

# iOS Device Management

VMware Workspace ONE UEM 2105

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](http://www.vmware.com)

Copyright © 2022 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

<b>1</b>	<b>Introduction to Managing iOS Devices</b>	<b>7</b>
	Supported iOS Devices	7
	iOS Admin Task Prerequisites	7
<b>2</b>	<b>Enroll iOS Devices</b>	<b>9</b>
	Enrollment Requirements	9
	Single Device Enrollment	9
	Hub-Based Enrollment	10
	Browser-Based Enrollment	10
	Bulk Device Enrollment	10
	iOS Device Enrollment Requirements	11
	Capabilities Based on Enrollment Type for iOS Devices	11
	Enroll an iOS Device with the Workspace ONE Intelligent Hub	13
	Enroll an iOS Device with the Safari Browser	14
	Bulk Enrollment of iOS Devices Using Apple Configurator	15
	Device Enrollment with the Apple Business Manager's Device Enrollment Program	16
	User Enrollment	16
<b>3</b>	<b>iOS Device Profiles</b>	<b>19</b>
	Configure an iOS Profile	20
	Device Passcode Profile for iOS	20
	Configure a Device Passcode Profile for iOS	21
	Restriction Profiles for iOS	21
	Device Restriction Profile for iOS	27
	Skip Setup Assistant Profile for iOS	27
	Wi-Fi Profile for iOS	28
	Virtual Private Network (VPN) Profile for iOS	29
	Forcepoint Content Filter for iOS	30
	VPN On Demand Profile for iOS	31
	Per-App VPN Profile for iOS	33
	Email Account Profile for iOS	34
	Notifications Profile for iOS	38
	LDAP Profile for iOS	38
	CalDAV or CardDAV Profile for iOS	39
	Subscribed Calendar Profile for iOS	39
	Web Clips Profile for iOS	39
	SCEP/Credentials Profile for iOS	40
	Global HTTP Proxy Profile for iOS	41

Single App Mode Profile for iOS	41
Web Content Filter Profile for iOS	43
Managed Domains Profile for iOS	45
Network Usage Rules for iOS	46
macOS Server Account Profile for iOS	46
Single Sign-On Profile for iOS	46
SSO Extension Profile for iOS	48
AirPlay Profile for iOS	49
AirPrint Profile for iOS	50
Cellular Profile for iOS	50
Home Screen Layout Profile (iOS Supervised)	51
Lock Screen Message Profile for iOS	51
Google Account Profile for iOS	52
Custom Settings Profile for iOS	52

## 4 Compliance Policies for iOS Devices 55

## 5 Apps for iOS Devices 56

Workspace ONE Intelligent Hub for iOS	57
Understanding the Certificate Exchange	57
Securing the Data in Transit	58
APIs and Application Functionality	58
Configure Workspace ONE Intelligent Hub Settings for iOS Devices**	58
VMware Workspace ONE Content	60
VMware Workspace ONE Web	60
VMware Workspace ONE Boxer	61
AirWatch Container for iOS	61
Enforcing Application-Level Single Sign On Passcodes	61
Apple Configurator Overview	62

## 6 Configure iOS Devices 64

Apple Industry Templates	64
Working with Profiles and Compliance Policies for Industry Templates	66
Create an Apple Industry Template	66
Edit Application Lists in Apple Industry Templates	67
Delete an Apple Industry Template	68

## 7 Apple iBeacon Overview 69

Requirements for iBeacon	69
iBeacon Operations Details	70
Enable iBeacon for iOS Devices	70

- Assign iBeacon Groups to Device Profiles 71
- Add Compliance Policies for iBeacon Groups 71

## 8 Activation Lock Overview 72

- Activation Lock for Unsupervised vs. Supervised Devices 72
- Enable Activation Lock for iOS Devices 73
- Viewing Activation Lock Status 73
- Clear Activation Lock on iOS Devices 73
- Use the Clear Activation Lock Command 74
- Enter an Activation Lock Bypass Code 74
- Perform a Device Wipe Command 74
- Activation Lock - Wipe Command Workflow Matrix 75

## 9 Remote View 76

- Prerequisites to initiate a Remote View 76
- Remote View Device Requirements 76
  - Configure the UEM Console with Remote View 76

## 10 Configure Managed Settings for iOS Devices 80

- Configure Organization Settings 81
- Override Default Roaming Settings (iOS) 82
- Set a Default Wallpaper 83
- Set Default Organization Information 83
- Install Fonts on iOS Devices 83
- Cisco QOS Marking for iOS Applications 84

## 11 Apple Push Notification Service (APNs) 85

- Apple Push Notification Service (APNs) Certificate 85
- Apple Push Notification Service Workflow 86

## 12 Device Management 87

- Device Dashboard 87
- Device List View 88
- Customize Device List View Layout 89
- Exporting List View 90
- Search in Device List View 90
- Device List View Action Button Cluster 90
- Remote Assist 90
- Using the Device Details Page for iOS Devices 91
- Configure and Deploy a Custom Command to a Managed Device 96

## **13 OS Update Management 98**

- iOS Update Management Features 99
- iOS Update Management Prerequisites 99
- Supported Devices 99
- Network Requirements 99
- View the Available iOS Updates 99
- Assign and Publish iOS Updates 100
- Pause and Unpause iOS Updates 101
- Monitor iOS Update Assignments 102
- Manage iOS Updates for Individual Devices 103
- Delay iOS Updates 103
- Set the Device Name for a Supervised iOS Device 104

## **14 AppleCare GSX 105**

- Create a GSX Account 105
- Obtain an Apple Certificate to Integrate AppleCare GSX 105
- Configure AppleCare in the UEM console 106
- Obtain an Apple Certificate to Integrate AppleCare GSX 106
- Configure AppleCare GSX in the UEM Console 106

## **15 Shared Devices 108**

- Define the Shared Device Hierarchy 109
- Configure Shared Devices 111
  - Log In and Log Out of Shared iOS Devices 112

## **16 iOS Functionality Matrix: Supervised vs. Unsupervised 114**

# Introduction to Managing iOS Devices

# 1

Workspace ONE UEM powered by AirWatch provides you with a robust set of mobility management solutions to enroll, secure, configure, and manage the iOS devices in your deployment.

Through the Workspace ONE UEM console you can:

- Manage the entire lifecycle of corporate and employee owned devices.
- Enable end users to perform tasks themselves including enrollment and by using the Self-Service Portal (SSP).
- Ensure that devices are compliant and secure by assigning profiles to specific groups and individuals in your organization.
- Integrate any of your existing enterprise apps with the Workspace ONE UEM Software Development Kit (SDK) to enhance their functionality.
- Use reporting tools and a searchable, customizable dashboard to perform ongoing maintenance and management of your device fleet.

This chapter includes the following topics:

- [Supported iOS Devices](#)
- [iOS Admin Task Prerequisites](#)

## Supported iOS Devices

Workspace ONE UEM supports iPhone, iPad, and iPod Touch devices running iOS 11.0 and higher. Certain Workspace ONE UEM and iOS features require later versions of the software. These additional requirements are noted in the documentation where applicable. For more information on supported versions, see KB article [here](#).

## iOS Admin Task Prerequisites

You need the following information to perform many of the tasks. Compile this information before proceeding.

- **UEM console** – Access to the UEM console with administrator permissions, which allows you to create profiles, policies, and manage devices within the Workspace ONE UEM environment.

- **Credentials** – This user name and password allow you to access your UEM console environment. These credentials may be the same as your network directory services or may be uniquely defined in the UEM console.
- **Apple Push Notification service (APNs) Certificate** – This certificate is issued to your organization to authorize the use of Apple's cloud messaging services.

# Enroll iOS Devices

# 2

Each device in your organization's deployment must be enrolled in your organization's environment before it can communicate with Workspace ONE UEM and access internal content and features using Mobile Device Management (MDM). iOS devices enroll using MDM functionality built into the native OS.

This chapter includes the following topics:

- [Enrollment Requirements](#)
- [Single Device Enrollment](#)
- [Hub-Based Enrollment](#)
- [Browser-Based Enrollment](#)
- [Bulk Device Enrollment](#)
- [iOS Device Enrollment Requirements](#)

## Enrollment Requirements

To enroll an iOS device, you or your end users must gather specific information. The information the users need depends on whether you associated an email domain to their environment as part of auto-discovery.

