# Application Management

VMware Workspace ONE UEM 1902

**vm**ware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

# Contents

# Introduction to Mobile Application Management

<div style="text-align: right; font-size: large;">1</div>

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.

This chapter includes the following topics:

- Application Types and Supported Platforms
- Benefits of Managed Applications
- Application Configurations
- App and Profile Monitor

## Application Types and Supported Platforms

Workspace ONE UEM classifies applications as native (internal, public, purchased), SaaS, and Web. You upload applications depending on the type.

Workspace ONE UEM supports many platforms and operating systems for most of the application types.

Table 1-1. Application Types and Supported OS Versions

| Application Type | Supported Platforms |
|---|---|
| Industry Templates<br>Any Supported App Type | Apple iOS v7.0+ with limitations for compliance policies |
| Internal | <ul><li>Android v4.0+</li><li>Apple iOS v7.0+</li><li>Apple macOS v10.9+</li><li>Apple tvOS v10.2+</li><li>Windows Phone</li><li>Windows Desktop</li></ul>**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. |

**Table 1-1. Application Types and Supported OS Versions (continued)**

| Application Type | Supported Platforms |
|---|---|
| Public (Free and Paid) | ■ Android v4.0+<br>■ Apple iOS v7.0+<br>■ Chrome OS<br>■ Workspace ONE UEM can manage free, public applications on Windows 10+ devices when you integrate with the Microsoft Store for Business.<br>■ Windows Desktop<br><br>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+<br>■ Apple macOS v10.9+ |
| Web Links | ■ Android v4.0+<br>■ Apple iOS v7.0+<br>■ Apple macOS v10.9+<br>■ Windows Desktop |
| SaaS | ■ Android v4.0+<br>■ Apple iOS v7.0+<br>■ Apple macOS v10.9+<br>■ Windows Desktop |

# Benefits of Managed Applications

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 Configurations

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

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

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

## App and Profile Monitor Statuses

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

**Table 1-2. Descriptions of Deployment Statuses in the App and Profile Monitor**

| Status | Description |
|---|---|
| Done | Devices report the Done status when the app or profile installs successfully. |
| Pending | Devices report the Pending Status when an app or profile reports the following statuses.<br><br>**Profiles**<br>■ Pending Install.<br>■ Pending Removal.<br>■ Unconfirmed Removal.<br>■ Confirmed Removal.<br><br>**Apps**<br>■ Needs Redemption.<br>■ Redeeming.<br>■ Prompting.<br>■ Installing.<br>■ MDM Removal.<br>■ MDM Removed.<br>■ Unknown.<br>■ Install Command Ready for Device.<br>■ Awaiting Install on Device.<br>■ Prompting for Login.<br>■ Updating.<br>■ Pending Release.<br>■ Prompting for Management.<br>■ Install Command Dispatched.<br>■ Download in Progress.<br>■ Command Acknowledged. |
| Incomplete | Device reports the Incomplete Status when an app or profile reports the following statuses.<br><br>**Profiles**<br>■ Pending Information.<br><br>**Apps**<br>■ User Removed.<br>■ Install Rejected.<br>■ Install Failed.<br>■ License Not Available.<br>■ Rejected.<br>■ Management Rejected.<br>■ Download Failed.<br>■ Criteria Missing.<br>■ Command Failed.<br><br>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 **Monitor > App and Profile Monitor**.

2    In the search field, enter the name of the app or profile. You must select the **Enter** key on your keyboard to start the search.

3    Select the app or profile from the drop-down menu and select **Add**.

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

# Configurations to Deploy and Manage Mobile Applications

<div style="text-align: right;">2</div>

Set up systems for the deployment and management of application resources. Systems include notifications, catalogs, and required configurations for certain platforms.

## 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 Application Types and Supported Platforms.

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 Benefits of Managed Applications 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 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.

## 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 Workspace ONE 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 Configurations.

# 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* on the VMWare Docs site https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/index.html.

# Windows Desktop 8.1 and Older Configurations

Set the Workspace ONE 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 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 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 Workspace ONE Intelligent Hub. 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. Review Enable Workspace ONE UEM for Windows Phone Application Distribution for the configurations to set.

This chapter includes the following topics:

- Create Custom Notifications for Applications
- Application Categories
- Configure Google Play Integration for On-Premises Customers
- Root CA for Windows Desktop to Push Internal Applications
- Enable Workspace ONE UEM to Distribute Windows Desktop Internal Applications
- Register Applications With the Windows Phone Dev Center
- Enable Workspace ONE UEM for Windows Phone Application Distribution

# 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.

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.

**Procedure**

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. |
| 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.<br><br>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.<br><br>Use the {ApplicationName} lookup value to populate the application name in each message, automatically. |

# Application Categories

Application categories help with organizing and managing application resources. Use the pre-coded categories or create custom categories.

## 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.

## Configure Application Categories

Application categories help organize your applications and help device users find applications easier. Use them to help organize applications in the console and in a resource catalog.

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.

**Procedure**

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. Enter placeholder information to help the system search for public, Android applications.

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.

**Procedure**

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. |

# Root CA for Windows Desktop to Push Internal Applications

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+.

**Prerequisites**

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.

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

**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, visit the Microsoft Developer Network site.

**Procedure**

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 Workspace ONE UEM console and automatically enables corporate devices to install the enterprise internal application.

# 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.

**Procedure**

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

Distribute applications to devices using the Workspace ONE Intelligent Hub instead of a catalog. 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.

**Procedure**

1  Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Phone > Hub 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.

# Internal Applications

<span style="color:#cccccc; font-size:2em;">3</span>

Use Workspace ONE UEM to manage the deployment and maintenance of your organization's internally developed mobile applications.

## Basics of Internal Applications

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

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

- Deploy Internal Applications as a Local File
- Options for 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 UEMto 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 Deploy Internal Applications as a Local File. After you upload internal applications, use the flexible deployment feature to schedule single or multiple deployments for internal applications. See Flexible Deployment to Assign Applications 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 Options for Internal Applications as a Link.

# 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 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. 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.

# 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 Configure Application Removal Protection 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 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 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.

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 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.

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.

This chapter includes the following topics:

- Supported File Types for Internal Applications

- Deploy Internal Applications as a Local File

- Options for Internal Applications as a Link

- Flexible Deployment to Assign Applications

- Benefits of Tracking Internal App Deployments

- Provisioning Profiles for Enterprise Distribution

- Distribution of Win32 Applications

- Peer Distribution for Win32 Applications

- Configure Application Removal Protection

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

## 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 the Apple iOS or macOS applications do not have spaces in the names. Spaces can cause issues when you load the application to the console.

**Table 3-1. Supported File Types for Internal Applications**

| Platform | File Type |
|----------|-----------|
| Android | APK |
| Apple iOS | IPA |
| macOS | DMG<br>MPKG<br>PKG<br><br>**Note**   You can also use the product provisioning feature to deploy macOS internal applications as DMG, PKG, and APP files. |
| tvOS | IPA |

Table 3-1. Supported File Types for Internal Applications (continued)

| Platform | File Type |
|---|---|
| Windows Desktop | APPX |
| | **Note**   Upload an APPX file, which can be x86, x64, or ARM. However, the APPX installs on only devices that use the same architecture. For example, if you use ARM, Workspace ONE UEM does not queue an installation command for the x64 and x86 architectures. It does not push the application to devices that use x64 or x86 architectures. |
| | 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. |
| Windows Phone | APPX |
| | **Note**   Upload a single APPX file, which can be x86, x64, or ARM. |
| | 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.

# 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.

For internal Apple iOS applications, you must provide a provisioning profile so that the internal application works when it is managed in Workspace ONE UEM. Obtain this file from your Apple iOS application developers.

**Procedure**

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.

| Details Setting | Details 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. |

| Details Setting | Details Description |
| --- | --- |
| Application ID | Represents the application with a unique string. This option is pre-populated and was created with the application.<br><br>Workspace ONE UEM uses the string to identify the application in systems like application whitelists and blacklists. |
| 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.<br><br>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. |
| Supported Processor Architecture | Select the bit-architecture value for applicable Windows applications. |
| 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.<br><br>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.<br><br>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.<br><br>A default scheme offers many integration features for your internal applications, including but not limited to the following options:<br><br>■ Use the scheme to integrate with other platform and web applications.<br>■ Use the scheme to receive messages from other applications and to initiate specific requests.<br>■ Use the scheme to launch Apple iOS applications in the AirWatch Container. |
| Description | Describe the purpose of the application.<br><br>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. |

| Details Setting | Details Description |
|---|---|
| URL | Enter the URL from where you can download the application and get information about it. |
| 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. |

| Developer Information Setting | Developer Information 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. |

| Log Notification for App SDK Setting - iOS | Log Notification for App SDK Description - iOS |
|---|---|
| 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. |

| Installer Package Deployment Setting - Windows Desktop MSI | Installer Package Deployment Description - Windows Desktop MSI |
|---|---|
| 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. |

| Installer Package Deployment Setting - Windows Desktop MSI | Installer Package Deployment Description - Windows Desktop MSI |
|---|---|
| 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. |

| Application Cost Setting | Application Cost 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. 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. 1  Select **Yes** for the **Application Supports Push Notification** option. 2  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 ■ APNs files for development or production | ■ A 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). ■ If the application supports Apple Push Notifications Services (APNs), this file enables messaging functionality. You must upload either the development or production APNs certificate. |
| macOS | Metadata file (pkginfo.plist) | Create this file with a third-party utility tool like Munki or AutoPkgr. You can also use the VMware Admin Assistant to make this file. The file is available in the console when you upload an internal, macOS application. |

| Platform | Auxiliary File | Description |
|---|---|---|
| Windows Desktop | Dependency files | Contains the application software to install and run the application for Windows Desktop. |
| Windows Phone | Dependency files | Contains the application software to install and run the application for Windows Phone. |

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 for tablets. |
| **Icon** | Upload or drag and drop images 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 | 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 | 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.

**What to do next**

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

# Options for Internal Applications as a Link

If you have application packages stored in a repository, internal to your network or in a cloud, you can use links to these repositories to add the application to the Workspace ONE UEM console.

Use these links in combination with flowing delivery configurations to deploy applications to end-users.

- Host applications on and distribute from, a cloud storage system.

- Host applications on internal network repositories and distribute with Content Gateway

- Host an application, either on an cloud storage or on internal network repository, and distribute with Workspace ONE UEM.

# Host and distribute applications from cloud storage

If you are using cloud storage to host an internal application, Workspace ONE UEM facilitates the connection for the device to get the application package from the cloud storage system when the deployment is initiated. Workspace ONE UEM currently does not support cloud storage system links that require authentication. It is important that the internal application package that you host on a cloud storage system is a direct link. This direct link allows the end users to accept the application package through the URL.

# Host application on internal network repository

If you are using a repository on your internal network, the Content Gateway facilitates the connection for the device to get the application from this repository when the Workspace ONE UEM console initiates the deployment. You can host internal applications on your network and manage the applications with Workspace ONE UEM. Workspace ONE UEM uses Windows File Share protocols to make externally hosted applications available to user devices.

For instructions on how to transfer data from the on-premises network to Workspace ONE UEM, see Transfer Data from the On-Premises Network.

# Download and Distribute with Workspace ONE UEM

Select to have Workspace ONE UEM retrieve the package file from a link and store it rather than distributing the link directly to end-users. This functionality is particularly useful for customers who use Workspace ONE UEM for continuous integration between systems to distribute applications. Go to the API help in the console to find the API value. Workspace ONE UEM downloads packages hosted on your internal network repository as well, but you must enable the option to access them with the Content Gateway.

# Transfer Data from the On-Premises Network

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

**Procedure**

1   Configure and use the Content Gateway for Windows to secure communications between your network and Workspace ONE UEM.

    Find information about the Content Gateway on the VMWare Docs site https://docs.vmware.com/en/ VMware-Workspace-ONE-UEM/index.html.

2   Enter the credentials for the external app repository so Workspace ONE UEM can direct users to the application packages hosted on your network in the app repository.

    Workspace ONE UEM supports one set of credentials to authenticate to repositories. If you have multiple repositories set up, use a common set of credentials to authenticate.

    See Add Credentials for the External App Repository.

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

See Add Internal Applications From External Repositories.

# 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

Application link must contain any of the following supported file extension in the URL. UEM console also supports links that contain query parameters at the end.

- app

- appx

- apk

- dmg

- exe

- ipa

- msi

- pkg

- xap

- zip

The following table lists the platform specific supported extensions for all the applications that are uploaded as a link:

Table 3-2. Supported Extensions by Platform

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

## 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.

See Add Internal Applications From External Repositories 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.

**Procedure**

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**.

**What to do next**

See Add Internal Applications From External Repositories for steps to upload internal applications from an external repository to Workspace ONE UEM.

## Add Internal Applications From External Repositories

Set Workspace ONE UEM to distribute a link to a resource or to retrieve a file package and store and distribute it. You can also configure access to an internal resource through the Content Gateway for Windows.

**Procedure**

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.

**http://<ExternalAppRepository > /<InternalAppFileName.FileExtension**

**4**  If this application is hosted on an internal network repository that you want to distribute, select **Access via Content Gateway** .

**5**  If you want Workspace ONE UEM to retrieve the file package, store it, and distribute it rather than just passing the link to devices, select **Download and Distribute Via Workspace ONE UEM Platform**.

**6**  Select **Save** and **Continue** and then configure the remaining tabs.

**What to do next**

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

# Flexible Deployment to Assign Applications

Flexible deployment let's you schedule multiple deployment scenarios for a single application.

You can configure deployments for 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.

