

AirWatch Express

VMware Workspace ONE UEM 1903



vmware®

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

<https://docs.vmware.com/>

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

docfeedback@vmware.com

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

Copyright © 2019 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1 Introduction to AirWatch Express 5**
 - [Upgrade From AirWatch Express 6](#)
 - [Privacy 6](#)
 - [Terms of Use 7](#)

- 2 Express Setup 8**
 - [Introduction and Survey 8](#)
 - [Apple Push Notification Service 9](#)
 - [Set Up VMware Enterprise Systems Connector 10](#)
 - [Set Up Active Directory 11](#)
 - [Set Up Apple's Volume Purchase Program 12](#)
 - [Devices & Users / Apple / VPP Managed Distribution 13](#)

- 3 Blueprints 15**
 - [Create a Blueprint 15](#)
 - [Name the Blueprint 16](#)
 - [Add Applications to a Blueprint 16](#)
 - [Workspace ONE UEM and Valid Google Play Store URLs 17](#)
 - [Add Resources to a Blueprint 18](#)
 - [Adding Policies to a Blueprint 19](#)
 - [Add Policies to a Blueprint 20](#)
 - [Android Policy Support 20](#)
 - [Adding Users and User Groups to a Blueprint 22](#)
 - [Add Existing Users to a Blueprint 22](#)
 - [Add New Users to a Blueprint 22](#)
 - [Add Group to a Blueprint 23](#)

- 4 Enrollment 24**
 - [Enroll a Device with Workspace ONE Intelligent Hub 24](#)
 - [Integrate Device Enrollment Program 25](#)
 - [Complete the DEP Enrollment Profile 26](#)

- 5 Admin View 30**
 - [Admin Console at a Glance 30](#)
 - [Header Menu 30](#)
 - [Admin Console Notifications 31](#)
 - [Main Menu 33](#)
 - [Monitor 34](#)

Admin Panel Dashboard	34
Exporting Reports	34
Blueprints	35
Managing Blueprints	35
Devices Dashboard	35
Device List View	37
Device Details	39
Enrollment Status	40
User and Admin Accounts	43
Basic and Directory Accounts	44
User Accounts List View	48
User Groups List View	51
Admin Accounts	52
6 Install VMware Enterprise Systems Connector	56
Enable VMware Enterprise Systems Connector From AirWatch Console	58
Install the VMware Enterprise Systems Connector	59
Using VMware Enterprise Systems Connector Auto-Update	59
Verify a Successful VMware Enterprise Systems Connector Installation	61
7 Introduction to Directory Services	62
Directory Services Setup	63
Set up Directory Services with a Wizard	63
Set Up Directory Services Manually	64
Directory Service User Integration	70
Map Directory Services User Information	70
Directory User Group Integration	72
Configure Map Directory Services Group Settings	73
Add Directory Service User Groups to AirWatch Express	74
Remove Users From User Groups Based on Directory Service Group Membership	77

Introduction to AirWatch Express

1

Mobile devices are valuable enterprise tools. They allow employees to have immediate access to your internal content and resources. However, the diversity of mobile platforms, operating systems, and versions can make managing devices difficult. VMware AirWatch[®] Express solves this problem by enabling you to configure, secure, monitor, and manage the most popular types of mobile devices in the enterprise.

AirWatch 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.

Supported Browsers

The AirWatch 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 AirWatch Express console, navigate to **Control Panel > Settings > Internet Options > Security** and ensure you have a security level or custom security level that includes the **Font Download** option being set to **Enabled**.

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

Supported Platforms

AirWatch Express supports the following devices and operating systems.

- | | |
|---------------------|---|
| ▪ Android 3.0+ | ▪ Apple iOS 7.0+ |
| ▪ Apple macOS 10.9+ | ▪ Windows 10 devices (mobile and desktop) |

This chapter includes the following topics:

- [Upgrade From AirWatch Express](#)
- [Privacy](#)
- [Terms of Use](#)

Upgrade From AirWatch Express

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

Contact Workspace ONE Support for more information.

Privacy

It is important that you inform your end users about how their data is collected, stored, and displayed when they enroll into AirWatch Express.

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

Privacy settings in AirWatch 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

Privacy Setting	Corporate-Dedicated	Employee-Owned
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.

Terms of Use

Ensure that all users with managed devices agree to the policy by defining and enforcing terms of use. If necessary, users must accept the terms of use before proceeding with enrollment, installing apps, or accessing the AirWatch Express Admin Console.

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

Express Setup

Setting up AirWatch 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 AirWatch 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.

This chapter includes the following topics:

- [Introduction and Survey](#)
- [Apple Push Notification Service](#)
- [Set Up VMware Enterprise Systems Connector](#)
- [Set Up Active Directory](#)
- [Set Up Apple's Volume Purchase Program](#)

Introduction and Survey

The Introduction and Survey page briefly acquaints you with AirWatch Express and asks you three questions about your deployment.

Setup
Exit

1 Introduction
2 Survey



Welcome to AirWatch Express

Everything you need to secure and manage your company's mobile devices is here. You can:

- Save time by configuring Wi-Fi and email for your devices
- Secure access to company data by enforcing a device passcode
- Locate, message, and wipe a device if lost or stolen
- And more!

Let's get started!

Continue

1 Are your employees using Apple devices?

2 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. AirWatch Express also supports other directory services such as Lotus Domino and Novell e-Directory.

3 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.

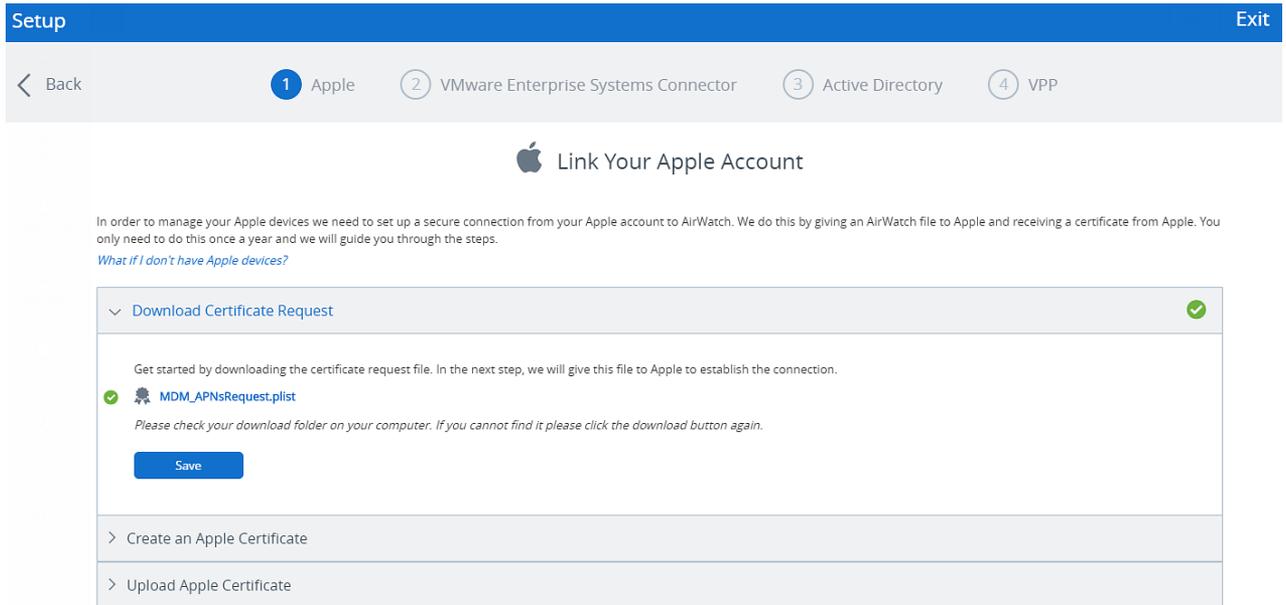
Apple Push Notification Service

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

You can always request Apple Push Notification Services (APNs) after the initial Express Setup.

Procedure

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



- 2 Download a Certificate Request.

- a Download the AirWatch 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.

Set Up VMware Enterprise Systems Connector

The VMware Enterprise Systems Connector Setup screen prompts you to download and run the VMware Enterprise Systems Connector Installer.