Associating an email domain with your environment requires end users to enter an email address and credentials (and sometimes select a Group ID from a list) to complete enrollment. This choice simplifies enrollment because end users likely already know this information.

Alternatively, if you do not set up an email domain for enrollment, users are additionally prompted for the Enrollment URL and Group ID, which admins must provide to them.

For more information on enrollment requirements, see *iOS Device Enrollment Requirements*.

## Single Device Enrollment

The device management capabilities available for enrolled devices depend on the type of enrollment you choose. Workspace ONE UEM provides a matrix comparing supported features for Hub-based and agentless enrollment types. Use this matrix to determine what type of enrollment meets your organization's needs.

For more information on the comparison matrix between Hub-based and browser-based enrollments, see *Capabilities Based on Enrollment Type for iOS Devices*.

## Hub-Based Enrollment

The Hub-based enrollment process secures a connection between iOS devices and your Workspace ONE UEM environment through the Workspace ONE Intelligent Hub app. The Workspace ONE Intelligent Hub application facilitates the enrollment, and then allows for real-time management and access to device information. Hub-based enrollment is best suited for deployments where users have an available Apple ID, which they must download the Workspace ONE Intelligent Hub from the App Store.

For more information on hub based enrollment, see *Workspace ONE Intelligent Hub for iOS and Enroll an iOS Device with Workspace ONE Intelligent Hub* in [Apps for iOS](#).

## Browser-Based Enrollment

You can also enroll devices using a web-based enrollment process through the iOS device's built-in Safari browser. This approach is best suited for deployments where users do not have an available Apple ID to download the Workspace ONE Intelligent Hub.

For more information on browser based enrollment, see *Enroll an iOS Device with the Safari Browser*.

## Bulk Device Enrollment

Depending on your deployment type and device ownership model, you may want to enroll devices in bulk. Workspace ONE UEM provides bulk enrollment capabilities using the Apple Configurator 2 and the Apple Business Manager's Device Enrollment Program (DEP).

### Bulk Enrollment with Apple Configurator 2

Workspace ONE UEM helps businesses take advantage of the unique setup capabilities offered by Apple Configurator 2, such as iOS versioning enforcement and complete backup prevention. You can bulk-enroll devices using Apple Configurator 2 on a macOS computer through a USB connection.

For more information on using Apple Configurator for bulk enrollment, see *Bulk Enrollment of iOS Devices Using Apple Configurator*.

### Bulk Enrollment with Apple Device Enrollment Program

Deploying a bulk enrollment through the Apple Device Enrollment Program (DEP) allows you to install a non-removable MDM profile on a device, which prevents end users from being able to remove the profile from their device. You can also provision devices in Supervised mode to access additional security and configuration settings.

For more information on enrollment with the Apple Business Manager, see *Device Enrollment with the Apple Business Manager's Device Enrollment Program*.

## iOS Device Enrollment Requirements

To enroll an iOS device, you or your end users need information that depends on whether you associate an email domain to their environment as part of auto discovery. **If an email domain is associated to their environment, users will need:**

**Email address** – Email address associated to your organization. For example, [JohnDoe@acme.com](mailto:JohnDoe@acme.com).

**QR Code** – Users can scan a QR code generated from the UEM console and received through email.

**Apple ID** – This Apple ID is needed for each user performing Hub-based enrollment.

**If an email domain is not associated to your environment:** If a domain is not associated to an environment, end users are prompted to enter an email address. Since auto discovery is not enabled, end users are also prompted for the following information:

**Enrollment URL** – This URL is unique to your organization's enrollment environment and takes the user directly to the enrollment screen. For example, <https://.com/enroll>.

**Group ID** – This Group ID associates a user's device with their corporate role and is defined in the UEM console for a given organization group. Point to the organization group drop-down menu to see the Group ID of the current group.

**Apple ID** – This Apple ID is needed for each user performing Hub-based enrollment.

## Capabilities Based on Enrollment Type for iOS Devices

Feature	Hub-Based	Agentless
Enrollment		
Requires Apple ID	Required	Optional
Force EULA/Terms of Use Acceptance	Yes	Yes
Active Directory/LDAP/SAML Integration	Yes	Yes
Two Factor Authentication	Yes	Yes
BYOD Support	Yes	Yes
Device Staging Support	Yes <sup>a</sup>	Yes
Branding	Partial	Yes
Configuration Profile Management		
View and Manage Profiles	Yes	Yes
Security Settings (Data Encryption, Password Policy, etc.)	Yes	Yes
Device Restrictions	Yes	Yes

Feature	Hub-Based	Agentless
Certificate Management	Yes	Yes
Email and Exchange ActiveSync management	Yes	Yes
Device Information		
Device Information (model, serial number, IMEI number, etc.)	Yes	Yes
GPS Tracking	Yes	No
Phone Number	Yes	Yes
Memory Information	Yes	Yes
Battery Information	Yes	Yes
UDID	Yes	Yes
Compromised/Jailbreak Detection	Yes	Yes†
Activation Lock Status	Yes	Yes
Find my iPhone Status	Yes	Yes
iCloud Back Up Status	Yes	Yes
Last Back Up Time	Yes	Yes
Network Information		
Cellular Information (MCC/MNC, SIM card info, etc.)	Yes	Yes
Telecom Roaming Information	Yes	Yes
Telecom Usage Information	Yes	Yes†
IP Address	Yes	Yes†
Bluetooth MAC address	Yes	Yes
Wi-Fi MAC address	Yes	Yes
Management Commands		
Full Device Wipe	Yes	Yes
Enterprise Wipe	Yes	Yes
Lock Device	Yes	Yes
Clear Passcode	Yes	Yes
Email Messaging	Yes	Yes
SMS Messaging	Yes	Yes
APNs Push Messaging	Yes	Yes†

Feature	Hub-Based	Agentless
Remote View	Yes	No
Set Device Name	Yes	Yes
Clear Restrictions Passcode	Yes	Yes
Application Management		
View and Manage Applications	Yes	Yes
Volume Purchase Program (VPP)	Yes	Yes
Application List	Yes	Yes
Number Badging for App Updates	Yes	Yes†
Content Management		
Content Management	Yes*	Yes*

° Requires end user to transfer purchases when syncing for first time.

† Requires Workspace ONE UEM SDK embedded application to be present on device.

\* Requires VMware Content Locker App from iTunes.

## Enroll an iOS Device with the Workspace ONE Intelligent Hub

The Hub-based enrollment process secures a connection between an iOS device and your Workspace ONE UEM environment. The Workspace ONE Intelligent Hub application facilitates enrollment and allows for real-time management and access to device information.

If you want to take full advantage of the Workspace ONE Intelligent Hub capabilities while also allowing the Web enrollment process, you can allow users to enroll through the Workspace ONE Intelligent Hub. This setting prevents the end users from enrolling if they have not downloaded the Workspace ONE Intelligent Hub.

Navigate to **Groups & Setting > All Settings > Devices & Users > General > Enrollment > Authentication**, and select the **Require Hub Enrollment for iOS**.

To enroll an iOS device with the Workspace ONE Intelligent Hub perform the following steps:

1. Navigate to **getwsone.com** from the Safari browser. Workspace ONE UEM automatically prompts the end user to go to the App Store and download the Workspace ONE Intelligent Hub application. Follow the download prompts. An Apple ID is required to download the Workspace ONE Intelligent Hub from the iTunes store.
2. Select the Workspace ONE Intelligent Hub application and then select either one of the following authentication methods:
  - a. **Email Address** – Select auto-discovery, if it is configured in your environment. In addition, you might be prompted to select a group from a drop-down menu.

