consider using this channel for your organization's testing process. ■ Semi-Annual Channel ■ This channel is the phase following targeted deployment. Consider using this channel after your testing process provides successful findings.
Defer Feature Updates Period in Days	Select the number of days to delay feature updates before installing the updates on the device. The maximum number of days you can defer an update changed in Windows 10 version 1703. Devices running a version before 1703 can only defer for 180 days. Devices running a version after 1703 can defer up to 365 days. If you defer an update for longer than 180 days and push the profile to a device running a version of Windows 10 before the 1703 update, the profile fails to install on the device.
Pause Feature Updates	Enable to pause all feature updates for 60 days or until disabled. This setting overrides the **Defer Feature Updates Period in Days** setting. Use this option to delay an update that causes issues that can normally install following your deferral settings.
Defer Quality Updates Period In Days	Select the number of days to delay quality updates before installing the updates on the device.
Pause Quality Updates	Enable to pause all quality updates for 60 days or until disabled. This setting overrides the **Defer Quality Updates Period in Days** setting. Use this option to delay an update that causes issues that can normally install following your deferral settings.

3 Configure the **Update Installation Behavior** settings.

Setting	Description
Automatic Updates	Set how updates from the selected **Update Branch** are handled. ■ Install Updates Automatically. ■ Install Updates but Let User Schedule the Computer. ■ Install Updates Automatically and Restart at Specified Time. ■ Install Updates Automatically and Prevent User from Modifying Control Panel Settings. ■ Check for Updates but Let User Choose Whether to Download and Install Them. ■ Never Check for Updates.
Active Hours Start Time	Active Hours is the time when the system is prevented from rebooting the device. Enter the start time for active hours.
Active Hours End Time	Enter the end time for active hours.

Setting	Description
Schedule Restart Warning in Hours	Allows the IT administrator to schedule the number of hours the user has before their device is automatically restarted due to an update.
Schedule Imminent Restart Warning in Minutes	Allows the IT administrator to select the number of minutes the user has to prepare for an imminent device restart.

4 Configure the **Update Policies** settings.

Setting	Description
Dual Scan	Dual Scan is a setting designed for environments that prefer Windows Update (WU) to be the primary update source while Windows Server Update Services (WSUS) provides all other content. It avoids the 'two masters' problem of having more than one official update source by categorizing updates. Enabling this setting causes the client to only accept WSUS updates that are unrelated to the "Windows" family of products, relying solely on WU for this type of update.
Mobile Operator App Download Limit	Specifies whether to ignore the Mobile Operator download limit over a cellular network for apps and their updates.
Mobile Operator Update Download Limit	Specifies whether to ignore the Mobile Operator download limit over a cellular network for OS updates.

Add Blueprint Security, Express+

The Blueprint Security step collects settings and preferences that make the Windows 10 device safer for business use but at the same time safeguarding privacy. The Security component of a Blueprint is exclusive to Workspace ONE Express+.

You can select settings including password complexity, privacy and VPN settings, device restrictions, encryption and firewall settings, and settings to integrate Defender and BIOS updates from Dell.

If you are interested in a Workspace ONE Express+ license, see Upgrade from Workspace ONE Express.

Password

This section of the Blueprint configuration enables you to customize password settings including complexity, minimum length, among many others.

Settings	Descriptions
Password Complexity	Set to **Simple** or **Complex** to your preferred level of password difficulty.
Require Alphanumeric	Enable to require the passcode to contain alphanumeric characters.
Minimum Password Length	Enter the minimum number of characters a Password must contain.
Maximum Password Age (days)	Enter the maximum number of days that elapse before the end user is required to change the Password.

Settings	Descriptions
Device Lock Timeout (in Minutes)	Enter the number of minutes before the device automatically locks and requires a passcode re-entry.
Maximum Number of Failed Attempts	Enter the maximum number of attempts the end user can enter before the device is restarted.
Password History (occurrences)	Enter the number of occurrences a password is remembered. The larger this number, the more strict it becomes. For example, if you set the history to 12, an end user cannot reuse the past 12 passwords.

Restrictions

Select from options including allowing (or disallowing) devices to unenroll, location service use, diagnostic and telemetry data use, sign-in options, VPN, bluetooth, camera, Cortana, USB storage, application use settings, and network settings.

1 Configure the **Administration** settings.

Settings	Description
Allow MDM Unenrollment	Allow the end user to unenroll from Workspace ONE Express manually through the Workplace/Work Access enrollment. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.

2 Configure the **Security & Privacy** settings.

Settings	Description
Location	Select how location services run on the device. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.
Send Diagnostic and Usage Telemetry Data	Select the level of telemetry data to send to Microsoft. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.

3 Configure the general **Settings**.

Settings	Description
Allow User to Change Sign-In Options	Allow the user to change the Sign-In Options. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.
VPN	Allow the user to change the VPN settings. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.

Settings	Description
Allow User to Change Workplace Settings	Allow the user to change Workplace settings and change how MDM functions on the device. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.
Allow the User to Change Account Settings	Allow the user to change Account settings. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.

4 Configure the **Bluetooth** settings.

Settings	Description
Bluetooth	Allow the use of Bluetooth on the device. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.

5 Configure the **Device Functionality** settings.

Settings	Description
Camera	Allow access the camera function of the device. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.
Cortana	Allow access to the Cortana application. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.
Smart Screen	Enable to allow the end user to use the Microsoft SmartScreen feature, which is a form of security requesting the end user to draw shapes on an image to unlock the device. This option also allows end users to use PINs as their passcode. **Note** After you disable function, you cannot reenable it through Workspace ONE UEM MDM. To reenable it, you must factory reset the device. The restriction does not apply to Windows 10 Home edition devices.
USB Storage	Enable to allow the connection of USB storage devices.

6 Configure the **Applications** settings.

Settings	Description
Allow Non-Windows Store Applications	Allows the downloading and installation of applications not trusted by the Microsoft Store. This restriction applies to all Windows 10 devices.
Allow App Store Auto Updates	Enable to allow apps downloaded from the Microsoft Store to update automatically when new versions are available. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.

Settings	Description
Allow Developer Unlock	Allows the use of the Developer Unlock setting for sideloading applications onto devices. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.
Allow DVR & Game Broadcasting	Enable to allow the recording and broadcasting of games on the device. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.

7 Configure the **Network** settings.

Setting	Description
Allow Auto Connect to Wi-Fi Hotspots	Enable to allow the device to connect to Wi-Fi hotspots automatically using the Wi-Fi Sense functionality. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.
Allow Cellular Data On Roaming	Enable to allow cellular data use while roaming. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.
Allow Internet Sharing	Enable to allow Internet sharing between devices. This restriction applies to Windows 10 devices only and is not supported for Windows 10 Home edition devices.

Encryption

Select from several encryption options such as whether to encrypt the entire hard disk or just the system partition, encryption method (default versus multiple 128-bit and 256-bit options), and BitLocker Authentication settings.

1 Complete the **Configure Encryption** settings.

Settings	Descriptions
Encrypted Volume	Use the drop-down menu to select the type of encryption as follows. ■ Complete Hard Disk – Encrypts the entire hard disk on the device, including the System Partition where the OS is installed. ■ System Partition – Encrypts a partition or drive in the same location Windows is installed and from which it starts.
Encryption Method	Select the encryption method for the device. These settings are only supported on Windows 10 1511 and later.
Only Encrypt Used Space During Initial Encryption	Enable to limit the BitLocker encryption to only the used space on the drive at the time of encryption.
Force Encryption	Enable to force encryption on the device. This enforcement means that the device immediately re-encrypts if BitLocker is manually disabled. Consider disabling this setting to prevent issues during upgrades or Enterprise Wipes.

2 Configure the **BitLocker Authentication Settings**.

Authentication Mode	Select the method for authenticating access to a BitLocker encrypted device. ■ TPM — Uses the devices Trusted Platform Module. Requires a TPM on the device. ■ Password — Uses a password to authenticate.
Enforce Encryption PIN on Login	Select the check box to require users to enter a PIN to unlock the device. This option locks out the OS startup and auto-resumes from suspend or hibernate until the user enters the correct PIN. To remove an existing pre-authorization PIN from an enrolled device, the end user must decrypt their device and re-encrypt with the updated encryption profile.
Use Password if TPM Not present	Select the check box to use a password as a fallback to decrypt the device if the TPM is unavailable. If this setting is not enabled, any devices without a TPM do not encrypt.

Firewall

Configure how the firewall behaves when connected to **Domain**, **Private**, and **Public** networks.

Setting	Description
Firewall	Set to **Enable** and enforce policy settings on the network traffic. If disabled, the device allows all network traffic, regardless of other policy settings.
Outbound Action	Select the default action the firewall takes on outbound connections. If you set this setting to **Block**, the firewall blocks all outbound traffic unless explicitly specified otherwise.
Inbound Action	Select the default action the firewall takes on inbound connections. If you set this setting to **Block**, the firewall blocks all inbound traffic unless explicitly specified otherwise.
Notify User When Windows Firewall Blocks a New App	Set the notification behavior for the firewall. If you select **Enable**, the firewall can send notifications to the user when it blocks a new app. If you select **Disable**, the firewall does not send any notifications.

Defender

You can make Windows Defender a part of your Blueprint by enabling and configuring its use on Windows 10 device. Options include threat default actions, selecting how much CPU to devote to a scan, enabling full scans and quick scans, and how long to wait before quarantined files are discarded.

1 Configure the **Real-Time Monitoring** settings.

Setting	Description
Real-time Monitoring	Enable to activate the real-time monitoring component of Defender.

2 Configure the **Exclusions** settings.

Setting	Description
Exclusions	Select the **Add New** button to exclude a **Path**, a file **Extension**, or a **Process** from Defender scans.

3 Configure the **Threat Default Action** settings to determine the default action when Defender encounters various levels of threat: **Low**, **Moderate**, **High**, and **Severe**.

- **Not Configured**
- **Clean** — Select to clean the issues with the threat.
- **Quarantine** — Select to separate the threat into a quarantine folder.
- **Remove** — Select to remove the threat from the device.
- **Allow** — Select to allow the threat to stay.
- **User Defined** — Select to let the user decide how the threat should be handled.
- **Block** — Select to block the threat from accessing the device.

4 Configure the **Advanced** settings.

Setting	Description
Scan Avg CPU Load Factor (%)	Allows you to set the average CPU load factor as a percentage, limiting the CPU load Defender is allowed to use during scans. The larger this number, the faster Defender can complete scans, but at the same time, the fewer CPU cycles are available for other tasks.
Catchup Full Scan	Enable to allow the running of a full scan that was interrupted or missed previously. A catch-up scan is a scan that is initiated because a regularly scheduled scan was missed. Usually these scheduled scans are missed because the device was turned off at the scheduled time.
Catchup Quick Scan	Enable to allow the running of a quick scan that was interrupted or missed previously.
Remove Quarantined Files After	Set how long files are kept in quarantine before being deleted permanently.

BIOS

If you are a Dell customer, you can incorporate BIOS updates into the Blueprints for your Windows 10 devices from Dell.

1 Configure the **Security** settings.

Setting	Description
BIOS Password	Enter the password used to unlock the BIOS of the device. This text box is required.
TPM Chip	Select **Enable** and enable the device Trusted Platform Module chip.

2 Configure the **Boot** settings.

Setting	Description
Boot Mode (drop-down menu)	Select whether the device starts in **BIOS** or **UEFI** mode.
Boot Mode Protection (check box)	Safeguards the start settings of a device when Boot Mode is changed. Disabling Boot Mode Protection can prevent the currently installed operating system from booting if Boot Mode is changed.
Secure Boot	Select **Enable** and use Secure Boot settings on the device. You cannot disable Secure Boot with DCM. If your devices already use Secure Boot, you must manually disable the settings on the device. Secure Boot requires **Boot Mode** to be set to **UEFI** and **Legacy Option ROMS** to be set to **Disable**.
Legacy Option ROMS	Select **Enable** and allow the use of legacy option ROMS during the boot process.

3 Configure the **Virtualization** settings.

Setting	Description
CPU Virtualization	Select **Enable** and allow hardware virtualization support.
Virtualization IO	Select **Enable** and allow input/output virtualization.
Trusted Execution	Select **Enable** and allow the device to use the TPM chip, CPU Virtualization, and Virtualization IO for trust decisions. Trust Execution requires the **TPM Chip**, **CPU Virtualization**, and **Virtualization IO** settings to be set to **Enabled**.

Add Users and User Groups to a Blueprint

After you have added policies to the Workspace ONE Express blueprint, you can add new and existing users and active directory-based user groups to your blueprint.

When users Chapter 4 Enrollment, they receive all the applications, resources, and policies from the blueprint.

Add Existing Users to a Blueprint

Add existing Workspace ONE Express users to a blueprint using the search bar.

1 Search current users with the search bar.

2 Add the search results to your blueprint.

Add New Users to a Blueprint

You can add Workspace ONE Express users to a blueprint as Basic users or Directory users.

