Application Lifecycle Management

VMware Workspace ONE UEM 2111

vmware

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

https://docs.vmware.com/

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

Copyright © 2022 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

Mobile Application Management

1

Workspace ONE UEM powered by AirWatch offers Mobile Application Management™ (MAM) functionality that helps you manage mobile applications, deploy them to the devices, and secure the applications with the compliance policies. Mobile Application Management solution is a management console that takes the control of selected applications on the end-user mobile device.

Mobile Application Management solution in general include a runtime library that can be integrated with a mobile application at the build time. The library might be packaged as a software development kit (SDK), for example. Integration of the library is not mandatory for all applications in the scope of the solution. Mobile Application Management (MAM) requires enrollment as a first step, also called onboarding. Enrollment is the establishment of a connection with the enterprise's management console. Depending on the solution, the connection is either between the device and the management console, or between the application and the management console, or both.

Some common enrollment mechanisms are as follows:

- Pre-enrollment, also known as out of box, in which the mobile device has been allocated to the enterprise at some point in the device's manufacture or packaging.
- Entry of enrollment credentials in a user interface that is part of the operating system.
- Entry of enrollment credentials in a dedicated Mobile Application Management solution endpoint application, sometimes called an agent or device administrator.
- Entry of enrollment credentials in an enterprise application that has integrated the SDK of the Mobile Application Management solution. The application can be an email client, for example.
- Facilitated enrollment by delegation to an application on the device that has already been enrolled using another mechanism.

This chapter includes the following topics:

Application Types and Platforms supported by Workspace ONE UEM

Workspace ONE UEM supports various app types and deployment scenarios on your devices. Workspace ONE UEM classifies the applications as native (internal, public, purchased) and Web applications. The information in this section describes the types of apps that you can deploy using Workspace ONE UEM and the various platforms or the operating systems that Workspace ONE UEM supports for each of the application types.

The following table provides the app type and the platforms supportability.

Application Type	Supported Platforms
Industry TemplatesAny Supported App Type	Apple iOS v7.0+ with limitations for compliance policies
Internal	Android v4.0+Apple iOS v7.0+Apple macOS v10.9+Apple tvOS v10.2+Windows Desktop**Note**: Ensure that the auxiliary files packaged with Apple iOS or macOS applications do not have spaces in the names. Spaces can cause issues when you load the application to the console.
Public (Free and Paid)	Android v4.0+Apple iOS v7.0+Chrome OSWindows Desktop**Note**: Workspace ONE UEM can manage free, public applications on Windows 10+ devices when you integrate with the Microsoft Store for Business.
Purchased – Custom Apps	Apple iOS v7.0+
Purchased – VPP	Apple iOS v7.0+Apple macOS v10.9+
Web Links	Android v4.0+Apple iOS v7.0+Apple macOS v10.9+Windows Desktop

Different types of Applications - Internal / Public / Purchased / Web

Depending on the type and mode of deployment, Workspace ONE UEM classifies applications as Internal, Public, Purchased, and Web apps. Internal apps are internally developed apps and uploaded directly to the Workspace ONE UEM console or can also be imported from an external app repository. Public apps are available on respective app stores of the platforms that are, App Store, Play Store, Windows Store and so on. Purchased apps are categorized as VPP (Volume Purchased Program) and Custom B2B apps. VPP allows businesses and educational institutions to purchase publicly available iOS applications. However, custom B2B apps are developed third party iOS applications in volume for distribution to corporate devices. Web apps provide end-users a way to access a URL directly from an icon on the menu of their device.

Platform/Type	Internal	Public	Web	Purchased
iOS	X	X	X	X
Android	X	X	X	

Platform/Type	Internal	Public	Web	Purchased
macOS	X		X	X
Windows Desktop	X	X	X	

Managed App configuration (AppConfig) in the form of key/value pairs

AppConfig is an initiative to standardize app development for easy configuration, security, and connectivity. By leveraging this standard, organizations can push managed app configuration (AppConfigp) in the form of key/value pairs or XML from EMM providers like Workspace ONE directly to their apps. Developers must program their applications appropriately to leverage this functionality. 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.

The application vendor sets the supported configurations for the application. 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.

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 Workspace ONE Managed App Configuration for Multiple Platforms.

Deploy Internal Applications on your Devices

2

You can use Workspace ONE UEM to distribute, track, and manage your internal applications. These are applications built in-house and not hosted on Public App Stores. You can upload the application files directly to Workspace ONE UEM console for deployment. However, if you use an external repository to host your internal applications, then you can easily integrate that host with Workspace ONE UEM, instead of migrating the entire catalog to Workspace ONE UEM

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.

This chapter includes the following topics:

Supported File Types for Internal Applications

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.

Platform	File Type
Android	APK. For more information, see Deploying Internal Application on Android Devices.
Apple iOS	IPA
macOS	DMGMPKGPKG**Note**: You can also use the product provisioning feature to deploy macOS internal applications as DMG, PKG, and APP files.
tvOS	IPA

Platform	File Type
Windows Desktop	APPX: 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.
Windows Phone	APPX: Upload a single APPX file, which can be x86, x64, or ARM.XAP

Internal Application Versions

Use **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. You can push beta versions for testing purposes, allow Apple iOS devices to 'roll back' to a previous version. and also 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. However, EXE, ZIP files can be some of the exceptions since the UEM console cannot interpret the package. If you add a different version of the application as if it were new, the system displays the **Retire Previous Version**s check box on the **Details** tab.

When adding a new version of an application, you can see the following in the **Details** tab:

- **Uploaded UEM Version** – This identifier is the UEM version you are uploading into the console.
- **Assignments Copied From** – This identifier is the version immediately preceding the uploaded version, from which the uploaded version inherits assignments.
- **Latest version** – This identifier is the highest numbered version in the console and it gets deployed to devices that enroll in the assigned group.

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.

Sourcing the App Version Value

Workspace ONE UEM gets the application version that displays in the AppVersion field from various places depending on the platform. You cannot upload duplicate versions of an app.

Platform	Parameter	Found In
Android	versionName displays App Version but versionCode controls the ability to version	.apk package
iOSmacOS	CFBundleVersionCFBuildShortVersionString	info.plist
Windows Desktop	Version="X.X.X.X"	AppManifest.xml
Windows Phone	Version="X.X.X.X"	WMAppManifest.xml

App Version and Incrementation

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

Platform	App Version
Android	versionCode must increment up because downgrading versions is not supported.Workspace ONE UEM can accept applications with lower versionCode values. However, it manages the assignments based on the order of the App Version.For example, if you have deployed an App Version 3.1 of an application, you have an older App Version 1.1 still in the console, and you upload App Version 2.1, Workspace ONE UEM manages the versions with these behaviors:Migrates assignments from version 1.1 (Assignments copied From) to 2.1 (Uploaded UEM Version).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.When you select Retire the Previous Version at the time of uploading 2.1, the console retires 1.1 (Assignments copied From) and not 3.1 (latest version).
iOS and macOS	BundleVersion or the BuildShortVersionString can increment up or down because downgrading versions is supported.**Note**: macOS does not support downgrading to a lower version of an app.You can upload a lower version of the application and push it as the available version.
Windows Desktop	App Version="X.X.X", the first three decimals, must increment up because downgrading versions is not supported.Workspace ONE UEM can accept applications with lower App Version values. However, it manages the assignments based on the order of the App Version and migrates assignments from the previous version to the Uploaded UEM Version (the one you are uploading).If devices have the Uploaded UEM 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.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.X", the first four decimals, must increment up because downgrading versions is not supported.Workspace ONE UEM can accept applications with lower App Version values. However, it manages the assignments based on the order of the App Version and migrates assignments from the previous version to the Uploaded UEM Version (the one you are uploading).If devices have the Uploaded UEM 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.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

You can 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.

Manage Version Control of Your Internal Application

The version control allows you to manage changes to files over time. Workspace ONE UEM uses two different version values to manage version control of internal applications. The App Version number is the coded version set by the developer of the application. The UEM Version number of the application set by the Workspace ONE UEM console. It is derived from the App Version number and is used to determine the order of all versions in the console so that assignments can be properly inherited.

Maintain Multiple Versions of Your Internal Application

You can control versions of internal applications with **Add Version** and **Retire Previous Versions**. 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 **App Version** value. If you want multiple versions of an application in the 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 **App Version** to devices. You can **Deactivate** application versions rather than retiring them to remove them from device assignments.