- b. **Server Details** – Select to enroll using the server URL. The server URL is the network location of your organization's Workspace ONE UEM instance and the Group ID of the group associated with your device.
  - c. **QR Code** – Select and use the device to scan the QR code received through email or Support tab.
- 3 Enter credentials, which can include either a **Username** and **Password**, or a **Token**, or a combination of both to authenticate the device.
  - a. If you enter the credentials incorrectly, a Captcha code appears. Enter the displayed Captcha code to complete the authentication.
- 4 Complete the following process flow as determined by the administrator. Select **Next** after you complete each page.
  - a. Select your **Device Ownership** type, if applicable.
  - b. Accept your organization's **Terms of Use**, if applicable.
  - c. Enter the device **Asset Number**, if applicable.
- 5 Select **Next** after reviewing privacy collection information.
- 6 Once redirected to Safari webview, you are prompted to download the MDM profile. The following message is displayed:
 

This website is trying to download a configuration file. Do you want to allow this?
- 7 Tap **Allow** and when the download is complete, tap **Close**.
  - a. For iOS devices 12.2 and later, tap **Continue** and open Hub to follow the instructional screens to install the MDM profile and accept the MDM warning message by selecting **Install**.
  - b. For devices below iOS 12.2, install the MDM profile when prompted and accept the MDM warning message by selecting **Install**.
- 8 Select **Allow** to download the MDM profile.
- 9 Install the MDM profile. Accept any prompts for trust, if applicable.
- 10 Once MDM profile is installed, navigate back to Hub.
- 11 Select **Done** to complete enrollment. A success message is displayed. The enrollment into Workspace ONE UEM is now complete.
  - a. If prompted, set up a **passcode** or enter more credentials for shared devices. To set up a passcode, log in to the Self-Service Portal and follow the instructions.
  - b. Optionally, select **Open** to see the Workspace ONE Intelligent Hub details.

## Enroll an iOS Device with the Safari Browser

You can enroll devices using a web-based enrollment process through the iOS device's built-in Safari browser. This approach is best suited for deployments where users do not have an available Apple ID to download the Workspace ONE Intelligent Hub.

To enroll an iOS device using a web-based enrollment process perform the following steps:

- 1 Open the Safari browser on the iOS device.
- 2 Navigate to **https://<Environment\_URL>.com/enroll**.
- 3 Select **Group ID** or your **Email Address** (if auto-discovery is set up for your environment) to enroll your iOS device. Select **Next**.
- 4 Enter the credentials, which can include either a **Username** and **Password**, or a **Token**, or a combination of both to authenticate the device.
  - a. If you enter the credentials incorrectly, a Captcha code appears. Enter the displayed Captcha code to complete the authentication.
- 5 Complete the following process flow as determined by the administrator. Select **Next** after you complete each page.
  - a. Select your **Device Ownership** type, if applicable.
  - b. Enter the device **Asset Number**, if applicable.
  - c. Accept the **Terms of Use** of your organization, if applicable.
- 6 When prompted, download the MDM profile. The following message is displayed:  
This website is trying to download a configuration file. Do you want to allow?
- 7 Tap **Allow** and when the download is complete, tap **Close**.  
You have successfully installed the profile. You can view the profile in **Settings** and continue with installation.
- 8 Download and install the MDM profile. Accept any prompts for trust, if applicable.
  - For devices below iOS 12.2, install the MDM profile when prompted and accept the MDM warning message by selecting **Install**.
  - For devices iOS 12.2 and later, follow the instructional screens to install the MDM profile and accept the MDM warning message by selecting **Install**. **Note:** You can also perform an agentless enrollment without using the Workspace ONE Intelligent Hub for web-based enrollment. To perform an agentless enrollment, navigate to **Groups & Settings > All Settings > Devices & Users > General** and ensure that the **Require Hub Enrollment for iOS** check box is not selected.

## Bulk Enrollment of iOS Devices Using Apple Configurator

You can bulk enroll devices using Apple Configurator on a macOS computer to configure and deploy iOS devices. By using Apple Configurator with Workspace ONE UEM, you can benefit from maintained management visibility of devices, complete backup prevention, and continued life-cycle management beyond the initial configuration.

With Apple Configurator, you can:

- Prepare a single, central backup image to consistently mass-configure devices.

- Install the Workspace ONE UEM MDM profile as part of the configuration to enroll and manage devices.
- Assign devices to specific users by adding registered device details such as serial number or IMEI to a user's registered device in the UEM console before enrolling with Configurator.
- Configure and update corporate device settings and apps over-the-air in Workspace ONE UEM.

For steps to use Apple Configurator with Workspace ONE UEM or for more information, refer to the **VMware Workspace ONE UEM Integration with Apple Configurator** document.

## Device Enrollment with the Apple Business Manager's Device Enrollment Program

Device Enrollment Program (DEP) maximizes the benefits of Apple devices enrolled in Mobile Device Management (MDM).

With DEP, you can perform the following.

- Install a non-removable MDM profile on a device, preventing end users from being able to delete it.
- Provision devices in Supervised mode (iOS only). Devices in supervised mode can access additional security and configuration settings.
- Enforce an enrollment for all end users.
- Meet your organization's needs by customizing and streamline the enrollment process.
- Prevent iCloud back up by disabling users from signing in with their Apple ID when generating a DEP profile.
- Force iOS updates for all end users.

For more information, see the following topics:

- Apple Business Manager - Device Enrollment Program in *Introduction to Apple Business Manager*.
- The Apple [Business Support Portal](#).
- The Apple [Device Enrollment Program Guide](#), or contact your Apple representative.

## User Enrollment

User Enrollment is a new enrollment method for iOS 13 and later devices that allow you to effectively manage settings, applications, and corporate data while protecting user privacy and personal data. With User Enrollment, you are permitted to install applications, configure profiles, and issue commands only to a managed user container on the device rather than the entire device.

User Enrollment is achieved through MDM providing a user context called a Managed Apple ID in the MDM profile installed on the device during enrollment. The user context instructs the device to prompt the user for their Managed Apple ID credentials to install the MDM profile. After enrollment, a specific Apple File System (APFS) volume is created for the managed data. Data in the personal volume cannot be accessed from the managed volume keeping user data private.

Due to the creation of the new managed volume of data, there are several existing management capabilities that are not possible for privacy purposes. For example, if any app is manually installed by the user from the App Store, that app is considered personal and cannot be managed by MDM. Such user installed apps must first be uninstalled and then reinstalled by Workspace ONE UEM to be managed.

For this reason, Workspace ONE does not permit User Enrollment using the Intelligent Hub app. If the Intelligent Hub is already installed by the user, uninstall and reinstall the Hub through MDM so that the app's data can be accessed by other Workspace ONE SDK enabled apps.

### User Enrollment Settings

Enable the User Enrollment option for iOS devices by accessing the Enrollment settings page on the Workspace ONE UEM console (**Groups & Setting > All Settings > Devices & Users > General > Enrollment**). Enabling the option allows the supported iOS 13 and later devices to enroll to the Organization Group using Apple's User Enrollment method. User Enrollment uses the users' Managed Apple IDs rather than the enrollment user name as a way to indicate which user the device is enrolling. The Managed Apple ID should correspond a user's email address in Workspace ONE UEM.

**Enroll an iOS Device Using User Enrollment** Enroll an iOS 13 and later device using Managed Apple IDs in Apple Business Manager federated to Azure AD. User Enrolled device allows the enhanced privacy focus for users by separating managed data from personal while still providing the core management capabilities such as installing apps, configuring Wi-Fi, and requiring a passcode.

Ensure that you have the following pre-requisites before the User Enrollment:

- Apple Business Manager w/ federation to Azure AD
- Azure AD
- Unsupervised iOS 13 and later device
- Exactly one enrollment user with an email address that matches a Managed Apple ID in Apple Business Manager.

To enroll an iOS device:

- 1 Open the Safari browser on the iOS 13 or later device and navigate to your environment's User Enrollment URL. The URL is your device services hostname appended with the `/enroll/user` path.

For example:

`https://ds22.awmdm.com/enroll/user`

- 2 Enter the enrollment user's email address matching a Managed Apple ID.

Optionally, enter the Group ID of an Organization Group at or below the Organization Group of the enrollment user. Otherwise, the user's enrollment Organization Group is used.

- 3 Confirm the download of the User Enrollment MDM profile.
- 4 Navigate to **Settings** in the app and tap **Enroll in {Your Company}**.
- 5 Tap through the prompts to redirect to Azure AD for authentication and conditional access prompts.

Azure AD configurations, user type, device, or organization determines the type and number of prompts .

User Enrollment is now complete. The device starts receiving the commands from the UEM console.

### App Management on User Enrolled Devices

Applications installed by Workspace ONE UEM on the User Enrolled devices are managed and associated to the Managed Apple ID, that is used to enroll the device. Any application installed by the user through the App Store is associated to the user's personal Apple ID and cannot be managed.

Since User Enrollment must associate the managed application to a Managed Apple ID, only managed distribution with User-Based Licenses purchased in Apple Business Manager is supported. For example, applications assigned through the **Public** tab under the **Resources > Apps** page on the UEM console are not supported on User Enrolled devices. There are no differences between managing User-Based Licenses on User Enrollment compared to Device Enrollment. When the application is assigned to a User Enrolled device, a VPP license is assigned to the Managed Apple ID associated with the device and the app is installed.