Once installed, it also prompts you to test the connection to the VMware Enterprise Systems Connector server.

Setup Exit

1 Apple 2 VMware Enterprise Systems Connector 3 Active Directory 4 VPP

VMware Enterprise Systems Connector (VMESC) Setup

Follow these simple steps to enable VMware Enterprise Systems Connector to securely access your organization's corporate resources without requiring changes to your network firewall. A list of hardware and software requirements and additional information about VMESC architecture is located [here](#).

Download Installer ✓

Create a password for your VMware Enterprise Systems Connector certificate below. You will need your certificate password when you launch the VMware Enterprise Systems Connector installer in the next step.

Your password must contain at least 6 characters.

Certificate Password * Show Characters

Confirm Password * Show Characters

[Download VMESC-Installer.exe](#)

> Run the VMware Enterprise Systems Connector installer

> Test the Connection to the VMware Enterprise Systems Connector

[Continue to ActiveDirectory Setup](#)

Set Up Active Directory

The AirWatch 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, AirWatch 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](#).

Setup
Exit

✔ Apple
✔ VMware Enterprise Systems Connector
3 Active Directory
4 VPP

Directory Setup

Use the forms below to give AirWatch access to your Active Directory, then begin importing users.

∨ **Connect Your Directory**

Directory Type *	Active Directory (i)
Server *	<input style="width: 90%;" type="text"/> (i)
Encryption Type *	None (i)
Port *	389 (i)
Protocol Version *	3 (i)
Binding Information	
Bind Authentication Type *	GSS-NEGOTIATE (i)
Bind Username *	1005AWEX (i)
Bind Password * Show Characters (i)
Domain	<input style="width: 90%;" type="text"/> (i)

Save

> Test Active Directory Connection

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.

Setup
Exit

 Apple
 VMware Enterprise Systems Connector
 Active Directory
 **4** VPP

Volume Purchase Program (VPP) Setup

Follow the steps below to connect your VPP account and begin adding apps to your environment.

v [Download the VPP Token](#)

Do you already have a VPP account?

Yes
 No

[Continue](#)

Upload your VPP Token

Sync your Apps

[Continue](#)

For more information, see [Add Applications to a Blueprint](#).

Devices & Users / Apple / VPP Managed Distribution

Use Apple's Managed Distribution system integrated with Workspace ONE UEM to distribute your free and purchased Volume Purchase Program (VPP) applications and books to Apple iOS 7+ devices. The managed distribution model uses service tokens (also called sTokens) to retrieve your VPP contents and distribute them to devices using the UEM console.

Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > VPP Managed Distribution**.

Setting	Description
Description	Enter your VPP Account ID. Using your VPP Account ID as the description has several advantages: <ul style="list-style-type: none"> ■ Identifies the correct account if you use multiple sTokens. ■ Reminds you the correct account when you renew the sToken. ■ Identifies the correct account to others in your organization who take over managing the VPP account.
SToken Upload	Select Upload to navigate to the sToken on your network.
Country	Select where Workspace ONE UEM should validate the sToken. This value reflects the region from where you bought content and ensures Workspace ONE UEM uploads the correct versions of your purchases. When you sync your licenses, Workspace ONE UEM pulls the correct regional version of the content. If Workspace ONE UEM cannot find the content in the app store from the region entered, Workspace ONE UEM automatically searches the iTunes App Store in the United States.

Setting	Description
Automatically Send Invites	<p>Send invitations to all the users immediately after you save the token. This is an invitation to join and register with Apple's VPP, so that users access the terms of use for participating in the program.</p> <p>Use the Message Preview option to review the invitation.</p> <hr/> <p>Note If your environment includes VPP applications set to the Assignment Type, Auto, then Workspace ONE UEM sends invitations no matter how you configure this option. This behavior facilitates quick access to applications upon enrollment.</p> <hr/> <p>Workspace ONE UEM automatically sends users of Apple iOS 7.0.3+ an invite command when you enable this option. It does not send them an email message.</p> <p>You do not have to enable this immediately. You can leave it disabled and still upload your token. Return and enable this feature to send invitations to all the enrolled devices whose users have not yet accepted to join the VPP.</p>
Message Template	<p>Select an email template for an email message invitation for Apple iOS devices on Apple iOS 7.0.0 through 7.0.2.</p>

Blueprints

Blueprints ensure that 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.

This chapter includes the following topics:

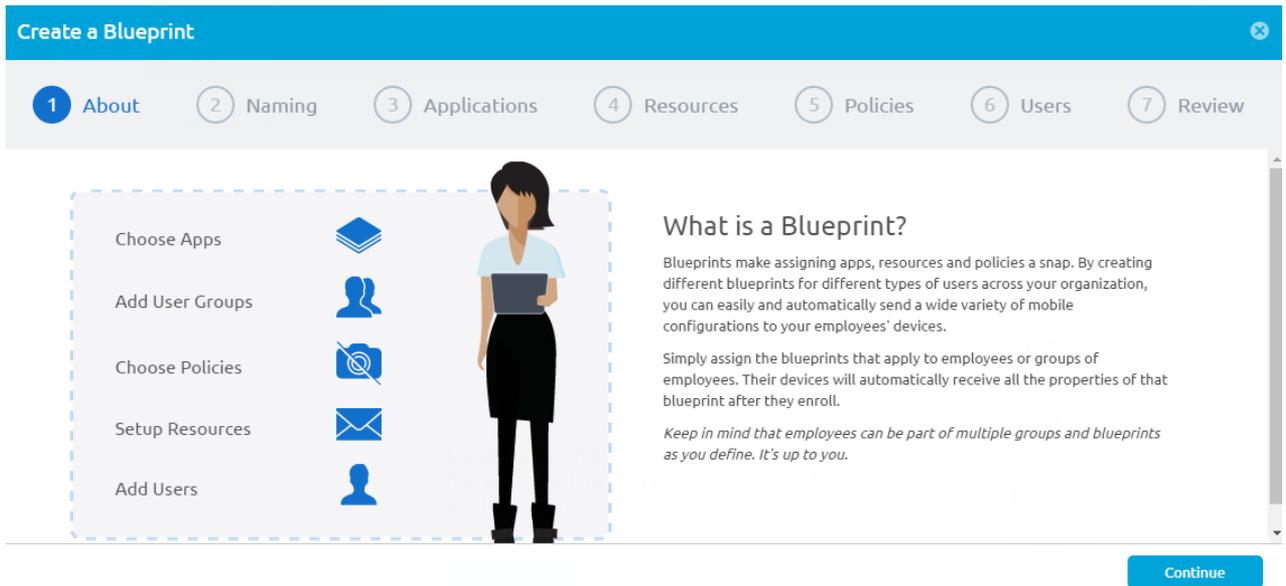
- [Create a Blueprint](#)
- [Name the Blueprint](#)
- [Add Applications to a Blueprint](#)
- [Add Resources to a Blueprint](#)
- [Adding Policies to a Blueprint](#)
- [Adding Users and User Groups to a Blueprint](#)

Create a Blueprint

You can create 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.

Procedure

- 1 From the main menu, navigate to **Blueprints > List View** and select **Add Blueprint**.



- 2 Select **Continue** to begin the blueprint creation process.
- 3 [Name the Blueprint](#).

Name the Blueprint

The first step in creating a blueprint is determining what it is called and whether the blueprint applies to everyone by default.

Setting	Description
Name	This required step is how the blueprint appears in the listing.
Include All Users In Blueprint	This optional setting ensures that all current and future users in your environment receive this "Global Blueprint" containing settings that all users need by default. You cannot manually remove users from Global Blueprints. If it comes down to removing individual users from the Global Blueprint, consider instead altering the content of the blueprint to make it truly global.

Add Applications to a Blueprint

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

This step is optional and you can skip ahead by selecting **Continue to Resources**. You can also **Save & Exit** at any time.

Procedure

- 1 Select **Add App**.

2 Select the Type of App to add: **Public App**, **Purchased App**, or **Web App**.

■ **Public App**

Add an app available in any of the major app stores to your blueprint. Choose among **Android**, **Apple**, **Windows Phone**, and **Windows Desktop**.

■ **Purchased App**

Add an app to a blueprint that has been purchased with the Volume Purchasing Program (VPP) by Apple. Requires VPP configuration during [Chapter 2 Express Setup](#) or [Devices & Users / Apple / VPP Managed Distribution](#).