Complete the following steps to manage multiple versions of internal application in the Workspace ONE UEM console:

1 Navigate to **Resources** > **Apps** > **Native** and select the **Internal** tab.

2 Click the application, and go to **Detail** view and select **Add Version**.

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 App Version and assigns the higher App Version to devices. 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 App Version assigned through retiring previous versions in the Workspace ONE UEM console.
Disable Retire Previous Version	Workspace ONE UEM unassigns the lower App Version and assigns the higher App Version to devices. If it is still Active, the lower version is available for deployment in the Workspace ONE UEM console.

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

Roll Back Versions Using Retire and Deactivate

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 App 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.

Protect Production Version of your Proprietary Application

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. You can 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.

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. You can add and remove the test version by following a specific task order. Consider the following best practices when you remove the test versions from the console:

- Whenever possible, test applications in a separate environment with a testing instance of theWorkspace ONE UEM console.
- Workspace ONE UEM always uses the application ID to identify the test version of the proprietary application. When you use the application removal command, 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.

Deploy Internal Applications as a Local File

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

Maximum Allowed File Size

If your workspace ONE UEM environment has CDN enabled, you can upload apps of up to 10 GB. Without CDN, you can upload apps that are 200 MB, maximum. All SaaS environments are setup with CDN by default.

If you should need more than this amount for an app, contact your VMware Global Services representative.

How To Upload Your Local File

Complete the following steps to upload an internal application to the Workspace ONE UEM console, as a local file.

1 Navigate to **Resources** > **Apps** > **Native** > **Internal** and select **Add Application**.

2 Select **Upload** > **Local File** and browse for the application file on the system.

3 Click **Save**.

4 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.
Application ID	Represents the application with a unique string. This option is pre-populated and was created with the application.Workspace ONE UEM uses the string to identify the application in systems for applications that are on allowed and denied lists.
App Version	Displays the coded version of the application set by the application's developer.
Build Version	Displays an alternate "File Version" for some applications.This entry ensures Workspace ONE UEM records all version numbers coded for applications because developers have two places within some applications they can code a version number.
UEM 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.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.

Details Setting	Details Description
Is App Restricted to Silent Install-Android	Assigns this application to those Android devices that support the Android silent installation feature. The end user does not have to confirm installation activity when you enable this option. This feature makes it easier to uninstall many applications simultaneously.Only Android devices in the smart group that supports the silent uninstallation benefit from this option. These Android devices are also called Android enterprise devices.
Default Scheme	Indicates the URL scheme for supported applications. The application is packaged with the scheme, so Workspace ONE UEM parses the scheme and displays the value in this field.A default scheme offers many integration features for your internal applications, including but not limited to the following options:Use the scheme to integrate with other platform and web applications.Use the scheme to receive messages from other applications and to initiate specific requests.Use the scheme to launch Apple iOS applications in the AirWatch Container.
Description	Describe the purpose of the application.Do not use '<' + String in the Description, as you might encounter an Invalid HTML content error.
Keywords	Enter words that might describe features or uses for the application. These entries are like tags and are specific to your organization.
URL	Enter the URL from where you can download the application and get information about it.
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 system uses to install the MSI application.
Timeout	Enter the time, in minutes, that the installer waits with no indication of installation completion before it identifies an installation failure.When the system reaches the timeout number, it stops monitoring the installation operation.
Retry count	Enter the number of attempts the installer tries to install the application before it identifies the process as failed.
Retry interval	Enter the time, in minutes, the installer waits between installation attempts.The maximum interval the installer waits is 10 minutes.

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.

5 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	Firebase Cloud Messaging (FCM) Token	This is a Workspace ONE SDK feature and does not apply to all Android applications.Some internal, Android applications support push notifications from the application to device users.Select **Yes** for the Application Supports Push Notification option and enter the Server API key in the FCM 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.

Platform	Auxiliary File	Description
Apple iOS	Provisioning ProfileAPNs files for development or production	By default, your application package contains the provisioning profile. However, for internal Apple iOS applications, you might have to provide a provisioning profile so that the internal application works when it is managed in Workspace ONE UEM if your application package does not contain the provisioning profile or if your provisioning profile has expired. You can obtain this file from your Apple iOS application developers.A provisioning profile authorizes developers and devices to create and run Apple iOS applications. See Apple iOS Provisioning Profiles for information about Workspace ONE UEM 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 your application supports Apple Push Notifications Services (APNs), you can enable this file for messaging functionality. Apple Push Notification service (APNs) is the centerpiece of the remote notifications feature that lets you push small amounts of data to devices on which your app is installed, even when your app isn't running. To make use of Apple Push Notifications Services (APNs), 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.
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.

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

Setting	Description
Mobile Images	Upload or drag images of the application to display in the app catalog for mobile devices.
Tablet Images	Upload or drag images of the application to display for tablets.
Icon	Upload or drag 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.

7 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.

8 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 Workspace ONE UEM communicate securely.

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

You cannot wrap an application that you previously saved in the Workspace ONE UEM console. You have two options:

- Delete the unwrapped version of the application, upload it to Workspace ONE UEM, 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 Workspace ONE UEM 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.Workspace ONE UEM 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.

10 Select **Save & Assign** to configure flexible deployment options for the application.

Deploy Internal Applications as a Link

Workspace ONE UEM console allows you to deploy 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. You can one use of the following delivery configurations to deploy applications as a link to end users.

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.

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 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.

Note: Windows app deployments currently require you to select **Download & Distribute via WS1 UEM server** when you deploy them as a Link.

Host application on internal network repository via Content Gateway

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.

Workspace ONE UEM. powered by AirWatch provides VMware Content Gateway as a service on the Unified Access Gateway appliance. The VMware Content Gateway provides a secure and effective medium for end users to access internal repositories.You can configure the the Content Gateway for Windows to transfer data from the on-premises network to Workspace ONE UEM.

Note: Adding application package link to an internal repository to access via Content Gateway is no longer supported. For more information, see End of General Support for VMware Content Gateway on Windows and Linux. We recommend that you host and distribute apps either from cloud storage or Workspace ONE UEM.

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 soWorkspace 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.

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

Deploy applications via Enterprise App Repository

Enterprise App Repository within Workspace ONE UEM speeds the delivery of frequently used Windows apps. Enterprise App Repository serves as a one-stop-shop for commonly used, pre-packaged apps that they can instantly deploy to employees Intelligent Hub catalog. The apps are pre-tested across the latest OS builds and kept up-to-date for protection against potential vulnerabilities. If you use the Content Gateway for Windows and house applications on an external server system, you can set external repositories for various platforms and application types. Workspace ONE UEM supports specific file types for external app repositories. The external app repository feature supports only internal applications.

Application link must contain any of the following supported file extensions 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:

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.

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.

Add Internal Applications From External Repositories

Configure Workspace ONE UEM to direct users to internal applications on your network in an external app repository. Manage setttings in Workspace ONE UEM to distribute a link to a resource or to retrieve a file package and store and distribute it. The Content Gateway for Windows uses this information to access the repository and to open communications between the device and the repository.

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

2 Complete the following options.

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

3 Click **Save**.

4 Navigate to **Resources** > **Apps** > **Native** > **Internal** and select **Add Application**.

5 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.

6 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. For example, http:// / <InternalAppFileName.FileExtension.

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

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**.

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

Protect your devices from the App Removal Commands Initiated by the UEM console

Internal applications are often developed to perform enterprise-specific tasks. Abrupt removal of these applications can cause frustration and halt work. You can prevent the removal of important internal applications, by using the application removal protection. Application Removal Protection ensures that the system does not remove business-critical applications unless approved by the admin and holds the app removal commands based on the threshold values.

You can either use the default values or enter the limits that trigger the system to hold application removal commands. These actions stops the system from removing associated internal applications from devices. Until an admin acts on the held app removal commands, the system does not remove internal applications. In general, threshold values apply to bundle IDs and apply at a customer type organization group, and is inherited by the child organization groups. When setting threshold values and acting on them, consider these characteristics so that you can take informed actions on applications and have the permissions they need to act on the app removal commands. Because 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.

Note: Admins cannot override threshold values in the child organization groups. Admins' placement in the organization group hierarchy controls their available roles and actions. Admins in child organization groups can act on the removal commands in their assigned organization groups. Admins in parent organization groups can edit the values and act on removal commands in the parent group and in the child organization groups.

Application 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. For example, application removal commands trigger when you edit your smart groups, publish applications, deactivate, or retire applications, delete applications and so on. Complete the following steps to configure application removal protection in an organization group at the customer level or below in the Workspace ONE UEM console.

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

2 Enter the following threshold settings:

Setting	Description
Devices Affected	Enter the maximum number of devices that can lose a critical application before the loss hinders the work of the enterprise.
Within (minutes)	Enter the maximum number 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 the 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.

3 **Save** the settings.

