VMware Workspace ONE Mobile Application Management Guide

Enable access to public and enterprise apps

Workspace ONE UEM v9.6

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Table of Contents

Chapter 1: Overview

Organizations use mobile applications to deploy mobile points of sale, configure sales kiosks, create business intelligence, and perform everyday work-related tasks. VMware Workspace ONE UEM Mobile Application Management™ (MAM) functionality can manage mobile applications, deploy them to devices, secure the applications with compliance policies. Workspace ONE UEM offers advanced management functionality to internal applications using the AirWatch SDK and app wrapping.

Workspace ONE UEM Application Types and Their Supported Platforms

Workspace ONE UEM classifies applications as internal, public, purchased, and Web and you upload applications depending on the type. Workspace ONE UEM supports many platforms and operating systems for most of the application types.

View which platform and OS versions Workspace ONE UEM supports for each application type.

Application Type	Supported Platforms
Industry Templates Any Supported App Type	Apple iOS v7.0+ with limitations for compliance policies
Internal	• Android v4.0+ • Apple iOS v7.0+ • Apple macOS v10.9+ • Apple tvOS v10.2+ • Windows Phone • Windows Desktop **Note:** Ensure that the auxiliary files packaged with Apple iOS or macOS applications do not have spaces in the names. Spaces can cause issues when you load the application to the console.

Application Type	Supported Platforms
Public (Free and Paid)	• Android v4.0+ • Apple iOS v7.0+ • Chrome OS • Windows Phone Workspace ONE UEM can manage free, public applications on Windows 10+ devices when you integrate with the Microsoft Store for Business. • Windows Desktop Workspace ONE UEM can manage free, public applications on Windows 10+ devices when you integrate with the Microsoft Store for Business.
Purchased – Custom B2B	Apple iOS v7.0+
Purchased – VPP	• Apple iOS v7.0+ • Apple macOS v10.9+
Web Links	• Android v4.0+ • Apple iOS v7.0+ • Apple macOS v10.9+ • Windows Desktop
SaaS	• Android v4.0+ • Apple iOS v7.0+ • Apple macOS v10.9+ • Windows Desktop

Explanations of Managed Applications and Their Benefits

Workspace ONE UEM can deploy your applications as managed and unmanaged. The Workspace ONE UEM console can perform particular tasks for the managed content that it cannot perform for the unmanaged content.

Explanation of Managed

Use the Workspace ONE UEM public application feature to search and upload public applications from app stores. If you use another way to add public applications to devices, Workspace ONE UEM does not manage these applications. Management functions include these features.

- Automatically deploy applications to devices through a catalog for installation.
- Deploy versions of applications.

- Feature applications in catalogs so that device users can easily access and install them.
- Track installations of applications and push the installation from the console.
- To remove the applications from devices but to keep them in Workspace ONE UEM, you can deactivate public applications.
- Delete applications and all their versions from Workspace ONE UEM and from devices.

Benefits of Management

Workspace ONE UEM can manage most applications unless there is a platform-specific reason hindering management or you upload the public content without searching for it in an app store.

- **Managed content**
  - Distribute – Workspace ONE UEM pushes managed content with a catalog to devices. The catalog automatically installs content or makes the content available for download depending upon the configured push mode.
  - Remove – Workspace ONE UEM can remove the managed content off devices.
- **Unmanaged content**
  - Distribute – Workspace ONE UEM must direct end users through the catalog to an app store to download documents.
  - Remove – Workspace ONE UEM cannot remove the unmanaged content from devices.

Application Configuration Information

Application configurations are key-value pairs that you can deploy with the application to preconfigure features for users. You can enter supported pairs when you upload applications to the Workspace ONE UEM console. You can also code them into your applications.

Currently, application configurations are available for Android and iOS. You must know the supported key-value pairs for your application to deploy them and to code them. To find supported application configurations, review the listed resources.

Find Supported Configurations

The application vendor sets the supported configurations for the application, so you can contact the vendor or visit other sites with information about application configurations.

- To find the supported application configurations, contact the application vendor.
- See these resources with information about application configurations.
  - AppConfig Community at https://www.appconfig.org/
  - VMware Workspace ONE UEM Developers at https://code.vmware.com/web/workspace-one .

Workspace ONE UEM Articles on Adding Application Configurations

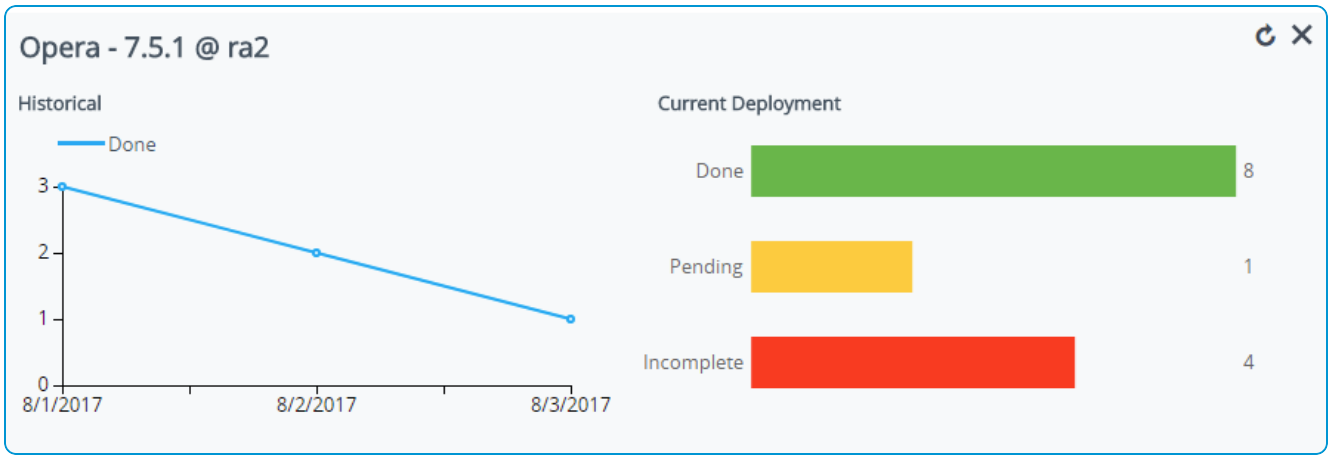
The Workspace ONE UEM knowledge base has articles about working with application configurations when you develop applications. See **Workspace ONE UEM Managed App Configuration** at https://support.air-watch.com/articles/115006248807.

App and Profile Monitor

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

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

When you search for an app or profile, a card containing the deployment data is added to the App and Profile Monitor view. You can only display five cards at a time. These cards remain added until you log out. Any cards must be added again when you log in again.



The Historical section only shows the past seven days of data. It shows the number of devices reporting the Done status for deployment. The Current Deployment section shows the device deployment status. For more information on the deployment statuses, see App and Profile Monitor Statuses on page 10. If you see an Incomplete status, select the number next to the status to see a Device List View of all devices reporting the status. This feature lets you examine devices with issues so you can troubleshoot your deployment.

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

App and Profile Monitor Statuses

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

Status	Description
Done	Devices report the Done status when the app or profile installs successfully.

Status	Description
Pending	Devices report the Pending Status when an app or profile reports the following statuses. **Profiles** ◦ Pending Install. ◦ Pending Removal. ◦ Unconfirmed Removal. ◦ Confirmed Removal. **Apps** ◦ Needs Redemption. ◦ Redeeming. ◦ Prompting. ◦ Installing. ◦ MDM Removal. ◦ MDM Removed. ◦ Unknown. ◦ Install Command Ready for Device. ◦ Awaiting Install on Device. ◦ Prompting for Login. ◦ Updating. ◦ Pending Release. ◦ Prompting for Management. ◦ Install Command Dispatched. ◦ Download in Progress. ◦ Command Acknowledged.

Status	Description
Incomplete	Device reports the Incomplete Status when an app or profile reports the following statuses. **Profiles** ◦ Pending Information. **Apps** ◦ User Removed. ◦ Install Rejected. ◦ Install Failed. ◦ License Not Available. ◦ Rejected. ◦ Management Rejected. ◦ Download Failed. ◦ Criteria Missing. ◦ Command Failed. If you see an Incomplete status, select the number next to the status to see a Device List View of all devices reporting the status. This feature lets you examine devices with issues so you can troubleshoot your deployment.

Track a Deployment with the App and Profile Monitor

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

To track a deployment:

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

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

Chapter 2: Introduction to Mobile Application Management

Organizations use mobile applications to deploy mobile points of sale, configure sales kiosks, create business intelligence, and perform everyday work-related tasks. VMware Workspace ONE UEM Mobile Application Management™ (MAM) functionality can manage mobile applications, deploy them to devices, secure the applications with compliance policies. Workspace ONE UEM offers advanced management functionality to internal applications using the AirWatch SDK and app wrapping.

Basics of Mobile Application Management

Workspace ONE UEM classifies applications as internal, public, purchased, and web. To find out what Workspace ONE UEM supports for platforms and operating systems, see Workspace ONE UEM Application Types and Their Supported Platforms on page 7.

Workspace ONE UEM can deploy your applications managed and unmanaged. The Workspace ONE UEM console can perform particular tasks for the managed content that it cannot perform for the unmanaged content. Read Explanations of Managed Applications and Their Benefits on page 8 for a description of the two.

Notifications

Update end users about changes to applications and books through custom notifications. You can send messages using email, SMS, or push notification. See Create Custom Notifications for Applications on page 14 for information about configure notifications for application management.

Application Categories for the AirWatch Catalog

Application categories help organize your applications and help device users find applications easier. For steps on how to configure application categories for use in your AirWatch Catalog, see Configure Application Categories on page 15.

Application Configurations

Application configurations are key-value pairs that you can deploy with the application to preconfigure features for users. You can enter supported pairs when you upload applications to the UEM console. You can also add them into your applications. To help find supported options and to find information on how to add them to your application during application development, see Application Configuration Information on page 9.

Android Configurations

To deploy public Android applications for an on-premises deployment, configure the mobile network to communicate with the Google Play Store. Google Play integration requires certain ports for communication. For port numbers and other architecture information, see on-premises Architecture Network Requirements.

Windows Desktop 8.1 and Older Configurations

Set the UEM console to distribute approved Windows Desktop internal applications automatically with a side loading key. See Enable Workspace ONE UEM to Distribute Windows Desktop Internal Applications on page 16 for the configurations.

Windows Phone Configurations

Before you can distribute internal applications to Windows Phone devices, you must create, register, and gain approval from the Windows Phone Dev Center. See the Windows Dev Center for current documentation on how to develop applications for Windows Phone and for prices to join the development center. See Register Applications With the Windows Phone Dev Center on page 17 for a general outline for this process.

The app catalog is not supported for Windows Phone devices. However, you can distribute applications to devices using the AirWatch Agent. Set the UEM console to distribute approved Windows Phone internal applications automatically with the AET you received when registering with the Windows Phone Dev Center. Review Enable Workspace ONE UEM for Windows Phone Application Distribution on page 18 for the configurations to set.

Create Custom Notifications for Applications

Update end users about changes to applications and books through custom notifications. You can send messages using email, SMS, or push notification.

Custom Notification Uses

Customize a message template to include application or book names, descriptions, images, and version information. Templates can also include links to your app and book catalogs, and they can prompt end users to download content from the notification.

Workspace ONE UEM sends this message when you use the **Notify Devices** option on the actions menu or from the manage devices feature.

Configure Custom Notifications

Use a message template to create a custom notification message.

1. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Message Templates**.
2. Select **Add**, complete the required information, and save the settings.

Setting	Description
Name	Enter the name of the new template. You can use *book* in this text box to distinguish the message notification from an application notification.
Description	Enter a description of the message that is used internally by Workspace ONE UEM to describe this template.
Category	Select **Application** as the message template category.
Type	Select **Application Notification** as the message template type.
Select Language	Enter a parameter to limit the message delivery to only devices that belong to end users who understand the specified languages.
Default	Select whether the Workspace ONE UEM console uses this message template by default for the **Category** – **Application** and the **Type** – **Application Notification**. This option enables email, SMS, and push notifications for your template. If you do not want to use all types, disable this option and select the ones to use in the **Message Type** option.
Message Type	If you do not want to use all three types, select the message types (email, SMS, or push) that Workspace ONE UEM uses for this template.
Message Body	Enter the message Workspace ONE UEM displays on the end-user devices for each message type. Use the {ApplicationName} lookup value to populate the application name in each message, automatically.

Configure Application Categories

Application categories help organize your applications and help device users find applications easier.

Apps Have Pre-Coded Categories

You do not have to create your own categories. Workspace ONE UEM installs applications and books with their native, pre-coded categories so that you can use them to organize content immediately and apply filters to them.

Uses for Custom Categories

However, if you want to customize categories, you can group applications in numerous ways. Two suggestions are to create categories based on the actual names of the business units or to create categories based on the needs of those units.

- Organization units – Make categories that match business units like IT, Accounting, Sales, Professional Services, and Human Resources. For example, you can apply categories to applications and books and filter them so that only Sales content displays on the app or book page.
- Organization needs – Make categories that match business needs like Security, Communication, Travel, Medical, and Education. You can filter applications and books to display security content and ensure that the latest version is deployed.

Add Custom Application Categories

When you add a new internal or public application or book, the system applies the category that best matches based on meta data from the developer or the app store. You can override this initial assignment and apply your own custom categories. Follow the listed steps to add custom categories.

1. Navigate to **Apps & Books > Applications > Applications Settings > App Categories**.
2. Select **Add Category**.
3. Provide the **Category Name** and **Category Description** and save the settings.

Configure Google Play Integration for on-premises Customers

For on-premises customers, Workspace ONE UEM has updated the logic for how to search for public Android applications from the Google Play Store for deploying applications.

1. Navigate to **Groups & Settings > All Settings > Device & Users > Android > Google Play Integration**.
2. Complete the form for a **Phone** or a **Tablet**, or both, with the applicable information.

Setting	Description
Google account user name	Enter a placeholder Google Account user name.
Google account password	Enter a placeholder Google Account password.
Android Device ID	Enter a placeholder Android Device ID.

If you used placeholder data, Test Connection might not verify a successful integration and it is a normal behavior. Your ability to search for public Android apps might not be affected.

Windows Desktop and Your Company's Root CA

You can push internal applications made for the latest Windows Desktop version from Workspace ONE UEM with the root certificate authority (CA) of your company instead of with a third-party root CA.

Trusted Root CA

Make sure that your root CA is part of the trusted root CA list of the device. If it is not trusted, the Workspace ONE UEM system cannot deploy the application to Windows devices.

The Certificate Authorities (CA) settings page is used to configure integration with various certificate authorities and you can find it at **Groups & Settings > All Settings > System > Enterprise Integration > Certificate Authorities**.

Enable Workspace ONE UEM to Distribute Windows Desktop Internal Applications

Set the Workspace ONE UEM console to distribute approved Windows Desktop internal applications automatically with a side loading key. This process is not needed for Windows 10+.

Pre-Requisites

Before you can distribute internal applications to Windows Desktop devices, you must obtain two items from Microsoft.

- Side loading key (not needed for Windows 10+)

  Workspace ONE UEM sets a property to allow the side loading of applications on Windows 10 devices. This step occurs after the device enrolls with the Workspace ONE UEM system.

- Code signing certificate

Visit the Windows Dev Center for information about side loading keys and code signing certificates for Windows Desktop applications.

Enter the Side Loading Key to Workspace ONE UEM

Enable Workspace ONE UEM to upload your side loading key so that it can distribute internal applications to Windows Desktop devices that are not on Windows 10+.

Important: The key provided by a Volume Licensing portal, such as https://www.Microsoft.com/licensing/servicecenter/default.aspx, might be limited to a specific number of device activations. Verify that there is a key available for your use. For more information about a Microsoft account, visit the Microsoft Developer Network site.

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Desktop > Enterprise Apps**.
2. Complete the following options.

Setting	Description
Enable Enterprise Application Manager	Allows Workspace ONE UEM to push approved internal applications to Windows Desktop devices.
Side Loading Key	Enter the key provided by the Windows Dev Center. For example: ADQ2Z-6TP3W-4QGHK-PSDAW-8WKYR

3. Select **Save**.

   This process uploads the side loading key into the UEM console and automatically enables corporate devices to install the enterprise internal application.

Important: These settings affect devices enrolled after you have prepared the UEM console for application distribution. If you change the side loading key after devices enroll, all devices must re-enroll to access internal applications.

Register Applications With the Windows Phone Dev Center

Before you can distribute internal applications to Windows Phone devices, you must create, register, and gain approval from the Windows Phone Dev Center.

See the Windows Dev Center for current documentation on how to develop applications for Windows Phone and for prices to join the development center.

1. **Register** a Microsoft account for your company with the Windows Phone Dev Center.

   There is a small fee to join, and the subscription enables your company to add applications to the Windows Phone Store. Registration creates a Windows account ID that you must use to obtain a Symantec authentication certificate. For more information about a Microsoft account, visit the Microsoft Developer Network site.

2. **Obtain** a Symantec Enterprise Mobile Code Signing Certificate for the internal application.

   Obtain an Enterprise Mobile Code Signing Certificate from Symantec with the Windows account ID. Use the certificate to sign and verify that your company built the application. Also, use the certificate to generate the application enrollment token (AET) used by each device to obtain a copy of the application.

3. **Build** and digitally sign the internal application.

   Develop and test the corporate application. When the application is ready for distribution, digitally sign the application by following the Precompile and Signature steps outlined in the Windows Phone Dev Center instructions.

4. **Generate** an AET for the internal application.

   Generate an AET that devices use to authenticate before installing the internal application. You can upload the AET to the Workspace ONE UEM console. This action automatically enables corporate devices to install the internal application. Generate an AET by following the AET generation walkthrough outlined by the Windows Phone Dev Center.

Enable Workspace ONE UEM for Windows Phone Application Distribution

The AirWatch Catalog is not supported for Windows Phone devices. However, you can distribute applications to devices using the AirWatch Agent. Set the Workspace ONE UEM console to distribute approved Windows Phone internal applications automatically with the AET you received when registering with the Windows Phone Dev Center.

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Phone > Agent Settings**.
2. Select the **Enable Enterprise App Management** option in the **Enterprise App Management** section.
3. Select **Upload** in the **Upload Enterprise Token** text box to browse for the AET file and save your settings.

Chapter 3: Internal Applications

Use Workspace ONE UEM to manage the deployment and maintenance of your organization's internally developed mobile applications. Management of internal apps differs slightly between platforms, review the topics in this section for getting a better understanding of these differences and successfully deploy the internal apps to the platforms you support.

Basics of Internal Applications

Use Workspace ONE UEM to distribute, track, and manage your internal applications. See Supported File Types for Internal Applications on page 20 for a list of supported file types that you can upload to the console.

You can use Workspace ONE UEM to manage the add your organization's internally developed mobile applications in two ways:

- Add and Deploy Internal Applications as a **Local File**
- Add and Deploy Internal Applications as a **Link**

Upload and Deploy Internal Applications as a Local File

Upload your application package as a Local File for Workspace ONE UEM to parse the application metadata and distribute it to your end-user devices.

For an explanation on how to add your internal applications to Workspace ONE UEM, see Add and Deploy Internal Applications as a Local File on page 22. After you upload internal applications, use the flexible deployment feature to schedule single or multiple deployments for internal applications. See Use Flexible Deployment to Assign Applications on page 30 for more information.

Upload and Deploy Internal Applications as a Link

Add a publicly accessible link or a link to a repository on your internal network that points to your application package location. In this case, Workspace ONE UEM does not have access to your application package. Hence, your application metadata will not be parsed and the same link will be distributed to your end-user devices to initiate the download.

> **Note:** If you are passing a publicly accessible link for your application, make sure the link does not require additional authentication.

Links to your internal network repository have to be routed through 'Content Gateway' for your end-user devices to successfully download and install them. For more details, see Add and Deploy Internal Applications as a Link on page 28.

Track Installations

Use the console to track the installation of internal applications. One benefit is to install applications on those devices that have yet to install the application. Benefits of Tracking Internal App Deployments on page 36 other reasons to track internal application installations.

The details view of the applications is where you install and remove applications from devices. Read about the features of this page in Track Internal Applications With Details View on page 36. See descriptions for reason codes so that you know what the system is doing at each stage of the installation in the topic Installation-Status Reason Code Descriptions on page 38.

Application Removal Protection and Application Removal Safeguard

Use the application removal protection feature to hold application removal commands and the removal of internal applications until an admin approves the removal. This feature protects against the unintended removal of critical internal applications. See Application Removal Protection on page 71 for more information.

If you test seeded Workspace ONE UEM applications before you deploy them to production, follow a specific order of steps to prevent the accidental removal of the production version of the test application. See Safeguards for Proprietary, Non-Store, Workspace ONE UEM Applications on page 74 for more information.

iOS Provisioning Profiles

Internal iOS applications require a provisioning profile to enable deploy and successful use. See Provisioning Profiles for Enterprise Distribution on page 40 for a brief description of provisioning profiles and where to get them.

Keep these files updated by renewing them with the steps in Renew Apple iOS Provisioning Profiles on page 40.

To mitigate issues in Workspace ONE UEM caused by the difference in time that provisioning profiles are valid and the time that development certificates are valid, you can renew the provisioning profiles . For more information, read Provisioning Profiles and Updates on page 40 for information.

Distribute Win32 Packages as Internal Applications

Use the internal applications area to upload, configure, and deploy Win32 application packages to Windows 10+ devices from a local file storage. For more information, reference Distribution of Win32 Applications on page 41.

You can also use the peer distribution system to deliver Win32 packages from peer to peer. This method reduces the traffic on single communication channels with a file storage system or a content delivery network. To see if this method works for your environment, see Peer Distribution for Win32 Applications on page 58.

Supported File Types for Internal Applications

Workspace ONE UEM supports specific file types for internal applications. For some file types, you upload more than one file so that the application works across devices.

Find out what file type the system supports and which file types require you to upload multiple files.

Note: Ensure that the auxiliary files packaged with Apple iOS or macOS applications do not have spaces in the names. Spaces can cause issues when you load the application to the console.

Platform	File Type
Android	APK
Apple iOS	IPA
macOS	APP package bundles Use the product provisioning feature to deploy macOS internal applications as DMG, PKG, and APP files.
Symbian	SIS SISX
tvOS	IPA
Windows Desktop	APPX • Upload a neutral file that works for all three processors. • Upload files for all three processors. On older Windows platforms, you must build processor files for the type of device you want the application to run on. For example, build the three processor files for a Windows Desktop device. Then create and build the processor files for a Windows Phone device. Then you must upload the files for each device type. • Upload a universal application that includes all three processors. Windows universal applications are a single version of an application accessed on any Windows device, including desktops, tablets, and phones. Workspace ONE UEM supports the upload of universal applications to your devices, and you can upload the three APPX files (desktops, tablets, and phones) for all architectures. **Note:** Upload the same APPX file for both Windows Phone and Windows Desktop in the Workspace ONE UEM console if you want the universal app to run on both types of devices. EXE Upload an EXE package of Win32 applications for Windows 10. MSI The MSI file, also called a Windows Installer, is a package that contains everything to install, maintain, and remove the software. ZIP Upload a ZIP package of Win32 applications for Windows 10. For information on the deployment of EXE, MSI, or ZIP files, see Distribution of Win32 Applications on page 41.

Platform	File Type
Windows Phone	APPX • Upload a neutral file. • Upload the ARM processor file build for Windows Phone devices. • Upload the ARM processor file of the universal application. Windows universal applications are a single version of an application accessed on any Windows device, including desktops, tablets, and phones. Workspace ONE UEM supports the upload of universal applications to your devices, and you can upload the three APPX files (desktops, tablets, and phones) for all architectures. **Note:** Upload the same APPX file for both Windows Phone and Windows Desktop in the UEM console if you want the universal app to run on both types of devices. XAP

Suggestion for Developing Internal Applications

Follow the requirements for application development on the Android Developers, iOS Developer, and Microsoft Developer sites. The UEM console accepts most applications built to platform specifications.

Add and Deploy Internal Applications as a Local File

Upload internal applications with local files to deploy them to your mobile network and to take advantage of the mobile application management features of Workspace ONE UEM.

Review instructions from platform sites about how to develop and package applications.

1. Navigate to **Apps & Books > Applications > Native > Internal** and select **Add Application**.
2. Select **Upload > Local File** to browse for the application file on the system.
3. Select **Continue** and configure the **Details** tab options. Not every option is supported for every platform.

Setting	Description
Name	Enter a name for the application.
Managed By	View the organization group (OG) that the application belongs to in your Workspace ONE UEM OG hierarchy.
Application ID	Represents the application with a unique string. This option is pre-populated and was created with the application. Workspace ONE UEM uses the string to identify the application in systems like application whitelists and blacklists.

Setting	Description
Actual File Version	Displays the coded version of the application set by the application's developer.
Build Version	Displays an alternate "File Version" for some applications. This entry ensures Workspace ONE UEM records all version numbers coded for applications because developers have two places within some applications they can code a version number.
Version	Displays the internal version of the application set by the Workspace ONE UEM console.
Is Beta	Tags the application as still under development and testing, a BETA version.
Change Log	Enter notes in this text box to provide comments and notes to other admins concerning the application.
Categories	Provide a category type in the text box to help identify how the application can help users. You can configure custom application categories or keep the application's pre-coded category.
Minimum OS	Select the oldest OS that you want to run this application.
Supported Models	Select all the models that you want to run this application.
Is App Restricted to Silent Install **Android**	Assigns this application to those Android devices that support the Android silent installation feature. The end user does not have to confirm installation activity when you enable this option. This feature makes it easier to uninstall many applications simultaneously. Only Android devices in the smart group that supports the silent uninstallation benefit from this option. These Android devices are also called Android enterprise devices.
Default Scheme	Indicates the URL scheme for supported applications. The application is packaged with the scheme, so Workspace ONE UEM parses the scheme and displays the value in this field. A default scheme offers many integration features for your internal applications, including but not limited to the following options: • Use the scheme to integrate with other platform and web applications. • Use the scheme to receive messages from other applications and to initiate specific requests. • Use the scheme to launch Apple iOS applications in the AirWatch Container.
Description	Describe the purpose of the application. **Note:** Do not use '<' + String in the Description, as you might encounter an Invalid HTML content error.
Keywords	Enter words that might describe features or uses for the application. These entries are like tags and are specific to your organization.
URL	Enter the URL from where you can download the application and get information about it.

Setting	Description
Support Email	Enter an email to receive suggestions, comments, or issues concerning the application.
Support Phone	Enter a number to receive suggestions, comments, or issues concerning the application.
Internal ID	Enter an identification string, if one exists, that the organization uses to catalog or manage the application.
Copyright	Enter the publication date for the application.

Complete the options in the **Developer Information** area:

Setting	Description
Developer	Enter the developer's name.
Developer Email	Enter the developer's email so that you have a contact to whom to send suggestions and comments.
Developer Phone	Enter a number so that you can contact the developer.

(Apple iOS only) Complete the options in the **Log Notification for App SDK** area:

Setting	Description
Send Logs To Developer Email	Enable sending logs to developers for troubleshooting and forensics to improve their applications created using a software development kit.
Logging Email Template	Select an email template uses to send logs to developers.

(Windows Desktop MSI files only) Complete the options in the **Installer Package Deployment** area:

Setting	Description
Command Line Arguments	Enter command-line options that the execution system uses to install the MSI application.
Timeout	Enter the time, in minutes, that the installer waits with no indication of installation completion before it identifies an installation failure. When the system reaches the timeout number, it stops monitoring the installation operation.
Retry count	Enter the number of attempts the installer tries to install the application before it identifies the process as failed.
Retry interval	Enter the time, in minutes, the installer waits between installation attempts. The maximum interval the installer waits is 10 minutes.

Complete the options in the **Application Cost Information** area:

Setting	Description
Cost Center	Enter the business unit charged for the development of the application.
Cost	Enter cost information for the application to help report metrics concerning your internal application development systems to the organization.
Currency	Select the type of currency that paid for the development, or the currency that buys the application, or whatever you want to record about the application.

4. Complete the **Files** tab options.

   Review the file initially uploaded and upload auxiliary files to distribute internal applications.

   You must upload a provisioning profile for Apple iOS applications and you must upload the architecture application files for Windows Desktop applications. If you do not upload the architecture application files, the Windows Desktop application does not function.

Platform	Auxiliary File	Description
All	Application File	Contains the application software to install and run the application and is the application you uploaded at the beginning of the procedure.
Android	Google Cloud Messaging (GCM) Token	This is an AirWatch SDK feature and does not apply to all Android applications. Some internal, Android applications support push notifications from the application to device-users. a. Select **Yes** for the **Application Supports Push Notification** option. b. Enter the **Server API** key in the **GCM Token (API Key)** option. Get this from the Google Developer's site. A developer codes a corresponding **SenderID** into the internal application. To use the feature, push the notification from the applicable device record in the console using the **Send** admin function on the **Devices** tab.
Apple iOS	Provisioning Profile	Authorizes developers and devices to create and run Apple iOS applications. See Apple iOS Provisioning Profiles for information about AirWatch integration with this auxiliary file. Ensure this file covers enterprise distribution and not app store distribution and that it matches the IPA file (Apple iOS application file).
Apple iOS	APNs files for development or production	If the application supports Apple Push Notifications Services (APNs), this file enables messaging functionality. You must upload either the development or production APNs certificate.

Platform	Auxiliary File	Description
Windows Desktop	Neutral architecture application file X64, X86, and ARM files built for Windows Desktop Universal X64, X86, and ARM files MSI file Dependency files	Contains the application software to install and run the application for the specific Windows Desktop architecture.
Windows Phone	Neutral ARM architecture application file ARM file built for Windows Phone devices Universal ARM file Dependency files	Contains the application software to install and run the application for the specific Windows Phone architecture.

5. Complete the options on the **Images** tab.

Setting	Description
Mobile Images	Upload or drag and drop images of the application to display in the App Catalog for mobile devices.
Tablet Images	Upload or drag and drop images of the application to display in the App Catalog for tablets.
Icon	Upload or drag and drop images of the application to display in the App Catalog as its icon.

Note: To achieve best results for Mobile and Tablet Images, refer https://help.apple.com/itunes-connect/developer/#/devd274dd925 for iOS and https://support.google.com/googleplay/android-developer/answer/1078870?hl=en for Android.

6. Complete the **Terms of Use** tab.

Terms of use state specifically how users are expected to use the application. They also make expectations clear to end users. When the application pushes to devices, users view a terms of use page that they must accept to use the application. If users do not accept, they cannot access the application.

7. Complete the **More > SDK** tab.

Setting	Description
SDK Profile	Select the profile from the drop-down menu to apply features configured in **Settings & Policies** (Default) or the features configured in individual profiles configured in **Profiles**.
Application Profile	Select the certificate profile from the drop-down menu so that the application and AirWatch communicate securely.

8. Complete the **More > App Wrapping** tab.

You cannot wrap an application that you previously saved in the AirWatch Console. You have two options:

- Delete the unwrapped version of the application, upload it to AirWatch, and wrap it on the App Wrapping tab.
- Upload an already wrapped version of the application, if you have one, which does not require deleting the unwrapped version.

Setting	Description
Enable App Wrapping	Enables AirWatch to wrap internal applications.
App Wrapping Profile	Assign an app wrapping profile to the internal application.
Mobile Provisioning Profile (iOS Apple)	Upload a provisioning profile for Apple iOS that authorizes developers and devices to create and run applications built for Apple iOS devices.
Code Signing Certificate (iOS Apple)	Upload the code signing certificate to sign the wrapped application.
Require encryption (Android)	Enable this option to use Data At Rest (DAR) encryption on Android devices. AirWatch uses the Advanced Encryption Standard, AES-256, and uses encrypted keys for encryption and decryption. When you enable DAR in App Wrapping, the App Wrapping engine injects an alternative file system into the application that securely stores all the data in the application. The application uses the alternative file system to store all files in an encrypted storage section instead of storing files in disk. DAR encryption helps protect data in case the device is compromised because the encrypted files created during the lifetime of the application are difficult to access by an attacker. This protection applies to any local SQLite database, because all local data is encrypted in a separate storage system.

9. Select **Save & Assign** to configure flexible deployment options for the application.
10. After adding Assignments, Click **Save & Publish**, then **Publish** to deploy the app to your Smart Glasses.

Assign the Application to Groups

To assign and deploy internal applications, configure the flexible deployment options explained in Add Assignments and Exclusions to Applications on page 30.

Add and Deploy Internal Applications as a Link

On-premises customer who do not want to store the application package in the AirWatch Server can choose to keep internal applications in an external application repository and enter the location of internal applications on the external app repository using a **Link**.

You can use Workspace ONE UEM to add your organization's internally developed applications in two ways:

- Host internal application on an external cloud storage system such as dropbox, OneDrive for Business and so on.
- Host internal applications on customer network with an external application repository.

Host internal application on a external cloud storage system

If you are using file storage system to host an internal application, the Devices Services server facilitates the connection for the device to get the application from the file storage system when the UEM console initiates the deployment. Workspace ONE UEM currently does not support external cloud storage system links that requires authentication. It is important that the internal application package that is hosted on a external cloud storage system is a direct link which allows the end users to accept the application package through the URL.

Host internal application on a Customer network

If you are using External App Repository, the Content Gateway facilitates the connection for the device to get the application from the external app repository when the UEM console initiates the deployment. You can host internal applications on your network with an external application repository and manage the applications with the Workspace ONE UEM. The Workspace ONE UEM uses Windows File Share protocols to make externally hosted applications available to user devices. Communication is secure because on-premises deployments must use the Content Gateway for Windows to transfer data from the on-premises network to the Workspace ONE UEM.

Complete the following steps to the Content Gateway for Windows to transfer data from the on-premises network to the Workspace ONE UEM.

1. Configure and use the Content Gateway for Windows to secure communications between your network and Workspace ONE UEM if you have an on-premises deployment.
2. Enter the credentials for the external app repository so Workspace ONE UEM can direct device users to the internal applications on your network in the external app repository. Workspace ONE UEM supports one set of credentials to authenticate to repositories that require it. If you have multiple repositories set up on the Content Gateway, use a common set of credentials, if your repositories require authentication.

   See Add Credentials for the External App Repository on page 29.

3. Enter the location of internal applications on the external app repository using a Link.

   See Add Internal Applications From External Repositories on page 30.

Supported Components for External App Repositories

If you use the Content Gateway for Windows and house applications on an external server system, set external repositories for various platforms and application types.

Supported App Types

The external app repository feature supports only internal applications.

Supported File Types

You can add the following supported file types to the external app repository feature.

- IPA for Apple iOS
- Application package bundles for macOS
- APK for Android
- SIS and SISX for Symbian
- XAP for Windows Phone
- APPX, msi, zip and .exe for Windows Desktop that works for all three processors, x64, x86, and ARM

Important: The link for the application must end in one of the supported file types or users cannot access the application.

Supported Deployments

- SaaS deployments using the Content Gateway for Windows for secure communications
- on-premises deployments using the Content Gateway for Windows for secure communications

Credentials for Multiple Repositories

If your repositories require authentication, Workspace ONE UEM uses one set of credentials to communicate between the Content Gateway and your repositories. For this feature to work, use a common set of credentials for the Content Gateway to communicate with your repositories.

Add one set of credentials for your repositories you configured with the Content Gateway. For details, see Add Credentials for the External App Repository on page 29.

See Add Internal Applications From External Repositories on page 30 for an explanation of how to upload the application to Workspace ONE UEM.

Add Credentials for the External App Repository

Allow Workspace ONE UEM to direct users to internal applications on your network in an external app repository. The Content Gateway for Windows uses this information to access the repository and to open communications between the device and the repository.

1. Navigate to **Groups & Settings > All Settings > Apps > Workspace ONE > External App Repository**.
2. Complete the following options:

Setting	Description
Username	Enter the username for the external app repository.
Password	Enter the password for the external app repository.

3. Select **Save**.

Add Internal Applications From External Repositories

Set an external resource that you store in a secure repository as an internal application that device users access through the Content Gateway for Windows.

1. Navigate to **Apps & Books > Applications > Native > Internal** and select **ADD APPLICATION**.
2. Select **Upload**, select **Link**, confirm that access uses the Content Gateway, and select the gateway you want to use. However if the link to the application is publicly available then the Content Gateway is not required.
3. Enter the location of the internal application in your external app repository.

   You can use a server file path, network file share path, an HTTP address, or an HTTPS address. The string must include the name of the internal application and the file extension. An example of this location is **http://<ExternalAppRepository>/<InternalAppFileName.FileExtension>**.
4. Select **Continue** and configure the remaining tabs.]
5. Select **Save & Assign** to configure flexible deployment options for the application.

Use Flexible Deployment to Assign Applications

Workspace ONE UEM offers a flexible deployment feature for internal and public applications. They are flexible because they allow you to schedule multiple application deployment scenarios.

You can configure deployments for internal applications for a specific time and let the Workspace ONE UEM console carry out the deployments without further interaction.

The flexible deployment feature resides in the **Assign** sections of the application area and offers advantages to the assigning process.

- Configure deployment assignments.
- Assign multiple deployments simultaneously.
- Order assignments so that critical deployments are not missed due to the limited bandwidth.
- Customize assignments for multiple smart groups.

Add Assignments and Exclusions to Applications

To control the deployment of applications, add a single assignment or multiple assignments. Also, exclude groups from receiving the assignment.

If you add multiple assignments, prioritize the importance of the assignment by moving its place in the list up for most important or down for least important.

Note: If you use APIs to assign applications, do not use the exclusions in the console. APIs for exclusions are in development at this time. If you want to use exclusions, assign applications through the console, do not use APIs for assignment.

1. Navigate to **Apps & Books > Applications > Native > Internal** or **Public**.
2. Upload an application and select **Save & Assign** or select the application and choose **Assign** from the actions menu.
3. On the **Assignments** tab, select **Add Assignment** and complete the following options:

Setting	Description
Select Assignment Groups	Type a smart group name to select the groups of devices to receive the assignment.
App Delivery Method	• **On Demand** – Deploys content to a catalog or other deployment agent and lets the device user decide if and when to install the content. This option is the best choice for content that is not critical to the organization. Allowing users to download the content when they want helps conserve bandwidth and limits unnecessary traffic. • **Automatic** – Deploys content to a catalog or other deployment agent on a device upon enrollment. After the device enrolls, the system prompts users to install the content on their devices. This option is the best choice for content that is critical to your organization and its mobile users.
Desired State Management macOS	Currently when installing a macOS software, administrators have an option to enable or disable the Desired State Management settings based on the business needs. Desired State Management is enabled by default to enforce application management while installing a macOS software. If enabled, and if the end-user deletes the app, the application is automatically reinstalled on the next Agent sync. If disabled, and if the end-user deletes the app, the application is not automatically reinstalled, unless pushed from the UEM Console or Catalog. Also, as an administrator you have the flexibility to deploy applications as one-time configuration and provide end-users the facility to uninstall the application locally if needed.

Setting	Description
Deployment Begins On Internal Applications	Set a day of the month and a time of day for the deployment to start. The **Priority** setting governs which deployments push first. Workspace ONE UEM then pushes deployments according to the **Effective** configuration. To set a beginning date with enough bandwidth for successful deployment, consider the traffic patterns of your network .
Policies	
DLP Android iOS Windows Desktop Windows Phone	Configure a device profile with a **Restrictions** profile to set data loss prevention policies for the application. Select **Configure**. The system navigates to **Devices > Profiles**. Select **Add > Add Profile** and the platform. • For Android and iOS devices, select **Restrictions** and enable options in the **Data Loss Prevention** section. • For Windows Desktop, select **Device Profile > Restrictions** and enable options that apply to the data you want to protect. • For Windows Phone, select **Restrictions** and enable options that apply to the data you want to protect.
Managed Access Android iOS	Enable adaptive management to set Workspace ONE UEM to manage the device so that the device can access the application. Workspace ONE controls this feature and is not supported by the AirWatch Catalog.
Remove on Unenroll iOS	Set the removal of the application from a device when the device unenrolls from Workspace ONE UEM. If you choose to enable this option, supervised devices are restricted from silent app installation because the device is locked and the provisioning profile installation is in the command queue which requires a device to be unlocked to complete the installation. If you choose to disable this option, provisioning profiles are not pushed along with the installed application. That is, if the provisioning profile is updated, the new provisioning profile is not automatically deployed to devices. In such cases, a new version of the application with the new provisioning profile is required.
Prevent Application Backup iOS	Disallow backing up the application data to iCloud.

Setting	Description
Make App MDM Managed if User Installed iOS	Assume management of applications previously installed by users on their devices, supervised and unsupervised. Enable this feature so that users do not have to delete the application version installed on the device. Workspace ONE UEM manages the application without having to install the application catalog version on the device.
App Tunneling Android iOS	Configure a VPN at the application level, and select the **Per-App VPN Profile**. Users access the application using a VPN, which helps ensure that application access and use is trusted and secure. **Note**: If you are adding an internal application, **Per-App VPN Profile** tunneling currently supports only the Android (Legacy) devices. However, Android Work Profile and the Work Managed devices do not support **Per-App VPN Profile** tunneling for all the internal applications.
Application Configuration Android iOS	Send application configurations to devices. **Upload XML (Apple iOS)** – Select this option to upload an XML file for your iOS applications that automatically populates the key-value pairs. Get the configurations supported by an application from the developer in XML format

4. Select **Add**.
5. Use the **Move Up** and **Move Down** options to order assignments if you have more than one. Place critical assignments at the top of the list. This configuration displays as the **Priority**.

   The **Priority** setting takes precedence when there are conflicting deployments assigned to a single device.
6. Select the **Exclusions** tab and enter smart groups, organization groups, and user groups to exclude from receiving this application.
   - The system applies exclusions from application assignments at the application level.
   - Consider the organization group (OG) hierarchy when adding exclusions. Exclusions at a parent OG do not apply to the devices at the child OG. Exclusions at a child OG do not apply to the devices at the parent OG. Add exclusions at the desired OG.
7. Select **Save & Publish**.

Application configurations are vendor-specific key-value pairs you can deploy with an application to preconfigure the application for users. For resources about application configurations, see Application Configuration Information on page 9.

For more information about the flexible deployment page, where you can edit schedules for deployments and view settings configured upon upload, see Flexible Deployment for Applications Setting Descriptions on page 34.

Flexible Deployment for Applications Setting Descriptions

The flexible deployment page contains information about your application assignments. From this page, edit schedules for deployments and view settings configured upon upload.

Options displayed on this window depend on the platform.

Setting	Description
Edit	Edit assignment configurations, including the smart group and push mode.
Delete	Remove the selected assignment from the application deployment.
Move Up	Raise the selected priority of the assignment by moving it up on the list of assignments.
Move Down	Reduce the selected priority of the assignment by moving it down on the list of assignments.
Name	View the assigned smart group.
Priority	View the priority of the assignment you configured when placing the selected assignment in the list of assignments. **Priority 0** is the most important assignment and takes precedence over all other deployments. You can use this option with **Effective** to help plan deployments to avoid times when your mobile network experiences heavy traffic.
App Delivery Method	View how the application pushes to devices. **Auto** pushes immediately through the AirWatch Catalog with no user interaction. **On Demand** pushes to devices when the user initiates an installation from the AirWatch Catalog.
Effective (Internal Applications)	Review the status of the assignment, whether it is in effect now or will be effective at some future date.
Managed Access	View whether the application has adaptive management enabled.
Remove on Unenroll (Apple iOS)	View whether Workspace ONE UEM removes the application from a device when the device is unenrolled from Workspace ONE UEM. If you choose to enable this option, supervised devices are restricted from silent app installation because the device is locked and the provisioning profile installation is in the command queue which requires a device to be unlocked to complete the installation. If you choose to disable this option, provisioning profiles are not pushed along with the installed application. That is, if the provisioning profile is updated, the new provisioning profile is not automatically deployed to devices. In such cases, a new version of the application with the new provisioning profile is required.
Application Backup (Apple iOS)	View whether Workspace ONE UEM disallows backing up the application data to iCloud. However, the application can still back up to iCloud.

Setting	Description
VPN Access (Apple iOS 7+)	View if Workspace ONE UEM uses a VPN connection at the application level. This option sets end users to access the application using a VPN, which helps ensure that application access and use is trusted and secure. This option is **Disabled** for platforms other than Apple iOS.
Send Configuration	View if Workspace ONE UEM sends configurations to managed Android and Apple iOS applications.
Assume Management	View if Workspace ONE UEM is enabled to assume management of user-installed applications without requiring the deletion of the previously installed application from the device. This option corresponds to the **Make App MDM Managed if User Installed** option.

For information about assuming management of applications installed by users, see Make App MDM Managed If User Installed on page 164.

Flexible Deployment Conflicts and Priorities

If a device belongs to more than one smart group and you assign these smart groups to an application with several flexible deployments, the device receives the scheduled flexible deployment with the most immediate **Priority**.

As you assign smart groups to flexible deployments, remember that a single device can belong to more than one smart group. In turn, one device can be assigned to more than one flexible deployment for the same application.

Example

Device 01 belongs to Smart Group HR and Smart Group Training. You configure and assign two flexible deployments for application X, which include both Smart Groups. Device 01 now has two assignments for application X.

The following example shows how Device 01 can receive an assignment later than expected due to the flexible deployment priority.

	Priority	Smart Group	Deployment Parameters	Deployment Received
Device 01	Priority **0**	Smart Group **HR**	Deploy in **10 days** time **On Demand**	**Receives this assignment**, 10 days later with installation initiated by the user (on demand).
Priority **1**	Smart Group **Training**	Deploy **now** **Auto**	**Not received** because it received the Priority 0 assignment.	

Control Batch Options for Flexible Deployments

Workspace ONE UEM offers the System Admin the ability to control some batching options for flexible deployments. You can change the size of batches, the frequency Workspace ONE UEM releases batches, and the frequency Workspace ONE UEM checks for new assignments. Make edits to batching using scheduler tasks and performance tuning.

Control Frequency

Control the frequency at which Workspace ONE UEM checks for new flexible deployment assignments.

1. Navigate to **Groups & Settings > All Settings > Admin > Scheduler**.
2. Find **Scheduled Application Publish** and select edit.
3. Complete the options in the Recurrence Type section and save your settings.

Control the frequency at which Workspace ONE UEM releases batches of applications.

1. Navigate to **Groups & Settings > All Settings > Admin > Scheduler**.
2. Find **Scheduled Application Batch Release** and select edit.
3. Complete the options in the Recurrence Type section and save your settings.