1 Select **Add User**.

You must Basic and Directory Accounts.

a For Basic users, fill out the user information, making sure to select 'Basic' as the **Security Type**.

b For Directory users, fill out the user information, making sure to select 'Directory' as the **Security Type**.

2 After all the settings have been selected, add the Basic or Directory user to the blueprint by selecting **Add User** at the bottom of the page.

You can assign multiple blueprints to users.

Applications and resources that are unique to the assigned blueprint are installed on the user device. Applications and resources that are duplicated across multiple blueprints do not get duplicated on the device.

Add Groups to a Blueprint

Use the **Add Group** button to search for existing directory-based user groups to assign Workspace ONE Express blueprints to users and their devices.

1 Complete the group settings.

Setting	Description
Directory Name	Read-only option displaying the address of your directory services server.
Domain	The domain automatically populates based on the directory services server information you enter on the **Directory Services** page (**System > Enterprise Integration > Directory Services**).
Group Base DN	The group base distinguished name is used as a starting point for the user group search. Information in this setting populates automatically based on the **Domain** setting.
Group Name	Identify the name of a user group in your active directory and select **Search** to search for it. If a directory group contains your search text, a list of group names displays. Select a Group Name from your **Search Results** list.

2 Select **Add Group** to add the user group to the list of users and user groups to be added to the blueprint.

3 Once your list of users and user groups is complete, select **Continue** to save your settings and apply your users to the blueprint.

4 Select **Publish** to finalize and push the blueprint out to user devices. You can return to the Blueprints listing to edit your blueprint configurations at any time.

How Do You Migrate Blueprints for Android Enterprise

You can migrate any Workspace ONE Express Blueprint you published before configuring Android EMM Registration to ensure that the Blueprint is pushed to your enrolled Android Enterprise devices.

Procedure

1 Navigate to **Blueprints > List View** and locate the Blueprint you want to migrate.

2 Select the **App** tile and begin migrating applications.

Applications for Android Enterprise require an approval process. Therefore, any applications you added to Android Blueprints before registering with Android Enterprise must be searched for in the Google Play Store, downloaded again, and readded to the migrated Blueprint.

a Select the **Add App** button.

b Select the **Add** button under **Public App**. Web applications do not need to be migrated.

c Select the check mark for Android and deselect the check marks for Apple and Windows Desktop.

d Enter the name of the application to be readded in the text box and select **Search**.

Search results display from the Google Play Store.

e Select the specific application you want to add to the Blueprint and select the green **Approve** button.

A separate popup window displays containing a list of elements the application has access to.

f Review this access list and select **Approve** again to proceed and add the application to the Blueprint.

g Another popup window displays containing **Approval Settings** and **Notifications**. Select the settings and notification options you want to enable and select **Save** to add the application to your Blueprint.

h **Set App Delivery** by selecting **On Demand** or **Automatic**.

i Select **Done**, select **View Applications**, then select **Done** again.

This process consolidates the old application and the new, readded application into one, single application which is then pushed to both Android Enterprise and legacy Android devices.

3 Select the **Resources** panel and begin migrating Email and Wi-Fi resources.

a Select **Edit** and change the existing **Email** configuration.

The **Configure Microsoft Exchange ActiveSync Email** screen appears. You are not required to change any of the options to migrate it. You only have to load it and immediately save it.

b Select **Save Changes**.

c Do the same thing for **Wi-Fi** resources. Select **Edit** and immediately select **Save Changes**.

4 Select the **Policies** panel and begin migrating the policy configuration.

   a Just like before, you must only select **Edit Policies** and immediately select **Save Changes**.

Results

You have successfully migrated a Blueprint you made for devices enrolled as Android (Legacy) and applied it to devices enrolled as Android Enterprise.

Enrollment

4

Even if users are added to a Blueprint and the Blueprint is published, those users must finish the Workspace ONE Express and Express+ enrollment process first before their devices are managed. The enrollment process might differ slightly depending on the device platform (iOS, Android, Windows 10 (Express+ Only)).

Android

You can configure your Android registration as Enterprise or Legacy but not both. To begin managing Android Enterprise devices, you must register Workspace ONE Express as your Enterprise Mobility Management (EMM) provider with Google. The Chapter 2 Express Setup provides a step by step solution to help configure the enterprise management tools required to secure and manage your Android devices.

If you configure the Android devices in your fleet as Enterprise devices, you have two modes from which to select.

- **Work Profile** enrollment mode creates a dedicated space on the device for only work applications and data. This deployment is ideal for Bring Your Own Device (BYOD) applications.

  Applications in the Work Profile are differentiated by a red briefcase icon, called badged applications, and are shown in a unified launcher with the user's personal applications. For example, your device shows both a personal icon for Google Chrome and a separate icon for Work Chrome denoted by the badge. From an end-user perspective, it looks like two different applications, but the application is installed only once but with business data stored separately from personal data.

  The Workspace ONE Intelligent Hub agent facilitates the Work Profile mode. You can download the Hub from the Google Play Store. Proceed to Enroll a Device With Workspace ONE Intelligent Hub.

- **Work Managed** enrollment mode gives Workspace ONE Express full control of the entire device. There is no separation of work and personal data. The ownership type known as COPE (Corporate-Owned, Personally Enabled) is not supported.

  The Work Managed mode is user-based, not device-based, which means the same Google account is used across all devices registered to an individual user.

Consider registering Work-Managed Android devices from a factory reset state and ensure that these devices are not configured for personal use.

The Work Managed mode is facilitated by using a special identifier with the Workspace ONE Intelligent Hub. For more information, see Enroll Android Devices Using VMware Workspace ONE Intelligent Hub Identifier.

Apple DEP Integration

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

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

Windows 10 Devices (Express+ Only)

Workspace ONE Express+ supports multiple Windows 10 enrollment flows that meet specific use cases.

- **Intelligent Hub Enrollment** — The simplest enrollment workflow uses the Workspace ONE Intelligent Hub for Windows to enroll devices. End users simply direct the native browser on the Windows 10 device to https://getwsone.com and select the **Download Hub for Windows 10** button.
- **Azure Active Directory Integration Enrollment** — Through integration with Microsoft Azure Active Directory, Windows devices automatically enroll into Workspace ONE Express+ with minimal end-user interaction. Azure AD integration enrollment simplifies enrollment for both end users and admins.

  Azure AD integration enrollment supports three different enrollment flows.

  - Join Azure AD.
  - Out of Box Experience enrollment.
  - Office 365 enrollment.

Enrollment through an Azure AD integration requires Windows 10 and an Azure Active Directory Premium License. The configuration requires entering information into your Azure AD and Workspace ONE Express+ deployments to facilitate communication. For more information, see Set Up Directory Services with a Wizard or Set Up Directory Services Manually.

This chapter includes the following topics:

Enroll a Device With Workspace ONE Intelligent Hub

Enrolling a device with the Workspace ONE Intelligent Hub is the main option for Android, iOS, and Windows devices in Workspace ONE Express and Workspace ONE UEM powered by AirWatch.

Procedure

1. Download and install the Workspace ONE Intelligent Hub from the Google Play Store (for Android devices) or from the App Store (for Apple devices).

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

   Windows 10 devices must point the default browser on the device to https://getwsone.com to download the Hub.

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

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

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

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

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

Results

The device is now enrolled with the Workspace ONE Intelligent Hub app. In the **Summary** tab of the **Device Details View** for this device, the security panel displays "Hub Registered" to reflect this enrollment method.

Integrate Device Enrollment Program

Integrating Workspace ONE Express with Apple Device Enrollment Program (DEP) requires completing tasks in both the Workspace ONE Express Console and in Apple's DEP portal. Your organization must already be registered with Apple's Deployment Programs.

When you begin the integration process, Workspace ONE Express suggests that you do not use Internet Explorer as your browser. Also, once you begin configuring the DEP wizard in the Workspace ONE Express Console, keep the browser session open. You cannot save your activity until you complete the final configuration step, so it is important to finish the entire configuration in one browser session.

Procedure

1. Start in the Workspace ONE Express Console to begin integrating with DEP.
2. Move between the DEP portal to create a virtual MDM server container for devices and the Workspace ONE Express Console to create an initial profile.
3. Assign devices to the virtual MDM container in Apple's portal, so they can be managed through Workspace ONE Express.

Create or Edit the DEP Enrollment Profile

After you register devices with the Apple Business Manager portal, use the DEP Enrollment Program wizard to create a DEP enrollment profile in Workspace ONE Express or Workspace ONE UEM powered by AirWatch. An enrollment profile is a collection of DEP settings assigned to your registered devices.

Create a DEP enrollment profile or edit an existing profile. If needed, you can create more profiles later.

1. In the Workspace ONE UEM console, navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Device Enrollment Program**.
2. Select **Upload** and select Apple Server Token File (.p7m). Select **Next**. Now Workspace ONE UEM and Apple can authenticate each other.

   For clarity, use only one token at the customer organization group. Only add multiple tokens if your organization has a complex configuration, or if you are enrolling devices with multiple DEP accounts.

3 Configure the **Authentication** settings, based on whether you turn authentication **On** or **Off**. Authentication settings are only available for devices running iOS 7.1 or later. If devices running iOS 7.0 and earlier are assigned an authentication profile, the devices are automatically enrolled using staging authentication.

- If you turn on **Authentication**, each user must tie a DEP device to their own user account.
- If you turn off **Authentication**, you can enable staging of all devices under a single user account, and extra configuration options appear on the Settings page to accommodate this option.

If you set Authentication to **On**, then configure:

Setting	Description
Device Ownership Type	Determines the ownership type of the device upon enrollment, which can be either Corporate-Dedicated or Employee-Owned.
Device Organization Group	Select the organization group your where your end users authenticate. Only end-user accounts created at this level or a parent above it can authenticate their devices. End users can authenticate using either their Active Directory credentials or basic Workspace ONE UEM credentials, depending on which authentication type you have enabled under Enrollment settings.
Custom Prompt	Turn **On** Custom Prompt to enable custom text to appear on the device authentication screen during the Setup Assistant. Authentication occurs when end users are prompted for their credentials. For Apple School Manager, turn **Off** Custom Prompt if you are deploying shared iPads.
Message Template	Select a message template to send as a Custom Prompt. (Supported for English-language only.) This option is not available when **Custom Prompt** is **Off**.

If you turn Authentication **Off**, then configure:

Setting	Description
Default Staging User	Select the Enrollment User assigned to the device.
Device Ownership Type	Select the ownership type of the device upon enrollment, which can be either Corporate-Dedicated or Employee-Owned.
Device Organization Group	Select the organization group where your devices are enrolled.

4 Configure **MDM features** of the device.

Setting	Description
Profile Name	Enter the name of the profile as it appears in the UEM console.
Department	Enter the name of your department as it appears in the device's **About Configuration** panel upon setup and enrollment.
Support Number	Enter your organizational support contact phone number as it appears in the device's **About Configuration** panel upon setup and enrollment.
Require MDM Enrollment	Select **Enable** and require end users to enroll into Workspace ONE UEM MDM. Use this setting to ensure end-user devices cannot be activated unless they enroll into Workspace ONE UEM MDM.

Setting	Description
Supervision	Enable the option to set the device in Supervised mode, which is an alternative to configuring Supervised devices using Apple Configurator. Supervision is required for shared devices.
Shared Devices	Enable the option to use shared devices with education functionality. This option must be enabled for shared devices using Apple School Manager.
Lock MDM Profile	Select **Enable** and prevent end users from unenrolling from Workspace ONE UEM MDM. This setting ensures that end users cannot remove the Workspace ONE UEM MDM profile installed on the device. This option can only be enabled if Supervision is enabled.
Anchor Certificate	Enable this option to upload the certificate as a trusted anchor certificate and push to devices during the DEP enrollment. These certificates are used as trusted anchor certificates when evaluating the trust of the connection to the MDM server URL. If no certificate is uploaded, the built-in root certificates are used.
Device pairing	Enable the option to allow the device to sync with any Workstation through iTunes, Configurator, and iPCU. Optionally, set Device Pairing to **Disable** when deploying education functionality, and **Upload** a **Device Pairing Certificate** for supervised identities. From Workspace ONE UEM 9.2.2, you can upload Device Pairing Certificates whether Device Pairing is set to Enabled or Disabled.
Await Configuration.	Enable this setting if the MDM server is expected to send extra commands before the device can allow the user to proceed in the Setup Assistant. Await Configuration is required for the education functionality. To override the Await Configuration setting on a device, navigate to **Device > Details View** and select the device to override. Select **More Actions > Device Configured**, note the device as configured, and skip the Awaiting Configuration screen during enrollment. If you enable **Await Configuration**, more options appear in the **Setup Assistant** section.
Auto Advance Setup	Enable this setting to apply the DEP configuration automatically to an enrolling device. Users can skip all setup panes, and the device is automatically set to the most restrictive option by default within around 30 seconds after network active. Applies to ethernet-connected tvOS devices only.