Review App Removal log to act on the held App Removal Commands

You can use the **App Removal Log** page to continue to hold application removal commands, dismiss commands, or release the commands to devices. The command status in the console displays the application removal log that represents a phase of the protection process until an admin acts on the held commands, the system does not remove internal applications.

Complete the following steps to review the App Removal log to act on the held App Removal Commands:

1 Navigate to **Resources** > **Apps** > **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**.

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

3 You can 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 select 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 select it, the system can remove the application when the device checks-in with the system.

Access Log files for Applications that use the Workspace ONE SDK framework

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. Log types include all logs, crash logs, and application logs. 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. The SDK-built application collects logs over time and stores them locally on the device until another API or command is invoked to transmit the 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 applications that use the SDK framework.

1 Navigate to **Resources** > **Apps** > **Native** and select the **Internal** tab.

2 Select the application and then select **More** > **View** > **Logs** option from the actions menu.

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.

Note: When an enterprise wipe occurs, the console does not purge the log files. You can retrieve logs after a device re-enrolls to determine what issues occurred in the last enrollment session to cause the enterprise wipe.

Level	Logging API	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.

Level	Logging API	Description
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.

3 You can 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 that use the Workspace ONE SDK framework.
Download Listed	Download all logs in all pages with information pertaining to applications that use the Workspace ONE SDK framework.
Delete Selected	Delete selected logs with information about applications that use the Workspace ONE SDK framework.
Delete Listed	Delete all logs in all pages with information about applications that use the Workspace ONE SDK framework.

Deploy Public Applications on your Devices

3

You can use Workspace ONE UEM to manage the deployment and maintenance of publicly available mobile applications from various app stores. These apps are available on respective app stores of the platforms that is App Store, Play Store, Windows Store and so on.Deploying public apps from the different app stores differs slightly between platforms.

This chapter includes the following topics:

Add Public Applications from an App Store

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

1 Navigate to **Resources** > **Apps** > **Native** > **Public** and select **Add Application**.

2 View the organization group from which the application uploads in **Managed By**.

3 Select the **Platform**.

4 Find the application in an app store by entering a search keyword in the **Name** text box.

5 Select from where the system gets the application, either Search App Store or Enter URL.

Setting	Description
Search App Store	iOS – Searches for the application in the app store.Windows Desktop and Phone – Searches for the application. If you acquire applications this way and not with the Microsoft Store for Business. The system does not manage them.Android: Uses the Google Play Store iFrame search experience and looks for the application in the Play Store. The iFrame allows Google Play to be embedded directly into the Workspace ONE UEM console for a unified mobility management experience**Note**: VMware Workspace ONE UEM announced End of General Support for the Play Store Integration Service on December 15th, 2018. Existing customers who utilize the Play Store Integration Service to search and add public Android apps to the Workspace ONE UEM console are encouraged to set up Android to use the official Play Store search experience. For more information, see End of General Support for the Play Store Integration Service in the https://my.workspaceone.com/ portal.
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.

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.

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

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.

Migrate Your User Group Exceptions 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.

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

1 Navigate to **Resources** > **Apps** > **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.

Deploy Web Applications on your Devices

4

Web applications are useful for navigating to complex URLs with many characters. You can place Web application icons on the springboard to minimize the frustration with accessing these websites. 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 or complex URL. 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 Workspace ONE UEM system. Web links are applications configured solely in the Workspace ONE UEM console. 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.

This chapter includes the following topics:

Web Links Application Features and Supported Platforms

Web links applications are useful for navigation to extended URLs with many characters. Web Links are also known as shortcuts. They require manual user approval to add the short-cut to the homescreen. 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.Web Links use a custom URI to open specific browsers and is managed as a profile.

You can add web links applications using two methods.

- As an application in the **Resources** section of the Workspace ONE UEM console.
- As a device profile in the Devices section of the Workspace ONE UEM console.

The Workspace ONE UEM console supports the Android, Apple iOS, macOS and Windows Desktop platforms to push and manage web links applications. 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.

Configure Web Application Admin Roles and 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 Links** tab of **Resources**. If you want to create such an admin, navigate to **Accounts** > **Administrators** > **Roles** > **Add Role** > **Resources** > **Web Links** in the Workspace ONE UEM console. The permissions for a Web App admin include many of the tasks carried out by the general admin.

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 Details** > **Profiles** > **Device Install Profile**
- **Device Management** > **Device Details** > **Profiles** > **Device Remove Profile**

You can add web links applications on the **Web Links** 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 Links is in the Resources 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.

You can notice a few diffrences between single web links applications created in **Resources** and single web links applications created using device profiles share configurations.

- All MAM functions are available in both areas of the console (**Resources** and **Devices**).
- A single web clip (or bookmark) payload that is the only payload in a profile added in **Devices** displays in the **Resources** 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 **Resources** 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.

Add Web Links Applications from the Workspace ONE UEM console

Add URLs for sites you want to manage and push to devices as web links applications with the Web Links tab in **Apps & Books**.

1 Navigate to **Resources** > **Apps** > **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.

Settings	Descriptions
Name	Name of the web links app to be displayed in the Workspace ONE UEM console, on the device, and in the AirWatch Catalog.
URL	The address of the Web app.
Descriptions	A brief description of the Web app that indicates its purpose.This option is not displayed in the AirWatch Catalog.
Managed By	The organization group with administrative access to the Web app.

4 Upload a custom icon using a GIF, JPG, or PNG format, for the application on the **Images** tab that end users view in the AirWatch Catalog before installing the application to their devices and that displays as the icon of the Web app on the device.Images are currently not available for Windows Desktop. For best results, provide a square image no larger than 400x400 pixels and less than 1 MB when uncompressed. The graphic is automatically scaled and cropped to fit. If necessary, the system converts it to PNG format. Web Clip icons are 104 x 104 pixels for devices with a Retina display or 57 x 57 pixels for all other devices.

5 Complete the settings on the **Assignment** tab.

Setting	Description
Assigned Groups	The smart group to which you want the Web app added. Includes an option to create a new smart group which can be configured with specifications for minimum OS, device models, ownership categories, organization groups and more.
Exclusions	If Yes is selected, a new option displays called Excluded Smart Groups. This setting enables you to select the smart groups you want to exclude from the assignment of this Web app.

Setting	Description
Push Mode	Select how the system pushes Web apps to devices.**On-Demand** – Deploys content to a catalog or other deployment agent and lets the device user decide if and when to install the content. This option is the best choice for content that is not critical to the organization. Allowing users to download the content when they want helps conserve bandwidth and limits unnecessary traffic.**Automatic** – Deploys content to a catalog or other deployment Hub on a device upon enrollment. After the device enrolls, the system prompts users to install the content on their devices.This option is the best choice for content that is critical to your organization and its mobile users.
Advanced	Offers extra functionality depending on the platform.For Android: **Add to Homescreen** – Adds the web links application to the home screen 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.For Apple iOS**Removable** – Allows end-users to use the long-press feature to remove this Web app from their devices.**Full Screen** – Opens the Web app in full-screen mode on iOS 6+ devices.

6 Select **Save & Publish** to push the web links application to the AirWatch Catalog.

Install and Delete your 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.

1 Navigate to **Resources** > **Apps** > **Web Links**.

2 Find the web links application you want to work with and select the linked numbers in the **Install Status** column.

3 Use the column data and the actions menu to access the listed functions.

Setting	Description
Friendly Name	Navigates to the Details View of the selected device.Use the Devices Details View to edit device information, view compliance policies, view assigned device profiles, view assigned users, and many more MDM features pertaining to the device.
C/E/S User	Navigates to the Details View of the user of the selected device.Use the User Details View to edit user information, view event logs, view assigned User Groups and view other assigned devices.
Install Profile	Installs a web links application and its corresponding device profile to a listed device.
Delete Profile	Deletes a web links application and its corresponding device profile from a device.

Volume Purchase Program (VPP) Application Management

5

To distribute public applications and custom applications to large deployments of Apple iOS and macOS devices, integrate Workspace ONE UEM with Apple Business Manager. Apple Business Manager is a portal for administrators to manage the Device Enrollment program (DEP), Volume Purchase Program (VPP), Apple IDs, and content distribution in their organizations. Apple Business Manager with Workspace ONE UEM powered by Workspace ONE UEM Mobile Device Management (MDM) solution makes it easy to enroll devices and deploy content. Apple Business Manager has consolidated the management features that you have been using through the DEP and VPP portals. Once your organization upgrades to Apple Business Manager from Apple Deployment programs, the DEP and VPP portals will no longer be used to manage devices, assignments, apps purchases, or manage content.