For more information, refer the *Managed Distribution by Apple IDs* section in the *Integration with Apple Business Manager* guide.

# iOS Device Profiles

## 3

Profiles are the primary means to manage devices. Configure profiles so your iOS 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.

iOS profiles apply to a device at either the user level or the device level. When creating iOS profiles, you select the level the profile applies to. Some profiles can only be applied to the user level or device level.

### Supervised Mode Requirement for Profiles

You can deploy some or all your iOS devices in **Supervised mode**. Supervised mode is a device-level setting that provides administrators with advanced management capabilities and restrictions.

Certain profile settings are available only to supervised devices. A supervised setting is tagged using an icon displayed to the right, which indicates the minimum iOS requirement needed for enforcement.



For example, prevent end users from using AirDrop to share files with other macOS computers and iOS devices, by deselecting the check box next to **Allow AirDrop**. The **iOS 7 + Supervised** icon means only devices that are running iOS 7 and set up in Supervised mode using Apple Configurator are affected by this restriction. For more information, see **Integration with Apple Configurator** or the **Apple Business Manager**. To see a complete list of the iOS system requirements and supervision options, see **iOS Functionality Matrix: Supervised vs. Unsupervised**.

This chapter includes the following topics:

- [Configure an iOS Profile](#)
- [Device Passcode Profile for iOS](#)

- [Restriction Profiles for iOS](#)
- [Device Restriction Profile for iOS](#)
- [Skip Setup Assistant Profile for iOS](#)
- [Wi-Fi Profile for iOS](#)

## Configure an iOS Profile

Using the following basic steps you can configure any iOS profile in the Workspace ONE UEM. Explore the available settings for each profile in the following sections.

- 1 Navigate to **Resources > Profiles & Baselines > Profiles** and select **Add > Apple iOS > Device Profile**.
- 2 Configure the profile's **General** settings.
- 3 Select the payload from the list.
- 4 Configure the profile settings.
- 5 Select **Save and Publish**

## Device Passcode Profile for iOS

Device passcode profiles secure iOS devices and their content. Configure the level of security based on your users' needs.

Choose strict options for high-profile employees or more flexible options for other devices or for employees who are part of a BYOD program. In addition, when a passcode is set on an iOS device, it provides hardware encryption for the device and also creates a device indicator **Data Protection is Enabled** in the **Security** tab of the **Device Details** page.

Create a passcode and configure:

- **Complexity** – Use simple values for quick access or alphanumeric passcodes for enhanced security. You can also require a minimum number of complex characters (@, #, &, !, , , ?) in the passcode. For example, require users with access to sensitive content to use more stringent passcodes.
- **Maximum Number of Failed Attempts** – Prevent unauthorized access by wiping or locking the device after determined number of attempts. This option works well for corporate-owned devices, but not for employee-owned devices in a BYOD program. For example, if a device is restricted to five passcode attempts, and a user entered a passcode incorrectly five times in a row, then the device automatically performs a full device wipe. If simply locking the device is preferable, set this option to **None**, that implies you can attempt passcode retries indefinitely.
- **Maximum Passcode Age** – Enforce renewal of passcodes at selected intervals. Passcodes that are changed more frequently may be less vulnerable to exposure to unauthorized parties.

- **Auto-Lock (min)** – Lock the device automatically after a certain amount of time. This lock ensures content on the device is not compromised if an end user accidentally leaves a phone unattended.

## Configure a Device Passcode Profile for iOS

Device passcode profiles secure iOS devices and their content. Configure several settings as part of a passcode payload to enforce device passcodes based on your users' needs.

Setting	Description
Require passcode on device	Enable mandatory passcode protection.
Allow simple value	Allow the end user to apply a simple numeric passcode.
Require Alphanumeric Value	Restrict the end user from using spaces or non-alphanumeric characters in their passcode.
Minimum Passcode Length	Select the minimum number of characters required in the passcode.
Minimum number of complex characters	Select the minimum number of complex characters (#, \$, !, @) a passcode required.
Maximum Passcode Age (days)	Select the maximum number of days the passcode can be active.
Auto-lock (min)	Select the amount of time the device can be idle before the screen is locked automatically.
Passcode History	Select the number of passcodes to store in history that an end user cannot repeat.
Grace period for the device lock (min)	Select an amount of time in minutes that a device can be idle before it is locked by the system, and the end user must reenter their passcode.
Maximum Number of Failed Attempts	Select the number of attempts allowed. If the end user enters an incorrect passcode that many times, the device performs a factory reset.

## Restriction Profiles for iOS

**Restriction profiles** limit how employees can use their iOS devices and give administrators the ability to lock down the native functionality of iOS devices and enforce data-loss prevention.

Certain restriction options on the **Restrictions** profile page have an icon displayed to the right, which indicates the minimum iOS version required to enforce that restriction. For example, the **iOS 7 + Supervised** icon next to the **Allow AirDrop** check box means only devices running iOS 7 that are also set to run in Supervised mode using **Apple Configurator** or **Apple's Device Enrollment Program** are affected by this restriction.



The step-by-step instructions listed here list a few functional examples of settings you can restrict. To see a complete list of iOS version and supervised requirements, see [iOS Functionality Matrix: Supervised vs. Unsupervised](#).

## Configure a Device Restriction Profile for iOS

A restriction profile can be customized to control what applications, hardware, and functionality your end users can access. Use these restrictions to enhance productivity, protect end users and devices, and separate personal and corporate data.

To create a restriction profile, see *Configure a Device Restriction Profile*.

The following restrictions are a representative, but not exhaustive, list of options.

### OS Restrictions

OS level software delay restrictions which allow you to hide iOS updates from end users for a specified number of days.

Settings	Description
Delay Updates (Days)	Enable this option and specify the number of days to delay the software update. Number of days range from 1 to 90. (iOS 11.3 and later, Supervised devices). The number of days dictate the length of time after the release of the software update and not after the time of installation of the profile.

### Device Functionality Restrictions

Device-level restrictions can deactivate the core device functionality such as the camera, FaceTime, Siri, and in-app purchases to help improve productivity and security.

- Restrict end users from modifying device Bluetooth settings. (iOS 10 and later).
- Prohibit the device screen captures to protect the corporate content on the device.
- Deactivate Siri when the device is locked to prevent access to email, phone, and notes without the secure passcode (iOS 7 and later).

By default, end users can hold down the **Home** button to use Siri even when a device is locked. This feature can allow unauthorized users to gain access to the sensitive information and perform actions on a device they do not own. If your organization has strict security requirements, consider deploying a **Restrictions** profile that restricts the use of Siri while a device is locked.

- Prevent automatic syncing while roaming to reduce data charges.
- Prevents Touch ID from unlocking a device (iOS 7 and later).
- Restrict end users from modifying the personal hotspot setting on the device (iOS 12.2 and later, Supervised). Whether the restriction is enabled or deactivated in the profile, you can override the personal hotspot setting using the PersonalHotspot Managed Settings command.
- Restrict the end user's logging request on Siri servers. When the restriction is deactivated, Siri does not log end user logging data to the server.

- Restrict the end users from toggling on the Wi-Fi in the device's settings or control center (even when switching the Airplane Mode on or off) by enabling the **Force on Wi-Fi** on the UEM console (iOS 10.3 and later).
- Deactivate **Files Network Drive Access** to restrict the users from connecting to the network drives in the Files app (iOS 10.3 and later).

### Featured iOS 8 Device Restrictions

- Deactivate Handoff, which can be used to start an activity on one device, locate other devices and resume activities on shared apps.
- Deactivate Internet search results in Spotlight. This restriction prevents suggested Websites from appearing when searching using Spotlight. (iOS 8 and later, Supervised)
- Deactivate configuration of the Restrictions setting. This permission allows administrators to override configuration of personal restrictions through the device's Settings menu (iOS 8 and later, Supervised).
- Deactivate the end user from erasing all content and settings on the device. This restriction prevents users from wiping and unenrolling the device (iOS 8 and later, Supervised).
- Deactivate the local data storage by backing up managed apps with iCloud.
- Deactivate the backup of enterprise books with iCloud.
- Prevent users from syncing notes and highlights in enterprise books with iCloud.
- Deactivate adding or removing existing Touch ID information (iOS 8.1.3 and later, Supervised).
- Deactivate Podcasts. This restriction prevents access to Apple's podcasts application (Supervised only).