Control Performance Tuning

Control the size of batches of applications that Workspace ONE UEM compiles and deploys to devices.

1. Navigate to **Groups & Settings > All Settings > Installation > Performance Tuning**.
2. Edit **Batch Size for Internal Application Deployment**.
3. Save your settings.

Bypass Batching

You can bypass the batching process and release all installation commands for applications.

1. Navigate to **Apps & Books > Applications > Native > Internal**, and select the application.
2. Select from the actions menu **More > Manage > Bypass Batching**.

Benefits of Tracking Internal App Deployments

You can use the application **Details View**, particularly the **Summary**, and **Devices** tabs, to track the deployment of applications.

The Details View consolidates application tracking functions to help with many application management commitments.

- Gather data concerning application deployments and install or remove applications from a single location.
- Comply with enterprise mandates to deploy required application versions.
- Notify devices of non-compliance with installation requirements.
- View reason codes that represent steps in the progress of installing applications.

Track Internal Applications With Details View

Track internal applications with the Summary and Devices tabs of the Details View to audit application deployments and perform management functions.

1. Navigate to **Apps & Books > Applications > List View > Internal**.
2. Search for and select the desired application.
3. Select the **Summary** tab and review the application information.

Analytic	Data Snapshot	Available Actions
Install Status	**Installed** – Lists the number of devices that have installed the application. **Not Installed** – Lists the number of devices that have not installed the application.	Select the **Not Installed** area to discover which devices have not installed the application. This action navigates to the **Devices** tab.
Deployment Progress	**Assigned To** – Lists the smart groups assigned to the application's Flexible Deployment. **Status** – Reports Workspace ONE UEM's release of the installation command to devices. **Deployment** – Displays the application's Push Mode, Auto, or On Demand.	Use the table to review if Workspace ONE UEM has released the installation of the application, the Push Mode used to deliver the application to devices, and the assigned smart groups.
Versions Installed	Displays all the versions installed on devices.	Select a non-compliant version area to determine which devices have not installed the required version of the application. This action navigates to the **Devices** tab.
Install Status Breakdown	Displays reasons for **Installed** and **Not Installed** statuses.	Select the **Not Installed** label to discover the reasons why devices have not installed a required application version. This action navigates to the **Devices** tab. See Reasons for Installation Status for descriptions.

4. Select the **Devices** tab, and use the following management functions to act on installation issues.

Setting	Description
Send Message to All	Send a notification to all devices listed on the **Devices** tab.
Install On All	Install the application on all devices listed on the **Devices** tab.
Remove From All	Remove the application, if managed, from all the devices listed on the **Devices** tab.

Select individual devices and use the available management functions.

Setting	Description
Query	Send a query to the device for data concerning the state of the application.
Send	Send a notification to the selected device concerning the application.
Install	Install the application on the selected device.
Remove	Remove the application, if managed, from the selected device.

Installation-Status Reason Code Descriptions

Workspace ONE UEM displays reasons that describe the installation progression of internal applications on the Details View, Devices tab. The reason codes help identify the status of an installation and if there is an issue with an installation, so that you can easily track and troubleshoot application deployments.

Workspace ONE UEM displays the reasons in **Apps & Books > Applications > Native > Internal > Details View [for the specific application] > Devices tab**.

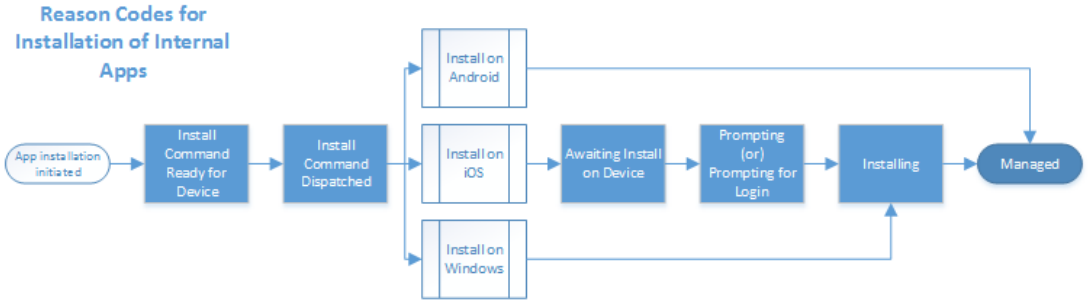
Reason	Description
All	Shows all devices. Acts as the default filter on the **Devices** tab.
Awaiting Install on Device	Workspace ONE UEM sent the installation command and it has not yet prompted device users to accept the installation.
Failed	Workspace ONE UEM attempted to install the application but encountered an error.
Install Command Dispatched	The device communicated that it received the install command.
Install Command Ready for Device	Workspace ONE UEM queued the command and communicated to devices to select in but devices have not checked in yet.
Installing	Workspace ONE UEM is installing the application.
Managed	Workspace ONE UEM installed the application and now manages it.
Management Rejected	The users of iOS 9+ devices rejected prompts to install applications or to enter their credentials, so Workspace ONE UEM cannot install the application.
MDM Removed	Workspace ONE UEM removed the application due to a mobile device management action performed with the console.
Pending Removal	Workspace ONE UEM sent an application removal command to devices but the application has not been removed yet.
Prompting	Workspace ONE UEM is prompting device users to install the application.
Prompting for Login	The app store is prompting device users for their app store credentials so that they can install the application.
Prompting for Management	Workspace ONE UEM is prompting iOS 9+ device users to accept the **Make App MDM Managed if User Installed** configuration. To accept the prompt permits Workspace ONE UEM to manage an application that users previously installed on their devices.
Rejected	The device user rejected the prompt to install a book.
Unknown	The device and Workspace ONE UEM are not communicating about the installation of the application.
Updating	Workspace ONE UEM pushed an application update command but the device has not communicated that the application update is complete.

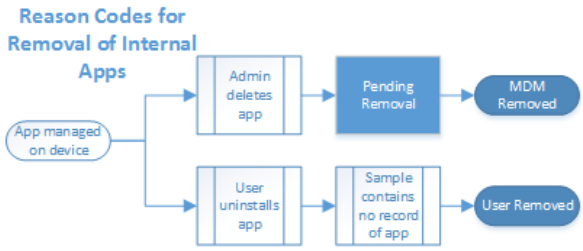
Reason	Description
User Installed	Workspace ONE UEM pushed a book to devices but device users had already installed it.
User Installed App	Workspace ONE UEM pushed an application to devices but device users already installed it.
User Rejected	Device user rejected the prompt to install the application.
User Removed	Workspace ONE UEM still manages the application but users removed it from their devices.

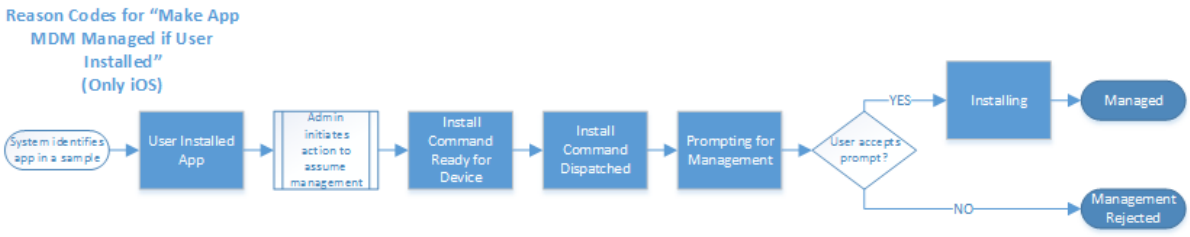
Reasons Display in Order of Installation Progression

Workspace ONE UEM displays the install status reasons, or reason codes, to help you determine the status of your application in the deployment process.

The clear shapes represent processes that trigger the reason code in the color block shapes.







Provisioning Profiles for Enterprise Distribution

When you upload an internal application to the Workspace ONE UEM console, upload the provisioning profile that you generated for that particular application, too. For an internal Apple iOS application to work, every device that runs the application must also have the provisioning profile installed on it.

The provisioning profile authorizes developers and devices to create and run applications built for Apple iOS devices.

For internal applications, use files from the Apple iOS Developer **Enterprise** Program and not the Apple iOS Developer Program.

These programs are different. When you get a mobile provisioning profile for your internal applications, verify that it is for enterprise (internal) distribution.

- **Apple iOS Developer Enterprise Program** – This program facilitates the development of applications for internal use. Use profiles from this program to distribute internal applications in Workspace ONE UEM.
- **Apple iOS Developer Program** – This program facilitates the development of applications for the app store.

Provisioning Profiles and Updates

Apple generates development certificates that expire within three years. However, the provisioning profiles for the applications made with the development certificates still expire in one year. This model can create issues in Workspace ONE UEM.

Issues exist for developers and device users.

- Developers who build and deploy multiple versions of an application need a way to remove expired provisioning profiles that are associated with active applications.
- Device users receive warnings concerning the status of an application 30 days before a provisioning profile expires.

However, if you can manage renewals, you can mitigate these issues. You can use the expiration dates Workspace ONE UEM displays to mitigate issues.

- Workspace ONE UEM displays expiration notices in the console 60 days before the expiration date.
- You can update provisioning profiles and apply them to all associated applications managed in Workspace ONE UEM.
- If the provisioning profiles are not associated to other applications, you can remove them or replace older ones.

Renew Apple iOS Provisioning Profiles

You can renew your Apple iOS provisioning profiles without requiring end users to reinstall the application. The Workspace ONE UEM console notifies you 60 days before the provisioning profile expires with the expiration links in the **Renewal Date** column on the **Internal** tab. Workspace ONE UEM also enables you to renew the file for all applications associated with it.

You can access expiration links for Apple iOS provisioning profiles from within the applicable organization group (OG). The UEM console does not allow access unless you are in the correct OG.

1. Navigate to **Apps & Books > Applications > Native > Internal**.
2. Select the expiration link (**Expires in XX days**) in the **Renewal Date** column for the application for which you want to update the provisioning profile.
3. Use the **Renew** option on the **Files** tab to upload the replacement file.

4. Select the **Update Provisioning Profile For All Applications** setting to apply the renewed file to all associated applications. Workspace ONE UEM displays this option only if multiple applications share the provisioning profile.

   Workspace ONE UEM lists the applications that share this provisioning profile for you on the **Files** menu tab. Workspace ONE UEM silently pushes the updated provisioning profile to all devices that have the application installed.

Expired Apple iOS Provisioning Profiles

When an Apple iOS provisioning profile expires, device users cannot access the associated application, and new device users cannot install the application.

Distribution of Win32 Applications

Workspace ONE UEM can deploy Win32 applications from the Apps & Books section so that you can use the application flow that exists for all internal applications. This feature is called software distribution.

If you have scripting needs, use the product provisioning feature described in the Introduction to Product Provisioning for Windows Desktop in the **VMware Workspace ONE UEM Product Provisioning for Windows Desktop Guide**.

For more information on software distribution and how to troubleshoot the system, see the following Workspace ONE UEM Knowledge Base article: https://support.workspaceone.com/articles/115001674888.

Requirements to Deploy Win32 Applications for Software Distribution

To deploy Win32 applications with the software distribution, use supported file types, operating systems, and platforms.

Supported Platforms

The supported platform to deploy Win32 Applications is Windows Desktop.

Supported File Types

- MSI
- EXE
- ZIP

CDNs and File Storage Systems

All deployments use a content delivery network (CDN) to deploy applications. This option has the advantage of sending content to devices in the network and to remote devices. It also offers increased download speeds and reduces bandwidth on Workspace ONE UEM servers. However, in some scenarios, a CDN is not a viable option. For these instances, use a file storage system.

Enable Software Package Deployment

Configure Workspace ONE UEM to recognize the deployment of Win32 applications through the software distribution method.

SaaS Environments

For the **Software Package Deployment** option to display, Workspace ONE UEM enables the CDN for the environment. Go to **Groups & Settings > All Settings > Device & Users > Windows > Windows Desktop > App Deployments** and enable **Software Package Deployment**.

Note: If your deployment whitelists Workspace ONE UEM IP addresses, the CDN does not work.

On-premises Environments

On-premises environments use a file storage system to store the large Win32 applications. They also use a CDN to download the applications and to reduce the bandwidth on other servers.

1. First, enable the CDN at **Groups & Settings > All Settings > System > Enterprise Integration > CDN**.
2. Enable the file storage system. See Workspace ONE UEM Reports on page 42 for more information and server requirements.

File Storage

Certain Workspace ONE UEM functionality uses a dedicated file storage service to handle processing and downloads, which reduces the overall burden on your Workspace ONE UEM database and increases its performance. It also includes certain Workspace ONE UEM reports, internal application deployment, and Workspace ONE UEM-managed content. When you enable file storage for any of these functionalities, it is applied to the others automatically. Setting up file storage causes all reports, all internal applications, and all managed content to be stored there.

Configuring file storage manually is only applicable to on-premises customers. It is automatically configured for SaaS customers.

Workspace ONE UEM Reports

As of console version 9.0.2, three new reports were added that appear the same as existing reports but use a revamped back-end framework. This new framework generates reports with greater reliability and faster download times. To take advantage of these benefits, you must set up file storage.

For more information about these reporting updates, see the following Knowledge Base article: https://support.air-watch.com/articles/115002346928.

Internal Applications

When file storage is enabled, all internal application packages that you upload through the UEM console are stored in a file storage location.

File storage is required to deploy Win32 applications (IPA, PAK, APPX, MSI, EXE, and so on) and macOS applications (.dmg, .pkg, .mpkg, and so on) from the Apps & Books area of the UEM console. This feature is called software distribution.

Workspace ONE UEM Managed Content

You can separate the managed content from the Workspace ONE UEM database by storing it in a dedicated file storage location. Uploading large amounts of managed content might cause issues with database performance. In this case, on-premises customers can free up space in the database by moving the managed content to an integrated local file storage solution.

Personal content also moves to the file storage solution is enabled. By default, personal content is stored in the SQL database. If you have a Remote File Storage enabled, personal content is stored in the RFS and not in the file storage or SQL database.

File Storage Requirements

To set up local file storage, you must meet the following requirements.

Important: File Storage is required for Windows 10 Software Distribution.

Create the Shared Folder on a Server in Your Internal Network

- File storage can reside on a separate server or the same server as one of the other AirWatch application servers in your internal network. It is only accessible to components that require access to it, such as the Console and Device Services servers.
- If the Device Services server, Console server, and the server hosting the shared folder are not in the same domain, then establish Domain Trust between the domains to avoid the authentication failure. If the Device Services server or Console server is not joined to any domain, then supplying the domain during service account configuration is sufficient.

Configure the Network Requirements

- **If using Samba/SMB** – TCP: 445, 137, 139. UDP: 137, 138
- **If using NFS** – TCP and UDP: 111 and 2049

Allocate Sufficient Hard Disk Capacity

Your specific storage requirements may vary depending on how you plan to use file storage. The file storage location should have enough space to accommodate the internal apps, managed content, or reports you intend to use. Take into the account the following considerations.

- If you enable caching for internal apps or content, then a best practice is to size the Device Services server for 120 percent of the cumulative size of all the apps/content you need to publish.
- For storing reports, your storage requirements depend on the number of devices, the daily amount of reports, and the frequency with which you purge them. As a starting point, you should plan to allocate at least 50 GB for deployment sizes up to 250,000 devices running about 200 daily reports. Adjust these numbers based on the actual amount you observe in your deployment. Apply this sizing to your Console server as well if you enable caching.

Create a Service Account with Correct Permissions

- Create an account with read and write permissions to the shared storage directory.
- Create the same local user and password on the Console, Device Services, and the server that is being used for File Storage.
- Give the local user read/write/modify permissions to the file share that is being used for the File Storage Path.
- Configure the File Storage Impersonation User in AirWatch with the local user.

You can also use a domain service account instead of a local user account.

Configure File Storage at the Global Organization Group

Configure file storage settings at the Global organization group level in the UEM Console.

For information about configuring Local File Storage, see Configure Local File Storage.

Enable File Storage for Applications

Configure file storage for internal applications using the procedure below. This is required if you are deploying Win32 apps using software distribution, but will apply to all internal apps once configured.

1. At the Global organization group level, navigate to **Groups & Settings > All Settings > Installation > File Path** and scroll to the bottom of the page.
2. Select the **File Storage Enabled** slider and configure the settings. When file storage is enabled, you can configure an external repository in which files are stored. A disabled setting means that files are stored as binary large objects in the database.

Setting	Description
File Storage Path	Enter the path files are to be stored in the following format: \\{Server Name}\{Folder Name}, where Folder Name is the name of the shared folder you create on the server.
File Storage Caching Enabled	When enabled, a local copy of files requested for download is stored on the Device Services server as a cache copy. Subsequent downloads of the same file retrieve it from the Device Services server as opposed to file storage. If you enable caching, consider accommodating for the amount of space needed on the server. For more information, see File Storage Requirements on page 43. If you integrate with a CDN, then apps and files are distributed through the CDN provider, and a local copy is not stored on the Device Services server. For more information, refer to the **VMware Workspace ONE UEM CDN Integration Guide** (https://resources.air-watch.com/view/8cr52j4hm6xfvt4v2wgg/en).
File Storage Impersonation Enabled	Select to add a service account with the correct permissions.
File Storage Impersonation Username	Provide a valid service account user name to obtain both read and write permissions to the shared storage directory.
Password	Provide a valid service account password to obtain both read and write permissions to the shared storage directory.

3. Select the **Test Connection** button to test the configuration.

Application Lifecycle for Software Distribution

Workspace ONE UEM can help manage Win32 applications with its lifecycle features, so that you can know their installation statuses, keep them current, and delete them.

To manage the deployment of your Win32 applications, use the life cycle of internal application.

Phase	Description
Upload Win32 Files on page 45	Add the Win32 application and define if it is a dependency file.
Configure, Assign, and Deploy Win32 Files on page 45	Enter details for the Win32 application, add supporting files, enter deployment criteria, and assign to devices.
Inventory Win32 Applications with Tracking Features on page 57	Track the installation progress of Win32 applications.
Add Versions for Internal Applications on page 171	Add full versions of Win32 applications and patches.
Delete Win32 Files on page 57	Delete applications with several options.

Upload Win32 Files

Upload Win32 applications as either main files or dependency files. Use the same process for EXE, MSI, and ZIP files.

1. Navigate to **Apps & Books > Applications > Native > Internal** and select **Add Application**.
2. Select **Upload**, and then select **Local File** and select the application to upload.
3. Select an answer to **Is this a dependency file**.

   Select **Yes** to tag a dependency file and associate it to Win32 applications. Examples of dependency files are libraries and frameworks. Select **Continue** to go to the next phase in the life cycle.

Configure, Assign, and Deploy Win32 Files

Configure details about the Win32 application, which include to define when to install it, how to install it, and when to identify the installation is complete. To complete the process, assign the application to smart groups with the flexible deployment feature.

For considerations to review when configuring the **How To Install** section, see Considerations for Retry Count, Retry Interval, and Install Timeout Options on page 54.

Configuration Process

1. Configure the **Details** tab options.

   The Workspace ONE UEM system cannot parse data from an EXE or ZIP file. Enter the information for the EXE and ZIP files on this tab.

   The system parses the listed information for MSI files.

   - Application name
   - Application version
   - Application identifier (also called a product code)
2. Complete the **Files** tab options.

   Review the file initially uploaded and upload dependencies, transforms, patches, and uninstallation processes.

File	Description	Configurations
App Dependencies MSI, EXE, ZIP	The environment and devices need these applications to run the Win32 application.	a. Select dependency files in the **Select Dependent Applications** option. b. Enable the system to apply dependencies in a specified order. The system works from top to bottom.
App Transforms MST file type	These files control the installation of the application and can add or prevent components, configurations, and processes during the process.	Select **Add** to browse to the MST file on the network.
App Patches MSP file type	These files add changes that are fixes, updates, or new features to applications. The two types are additive and cumulative. • **Additive** – Includes only changes developed after the latest version of the application or the last additive patch. • **Cumulative** – Includes the entire application including any changes since the latest version of the application or the last patches.	a. Select **Add**. b. Identify the patch as cumulative or additive. c. Select **File** to browse to the MSP file on the network.
App Uninstall Process	These scripts instruct the system to uninstall an application under specific circumstances. Customized scripts are optional for MSI files.	a. Select the **Use Custom Script** option. b. Select to upload or enter a script to the system for **Custom Script Type**. • Select **Upload** and browse to the script file on the network. • Select **Input** and enter the custom script.

3. Complete the settings on the **Deployment Options** tab.

   This tab instructs the system to install the application with specific criteria. The system can parse information for MSI files. However, for EXE and ZIP files, the system requires you to enter this information.

   a. **When To Install**

      Configure Workspace ONE UEM to install Win32 applications when devices and your mobile network are in a specific state.

      Data contingencies work for both when to install and when to call install complete.

      - Instruction – This explanation describes system behavior for When To Install.
      - Completion – This explanation describes system behavior for When To Call Install Complete.

Setting	Description
Data Contingencies	Select **Add** and complete the options that depend on the criteria type you select. Set contingencies for these scenarios: • Instruction – Contingencies instruct the system to install applications when the device meets specific criteria. • Completion – Contingencies identify when an installation is complete. Add multiple criteria and configure the system to apply all contingencies (and) or to apply alternative ones (OR).
Criteria Type – App	
App exists **App does not exist**	• Instruction – Configure the system to install the application when a specific application is or is not on devices. • Completion – Configure the system to identify the installation is complete when a specific application is or is not on devices. Workspace ONE UEM checks for the existence of the application but it does not deploy the application to devices.
Application Identifier	Enter the application identifier so the system can recognize the existence or non-existence of the auxiliary application. This value is also known as the product code of the application.
Application Version	Enter the specific version.
Criteria Type – File	
File exists **File does not exist**	• Instruction – Configure the system to install the application when a specific file is or is not on devices. • Completion – Configure the system to identify the installation is complete when a specific file is or is not on devices.
Path	Enter the path on the device where you want the system to look for the file and include the filename.
Modified On	Enter the date the file was last modified.
Criteria Type – Registry	
Registry exists **Registry does not exist**	• Instruction – Configure the system to install the application when a specific registry is or is not on devices. • Completion – Configure the system to identify the installation is complete when a specific registry is or is not on devices.
Path	Enter the path on the device where the system can find the keys and values. Include the entire path, beginning with HKLM\ or HKCU\.

Setting	Description
Value Name	Enter the name of the key. This container object stores the value and it displays in the file structure of the device.
Value Type	Select the type of key displayed in the file structure of the device.
Value Data	Enter the value of key. The name-data pairs stored in the key display in the file structure of the device.

Select **Add** to continue setting deployment options.

Setting	Description
Disk Space Required	Set the disk space devices must have available for the system to install the application.
Device Power Required	Set the battery power devices must have available for the system to install the application.
RAM Required	Set the random access memory devices must have available for the system to install the application.

b. **How To Install**

Configure Workspace ONE UEM to install Win32 applications to define the installation behavior on devices. While configuring the Win32 applications in the Workspace ONE UEM console, you have different combinations that you could choose while setting the **Install Context** and **Admin Privileges** under the **Deployment** tab. Your installation process may vary based on the settings. To understand more about Win 32 application installation behavior see Win32 Application Installation Behavior on page 51 .

Setting	Description
Install Context	Select how the system applies the installation. • Device- Define the installation by the device and all the users of that device. • User- Define the installation by particular user accounts (enrolled).

Setting	Description
Install Command	Enter a command to control the installation of the application. • **MSI**- The system automatically populates the installation commands, and the commands include patches and transforms. ◦ Patches- To update the order in which the patches install on devices, update their listed order in the install command. ◦ Transforms- The order in which the system applies transforms is set when you assign the application. You see a placeholder name for the transform until you associate the transform during the assignment process. • **EXE and ZIP**- Populate the install command and specify the patch names and their order of application in the command. You must also enter the install command that triggers the installation of the Win32 application. If you do not package the patches and transforms in the EXE or ZIP file and you add them separately, ensure to add the patch filenames and the transform lookup text boxes in the install command.
Admin Privileges	Set the installation to bypass admin privilege requirements.
Device Restart	Require the device to restart after the application installs successfully, require the device to restart only if necessary for the application to function, or do not require the device to restart.
Retry Count	Enter the number of times the system attempts to install the application after an unsuccessful attempt.
Retry Interval	Enter the time, in minutes, the system waits when it tries to install the application after an unsuccessful attempt.
Install Timeout	Enter the maximum time, in minutes, the system allows the installation process to run without success.
Installer Reboot Exit Code	Enter the code the installer outputs to identify a reboot action. Review the entry for **Device Restart**. If you selected to **Do not restart** but you enter a reboot exit code, the system considers the installation a success after the reboot completes even though the Device Restart settings do not require a restart for success.
Installer Success Exit Code	Enter the code the installer outputs to identify a successful installation.

c. **When To Call Install Complete**

Configure Workspace ONE UEM to identify the successful installation of Win32 applications. The system requires this information for EXE and ZIP files.

Setting	Description
Use Additional Criteria	Configure the system to use specific criteria to recognize the completion of the installation process.
Identify Application By	To identify the installation completion or use custom scripts, add a specific criteria.
Defining Criteria	
Select **Add** to enter criteria to identify the installation is complete. These settings are the same as the data contingencies.	
Using Custom Script	
Script Type	Select the type of script.
Command to Run the Script	Enter the value that triggers the script.
Custom Script Type	Select **Upload** and navigate to the custom script file on the network.
Success Exit Code	Enter the code that the script outputs to identify the successful installation.

4. Select **Save & Assign** to configure flexible deployment options.

5. Select **Add Assignment** and complete the options.

Setting	Description
Select Assignment Groups	Type a smart group name to select the groups of devices to receive the assignment.
App Delivery Method	• **On Demand** – Deploys content to a catalog or other deployment agent and lets the device user decide if and when to install the content. This option is the best choice for content that is not critical to the organization. Allowing users to download the content when they want helps conserve bandwidth and limits unnecessary traffic. • **Automatic** – Deploys content to a catalog or other deployment agent on a device upon enrollment. After the device enrolls, the system prompts users to install the content on their devices. This option is the best choice for content that is critical to your organization and its mobile users.
Deployment Begins On	Set a day of the month and a time of day for the deployment to start. The **Priority** setting governs which deployments push first. Workspace ONE UEM then pushes deployments according to the **Effective** configuration. To set a beginning date with enough bandwidth for the successful deployment, consider the traffic patterns of your network.

Setting	Description
	Policies
DLP	Configure a device profile with a **Restrictions** profile to set data loss prevention policies for the application. Select **Configure**. The system navigates to **Devices > Profiles**. Select **Add > Add Profile** and the platform. For Windows Desktop, select **Device Profile > Restrictions** and enable options that apply to the data you want to protect.
Make App MDM Managed if User Installed	Assume management of Win32 applications. The system does not prompt users to allow or deny this action when you enable this feature. If a device is employee owned, this option does not work.
Application Transforms	Associate transform files to the Win32 applications. This setting replaces the placeholder transform name in the Install Command option.

6. Select **Add** and then **Save & Publish**.

For information about considerations and system behavior for setting **Make App MDM Managed if User Installed**, see Assume Management of Win32 Applications on page 56.

Win32 Application Installation Behavior

While configuring the Win32 applications in the Workspace ONE UEM console, you have different combinations that you can select while setting the **Install Context** and **Admin Privileges** under the **Deployment** tab. Your installation process can vary based on the settings.

It is a best practice to deploy Win 32 applications from **Apps & Books**. However, if you have tried deploying the application with **Apps & Books** and you are not able to meet your needs, as an alternative method you can complete the deployment onto your devices using **Product Provisioning**. For more information, see Win32_Application_Installation_Behavior_using_Product_Provisioning.

Note: Users do not receive User Account Control (UAC) prompts for all the applications that only require standard permissions.

Win32 Application Installation Behavior Using Apps & Books

Refer the table to understand Win 32 Application Installation Behavior for all the apps that require admin privileges.

Configuring Win32 Application from **Apps & Books**	Install Context **Settings** **In the Workspace ONE UEM console**	**User is an Admin**	**User is a standard user**
Navigate to**Apps & Books > Applications > Native > Internal** and select **Add Application**	Navigate to **Deployment options> How To Install** and set **Install Context = Device** **Admin Privileges = Yes** The settings indicate that the app is configured for all the users on each of your devices and the user account has an elevated access token to install the application.	With the Install Context set to **Device**, and the Admin Privileges set to **Yes** and if the user is an admin. The installation completes without any prompt.	With the Install Context set to **Device**, and the Admin Privileges set to **Yes** and if the user is a standard user, installation completes without any prompt.
Navigate to**Apps & Books > Applications > Native > Internal** and select **Add Application**	Navigate to **Deployment options> How To Install** and set **Install Context = Device** **Admin Privileges = No** The settings indicate that the app is configured for all the users on each of your devices and the user account need not have an elevated access token to install the application.	With the Install Context set to **Device**, and the Admin Privileges set to **No** and the user is an admin. The installation completes without any prompt.	With the Install Context set to **Device**, and the Admin Privileges set to **No** and the user is a standard user, installation completes without any prompt.
Navigate to**Apps & Books > Applications > Native > Internal** and select **Add Application**	Navigate to **Deployment options> How To Install** and set **Install Context = User** **Admin Privileges = Yes** The settings indicate that the app is configured for all the users on each of your devices and the user account has an elevated access token to install the application.	With the Install Context set to **User**, and the Admin Privileges set to **Yes** and the user is an admin. The installation completes without any prompt.	With the Install Context set to **User**, and the Admin Privileges set to **Yes** and the user is a standard user, installation fails.

Configuring Win32 Application from **Apps & Books**	Install Context **Settings** **In the Workspace ONE UEM console**	**User is an Admin**	**User is a standard user**
Navigate to**Apps & Books > Applications > Native > Internal** and select **Add Application**	Navigate to **Deployment options> How To Install** and set **Install Context = User** **Admin Privileges = No** The settings indicate that the app is configured for all the users on each of your devices and the user account need not have an elevated access token to install the application.	With the Install Context set to **User**, and the Admin Privileges set to **No** and the user is an admin. The installation completes with prompt.	With the Install Context set to **User**, and the Admin Privileges set to **No** and the user is a standard user, installation fails.

Win32 Application Installation Behavior Using Product Provisioning

It is a best practice to deploy Win 32 applications from **Apps & Books**. However, if you have tried deploying the application with **Apps & Books** and you are not able to meet your needs, as an alternative method you can complete the deployment onto your devices using **Product Provisioning**. To review the Win32 Application Installation Behavior using Apps & Books, see Win32_Application_Installation_Behavior_using_Apps_&_Books.

If you are configuring Win32 applications using product provisioning, you can use the following table to understand the combinations of **Install** and **Run** manifest and the context of the command. You can select install or run at the system level, user level, or admin account level. Based on the selections made, your installation can vary.

Refer the table to understand the Win32 Application Installation Behavior Using Product Provisioning

Configuring Win32 Application	**Install/ Run Settings** **in the Products Provisioning in the UEM console**	**User is an Admin**	**User is a standard user**
Navigate to **Devices > Staging & Provisioning > Components > Files/Actions and select Add Files/Actions**.	Navigate to**Manifest** tab and set **Action(s) To Perform** = Install/ Run **Execution Context = System**	With the **Action(s) To Perform** = Install/ Run and **Execution Context** = System and the user is an admin. The installation completes without any prompt.	With the **Action(s) To Perform** = Install/ Run **Execution Context** = System and the user is a standard user, installation completes without any prompt.

Configuring Win32 Application	Install/ Run Settings in the Products Provisioning in the UEM console	User is an Admin	User is a standard user
Navigate to **Devices > Staging & Provisioning > Components > Files/Actions and select Add Files/Actions**	Navigate to **Manifest** tab and set **Action(s) To Perform** = Install/ Run **Execution Context = Admin**	With the **Action(s) To Perform** = Install/ Run, **Execution Context** = Admin and the user is an admin. The installation completes without any prompt.	With the **Action(s) To Perform** = Install/ Run,**Execution Context** = Admin and the user is a standard user, installation completes with prompt.
Navigate to **Devices > Staging & Provisioning > Components > Files/Actions and select Add Files/Actions**	Navigate to **Manifest** tab and set **Action(s) To Perform = Install/ Run** **Execution Context = User**	With the Install Context **Action(s) To Perform** = Install/ Run, **Execution Context** = User and the user is an admin. The installation completes without any prompt.	With the **Action(s) To Perform** = Install/ Run,**Execution Context** = User and the user is a standard user, installation fails.

Considerations for Retry Count, Retry Interval, and Install Timeout Options

The values for **Retry Count**, **Retry Interval**, and **Install Timeout** options for Win32 applications affect the length the system takes to report a failed installation process. Consider changing the default values to decrease deployment times.

Default Values and Time to Installation Failure Reported

The default values for the options

- **Retry Count** - three times
- **Retry Interval** - five minutes
- **Install Timeout** - 60 minutes

work in the following sequence for a single failed installation process.

60 minute (one hour)	65 minutes (one hour and five r	125 minutes (two hours and five r	130 minutes (two hours and 10 r	190 minutes (three hours and 10 r	195 minutes (three hours 15 r
Win32 app fails to install and reaches install the timeout of 60 minutes.	System retries the installation (retry count #1) at a retry interval of 5 minutes.	Win32 app fails to install and reaches install timeout of 60 minutes.	System retries the installation (retry count #2) at a retry interval of 5 minutes.	Win32 app fails to install and reaches install the timeout of 60 minutes.	System retries the installation (retry count #3) at a retry interval of 5 minutes.

After 3 hours and 15 minutes, the system reports a single application installation as failed. Then, the system installs the next application.

Configure Options Depending on the Application

Configure values that compliment the application.

Fast Installation Example

A browser application installs on a device in four minutes. Consider setting these values for this application.

- Retry Count - two times
- Retry Interval - five minutes
- Install Timeout - five minutes

The system reports the failure of this application within 20 minutes. Then, it installs the next application.

Slow Installation Example

A large productivity application installs on a device in 30 minutes. Consider these values for these applications.

- Retry Count - three times
- Retry Interval - five minutes
- Install Timeout - 35 minutes

The system might report the failure of this application within 120 minutes. Then, it installs the next application.

For information on configuring **How To Install** settings for the software distribution application, see Configure, Assign, and Deploy Win32 Files on page 45.

Dependency Files in Software Distribution

Dependency files in the software distribution feature are applications that are necessary for a Win32 application to function. Examples include framework packages and libraries. Although you upload them like a file and you can view them in the List View, they have reduced features.

Dependency File Features

- Dependency file does not have assignments of their own. The applications to which they are associated give the dependency files their assignments.
- Every dependency file is a separate file and the system does not create versions for the file.
- The system cannot parse information from dependency files so you must enter details such as uninstallation processes.
- Dependency files have reduced options on the Deployment Options tab.
- You cannot associate patches or transforms to dependency files.

Delete Considerations

Before you delete a dependency, ensure that other applications are not associate to it. When you delete the dependency file, the system removes its association from all applications. Devices newly assigned to the application do not get the dependency. Deletion does not remove the dependency from devices that had the application previous to deletion.

Assume Management of Win32 Applications

The system to assume management of Win32 applications includes certain caveats to work. After you enable the option, the system acts in a specific order to complete the assuming management process.

Considerations

This feature works for devices that meet these caveats.

- Devices that enrolled or were assigned after you enabled this option and did not have the application installed.
- Devices that enrolled or were assigned after you enabled this option and did have the application installed with a status of user-installed.

This feature does not support the management assumption process on devices that meet these caveats.

- Devices that enrolled or were assigned before you enabled this option and have the application installed with a status of user-installed.
- Devices that are employee owned. If users have BYODs, you cannot assume management of Win32 applications on these devices.

System Behavior

If you enable **Make App MDM Managed if User Installed**, the management assumption process takes the listed actions.

1. Enable **Make App MDM Managed if User Installed** and publish the Win32 application.
2. VMware Workspace ONE UEM sends install commands to devices that enroll after publication.
3. The device responds that it received the command.
4. If the admin is trying to assume management of the application, the device processes the command by selecting

- Not assuming management - The application installs with the usual process.
- Assuming management - The system looks for the application on the device.
  - Application installed - The system re downloads and reinstall the application.

5. The device reports the status of the application as managed to the console.

If you disable the option and the user installs the application, the system marks the application as user-installed.

Inventory Win32 Applications with Tracking Features

Monitor your Win32 applications deployed through software distribution with the statistics on the Details View and by reviewing installation status codes.

Use the Details View of internal applications to view the progress and status of installations. See Track Internal Applications With Details View on page 36.

View the reasons in the Details View to track the progression of an installation. The reason codes help identify the status of an installation and if there is an issue with an installation, so that you can easily track and troubleshoot application deployments. Find descriptions for common reason codes in the topic Installation-Status Reason Code Descriptions on page 38.

Delete Win32 Files

AirWatch includes several methods to remove Win32 applications off devices.

Several admin functions impact multiple assets, so understand the changes before you proceed.

Method	Description
Details View	Select the **Delete Application** function in the details view of the application. This action removes the Win32 application off devices in smart groups assigned to the application.
Device	Delete the applicable device from the console.
Organization Group	Delete the organization group. This action impacts all assets and devices in the organization group.
Assignment Group	Delete the smart or user group assigned to the Win32 application. This action impacts every device in the group.
User	Delete the applicable user account from the console.

Patches in Software Distribution

Use patches to update and fix Win32 applications. Workspace ONE UEM supports additive and cumulative patches. In certain cases, a cumulative patch might trigger the system to create a version of an application.

Cumulative Patches and System Deployment Behavior

When you apply a cumulative patch by editing an application, the system creates a version of the application with the new patch applied. It makes the non-patched version inactive and creates and deploys the patched version of the application to devices.

Patch Restrictions

Workspace ONE UEM does not support patches that do not update the version, and the upgrade code must match the Win32 MSI application.

Peer Distribution for Win32 Applications

Workspace ONE UEM offers a peer distribution system to deploy Win32 applications to enterprise networks. Peer distribution can reduce the time to download large applications to multiple devices in deployments that use a branch office structure.

Win32 Distribution Challenge

In the default distribution process, software distribution, the Workspace ONE UEM console deploys Win32 applications from a secure file storage system or from a content delivery network (CDN). Win32 applications are large and it takes time for them to download to devices. The downloading of Win32 applications can also increase the traffic on communication channels. Multiple devices use the channel to retrieve the large application simultaneously from the CDN or file storage. This constant traffic can hamper the network availability needed for other critical applications.

Win32 Distribution Option - Peer Distribution

VMware Workspace ONE UEM partners with Adaptiva to offer the peer distribution system.

The peer distribution system works to reduce the traffic on networks and the time to install Win32 applications. Installation begins with a specific device in the office or subnet called the rendezvous point (RVP). This initial download takes time. However, installation times improve because devices are not taxing the storage system or the line of communication for the application package. Instead, devices receive the package from other devices in the network. The system also monitors the network for traffic. If the network is busy, installations pause until the network availability increases.

Environments That Benefit from Peer Distribution

Peer distribution benefits environments with specific characteristics.

- Offices in remote locations with the low bandwidth and with little means to increase the network bandwidth.
- Enterprises that use branch office hierarchies.
- Enterprises that have multiple branch offices that have many devices.

For required components of the peer distribution system, see Requirements for Peer-To-Peer Distribution on page 59.

Peer Distribution Component Roles

Peer distribution uses two main components: a peer-to-peer server and peer-to-peer clients.

- **Peer-to-peer server**
  - This component maintains the metadata of the Win32 applications but not the actual application packages. It also maintains information about clients, client IP addresses, the number of active clients, and the content presently at each client.

- This component resides in your network and it must communicate with these components.
  - VMware Enterprise Systems Connector

    You can install the server and the VMware Enterprise Systems Connector on the same machine.
  - SQL Database or SQL Server Express
  - Peer-to-peer clients on devices
- Download and install the server from the UEM console before you configure the peer distribution.

- **Peer-to-peer clients**
  - This component distributes application packages between peers, or devices, and it receives application metadata from the server. These clients use licenses you buy with the peer distribution feature.
  - This component resides on devices and it must communicate with these components:
    - Software distribution clients on devices
    - Peer-to-peer server
  - The peer distribution system automatically deploys clients to devices when you complete the peer distribution software setup. An installed peer-to-peer client uses one license.

- **Network Topology**
  - This component represents your network as offices in a hierarchy. It enables the peer distribution system to deploy applications more efficiently. It uses the hierarchy to control what clients get downloads and in what order. It uses devices called rendezvous points, or RVPs, as master clients in an office. The RVP receives downloads and disseminates the applications to peer clients.
  - This component is a spreadsheet that you upload to the UEMconsole. If you do not have a network topology, you can download the spreadsheet from the console and edit the topology initially identified by the peer distribution system.
  - Though this component is optional, it greatly improves efficiencies and download speeds.

Requirements for Peer-To-Peer Distribution

Peer distribution needs the listed components and configurations to work. Ensure that your Workspace ONE UEM deployment includes these requirements.

Supported Platforms and Application Types

- Windows Desktop (Windows 10)
- Win32 applications

Required Components

- **SQL** - Get SQL Server Express or see if your organization uses SQL Database. The peer-to-peer server uses SQL Database to store application metadata and information about the network topology. To download SQL Server Express, outbound port 443 must be open.

  Ensure that the peer-to-peer server can communicate with SQL Server Express or the organization's SQL Database.

- **VMware Enterprise Systems Connector** - Ensure that VMware Enterprise Systems Connector is enabled. This component ensures secure communication between your network and Workspace ONE UEM. Ensure that the **All Other Components** option is enabled in the VMware Enterprise Systems Connector configurations located in the console at **Groups & Settings > All Settings > Enterprise Integration > VMware Enterprise Systems Connector > Advanced > AirWatch UEM Services > All Other Components**.
- **Software Package Deployment** - Configure Workspace ONE UEM to recognize the deployment of application packages through the software distribution method. The software distribution client resides on devices to communicate with the peer-to-peer system and the Workspace ONE UEM console. Go to **Groups & Settings > All Settings > Device & Users > Windows > Windows Desktop > App Deployments** and enable **Software Package Deployment**.
- **File Storage (on-premises)** - Workspace ONE UEM stores Win32 applications on a secure file storage system. Peer-to-peer clients receive application packages from the storage system when clients cannot find other clients with the application package.

  See Workspace ONE UEM Reports on page 42 for more information and server requirements.

Peer-to-Peer Server Requirements

Ensure that the machine that houses the peer-to-peer server meets these requirements.

Component	Requirement
Operating system	Windows Server 2008+
Processor	Xeon Processor, single quad core
Memory allocation	• 0–5,000 clients - 2048 MB • 5,001 to 10,000 clients - 3072 MB • 10,001–19,999 clients - 5120 MB • 20,000–49,999 clients - 6144 MB • 50,000+ - 8192 MB

SQL Requirements

Service Account Permissions on the SQL Database

On the machine hosting the SQL Database instance or SQL Server Express, grant the entity Service Account Permissions SQL sysadmin server roles for the initial installation of the peer distribution system. The role is not needed for everyday operation of the peer distribution system.

Required Databases

- db_datareader
- db_datawriter
- db_ddladmin

Required Database Size

The database requires 200 KB per client.

Required Configurations for Deployment

The deployment of applications with the peer-to-peer distribution system requires you to set the listed configurations in the UEM console and on devices.

- Enable the software package deployment. See Requirements to Deploy Win32 Applications for Software Distribution on page 41.
- Configure the peer distribution software. See Configure Peer Distribution Software Setup on page 67.
- Install and activate peer-to-peer clients on devices. See Configure Peer Distribution Software Setup on page 67.
- Upload and publish applications to the peer-to-peer server. See Application Lifecycle for Software Distribution on page 44.

CDN for on-premises, Optional

On-premises deployments can use a content delivery network (CDN) as the backup delivery system instead of the file storage system. Workspace ONE UEM partners with a third-party vendor to offer a CDN for the on-premises environment at a cost. Workspace ONE UEM also integrates this CDN solution for SaaS environments.

This option has the advantage of sending the content to devices in the network and to remote devices. Whereas the peer distribution system with the file storage backup, sends content to only devices in the network. Although optional, a CDN offers increased download speeds and reduces bandwidth on Workspace ONE UEM servers. Find settings for this option in **Groups & Settings > All Settings > System > Enterprise Integration > CDN**.

Considerations for Peer Distribution

Understand the behavior of the network, the types of communication, the communication channels between components, and license management. To avoid possible issues, review the considerations

Important: Do not send confidential packages with the peer distribution. See the encryption section in this topic for information.

- **Common Network** - The peer-to-peer server, the VMware Enterprise Systems Connector, and the peer-to-peer clients must all communicate on the same network. If these system components are on subnets of your network and the subnets can communicate, then the feature can transfer applications. Clients that are not on the network cannot receive applications with the peer-to-peer distribution.
- **Encryption** - Communication between the peer-to-peer server and Workspace ONE UEM is encrypted. The communication is not encrypted between peer-to-peer clients in the network. This communication uses UDP but the package itself is not encrypted between clients. Although the system checks for tampered packages, a best practice is not to send confidential packages with the peer-to-peer distribution.
- **UDP** - The peer-to-peer server and client use UDP to communicate with Workspace ONE UEM.
- **Central Office** - The peer-to-peer server must reside in one of the subnets in the top-tiered Central Office.
- **License Overages** - The peer-to-peer system does not stop you from assigning more licenses than you have bought.

If you assign extra licenses, the system charges you for them.

To help gauge license usage, the ratio of client installation to the used license is one to one.

- **Open Ports** - The peer-to-peer client needs specific ports open to transfer metadata. Find out if your network management team has closed the required ports or has blocked broadcasting on these ports. If these ports are closed or do not allow broadcasting, contact your VMware Workspace ONE UEM representative about alternative ports. See Ports Used for Peer Distribution on page 62 for information.
- **Console, Client, and Server Versions** - You must deploy and use the supported version of the peer-to-peer client and the peer-to-peer server. Update the peer-to-peer server when the Workspace ONE UEM console includes an update to the peer-to-peer client. If the versions are not supported, the feature does not work.
- **SQL Server Express** - Download and install SQL Server Express on the same server that has the VMware Enterprise Systems Connector. Install this component before configuring peer-to-peer setup because it might take some time to complete its installation.
- **Application Metadata** - The peer-to-peer system stores and transmits the blob ID (or content ID), the application size, and the application hash. It does not store or transfer any other data.
- **Initial Downloads** - The first download in a peer distribution process takes the longest time. After the initial downloads and as more devices in the subnet receive the application, download times get faster.
- **Activation Processes** - After you save your configurations, the system activates the peer-to-peer server and clients with a license key. You can input your topology or use the one the network generates at activation. Also at the time of activation, the system publishes all the existing Win32 application content to the peer-to-peer server. From this point on, devices that belong to the peer distribution network begin to receive the application download.

