Apple tvOS Device Management

VMware Workspace ONE UEM

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

1 Introduction to Apple tvOS 4

2 Apple tvOS Enrollment 5

3 Apple tvOS Profiles 7

4 Apple tvOS Management 10

Introduction to Apple tvOS 1

Workspace ONE UEM powered by AirWatch manages Apple TVs to prevent unauthorized users from accessing the network to which Apple TVs are connected. Workspace ONE UEM also enables specific management of tvOS features and functions to maximize their effectiveness in your deployment environment.

Apple TVs are quickly becoming the ideal choice for presentation and collaboration in a variety of settings.

In a corporate setting, Apple TVs enable presenters to share visuals and projections from multiple devices at conferences and large meetings.

In a retail setting, Apple TVs broadcast product displays or store announcements to monitors throughout a store or lobby area.

In an education environment, teachers can allow AirPlay destinations to prevent students from accidentally - or purposefully - projecting their iPhone or iPad to the Apple TVs in the classroom. Additionally, teachers can prompt a student to mirror their device to a specific Apple TV to present a project or class material.

tvOS Supported Devices

The list of supported devices mentioned are based on the use of Apple Configurator 2.0. Any other versions of the software may function differently.

The tvOS features and AirPlay management settings profiled in this guide are supported by 2nd, 3rd, and 4th generation Apple TVs, and iPhones, iPod Touches, and iPads running iOS 7 and higher.

Note Integration with any third-party software product is not guaranteed, and is dependent upon the proper functioning of those third-party solutions.

Apple tvOS Enrollment

2

The first step to integrating your Apple TVs with Workspace ONE UEM is to enroll the device. You must enroll your device into your Workspace ONE UEM environment before it can be monitored and managed.

Prerequisites

Unlike other devices and platforms, tvOS enrollment does not require the Workspace ONE Intelligent Hub or access to a web browser on the device itself. However, the tvOS devices should be connected to a secure network to enroll successfully.

If you choose to enroll using Apple DEP, you must have an Apple DEP account.

Connect a tvOS Device to a Network

Begin the enrollment process for your tvOS devices by connecting devices to your network so they can receive enrollment commands. Create a Wi-fi profile to push to your devices if necessary.

For more information, see *Connect a tvOS Device to a Network.*

Enroll a tvOS Device

To complete the enrollment of a tvOS device, you must configure the specific device you are enrolling using Apple Configurator 2. You need an Apple computer to complete this procedure.

For more information, see *Enroll a tvOS Device.*

Enroll a tvOS Device Using Apple DEP

Apple TV 4th generation devices running tvOS 10.2 and higher can be enrolled using the Apple Device Enrollment Program. The DEP enrollment simplifies the setup and deployment of enrollment and use profiles.

For more information, see *DEP Enrollment for tvOS Devices.*

DEP Enrollment for tvOS Devices

With 4th generation Apple TV devices running tvOS 10.2, you can enroll Apple TVs through the Apple Device Enrollment Portal.

Using a registered device, follow the standard Setup Assistant process, including language, country or region, and Wi-Fi network. From this point, the Setup Assistant flow varies as determined by settings in the DEP profile that you assigned to the device.

Currently, tvOS devices do not support the following set-up options:

- Skip the configuration for the device screensaver
- Skip the configuration for Tap to Set Up

For more information on DEP Enrollment for tvOS devices, see the **VMware Workspace ONE UEM Guide for the Apple Device Enrollment Program**.

Apple tvOS Profiles

3

Profiles are the primary means to manage devices. Configure profiles so your tvOS devices remain secure and configured to your preferred settings.

You can think of profiles as the settings and rules that, when combined with compliance policies, help you enforce corporate rules and procedures. They contain the settings, configurations, and restrictions that you want to enforce on devices.

A profile consists of the general profile settings and a specific payload. Profiles work best when they contain only a single payload.

Device Access

Some device profiles configure the settings for accessing a tvOS device. Use these profiles to ensure that access to a device is limited only to authorized users.

- Use a Wi-Fi profile to connect enrolled devices to your corporate Wi-Fi without sending the network credentials to users. For more information, see *Configure Wi-Fi Access for tvOS Devices*.

Device Security

Ensure that your macOS devices remain secure through device profiles. These profiles configure the native tvOS security features or configure corporate security settings on a device through Workspace ONE UEM.

- Implement digital certificates to protect corporate assets. For more information, see *Configure Credentials for tvOS Devices.*

Device Configuration

Configure your tvOS devices with configuration profiles. These profiles configure the device settings to meet your business needs.