**Procedure**

**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.<br><br>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.<br><br>■ **Automatic** – Deploys content to a catalog or other deployment Hub on a device upon enrollment. After the device enrolls, the system prompts users to install the content on their devices.<br><br>This option is the best choice for content that is critical to your organization and its mobile users. |
| **Display in App Catalog - Windows Desktop** | Select **Show** or **Hide** to display an internal or public application in the catalog.<br><br>**Note** The **Show** or **Hide** option is applicable only to the Workspace ONE Catalog and not legacy VMware AirWatch Catalog.<br><br>Use this feature to hide applications in the app catalog you do not want users to access. |
| **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.<br>Desired State Management is enabled by default to enforce application management while installing a macOS software.<br>If enabled, and if the end-user deletes the app, the application is automatically reinstalled on the next Workspace ONE Intelligent Hub sync.<br>If disabled, and if the end-user deletes the app, the application is not automatically reinstalled, unless pushed from the Workspace ONE 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. |
| **Deployment Begins On - Internal Apps** | Set a day of the month and a time of day for the deployment to start.<br>The **Priority** setting governs which deployments push first. Workspace ONE UEM then pushes deployments according to the **Effective** configuration.<br>To set a beginning date with enough bandwidth for successful deployment, consider the traffic patterns of your network. |

| Setting | Description |
|---|---|
| **Policies - DLP**<br>■ **Android**<br>■ **iOS**<br>■ **Windows Desktop**<br>■ **Windows Phone** | Configure a device profile with a **Restrictions** profile to set data loss prevention policies for the application.<br><br>Select **Configure**. The system navigates to **Devices > Profiles**. Select **Add > Add Profile** and the platform.<br><br>■ For Android and iOS devices, select **Restrictions** and enable options in the **Data Loss Prevention** section.<br><br>■ For Windows Desktop, select **Device Profile > Restrictions** and enable options that apply to the data you want to protect.<br><br>■ For Windows Phone, select **Restrictions** and enable options that apply to the data you want to protect. |
| **Policies - Managed Access**<br>■ **Android**<br>■ **iOS** | Enable adaptive management to set Workspace ONE UEM to manage the device so that the device can access the application.<br><br>Workspace ONE controls this feature and is not supported by the AirWatch Catalog. |
| **Policies - Remove on Unenroll**<br>■ **Android**<br>■ **iOS** | Set the removal of the application from a device when the device unenrolls from Workspace ONE UEM.<br><br>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.<br><br>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. |
| **Policies - Prevent Application Backup - iOS** | Prevent backing up the application data to iCloud. |
| **Policies - Make App MDM Managed if User Installed**<br>■ **iOS**<br>■ **Windows Desktop** | Assume management of applications previously installed by users on their devices, supervised and unsupervised.<br><br>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. |
| **Policies - App Tunneling**<br>■ **Android**<br>■ **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. |
| **Policies - Application Configuration**<br>■ **Android**<br>■ **iOS** | Send application configurations to devices.<br><br>**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**.

# Flexible Deployment 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.

Table 3-3. Flexible Deployment Options

| 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.<br><br>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 a catalog. |
| Effective<br>(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<br>(Apple iOS) | View whether Workspace ONE UEM removes the application from a device when the device is unenrolled from Workspace ONE UEM.<br><br>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.<br><br>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<br>(Apple iOS) | View whether Workspace ONE UEM disallows backing up the application data to iCloud. However, the application can still back up to iCloud. |

**Table 3-3. Flexible Deployment Options (continued)**

| 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.<br><br>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. |

# 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.

- Priority 0 = Smart Group HR, to deploy in 10 days with On Demand
- Priority 1 = Smart Group Training, to deploy now with Auto

Device 01 receives the priority 0 assignment and gets the application in 10 days because of the assignments priority rating. Device 01 does not receive the priority 1 assignment.

# Control Flexible Deployment Checks

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

Make edits to batching using scheduler tasks and performance tuning as a System Admin.

**Procedure**

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 Flexible Deployment Batch Frequency

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

**Procedure**

**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 Batch Size For Flexible Deployment

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

Make edits to batching using scheduler tasks and performance tuning as a System Admin.

**Procedure**

**1**   Navigate to **Groups & Settings > All Settings > Installation > Performance Tuning**.

**2**   Edit **Batch Size for Internal Application Deployment**.

## Bypass Batching For Flexible Deployment

Bypass the batching process and release all installation commands for applications.

Make edits to batching using scheduler tasks and performance tuning as a System Admin.

**Procedure**

**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.

**Procedure**

**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.<br><br>**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.<br><br>This action navigates to the **Devices** tab. |
| **Deployment Progress** | **Assigned To** – Lists the smart groups assigned to the application's Flexible Deployment.<br><br>**Status** – Reports Workspace ONE UEM's release of the installation command to devices.<br><br>**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.<br><br>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.<br><br>This action navigates to the **Devices** tab.<br><br>See Reasons for Installation Status for descriptions. |

**4** Select the **Devices** tab and use management functions.

    a Act on installation issues with management functions.

| 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. |

    b Act on devices with 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. The reason codes identify if there is an issue with an installation, so that you can 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. |
| 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 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 blocks represent processes that trigger the reason code in the color blocks.
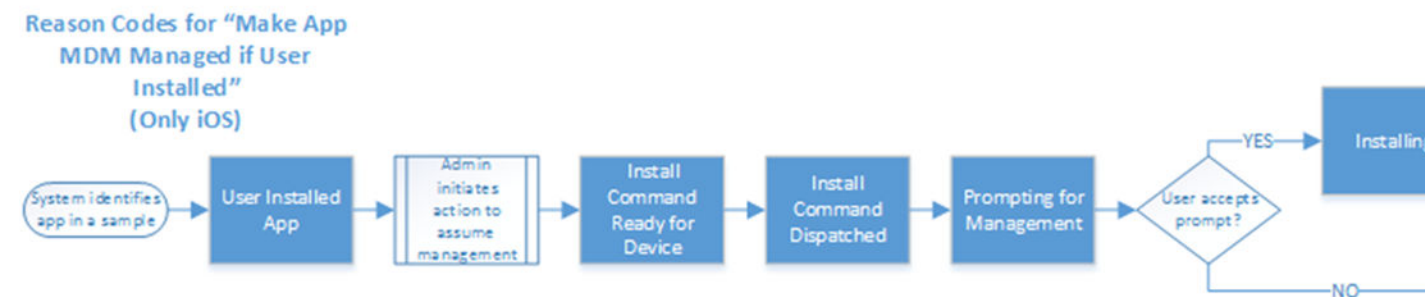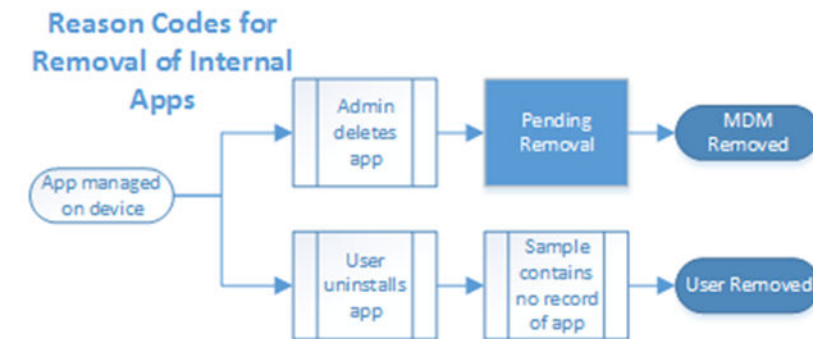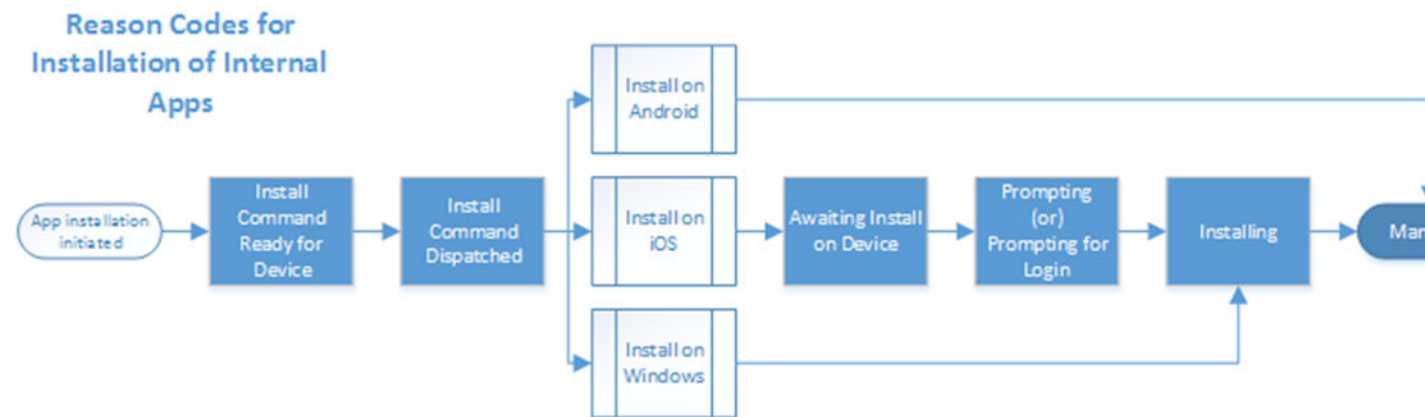
# Provisioning Profiles for Enterprise Distribution

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

With software distribution, Workspace ONE UEM can deploy macOS and Win32 applications from the **Apps & Books** section so that you can use the application flow that exists for all internal applications.

For more information on macOS software distribution configuration and assignment and deployment of applications to macOS devices through the software distribution process, refer the macOS Device Management guide.

If you have scripting needs, use the product provisioning feature described in the *VMware Workspace ONE UEM Product Provisioning for Windows Desktop Guide* on the VMware Docs site at https:// docs.vmware.com/en/VMware-Workspace-ONE-UEM/index.html.

## Prerequisites for Software Distribution

See Requirements to Deploy Win32 Applications for Software Distribution to ensure that you have the systems in place before you deploy Win32 applications through the software distribution feature.

See Win32 Application Installation Behavior, Software Distribution or Product Provisioning to different combinations that you could choose while setting the **Install Context** and **Admin Privileges** during the deployment of Win32 applications.

See the topic *Configure Local File Storage* on the VMware Docs site https://docs.vmware.com/en/ VMware-Workspace-ONE-UEM/index.html to read about how to set up a local file storage as an alternative storage location for on-premises deployments.

## Use the Application Lifecycle for Software Distribution

Read Application Lifecycle for Software Distribution for an overview of the steps to take to deploy Win32 applications and how you can manage them with the application lifecycle features in Workspace ONE UEM.

Follow Upload Win32 Files for Software Distribution for the steps to upload Win32 files to the Workspace ONE UEM console for the software distribution.

See Configure Win32 Files for Software Distribution for the steps to add patches, transforms, and dependencies, and to set other configurations for deployment.

Review Inventory Win32 Applications with Tracking Features for information about use the Details View to track application installations.

Read Methods to Delete Win32 Files to review the options to delete Win32 files off devices.

## Auxiliary File Descriptions

See Dependency Files in Software Distribution for an explanation of what dependency files can do when deployed through Workspace ONE UEM. Also, you can understand the issues that arise when you delete dependency files that are associated with many Win32 applications.

See Patches in Software Distribution for an explanation of the system behavior for assigning cumulative patches to applications and restrictions for patches.

## 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

**Note**  If using a ZIP file, compress application packages that are 4GB or larger using 7-Zip. Workspace ONE UEM does not decompress ZIP packages containing application packages of 4GB or larger when compressed using the native Windows zip compressor.

## CDNs and File Storage Systems

It is considered to be a best practice to use 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 - SaaS Environments

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

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.

## Enable Software Package Deployment - On-premises Environments

Software distribution is now turned on by default in the Workspace ONE UEM console for all on-premises customers. By default, customers get up to 5 GB of storage for applications in the database. For storing large Win32 applications, you can use a file storage system.

It is considered to be a best practice to use content delivery network (CDN) to deploy applications. This option has the advantage of reducing the bandwidth on other servers.

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

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.

### 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.

### 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

Separate the managed content from the Workspace ONE UEM database by storing it in a dedicated File Storage. To set up a file storage, you must determine the location and storage capacity for your file storage, configure the network requirements, and create an impersonation account.

**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.

## 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.<br>If you enable caching, consider accommodating for the amount of space needed on the server.<br>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. |

| Setting | Description |
|---|---|
| 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.

- Upload Win32 Files for Software Distribution - Add the Win32 application and define if it is a dependency file.

- Configure Win32 Files for Software Distribution - Enter details for the Win32 application, add supporting files, and enter deployment criteria. You use the flexible deployment feature to assign to devices.

- Inventory Win32 Applications with Tracking Features - Track the installation progress of Win32 applications.

- Manage Versions of Internal Applications - Add full versions of Win32 applications and patches.

- Methods to Delete Win32 Files - Delete applications with several options.

## Upload Win32 Files for Software Distribution

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

### Prerequisites

If using a ZIP file, compress application packages that are 4GB or larger using 7-Zip. Workspace ONE UEM does not decompress ZIP packages containing application packages of 4GB or larger when compressed using the native Windows zip compressor.

### Procedure

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 Win32 Files for Software Distribution

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.

**Procedure**

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 by uploading dependencies, transforms, patches, and uninstallation processes.

| File | Description | Configurations |
|------|-------------|----------------|
| **App Dependencies**<br>MSI, EXE, ZIP | The environment and devices need these applications to run the Win32 application. | 1 Select dependency files in the **Select Dependent Applications** option.<br>2 Enable the system to apply dependencies in a specified order. The system works from top to bottom. |
| **App Transforms**<br>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**<br>MSP file type | These files add changes that are fixes, updates, or new features to applications. The two types are additive and cumulative.<br>■ **Additive** – Includes only changes developed after the latest version of the application or the last additive patch.<br>■ **Cumulative** – Includes the entire application including any changes since the latest version of the application or the last patches. | 1 Select **Add**.<br>2 Identify the patch as cumulative or additive.<br>3 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.<br>Customized scripts are optional for MSI files. | 1 Select the **Use Custom Script** option.<br>2 Select to upload or enter a script to the system for **Custom Script Type**.<br>■ Select **Upload** and browse to the script file on the network.<br>■ Select **Input** and enter the custom script. |

**3** Complete the settings in **Deployment Options > When To Install**.

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  Select**Data Contingecies > Add** and complete the options that depend on the criteria type you select.