5 Select the items seen by end users during the Apple **Setup Assistant** workflow that appears after the device is powered on for the first time. For Apple School Manager, **Skip** all Setup Assistant options.

Setting	Description
Passcode	Select **Don't Skip** and require the user to set a passcode during setup. If an MDM passcode profile is already set up through Workspace ONE UEM, select **Skip**.
Touch ID	Select **Don't Skip** and prompt the user to configure Touch ID during setup.
Location Services	Select **Don't Skip** and prompt user to enable or disable Location Services during setup. If you plan on tracking GPS locations for your devices, select **Don't Skip**.
Restoring from Backup	Select **Don't Skip** and prompt user to restore from the backup during setup. You must select **Don't Skip** to allow users to move data from a previous device, including an Android Device.
Move from Android	If **Restoring from Backup** is set to **Don't Skip**, select **Don't Skip** in this pane to prompt users to move accounts and data from an Android device during setup.
Sign in with Apple ID and iCloud	Select **Don't Skip** and prompt the user to sign in with an Apple ID and iCloud account during setup.

Setting	Description
Terms of Use and Conditions	Select **Don't Skip** and prompt users to read and accept the Terms of Use and Conditions during setup.
Siri	Select **Don't Skip** to prompt the user to configure Siri. If you select **Skip**, Siri is disabled on enrolled devices.
Diagnostics	Select **Don't Skip** and prompt the user to enable or disable sending diagnostic data to Apple. If you select **Skip**, sending diagnostic data is disabled on enrolled devices.
Registration	Select **Don't Skip** and prompt the user to register the device with Apple during setup.
Apple Pay	Select **Don't Skip** and prompt the user to set up an Apple Pay account during setup. If you select **Skip**, Apple Pay is disabled on enrolled devices.
Zoom	Select **Don't Skip** and prompt the user to enable the zoom functionality during setup.
FileVault 2	Select **Don't Skip** and prompt the user to set up a FileVault. The device determines whether or not to display this setup step.
Display Tone	Select **Skip** and allow users to skip the display tone setup step for enrolling iOS devices.
Home Button Sensitivity	Select **Skip** and allow users to enroll devices without configuring the Home button sensitivity on enrolling iOS devices.
Tap to Setup	Select **Skip** and allow enrolling tvOS devices to enroll without an associated iOS device.
Screen Saver	Select **Skip** and allow users to enroll a tvOS device without configuring a screen saver.
Keyboard	Select **Skip** and omit the prompt for users to select a keyboard type during the Setup Assistant process.
Onboarding	Select **Skip** and prevent users from viewing on-boarding informational screens for the user education during the Setup Assistant process.
Watch Migration	Set to **Skip** and prevent users from viewing options for the watch migration during the Setup Assistant process.
iCloud Analytics	Set to **Skip** and omit a user prompt to send analytics to iCloud during setup.
iCloud Documents and Desktop	Set to **Skip** and prevent users from viewing iCloud Documents and Desktop screen in macOS.
TV Home Screen Sync	Set to **Skip** and prevent users from toggling the TV home screen layout during setup.
TV Provider Sign In	Set to **Skip** and prevent users from signing in to a TV provider during setup.
Where is the TV?	Set to **Skip** and omit the **Where is this Apple TV** screen on tvOS devices enrolling through DEP.
Privacy	Set **Skip** and omit the **Privacy** screen in the DEP setup assistant while onboarding.
iMessage And FaceTime	Set to **Skip** and prevent the iMessage and FaceTime prompt during setup.
Software Update	Set to **Skip** and prevent informing users about Software Updates during setup.
Screen Time	Set to **Skip** and prevent informing users about Screen Time during setup.
SIM Setup	Set to **Skip** and prevent users from viewing the SIM Setup screen during setup.
Welcome	Set to **Skip** the Get Started screen during setup.
Express Language	Set to **Skip** the Express Language Setup screen during setup.

Setting	Description
Preferred Language	Set to **Skip** the Preferred Language Order screen during setup.
Appearance	Set to **Skip** the Choose Your Look screen during setup.
Primary Account Setup	This item appears only if **Await Configuration** is set to **Enabled**. Select **Don't Skip** to require users to create an account during setup. Configure the type of account the user creates in **Account Type**. Select **Skip** if you have created a Directory Profile for the user and they do not need to create an account. Configure the admin account for this selection in the **Admin Account Creation** section and auto log in after the Setup Assistant is disabled.

6 For certain configurations detailed in the **Setup Assistant** configuration, use the **Primary User Account** section to define the type of account the end users are allowed to create at the end of the setup. create an admin account for local and remote macOS device admin actions.

Setting	Description
Primary Account Creation	
Account Type	This item appears only if the **Primary Account Setup** is set to **Don't Skip**. Select **Standard** and give users access to a standard user account on their macOS device. If you select Standard, you must create an admin account to manage the Standard account. Select **Administrator** and allow users to create an Administrator account on their macOS device.
Autofill	Enable the option to auto populate the primary account information.
User Name	Enter the account name for the primary account. To automatically populate the enrollment user's organization user name, use the lookup values, such as {EmailUserName}, {EnrollmentUser}.
Full Name	Enter the full name for the primary account. To automatically populate the enrollment user's first and last name, use the default lookup values, such as {FirstName}, {LastName}.
Allow Editing	If the option is disabled and the primary account user name and full name is predefined, the user cannot modify the User Name and Full Name fields in Setup Assistant. **Note** Allow editing is applicable only if Autofill is enabled.
Create New Admin Account	Enable the option to create a managed admin account during the DEP enrollment. Currently, on macOS only one managed admin account can be created.
Admin Account Creation	
User Name	Enter the account name for the admin account.
Full Name	Enter the full name for the admin account.
Unique Random Password	Generate a unique random password of 14 characters, with at least 2 symbols, 1 lowercase, 1 uppercase, and 1 digit. If enabled, cannot be changed back to static password. (macOS 10.11)

Setting	Description
Password	Disable Unique Random Password toggle to create a static password for the account. This password will be used for all assigned devices that enroll with this configuration.
Hidden	Select **Enabled** and hide the admin account on the macOS device. Hidden accounts are not visible in the Login Window to end-users. Select **Disabled** and make the admin account visible when a user logs in.

7 Select **Save** to view the **Summary** page and review the settings you have selected. Assign the settings to devices registered in the Device Enrollment Program.

Setting	Description
Sync Now and Assign to All Devices	Select **Yes** and save and deploy the DEP profile settings to all devices that are currently registered with the MDM server that you just created in the DEP portal. Selecting **No** saves the DEP profile settings but does not deploy them to devices.
Auto Assign Default Profile	Select **Yes** and push the DEP profile settings to all devices that are currently registered once they are synced with Workspace ONE UEM **and** any devices from that point on as they are newly registered with Apple and synced with Workspace ONE UEM. Selecting **No** means that the newly registered devices do not automatically receive the DEP profile settings. Enable this setting if you plan to create multiple DEP profiles for different devices.

8 Once the deployment options are configured, select **Save**. You are now ready to manage profiles on DEP-enabled devices from the UEM console.

Enroll Android Devices Using VMware Workspace ONE Intelligent Hub Identifier

During Work Managed Device enrollment, the user must enter a special DPC-specific identifier token when they are prompted to add an account. A token is in the format “afw#EMM_Identifier” and automatically identifies Workspace ONE Express as your EMM provider.

Important This enrollment flow is only for Android accounts using Android 6.0 (M+) devices.

Procedure

1 Tap **Get Started** on your factory reset device.

2 Select your **Wi-Fi** network and login with your credentials to connect the device.

3 Enter the identifier “afw#hub” when prompted to add a Google account. The setup wizard adds a temporary Google Account to the device. This account is only used to download the DPC from Google Play and is removed upon completion.

If the identifier is entered incorrectly, you are prompted to reenter it.

4 Tap **Install** and begin configuration of the Workspace ONE Intelligent Hub to the device. The Hub will automatically open after install is complete.

5 Select the **Authentication Method** and continue enrollment:

   a Select **Server Details** and enter Server, Group ID, and user credentials.

   b Select **QR Code** if you have created a QR Code in the Express console.

6 Follow the remaining prompts and complete enrollment.

7 Any Blueprint created after registering with Android EMM initiates an automatic push to the device. The Workspace ONE Express console reports the status of Android on the users devices. You can review the **Details View** page to verify that Android was successfully created.

Admin View

5

Once the Express Setup, device enrollment, and blueprint creation processes are complete, the Workspace ONE Express Admin Console allows you to manage every aspect of your device deployment.

With this single, web-based resource, you can quickly and easily add new devices and users to your fleet, manage blueprints, and configure system settings.

Before you begin managing devices with Workspace ONE Express, acquaint yourself with the Admin Console buttons and panels containing the most helpful information about your device fleet.

Collapse and Expand the Main Menu

Collapse or close the secondary menu, which creates more space on the screen for device information, by selecting the bottom-left arrow  . To expand or reopen the secondary menu, select the modified right arrow  .

Exporting Reports

You can export reports in the default Excel format (XLSX) or a comma-separated values format (CSV) of the exported list views from two locations in Workspace ONE Express.

- **Enrollment Status List View**, which is found by navigating to **Devices > Lifecycle > Enrollment Status**.
- **Device List View**, which is found by navigating to **Devices > List View**.

Save the exported listings by selecting the **Export** button from these locations.

You can view and download these reports for viewing with Excel by navigating to **Monitor > Reports & Analytics > Exports**.

This chapter includes the following topics:

- Basic and Directory Accounts
- User Accounts List View, Express
- User Groups List View, Express
- Admin Accounts
- Configurations

Blueprints

Once you have created a library of blueprints in Workspace ONE Express, you may find that editing an existing blueprint is preferable to creating a blueprint from scratch. You can also delete unwanted blueprints.

View the listing and make desired changes by navigating to **Blueprints**.

Rename the Blueprint

Change the name of the blueprint as it appears in the listing by selecting the edit icon ( ) next to the blueprint name.

Edit the Blueprint Configuration

You can edit the **Applications**, **Resources**, **Policies**, **Users**, and **Groups** that are defined in a blueprint and view those **Devices** they are assigned to. Select the icon that corresponds to the specific blueprint element you want to edit.

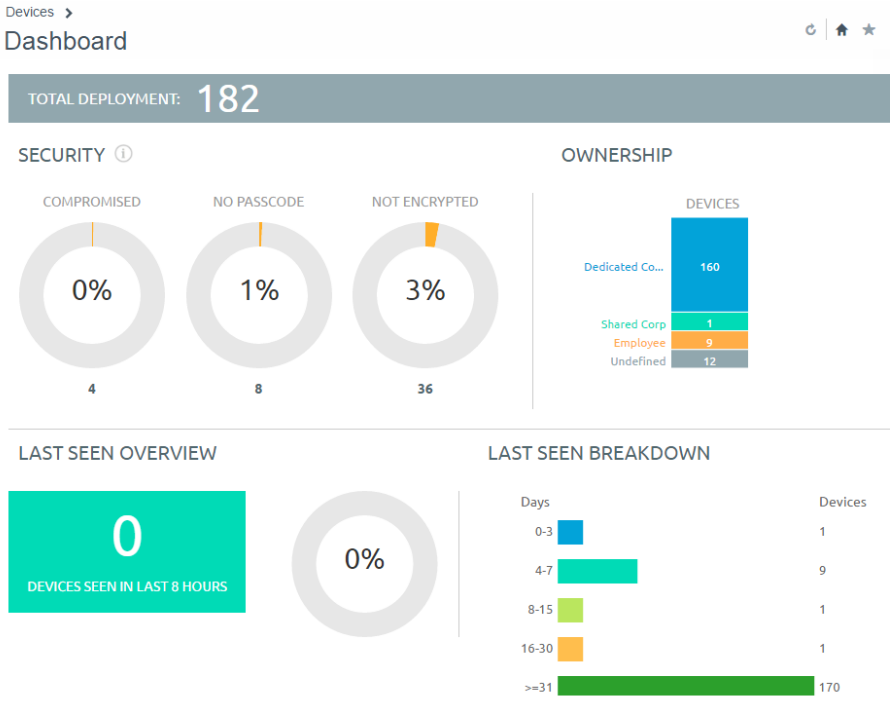
Selecting the Devices icon only displays those devices to which a blueprint has been assigned. Editing the **users** changes the devices of a blueprint.

Delete the Blueprint

You can delete an unwanted blueprint by selecting the **Delete Blueprint** link above the Devices icon. You are asked to confirm the deletion.

Devices Dashboard

You can view and manage enrolled devices from the Workspace ONE Express **Device Dashboard**. The device dashboard provides a high-level view of your entire device fleet and allows you to examine individual devices and take MDM actions.