You can search for a purchased app by name or keyword. VPP information includes a license count information.

■ **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. Optionally, you can **Upload Icon** representing the Web app. When adding an application using a Google Play Store URL, additional information such as name and application icons cannot be retrieved.

3 Select the country in which the app is used.

This selection determines where AirWatch searches for the app.

4 Search the applicable app stores (Google, Apple, and Windows) for the apps you want to add. Once you have located and selected 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.

5 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.

Workspace ONE UEM and Valid Google Play Store URLs

When you add an Android public application, you can enter the Google Play Store URL. You can also add a URL that you know to be valid but that is not from the Google Play Store. This method is useful to deploy applications when Workspace ONE UEM cannot validate URLs with the Google Play Store.

The AirWatch Catalog uses the entered URL as a link so end users can access the application. The system can manage these applications depending on where your source the URL.

- Valid Google Play Store URL – The Workspace ONE UEM system can manage these applications but it cannot retrieve the application icons.
- Valid URLs From Other Sources – The Workspace ONE UEM system cannot manage these applications and it cannot return the application in its results because it cannot validate the URL with the store.

Add Resources to a Blueprint

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

Procedure

- 1 Complete the **Configure Email** settings.

Setting	Description
Mail Client	Choose the email client your users run on their devices. The default selection is Native for all platforms.
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	Choose to use 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.
Password	Enter the login password. Select Show Characters check box to replace the redacted password and view the password as entered.

- 2 Complete the **Configure Wi-Fi** settings.

Setting	Description
Service Set Identifier (SSID)	Enter a unique identifier for the wireless access point.
Hidden Network	Choose whether or not you want the network access point to be visible in the Wi-Fi listing.

Setting	Description
Auto-Join	Choose whether or not you want authenticated devices to be automatically joined upon return to the Wi-Fi hot spot.
Security Type	Choose the type of wireless network encryption: None , WEP , 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.

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

Adding Policies to a Blueprint

Blueprints can contain Device Feature, Application, and Data Loss Prevention policies, which determine which permissions are available.

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 Enterprise Wipe.**
- **Allow use of Google/iCloud Backup.**

Application Policies

- **Allow access to the App store.**
- **Allow use of YouTube** – Allow access to YouTube. For Apple devices, applicable only to iOS 5.0 and earlier.
- **Allow use of GameCenter** – Allow 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 apps.**
- **Allow SD card.**

- **Allow unmanaged use of managed documents** – 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 Policies to a Blueprint

Once you have added resources to the blueprint, you can define how the device is used while being managed. This definition can include a passcode requirement, length, and complexity of the passcode, camera use, native browser use, copy/paste capability, and many other options. This step is optional.

Procedure

- 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 chart that is included on the **Edit Policies** page in AirWatch Express and the [Android Policy Support](#).
- 2 After completing each of the sections detailed below, select **Continue** to proceed to the next step, adding users and user groups.
- 3 Insert check marks to enable each applicable policy setting.

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

Android Policy Support

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

Table 3-1. Android OEM Support

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

Table 3-1. Android OEM Support (Continued)

	Standard	SAFE	LG	Lenovo	HTC	Moto MX	Pana- sonic	Amazon	Nook	Sony	Intel	ASUS	Blue- bird
Device Functionality													
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+			
Encryption													
Require Storage Encryption	v3.0+	v2.0+	v1.0+	v1.0+	v1.0+	MX v1.3+							
Sync and Storage													
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+		
Applications													
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 Apps		v2.0+	v1.0+	v1.0+	v2.0+	MX v1.3+		v1.0+		v5.0			v1.0
Bluetooth													
Allow Bluetooth		v2.0+	v1.0+	v1.0+	v2.0+	MX v1.3+		v1.0+		v2.0+			v1.0
Browser													
Allow Native Android Browser		v2.0+	v1.0+							v2.0+			

Adding Users and User Groups to a Blueprint

Once you have added policies to the 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 apps, resources, and policies from the blueprint.

Add Existing Users to a Blueprint

Add existing users to a blueprint using the search bar.

Procedure

- 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 new users to a blueprint as Basic users or Directory users.

Procedure

- 1 Select **Add User**.

You must [Basic and Directory Accounts](#).

- a For Basic users, complete the user information.

Setting	Description
Security Type	Choose Basic to add a basic user.
Email Address	Enter or edit the user's email address.
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.
First Name	Enter the first name of the user.
Middle Name	Optional. Enter the middle name of the user.
Last Name	Enter the last name of the user.

- b For Directory users, complete the user information.

Setting	Description
Security Type	Add an active directory user by choosing Directory from the drop-down menu.
Directory Name	This pre-populated setting identifies the Active Directory name.
Domain	Choose the domain name from the drop-down menu.
User Name	Enter the directory user name and select Find User . If the system finds a match, the user information is populated automatically in the Name and Email settings.

- 2 Once all the settings have been completed, 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.

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

Add Group to a Blueprint

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

Procedure

- 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.

Enrollment

Even if users are added to a blueprint and the blueprint is published, those users must complete the enrollment process first before their devices are managed. The enrollment process may differ slightly depending on the device platform (iOS, Android, Windows Phone).

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

This chapter includes the following topics:

- [Enroll a Device with Workspace ONE Intelligent Hub](#)
- [Integrate Device Enrollment Program](#)
- [Complete the DEP Enrollment Profile](#)

Enroll a Device with Workspace ONE Intelligent Hub

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

Procedure

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

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

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

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

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

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

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

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

Integrate Device Enrollment Program

Integrating AirWatch Express with Apple Device Enrollment Program (DEP) requires completing tasks in both the AirWatch 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, AirWatch suggests that you do not use Internet Explorer as your browser. Also, once you begin configuring the DEP wizard in the AirWatch 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 AirWatch Express Console to begin integrating with DEP.
- 2 Move between the DEP portal to create a virtual MDM server container for devices and the AirWatch 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 AirWatch Express.

Complete the DEP Enrollment Profile

After you register devices with Apple Business Manager portal, use the DEP Enrollment Program wizard to create a DEP enrollment profile. An enrollment profile is a collection of DEP settings assigned to your registered devices. You can create more profiles later if needed.

Create a new DEP enrollment profile or edit an existing profile.

- 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 and higher. If devices running iOS 7.0 and lower 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 may 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.
Message Template	Choose 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 to 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.
Supervision	Enable 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 this option to use shared devices with education functionality.
Lock MDM Profile	Select Enable to 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 may only be enabled if Supervision is enabled.
Anchor Certificate	Enable this option to upload certificates as trusted anchor certificate and push to devices during 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 will be used.
Device pairing	Enable 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 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 to 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 automatically apply DEP configuration 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 Choose the items seen by end users during the Apple **Setup Assistant** workflow that appears after the device is powered on for the first time.

Setting	Description
Passcode	Select Don't Skip to require 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 to prompt user to configure Touch ID during setup.
Location Services	Select Don't Skip to 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 to prompt user to restore from 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 to prompt user to sign in with an Apple ID and iCloud account during setup.
Terms of Use and Conditions	Select Don't Skip to prompt users to read and accept the Terms of Use and Conditions during setup.
Siri	Select Don't Skip to prompt user to configure Siri. If you select Skip , Siri is disabled on enrolled devices.
Diagnostics	Select Don't Skip to prompt 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 to prompt user to register the device with Apple during setup.
Apple Pay	Select Don't Skip to prompt 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 to prompt user to enable zoom functionality during setup.
FileVault 2	Select Don't Skip to prompt user to set up a FileVault account.
Display Tone	Select Skip to allow users to skip the display tone setup step for enrolling iOS devices.
Home Button Sensitivity	Select Skip to allow users to enroll devices without configuring the Home button sensitivity on enrolling iOS devices.
Tap to Setup	Select Skip to allow enrolling tvOS devices to enroll without an associated iOS device.
Screen Saver	Select Skip to allow users to enroll a tvOS device without configuring a screen saver.
Keyboard	Select Skip to omit the prompt for users to select a keyboard type during the Setup Assistant process.
Onboarding	Select Skip to prevent users from viewing on-boarding informational screens for user education during the Setup Assistant process.
Watch Migration	Set to Skip to prevent users from viewing options for watch migration during the Setup Assistant process.
iCloud Analytics	Set to Skip to omit a user prompt to send analytics to iCloud during setup.
iCloud Documents and Desktop	Set to Skip to prevent users from viewing iCloud Documents and Desktop screen in macOS.
TV Home Screen Sync	Set to Skip to prevent users from toggling the TV home screen layout during setup.
TV Provider Sign In	Set to Skip to prevent users from signing in to a TV provider during setup.

