Application Management for iOS

VMware Workspace ONE UEM 2203

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

Contents

Introduction to Managing iOS Applications

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.

Application Types and Suported OS Versions for iOS

Workspace ONE UEM classifies applications as native (internal, public, purchased), SaaS, and Web apps. You can use Workspace ONE UEM to manage the deployment and maintenance of your iOS applications. You can upload applications depending on the type. Workspace ONE UEM supports the OS Versions for iOS applications based on the application type.

You can choose from the following app types:

- Public Apps: Apps that have been uploaded to the App store, or the Google Play store are examples of public apps. The provider of a store app maintains and provides updates to the app. You select the app in the store list and add it by usingWorkspace ONE UEM as an available app for your users.
- Internal Apps: Apps that are created in-house are internal apps. Your organization creates and provides you with updates as a separate file. You provide updates of the app to users by adding and deploying the updates using Workspace ONE UEM.
- Web Apps: Web apps are client-server applications. The server provides the web app, which includes the UI, content, and functionality. Also, modern web hosting platforms commonly offer security, load balancing, and other benefits. This type of app is separately maintained on the web.

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+

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

Application Type	Supported Platforms
Purchased – Custom B2B	Apple iOS v7.0+
Purchased – VPP	■ Apple iOS v7.0+
Web Links	■ Apple iOS v7.0+
SaaS	■ Apple iOS v7.0+

Paid Public iOS Applications and Workspace ONE UEM

2

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.
(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 Console

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

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 2-1. 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 UEM console to make it available in a catalog.

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

Prevent Paid Public Application downloads from the App Store through Device Restriction

You can configure device restrictions to control what applications, hardware, and functionality your end users can access. You can use these restrictions to enhance productivity, protect end users and devices. Workspace ONE UEM supports native iOS restrictions and an in-house developed restriction that controls access to the app store.You can configure the **Allow App Store icon on home screen** restriction in the UEM console to hide the App Store. This restriction removes the icon from the Home Screen and end users cannot access the App Store. However, end users can still use MDM to install or update their apps, giving full application control to the administrator.

The **Allow App Store icon on home screen** restriction is available only for iOS 9+ supervised devices. In general, supervised devices give you more control over the devices you own and lets you set restrictions.Control the app store to restrict or allow device users to access the public applications available therein.

1 Navigate to **Devices > Profiles &Resources > Profiles > Add**.

2 Select **Apple iOS**.

3 Configure the profile's **General** settings.

4 Select the **Restrictions** payload from the list. You can select multiple restrictions as part of a single restrictions payload.

Table 2-2. Descriptions of App Store Restriction Methods

Restriction	Configuration	Description
Allow App Store icon on Home screen This restriction is supported for all supervised iOS 9+ devices as it uses the latest technologies and can push applications through several systems.	Deactivate	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.
	Activate	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 This restriction is supported for all iOS 4-12 devices and supervised iOS 13+ devices.	Deactivate	Restrict the device user from using the Apple App Store.
	Activate	Allow the Apple App Store on the device and the device user can install any public free applications using the App Store.

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

Restrict your Device to only Install Assigned public Apps from the App Store

You can control from where end users install public applications by enabling Restricted Mode on Apple iOS devices. After enrollment, end users can access free public applications deployed to their catalogs, but they are unable to download free public applications from the App Store. Control from where end users install public applications by enabling **Restricted Mode for Public iOS Applications**. Restricted Mode restricts the device by allowing you to install only the assigned applications approved by the organization. Enabling the setting SEsends a restricted profile to Apple iOS devices. The presence of this restricted profile does not require an extra restriction profile with the **Allow installing public apps** option enabled to block the app store.

This restriction is the same as the iOS restriction **Allow App Store icon on Home screen** found in **Devices** > **Profiles & Resources** > **Profiles**. 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 ensures that your organization approves them.

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

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

3 Click **Save**

Provisioning Profiles for an Internal iOS Application

3

A Provisioning Profile is a combination of your App ID and distribution certificates.The profile authorizes developers and devices to create and run applications built for Apple iOS devices. If you want to develop and distribute apps privately within your company or to a selected number of end users, you can use a provisioning profile for internal distribution.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. Each Provisioning Profile contain a set of iPhone Development Certificates, Unique Device Identifiers and an App ID. Devices specified within the provisioning profile can be used for testing only by those individuals whose iPhone Development Certificates are included in the profile. A single device can contain multiple provisioning profiles.

We have two types of program that lets you distrubute applications:

- **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. An App Store Provisioning Profile lets you post your apps in the Apple App Store.

For internal applications, use files from the Apple iOS Developer Enterprise Program When you get a mobile provisioning profile for your internal applications, verify that it is for enterprise (internal) distribution.

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 console 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 console .
- 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.

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