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

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

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

- **Last Seen Overview/Breakdown** – View the number and percentage of devices that have recently communicated with the Workspace ONE Express server. For example, if devices have not been seen in over 30 days, select the bar graph to display a filtered **Device List** of only those devices. You can add more filters if needed (for example, Corporate Dedicated), and follow-up with the users accordingly.
- **Platforms** – View the total number of devices in each device platform category. Select any bar graph to display a filtered **Device List** view comprised of devices under the selected platform.
- **Enrollment** – View the total number of devices in each enrollment category. Selecting any of the bar graph segments displays a filtered **Device List** view comprised of devices with the selected enrollment status.
- **Operating System Breakdown** – View devices in your fleet based on operating system. There are separate charts for the major supported platforms. Display a filtered **Device List** view comprised of devices running the selected OS version by selecting any bar graph.

Device List View

Use the Device List View in Workspace ONE Express to see a full listing of devices in the currently selected organization group.

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

Select a device-friendly name in the **General Info** column at any time to open the details page for that device. A **Friendly Name** is the label you assign to a device to help you differentiate devices of the same make and model.

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

Search in Device List View

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

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

Customize Device List View Layout

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

There is also an option to apply your customized column view to all administrators. For instance, you can hide 'Asset Number' from the **Device List** views seen by your admins.

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

Add a Device from List View, Express

You can add or register a device in your Workspace ONE Express environment including user assignment, custom attributes, and tagging.

Procedure

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

2 Select the **Add Device** button. The **Add Device** page displays. Complete the following settings.

Table 5-1. User

Setting	Description
Search Text	Each device must be assigned to a user. Search for a user with this text box by entering search parameters and select the **Search User** button. You can select a user from among the search results or select the link **Create New User**.

Table 5-2. Create New User

Settings	Description
Security Type	Select between **Basic** and **Directory** users. For more information, see the topics, Basic Authentication, and Active Directory Authentication.
User name	Enter the user name by which your user is identified in your environment.
Password, **Confirm Password**	Enter and confirm the password that corresponds to the user name.
Email Address	Enter the email address for the user account.
Enrollment Organization Group	The organization group (OG) that serves as the enrollment OG for the device enrollment.
Show advanced user details	Display all the advanced user details, including comprehensive information covering user name, user phone number, and manager name. Also included are optional identification settings such as department, employee ID, and cost center. Select the default **User Role** for the user you are adding which determines which permissions the user has while using a connected device. For more information, see the topic User Roles.

Table 5-3. Device

Settings	Description
Expected Friendly Name	A device's **Expected Friendly Name** is the label you assign to a device to help you differentiate devices of the same make and model. You can opt for a manually entered friendly name or you can incorporate lookup values. For details, see Chapter 8 Lookup Values.
Organization Group	Pre-populated setting reflects the existing organization group.
Ownership	Select the device ownership from the drop-down menu. Select between **None**, **Corporate - Dedicated**, **Corporate - Shared**, and **Employee-Owned**.
Platform	Select the platform of the device from the drop-down menu.
Show advanced device information options	Display all the advanced device information settings.

Table 5-4. Advanced Device Information Settings

Settings	Description
Model	Select the device model from the drop-down listing. The contents of this drop-down menu depend upon the selection made in the **Platform** drop-down menu.
OS	Select the device's operating system from the drop-down listing. The contents of this drop-down menu depend upon the selection made in the **Platform** drop-down menu.
UDID	Enter the device's Unique Device Identifier.
Serial Number	Enter the device's serial number.
IMEI	Enter the device's 15-digit International Mobile Station Equipment Identity.
SIM	Enter the device's SIM card specifications.
Asset Number	Enter the asset number for the device. This number is created internally from within your organization and this setting is provided to hold this data point.

Table 5-5. Messaging

Setting	Description
Message Type	Select the type of message you want to send (**None**, **SMS**, or **Email**) to the device upon a successful enrollment to the environment.
Email Address	Enter the email address to which you want the enrollment message sent. This text box is only available when Email is selected as the **Message Type**.
Email Message Template	Select the email template from the drop-down menu. There is a link you can use to open the Message Template page where you can create an email message template.
Phone Number	Enter the phone number to which you want the SMS text message sent. This text box is only available when SMS is selected as the **Message Type**.
SMS Message Template	Select the SMS template from the drop-down menu. There is a link you can use to open the Message Template page where you can create an SMS message template.

3 (Optional) Assign **Custom Attributes** to the device. Select the **Add** button and supply an **Attribute** and its **Value**.

4 (Optional) Assign **Tags** to the device. Select the **Add** button and select a tag from the drop-down menu for each tag you want to assign.

5 Select **Save**.

Device Details

The Device Details page in Workspace ONE Express contains detailed information for a single device and grants access to user and device management actions quickly.

Access Device Details by selecting a device-friendly name from one of the available Dashboards, or by navigating to **Devices > Details View**.

The main page features several major sections.

- **Notification Badges** – Displays the Compromised State, Enrollment Date, time Last Seen, and the Do Not Disturb setting for the selected device.
- **Summary** – Displays details such as organization group, smart groups, phone number, serial number, UDID, asset number, power status, storage capacity, physical memory, and available updates.
- **Profiles** – Displays all profiles such as installed (active), assigned (inactive), and unmanaged (sideloaded).
- **Apps** – Displays all installed applications, both automatic apps and on-demand apps.
- **Updates** – Displays a list of application and OS updates that apply to the selected device, including each installation status.
- **Location** – If you have accepted the Third-Party Supplemental Terms of Use, you can select this tab to see the location of the selected device on a Microsoft Bing Map.
- **More** – Displays other device details categories.
  - **Security** – Displays all the major security subgroups and their corresponding statuses.
  - **Troubleshooting** – Displays the Event Log and Commands listings including a filter and search capabilities, enabling you to perform troubleshooting on the device.

Device Details Dashboard

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

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

Device Details Action Button Cluster

The device action button cluster enables you to perform common device actions such as **Send** [Message], **Lock** [Device], and **More Actions**. The Actions Button Cluster can be found in the upper-right corner of the **Devices > Details View**.

It can also be found in the **Devices > List View** when you select one or more devices from the listing.

Available Device Actions vary by platform, device manufacturer, model, and enrollment status, and the specific configuration of your Workspace ONE Express Console.

Device Action Descriptions in Workspace ONE Express

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

- **Activation Lock Bypass** – Clear the Activation Lock on an iOS device. With the Activation Lock enabled, the user requires an Apple ID and password before taking the following actions: disabling Find My iPhone, factory wipe, and reactivate to use the device.
- **Clear Passcode** – Clear the device passcode. To be used in situations where the user has forgotten their device's passcode.
- **Delete Device** – Delete and unenroll a device from the console. Sends the enterprise wipe command to the device that gets wiped on the next check-in.
- **Device Check-In** – Send an MDM query command to the device to return basic information on the device such as friendly name, platform, model, operating system version, and ownership status.
- **Device Wipe** – Send an MDM command to wipe a device clear of all data and operating system. This puts the device in a state where recovery partition is needed to reinstall the OS. This action cannot be undone.
- **Disable Lost Mode** – Use this command to unlock a DEP or supervised device stuck in Lost Mode. When Lost Mode is disabled by an administrator, the device returns to normal functionality.
- **Edit Friendly Name** – Edit the Friendly Name of a device. A Friendly Name is the label you assign to a device to help you differentiate it from other devices, particularly devices of the same make and model.
- **Enterprise Reset** – Enterprise Reset a device to factory settings, keeping only the Workspace ONE Express enrollment.
- **Enterprise Wipe** – Enterprise Wipe a device to unenroll and remove all managed enterprise resources including applications and profiles. This action cannot be undone and re-enrollment will be required to manage this device again.
- **Find Device** – Send a text message to the applicable application together with an audible sound.

- **Location** – Reveal a device's location by showing it on a map using its GPS capability.
- **Lock Device** – Send an MDM command to lock a selected device, rendering it unusable until it is unlocked.
- **OS Update** – Push an operating system update to one or more iOS (version 9 or later) or macOS devices. Applicable only to supervised, DEP-enrolled devices.
- **Request Device Check-In** – Request that the selected device check itself in to the Workspace ONE Express console. This action updates the **Last Seen** column status.
- **Send Message** – Send a message to the user of the selected device. Select between **Email**, **Push Notification** (through AirWatch Cloud Messaging), and **SMS**.

Enrollment Status, Express

You can assess enrollment status into Workspace ONE Express on a per-device basis and revoke/reset device tokens by reviewing the Enrollment Status.

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

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

Setting	Description
Filters	You can filter out entire device categories by using filters which enable you to see only those devices that you are interested in. ■ **Enrollment Status** ■ **Platform** ■ **Ownership** ■ **Token Status** ■ **Token Type** ■ **Source** ■ **First Seen**
Add	■ **Register Device** – You can register or **Add** a single device to be enrolled. ■ **Allowlist or Denylist Devices** – You can allow only those devices to enroll that you have identified or allowlisted. Alternatively, you can restrict devices from an enrollment by denylisting devices. ■ **Batch Import** – Import multiple devices or multiple users with the Batch Import screen.
Resend Message	Resend the original message sent to a user, including Self-Service Portal URL, Group ID, and login credentials.
More Actions	
Change Organization Group	Pre-populated setting reflects the existing organization group.
Change Ownership	Change the type of ownership for the selected device.

Setting	Description
Delete	Permanently delete the registration information for selected devices. This action forces the user to re-register to enroll. Where applicable, you must first revoke the token before deleting a device registration.
Reset Token	Reset the status of a token if it has been revoked or is expired.
Revoke Token	Force the registration token status of selected devices to expire, essentially blocking access for unwanted users or devices. For the **Reset Token** and **Revoke Token** actions, you can select to disable the **Notify Users** setting which prevents the default email notification from being sent.
Selecting Multiple Devices	Act on individual devices or multiple devices by selecting the check box next to each device and using the action buttons. Once you have applied a filter to show a specific set of devices, you can perform bulk actions to multiple selected devices. Perform this action by selecting the devices and selecting an action from the **Resend Message** and **More Actions** buttons. You can select individual check boxes. You can also select the entire set of filtered devices by selecting the global check box located atop the check box column. When you select an action for one or more devices, a confirmation screen displays allowing you to **Save** or **Cancel** the action.
Layout	Display the full listing of visible columns or choose to display or hide columns per your preferences by selecting the **Custom** option. There is also an option to apply your customized column view to all administrators. You can return to the **Layout** button settings at any time to modify your column display preferences.

Enrollment Status Details View

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

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

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

- **Summary** – View the registration date, time elapsed since the device was first seen, basic device and user info.
- **User** – View user details.
- **Message** – View the outgoing Device Activation email message including credential information and QR code. There is a resource available, called "User Registration Message," that allows the administrator to hide the **Message** tab after the device has successfully enrolled.
- **Custom Attributes** – View the Custom Attributes associated with the device.
- **Tags** – View the tags currently associated with the device.

- **Offline Enrollment** – If available, this tab allows you to enroll the device while it is offline. This feature is useful for when you want to use the device while offline (for example, while traveling).

Add a Denylisted or Allowlisted Device

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

Note Denylisting devices that are registered in the Device Enrollment Program (DEP) restricts those devices from having a DEP profile assigned to them in the future.

Procedure

1. Navigate to **Devices > Lifecycle > Enrollment Status** and select **Add**.
2. Select **Denylist Devices** or **Allowlist Devices** from the **Add** drop-down menu and complete the settings.

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

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

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.

- **Denylisted Devices**

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

- **Allowlisted 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**.

Use the Android Migration Tool

You can migrate your Android legacy-enrolled devices in Workspace ONE Express to take advantage of all the benefits of being enrolled in the Android Enterprise, including the use of work profiles and automatic separation of your work and personal applications.

Prerequisites

You must have completed the following tasks before you can migrate Android devices.

- Register Workspace ONE Express with Google as your Enterprise Mobility Manager. For details, see Android EMM Registration.
- Approve public applications, Resave resources, and Resave Policies.

  Android Enterprise Apps must be approved before they can be installed on devices. Also, you must resave any Email or Wi-fi resources and policies you configured in existing Blueprints that you published before registering with Android EMM. Resaving resources and policies ensures that your devices receive all the corporate apps and settings upon migration to Android Enterprise Work Profile. You can perform all these tasks by following How Do You Migrate Blueprints for Android Enterprise.

After these prerequisites are complete, take the following steps.

Procedure

1 Navigate to **Devices > Lifecycle > Legacy Android Migration**.

2 Select the **New Migration** button.

  A **New Migration** screen displays.

3 Review the **Pre Requisites**. If you are sure that they have been completed, select **Next** to proceed.

4 Complete the **Details** tab.

  a Enter the **Name** and **Description** for this migration effort. Providing a name and description is useful for when you have more than one migration to perform. For example, you can migrate all the Android devices in one Blueprint, then later, migrate Android devices from another Blueprint.

  b In **Devices**, select 'Devices in Blueprint <your Blueprint name>' to target only the legacy Android devices in a specific Blueprint or select 'All Devices' to target all legacy Android devices in your entire fleet. You can use the Search text box to locate a specific Blueprint.

  c Customize the **Message** viewed by the device end user when they open the notification from their device.

d Select **Validate** and confirm that all legacy Android devices are eligible to be migrated.

e Select **Continue** to proceed.