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

This chapter includes the following topics:

Volume Purchase Program (VPP)

To distribute App Store applications and custom applications to Apple iOS and macOS devices, utilize Volume Purchase Program by integrating Apple Business Manager and Workspace ONE UEM.

The Apple Business Manager enables organizations to purchase publicly available applications for distribution. Any paid application from the App Store is available for purchase, in volume, at the existing App Store price. Custom applications can be free or purchased at a price set by the developer.

See Apple's website for the availability by country and for other details.

Supported Content for Purchased Applications

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

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

OperatingSystem	Free PublicApps	Purchased PublicApps	FreeCustom Apps	PurchasedCustom Apps
Apple iOS 7.x – 8.x	MD & RC	MD & RC	MD & RC	MD & RC
Apple iOS 9+	MD, RC, & DB	MD, RC, & DB	MD & RC	MD & RC
macOS 10.9 – 10.10	MD	MD	X	X
macOS 10.11-10.15	MD & DB	MD & DB	X	X
macOS 11.0+	MD & DB	MD & DB	MD & DB	MD & DB

Add Assignments and Exclusions to your Applications

6

Adding assignments and exclusions lets 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. You can add a single assignment or multiple assignments to control your application deployment and prioritize the importance of the assignment by moving its place in the list up for most important or down for least important. Also, you can also exclude groups from receiving the assignment.

The flexible deployment feature resides in the **Assign** sections of the application area and offers advantages to the assigning process. You can also exclude groups from receiving the assignment from the **Exclusions** tab.

You can assign multiple deployments simultaneously and order assignment so that the right distribution criteria and app policies get applied to your devices.You can also customize distribution and app policies for one or more smart groups.

1 Navigate to **Resources** > **Apps** > **Native** > **Internal** or **Public**.

2 Upload an application and select **Save & Assign** or select the application and select **Assign** from the actions menu.

3 On the **Assignments** tab, select **Add Assignment** and complete the following options.

   a In the **Distribution** tab, enter the following information:

   Platform-specific configurations are listed separately.

Setting	Description
Name	Enter the assignment name.
Description	Enter the assignment description.
Assignment Groups	Enter a smart group name to select the groups of devices to receive the assignment.

Setting	Description
Deployment Begins On	Deployment Begins On is available only for internal applications.Set a day of the month and a time of day for the deployment to start.For successful deployment, consider traffic patterns of your network before you set a beginning date with bandwidth.
App Delivery Method	On-Demand – Deploys content to a catalog or other deployment agent and lets the device user decide if and when to install the content. This option is the best choice for content that is not critical to the organization. Allowing users to download the content when they want helps conserve the bandwidth and limits unnecessary traffic.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. This option is the best choice for content that is critical to your organization and its mobile users.

Platform-specific Setting

Platform	Setting	Description
macOS and Windows	Display in App Catalog	Select Show or Hide to display an internal or public application in the catalog.**Note**: The Show or Hide option is applicable only to the Workspace ONE Catalog and not legacy VMware AirWatch Catalog.Use this feature to hide applications in the app catalog you do not want users to access.
Windows	Application Transforms	This option is visible when your app has transform files associated. Select the transform file that must be used on the devices selected in the Distribution section. If the transform file selection is changed after the app is installed, the update does not get applied on the devices. Only the newly added devices which do not have the app installed receives the updated transform.

b In the **Restrictions** tab, enter the following information:

Platform	Setting	Description
Android and iOS	EMM Managed Access	Enable adaptive management to set Workspace ONE UEM to manage the device so that the device can access the application.Workspace ONE controls this feature and not AirWatch Catalog.Only the devices that are enrolled in EMM are allowed to install the app and receive app policies when you enable this setting.The setting only impacts Workspace ONE Intelligent Hub users, not the legacy AirWatch Catalog users.
iOS	Remove on Unenroll	Set the removal of the application from a device when the device unenrolls from Workspace ONE UEM.If you choose to activate this option, supervised devices are restricted from the silent app installation.If you choose to deactivate this option, provisioning profiles are not pushed 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.
iOS	Prevent Application Backup	Prevent backing up the application data to iCloud.

Platform	Setting	Description
iOS	Prevent Removal	If you enable this setting, the user is prevented from uninstalling the app. This is supported in iOS 14 and later.
iOS and Windows	Make App MDM Managed if User Installed	Assume management of applications previously installed by users on their iOS devices (supervised and unsupervised) and Windows Desktop. MDM management occurs automatically regardless of the application delivery method and requires privacy settings to allow the collection of personal applications. For unsupervised iOS devices, the apps get converted to MDM managed only upon the user's approval.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.

c In the **Tunnel** tab, enter the following information:

Platform	Setting	Description
Android	Android	Select the Per-App VPN Profile you like to use for the application and configure a VPN at the application level.
Android	Android Legacy	Select the Per-App VPN Profile you like to use for the application and configure a VPN at the application level.
iOS	Per-App VPN Profile	Select the Per-App VPN Profile you like to use for the application.
iOS	Other Attributes	App attributes provide device-specific details for apps to use. For example, when you want to set a list of domains that are associated to a distinct organization.

d In the **Application Configuration** tab, enter the following information:

Setting	Description
Android	Send application configurations to devices.
iOS	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.

Note: You might see additional configuration tabs while configuring productivity apps. For example, if you are configuring a Workspace ONE Notebook application, **Account Settings** and **App policies** are displayed. For more information, go to the productivity app documentation.

4 Select **Create**.

5 Select **Add Assignment** to add new app assignments for your application.

6 Configure flexible deployment settings for your application by editing the schedules and priority for your deployments. Options that are displayed on this window are platform-specific.

Setting	Description
Copy	From the ellipses-vertical, you can click copy if you choose to duplicate the assignment configurations.
Delete	From the ellipses-vertical, you can delete to remove the selected assignment from the application deployment.
Priority	You can modify the priority of the assignment you configured from the drop-down menu while placing the selected assignment in the list of assignments. Priority 0 is the most important assignment and takes precedence over all other deployments. Your devices receive all the restrictions distribution policies and the app configuration policies from the assignment group which has the highest priority.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.For example, if 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 assignment's priority rating. Device 01 does not receive the priority 1 assignment.
Assignment Name	View the assignment name.
Description	View the assignment description.
Smart Groups	View the assigned smart group.
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.
EMM Managed Access	View whether the application has adaptive management enabled.When you enable this setting, the end-user is allowed to access the applications using Workspace ONE SDK only when it is EMM managed. To avoid any disruption to the service, ensure to take over management if the 'user installed' flag is enabled.

7 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.

8 Select **Save & Publish**.

Flexible Batch Deployment Settings for your Internal Application

7

You can control the frequency at which Workspace ONE UEM checks for new flexible deployment assignments, the frequency at which Workspace ONE UEM releases batches of applications, size of batches of applications that Workspace ONE UEM compiles and deploys to devices, and bypass the batching process for internal applications.

This chapter includes the following topics:

Control the Frequency of your 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.

1 Navigate to **Groups & Settings** > **All Settings** > **Admin** > **Scheduler**.

2 Find **Scheduled Application Publish** and select edit.

3 Complete the options in the Recurrence Type section and save your settings.

Control the Frequency of Flexible Batch Deployment

You can control the frequency at which Workspace ONE UEM releases batches of applications.

1 Navigate to **Groups & Settings** > **All Settings** > **Admin** > **Scheduler**.

2 Find **Scheduled Application Batch Release** and select edit.

3 Complete the options in the Recurrence Type section and save your settings.

Control the Batch Size For your Flexible Deployment

You can 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.

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

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

Bypass the Batching for your Flexible Deployment

You can 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.

1 Navigate to **Resources** > **Applications** > **Native** > **Internal**, and select the application.

2 Select from the actions menu **More** > **Manage** > **Bypass Batching**.

Tracking and Monitoring your Application Deployment

8

You can track recent deployment of apps and profiles to your devices in Workspace ONE UEM by reviewing deployment historical data and the install status on devices. You can also monitor the app deployment progress and track the true state of the application as reported by the device.

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. 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.

This chapter includes the following topics:

View your Application Deployment Status in 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.

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.