### Featured iOS 9 Restrictions

- Deactivate passcode modification, which prevents a device passcode from being added, changed or removed (Supervised only).
- Hide the App Store. This restriction deactivates the App Store and removes the icon from the Home Screen. End users can still use MDM to install or update their apps, giving full application control to the administrator (Supervised only).
- Deactivate automatic app download. This restriction prevents apps purchased on other devices from automatically syncing. This restriction does not affect updates to existing apps (Supervised only).
- Deactivate device name modification. This restriction prevents end users from changing the device name. Consider this restriction for shared and staged device deployments (Supervised only).
- Deactivate wallpaper modification. This restriction prevents the user from changing the device wallpaper (Supervised only).

- Deactivate AirDrop as an unmanaged drop destination, which prevents users from sending enterprise data or attachments from a managed application to AirDrop. This restriction also requires the restriction for Apple's managed open in feature.
- Deactivate keyboard shortcuts to prevent users from creating and using keyboard shortcuts (Supervised only).
- Deactivate News to prevent access to Apple's News application (Supervised only).
- Deactivate iCloud Photo Library. This restriction prevents photos that are not fully downloaded from the library from being stored locally.
- Deactivate trust of external enterprise apps, which prevents end users from installing any untrusted enterprise-signed, unmanaged apps. Managed in-house enterprise apps are implicitly trusted.
- Deactivate video recording by restricting screen capture to prevent end users from capturing the device display.
- Deactivate Music service, which restricts the Music app from installing (iOS 8.3.3+, Supervised only).

### **Featured iOS 9.3 Restrictions**

- Deactivate iTunes Radio service, which restricts iTunes Radio from installing. If Apple Music is not restricted, the Radio service shows in the Apple Music app (Supervised only).

### **Featured watchOS Restrictions**

- Deactivate Apple Watch pairing, which unpairs and erases any currently paired Apple Watch (iOS 9 and later, Supervised).
- Enforce Wrist Detection, which locks an Apple Watch when not being worn.

### **Application-Level Restrictions**

Application-level restrictions deactivates certain applications such as YouTube, iTunes, and Safari, or some of their features, to enforce corporate use policies. Available restrictions include:

- Deactivate Autofill to ensure that sensitive information does not automatically appear on certain forms.
- Enable the Force Fraud Warning feature to force Safari to display a warning when end users visit suspected phishing Websites.
- Control cookie acceptance in Safari. You can set Safari to not accept any cookies or to accept cookies only from specific sites.
- Forbid access to the Game Center and multiplayer gaming to enforce corporate policies for device use while at work.

- Activate or deactivate the individual, native, and other applications by adding them to the **Show Apps** or the **Hide Apps** section. This restriction enables you to show or hide applications as required (for iOS 9.3 and later, Supervised only).
  - For allowing the web clips, add the bundleID **com.apple.webapp** to the **Show Apps** text box.

## iCloud Restrictions

For devices running iOS 7 and later, end users can store, back up or sync data on their devices to the iCloud, a collection of Apple servers. This data includes photos, videos, device settings, app data, messages, documents, and more. To align with your business needs, Workspace ONE UEM provides restrictions for iOS 7 and later devices that can deactivate iCloud or iCloud functionality if needed.

Exchange ActiveSync content (Mail, Contacts, Calendars, Tasks) and any mobile provision profiles are not synchronized to an end user's iCloud.

Administrative Requirement	Restriction	Setting Deactivated on Device
Restrict iCloud Configuration (device functionality restriction)		
Restrict the ability to sign into and configure iCloud settings	Allow Account Modification (requires Supervision)	Deactivates iCloud option under device Settings (iOS 7 and later, Supervised) This restriction also prevents modification of other accounts such as email within device settings.
iCloud Management (granular iCloud restrictions)		
Prevent users from backing up data to iCloud	Allow backup	Turns off the "Backup" option under iCloud settings (iOS 7)
Prevent users from storing documents and data to iCloud Drive	Allow document sync	Removes "iCloud Drive" option under iCloud settings (iOS 7)
Prevent users from keeping password and credit card information in iCloud	Allow keychain sync	Removes "Keychain" option under iCloud Settings (iOS 7)
Prevent users of managed applications from storing documents to iCloud	Allow managed apps to store data	Deactivates managed applications from storing documents within iCloud drive (iOS 8)
Prevent users from backing up Enterprise books to iCloud	Allow backing up Enterprise books	Deactivates managed books from being backed up through iCloud or iTunes (iOS 8)
Prevent syncing of enterprise books, notes, highlights	Allow synchronizing Enterprise Books notes and highlights	Deactivates notes and highlights for Enterprise books within iBooks (iOS 8)
Prevent users from syncing photos to iCloud	Allow Photo Stream and Allow Shared Photo Stream	Remove the "Photos" option under iCloud Settings (iOS 7)
Prevent automatically uploading new photos and sending them to iCloud devices	Allow Shared Photo Stream	Deactivates "My Photo Stream" in "Photos" under iCloud Settings (iOS 7)

iCloud backups only take place when:

- No restriction exists on iCloud backup.
- The iCloud toggle setting is enabled in **Settings > iCloud > Backup** on the device.
- Wi-Fi is enabled.
- The device is connected to a power source and locked.

### Security and Privacy Restrictions

Security and privacy-based restrictions prohibit end users from performing certain actions that might violate corporate policy or otherwise compromise their device. Available restrictions include to:

- Prevent iOS 11.4.1 and later device users to enter passcode to initially connect or remain connected to USB accessories while the device is locked.
- Prevent user to trust unmanaged enterprise apps.
- Prevent force iTunes Store Password entry.
- Prevent diagnostic data, which includes location information and usage data, being sent to Apple to help improve the iOS software.
- Prevent end users from accepting untrusted TLS certificates so they cannot access Websites with invalid SSL certificates. If you permit untrusted TLS certificates, users are still notified of invalid certificates but can proceed if needed.
- Prevent over the air PKI updates.
- Force encrypted backups. Encrypted backups ensure all personal information, such as email account passwords or contact information, is encrypted when it is backed up and stored on devices.
- Prevent pairing with non-configurator hosts.
- Prevent iOS 10.3 and later devices from connecting to unknown or malicious networks. Devices enabled with this restriction can only connect to managed WiFi networks. Select **Require Managed Wi-Fi** to enforce this restriction.

### Media Content Restrictions

Ratings-based restrictions prevent access to certain content based on its rating, which is managed by region. Available restrictions include:

- Restrict access to adult or mature content on corporate-owned devices as part of a corporate policy.
- Prohibit access to apps with a 17+ age restriction during normal business hours.
- Block access to inappropriate or explicit iBook content on corporate-owned devices.

## Device Restriction Profile for iOS

**Restriction profiles** limit how employees use their iOS devices, and give administrators the ability to lock down the native functionality of iOS devices and enforce data-loss prevention.

- 1 Navigate to **Resources > Profiles & Baselines > Profiles > Add**. Select **Apple iOS**.
- 2 Configure the profile's **General** settings.
- 3 Select the **Restrictions** payload from the list. You can select multiple restrictions as part of a single restrictions payload.
- 4 Configure **Restrictions** settings. For more information on restrictions, see *Restriction Profile Configuration*.
- 5 Select **Save & Publish**.

## Skip Setup Assistant Profile for iOS

Use Setup Assistant profile to skip Setup Assistant screens on the device after an OS update. This profile is applicable only to iOS 14, iPadOS 14 and later.

Settings	Description
Setup Assistant	Select either skip all Setup Assistant screens after an OS update or skip selected screens from the list below. <b>Note:</b> By default, Skip all screens option is selected. When users select option to Skip some screens, the rest of the text boxes are editable.
Move from Android	If the Restore pane is not skipped, skips the Move from Android option in the Restore pane on iOS.
Choose Your Look	Skips the Choose Your Look screen.
Apple ID Setup	Skips Apple ID setup.
Biometric ID	Skips biometric setup. Device To Device Migration
Device To Device Migration	Skips Device to Device Migration pane.
Diagnostics	Skips the App Analytics pane.
Display Tone	Skips DisplayTone setup.
Home Button	Skips the Meet the New Home Button screen on iPhone 7, iPhone 7 Plus, iPhone 8, iPhone 8 Plus, and iPhone SE.
iMessage and FaceTime	Skips the iMessage and FaceTime screen in iOS.
Location Services	Skips Location Services.
Passcode	Skips the passcode pane.
Payment	Skips Apple Pay setup.
Privacy	Skips the privacy pane.
Restore	Deactivates restoring from backup restore.