5 Review the migration **Summary**. You can see a listing of each Android device, the user name, eligibility status, and reason for ineligibility. You can also use the **Search List** option to locate a device in the listing.

6 Select **Create** to send the notification.

The **New Migration** screen closes and you are taken back to the **Legacy Android Migration** page in the Workspace ONE Express console.

Table 5-6. Legacy Android Migration

Setting	Description
New (button)	Select to create an Android Migration.
Edit (button)	You can edit the settings of an existing migration. 1 Locate the migration from the listing that you want to edit. 2 Enable it by selecting the radio button located to the left of the migration name. 3 Select the **Edit** button and change the migration configuration.
Delete (button)	You can delete an existing migration. 1 Locate the migration from the listing that you want to delete. 2 Enable it by selecting the radio button located to the left of the migration name. 3 Select the **Delete** button and remove the migration from the listing permanently.
Search	Locate a specific migration from the listing by entering a search keyword.
Refresh (button)	Select to refresh the statuses of all active migrations.

You can see the listing of all your Android migrations here, including columns for **Name**, **Description**, **Devices**, **Devices Migrated**, **Total Devices**, and **Status**.

7 The end user receives a notification about the migration. When this notification is opened, it displays the **Message** you customized plus information about the migration including a way to opt out.

8 Direct the user to select the **Continue** button to proceed with the migration.

a They can also postpone the migration, for example if their battery is low, by selecting the **Not Now** button.

Results

- The end user's Android legacy-enrolled device is upgraded to Android Enterprise Work Profile mode.
- Their work and personal apps are separated.
- New versions of work applications now feature a small, red toolbox badge in the corner of the app icon. This badge makes it easy to identify new versions of work apps and differentiate them from the old versions.
- New versions of work apps can only access data from other new versions of work apps.

What to do next

Direct end users to uninstall old versions of work apps (the ones without the small, red toolbox) to limit work apps' access to personal data.

Basic and Directory Accounts

The type of authentication in Workspace ONE Express you select depends on the amount of administrator setup work and the number of login steps by the end user at enrollment.

If you want the enrollment process to be as simple as possible for the end user, the administrator must do more work to set it up. Likewise, a lighter workload for the administrator means that there is more setup to do by the end user.

Basic User Accounts

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

Pros

- Basic users require no enterprise infrastructure.
- Requires no technical integration.

Cons

- Offers no federated security and no single sign-on.
- Credentials for basic users only exist in Workspace ONE Express and do not necessarily match existing corporate credentials.
- Basic user names and passwords are stored in Workspace ONE Express.

Directory User Accounts

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

Pros

- Directory users authenticate with existing corporate credentials.
- Secure method of integrating with LDAP/AD.
- Standard integration practice.

Cons

- Requires an active directory or other LDAP server.

Create Basic User Account

After you decide which Authentication Type you want to use, you can create users in the Workspace ONE Express console powered by AirWatch. If your authentication type is Basic, then consider creating Basic User Accounts.

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** and 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.
Display Name	Represent the user in the 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.
Enrollment Organization Group	Pre-populated setting reflects the existing organization group.
Allow the user to enroll into additional Organization Groups.	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. Workspace ONE Express customers have a single organization group to enroll into. Contact Support to inquire about upgrading to benefit from having multiple organization groups.
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.
Message Type	Select the type of message you want to send to the user, **Email** or **None**.
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 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 (Optional) Select the **Advanced** tab and complete the following settings.

Setting	Description
Email Password	Enter the email password of the user you are adding.
Confirm Email Password.	Confirm the email password of the user you are adding.
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.
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.
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** and save only the new user or select **Save and Add Device** to save the new user and proceed to the **Add Device** page.

Create Directory User Account

After you decide which Authentication Type you want to use, you can create users in the Workspace ONE Express console. If your authentication type is based on your existing active directory structure, then consider creating Directory User Accounts.

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 selecting **Directory** as the Security Type.
Directory Name	This pre-populated setting identifies the Active Directory name.
Domain	Select the domain name from the drop-down menu.

Setting	Description
User name	Enter the user's directory user name and select **Check User**. If the system finds a match, the user's information is auto-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 the 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.
Enrollment Organization Group	For Workspace ONE Express customers, this setting is pre-populated and reflects the existing organization group.
Allow the user to enroll into additional Organization Groups.	Workspace ONE Express customers have a single organization group to enroll into. If you want to inquire about upgrading to benefit from having multiple organization groups, contact Support.
User Role	Select the role for the user you are adding from this drop-down menu.
Message Type	Select the type of message you can send to the user, **Email** or **None**.
Message Template	Select the template for email 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 (Optional) Select the **Advanced** tab and complete the following settings.

Setting	Description
Email Password	Enter the email password of the user you are adding.
Confirm Email Password.	Confirm the email password of the user you are adding.
Distinguished Name	For directory users recognized by Workspace ONE Express, this text box is pre-populated with the distinguished name of the user. Distinguished Name is a string representing the user name and all authorization codes associated with an Active Directory user.
Manager Distinguished Name	Enter the distinguished name of the user's manager. This text box is optional.
Category	Select 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.

Setting	Description
Cost Center	Enter the user's cost center for your company's administrative purposes.
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** and save only the new user or select **Save and Add Device** to save the new user and proceed to the **Add Device** page.

User Accounts List View, Express

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.

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 a 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 ■ Status
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. ■ **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.
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.
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 two action buttons to appear, **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 Edit User Group Permissions.
Remove from User Group.	Remove selected users from the existing user group.
Change Organization Group	Pre-populated setting reflects the existing organization group.
Delete	If a member of your organization permanently ends 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 is allowed 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 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.

- **Denylisted Devices**

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

- **Allowlisted 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**.

User Groups List View, Express

The User Groups List View page in Workspace ONE Express 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.

Action	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 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.
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 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 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 an empty user group.

Edit User Group Permissions

Fine-tuning user group permissions in Workspace ONE Express 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** tab to control who can manage certain user groups and who can assign profiles, compliance policies, and applications to user groups.

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 the **Add** button.

4 The **Organization Group** displays the prepopulated organization 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.

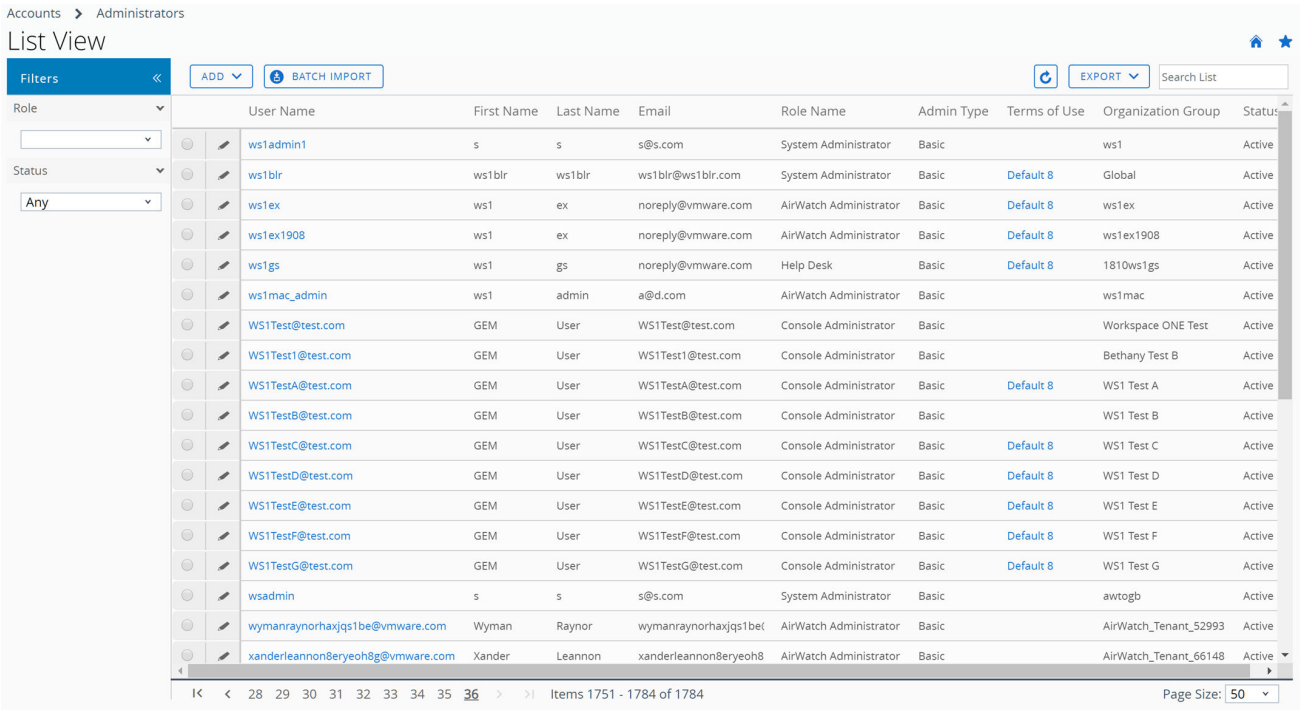
- **Administrator Only** – The permissions affect only those administrators at the parent OG.
- **All Administrators at or below this Organization Group** – The permissions affect the administrators in the OG.

7 Select **Save**.

Admin Accounts

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

Admin Account List View



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.

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.

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.

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.
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 Ticket Number from ZenDesk, Bugzilla, JIRA, or other help desk tool 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 role.
- Delete a role by selecting the delete icon ( ).

Directory User Status Syncing

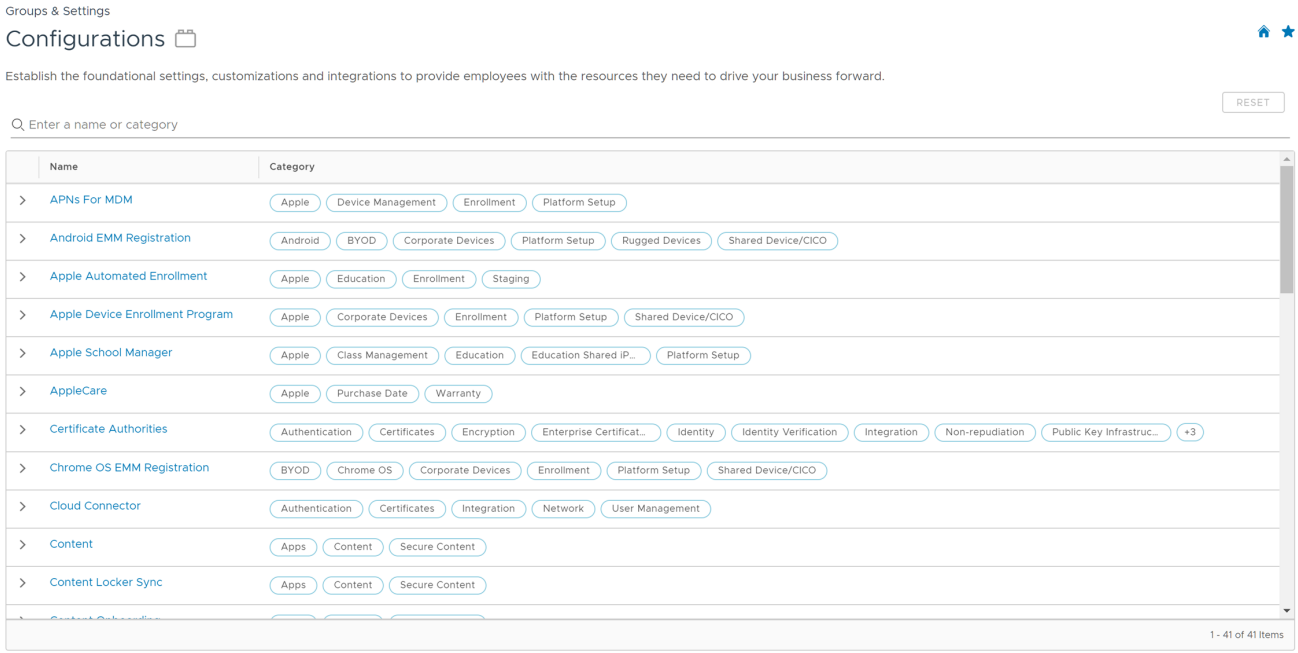
When you make users inactive in your directory service, it impacts the corresponding Workspace ONE UEM and Workspace ONE Express account in a similar way but only assuming these prerequisite conditions.

- 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**, and in the **Server** tab, look for the **Bind User Name** text box.
  - Workspace ONE Express customers can find the **Bind User Name** text box in the same **Server** tab by navigating to **Groups & Settings**, then select **Directory Services** from the **Name** column.
- 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.