Ports Used for Peer Distribution

The listed ports must be open so that the peer-to-peer clients can transfer metadata to the peer-to-peer server.

Note: If you have no group policies that block the creation of firewall policies, the peer distribution component installers create the necessary firewall rules.

Sending Component	Receiving Component	Protocol	Port	Description
Messaging from Client to Server				
Peer-to-peer clients	Peer-to-peer server	UDP	34322	After clients receive small messages, they acknowledge or reply to the server.
34323	Clients send small messages to the server.			
34331	Large replies from clients to the server using Foreground Protocol.			

Sending Component	Receiving Component	Protocol	Port	Description
34333	Clients send large messages to the server using Foreground Protocol.			
34339	Large replies from clients to the server using Background Protocol.			
34341	Clients send large messages to the server using Background Protocol.			
Messaging From Server to Client				
Peer-to-peer server	Peer-to-peer clients	UDP	34324	After the server receives small messages, it acknowledges or replies to clients.
34325	Server sends small messages to clients.			
34335	Large replies from the server to clients using Foreground Protocol.			
34337	Server sends large messages to clients using Foreground Protocol.			
34343	Large replies from the server to clients using Background Protocol.			
34345	Server sends large messages to clients using Background Protocol.			
Messaging from Client to Client				
Peer-to-peer clients	Peer-to-peer clients • Same office • Parent offices • Child offices	UDP	34324	After clients receive small messages from another client, acknowledgments and replies are sent to this port

Sending Component	Receiving Component	Protocol	Port	Description
34325	Clients send small messages to other clients			
34335	Large replies from clients to clients using Foreground Protocol.			
34337	Clients send large messages to other clients using Foreground Protocol.			
34343	Large replies from clients to clients using Background Protocol.			
34345	Clients send large messages to other clients using Background Protocol.			
Messaging Client to Client Broadcast				
Peer-to-peer clients	Peer-to-peer clients in the same subnet	UDP	34329	Clients broadcast requests to other clients
Data Transfer from Server to Client				
Peer-to-peer server	Peer-to-peer clients in the Central Office	UDP	34760	Server sends content to clients using Foreground Protocol.
Data Transfer from Client to Client				
Peer-to-peer clients	Peer-to-peer clients in the same office	UDP	34760	Clients send content to other clients in the same logical office using Foreground Protocol.
Peer-to-peer clients in child offices	34750	Clients send content to clients in child offices using Background Protocol.		
Data Transfer Control Ports				
Peer-to-peer clients	Peer-to-peer server	UDP	34545	Clients send a control signal to the server for any large transfer using Adaptive Protocol.
Peer-to-peer clients in the same office, in parent offices, and in child offices	34546	Clients send a control signal to other clients for any large transfer using Adaptive Protocol.		

Sending Component	Receiving Component	Protocol	Port	Description
Data Transfer between VESC, Server, and Database				
VMware Enterprise Systems Connector (VESC)	Peer-to-peer server	UDP	34323	VESC sends messages for activation, health checks, application metadata to the peer-to-peer server.
Peer-to-peer server	VESC	UDP	34320	Peer-to-peer server responds to requests from the VESC.

Data Transport Behaviors for Peer-To-Peer Networks

To plan for the distribution optimization in your peer-to-peer deployment, consider how data transfers within networks.

Offices and Subnets

Define an office with one or more subnets or subnet ranges connected over a local area network (LAN). Offices retrieve the content from their parent offices, and distribute them to their child offices.

Office Types

Peer distribution has three types of offices, and these office types share data in specific ways.

- **Default** - Defines a standard wired LAN. Clients attempt to the share content and they send broadcast discovery requests.
- **VPN** - Defines an office and subnet range allocated for clients connecting through VPN. Clients within a VPN office do not attempt to the share content, but they do send broadcast discovery requests.
- **WiFi** - Defines an office and subnet range allocated to clients connected over WiFi. Clients within a WiFi office share content, but they do not send broadcast discovery requests.

Note: If you have a physical office with a wired (default) subnet and a WiFi subnet, create an office for each network. Make the WiFi office a child of the wired office so that the WiFi network receives packages from the wired parent office.

Central Office and the Peer-to-Peer Server

The peer-to-peer server must reside in one of the subnets in the top-tiered Central Office. This placement makes it available to all clients in the hierarchy.

Data Transport in Offices

The system distributes content from a parent to child office once. This behavior limits data sent across wide area network (WAN) links.

Adaptive Protocol

The adaptive protocol is a proprietary protocol that monitors the length of edge router queues and sends data when queues are nearly empty. This protocol, implemented by an advanced kernel driver, removes the need to throttle the bandwidth when deploying applications with the peer distribution.

Within Offices

Data transport within offices uses the LAN, or Foreground protocol. The peer distribution system does not manage this protocol.

Between Offices

Data transport between offices uses the WAN, or Background protocol. This protocol is also called the Adaptive Protocol that protects the bandwidth availability on WAN links.

Between Subnets

Define subnets connected over a WAN link as separate offices. If offices are misconfigured, the LAN protocol might be used over a WAN link, causing saturation of the WAN.

Clients Receive Applications According to Ordered Criteria

The peer-to-peer system sends and receives applications according to many factors, including the available device space, device form factor, and operating system type. The download order follows these elections from top to bottom.

1. Devices with the largest actual free space
2. Devices that are identified as preferred, also called RVPs (rendezvous points)
3. Device chassis type (desktops are selected over laptops)
4. Device operating system type (servers are selected over work stations)
5. Devices with the longer system up-times
6. Devices with the largest usable free space

Backup Systems

Peer-to-peer clients receive application packages from a CDN or a file storage system when they cannot find packages within the hierarchy. A CDN, which is optional for on-premises deployments, offers increased download speed over the file storage system.

Plan for Distribution Optimization with a Network Hierarchy

Use the distribution optimization feature to control the sources of the application package. Download the spreadsheet from the Peer Distribution page and add offices, subnets, and IP ranges to represent your peer-to-peer network. Consider asking your network management team for their topology of the network.

During your planning, review the system behaviors outlined in Data Transport Behaviors for Peer-To-Peer Networks on page 65.

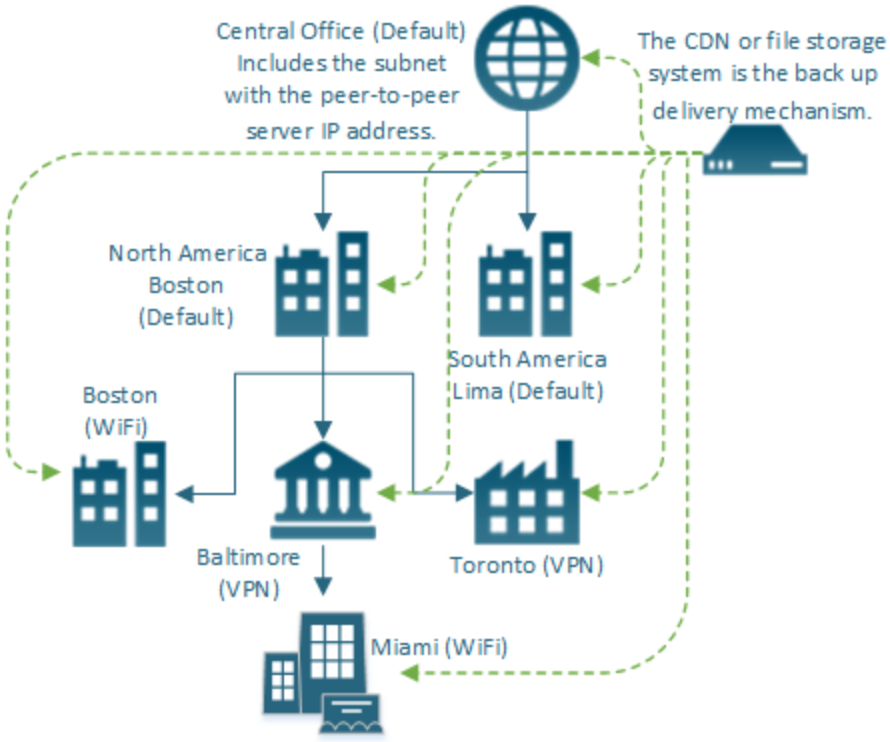
Disabling Distribution Optimization

When you do not use the distribution optimization, the peer distribution system assumes that every subnet receives one package download.

The system generates the default topology based on the clients that get registered with the server. One office location is created per subnet. When the clients in the office or subnet try to download a new piece of content, the system initiates one download per subnet.

Hierarchical Representation

Optimization works best if you represent your peer-to-peer network as a hierarchy. One example of a simple network topology is pictured.



In the example, the rendezvous point (RVP) in the central office sends the initial application package to Boston (Default) and Lima. Following the North American side, the RVPs in the Boston (WiFi), Baltimore, and Toronto offices receive the application package from the Boston (Default) office. The RVP in Miami receives the package from the Baltimore office. If a package is not available for any reason, offices receive it from the backup file storage system or content delivery network.

Configure Peer Distribution Software Setup

Enable the peer-to-peer distribution and download the peer-to-peer distribution server.

Important: Copy the shared key the peer-to-peer server installer displays. If you lose this key, you must install the server again and select to regenerate the key. You enter this shared key in the Workspace ONE UEM console.

1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Peer Distribution**.
2. Download the peer-to-peer server and install it, as the admin, in your network on the same server as the VMware Enterprise Systems Connector and the SQL database or SQL Server Express. Ensure to copy and save the shared key to enter to the UEM console.

   If you do not install the server on the same machine with the other components, then install the server in the secured network so that it can communicate with the other components and the clients after you distribute them.
3. After installing the peer-to-peer server, complete the rest of the options on the Peer Distribution page.

Setting	Description
Configuration	
Server Name/ IP	Enter the server name or IP address of the peer-to-peer server. If you put the server on the same machine as the VMware Enterprise Systems Connector, use that name or IP address.
Shared Authentication Key	Enter the key copied during the installation of the peer-to-peer server. This key activates trusted communication between the peer-to-peer server, the peer-to-peer clients, and the Workspace ONE UEM infrastructure. If you do not enter the most recent key generated, the system displays a key mismatch error.
Distribution Optimization	Enable this optional feature to upload a spreadsheet of your network topology. You can also download the topology for your network as recorded by the peer-to-peer system. Network topologies can be intricate. Before you enable this feature, speak with your network team about the company's network topology. If you disable this option, the system creates one office for each subnet of the registered clients. These offices are connected to the central office as children. There are benefits to this setting. • It helps control the initial download to preferred devices in a subnet. Preferred devices have a history of being available on the network and successfully downloading to other devices in their subnet. • It keeps IP ranges intact because split network ranges cause no-office clients and no-office clients do not get downloads from the peer-to-peer server. • It ensures downloads initiate on configured networks before defaulting to content delivery networks or file storage systems.
Assigned To Groups	Enter groups to receive applications with the peer-to-peer system.
Troubleshooting	
Server ID	Use this value when you talk to a Workspace ONE UEM representative about issues with the peer distribution system.
Health select	Validates that communication works between the peer-to-peer system and the Workspace ONE UEM infrastructure. It also validates that the current system is using the supported peer-to-peer client and server versions.
Publish Content.	Publishes every application in the system. This option helps to rebuild application deployments if there is a catastrophic incident.
Activated Licenses	**Download Activated Devices** is a report that lists the devices that have installed the peer-to-peer client and are currently using a license.

4. Save the settings and the system automatically deploys peer-to-peer clients to the devices in the groups entered on this page.

Once you complete the peer-to-peer server configuration, and save the settings, the Workspace ONE UEM server reaches to the Adaptiva cloud licensing server to get a license key. The license key is sent to the peer distribution server for activation.

The peer distribution server periodically connects to the Adaptiva cloud licensing server and sends the number of used licenses to receive a new token.

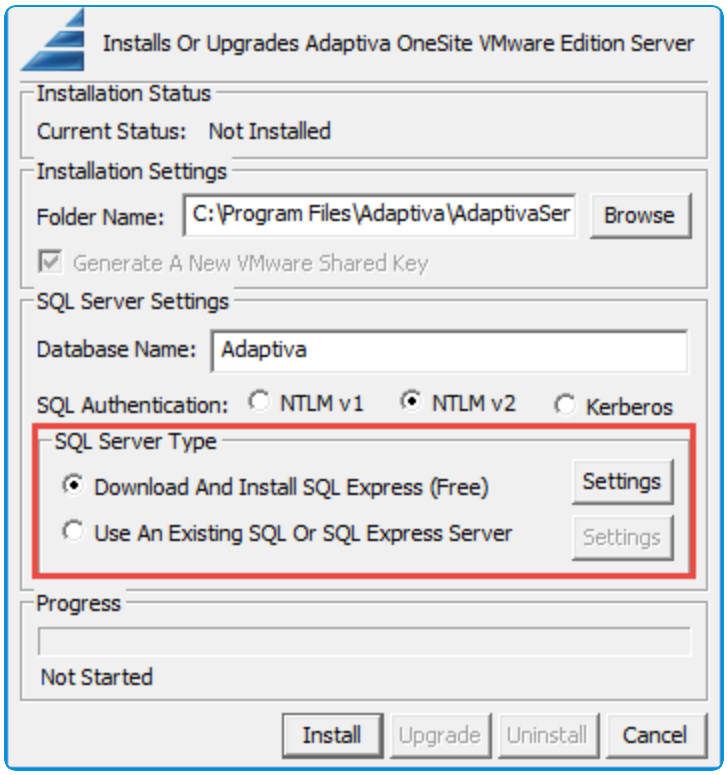
For more information on the Peer Distribution setup, configuration, and installation see Peer Distribution for Win32 Applications on page 58.

Install the Peer-to-Peer Server

Download the peer-to-peer server from the Peer Distribution page in the Workspace ONE UEM console. Follow the prompts in the installation wizard. For reference, the wizard includes the depicted instances.

1. Ensure the machine that hosts the peer-to-peer server meets the requirements listed in Requirements for Peer-To-Peer Distribution on page 59.
2. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Peer Distribution** and download the server.
3. Open the server installer executable.
4. Select a **SQL Server Type** and configure the **Settings**.
   - To download and use a new instance of SQL Server Express, configure where the wizard installs SQL Server Express.
   - To use an existing SQL Database or SQL Express Server, enter the SQL server and login information. Details include the name of the database server, the SQL instance name, the port of connection and the authentication

details.

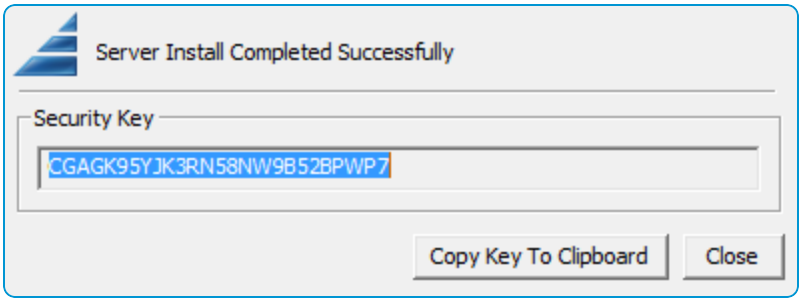


5. Select **Install**.

   The peer distribution server downloads and installs.

   If you downloaded a new instance of SQL Server Express, the server downloads and installs with the peer distribution server.

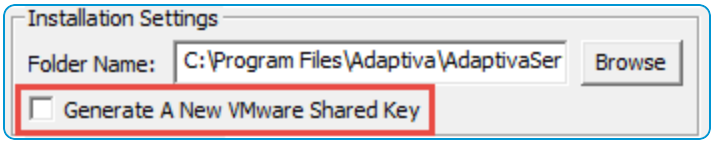
6. Copy the **Security Key** to enter in to the UEM console. Also, enter the name and IP address of the new.



Re-Run the Installer for a New Security Key

If you misplace the original one, you can generate a new key:

1. Rerun the installer.
2. Select the option **Generate a New VMware Shared Key** in the **Installations Settings** area.



3. Select **Upgrade**.

Firewall Rules Block SQL Server Express

If your firewall rules on the server block the free SQL Server Express download, install it manually.

1. Download SQL Server Express from http://redirect.adaptiva.cloud/sqlexpress2014 on a machine without firewall restrictions.
2. On the server machine, copy and extract the downloaded SQL Server Express setup in `c:\sqltemp`.
3. Enter the command-line parameter.

```
C:\sqltemp\Setup.exe /q /Hideconsole /ACTION=Install /IACCEPTSQLSERVERLICENSETERMS
/Features=SQLEngine /TCPENABLED=1 /BROWSERSVCSTARTUPTYPE=Automatic /AddCurrentUserAsSQLAdmin
/SQLSYSADMINACCOUNTS="NT AUTHORITY\LOCAL SERVICE" "NT AUTHORITY\SYSTEM" /SQLSVCACCOUNT="NT
AUTHORITY\SYSTEM" /SQLSVCSTARTUPTYPE=Automatic /INSTANCENAME=ADAPTIVASQL
```

   The system generates SQL setup logs in **%temp%**.

4. Run the peer-to-peer server installation wizard with the SQL Server Express.

Application Removal Protection

The application removal protection feature helps ensure that the system does not remove business-critical applications unless approved by the admin.

Internal applications are often developed to perform enterprise-specific tasks. Their abrupt removal can cause user frustration and halt work.

To prevent the removal of important internal applications, the feature holds removal commands according to threshold values. Until an admin acts on the held commands, the system does not remove internal applications.

General Steps for the Feature

Configure the feature with the outlined steps.

1. View default threshold values or edit the threshold values for the organization group.
   - If threshold values are met, Workspace ONE UEM holds the application removal commands and displays them by application in the **App Removal Log**.
   - Enter email addresses that receive notifications about the problem with the **App Remove Limit Reached Notification** template.
2. Act on the application removal commands held by the system.

- Purge application removal commands from the command queue by selecting **Dismiss**.
- Remove internal applications from devices by selecting **Release**, which sends application removal commands.

3. Assign those applications back to the desired smart groups if you dismissed the commands.

Application Removal Protection System Behaviors

To help set effective threshold values and to decide how best to handle held commands, review the behaviors of the protection system.

Triggers of Application Removal Commands

The system canvasses the application removal command queue for values that meet or exceed your threshold values. The listed actions trigger application removal commands.

- Edit smart groups
- Publish applications
- Deactivate applications
- Retire applications
- Delete applications

Configurations and Actions Apply to Bundle IDs

The system applies threshold values per bundle ID. It is possible for a single application to have varying names and still have the same bundle ID.

If this problem arises, the protection system selects one name to display in the log. However, the system applies admin commands to the bundle ID.

The System Follows Organization Group Hierarchies

The system sets default threshold values at a Customer type organization group. Child organization groups inherit these values.

> **Note:** Admins cannot override threshold values in child organization groups.

Admins' placement in the organization group hierarchy controls their available roles and actions. Admins in child organization groups can act on removal commands in their assigned organization groups. Admins in parent organization groups can edit values and act on removal commands in the parent group and in child organization groups.

Held Command Status Explanations

The command status the console displays in the application removal log represents the listed phase of the protection process.

Status	Description	Cause
Held for approval	The protection system holds removal commands, and the system does not remove the associated internal application. The removal commands are in the command queue but the system cannot process them without admin approval.	The system holds removal commands because the threshold values were met.
Released to device	The protection system sent the commands to remove applicable internal applications off devices.	The system released the commands because an admin configured the release.
Dismissed by admin	The protection system purged the removal commands from the command queue. The system did not remove applicable internal applications off devices.	The system purged the commands because an admin configured the dismissal.

Edit Threshold Values for Application Removal Protection

Use the default values or enter the limits that trigger the system to hold application removal commands. These actions stop the system from removing the associated internal applications off devices.

Select values that reflect the level of risk the enterprise tolerates if the system removes one critical application from a set of devices.

1. Configure the feature in an organization group at the customer level or below in the Workspace ONE UEM console.
2. Navigate to **Groups & Settings > All Settings > Apps > Workspace ONE > App Removal Protection**.
3. Complete the threshold options.

Setting	Description
Devices Affected	Enter the maximum amount of devices that can loose a critical application before the loss hinders the work of the enterprise.
Within (minutes)	Enter the maximum amount of minutes that the system sends removal commands before the loss of a critical application hinders devices from performing business tasks.
Email Template	Select an email notification template and make customizations. The system includes the **App Remove Limit Reached Notification** template, which is specific to app removal protection.
Send Email to	Enter email addresses to receive notifications about held removal commands so that the recipients can take actions in the app removal log.

4. Save the settings.

Act on Held Application Removal Commands

Use the App Removal Log page to continue to hold application removal commands, dismiss commands, or release the commands to devices.

1. Navigate to **Apps & Books > Application Settings > App Removal Log**.
2. Filter, sort, or browse to select data.

- Filter results by **Command Status** list applications.
- Sort by **Bundle ID** to select data.
- Select an application.
- You can select the **Impacted Device Count** link to browse the list of devices affected by actions. This action displays the **App Removal Log Devices** page that lists the device name of the devices. You can use the device name to navigate to the devices' **Details View**.

3. Select **Release** or **Dismiss**.
   - The **Release** option sends the commands to devices and the system removes the internal application off devices.
   - The **Dismiss** option purges the removal commands from the queue and the system does not remove the internal application off devices.
4. For dismissed commands, return to the internal applications area of the console and check the smart group assignments of the application for which you dismissed commands. Ensure that the internal application's smart group assignments are still valid.

   If the smart group assignment is invalid and you do not check it, the system might remove the application when the device checks-in with the system.

Safeguards for Proprietary, Non-Store, Workspace ONE UEM Applications

Workspace ONE UEM includes safeguards to prevent the removal of production versions of Workspace ONE UEM proprietary applications when you remove the test versions from the console. Add and remove the test version by following a specific task order.

Definition of Proprietary, Non-Store, Workspace ONE UEM Applications

A proprietary, non-store, Workspace ONE UEM application, like Secure Launcher, is seeded or included in the Workspace ONE UEM instance. It is part of the Workspace ONE UEM Installer and you deploy it to devices with a profile or with other settings in the console. Some enterprises want to test versions of these applications before they deploy them to production.

Considerations

Separate Testing Workspace ONE UEM console Instance and Test Groups

If possible, test applications in a separate environment with a testing instance of the UEM console.

Application ID

Workspace ONE UEM uses the application ID to identify the test version of the proprietary application.

Application Removal Commands

Remove the test version before you retire or delete the application. If you skip this step, Workspace ONE UEM does not queue application removal commands for these test applications.

Add Process of Test Applications

Add a test version of a proprietary Workspace ONE UEM application with these steps.

1. Use a test instance of the Workspace ONE UEM console.
2. Create a group of devices on which to deploy the test application in their own organization group.
3. Upload the test application to the **Internal** tab of **Apps & Books**, enter information you want, and select **Save & Assign**.
4. Assign the application to the test group with the **Add Assignment** option.

   The **App Delivery Method** for seeded applications is **On Demand** and is not configurable.

   You can also edit the application, select the **Devices** tab, and select the **Install On All** option.

Removal Process of Test Applications

Remove a test version of a proprietary Workspace ONE UEM application with these steps.

1. Go to the **Internal** tab in **Apps & Books** and edit the application.
2. On the **Devices** tab, select the **Remove From All** option.
3. Go to the **Details View** of the application on the **Internal** tab of **Apps & Books** and delete or retire the application from the actions menu.

Chapter 4:
Public Applications

Use Workspace ONE UEM to manage the deployment and maintenance of publicly available mobile applications from various app stores. Deploying public apps from the different app stores differs slightly between platforms. To get a better understanding on these differences and successfully deploying public apps to the platforms you support, you can read through the topics in this section.

Basics of Public Applications

Use the Workspace ONE UEM console to search for public applications in the available app stores. Once you find the app you want to provision, you can set the specific device assignments that determine who receives the app. For more information on this process, see Add Public Applications from an App Store on page 77.

To view the platforms and versions that are required to provision public applications, see Workspace ONE UEM Application Types and Their Supported Platforms on page 7.

If you use the Workspace ONE app catalog, then you can control access to public applications through either open or managed access. For more information, see Workspace ONE UEM Applications and Workspace ONE.

Features for iOS Public Applications

Paid Public Applications for iOS

In a typical deployment, you can deploy paid iOS apps after integrating with the Volumes Purchase Program (VPP). The VPP can manage bulk paid public apps efficiently and offers several management options. For more information on that setup, see Volume Purchase Program (VPP) in Workspace ONE UEM on page 96 .

In some scenarios, however, it is not feasible to use Apple's VPP. In this case, you can upload paid public applications for iOS devices using the same process as other apps. See Paid Public iOS Applications and Workspace ONE UEM on page 80 for more information on this process.

For information about uploading paid public iOS applications, see Enable and Upload Paid Public iOS Apps to the Console on page 81.

Read how to configure paid public applications for iOS at an optimal organization group in Organization Groups and Paid Public Applications on page 81.

Control Public Applications on iOS Devices

For iOS devices you can configure extra restrictions on App Store functionality, including the App Store icon and installation of public apps. For more information on these restrictions, see Apple iOS App Store Restriction Descriptions on page 82.

Integrations and Public Applications

Microsoft Store for Business

Microsoft's Microsoft Store for Business enables you to acquire, manage, and distribute applications in bulk. If you use Workspace ONE UEM to manage your Windows 10+ devices, you can integrate the two systems. After integration, acquire applications from the Microsoft Store for Business and distribute the applications and manage their updated versions with Workspace ONE UEM. For more information, reference the topics under the The Microsoft Store for Business and Workspace ONE UEM section.

Android for Work

Use Workspace ONE UEM to push Android for Work public applications to devices. This process includes adding and approving applications for integration between Workspace ONE UEM and Android for Work from the Google Play Store which can be accessed from the UEM console.

Add Public Applications from an App Store

Deploy public applications to devices with Workspace ONE or the AirWatch Catalog.

When you upload a public application, for some platforms you have the option enable managed access. For information about managed access and open access, see Workspace ONE UEM Applications and the Workspace ONE Managed Access Feature on page 200.

1. Navigate to **Apps & Books > Applications > Native > Public** and select **Add Application**.
2. View the organization group from which the application uploads in **Managed By**.
3. Select the **Platform**.
4. Find the application in an app store by entering a search keyword in the **Name** text box.
5. Select from where the system gets the application, either **Search App Store** or **Enter URL**.

Setting	Description
Search App Store	• **iOS** – Searches for the application in the app store. • **Windows Desktop and Phone** – Searches for the application. If you acquire applications this way and not with the Microsoft Store for Business. The system does not manage them. • **Android** – If you have configured integration with the Google Play Store, the system searches for the application in the app store. This configuration also works when integrating with the Android for Work system. See the **Workspace ONE UEM Integration with Android for Work** guide. **Add Google Play URL** – This option only displays for Android applications, and the system displays it because Google Play Stores are localized. The stores offer applications based on regions. This option enables you to deploy applications that are in a different region from your Workspace ONE UEM server.

Setting	Description
Enter URL	Adds the application using a URL for the application. If you add applications with this method, the system does not manage them.

6. Select **Next** and **Select** the desired application from the app store result page.

7. Configure options on the **Details** tab.

Setting	Description
Name	View the name of the application.
View in App Store	View the store record for the application where you can download it and get information about it.
Categories	Use categories to identify the use of the application. You can configure custom application categories or keep the application's pre-coded category.
Supported Models	Select all the device models that you want to run this application.
Is App Restricted to Silent Install **Android**	Assign this application to those Android devices that support the Android silent uninstallation feature. Workspace ONE UEM cannot silently install or uninstall public applications. However, you can control what applications you push to your Android standard devices or your Android enterprise devices. Android enterprise devices support silent activity.
Size **Apple iOS**	View the size of the application for storage.
Managed By	View the organization group (OG) that the application belongs to in your Workspace ONE UEM OG hierarchy.
Rating	View the number of stars that represents the popularity of the application in the Workspace ONE UEM console and in the AirWatch Catalog.
Comments	Enter comments that explain the purpose and use of the application for the organization.
Default Scheme **Apple iOS** **Windows Desktop** **Windows Phone**	Indicates the URL scheme for supported applications. The application is packaged with the scheme, so the system parses the scheme and displays the value in this text box. A default scheme offers many integration features for your applications. • Use the scheme to integrate with other platforms and Web applications. • Use the scheme to receive messages from other applications and to initiate specific requests. • Use the scheme to run the Apple iOS applications in the AirWatch Container.

8. Assign a **Required Terms of Use** for the application on the **Terms of Use** tab. This setting is optional.

   Terms of use state specifically how to use the application. They make expectations clear to end users. When the application pushes to devices, users view the terms of use page that they must accept to use the application. If users do not accept the terms of use, they cannot access the application.

9. Select the **SDK** tab and assign the default or custom **SDK Profile** and an **Application Profile** to the application. SDK profiles apply advanced application management features to applications.
10. Select **Save & Assign** to configure flexible deployment options for the application.

Application configurations are vendor-specific key-value pairs you can deploy with an application to preconfigure the application for users. For resources about application configurations, see Application Configuration Information on page 9.

Assign the Application

To assign and deploy public applications, configure the flexible deployment options explained in Add Assignments and Exclusions to Applications on page 30.

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.

Migrate Your User Group Exceptions to the Flexible Deployment Feature

AirWatch offers a migration process to move your user groups configured with assignment exceptions for public applications to the flexible deployment feature.

Reason For Migration

Public applications now use the flexible deployment feature to assign applications to devices. The flexible deployment system does not include exceptions. In the past, you used exceptions to deploy public applications to special user groups with a specified device ownership type.

Flexible deployments replace exceptions and the system gives you additional control of deployments. The feature enables you to assign deployments to smart groups, to assign multiple deployments for an application, and to prioritize those deployments.

Migration Process

To use the migration wizard:

1. Navigate to **Apps & Books > Applications > Native > Public**.
2. Edit an application that you know had exceptions.
3. Select **Assign**.

The system displays a warning message prompting you to migrate your exceptions.

4. Select **Migrate** and complete the wizard.

For information on flexible deployment, see Use Flexible Deployment to Assign Applications on page 30.

Paid Public iOS Applications and Workspace ONE UEM

Workspace ONE UEM allows you to upload paid public iOS applications and distribute them in those scenarios where it is not feasible to use Apple's Volume Purchase Program (VPP). Workspace ONE UEM can distribute several OS versions, but iOS 9+ management does not require users to take extra steps.

It is best to use the Apple VPP, if possible. The VPP can manage bulk public paid applications efficiently and offers several management options.

Compare Paid Public App Procedures

When you compare the steps necessary to push paid public iOS applications to devices, iOS has simplified the process. It allows Workspace ONE UEM to take management of an application previously installed on a device, and end users do not have to delete applications.

Note: Workspace ONE UEM cannot assume management of user-installed applications on iOS 8 and below.

Any Supported iOS Version

1. Enable the paid public iOS applications process in the Workspace ONE UEM console.
2. Add the public application to the UEM console. Add any other management parameters like SDK features and enabling per-app VPN.
3. (User) Purchase the application. If the device user does not purchase the application, the application installation from the AirWatch Catalog fails.

   Apple installs the application automatically to the device after purchase.
4. **(User) Delete the application installed by Apple.**
5. (User) Open the AirWatch Catalog and initiate the installation from Workspace ONE UEM to receive the managed version of the application.

iOS 9+

1. Enable the paid public iOS applications process in the UEM console.
2. Add the public application to the UEM console and enable **Make App MDM Managed if User Installed** on the **Deployment** tab.

   Add any other management parameters like SDK features and enabling per-app VPN.
3. (User) Purchase the application.

   Apple installs the application automatically to the device after purchase.

4. (User) Open the AirWatch Catalog and initiate the installation from Workspace ONE UEM to receive the managed version of the application.

Organization Groups and Paid Public Applications

Keep your VPP deployment and your paid public iOS applications in separate organization groups. Enable the paid public status option in an organization group where applicable devices are enrolled.

Use the VPP When It Is Available

Do not deploy the same paid public iOS applications in an organization group that has VPP configured and that contains a service token (sToken). If you have the VPP configured in the organization group, use licenses from the sToken, which offers greater management and control of the application.

Enable Paid Public Applications Near or Where Devices Are Enrolled

Devices receive application assignments from the closest organization group to them. Be aware of the organization group hierarchy and where you enable paid public iOS applications. If you assign the application in an organization group that has no effect on the device, installations can fail or the application can install on the wrong device.

Organization Group	Paid Public Status	Device Enrolled	Result
Parent	Enabled	No	The device does **not** receive the managed paid public application and the system redirects the device to the store to install the application.
Child	Disabled	Yes	

Enable and Upload Paid Public iOS Apps to the Console

Enable the deployment of paid public iOS applications in the Workspace ONE UEM console. Then upload the paid public iOS application from the app store to the UEM console to make it available in the AirWatch Catalog.

Enable Process

1. Navigate to **Groups & Settings > All Settings > Apps > Workspace ONE > Paid Public Applications**.
2. Select **Enabled**, and then save the settings.

Upload Process

1. Navigate to **Apps & Books > Applications > Native > Public**, and select **Add Application**.
2. Select **Managed By** to view the organization group from which the application uploads.
3. Select the **Platform**.
4. Enter a keyword in the **Name** text box to find the application in the app store.
5. Select **Next** and use **Select** to pick the application from the app store result page.
6. Configure options on the **Details** tab. Entering data on this tab is optional, but you can record data like the store URL for the application, supported models, and associated categories.
7. Assign a **Required Terms of Use** for the application on the **Terms of Use** tab. This is optional.
8. Select **Save & Assign** to make the application available to end users.

9. Configure flexible deployment rules for the assignment of the applications.

   Only the on-demand push mode is available. It enables the user to initiate installation so that the system does not use excessive bandwidth by automatically installing applications. It also gives the user time to buy the application and delete the initial version from the device.

Public Application Installation Control on iOS Devices

The restriction **Allow App Store on Home screen** allows you to control the installation of free public applications on iOS 9+ devices without having to enable any other restriction in Workspace ONE UEM.

This option is native to the operating system version so it is the best restriction of this type available for iOS 9+ devices that are supervised.

Apple iOS App Store Restriction Descriptions

You control the app store to restrict or allow device users to access the public applications available therein. Workspace ONE UEM supports native iOS restrictions and an in-house developed restriction that control access the app store.

Find out if you can set the **Allow App Store icon on Home screen** as the restriction for your deployment.

Restriction	Supported Device Supervision Status	Configuration	Description
Allow App Store icon on Home screen The best option for iOS 9+ devices because it uses the latest technologies and can push applications through several systems.	Supervised	Disable	Restrict the Apple App Store from being installed on the device so the device user cannot install public free applications using the App Store. However, push public free applications using Workspace ONE UEM, iTunes, or Apple Configurator.
Enable	Allow the Apple App Store on the device and the device user can install any public free applications using the App Store.		
Allow installing public apps An option for many iOS versions but does not offer the ability to select the system that restricts the installation of non-enterprise applications.	Supervised Unsupervised	Disable	Restrict the device user from using the Apple App Store.

Restriction	Supported Device Supervision Status	Configuration	Description
Enable	Allow the Apple App Store on the device and the device user can install any public free applications using the App Store.	Disable	Allow the Apple App Store on the device and the device user can install any public free application using the App Store.
Restricted Mode for Public iOS Applications Workspace ONE UEM developed ways to allow the installation of enterprise-approved free public applications when this option is enabled. When you configure this option, you do not need to configure and apply a restriction profile with **Allow installing public apps**.	Supervised Unsupervised		
Enable	Block the device from installing free public applications from the Apple App Store. Push free public applications using Workspace ONE UEM.		

Configure the Apple App Store Restriction

Configure the **Allow App Store icon on home screen** restriction in Workspace ONE UEM to allow device users to acquire public applications from the App Store. This restriction works for iOS 9+ devices.

1. Navigate to **Devices > Profiles > List View > Add**. Select **Apple iOS**.
2. Configure the **General** settings of the profile.
3. Select **Allow App Store icon on Home screen** located in the **Device Functionality** section of the **Restrictions** payload, to allow the device to install public free applications from the app store.
4. Select **Save & Publish** to push the profile to devices.

Enable Restricted Mode for Free Public iOS Applications Older Than iOS 9

You can control from where end users install public applications by enabling **Restricted Mode** on Apple iOS devices. After enrollment, end users can access free public applications deployed to their catalogs, but they are unable to download free public applications from the App Store.

This restriction is the same as the iOS restriction found in **Devices > Profiles**, labeled **Allow installing public apps**.Workspace ONE UEM deploys the **Restricted Mode** option to devices and it blocks end users from the app store. Workspace ONE UEM can deploy the public applications, which ensure that your organization approves them.

Enabling Restricted Mode

This option restricts the device by allowing you to install only the assigned applications approved by the organization. Enabling the setting automatically sends a restricted profile to Apple iOS devices. The presence of this restricted profile does not require an extra restriction profile with the **Allow installing public apps** option enabled to block the app store.

To enable Restricted Mode for Apple iOS Applications, follow the steps.

1. Navigate to **Groups & Settings > All Settings > Apps > Workspace ONE > App Restrictions**.
2. Enable **Restricted Mode for Public iOS Applications**.

The Microsoft Store for Business and Workspace ONE UEM

Microsoft's Microsoft Store for Business enables you to acquire, manage, and distribute applications in bulk. If you use Workspace ONE UEM to manage your Windows 10+ devices, you can integrate the two systems. After integration, acquire applications from the Microsoft Store for Business and distribute the applications and manage their updated versions with Workspace ONE UEM.

This topic explains how to deploy acquired apps using Workspace ONE UEM. For information on Microsoft Store for Business processes, refer to https://technet.microsoft.com/itpro/windows/manage/windows-store-for-business.

Disclaimer

Third-party URLs are subject to changes beyond the control of VMware Workspace ONE UEM. If you find a URL in VMware Workspace ONE UEM documentation that is out of date, submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Requirements for Microsoft Store for Business Integration

Workspace ONE UEM integrates with the Microsoft Store for Business. It supports the offline and online licensing models with Windows 10+ devices that communicate with your Azure Active Directory services.

For successful integration, use the listed components in your environment.

Offline and Online License Model Requirements

- **Windows 10+ Devices**

  Deploy to Windows 10+ devices because they are compatible with the bulk-acquirement and application deployment processes.

  Use the Windows Desktop or Windows Phone platforms when assigning applications.

  You can deploy applications acquired through the bulk purchase process to older devices, like Windows 8 devices. The devices receive applications from Workspace ONE UEM through the regular process, and the system does not manage these applications.

- **Azure Active Directory Services**

Configure Azure Active Directory services in Workspace ONE UEM to enable the communication between the systems. This configuration enables Workspace ONE UEM to manage Windows devices and applications on these devices.

You do not need an Azure AD Premium account to integrate with the Microsoft Store for Business. This integration is a separate process from the automatic MDM enrollment.

Important: Integration only works when you configure it in the same organization group where you configured Azure Active Directory Services.

- **Microsoft Store for Business Admin Account with Global Permissions**

  Acquire applications with a Microsoft Store for Business admin account. Global permissions enable admins to access all systems to acquire, manage, and distribute applications.

Online License Model Requirements

Azure Active Directory

Device users must use Azure Active Directory to authenticate to content.

Offline License Model Requirements

File Storage Enabled for on-premises

Workspace ONE UEM stores Microsoft Store for Business applications on a secure file storage system. On-premise environments must enable this feature in the Workspace ONE UEM console by adding the tenant identifier and tenant name on the Directory Services page. This requirement is part of the process to configure Azure AD Services.

Compare Features of the Online and Offline Models of the Microsoft Store for Business

Workspace ONE UEM integrates with both the online and offline models in the Microsoft Store for Business. Compare available features to see which model benefits your application management needs.

Feature	Online License Model	Offline License Model
Different Capabilities		
License control	Licenses managed by the Microsoft Store for Business. Users can receive applications and claim licenses outside of your Workspace ONE UEM deployment.	Licenses managed by the enterprise. Use the offline licensing model to control application packages and updates. This model offers flexibility but requires attention to ensure that applications stay updated and licenses get renewed.
App package host	App package hosted by the Microsoft Store for Business.	App package hosted by the Workspace ONE UEM file storage for on-premises or in the Workspace ONE UEM SaaS environment.

Feature	Online License Model	Offline License Model
Azure Active Directory	Devices must use your Azure Active Directory system to authenticate. Enable the Azure Active Directory system so Workspace ONE UEM and the Microsoft Store for Business can communicate.	Devices do not have to use the Azure Active Directory system to authenticate. However, you must enable the Azure Active Directory system so Workspace ONE UEM and the Microsoft Store for Business can communicate.
Restrict the app store	Devices cannot install applications because the restriction prevents the Microsoft Store for Business on the device.	Devices can still install applications because the app packages are hosted in the Workspace ONE UEM environment.
Same Capabilities		
Level where licenses are claimed	Licenses claimed by Workspace ONE UEM for the application at the user level.	Licenses claimed by Workspace ONE UEM for the application at the user level.
License reuse	Admins can revoke licenses through Workspace ONE UEM and reuse them.	Admins can revoke licenses through Workspace ONE UEM and reuse them.

Configure Azure AD Identity Services Integration

Before you can use Azure AD to enroll your Windows devices, you must configure Workspace ONE UEM to use Azure AD as an Identity Service. Enabling Azure AD is a two-step process which requires the MDM-enrollment details to be added to Azure.

Prerequisites

You must have a Premium Azure AD P1 or P2 subscription to integrate Azure AD with Workspace ONE UEM. Azure AD integration with Workspace ONE UEM must be configured at the tenant where Active Directory (such as LDAP) is configured.

Important: If you are setting the **Current Setting** to **Override** on the Directory Services system settings page, the LDAP settings must be configured and saved before enabling Azure AD for Identity Services.

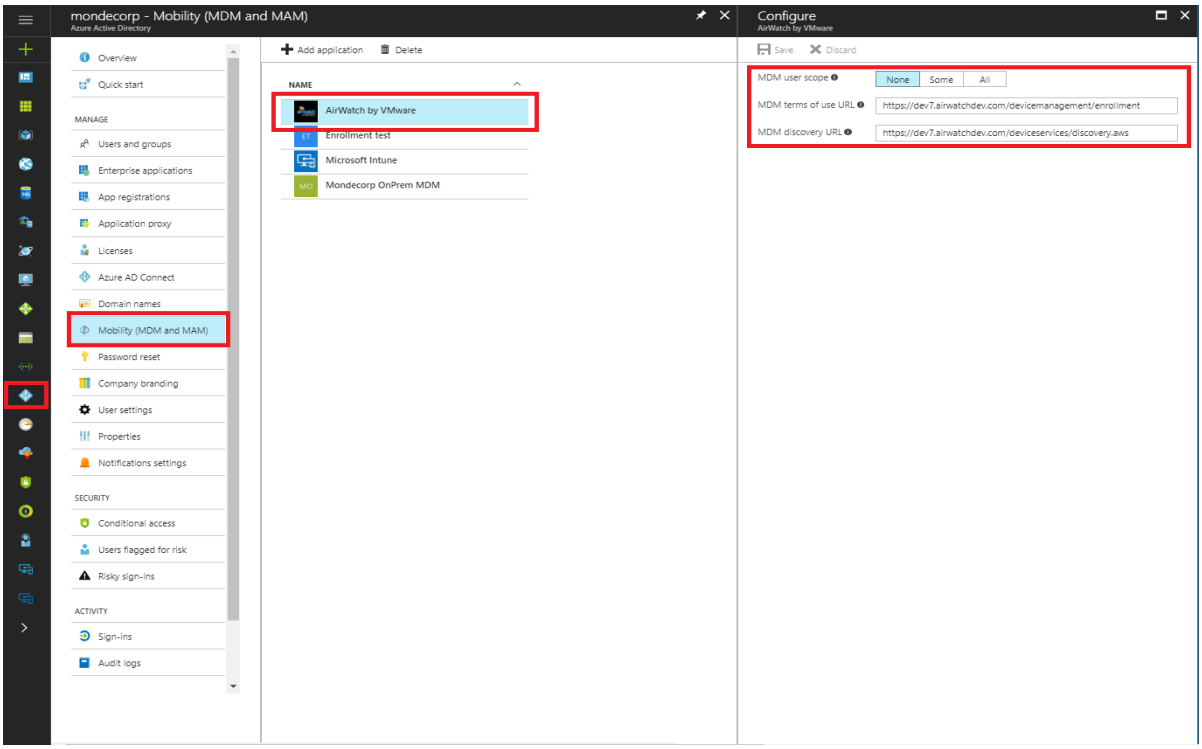
Procedure

To Configure Azure AD for Identity Services:

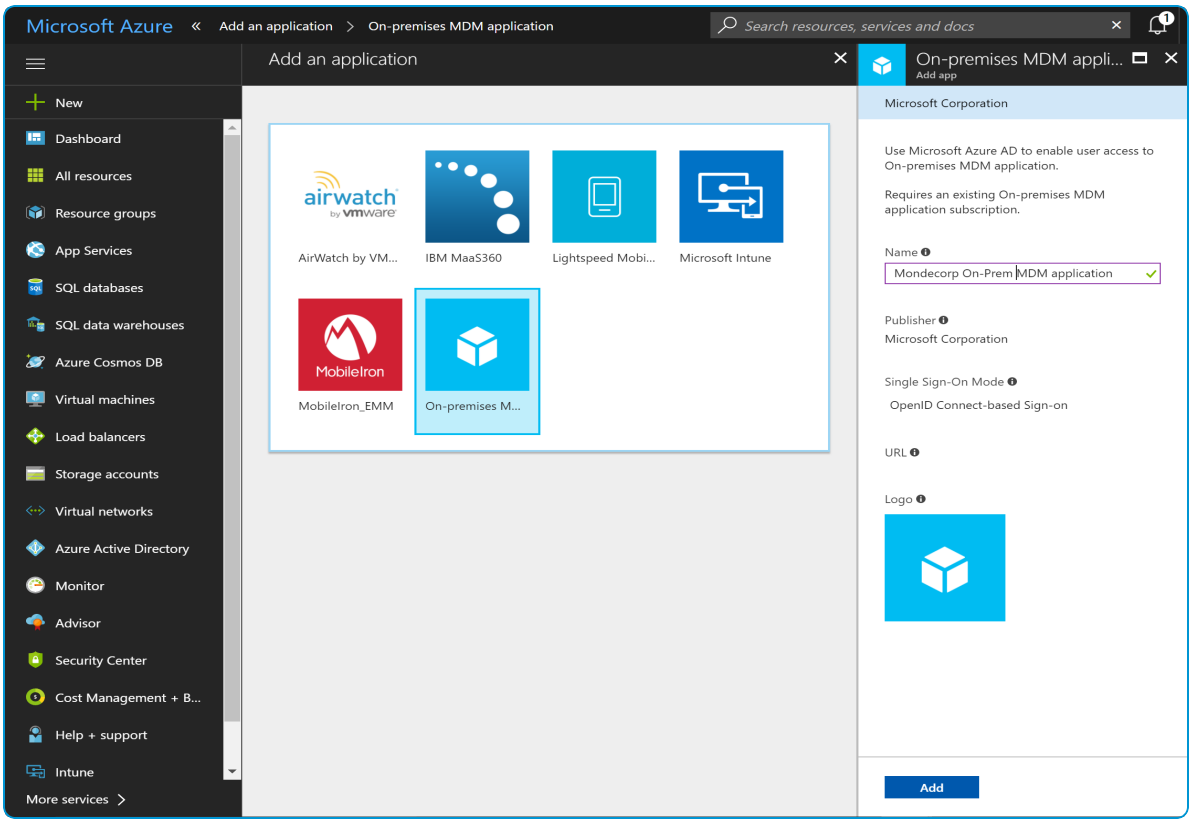
1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services**.
2. Enable **Use Azure AD for Identity Services** under **Advanced** settings.