Settings	Description
Restore Completed	Skips the Restore Completed pane.
Screen Time	Skips the Screen Time pane.
Add Cellular Plan	Skips the add cellular plan pane.
Siri	Skips Siri.
Software Update	Skips the mandatory software update screen in iOS.
Terms and Conditions	Skips Terms and Conditions.
Update Completed	Skips the Software Update Complete pane.
Watch Migration	Skips the screen for watch migration.
Welcome	Skips the Get Started pane.
Zoom	Skips zoom setup.

## Wi-Fi Profile for iOS

Configuring a Wi-Fi profile allows devices to connect to corporate networks, even if they are hidden, encrypted, or password protected. This payload is useful to end users who travel and use their own unique wireless network or to end users in an office setting where they are able to automatically connect their devices to a wireless network on-site.

- 1 Configure the wi-fi settings including:

Setting	Description
<b>Service Set Identifier</b>	Enter the name of the network where the device connects.
<b>Hidden network</b>	Enter a connection to a network that is not open or broadcasting.
<b>Auto-Join</b>	Determine whether the device automatically connects to the network when starting the device. The device keeps an active connection until the device is restarted or a different connection is chosen manually.
<b>Security Type</b>	Select the type of access protocol to be used. Enter the <b>Password</b> or select the <b>Protocols</b> that apply to your Wi-Fi network.
<b>Protocols</b>	Choose protocols for network access. This option appears when <b>WiFi</b> and <b>Security Type</b> is any of the <b>Enterprise</b> choices. This option also appears when <b>Ethernet</b> is selected.

Configure **Proxy** settings for either **Manual** or **Auto** proxy types.

If you use a Cisco infrastructure, configure the QoS Marking Policy (iOS v11 and higher).

Setting	Description
<b>Fastlane QoS Marking</b>	Select the marking setup that you require.
<b>Enable QoS Marking</b>	Select this option to choose apps for prioritized data allocations.
<b>Allow Apple Calling</b>	Select Allow Apple Calling to add Apple Wifi Calling to your QoS allowlist.
<b>Allow Apps for QoS Marking</b>	Search for and add Apps to allocate prioritized data.

Configure **Captive Portal** to bypass the portal.

Select **Save & Publish** when you are finished to push the profile to devices.

## Virtual Private Network (VPN) Profile for iOS

Virtual private networks (VPNs) provide devices with a secure and encrypted tunnel to access internal resources. VPN profiles enable each device to function as if it were connected through an on-site network. Configuring a VPN profile ensures that end users have the seamless access to email, files, and content.

The settings that you see may vary depending on the **Connection Type** you choose. For more information on using the Forcepoint content filtering, see *Creating a Forcepoint Content Filter Profile*.

Settings	Description
<b>Connection Name</b>	Enter the name of the connection to be displayed on the device.
<b>Connection Type</b>	Use the drop-down menu to select the network connection method.
<b>Server</b>	Enter the hostname or IP address of the server for connection.
<b>Account</b>	Enter the name of the VPN account.
<b>Send All Traffic</b>	Force all traffic through the specified network.
<b>Disconnect on Idle</b>	Allow the VPN to auto-disconnect after a specific amount of time. Support for this value depends on the VPN provider.
<b>Connect Automatically</b>	Select to allow the VPN to connect automatically to the following domains. This option appears when <b>Per App VPN Rules</b> is selected. Safari Domains Mail Domains Contacts Domains Calendar Domains
<b>Provider Type</b>	Select the type of the VPN service. If the VPN service type is an App proxy, the VPN service tunnels the traffic at the application level. If it is a Packet tunnel, the VPN service tunnels the traffic at the IP layer.
<b>Per App VPN Rules</b>	Enables the Per App VPN for devices. For more information, see <i>Configuring Per-App VPN for iOS Devices</i> in this guide
<b>Authentication</b>	Select the method to authenticate to end users. Follow the related prompts to upload an <b>Identity Certificate</b> , or enter a <b>Password</b> information, or the <b>Shared Secret</b> key to be provided to authorize end users for VPN access.

Settings	Description
<b>Enable VPN On Demand</b>	Enable VPN On Demand to use certificates to establish VPN connections automatically using the <i>Configuring VPN On Demand for iOS Devices</i> section in this guide.
<b>Proxy</b>	Select either <b>Manual</b> or <b>Auto</b> as the proxy type to configure with this VPN connection.
<b>Server</b>	Enter the URL of the proxy server.
<b>Port</b>	Enter the port used to communicate with the proxy.
<b>Username</b>	Enter the user name to connect to the proxy server.
<b>Password</b>	Enter the password for authentication.
<b>Vendor Keys</b>	Select to create custom keys to go into the vendor config dictionary.
<b>Key</b>	Enter the specific key provided by the vendor.
<b>Value</b>	Enter the VPN value for each key.
<b>Exclude Local Networks</b>	Enable the option to include all networks to route the network traffic outside the VPN.
<b>Include All Networks</b>	Enable the option to include all networks to route the network traffic through the VPN.

**Note:** If you have chosen IKEv2 as the type, you are eligible to enter the minimum and the maximum TLS version for the VPN connection. Provided that you enable the **Enable EAP** check box before you enter the TLS version.

After saving the profile, end users have access to permitted sites.

## Forcepoint Content Filter for iOS

With the Workspace ONE UEM integration with Forcepoint, you can use your existing content filtering categories in Forcepoint and apply them to devices you manage within the UEM console.

Allow or block access to websites according to the websites you configure in Forcepoint and then deploy a VPN payload to force devices to comply with those rules. Directory users enrolled in Workspace ONE UEM are validated against Forcepoint to determine which content filtering rules to apply based on the specific end user.

You can enforce content filtering with Forcepoint in one of following two ways.

- Use the **VPN** profile as described in this topic. Enforcing content filtering using VPN profile can be applied to all Web traffic using browsers other than the VMware Browser.
- Configure the **Settings and Policies** page, which applies to all Web traffic using browsers other than the VMware Browser. For instructions on configuring **Settings and Policies**, refer to the **VMware Browser Guide**.

### Procedure

- After you select the payload, then select **Websense (Forcepoint)** as the **Connection Type**.

- 2 Configure **Connection** Info including:

Settings	Description
<b>Connection Name</b>	Enter the name of the connection name to be displayed.
<b>Username</b>	Enter the user name to connect to the proxy server.
<b>Password</b>	Enter the password for connection.

- 3 You can also **Test Connection**.
- 4 Configure **Vendor Configurations** settings.

Setting	Description
<b>Vendor Keys</b>	Create custom keys and add to the vendor config dictionary.
<b>Key</b>	Enter the specific key provided by the vendor.
<b>Value</b>	Enter the VPN value for each key.

- 5 Select **Save & Publish**. Directory-based end users can now access permitted sites based on your Forcepoint categories.

## VPN On Demand Profile for iOS

VPN On Demand is the process of automatically establishing a VPN connection for specific domains. For increased security and ease of use, VPN On Demand uses certificates for authentication instead of simple passcodes.

Ensure your certificate authority and certificate templates in Workspace ONE UEM are properly configured for certificate distribution. Make your third-party VPN application of choice available to end users by pushing it to devices or recommending it in your enterprise App Catalog.

- 1 Configure your base VPN profile accordingly.
- 2 Select **Certificate** from the **User Authentication** drop-down menu. Navigate to the **Credentials** payload.
  - a. From the **Credential Source** drop-down menu, select **Defined Certificate Authority**.
  - b. Select the **Certificate Authority** and **Certificate Template** from the respective drop-down menus.
  - c. Navigate back to the **VPN** payload.
- 3 Select the **Identity Certificate** as specified through the **Credentials** payload if you are applying certificate authentication to the VPN profile.
- 4 Select the **Enable VPN On Demand** box.