- Furthermore, the recycle bin must be enabled using the Active Directory Administrative Center but only if you are deleting users in AD.
  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.

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.

AirWatch Cloud Connector

6

The AirWatch Cloud Connector runs in the internal network. The connector serves as a proxy that securely transmits requests from Workspace ONE Express to the organization's critical enterprise infrastructure components.

It runs from within your internal network and allows you to benefit from Workspace ONE Mobile Device Management (MDM). AirWatch Cloud Connector works with your existing Active Directory (AD), Lightweight Directory Access Protocol (LDAP), email, and other internal systems.

While completion of the Chapter 2 Express Setup configures the AirWatch Cloud Connector, refer to this section for information which has been designed for Workspace ONE Express. If you need further details about any specific AirWatch Cloud Connector element, consult the **AirWatch Cloud Connector Documentation** (available on docs.vmware.com) or contact Workspace ONE Support.

Prerequisites

Ensure that your system meets the necessary **Hardware Requirements** to deploy AirWatch Cloud Connector as part of a SaaS deployment.

- Virtual Machine or Physical Server, one CPU Core, 2.0+ GHz, Intel processor required.
- 2-GB RAM or more.
- 6-GB disk space for the VMware Enterprise Systems Connector application, Windows OS, .NET runtime, and Workspace ONE Express logging operations.

Ensure the server running Workspace ONE Express meets the necessary Software Requirements.

- Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 Desktop Experience.
- .NET Framework version 4.6.2.
  - The AirWatch Cloud Connector (ACC) auto-update feature does not function correctly until your ACC server is updated to .NET Framework 4.6.2.
  - The ACC auto-update feature does not update the .NET Framework automatically.
  - Install .NET 4.6.2 manually on the ACC server before performing an upgrade.

Ensure that the Network Requirements for the AirWatch Cloud Connector Server are met.

- **Workspace ONE Express Console** (for example, https://cn274.awmdm.com)
  - Protocol: HTTP or HTTPS
  - Port: 80 or 443
  - Verify by entering https://cnXXX.awmdm.com and ensure that there is no certificate trust error.
  - Replace 'XXX' with the same number as used in your environment URL, for example, '100' for cn100.
  - If an auto-update is enabled, AirWatch Cloud Connector must query the Workspace ONE Express console for updates using port 443.
- **AirWatch API** (for example, https://cn274.awmdm.com)
  - Protocol: HTTPS
  - Port: 443
  - Verify by entering https://asXXX.awmdm.com/api/help and ensure that you are prompted for credentials.
  - Replace 'XXX' with the same number as used in your environment URL, for example, '100' for cn100.
  - AirWatch Cloud Connector to API access is required for the proper functioning of the AirWatch Diagnostics service.
- **CRL** (for example http://csc3-2010-crl.verisign.com/CSC3-2010.crl)
  - Protocol: HTTP
  - Port: 80
  - For various services to function properly.
- **Optional Network Requirements**
  - Internal SMTP using port 25.
  - Internal LDAP under protocol LDAP or LDAPS using port 389, 636, 3268, or 3269.

Procedure

1 Enable AirWatch Cloud Connector from Console.

   a Generate certificates and select the enterprise services and Workspace ONE Express services to be integrated.

2 Install the AirWatch Cloud Connector.

   a Run the AirWatch Cloud Connector installer on your configured server that meets all the prerequisites.

3 Verify a Successful AirWatch Cloud Connector Installation from within the console.

Enable AirWatch Cloud Connector from Console

Before you install AirWatch Cloud Connector (ACC), you must first enable it, generate certificates, and select the enterprise services and Workspace ONE Express services to be integrated. After completing this step, you can install ACC.

Important Perform the following steps on the server running AirWatch Cloud Connector. Do not download the installation application onto another computer and copy it to the AirWatch Cloud Connector server.

Procedure

1 Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Cloud Connector**.

2 Configure the following settings on the **General** tab.

Setting	Description
Enable AirWatch Cloud Connector.	Enable AirWatch Cloud Connector and display the **General** tab.
Enable Auto Update.	Enable AirWatch Cloud Connector to update automatically when a newer version is available.

3 Configure the following settings on the **Advanced** tab.

Setting	Description
Generate Certificates.	Generate a certificate for the AirWatch Cloud Connector and Workspace ONE Express server. Certificates are generated for both and displayed under AirWatch Cloud Connector and AirWatch certificates. Once certificates are generated, the button changes to **Regenerate**.
Enterprise Services	Enable or disable **Enterprise Services**. The services you select (enabled) integrate with AirWatch Cloud Connector. ■ SMTP (Email Relay), AirWatch SaaS offers email delivery through its own SMTP. ■ Directory Services (LDAP/AD).
AirWatch Services	Enable or disable **AirWatch Services**. The AirWatch components you select (enabled) integrate with AirWatch Cloud Connector (ACC). Consider leaving all services enabled. ■ Device Services (Admin Console and all services required for it to operate, including related Windows services). ■ Device Management (Enrollment, App Catalog, and related Windows services).

4 Select **Save**.

5 Navigate back to the **General** tab and select **Download AirWatch Cloud Connector Installer**.

6 A **Download ACC-Installer.exe** screen displays. Enter a password for the AirWatch Cloud Connector certificate in the text box. The password is needed later when you run the AirWatch Cloud Connector installer.

7 Select **Download** and save the **AirWatch Cloud Connector x.x Installer.exe** file on the ACC server.

Use this file later in Install the AirWatch Cloud Connector.

Install the AirWatch Cloud Connector

The AirWatch Cloud Connector (ACC) must be installed and running for Workspace ONE Express to manage your devices.

Procedure

1 Open the installer on the ACC server.

2 When the **Welcome** screen appears, select **Next**.

The installer verifies prerequisites on your ACC server. If a previous version of AirWatch Cloud Connector is installed, the installer auto-detects it. The installer then offers the option to update the AirWatch Cloud Connector automatically.

3 Accept the license agreement, and then select **Next**.

4 Select **Change** and select the installation directory. Select **Next**.

5 Enter the **Certificate Password** that you provided on the **System Settings** page in Workspace ONE Express. Select **Next**.

6 If you plan on routing ACC traffic through an outbound proxy, select the check box and provide proxy server information. Enter the **User Name** and **Password** credentials and then select **Next**.

7 When the installation screen appears, select **Install** to begin the installation.

The installer displays a check box for auto-updating AirWatch Cloud Connector.

8 Select **Finish**.

Results

By default, the Install the AirWatch Cloud Connector check box is selected. It updates without any user intervention by querying Workspace ONE Express for newer versions of ACC.

Using AirWatch Cloud Connector Auto-Update

Auto-update allows AirWatch Cloud Connector (ACC) to upgrade automatically to the latest version so Workspace ONE Express can continue to function smoothly.

While you are Install the AirWatch Cloud Connector, by default, the auto-update check box is selected. It updates without any user intervention by querying Workspace ONE Express for newer versions of AirWatch Cloud Connector.

Benefits

- No requirement to determine manually if you must upgrade and then have to search for the latest version – the software does it for you.
- Since it assures you stay updated, you always have the latest features, enhancements, and fixes.
- Most importantly, it ensures that you have the most up-to-date security.

Update Process

AirWatch Cloud Connector auto-update is performed using the **Bank1** and **Bank2** folders inside the **CloudConnector** folder. Workspace ONE Express detects which of these folders is empty and streams into it the appropriate ACC files. Also, the update process empties the contents of the other folder. For the following update, Workspace ONE Express repeats the process except for the alternate folder. This process repeats each time a new version is auto-updated.

Important Do not delete the **Bank1** or **Bank2** folders. The **Bank1** and **Bank2** folders are integral to the AirWatch Cloud Connector auto-update process.

Auto-Update Security

AirWatch Cloud Connector auto-updates are performed with security in mind. The Workspace ONE Express Console signs every update and AirWatch Cloud Connector verifies it. It only updates itself with a signed and verified upgrade. The upgrade process is also transparent to the AirWatch Admin. AirWatch Cloud Connector knows when a newer version is available by querying the Workspace ONE Express Console on port 443. An upgrade only occurs after this newer version becomes available.

While AirWatch Cloud Connector is upgrading to the latest version, it is temporarily unavailable. Therefore, there is a short loss of service of approximately 1 minute. Customers with multiple AirWatch Cloud Connector servers benefit from Workspace ONE Express incorporating a random timer to direct the upgrade process. This random timer means that outages occur at different times. Such an arrangement ensures that all AirWatch Cloud Connector services are not down at the same time.

When the AirWatch Cloud Connector auto-updates, the version under Add or Remove Programs does not change. The original version is still listed. The version under Add or Remove Programs only changes when you run the full AirWatch Cloud Connector installer. The best way to verify if the auto-update succeeded is to look at the version number in the AirWatch Cloud Connector logs.

Verify a Successful AirWatch Cloud Connector Installation

After you install AirWatch Cloud Connector, you can verify a successful installation from within the Workspace ONE Express Console.

Procedure

1 Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > AirWatch Cloud Connector**.

2 Select **Test Connection** at the bottom of the screen.

The following message displays.

What to do next

Now that you have successfully installed AirWatch Cloud Connector, you can use it to integrate with your directory service infrastructure. Proceed to the Directory Services Setup.

Introduction to Directory Services 7

Workspace ONE Express integrates with your organization's existing directory service – such as Active Directory including Azure AD, Lotus Domino, and Novell e-Directory – to provide directory-based account access. With directory services integrated, you can authenticate with apps and enroll devices using their existing directory service credentials.

Integrating with directory services eliminates the need to create basic user accounts for everyone in your organization. Integration can also help simplify the enrollment process for end users by using information they already know.

Ongoing LDAP synchronization detects any changes within the system and can automatically perform necessary updates across all devices for affected users. This ongoing synchronization also means that changes do not occur without required administrative approval.

Integrating Workspace ONE Express with your directory service provides many benefits.

- Conduct an easy enrollment for both users and administrators.
- Map directory groups to Workspace ONE Express user groups.
- Control Workspace ONE Express Console access.
- Apply existing credentials for VMware Content access.
- Assign apps, profiles, and policies by user group.
- Automatically retire end users when they go inactive.

The following sections explain how to integrate your Workspace ONE Express environment with your directory service of choice. The sections also describe how to add directory user accounts to Workspace ONE Express and how to integrate user groups with Workspace ONE Express.

Important The Directory Service information presented in this guide has been designed for Workspace ONE Express customers. If you need details about any Directory Service element or concept, consult the **VMware Workspace ONE UEM Directory Services Guide**.

This chapter includes the following topics:

- Directory Service User Integration
- Directory User Group Integration

Directory Services Setup

Directory services setup requires you to integrate your Workspace ONE Express environment with your directory service including attribute mapping for users and user groups.

Use the **Directory Services** page to configure the settings that let you integrate your Workspace ONE Express server with your organization's domain controller. The domain controller is the server that hosts your directory services system.

After entering server settings, you can filter searches to identify users and user groups. You can set options to auto merge and sync changes between your Workspace ONE Express configured groups and directory service groups. You can also map attribute values between Workspace ONE Express user attributes and your directory attributes.

Note For Software as a Service (SaaS) customers, directory services integration requires you to install the Chapter 6 AirWatch Cloud Connector.

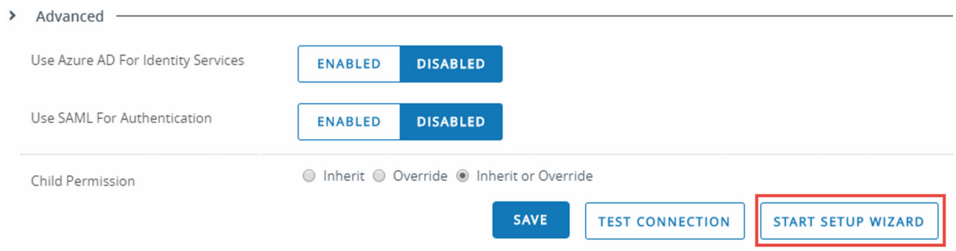
Set Up Directory Services with a Wizard

During the initial setup, Workspace ONE Express provides a simplified wizard to streamline the directory services setup process. The wizard includes steps to integrate either Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), or both.

Note If SAML or LDAP settings are already configured, the Workspace ONE Express Console can detect it.

Procedure

1 Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services** and select **Launch Setup Wizard**.



2 Upon launching the wizard, select **Configure** to follow the steps.

Alternately, you can **Skip wizard and configure manually** to Set Up Directory Services Manually.

Set Up Directory Services Manually

If you want to customize your directory service settings, you can skip the wizard and configure your settings manually to get up and running with Workspace ONE Express or Workspace ONE UEM powered by AirWatch.

Navigate to **Accounts > Administrators > Administrator Settings > Directory Services** to manually configure the Server, User, and Group settings for the Directory service.