Set contingencies for instrction and completion scenarios.

- Instruction – Contingencies instruct the system to install applications when the device meets specific criteria.

- Completion – Contingencies identify when an installation is complete.

| Setting - App | Description - App |
|---|---|
| Criteria Type<br><br>**App exists**<br><br>**App does not exist** | ■ Instruction – Configure the system to install the application when a specific application is or is not on devices.<br>■ Completion – Configure the system to identify the installation is complete when a specific application is or is not on devices.<br><br>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.<br><br>This value is also known as the product code of the application. |
| **Version** | Enter the specific version. |

| Setting - File | Description - File |
|---|---|
| Criteria Type<br><br>**File exists**<br><br>**File does not exist** | ■ Instruction – Configure the system to install the application when a specific file is or is not on devices.<br>■ 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. |
| **Version** | Enter the specific version. |
| **Modified On** | Enter the date the file was last modified. |

| Setting - Registry | Description - Registry |
|---|---|
| Criteria Type<br><br>**Registry exists**<br><br>**Registry does not exist** | ■ Instruction – Configure the system to install the application when a specific registry is or is not on devices. |

| Setting - Registry | Description - Registry |
|---|---|
| | ■ 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\. |
| Configure Registry Values | ■ **Value Name**- Enter the name of the key. This container object stores the value and it displays in the file structure of the device.<br>■ **Valut Type**- Select the type of key displayed in the file structure of the device.<br>■ **Value Data** - Enter the value of key. The name-data pairs stored in the key display in the file structure of the device. |

    b   Set the disk space devices must have available for the system to install the application for **Disk Space Required**.

    c   Set the battery power devices must have available for the system to install the application for **Device Power Required**.

    d   Set the random access memory devices must have available for the system to install the application for **RAM Required**.

**4**   Complete the settings in **Deployment Options > How To Install**.

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, Software Distribution or Product Provisioning.

| Setting | Description |
|---|---|
| Install Context | Select how the system applies the installation.<br>■ Device- Define the installation by the device and all the users of that device.<br>■ User- Define the installation by particular user accounts (enrolled). |
| Install Command | Enter a command to control the installation of the application.<br>■ **MSI**- The system automatically populates the installation commands, and the commands include patches and transforms.<br>   ■ Patches- To update the order in which the patches install on devices, update their listed order in the install command.<br>   ■ 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.<br>■ **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.<br><br>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. |

| Setting | Description |
|---------|-------------|
| 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.<br><br>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. |

**5** Complete the settings in **Deployment Options > 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.

a Configure the system to use specific criteria to recognize the completion of the installation process for **Use Additional Criteria**.

b To identify the installation completion or use custom scripts, add a specific criteria for **Identify Application By**.

| Setting - Defining Criteria - App | Description - Defining Criteria - App |
|---|---|
| **Criteria Type**<br>**App exists**<br>**App does not exist** | ■ Instruction – Configure the system to install the application when a specific application is or is not on devices.<br>■ Completion – Configure the system to identify the installation is complete when a specific application is or is not on devices.<br>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.<br>This value is also known as the product code of the application. |
| **Version** | Enter the specific version. |

| Setting - Defining Criteria - File | Description - Defining Criteria - File |
|---|---|
| **Criteria Type**<br>**File exists**<br>**File does not exist** | ■ Instruction – Configure the system to install the application when a specific file is or is not on devices.<br>■ 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. |
| **Version** | Enter the specific version. |
| **Modified On** | Enter the date the file was last modified. |

| Setting - Defining Criteria - Registry | Description - Defining Criteria - Registry |
|---|---|
| **Criteria Type**<br>**Registry exists**<br>**Registry does not exist** | ■ Instruction – Configure the system to install the application when a specific registry is or is not on devices.<br>■ 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\. |
| **Configure Registry Values** | ■ **Value Name**- Enter the name of the key. This container object stores the value and it displays in the file structure of the device.<br>■ **Valut Type**- Select the type of key displayed in the file structure of the device. |

| Setting - Defining Criteria - Registry | Description - Defining Criteria - Registry |
|---|---|
| | ■ **Value Data** - Enter the value of key. The name-data pairs stored in the key display in the file structure of the device. |

| Setting - Using Custom Script | Description - 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 |
| Custom Script File | Select **Upload** and navigate to the custom script file on the network. |
| Success Exit | Enter the code that the script outputs to identify the successful installation. |

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

**What to do next**

Assign flexible deployment schedules to the Win32 application. See Add Assignments and Exclusions to Applications.

# Win32 Application Installation Behavior, Software Distribution or Product Provisioning

Workspace ONE UEM console includes different ways you can deploy Win32 applications. Select various installation combinations for software distribution or use product provisioning.

## Product Provisioning Alternative

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**.

**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** select **Add Application** | Navigate to **Deployment options > How To Install** and set<br><br>■ **Install Context = Device**<br>■ **Admin Privileges = Yes**<br><br>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. | ■ **Install Context** set to **Device**<br>■ **Admin Privileges** set to **Yes**<br>■ User is an admin<br><br>The installation completes without any prompt. | ■ **Install Context** set to **Device**<br>■ **Admin Privileges** set to **Yes**<br>■ User is a standard user<br><br>The installation completes without any prompt. |
| Navigate to **Apps & Books > Applications > Native > Internal** select **Add Application** | Navigate to **Deployment options > How To Install** and set<br><br>■ **Install Context = Device**<br>■ **Admin Privileges = No**<br><br>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. | ■ **Install Context** set to **Device**<br>■ **Admin Privileges** set to **No**<br>■ User is an admin<br><br>The installation completes without any prompt. | ■ **Install Context** set to **Device**<br>■ **Admin Privileges** set to **No**<br>■ User is a standard user<br><br>The installation completes without any prompt. |
| Navigate to **Apps & Books > Applications > Native > Internal** select **Add Application** | Navigate to **Deployment options > How To Install** and set<br><br>■ **Install Context = User**<br>■ **Admin Privileges = Yes**<br><br>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. | ■ **Install Context** set to **User**<br>■ **Admin Privileges** set to **Yes**<br>■ User is an admin<br><br>The installation completes without any prompt. | ■ **Install Context** set to **User**<br>■ **Admin Privileges** set to **Yes**<br>■ User is a standard user<br><br>The installation fails. |
| Navigate to **Apps & Books > Applications > Native > Internal** select **Add Application** | Navigate to **Deployment options > How To Install** and set<br><br>■ **Install Context = User**<br>■ **Admin Privileges = No**<br><br>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. | ■ **Install Context** set to **User**<br>■ **Admin Privileges** set to **No**<br>■ User is an admin<br><br>The installation completes with prompt. | ■ **Install Context** set to **User**<br>■ **Admin Privileges** set to **No**<br>■ User is a standard user<br><br>The 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**.

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

**Table 3-4. 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 > Provisioning > Components > Files/ Actions** and select Add Files/Actions. | Navigate to**Manifest** tab and set <br>■ **Action(s) To Perform** = **Install/ Run** <br>■ **Execution Context** = **System** | ■ **Action(s) To Perform** = **Install/ Run** <br>■ **Execution Context** = **System** <br>■ User is an admin <br>The installation completes without any prompt. | ■ **Action(s) To Perform** = **Install/ Run** <br>■ **Execution Context** = **System** <br>■ User is a standard user <br>The installation completes without any prompt. |
| Navigate to **Devices > Provisioning > Components > Files/ Actions** and select Add Files/Actions | Navigate to **Manifest** tab and set <br>■ **Action(s) To Perform** = **Install/ Run** <br>■ **Execution Context** = **Admin** | ■ **Action(s) To Perform** = **Install/ Run** <br>■ **Execution Context** = **Admin** <br>■ The user is an admin <br>The installation completes without any prompt. | ■ **Action(s) To Perform** = **Install/ Run** <br>■ **Execution Context** = **Admin** <br>■ User is a standard user <br>The installation completes with prompt. |
| Navigate to **Devices > Provisioning > Components > Files/ Actions** and select Add Files/Actions | Navigate to **Manifest** tab and set <br>■ **Action(s) To Perform** = **Install/ Run** <br>■ **Execution Context** = **User** | ■ **Action(s) To Perform** = **Install/ Run** <br>■ **Execution Context = User** <br>■ User is an admin <br>The installation completes without any prompt. | ■ **Action(s) To Perform** = **Install/ Run** <br>■ **Execution Context = User** <br>■ User is a standard user <br>The 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. You can change 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.

**Table 3-5. Time to Install and Failure Reported**

| 60 minutes (one hour) | 65 minutes (one hour and five min) | 125 minutes (two hours and five min) | 130 minutes (two hours and 10 min) | 190 minutes (three hours and 10 min) | 195 minutes (three hours 15 min) |
|---|---|---|---|---|---|
| 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.

# Dependency Files in Software Distribution

Dependency files in software distribution 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.

## Supported Scenarios to Assume Management of Win32 Applications

Assuming management of Win32 applications includes certain caveats to work.

### Supported and Unsupported Scenarios

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.

## Assuming Management of Win32 Applications for Software Distribution

When you enable **Make App MDM Managed if User Installed** for Win32 applications, the system processes the command to assume managemet of the Win32 application.

If you enable **Make App MDM Managed if User Installed**, the management assumption process begins with an install command.

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

**Procedure**

1    Workspace ONE UEM sends install commands to devices that enroll after publication.

2   The device responds that it received the command.

3   The next check depends if the admin is assuming management.

4   The system looks for the application on the device.

   If the application is already installed, the system re-downloads and reinstalls the application. If the application is not installed yet, it insalls following the regular configured flexible deployment configurations.

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

## 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.

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.

## Methods to Delete Win32 Files

Workspace ONE UEM includes several methods to remove Win32 applications off devices. Choose from deleting, the application, devices, organiztion group, assignment group, or user. Several admin functions impact multiple assets, so understand the changes before you take action.

Table 3-6. Win32 Application Deletion Methods

| Deletion 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

Use the peer distribution system as another method 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

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 Adaptiva Peer-To-Peer Distribution.

# 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 Workspace ONE 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 Workspace ONE UEM console. 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 Adaptiva Peer-To-Peer Distribution

Peer distribution requires components for communication, data management, application deployment, and optional storage.

## 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.

  For more information on server requirements, see File Storage.

## Peer-to-Peer Server Requirements

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

**Table 3-7. Peer-to-Peer Server Component Requirements**

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

## 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 - Ensure SQL includes the following 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 Workspace ONE UEM console and on devices.

- Enable the software package deployment. See Requirements to Deploy Win32 Applications for Software Distribution.

- Configure the peer distribution software. See Configure Peer Distribution Software Setup with Adaptiva.

- Install and activate peer-to-peer clients on devices. See Configure Peer Distribution Software Setup with Adaptiva.

- Upload and publish applications to the peer-to-peer server. See Application Lifecycle for Software Distribution.

## 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 with Adaptiva

To help set up your peer distribution system and to avoid configuration issues, review the network behaviors, the types of communication, the communication channels between components, and license management.

**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 Workspace ONE UEM representative about alternative ports. See Ports Used for Peer Distribution with Adaptiva 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 with Adaptiva

Open specific ports in your network 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.

### Table 3-8. Messaging from Client to Server

| Sending Component | Receiving Component | Protocol | Port | Description |
|---|---|---|---|---|
| Peer-to-peer clients | Peer-to-peer server | UDP | 34322 | After clients receive small messages, they acknowledge or reply to the server. |
| Peer-to-peer clients | Peer-to-peer server | UDP | 34323 | Clients send small messages to the server. |
| Peer-to-peer clients | Peer-to-peer server | UDP | 34331 | Large replies from clients to the server using Foreground Protocol. |
| Peer-to-peer clients | Peer-to-peer server | UDP | 34333 | Clients send large messages to the server using Foreground Protocol. |
| Peer-to-peer clients | Peer-to-peer server | UDP | 34339 | Large replies from clients to the server using Background Protocol. |
| Peer-to-peer clients | Peer-to-peer server | UDP | 34341 | Clients send large messages to the server using Background Protocol. |

## Table 3-9. Messaging from Server to Client

| Sending Component | Receiving Component | Protocol | Port | Description |
|---|---|---|---|---|
| Peer-to-peer server | Peer-to-peer clients | UDP | 34324 | After the server receives small messages, it acknowledges or replies to clients. |
| Peer-to-peer server | Peer-to-peer clients | UDP | 34325 | Server sends small messages to clients. |
| Peer-to-peer server | Peer-to-peer clients | UDP | 34335 | Large replies from the server to clients using Foreground Protocol. |
| Peer-to-peer server | Peer-to-peer clients | UDP | 34337 | Server sends large messages to clients using Foreground Protocol. |
| Peer-to-peer server | Peer-to-peer clients | UDP | 34343 | Large replies from the server to clients using Background Protocol. |
| Peer-to-peer server | Peer-to-peer clients | UDP | 34345 | Server sends large messages to clients using Background Protocol. |

## Table 3-10. Messaging from Client to Client

| Sending Component | Receiving Component | Protocol | Port | Description |
|---|---|---|---|---|
| Peer-to-peer clients | Peer-to-peer clients<br>■ Same office<br>■ Parent offices<br>■ Child offices | UDP | 34324 | After clients receive small messages from another client, acknowledgments and replies are sent to this port. |
| Peer-to-peer clients | Peer-to-peer clients<br>■ Same office<br>■ Parent offices<br>■ Child offices | UDP | 34325 | Clients send small messages to other clients. |
| Peer-to-peer clients | Peer-to-peer clients<br>■ Same office<br>■ Parent offices<br>■ Child offices | UDP | 34335 | Large replies from clients to clients using Foreground Protocol. |
| Peer-to-peer clients | Peer-to-peer clients<br>■ Same office<br>■ Parent offices<br>■ Child offices | UDP | 34337 | Clients send large messages to other clients using Foreground Protocol. |