Setting	Description
Where is the TV?	Set to Skip to omit the Where is this Apple TV screen on tvOS devices enrolling through DEP.
Privacy	Set to Skip to omit the Privacy screen in DEP setup assistant while onboarding.
iMessage And FaceTime	Set to Skip to prevent the iMessage and FaceTime prompt during setup.
Software Update	Set to Skip to prevent informing users about Software Updates during setup.
Screen Time	Set to Skip to prevent informing users about Screen Time during setup.

- 6 For certain configurations detailed in the **Setup Assistant** configuration, use the **Admin Account Creation** section to create an admin account for local and remote macOS device admin actions.

Setting	Description
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.
Account Type	This item appears only if Account Setup is set to Don't Skip . Select Standard to 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 to allow users to create an Administrator account on their macOS device.
Password	Create a password for the admin account.
Hidden	Select Enabled to hide the admin account on the macOS device. Hidden admin accounts can enhance security and user experience. Select Disabled to make the admin account visible when a user logs in.
Choose Your Look	Set to Skip to the prompt for users to choose between Light and Dark mode on macOS Mojave 10.14.
Display Tone	Set to Skip to prevent the Display Tone screen during Setup Assistant.

- 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 to 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 to 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 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.

Admin View

Once the Express Setup, device enrollment, and blueprint creation processes are complete, the 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.

This chapter includes the following topics:

- [Admin Console at a Glance](#)
- [Blueprints](#)
- [Devices Dashboard](#)
- [User and Admin Accounts](#)

Admin Console at a Glance

Before you begin managing devices with AirWatch 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

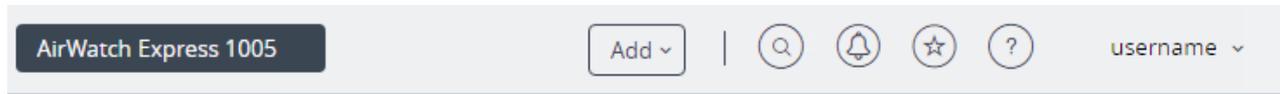
Collapse or close the secondary menu, which creates more space on the screen for device information,

by selecting the bottom-left arrow . To expand or reopen the secondary menu, select the modified

right arrow .

Header Menu

The **Header Menu** appears at the top of nearly every page of the Admin Console. The header menu enables you to view summary panels, run searches, and get online help.



- **Organization Group** – Displays the Organization Group (the tab labeled AirWatch Express 1005 in the screenshot) under which your device fleet is managed.
- **Add** – Get quick access to adding an admin, device, or user.
- **Global Search** – () Search for devices, users, and administrators using the global search bar.
- **Notifications** – () Stay informed about expired APNs certificates with [Admin Console Notifications](#). The number badge on the Notifications icon indicates the number of alerts requiring your attention.
- **Saved** – () Access your favorite and most-utilized pages within the Admin Console.
- **Help** – () Browse or search the available guides and feature documentation.
- **Account** – View your account information. Change the **Account Role** that you are assigned to within the current environment. Customize settings for contact information, language, [Admin Console Notifications](#), view history of **Logins**, and **Security** settings including PIN reset. You can also **Log out** of the AirWatch Console and return to the Login screen.
- **Refresh** – () Resend a query to the console and retrieve an up-to-date listing of devices and other data. Such a refresh can be useful in high-volume, high-activity environments.
- **Home** – () Use this icon to assign any screen in the AirWatch Console as your home page. The next time you open the Admin Console, your selected screen displays as your home page.
- **Save** – () Save the current page or view for quick access from your list of Saved pages.

Admin Console Notifications

The Notifications button is located next to the Global Search bar. Notifications appear when APNs for MDM certificates expire within 30 days.

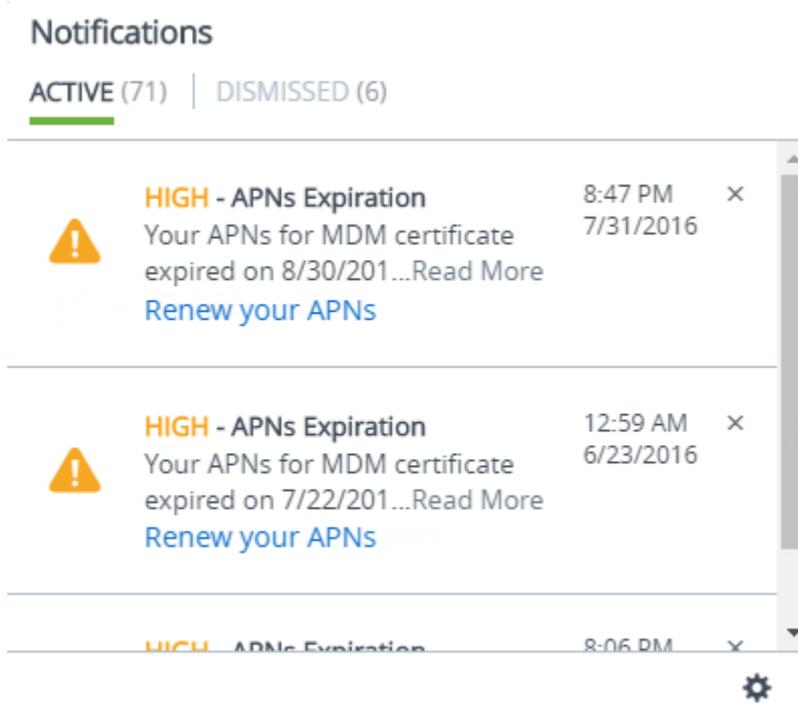
Notifications help you avoid the hassles involved with expired certificates and keep your devices in touch with the AirWatch Express Admin Console.



- **APNs Expiration and APNs Expired** – You are notified 30 days before APNs for MDM certificates expire. APNs alerts are Critical Priority alerts. After the APNs certificate expires, the Critical Priority alert is reduced to a High Priority alert.

Manage Console Notifications

When there are active notifications that require your attention, a numeral badge appears on the alert icon indicating the number of active alerts. Selecting the Notifications icon displays the **Notifications** pop-up screen.



You can manage the notifications you receive including view the list of active alerts. You can also renew your APNs, dismiss expired alerts, view the list of dismissed alerts, and [Configure Notifications Settings](#).

Each alert displays the organization group under which the APNs certificate is located, the certificate expiration date, and a link to Renew your APNs.

- **View Active Alerts** – The default view displays the list of active alerts.
- **Renew your APNs** – Selecting the link displays the **APNs For MDM** settings page. Renew the license by following the on-screen instructions.

- **Dismiss Alert** – Close the expired alert and send it to the Dismissed alert listing by selecting the **X** button. You cannot close critical priority notifications.
- **Dismiss All** – Close all active alerts and send them to the Dismissed alert listing.
- **View Dismissed Alerts** – Select the **Dismissed** tab at the top of the Notifications pop-up to view the listing of dismissed alerts.

Configure Notifications Settings

You can use the Notifications settings page to enable or disable APNs Expiration alerts. You can also choose whether to receive console alerts, email alerts, or both, and change the email address to which it sends alerts.

Procedure

- 1 Select the **Account** button, which is accessible from almost every page on the AirWatch Express Console, then select **Manage Account Settings** and click the **Notifications** tab.

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

- 2 Complete the notification settings.

Setting	Description
APNs Expiration	Trigger alerts when APNs licenses expire or are in jeopardy of expiring.
Notification	Select the notification delivery method. Choose from Console , Email , or Both .
Send email to	Enter the email address for when Email or Both is selected in Notification .

- 3 **Save** or **Cancel** your changes.