1 Navigate to **Accounts** > **Administrators** > **Administrator Settings** > **Directory Services** > **Server** and configure **LDAP** settings.

Setting	Description
Directory Type	Select the type of directory service that your organization uses. Workspace ONE UEM and Workspace ONE Express supports open-source LDAP for directory services. For more information on the best practices that can be followed while configuring open-source LDAP Directory Service, see the Workspace ONE UEM Directory Service Integration guide.
DNS SRV	Allow the Domain Name System Service Record to decide which server in its prioritized list of servers can best support LDAP requests. This feature ensures continuity of services in a high availability environment. The default setting is Disabled. With this option disabled, Workspace ONE UEM uses your existing directory server, the address of which you enter in the Server setting. Supported DNS servers: ■ Active Directory integrated Microsoft DNS servers ■ Standalone Microsoft DNS servers
Server	Enter the address of your directory server. This setting is only available when **Enable DNS SRV** is Disabled.
Encryption Type	Select the type of encryption to use for a directory services communication. The options available are **None** (unencrypted), **SSL**, and **Start TLS**.
Port	Enter the Transmission Control Protocol (TCP) port used to communicate with the domain controller. The default for the unencrypted LDAP directory service communication is port 389. To view a KnowledgeBase article that lists the most up-to-date Workspace ONE UEM SaaS data center IP ranges, refer to https://support.air-watch.com/articles/115001662168. ■ When you change the **Encryption Type** setting to **SSL**, the **Port** setting automatically changes to 636. ■ When you select the **Add Domain** button, the **Port** setting automatically changes to 3268.
Verify SSL Certificate.	This setting is only available when the **Encryption Type** is **SSL** or **Start TLS**. Receive SSL errors by selecting the SSL check box.
Protocol Version	Select the version of the Lightweight Directory Access Protocol (LDAP) that is in use. Active Directory uses LDAP versions 2 or 3. If you are unsure of which Protocol Version to use, try the commonly used value of '3'.
Use Service Account Credentials.	Use the App pool credentials from the server on which the VMware Enterprise Systems Connector is installed for authenticating with the domain controller. Enabling this option hides the **Bind user name** and **Bind Password** settings.

Setting	Description
Bind Authentication Type.	Select the type of bind authentication to enable the AirWatch server to communicate with the domain controller. You can select **Anonymous**, **Basic**, **Digest**, **Kerberos**, NTLM, or **GSS-NEGOTIATE**. If you are unsure of which Bind Authentication Type to use, start by setting the bind authentication type to **Basic**. You know if your selection is not correct when you click **Test Connection**.
Bind User Name.	Enter the credentials used to authenticate with the domain controller. For example, you can enter either "Username or Domain\username". This account (which the entered user name identifies) allows a read-access permission on your directory server and binds the connection when authenticating users. If you are unsure of which Bind Authentication Type to use, try the commonly used GSS-NEGOTIATE. You know if your selection is not correct when you click Test Connection. Clear the bind password from the database by selecting the **Clear Bind Password** check box.
Bind Password	Enter the password for the bind user name to authenticate with the directory server.
Domain /Server	Enter the default domain and server name for any directory-based user accounts. If only one domain is used for all directory user accounts, fill in the text box with the domain. This entry means that users are authenticated without explicitly stating their domain. You can add more domains by selecting the **Add Domain** option. Make sure that all the domains are in the same forest. In this case, Workspace ONE UEM automatically changes the port setting to 3268 for global catalog. You can change the port setting to 3269 for SSL encrypted traffic, or override it completely by entering a separate port.
Is there a trust relationship between all domains?	This setting is available only when you have more than one domain added. Select **Yes** if the binding account has permission to access other domains you have added. This added permission means that the binding account can successfully log in from more domains.

a Complete the following options are available after selecting the Advanced section drop-down.

Setting	Description
Search Subdomains	Enable subdomain searching to find nested users. Leaving this option disabled can make searches faster and avoids network issues. However, users and groups located in subdomains under the base Domain Name (DN) are not identified.
Connection Timeout	Enter the LDAP connection timeout value (in seconds).
Request Timeout	Enter the LDAP query request timeout value (in seconds).
Search without base DN	Enable this option when using a global catalog and when you do not want to require a base DN to search for users and groups.
Use Recursive OID at Enrollment.	Verify the user group membership at the time of enrollment. As the system runs this feature at enrollment time, your performance can decrease with some directories.
Use Recursive OID For Group Sync.	Verify the user group membership at the time of Group synchronization.
Object Identifier Data Type	Select the unique identifier that never changes for a user or group. The options available are **Binary** and **String**. Typically, the Object Identifier is in a **Binary** format.
Sort Control	Option to enable sorting. If this option is disabled, it can make searches faster and you can avoid sync timeouts.

b (Optional) Configure Azure AD For Identity Services.

The following settings are available only if enabling **Use Azure AD for Identity Services** and are only applicable if you are integrating with Azure Active Directory.

Azure AD integration with Workspace ONE UEM must be configured at the tenant where Active Directory (such as LDAP) is configured.

Setting	Description
MDM Enrollment URL	Enter the URL address used to enroll devices.
MDM Terms of Use URL	Enter the URL address of your terms of use agreement. There is a helpful link that displays exactly where in the Workspace ONE UEM in the Azure AD config panel these MDM URLs belong. This link is labeled, "Where in AAD do I paste this info?"
Directory ID	Enter the identification number used to authenticate your Azure AD license. The Azure **Directory ID** is found in your Azure AD Directory Instance URL. For example, if your URL is acme.com/WS/ADExt/Dir/0a12bc34-56d7-93f1-g2h3-i4-jk56lm78n, only the last section (0a12bc34-56d7-93f1-g2h3-i4-jk56lm78n) is your **Directory ID**.
Tenant Name	Enter the tenant name of your Azure AD instance. There is a helpful link that displays exactly how to obtain the tenant info from your AAD Directory Instance. This link is labeled, "How To Obtain Tenant Info"
Immutable ID-Mapping Attribute	The Immutable ID-Mapping Attribute points to the sourceAnchor field in Active Directory that is mapped to Azure AD. This setting enables Workspace ONE UEM to match the Azure AD immutable ID to the correct local active directory attribute.
Mapping Attribute Data Type	Select the mapping attribute data type of the field used by Workspace ONE UEM as the sourceAnchor for Azure AD. The default type is Binary.
Automatically revoke user tokens when wiping devices.	Enable this option to revoke Microsoft Azure AD user tokens when a device or enterprise wipe is run. It is not a best practice to disable this functionality as it might reduce the security posture of your configuration. If a wiped device is lost, it can still contain a valid AAD authentication token.

c (Optional) Configure SAML For Authentication.

The following Security Assertion Markup Language (SAML) options are available after enabling **Use SAML for Authentication**.

These options are only applicable if you are integrating with a SAML identity provider.

Setting	Description
Enable SAML authentication For	You have the choice of using SAML authentication for **Admin**, **Enrollment**, or **Self Service Portal**. UEM console administrators can select all three, or any combination of two, or select any one of the three components.
Use new SAML Authentication endpoint	A new SAML authentication endpoint has been created for end-user authentication (device enrollment and login to SSP). This authentication replaces the two dedicated enrollment and SSP endpoints with a single endpoint. While you may choose to keep your existing settings, Workspace ONE UEM suggests updating your SAML settings to take advantage of the new combined endpoint. If you want to use the new endpoint, enable this setting and save the page. Then use the **Export Service Provider Settings** to export the new metadata file and upload it to your IdP. Doing so establishes trust between the new endpoint and your IdP.

Table 7-1. SAML 2.0

Setting	Description
Import Identity Provider Settings	Upload a metadata file obtained from the identity provider. This file must be in Extensible Markup Language (XML) format.
Service Provider (Workspace ONE UEM**) ID**	Enter the Uniform Resource Identifier (URI) with which Workspace ONE UEM identifies itself to the identity provider. This string must match the ID that has been established as trusted by the identity provider.
Identity Provider ID	Enter the URI that the identity provider uses to identify itself. Workspace ONE UEM reviews authentication responses to verify that the identity matches the ID provided here.

Table 7-2. RESPONSE

Setting	Description
Response Binding Type	Select the binding types of the response. The options include **Redirect**, **POST**, and Artifact.
Sp Assertion URL	Enter the Workspace ONE UEM URL that the identity provider configures to direct its authentication responses. “Assertions” regarding the authenticated user are included in success responses from the identity provider.
Authentication Response Security	This value specifies whether the IdP signs the response. You can select between **None**, **Validate Response Signatures**, and **Validate Assertions Signatures**. Consider selecting Validate Response Signatures for a more secure authentication.

Table 7-3. CERTIFICATE

Setting	Description
Identity Provider Certificate	Upload the identity provider certificate.
Service Provider (AirWatch) Certificate	Upload the service provider certificate.**Note:**Currently we only support SHA256 based algorithms. For more information on all the providers that support SHA256, see https://docs.microsoft.com/en-us/windows/desktop/SecCertEnroll/cryptoapi-cryptographic-service-providers.
Export Service Provider Settings button	Exports the metadata file for uploading to your Identity Provider (IdP). This setting establishes trust between the new SAML endpoint (for enrollment and SSP login) and your IdP.

2 Navigate to **Accounts** > **Administrators** > **Administrator Settings** > **Directory Services** > **User** and configure the **User** settings.

Setting	Description
User Object Class	Enter the appropriate Object Class. In most cases, this value is "user."
User Search Filter	Enter the search parameter used to associate user accounts with Active Directory accounts. The suggested format is "<LDAPUserIdentifier>={EnrollmentUser}" where <LDAPUserIdentifier> is the parameter used on the directory services server to identify the specific user. ■ For AD servers, use "(&(objectCategory=person)(sAMAccountName={EnrollmentUser}))" exactly. ■ For other LDAP servers, use "CN={EnrollmentUser}" or "UID={EnrollmentUser}"

Advanced

Setting	Description
Auto Merge	Enable setting to allow user group updates from your directory service to merge with the associated users and groups in Workspace ONE UEM automatically.
Automatically Sync Enabled Or Disabled User Status	Select Enabled to deactivate the associated user in Workspace ONE UEM when that user is disabled in your LDAP directory service (for example, Active Directory, Novell e-Directory, and so on). ■ **Value For Disabled Status** – Enter a numeric value and select the type of Lightweight Directory Access Protocol (LDAP) attribute used to represent a user's status. Select "Flag Bit Match" if the user status is designated by a bitwise flag (which is the default for Active Directory). Select "Flag Bit Match" if the user status is designated by a bitwise flag (which is the default for Active Directory). When "Flag Bit Match" is selected, Directory Services will consider the user to be disabled if any bits from the property match the given value. **Note:**If you select this option and you disable users in your directory service, the corresponding user account in Workspace ONE UEM is marked inactive and those administrators and users are not able to log in. In addition, enrolled devices assigned to users who are set as inactive in your directory service are automatically unenrolled.
Enable Custom Attributes	Enable custom attributes. Custom Attributes is a section that appears under the main **Attribute** – Mapping Value table. You must scroll down to the bottom of the page to see the Custom Attributes.

Setting	Description
Attributes	Review and edit the **Mapping Values** for the listed Attributes, if necessary. These columns show the mapping between Workspace ONE UEM user attributes (left) and your directory service attributes (right). By default these attributes are values most commonly used in Active Directory (AD). Update these mapping values to reflect the values used for your own or other directory service types. If you add or remove a custom attribute, you should initiate a manual sync afterward by selecting the **Sync Attributes** button.
Sync Attributes button	Manually sync the attributes mapped here to the user records in Workspace ONE UEM. Attributes sync automatically on the time schedule configured for the Workspace ONE UEM environment.

3 Navigate to **Accounts** > **Administrators** > **Administrator Settings** > **Directory Services** > **Group** and configure **Group** settings.

Setting	Description
Group Object Class	Enter the appropriate Object Class. In most cases this value should be **group**.
Organizational Unit Object Class	Enter the appropriate Organizational User Object Class.

Advanced

Setting	Description
Group Search Filter	Enter the search parameter used to associate user groups with directory service accounts.
Auto Sync Default	Select this checkbox to automatically add or remove users in Workspace ONE UEM configured user groups based on their membership in your directory service.
Auto Merge Default	Select this check box to automatically apply sync changes without administrative approval.
Maximum Allowable Changes	Enter the number of maximum allowable group membership changes to be merged into Workspace ONE UEM. Any number of changes detected upon syncing with the directory service database under this number are automatically merged. If the number of changes exceed this threshold, an administrator must manually approve the changes before they are applied. A single change is defined by a user either leaving or joining a group. A setting of 100 Maximum Allowable Changes means the Console does not need to sync with your directory service as much.
Conditional Group Sync	Enable this option to sync group attributes only after changes occur in Active Directory. Disable this option to sync group attributes regularly, regardless of changes in Active Directory.
Auto-Update Friendly Name	When enabled, the friendly name is updated with group name changes made in active directory. When disabled, the friendly name can be customized so admins can tell the difference between user groups with identical common names. This can be useful if your implementation includes organizational unit (OU)-based user groups with the same common name.
Attribute	Review and edit the **Mapping Value** for the listed **Attribute**, if necessary. These columns show the mapping between Workspace ONE UEM user attributes (left) and your directory service attributes (right). By default these attributes are values most commonly used in AD. Update these mapping values to reflect the values used for your own or other directory service types.