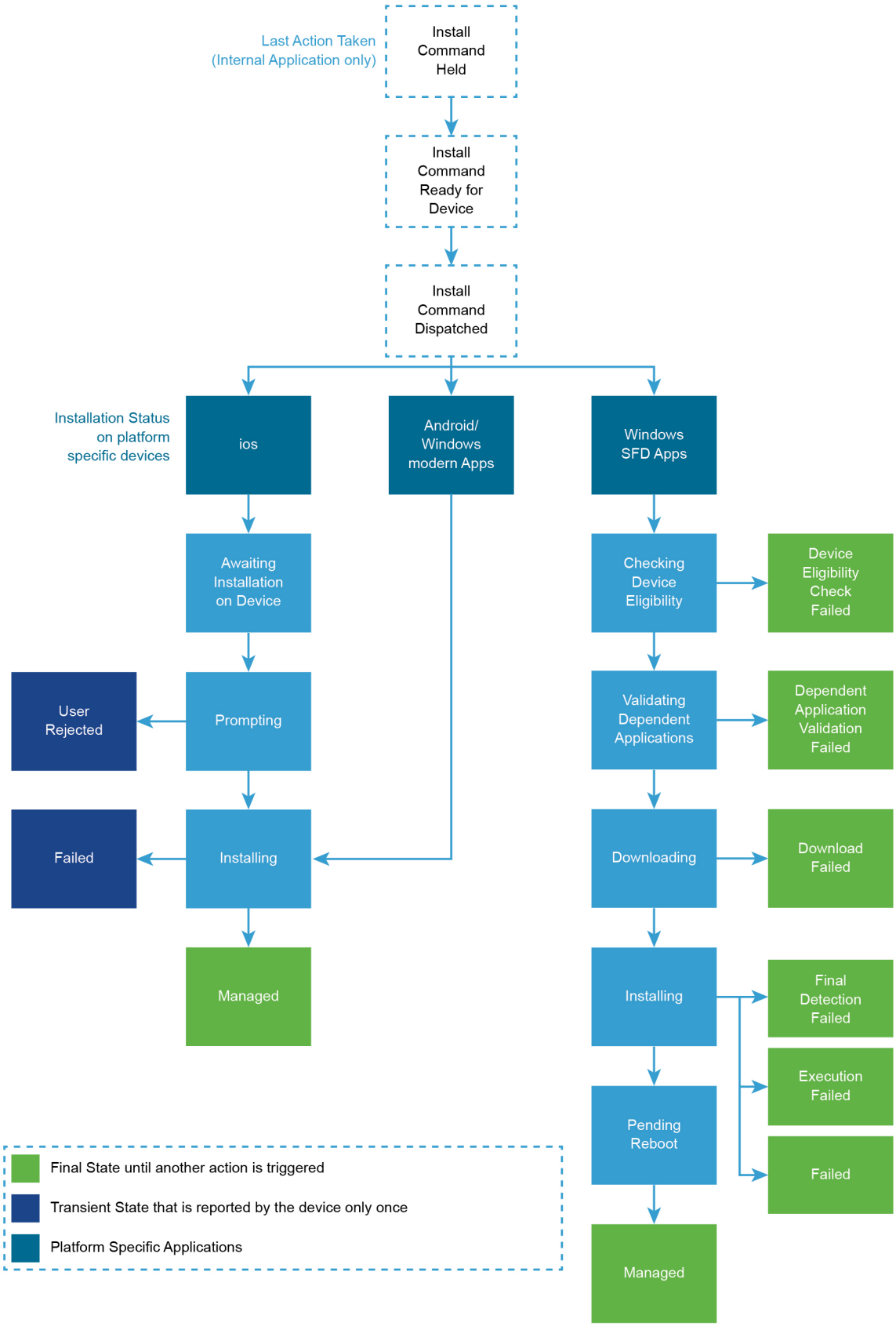
3 Select the app or profile from the drop-down menu and select **Add**. The App and Profile Monitor displays the current deployment status for devices during a deployment. The status combines different app and profile installation statuses into Done, Pending, or Incomplete.

Status	Description
Done	Devices report the Done status when the app or profile installs successfully.
Pending	Devices report the Pending Status when an app or profile reports the following statuses.**Profiles**Pending Install.Pending Removal.Unconfirmed Removal.Confirmed Removal.**Apps**Needs Redemption.Redeeming.Prompting.Installing.MDM Removal.MDM Removed.Unknown.Install Command Ready for Device.Awaiting Install on Device.Prompting for Login.Updating.Pending Release.Prompting for Management.Install Command Dispatched.Download in Progress.Command Acknowledged.
Incomplete	Device reports the Incomplete Status when an app or profile reports the following statuses.**Profiles**Pending Information.**Apps**User Removed.Install Rejected.Install Failed.License Not Available.Rejected.Management Rejected.Download Failed.Criteria Missing.Command Failed.If you see an Incomplete status, select the number next to the status to see a Device List View of all devices reporting the status. This feature lets you examine devices with issues so you can troubleshoot your deployment.

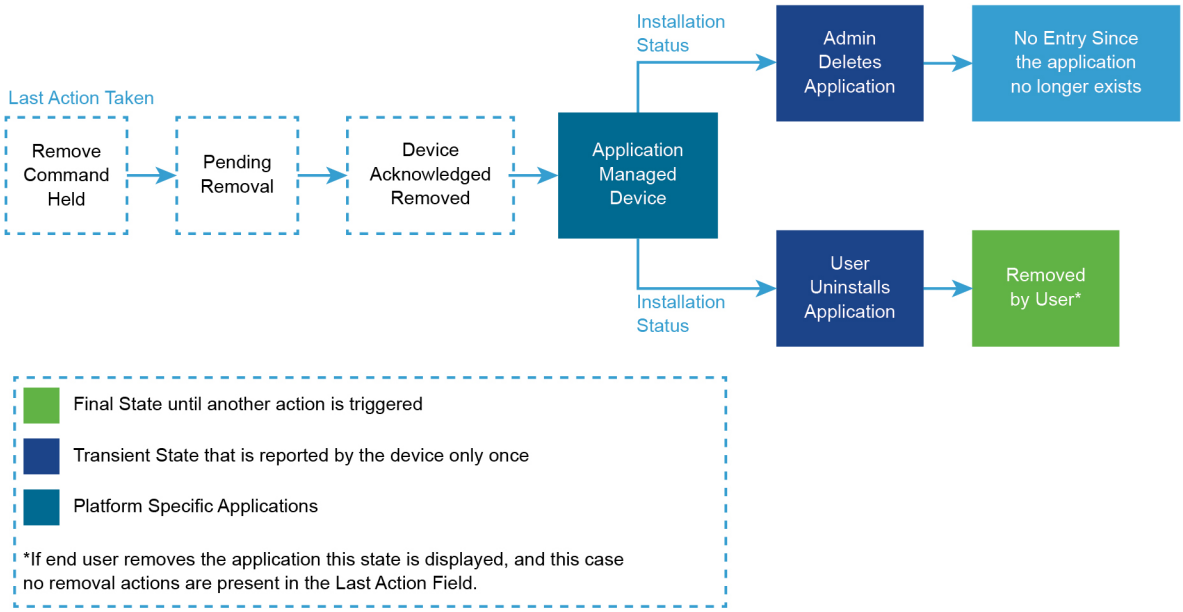
Application Status Tracking Workflow

Workspace ONE UEM displays information on the Last Action Taken by the system and the Installation Status of the applications on each of your end user's devices that helps you determine the deployment process.

The following workflow indicates the application installation status:


Last Action Taken
(Internal Application only)
Install Command Held
Install Command Ready for Device
Install Command Dispatched
Installation Status on platform specific devices
ios
Android/ Windows modern Apps
Windows SFD Apps
Awaiting Installation on Device
Prompting
User Rejected
Failed
Installing
Managed
Checking Device Eligibility
Device Eligibility Check Failed
Validating Dependent Applications
Dependent Application Validation Failed
Downloading
Download Failed
Installing
Final Detection Failed
Execution Failed
Failed
Pending Reboot
Managed
Final State until another action is triggered
Transient State that is reported by the device only once
Platform Specific Applications

The following workflow indicates the application removal status:



Monitor Application Deployment Progress From the Device Details Page

The application deployment information in the **Device Details** page provides information to the administrators about the applications that they want to deploy to their end-user devices through Workspace ONE UEM console. The deployment progress provides information about the apps that are entitled to a particular user's device and user's personal apps (depending on the privacy policy). The information can be useful for troubleshooting the application status on the individual device.

Complete the following steps to track the application deployment progress from the **Device Details** page.

The application deployment information in the **Device Details** page provides information to the administrators about the applications that they want to deploy to their end-user devices through Workspace ONE UEM console. The deployment progress provides information about the apps that are entitled to a particular user's device and user's personal apps (depending on the privacy policy). The information can be useful for troubleshooting the application status on the individual device.

Complete the following steps to track the application deployment progress from the **Device Details** page.