- 5 Configure the **Use the New on Demand Keys (iOS 7)** to enable a VPN connection when end users access any of the domains specified:

Setting	Description
<b>Use new On Demand Keys (iOS 7 and higher)</b>	Select to use the new syntax that allows for specifying more granular VPN rules.
<b>On Demand Rule/Action</b>	Choose an <b>Action</b> to define VPN behavior to apply to the VPN connection based on the defined criteria. If the criterion is true, then the action specified takes place. <b>Evaluate Connection:</b> Automatically establish the VPN tunnel connection based on the network settings and on the characteristics of each connection. The evaluation happens every time the VPN connects to a Web site. <b>Connect:</b> Automatically establish the VPN tunnel connection on the next network attempt if the network criteria met. <b>Disconnect:</b> Automatically deactivate the VPN tunnel connection and do not reconnect on demand if the network criteria are met. <b>Ignore:</b> Leave the existing VPN connection, but do not reconnect on demand if the network criteria are met.
<b>Action Parameter</b>	Configure <b>Action Parameters</b> for specified domains to trigger a VPN connection attempt if domain name resolution fails, such as when the DNS server indicates that it cannot resolve the domain, responds with a redirection to a different server, or fails to respond (timeout). If choosing <b>Evaluate Connection</b> , these options appear: Choose <b>Connect If Needed/Never Connect</b> and enter additional information: <b>Domains</b> – Enter the domains for which this evaluation applies. <b>URL Probe</b> – Enter an HTTP or HTTPS (preferred) URL to probe, using a GET request. If the URL's hostname cannot be resolved, if the server is unreachable, or if the server does not respond with a 200 HTTP status code, a VPN connection is established in response. <b>DNS Servers</b> – Enter an array of DNS server IP addresses to be used for resolving the specified domains. These servers need not be part of the device's current network configuration. If these DNS servers are not reachable, a VPN connection is established in response. These DNS servers must be either internal DNS servers or trusted external DNS servers. (optional)
<b>Criteria/Value for Parameter</b>	<b>Interface Match</b> – Select the type of connection that matches device's network current adapter. Values available are <b>any</b> , <b>Wifi</b> , <b>Ethernet</b> , and <b>Cellular</b> . <b>URL Probe</b> – Enter the specified URL for criteria to be met. When criteria is met, a 200 HTTP status code is returned. This format includes protocol (https). <b>SSID Match</b> – Enter the device's current network ID. For the criteria to be met, it must match at least one of the values in the array. - Use the + icon to enter multiple SSIDs as needed. <b>DNS Domain Match</b> – Enter the device's current network search domain. A wildcard is supported (*.example.com). <b>DNS Address Match</b> – Enter the DNS address that matches the device's current DNS server's IP address. For criteria to be met, all the device's listed IP addresses must be entered. Matching with a single wildcard is supported (17.*).

- 6 Alternatively, choose legacy **VPN On Demand**:

Setting	Description
<b>Match Domain or Host</b>	On Demand Action <b>Establish if Needed</b> or <b>Always Establish</b> – Initiates a VPN connection only if the specified page cannot be reached directly. <b>Never Establish</b> – Does not establish a VPN connection for addresses that match the specified the domain. However, if the VPN is already active, it can be used.

- 7 Use the + icon to add more **Rules** and **Action Parameters** as desired.

8 Choose a **Proxy** type:

Setting	Description
<b>Proxy</b>	Select either <b>Manual</b> or <b>Auto</b> proxy type to configure with this VPN connection.
<b>Server</b>	Enter the URL of the proxy server.
<b>Port</b>	Enter the port used to communicate with the proxy.
<b>Username</b>	Enter the user name to connect to the proxy server.
<b>Password</b>	Enter the password for authentication.

9 Complete **Vendor Configurations**. These values are unique to every VPN provider.

Setting	Description
<b>Vendor Keys</b>	Select to create custom keys to add to the vendor config dictionary.
<b>Key</b>	Enter the specific key provided by the vendor.
<b>Value</b>	Enter the VPN value for each key.

- 10 Click **Save and Publish**. Once the profile installs on a user's device, a VPN connection prompt automatically displays whenever the user navigates to a site that requires it, such as SharePoint.

## Per-App VPN Profile for iOS

For iOS 7 and higher devices, you can force selected applications to connect through your corporate VPN. Your VPN provider must support this feature, and you must publish the apps as managed applications.

- 1 Configure your base VPN profile accordingly.
- 2 Select **Per-App VPN** to generate a VPN UUID for the current VPN profile settings. The VPN UUID is a unique identifier for this specific VPN configuration.
- 3 Select **Connect Automatically** to display text boxes for the **Safari Domains**, which are internal sites that trigger an automatic VPN connection.
- 4 Choose a **Provider Type** to determine how to tunnel traffic, either through an application layer or IP layer.
- 5 Select **Save & Publish**.

If saving was done as an update to an existing VPN profile, then any existing devices/applications that currently use the profile are updated. Any devices/applications that were not using any VPN UUID are also updated to use the VPN profile.

## Configure Public Apps to Use Per App Profile

After you create a per app tunnel profile, you can assign it to specific apps in the application configuration screen. This tells the application to use the defined VPN profile when establishing connections.

- 1 Navigate to **Resources > Apps > Native**.
- 2 Select the **Public** tab.
- 3 Select **Add Application** to add an app or **Edit** an existing app.
- 4 On the Deployment tab, select **Use VPN** and then select the profile you created.
- 5 Select **Save** and publish your changes.

For more information on adding or editing apps, see the **Mobile Application Management** guide.

## Configure Internal Apps to Use Per App Profile

After you create a per app tunnel profile you can assign it to specific apps in the application configuration screen. This tells the application to use the defined VPN profile when establishing connections.

- 1 Navigate to **Resources > Apps > Native**.
- 2 Select the **Internal** tab.
- 3 Select **Add Application** and add an app.
- 4 Select **Save & Assign** to move to the Assignment page.
- 5 Select **Add Assignment** and select **Per-App VPN Profile** in the **Advanced** section.
- 6 **Save & Publish** the app.

For more information on adding or editing apps, see **Mobile Application Management** guide in [VMware AirWatch documentation](#)

## Email Account Profile for iOS

Configure an email profile for iOS devices to configure email settings on the device.

Settings	Descriptions
<b>Account Description</b>	Enter a brief description of the email account.
<b>Account Type</b>	Use the drop-down menu to select either IMAP or POP.
<b>Path Prefix</b>	Enter the name of the root folder for the email account(IMAP only).
<b>User Display Name</b>	Enter the name of the end user.
<b>Email Address</b>	Enter the address for the email account.
<b>Prevent Moving Messages</b>	Select to block the user from forwarding email or opening in third-party apps.
<b>Prevent Recent Address Syncing</b>	Select to restrict the user from syncing email contacts to their personal device.

Settings	Descriptions
<b>Prevent Use in Third Party Apps</b>	Select to prevent users from moving corporate email into other email clients.
<b>Prevent Mail Drop</b>	Select to prevent users from using Apple's Mail Drop feature.
<b>Use S/MIME</b>	Select to use more encryption certificates.
<b>Host Name</b>	Enter the name of the email server.
<b>Port</b>	Enter the number of the port assigned to incoming mail traffic.
<b>Username</b>	Enter the user name for the email account.
<b>Authentication Type</b>	Use the drop-down menu to select how the email account holder is authenticated.
<b>Password</b>	Enter the password required to authenticate the end user.
<b>Use SSL</b>	Select to enable Secure Socket Layer use for incoming email traffic.
<b>Host Name</b>	Enter the name of the email server.
<b>Port</b>	Enter the number of the port assigned to outgoing mail traffic.
<b>Username</b>	Enter the user name for the email account.
<b>Authentication Type</b>	Use the drop-down menu to select how the email account holder is authenticated.
<b>Outgoing Password Same As Incoming</b>	Select to auto-populate the password text box.
<b>Password</b>	Enter the password required to authenticate the end user.
<b>Use SSL</b>	Select to enable Secure Socket Layer use for outgoing email traffic.

## Exchange ActiveSync (EAS) Mail for iOS Devices

The industry standard protocol designed for email synchronization on mobile devices is called **Exchange Active Sync (EAS)**. Through EAS profiles, you can remotely configure devices to check into your mail server to sync email, calendars and contacts.

The EAS profile uses information from each user, such as user name, email address, and password. If you integrate Workspace ONE UEM with Active Directory services, then this user information is automatically populated for the user and can be specified in the EAS profile by using look-up values.