Main Menu

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

Monitor	View and manage MDM information that drives decisions you must make and access a quick overview of your device fleet.
Blueprints	Manage the applications, resources, and policies that you have created and assigned to users, user groups, and their devices with the Blueprints List View. Perform edits to any individual blueprint element, add a blueprint, and delete unused blueprints.
Devices	Access a dashboard overview of common aspects of devices in your fleet. Display and customize the view of an entire list of all devices in your deployment and filter them by platform, ownership type, OS version, and more.
Accounts	Survey and manage users and administrators involved with your MDM deployment. Access and manage user groups, roles, enrollment status, and settings associated with your users.
Groups & Settings	Configure system settings for the VMware Enterprise Systems Connector and Directory Services. Request and renew Apple Push Notification Service certificates.

Monitor

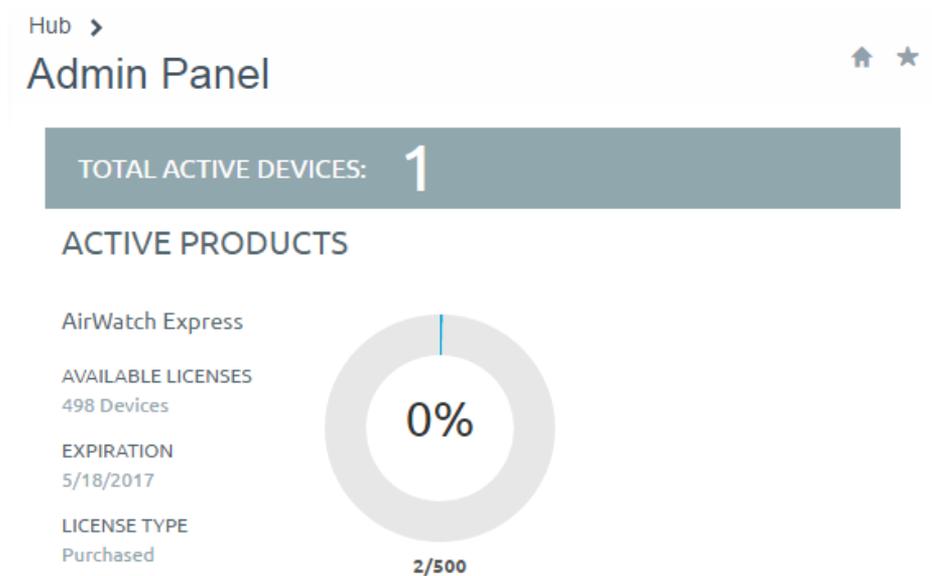
The VMware AirWatch Express Monitor is your central portal for fast access to critical information. Select any metric to open the **List View** for that specific set of devices.

It is from this screen where you can perform actions such as sending a message to a device.

Admin Panel Dashboard

Access an at-a-glance overview of AirWatch Express license information.

Navigate to **Monitor > Admin Panel**.



Exporting Reports

You can save a downloadable comma-separated values (CSV) file of the exported list views from two locations in AirWatch Express.

- Enrollment Status List View.
- Device List View.

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

You can view and download the comma-separated values (CSV) file for viewing with Excel by navigating to **Monitor > Reports & Analytics > Exports**.

Blueprints

Once you have created a library of blueprints, 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**.

Managing Blueprints

You can manage blueprints including renaming, deleting, and editing the configuration of 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 AirWatch 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.

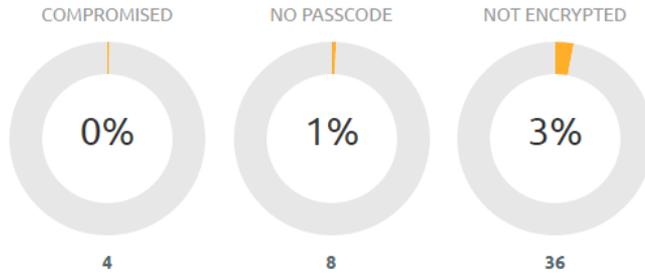
Devices >

Dashboard

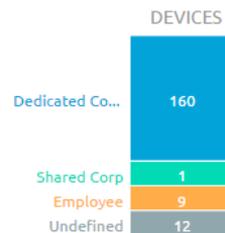


TOTAL DEPLOYMENT: 182

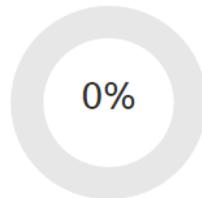
SECURITY ⓘ



OWNERSHIP



LAST SEEN OVERVIEW



LAST SEEN BREAKDOWN



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 AirWatch 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 displays a filtered **Device List** view comprised of devices under the selected platform.
- **Enrollment** – View the total number of devices in each enrollment category. Selecting any of the 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 Apple iOS, Android, Windows Phone, and Windows Rugged. Display a filtered **Device List** view comprised of devices running the selected OS version by selecting any bar graph.

Device List View

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

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

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

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

Customize Device List View Layout

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

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

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

Search in Device List View

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

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

Add a Device from List View

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

Procedure

- 1 Navigate to **Devices > List View** or **Devices > Lifecycle > Enrollment Status**.
- 2 Select the **Add Device** button. The **Add Device** page displays. Complete the following in the **User** tab.

Setting	Description
User	
Search Text	Each device must be assigned to a user. Search for a user with this text box by entering search parameters and select the Search User button. You can select a user from among the search results or select the link Create New User .
Create New User	
Security Type	Select between Basic and Directory users.
User name	Enter the user name by which your user is identified in your Workspace ONE UEM environment.
Password, Confirm Password	Enter and confirm the password that corresponds to the user name.
Email Address	Enter the email address for the user account.
Enrollment Organization Group	The organization group (OG) that serves as the enrollment OG for the device enrollment.
Show advanced user details	Display all the advanced user details, including comprehensive information covering user name, user phone number, and manager name. Also included are optional identification settings such as department, employee ID, and cost center. Select the default User Role for the user you are adding which determines which permissions the user has while using a connected device.
Device	
Expected Friendly Name	Enter the name of the device that appears in the device list view. You can also incorporate 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.

Setting	Description
Show advanced device information options	Display all the advanced device information settings.
Advanced Device Information Settings	
Model	Select the device model from the drop-down listing. The contents of this drop-down menu depend upon the selection made in the Platform drop-down menu.
OS	Select the device's operating system from the drop-down listing. The contents of this drop-down menu depend upon the selection made in the Platform drop-down menu.
UDID	Enter the device's Unique Device Identifier.
Serial Number	Enter the device's serial number.
IMEI	Enter the device's 15-digit International Mobile Station Equipment Identity.
SIM	Enter the device's SIM card specifications.
Asset Number	Enter the asset number for the device. This number is created internally from within your organization and this setting is provided to hold this data point.
Messaging	
Message Type	Select the type of message you want to send (None or Email) to the device upon a successful enrollment to the Workspace ONE UEM environment.
Email Address	Enter the email address to which you want the enrollment message sent. This text box is only available when Email is selected as the Message Type .
Email Message Template	Select the email template from the drop-down menu. There is a link you can use to open the Message Template page where you can create an email message template.

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

Device Details

The Device Details page 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.
- **Device Info** – 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 apps, both automatic apps and on-demand apps.

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 found on the Device Details dashboard enables you to perform common device actions such as Send [Message], Lock, and More Actions.

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

Enrollment Status

Use the **Enrollment Status** page to assess enrollment status on a per-device basis and revoke/reset device tokens.

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

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

Setting	Description
Filters	You can filter out entire device categories by using filters which enable you to see only those devices that you are interested in. <ul style="list-style-type: none"> ▪ Enrollment Status ▪ Platform ▪ Ownership ▪ Token Status ▪ Token Type ▪ Source ▪ First Seen
Resend Message	Resend the original message sent to a user, including Self-Service Portal URL, Group ID, and login credentials.

