Application Management for iOS

VMware Workspace ONE UEM 2001

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Copyright © 2020 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

Application Management for iOS

1

You can use Workspace ONE UEM powered by AirWatch to push industry templates, purchased, purchased VPP, public and internal applications, web apps and SaaS applications to iOS devices.

This chapter includes the following topics:

Application Types and Suported OS Versions for iOS

Workspace ONE UEMclassifies applications as native (internal, public, purchased), SaaS, and Web. You can upload applications depending on the type. Workspace ONE UEM supports the OS Versions for Android applications based on the application type.

Table 1-1. Application Types and Supported OS Versions

Application Type	Supported Platforms
Industry Templates Any Supported App Type	Apple iOS v7.0+ with limitations for compliance policies
Internal	■ Apple iOS v7.0+ **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)	■ Apple iOS v7.0+
Purchased – Custom B2B	Apple iOS v7.0+
Purchased – VPP	■ Apple iOS v7.0+
Web Links	■ Apple iOS v7.0+
SaaS	■ Apple iOS v7.0+

Provisioning Profiles for an Internal iOS Application

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

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

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

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

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

iOS Provisioning Profile Management

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

Issues exist for developers and device users.

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

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

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

Renew your iOS Provisioning Profiles

Renew your Apple iOS provisioning profiles without requiring end users to reinstall the application. You can also renew the file for all applications associated with it. The Workspace ONE UEM console notifies you 60 days before the profile expires.

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

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

Procedure

1. Navigate to **Apps & Books > Applications > Native > Internal**.
2. Select the expiration link (**Expires in XX days**) in the **Renewal Date** column for the application for which you want to update the provisioning profile.
3. Use the **Renew** option on the **Files** tab to upload the replacement file.
4. Select the **Update Provisioning Profile For All Applications** setting to apply the renewed file to all associated applications.

   Workspace ONE UEM displays this option only if multiple applications share the provisioning profile.

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

Paid Public iOS Applications and Workspace ONE UEM

Workspace ONE UEM allows you to upload paid public iOS applications and distribute them in those scenarios where it is not feasible to use Apple's Volume Purchase Program (VPP). Also for the iOS devices you can configure extra restrictions on the App Store functionality, including the App Store icon and installation of public apps.Workspace ONE UEM can distribute several OS versions, but iOS 9+ management does not require users to take extra steps. It is best to use the Apple VPP, if possible. The VPP can manage bulk public paid applications efficiently and offers several management options.

Compare Paid Public App Procedures

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

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

Add Any Supported iOS Version as Paid Public App	Add iOS 9+ Version as Paid Public App
Enable the paid public iOS applications process in the Workspace ONE UEM console.	Enable the paid public iOS applications process in the Workspace ONE UEM console.
Add the public application to the Workspace ONE UEM console. Add any other management parameters like SDK features and enabling per-app VPN.	Add the public application to the Workspace ONE UEM console and enable **Make App MDM Managed if User Installed** on the **Deployment** tab. Add any other management parameters like SDK features and enabling per-app VPN.

Add Any Supported iOS Version as Paid Public App	Add iOS 9+ Version as Paid Public App
(User) Purchase the application.	(User) Purchase the application. Apple installs the application automatically to the device after purchase.
(User) Delete the application installed by Apple.	Not applicable
(User) Open the AirWatch Catalog and initiate the installation from Workspace ONE UEM to receive the managed version of the application.	(User) Open the AirWatch Catalog and initiate the installation from Workspace ONE UEM to receive the managed version of the application.

Configure your Paid Public iOS Application in the UEM Console

You can configure the deployment of the paid public iOS applications in the Workspace ONE UEM console.

Complete the following steps to configure the deployment of the paid public iOS applications in the Workspace ONE UEM console.

Procedure

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

Assign your Paid Public Application based on the Organization Group

You can keep your VPP deployment and your paid public iOS applications in separate organization groups. You can also enable the paid public status option in the organization group where applicable devices are enrolled.

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

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

Table 1-2. Example of a Paid Public Application Assignment Depending on the Organization Group

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

Upload your Paid Public Application to the UEM Console

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

Prerequisites

Configure your paid public iOS application in the Workspace ONE UEM console. See Configure your Paid Public iOS Application in the UEM Console.

Procedure

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

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

Control your Paid Public Applications access from the App Store

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

Procedure

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

What to do next

Workspace ONE UEM supports both native iOS restrictions and in-house developed restriction that control access to the app store.

Table 1-3. Descriptions of Available App Store Restriction Methods

Restriction	Supported Device Supervision Status	Configuration	Description
Allow App Store icon on Home screen The best option for iOS 9+ devices because it uses the latest technologies and can push applications through several systems.	Supervised	Disable	Restrict the Apple App Store from being installed on the device so the device user cannot install public free applications using the App Store. However, push public free applications using Workspace ONE UEM, iTunes, or Apple Configurator.
		Enable	Allow the Apple App Store on the device and the device user can install any public free applications using the App Store.
Allow installing public apps An option for many iOS versions but does not offer the ability to select the system that restricts the installation of non-enterprise applications.	Supervised Unsupervised	Disable	Restrict the device user from using the Apple App Store.
		Enable	Allow the Apple App Store on the device and the device user can install any public free applications using the App Store.
Restricted Mode for Public iOS Applications Workspace ONE UEM developed ways to allow the installation of enterprise-approved free public applications when this option is enabled. When you configure this option, you do not need to configure and apply a restriction profile with **Allow installing public apps**.	Supervised Unsupervised	Disable	Allow the Apple App Store on the device and the device user can install any public free application using the App Store.
		Enable	Block the device from installing free public applications from the Apple App Store. Push free public applications using Workspace ONE UEM.

Control your Paid Public iOS Application Installation

You can configure the **Allow App Store icon on Home screen** restriction to control the installation of free public applications on iOS 9+ devices without having to enable any other restriction in the Workspace ONE UEM console.

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

Configure the Restricted Mode for your Public iOS Applications

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

Procedure

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

Configure the Restricted Mode for your Public iOS Application on Devices that are Older Than iOS 9

You can configure the Restricted Mode on the devices older than iOS 9 that allows you to install only the assigned applications approved by the organization. Enabling the setting automatically sends a restricted profile to Apple iOS devices. Restricted Mode does not require an extra restriction with **Allow installing public apps** enabled.

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