   Once enabled, take note of the MDM Enrollment and MDM Terms of Use URLs as they are needed when configuring the Azure directory.
3. Log in to the Azure Management Portal with your Microsoft account or organizational account.
4. Select your directory and navigate to the **Mobility (MDM and MAM)** tab. This tab was formerly the Applications tab.
5. Select **Add Application** and select the AirWatch by VMware application.

You can use the default URLs if the user scope is set to none. If needed, you can also use placeholder URLs.



6. Leave the AirWatch by VMware application on the default settings. Change the **MDM user scope** to **None**.

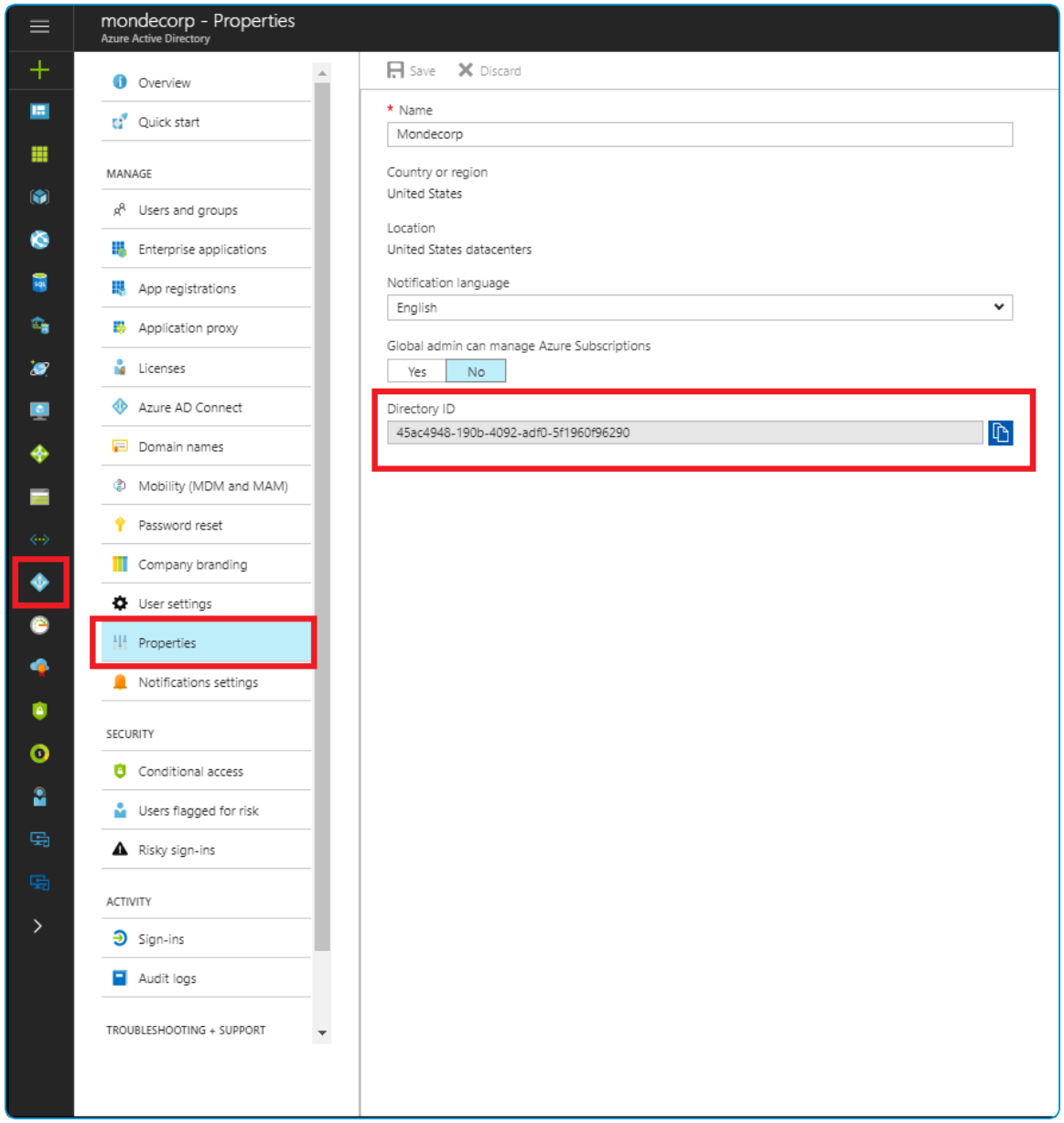


7. Select **Add Application** again and select the **On Premises MDM application**. You can rename the application when you add it.
8. Configure the On-Premises MDM application by entering the **MDM Enrollment URL** and **MDM Terms of Use** URLs from the Workspace ONE UEM Console.
9. Select **On-premises MDM application settings** then select **Required Permissions > Windows Azure Active Directory**.
10. Change the Permissions as follows:
    - Application Permissions
        - Select **Read and write directory data**.
        - Select **Read and write devices**.
    - Delegated Permissions
        - Select **Access the directory as the signed-in user**.
        - Select **Read directory data**.
        - Select **Sign in and read user profile**.
11. Select the Properties settings and enter your device services host in the **APP ID URI** text box.

    Use the same host that you used in the **MDM Enrollment URL** and **MDM Terms of Use** text boxes.

    Example format: https:// <MDM DS SERVER>
12. Set **MDM user scope** to **All** to apply these settings to all users.

    You can also limit the OOBE enrollment to selected Azure AD groups by selecting **Some** and adding the preferred groups.
13. Select **Save** to continue.
14. Navigate to the Properties tab and find the Azure Directory ID. This setting was formerly called the **Tenant ID**.



15. Select **User Account Details** in the top right corner.
    The Azure **Tenant Name** is the name of your Azure Directory. You can find the name under the **Domain** tab.
16. Return to the UEM Console and select **Use Azure AD for Identity Services** to configure Azure AD Integration.
17. Enter the **Azure Directory ID** as the **Tenant Identifier**. Enter the default domain as your Azure Directory **Tenant Name**.
18. Select **Save** to finish the process.

Sign up and Acquire Applications From the Microsoft Store for Business for Offline and Online Licensing

For integration to work, use an Azure admin account to sign up with the store and to activate the VMware Workspace ONE UEM management tool.

See the Microsoft Store for Business portal for the most current documentation on creating an Azure admin account.

Create an Azure Admin Account for VMware Workspace ONE UEM

Configure an admin account with global admin roles in your Default Directory in Microsoft Azure. Use this account to acquire applications in the Microsoft Store for Business. You do not need an Azure premium account to create an admin account for the Microsoft Store for Business.

1. In Azure, navigate to your Azure Active Directory.
2. Select **Users and groups** and **+ New user**.

   Complete applicable fields.
3. Configure the **Directory role** as **Global administrator**.
4. Create a temporary password so you can log in to the Microsoft Store for Business.

Activate VMware Workspace ONE UEM in the Microsoft Store for Business and Acquire Apps

Activate the Workspace ONE UEM management tool in the Microsoft Store for Business with your Azure admin account credentials. If you use offline licensing, enable the acquirement of offline license applications.

1. Navigate to the Microsoft Store for Business and log in with your Azure admin account.
2. Navigate to **Manage> Settings > Distribute > Management tools** and activate the Workspace ONE UEM by VMware tool.
3. For offline licenses, go to **Manage> Settings > Shop > Shopping experience** and enable **Show offline licensed apps to people shopping in the store**.
4. In the Store for Business, add applications to your inventory. You can add applications with either offline or online licenses depending on your license management strategy.

Import Microsoft Store for Business Apps

Import public applications acquired from the Microsoft Store for Business to the Workspace ONE UEM console. The process is the same for the online and offline license models.

For the offline license model, plan to import these applications when your corporate network is not busy. Due to the number of applications concerned, the import process can use more bandwidth than other Workspace ONE UEM systems.

1. Go to the organization group where you set your Azure Active Directory services.
2. Navigate to **Apps & Books > Applications > Native > Public** and select **Add Application**.
3. Select the **Platform**, Windows Desktop or Windows Phone.
4. Select **Import from BSP** and choose **Next**.
5. View a list of the applications that Workspace ONE UEM imports from your Microsoft Store for Business account.

   You cannot edit this list in the UEM console.
6. Select **Finish**.

- Offline license model - The system downloads applications to the remote file storage system.
- Online license model - The system stores the applications in the Microsoft Store for Business and awaits an install command.

Package Downloads and Updates for the Offline License Model

Workspace ONE UEM imports all the application packages and disables assignment actions while the process is in progress. When you reimport packages for purposes such as updates, Workspace ONE UEM downloads only those packages that changed.

If you do not restrict the use of the app store on devices, then application updates push to devices from the Microsoft Store for Business.

If you restrict the use of the app store on devices, then import updated applications in Workspace ONE UEM. Then, notify device users to install the updated version from the AirWatch Catalog.

Deploy Microsoft Store for Business Apps

Assign public applications imported from the Microsoft Store for Business to apply them to devices with the flexible deployment feature. Assign online and offline licenses depending on your license management strategy.

For general information about the flexible deployment feature, how to prioritize assignments, and for setting descriptions, see Use Flexible Deployment to Assign Applications on page 30.

1. Navigate to **Apps & Books > Applications > Native > Public**.
2. Select the application and choose **Assign**.
3. Complete the **Add Assignment** options to add a rule.

Setting	Description
Assignment	
Online Licenses	Assign groups to the application with online licenses. If devices are part of your Azure Active Directory system and your deployment has online licenses available, devices receive the application. If you assign both online and offline licenses to the group, the system gives preference to online licenses.
Offline Licenses	Assign groups to the application with offline licenses. If your deployment has offline licenses available, devices receive the application. If you assign both online and offline licenses to the group, the system gives preference to online licenses.
Deployment	
App Delivery Method	View the delivery method. On demand deploys content to a deployment agent and lets the device user decide if and when to install the content.

Setting	Description
DLP	Configure a device profile with a **Restrictions** profile to set data loss prevention policies for the application. Select **Configure**. The system navigates to **Devices > Profiles**. Select **Add > Add Profile** and the platform. • For Windows Desktop, select **Device Profile > Restrictions** and enable options that apply to the data you want to protect. • For Windows Phone, select **Restrictions** and enable options that apply to the data you want to protect.

4. Select **Add** and prioritize assignments if you have more than one assignment rule.
5. Deploy the application with **Save & Publish**.

Sync and Reclaim Licenses for Microsoft Store for Business Apps

Sync offline and online licenses with the details view of the application, and view the corresponding users of the licenses. For any reclaims, reassign the licenses.

Sync Licenses to View Users and Claimed Licenses

When you assign Microsoft Store for Business applications to devices, the assignment process claims corresponding licenses before the system initiates the installation of the application. Use the details view to see the list of user devices and the associated, claimed license.

Navigate to **Apps & Books > Applications > List View > Public** and select the Microsoft Store for the Business application. This action displays the details view. In this view, use the **Sync License** action to import the list of users that correspond to claimed licenses. To see the claimed licenses, select the **Licenses** tab.

Note: Workspace ONE UEM also imports the license associations when you select the **Import from BSP** option upon the initial import of your Microsoft Store for Business applications. This sync is performed asynchronous to the application package sync.

Reclaim Licenses

You can reclaim and reuse the licenses displayed on the **Licenses** tab by deleting the assignment of the application to the user's device. Workspace ONE UEM includes several methods to delete assignments. Deletion results in the removal of the application from the device.

Method	Description
Details View	Select the **Delete Application** function in the details view of the application. This action removes the application off devices in groups assigned to the application.
Device	Delete the applicable device from the console.
Organization Group	Delete the organization group. This action impacts all assets and devices in the organization group.

Method	Description
Assignment Group	Delete the smart or user group assigned to the application. This action impacts every device in the group.
User	Delete the applicable user account from the console.

Chapter 5: Purchased Applications -Apple VPP Feature

To distribute public applications and custom business to business (B2B) applications to large deployments of Apple iOS and macOS devices, integrate Apple's Volume Purchase Program (VPP) and Workspace ONE UEM.

The Apple VPP enables organizations to purchase publicly available applications for distribution. Any paid application from the App Store is available for purchase, in volume, at the existing App Store price. Custom B2B applications can be free or purchased at a price set by the developer. If your organization uses free public applications collected through the Apple VPP, Workspace ONE UEM can distribute these applications, as well.

See the **Volume Purchase Program for Business**and the **Volume Purchase Program for Education** on the Apple website for availability by country and other details.

Basics of Purchased Applications

For a general overview of the steps to buy applications from Apple and to add and deploy VPP applications to the console, see Deploy VPP Process on page 97.

Apple offers several methods to deploy VPP applications. The operating system, the type of content, and the method of deployment are related. For a matrix outlining which VPP deployment methods are available by content type and operating system version, see Supported Content for Purchased Applications on page 98.

VPP Application Deployment Methods

Managed Distribution by Device Serial Number

If your VPP deployment consists of iOS 9+ or macOS 10.11+ devices, you can assign VPP applications by device serial number. This method offers management benefits including not having to manage Apple IDs and the ability to reuse licenses. See Managed Distribution by Device Serial Number on page 123 for more information.

For information on enabling automatic updates for device-based VPP applications, see Update Device-Based VPP Applications Manually or Automatically on page 124 and Update Challenge for Device-Based VPP Applications on page 126.

Managed Distribution by Apple IDs

The managed distribution model by Apple IDs uses service tokens (also called sTokens) to retrieve your VPP contents and to distribute them to devices using the Workspace ONE UEM console. This method enables the reuse of licenses. See Managed Distribution and Workspace ONE UEM on page 107 for an outline of the steps to use this deployment method.

Redemption Code Deployment Method

The redemption code deployment method uses codes from a spreadsheet to retrieve your VPP contents and to distribute them to devices using the UEM console. Use this method if your deployment consists of devices running iOS 6 or earlier. For an outline of the steps to upload the redemption codes spreadsheet and deploy VPP applications to devices, see Redemption Codes and Workspace ONE UEM on page 100.

Deploy Custom B2B Applications with VPP

You can deploy custom B2B applications bought through the VPP, but the ability to manage these applications depends on whether you deploy with redemption codes or managed distribution. See Custom B2B Applications and Apple's VPP on page 120 for details.

Volume Purchase Program (VPP) in Workspace ONE UEM

To distribute public applications and custom business to business (B2B) applications to Apple iOS and macOS devices, integrate Apple's Volume Purchase Program (VPP) and Workspace ONE UEM.

The Apple VPP enables organizations to purchase publicly available applications for distribution. Any paid application from the App Store is available for purchase, in volume, at the existing App Store price. Custom B2B applications can be free or purchased at a price set by the developer. If your organization uses free public applications collected through the Apple VPP, Workspace ONE UEM can distribute these applications, as well.

See Apple's website for the availability by country and for other details. Apple has two programs; **Volume Purchase Program for Business** and the **Volume Purchase Program for Education**.

Deploy VPP Process

To purchase and deploy content with Apple's Volume Purchase Program (VPP), enroll and acquire content on the VPP site and then use Workspace ONE UEM to distribute content.

1. **VPP Enrollment** – Enroll in the program and verify with Apple that you are a valid organization.
2. **Content Purchase** – Purchase content in the bulk through the VPP website.
3. **Application Deployment** – Distribute the assets throughout your device fleet using redemption codes or managed distribution service token files (sTokens).
    - Redemption Code Method on page 99
    - Managed Distribution by Apple IDs on page 106
    - Custom B2B Applications and Apple's VPP on page 120
    - Managed Distribution by Device Serial Number on page 123

For more information on the VPP process, see the following Workspace ONE UEM Knowledge Base article:https://support.workspaceone.com/articles/115001674208.

Supported Content for Purchased Applications

Workspace ONE UEM supports the various content types in the purchased section. The level of management varies according to the method used to get the content and the platform.

View support by operating system, application type, and acquirement method, Managed Distribution (**MD**), or Redemption Codes (**RC**). The letters **DB** represents systems that can retrieve applications without an Apple ID, and an **X** represents no support.

Operating System	Free Public Apps	Purchased Public Apps	Free Custom B2B Apps	Purchased Custom B2B Apps
Apple iOS 7.x – 8.x	MD & RC	MD & RC	MD & RC	MD & RC
Apple iOS 9+	MD, RC, & DB	MD, RC, & DB	MD & RC	MD & RC
macOS 10.9 – 10.10	MD	MD	X	X
macOS 10.11+	MD & DB	MD & DB	X	X

Note: The Workspace ONE UEM Container for iOS does not support the deployment of iOS applications purchased through Apple's Volume Purchase Program (VPP).

Redemption Code Method

This method uses redemption codes to allocate the content to devices, and it does not support revoking the codes from Apple iOS devices. Once the redemption code is redeemed, it cannot be recycled. Also, Workspace ONE UEM cannot delete content bought using redemption codes off devices.

Devices older than Apple iOS 7 must use this method for purchasing VPP content because the managed distribution is not available for older systems.

You cannot use redemption codes for macOS systems.

Redemption Codes and Workspace ONE UEM

Apple's Managed Distribution system integrates with Workspace ONE UEM, and you can distribute your free and purchased Volume Purchase Program (VPP) applications and books. The redemption code model uses codes from a spreadsheet to retrieve your VPP contents and to distribute them to devices using the Workspace ONE UEM console.

For the successful distribution of the VPP content to end users, perform all steps of the deployment process. In return, end users must complete all steps on their devices to receive the VPP content.

Admins Send VPP content to end users	1. Purchase you applications and download your redemption code spreadsheet from the Apple iTunes Store. 2. Upload the spreadsheet to Workspace ONE UEM. 3. Allocate redemption codes to organization groups and smart groups in the Workspace ONE UEM console and save the settings.
End-Users Receive content	1. Obtain a redemption code from Workspace ONE UEM. This step occurs automatically when admins publish the content. 2. Install the content from the catalog.

Upload a Redemption Code Spreadsheet

You can use Workspace ONE UEM to manage and distribute applications and books purchased through the VPP to your Apple iOS devices. Apple uses Web services to manage redemption codes. For the Workspace ONE UEM console to access Apple's Web services, you must first upload the redemption code spreadsheet.

1. Navigate to either **Apps & Books > Applications > Orders** or **Apps & Books > Books > Orders**.
2. Select **Add** or **Order** to add a redemption code spreadsheet.

   Select **Purchased Public App** or **Purchased Custom App** (Custom B2B), for applications. This option is not available for books.
3. Select **Choose File** to upload the **CSV** or **XLS** file that you downloaded from the Apple portal. This action creates the order.
4. Select **Save** to continue to the **Product Selection Form**.
5. Locate the appropriate product and choose **Select** to finish uploading the spreadsheet. If your spreadsheet contains an Adam ID, Workspace ONE UEM does not display this step.
   - If your spreadsheet contains an Adam ID, you do not have to locate the product. Workspace ONE UEM automatically adds applications and books from the app store when the spreadsheet contains the Adam ID. Adam IDs are specific to iTunes, are components of the Apple Search API, and are unique for each application.
   - If the Apple VPP redemption code spreadsheet contains codes for multiple applications or books, Workspace ONE UEM lists several products on this form. You can select only one per order.

Using iTunes Adam IDs

iTunes uses Adam IDs, which are item identifiers, to automate connections to content. If your spreadsheet contains an Adam ID, then you do not have to locate applications and books in the app store. For custom B2B applications, the Adam ID enables Workspace ONE UEM to update application IDs in the UEM console.

Assign Content to Users

You must enable the Workspace ONE UEM console to assign redemption codes to users and devices. Select the applicable organization groups and smart groups to which to assign redemption codes.

1. Navigate to the organization group where you uploaded the redemption code spreadsheet.
2. Go to **Apps & Books > Applications > Native > Purchased**.
3. Select the application you want to assign.

4. On the **Orders Assignment** tab, complete the following options.

Setting	Description
Add Assignment By	Assign redemption codes to organization groups or smart groups. • **Organization Group** – Allocate redemption codes to an organization group. Select **All Users** to include all users in that organization group, or choose Selected **Users** to display a list of users in the organization group. Use the **Add** and **Remove** buttons to choose the specific users to receive the application. • **Smart Group** – Allocate redemption codes to a smart group by typing the name of the group. Options display and you can select the appropriate smart group from the list. You can create a new smart group, if necessary. ◦ You can apply redemption codes to organization groups and to smart groups simultaneously. However, you can only specify the users for organization groups of the **Customer** type. ◦ You cannot specify users for smart groups. However, you can edit the smart group so that it contains the necessary users. • Verify the information in the following columns for each assignment rule: ◦ **Users** – View the number of users for the order. ◦ **Allocated** – Enter the number of licenses to allocate to the selected users. Do not exceed the total number in the order. ◦ **Redeemed** – View the number of licenses that have already been redeemed, if any.
Redemption Codes On Hold	Enter the number of redemption codes that you want to place on hold. Use this option to save the redemption codes for later use.
SDK Profile	If you use AirWatch SDK functionality, assign an SDK profile to the application.

Setting	Description
	Deployment
Assignment Type	• **On Demand** – Deploys content to a catalog or other deployment agent and lets the device user decide if and when to install the content. This option is the best choice for content that is not critical to the organization. Allowing users to download the content when they want helps conserve bandwidth and limits unnecessary traffic. • **Automatic** – Deploys content to a catalog or other deployment agent on a device upon enrollment. After the device enrolls, the system prompts users to install the content on their devices. This option is the best choice for content that is critical to your organization and its mobile users. You can only use **On-Demand** for custom B2B applications acquired using redemption codes. When the **Assignment Type** is **Auto**, only eligible Apple iOS 7+ devices receive the application or book automatically.
Remove On Unenroll	Set the removal of the application from a device when the device unenrolls from Workspace ONE UEM. Workspace ONE UEM enables this option by default. If you choose to enable this option, supervised devices are restricted from silent app installation because the device is locked and the provisioning profile installation is in the command queue which requires a device to be unlocked to complete the installation. If you choose to disable this option, provisioning profiles are not pushed along with the installed application. That is, if the provisioning profile is updated, the new provisioning profile is not automatically deployed to devices. In such cases, a new version of the application with the new provisioning profile is required. Removing an application when a device is unenrolled does not recover the redeemed code. When installed, the application is associated to the app store account of the user.
Prevent Application Backup	Disable backing up the application data to iCloud. However, the application can still back up to iCloud.
Make App MDM Managed if User Installed	Assume management of applications previously installed by users on their devices, supervised and unsupervised. Enable this feature so that users do not have to delete the application version installed on the device. Workspace ONE UEM manages the application without having to install the AirWatch Catalog version on the device.
Use VPN	Configure a VPN at the application level, and select the **Per-App VPN Profile**. Users access the application using a VPN, which helps ensure that application access and use is trusted and secure.
Send Application Configuration	Send application configurations to Apple iOS devices, so users do not have to configure these specified values themselves.

5. Select **Save** when you finish allocating codes.

Redemption Code Information

Access information about your redemption codes so that you can manage and track your VPP deployments.

To access orders of applications you acquired using redemption codes, navigate to **Apps & Books > Orders > Redemption Codes**.

- View the availability status of the code.

Status	Description
Available	Identifies an available key code to use to distribute the purchased content. You can make this key code unavailable or delete it.
Externally Redeemed	Identifies a key code that was assigned and redeemed outside of the Workspace ONE UEM Purchased (VPP) system. You cannot perform actions for this key code.
Redeemed	Identifies a key code that was assigned and redeemed within the Workspace ONE UEM Purchased (VPP) system. You can make this key code unavailable or delete it.
Unavailable	Identifies a key code that was explicitly made unavailable for various reasons. Reasons include separating codes that you want to save for users who might not be in your Workspace ONE UEM deployment.

- View each redemption code and the order number.
- View the date the redemption code was redeemed.
- View to whom the code is assigned.
- Delete a redemption code.

Managed Distribution by Apple IDs

This method uses service token files, also called sTokens, to authenticate assignments. It allows you to assign license codes to Apple IDs to allocate content to devices, and the method supports the revocation and recycling of these license codes.

View Managed Distribution and Workspace ONE UEM on page 107 for a list of all required steps for successful deployment.

Managed Distribution and Workspace ONE UEM

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

For successful distribution of VPP content to end users, perform all steps of the deployment process. In return, end users must complete all steps on their devices to receive VPP content.

Admins Send VPP content to end users	1. Purchase content and download your sToken from the Apple iTunes Store. 2. Upload the sToken to Workspace ONE UEM. **Note:** You can use multiple sTokens within your Workspace ONE UEM hierarchy but you can only have one sToken in each organization group. 3. Sync licenses to display the content in the UEM console. 4. Add the bundle IDs for custom B2B applications. This action activates management. This step is unnecessary for non-B2B applications and books. 5. Allocate licenses and assign licenses to smart groups, and enable eligible applications for device-based assignment. Then publish managed distribution content with the flexible deployment feature. Publishing content triggers invitations to end users whose content is tied to their Apple IDs.
End-Users Accept invitations and receive content	1. Accept the invitation and register with the Apple VPP. This step ensures that they have the terms of agreement for participating in the program. This step is not necessary for device-based use. 2. Obtain the license from Workspace ONE UEM. This step occurs automatically when admins publish content. 3. Install content from the AirWatch Catalog.

Users With Multiple Devices

Users that have multiple Apple iOS devices must select and apply a single Apple ID to all the devices. If admins make content available on demand, then users can accept the invitation and join and register with the VPP. They install the content from the catalog to any of their devices.

Manage VPP sTokens to Retrieve Managed Distribution Licenses and Content

Apple uses Web services to manage license codes. The Workspace ONE UEM console accesses Apple's Web services with the service token, or sToken, you upload to the console. Workspace ONE UEM retrieves your VPP content with the license data on the sToken. Keep sTokens current, and if you are not using the licenses, clear the sTokens.

Upload sTokens

You can upload an sToken at the top Customer level and below. The Workspace ONE UEM system prompts you to register your sToken, so that Workspace ONE UEM can detect if the sToken is used in other environments.

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > VPP Managed Distribution**.
2. Configure the following settings.

Setting	Description
Description	Enter your VPP Account ID. Using your VPP Account ID as the description has several advantages. • If you use multiple sTokens, it identifies the correct account. • Reminds you the correct account when you renew the sToken. • Identifies the correct account to others in your organization who assume management of the VPP account.
sToken Upload	Select **Upload** to navigate to the sToken on your network. VPP accounts in Apple School Manager and Apple Business Manager can now be associated to locations to allow moving licenses from one VPP account to another. If an sToken that is associated to a location is uploaded, the location name is displayed in the UEM console.
Country	Select where Workspace ONE UEM validates 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	Send invitations to all the users immediately after you save the token. The invitation request users to join and register with Apple's VPP. Registration gives users access to the terms of use to participate in the program. Use the **Message Preview** option to review the invitation. 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. Workspace ONE UEM automatically sends users of Apple iOS v7.0.3+ and macOS 10.9+ an invite command when you enable this option. It does not send them an email message. You do not have to enable this option 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. **Device-Based VPP** Disable this check box for the device-based VPP system because invitations are not necessary. If you assign a device-based VPP device to a regular VPP app (a user-based VPP app), devices still receive invitations.
Message Template	Select an email template for an email message invitation for Apple iOS devices on Apple iOS v7.0.0 through v7.0.2.

3. **Save** the sToken and confirm the addition of the token.

Renew sTokens Before Expiration

Managed distribution sTokens are valid for 12 months. Renew your sTokens before they expire to avoid any disruption in your deployment. If your token expires, you cannot perform management tasks.

- Sync new managed distribution licenses.
- Send invitations to join the VPP.
- Assign and pushing managed distribution applications to newly enrolled devices.
- Revoke managed distribution licenses (the system cannot revoke licenses for books).

If a token expires, Workspace ONE UEM does not revoke managed distribution licenses previously assigned to devices already enrolled with Workspace ONE UEM.

1. Navigate to the correct organization group where the sToken resides.
2. Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > VPP Managed Distribution**.
3. Select **Renew** and browse to the renewed sToken on your network for upload.
4. **Save** your settings.

Clear sTokens

Clear sTokens to remove them from the Workspace ONE UEM console. Clear sTokens if you never used it to distribute content or if it has expired.

1. Go to the applicable organization group.
2. Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > VPP Managed Distribution**.
3. Select **Clear** and follow the prompts.

> **Note:** Deleting the sToken, uninstalls the applications purchased for your VPP account from all the assigned devices and revoke the licenses. All the applications that is purchased using the sToken will not be available for assignment.

For an outline of the support for the managed distribution method by Apple IDs, see Managed Distribution by Apple IDs on page 106.

Sync Managed Distribution Content

Workspace ONE UEM has two methods that sync-managed distribution content: By assets and by license. The assets function syncs the metadata on an sToken and claimed licenses information. The license function syncs information for a single asset. It is useful for sTokens that contain thousands of licenses and you only want to sync the licenses applied to one asset.

Sync Assets

1. Go to the organization group where you uploaded the sToken.
2. Navigate to one of the following areas:
   - **Apps & Books > Applications > Native > Purchased**
   - **Apps & Books > Books > List View > Purchased**
3. Select **Sync Assets**.
4. Confirm to register an sToken with Workspace ONE UEM, if applicable. The system prompts for registration if it detects an sToken is used in another environment.
5. To select that the sync completed, refresh the screen.

   Workspace ONE UEM syncs purchased asset meta data and if there are claimed licenses, the system syncs for those assets of the claimed licenses. Workspace ONE UEM makes the sync features inaccessible until reconciliation completes.

Sync Licenses

1. Go to the organization group where you uploaded the sToken.
2. Navigate to one of the following areas:
   - **Apps & Books > Applications > Native > Purchased**
   - **Apps & Books > Books > List View > Purchased**
3. Select the asset check box and select **Sync Licenses** option from the actions menu.

Configure Licenses and Assign with Flexible Deployment

To retrieve the data on the sToken, Workspace ONE UEM syncs with Apple Web services, and then it can display content for assignment and deployment. Workspace ONE UEM distributes licenses by smart group and publishes content when you save an assignment rule in the flexible deployment feature.

The **Enable Device Assignment** option displays for applications that are eligible for distribution by device serial number. For information about the device-based distribution method, see Managed Distribution by Device Serial Number on page 123.

For information on flexible deployment and how to prioritize assignment rules, see Flexible Deployment for Applications Setting Descriptions on page 34.

Assign Content to Groups and Publish with Flexible Deployment

Assign content acquired from Apple's Volume Purchase Program (VPP) with managed distribution codes to smart groups.

1. Navigate to **Apps & Books > Applications > Native > Purchased**
2. Select the application and optionally hold licenses and apply an SDK profile.

Setting	Description
Licenses on hold	Enter the number of licenses that you want to place on hold. Use this setting to save the managed distribution codes for later use. You do not have to enter a value.
SDK Profile	If you use AirWatch SDK functionality, assign an SDK profile to the application.

3. Select **Save & Assign** to move to the flexible deployment section. You add assignment rules that you can prioritize.
4. On the **Assignments** tab, select **Add Assignment** and complete the options.

Setting	Description
Add Assignment By	Select **License Codes By Smart Group** and assign managed distribution codes. Allocate codes to a smart group by typing the name of the group. Options display, and you can select the appropriate smart group from the list. If necessary, you can create a new smart group. • **Users or Devices** – View the number of users for the order. • **Allocated** – Enter the number of licenses to allocate to the selected users. Do no exceed the total number in the order. • **Redeemed** – View the number of licenses that have already been redeemed, if any.

Setting	Description
Assignment Type	• **On Demand** – Deploys content to a catalog or other deployment agent and lets the device user decide if and when to install the content. This option is the best choice for content that is not critical to the organization. Allowing users to download the content when they want helps conserve bandwidth and limits unnecessary traffic. • **Automatic** – Deploys content to a catalog or other deployment agent on a device upon enrollment. After the device enrolls, the system prompts users to install the content on their devices. This option is the best choice for content that is critical to your organization and its mobile users. If the Assignment Type is set to **Auto** when you **Publish**, Workspace ONE UEM sends an invitation to Apple iOS 7.0.3+ and macOS 10.9+ devices. The invitation enables users to register with Apple's VPP.
Remove On Unenroll	Set the application to be removed from a device when the device unenrolls from Workspace ONE UEM. Workspace ONE UEM enables this option by default. If you choose to enable this option, supervised devices are restricted from silent app installation because the device is locked and the provisioning profile installation is in the command queue which requires a device to be unlocked to complete the installation. If you choose to disable this option, provisioning profiles are not pushed along with the installed application. That is, if the provisioning profile is updated, the new provisioning profile is not automatically deployed to devices. In such cases, a new version of the application with the new provisioning profile is required.
Prevent Application Backup	Disallow backing up the application data to iCloud. However, the application can still back up to iCloud.
Make App MDM Managed if User Installed **Apple iOS**	Assume management of applications previously installed by users on their devices, whether applications are supervised or unsupervised. Enable this feature so that users do not have to delete the app version installed on the device. Workspace ONE UEM manages the app without having to install the AirWatch Catalog version on the device.
Use VPN	Configure a VPN at the application level, and select the **Per-App VPN Profile**. Users access the application using a VPN, which helps ensure that application access and use is trusted and secure.
Send Application Configuration	Send application configurations to devices.

5. Select **Save**.
6. If you have more than one assignment rule, use the **Move Up** and **Move Down** options to order assignments. Place

critical assignments at the top of the list. This configuration displays as the **Priority**.

7. Select **Save & Publish**.

Methods to Revoke Managed Distribution Codes

Workspace ONE UEM offers several ways to revoke managed distribution codes so that you can reuse them. You can manually revoke codes. The system revokes codes in response to you deleting or unassigning another system component like organization groups, sTokens, and smart groups.

See what methods are available to you to revoke your managed distribution codes for reuse.

Revoke Method	Description
Organization Group	Delete an OG and Workspace ONE UEM makes the distribution codes available for reuse.
User	Unenroll all devices from a user. If another device does not use the unassigned managed distribution code, then the Workspace ONE UEM console revokes it so that it is available for reuse.
Manual	Revoke the code manually off the device. You can use the manual method only for those codes that are redeemed from an external system. This method is useful for adopting these codes into Workspace ONE UEM.
VPP Asset	Delete VPP assets from the UEM console. Once deleted, the code is available for reuse after the scheduler task runs.
sToken	Delete the sToken. Workspace ONE UEM makes all associated codes available for reuse.
Unassign	Unassign an asset from a user. If that license is not used by anyone else, Workspace ONE UEM revokes the distribution code.
Smart Group	Delete a managed distribution device user from a smart group. If that license is not used by anyone else, Workspace ONE UEM revokes the distribution code.

Workspace ONE UEM makes codes available immediately after revoking or at a scheduled interval depending on the interval you set in the scheduler task, VPP revoke licenses. Find the scheduler task in **Groups & Settings > All Settings > Admin > Scheduler**.

Managed Distribution Information

You can access managed distribution information from the Device Details, Licenses, and Manage Devices pages. Each page offers various auditing and management actions depending on the type of asset.

Device Details

From the Device Details page, audit assignments and perform installations and removals.

Go to **Devices > List View > Apps** or to **Devices > List View > More > Books**. The system does not support all management functions for all asset types. The system does not display unsupported options.

- View the content assigned to the device.
- If supported, install and remove the content on the specified device.

Licenses

From the Licenses page, track sync processes, audit licenses available for reuse, and revoke licenses if supported.

Go to **Apps & Books > Applications > Native > Purchased > Managed Distribution** or to **Apps & Books > Books > List View > Purchased > Managed Distribution**.

- View when assigned licenses were last synced.
- Filter by **License Owner Type** to access licenses that are available to reuse due to error using the **Not Assigned** option.
- Use the **Revoke** action to make licenses available for reuse.

Manage Devices

From the Manage Devices page, install and remove content, send invitations to join the VPP if supported, and audit application installations and VPP program registrations.

Go to **Apps & Books > Applications > Native > Purchased > Manage Devices** or to **Apps & Books > Books > List View > Purchased > Manage Devices** to access the page. The system does not support all management functions for all asset types. The system does not display unsupported options.

- Install the content to devices.
- Remove the content from devices, if supported by the asset.
- Notify devices concerning the VPP.
- Reinvite user-based VPP members who have not registered their Apple IDs with the program.
- Filter data using the **Status** option and find devices that have not installed VPP content.
- Filter data using **User Invite** and find those user-based members who have not registered their Apple IDs with the program.

Staging Users and Managed Distribution for Apple's VPP

Apple offers the Apple Configurator and the Apple Device Enrollment Plan (DEP) to help IT administrators to deploy and manage large numbers of Apple iOS devices. Workspace ONE UEM integrates with both applications, and integrating with Apple's Volume Purchase Program (VPP). All applications aim to help maintain and manage bulk device and content.

To reduce the risk of license inconsistencies, review these suggestions and guidelines for deploying Apple Volume Purchase Program (VPP) content to devices that you stage using Configurator and the DEP.

Note: This information does not apply to VPP applications assigned to device serial numbers.

Avoiding License Inconsistencies

Distribute Volume Purchase Program (VPP) content bought using the managed distribution method:

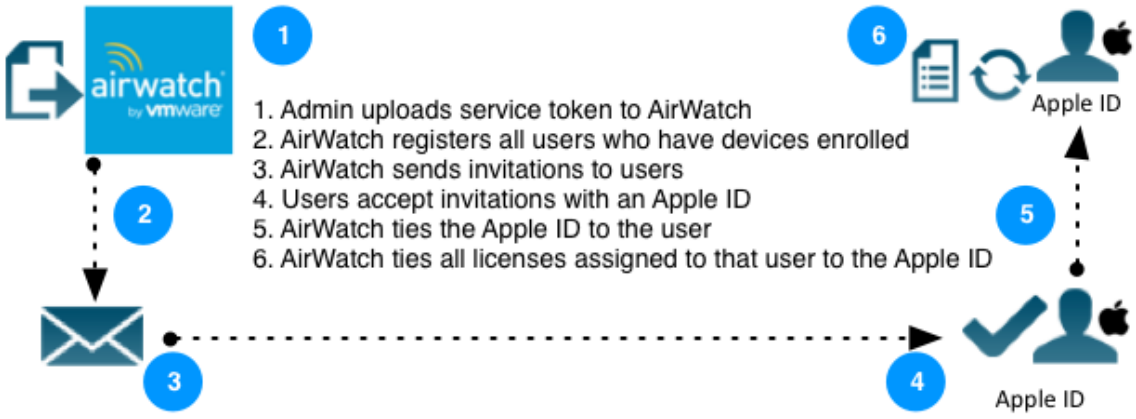
- Use a service token (sToken) in one MDM environment and not in multiple environments. Some examples include not using an sToken in Workspace ONE UEM and in another MDM system or in a trial environment and in a production environment.
- Use an sToken in one organization group and not in multiple organization groups within Workspace ONE UEM.
- Apply one device to one Apple ID and do not change the Apple ID on the device.

These actions reduce the risk of losing a license in one environment because it was revoked in another environment. However, it cannot be economically possible to have the number of licenses to cover your staged devices using these actions. VPP deployment in a staged environment is still manageable but it can take extra maintenance with special attention paid to the Apple ID.

Apple IDs

Apple IDs are an important part of the system Workspace ONE UEM uses to manage the VPP content for staged users. An Apple ID is an identification created by users registering with Apple applications. Users in this scenario also have their credentials for Workspace ONE UEM. The user enrolls with Workspace ONE UEM and then Workspace ONE UEM registers the user with Apple and sends an invitation to join the Apple VPP. The user accepts the invitation and joins the VPP using the Apple ID. Currently, Workspace ONE UEM stores the association of the Apple ID with the user.

It is important to manage the Apple ID in staged environments because the Apple ID controls access to the user's specific set of VPP content. When users change Apple IDs on devices without communicating the change to their admins, they might experience access difficulties.



Guidelines for Staging

Use the following processes to reduce license inconsistencies in Workspace ONE UEM.

Staging Method	Assign VPP Content To	Accepts VPP Invitation	Installs applications	Updates applications	Maintenance	Risks
Single User, Standard (Self-Registration)	Individual devices with unique Apple IDs **Not a staging user**	End users with unique Apple IDs	End-users install applications	End-users update applications	No maintenance of Apple IDs	Least risk because end users maintain their own Apple IDs on individual devices
Single User, Advanced (Pre-Configured)	Pre-configured devices with pre-configured Apple IDs	End users with pre-configured Apple IDs	End-users install applications	End-users update applications	• Maintain pre-configured Apple IDs • Provide pre-configured Apple IDs to end users	• End-users change Apple IDs • End users do not return devices to the pre-configured Apple ID

Staging Method	Assign VPP Content To	Accepts VPP Invitation	Installs applications	Updates applications	Maintenance	Risks
Multi Users	• Staging user • Individual users	• Admin with the staging user Apple ID • End users with respective unique Apple IDs	• Admin installs common applications with staging user Apple ID • End-users install unique applications with individual Apple IDs	• Staging user ID must update common applications with staging user Apple ID • End users update unique applications with their individual Apple IDs	• Maintain a staging user Apple ID for a common set of VPP content on all devices selected to staging user • Maintain end-user Apple ID at device check-out	• All devices selected in to the staging user do not have the same Apple ID • Admins do not change devices to the staging user Apple ID upon device check-in • End users do not change the staging user Apple ID to their unique Apple IDs upon device check-out

Custom B2B Applications and Apple's VPP

You can upload custom B2B applications acquired through Apple's Volume Purchase Program (VPP) to Workspace ONE UEM. Workspace ONE UEM works with the redemption code method and with the managed distribution method.

The ability of Workspace ONE UEM to manage custom B2B applications, depends upon the VPP system used to get the applications.

- Redemption codes – Workspace ONE UEM can install custom B2B applications bought using redemption codes on to devices. End users can install these applications on-demand, but Workspace ONE UEM cannot manage these applications. Upload custom B2B applications acquired with redemption codes like other applications acquired with redemption codes.

  Go to Redemption Code Method on page 99 for details.

- Managed distribution – Workspace ONE UEM can install custom B2B applications bought using managed distribution. End users can install these applications on-demand or you can push these applications automatically. Workspace ONE UEM can manage these applications. Upload custom B2B applications acquired with the managed distribution like other applications acquired with the managed distribution. However, between the sync-steps and assign-steps, activate management of the applications.

  - Go to Managed Distribution by Apple IDs on page 106 for details on uploading applications acquired with the managed distribution.
  - Go to Activate Management of Custom B2B Applications on page 122 for details to activate management.

VPP, Custom B2B Applications, and Push Mode

Workspace ONE UEM can manage custom B2B applications acquired with managed distribution codes but it cannot manage custom B2B applications acquired with redemption codes.

The ability of Workspace ONE UEM to manage the custom B2B application determines the push modes available to distribute the application.

VPP Method	Management Ability	Available Push Mode
Managed distribution	Manage Workspace ONE UEM can manage custom B2B applications acquired with managed distribution codes.	Auto On-Demand
Redemption code	Cannot manage Workspace ONE UEM cannot manage custom B2B applications acquired with redemption codes.	On-Demand

Activate Management of Custom B2B Applications

When you acquire applications from Apple's Volume Purchase Program (VPP) with managed distribution codes, Workspace ONE UEM creates place holders for all applications it deems as custom B2B. The system creates the place holders because it cannot retrieve the metadata like the icon, the name, and the bundle ID from an app store. Activate management by entering the missing metadata.

If there is a version of the custom B2B application bought using redemption codes, Workspace ONE UEM can pull the icon and name from the redemption code version. However, you must still enter the bundle ID.

Activate management of custom B2B applications after you sync licenses and before you assign licenses to smart groups. This process is outlined in the topic Managed Distribution and Workspace ONE UEM.

1. Upload an sToken and sync licenses.
2. Navigate to **Apps & Books > Applications > Native > Purchased**.
3. Select the **Unknown** link in the **Name** column for the custom B2B application. Use the **App Type > Custom B2B** filter for locating **Unknown** links.

   Workspace ONE UEM changes the status and makes actions available after you enter the information.
4. Complete the following options.

Setting	Description
Application Name	Enter a name that the Workspace ONE UEM console displays.
Application ID	View the ID populated using the Adam ID.
Bundle ID	Enter the value given to you by the developer
Managed By	Identifies the managing organization group.
Description	Enter a description with useful information like the purpose of the application.

5. Select **Save**.

Applications you do not activate for management display as **Inactive** in the Console.

Managed Distribution by Device Serial Number

If your VPP deployment consists of iOS 9+ or macOS 10.11+ devices, consider enabling the assignment of Volume Purchase Program (VPP) applications by device serial number. This method removes the need to invite users to the VPP.

Deploy device-based VPP applications using the outlined processes in Managed Distribution and Workspace ONE UEM on page 107.

Workspace ONE UEM does not migrate applications to the device-based system. VPP applications already assigned to Apple IDs remain assigned as such.

Benefits

The device-based system offers several advantages.