Setting	Description
More Actions	
Change Organization Group	Pre-populated setting reflects the existing organization group.
Change Ownership	Change the type of ownership for the selected device.
Delete	Permanently delete the registration information for selected devices. This action forces the user to re-register to enroll. Where applicable, you must first revoke the token before deleting a device registration.
Reset Token	Reset the status of a token if it has been revoked or is expired.
Revoke Token	Force the registration token status of selected devices to expire, essentially blocking access for unwanted users or devices. For the Reset Token and Revoke Token actions, you can select to disable the Notify Users setting which prevents the default email notification from being sent.
Selecting Multiple Devices	Act on individual devices or multiple devices by selecting the check box next to each device and using the action buttons. Once you have applied a filter to show a specific set of devices, you can perform bulk actions to multiple selected devices. Perform this action by selecting the devices and selecting an action from the Resend Message and More Actions buttons. You can select individual check boxes. You can also select the entire set of filtered devices by selecting the global check box located atop the check box column. When you select an action for one or more devices, a confirmation screen displays allowing you to Save or Cancel the action.
Layout	Display the full listing of visible columns or choose to display or hide columns per your preferences by selecting the Custom option. There is also an option to apply your customized column view to all administrators. 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.
- **Message** – View the outgoing Device Activation email message including credential information and QR code. There is a resource available, called "User Registration Message," that allows the Workspace ONE UEM administrator to hide the **Message** tab after the device has successfully enrolled.

- **Offline Enrollment** – If available, this tab allows you to enroll the device while it is offline. This feature is useful for when you want to make the most of scheduled time for a device in an unavailable state (for example, while traveling).

Add a Blacklisted or Whitelisted Device

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

Procedure

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

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

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

Batch Import Users or Devices

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

Procedure

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

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

- **Whitelisted Devices**

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

- **User and/or Device**

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

- **Change Organization Group**

Move users to a different organization group.

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

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

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

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

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

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

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

User and Admin Accounts

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

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

Basic and Directory Accounts

The type of authentication you choose 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 AirWatch 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 AirWatch Express and do not necessarily match existing corporate credentials.
- Basic user names and passwords are stored in AirWatch Express.

Directory User Accounts

Active Directory (AD)/Lightweight Directory Access Protocol (LDAP) authentication is used to integrate user and admin accounts of AirWatch 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 AirWatch Console. If your authentication type is Basic, then consider creating Basic User Accounts.

Procedure

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

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

Setting	Description
Security Type	Select Basic to add a basic user.
User name	Enter a user name with which the new user is identified.
Password	Enter a password that the user can use to log in.
Confirm Password	Confirm the password.
Full Name	Complete the First Name , Middle Name , and Last Name of the user.
Display Name	Represent the user in the UEM console by entering a name.
Email Address	Enter or edit the user's email address.
Email user name	Enter or edit the user's email user name.
Domain	Select the email domain from the drop-down setting.
Phone Number	Enter the user's phone number including plus sign, country code, and area code.
Enrollment Organization Group	Pre-populated setting reflects the existing organization group.
Allow the user to enroll into additional Organization Groups	<p>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.</p> <p>Workspace ONE UEM Express customers have a single organization group to enroll into. Contact Support to inquire about upgrading to benefit from having multiple organization groups.</p>
Additional Organization Groups	<p>This setting only appears when the option to allow the user to enroll into additional OGs is Enabled.</p> <p>This setting allows you to add additional organization groups from which your basic user can enroll.</p>
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	<p>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.</p> <p>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.</p>

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.

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

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

Create Directory User Account

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

Procedure

- 1 Navigate to **Accounts > Users > List View** and select **Add** and then **Add User**.

The **Add / Edit User** page displays.

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

Setting	Description
Security Type	Add an Active Directory user by choosing Directory as the Security Type.
Directory Name	This pre-populated setting identifies the Active Directory name.
Domain	Choose the domain name from the drop-down menu.
User name	Enter the user's directory user name and select Check User . If the system finds a match, the user's information is automatically populated. The remaining settings in this section are only available after you have successfully located an active directory user with the Check User button.
Full Name	Use Edit Attributes to allow any option that syncs a blank value from the directory to be edited. Edit Attributes also enables you to populate matching user's information automatically. If a setting syncs an actual value from the directory, then that setting must be edited in the directory itself. The change takes effect on the next directory sync. Complete any blank option returned from the directory in Full Name and select Edit Attributes to save the addition.
Display Name	Enter the name that displays in the admin console.

Setting	Description
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 AirWatch Express customers, this setting is pre-populated and reflects the existing organization group.
Allow the user to enroll into additional Organization Groups	AirWatch 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	Choose the type of message you may send to the user, Email or None .
Message Template	Choose 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 UEM, this text box is pre-populated with the distinguished name of the user. Distinguished Name is a string representing the user name and all authorization codes associated with an Active Directory user.
Manager Distinguished Name	Enter the distinguished name of the user's manager. This text box is optional.
Category	Choose the user category for the user being added.
Department	Enter the user's department for your company's administrative purposes.
Employee ID	Enter the user's employee ID for your company's administrative purposes.
Cost Center	Enter the user's cost center for your company's administrative purposes.
Enable Device Staging	Enable or disable the staging of devices. If enabled, you must choose between Single User Devices and Multi User Devices . If Single User Devices , you must select between Standard , where users themselves log in and Advanced , where a device is enrolled on behalf of another user.

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

User Accounts List View

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

The screenshot displays the 'List View' page for user accounts. The interface includes a navigation breadcrumb 'Accounts > Users', a title 'List View', and a search bar. A 'Filters' sidebar on the left allows filtering by Security Type, Enrollment Organization Group, Enrollment Status, User Group, and User Role. The main table lists users with columns for General Info, Status, Enrollment Organization Group, Devices, User Groups, and Contact Info. The table shows 9 users, all with an 'Active' status. A pagination bar at the bottom indicates 'Items 1 - 50 of 172265' and a 'Page Size' of 50.

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

Customize List View

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

Action	Description
Filters	View only the desired users by using the following filters. <ul style="list-style-type: none"> ■ Security Type ■ Enrollment Organization Group ■ Enrollment Status ■ User Group ■ User Role
Add	<ul style="list-style-type: none"> ■ 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™ UEM by importing a comma-separated values (CSV) file. Enter a unique name and description to group and organize multiple users at a time. For more information, see Batch Import Users or Devices.
Layout	Enables you to customize the column layout. <ul style="list-style-type: none"> ■ 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 a comma-separated values (CSV) file of the entire List View that can be viewed and analyzed in Excel.

Interact with User Accounts

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

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

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

Action	Description
Send Message.	Provide immediate support to a single user or group of users. Send a User Activation (user template) email to a user notifying them of their enrollment credentials.
Add Device.	Add a device for the selected user. Only available for single user selections.
More Actions	Display the following options.
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 terminates employment, you can quickly and completely delete a user account. Deleting account information is the equivalent of the account never having existed in the first place. A deleted account cannot be reactivated. If a deleted account owner returns, a new account must be created for them.

Action	Description
Activate	Activate a previously deactivated account if a user returns to an organization or must be reinstated in the company.
Deactivate	<p>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.</p> <p>A deactivated account simply means no one with these account credentials will be able to log in to Workspace ONE UEM console while the account is deactivated. Once the security issue is resolved (user is located, device becomes compliant, the device is recovered) then you can Activate the account.</p>

Batch Import Users or Devices

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

Procedure

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

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

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

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

Move users to a different organization group.

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

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

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

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

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

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

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

User Groups List View

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

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

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

Action	Description
Filters	Display only the desired user groups by using the following filters. <ul style="list-style-type: none"> ■ User Group Type. ■ Sync Status. ■ Merge Status.
Add	
Add User Group.	Perform a one-off addition of.
Sorting and Resizing Columns	Columns in the List View that are sortable are Group Name, Last Sync On, Users, and Merge Status. Columns that can be resized are Group Name and Last Sync On.
Details View	View basic user group information in the Details View by selecting the link in the Group Name column. This information includes group name, group type, external type, manager, and number of users. .
Export 	Save a comma-separated values (CSV) file of the entire unfiltered or filtered List View that can be viewed and analyzed in Excel.

The **User Groups List View** also features a selection check box and **Edit** icon to the left of the user.

Selecting the **Edit** icon () enables you to make basic changes to the user group. You can make bulk actions on user groups by selecting one or more groups which reveals the action buttons for the listing.

More Actions for User Groups

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

Action	Description
Sync	Copy recently added user group users to the temporary table, manually, ahead of the scheduled, automated Active Directory sync by Workspace ONE UEM.
View Users	Displays the User Group Members screen, enabling you to review the user names of all the members in the selected user group.
More Actions	
View and Merge	View, Add, and Remove users recently added to the temporary user group table. User group users that appear in this table await the automated Workspace ONE UEM user group sync.
Add Missing Users	Combine the temporary user group table with the Active Directory table, making the addition of these new users in the user group official.
Delete	Delete a user group.