Monitor your Individual Application Version

You can track individual application versions from the **Summary** and **Devices** tabs of the the **Details View** to audit application deployments and perform management functions. For all the internal Applications, you can view a summary of a particular application version deployment progress and take actions on the subset of devices. To improve accuracy, Workspace ONE UEM provides different dimensions to the information and allow bulk actions. Public Applications summary metrics for the store applications that are deployed to your end-user devices and the devices list associated with a particular VPP application can be used for reporting and taking bulk actions.

Complete the following steps to track the deployment of individual application versions:

1 Navigate to **Resources** > **Apps**.

2 Select the Application Type.

3 Search for and select the desired application.

4 Select the **Summary** tab and review the application information.

Analytic	Data Snapshot
Filter by Smart Group	You can use the filed to view the summary of the devices that belong to a particular smart group.For example, if an application is deployed to all your end-user devices and you like to get an understanding of how the deployment is progressing for your 'APAC' region, you can select APAC Smart Group from the Filter by Smart Group drop-down.
Assignment and Install Details	The view provides a clear picture of all the devices that have the assignment for the particular version.**Installed** – Lists the number of devices that have installed the application.**Not Installed** – Lists the number of devices that have not installed the application.
Deployment Progress	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.**Assigned To** – Lists the smart groups assigned to the application's Flexible Deployment.**Status** – Reports Workspace ONE UEM's release of the installation command to devices.**Deployment** – Displays the application's Push Mode, Auto, or On Demand.
Installs without assignments	For the ease of access and to drive actions, displays all the devices that have a particular version of an application installed but do not have a valid assignment from Workspace ONE UEMconsole. Can list the devices that were previously assigned to this version of the application or the ones that side-loaded the application.

Analytic	Data Snapshot
Last Action Details	Displays the actions that were last taken by Workspace ONE UEMconsole on the particular version.
Peer Distribution Details	Displays the number of devices that have downloaded the application using peer distribution, the amount of data downloaded, and the source of the downloaded data.You can get access to the following information in the Peer Distribution Details section:1. Total number of devices that have the application installed.2. Total number of devices that have the Peer Distribution Profile installed and the percentage against the total number of devices.3. Pie chart of devices with Peer Distribution enabled displaying the percentage of devices that used peers to download the application against the percentage of devices that did not use peers.4. Total bytes that are saved by using Peer Distribution.5. Percentage showing the total bytes that are saved by downloading content from peers against total bytes that is downloaded with Peer Distribution enabled from either the server or the peers.6. Total bytes downloaded by all devices from either the CDN or Device Services server.7. Total bytes downloaded by all devices from their peers.

5 Select the **Devices** tab of the particular application version for reporting and taking bulk actions.

Analytic	Data Snapshot
App Sample Last Seen	Indicates when the device last reported the application information.
App Status	Indicates if the particular version of the application is installed or not-installed on the end-user devices.
Assigned Configuration	Links you to the Assigned configuration that your devices would receive based on the priority that is set.
Assignment Status	Indicates whether a particular device has a valid assignment from Workspace ONE UEM console or if it has been explicitly excluded from the assignment.
Last Action Taken	For scenarios where the actions are not successful, it is important for you to know what actions were last taken by the Workspace ONE UEM console on the particular version to narrow down the failure that occurred on the devices. You can point to the action to see the time when the action was taken.**Note**: All the actions taken by the Workspace ONE UEM console on a specific version of the application for a device can be found under this column.
Installation Status	Displays information about the latest installation event reported by the devices.
Device	Gives more information about the device.

Analytic	Data Snapshot
User	Gives more information about the user.
Peer Distribution	Displays one of the Peer Distribution Status:**On/Utilized**: Displays the list of devices that have the Peer Distribution Profile installed and have used peers in obtaining the application.**On/Not Utilized**: Displays the list of devices that have the Peer Distribution Profile installed and did not use peers in obtaining the application.**Off**: Displays the list of devices that have the Peer Distribution Profile installed, but is turned off.When you point to the Peer Distribution Status, you can get the following details:1. Download the source that indicates the Origin Source (CDN/Device Services) of the application.2. Cache Enabled (True/False) that indicates the BranchCache service status on the device.3. Current Client Mode (Disabled/Distributed/Hosted/Local) that indicates the Peer Distribution Mode that is set in the profile.4. Hosted Cache Server List (hosted server names) that indicates the list of hosted servers set in the profile when the Current Client Mode is 'Hosted'.5.Cache Bytes indicates the bytes that are downloaded from the peers or the hosted server.6. Server Bytes indicates the bytes that are downloaded from the CDN/Directory Services server.

6 Additionally, from the **Devices** tab you can use the following management functions.

Note: You can filter the devices by certain criteria and take actions on all the filtered devices.

Setting	Description
Send Message	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.
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.

Monitor all the versions of your Internal Application

You can get the summary of different versions of an internal application that is managed at a particular OG are bundled together. You can click on the bundle name to view the summary and details of the devices that are entitled to various versions. You may also choose to view the assignments across multiple active versions of an application from the **App Details** view. The summary can be beneficial if you maintain multiple active versions of your application that is assigned to different groups. The view provides a granular installation state of the application on various assigned devices and also provides information on devices that have the application installed by sideloading or previously assigned.

Complete the following steps if you wish to track the application deployment of all the versions of an application.

1 Navigate to **Resources** > **Apps** > **Internal**.

2 Search for and select all the versions of the desired application.

3 Select the **Summary** tab and review the application information.

Analytic	Data Snapshot
Filter by Smart Group	You can use the filed to view the summary of the devices that belong to a particular smart group.For example, if an application is deployed to all your end-user devices and you like to get an understanding of how the deployment is progressing for your 'APAC' region, you can select APAC Smart Group from the Filter by Smart Group drop-down.
Assignment and Install Details	Displays installation details of devices that have the application assigned from Workspace ONE UEM. The view provides a clear picture of all the devices that have an assignment for each active version managed at the current OG.**Installed** – Lists the number of devices that have installed the application.**Not Installed** – Lists the number of devices that have not installed the application.
Installs without assignments	For the ease of access and to drive actions, all the devices that have a particular version of an application installed but do not have a valid assignment from Workspace ONE UEMconsole are displayed in this chart.
Installation Status Details	This is a representation of the data reported by devices that includes the detailed information about the installation state of this application and is not tied to a particular version.**Note**:The final state for is field is Managed.

4 Select the **Devices** tab for reporting and taking bulk actions.

Analytic	Data Snapshot
App Sample Last Seen	Indicates when the device last that the device reported application information.
App Status	Indicates if the application is installed or not-installed on end-user devices
Assigned Configuration	Links you to the Assigned configuration that your devices would receive based on the priority that is set.
Last Action Taken	For scenarios where the actions are not successful, it is important for you to know what actions were last taken by the Workspace ONE UEM console on the particular version to narrow down the failure that occurred on the devices. You can hover on the action to see the time when the action was taken. All the actions taken by the Workspace ONE UEM console on a specific version application for a device can be found in this column.
Installation Status	Displays the last installation that was reported by the device. The information visible in this column is version agnostic but administrators can use it for troubleshooting based on the time stamp of the last action taken and the time stamp of when the event was reported by the device.
Assignment Status	Indicates whether or not a particular device has a valid assignment from Workspace ONE UEM console or if it has been explicitly excluded from the assignment.

5 Additionally, from the **Devices** tab you can use the following management functions:

Note: Currently, we only support actions on a particular page of devices and not on all the filtered devices.

Setting	Description
Install	Install the application on the selected device.
Remove	Remove the application, if managed, from the selected device.

Monitor your Public Applications

Public Applications summary metrics for the store applications that are deployed to your end-user devices and the devices list associated with a particular VPP application can be used for reporting and taking bulk actions. The view provides visual indications of your application deployment progress. You can get a summary of all the public applications that are managed at a particular OG. The granular view provides you with the application information the includes **Application Status**, **Managed By** and the **Application ID**. You can also filter the public applications deployment status view using the Smart Groups filter.Complete the following steps if you wish to track the application deployment of public applications.

1 Navigate to **Resources** > **Apps** > **Public**.

2 The **Summary** tab displays deployment charts that lets you to take a deep dive into the application deployment progress.

Analytic	Data Snapshot
Filter by Smart Group	You can use the filed to view the summary of the devices that belong to a particular smart group.For example, if an application is deployed to all your end-user devices and you like to get an understanding of how the deployment is progressing for your 'APAC' region, you can select APAC Smart Group from the Filter by Smart Group drop-down.
Assignment and Install Details	Displays installation details of devices that have the application assigned from Workspace ONE UEM. The view provides a clear picture of all the devices that have an assignment for each active version managed at the current OG.**Installed** – Lists the number of devices that have installed the application.**Not Installed** – Lists the number of devices that have not installed the application.
Last Action Details	Displays the actions that were last taken by Workspace ONE UEM console on the particular version.
Installation Status Details	This is a representation of the data reported by devices that include the detailed information about the installation state of this application and is not tied to a particular version.**Note**: The final state for is field is Managed.
Installs without assignments	For the ease of access and to drive actions, dislpays all the devices that have a particular version of an application installed but do not have valid assignment from Workspace ONE UEM console. Could list the devices that were previously assigned to this version of the application or the ones that side-loaded the application.