- Simplify the enrollment setup process for tvOS devices by creating a streamlined enrollment workflow using Auto Advance Setup profile. For more information, see *Configure an Auto-Advance Setup Profile (tvOS).*

Configure a Wi-Fi Access Profile (tvOS)

A Wi-Fi profile lets devices connect to corporate networks, even if they are hidden, encrypted, or password protected. This can be useful for automatically configuring devices to connect to the appropriate wireless network while in an office.

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add a Profle**. Select **tvOS**.

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

3 Select the **Wi-Fi** payload from the list.

4 Configure **Wi-Fi** settings, including:

Table 3-1.

Settings	Description
Service Set Identifier	This is the name of the network the device connects to.
Auto-Join	This determines whether the device automatically connects to the network.
Security Type	This is the type of access protocol used and whether certificates are required.
Password	This is the password required for the device to connect to the network.
Proxy	This enables an automatic or manual proxy that you can configure for your Wi-Fi profile.

5 Select **Save & Publish**.

Configure a Credentials Profile (tvOS)

Push certificates to streamline and secure Wi-Fi login for tvOS devices.

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add a Profile**. Choose **tvOS** from the platform list.

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

3 Configure the Wi-Fi payload.

4 Select the **Credentials** payload and **Upload** a certificate, select **Defined Certificate Authority**, or select **User Certificate** from the Credential Source drop-down menu, depending on your needs

5 Select the **Certificate Authority** and **Certificate Template** from their respective drop-down menus. Navigate back to the previous payload for Wi-Fi.

6 Select a compatible **Security Type** (WEP Enterprise, WPA/WPA2 Enterprise or Any (Enterprise)) and select the **Identity Certificate** under Authentication.

7 Click **Save and Publish** when you are done configuring any remaining settings.

Configure an Auto-Advance Setup Profile (tvOS)

Take advantage of zero-touch deployment functionality for tvOS devices enrolled using DEP. This feature simplifies the setup process for tvOS devices by creating a streamlined enrollment workflow.

tvOS devices enrolled through Apple DEP can be set to enroll using Auto Advance Setup. Auto Advance Setup lets users turn on an Apple TV device that is configured for DEP enrollment and immediately have access to the device to broadcast to connected televisions. The tvOS device queries the DEP Profile and enrolls instantaneously.

For more information about setting up Auto Advance Setup for DEP-enrolled tvOS devices, see **Complete the DEP Enrollment Profile** in the **VMware Workspace ONE UEM Guide for the Apple Device Enrollment Program**.

Apple tvOS Management

4

Start managing Apple tvOS devices after they get enrolled to the Workspace ONE UEM console

Device Dashboard

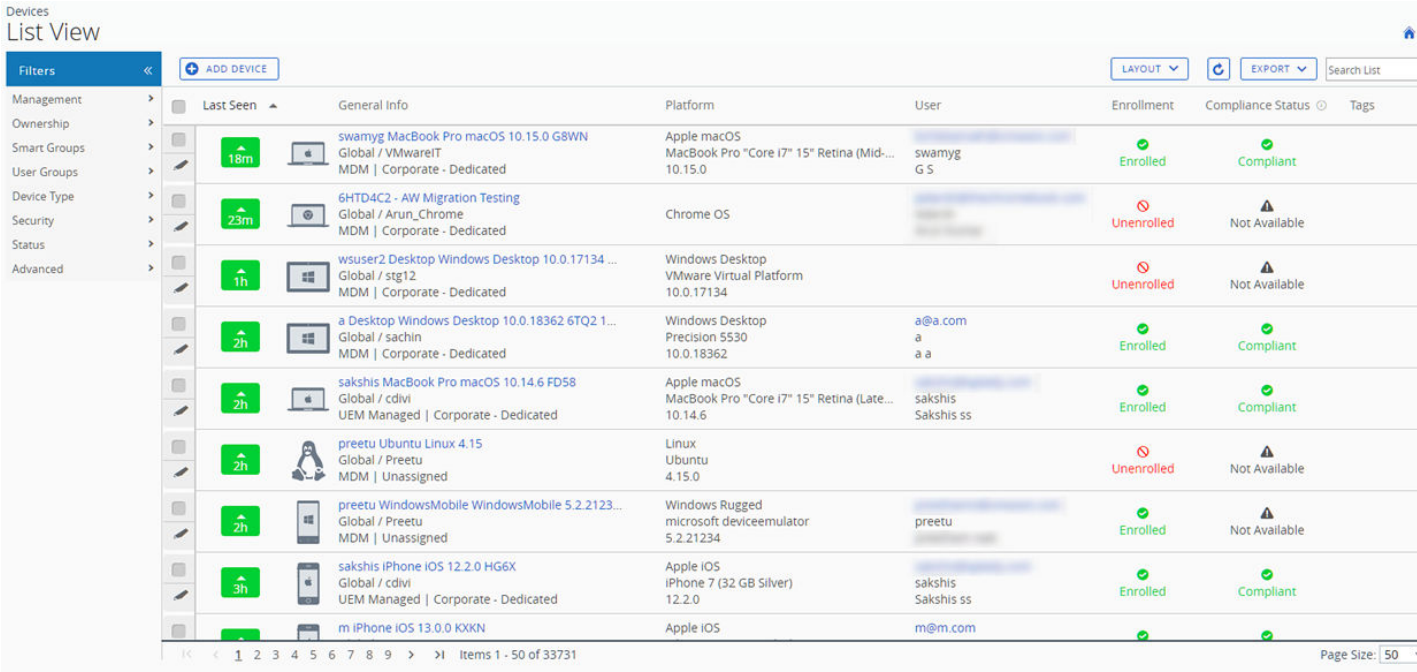
As devices are enrolled, you can manage them from the Workspace ONE ™ UEM **Device Dashboard**. The **Device Dashboard** provides a high-level view of your entire fleet and allows you to act on individual devices quickly.