- Users do not have to accept invitations and register with the VPP.
- Admins with multiple sTokens in their VPP deployment do not have to manage invitations.
- Admins do not have to manage Apple IDs.

Uses

Device-based assignment is the best choice for deployments in the following scenarios.

- Shared devices with check-in and check-out systems
- Corporate owned devices
- Staged environments with one-device-to-one-user ratios
- Devices in Workspace ONE UEM for Education deployment

The user-based system is the best choice for the following scenarios.

- Multiple devices assigned to a single Apple ID
- Need to conserve licenses

Supported Platforms and Operating Systems

Configure a supported OS to use the device-based method to distribute applications acquired through Apple's Volume Purchase Program (VPP).

- iOS 9+
- macOS 10.11+

App Eligibility

Developers of VPP applications must enable the applications for use in the device-based VPP.

Invitations

With the Apple ID removed from the process, the device-based method no longer relies on invitations to register Apple IDs. However, if a device meets the requirements, the system still sends invitations.

- Device does not use iOS 9+ or macOS 10.11+
- App is not enabled for device-based VPP use
- Device receives a user-based VPP application
- **Automatically Send Invites** is enabled in Workspace ONE UEM

Device-Based VPP Deployment Process

The process to upload device-based (serial number) applications is similar to uploading user-based (Apple ID) VPP applications. The only difference is that the device-based method does not involve sending invitations.

Important: Once an application is enabled for device-based use in the Workspace ONE UEM console, you cannot reverse its status and use it in the user-based system.

1. **sTokens** – Upload or register an sToken in the desired organization group in Workspace ONE UEM. If you do not want Workspace ONE UEM to send invitations to devices, disable **Automatically Send Invites**.
2. **Syncs** – Start here in the process if you already have sTokens in Workspace ONE UEM. If needed, Workspace ONE UEM prompts you to register an sToken with the Workspace ONE UEM environment. It sends invitations automatically for user-based applications that have an **Auto** push mode.
3. **Assign with Flexible Deployment** – Assign and publish device-based VPP applications with the flexible deployment feature. During the assignment process, Workspace ONE UEM prompts you to enable applications for the device-based method with the setting **Enable Device Assignment**.
4. **Information Access** – Access license and application information using the Licenses page, the Device Details page, and the Manage Devices page.
5. **Revoke and Reuse** – Revoke licenses with various management functions.
    - Unenroll devices.
    - Select the revoke action on the information pages (Licenses, Device Details, and Manage Devices pages).
    - Deactivate and delete assignments.
    - Remove devices from smart groups assigned to the VPP application.

Update Device-Based VPP Applications Manually or Automatically

Configure automatic updates or manually push updates to device-based VPP applications at the application level. This feature offers management of updates by Workspace ONE UEM or allows you to push updates as a way to control application versions.

This feature does not work for managed distribution by Apple ID. The VPP application must be enabled for device-based distribution, also called distribution by device serial number. For general information about the managed distribution

method by device serial number, see Managed Distribution by Device Serial Number on page 123. This topic includes supported operating systems, benefits, and the need for no VPP invitations.

Note: Custom B2B applications and non device-based VPP applications are tagged as **Not Applicable**. These types of VPP applications are not supported for this feature.

System Behavior on Initial Setup

The system does not automatically queue application installation commands at the time you first configure **Enable Auto Updates**. Initially, Workspace ONE UEM stores the currently available version number from the App Store in the database. As this is the initial version being recorded, it does not automatically trigger application upgrades.

When a newer version becomes available in the future, the Workspace ONE UEM system that canvases the App Store for updates records that new version in the database. At this point, Workspace ONE UEM can automatically trigger install commands for devices to perform application updates.

Enable or Push an Update

Enable automatic updates or push them manually. Disabling automatic updates and pushing them manually allows you to control what application versions are on devices.

1. Navigate to **Apps & Books > Applications > Native > Purchased**.
2. Select a device-based VPP application.

   The system displays the Enable Auto Updates option.
3. Select to **Enable Auto Updates**.

   If you disable automatic updates, you can select **Update App** to push an update to devices if there is an update available.

Use Filters to Find Applications and Perform Tasks in Bulk

Use the **Auto Update** filter or the **Update Status** filter to find and act on applications.

Filter Example

Use these filters to enable automatic updates on multiple applications.

1. Filter the **Purchased** tab by **Auto Update > Disabled** and **Updated Status > Update Available**.

   Workspace ONE UEM displays the application results.
2. Select all listed applications with the bulk-selection check box.

   This action triggers the UI to display the option to **Enable Auto Updates**.
3. Select **Enable Auto Updates** to enable the feature in bulk.

Other bulk options include **Manage Devices**, **Sync Licenses**, **Disable Auto Updates**, **Update App**, **More Actions > Notify Devices**, and **More Actions > View Events**.

Update Notifications

Configure Workspace ONE UEM to notify you about updates using the notification icon and email.

Notification Icon

The Workspace ONE UEM console sends notifications when it identifies an update. The bell icon in the upper right of the UI displays the number of notifications you have. Select the bell icon and look for the **App Update Available** notification.

Email

If you prefer notification by email, select the **Account Settings** icon, which resembles a gear, at the bottom of the notifications window. Edit the **Notification** options.

Convert Non Device-Based Applications to Use the Feature

> **Important:** You cannot reverse an application back to the Apple ID-managed distribution system (user-based). Do not convert applications if you need the Apple ID to manage VPP applications.

If you want to use this feature on non device-based VPP applications, use the **Enable Device Assignment** option on the **Assignment** tab in the application's record. Select it to convert the application from the user-based (Apple ID) managed distribution system to the device-based method.

The system checks for updates every 24 hours by default. Workspace ONE UEM identifies newly converted applications with the **Pending Check** status. After the system updates the application, it changes the status to **Update Pushed**.

Update Challenge for Device-Based VPP Applications

Device-based VPP applications had update issues due to their disassociation from the Apple ID. Workspace ONE UEM developed a system to help with the updates of device-based applications. You can configure automatic updates or manually push updates.

Challenge

In the device-based VPP method of managed distribution, the device serial number is the connection between licenses and the application. It replaces the Apple ID. However, the update of the application is still tied to the Apple ID because the Apple ID is tied to the purchase history. Device-based applications can miss updates because the Apple ID is removed from the license-assignment process.

Solution

Workspace ONE UEM checks the app store for updates of your device-based VPP applications and identifies when updates are available in the UI.

Enable automatic updates for device-based VPP applications and Workspace ONE UEM updates these applications whenever it identifies an updated is available.

If you want to control the version of an application, leave automatic updates disabled and manually push updates when needed.

Chapter 6: SaaS Applications in Workspace ONE UEM

Manage your SaaS applications in the same console as your native applications and web links. When you use access policies with SaaS applications, you can control access to the application at the point of authentication.

SaaS Applications and Web Applications Are the Same

SaaS applications are called Web applications in VMware Identity Manager and you can now add, edit, and delete these applications in one management console. They consist of a URL address to the landing page of the resource. They also include an application record. Add SaaS applications to the Workspace ONE UEM console from your web applications in the Workspace ONE catalog. You can also add new SaaS applications in the UEM console.

VMware Identity Manager Documentation

For information about configuring web applications in VMware Identity Manager, see **Providing Access to Web Applications**, in VMware Identity Manager Documentation.

Web Links Applications

Web links applications were called web applications in past Workspace ONE UEM releases. For information about Web links applications, see Web Links Application Features and Supported Platforms on page 151.

Control Access at the Time of Authentication

SaaS applications and access policies offer control of resources at the time of authentication.

Component	Description
Authentication method	Require the use of federation protocols when accessing the SaaS application. Federation protocols use tokens to allow access and to establish trust between the resource and the user.
Identity and Service Providers	To configure trust between your providers, SaaS applications, and users in your network, use the identity provider and the service provider metadata from the Workspace ONE system in Workspace ONE UEM.

Component	Description
Certificates	To control trust between users in your Workspace ONE system and the SaaS application, use the self-signed certificate from the VMware Identity Manager service or enter one from your certificate authority.
Users and User Groups	Configure users and user groups in VMware Identity Manager and then assign them to SaaS applications in the UEM console.
Secured Connection	Enable trusted connections with the VMware Enterprise System between the Workspace ONE system, SaaS applications, and users.
Session Access & Length	Configure access policies and mobile SSO to control the allowable time to access SaaS applications before users must reauthenticate with Workspace ONE.

More SaaS Application Topics

For prerequisites for the configuration of SaaS applications, see Requirements to Support SaaS Applications on page 128.

For information about configuring SaaS applications, see Add SaaS Applications in the Workspace ONE UEM console on page 130.

For information about adding Microsoft Intune® App Protection Policies applications and assigning client access policies to them, see Add Office 365 Applications with a Client Access Policy on page 136.

For information about assign SaaS applications to users and user groups, see Assign SaaS Applications on page 139.

Requirements to Support SaaS Applications

Configure the listed components and ensure that the Workspace ONE UEM environment has the correct settings so that you can access the content on the **SaaS** page.

Required Systems

Configure or integrate the listed systems so that you can access the SaaS applications page. You can find a wizard to set up these systems in the **Workspace ONE** tract of the **Getting Started** section of the Workspace ONE UEM console.

- **VMware Enterprise System Connector** - This component is the unified connector for Workspace ONE, Workspace ONE UEM, and VMware Identity Manager.
- **Active Directory** - This component integrates Workspace ONE UEM and VMware Identity Manager to sync users and groups from Active Directory (AD) to the service. You assign SaaS applications to the users and groups synced from Active Directory.

  Note: With setup of the connector, AD users and groups are in sync between Workspace ONE UEM and VMware Identity Manager.

- **VMware Identity Manager** - This component serves many functions including managing your users and groups and managing authentication to resources. For detailed information on the integration of the two systems, search for

Integrating Workspace ONE UEM and VMware Identity Manager, at VMware Identity Manager Documentation on docs.vmware.com.

- **Mobile SSO -**This component manages single sign-on (SSO) capabilities in the Workspace ONE portal for Workspace ONE UEM-managed Android and iOS devices. For Android devices, mobile SSO uses certificate authentication. For iOS devices, it uses the identity provider in the identity manager service in VMware Identity Manager. Go to VMware Identity Manager documentation on docs.vmware.com and review on of the listed topics for information on mobile SSO.
  - **Implementing Mobile Single Sign-in Authentication for Workspace ONE UEM-Managed iOS Devices**
  - **Implementing Mobile Single Sign-On Authentication for Workspace ONE UEM-Managed Android Devices**

  Note: Mobile SSO is different from the SSO feature for applications that use the AirWatch SDK.

- **Access Policies** - This component provides secure access to the Workspace ONE apps portal to start Web applications. Access policies include rules that specify criteria that must be met to sign in to the apps portal and to use resources.

  A default policy is available that controls access as a whole. This policy is set up to allow access to all network ranges, from all device types, for all users. You can create stricter access policies that restrict users access to applications based on access rules you define. For information, see Use Access Policies with SaaS Applications on page 157.

Supported Applications

Deploy SaaS applications to these platforms.

- Android
- Apple iOS
- Apple macOS
- Windows Desktop (Windows 10)

Methods to Add SaaS Applications

Select from several ways to add or export SaaS applications in your Workspace ONE environment.

Method	Description	Topic
Catalog or manual	Select the application from a catalog list or enter the corresponding URL and information.	Add SaaS Applications in the Workspace ONE UEM console on page 130
Copy an existing SaaS application	Use this method to make copies of the same SaaS application available to different business units.	Copy SaaS Applications in the Workspace ONE UEM console on page 135
Export a ZIP file	Use this method to save a ZIP file of the application bundle as a JSON to a local machine.	Export SaaS Applications From the Workspace ONE UEM console on page 136

Add SaaS Applications in the Workspace ONE UEM console

You can add SaaS applications in the Workspace ONE UEM console. Browse applications already added to your Workspace ONE catalog or add new ones.

For information about access policies that secure SaaS applications, see Use Access Policies with SaaS Applications on page 157.

For information about the Approvals feature that activates licenses for use, see Configure Approvals on page 142.

1. Navigate to **Apps & Books > Applications > Web > SaaS** and select **New**.
2. Complete the options on the **Definition** tab.

Setting	Description
Search	You can create an application by copying it from global catalog. Enter the name of the SaaS application and search for the application in the global catalog. You can also browse the application from the global catalog.
Name	Enter a name for the SaaS application.
Description	(Optional) Provide a description of the application.
Icon	(Optional) Click Browse and upload an icon for the application. SaaS applications use icons in PNG, JPG, and ICON file formats. The application icons that you upload must be a minimum of 180 x 180 pixels. If the icon is too small, the icon does not display. In this instance, the system displays the default icon.
Category	Assign categories to help users sort and filter the application in the Workspace ONE catalog. Configure categories in VMware Identity Manager so that they display in the category list.

3. Complete the options on the **Configuration** tab.
   a. **Authentication Type** - Select the authentication type for the SaaS application.

      Available options vary depending on the type you select. The authentication type determines the available settings on the user interface. There are several permutations.

      - **SAML 2.0** - Select this option to provide single sign-on for applications that use the SAML 2.0 authentication.
      - **SAML 1.1** - The SAML 1.1 is an older SAML authentication profile. For better security, implement SAML 2.0.
      - **WSFed 1.2** - Select this option to provide single sign-on to applications that use WS-Federation authentication.
      - **Web Application Link** - If the application does not use a federation protocol, select this option. Enter the target URL of the application.
      - **OpenID Connect** - Select this option to provide single sign-on to applications that use the OAuth 2.0 protocol.

      Go to the authentication type for your SaaS application for available configurations.

- **SAML 2.0**

Setting	Description
Configuration	◦ **URL/XML** is the default option for SaaS applications that are not yet part of the Workspace ONE catalog. ◦ **Manual** is the default option for SaaS applications added from the catalog.
URL/XML	
URL/XML	Enter the URL if the XML metadata is accessible on the Internet. Paste the XML in the text box if the XML metadata is not accessible on the Internet, but you have it. Use manual configuration if you do not have the XML metadata. T
Relay State URL	Enter a URL where you want SaaS application users to land after a single sign-on procedure in an identity provider-initiated (IDP) scenario.
Manual	
Single Sign-On URL	Enter the Assertion Consumer Service (ACS) URL. Workspace ONE sends this URL to your service provider for single sign-on.
Recipient URL	Enter the URL with the specific value required by your service provider that states the domain in the SAML assertion subject. If your service provider does not require a specific value for this URL, enter the same URL as the **Single Sign-On URL**.
Application ID	Enter the ID that identifies your service provider tenant to Workspace ONE. Workspace ONE sends the SAML assertion to the ID. Some service providers use the **Single Sign-On URL**.
Username Format	Select the format required by the service providers for the SAML subject format.
Username Value	Enter the Name ID Value that Workspace ONE sends in the SAML assertion's subject statement. This value is a default profile text box value for a username at the application service provider.
Relay State URL	Enter a URL where you want SaaS application users to land after a single sign-on procedure in an identity provider-initiated (IDP) scenario.

- **SAML 1.1**

Setting	Description
Target URL	Enter the URL to direct users to the SaaS application on the Internet.
Single Sign-On URL	Enter the Assertion Consumer Service (ACS) URL. Workspace ONE sends this URL to your service provider for single sign-on.

Setting	Description
Recipient URL	Enter the URL with the specific value required by your service provider that states the domain in the SAML assertion subject. If your service provider does not require a specific value for this URL, enter the same URL as the **Single Sign-On URL**.
Application ID	Enter the ID that identifies your service provider tenant to Workspace ONE. Workspace ONE sends the SAML assertion to the ID. Some service providers use the **Single Sign-On URL**.

- **WSFed 1.2**

Setting	Description
Target URL	Enter the URL to direct users to the SaaS application on the Internet.
Single Sign-On URL	Enter the Assertion Consumer Service (ACS) URL. Workspace ONE sends this URL to your service provider for single sign-on.
Application ID	Enter the ID that identifies your service provider tenant to Workspace ONE. Workspace ONE sends the SAML assertion to the ID. Some service providers use the **Single Sign-On URL**.
Username Format	Select the format required by the service providers for the SAML subject format.
Username Value	Enter the Name ID Value that Workspace ONE sends in the SAML assertion's subject statement. This value is a default profile text box value for a username at the application service provider.

- **Web Application Link**

Setting	Description
Target URL	Enter the URL to direct users to the SaaS application on the Internet.

- **OpenID Connect**

Setting	Description
Target URL	Enter the URL to direct users to the SaaS application on the Internet.
Redirect URL	Enter the URL of the client that receives the authorization code and access token.
Client ID	Enter the unique string for the client.
Client Secret	Enter the secret used to authorize the client.

b. **Application Parameters** - Add values for advanced parameters to allow the application to start. This option is not available for all applications.

c. **Advanced Properties** - If you want greater control of messaging in single sign-on processes with Workspace ONE,

add optional parameters. The authentication type determines the available settings on the user interface. There are several permutations. Go to the authentication type for your SaaS application.

Setting	Description
SAML 2.0	
Sign Response	Require Workspace ONE to sign the response message to the service provider. This signature verifies that Workspace ONE created the message.
Sign Assertion	Require Workspace ONE to sign the assertion within the response message sent to the service provider. Some service providers require this option.
Encrypt Assertion	Encrypt the SAML assertion the system sends to the application service provider.
Include Assertion Signature	Require Workspace ONE to include its signing certificate within the response message sent to the service provider. Some service providers require this option.
Signature Algorithm	Select the signature algorithm that matches the digest algorithm. If your service provider supports SHA256, select this algorithm.
Digest Algorithm	Select the digest algorithm that matches the signature algorithm. If your service provider supports SHA256, select this algorithm.
Assertion Time	Enter the seconds that the assertion Workspace ONE sends to the service provider for authentication is valid.
Request Signature	If you want the service provider to sign the SAML request it sends to Workspace ONE, enter the public signing certificate.
Encryption Certificate	Enter the public encryption certificate that signs the SAML request from the application service provider to Workspace ONE.
Application Login URL	Enter the URL for your service provider's login page. This option triggers the service provider to initiate a login to Workspace ONE. Some service providers require authentication to start from their login page.
Proxy Count	Enter the allowable proxy layers between the service provider and an authenticating identity provider.
API Access	Enable API access to the SaaS application.
Custom Attribute Mapping	If your service provider allows custom attributes other than ones for single sign-on, add them.

Setting	Description
Open in VMware Browser **Android and iOS**	Require Workspace ONE to open the application in the VMware Browser. If you use VMware Browser, opening SaaS applications within it adds extra security. This action keeps access within internal resources.
SAML 1.1	
Signature Algorithm	Select the signature algorithm that matches the digest algorithm. If your service provider supports SHA256, select this algorithm.
Digest Algorithm	Select the digest algorithm that matches the signature algorithm. If your service provider supports SHA256, select this algorithm.
Assertion Time	Enter the seconds that the assertion Workspace ONE sends to the service provider for authentication is valid.
Custom Attribute Mapping	If your service provider allows custom attributes other than ones for single sign-on, add them.
Open in VMware Browser **Android and iOS**	Require Workspace ONE to open the application in the VMware Browser. If you use VMware Browser, opening SaaS applications within it adds extra security. This action keeps access within internal resources.
WSFed 1.2	
Credential Verification	Select the method for credential verification.
Signature Algorithm	Select the signature algorithm that matches the digest algorithm. If your service provider supports SHA256, select this algorithm.
Digest Algorithm	Select the digest algorithm that matches the signature algorithm. If your service provider supports SHA256, select this algorithm.
Assertion Time	Enter the seconds that the assertion Workspace ONE sends to the service provider for authentication is valid.
Custom Attribute Mapping	If your service provider allows custom attributes other than ones for single sign-on, add them.

Setting	Description
Open in VMware Browser **Android and iOS**	Require Workspace ONE to open the application in the VMware Browser. If you use VMware Browser, opening SaaS applications within it adds extra security. This action keeps access within internal resources.

d. **Access Policies** - Assign policies to secure signing in to application resources.

Setting	Description
Access Policy	Select a policy for Workspace ONE to use to control user authentication and access. The default access policy is available if you do not have custom access policies. You can configure these policies in the UEM console.
License Approval Required	For this option to display, enable the corresponding **Approvals** in the **Settings** section of SaaS applications. Require approvals before the application installs and activates a license. • **License Pricing** - Select the pricing model to buy licenses for the SaaS application. • **License Type** - Select the user model for the licenses, named or concurrent users. • **Cost Per License** - Enter the price per license. • **Number of Licenses** - Enter the number of licenses bought for the SaaS application.

4. View the **Summary** for the SaaS application and move to the assignment process.

Assign SaaS Applications

Assign SaaS applications to users and groups configured in VMware Identity Manager. See Assign SaaS Applications on page 139.

Copy SaaS Applications in the Workspace ONE UEM console

Create copies of SaaS applications and assign them to different users and groups.

When users log into Workspace ONE and select the application to which they are assigned, the Workspace ONE system sends them the assign application version.

Using copies of applications is useful if your deployment has different business units that use the same application.

To copy a SaaS application, use the Copy feature, update configurations for that version, and assign the version to the applicable users and groups.

1. Navigate to **Apps & Books > Applications > Web > SaaS** and select the application.
2. Select **Copy**.
3. Complete settings on the **Definition** tab.

   To help find the copied application, enter a name in the **Name** field. Complete any other desired settings.

4. Edit settings on the **Configuration** tab as needed.
5. Use the default access policy or select an application-specific access policy on the **Access Policies** tab.
6. Review the information on the Summary tab and move to the assignment process.

Assign SaaS Applications

Assign copies of SaaS applications to different users and groups configured in VMware Identity Manager. See Assign SaaS Applications on page 139.

Export SaaS Applications From the Workspace ONE UEM console

Export SaaS applications that you want to test in a staging area or that you want to use on a local machine without the Workspace ONE system.

Task

To export a SaaS application, use the Export feature and save it to a local machine.

1. Navigate to **Apps & Books > Applications > Web > SaaS** and select the application.
2. Select **Export**.
3. Confirm that you want to export the application.

   The system saves a ZIP file of the JSON application bundle to the local machine.

Client Access Policy Description

A client access policy uses Office 365 client authentication credentials to access Office 365 applications in your Workspace ONE deployment.

An Office 365 client, such as VMware Boxer, Microsoft Outlook, and iOS and Android native email clients, collects credentials in their UI to authenticate. A client access policy enables VMware Identity Manager to manage the collected credentials for authentication.

Client access policies also enable you to set other access parameters for Office 365 applications. Policies set in a single Office 365 application apply to all Office 365 applications. Any edits to client access policies impact the users' ability to access these applications.

Order of Client Access Policies

Arrange the client access policies in order because the system enforces policies from top to bottom. The system uses the first policy to authenticate a client or to deny it access.

For example, if you create a policy denying access to all device types and drag it above a policy allowing access for Android devices, the system denies all devices access that attempt the user name and password. The system does not enforce the policy allowing access to Android devices. The first policy that denies access takes the precedent.

Add Office 365 Applications with a Client Access Policy

Add Office 365 applications to the Workspace ONE UEM console so that you can control access with client access policies.

1. Navigate to **Apps & Books > Applications > Web > SaaS** and select **New**.
2. Complete the options on the **Definition** tab.

Setting	Description
Search	Enter Office 365 to see a list of available applications.
Name	Enter or view a name for the SaaS application.
Description	(Optional) Provide a description of the application. Often, this text box pre-populates.
Icon	(Optional) if an icon does not pre-populate, select an icon.
Category	(Optional) Assign categories to help users sort and filter the application in the Workspace ONE catalog. Configure categories in VMware Identity Manager so that they display in the category list.

3. Complete the options on the **Configuration** tab.
   a. **Authentication Type** - Office 365 applications use **WSFed 1.2** for authentication type to provide single sign-on.

Setting	Description
Target URL	Enter the URL to direct users to the SaaS application on the Internet.
Single Sign-On URL	Enter the Assertion Consumer Service (ACS) URL. Workspace ONE sends this URL to your service provider for single sign-on.
Application ID	Enter the ID that identifies your service provider tenant to Workspace ONE. Workspace ONE sends the SAML assertion to the ID. Some service providers use the **Single Sign-On URL**.
Username Format	Select the format required by the service providers for the SAML subject format.
Username Value	Enter the Name ID Value that Workspace ONE sends in the SAML assertion's subject statement. This value is a default profile text box value for a username at the application service provider.

   b. **Application Parameters** - Add values for advanced parameters to allow the application to start.
   c. **Advanced Properties** - If you want greater control of messaging in single sign-on processes with Workspace ONE, add optional parameters.

Setting	Description
WSFed 1.2	
Credential Verification	Select the method for credential verification.
Signature Algorithm	Select the signature algorithm that matches the digest algorithm. If your service provider supports SHA256, select this algorithm.

Setting	Description
Digest Algorithm	Select the digest algorithm that matches the signature algorithm. If your service provider supports SHA256, select this algorithm.
Assertion Time	Enter the seconds that the assertion Workspace ONE sends to the service provider for authentication is valid.
Custom Attribute Mapping	If your service provider allows custom attributes other than ones for single sign-on, add them.

d. **Access Policies** - Assign policies to secure signing in to application resources.

Setting	Description
Access Policy	Select a policy for Workspace ONE to use to control user authentication and access. The default access policy is available if you do not have custom access policies. You can configure these policies in the UEM console.
Open in VMware Browser	Require Workspace ONE to open the application in the VMware Browser. If you use VMware Browser, opening SaaS applications within it adds extra security. This action keeps access within internal resources.
License Approval Required	Require approvals before the application installs and activates a license. • **License Pricing** - Select the pricing model to buy licenses for the SaaS application. • **License Type** - Select the user model for the licenses, named or concurrent users. • **Cost Per License** - Enter the price per license. • **Number of Licenses** - Enter the number of licenses bought for the SaaS application. Configure the corresponding **Approvals** in the **Settings** section of SaaS applications.

4. Add **Client Access Policies** for Office 365 clients. A client access policy allows VMware Identity Manager to manage the Office 365 client UI credentials collected for authentication. Some client examples include VMware Boxer and Microsoft Outlook.

   Select **Add Policy Rule** and complete the settings.

Setting	Description
If the user's client is	Select an available Office 365 client.
And a user's network range is	Select a network range previously configured in the network ranges process.
And the user's device type is	Select the allowed device platform for access.
and user belongs to group(s)	Select user groups allowed to access content according to the criteria in this policy. If you select no groups, the policy applies to all users.
And the client's email protocol is	Select the allowable protocol for the Office 365 client.

Setting	Description
Then perform this action	Allow or deny access to Office 365 applications.

5. View the **Summary** for the SaaS application and move to the assignment process.

Assign SaaS Applications

Assign SaaS applications to users and groups configured in VMware Identity Manager. See Assign SaaS Applications on page 139.

Assign SaaS Applications

Deploy SaaS applications to users and groups configured from your Active Directory system. The system identifies users and groups by a name and a domain. These resources are not the same as Workspace ONE UEM console smart groups.

About Users and User Groups

Configure users and user groups in the VMware Identity Manager administration console. For information, see the topic **Managing Users and Groups** at the VMware Identity Manager documentation site on docs.vmware.com.

Assign Users and Groups to SaaS Applications

Assign SaaS applications by giving users access and use permissions for the application. Users access the SaaS application from Workspace ONE.

1. Navigate to **Apps & Books > Applications > Web > SaaS**.
2. Select the SaaS application and then choose **Assign**.
3. Complete the assignment options.

Setting	Description
Users / User Groups	Enter users and user groups that receive the application assignment. Users and user groups are enabled to sign in to Workspace ONE.
Deployment Type	• **User-Activated** - Requires users to select applications in the Workspace ONE Catalog and to add them to the Launcher to activate them. • **Automatic** - Displays applications in the Launcher of Workspace ONE the next time users log in to the Workspace ONE portal.

4. Save assignment settings.

Provisioning Adapters

Provisioning provides automatic application user management from a single location.

Provisioning adapters allow Web applications to retrieve specific information from the VMware Identity Manager service as required. If provisioning is enabled for a Web application, when you entitle a user to the application in the VMware

Identity Manager service, the user is provisioned in the Web application. The VMware Identity Manager service currently includes provisioning adapters for Microsoft Office 365.

Configuring the Provisioning Adapter for Office 365

The VMware Identity Manager service currently includes provisioning adapters for Microsoft Office 365. Complete the following steps to configuring the Provisioning Adapter for Office 365.

1. Navigate to **Apps & Books > Applications > Web > SaaS** and select **New**.
2. In the **Definition** tab browse for Office 365. Complete the **Definition** tab and Select **Next**. For more information, see Add SaaS Applications in the Workspace ONE UEM console on page 130.
3. Complete the text boxes in the **Configuration** tab. For more information, see Add SaaS Applications in the Workspace ONE UEM console on page 130.
4. Enable **Setup Provisioning**. By default, the provisioning setup is disabled. Once you select **Setup Provisioning**, **Provisioning**, **User Provisioning,** ' **and Group Provisioning** tabs added to the left navigation.
5. Add **Client Access Policies** for Office 365 clients. For information, see Add Office 365 Applications with a Client Access Policy on page 136.
6. In the **Provisioning** tab, select **Enable Provisioning**, and enter the following information:

Setting	Description
Office 365 Domain	Enter the Office 365 domain name. For example, **example.com**. Users are provisioned under this domain.
Application Client ID	Enter the AppPrincipalId obtained when creating the service principal user.
Application Client Secret	Enter the password created for the service principal user.

7. By default, **Provision With License** is disabled. On selecting **Provision With License**, you can enter the following information:

Setting	Description
SKU ID	Enter the SKU information.
Remove License When De-Provisioned	Select the option if you want to remove the license when you deprovision Office 365 application.

8. To verify that the Office 365 tenant can be reached, Select **Test Connection**.
9. Select **Next**.
10. In the **User Provisioning** tab, select the attributes with which to provision users in Office 365.

    Make sure that the following required Active Directory attributes are configured to one of the required attribute names in the User Attributes page:

    a. The Mail Nickname attribute must be unique within the directory and cannot contain any special characters. Map the Mail Nickname attribute to user name. Once mapped, do not change the Mail Nickname.

b. The objectGUID attribute is a custom attribute that first must be added to the User Attribute list. The ObjectGUID

is mapped to the GUID attribute.

Select **Add Mapped Value**, if you want to add an **Attribute Name** and **Value**.

> **Note:** The UserPrincipalName (UPN) is constructed automatically. You do not see the mapped value. The provisioning adapter appends the Office 365 domain to the mailNickname attribute value (user.userName) to create the UPN. This is appended as, user name +@+ O365_domainname. For example, jdow@office365example.com

11. Select **Next**.
12. In the **Group Provisioning** screen, you can complete the **Group Provisioning** task. When a group is provisioned in Office 365, the group is provisioned as a security group. The members of the group are provisioned as users, if they do not exist in the Office 365 tenant. The group is not entitled to resources when provisioned. If you want to entitle the group to resources, create the group and then entitle resources to that group. Select **Add Group** and complete the following steps:
    a. In the **Select Group** text box, search for the group to be provisioned in Office 365.
    b. In the **Mail Nickname** text box, enter a name for this group. The nickname is used as an alias: Special characters are not allowed in the nickname.
    c. Select **Save**.

    You can deprovision a group in the Office 365 application. The security group is removed from the Office 365 tenant. Users in the group are not deleted. To deprovision a group, select the user group and Select **Deprovision** .
13. Select **Next** to view the **Summary** tab.
14. Select Save to Save the configurations or **Save and Assign** to deploy Office 365 to users and groups configured from your Active Directory system.

Settings for SaaS Applications

Settings include features that apply to all SaaS applications in your Workspace ONE environment. Control access with configurations for SAML authentication and with required approvals.

Approvals

Configure SaaS applications to require approval before users can access them. Use this feature when you have SaaS applications that use licenses for access to help manage license activations. When you enable approvals, configure the corresponding, **License Approval Required**, in the applicable SaaS application record.

Approval Workflow

Users view the application in their Workspace ONE catalog and request use of the application. VMware Identity Manager sends the approval request message to the organization's configured approval REST endpoint URL. The system reviews the request and sends back an approved or denied message to VMware Identity Manager. When an application is

approved, the application status turns from **Pending** to **Added** and the application displays in the user's Workspace ONE launcher page.

Approval Engines

The system offers two approval engines.

- **REST API** - The REST API approval engine uses an external approval tool that routes through your Webserver REST API to perform the request and approval responses. You enter your REST API URL in the VMware Identity Manager service and configure your REST APIs with the VMware Identity Manager OAuth client credential values and the callout request and response action.
- **REST API via Connector** - The REST API via the Connector approval engine routes the callback calls through the connector using the Websocket-based communication channel. You configure your REST API endpoint with the callout request and response action.

For information on approvals, see Configure Approvals on page 142.

SAML Metadata

You can use the SAML certificates from the **Settings** page for authentication systems like mobile single sign-on.

Self-Signed Certificates or Certificates from CAs

The VMware Identity Manager service automatically creates a self-signed certificate for SAML signing. However, some organizations require certificates from certificate authorities (CAs). To request a certificate from your CA, generate a certificate signing request (CSR) in **Settings**. You can use either certificate to authenticate users to SaaS applications.

Send the certificate to relying applications to configure authentication between the application and the Workspace ONE system.

For information on retrieving SAML metadata and certificates from the **Settings** page, see SAML Metadata for Single Sign-On with SaaS Applications on page 143.

Application Sources

You can add third-party identity providers to authenticate users in VMware Identity Manager. To configure the provider instance, use the identity provider and service provider metadata you copied from the **Settings** section in the AirWatch Console. For detailed information on how to configure third-party providers, see **Configure a Third-Party Identity Provider Instance to Authenticate Users**, in VMware Identity Manager Documentation.

You can configure your Application Source by selecting the corresponding third-party Identity provider. After the Application source is set up, you can then create the associated applications. For more information, see Configuring Third-Party Identity Providers as an Application Source on page 144.

Configure Approvals

Use approvals for SaaS applications that activate licenses for use. When enabled with the corresponding **License Approval Required** option, users request access to applicable SaaS applications from the Workspace ONE catalog before installation and license activation.

1. Navigate to **Apps & Books > Applications > Web > SaaS** and select **Settings**.
2. Select **Approvals**.
3. Select **Yes** to enable the feature.
4. Select an **Approval Engine** the system uses to request approvals.
5. Enter the callback **URI** (Uniform Resource Identifier) of the REST resource that listens for the callout request.
6. Enter the **Username**, if the REST API requires credentials to access.
7. Enter the **Password** for the user name, if the REST API requires credentials to access.
8. Enter the SSL certificate in PEM (privacy-enhanced electronic mail) format for the **PEM-format SSL Certificate** option, if the REST resource runs on a server that has a self-signed certificate or a certificate not trusted by a public certificate authority and uses HTTPS.

For information on the corresponding option **License Approval Required**, see the applicable topic:

- For Office 365 applications, see Add Office 365 Applications with a Client Access Policy on page 136.
- For regular SaaS applications, see Add SaaS Applications in the Workspace ONE UEM console on page 130.

SAML Metadata for Single Sign-On with SaaS Applications

Retrieve SAML metadata and certificates from the **Settings** page. Use the metadata and certificates with other systems for single sign-on capabilities.

Before Replacing SSL Certificates

If you replace an existing SSL certificate, this action changes the existing SAML metadata.

Important: All single sign-on connections that depend on the existing SAML metadata break when the CSR generation creates the SAML metadata.

Note: If you do replace an SSL certificate, you must update SaaS applications that you configure for mobile single sign-on with the latest certificate.

Download the Self-Signed SAML Metadata or Generate a CSR

Copy the SAML signing certificate, and copy and save the identity and service provider metadata. You can also generate a certificate signing request to apply for an SSL certificate from your certificate authority.

1. Navigate to **Apps & Books > Applications > Web > SaaS** and select **Settings**.
2. Select **SAML Metadata > Download SAML Metadata** and complete the tasks.

Setting	Description
SAML Metadata	Copy and save the **Identity Provider** metadata and the **Service Provider** metadata. Select the links and open a browser instance with the XML data. Configure your third-party identity provider with this information.

Setting	Description
Signing Certificate	Copy the signing certificate that includes all the code in the text area. You can also download the certificate to save it as a TXT file.

3. Select **Generate CSR** and complete the tasks for requesting a digital identity certificate (SSL certificate) from your certificate authority. This request identifies your company, domain name, and public key. The third-party certificate authority uses it for issuing the SSL certificate. To update the metadata, upload the signed certificate.

Setting	Description
Enter a New Certificate Signing Request	
Common Name	Enter the fully qualified domain name for the organization's server.
Organization	Enter the name of the company that is legally registered.
Department	Enter the department in your company that the certificate references.
City	Enter the city where the organization is legally located.
State / Province	Enter the state or province where the organization legally resides.
Country	Enter the legal country of residence for the organization.
Key Generation Algorithm	Select an algorithm used to sign the CSR.
Key Size	Select the number of bits used in the key. Select 2048 or larger. RSA key sizes smaller than 2048 are considered insecure.
Replace a Certificate Signing Request	
Certificate Signing Request	Download the certificate signing request (CSR). Send the CSR to the third-party certificate authority. The third-party certificate authority sends you an SSL certificate.
Upload SSL Certificate	Upload the SSL certificate received from your third-party certificate authority.

Configuring Third-Party Identity Providers as an Application Source

You can add third-party identity providers as an application source in the Settings for SaaS Applications. Adding an identity provider as an application source streamlines the process of adding individual applications from that provider to the end-user catalog. Adding an identity provider as an application source streamlines the process of adding individual applications from that provider to the end-user catalog. To begin, entitle the ALL_USERS group to the application source and select an access policy to apply.

Web applications that use the SAML 2.0 authentication profile can be added to the catalog. The application configuration is based on the settings configured in the application source. Only the application name and the target URL are required to be configured.

When you add applications, you can entitle specific users and groups and apply an access policy to control user access to the application. Users can access these applications from their desktops and mobile devices.

The configured settings and policies from the third-party application source can be applied to all applications managed by the application source. Sometimes, third-party identity providers send an authentication request without including which application a user is trying to access. If VMware Identity Manager receives an authentication request that does not include the application information, the backup access policy rules configured in the application source are applied.

The following identity providers can be configured as application sources.

- Okta
- PingFederated server from Ping Identity
- Active Directory Federation Services (ADFS)

Adding an Application Source

You can configure your Application Source by selecting the third-party identity provider. After the Application Source is set up, you can then create the associated applications and entitle the users. For more information, see Add Application Source for the Third-Party Identity Providers on page 145.

Entitling Users to the Application Source

You can set the entitlements for the Application Source to **All Users** or add Users / User Group. For more information, see Add Users to the Application Source on page 148.

Adding Applications Managed by the Application Source

After the identity provider is configured as an application source, you can create the associated applications for each of the third-party identity providers. For more information, Add Applications Managed by the Application Source on page 148.

Add Application Source for the Third-Party Identity Providers

Configure your Application Source by selecting the third-party identity provider. After the Application Source is set up, you can then create the associated applications and entitle the users.

1. Navigate to **Apps & Books > Applications > Web > SaaS** and select **Settings**.
2. Select **Application Sources**.
3. Select the third-party identity provider. The third-party identity provider's Application Source wizard is displayed.
4. Enter a descriptive name for the application source and click **Next**.
5. **Authentication Type** is defaulted to SAML 2.0 and is read-only.

6. Modify the application source **Configuration**.

Setting	Description
Configuration	• **URL/XML** is the default option for SaaS applications that are not yet part of the Workspace ONE catalog. • **Manual** is the default option for SaaS applications added from the catalog.
URL/XML	
URL/XML	Enter the URL if the XML metadata is accessible on the Internet. Paste the XML in the text box if the XML metadata is not accessible on the Internet, but you have it. Use manual configuration if you do not have the XML metadata.
Relay State URL	Enter a URL where you want SaaS application users to land after a single sign-on procedure in an identity provider-initiated (IDP) scenario.
Manual	
Single Sign-On URL	Enter the Assertion Consumer Service (ACS) URL. Workspace ONE sends this URL to your service provider for single sign-on.
Recipient URL	Enter the URL with the specific value required by your service provider that states the domain in the SAML assertion subject. If your service provider does not require a specific value for this URL, enter the same URL as the **Single Sign-On URL**.
Application ID	Enter the ID that identifies your service provider tenant to Workspace ONE. Workspace ONE sends the SAML assertion to the ID. Some service providers use the **Single Sign-On URL**.
Username Format	Select the format required by the service providers for SAML subject format.
Username Value	Enter the Name ID Value that Workspace ONE sends in the SAML assertion's subject statement. This value is a default profile field value for a username at the application service provider.
Relay State URL	Enter a URL where you want SaaS application users to land after a single sign-on procedure in an identity provider-initiated (IDP) scenario.

7. Modify the **Advanced Properties**.

Setting	Description
Sign Response	Enter the URL to direct users to the SaaS application on the Internet.
Sign Assertion	Enter the Assertion Consumer Service (ACS) URL. Workspace ONE sends this URL to your service provider for single sign-on.

Setting	Description
Encrypt Assertion	Enter the URL with the specific value required by your service provider that states the domain in the SAML assertion subject. If your service provider does not require a specific value for this URL, enter the same URL as the **Single Sign-On URL**.
Include Assertion Signature	Enter the ID that identifies your service provider tenant to Workspace ONE. Workspace ONE sends the SAML assertion to the ID. Some service providers use the **Single Sign-On URL**.
Signature Algorithm	Select SHA256 with RSA as the secure encrypted hash algorithm.
Digest Algorithm	Select SHA256.
Assertion Time	Enter the SAML assertion time in seconds.
Request Signature	If you want the service provider to sign the request it sends to Workspace ONE, enter the public signing certificate.
Encryption Certificate	Enter the public encryption certificate if you want the SAML request from the application service provider to Workspace ONE to be signed.
Application Login URL	Enter the URL for your service provider's login page. This option triggers the service provider to initiate a login to Workspace ONE. Some service providers require authentication to start from their login page.
Proxy Count	Enter the allowable proxy layers between the service provider and an authenticating identity provider.
API Access	Allow API access to this application.

8. Configure **Custom Attribute Mapping**.If your service provider allows custom attributes other than ones for single sign-on, add them.
9. Select **Open in VMware Browser**if you want to open the application in the VMware Browser. However, it requires Workspace ONE to open the application in the VMware Browser. If you use VMware Browser, opening SaaS applications within it adds extra security. This action keeps access within internal resources.
10. Click **Next**.
11. To secure signing in to application resources, select the **Access policies**. Click **Next** to view the **Summary** page.
12. Click **Save**.

Note: If you select **Save and Assign** while configuring the application source, you set the entitlements for the application source to **All Users**. However, you can change the default settings and manage the user entitlements and add users or user groups. For more information, see Add Users to the Application Source on page 148

Add Applications Managed by the Application Source

After the identity provider is configured as an application source, you can create the associated applications for each of the third-party identity providers.

For example, use the following instructions to add applications for **OKTA** identity provider.

1. Navigate to **Apps & Books > Applications > Web > SaaS > New**.
2. Complete the options on the **Definition** tab.
3. In the **Configuration** tab, you can select **OKTA** from the **Authentication Type** drop-down menu.

Add Users to the Application Source

You can set the entitlements for the application source to **All Users** or add Users / User Groups. By default, if you select **Save and Assign** while configuring the application source, you set the entitlements for the application source to **All Users**.

To manage the user assignment:

1. Navigate to **Apps & Books > Applications > Web > SaaS** and select **Settings**.
2. Select **Application Sources**.
3. Click **All Users** for the corresponding Application Source if you want to override the settings.
4. Enter the names of the groups or users.
5. You can search for users or groups by starting to type a search string and allowing the auto-complete feature to list the options, or you can click browse to view the entire list.
6. Click **Save**.

SSO Between Workspace ONE UEM and VMware Identity Manager for SaaS Apps and Access Policies

The Workspace ONE UEM console and the VMware Identity Manager console use an authorization code work flow that allows access to both consoles with single sign-on (SSO). This feature aims to allow access to the VMware Identity Manager console for admins in the UEM console to work on SaaS application configurations.

This flow is specific to SaaS applications and access policies in Workspace ONE UEM. Additions and edits made in Workspace ONE UEM are reflected in Identity Manager.

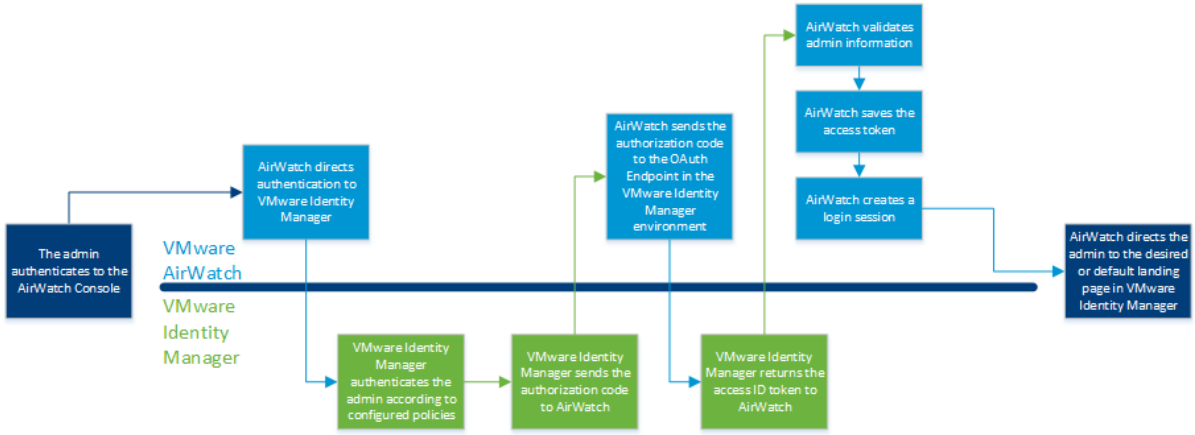
Register the OAuth Client During Setup

When you set up VMware Identity Manager in the UEM console, you register the OAuth client as part of the setup wizard. The OAuth client registration is a prerequisite for this SSO feature to work.

Workflow

VMware Identity Manager and Workspace ONE UEM work in the back-end to authenticate the Workspace ONE UEM admin to VMware Identity Manager. The VMware Identity Manager Console passes an ID token to Workspace ONE UEM.

This token contains information about the admin and the authentication so that the admin can access both consoles. The two consoles follow the depicted process.