Managing your Application Deployment

9

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.

This chapter includes the following topics:

Manage Custom Notifications

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.

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
Copy	From the ellipses-vertical, you can click copy if you choose to duplicate the assignment configurations.
Delete	From the ellipses-vertical, you can delete to remove the selected assignment from the application deployment.
Priority	You can modify the priority of the assignment you configured from the drop-down menu while placing the selected assignment in the list of assignments. Priority 0 is the most important assignment and takes precedence over all other deployments. Your devices receive all the restrictions distribution policies and the app configuration policies from the assignment group which has the highest priority.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.For example, if 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 assignment's priority rating. Device 01 does not receive the priority 1 assignment.
Assignment Name	View the assignment name.
Description	View the assignment description.
Smart Groups	View the assigned smart group.
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.
EMM Managed Access	View whether the application has adaptive management enabled.When you enable this setting, the end-user is allowed to access the applications using Workspace ONE SDK only when it is EMM managed. To avoid any disruption to the service, ensure to take over management if the 'user installed' flag is enabled.

Benefits of Deploying your applications as Managed

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.

##Native List View Settings and Descriptions of your Application

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 **Resources** is slightly different and available functions vary, so the system does not display every option for every application type.

Setting	Description
Filters	**Platform** – View applications by platform. This filter helps you find numerous applications so you can perform large-scale management functions simultaneously.**Status** – View applications by status: Active, Retired, or Inactive. This view is helpful to return applications to previous statuses.**Category** – Locate applications specifically for a default or custom category. Find applications tagged as Finance, Business, Social Networking, and many other options. This filter helps you find large groups of applications.**Requires Renewal** – Find Apple iOS applications that use a provisioning profile to function. This filter locates applications with provisioning profiles you can update.**App Type** – View applications depending on type. Types include Public or Custom App 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 applications 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 in 32 Applications that are installed in the user contextUniversal 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 the Workspace ONE UEM console by selecting the radio button to the left of the application icon.You must select the radio button to display the Delete function, and the system deletes one application at a time.
Edit	To change the application record, select the pencil icon.
Name	Access the Summary tab of the Details View for internal applications so you can edit flexible deployments, track application installations, renew provisioning profiles, and select app wrapping statuses.
Install Status	Access a page with information about devices assigned to the application.Internal applications go to the Devices tab of the Details View. Perform management functions on devices like send messages, install applications, and remove applications.Web applications go to the View Devices page which offers management functions to install or delete applications.
Actions Menu	**Manage Devices** – Offers options for installing, removing, or notifying users about applications.**Manage Feedback** – Control feedback for applications for Apple iOS. This option displays under specific conditions. Displays only under specific conditions**Publish** – Publish the managed distribution content, manually, to devices.**Notify Devices** – Send a notification to devices concerning the VPP application.**Deactivate** – Removes an application and all versions of it from all managed devices.**User Ratings** – This 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 Settings and Descriptions of your Application

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:**Images** – If you uploaded mobile images, tablet images, and icons with the application, displays them.**Terms of Use** – Displays the terms of use, if configured, that device users must view and accept before they can use the application.**SDK** – Displays information pertaining to the use of the 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.**App Wrapping** – Displays information pertaining to the wrapping of the application. Some of the information on this tab includes the app wrapping status, the wrapped engine version used, and the size of the wrapped application.

Actions Menu Options

Setting	Description
Edit	Displays the application record for editing the tabs first configured when you uploaded the application.
Assign	Displays the flexible deployment record allowing you to add assignments and prioritize them or enables you to assign and edit groups assigned to the application.
Sync Licenses	Syncs online and offline licenses claimed by applications in a Microsoft Store Business integration.
Add Version	Upload a different version of an application and push it to devices.

Setting	Description
Manage	Control removal of applications and flexible deployment batching. This feature is for admins and is not available to all users.**Retire** – Removes an application from all managed devices. For iOS devices, if an older version of the application exists in the Workspace ONE UEM solution, then this older version is pushed to devices.**Deactivate** – Removes an application and all versions of it from all managed devices.**Bypass Batching** – Bypasses flexible deployment batching and releases all installation commands for applications.
View	Display the popularity of applications and issues with applications for troubleshooting application problems.**User Ratings** – Accesses ratings of applications using the star system, which you can use to gauge the popularity of internal applications.**Events** – Shows device and console events for applications and allows you to export these events as a CSV file.
Version	Add updated versions of applications, and accesses previous versions of internal applications.**Add Version** – Updates your internal application with a new version.**Other Versions** – Shows previous versions of an internal application that were added to the 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.**Manage Feedback** – Control feedback for applications for Apple iOS. This option appears under specific conditions so review the topic for these conditions.**View Analytics** – Exports the analytics for internal applications that use the VMware Workspace ONE SDK.**View Logs** – Downloads or deletes log files for internal SDK and wrapped applications.

Organize your Applications with Application Category

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.

1 Navigate to **Resources** > **Apps** > **Settings** > **App Categories**.

2 Select **Add Category**.

3 Provide the **Category Name** and **Category Description** and save the settings.

Manage Active and Inactive Status of your Application

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 activates the application for the assignment in retiring and rolling back scenarios and other management functions.

- **Inactive** – This status deactivates 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.

Install and Remove Applications using The Manage Devices Action

You can 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.

1 Navigate to **Resources** > **Apps** > **Native** and select either the **Public** or **Purchased** tab.

2 Select the **Manage Devices** option from the actions menu.

3 Select from the actions menu or select the desired options. You can act on specific devices (selected and filtered) or act on all devices (listed).

Setting	Description
Install	Install an application on a single device or on multiple devices.
Remove	Remove an application from a single device or off multiple devices.**macOS**: Workspace ONE UEM cannot remove VPP applications (purchased) for macOS devices.**Windows Desktop and Phone**: This function removes the application but not the license for public applications acquired through the Microsoft Store for Business.
Notify	Notify devices about an asset.Settings include email, SMS, push, and message template options for sending messages.
Reinvite(Only Purchased)	Send an invitation to join the Apple VPP, managed distribution, to devices. Devices must run Apple iOS v7.0.3+.The page also lists devices that accepted the invitation.

Alternatives for Deleting your Application

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. 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.

Deactivating your Application

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.

Retiring your Application

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.

Retire Scenario	Retired App Version Action	Lower App Version Action
Two active versions and retire the higher version	Replaced on the device	If the push mode is Auto, the device user does nothing and the app pushes to devices, which results in having the lower, active version on the device.If the push mode is On Demand, the device user must initiate an installation from the AirWatch Catalog, which results in having the lower, active version on the device.
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.

Manage User-Installed Application

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.

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.

Manage your Per-App VPN and Native Applications

10

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 organization, 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.

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.

This chapter includes the following topics:

Edit the Per-App VPN Profile of an Internal Application

You can 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.

1 Navigate to **Resources** > **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**.

Change the Assignment Priority of the Per-App VPN Profile

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

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 **Resources** > **Apps** > **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**.

Remove the Per-App VPN Profile from your Application

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

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 **Resources** > **Apps** > **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**.

Edit a Smart Group

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

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.

Manage your Application Groups and Compliance

11

You can use application groups (app groups) and compliance policies to protect resources in your Workspace ONE UEM environment. Application groups identify permitted and restricted applications so that compliance policies can act on devices that do not follow protective standards.

You can configure app groups for several platforms but you cannot combine all of them with compliance polices. For those platforms that you cannot combine with compliance policies, apply an application control profile.

App Group Platform	Works with Compliance Policies	Works with Application Control Profiles
Android	Yes	Yes
Apple iOS	Yes	No
Windows Phone	No	Yes

You are not required to configure application groups. However, application groups enhance the efficacy and reach of your compliance policies with minimal configurations.

Relationships Between Application Groups and Compliance Policies

Application Group	Description	Compliance Policy	Action
Allowlist	Managed devices can install these applications from the AirWatch Catalog.If an application is not on the list, it is not permitted on managed devices.	Contains Non-allowlisted Apps	The compliance engine identifies applications not in the allowlisted app group installed on the device and applies the actions that are configured in the compliance rule.
Denylist	Managed devices do not install these applications from the AirWatch Catalog.If an application is on this list, it is not allowed on managed devices.	Contains denylisted Apps	The compliance engine identifies applications from the denylisted app group on the device and applies the actions that are configured in the compliance rule.
Required	Managed devices are required to install these applications from the AirWatch Catalog.If an application is on this list, it is required device users install it on managed devices.	Does Not Contain Required Apps	The compliance engine identifies applications from the required app group missing on the device and applies the actions that are configured in the compliance rule.