Admin Accounts

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

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

Create an Admin Account

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

Create a Temporary Admin Account

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

Add, Edit, and Delete Admin Accounts

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

Create an Admin Account

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

Procedure

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

Create a Temporary Admin Account

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

Procedure

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

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

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

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

- 3 In the **Roles** tab, you can add, edit, and delete roles applicable to the temporary admin account.
- Add a role by selecting the **Add Role** button and then select the organization group and role for which the temporary admin account applies.
 - Edit an existing role by selecting the edit icon () and select a different role.
 - Delete a role by selecting the delete icon ().
- 4 Select **Save**.

Managing Admin Accounts

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

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

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

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

- **View History** – Track when admins log in and out of the Workspace ONE UEM console.
- **Deactivate** – Change the status of an admin account from active to inactive. This feature allows you to suspend the management functions and privileges temporarily. At the same time, this feature enables you to keep the defined roles of the admin account for later use.
- **Activate** – Change the status of an admin account from inactive to active.
- **Delete** – Remove the admin account from the UEM console. Such an action is useful for when an administrator ends employment.

- **Reset Password** – Available to basic administrators only. Sends an email to the basic admin's email address on record. The email contains a link that expires in 48 hours. To reset the password, the basic admin must select the link and answer the password recovery question. This enables the basic admin to change their own password.

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

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

Install VMware Enterprise Systems Connector

6

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

It runs from within your internal network and allows you to benefit from AirWatch Mobile Device Management (MDM). VMware Enterprise Systems 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 VMware Enterprise Systems Connector, refer to this section for information which has been designed for AirWatch Express. If you need further details about any specific VMware Enterprise Systems Connector element, consult the **VMware Enterprise Systems Connector Documentation** (available on docs.vmware.com) or contact Workspace ONE Support.

Prerequisites

Ensure that your system meets the necessary **Hardware Requirements** to deploy VMware Enterprise Systems 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 higher.
- 6-GB disk space for the VMware Enterprise Systems Connector application, Windows OS, .NET runtime, and AirWatch Express logging operations.

Ensure the server running AirWatch Express meets the necessary Software Requirements.

- Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.
- .NET Framework version 4.6.2.
 - The VMware Enterprise Systems Connector auto-update feature does not function correctly until your VMware Enterprise Systems Connector server is updated to .NET Framework 4.6.2.
 - The VMware Enterprise Systems Connector auto-update feature does not update the .NET Framework automatically.
 - Install .NET 4.6.2 manually on the VMware Enterprise Systems Connector server before performing an upgrade.

Ensure that the Network Requirements for the VMware Enterprise Systems Connector Server are met.

- **AirWatch 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, VMware Enterprise Systems Connector must query AirWatch 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.
 - VMware Enterprise Systems 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 VMware Enterprise Systems Connector From AirWatch Console.](#)
 - a Generate certificates and select the enterprise services and AirWatch services to be integrated.
- 2 [Install the VMware Enterprise Systems Connector.](#)
 - a Run the VMware Enterprise Systems Connector installer on your configured server that meets all the prerequisites.
- 3 [Verify a Successful VMware Enterprise Systems Connector Installation](#) from within the AirWatch Console.

This chapter includes the following topics:

- [Enable VMware Enterprise Systems Connector From AirWatch Console](#)
- [Install the VMware Enterprise Systems Connector](#)
- [Using VMware Enterprise Systems Connector Auto-Update](#)
- [Verify a Successful VMware Enterprise Systems Connector Installation](#)

Enable VMware Enterprise Systems Connector From AirWatch Console

Before you install VMware Enterprise Systems Connector, you must first enable it, generate certificates, and select the enterprise services and AirWatch services to be integrated. After completing this step, you can install VMware Enterprise Systems Connector.

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

Procedure

- 1 Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Enterprise Systems Connector**.
- 2 Configure the following settings on the **General** tab.

Setting	Description
Enable VMware Enterprise Systems Connector	Enable VMware Enterprise Systems Connector and display the General tab.
Enable Auto Update	Enable VMware Enterprise Systems Connector to update automatically when a newer version is available.

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

Setting	Description
Enterprise Services	<p>Enable or disable Enterprise Services. The services you select (enabled) integrate with VMware Enterprise Systems Connector.</p> <ul style="list-style-type: none"> ■ SMTP (Email Relay), AirWatch SaaS offers email delivery through its own SMTP. ■ Directory Services (LDAP/AD).
AirWatch Services	<p>Enable or disable AirWatch Services. The AirWatch components you select (enabled) integrate with VMware Enterprise Systems Connector. AirWatch suggests leaving all services enabled.</p> <ul style="list-style-type: none"> ■ 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** to keep all these settings.
- 5 Navigate back to the **General** tab and select **Download Cloud Connector Installer**.
- 6 A **Download VMware Enterprise Systems Connector Installer** screen displays. Enter a password for the VMware Enterprise Systems Connector certificate in the text box. The password is needed later when you run the VMware Enterprise Systems Connector installer.
- 7 Select **Download** and save the **VMware Enterprise Systems Connector x.x Installer.exe** file on the VMware Enterprise Systems Connector server.

Use this file later in [Install the VMware Enterprise Systems Connector](#).

Install the VMware Enterprise Systems Connector

The VMware Enterprise Systems Connector must be installed and running for AirWatch Express to manage your devices.

Procedure

- 1 Open the installer on the VMware Enterprise Systems Connector server.
- 2 When the **Welcome** screen appears, select **Next**.
The installer verifies prerequisites on your VMware Enterprise Systems Connector server.
- 3 Accept the license agreement, and then select **Next**.
- 4 Select **Change** and choose the installation directory. Select **Next**.
- 5 Enter the **Certificate Password** that you provided on the **System Settings** page in AirWatch. Select **Next**.
- 6 If you plan on proxying VMware Enterprise Systems Connector 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 VMware Enterprise Systems Connector.
- 8 Select **Finish**.

By default, the [Install the VMware Enterprise Systems Connector](#) check box is selected. It updates without any user intervention by querying AirWatch for newer versions of VMware Enterprise Systems Connector.

Using VMware Enterprise Systems Connector Auto-Update

Auto-update allows VMware Enterprise Systems Connector to upgrade automatically to the latest version.

While you are [Install the VMware Enterprise Systems Connector](#), by default, the auto-update check box is selected. It updates without any user intervention by querying AirWatch for newer versions of VMware Enterprise Systems 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

VMware Enterprise Systems Connector auto-update is performed using the **Bank1** and **Bank2** folders inside the **CloudConnector** folder. AirWatch detects which of these folders is empty and streams into it the appropriate VMware Enterprise Systems Connector files. Also, the update process empties the contents of the other folder. For the following update, AirWatch 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 VMware Enterprise Systems Connector auto-update process.



Auto-Update Security

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

While VMware Enterprise Systems 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 VMware Enterprise Systems Connector servers benefit from AirWatch 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 VMware Enterprise Systems Connector services are not down at the same time.

When the VMware Enterprise Systems 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 VMware Enterprise Systems Connector installer. The best way to verify if the auto-update succeeded is to look at the version number in the VMware Enterprise Systems Connector logs.

Verify a Successful VMware Enterprise Systems Connector Installation

After you install VMware Enterprise Systems Connector, you can verify a successful installation from within the AirWatch Express Console.

Procedure

- 1 Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Enterprise Systems 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 VMware Enterprise Systems Connector, you can use it to integrate with your directory service infrastructure. Proceed to the [Chapter 7 Introduction to Directory Services](#).

Introduction to Directory Services

7

AirWatch Express integrates with your organization's existing directory service – such as Active Directory, Lotus Domino, and Novell e-Directory – to provide directory-based account access. This integration lets users authenticate with AirWatch 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 AirWatch with your directory service provides many benefits.

- Conduct an easy enrollment for both users and administrators.
- Map directory groups to AirWatch user groups.
- Control AirWatch Console access.
- Apply existing credentials for VMware Content Locker 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 AirWatch environment with your directory service of choice. The sections also describe how to add directory user accounts to AirWatch and how to integrate user groups with AirWatch Express.