## Table 3-10. Messaging from Client to Client (continued)

| Sending Component | Receiving Component | Protocol | Port | Description |
|---|---|---|---|---|
| Peer-to-peer clients | Peer-to-peer clients<br>■ Same office<br>■ Parent offices<br>■ Child offices | UDP | 34343 | Large replies from clients to clients using Background Protocol. |
| Peer-to-peer clients | Peer-to-peer clients<br>■ Same office<br>■ Parent offices<br>■ Child offices | UDP | 34345 | Clients send large messages to other clients using Background Protocol. |

## Table 3-11. Messaging client to Client Broadcast

| Sending Component | Receiving Component | Protocol | Port | Description |
|---|---|---|---|---|
| Peer-to-peer clients | Peer-to-peer clients in the same subnet | UDP | 34329 | Clients broadcast requests to other clients |

## Table 3-12. Data Transfer from Server to Client

| Sending Component | Receiving Component | Protocol | Port | Description |
|---|---|---|---|---|
| Peer-to-peer server | Peer-to-peer clients in the Central Office | UDP | 34760 | Server sends content to clients using Foreground Protocol. |

## Table 3-13. Data Transfer from Client to Client

| Sending Component | Receiving Component | Protocol | Port | Description |
|---|---|---|---|---|
| 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 | Peer-to-peer clients in child offices | UDP | 34750 | Clients send content to clients in child offices using Background Protocol. |

**Table 3-14. Data Transfer Control Ports**

| Sending Component | Receiving Component | Protocol | Port | Description |
|---|---|---|---|---|
| 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 | Peer-to-peer clients in the same office, in parent offices, and in child offices | UDP | 34546 | Clients send a control signal to other clients for any large transfer using Adaptive Protocol. |

**Table 3-15. Data Transfer between VESC, Server, and Database**

| Sending Component | Receiving Component | Protocol | Port | Description |
|---|---|---|---|---|
| VMware Enterprise Systems Connector (VESC) | Peer-to-peer server | UDP | 34323 | VESC sends messages for activation, health checks, application metadata to the peerto-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 control the sources of application packages, also called distribution optimization, in your peer-to-peer deployment, consider how data transfers within networks and subnetworks.

## 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.

## 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.
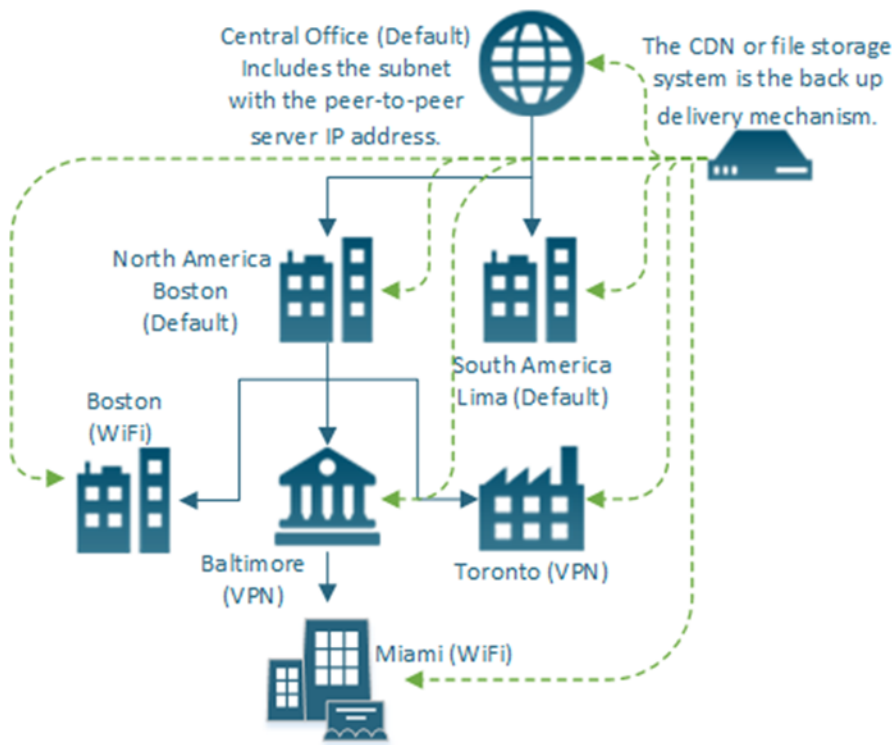


In the example, the rendezvous point (RVP) in the central office sends the initial application package to Boston (Default) and Lima. Following the North American side, the RVPs in the Boston (WiFi), Baltimore, and Toronto offices receive the application package from the Boston (Default) office. The RVP 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 with Adaptiva

Configure the peer distribution system as another method to deploy Win32 applications to enterprise networks. Workspace ONE UEM partners with Adaptiva to offer the peer distribution system.

**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.

**Procedure**

1   Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Peer Distribution > Adaptiva**.

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 Workspace ONE 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 - Configuration | Description - Configuration |
|---|---|
| **Server Name/ IP** | Enter the server name or IP address of the peer-to-peer server.<br>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.<br>This key activates trusted communication between the peer-to-peer server, the peer-to-peer clients, and the Workspace ONE UEM infrastructure.<br>If you do not enter the most recent key generated, the system displays a key mismatch error. |
| **Certificate** | Enable this optional feature to configure a secure mutual authentication between AirWatch Cloud Connector and Adaptiva Server.<br>On enabling this setting, you can upload Adaptiva Public Certificate to the Workspace ONE UEM console.<br>There are benefits to this setting:<br>■ AirWatch Cloud Connector and Adaptiva Server can make sure they are talking to a legit service.<br>■ Achieve Transport Layer Security (TLS) between AirWatch Cloud Connector and Adaptiva Server. |

| Setting - Configuration | Description - Configuration |
|---|---|
| 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.<br><br>Network topologies can be intricate. Before you enable this feature, speak with your network team about the company's network topology.<br><br>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.<br><br>There are benefits to this setting.<br><br>■ 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.<br><br>■ 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.<br><br>■ 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. |

| Setting - Troubleshooting | Description - 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 theWorkspace 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.<br><br>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.

After 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.

## Install the Peer-to-Peer Server

Download the peer-to-peer server from the **Peer Distribution** page in the Workspace ONE UEM console. Install the server and follow the prompts in the installation wizard.

**Procedure**

1   Ensure the machine that hosts the peer-to-peer server meets the requirements listed in Requirements for Adaptiva Peer-To-Peer Distribution.

**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.
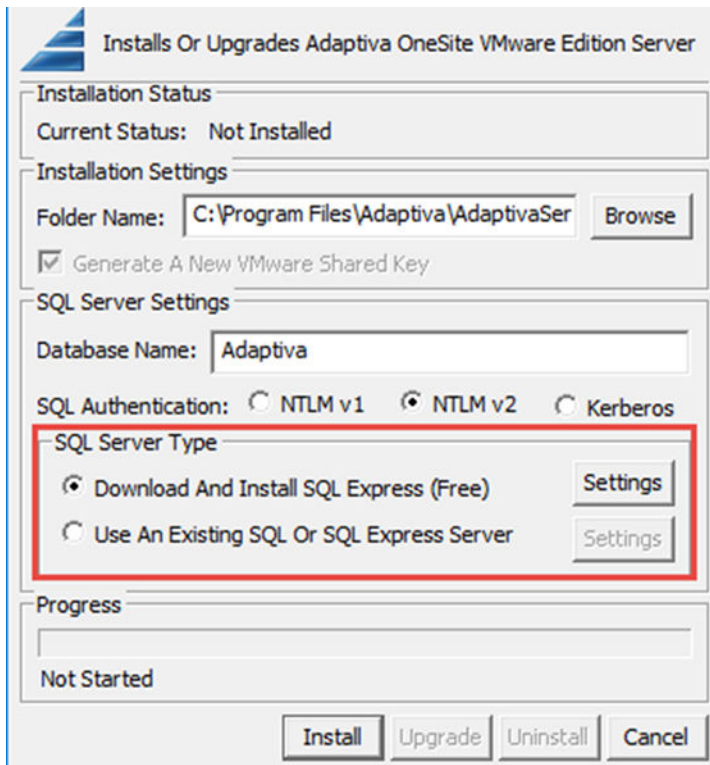


**5** Select **Install**.

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

The peer distribution server downloads and installs.

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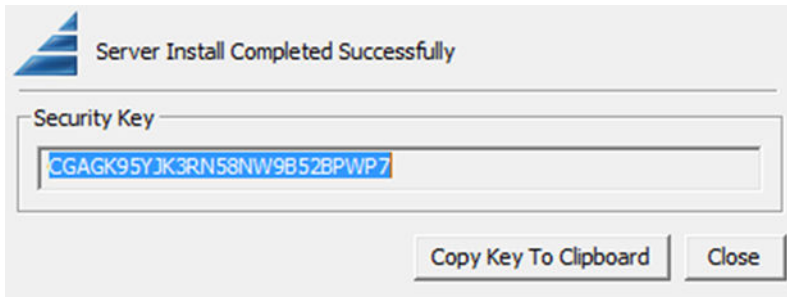


## Generate a New Key for Peer Distribution Installer

If you misplace the original security key, you can generate a new key by re-running the peer distribution installer.

**Procedure**

**1** Rerun the peer-to-peer server installer.

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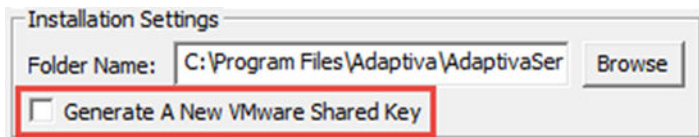


**3** Select **Upgrade**.

## Install SQL Server Express Manually

When installing the peer-to-peer distribution server, some instances need SQL Server Express. If your firewall rules on the peer-to-eer server block the free SQL Server Express download, install it manually.