Chapter 7: Web Applications

Web applications provide end-users access to URLs directly from an icon on their devices. The Workspace ONE UEM system has two types of web applications, SaaS and web links. SaaS applications are integrated with the VMware Identity Manager system. Web links are applications configured solely in the Workspace ONE UEM console.

Application Type Descriptions

To find out what Workspace ONE UEM supports for platforms and operating systems, see Workspace ONE UEM Application Types and Their Supported Platforms on page 7.

SaaS Applications

SaaS applications are URLs that users can start from an icon on their device. These applications offer access control with single sign-on features and conditional access policies. Originally, admins managed these applications in their VMware Identity Manager instance. As the Workspace ONE platform extends with features, one feature enables admins to manage SaaS applications in the UEM console.

For general information about SaaS applications and where to find information for VMware Identity Manager, see SaaS Applications in Workspace ONE UEM on page 127.

For requirements to set up before you can access SaaS applications, see Requirements to Support SaaS Applications on page 128.

Configure and Assign

For information about configure SaaS applications in the UEM console, see Add SaaS Applications in the Workspace ONE UEM console on page 130.

For information on client access policies and how to assign them to Office 365 applications, see Client Access Policy Description on page 136 and Add Office 365 Applications with a Client Access Policy on page 136.

For information on assigning SaaS applications to users and user groups, see Assign SaaS Applications on page 139.

For information on settings for SaaS applications, see Settings for SaaS Applications on page 141.

Access Policies

Use access policies to control authentication and access sessions of SaaS applications. For information, see Use Access Policies with SaaS Applications on page 157.

VMware Identity Manager Information

For information about VMware Identity Manager, see VMware Identity Manager Documentation.

Web Links Applications

Web links are URLs that users can start from an icon on their device. Read a description of web links applications and view a list of platforms that support their use in Web Links Application Features and Supported Platforms on page 151.

Read a description of web applications and view a list of platforms that support their use in Web Links Application Features and Supported Platforms on page 151.

Web Links Admins and Management

Your deployment might have an admin that manages your web applications. For configurations specific to this type of admin, see Web Apps Admins and Roles Exceptions on page 153.

Use the View Devices page to manage your web applications. For the actions available on the View Devices page, see Configure View Devices for Web Links Applications on page 155.

Deployment Methods

There are two methods to deploy web applications. For an explanation of the two methods, see Web Links Tab or Device Profiles on page 152.

You can edit configurations in either system because the systems share settings. See Web Links Application Behaviors in Apps & Books and Devices on page 152 for more information.

Apps & Books Web Tab Method

For the configurations to add web applications in the Apps & Books section of the console, see Add Web Links Applications on page 153.

Device Profile Method

For the configurations to add web applications by device profile, see the listed topics.

- Android – Configure Bookmarks (Android)
- iOS –
- macOS – Configure a Web Clips Profile (macOS)
- Windows Desktop – Configure a Web Clips Profile (Windows Desktop)

Web Links Application Features and Supported Platforms

Web links applications function much like an application on a device. They provide end users a way to access a URL directly from an icon on the menu of their device. The end user sees the web links application icon and title, selects the application, and connects directly to a specified URL.

Web links applications are useful for navigation to extended URLs with many characters. You can place web links application icons on the springboard. These icons connect end users to internal content repositories or login screens, so end users do not open a browser and type out a long URL.

You can add web links applications using two methods.

- As an application in the Apps & Books section of the Workspace ONE UEM console.
- As a device profile in the Devices section of the UEM console.
  See the applicable platform guide for the profile you want to push.
  - Bookmark profiles – Android
  - Web clip profiles – Apple iOS, macOS, and Windows Desktop

Supported Platforms for Web Links Applications

The UEM console supports the various platforms to push and manage web links applications.

- Android
- Apple iOS
- macOS
- Windows Desktop

Workspace ONE UEM Web Links Apps and Workspace ONE

Workspace ONE now displays and allows access to applications located in the **Web Links** tab in the UEM console. Workspace ONE pulls the URL, the application description, and the icon from Workspace ONE UEM.

Web Links Tab or Device Profiles

Add web links applications on the Web tab and with a device profile. You can add web links applications with both methods because the two methods are not mutually exclusive.

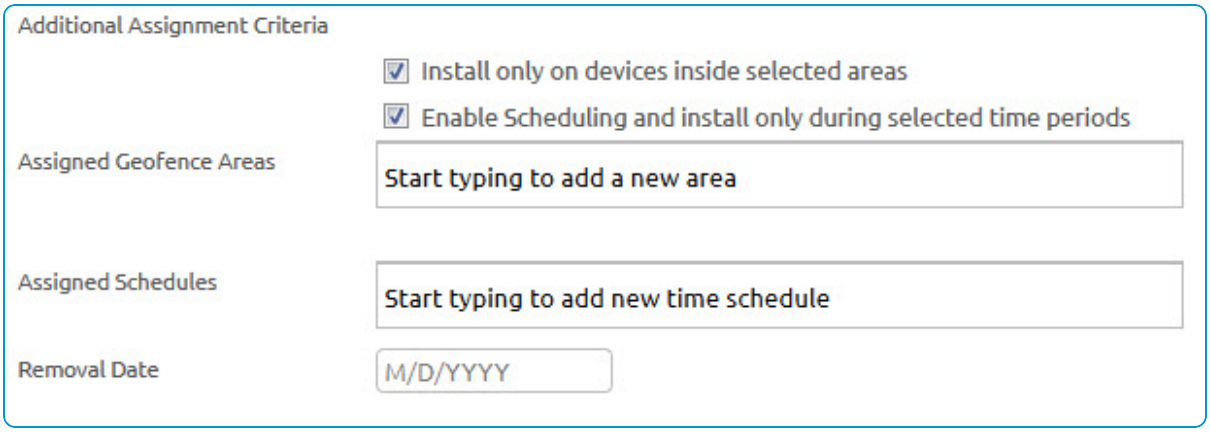
Option	Description
Web Tab	The Web tab is in the Apps & Books section of the Workspace ONE UEM console. This placement allows you to add and edit web links applications without having to add Bookmarks and Web Clips in the Devices section of the UEM console. To add more functionality, edit the device profile version of the web links application.
Device Profiles	Device profiles let you do everything that the Web tab does. The device profile also includes MDM features that you can control.

Web Links Application Behaviors in Apps & Books and Devices

Single web links applications created in **Apps & Books** and single web links applications created using device profiles share configurations.

- All MAM functions are available in both areas of the console (**Apps & Books** and **Devices**).
- A single web clip (or bookmark) payload that is the only payload in a profile added in **Devices** displays in the **Apps & Books** section. You can edit these singular web clips in both sections.

- Multiple web clips in a single profile or a single web clip with other payloads in the **Devices** section do not display in the **Apps & Books** section. You must work with these web clips in **Devices**.
- You can add MDM features from the **Devices** section with the device profile version of the web links application. For example, enter assignment criteria like a Geofencing area and installation scheduling using the **General** payload of a web clip or bookmark.



Web Apps Admins and Roles Exceptions

You can configure an administrative role that manages only web links applications. You can restrict the access and permissions of the admin to what is available on the **Web** tab of **Apps & Books**.

If you want to create such an admin, navigate to **Accounts > Administrators > Roles > Add Role > Apps & Books > Web Apps** in the Workspace ONE UEM console. The permissions for a Web App admin include many of the tasks carried out by the general admin.

Roles Exception

Your deployment may require the Web App admin to install and delete web links applications and their corresponding device profiles. If your Web App admin performs these tasks, enable the permissions for it in **Accounts > Administrators > Roles** in the UEM console.

Enable the following categories to give the Web App admin access to device profiles.

- **Device Management > Device Details > Profiles > Device Install Profile**
- **Device Management > Device Details > Profiles > Device Remove Profile**

Add Web Links Applications

Add URLs for sites you want to manage and push to devices as web links applications with the Web Links tab in Apps & Books.

1. Navigate to **Apps & Books > Applications > Web > Web Links** and select **Add Application**.
2. Select the **Organization Group** and the **Platform** and then choose **Continue**.
3. Complete the settings on the **Details** tab.

Setting	Description
Name	Name of the web links app to be displayed in the Workspace ONE UEM console, on the device, and in the AirWatch Catalog.
URL	The address of the Web app.
Descriptions	A brief description of the Web app that indicates its purpose. This option is not displayed in the AirWatch Catalog.
Managed By	The organization group with administrative access to the Web app.

4. Upload a custom icon using a GIF, JPG, or PNG format, for the application on the **Images** tab that end users view in the AirWatch Catalog before installing the application to their devices and that displays as the icon of the Web app on the device.

   Images are currently not available for Windows Desktop.

   For best results, provide a square image no larger than 400x400 pixels and less than 1 MB when uncompressed. The graphic is automatically scaled and cropped to fit. If necessary, the system converts it to PNG format. Web Clip icons are 104 x 104 pixels for devices with a Retina display or 57 x 57 pixels for all other devices.

5. Complete the settings on the **Assignment** tab.

Setting	Description
Assigned Groups	The smart group to which you want the Web app added. Includes an option to create a new smart group which can be configured with specifications for minimum OS, device models, ownership categories, organization groups and more.
Exclusions	If **Yes** is selected, a new option displays called **Excluded Smart Groups**. This setting enables you to select the smart groups you want to exclude from the assignment of this Web app.
Push Mode	Select how the system pushes Web apps to devices. • **On Demand** – Deploys content to a catalog or other deployment agent and lets the device user decide if and when to install the content. This option is the best choice for content that is not critical to the organization. Allowing users to download the content when they want helps conserve bandwidth and limits unnecessary traffic. • **Automatic** – Deploys content to a catalog or other deployment agent on a device upon enrollment. After the device enrolls, the system prompts users to install the content on their devices. This option is the best choice for content that is critical to your organization and its mobile users.

Setting	Description
Advanced	Offers extra functionality depending on the platform. • **Android** **Add to Homescreen** – Adds the web links application to the homescreen of the device. ◦ The system always places Web apps in the bookmark section if the default browser of the device. If you do not enable this option, end-users can access Web apps from the bookmarks. • **Apple iOS** ◦ **Removable** – Allows end users to use the long press feature to remove this Web app off their devices. ◦ **Full Screen** – Opens the Web app in full screen mode on iOS 6+ devices.

6. Select **Save & Publish** to push the web links application to the AirWatch Catalog.

Configure View Devices for Web Links Applications

Use the View Devices page to display devices to which you assigned web links applications. You can also manually install and delete web links applications from listed devices.

Web App admins must have the correct Administrator Role permissions or they cannot manually install or delete web links applications. See Web Apps Admins and Roles Exceptions on page 153 for more information.

1. Navigate to **Apps & Books > Applications > List View > Web**.
2. Find the web links application you want to work with and select the linked numbers in the **Install Status** column.
3. Use the column data and the actions menu to access the listed functions.

Setting	Description
Friendly Name	Navigates to the **Details View** of the selected device. Use the **Devices Details View** to edit device information, view compliance policies, view assigned device profiles, view assigned users, and many more MDM features pertaining to the device.
C/E/S User	Navigates to the **Details View** of the user of the selected device. Use the **User Details View** to edit user information, view event logs, view assigned User Groups, and view other assigned devices.
Install Profile	Installs a web links application and its corresponding device profile to a listed device.
Delete Profile	Deletes a web links application and its corresponding device profile from a device.

Chapter 8:
Manage Applications

After deploying applications, you can confirm their assignment and installation from the Workspace ONE UEM console. You can also manage application versions and deploy new updated applications. Use access policies to manage access to SaaS applications.

Basics of Managing Applications

You have many views and pages available to manage applications.

General Pages – Native List View, Details View, and Manage Devices

Use the Native List View as a central location to sort, filter, and search for data so you can perform management functions on internal, public, purchased, and web applications. See Native List View Option Descriptions for Applications on page 160 for options displayed in the Native List View.

Use the Details View for internal applications as an alternative page to perform management functions and audit information about the application. See Details View Setting Descriptions on page 161 for options displayed in the Details View.

Use the Manage Devices option to install and remove many applications at once, to notify many devices at once, and to reinvite users to the Apple Volume Purchase Program (VPP). See Configure Manage Devices on page 164 for details on available options.

Specialized Pages – Manage Feedback, User Ratings, View Logs, and SDK Analytics

Use the Manage Feedback option to request, clear, and view feedback for applications that run on Apple iOS 7+. See Configure Manage Feedback on page 165 for configurations.

View user ratings and comments and delete user comments about applications on the User Ratings page. See Configure User Ratings on page 166 for listed options.

Use the View Logs feature to access available log files pertaining to your SDK applications and wrapped applications. See Configure View Logs for Internal Applications on page 172 .

Display events and data use information for applications that use SDK functionality. Workspace ONE UEM reports event analytics by the application ID and event name and data use analytics by device. For descriptions of event and data analytics and to know how to export the data from the console, see Access SDK Analytics Apps That Use SDK Functionality on page 173.

Application Longevity Management

Application longevity depends on the application's status as active or inactive. See Active and Inactive Status on page 166 for an explanation of these states.

Delete, Retire, and Deactivate

You might occasionally need to delete applications to free up space and to remove unused applications. For a description of the delete function and for suggestions to alternatives to the delete function, see The Delete Action Description and Its Alternatives on page 166.

To remove all versions from devices at a specific organization group and all children organization groups, you can deactivate an application. See The Deactivate Option Description and the Relation to Other Active Versions on page 167 for information about this alternative to the delete function.

You can retire an application and this action has several outcomes depending on the push mode, application status, and the enabling of the Retire Previous Version option. See The Retire Option Description and the Relation to Application Lifecycle Components on page 167 for information about this alternative to the delete function.

Version Option

You can version internal applications to test these applications in the text box. For information on versioning and its uses, see Internal App Versions in Workspace ONE UEM on page 169.

Access Policies

Access policies secure SaaS applications by mapping requesting IP addresses to network ranges before allowing users access. These policies also designate the type of devices that users can use to access SaaS applications. For information, see Use Access Policies with SaaS Applications on page 157.

Use Access Policies with SaaS Applications

To provide secure access to start SaaS applications, you configure access policies. Access policies include rules that specify criteria that must be met to sign in to the Workspace ONE portal and to use applications.

For details about access policies in the VMware Identity Manager system, see VMware Identity Manager Documentation and search for **Managing Access Policies.**

For information on SaaS applications, see SaaS Applications in Workspace ONE UEM on page 127.

Flexibility of Access Policies

Access policies allow lenient control in the network and restrict access out of the network. For example, you can configure one access policy with the following rules.

- Allow a network range access with single sign-on within the company network.
- Configure the same policy to require multi-factor authentication (MFA) when off the company network.
- Configure the policy to allow access to a specific user group with a specific device-ownership type. It can block access to others not in the group.

Default Access Policy and Application-Specific Access Policies

Default Access Policy - The VMware Identity Manager service and the Workspace ONE UEM console include a default policy that controls access to SaaS applications as a whole. This policy allows access to all network ranges, from all device

types, for all users. You can edit the default access policy but you cannot delete it.

Important: Edits to the default access policy apply to all applications and can impact all users ability to access Workspace ONE.

To edit the default access policy, navigate to **Apps & Books > Applications > Access Policies > Edit Default Policy**. Then, follow the procedure listed in Configure Application-Specific Access Policies on page 158.

Application-Specific Access Policies - Create application-specific access policies to restrict access to applications. Configure IP addresses, authentication methods, and session time permitted for access.

Prerequisites

- Configure the network ranges for your deployment. See Add Network Ranges for Use in Access Policies on page 158.
- If you plan to edit the default policy (to control user access to the service as a whole), configure it before creating an application-specific policy.

Add Network Ranges for Use in Access Policies

Define network ranges with IP addresses allowed for user login to SaaS applications. Assign these ranges when you apply access rules to SaaS applications.

Prerequisites

You need the network ranges for your VMware Identity Manager deployment and your Workspace ONE UEM deployment. The organization's network department usually has the network topology.

Procedure

1. Navigate to **Apps & Books > Applications > Access Policies > Network Ranges**.
2. Select a name and edit the range or select **Add Network Range**.
3. Complete the options for defining ranges.

Setting	Description
Name	Enter a name for the network range.
Description	Enter a description for the network range.
IP Ranges	Enter IP addresses that include the applicable devices in the range.
Add Row	Define multiple IP ranges.

Add Network Ranges to Access Policies

Assign network ranges to application-specific access policies. For more information, see Configure Application-Specific Access Policies on page 158.

Configure Application-Specific Access Policies

Add application-specific access policies for control of user access to SaaS applications.

1. Navigate to **Apps & Books > Applications > Access Policies > Add Policy.**
2. Complete the options on the **Definition** tab.

Setting	Description
Policy Name	Enter a name for the policy. Allowable name criteria includes the listed parameters. • Begin with a letter, either lowercase or uppercase, from a-Z. • Include other letters, either lowercase or uppercase, from a-Z. • You can include dashes. • You can include numbers.
Description	(Optional) Provide a description of the policy.
Applies to	Select SaaS applications to which you want to assign the policy.

3. Complete the options on the **Configuration** tab and select **Add Policy Rule** or edit an existing policy.

Setting	Description
If a user's network range is	Select a network range previously configured in the network ranges process.
And user accessing content from	Select device types allowed to access content according to the criteria in this policy.
and user belongs to group(s)	Select user groups allowed to access content according to the criteria in this policy. If you select no groups, the policy applies to all users.
Then perform this action	Allow authentication, deny authentication, or allow access with no authentication.
then the user might authenticate using	Select the initial authentication method for accessing content.
If the preceding method fails or is not applicable, then	Select a fallback method for authenticating to content in case the initial method fails.
Add fallback method	Add another authentication method. The system processes methods from the top down, so add them in the order you want the system to apply them.
Reauthenticate after	Select the length of an allowable access session before the user must reauthenticate to access the content.
Advanced Properties	

Setting	Description
Custom Error Message	Enter a custom "access denied" error message the system displays when user authentication fails.
Custom Error Link Text	Enter the text for the link that navigates users away from the "access denied" error page when authentication fails.
Custom Error Link URL	Enter the URL address that navigates users away from the failed authentication page.

4. View the **Summary** for the application-specific access policy.

Native List View Option Descriptions for Applications

The Native List View is a central location to sort, filter, and search for data so you can perform management functions on internal, public, purchased, and web applications.

Each Native List View in Apps & Books is slightly different and available functions vary, so the system does not display every option for every application type.

Setting	Description
Filters	• **Platform** – View applications by platform. This filter helps you find numerous applications so you can perform large-scale management functions simultaneously. • **Status** – View applications by status: Active, Retired, or Inactive. This view is helpful to return applications to previous statuses. • **Category** – Locate applications specifically for a default or custom category. Find applications tagged as Finance, Business, Social Networking, and many other options. This filter helps you find large groups of applications. • **Requires Renewal** – Find Apple iOS applications that use a provisioning profile to function. This filter locates applications with provisioning profiles you can update. • **App Type** – View applications depending on type. Types include Public or Custom B2B options.
Add	Upload a local application, search for a public application in an app store, or add an order with redemption codes.
Layout	Arrange items on the tab using the available formats. • Summary lists details of the application in the UI. • Custom selects what details you want the system to display.
Refresh	Refresh the items in the UI. Use refresh when you edit items and push edits to applications on devices.
Export	Export all items on all pages to a CSV file.
Search List	Find applicable applications you want to locate by name.

Setting	Description
Toggle Filters	Display or hide filters.
Assign	To deploy the application, navigate to the flexible deployment page by selecting the radio button to the left of the application icon. You must select the radio button to display the **Assign** function.
Delete	Delete applications from the Workspace ONE UEM console by selecting the radio button to the left of the application icon. You must select the radio button to display the **Delete** function, and the system deletes one application at a time.
Edit	To change the application record, select the pencil icon.
Name	Access the **Summary** tab of the **Details View** for internal applications so you can edit flexible deployments, track application installations, renew provisioning profiles, and select app wrapping statuses.
Install Status	Access a page with information about devices assigned to the application. Internal applications go to the **Devices** tab of the **Details View**. Perform management functions on devices like send messages, install applications, and remove applications. Web applications go to the View Devices page which offers management functions to install or delete applications.
Actions Menu	• **Manage Devices** – Offers options for installing, removing, or notifying users about applications. • **Manage Feedback** – Control feedback for applications for Apple iOS. This option displays under specific conditions. Displays only under specific conditions • **Publish** – Publish the managed distribution content, manually, to devices. • **Notify Devices** – Send a notification to devices concerning the VPP application. • **Deactivate** – Removes an application and all versions of it from all managed devices. • **User Ratings** – Shows the application rating and feedback. You can clear ratings with the **Delete Rating** option for internal and public applications. • **View Events** – Shows device and console events for applications and allows you to export these events as a CSV file. • **Delete** – Removes the application from devices and from the UEM console.

Details View Setting Descriptions

Access the details view from the name of the application on the list view in the Workspace ONE UEM console. It is an alternative page to perform management functions and audit information about internal applications and public applications that are part of a Microsoft Store for the Business deployment.

Supported Application Types

This view is available for the following application types:

- Internal applications
- Public applications that are part of a Microsoft Store for the Business deployment

Setting Descriptions

Available tabs vary depending on the application type.

- Details View Tabs

Setting	Description
Summary	Displays information to help you track installed application versions and application deployments.
Details	Displays information configured on the **Details** tab during the initial upload.
Licenses	Displays online and offline licenses claimed for a Microsoft Store for Business, public application.
Devices	Offers options to notify devices about applications and to install or remove applications from the device.
Screenshots	Displays screenshots of the Microsoft Store for the Business application's user interface.
Assignment	Displays the configured flexible deployments (assignments) for the application or the groups assigned to the application.
Files	Displays the files added during the initial upload. Find application files, provisioning profiles, Apple Push Notification Service (APNs) files, and architecture applications files. Auxiliary files are required to run certain application files in the mobile environment.
More	Lists optional features: ◦ **Images** – If you uploaded mobile images, tablet images, and icons with the application, displays them. ◦ **Terms of Use** – Displays the terms of use, if configured, that device users must view and accept before they can use the application. ◦ **SDK** – Displays information pertaining to the use of the Workspace ONE UEM Software Development Kit (SDK). It lists the SDK profile that applies to the application, which enables its Workspace ONE UEM functionality. It also lists the application profile, which controls the use of certificates for communication. ◦ **App Wrapping** – Displays information pertaining to the wrapping of the application. Some of the information on this tab includes the app wrapping status, the wrapped engine version used, and the size of the wrapped application.

- Actions Menu Options

Setting	Description
Edit	Displays the application record for editing the tabs first configured when you uploaded the application.
Assign	Displays the flexible deployment record allowing you to add assignments and prioritize them or enables you to assign and edit groups assigned to the application.
Sync Licenses	Syncs online and offline licenses claimed by applications in a Microsoft Store Business integration.
Add Version	Upload a different version of an application and push it to devices.
Manage	Control removal of applications and flexible deployment batching. This feature is for admins, and is not available to all users. ◦ **Retire** – Removes an application from all managed devices. For iOS devices, if an older version of the application exists in the Workspace ONE UEM solution, then this older version is pushed to devices. ◦ **Deactivate** – Removes an application and all versions of it from all managed devices. ◦ **Bypass Batching** – Bypasses flexible deployment batching and releases all installation commands for applications.
View	Display the popularity of applications and issues with applications for troubleshooting application problems. ◦ **User Ratings** – Accesses ratings of applications using the star system, which you can use to gauge the popularity of internal applications. ◦ **Events** – Shows device and console events for applications and allows you to export these events as a CSV file.
Version	Add updated versions of applications, and accesses previous versions of internal applications. ◦ **Add Version** – Updates your internal application with a new version. ◦ **Other Versions** – Shows previous versions of an internal application that were added to the UEM console.
Delete Application	Remove the application from devices and from the UEM console.
Other Actions	If the application uses app wrapping or SDK functionality, displays other options. If the application does not use app wrapping or SDK, the system does not display them. ◦ **Manage Feedback** – Control feedback for applications for Apple iOS. This option appears under specific conditions so review the topic for these conditions. ◦ **View Analytics** – Exports the analytics for internal applications that use the Workspace ONE UEM Software Developers Kit (SDK). ◦ **View Logs** – Downloads or deletes log files for internal SDK and wrapped applications.

Make App MDM Managed If User Installed

Workspace ONE UEM can assume management of user-installed applications (iOS and Windows) without requiring the deletion of the previously installed application from the device. Workspace ONE UEM labels the feature **Make App MDM Managed if User Installed**. In the past, Workspace ONE UEM did not manage these applications unless the user removed the previous version.

Enable **Make App MDM Managed if User Installed** when you assign the application with the flexible deployment feature.

Supported iOS Device Statuses

Workspace ONE UEM can assume management of user-installed applications on devices in either the supervised or unsupervised status.

Time to Managed Status

The time the system takes over management capabilities of applications depends on the enrollment status of the device. The system manages the application upon the device enrollment or when you publish it. The following table outlines these two scenarios.

Device Enrollment Status	Initiate MDM Managed	Result
Not enrolled	Select **Make App MDM Managed if User Installed**, save, and publish the application.	System manages the application when the device enrolls.
Enrolled	Select **Make App MDM Managed if User Installed**, save, and publish the application.	System manages the application when you save and publish it.

Configure Manage Devices

Use the Manage Devices option to install and remove many applications at once, to notify many devices at once, and to reinvite users to the Apple Volume Purchase Program (VPP).

Filters

- **Status** helps find devices that have installed or not installed assets.
- **User Invite** helps find devices to invite to the Apple VPP.

Manage Devices

1. Navigate to **Apps & Books > Applications > Native** and select either the **Public** or **Purchased** tab.
2. Select the **Manage Devices** option (🔍) from the actions menu.
3. Select from the actions menu or select the desired options. You can act on specific devices (selected and filtered) or act on all devices (listed).

Setting	Description
Install	Install an application on a single device or on multiple devices.
Remove	Remove an application from a single device or off multiple devices. • macOS Workspace ONE UEM cannot remove VPP applications (purchased) for macOS devices. • Windows Desktop and Phone This function removes the application but not the license for public applications acquired through the Microsoft Store for Business.
Notify	Notify devices about an asset. Settings include email, SMS, push, and message template options for sending messages.
Reinvite (Only Purchased)	Send an invitation to join the Apple VPP, managed distribution, to devices. Devices must run Apple iOS v7.0.3+. The page also lists devices that accepted the invitation.

Access the Manage Feedback Page

To access and use the **Manage Feedback** feature for applications running Apple iOS 7+, the Workspace ONE UEM console requires assignment of the application to a device and communication from a device about the application.

1. You must assign at least one Apple iOS 7+ device to the application.
2. An assigned Apple iOS 7+ device must transmit to the UEM console that it contains feedback and data.

Note: You cannot see the **Manage Feedback** option in the Console unless at least one Apple iOS 7+ device is assigned to the application and that device has transmitted feedback data to the Console.

Configure Manage Feedback

Use the **Manage Feedback** option to request, clear, and view feedback applications that run on Apple iOS 7+.

Follow the procedure to access and configure **Manage Feedback** options.

1. Navigate to **Apps & Books > Applications > Native** and select either the **Public** or **Internal** tab.
2. Perform one of the following actions:
   - For Public applications – Select the **Manage Feedback** option from the actions menu.
   - For Internal applications – Select the application and then select **Manage Feedback** from the actions menu.
3. Complete the applicable settings.

Setting	Description
Request Feedback	Initiate a command to the device to retrieve the feedback from its location in the application on the device.
Clear Feedback	Initiate a command to clear data in the directory where the feedback is stored in the application on the device.
View Feedback	Display the **View Feedback** page to download and delete feedback. Download the file as a ZIP file. When you delete the feedback from here, the system deletes the information from the Workspace ONE UEM console.

Configure User Ratings

Clear the star values by deleting ratings on the **User Ratings** page. Delete ratings values if they no longer accurately reflect the effectiveness and popularity of applications in your deployment.

1. Navigate to **Apps & Books > Applications > Native** or to **Apps & Books > Books > List View** and select either the **Public** or **Internal** tab.
2. Select **More>Users Rating** from the actions menu or from the details view of the asset.
3. Select **Delete Rating** to clear the stars.

Active and Inactive Status

The active or inactive status marks applications as available or unavailable for versioning features such as retire and roll back.

If you try to version an application and it is the wrong status, then you might not make the expected version of an application available to your device users.

- **Active** – This status enables the application for the assignment in retiring and rolling back scenarios and other management functions.
- **Inactive** – This status disables the application for the assignment from any management functions. You must manually set this status using the **Deactivate** option in the actions menu. You can manually reverse this status using the **Activate** option from the actions menu so you can deploy multiple versions of an application.

The Delete Action Description and Its Alternatives

You might occasionally need to delete applications to free up space and to remove unused applications. However, the delete action removes applications and all their versions, permanently, from Workspace ONE UEM.

Alternatives for Delete Are Deactivate and Retire

As an alternative, Workspace ONE UEM offers the menu items to deactivate and retire applications. Review the differences between deactivating, retiring, and deleting before you perform any deleting actions to decide if the deactivation or retirement of applications can meet your needs.

When to Use Delete

You know that your organization has no future use for any version of the application. You want space in your Workspace ONE UEM environment so remove retired applications.

Active and Inactive Applications

When you use the **Delete** action, Workspace ONE UEM checks to see if the application is active or inactive.

- An **active** application, when deleted, behaves as a retired application. You also lose the ability to audit the application.

  If Workspace ONE UEM has a previous version of this application, depending on the **Push Mode**, the system pushes a previous version to devices.

- An **inactive** application is deleted completely from the Workspace ONE UEM application repository.

The Deactivate Option Description and the Relation to Other Active Versions

To remove all versions from devices, you can deactivate an application. An advantage of this option is that you can reverse an inactive status in the future.

Deactivate does not delete an application from your repository in the Workspace ONE UEM console. You can still view deactivated applications in the UEM console so that you can track devices that remove applications.

Numbered Active Versions

Active versions of an inactive app (deactivated) either push to devices or are still available to devices.

- Lower numbered version – If there is a lower numbered, active version of the application, then that lower version pushes to devices.
- Higher numbered version – If there is a higher numbered, active version in a higher organization group, that version is still available to devices.

When to Use Deactivate

Your organization is changing strategies and no longer needs applications and their versions that reflect the old focus. You can deactivate unnecessary applications so that they no longer clutter application repositories on devices. However, you can still access them in the UEM console.

The Retire Option Description and the Relation to Application Lifecycle Components

You can retire an application and this action has several outcomes depending on the push mode, application status, and the enabling of the **Retire Previous Version** option.

When to Use Retire

A new version of an application has several bugs and is costing end-users productivity. The previous version worked fine for your organization. You can retire the current version of the application and the Workspace ONE UEM console pushes the previous version to devices.

Push Mode and Retire

Configuring **Push Mode** as **Auto** or **On-Demand** impacts how the UEM console behaves when you use the **Retire** option.

- **Auto** – Set the application deployment option to **Auto** to push previous versions of an application to devices when you retire the current version.

  Note: In order for the **Auto** setting to work, the previous version must be active. If you deactivated the previous version, then Workspace ONE UEM does not automatically push it to devices.

- **On-Demand** – Set the application deployment to **On-Demand** to allow device users to install older versions to devices. End users must initiate a search and then install the application version.

Retire Previous Version

When you upload a new version of an application, using the actions menu and the **Add Version** option, Workspace ONE UEM displays the **Retire Previous Version** check box on the **Details** tab. Configure the check box depending on the desired outcome.

Setting	Description
Enable **Retire Previous Version**	Workspace ONE UEM unassigns the lower **Actual File Version** and assigns the higher **Actual File Version** to devices. However, the lower version is not available for the deployment in the UEM console. Apple iOS is the exception. These devices can receive lower **Actual File Versions** assigned through retiring previous versions in the UEM console.
Disable **Retire Previous Version**	Workspace ONE UEM unassigns the lower **Actual File Version** and assigns the higher **Actual File Version** to devices. If it is still **Active**, the lower version is available for the deployment in the UEM console. Workspace ONE UEM can assign multiple versions to Apple iOS devices irrespective of the versions increment.

Although this option removes updates, retiring a previous version also helps to manage security issues or bugs that might exist in the current version.

Disabling the **Retire Previous Version** check box upon upload pushes the working version of the application depending on the **Push Mode** (automatically or on-demand). It does not mark the alternate application version as retired.

To see the alternate versions of the application that are available in the Console, select **View Other Versions** from the actions menu

Retirement Scenarios

Retiring an application can have several results depending on the presence of other active versions and the Push Mode. The table covers the most common scenarios.

Retire Scenario	Retired App Version Action	Lower App Version Action
Two active versions and retire the higher version	Replaced on the device	If the push mode is **Auto**, the device user does nothing and the app pushes to devices, which results in having the lower, active version on the device. If the push mode is **On Demand**, the device user must initiate an installation from the AirWatch Catalog, which results in having the lower, active version on the device.

Retire Scenario	Retired App Version Action	Lower App Version Action
One active version and retire it	Removed from the device	No action results because Workspace ONE UEM has no other version to push to devices.
One active version and one inactive, lower version	Removed from the device	No action results because Workspace ONE UEM does not push inactive applications to devices.

Internal App Versions in Workspace ONE UEM

Use the Add Version feature to update versions of your internal applications to incorporate new features and fixes, test beta versions, and comply with organizational compliance standards.

Versioning has many benefits for testing and for compliance.

- Deploy multiple versions of the same application.
- Push beta versions for testing purposes.
- Allow Apple iOS devices to 'roll back' to a previous version.
- Push approved or compliant versions of applications to devices.

Note: The system can recognize a different version of an application without using the **Add Version** option. If you add the different version of the application as if it were new, the system still displays the **Retire Previous Versions** check box on the **Details** tab.

Supported Decimal Format

Workspace ONE UEM supports application version numbers with three numbers and two decimal places: **<MajorNumber>.<MinorNumber>.<Number>** or **9.1.1**.

Versioning Example – Beta Testing

Deploy multiple versions to test applications. Upload a beta version of an application and deploy it to beta users at the same time you have a non-beta version available to your regular users. After you test the beta version, you can replace the existing, non-beta, version with the tested version.

Version Values for Internal Apps

Workspace ONE UEM uses two different version values to manage version control of internal applications. The two version values are the **Actual File Version** and the **Version**, and Workspace ONE UEM displays them on the **Info** tab located in the Workspace ONE UEM console application record.

- **Actual File Version** – The coded version of the application set by the developer of the application.
- **Version** – The internal version of the application set by the UEMconsole.

Sourcing the Actual File Version Value

Workspace ONE UEM gets the application version that displays in the Actual File Version option from various places depending on the platform. These values must increment to allow the application version to override the current version in Workspace ONE UEM.

Platform	Parameter	Found In
Android	**versionName** displays in Actual File Version [but] **versionCode** controls the ability to version	.apk package
Apple iOS	**CFBundleVersion** [or] **CFBuildShortVersionString**	info.plist
Windows Desktop	**Version="X.X.X.X"** but Workspace ONE UEM only displays three decimal places	AppManifest.xml
Windows Phone	**Version="X.X.X.X"** but Workspace ONE UEM only displays three decimal places	WMAppManifest.xml

Versioning Identifiers and Incrementation

The Version option increments up for all platforms when you upload another version of an internal application.

The Actual File Version value, however, for some platforms, does not have to increment up. You can retire a previous version and replace it with a lower version value for certain platforms.

Platform	Actual File Version	Workspace ONE UEM Version
Android	**versionCode** must increment **up** because downgrading versions is not supported. Workspace ONE UEM cannot accept applications with lower **versionCode** values.	Workspace ONE UEM increments **up**.
Apple iOS	**BundleVersion** or the **BuildShortVersionString** can increment **up or down** because downgrading versions is supported. You can upload a lower version of the application and push it as the available version.	Workspace ONE UEM increments **up**.
Windows Desktop	**Version="X.X.X"**, the first three decimals, must increment **up** because downgrading versions is not supported. Workspace ONE UEM cannot accept applications with lower **Version="X.X.X"** values.	Workspace ONE UEM increments **up**.
Windows Phone	**Version="X.X.X"**, the first three decimals, must increment **up** because downgrading versions is not supported. Workspace ONE UEM cannot accept applications with lower **Version="X.X.X"** values.	Workspace ONE UEM increments **up**.

Multiple Versions of Internal Applications

Workspace ONE UEM can replace an internal application or it can deploy multiple versions of the same internal application. Replacing a retired version or having multiple versions depends on the **Actual File Version** value.

If you want multiple versions of an application, do not select the **Retire Previous Version** check box on the **Details** tab. This check displays when you add a version of an application. Workspace ONE UEM assigns the higher **Actual File Version** to devices and the lower **Actual File Version** remains assigned, too. If all versions are **Active**, then multiple versions work.

You can **Deactivate** application versions to remove them from the retiring process and from device assignments.

Note: Workspace ONE UEM can still assign multiple versions to iOS devices irrespective of the Apple iOS version increment.

Roll Back Results, Apple iOS Internal Apps

Workspace ONE UEM uses the **Retire Previous Version** option to roll Apple iOS applications back to a previous version that is marked active. Rolling back versions depends on the **Version** value. Workspace ONE UEM pushes the application version with the previous **Version** number, not the previous Actual File Version number.

You can roll back versions using Retire and Deactivate.

- When you **Retire** an application, the results might vary depending on the presence of other active versions and the Push Mode of the active versions.
- When you **Deactivate** an application, Workspace ONE UEM removes it from the devices it is assigned to at the specified organization group and all its child organization groups.

  If there is a lower, active version of the application, then that lower version pushes to devices. If there is a higher numbered version in a higher organization group, that version is still available to devices.

Add Versions for Internal Applications

Control versions of internal applications available to end users with the Add Version feature.

1. Navigate to **Apps & Books > Applications > Native** and select the **Internal** tab.
2. Select the application and then select **Add Version** from the actions menu.
3. Upload the updated file.

4. Configure the **Retire Previous Versions** check box on the **Details** tab:

Setting	Description
Enable **Retire Previous Version**	Workspace ONE UEM unassigns the lower **Actual File Version** and assigns the higher **Actual File Version** to devices. Apple iOS is the exception. These devices can receive lower **Actual File Versions** assigned through retiring previous versions in the Workspace ONE UEM console.
Disable **Retire Previous Version**	Workspace ONE UEM assigns the higher **Actual File Version** to devices and the lower **Actual File Version** remains assigned, too. Multiple versions work only if all versions are **Active**. Workspace ONE UEM can assign multiple versions to Apple iOS devices no matter if the versions increment up or down.

5. Select **Save & Assign** to use the flexible deployment feature.

The actions menu also offers an **Other Versions** option to view all the versions of an application in the Workspace ONE UEM console.

Configure View Logs for Internal Applications

Use the View Logs feature to access available log files pertaining to your internal SDK applications and wrapped applications, quickly. Log types include all logs, crash logs, and application logs. With this feature, you can download or delete logs.

Filter Logs

Filter options using the **Log Type** and **Log Level** menus so that you can find the type or amount of information to research and troubleshoot SDK and App Wrapping applications.

Download and Delete Logs

1. Navigate to **Apps & Books > Applications > Native** and select the **Internal** tab.
2. Select the application and then select **More > View > Logs** option from the actions menu.
3. Select desired options depending on if you want to act on specific devices (selected) or to act on all devices (listed).

Setting	Description
Download Selected	Download selected logs with information pertaining to applications created with the AirWatch SDK or using the AirWatch App Wrapping feature.
Download Listed	Download all logs in all pages with information pertaining to applications created with the AirWatch SDK or using the AirWatch App Wrapping feature.
Delete Selected	Delete selected logs with information about applications created with the AirWatch SDK or using the AirWatch App Wrapping feature.
Delete Listed	Delete all logs in all pages with information about applications created with the AirWatch SDK or using the AirWatch App Wrapping feature.

SDK Log Types

Workspace ONE UEM displays logs for applications that report application fails and that report application-specific data. These logs integrate with the AirWatch SDK so that you can manage applications built by it.

Find logs for applications in **Apps & Books > Analytics > App Logs**.

Setting	Description
Application Logs	This type of log captures information about an application. You set the log level in the default SDK profiles section, **Groups & Settings > All Settings > Apps > Settings and Policies > Settings > Logging**. You must add code into the application to upload these logs to the Workspace ONE UEM console.
Crash Logs	This type of log captures data from an application the next time the application runs after it crashes. These logs are automatically collected and uploaded to the UEM console without the need for extra code in the SDK application.

Use the View Logs feature to access available log files pertaining to your internal SDK applications and wrapped applications. See Configure View Logs for Internal Applications on page 172 for more information.

SDK Log Levels

Workspace ONE UEM groups logging messages into categories to distinguish critical issues from normal activities.

The Workspace ONE UEM console reports the messages that match the configured logging level plus any logs with a higher critical status. For example, if you set the logging level to Warning, messages with a Warning and Error level display in the UEM console.

Level	Logging Syntax	Description
Error	AWLogError("{log message}")	Records only errors. An error displays failures in processes such as a failure to look up UIDs or an unsupported URL.
Warning	AWLogWarning("{log message}")	Records errors and warnings. A warning displays a possible issue with processes such as bad response codes and invalid token authentications.
Information	AWLogInfo("{log message}")	Records a significant amount of data for informational purposes. An information logging level displays general processes, warning, and error messages.
Debug or Verbose	AWLogVerbose("{log message}")	Records all data to help with troubleshooting. This option is not available for all functions.

Use the View Logs feature to access available log files pertaining to your internal SDK applications and wrapped applications. See Configure View Logs for Internal Applications on page 172 for more information.

Access SDK Analytics Apps That Use SDK Functionality

Display events and data-use-information for applications that use SDK functionality. Workspace ONE UEM reports event analytics by the application ID and event name and data-use analytics by device.

Event Analytics

These events are custom created and developers can code any process or behavior they want to track.

1. Navigate to **Apps & Books > Applications > Logging > SDK Analytics**.
2. View events for SDK applications and retrieve data including application ID, the device on which it happened, and the event name.

Access SDK Event Analytics for a Specific Application

Export analytics data for your Apple iOS applications built using the SDK or using SDK functionality.

1. Navigate to **Apps & Books > Applications > List View > Internal**.
2. Select the SDK application and view the Details View.
3. Choose **View > Analytics** from the actions menu.

Data Usage Analytics

These events are embedded in the PLIST file for the Apple iOS application by the developer. They track telecom use for SDK developed applications.

1. Navigate to **Telecom > List View**.
2. Select devices that have the application installed and navigate to the **Details View**.
3. View data for the SDK application on the **Telecom** tab and use the **Export** option to retrieve a CSV version of the data.

Chapter 9:
Application Groups and Compliance

Use application groups (app groups) and compliance policies to protect mobile devices in your Workspace ONE UEMenvironment.

App Groups and Compliance Relationship

Application groups identify permitted and restricted applications so that compliance policies can act on devices that do not follow protective standards. To learn about the relationship between app groups and compliance policies, see Application Groups and Compliance Policies Work Together to Apply Standards Across Devices on page 176.

App Groups Features

Application groups identify permitted and restricted applications so that compliance policies can act on devices that do not follow protective standards.

For more information, see Configure an Application Group on page 176.

App Groups and the AirWatch Catalog

Use app groups to push notifications to app catalogs about applications you require devices to install. For instructions on how to configure this feature, see Create Required Lists for the AirWatch Catalog on page 178.

For more information on the AirWatch Catalog, see VMware AirWatch Catalog on page 183.

App Groups and Custom MDM Applications

Custom MDM applications are a type of app group and they are custom-made to track device information, such as location and jailbreak status. To gather information, troubleshoot, and track assets, enable Workspace ONE UEM to recognize custom MDM applications and assign them to special app groups. Enable the Use Custom MDM Applications so that you can select the option in the application group menu in Workspace ONE UEM. See Enable Custom MDM Applications for Application Groups on page 178 for details.

Compliance Features

Compliance policies enable you to act upon devices that do not comply with set standards.

For examples of compliance policy actions and for a list of the platforms the compliance engine supports for management, see Compliance for Mobile Application Management on page 180.

For information about adding compliance policies that work with app groups, see Build an Application Compliance Policy on page 180.

Application Groups and Compliance Policies Work Together to Apply Standards Across Devices

Application groups identify permitted and restricted applications so that compliance policies can act on devices that do not follow protective standards.

You can configure app groups for several platforms but you cannot combine all of them with compliance polices. For those platforms that you cannot combine with compliance policies, apply an application control profile.

App Group Platform	Works with Compliance Policies	Works with Application Control Profiles
Android	Yes	Yes
Apple iOS	Yes	No
Windows Phone	No	Yes

You are not required to configure application groups. However, application groups enhance the efficacy and reach of your compliance policies with minimal configurations.

Application Group	Description	Compliance Policy	Action
Whitelisted	Managed devices can install these applications from the AirWatch Catalog. If an application is not on the list, it is not permitted on managed devices.	**Contains Non-Whitelisted Apps**	The compliance engine identifies applications not in the whitelisted app group installed on the device and applies the actions that are configured in the compliance rule.
Blacklisted	Managed devices do not install these applications from the AirWatch Catalog. If an application is on this list, it is not allowed on managed devices.	**Contains Blacklisted Apps**	The compliance engine identifies applications from the blacklisted app group on the device and applies the actions that are configured in the compliance rule.
Required	Managed devices are required to install these applications from the AirWatch Catalog. If an application is on this list, it is required device users install it on managed devices.	**Does Not Contain Required Apps**	The compliance engine identifies applications from the required app group missing on the device and applies the actions that are configured in the compliance rule.

Configure an Application Group

Configure application groups, or app groups, so that you can use the groups in your compliance policies. Take set actions on devices that do not comply with the installing, updating, or removing applications.

Note: You assign application groups to organization groups. When you assign the application group to a parent organization group, the child organization groups inherit the application group configurations.

1. Navigate to **Apps & Books > Applications > Applications Settings > App Groups**.
2. Select **Add Group**.
3. Complete options on the **List** tab.

Setting	Description
Type	Select the type of application group you want to create depending on the desired outcome: allow applications, block applications, or require application installations. If your goal is to group custom MDM applications, select**MDM Application**. You must enable this option for it to display in the menu.
Platform	Select the platform for the application group.
Name	Enter a display name for the application group in the Workspace ONE UEM console.
Add Application	Display text boxes that enable you to search for applications to add to the application group.
Application Name	Enter the name of an application to search for it in the respective app store.
Application ID	Review the string that automatically completes when you use the search function to search for the application from an app store.
Add Publisher **Windows Phone**	Select for Windows Phone to add multiple publishers to application groups. Publishers are organizations that create applications. Combine this option with **Add Application** entries to create exceptions for the publisher entries for detailed whitelists and blacklists on Windows Phone.