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

This chapter includes the following topics:

Impact of Privacy Settings on Application List Compliance and Application Control profile

In the Workspace ONE UEM console, if you configure the Privacy settings of the Personal Application as **Do Not Collect** the system does not collect the personal app information from the devices. That is, the end user's personal application information is not transmitted from their devices.

The Privacy settings however have the following caveats that impact the Application List Compliance and Application Control profile settings:

- The compliance policy for the Application List checks to verify that a device has the appropriate applications (denylist, whitelist, or required). If the system does not query for the Application List, it might not check for these applications. As a result, the devices that contain certain applications in the denylist group are not marked as 'non-compliant'. Similarly the devices that do contain certain 'required' (personal) applications is marked as 'non-compliant'.
- Application control profile with the action on 'denylist' apps is not applied to the devices whose personal app privacy is set to **Do Not Collect** and is applied only on the devices for which we collect the personal app information.

If you want to take actions on your end-user's personal applications list, keep a track of the personal app privacy configuration for the concerned device ownership type at all OGs, and verify the following:

- Ensure that the configuration is not set to **Do Not Collect**. If you want to ensure privacy of your end-users and detect any malicious applications, set the privacy configuration to **Collect but do not display**.

- Ensure that your end-user devices have the entitlements to receive the applications, that you intend to take actions on, from Workspace ONE UEM.

Configure your 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.

1 Navigate to **Resources** > **Apps** > **Settings** > **App Groups**.

2 Select **Add Group**.

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

Settings	Description
Type	Select the type of application group you want to create depending on the desired outcome: allow applications, block applications, or require application installations.If your goal is to group custom MDM applications, select MDM Application. You must enable this option for it to display in the menu.
Platform	Select the platform for the application group.
Name	Enter a display name for the application group in the Workspace ONE UEM console.
Add Application	Display text boxes that enable you to search for applications to add to the application group.
Application Name	Enter the name of an application to search for it in the respective app store.
Application ID	Review the string that automatically completes when you use the search function to search for the application from an app store.
Add Publisher - Windows Phone	Select for Windows Phone to add multiple publishers to application groups. Publishers are organizations that create applications.Combine this option with Add Application entries to create exceptions for the publisher entries for detailed allowlists and denylists 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.

Settings	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.

Settings	Description
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 your App Groups and Application Control Profile

You can edit your App Groups and Application Control Profile. When you edit app groups for Android and Windows phone, edit the app group first, then the application profile.

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

You can use app groups to push application notifications to app catalogs you require devices to install.

1 Navigate to **Resources** > **Apps** > **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 your 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.

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

2 Select **Customization**.

3 Enable **Use Custom MDM Applications**.

Compliance Policies for your Application

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 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.

You can configure an application list compliance policy for several platforms that acts on non-compliant devices.

Supported Platforms for Compliance Policies and Applications:

- Android
- Apple iOS
- macOS

Build an Application Compliance Policy

Add compliance policies that work with app groups to add a layer of security to the mobile network. Policy configurations enable the Workspace ONE UEM compliance engine to take set actions on non-compliant devices.

1 Navigate to **Devices** > **Compliance Policies** > **List View**. Select **Add**.

2 Select the platform, **Android**, **Apple iOS**, or **Apple macOS**.

3 Select **Application List** on the **Rules** tab.

4 Select the options that reflect your desired compliance goals.

Setting	Description
Contains	Add the application identifier to configure the compliance engine to monitor for its presence on devices.If the engine detects the application is installed on devices assigned to the Compliance Rule, the engine performs the actions configured in the rule.
Does Not Contain	Add the application identifier to configure the compliance engine to monitor for its presence on devices.If the engine detects the application is not installed on devices assigned to the Compliance Rule, the engine performs the actions configured in the rule.
Contains Denied Apps	If the engine detects applications listed in denylist app groups on devices assigned to the Compliance Rule, the engine performs the actions configured in the rule.
Contains Non-Allowed Apps	If the engine detects applications not listed in whitelisted app groups on devices assigned to the Compliance Rule, the engine performs the actions configured in the rule.
Does Not Contain Required Apps	If the engine detects that devices assigned to the Compliance Rule are missing applications in required app groups, the engine performs the actions configured in the rule.
Does Not Contain Version	Add the application identifier and the application version the compliance engine monitors device to ensure the correct version of the application is installed on devices.If the engine detects the wrong version of the application is installed on devices assigned to the Compliance Rule, the engine performs the actions configured in the rule.

You can get the **Application Identifier** from an app store or from its record in the Workspace ONE UEM console. Navigate to **Resources** > **Apps** > **List View** > **Internal** or **Public**. Select **View** from the actions menu for the application and then look for the **Application ID** information.

1 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.

Settings	Description
Mark as Not Compliant	Select 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.Deselect this option when you do not want to quarantine the device immediately.
Application	Select to remove the managed application.
Command	Select to configure the system to command the device to check in to the console, to perform an enterprise wipe, or to change roaming settings.
Email	Select to block email on the non-compliant device.
Notify	Select to notify the non-compliant device with an email, SMS, or push notification using your default template.You can also send a note to the admin concerning the rule violation.
Profile	Select to use Workspace ONE UEM profiles to restrict functionality on the device.

2 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.

3 Select the **Summary** tab to name the rule and give it a brief description.

4 Select **Finish and Activate** to enforce the newly created rule.

Legacy App Catalogs and the Workspace ONE Intelligent Hub

12

Use the Workspace ONE Intelligent Hub, with its app catalog component, to manage your applications and devices in your Workspace ONE UEM deployment. There are legacy app catalogs that still have settings in the Workspace ONE UEM console, the AirWatch Catalog and the Workspace ONE app. However, these apps are no longer the best systems to use as an app catalog for Workspace ONE UEM.

This chapter includes the following topics:

Documentation for the Workspace ONE Intelligent Hub

The Workspace ONE Intelligent Hub is a component of Workspace ONE Hub Services. Although the Workspace ONE Intelligent Hub has an app catalog, it serves many other purposes in managing your Workspace ONE UEM-deployed devices.

- Workspace ONE Hub Services: See the VMware Workspace ONE Hub Services Documentation site for information about Workspace ONE Hub Services and its components and features.
- Workspace ONE Intelligent Hub:
  - See Setting up the App Catalog in Hub Services for details on the app catalog component.
  - See Deploying the Workspace ONE Intelligent Hub Application App for information on deploying the app for Android, iOS, and macOS platforms.

Other Documentation for Workspace ONE UEM and the Workspace ONE Intelligent Hub

- Android: Enrolling with Workspace ONE Intelligent Hub Identifier
- iOS: Enroll an iOS Device with the Workspace ONE Intelligent Hub
- macOS: Enrollment with macOS Intelligent Hub
- Windows Desktop: Workspace ONE Intelligent Hub for Windows 10 Enrollment

- Windows Rugged: Windows Rugged Enrollment

Legacy Apps - Workspace ONE App and AirWatch Catalog

These apps still have settings in the Workspace ONE UEM console. However, consider using the Workspace ONE Intelligent Hub and its app catalog component.

The Workspace ONE catalog integrates resources from environments that use Workspace ONE UEM and Workspace ONE Access. If your deployment does not use Workspace ONE UEM , you still have access to the features previously released for the AirWatch Catalog.

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.

Review brief descriptions of the options available for both Workspace ONE and the AirWatch Catalog and those options that apply specifically to the AirWatch Catalog.

Setting	Description
Application Categories	Group applications and identify their uses with custom application categories.
Paid Public Applications	Deploy paid public iOS applications in situations not feasible to use Apple's Volume Purchase Program (VPP).
App Restrictions	Restrict iOS devices older than iOS 9 by restricting installations of only assigned applications approved by the organization.
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.
Application Removal Protection	Configure threshold values to control the dispatch of application removal commands for critical internal applications.

AirWatch Catalog Specific Settings

Setting	Description
AirWatch Catalog > **Standalone Catalog**	Configure a standalone catalog if your environment does not use MDM functionality. The standalone catalog has limited features.
AirWatch Catalog > **Feature Applications**	Display featured applications in a prominent place in the AirWatch Catalog.
AirWatch Catalog > **General**	Configure general settings for the AirWatch Catalog.

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.