**Procedure**

**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
```

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

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

# Configure Application Removal Protection

Application removal protection helps ensure that the system does not remove business-critical applications unless approved by the admin. Configure this feature using threshold values and management actions.

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.

**Procedure**

1 View default threshold values or edit the threshold values for the organization group. Enter email addresses that receive notifications about the problem with the **App Remove Limit Reached Notification** template.

If threshold values are met, Workspace ONE UEM holds the application removal commands and displays them by application in the **App Removal Log**.

2 Act on the application removal commands held by the system.

a Purge application removal commands from the command queue by selecting **Dismiss**.

b 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.

## Triggers of Application Removal Protection

The applicatin removal protection system canvasses the application removal command queue for values that meet or exceed your threshold values. Several application or group state changes can trigger application removal commands.

- Edit smart groups.

- Publish applications.

- Deactivate applications.

- Retire applications.

- Delete applications.

## Threshold Values for Application Removal Protection

Threshold values apply to bundle IDs and apply at a Customer type organization group, and in turn are inherited by child organization groups. When setting threshold values and acting on them, consider these characteristics so that admins take informed actions on applications and have the permissions they need to act on commands.

## 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.

# Statuses for Application Removal Protection

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

**Table 3-16. Descriptions and Causes for Statuses in Application Removal Protection**

| Status | Description | Cause |
| --- | --- | --- |
| Held for approval | The protection system holds removal commands, and the system does not remove the associated internal application. <br><br> 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. <br><br> 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.

**Procedure**

**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.

**Procedure**

**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 Workspace ONE 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 Test Application

Add a proprietary Workspace ONE UEM application to the Workspace ONE UEM console for testing using test groups to keep the application separate from your production environment.

**Procedure**

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.

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

# Remove test app

Remove a test version of a proprietary Workspace ONE UEM application with **Remove From All** and the delete or retire actions to ensure complete removal.

**Procedure**

**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.

# Public Applications

# 4

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.

## 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.

To view the platforms and versions that are required to provision public applications, see Application Types and Supported Platforms.

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 the Workspace ONE Managed Access Feature.

## Features for iOS Public Applications

- Paid Public Applications for iOS

  - In some scenarios, 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 for more information on this process.

  - For information about uploading paid public iOS applications, see Enable Paid Public iOS Apps to the Console.

  - Read how to configure paid public applications for iOS at an optimal organization group in Organization Groups, Paid Public Applications.

- 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.

## 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 Integration with the Microsoft Store for Business section.

■ Android - 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.

This chapter includes the following topics:

■ Add Public Applications from an App Store

■ Paid Public iOS Applications and Workspace ONE UEM

■ Public Application Installation Control on iOS Devices

■ Integration with the Microsoft Store for Business

# Add Public Applications from an App Store

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

**Procedure**

**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.<br>■ **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.<br>■ **Android** – If you have configured integration with the Google Play Store, the system searches for the application in the app store.<br><br>This configuration also works when integrating with the Android for Work system. See the **Workspace ONE UEM Integration with Android for Work** guide.<br><br>**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.<br><br>This option enables you to deploy applications that are in a different region from your Workspace ONE UEM server. |
| 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.<br>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.<br>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 - 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. |

| Setting | Description |
|---|---|
| Comments | Enter comments that explain the purpose and use of the application for the organization. |
| Default Scheme<br>■ iOS<br>■ Windows Desktop<br>■ 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.<br>A default scheme offers many integration features for your applications.<br>■ Use the scheme to integrate with other platforms and Web applications.<br>■ Use the scheme to receive messages from other applications and to initiate specific requests.<br>■ 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.

**What to do next**

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

## 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

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

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.

**Procedure**

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.

# 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.

| Add Any Supported iOS Version as Paid Public App | Add iOS 9+ Version as Paid Public App |
|---|---|
| Enable the paid public iOS applications process in the Workspace ONE UEM console. | Enable the paid public iOS applications process in the Workspace ONE UEM console. |
| Add the public application to the Workspace ONE UEM console. Add any other management parameters like SDK features and enabling per-app VPN. | Add the public application to the Workspace ONE 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. |
| (User) Purchase the application. | (User) Purchase the application. Apple installs the application automatically to the device after purchase. |
| (User) Delete the application installed by Apple. | Not applicable |
| (User) Open the AirWatch Catalog and initiate the installation from Workspace ONE UEM to receive the managed version of the application. | (User) Open the AirWatch Catalog and initiate the installation from Workspace ONE UEM to receive the managed version of the application. |

# Organization Groups, 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.

Table 4-1. Example of Paid Public Application Assignment Depending on Organization Group

| 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 Paid Public iOS Apps to the Console

Enable the deployment of paid public iOS applications in the Workspace ONE UEM console.

**Procedure**

**1**  Navigate to **Groups & Settings > All Settings > Apps > Workspace ONE > Paid Public Applications**.

**2**  Select **Enabled**, and then save the settings.

## Deploy Paid Public App

Upload the paid public iOS application from the app store to the Workspace ONE UEM console to make it available in a catalog.

**Prerequisites**

Enable paid public applications in the Workspace ONE UEM console. See Enable Paid Public iOS Apps to the Console.

**Procedure**

**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 icon 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.

Workspace ONE UEM supports native iOS restrictions and an in-house developed restriction that control access to the app store. For a matrix that outlines the supported options, see Apple iOS App Store Restriction Descriptions.

For information about the **Allow App Store icon on Home screen** restriction , see Configure the Apple App Store Restriction. For the steps to use the restriction for older iOS devices, see Restricted Mode for Free Public iOS Applications Older Than iOS 9.

## Apple iOS App Store Restriction Descriptions

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

**Table 4-2. Descriptions of Available App Store Restriction Methods**

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

## Configure the Apple App Store Restriction

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

**Procedure**

1   Navigate to **Devices > Profiles > List View > Add**.

2   Select **Apple iOS**.

3   Configure the **General** settings of the profile.

4   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.

5   Select **Save & Publish** to push the profile to devices.

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

Restriced Mode restricts iOS devices older than iOS 9 from accessing free public applications unless the application is approved and deployed by the organization.

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.

Restricted Mode 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. Restricted Mode does not require an extra restriction with **Allow installing public apps** enabled.

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

Control from where end users install public applications by enabling **Restricted Mode for Public iOS Applications**.

**Procedure**

1   Navigate to **Groups & Settings > All Settings > Apps > Workspace ONE > App Restrictions**.

2   Enable **Restricted Mode for Public iOS Applications**.

# Integration with the Microsoft Store for Business

The 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, integrate the two systems. After integration, acquire applications from the Microsoft Store for Business, distribute them, 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.

## Required Components to Integrate

See Requirements for Microsoft Store for Business Integration for information on the components that integrate Workspace ONE UEM and the Microsoft Store for Business.

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. For more information, see Configure Azure AD Identity Services Integration.

Workspace ONE UEM supports both online and offline licensing models. For a comparison of the two models, see Comparison of the Online and Offline Models of the Microsoft Store for Business .

## Import and Deploy with the Workspace ONE UEM console

See Import Microsoft Store for Business Apps for the steps to import Microsoft Store for Business applications to Workspace ONE UEM. Follow the import by deploying applications as outlined in Deploy Microsoft Store for Business Apps.

## Manage Microsoft Store for Business Applications with Details View

Use the Details View of public, Microsoft Store for Business applications to sync licenses, assign the application to groups, and to edit details about the application.

See Details View Setting Descriptions for information on settings. See Methods to Reclaim Licenses for Microsoft Store for Business Apps for information on license management in the Workspace ONE UEM console.

## Requirements for Microsoft Store for Business Integration

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

### 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 DirectoryDevice 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.

## Comparison of the Online and Offline Models of the Microsoft Store for Business

Online and offline models of the Microsoft Store for Business offer different capabilities. Select the model depending on how you want to manage your deployment. Capabilities include what system manages licenses, where app packages are stored, and what system authenticates to resources.

**Table 4-3. Online and Offline Model Comparison - Different Capabilities**

| Feature | Online License Model | Offline License Model |
| --- | --- | --- |
| 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. |

**Table 4-3. Online and Offline Model Comparison - Different Capabilities (continued)**

| Feature | Online License Model | Offline License Model |
|---|---|---|
| Azure Active Directory | Devices must use your Azure Active Directory system to authenticate.<br><br>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.<br><br>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. |

**Table 4-4. Online and Offline Model Comparison - Same Capabilities**

| Feature | Online License Model | Offline License Model |
|---|---|---|
| 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.
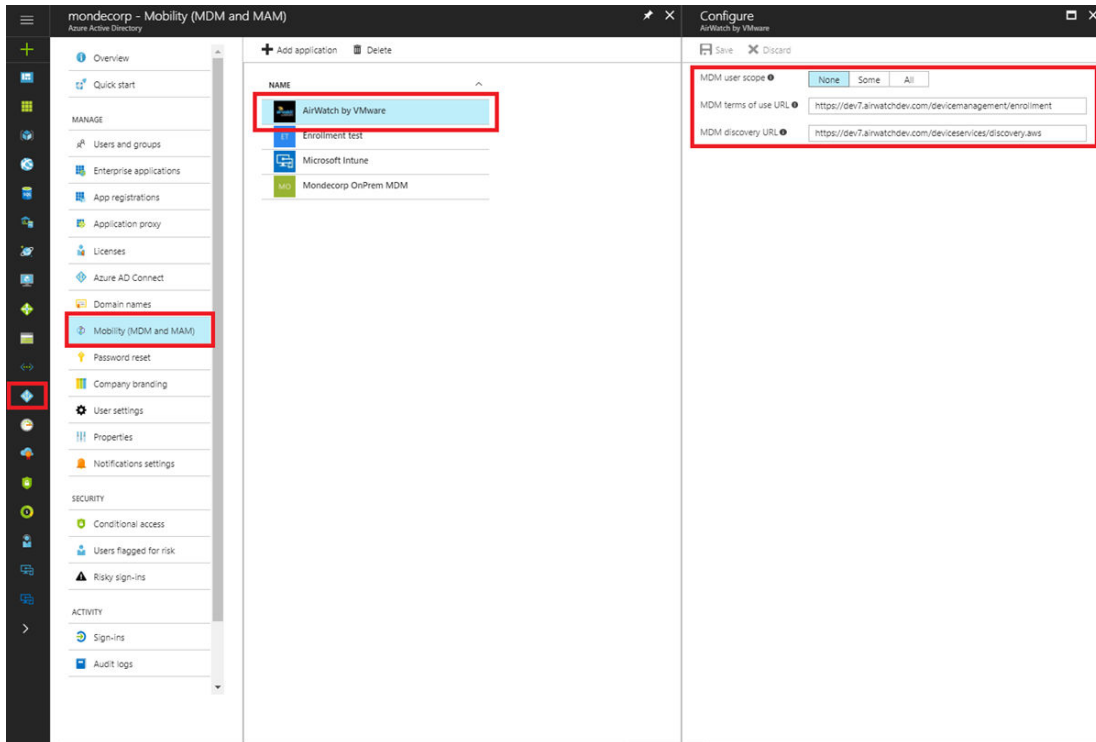


6    Leave the AirWatch by VMware application on the default settings. Change the **MDM user scope** to **None**.
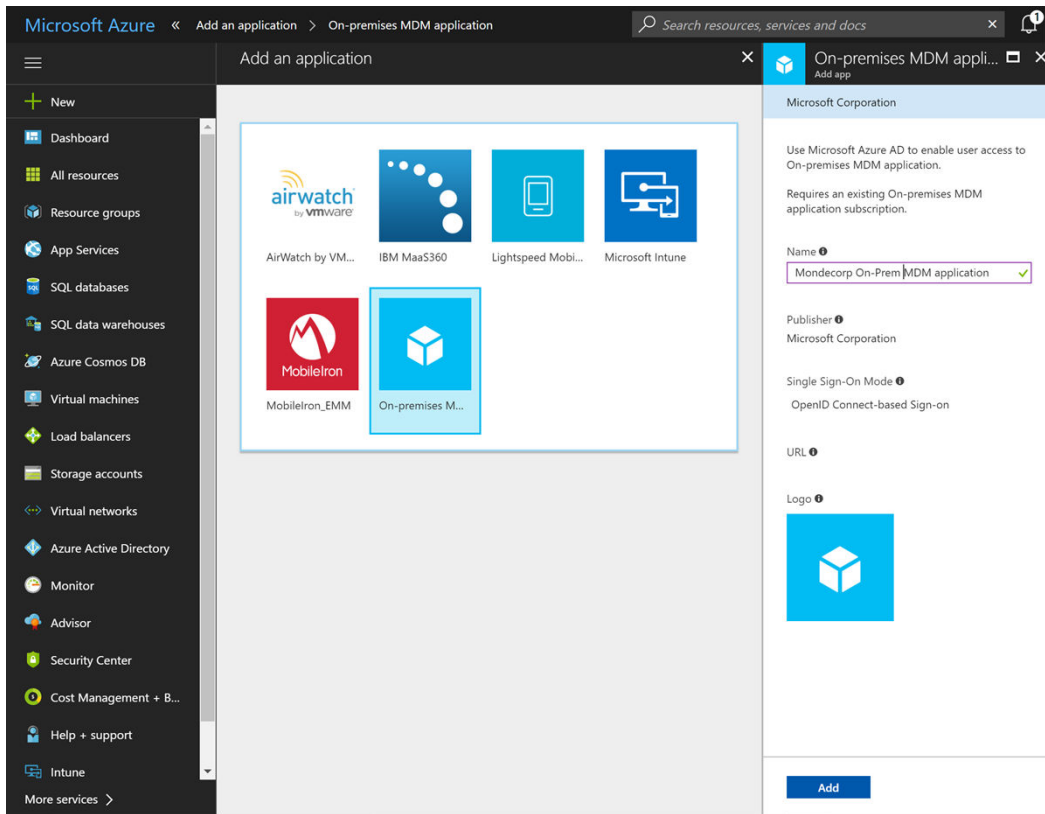
7   Select **Add Application** again and select the **On Premises MDM application**. You can rename the application when you add it.

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**.
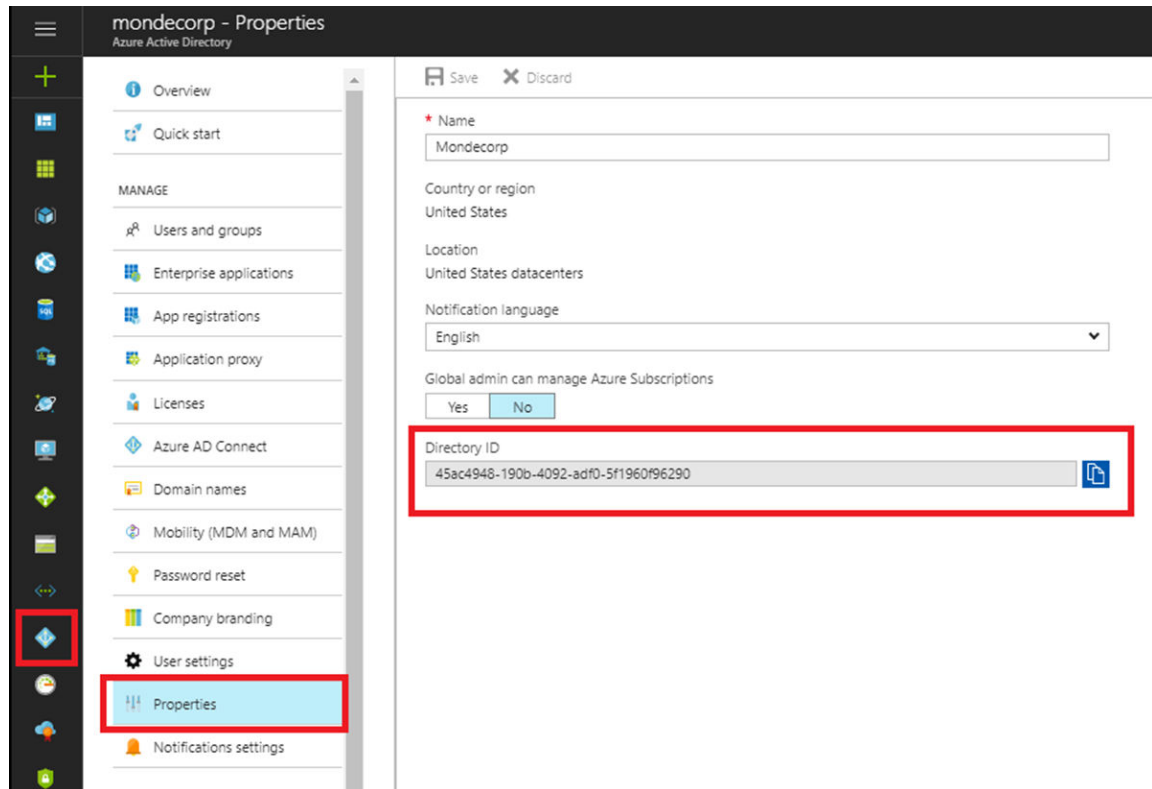


15  Select **User Account Details** in the top right corner. The Azure **Tenant Name** is the name of your Azure Directory. You can find the name under the **Domain** tab.

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 VMwareWorkspace ONE UEM management tool.

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

**Procedure**

**1**  Create an Azure sdmin account for 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.

a  In Azure, navigate to your Azure Active Directory.

b  Select **Users and groups** and **+ New user**.

c  Configure the **Directory role** as **Global administrator**.

d  Create a temporary password so you can log in to the Microsoft Store for Business.

**2**  Activate 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.

a  Navigate to the Microsoft Store for Business and log in with your Azure admin account.

b  Navigate to **Manage > Settings > Distribute > Management tools** and activate the Workspace ONE UEM by VMware tool.

c  For offline licenses, go to **Manage > Settings > Shop > Shopping experience** and enable **Show offline licensed apps to people shopping in the store**.

d  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.

**Procedure**

**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 Workspace ONE 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.

**What to do next**

Follow the import by deploying applications outlined in Deploy Microsoft Store for Business Apps.

## 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 Flexible Deployment to Assign Applications.

**Procedure**

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.<br><br>If devices are part of your Azure Active Directory system and your deployment has online licenses available, devices receive the application.<br><br>If you assign both online and offline licenses to the group, the system gives preference to online licenses. |
| **Assignment - Offline Licenses** | Assign groups to the application with offline licenses.<br><br>If your deployment has offline licenses available, devices receive the application.<br><br>If you assign both online and offline licenses to the group, the system gives preference to online licenses. |

| Setting | Description |
|---|---|
| **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. |
| **Deployment - 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**.

## Methods to Reclaim Licenses for Microsoft Store for Business Apps

Sync offline and online licenses with the details view of the application to view the corresponding users of the licenses. Choose a way to delete the assignment of the application off devices to reclaim and reassign 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.

## Table 4-5. Methods to Reclaim Licenses

| Method | Description |
| --- | --- |
| Details View | Select the **Delete Application** function in the details view of the application.<br>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.<br>This action impacts all assets and devices in the organization group. |
| Assignment Group | Delete the smart or user group assigned to the application.<br>This action impacts every device in the group. |
| User | Delete the applicable user account from the console. |

# Purchased Applications -Volume Purchase Program (VPP)

<div style="text-align: right">5</div>

To distribute public applications and custom business to business (B2B) applications to large deployments of Apple iOS and macOS devices, integrate Workspace ONE UEM with Apple Business Manager.

For information on the Device Enrollment Program (DEP) and the Volume Purchase Program (VPP), see *Integration with Apple Business Manager*.

# SaaS Applications in Workspace ONE UEM

<span style="font-size:3em; color:#ccc;">6</span>

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 Workspace ONE 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.

## Control Access at the Time of Authentication

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

**Table 6-1. Access Control Options**

| 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. |

**Table 6-1. Access Control Options (continued)**

| 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 Workspace ONE 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.

For information about configuring SaaS applications, see Add SaaS Applications in the Workspace ONE UEM Console.

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.

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

This chapter includes the following topics:

- Requirements to Support SaaS Applications

- Methods to Add SaaS Applications

- Client Access Policy Description

- Assign SaaS Applications

- Provisioning Adapters

- Settings for SaaS Applications

- SSO Between Workspace ONE UEM and VMware Identity Manager for SaaS Apps and Access Policies

# Requirements to Support SaaS Applications

To access your SaaS applications managed in VMware Identity Manager in Workspace ONE UEM console, set up peripheral systems to communicate between the systems.