You can view graphical representations of relevant device information for your fleet, such as device ownership type, compliance statistics, and platform and OS breakdowns. You can access each set of devices in the presented categories by selecting any of the available data views from the **Device Dashboard**.

From the **List View**, you can take administrative action: send messages, lock devices, delete devices, and change groups associated with the device.

Device List View

Use the Device List View in Workspace ONE UEM powered by AirWatch to see a full listing of devices in the currently selected organization group.



The **Last Seen** column displays an indicator showing the number of minutes elapsed since the device has checked-in. The indicator is red or green, depending on how long the device is inactive. The default value is 480 minutes (8 hours) but you can customize this by navigating to **Groups & Settings > All Settings > Devices & Users > General > Advanced** and change the **Device Inactivity Timeout (min)** value.

Sort by columns and configure information filters to review activity based on specific information. For example, sort by the **Compliance Status** column to view only devices that are currently out-of-compliance and target only those devices. Search all devices for a friendly name or user name to isolate one device or user.

Select a device-friendly name in the **General Info** column at any time to open the details page for that device. A **Friendly Name** is the label you assign to a device to help you differentiate devices of the same make and model.

Customize Device List View Layout

Display the full listing of visible columns in the **Device List** view by selecting the **Layout** button and select the **Custom** option. This view enables you to display or hide Device List columns per your preferences.

Once all your customizations are complete, select the **Accept** button to save your column preferences and apply this new column view. You can return to the **Layout** button settings at any time to tweak your column display preferences.

Some notable device list view custom layout columns include the following.

- Android Management
- SSID (Service Set Identifier or Wi-Fi network name)
- Wi-Fi MAC Address

- Wi-Fi IP Address
- Public IP Address

There is also an option to apply your customized column view to all administrators at or below the current organization group (OG). For instance, you can hide 'Asset Number' from the **Device List** views of the current OG and of all the OGs underneath.

Exporting List View

Select the **Export** button to save an XLSX or CSV (comma-separated values) file of the entire **Device List View** that can be viewed and analyzed with MS Excel. If you have a filter applied to the **Device List View**, the exported listing reflects the filtered results.

Search in Device List View

You can search for a single device for quick access to its information and take remote action on the device.

To run a search, navigate to **Devices > List View**, Select the **Search List** bar and enter a user name, device-friendly name, or other device-identifying element. This action initiates a search across all devices, using your search parameter, within the current organization group and all child groups.

Device List View Action Button Cluster

With one or more devices selected in the Device List View, you can perform common actions with the action button cluster including Query, Send [Message], Lock, and other actions accessed through the **More Actions** button.

Available Device Actions vary by platform, device manufacturer, model, enrollment status, and the specific configuration of your Workspace ONE UEM console.

Remote Assist

You can start a **Remote Assist** session on a single qualifying device allowing you to remotely view the screen and control the device. This feature is ideal for troubleshooting and performing advanced configurations on devices in your fleet.

To use this feature, you must satisfy the following requirements.

- You must own a valid license for Workspace ONE Assist.
- You must be an administrator with a role assigned that includes the appropriate Assist permissions.
- The Assist app must be installed on the device.
- Supported device platforms:
  - Android
  - iOS

- macOS
- Windows 10
- Windows Mobile

For more information, see the **Workspace ONE Assist** guide, available on docs.vmware.com.

Select the check box to the left of a qualifying device in the **Device List View** and the **Remote Assist** button displays. Select this button to initiate a Remote Assist session.

Configure and Deploy a Custom Command to a Managed Device

Workspace ONE UEM enables administrators to deploy a custom XML command to managed Apple devices. Custom commands allow more granular control over your devices.