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

This chapter includes the following topics:

- [Directory Services Setup](#)
- [Set up Directory Services with a Wizard](#)
- [Set Up Directory Services Manually](#)

- [Directory Service User Integration](#)
- [Directory User Group Integration](#)

Directory Services Setup

Directory services setup requires you to integrate your AirWatch 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 AirWatch 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 AirWatch configured groups and directory service groups. You can also map attribute values between AirWatch user attributes and your directory attributes.

Note For Software as a Service (SaaS) customers, directory services integration requires you to install the [Chapter 6 Install VMware Enterprise Systems Connector](#).

Set up Directory Services with a Wizard

The AirWatch Console 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 AirWatch Console can detect it.

Procedure

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

> Advanced

Use Azure AD For Identity Services ENABLED DISABLED

Use SAML For Authentication ENABLED DISABLED

Child Permission Inherit Override Inherit or Override

- 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.

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

Procedure

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

Setting	Description
Directory Type	Select the type of directory service that your organization uses. Workspace ONE UEM 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 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: <ul style="list-style-type: none"> ▪ 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 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 . <ul style="list-style-type: none"> ▪ 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'.

Setting	Description
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.
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 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. If you are unsure of which Bind Authentication Type to use, try the commonly used GSS-NEGOTIATE. You will 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 may choose to 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 user group membership at the time of enrollment. As the system runs this feature at enrollment time, your performance may decrease with some directories.
Use Recursive OID For Group Sync	Verify user group membership at the time of Group synchronization.

Setting	Description
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 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 enables Workspace ONE UEM to match the Azure AD immutable ID to the correct local active directory attribute.
Mapping Attribute Data Type	Choose 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 executed. It is not a best practice to disable this functionality as it may reduce the security posture of your configuration. If a wiped device is lost, it may 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.
SAML 2.0	
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 checks authentication responses to verify that the identity matches the ID provided here.
REQUEST	
Request Binding Type	Select the binding types of the request. The options include Redirect , POST , and Artifact .
Identify Provider Single Sign On URL	Enter the identity provider's Uniform Resource Locator (URL) that Workspace ONE UEM uses to send requests.
NameID Format	Enter the format in which the identity provider sends a NameID for an authenticated user. This value is not required as Workspace ONE UEM obtains the user name from the FriendlyName "uid" required attribute.
Authentication Request Security	Select from the dropdown whether or not the Service Provider (Workspace ONE UEM) signs the authentication requests. You can select None , Sign Authentication Requests (SHA1) , and Sign Authentication Requests (SHA256) . Consider selecting Sign Authentication Requests (SHA256) for a more secure authentication.
RESPONSE	
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.
CERTIFICATE	
Identity Provider Certificate	Upload the identity provider certificate.

Setting	Description
Service Provider (AirWatch) Certificate	Upload the service provider certificate.
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** to configure the **User** settings.

Setting	Description
User Object Class	Enter the appropriate Object Class. In most cases, this value is "user."
User Search Filter	<p>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.</p> <ul style="list-style-type: none"> For AD servers, use <pre>(&(objectCategory=person)(sAMAccountName={EnrollmentUser}))</pre> For other LDAP servers, use <pre>(&(objectClass=inetOrgPerson)(uid={EnrollmentUser}))</pre> <p>This format, (&(...)), must be used even when only a single search parameter is specified in either AD servers or other LDAP servers.</p> <ul style="list-style-type: none"> For example, <pre>(&(uid={EnrollmentUser}))</pre>

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 Set Disabled Users to Inactive	<p>Select Enable to deactivate the associated user in Workspace ONE UEM when that user is disabled in your LDAP directory service (for example, Novell e-Directory).</p> <ul style="list-style-type: none"> 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). <p>When "Flag Bit Match" is selected, if any bits from the property match the entered numeric value, then directory service considers the user to be disabled. This setting is only visible when the option Automatically Set Disabled Users to Inactive is checked.</p> <p>Note If you select this option, then Workspace ONE UEM administrators set as inactive in your directory service are not able to log in to the Workspace ONE UEM console. In addition, enrolled devices assigned to users who are set as inactive in your directory service are automatically unenrolled.</p>

Setting	Description
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.

- 3 Navigate to **Accounts > Administrators > Administrator Settings > Directory Services > Group** to 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.
- 5 Select **Save**.

Directory Service User Integration

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

Integrating directory service users into AirWatch Express users is entirely optional. However, the benefits of applying the user data already stored within your directory service are of a high order.

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 AirWatch 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 AirWatch Express.

Map Directory Services User Information

After entering server settings, you can filter searches to identify users and map values between Workspace ONE UEM 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	<p>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.</p> <ul style="list-style-type: none"> For AD servers, use <pre>(&(objectCategory=person)(sAMAccountName={EnrollmentUser}))</pre> For other LDAP servers, use <pre>(&(objectClass=inetOrgPerson)(uid={EnrollmentUser}))</pre> <p>This format, (&(...)), must be used even when only a single search parameter is specified in either AD servers or other LDAP servers.</p> <ul style="list-style-type: none"> For example, <pre>(&(uid={EnrollmentUser}))</pre>

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 Set Disabled Users to Inactive	<p>Select Enable to deactivate the associated user in Workspace ONE UEM when that user is disabled in your LDAP directory service (for example, Novell e-Directory).</p> <ul style="list-style-type: none"> 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). <p>When "Flag Bit Match" is selected, if any bits from the property match the entered numeric value, then directory service considers the user to be disabled. This setting is only visible when the option Automatically Set Disabled Users to Inactive is checked.</p> <p>Note If you select this option, then Workspace ONE UEM administrators set as inactive in your directory service are not able to log in to the Workspace ONE UEM console. In addition, enrolled devices assigned to users who are set as inactive in your directory service are automatically unenrolled.</p>
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.

Directory User Group Integration

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

Once you import existing directory service user groups as AirWatch 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 AirWatch Express with the existing organizational systems.
- **Profiles and Policies** – Assign profiles, applications, and policies across an AirWatch 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 AirWatch Express using their existing credentials.

Similar to the way [Map Directory Services User Information](#), mapping user group data integrates your existing directory service groups into AirWatch Express user groups.

Configure Map Directory Services Group Settings

After entering server settings, you can filter searches to identify user groups. You can also set options to auto merge and sync changes between your Workspace ONE UEM groups and directory service groups.

Note No AD passwords are 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.

Note In some instances, global catalogs are used to manage multiple domains or AD Forests. Delays while searching for or authenticating users may 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. 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.

Procedure

- 1 Navigate to **Accounts > Administrators > Administrator Settings > Directory Services**.
- 2 Select the **Group** tab. By default, only the **Base DN** information displays.
- 3 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.
- 4 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.

- 5 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.

Setting	Description
Maximum Allowable Changes	<p>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.</p> <p>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.</p>
Conditional Group Sync	<p>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.</p>
Auto-Update Friendly Name	<p>When enabled, the friendly name is updated with group name changes made in active directory.</p> <p>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.</p>
Attribute	<p>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.</p>

Add Directory Service User Groups to AirWatch Express

User groups added in AirWatch 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 AirWatch user accounts. Therefore, if you have restricted enrollment for known users, you must add those user accounts into the AirWatch Express Admin 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	<p>Select the type of User Group.</p> <ul style="list-style-type: none"> ▪ 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	<p>Select the external type of group you are adding.</p> <ul style="list-style-type: none"> ▪ 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	<p>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.</p>
Directory Name	<p>Read-only setting displaying the address of your directory services server.</p>
Domain and Group Base DN	<p>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).</p> <p>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.</p>
Custom Object Class	<p>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.</p>
Group Name	<p>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.</p>
Distinguished Name	<p>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.</p>
Custom Base DN	<p>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.</p>
Organization Group Assignment	<p>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.</p>

Setting	Description
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. For more information, see the VMware AirWatch Mobile Device Management Guide . This option is available only when Auto Merge Changes is enabled.
Add Group Members Automatically	Enable this setting to add users to the user group automatically. If you want to prevent user groups from automatically syncing during a scheduled sync, this setting must be disabled.

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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>

- 3 Select **Save**.

Remove Users From User Groups Based on Directory Service Group Membership

You can enable Workspace ONE UEM 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 **Show Advanced** hyperlink.
- 4 Select the **Auto Sync Default** check box.