## Required Systems

Configure or integrate the listed systems so that you can access the SaaS applications page.

- 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.

- 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.

  **Note**   Mobile SSO is different from the SSO feature for applications that use the Workspace ONE 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.

## 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.

Table 6-2. Methods to Add SaaS Applications

| 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 |
| 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 Workspace ONE UEM |
| 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 Workspace ONE UEM |

# 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.

**Procedure**

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.<br>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.<br>SaaS applications use icons in PNG, JPG, and ICON file formats.<br>The application icons that you upload must be a minimum of 180 x 180 pixels.<br>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.<br>Configure categories in VMware Identity Manager so that they display in the category list. |

**3** Complete the options on the **Configuration** tab.

a 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.

Table 6-3. Authentication Settings for SAML 2.0 - URL/XML

| Setting | Description |
| --- | --- |
| Configuration | URL/XML is the default option for SaaS applications that are not yet part of the Workspace ONE catalog. |
| 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. |

Table 6-4. Authentication Settings for SAML 2.0 - Manual

| Setting | Description |
| --- | --- |
| Configuration | **Manual** is the default option for SaaS applications added from the catalog. |
| 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. |

### Table 6-4. Authentication Settings for SAML 2.0 - Manual (continued)

| Setting | Description |
|---------|-------------|
|  | 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** - The SAML 1.1 is an older SAML authentication profile. For better security, implement SAML 2.0.

| 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.<br>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.<br>Some service providers use the **Single Sign-On URL**. |

- **WSFed 1.2** - Select this option to provide single sign-on to applications that use WS-Federation authentication

| 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.<br>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.<br>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.<br>This value is a default profile text box value for a username at the application service provider. |

- **Web Application Link** - If the application does not use a federation protocol, select this option. Enter the target URL of the application.

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

- **OpenID Connect** - Select this option to provide single sign-on to applications that use the OAuth 2.0 protocol.

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

c  If you want greater control of messaging in single sign-on processes with Workspace ONE, add optional parameters in **Advanced Properties**. The authentication type determines the available settings on the user interface. There are several permutations. Go to the authentication type for your SaaS application.

Table 6-5. Advanced Properties - SAML 2.0

| Setting | Description |
|---|---|
| **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.<br>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.<br>Some service providers require this option. |
| **Signature Algorithm** | Select the signature algorithm that matches the digest algorithm.<br>If your service provider supports SHA256, select this algorithm. |
| **Digest Algorithm** | Select the digest algorithm that matches the signature algorithm.<br>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.<br>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. |
| **Open in VMware Browser**<br>Android and iOS | Require Workspace ONE to open the application in the VMware Browser.<br>If you use VMware Browser, opening SaaS applications within it adds extra security. This action keeps access within internal resources. |

## Table 6-6. Advanced Properties - SAML 1.1

| Setting | Description |
| --- | --- |
| 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<br>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. |

## Table 6-7. Advanced Properties - WSFed 1.2

| Setting | Description |
| --- | --- |
| 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. |
| Open in VMware Browser<br>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   Assign policies to secure signing in to application resources with **Access Policies**.

| 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. |

| Setting | Description |
| --- | --- |
| | Require approvals before the application installs and activates a license. <br> ■ **License Pricing** - Select the pricing model to buy licenses for the SaaS application. <br> ■ **License Type** - Select the user model for the licenses, named or concurrent users. <br> ■ **Cost Per License** - Enter the price per license. <br> ■ **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.

**What to do next**

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

## Copy SaaS Applications in Workspace ONE UEM

Create copies of SaaS applications and assign them to different users and groups. Using copies of applications is useful if your deployment has different business units that use the same application.

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

**Procedure**

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.

**What to do next**

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

## Export SaaS Applications From Workspace ONE UEM

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.

**Procedure**

**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.

**Procedure**

**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. |

| Setting | Description |
| --- | --- |
| **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.<br><br>Configure categories in VMware Identity Manager so that they display in the category list. |

3    Complete the options on the **Configuration** tab.

    a    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.<br><br>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.<br><br>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.<br><br>This value is a default profile text box value for a username at the application service provider. |

    b    Add values for **Application Parameters** to allow the application to start.

c   If you want greater control of messaging in single sign-on processes with Workspace ONE, add **Advanced Properties** for **WSFed 1.2**.

| Setting | Description |
| --- | --- |
| 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. |

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

| 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.

| | |
| --- | --- |
| 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. |
| **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.

**What to do next**

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

# 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. Users and groups are not the same as Workspace ONE UEM console smart groups and you configure them in VMware Identity Manager.

**Procedure**

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. <br> ■ **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.

# Configure 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.

**Procedure**

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.

3  Complete the text boxes in the **Configuration** tab. For more information, see Add SaaS Applications in the Workspace ONE UEM Console.

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.

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.

■  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.

■ 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.

## SAML Metadata and Self-Signed Certificates or Certificates from CAs

You can use the SAML certificates from the **Settings** page for authentication systems like mobile single sign-on.

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 Use SAML Metadata for Single Sign-On.

## 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 Third-Party Identity Providers as an Application Source.

## 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.

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.

■ For regular SaaS applications, see Add SaaS Applications in the Workspace ONE UEM Console.

**Procedure**

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.

## Use SAML Metadata for Single Sign-On

Retrieve SAML metadata and certificates from the **Settings** page for single sign-on capabilities with SaaS applications.

**Prerequisites**

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.

**Procedure**

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.<br>Select the links and open a browser instance with the XML data.<br>Configure your third-party identity provider with this information. |
| Signing Certificate | Copy the signing certificate that includes all the code in the text area.<br>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 - New Certificate | Description |
|---|---|
| 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.<br>RSA key sizes smaller than 2048 are considered insecure. |

| Setting - Replace a Certificate | Setting |
|---|---|
| Upload SSL Certificate | Upload the SSL certificate received from your third-party certificate authority. |
| Certificate Signing Request | Download the certificate signing request (CSR). Send the CSR to the third-party certificate authority. |

# Third-Party Identity Providers as an Application Source

Adding an identity provider as an application source streamlines the process of adding individual applications from that provider to the end-user catalog because you can apply configured settings and policies from the third-party application source to all applications managed by the application source.

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 Configure Application Source for the Third-Party Identity Providers.

## 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 .

## 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 .

## Configure 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.

**Procedure**

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**.

## Table 6-8. Configuration Settings - URL/XML

| Setting | Description |
| --- | --- |
| Configuration | **URL/XML** is the default option for SaaS applications that are not yet part of the Workspace ONE catalog. |
| URL/XML | Enter the URL if the XML metadata is accessible on the Internet.<br>Paste the XML in the text box if the XML metadata is not accessible on the Internet, but you have it.<br>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. |

## Table 6-9. Configuration Settings - Manual

| Setting | Description |
| --- | --- |
| Configuration | **Manual** is the default option for SaaS applications added from the catalog. |
| Single Sign-On URL | Enter the Assertion Consumer Service (ACS) URL.<br>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.<br>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.<br>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.<br>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.<br>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.<br><br>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.<br><br>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**.

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

## 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.

**Procedure**

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

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**.

**Procedure**

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 consoles use an authorization code work flow that allows access to the VMware Identity Manager console through the Workspace ONE UEM console and that allows admins 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 VMware Identity Manager.

## Register the OAuth Client During Setup

When you set up VMware Identity Manager in the Workspace ONE 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.
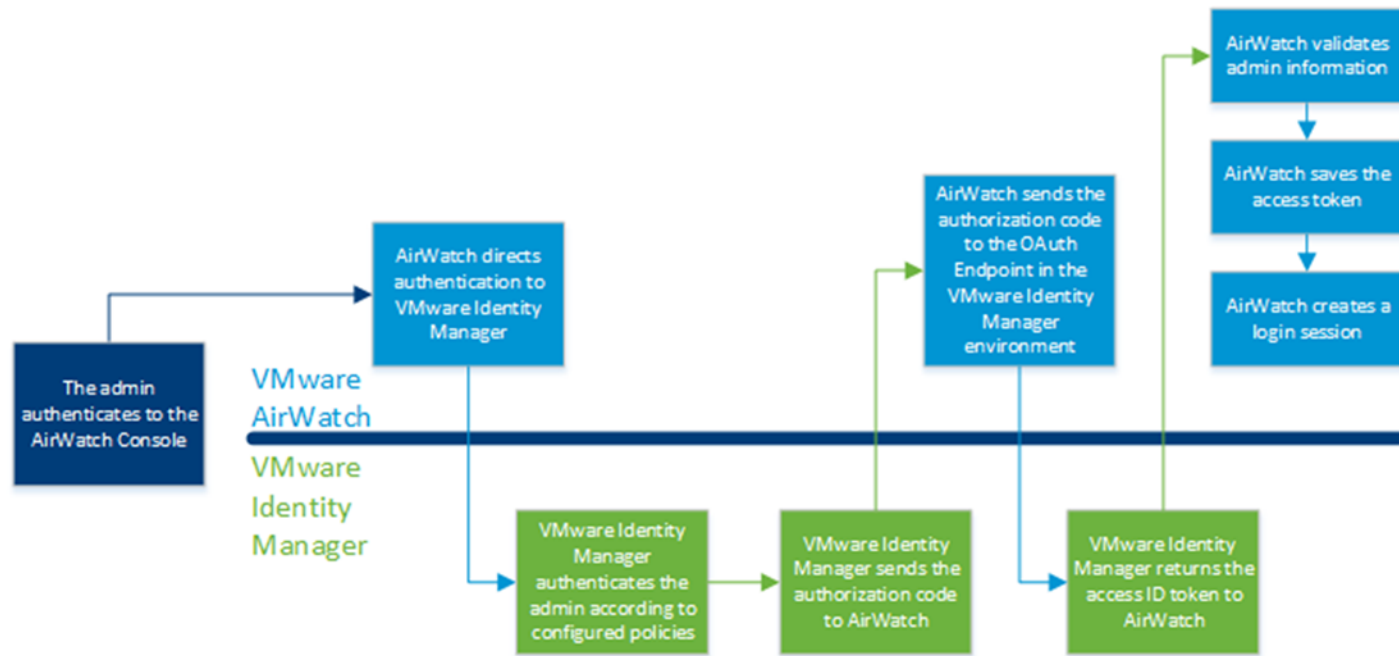
# Web Applications

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.

## 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.

## 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.

Use the View Devices page to manage your web applications. For the actions available on the View Devices page, see View Devices Assigned To, Install, and Delete Web Links Applications.

## Deployment Methods

There are two methods to deploy web applications. For an explanation of the two methods, see Web Links Tab or Device Profiles.

You can edit configurations in either system because the systems share settings. See Web Links in Apps & Books and Devices Share Settings 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 .

## Device Profile Method

For the configurations to add web applications by device profile, see the listed topics on the VMware Docs site https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/index.html.

- Android – *Configure Bookmarks (Android (Legacy) )*

- iOS – *Configure a Web Clips Profile (iOS)*

- macOS – *Configure a Web Clips Profile (macOS)*

- Windows Desktop – *Configure a Web Clips Profile (Windows Desktop)*

This chapter includes the following topics:

- Web Links Application Features and Supported Platforms

- Web Links Tab or Device Profiles

- Web Links in Apps & Books and Devices Share Settings

- Web Apps Admins and Roles Exceptions

- Add Web Links Applications

- View Devices Assigned To, Install, and Delete Web Links Applications

# Web Links Application Features and Supported Platforms

Web links applications function much like an application on a device, but they provide end users a way to access a URL directly from an icon on their devices. 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 Workspace ONE 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 Workspace ONE 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 fromWorkspace 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 Workspace ONE 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 in Apps & Books and Devices Share Settings

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 Workspace ONE UEM console.

Enable the following categories to give the Web App admin access to device profiles.

- **Device Management > Device DetailsProfiles > 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**.

**Procedure**

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.<br><br>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.<br><br>■ **On Demand** – Deploys content to a catalog or other deployment agent and lets the device user decide if and when to install the content.<br><br>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.<br><br>■ **Automatic** – Deploys content to a catalog or other deployment Hub on a device upon enrollment. After the device enrolls, the system prompts users to install the content on their devices.<br><br>This option is the best choice for content that is critical to your organization and its mobile users. |
| Advanced | Offers extra functionality depending on the platform.<br><br>■ **Android**<br><br>**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.<br><br>■ **Apple iOS**<br>　■ **Removable** – Allows end users to use the long press feature to remove this Web app off their devices.<br>　■ **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.

# View Devices Assigned To, Install, and Delete 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 for more information.

**Procedure**

**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.<br><br>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.<br><br>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. |

# Manage Applications

<div style="text-align: right;">**8**</div>

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 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 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 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 for configurations.

  - View user ratings and comments and delete user comments about applications on the User Ratings page. See Configure User Ratings 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 .

## Application Longevity Management

Application longevity depends on the application's status as active or inactive. See Active and Inactive Status 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 and Its Alternatives.

- 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 and the Relation to Its Active Versions 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 and Its Relation to Application Lifecycle Components 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 .

# 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 SaaS Applications Acces with Access Policies .

This chapter includes the following topics:

- SaaS Applications Acces with Access Policies
- Native List View Option Descriptions for Applications
- Details View Setting Descriptions
- Management of User-Installed Applications
- Configure Manage Devices
- Requirements to See the Manage Feedback Page
- Configure User Ratings
- Active and Inactive Status
- The Delete Action and Its Alternatives
- The Deactivate Option and the Relation to Its Active Versions
- The Retire Option and Its Relation to Application Lifecycle Components
- Internal App Versions
- Configure View Logs for Internal Applications
- Per-App VPN Associations and Native Applications

## SaaS Applications Acces with Access Policies

To provide secure access to 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 Chapter 6 SaaS Applications in Workspace ONE UEM .

# 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.

**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.

# Add Network Ranges for Access Policies

Define network ranges with IP addresses allowed for user logins 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. |

**What to do next**

Assign network ranges to application-specific access policies. For more information, see Configure Application-Specific Access Policies.

# Configure Application-Specific Access Policies

Add application-specific access policies to control user access to SaaS applications.