Use custom commands to support device actions that the UEM console does not currently support. Do not use custom commands to send commands that exist in the UEM console as Device Actions. Samples of XML code you can deploy as custom commands are available in the Workspace ONE UEM Knowledge Base at https://kb.vmware.com/s/article/2960669.

Important Improperly formed or unsupported commands can impact the usability and performance of managed devices. Test the command on a single device before issuing custom commands in bulk.

1 In the UEM console, navigate to **Devices > List View**.

2 Select one or more macOS or iOS devices using the check boxes in the left column.

3 Select the **More Actions** drop-down and select **Custom Commands**. The Custom Commands dialogue box opens.

4 Enter the XML code for the action you want to deploy and select **Send** to deploy the command to devices.

   Browse XML code for Custom Commands on the Workspace ONE UEM Knowledge Base at https://kb.vmware.com/s/article/2960669.

   If the Custom Command does not run successfully, delete the command by navigating to **Devices > List View**. Select the device to which you assigned the custom command. In the Device **Details View**, select **More > Troubleshooting > Commands**. Select the Command you want to remove, and then select **Delete**. The Delete option is only available for Custom Commands with a Pending status.

tvOS Device Details

Use the Device Details page to track device information and to access user and device management actions.

You can access the Device Details page by selecting a device's Friendly Name from the Device Search page, from one of the available Dashboards, or by using any of the available search tools with the UEM console.

Use the **Device Details** menu tabs to access specific device information.

Tab	Description
Summary	View general statistics such as enrollment status, compliance, last seen, platform/model/OS, organization group, contact information, serial number, Device ID, UDID, asset number, power status, storage capacity, physical memory and virtual memory.
Profiles	View all MDM profiles currently installed on a device.
Location	View current location or location history of a device.
User	Access details about the user of a device as well as the status of the other devices enrolled to this user.

Select **More** on the main Device Details tab for additional options.

Security	View current security status of a device based on security settings.
Restrictions	View the types of restrictions that currently apply to the device.
Notes	View and add notes regarding the device. For example, note the shipping status or if the device is in repair and out of commission.
Certificates	Identify device certificates by name and issuant. This tab also provides information about certificate expiration.
Troubleshooting	View event logs to see history of device in relation to MDM, including instances of debug, information and server check-ins.
Alerts	View all alerts associated with the device.
Device Registration (iOS)	View all restrictions currently applied to a device. This tab also shows specific restrictions by Device, Apps, Ratings and Passcode.
Status History	View history of device in relation to enrollment status.
Attachments	Add files associated to the device.

Enterprise Application Management (tvOS)

Deploy applications to tvOS devices to manage internal apps on tvOS devices over-the-air. Manage an application by installing it or removing it from devices.

In the Workspace ONE UEM console, you can:

- Assign a tvOS app with options to configure minimum OS and Supported models.
- Deploy a tvOS app to devices by assigning them to smart groups.
- Specify the App Delivery Method for tvOS apps.
- Get installation statuses with sampling during installation and at scheduled intervals using the MDM Sample Schedule.

Following are some of the actions supported for apps on tvOS devices:

- Add new app
- Renew provisioning profile
- Add application configuration
- Add on demand install functionality

Public Application Management (tvOS)

Public applications can only be deployed to tvOS devices using device-based licenses purchased in Apple Business Manager (formerly Volume Purchase Program or VPP). This extends Apple Business Manager app support to tvOS devices alongside iOS and macOS support.

Prerequisites

- tvOS 12 and later
- Content Manager admin access to Apple Business Manager integrated with Workspace ONE UEM

Steps to Deploy Public Apps

Syncing, assigning and deploying Apple Business Manager applications to tvOS devices is done in the same manner as iOS devices. When purchasing licenses in Apple Business Manager, tvOS apps will frequently be the same app used to install on iOS. This means that an app synced into Workspace ONE UEM can show as available for both iOS and tvOS in a single record. This also includes Custom Apps synced from Apple Business Manager.

For information on how to setup and deploy Apple Business Manager applications, see Deploy Volume Purchase Program. For assigning licenses, see Configure Licenses and Assign with Flexible Deployment.

Important Details for Public Apps on tvOS:

While tvOS apps are very similar to iOS, there are some details unique to tvOS that differ from deploying iOS apps.

- tvOS apps will always be deployed using device-based licenses. If device-based licenses have not been enabled for an app, iOS devices will be assigned user-based licenses while tvOS devices will be assigned device-based licenses.
- tvOS apps do not support VPN tunneling. Any VPN configuration will only apply to iOS devices the app is installed and not tvOS devices.
- tvOS apps can be set to **On Demand** for their App Delivery Method but there is no app catalog available on tvOS devices for users to manually install these apps. Admins will still be able to initiate installs to tvOS devices in the Workspace ONE UEM console.