4. Select **Next** to navigate to an application control profile. You must complete and apply an application control profile for Windows Phone. You can use an application control profile for Android devices.

   See the applicable platform guide for information on configuring application control profiles.

5. Complete settings on the **Assignment** tab:

Setting	Description
Description	Enter the purpose of the application group or any other pertinent information.
Device Ownership	Select the type of devices to which the application group applies.
Model	Select device models to which the application group applies.
Operating System	Select operating systems to which the application group applies.
Managed By	View or edit the organization group that manages the application group.
Organization Group	Add more organization groups to which the application group applies.
User Group	Add user groups to which the application group applies.

6. Select **Finish** to complete configurations.

Edit App Groups and the Application Control Profile

When you edit app groups for Android and Windows phone, follow these steps to reflect the update on devices.

1. Edit the app group first.
2. Edit the application profile to create a new version of it.
3. Save and publish the new version of the application profile to devices.

   The system does not reflect the changes to the app group unless the new version of the application control profile deploys to devices.

Create Required Lists for the AirWatch Catalog

Use app groups to push notifications to app catalogs about applications you require devices to install.

1. Navigate to **Apps & Books > Applications > Applications Settings > App Groups**.
2. Add or edit an app group.
3. On the **List** tab, select **Type** as **Required**.
4. On the **Assignment** tab, select the applicable organization groups and user groups that include the devices you want to push required applications to.

Enable Custom MDM Applications for Application Groups

Custom MDM applications are a type of app group and they are custom-made to track device information, such as location and jailbreak status. Enable Workspace ONE UEMto recognize custom MDM applications so you can assign them to special app groups to gather information, troubleshoot, and track assets.

Supported Application Types

Upload these custom-made applications to the internal applications section of the Workspace ONE UEM console.

Supported Platforms

Workspace ONE UEM supports custom MDM applications made for the Android and Apple iOS platforms.

Configure the Use Custom MDM Applications Feature

Enable the Use Custom MDM Applications so that you can select the option in the application group menu in Workspace ONE UEM. Workspace ONE UEM does not remove custom MDM applications after the compliance engine detects them on devices. These applications are for auditing, tracking, and troubleshooting.

1. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment**.
2. Select **Customization**.
3. Enable **Use Custom MDM Applications**.

Chapter 10: Compliance for Mobile Application Management

Compliance policies enable you to act upon devices that do not comply with set standards. For example, you can create compliance policies that detect when users install forbidden applications. Then configure the system to act automatically on devices with the non-compliance status.

You can create compliance policies for single applications using the Compliance List View, or for lists of applications using application groups. Although you are not required to use application groups, these groups enable you to take preventive actions on large numbers of non-compliant devices.

Example of Compliance Policy Actions

The compliance engine detects a user with a game-type application, which is one of the blacklisted applications in a blacklisted app group list. You can configure the compliance engine to take several actions.

- Send a push notification to the user prompting them to remove the application.
- Remove certain features such as Wi-Fi, VPN, or email profiles from the device.
- Remove specific managed applications and profiles.
- Send a final email notification to the user copying IT Security and HR.

Supported Platforms for Compliance Policies and Applications

You can configure an application list compliance policy for several platforms that acts on non-compliant devices.

- Android
- Apple iOS
- macOS

Build an Application Compliance Policy

Add compliance policies that work with app groups to add a layer of security to the mobile network. Policy configurations enable the Workspace ONE UEM compliance engine to take set actions on non-compliant devices.

1. Navigate to **Devices > Compliance Policies > List View**. Select **Add**.
2. Select the platform, **Android**, **Apple iOS**, or **Apple macOS**.
3. Select **Application List** on the **Rules** tab.

4. Select the options that reflect your desired compliance goals.

Setting	Description
Contains	Add the application identifier to configure the compliance engine to monitor for its presence on devices. If the engine detects the application is installed on devices assigned to the Compliance Rule, the engine performs the actions configured in the rule.
Does Not Contain	Add the application identifier to configure the compliance engine to monitor for its presence on devices. If the engine detects the application is not installed on devices assigned to the Compliance Rule, the engine performs the actions configured in the rule.
Contains Blacklisted Apps	If the engine detects applications listed in blacklisted app groups on devices assigned to the Compliance Rule, the engine performs the actions configured in the rule.
Contains Vendor Blacklisted Apps	Add applications from your application reputation scanning system to configure the compliance engine to monitor for their presence on devices. If the engine detects applications listed in these unique blacklisted app groups on devices assigned to the Compliance Rule, the engine performs the actions configured in the rule. Use this option if you integrate your App Scanning service with Workspace ONE UEM. You must enable this option to view it in the menu. It is an advanced application management feature that requires the correct SKU for use.
Contains Non-Whitelisted Apps	If the engine detects applications not listed in whitelisted app groups on devices assigned to the Compliance Rule, the engine performs the actions configured in the rule.
Does Not Contain Required Apps	If the engine detects that devices assigned to the Compliance Rule are missing applications in required app groups, the engine performs the actions configured in the rule.
Does Not Contain Version	Add the application identifier and the application version the compliance engine monitors device to ensure the correct version of the application is installed on devices. If the engine detects the wrong version of the application is installed on devices assigned to the Compliance Rule, the engine performs the actions configured in the rule.

You can get the **Application Identifier** from an app store or from its record in the Workspace ONE UEM console. Navigate to **Apps & Books > Applications > List View > Internal** or **Public**. Select **View** from the actions menu for the application and then look for the **Application ID** information.

5. Select the **Actions** tab to set escalating actions to perform if a user does not comply with an application-based rule.

   The first action is **immediate** but is not compulsory to configure. Use it or delete it. You can augment or replace the immediate action with further delayed actions with the **Add Escalations** feature.

Setting	Description
Mark as Not Compliant	Enable the check box to tag devices that violate this rule, but once the device is tagged non-compliant and depending on escalation actions, the system might block the device from accessing resources and might block admins from acting on the device. Disable this option when you do not want to quarantine the device immediately.
Application	Select to remove the managed application.
Command	Select to configure the system to command the device to check in to the console, to perform an enterprise wipe, or to change roaming settings.
Email	Select to block email on the non-compliant device.
Notify	Select to notify the non-compliant device with an email, SMS, or push notification using your default template. You can also send a note to the admin concerning the rule violation.
Profile	Select to use Workspace ONE UEM profiles to restrict functionality on the device.

6. Select the **Assignment** tab to assign the Compliance rule to smart groups.

Setting	Description
Managed By	View or edit the organization group that manages and enforces the rule.
Assigned Groups	Type to add smart groups to which the rule applies.
Exclusions	Select Yes to exclude groups from the rule.
View Device Assignment	Select to view the devices affected by the rule.

7. Select the **Summary** tab to name the rule and give it a brief description.
8. Select **Finish and Activate** to enforce the newly created rule.

Chapter 11:
VMware AirWatch Catalog

Deploy an app catalog so device users can access enterprise applications that you manage in the Workspace ONE UEM console. Your end users can find and access applications based on the app catalog settings you establish in the UEM console.

Basics of the AirWatch Catalog

For a description of the AirWatch Catalog features and a list of how to deploy the AirWatch Catalog, read AirWatch Catalog Features and Deployment Methods on page 186.

Workspace ONE UEMsupports a catalog for most platforms. For a list of the platforms that support the use of the AirWatch Catalog, see AirWatch Catalog Supported Platforms on page 187.

For an explanation of the options available for the AirWatch Catalog and for the Workspace ONE catalog, see Workspace ONE and AirWatch Catalog Settings on page 184.

Deployment Methods

Select from two ways to deploy the AirWatch Catalog; through the groups and settings area or with a device profile.

Groups & Settings Method

Push your AirWatch Catalog with catalog settings when you want devices to receive the catalog immediately upon enrollment. See Deploy the AirWatch Catalog With Groups & Settings Options on page 187 for more information.

Device Profile Method

Push your AirWatch Catalog with a profile when it does not matter that devices receive the catalog immediately upon enrollment with a web clip or bookmark. See Deploy the AirWatch Catalog with a Profile on page 188 for more information.

Configure the AirWatch Catalog

To highlight special applications in your AirWatch Catalog, you can use the featured application option. See Configure Featured Applications on page 189 for instructions on how to feature applications.

AirWatch Catalog Installation Behaviors and Messages

For a description of how the AirWatch Catalog and the Standalone Catalog install applications to devices and the messages installations present on devices, see Application Installation and AirWatch Catalogs on page 189.

Standalone Catalog

Workspace ONE UEM offers the flexibility of deploying the standalone catalog that works independently of the MDM feature. See Standalone Catalog for MAM Only Deployments on page 196 for more details.

Workspace ONE and AirWatch Catalog Settings

Workspace ONE UEM offers two app catalogs: Workspace ONE and the AirWatch Catalog. Both catalogs support the features in the Apps Settings of the Workspace ONE UEM console.

The Workspace ONE catalog integrates resources from environments that use VMware Identity Manager and Workspace ONE UEM. If your deployment does not use VMware Identity Manager, you still have access to the features previously released for the AirWatch Catalog.

Features Supported in Both Catalogs

The navigation in the UEM console, **Groups & Settings > All Settings > Apps > Workspace ONE**, highlights the Workspace ONE catalog. However, options under the Workspace ONE title are supported for the AirWatch Catalog. The options under the AirWatch Catalog apply specifically to it and are not necessary for the Workspace ONE catalog.

Option Descriptions

Review brief descriptions of the options available for both Workspace ONE and the AirWatch Catalog and those options that apply specifically to the AirWatch Catalog.

Setting	Description	More Information
Workspace ONE and AirWatch Catalog Settings		
Application Categories	Group applications and identify their uses with custom application categories.	Configure Application Categories on page 15
Paid Public Applications	Deploy paid public iOS applications in situations not feasible to use Apple's Volume Purchase Program (VPP).	Paid Public iOS Applications and Workspace ONE UEM on page 80
App Restrictions	Restrict iOS devices older than iOS 9 by restricting installations of only assigned applications approved by the organization.	Enable Restricted Mode for Free Public iOS Applications Older Than iOS 9 on page 83
External App Repository	Enable an external app repository if you want to host internal applications on your network with an external application repository and manage the applications with Workspace ONE UEM.	Supported Components for External App Repositories on page 29
Application Removal Protection	Configure threshold values to control the dispatch of application removal commands for critical internal applications.	Application Removal Protection on page 71
AirWatch Catalog Settings		
AirWatch Catalog > General	Configure general settings for the AirWatch Catalog.	Deploy the AirWatch Catalog With Groups & Settings Options on page 187

Setting	Description	More Information
AirWatch Catalog > Standalone Catalog	Configure a standalone catalog if your environment does not use MDM functionality. The standalone catalog has limited features.	Standalone Catalog for MAM Only Deployments on page 196
AirWatch Catalog > Feature Applications	Display featured applications in a prominent place in the AirWatch Catalog.	Configure Featured Applications on page 189

Transition Behavior from the AirWatch Catalog to Workspace ONE

As Workspace ONE UEM migrates to the Workspace ONE catalog, many AirWatch Catalog behaviors in previous releases change.

Web Clips and Show in App Catalog / Container

When you added a **Web Clips** profile, you can show it in the AirWatch Catalog. The option was editable.

In some Workspace ONE UEM versions, the **Show in App Catalog / Container** option is not editable. If you use the Workspace ONE catalog, that catalog displays all **Web Clips**, no matter what is configured for **Show in App Catalog / Container**. If you use the AirWatch Catalog, saving the **Web Clips** shows it in the AirWatch Catalog.

Migrating VMware AirWatch Catalog to Workspace ONE Catalog

When AirWatch and VMware Identity Manager are integrated, the Workspace ONE app catalog acts as the repository of all the resources that you can entitle to users. Users can access enterprise applications that you manage in the Workspace ONE catalog based on the settings you establish for the application. Administrators with the **AirWatch administrator** role can migrate customers from the legacy VMware AirWatch Catalog to Workspace ONE Catalog.

Before you begin:

1. Log into the **VMware Identity Manager** and configure the integration between **VMware Identity Manager** and AirWatch. For more information, see **Guide to Deploying VMware Workspace ONE** at https://docs.vmware.com/en/VMware-Identity-Manager/index.html.
2. For a better user experience, perform the following two steps:
   a. Configure the AirWatch Application for Enterprise Key Value Pairs. For more information, search for AirWatch Application Configuration for Enterprise Key Value Pairs at https://docs.vmware.com/en/VMware-Identity-Manager/index.html.
   b. Configure the Mobile Single Sign-in Authentication for AirWatch-Managed iOS and Android devices. For more information, search for Implementing Mobile single sign-on Authentication for AirWatch-Managed iOS Devices and Implementing Mobile Single Sign-On Authentication for AirWatch-Managed Android Devices at https://docs.vmware.com/en/VMware-Identity-Manager/index.html.

Migrate VMware AirWatch Catalog to Workspace ONE Catalog:

1. Manually push Workspace ONE as a managed application. That is, add Workspace ONE as a public application from an App store. For more information on deploying public applications, see Add Public Applications from an App Store

on page 77.

2. Disable the AirWatch Catalog in the **Groups & Settings** menu. For more information on how to disable the authentication of the AirWatch Catalog in the **Groups & Settings** menu. For more information, see Deploy the AirWatch Catalog With Groups & Settings Options on page 187.

AirWatch Catalog Features and Deployment Methods

Deploy an AirWatch Catalog so device users can access enterprise applications that you manage in the Workspace ONE UEM console. Your end users can find and access applications based on the AirWatch Catalog settings you establish in the Workspace ONE UEM console.

Note: Download URLs for applications expire in 60 minutes. To install applications within this time frame, notify the devices

View

- See overall ratings and comments for the applications based on submissions provided by other users.
- View application installation statuses.
- View application descriptions, file sizes, versions, and icons.
- View granular messaging to help with installing applications and to help with network connections.

Install

- Install required applications to devices.
- Install application updates for managed applications.

Filter, Search, and Sort

- Filter applications by categories.
- Search for applications by name or category.
- Sort applications in various orders including alphabetical, date added, and installation status.

Customize

- Define the sorting order.
- Add a unique branding logo.
- Define default categories and filters.

AirWatch Catalog Deployment Methods

Deploy your AirWatch Catalog automatically to devices upon enrollment or with a device profile. Select a method according to the range of device platforms in your mobile deployment.

- Automatically – Configure AirWatch Catalog deployment options in a central location in Workspace ONE UEM. Your configurations apply to all supported platforms.

- Profile – Configure AirWatch Catalog deployment options for individual platforms with a separate profile (Web clip or bookmark) for each platform.

AirWatch Catalog Supported Platforms

The AirWatch Catalog integrates the platforms listed on the **Groups & Settings > All Settings > Apps > Catalog > General** page in the Workspace ONE UEM console.

- Android
- Apple iOS
  - The system directs iOS 6+ devices to the current AirWatch Catalog. This AirWatch Catalog works in full-screen mode or non-full-screen mode.
  - The system automatically directs iOS devices to the previous AirWatch Catalog. This AirWatch Catalog does not support the full screen mode. If you are currently using the full screen mode, you do not need to change the URL but you must disable the mode.
- macOS
- Windows Desktop

Deploy the AirWatch Catalog With Groups & Settings Options

Push your AirWatch Catalog with catalog settings when you want devices to receive the catalog immediately upon enrollment with Workspace ONE UEM.

1. To set the active organization group to receive the AirWatch Catalog, navigate to**Groups & Settings > All Settings > Apps > Workspace ONE > AirWatch Catalog > General**.
2. Configure the following settings on the **Authentication** tab.

Setting	Description
Require Authentication	Require users to log in with their username and password before they can access the app catalog. This option is disabled by default which sets Workspace ONE UEM to require no authentication to access the app catalog.
Reauthenticate	Select a reauthentication option. • **Never - Keep User Signed In** – Keeps users signed in and does not require them to log in each time. • **After XX day(s)** – Require users to authenticate (log in) after a set number of days. Users still have to reauthenticate if they clear cookies on their devices, even with this option enabled.

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

Setting	Description
Catalog Title	Enter a name for your app catalog. This title appears on the home screen of the device.
Platforms	Select the supported platforms for your app catalog. If this is enabled for the platform, the profile gets pushed to the device. Apple iOS offers the option to open the app catalog web clip in full screen mode, if desired. Set this using the **Full Screen** option for iOS 6+ devices.
Icon	Upload an icon for your app catalog. This icon appears on the home screen of the device. If you do not upload an icon, Workspace ONE UEM pushes a default icon to devices.

4. Configure the following settings on the **Customization** tab.

Setting	Description
Branding Logo	Upload a logo to brand the app catalog for your organization. • This logo overrides any logo you set in **Groups & Settings > All Settings > System > Branding**. • If you do not upload a logo for the app catalog, Workspace ONE UEM uses the logo from your **System > Branding** settings. • If you do not configure any branding scheme or logo the **System > Branding** settings, Workspace ONE UEM uses a default scheme.
Default Filter	Sets the app catalog to open with this filter enabled on the catalog's main page. However, if users need to install featured applications, the app catalog defaults to open with the **Featured** filter. Users can change the default filter at any time and their selection stays active if they use the app catalog within a 24 hour period. After more than 24 hours of inactivity, the app catalog returns to the set default filter.
Default Sort	Sets the app catalog to open with a configured sorting option enabled. Users can change the default sort at any time and their selection stays active and does not depend on activity.
Pinned Categories	Pins specific categories to the default menu. Users can elect to see more categories.

Deploy the AirWatch Catalog with a Profile

Push your AirWatch Catalog with a profile when it does not matter that devices receive the catalog immediately upon enrollment. Configure a Web clip or bookmark payload depending on the platform.

1. Navigate to **Devices > Profiles > List View** and select **Add**.

   Apple macOS only – Select **User Profile**.

2. Enter **General**information for the profile to assign the AirWatch Catalog to devices using smart groups. Also use this section to define the push mode as auto so that the AirWatch Catalog pushes to the device.

3. Select one of the following payloads:
   - **Web Clips** for Apple iOS, macOS, and Windows Desktop
   - **Bookmarks** for Android
4. Enter a title for the web application in the **Label**text box.
5. Enter the location for the AirWatch Catalog in the**URL**text box.
   https://{Environment}/Catalog/ViewCatalog/{SecureDeviceUdid}/{DevicePlatform}.
6. Set the **Full Screen**option for the AirWatch Catalog to open in full screen mode on Apple iOS 6+ devices.
   You do not need to configure the option **Show in App Catalog/Container**. Leave this option disabled.
7. Select **Save & Publish**to push the AirWatch Catalog to the devices in the smart groups you assigned in the general section.

Configure Featured Applications

Use the featured application option to set a few select applications apart from other applications. The option highlights specific applications within the AirWatch Catalog for your end users.

You can configure Featured Applications for Android and iOS platforms. The Workspace ONE UEM system displays featured applications in a prominent place in the AirWatch Catalog.

- Android
  - Internal applications
  - Public applications
- Apple iOS
  - Internal applications
  - Public applications

The AirWatch Catalog lists featured applications in the main list of applications. You can feature public and internal applications.

1. Navigate to **Apps & Books > Applications > Applications Settings > Featured Apps**.
2. Select **Add Application** by platform type, either Apple or Android.
3. Select **Public** or **Internal** for the **Application Type**.
4. Select the application you want to feature in the **Application** drop-down menu.
5. Select to use the default icon for the application or to upload a different one in the **Banner** option.

Application Installation and AirWatch Catalogs

Applications from the AirWatch Catalog install on devices in specific ways. For example, some applications install from a push notification on the device while other applications install silently. Installation depends on the platform of the device, the type of application and whether the device uses a standard AirWatch Catalog or the Standalone Catalog.

Review the device behaviors and the application prompts and messages devices display when users install applications.

Important: This information is not comprehensive. It shows general trends in installation processes and messaging. The information was current at the time of writing. However, the behaviors and messages might change between Workspace ONE UEM releases.

Platform Specific Device Modes

Review brief explanations for Apple iOS and Android device modes.

- **Apple iOS**
  - **Supervised** – These devices benefit from extra management features created by Apple iOS specifically for devices in supervised mode. You can use these iOS management features to enhance Workspace ONE UEM management capabilities.
  - **Non-Supervised** – These devices do not support the specific Apple iOS management features offered by supervised mode; however, Workspace ONE UEM can manage these devices and secure these devices.
- **Android**
  - **Enterprise** – If the device manufacturer supplies a compatible API to support the silent installation and uninstallation, these devices support silent activity. Workspace ONE UEM supports enterprise Android devices when Workspace ONE UEM is supplied with the necessary APIs to perform silent processes.

    You can now silently install and uninstall only internal applications.
  - **Standard** – These devices do not support silent activity; however, Workspace ONE UEM can manage these devices and can secure these devices.
  - **Android For Work** – These devices support silent activity and are part of the integration of Workspace ONE UEM and Android For Work system. The system provides data separation and security.

    See the **Workspace ONE UEM Integration with Android for Work Guide** for information on this system on the Workspace ONE UEM Resources Portal at https://resources.air-watch.com.

Device Behavior of Installed Applications from the AirWatch Catalog

The following table displays the general device and application behavior end users see when you push an application from the Workspace ONE UEM console to a device that has an AirWatch Catalog.

Application Type	Apple iOS Supervised Device	Apple iOS Unsupervised Device	Android Enterprise Device	Android Standard Device	Android for Work	Windows Desktop Device	macOS
Internal	App silently installs. The device takes the user from the App Catalog to the app home screen.	The device receives a notification about the app.	App silently installs. The device does not leave the App Catalog while the app installs in the background.	App attempts to install. The device takes the user to the Managed Apps section of the Airwatch Agent.	Not applicable because Workspace ONE UEM treats internal apps as public apps.	App silently installs. The device does not leave the App Catalog while the app installs in the background.	App silently installs. The device does not leave the App Catalog while the app installs in the background.
Public, Free	The App Catalog stays open while the app installs silently in the background.	The device receives a notification about the app.	The App Catalog directs the user to the app store to get the app.	The App Catalog directs the user to the app store to get the app.	App silently installs. The device does not leave the App Catalog while the app installs in the background.	The App Catalog directs the user to the app store to get the app.	Not applicable.
Public, Paid	The App Catalog directs the user to the app store to get the app.	The App Catalog directs the user to the app store to get the app.	The App Catalog directs the user to the store to get the app.	The App Catalog directs the user to the store to get the app.	Not applicable.	The App Catalog directs the user to the app store to get the app.	Not applicable.
Purchased, VPP	The App Catalog stays open while the app installs silently in the background.	The device receives a notification about the app.	Not applicable.	Not applicable.	Not applicable.	Not applicable.	The App Catalog stays open while the app installs silently in the background.

Application Type	Apple iOS Supervised Device	Apple iOS Unsupervised Device	Android Enterprise Device	Android Standard Device	Android for Work	Windows Desktop Device	macOS
Web	The App Catalog stays open while the app installs silently in the background.	The App Catalog stays open while the app installs silently in the background.	Enable **Add to Homescreen** option in the bookmark profile in the Console. The device does not leave the App Catalog and the device displays message that **Shortcut Web Clips created** when the user installs the app. Disable **Add to Homescreen** option in the bookmark profile in the Console. The Console silently adds the bookmark to the native browser.	Enable **Add to Homescreen** option in the bookmark profile in the Console. The App Catalog stays open and the device displays the message that **Shortcut Web Clips created** when the user installs the app. Disable **Add to Homescreen** option in the bookmark profile in the Console. The Console silently adds the bookmark to the native browser.	Not applicable.	App silently installs. The device does not leave the App Catalog while the app installs in the background.	App silently installs. The App Catalog stays open while the app installs in the background.

Device Behavior of Installed Applications from the Standalone Catalog

The following table displays the general device and application behavior end users see when you push an application from the UEM console to a device that has a Standalone Catalog.

Workspace ONE UEM does not offer a Standalone Catalog for Windows Desktop and macOS devices. Also, applications in a Standalone Catalog are unmanaged so the platform-specific device mode does not apply.

Application Type	Apple iOS Device	Android Device
Internal	The device receives a notification about the app.	App installs in the Download folder on the device. User must go to the Download folder to install the app.
Public, Free	The App Catalog directs the user to the app store to get the app.	The App Catalog directs the user to the store to get the app.
Public, Paid	The App Catalog directs the user to the app store to get the app.	The App Catalog directs the user to the store to get the app.
Purchased, VPP – Redemption Codes	The App Catalog directs the user to the app store to get the app.	Not applicable.
Web	Device prompt directs users to install the web clip profile for the app.	App opens in the native browser and the Console does not add the bookmark to the native browser.

Application Messages in the App Catalog

The following table displays the general messages the end user sees when you push applications from the UEM console to a device that has the App Catalog.

If the price and size of the application are available from the app store, Workspace ONE UEM displays these values in the message.

Application Type	Apple iOS Supervised Device	Apple iOS Unsupervised Device	Android Enterprise Device	Android Standard Device	Android For Work	Windows Desktop Device	macOS Device
Internal	Install {appname}? You are taken out of this catalog to the home screen on your device, and the download begins automatically.	Install {appname}? You receive a push notification to continue with installation.	Install {appname}? The app downloads automatically and appears on your device.	Install {appname}? Tap the notification that appears in the Managed Apps section of the Airwatch Agent to continue with the installation.	Not applicable because Workspace ONE UEM treats internal apps as public apps	Install {appname}? The app downloads automatically and appears on your device.	Install {appname}? The app downloads automatically and appears on your device.

Application Type	Apple iOS Supervised Device	Apple iOS Unsupervised Device	Android Enterprise Device	Android Standard Device	Android For Work	Windows Desktop Device	macOS Device
Public, Free	Install {appname}? The app downloads automatically and appears on your device.	Install {appname}? You receive a push notification to continue with installation.	Install {appname}? You are redirected to the app store to download this app.	Install {appname}? You are redirected to the app store to download this app.	Install {appname}? The app downloads automatically and appears on your device.	Install {appname}? You are redirected to the app store to download this app.	Not applicable.
Public, Paid	Install {appname}? You are redirected to the app store to download this app.	Install {appname}? You are redirected to the app store to download this app.	Install {appname}? You are redirected to the app store to download this app.	Install {appname}? You are redirected to the app store to download this app.	Note applicable.	Install {appname}? You are redirected to the app store to download this app.	Not applicable.
Purchased, Custom B2B	Install {appname}? You are redirected to the app store to download this app.	Install {appname}? You are redirected to the app store to download this app.	Not applicable.	Not applicable.	Not applicable.	Not applicable.	Not applicable.
Purchased, VPP	Install {appname}? The app downloads automatically and appears on your device.	Install {appname}? You receive a push notification to continue with installation.	Not applicable.	Not applicable.	Not applicable.	Not applicable.	Install {appname}? The app downloads automatically and appears on your device.

Application Type	Apple iOS Supervised Device	Apple iOS Unsupervised Device	Android Enterprise Device	Android Standard Device	Android For Work	Windows Desktop Device	macOS Device
Web	Install {appname}? The app downloads automatically and appears on your device.	Install {appname}? The app downloads automatically and appears on your device.	Enable **Add to Homescreen** option in the bookmark profile in the Console. Install {appname}? The app downloads automatically and appears on your device. **Bookmark the download** Install {appname}? Web app that appears as a bookmark in your native browser.	Enable **Add to Homescreen** option in the bookmark profile in the Console. Install {appname}? The app downloads on your device. **Bookmark the download** Install {appname}? Web app appears as a bookmark in your native browser.	Not applicable.	Install {appname}? The app downloads automatically and appears on your device.	Install {appname}? The app downloads automatically and appears on your device.

Application Messages in the Standalone Catalog

The following table displays the general messages end users see when you push applications from the UEM console to an unmanaged device that has the Standalone Catalog.

If the price and size of the application are available from the app store, Workspace ONE UEM displays these values in the message.

Workspace ONE UEM does not offer a Standalone Catalog for Windows Desktop and macOS devices.

Application Type	Apple iOS Supervised Device	Apple iOS Unsupervised Device	Android Enterprise Device	Android Standard Device
Internal	Install {appname}? You receive a push notification with installation.	Install {appname}? You receive a push notification to continue with installation.	Install {appname}? This file is downloaded and available to install from the downloads folder on your device.	Install {appname}? This file is downloaded and available to install from the downloads folder on your device.
Public, Free	Install {appname}? You are redirected to the app store	You are redirected to the app before to download this app.	Install {appname}? You are redirected to the app store to download this app.	Install {appname}? You are redirected to the app store to download this app.
Public, Paid	Install {appname}? You are redirected to the app store to download this app.	Install {appname}? You are redirected to the app store to download this app.	Install {appname}? You are redirected to the app store to download this app.	Install {appname}? You are redirected to the app store to download this app.
Purchased, Custom B2B	Install {appname}? You are redirected to the app store to download this app.	Install {appname}? You are redirected to the app store to download this app.	Not applicable.	Not applicable.
Purchased, VPP	Install {appname}? You are redirected to the app store to download this app.	Install {appname}? You are redirected to the app store to download this app.	Not applicable.	Not applicable.
Web	Install {appname}? To install, tap on the profile installation prompt that appears when you continue.	Install {appname}? To install, tap on the profile installation prompt that appears when you continue.	Continue to {appname}? You are taken to this web app in your browser	Continue to {appname}? You are taken to this web app in your browser

Standalone Catalog for MAM Only Deployments

Many organizations do not need to manage devices for their mobile fleets for various reasons, including possible privacy or legal issues. However, they might need to distribute mobile applications, so Workspace ONE UEM offers the flexibility of deploying the standalone catalog that works independently of the MDM feature.

Users do not have to enroll with Workspace ONE UEM using a Hub, but rather enroll with the Workspace ONE UEM standalone catalog. This catalog distributes all application types, public, purchased, internal, and Web.

Although end-user devices are not enrolled in MDM, you can access a device record in the Workspace ONE UEM console. The device record is for auditing purposes and the status of these devices in the UEM console displays as **App Catalog Only**.

Supported Platforms

You can configure a standalone catalog for Android and Apple iOS platforms, but it can only distribute applications with the on-demand push mode.

Standalone Catalogs and Organization Groups

Set configurations for the standalone catalog in an organization group level depending on the type of deployment you have.

- On-premise deployments – Configure the catalog at the first level after the **Global** organization group.
- SaaS and Shared SaaS deployments – Configure the catalog at the first level after the **Customer** organization group.

Standalone Catalog Functionality

The standalone catalog has limited functionality compared to other catalogs. To decide if it can benefit your deployment, determine how end users interact with it and if the unmanaged deployment of applications is sufficient. Also, consider what SDK functions your deployment needs.

End-User

- End users enroll with Workspace ONE UEM using the Internet and not with the AirWatch Agent.
- End users must re-enroll with the standalone catalog when you change versions. Even if they do not re-enroll, they still have access to applications. However, they cannot receive an updated version for the catalog unless they re-enroll.

Deployment

- Devices in your standalone catalog deployment are unmanaged. An unmanaged device does not have the security controls offered by the Workspace ONE UEM MDM feature.
- Applications distributed with the standalone catalog remain on devices after an end user unenrolls with the standalone catalog.
- You cannot track application downloads but you can see a list of assigned applications for the device in the device record in the Workspace ONE UEM console.

Available SDK Functions

Supported applications can use limited AirWatch SDK functions when accessed through the Standalone Catalog.

- SDK profile retrieval
- user name and password authentication
- Jailbreak detection
- Beacon technology support

Steps to Deploy a Standalone Catalog

To configure a Workspace ONE UEM standalone MAM deployment with the standalone catalog, configure a special organization group. Then, add the standalone catalog to that organization group and instruct end users to enroll with

the standalone MAM deployment.

1. Configure an organization group for the standalone MAM deployment. Name the group with a title such as App-Catalog-Only-Organization-Group so you easily recognize the function of the special group. For information on configuring organization groups, see Create Organization Groups in the MDM Guide.
2. Configure a standalone catalog at the same organization group of the standalone MAM deployment or in a parent group above it.
3. Send end users their enrollment credentials and the Workspace ONE UEM environment URL so that they can enroll with Workspace ONE UEM. Enrolling pushes the standalone catalog profile to their devices.

Enable the Standalone Catalog

Workspace ONE UEM provides a solution for deploying the standalone catalog without requiring users to enroll in full MDM, and no AirWatch Agent is required. Instead, end users can access just MAM applications assigned to an App-Catalog-Only-Organization-Group through the standalone catalog.

1. Navigate to **Groups & Settings > All Settings > Apps > Workspace ONE > AirWatch Catalog > Standalone Catalog**.
2. Configure the following settings.

Setting	Description
Standalone Catalog	Enable the **Standalone Catalog** to prevent users that enroll into the selected App-Catalog-Only-Organization-Group from enrolling into MDM. Configure this setting in the App-Catalog-Only-Organization-Group or in a parent above it.
Allow New User Registration	Enable the **Allow New User Registration** check box to allow new users to register for access to the Standalone Catalog.
Enable Email Domain Validation	Select the **Enable Email Domain Validation** option to use specified email domains to validate users when they register to access to the Standalone Catalog. Enter email domains in the **Allowed Email Domains** field for the standalone MAM users. End users enter their email addresses and a Group ID to enroll with this Standalone Catalog. Workspace ONE UEM matches the domains entered in this field to the domains of MAM-only users.
Catalog Title	Enter a title in the **Catalog Title** field.
Icon	Upload an image in the **Icon** field for the Standalone Catalog.

3. Select **Save**.

End users can enroll and select or enter the Group ID of the Catalog-Only-Organization-Group you set up. After finishing enrollment, the standalone catalog profile prompts for install. When finished, it displays on the device.

Unmanaged Devices and the Standalone Catalog

The system creates device records for unmanaged devices enrolled with the standalone catalog in the Workspace ONE UEM console for audit purposes. The status of these devices is **App Catalog Only**. You cannot track the download status of applications on this device, but you can see a list of all assigned applications. If a user removes the unmanaged profile, Workspace ONE UEM does not remove the application but it does remove the Web clip.

Set SDK Communication With the Standalone Catalog

For applications created using the AirWatch SDK to communicate and work with the standalone catalog, the device user must activate the application within the catalog.

1. Access the SDK-created application in the standalone catalog and install it.
2. Open the application and select to **Activate** the application.

   This action begins the communication between Workspace ONE UEM and the application.

Chapter 12: Workspace ONE UEM Applications and Workspace ONE

To take the advantage of the Workspace ONE experience, integrate Workspace ONE UEM and VMware Identity Manager. You can use it as a unified app catalog to distribute numerous types of applications.

Basics of Workspace ONE

Control access to applications with managed access and open access. For an explanation of these access types, see Workspace ONE UEM Applications and the Workspace ONE Managed Access Feature on page 200.

View a matrix that outlines what applications and platforms support open and managed access in Supported Platforms for Open and Managed Access on page 201.

For instructions on how to add public applications for the deployment through Workspace ONE, see Add Public Applications from an App Store on page 77.

For more information about configuring managed access options for internal applications, see Add Assignments and Exclusions to Applications on page 30.

Workspace ONE Catalog and Workspace ONE UEM-Only Mode

You can configure the Workspace ONE catalog to fetch resources to Workspace ONE UEM from VMware Identity Manager. Integrate VMware Identity Manager and Workspace ONE UEM and then set the **Fetch** option. You do not have to set up other features in VMware Identity Manager such as activating a directory, setting up authentication, or setting up access policies.

For information about this feature, see the topic **Using Workspace ONE UEM-Only Mode for Access to Workspace ONE Catalog** on https://docs.vmware.com/en/VMware-Workspace-ONE/index.html.

Workspace ONE UEM Applications and the Workspace ONE Managed Access Feature

To take the advantage of the Workspace ONE experience, integrate Workspace ONE UEM and VMware Identity Manager . You can use it as a unified app catalog to distribute numerous types of applications.

Workspace ONE UEM Public and Internal Apps and Workspace ONE

For public and internal, you can configure to deploy the application depending on the device management status. Set an application for open access and any device can access the application. Set an application for managed access and a device must grant admins permissions to their device to access the application.

Access Type	Suggested Uses
Managed Access Device users access resources by granting admins permissions on their devices (installs a management profile on the device). The application is available to devices already managed by Workspace ONE UEM. If Workspace ONE UEM does not manage the device, Workspace ONE prompts the device to enroll with Workspace ONE UEM. If it enrolls, it can access the application. If it does not enroll, it cannot access the application through Workspace ONE.	• Remove sensitive corporate data from applications when device users leave the organization or lose their devices. • Require app tunneling when applications access the intranet. • Enable single sign-on for applications. • Track user adoption and installation statuses for applications. • Deploy the application automatically upon enrollment.
Open Access Device users access resources without granting admins permissions on their devices. The application is available to devices no matter their managed status.	• Provide application access to end-users immediately upon login, without elevated security permissions. • Suggest the use of the application without requiring its installation, and let device users install it when they want. These applications do not contain sensitive corporate data and they do not access protected corporate resources. • Distribute applications without the Workspace ONE UEM MDM profile to auxiliary personnel like contractors and consultants.

Workspace ONE UEM Web Apps and Workspace ONE

Workspace ONE enables access to applications located in the **Web** tab of the Workspace ONE UEM console. It pulls the URL, the application description, and the icon.

Supported Platforms for Open and Managed Access

Configure the access type for internal and public applications based on the platform.

	Managed Access	Open Access
Internal Applications		
Android	✓	✓
iOS	✓	✓
Windows Desktop	✓	X
Windows Phone	✓	X
MacOS	✓	X

	Managed Access	Open Access
Public Applications		
Android	✓	✓
iOS	✓	✓
Windows Desktop	X	✓
Windows Phone	X	✓

View the Installation Status of Windows 10 Applications in the Workspace ONE Catalog

Windows 10 device users can view the installation status of applications in their Workspace ONE catalog.

Reason

Applications for Windows 10 devices are often large and take several minuets to download. In the past, users did not have a visual representation of the application installation. If an installation took 10 minutes, a user might decide the installation had failed after five minutes and prematurely cancel the installation.

Workspace ONE now displays the installation status of applications so users can estimate when downloads complete and when applications are available for use.

Supported Application Types

Workspace ONE supports this feature for these file formats and application types.

Platform	Application Type	File Formats
Windows Desktop Windows Phone	Internal	XAP APPX Win32 (EXE, MSI, ZIP)
Windows Desktop Windows Phone	Public	XAP APPX

Required Components

Ensure that you configure the required components for the software distribution system. This system, also called software package deployment, is required because it communicates the installation status to Workspace ONE on devices. For software distribution requirements, see Requirements to Deploy Win32 Applications for Software Distribution on page 41.

Other Components on Devices

- Workspace ONE v3.0
- Workspace ONE UEM App Deployment Agent v2.1 (available in the Workspace ONE UEM console v9.1.2+)

  The system deploys this agent when you enable the software package deployment.

Chapter 13:
MAM Features with SDK Functions

The Settings and Policies section of the Workspace ONE UEM console contains settings that can control security, behaviors, and the data retrieval of specific applications. The settings are sometimes called SDK settings because they run on the AirWatch SDK framework.

You can apply these SDK features to applications built with the AirWatch SDK, to supported Workspace ONE UEM applications, and to applications wrapped by the AirWatch App Wrapping engine. You can apply the SDK features because the AirWatch SDK framework processes the functionality.

Default and Custom Options

There are two types of SDK options that you can apply to internal applications, Workspace ONE UEM applications, and wrapped applications. Workspace ONE UEM identifies them as default and custom. For more information, see MAM Functionality with Settings and Policies and the AirWatch SDK on page 204.

Apply Options to Applications with Profiles

Whether you use default settings to create the SDK profile or use custom device profiles, you must apply this default or the custom profiles to the application.

For more information, refer Assign the Default or Custom Profile on page 215.

Available SDK Functions

There are many SDK functions available to apply to applications. See Supported Settings and Policies Options for the SDK on page 216 for a matrix of all supported default functions.

Some Available Functions

Many functions control access to applications that use SDK capabilities.

Use the authentication function to set a passcode or a user name and password challenge to restrict access. See Configure Authentication Type for the Default SDK Profile on page 219 for more instruction.

The integrated authentication function allows you to direct traffic through configured tunnels when you enter sites and corporate resources users can visit. This function works with systems to protect access like certificates. See Configure Integrated Authentication for the Default SDK Profile on page 226 for information about configure the feature.

The data loss prevention (DLP) function lists components and actions to prevent or allow in applications that use SDK capabilities. See Configure Data Loss Prevention for the Default SDK Profile on page 230 for available settings.

MAM Functionality with Settings and Policies and the AirWatch SDK

The Settings and Policies section of the Workspace ONE UEM console contains settings that can control security, behaviors, and the data retrieval of specific applications. The settings are sometimes called SDK settings because they run on the AirWatch SDK framework.

You can apply these SDK features to applications built with the AirWatch SDK, to supported Workspace ONE UEM applications, and to applications wrapped by the AirWatch App Wrapping engine. Same features can be applied in both the places as the AirWatch SDK framework processes the functionality.

Types of Options for SDK Settings

Workspace ONE UEM has two types of the SDK settings, default and custom. To choose the type of SDK setting, determine the scope of deployment.

- Default settings work well across organization groups, applying to large numbers of devices.
- Custom settings work with individual devices or for small numbers of devices with applications that require special mobile application management (MAM) features.

Default Settings

Find the default settings in **Groups & Settings > All Settings > Apps > Settings and Policies** and then select **Security Policies**, **Settings**, or **SDK App Compliance**. You can apply these options across all the Workspace ONE UEM applications in an organization group. Shared options are easier to manage and configure because they are in a single location.

View the matrices for information on which default settings apply to specific Workspace ONE UEM applications or the AirWatch SDK and app wrapping.

Custom Settings

Find the custom settings in **Groups & Settings > All Settings > Apps > Settings and Policies > Profiles**. Custom settings for profiles offer granular control for specific applications and the ability to override default settings. However, they also require separate input and maintenance.

Configure Default SDK Security Settings

Default SDK settings apply across AirWatch and wrapped applications, providing a unified user experience on devices. Because the configured SDK settings apply to all AirWatch and wrapped applications by default, you can configure the default SDK profile with the entire AirWatch and wrapped application suite in mind.

Before You Begin

Not all platforms or AirWatch applications support all available default SDK profile settings. A configured setting only works on the device when it is supported by the platform and app. This also means that an enabled setting might not work uniformly across a multi-platform deployment, or between applications. The SDK Settings matrix covers the available SDK profile settings and the apps and platforms they apply to.

Key Assumptions

The recommendations provided apply to an app suite that includes:

- VMware Browser
- AirWatch Inbox
- VMware Content Locker

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.
2. Configure **Security Policies**.

Action	Description	Rec
Authentication Type		
Passcode	Prompt end users to authenticate with a user-generate passcode when the app first launches, and after an app session timeout. Enabling or disabling SSO determines the number of app sessions that get established.	–
Username and Password	Prompt end user to authenticate by re-entering their enrollment credentials when the app first launches, and after an app session timeout. Enabling or disabling SSO determines the number of app sessions that get established.	–
Disabled	Allow end user to open apps without entering credentials.	√
SSO		
Enabled	Establish a single app session across all AirWatch and AirWatch wrapped apps.	√
Disabled	Establish app sessions on a per app basis.	–
Offline Access		
Enabled	Allow end users to open and use AirWatch and wrapped apps when disconnected from Wi-Fi. Offline AirWatch apps cannot perform downloads, and end users must return online for a successful download. Configure the Maximum Period Allowed Offline to set limits on offline access.	√
Disabled	Remove access to AirWatch and wrapped apps on offline devices.	–
Compromised Protection		
Enabled	Override MDM protection. App level Compromised Protection blocks compromised devices from enrolling, and enterprise wipes enrolled devices that report a compromised status.	√
Disabled	Rely solely on the MDM compliance engine for compromised device protection.	–
Data Loss Prevention		
Enabled	Access and configure settings intended to reduce data leaks.	**√**

Enable Copy And Paste	
Allows an application to copy and paste on devices when set to **Yes**.	
Enable Printing	
Allows an application to print from devices when set to **Yes**.	
Enable Camera	
Allows applications to access the device camera when set to **Yes**.	
Enable Composing Email	
Allows an application to use the native email client to send emails when set to **Yes**.	

Enable Data Backup	
Allows wrapped applications to sync data with a storage service like iCloud when set to **Yes**.	
Enable Location Services	
Allows wrapped applications to receive the latitude and longitude of the device when set to **Yes**.	
Enable Bluetooth	
Allows applications to access Bluetooth functionality on devices when set to **Yes**.	
Enable Screenshot	
Allows applications to access screenshot functionality on devices when set to **Yes**.	

Enable Watermark	
Displays text in a watermark in documents in the VMware Content Locker when set to Yes. Enter the text to display in the Overlay Text field or use lookup values. You cannot change the design of a watermark from the AirWatch Console	

Limit Documents to Open Only in Approved Apps		
Enter options to control the applications used to open resources on devices. (iOS only) You can use VMware AirWatch Configuration values to restrict users from importing files from third-party applications into Content Locker. For more information, see **Configure Import Restriction in Content Locker** section.		
Allowed Applications List		
Enter the applications that you allow to open documents.		
Disabled	Allow end user access to all device functions.	–

3. **Save**.

4. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Settings**.

5. Configure **Settings**.

Branding		
Enabled	Apply specific organizational logo and colors, where applicable settings apply, to the app suite.	–
Disabled	Maintain the AirWatch brand throughout the app suite.	√
Logging		
Enabled	Access and configure settings related to collecting logs.	√
Logging Level Choose from a spectrum of recording frequency options: • **Error** – Records only errors. An error displays failures in processes such as a failure to look up UIDs or an unsupported URL. • **Warning** – Records errors and warnings. A warning displays a possible issue with processes such as bad response codes and invalid token authentications. • **Information** – Records a significant amount of data for informational purposes. An information logging level displays general processes as well as warning and error messages. • **Debug** – Records all data to help with troubleshooting. This option is not available for all functions.		
Send logs over Wi-Fi only Select to prevent the transfer of data while roaming and to limit data charges.		
Disabled	Do not collect any logs.	–
Analytics		
Enabled	Collect and view useful statistics about apps in the SDK suite.	√
Disabled	Do not collect useful statistics.	–
Custom Settings		
Enabled	Apply custom XML code to the app suite.	–
Disabled	Do not apply custom XML code to the app suite.	√

6. **Save**.