**Procedure**

**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. <br><br> Allowable name criteria includes the listed parameters. <br><br> ■ Begin with a letter, either lowercase or uppercase, from a-Z. <br> ■ Include other letters, either lowercase or uppercase, from a-Z. <br> ■ You can include dashes. <br> ■ 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. |

| Setting | Description |
|---|---|
| **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. |

| Setting - Advanced Properties | Description - Advanced Properties |
|---|---|
| **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. <br> ■ **Status** – View applications by status: Active, Retired, or Inactive. This view is helpful to return applications to previous statuses. <br> ■ **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. <br> ■ **Requires Renewal** – Find Apple iOS applications that use a provisioning profile to function. This filter locates applications with provisioning profiles you can update. <br> ■ **App Type** – View applications depending on type. Types include Public or Custom B2B options. |
| Add Application | Upload a local application, search for a public application in an app store, or add an order with redemption codes. |
| Export | **Export CSV**: Export all the items on all the pages to a CSV file. |

| Setting | Description |
|---------|-------------|
| | **Export PPKG**:Choose the applications from the list of supported applications, and select **Export**. The applications are exported to a Windows Provisioning Package (PPKG).When the PPKG export is complete, you receive a notification with a download link. You can only export one PPKG at a time. |
| | We currently support only Win32 application whose deployment is recognized via software distribution method. We do not support PPKG export for the following applications: |
| | ■ Win 32 Applications that are uploaded before enabling the software distribution |
| | ■ Win 32 Applications that are installed in the user context |
| | ■ Universal Windows Platform applications |
| 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. |
| Search List | Find applicable applications you want to locate by name. |
| 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 theWorkspace ONE UEM consoleby 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

The **Details View** of an application 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 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:<br>- **Images** – If you uploaded mobile images, tablet images, and icons with the application, displays them.<br>- **Terms of Use** – Displays the terms of use, if configured, that device users must view and accept before they can use the application.<br>- **SDK** – Displays information pertaining to the use of the VMware Workspace ONE 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.<br>- **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. |

| Setting | Description |
| --- | --- |
| 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.<br><br>■ **Retire** – Removes an application from all managed devices.<br><br>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.<br><br>■ **Deactivate** – Removes an application and all versions of it from all managed devices.<br><br>■ **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.<br><br>■ **User Ratings** – Accesses ratings of applications using the star system, which you can use to gauge the popularity of internal applications.<br><br>■ **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.<br><br>■ **Add Version** – Updates your internal application with a new version.<br><br>■ **Other Versions** – Shows previous versions of an internal application that were added to the Workspace ONE UEM console. |
| Delete Application | Remove the application from devices and from the Workspace ONE 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.<br><br>■ **Manage Feedback** – Control feedback for applications for Apple iOS. This option appears under specific conditions so review the topic for these conditions.<br><br>■ **View Analytics** – Exports the analytics for internal applications that use the VMware Workspace ONE SDK.<br><br>■ **View Logs** – Downloads or deletes log files for internal SDK and wrapped applications. |

# Management of User-Installed Applications

Workspace ONE UEM can assume management of user-installed applications (iOS and Windows) without requiring the deletion of the previously installed application.Workspace ONE UEM labels the feature **Make App MDM Managed if User Installed**.

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.

**Table 8-1. Management Depends on Enrollment Status**

| 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).

Use the **Status** filter to find devices that have installed or not installed assets. Use the **User Invite** filter to find devices to invite to the Apple VPP.

**Procedure**

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.<br><br>■ macOS<br><br>Workspace ONE UEM cannot remove VPP applications (purchased) for macOS devices.<br><br>■ Windows Desktop and Phone<br><br>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.<br><br>Settings include email, SMS, push, and message template options for sending messages. |
| **Reinvite**<br>**(Only Purchased)** | Send an invitation to join the Apple VPP, managed distribution, to devices.<br><br>Devices must run Apple iOS v7.0.3+.<br><br>The page also lists devices that accepted the invitation. |

# Requirements to See 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.

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.

- You must assign at least one Apple iOS 7+ device to the application.

- An assigned Apple iOS 7+ device must transmit to the UEM console that it contains feedback and data.

# Configure Manage Feedback

Use the **Manage Feedback** option to request, clear, and view feedback applications that run on Apple iOS 7+.

**Procedure**

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.

**Procedure**

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 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 yourWorkspace 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 and the Relation to Its Active Versions

Deactivating an application, removes it from devices and makes the version inactive. Depending on their relation to the inactive version, Workspace ONE UEM pushes or makes available active versions to devices. A benefit of deactivation 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 Workspace ONE 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 Workspace ONE UEM console.

# The Retire Option and Its 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 configuration 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 Workspace ONE 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.

**Table 8-2. Results for Setting Retire Previous Version**

| 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 Workspace ONE UEM console. |
| | 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 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 Workspace ONE 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 Workspace ONE UEM 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.

**Table 8-3. Examples of the Retire Action**

| 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.<br><br>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. |
| 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

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.

- 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 **Actual File Version** and the **Version**. Workspace ONE UEM displays them on the **Details** tab of the 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 Workspace ONE UEM console for management. When you upload an internal app version to the console, this number is identified as Latest Version, New Version, and Previous Version.

  - **Latest Version** - This identifier is usually the highest numbered version and it gets deployed to devices that enroll in the assigned group.

  - **Previous Version** - This identifier is usually a lower version than the current version.

  - **Current Version** - This identifier is the version you are uploading to the console. You can upload numbers lower than the latest version and higher than the previous version.

## Sourcing the Actual File Version Value

Workspace ONE UEM gets the application version that displays in the actual file version field 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.

**Table 8-4. Location of File Version Value by Platform**

| Platform | Parameter | Found In |
| --- | --- | --- |
| Android | `versionName` displays in actual file version<br>but<br>`versionCode` controls the ability to version | .apk package |
| iOS<br>macOS | `CFBundleVersion`<br>or<br>`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 |

## Actual File Version and Incrementation

You can upload multiple versions of an application no matter the actual file version number, but for most platforms, the actual file version controls the application's deployment. Workspace ONE UEM manages the new version depending on its actual file version value.

Table 8-5. Actual File Version Incrementation Behaviors

| Platform | Actual File Version |
|---|---|
| Android | `versionCode` must increment up because downgrading versions is not supported.<br><br>Workspace ONE UEM can accept applications with lower `versionCode` values. However, it manages the assignments based on the order of the actual file version.<br><br>For example, if you have deployed an actual file version 3.1 of an application, you have an older actual file version 1.1 still in the console, and you upload actual file version 2.1, Workspace ONE UEMmanages the versions with these behaviors.<br><br>■ Migrates assignments from version 1.1 (previous version) to 2.1 (new version).<br>■ If devices have 2.1 and 3.1 assigned (and both are active), Workspace ONE UEM sends install commands for 3.1 (latest version) since that is the highest version that devices are eligible to receive.<br>■ When you select **Retire Previous Version** at the time of uploading 2.1, the console retires 1.1 (previous version) and not 3.1 (latest version). |
| iOS<br>macOS | `BundleVersion` or the `BuildShortVersionString` can increment up or down because downgrading versions is supported.<br><br>You can upload a lower version of the application and push it as the available version. |
| Windows Desktop | Actual file version="X.X.X", the first three decimals, must increment up because downgrading versions is not supported.<br><br>Workspace ONE UEM can accept applications with lower actual file version values. However, it manages the assignments based on the order of the actual file version.<br><br>■ Migrates assignments from the previous version to the new version (the one you are uploading).<br>■ If devices have the new version and the latest version assigned (and both are active), Workspace ONE UEM sends install commands for the latest file version since that is the highest version that devices are eligible to receive.<br>■ When you select **Retire Previous Version** at the time of uploading the new file version, the console retires the previous version and not the latest version. |
| Windows Phone | Version="X.X.X", the first three decimals, must increment up because downgrading versions is not supported.<br><br>Workspace ONE UEM can accept applications with lower actual file version values. However, it manages the assignments based on the order of the actual file version.<br><br>■ Migrates assignments from the previous version to the new version (the one you are uploading).<br>■ If devices have the new version and the latest version assigned (and both are active), Workspace ONE UEM sends install commands for the latest file version since that is the highest version that devices are eligible to receive.<br>■ When you select **Retire Previous Version** at the time of uploading the new file version, the console retires the previous version and not the latest version. |

# Multiple Versions of Internal Applications

Workspace ONE UEM can replace an internal application on devices but it does not deploy multiple versions to devices. You can have multiple, active versions in the console for management. Replacing a retired version depends on the **Actual File Version** value.

If you want multiple versions of an application in the Workspace ONE UEM console, do not select the **Retire Previous Version** check box on the **Details** tab. This check displays when you add a version of an application.

If you do not select **Retire Previous Version**, and you add an application version, Workspace ONE UEM assigns the higher **Actual File Version** to devices.

You can **Deactivate** application versions rather than retiring them to remove them from device assignments.

# 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.

# Manage Versions of Internal Applications

Control versions of internal applications with **Add Version** and **Retire Previous Versions**..

The actions menu offers an **Other Versions** option to view all the versions of an application in the Workspace ONE UEM console.

**Procedure**

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. The lower version is not available for deployment in the Workspace ONE UEM console. <br><br> 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 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 deployment in the Workspace ONE UEM console. |

5   Select **Save & Assign** to use the flexible deployment feature.

# Configure View Logs for Internal Applications

Use the View Logs feature to access available log files pertaining to applications that use the Workspace ONE SDK framework. Log types include all logs, crash logs, and application logs. With this feature, you can download or delete 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.

**Procedure**

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 Workspace ONE SDK or using the App Wrapping feature. |
| **Download Listed** | Download all logs in all pages with information pertaining to applications created with the Workspace ONE SDK or using the app wrapping feature. |
| **Delete Selected** | Delete selected logs with information about applications created with the Workspace ONE SDK or using the App Wrapping feature. |
| **Delete Listed** | Delete all logs in all pages with information about applications created with the Workspace ONE SDK or using the App Wrapping feature. |

## SDK Log Types

Workspace ONE UEM displays logs for applications that report application failures and that report application-specific data. These logs integrate with the VMware Workspace ONE 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 Workspace ONE UEM console without the need for extra code in the SDK application. |

## VMware Workspace ONE 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 Workspace ONE UEM console.

**Table 8-6. SDK Logging Level Descriptions**

| 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. |

# Per-App VPN Associations and Native Applications

Workspace ONE UEM has several options for editing or removing the per-app VPN profile assigned to native applications.

Changes to resources can require a change or the removal of VPN tunnels used to access applications. For example, when users move to different departments in an orrnganization, their access to resources can change. In instances where you need to change or remove the VPN tunnel access for an application, you have several options.

**Table 8-7. Edit Per-App VPN Profile Actions and Their Results**

| Action | Result |
|---|---|
| Edit the per-app VPN profile associated in the application's flexible deployment assignment. | The system associates the changed per-app VPN profile to the application and applicable groups receive the application depending on the assignment settings and priorities. |
| Change the priority of the flexible deployment assignment. | The system pushes the assignment and its configurations, including the per-app VPN profile, depending on the priority. If the assignment is at the top, the devices in the applicable groups receive the profile first. |
| Deselect the per-app VPN profile in the flexible deployment assignment of the application. | The system unassigns the per-app VPN profile from the groups assigned to the application. |
| Change a device's smart group and the device receives applications entitled to the new group. | Flexible deployment assignments are assigned by smart groups. The **App Tunneling** and **Per-App VPN** settings are part of the flexible deployment assignment configurations. Move a device to a smart group that you know has the desired application and per-app VPN, and this action changes the profile for the device. |

# Edit the Per-App VPN Profile of an Internal Application

Change the app tunnel VPN profile on approved apps to use a different app tunnel to connect to backend and corporate networks.

This is a general example of how to edit the per-app VPN profile of an internal application. For public and purchased applications, follow a similar workflow by editing the flexible deployment assignment for that specific application.

**Procedure**

1    Navigate to **Apps & Books > Native > Internal** in the Workspace ONE UEM console.

2    Select the radio button for the application and select **Assign**.

3    Select the assignment and choose **Edit**.

4    In the menu in the setting below **App Tunneling**, select a different per-app VPN profile.

5    Select **Add** and then **Save And Publish**.

The system associates the changed per-app VPN profile to the application and applicable groups receive the application depending on the assignment settings and priorities.

# Edit a Per-App VPN by Changing the Assignment Priority

Move the flexible deployment priority up or down to change the app tunnel approved applications use to connect to backend and corporate networks.

This task works for applications that have more than one flexible deployment assignment configured. If you want information on flexible deployment priorities, see Flexible Deployment Conflicts and Priorities.

**Procedure**

1    Access the flexible deployment assignments of a native application. Follow the substeps to access the assignments for a public application. Internal and purchased applications follow a similar workflow.

   a    To access the assignments of a public application, navigate to **Apps & Books > Native > Public** in the Workspace ONE UEM console.

   b    Select the radio button for the application and select **Assign**.