4 Verify that you have established proper connectivity by selecting the Test Connection button.

   The server connection is tested for all the domains listed on the page using the server name, bind user name, and the password provided by the administrator. You can rerun the test by clicking the **Test Again** button.

5 Select **Save**.

Best Practices for Configuring Open Source LDAP Directory Service Type

Workspace ONE UEM supports open source LDAP for directory services. For instance, similar to Microsoft Active Directory, Novell e-Directory, Lotus Domino, we have Samba OpenLDAP server for Directory services. Samba OpenLDAP is a widely used LDAP server in Linux environment.

If you choose to select any other LDAP server other than Active Directory, Novell e-Directory or Lotus Domino, you can refer through the following configuration tips that covers the most critical steps while configuring open source LDAP directory service.

Bind Authentication Type

You are required to select the type of bind authentication to enable the AirWatch server to communicate with the domain controller.

You can select **Anonymous**, **Basic**, **Digest**, **Kerberos**, **NTLM**, or **GSS-NEGOTIATE**. If unsure start by setting the bind authentication type to **Basic**. You will know if your selection is not correct when you click **Test Connection**.

Bind User Name

Enter the credentials used to authenticate with the domain controller. This account (which the entered user name identifies) allows a read-access permission on your directory server and binds the connection when authenticating users. It is considered to be a best practice to use the full base distinguished name for the bind username. For example, you can use **CN=admin**,**DC=domain**,**DC=com**.

User Search Filter

In the User Tab, enter the search parameter that is used to associate user accounts with Active Directory accounts and make sure your user search filter is appropriately configured. You could expect appropriate results if you set the search filter as **(&(objectCategory=person)(sAMAccountName={EnrollmentUser}))**.

Directory Service User Integration

Every directory user you want to manage through Workspace ONE Express must have a corresponding user account.

Integrating directory service users into Workspace ONE Express users is entirely optional. However, there are many benefits to applying the user data already stored within your directory service.

Integrating the two systems means that you gain the benefit of having the two systems linked. When a user becomes inactive in directory services, their linked user account status and device enrollment in Workspace ONE Express come to an end automatically. User inactivity includes employment termination, retirement, and so on.

Linking the two systems means mapping your directory service user information onto Workspace ONE Express.

Filter Your Searches to Map the Directory Services User Information

After entering server settings, you can filter searches to identify users and map values between Workspace ONE user attributes and your directory attributes.

Procedure

1 Navigate to **Accounts > Administrators > Administrator Settings > Directory Services**.

2 Select the **User** tab. By default, only the **Base DN** information displays.

3 Select the **Fetch DN** plus sign (+) next to the **Base DN** column.

This plus sign displays a list of Base DNs from which you can select to populate this text box. If it does not, revisit the settings you entered on the **Server** tab before continuing.

4 Enter data in the following settings.

Setting	Description
User Object Class	Enter the appropriate Object Class. In most cases, this value is "user."
User Search Filter	Enter the search parameter used to associate user accounts with Active Directory accounts. The suggested format is "<LDAPUserIdentifier>={EnrollmentUser}" where <LDAPUserIdentifier> is the parameter used on the directory services server to identify the specific user. ■ For AD servers, use "(&(objectCategory=person)(sAMAccountName={EnrollmentUser}))" exactly. ■ For other LDAP servers, use "CN={EnrollmentUser}" or "UID={EnrollmentUser}"

5 Display more settings by selecting **Show Advanced**.

Setting	Description
Auto Merge	Enable setting to allow user group updates from your directory service to merge with the associated users and groups in Workspace ONE UEM automatically.
Automatically Sync Enabled Or Disabled User Status	Select Enabled to deactivate the associated user in Workspace ONE UEM when that user is disabled in your LDAP directory service (for example, Active Directory, Novell e-Directory, and so on). ■ **Value For Disabled Status** – Enter a numeric value and select the type of Lightweight Directory Access Protocol (LDAP) attribute used to represent a user's status. Select "Flag Bit Match" if the user status is designated by a bitwise flag (which is the default for Active Directory). Select "Flag Bit Match" if the user status is designated by a bitwise flag (which is the default for Active Directory). When "Flag Bit Match" is selected, Directory Services will consider the user to be disabled if any bits from the property match the given value. **Note** If you select this option and you disable users in your directory service, the corresponding user account in Workspace ONE UEM is marked inactive and those administrators and users are not able to log in. In addition, enrolled devices assigned to users who are set as inactive in your directory service are automatically unenrolled.
Enable Custom Attributes	Enable custom attributes. **Custom Attributes** is a section that appears under the main **Attribute** – **Mapping Value** table. You must scroll down to the bottom of the page to see the Custom Attributes.
Attributes	Review and edit the **Mapping Values** for the listed **Attributes**, if necessary. These columns show the mapping between Workspace ONE UEM user attributes (left) and your directory service attributes (right). By default these attributes are values most commonly used in Active Directory (AD). Update these mapping values to reflect the values used for your own or other directory service types. If you add or remove a custom attribute, you should initiate a manual sync afterward by selecting the **Sync Attributes** button.
Sync Attributes button	Manually sync the attributes mapped here to the user records in Workspace ONE UEM. Attributes sync automatically on the time schedule configured for the Workspace ONE UEM environment.

6 Select **Test Connection** to verify connectivity.

The server connection is tested for all the domains listed on the page, using the server name, bind user name, and the password provided by the administrator. You can rerun the test by clicking the **Test Again** button.

From the **User** tab, you can perform the following actions:

a Select the **Domain** name from the drop-down menu.

b Enter the user's directory user name and select **Check User**. If the system finds a match, the user's information is auto-populated. The remaining settings in this section are only available after you have successfully located an active directory user with the **Check User** button.

From the **Group** tab, you can perform the following actions:

a Select the **External Type** of the 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**.

b Enter the directory user group name in the **Search** text.

c **Directory Name** is the pre-populated setting that identifies the Active Directory name.

d Select the **Domain** name from the drop-down menu.

e **Group Base DN** displays a list of Domain Names from which you can select.

f Select **Check Group** to verify the group information.

Directory User Group Integration

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

After you import existing directory service user groups as Workspace ONE Express user groups, you can perform tasks in the following areas.

- **User Management** – Reference your existing directory service groups (such as security groups or distribution lists) and align user management in Workspace ONE Express with the existing organizational systems.
- **Profiles and Policies** – Assign profiles, applications, and policies across a WorkspaceWorkspace ONE Express deployment to groups of users.
- **Integrated Updates** – Automatically update user group assignments based on group membership changes.
- **Management Permissions** – Set management permissions to allow approved administrators only to change policy and profile assignments for certain user groups.
- **Enrollment** – Allow users to enroll in Workspace ONE Express using their existing credentials.

Similar to the way Filter Your Searches to Map the Directory Services User Information, mapping user group data integrates your existing directory service groups into Workspace ONE Express user groups.

Merge and Sync Changes Between Your Directory Service Groups and Groups in Workspace ONE

You can set options to auto merge and sync changes between your directory service groups and groups in Workspace ONE Express and Workspace ONE UEM powered by AirWatch.

AD passwords are not stored in the Workspace ONE UEM database except the Bind account password used to link directory services into your Workspace ONE UEM environment.

The Bind account password is stored in an encrypted form in the database and is not accessible from the console. Unique session keys are used for each sync connection to the Active Directory server. This AD password storage arrangement is the same for Workspace ONE Express.

In some instances, global catalogs are used to manage multiple domains or AD Forests. Delays while searching for or authenticating users might be due to a complex directory structure. You can integrate directly with the global catalog to query multiple forests using one Lightweight Directory Access Protocol (LDAP) endpoint for better results.

Prerequisites

To integrate with the global catalog directly, configure the following settings.

- **Encryption Type** = None
- **Port** = 3268
- Verify that your firewall allows for this traffic on port 3268.

Complete the following steps to auto merge and sync changes between your Directory Service Groups and Groups in the Workspace ONE UEM console.

Procedure

1. Navigate to **Accounts > Administrators > Administrator Settings > Directory Services**.
2. If necessary, select 'Override' as the **Current Setting** so that changes can be made to this settings page.
3. Ensure your organization's Directory Service is selected in the **Directory Type**.
4. Select the **Group** tab. By default, only the **Base DN** information displays.
5. For **Base DN**, select the **Fetch DN** plus sign (+) next to the **Base DN** setting to display a list of Base DNs. Populate this text box by selecting from the list.
   a. If a list of Base DNs does not display, revisit the settings you entered on the **Server** tab before continuing.
6. Enter data in the following settings.

Setting	Description
Group Object Class	Enter the appropriate Object Class. In most cases this value should be **group**.
Organizational Unit Object Class	Enter the appropriate Organizational User Object Class.

7 To display more settings, select **Advanced**. Enter data in the following text boxes.

Setting	Description
Group Search Filter	Enter the search parameter used to associate user groups with directory service accounts.
Auto Sync Default	Select this checkbox to automatically add or remove users in Workspace ONE UEM configured user groups based on their membership in your directory service.
Auto Merge Default	Select this check box to automatically apply sync changes without administrative approval.
Maximum Allowable Changes	Enter the number of maximum allowable group membership changes to be merged into Workspace ONE UEM. Any number of changes detected upon syncing with the directory service database under this number are automatically merged. If the number of changes exceed this threshold, an administrator must manually approve the changes before they are applied. A single change is defined by a user either leaving or joining a group. A setting of 100 Maximum Allowable Changes means the Console does not need to sync with your directory service as much.
Conditional Group Sync	Enable this option to sync group attributes only after changes occur in Active Directory. Disable this option to sync group attributes regularly, regardless of changes in Active Directory.
Auto-Update Friendly Name	When enabled, the friendly name is updated with group name changes made in active directory. When disabled, the friendly name can be customized so admins can tell the difference between user groups with identical common names. This can be useful if your implementation includes organizational unit (OU)-based user groups with the same common name.
Attribute	Review and edit the **Mapping Value** for the listed **Attribute**, if necessary. These columns show the mapping between Workspace ONE UEM user attributes (left) and your directory service attributes (right). By default these attributes are values most commonly used in AD. Update these mapping values to reflect the values used for your own or other directory service types.

8 Select **Test Connection** to verify connectivity.

The server connection is tested for all the domains listed on the page, using the server name, bind user name, and the password provided by the administrator. You can rerun the test by clicking the **Test Again** button.

From the **User** tab, you can perform the following actions:

a Select the **Domain** name from the drop-down menu.

b Enter the user's directory user name and select **Check User**. If the system finds a match, the user's information is auto-populated. The remaining settings in this section are only available after you have successfully located an active directory user with the **Check User** button.

From the **Group** tab, you can perform the following actions:

a Select the **External Type** of the 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**.

b Enter the directory user group name in the **Search** text.

c **Directory Name** is the pre-populated setting that identifies the Active Directory name.

d Select the **Domain** name from the drop-down menu.

e **Group Base DN** displays a list of Domain Names from which you can select.

f Select **Check Group** to verify the group information.

Add Directory Service User Groups to Workspace ONE Express

User groups added in Workspace ONE Express can be synced – automatically when configured with a scheduler – with your directory service groups to merge changes or add missing users.

- Pros

  You have the option of restricting the enrollment to only known groups, which lets you restrict on a user group level who can enroll. This method also keeps your existing directory service group infrastructure and allows you to assign profiles, policies, content, and apps based on these existing group setups.

- Cons

  Uploading directory service user groups does not automatically create Workspace ONE Express user accounts. Therefore, if you have restricted enrollment for known users, you must add those user accounts into the Workspace ONE Express console manually.

Procedure

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

2 Complete the settings in the **Add User Group** screen as applicable, ensuring the user group **Type** is **Directory**.

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.
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**.

Setting	Description
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.
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.

Setting	Description
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.

3 Select **Save**.

Remove Users From User Groups Based on the Directory Service Group Membership

You can enable Workspace ONE UEM and Workspace ONE Express to detect when a directory service user account is removed and automatically remove its associated user account from the associated group.

Procedure

1 Navigate to **Accounts > User Groups > Settings > Directory Services**.

2 Select the **Group** tab.

3 See advanced configuration options by selecting the **Advanced** drop-down.

4 Select the **Auto Sync Default** check box to add and remove users in user groups automatically based on membership in directory service.

Lookup Values

8

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

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

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

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

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

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

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

```
jsmith iPad iOS GHKD
```

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

Data Overhead

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

Static Strings Versus Lookup Values

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

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

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