(iOS Only) Configure Import Restriction in Content Locker

You can use the configuration keys in UEM console to restrict import of content from third-party applications into the Content Locker. The configuration keys can be used to allow content import from only whitelisted set of native applications.

Use the following configuration keys to restrict or allow content import from third-party applications into Content Locker.

Configuration Key	Value Type	Supported Values	Description
{"ContentImportRestriction"}	Boolean	true = restriction enabled false = restirction disabled For example, {"ContentImportRestriction": true}.	When enabled, device users cannot import content from any non-whitelisted third-party applications including the native iOS applications into the Content Locker.
{"ContentImportAllowNativeApps"}	Boolean	true = import from native applications are allowed false = import from native applications are not allowed For example, {"ContentImportAllowNativeApps": true}	When enabled, the device users can import content from native applications when the import restriction is enabled.

The ContentImportRestriction and ContentImportAllowNativeApps configuration values can be used in combination to configure the import restriction as per your requirement. If you want to allow import of content from all native apps, enable the ContentImportAllowNativeApps key. The ContentImportAllowNativeApps key is enabled by default and allows import from all native apps such as iOS native Email, Files, Safari, AirDrop, and such. When enabled, the device users can open and import content from non-whitelisted apps into Content Locker using the web versions of the non-whitelisted applications (using Safari).

If you want to allow only specific applications, disable the ContentImportAllowNativeApps key and add the allowed applications in the whitelist.

If you want to restrict importing of content from specific native apps, disable the ContentImportAllowNativeApps key and add the allowed native applications in the whitelist.

Note: The Limit Documents to Open Only in Approved Apps option must be enabled in the Data Loss Prevention settings before enabling the configuration key values. Safari and AirDrop cannot be whitelisted as there is no associated bundle ID.

If you are using SDK Default settings:

1. Navigate to **Group & Settings** > **All Settings**.
2. From All Settings, navigate to **Apps** > **Settings&Policies** > **Settings**.
3. Select **Enable Custom Settings** and paste the configuration keys as per your requirement. For example, to allow import only from native apps, { "ContentImportRestriction": true, "ContentImportAllowNativeApps": true}.
4. To allow importing from a specific list of apps (whitelist):
   a. Navigate to **Settings and Policies** > **Security Policies**.
   b. Select the **Allowed Applications List** text box and list the applications you want to allow the users to import content into the Content Locker.
5. Select **Save**.

If you are using a custom SDK profile for Content Locker:

1. Navigate to **Group & Settings** > **All Settings**.
2. If you have an existing custom profile, navigate to **Apps** > **Settings & Policies** > **Profiles** > **Custom Profile** > **Custom Settings**.
3. If you want to add a custom profile, navigate to **Apps** > **Settings & Policies**> **Profiles** > **Add Profile** > **SDK Profile** > **iOS**> **Custom Settings**.
4. From Custom Settings, select **Configure** and paste the configuration keys as per your requirement. For example to allow import only from native apps, { "ContentImportRestriction": true, "ContentImportAllowNativeApps": true}.
5. From the Restriction section, select **Restrict documents to be opened in following apps** and add the list of apps that you want to allow as per your requirement (whitelist).
6. Select **Save**.

(iOS Only) Configure PDF Autosave in Content Locker

From Content Locker v4.13.2, the device users can enable or disable the PDF Autosave functionality by using the Enable PDF Autosave setting in the Content Locker app. The PDF Autosave setting is disabled by default. The PDF Autosave function can be set to 30 seconds, 60 seconds, and 120 seconds respectively using the Autosave time in seconds setting in the Content Locker. The administrators can use the configuration key provided by VMware AirWatch in the AirWatch Console to force enable the PDF Autosave functionality in Content Locker. When enabled using the configuration key, the device users cannot disable the PDF Autosave function and the Enable PDF Autosave setting is unavailable in the Content Locker. When the PDF Autosave function is enabled, the changes made to a PDF file when an autosave is in progress are not saved. After every instance of an autosave, the PDF document is reloaded.

Use the following configuration key to enable PDF Autosave function is Content Locker:

Configuration Key	Value Type	Supported Values	Description
{ "ContentPDFAutoSaveEnabled" }	Boolean	true = enabled false = can be enabled or disabled by the device user	When set to True, the PDF Autosave functionality is enabled and the device users cannot disable the setting. The Enable PDF Autosave setting in the Content Locker is unavailable to the device users.

If you are using SDK Default settings:

1. Navigate to **Group & Settings** > **All Settings**.
2. From All Settings, navigate to **Apps** > **Settings & Policies** > **Settings**.
3. Select **Enable Custom Settings** and paste the configuration keys as per your requirement.
   For example, to enable PDF Autosave, { "ContentPDFAutoSaveEnabled": true }.
4. Select **Save**.

If you are using a custom SDK profile for Content Locker:

1. Navigate to **Group & Settings** > **All Settings**.
2. If you have an existing custom profile, navigate to **Apps** > **Settings & Policies** > **Profiles** > **Custom Profile** > **Custom Settings**.
3. If you want to add a custom profile, navigate to **Apps** > **Settings & Policies**> **Profiles** > **Add Profile** > **SDK Profile** > **iOS**> **Custom Settings**.
4. From Custom Settings, select **Configure** and paste the configuration keys as per your requirement.
   For example, to enable PDF Autosave, { "ContentPDFAutoSaveEnabled": true }.
5. Select **Save**.

(iOS and Android Only) Configure Privacy Settings for Content Locker

Use the configuration keys in the UEM console to perform additional privacy disclosure and data collection practices. End users who are upgrading or are starting to use the latest version of Content Locker are presented with new privacy dialog screen upon the application launch. For more information about the privacy notice and data sharing settings, see https://support.workspaceone.com/articles/360005402834.

The privacy dialog screen lets the user know the following information:

- **Data collected by the app** – Provides a summary of data that is collected and processed by the application. Some of this data is visible to administrators of the Workspace ONE UEM administration console.
- **Device Permissions** – Provides a summary of device permissions requested for the app to enable product features and functionality, such as push notifications to the device.
- **Company's privacy policy** – By default, a message is displayed to the user to contact their employer for more information. You can configure the privacy policy URL in the UEM console. Once configured, the user can access the employer's privacy policy from the app.

Use the following configuration keys to enable privacy notice and data sharing settings in Content Locker:

Configuration Key	Value Type	Supported Values	Description
{ "DisplayPrivacyDialog" }	Integer	0 = disabled 1 = enabled (default)	When set to '1' (enabled), Content locker displays a privacy notice to the users about the data that is collected and the permissions that are required on the device for the optimal functioning of the app.
{ "PolicyAllowFeatureAnalytics" }	Integer	0 = disabled 1 = enabled (default)	When set to '1' (enabled), Content locker displays a notice to the users about the option to opt-in to anonymous feature usage analytics that help VMware improve product functionality and invent new product capabilities. When set to '0', the data sharing notice is not displayed and no data is collected from the device to optimize the app experience.
{ "PolicyAllowCrashReporting" }	Boolean	True = enabled False = disabled	When set to True, app crashes are reported back to VMware.
{ "PrivacyPolicyLink" }	String	"https://www.url.com"	Provide the Policy URL that you want your users to visit when Your company's privacy policy is selected from the Privacy notice.

If you are using SDK Default settings:

1. Navigate to **Group & Settings** > **All Settings**.
2. From All Settings, navigate to **Apps** > **Settings & Policies** > **Settings**.
3. Select **Enable Custom Settings** and paste the configuration keys as per your requirement.
   For example, to enable Crash reporting, { "PolicyAllowCrashReporting": true}.
4. Select **Save**.

If you are using a custom SDK profile for Content Locker:

1. Navigate to **Group & Settings** > **All Settings**.
2. If you have an existing custom profile, navigate to **Apps** > **Settings & Policies** > **Profiles** > **Custom Profile** > **Custom Settings**.
3. If you want to add a custom profile, navigate to **Apps** > **Settings & Policies**> **Profiles** > **Add Profile** > **SDK Profile** > **iOS**> **Custom Settings**.
4. From Custom Settings, select **Configure** and paste the following configuration keys as per your requirement.
5. Select **Save**.

Assign the Default or Custom Profile

To apply Workspace ONE UEM features built with the AirWatch SDK, you must apply the applicable default or custom profile to an application. Apply the profile when you upload or edit the application to the Workspace ONE UEM console.

1. Navigate to **Apps & Books > Applications > Native > Internal** or **Public**.
2. Add or edit an application.
3. Select a profile on the **SDK** tab:
   - **Default Settings Profile**
     - For Android applications, select the **Android Default Settings @ <Organization Group>**.
     - For Apple iOS applications, select the **iOS Default Settings @ <Organization Group>**.
   - **Custom Settings Profile** – For Android and Apple iOS applications, select the applicable legacy or custom profile.
4. Make other configurations and then save the application and create assignments for its deployment.

Changes to Default and Custom Profiles

When you make changes to the default or custom profile, Workspace ONE UEM applies these edits when you select **Save**.

Changes can take a few minutes to push to end-user devices. Users can close and restart Workspace ONE UEM applications to receive updated settings.

Set the AirWatch Agent for Apple iOS

Configure the AirWatch Agent for Apple iOS to use the correct default profile to apply SDK functionality.

If you do not set the AirWatch Agent to apply the configurations, your configurations in Settings and Policies do not work on devices.

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Apple iOS > Agent Settings**.
2. Set the **SDK Profile V2** option in the **SDK PROFILE** section to the default profile by selecting **iOS Default Settings @ <Organization Group>**.
3. **Save** your settings.

Set the AirWatch Agent for Android

Configure the AirWatch Agent for Android to use the correct default profile to apply SDK functionality.

If you do not set the AirWatch Agent to apply the configurations, your configurations in Settings and Policies do not work on devices.

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Android > Agent Settings**.
2. Set the **SDK Profile V2** option in the **SDK PROFILE** section to the default profile by selecting **Android Default Settings @ <Organization Group>**.
3. **Save** your settings.

Supported Settings and Policies Options for the SDK

Use the default settings profile to apply an AirWatch SDK feature to an SDK-built application, a Workspace ONE UEM application, or a wrapped application by setting the configurations in **Policies and Settings**. View which SDK default settings are supported by the SDK and app wrapping by platform.

Scope

The table lists the default settings supported by the SDK and app wrapping. For information about supported features for Workspace ONE UEM applications, see the content for that application.

- VMware Boxer Comparison Matrix for Microsoft Exchange
- VMware Browser Features Matrix
- VMware Content Locker Capabilities by Platform

Settings and Policies Supported Options for SDK and App Wrapping

UI Label	SDK		App Wrapping	
iOS	Android	iOS	Android	
Force Token For App Authentication: Enable	✓	✓	X	X
Passcode: Authentication Timeout	✓	✓	✓	✓
Passcode: Maximum Number Of Failed Attempts	✓	✓	✓	✓

UI Label	SDK		App Wrapping	
iOS	Android	iOS	Android	
Passcode: Passcode Mode Numeric	✓	✓	✓	✓
Passcode: Passcode Mode Alphanumeric	✓	✓	✓	✓
Passcode: Allow Simple Value	✓	✓	✓	✓
Passcode: Minimum Passcode Length	✓	✓	✓	✓
Passcode: Minimum Number Complex Characters	✓	✓	✓	✓
Passcode: Maximum Passcode Age	✓	✓	✓	✓
Passcode: Passcode History	✓	✓	✓	✓
Passcode: Biometric Mode	✓	✓	✓	✓
Username and Password: Authentication Timeout	✓	✓	✓	✓
Username and Password: Maximum Number of Failed Attempts	✓	✓	✓	✓
Single Sign On: Enable	✓	✓	✓	✓
Integrated Authentication: Enable Kerberos	x	x	x	x
Integrated Authentication: Use Enrollment Credentials	✓	✓	✓	*✓
Integrated Authentication: Use Certificate	✓	✓	x	x
AirWatch App Tunnel: Mode	✓	✓	✓	✓
AirWatch App Tunnel: URLs (Domains)	✓	✓	✓	✓
Content Filtering: Enable	✓	x	x	x
Geofencing: Area	✓	x	x	x
DLP: Bluetooth	✓	✓	x	✓
DLP: Camera	✓	✓	✓	✓
DLP: Composing Email	✓	x	✓	✓
DLP: Copy and Paste Out	✓	✓	✓	✓
DLP: Copy and Paste Into	✓	✓	✓	✓
DLP: Data Backup	✓	x	✓	x
DLP: Location Services	✓	x	✓	✓

UI Label	SDK		App Wrapping	
iOS	Android	iOS	Android	
DLP: Printing	✓	✓	✓	✓
DLP: Screenshot	x	✓	x	✓
DLP: Third Party Keyboards	✓	x	x	x
DLP: Watermark	✓	✓	✓	✓
DLP: Limit Documents to Open Only in Approved Applications	✓	✓	✓	✓
NAC: Cellular Connection	✓	x	✓	x
NAC: Wi-Fi Connection	✓	x	✓	✓
Branding: Enable	✓	✓	✓	x
Logging: Enable	✓	✓	✓	✓
Analytics: Enable	✓	✓	x	x
SDK App Compliance: Enable	✓	✓	x	x
Compromised Detection: Enable	✓	✓	x	x
Offline Access: Enable	✓	✓	x	x

*✓ This option is supported only on Android apps that use Webview.

Configure to Force Authentication Token for the Default SDK Profile

Force the use of an app token to access SDK-built applications with the **Force Token For App Authentication** option.

Behavior

This setting controls how the system allows users to access SDK-built applications, either initially or through a forgot-passcode procedure. When enabled, the system forces the user to generate an application token through the Self-Service Portal (SSP) and does not allow username and password.

Procedure

See **Supported Settings and Policies Options for the SDK** to find out which default settings the SDK supports. Find the matrix in the **Workspace ONE UEM Mobile Application Management Guide**. To know what default settings Workspace ONE UEM applications support, see the topics for that specific application.

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.
2. Enable the **Force Token For App Authentication** to force the use an application token. This does not force the reset of the enrollment token.

Authentication Type

Configure Workspace ONE UEM applications, applications built using the AirWatch SDK, and app wrapped applications to allow access when users authenticate with a set process. Select an authentication type depending on the credentials desired for access; users can set their own or use their Workspace ONE UEM credentials.

Select an authentication type that meets the security needs of your network. The passcode gives device users flexibility while user name and password offers compatibility with the Workspace ONE UEM system. If security is not an issue, then you do not have to require an authentication type.

Setting	Description
Passcode	Designates a local passcode requirement for supported applications. Device users set their passcode on devices at the application level when they first access the application.
User name and Password	Requires users to authenticate to supported applications using their Workspace ONE UEM credentials. Set these credentials when you add users in the **Accounts** page of the Workspace ONE UEM console.
Disabled	Requires no authentication to access supported applications.

Authentication Type and SSO

Authentication Type and SSO can work together or alone.

- Alone – If you enable an Authentication Type (passcode or user name/password) without SSO, then users must enter a separate passcode or credentials for each individual application.
- Together – If you enable both Authentication Type and SSO, then users enter either their passcode or credentials (whichever you configure as the Authentication Type) once. They do not have to reenter them until the SSO session ends.

Configure Authentication Type for the Default SDK Profile

Configure how device users authenticate to various components after you configure the app to use the default SDK settings. Components include Workspace ONE UEM applications, applications built using the AirWatch SDK, and wrapped applications.

See **Supported Settings and Policies Options for the SDK** to find out which default settings the SDK supports. Find the matrix in the **Workspace ONE UEM Mobile Application Management Guide**. To know what default settings Workspace ONE UEM applications support, see the topics for that specific application.

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.
2. Set the **Authentication Type** and complete settings for the desired authentication method.

- **Passcode**

Passcode Setting	Description
Passcode	Enable this option to require a local passcode requirement.
Authentication Timeout	Define the time elapsed, ranging from the last successful authentication to the value set here, that triggers the system to prompt for Workspace ONE UEM credentials. On newer Android applications, authentication timeout prompts for credentials when the session is inactive for the set time.
Maximum Number Of Failed Attempts	Set the maximum times, a user can log in, with an incorrect passcode before the system throws an error. Actions depend on the platform. ◦ Android – The system performs an enterprise wipe on the device. ◦ iOS – The system performs an enterprise wipe on the device.
Passcode Mode	Set as **Numeric** or **Alphanumeric**.
Allow Simple Value	Set the passcode to allow simple strings. For example, allow strings like *1234* and *1111*.
Minimum Passcode Length	Set the minimum number of characters for the passcode.
Minimum Number Of Complex Characters (if Alphanumeric is selected)	Set the minimum number of complex characters for the passcode. For example, allow characters like **[]**, **@**, and **#**.
Maximum Passcode Age (days)	Set the number of days the passcode remains valid before you must change it.
Passcode History	Set the number of passcodes the Workspace ONE UEM console stores so that users cannot use recent passcodes.
Biometric Mode	Select the system used to authenticate for access. ◦ **Fingerprint** – Require users to access the application with their fingerprints. You must configure a device passcode and fingerprint before using the application. ◦ **Disabled** – Does not require biometric authentication systems to access the application.

- **User Name and Password**

Username and Password Setting	Description
Username and Password	Enable this option to set authentication to use the Workspace ONE UEM credentials.*
Authentication Timeout	Define the time elapsed, ranging from the last successful authentication to the value set here, that triggers the system to prompt for Workspace ONE UEM credentials. On newer Android applications, authentication timeout prompts for credentials when the session is inactive for the set time.
Maximum Number Of Failed Attempts	Set the maximum times, a user can log in, with an incorrect passcode before the system throws an error. Actions depend on the platform. ◦ Android – The system prompts the user for their Workspace ONE UEM credentials. ◦ iOS – The system performs an enterprise wipe on the device.
Biometric Mode	Select the system used to authenticate for access. ◦ **Fingerprint** – Require users to access the application with their fingerprints. You must configure a device passcode and fingerprint before using the application. ◦ **Disabled** – Does not require biometric authentication systems to access the application.
*For Workspace ONE UEM Video stand-alone applications, configure Username and Password so that users can log out of the application.	

- **Disabled**

  Select to require no authentication to access the application.

3. **Save** your settings.

Enable Single Sign On for the Default SDK Profile

Apply single sign-on (SSO) to Workspace ONE UEM applications, wrapped applications, and SDK-enabled applications. This option allows users to enter a single SSO passcode to access supported resources without having to enter login credentials in each application.

Using either the AirWatch Agent or the AirWatch Container as a "broker application", end users can authenticate once using either their normal credentials or an SSO passcode. They gain access to other applications so long as the SSO session is active. See SSO Session and the Airwatch Agent on page 222 for information.

For information about SSO for Apple iOS 7+ using Kerberos authentication, refer to the **VMware Workspace ONE UEM Apple iOS Platform Guide**.

See **Supported Settings and Policies Options for the SDK** to find out which default settings the SDK supports. Find the matrix in the **Workspace ONE UEM Mobile Application Management Guide**. To know what default settings Workspace ONE UEM applications support, see the topics for that specific application.

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.
2. Set **Single Sign On** to **Enabled** to give end-users access to all Workspace ONE UEM applications and to maintain a persistent login.
3. Optionally, set **Authentication Type** to **Passcode** and set the **Passcode Mode** to either **Numeric** or **Alphanumeric** to require an SSO Passcode on the device.

   If you enable SSO but do not enable an Authentication Type, the system does not prompt end users with any recurring authentication. An exception to this behavior occurs when end users must authenticate during an initial installation of the application. They use their normal credentials to authenticate in this instance.

SSO Session and the Airwatch Agent

Once an end user authenticates with an application participating in SSO, a session establishes. The session is active until the **Authentication Timeout** defined in the SDK profile is reached or if the user manually locks the application.

When using the AirWatch Agent as a "broker application" for features such as the single sign-on feature, configure the Airwatch Agent with the applicable SDK profile. If you are using the default SDK profile, ensure that the AirWatch Agent is configured to use this profile. If you do not set the AirWatch Agent to use the default SDK profile, then the system does not apply your configurations you configure in the Settings and Policies section.

SSO Configurations and System Login Behavior

Workspace ONE UEM allows access to iOS applications with single sign on enabled in two phases. Workspace ONE UEM checks the identity of the application user and then it secures access to the application.

Application Access With SSO Enabled

The authentication process to an application with Workspace ONE UEM SSO enabled follows the general process.

Access Phase	User Actions	Authentication Method
Identify for app access	Install app	
	Log in to app	• Silent login (managed MDM token) • Authenticate (username and password, token, or SAML)
Secure persistent app access	Successfully log in	
	Access app	Recurring authentication • Passcode • Username and password • Disabled

The first phase ensures that the user's credentials are valid. The system identifies the user first by silent login. If the silent login process fails, then the system uses a configured, authentication system. Workspace ONE UEM supports username and password, token, and SAML.

The second phase grants the user access to the application and keeps the session live with a recurring authentication process. Workspace ONE UEM supports passcode, username and password, and no authentication (disabled).

Authentication Behavior By SSO Configuration

The SSO configuration controls the login behavior users experience when they access applications. The authentication setting and the SSO setting affect the experience of accessing the application.

Authentication phase	SSO enabled	SSO disabled
Passcode		
Identify	**Silent login**: The system registers credentials with the managed token for MDM. If silent login fails, the system moves to the next identification process. **Authenticate**: The system identifies credentials against a common authentication system (username and password, token, and SAML).	**Silent login**: The system registers credentials with the managed token for MDM. If silent login fails, the system moves to the next identification process. **Authenticate**: The system identifies credentials against a common authentication system (username and password, token, and SAML).
Secure	**Prompt if passcode exists**: The system does not prompt for the passcode if the session instance is live. **Prompt if passcode does not exist**: The system prompts users to create a passcode. **Session shared**: The system shares the session instance across applications configured with Workspace ONE UEM SSO enabled.	**Prompt if passcode exists**: The system prompts users the application passcodes. **Prompt if passcode does not exist**: The system prompts users to create a passcode. **Session not shared**: The system does not share the session or the passcode with other applications.
Username and password		
Identify	**Silent login**: The system registers credentials with the managed token for MDM. If silent login fails, the system moves to the next identification process. **Authenticate**: The system identifies credentials against a common authentication system (username and password, token, and SAML).	**Silent login**: The system registers credentials with the managed token for MDM. If silent login fails, the system moves to the next identification process. **Authenticate**: The system prompts for application login credentials.

Authentication phase	SSO enabled	SSO disabled
Secure	**Prompt**: The system does not prompt for the login credentials if the session instance is live. **Session shared**: The system shares the session instance across applications configured with Workspace ONE UEM SSO enabled.	**Prompt**: The system prompts for the login credentials for the application on every access attempt. **Session not shared**: The system does not share the session with other applications.
Disabled		
Identify	**Silent login**: The system registers credentials with the managed token for MDM. If silent login fails, the system moves to the next identification process. **Authenticate**: The system identifies credentials against a common authentication system (username and password, token, and SAML).	**Silent login**: The system registers credentials with the managed token for MDM. If silent login fails, the system moves to the next identification process. **Authenticate**: The system prompts for application login credentials.
Secure	**Prompt**: The system does not prompt users for authentication.	**Prompt**: The system does not prompt users for authentication.

SSO Status Changes and Authentication Behavior

Applications built with the VMware AirWatch SDK behave according to the single-sign on (SSO) session status and the type of authentication configured.

Status Change Triggers Migration for iOS (Swift)

When you change the SSO setting for an SDK-built, iOS (Swift) application, the application joins or exits the existing SSO session sharing cluster. Joining or exiting the cluster triggers the migration of application-specific data.

Note: The SDK for iOS (Objective-C) does not migrate data. When the SSO status changes, the data in the application resets and re-creates where possible.

SSO Status - On to Off

If the admin disables SSO, the SDK migrates data stored from the SSO sharing cluster to the application storage. In some instances, to migrate data, users enter their authentication information. In other scenarios, users experience no difference in the use of the SDK-built application. This migration behavior depends on the authentication type.

Note: The SDK for iOS (Swift) system does not migrate the integrated authentication certificate. The SDK-built application fetches a new certificate and stores it to use specifically for itself.

Authentication Type	Migration Behavior
iOS (Swift)	
Passcode	The system prompts users for SDK-SSO passcodes the next time they open the application. This action triggers the migration of application-specific data from the SSO cluster to the application storage. The system does not migrate the SSO passcode. If the application still requires a passcode for access, the user creates a new one. The system no longer shares this application session with other SSO-enabled applications.
Username and Password	Users perceive no behavior change with the application. They continue to authenticate with their Workspace ONE UEM credentials, username and password. The system migrates application-specific data from the SSO cluster to the application storage. The system does migrate username and password data along with other application-specific data. The system no longer shares this application session with other SSO-enabled applications.
None	Users perceive no behavior change with the application. The system migrates application-specific data from the SSO cluster to the application storage. The system no longer shares this application session with other SSO-enabled applications.
iOS (Objective-C)	
Any	The SDK does not migrate data when admins disable the SSO status. All application-specific data is lost except for the SDK profile configured in the Workspace ONE UEM console.

SSO Status - Off to On

If the admin changes the SSO status to enabled, the SDK migrates data from the application storage to the SSO cluster. The authentication type controls the trigger to migrate data from the application storage to the SSO cluster. The SDK includes two methods for accessing application-specific data to migrate.

1. The SDK attempts to access the application storage.
2. If the first process fails, the SDK attempts to access and to start using the information stored in the SSO cluster. This process requires that another SDK-built application is on the device with SSO enabled.

Note: The SDK for iOS (Swift) system deletes the integrated authentication certificate that was used by the non-SSO SDK-built application. If a certificate exists in the SSO cluster, the system uses this certificate.

Authentication Type	Migration Behavior
iOS (Swift)	
Passcode	The system must change the non-SSO passcode to the SSO passcode. To make this change, the system prompts users for the non-SSO passcode to access the application. Then, the system prompts the users for the SSO passcode used by other SDK-built applications on the device. The system migrates application-specific data from the application storage to the SSO cluster. If no other SDK-built application is on the device with an SSO passcode, the system prompts for the creation one. If the user installs other SDK-built applications, the system shares the SSO session with these applications.
Username and Password	Users perceive no behavior change with the application. They continue to authenticate with their Workspace ONE UEM credentials, username and password. The system migrates application-specific data from application storage to the SSO cluster. The system shares the SSO session with other SDK-built applications.
None	Users perceive no behavior change with the application. The system migrates application-specific data from application storage to the SSO cluster. The system shares sessions with other SDK-built applications.
iOS (Objective-C)	
Any	The SDK does not migrate data when admins enable SSO. All application-specific data is lost except for the SDK profile configured in the Workspace ONE UEM console.

Configure Integrated Authentication for the Default SDK Profile

Enable **Integrated Authentication** to allow access to corporate resources, such as content repositories, through the AirWatch Container or the AirWatch Agent using Workspace ONE UEM SSO credentials.

See **Supported Settings and Policies Options for the SDK** to find out which default settings the SDK supports. Find the matrix in the **Workspace ONE UEM Mobile Application Management Guide**. To know what default settings Workspace ONE UEM applications support, see the topics for that specific application.

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.
2. Select **Enabled** and configure the following settings.

Setting	Description
Enable Kerberos	Use your Kerberos system for authenticating to corporate resources and sites.
Use Enrollment Credentials	Access corporate resources listed in the **Allowed Sites** field with the SSO credentials. Enter systems in the **Allowed Sites** text box to control access to a specific set of sites and domains. You must complete this setting for **Integrated Authentication** to work. This setting ensures that Workspace ONE UEM does not expose credentials to non-trusted resources.

Setting	Description
Use Certificate	Upload the **Credential Source** or set a **Defined Certificate Authority** to access corporate resources listed in the **Allowed Sites** text box with the SSO credentials. Enter systems in the **Allowed Sites** text box to control access to a specific set of sites and domains. You must complete this setting for **Integrated Authentication** to work. This setting ensures that Workspace ONE UEM does not expose credentials to non-trusted resources.

3. **Save** your settings.

App Tunnel Supported Technologies

Workspace ONE UEM supports various application tunneling (app tunneling) solutions that helps individual applications to authenticate and securely communicate with internal back-end resources. By enabling an app tunnel for a specific set of business applications, you can secure you network from unauthorized or malicious applications.

Workspace ONE UEM supports several app tunnel features. Review the menu items and see if you can use them to increase security when users access applications.

App Tunnel Option	Description
Standard Proxy	Enables devices to rely on an existing HTTP or SSL Proxy to determine which content the VMware Browser or other browser accesses.
VMware Tunnel	Accesses corporate content from within your network such as an intranet site. With the VMware Tunnel enabled, you can access the internal corporate content on devices.
F5 Proxy	Accesses your internal network as an alternative to the VMware Tunnel.

Conventional Technology Vulnerabilities

From a security standpoint, app tunneling solutions are more secure than conventional technologies such as SSL VPNs. Conventional technologies allow devices to gain full access to enterprise resources regardless of whether resources are accessed within a business, personal, or malicious application. Full device connectivity through VPN or Wi-Fi carries the risk of data loss, because sensitive data is collected in personal applications and potentially distributed. Also, these conventional technologies put IT at the mercy of end users who might unknowingly have malicious applications on their devices.

VMware Tunnel and F5

The VMware Tunnel and F5 APM serve as relays between your mobile devices and enterprise systems. They authenticate and encrypt traffic from individual applications on compliant devices to the back-end system they are trying to reach.

The F5 APM relay lets you access internal websites and Web apps through the VMware Browser. It also helps access to enterprise systems from your business applications that are wrapped with the AirWatch App Wrapping engine.

Configure App Tunnel for the Default SDK Profile

Enable **App Tunnel** to allow an application to communicate through a VPN or reverse proxy to access internal resources, such as a SharePoint or intranet sites.

See **Supported Settings and Policies Options for the SDK** to find out which default settings the SDK supports. Find the matrix in the **Workspace ONE UEM Mobile Application Management Guide**. To know what default settings Workspace ONE UEM applications support, see the topics for that specific application.

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.
2. Select **Enabled** and then select the **App Tunnel Mode**.

Tunnel Type	Description
AirWatch App Tunnel	Sets devices to access corporate resources using the VMware Tunnel that serves as a relay between mobile devices and enterprise systems. • Select **Configure Tunnel Settings** to enable the VMware Tunnel if you have not already set this feature. • To restrict the communication to a set of tunnel domains, enter domains in the **App Tunnel URLs** text box. All other traffic not listed in this text box, goes directly to the Internet. Use wildcards to allow access to any site with a domain subset. For example, ***.<example>.com** allows traffic to any site that contains **.<example>.com** in its domain. Similarly, it allows access to any port on that site with an implementation similar to ***.<example>.com**. If nothing is listed in this text box, all traffic directs through the app tunnel.
F5	Sets devices to access Web services behind a firewall defined by specific policies that allow secure connections through your F5 components. • To access your internal network, select an **App Tunnel Proxy** from the menu. Add third-party proxies by selecting **Configure F5 Settings**. • To restrict the communication to a set of tunnel domains, enter domains in the **App Tunnel URLs** text box. All other traffic not listed in this text box, goes directly to the Internet. Use wildcards to allow access to any site with a domain subset. For example, ***.<example>.com** allows traffic to any site that contains **.<example>.com** in its domain. Similarly, it allows access to any port on that site with an implementation similar to ***.<example>.com**. If nothing is listed in this text box, all traffic directs through the app tunnel.

Tunnel Type	Description
Standard Proxy	Sets devices to request resources using a proxy server that allows or denies connections to enterprise systems. • To access your internal network, select an **App Tunnel Proxy** from the menu . Add standard proxies by selecting **Configure Standard Proxy Settings**. • To restrict the communication to a set of tunnel domains, enter domains in the **App Tunnel URLs** text box. All other traffic not listed in this text box, goes directly to the Internet. Use wildcards to allow access to any site with a domain subset. For example, ***.<example>.com** allows traffic to any site that contains **.<example>.com** in its domain. Similarly, it allows access to any port on that site with an implementation similar to ***.<example>.com**. If nothing is listed in this text box, all traffic directs through the app tunnel.

3. **Save** your settings.

Content Filtering Integration Settings

Use the **Content Filter** menu item to integrate your Forcepoint (Websense) content filtering service and the VMware Browser.

This integration requires configurations on different pages in the AirWatch Console.

- Third-Party Proxies – Add information on the Third-Party Proxies page for your content filtering system so AirWatch can communicate with it. Configure your Forcepoint information in **Groups & Settings > All Settings > System > Enterprise Integration > Third Party Proxies**.
- Settings and Policies – Used for content filtering on the Settings and Policies page. Using the Settings and Policies, you can filter traffic in the VMware Browser with the policies and rules set in your Forcepoint service.

Integration results in the system filtering the VMware Browser traffic with the settings in the content filtering system. If you use another application tunnel, AirWatch sends data that is not going through your content filtering service to the configured app tunnel.

Configure Content Filtering for the Default SDK Profile

Enable **Content Filtering** to allow or block access to sites in the VMware Browser depending on rules and policies you set in your Forcepoint service.

See **Supported Settings and Policies Options for the SDK** to find out which default settings the SDK supports. Find the matrix in the **Workspace ONE UEM Mobile Application Management Guide**. To know what default settings Workspace ONE UEM applications support, see the topics for that specific application.

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.
2. Enable content filtering and select your system from the list of content filters.
3. **Save** your settings.

Content Filtering and App Tunnel

To benefit from your content filtering system with Workspace ONE UEM, integrate the content filtering feature and the app tunnel . Enter sites in the app tunnel area so the content filter can work on them.

Enter trusted resources or sites in the **App Tunnel URLs** text box on the **Settings and Policies** page. Users can access these internal sites using the app tunnel while Workspace ONE UEM sends the rest of the traffic to your content filter service.

If you do not enter sites in the **App Tunnel URLs** text box, Workspace ONE UEM sends all traffic through the tunnel and your content filter receives no traffic.

Configure Geofencing for the Default SDK Profile

Enable **Geofencing** to restrict access to applications depending on the distances set in Geofencing settings in the Workspace ONE UEM console.

See **Supported Settings and Policies Options for the SDK** to find out which default settings the SDK supports. Find the matrix in the **Workspace ONE UEM Mobile Application Management Guide**. To know what default settings Workspace ONE UEM applications support, see the topics for that specific application.

1. Ensure that a Geofencing area is set in **Device > Profiles > Profile Settings > Areas**.
2. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.
3. Select **Enabled** and then enter the specific area in the **Geofencing Area** text box.
4. **Save** your settings.

Configure Data Loss Prevention for the Default SDK Profile

Enable **Data Loss Prevention** (DLP) to protect sensitive data in applications. DLP options control how and what data transmits back and forth.

See **Supported Settings and Policies Options for the SDK** to find out which default settings the SDK supports. Find the matrix in the **Workspace ONE UEM Mobile Application Management Guide**. To know what default settings Workspace ONE UEM applications support, see the topics for that specific application.

Data loss prevention is not available for AirWatch Container, but it is available for applications in the AirWatch Container.

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.
2. Select **Enabled** for the specific DLP option.

Setting	Description
Enable Bluetooth	Allows applications to access Bluetooth functionality on devices when set to **Yes**.
Enable Camera	Allows applications to access the device camera when set to **Yes**.
Enable Composing Email	Allows an application to use the native email client to send emails when set to **Yes**.

Setting	Description
Enable Copy and Paste Out	Allows users to copy and paste content from SDK-built applications to external destinations when set to **Yes**. When you set it to **No**, the system allows copy and paste only between Workspace ONE UEM applications. Encryption of the pasted content depends upon the configurations for authentication and SSO. If you enable authentication and SSO, the system encrypts the content with a user pin-based key. Otherwise, the system encrypts content with a randomly generated key. The system migrates the setting configured previously in the option to **Enable Copy and Paste** to this feature.
Enable Copy and Paste Into	Allows users to copy and paste content from external destinations into SDK-built applications when set to **Yes**. When you set it to **No**, the system allows copy and paste only between Workspace ONE UEM applications.
Enable Data Backup	Allows wrapped iOS applications to sync data with a storage service like iCloud when set to **Yes**.
Enable Location Services	Allows wrapped applications to receive the latitude and longitude of the device when set to **Yes**.
Enable Printing	Allows an application to print from devices when set to **Yes**.
Enable Screenshot	Allows applications to access screenshot functionality on devices when set to **Yes**.
Enable Third-Party Keyboards	On iOS devices when set to **No**, SDK-built applications always open in the native keyboard and prevent the use of third-party keyboards. On Android devices when set to **No** and the user did not set the system keyboard as the primary keyboard, SDK-built applications prevent user access.
Enable Watermark	Displays text in a watermark in documents in the VMware Content Locker when set to **Yes**. Enter the content to display in the **Overlay Text** text box or use lookup values. You cannot change the design of a watermark from the Workspace ONE UEM console.
Limit Documents to Open Only in Approved Apps	Enter options to control the applications used to open resources on devices.
Allowed Applications List	Enter the applications that you allow to open documents.

3. **Save** your settings.

Configure Network Access for the Default SDK Profile

Enable **Network Access** to allow applications to access the mobile network.

See **Supported Settings and Policies Options for the SDK** to find out which default settings the SDK supports. Find the matrix in the **Workspace ONE UEM Mobile Application Management Guide**. To know what default settings Workspace ONE UEM applications support, see the topics for that specific application.

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.
2. Select **Enabled** and then complete the following options.

Setting	Description
Allow Cellular Connection	Controls cellular connections by allowing them all the time, allowing connections when the device is not roaming, or never allowing cellular connections.
Allow Wi-Fi Connection	Allows connections using Wi-Fi networks, or limits connections by Service Set Identifier (SSID).
Allowed SSIDs	Enter the Service Set Identifiers (SSIDs) that devices can use to access the Wi-Fi network during limiting connections.

3. **Save** your settings.

Configure Branding for the Default SDK Profile

Change the look and feel of applications to reflect the unique brand of your company with **Branding** settings when you configure the app to use the default SDK settings.

See **Supported Settings and Policies Options for the SDK** to find out which default settings the SDK supports. Find the matrix in the **Workspace ONE UEM Mobile Application Management Guide**. To know what default settings Workspace ONE UEM applications support, see the topics for that specific application.

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Settings**.
2. Select **Enabled** for **Branding** and then complete the following options.

Setting	Description
Colors	Reflect your company colors by choosing colors for the Workspace ONE UEM console from the color palette beside the color options. Choose primary and secondary colors listed options including tool bars and text.
Organization Name	Enter the name that represents your organization to display in the Workspace ONE UEM system.

Setting	Description

Device Backgrounds	Upload images that the system displays as the background and as the logo for the organization on the listed device types.
	• Apple iOS options
	  ◦ Background Image iPhone
	  ◦ Background Image iPhone (Retina)
	  ◦ Background Image iPhone 5 (Retina)
	  ◦ Background Image iPad
	  ◦ Background Image iPad (Retina)
	• Android options
	  ◦ Background Image Small
	  ◦ Background Image Medium
	  ◦ Background Image Large
	  ◦ Background Image Extra Large
	• Platform neutral options
	  ◦ Company Logo Phone
	  ◦ Company Logo Phone High Res
	  ◦ Company Logo Tablet
	  ◦ Company Logo Tablet High Resolution

3. **Save** your settings.

Dimensions for Images on iOS Devices

It is difficult to find a single image that displays perfectly on every mobile device. However, certain ratios and dimensions for the images displayed on iOS devices can work for most displays.

Find out the ratios that often work best for branding and icons when you upload images for iOS devices.

Max Constraints

- iPhone – Not exceeding a ratio of 2.88 width over height.
- iPad – Not exceeding a ratio of 4.39 width over height.

Logo Ratios

- iPhone – 1.35 width over height.
- iPad – 1.26 width over height.

Other Considerations

If the image exceeds a height of 111 points (iPhone) or 175 points (iPad), then the image scales down while maintaining the aspect ratio. Points, which are specific to Apple iOS, differ from pixels. The conversion from points to pixel depends specifically on the device. Examples include the following ratios:

- iPhone 4 – 1 point = 1 pixel.
- Retina iPads – 1 point = 2 pixels.
- iPhone 6 Plus – 1 point = 3 pixels.

Configure Logging for the Default SDK Profile

Enable **Logging** so the system records data for applications built with the AirWatch SDK, supported Workspace ONE UEM applications, and wrapped applications.

See **Supported Settings and Policies Options for the SDK** to find out which default settings the SDK supports. Find the matrix in the **Workspace ONE UEM Mobile Application Management Guide**. To know what default settings Workspace ONE UEM applications support, see the topics for that specific application.

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Settings**.
2. Select **Enabled** for **Logging**.
3. Choose your **Logging Level** from a spectrum of recording frequency options.
4. Select **Send logs over Wi-Fi only** to prevent the transfer of data while roaming and to limit data charges.
5. **Save** your settings.

Application Log Limits for SaaS Deployments

The Workspace ONE UEM system collects logs until the log file size reaches 200 MB for SaaS environments. If the log size exceeds 200 MB, the system stops collecting logs. The Workspace ONE UEM console notifies you when your application log size reaches 75% of 200 MB.

To act on the application log size, contact your VMware Workspace ONE UEM Representative.

- Ask for an increase in your application log size.
- Ask for a purge of your application log. The system can purge logs older than two weeks.

You can access the feature to download logs and delete unneeded logs that you enable in this logging feature. See Configure View Logs for Internal Applications on page 172 for details.

Configure Analytics for the Default SDK Profile

Use SDK **Analytics** to view useful statistics for your applications created with the AirWatch SDK or using AirWatch SDK functionality.

For example, you can use SDK analytics to view how many times a file or an application has been opened and how long the file or application remained open. These statistics offer a quick view of which end users have downloaded and viewed high-priority content.

See **Supported Settings and Policies Options for the SDK** to find out which default settings the SDK supports. Find the matrix in the **Workspace ONE UEM Mobile Application Management Guide**. To know what default settings Workspace ONE UEM applications support, see the topics for that specific application.

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Settings**.
2. Select **Enabled** for **Analytics**.
3. **Save** your settings.

Display events and data-use-information for applications that use SDK functionality. See Access SDK Analytics Apps That Use SDK Functionality on page 173 for more information.

Configure Custom Settings for the Default SDK Profile

Enter **Custom Settings** to enter XML code. This XML code allows you to enable or disable certain settings, manually. You can add custom features to your environment to support the unique needs of your mobile network.

See **Supported Settings and Policies Options for the SDK** to find out which default settings the SDK supports. Find the matrix in the **Workspace ONE UEM Mobile Application Management Guide**. To know what default settings Workspace ONE UEM applications support, see the topics for that specific application.

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Settings**.
2. Select **Enabled** for **Custom Settings**.
3. Enter the code in the **Custom Settings** text box.
4. **Save** your settings.

Supported Lookup Values

For the most current list of the supported lookup values for custom settings, select the **Insert Lookup** icon, the plus sign (+), next to the text box.

Configure SDK App Compliance for the Default SDK Profile

You can monitor and enforce compliance on devices that do not have MDM profiles but do have SDK-built applications with the **SDK App Compliance** page. Use the page to configure **Compromised Protection**, **Offline Access**, **OS Version** , and **Security Patch Date**.

See **Supported Settings and Policies Options for the SDK** to find out which default settings the SDK supports. Find the matrix in the **Workspace ONE UEM Mobile Application Management Guide**. To know what default settings Workspace ONE UEM applications support, see the topics for that specific application.

The **SDK App Compliance** setting controls all the items underneath it. If you disable the **SDK App Compliance** setting, you disable the other app compliance features on the page.

Note: There is no custom profile for the **SDK App Compliance** feature.

Block and Wipe Functions for SDK App Compliance Settings

SDK app compliance settings identify non-compliant devices with SDK-built applications installed and act with the block or wipe function.

Wipe

The **Wipe** function, also called an enterprise wipe, clears privileged corporate data off devices that are not compliant with the applicable parameter. The system does not perform wipe actions on data unrelated to the enterprise.

The **Compromised Protection** setting uses only the wipe function.

Block

The **Block** function prevents user access to SDK-built applications that meet a configured parameter.

The **Offline Access**, **OS Version**, and **Security Patch Date** settings use only the block function.

Configure Compromised Protection for the Default SDK Profile

Enable **Compromised Protection** to protect your mobile network from compromised resources.

System Performs an Enterprise Wipe on Compromised Devices

When the system detects that a device is compromised, it performs an enterprise wipe on the device. This behavior happens regardless of configured compliance policies in the Workspace ONE UEM console.

See **Supported Settings and Policies Options for the SDK** to find out which default settings the SDK supports. Find the matrix in the **Workspace ONE UEM Mobile Application Management Guide**. To know what default settings Workspace ONE UEM applications support, see the topics for that specific application.

Configure Compromised Protection

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > SDK App Compliance**.
2. Select **Enabled** for the **SDK App Compliance** menu item to access the compromised protection menu items.

   If you disable this setting, you also disable Compromised Protection.
3. Select **Enabled** to stop a compromised device from accessing your mobile network.
4. The **Block** or **Wipe** functions are read-only. **Compromised Protection** always uses the **Wipe** function. The **Wipe** function, also called an enterprise wipe, clears privileged corporate data off devices. The system does not perform wipe actions on data unrelated to the enterprise.

Configure Offline Access for the Default SDK Profile

Select **Offline Access** to give users access to SDK-built applications when not connected to the network.

See **Supported Settings and Policies Options for the SDK** to find out which default settings the SDK supports. Find the matrix in the **Workspace ONE UEM Mobile Application Management Guide**. To know what default settings Workspace ONE UEM applications support, see the topics for that specific application.

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > SDK App Compliance**.
2. Select **Enabled** for **SDK App Compliance** to access the offline access menu items.

   If you disable this setting, you disable Offline Access.

3. Select **Enabled** to give devices access to resources when not on the network.
4. In the **Maximum Period Allowed Offline** text box, set the time limit for offline access before the device requires reauthentication to the network and applications.
5. The **Block** or **Wipe** functions are read-only. **Offline Access** always uses the **Block** function when the SDK identifies the parameter set for **Maximum Period Allowed Offline**. The **Block** function prevents user access to SDK-built applications.

SDK App Compliance and Offline Access Configurations and SDK Behavior

The SDK restricts or allows offline access depending on the configurations for SDK App Compliance and Offline Access.

SDK App Compliance	Offline Access	Behavior
Enabled	Enabled Maximum Period Allowed = time	The SDK allows offline access and then executes the Block action when the access time meets the time set.
Enabled	Disabled	The SDK prevents offline access.
Disabled	Disabled due to SDK App Compliance configuration	The SDK prevents offline access.