2    Select the assignment you want to move and select to **Move Up** or **Move Down**. Make any priority changes needed.

3    Select to **Save And Publish**.

The system pushes the assignment and their configurations, including the per-app VPN profile, depending on the priority. If the assignment is at the top, the devices in the applicable groups receive the profile first.

# Remove the Per-App VPN Profile

Deselect the **App Tunnel** option in the flexible deployment assignment to dissassociate the per-app VPN profile from applications and devices.

**Procedure**

1   Access the flexible deployment assignments of a native application. Follow the substeps to access the assignments for a public application. Internal and purchased applications follow a similar workflow.

   a   To access the assignments of a public application, navigate to **Apps & Books > Native > Public** in the Workspace ONE UEM console.

   b   Select the radio button for the application and select **Assign**.

2   Select the assignment and choose **Edit**.

3   Select **Disabled** for **App Tunneling**.

4   Select **Add** and then **Save And Publish**.

The system unassigns the per-app VPN profile from the groups assigned to the application.

# Edit, Delete, and Unassign a Smart Group

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

For example, a smart group for executives is assigned to a compliance policy, device profile, and two internal apps. If you want to exclude some of the executives, then simply edit the smart group by specifying **Exclusions**. This action removes not only the two internal apps but also the compliance policy and device profile from those excluded devices.

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

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

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

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

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

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

## Delete a Smart Group

When you have no further use for a smart group, you can delete it. You can only delete one smart group at a time. Selecting more than one smart group causes the **Delete** button to be unavailable. If a smart group is assigned, you are not permitted to delete it.

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

2   Select the check box to the left of the smart group name and select **Delete** from the actions menu that displays.

## Unassign a Smart Group

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

1   Unassign smart groups from applications, books, compliance policies, device profiles, or product provisions. Follow the navigation paths shown.

- **Applications** – Navigate to **Apps & Books > Applications > List View** and select the **Public**, or **Internal** tab.

- **Books** – Navigate to **Apps & Books > Books > List View** and select the **Public**, **Internal**, or **Web** tab.

- **Channels** – Navigate to **Content > Video > Channels**.

- **Compliance Policy** – Navigate to **Devices > Compliance Policies > List View**.

- **Device Profile** – Navigate to **Devices > Profiles & Resources > Profiles**.

- **Product Provision** – Navigate to **Devices > Provisioning > Products > List View**.

2   Locate the content or setting from the listing and select the **Edit** icon  from the actions menu.

3   Select the **Assignment** tab or locate the **Assigned Smart Groups** text box.

4   Select Delete (**X**) next to the smart group that you want to unassign. This action does not delete the smart group. It simply removes the smart group assignment from the saved setting.

5   Follow the required steps to **Save** your changes.

# Application Groups and Compliance

<span style="float:right; font-size:3em;">9</span>

Use application groups (app groups) and compliance policies to protect resources in your Workspace ONE UEM environment.

## 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 .

## 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.

- 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. For more information on the AirWatch Catalog, see Chapter 11 VMware AirWatch Catalog.

- 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 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 Chapter 10 Compliance for Application Management.

For information about adding compliance policies that work with app groups, see Build an Application Compliance Policy.

This chapter includes the following topics:

- Application Groups and Compliance Policies Work Together

- Configure an Application Group

- Edit App Groups and the Application Control Profile

- Create Required Lists for the AirWatch Catalog

- Enable Custom MDM Applications for Application Groups

# Application Groups and Compliance Policies Work Together

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.

Table 9-1. App Groups and Compliance Policies by Platform

| 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.

**Table 9-2. Relationships Between Application Groups and Compliance Policies**

| Application Group | Description | Compliance Policy | Action |
|---|---|---|---|
| Whitelisted | Managed devices can install these applications from the AirWatch Catalog.<br><br>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.<br><br>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.<br><br>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. |

**Note**   An application that is set for auto deployment mode in the UEM console does not automatically deploy under the following conditions:

- Adding the application to the Blacklist app group that assigned to the device.

- Excluding the application in the Whitelist app group that is assigned to the device.

# 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.

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.

**Procedure**

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.<br><br>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. |

| Setting | Description |
|---|---|
| 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.

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, edit the app group first, then the application profile.

**Procedure**

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 application notifications to app catalogs you require devices to install.

**Procedure**

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 UEM to recognize custom MDM applications so you can assign them to special app groups to gather information, troubleshoot, and track assets.

Workspace ONE UEM supports custom MDM applications made for the Android and Apple iOS platforms. Upload them as internal applications.

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.

**Procedure**

1   Navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment**.

2   Select **Customization**.

3   Enable **Use Custom MDM Applications**.

# Compliance for Application Management

<div align="right">

# 10

</div>

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

This chapter includes the following topics:

- Build an Application Compliance Policy

# 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.

**Procedure**

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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.

# 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 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.

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.

For an explanation of the options available for the AirWatch Catalog and for the Workspace ONE catalog, see Workspace ONE and AirWatch Catalog Settings.

## 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 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 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 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.

# 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 for more details.

This chapter includes the following topics:

- Workspace ONE and AirWatch Catalog Settings

- Prerequisites to Migrate Catalogs

- Migrate VMware AirWatch Catalog to Workspace ONE Catalog

- AirWatch Catalog Features and Deployment Methods

- Standalone Catalog for MAM Only Deployments

# 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 andWorkspace 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 Workspace ONE 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.

Table 11-1. Common Catalog Settings

| Setting | Description | More Information |
| --- | --- | --- |
| Application Categories | Group applications and identify their uses with custom application categories. | Configure Application Categories |
| 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 |
| App Restrictions | Restrict iOS devices older than iOS 9 by restricting installations of only assigned applications approved by the organization. | Restricted Mode for Free Public iOS Applications Older Than iOS 9 |

**Table 11-1. Common Catalog Settings (continued)**

| Setting | Description | More Information |
|---|---|---|
| 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 |
| Application Removal Protection | Configure threshold values to control the dispatch of application removal commands for critical internal applications. | Configure Application Removal Protection |

**Table 11-2. AirWatch Catalog Specific Settings**

| 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 |
| **AirWatch Catalog > Feature Applications** | Display featured applications in a prominent place in the AirWatch Catalog. | Configure Featured Applications |
| **AirWatch Catalog > General** | Configure general settings for the AirWatch Catalog. | Deploy the AirWatch Catalog With Groups & Settings Options |

## 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.

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.

## Prerequisites to Migrate Catalogs

To migrate users from the AirWatch Catalog to the Workspace ONE catalog, ensure theat Workspace ONE UEM and VMware Identity Manager are connected. Also, add key value pairs for the catalogs and configure SSO.

**Procedure**

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    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.

3    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

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.

**Prerequisites**

For a better user experience, see Prerequisites to Migrate Catalogs.

**Procedure**

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.

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.

# 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.

**Procedure**

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.<br>■ **Never - Keep User Signed In** – Keeps users signed in and does not require them to log in each time.<br>■ **After XX day(s)** – Require users to authenticate (log in) after a set number of days.<br>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.

| Settings | 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. |
| **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.

| Settings | Description |
|---|---|
| Branding Logo | Upload a logo to brand the app catalog for your organization.<br>■ This logo overrides any logo you set in **Groups & Settings > All Settings > System > Branding**.<br>■ If you do not upload a logo for the app catalog, Workspace ONE UEM uses the logo from your **System > Branding** settings.<br>■ 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.

**Procedure**

**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.

   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. TheWorkspace 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.

**Procedure**

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.

## 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.

## Table 11-3. Installed Application Behaviors from the 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 Workspace ONE Intelligent Hub. | 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. |

**Table 11-3. Installed Application Behaviors from the AirWatch Catalog (continued)**

| Application Type | Apple iOS Supervised Device | Apple iOS Unsupervised Device | Android Enterprise Device | Android Standard Device | Android for Work | Windows Desktop Device | macOS |
|---|---|---|---|---|---|---|---|
| **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. |
| **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 Workspace ONE 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.

Table 11-4. Installed Application Behaviors from the Standalone Catalog

| 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 theWorkspace ONE 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.

## Table 11-5. Messages in the 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 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 Workspace ONE Intelligent Hub 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. |
| **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. |

**Table 11-5. Messages in the AirWatch Catalog (continued)**

| Application Type | Apple iOS Supervised Device | Apple iOS Unsupervised Device | Android Enterprise Device | Android Standard Device | Android For Work | Windows Desktop Device | macOS Device |
|---|---|---|---|---|---|---|---|
| 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. |
| 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 Workspace ONE 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.

Table 11-6. Messages in the Standalone Catalog

| 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 the , 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 Workspace ONE 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.

## Basics of the Standalone Catalog

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. See Standalone Catalog Functionality for more information.

Read Enable the Standalone Catalog for instructions to enable the standalone catalog without requiring users to enroll in full MDM.

See Steps to Deploy a Standalone Catalog for an outline of how to configure the standalone catalog.

## The Standalone Catalog and the SDK

For applications created using the Workspace ONE SDK to communicate and work with the standalone catalog, the device user must activate the application within the catalog. See Set SDK Communication With the Standalone Catalog for more information.

## Regular AirWatch Catalog

For information on the regular AirWatch Catalog, see Chapter 11 VMware AirWatch Catalog.

## 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 Workspace ONE Intelligent Hub.

- 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 Workspace ONE 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.

**Procedure**

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.

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 Workspace ONE Intelligent Hub is required. Instead, end users can access just MAM applications assigned to an App-Catalog-Only-Organization-Group through the standalone catalog.

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.

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.

**Procedure**

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. |
| **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**.

## Set SDK Communication With the Standalone Catalog

For applications created using the Workspace ONE SDK to communicate and work with the standalone catalog, the device user must activate the application within the catalog.

**Procedure**

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.

# 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.

View a matrix that outlines what applications and platforms support open and managed access in Supported Platforms for Open and Managed Access.

For instructions on how to add public applications for the deployment through Workspace ONE, see Add Public Applications from an App Store.

For more information about configuring managed access options for internal applications, see Add Assignments and Exclusions to Applications.

## 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.

This chapter includes the following topics:

- Workspace ONE UEM Applications and the Workspace ONE Managed Access Feature

- Supported Platforms for Open and Managed Access

- View the Installation Status of Windows 10 Applications in the Workspace ONE Catalog

# 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).<br><br>The application is available to devices already managed by Workspace ONE UEM.<br><br>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.<br>■ Require app tunneling when applications access the intranet.<br>■ Enable single sign-on for applications.<br>■ Track user adoption and installation statuses for applications.<br>■ Deploy the application automatically upon enrollment. |
| **Open Access** Device users access resources without granting admins permissions on their devices.<br><br>The application is available to devices no matter their managed status. | ■ Provide application access to end-users immediately upon login, without elevated security permissions.<br>■ 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.<br>■ 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, open or managed, for applications based on the platform.

**Table 12-1. Open and Managed Access Support - Internal Applications**

| Platform | Managed Access | Open Access |
| --- | --- | --- |
| Android | Supported | Supported |
| iOS | Supported | Supported |

**Table 12-1. Open and Managed Access Support - Internal Applications (continued)**

| Platform | Managed Access | Open Access |
|---|---|---|
| Windows Desktop | Supported | Not Supported |
| Windows Phone | Supported | Not Supported |
| macOS | Supported | Not Supported |

**Table 12-2. Open and Managed Access Support - Public Applications**

| Platform | Managed Access | Open Access |
|---|---|---|
| Android | Supported | Supported |
| iOS | Supported | Supported |
| Windows Desktop | Not Supported | Supported |
| Windows Phone | Not Supported | Supported |

# 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. This feature let's users know when installation of these large applications is complete and ready for use.

## 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.

**Table 12-3. View Application Installation Status Support for Windows 10**

| Platform | Application Type | File Formats |
|---|---|---|
| Windows Desktop<br>Windows Phone | Internal | XAP<br>APPX<br>Win32 (EXE, MSI, ZIP) |
| Windows Desktop<br>Windows Phone | Public | XAP<br>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.

Other components on devices include the following list.

- 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.