## Create a Generic EAS Profile for Multiple Users

Before you create an EAS profile that automatically enables devices to pull data from your mail server, you must first ensure that users have the appropriate information in their user account records. For **Directory Users**, or those users that enrolled with their directory credentials, such as Active Directory, this information is automatically populated during enrollment. However, for **Basic Users** this information is not automatically known and must be populated in one of two ways:

- You can edit each user record and populate the **Email Address** and **Email Username** text boxes.
- You can prompt users to enter this information during enrollment by navigating to **Devices > Device Settings > General > Enrollment** and under the **Optional Prompt** tab, checking the **Enable Enrollment Email Prompt** box.

## Configure an EAS Mail Profile for the Native Mail Client

Create an email configuration profile for the native mail client on iOS devices.

- 1 Navigate to **Resources > Profiles & Baselines > Profiles > Add**. Select **Apple iOS**.
- 2 Configure the profile's **General** settings.
- 3 Select the **Exchange ActiveSync** payload.
- 4 Select **Native Mail Client** for the **Mail Client**. Fill in the **Account Name** text box with a description of this mail account. Fill in the **Exchange ActiveSync Host** with the external URL of your company's ActiveSync server.

The ActiveSync server can be any mail server that implements the ActiveSync protocol, such as Lotus Notes Traveler, Novell Data Synchronizer, and Microsoft Exchange. In the case of Secure Email Gateway (SEG) deployments, use the SEG URL and not the email server URL.

- 5 Select the **Use SSL** check box to enable Secure Socket Layer use for incoming email traffic.
- 6 Select the **S/MIME** check box to use more encryption certificates. Prior to enabling this option, ensure you have uploaded necessary certificates under **Credentials** profile settings.
  - a. Select the **S/MIME Certificate** to sign email messages.
  - b. Select the **S/MIME Encryption Certificate** to both sign and encrypt email messages.
  - c. Select the **Per Message Switch** check box to allow end users to choose which individual email messages to sign and encrypt using the native iOS mail client (iOS 8+ supervised only).
- 7 Select the **Use OAuth** check box to enable OAuth for authentication. OAuth is required for modern authentication-enabled accounts.
  - a. **OAuth Sign In URL** - Enter the OAuth Sign In URL.
  - b. **OAuth Token URL** - Enter the OAuth Token URL.

- 8 Fill in the **Login Information** including **Domain Name, Username and Email Address** using look-up values. Look-up values pull directly from the user account record. To use the {EmailDomain}, {EmailUserName} {EmailAddress} look-up values, ensure your Workspace ONE UEM user accounts have an email address and email user name defined.
- 9 Leave the **Password** field empty to prompt the user to enter a password.
- 10 Select the **Payload Certificate** to define a certificate for cert-based authentication after the certificate is added to the **Credentials** payload.
- 11 Configure the following **Settings and Security** optional settings, as necessary:
  - a. **Past Days of Mail to Sync** – Downloads the defined amount of mail. Note that longer time periods will result in larger data consumption while the device downloads mail.
  - b. **Prevent Moving Messages** – Disallows moving mail from an Exchange mailbox to another mailbox on the device.
  - c. **Prevent Use in 3rd Party Apps** – Disallows other apps from using the Exchange mailbox to send message.
  - d. **Prevent Recent Address Syncing** – Deactivates suggestions for contacts when sending mail in Exchange.
  - e. **Prevent Mail Drop** – Deactivates use of Apple's Mail Drop feature.
  - f. (iOS 13) **Enable Mail** – Enables the configuration of a separate Mail app for the Exchange account.
  - g. (iOS 13) **Allow Mail toggle** – If deactivated, prevents the user to toggle Mail on or off.
  - h. (iOS 13) **Enable Contacts** – Enables the configuration of a separate Contacts app for the Exchange account.
  - i. (iOS 13) **Allow Contacts toggle** – If deactivated, prevents the user to toggle Contacts on or off.
  - j. (iOS 13) **Enable Calendars** – Enables the configuration of a separate Calendar app for the Exchange account.
  - k. (iOS 13) **Allow Calendars toggle** – If deactivated, prevents the user to toggle Calendars on or off.
  - l. **Enable Notes** – Enables the configuration of a separate Notes app for the Exchange account.
  - m. (iOS 13) **Allow Notes toggle** – If deactivated, prevents the user to toggle Notes on or off.
  - n. (iOS 13) **Enable Reminders** – Enables the configuration of a separate Reminders app for the Exchange account.
  - o. (iOS 13) **Allow Reminders toggle** – If deactivated, prevents the user to toggle Reminders on or off.

- 12 Assign a **Default Audio Call App** that your Native EAS account will use to make calls when you select a phone number in an email message.
- 13 Select **Save and Publish** to push the profile to available devices.

## Notifications Profile for iOS

Use this profile to allow notifications for specific apps to appear on the home screen when it is locked.

Control when and how the notifications appear. This profile applies to iOS 9.3 + Supervised devices.

- 1 Choose **Select App**. A new window appears.

Setting	Description
<b>Select App</b>	Choose the app that you want to configure.
<b>Allow Notifications</b>	Select whether to allow any notifications.
<b>Show in Notification Center</b>	Select whether to allow notifications to appear in the Notification Center.
<b>Show in Lock Screen</b>	Select whether to allow notifications to appear in the lock screen.
<b>Allow Sound</b>	Select whether to allow a sound to occur with the notification.
<b>Allow Badging</b>	Select whether to allow badges to appear on the application icon.
<b>Alert Style when Unlocked</b>	Choose the style for the notification when unlocked: <b>Banner</b> - A banner appears across the home screen alerting the user. <b>Modal Alert</b> - A window appears across the home screen. The user must interact with the window before proceeding.

- 2 Select **Save** to push the payload to the device.

## LDAP Profile for iOS

Configure an LDAP profile to allow end users to access and integrate with your corporate LDAPv3 directory information.

Setting	Description
<b>Account Description</b>	Enter a brief description of the LDAP account.
<b>Account Hostname</b>	Enter/view the name of the server for Active Directory use.
<b>Account Username</b>	Enter the user name for the Active Directory account.
<b>Account Password</b>	Enter the password for the Active Directory account.
<b>Use SSL</b>	Select this check box to enable Secure Socket Layer use.
<b>Search Settings</b>	Enter settings for Active Directory searches ran from the device.

## CalDAV or CardDAV Profile for iOS

Deploy a CalDAV or CardDAV profile to allow end users to sync corporate calendar items and contacts, respectively.

Setting	Description
<b>Account Description</b>	Enter a brief description of the account.
<b>Account Hostname</b>	Enter/view the name of the server for CalDAV use.
<b>Port</b>	Enter the number of the port assigned for communication with the CalDAV server.
<b>Principal URL</b>	Enter the Web location of the CalDAV server.
<b>Account Username</b>	Enter the user name for the Active Directory account.
<b>Account Password</b>	Enter the password for the Active Directory account.
<b>Use SSL</b>	Select to enable Secure Socket Layer use.

## Subscribed Calendar Profile for iOS

Push calendar subscriptions using the native Calendar app in macOS to your iOS devices by configuring this payload.

Configure the calendar settings, including:

Setting	Description
<b>Description</b>	Enter a brief description of the subscribed calendars.
<b>URL</b>	Enter the URL of the calendar to which you are subscribing.
<b>Username</b>	Enter the user name of the end user for authentication purposes.
<b>Password</b>	Enter the password of the end user for authentication purposes.
<b>Use SSL</b>	Check to send all traffic using SSL.

## Web Clips Profile for iOS

Web Clips are Web bookmarks that you can push to devices that display as icons on the device springboard or in your app catalog.

Configure **Web Clip** settings, including:

Setting	Description
<b>Label</b>	Enter the text displayed beneath the Web Clip icon on an end user's device. For example: "AirWatch Self-Service Portal."
<b>URL</b>	Enter the URL of the Web Clip that displays. Here are some examples for Workspace ONE UEM pages: For the SSP, use: <code>https://{Airwatch Environment}/mydevice/</code> For the app catalog, use: <code>https://{Environment}/Catalog/ViewCatalog/{SecureDeviceUdid}/{DevicePlatform}</code> For the book catalog, use: <code>https://{Environment}/Catalog/BookCatalog?uid={DeviceUUID}</code>
<b>Removable</b>	Enable device users to use the long press feature to remove the Web Clip off their devices.
<b>Icon</b>	Select this option to upload as the Web Clip icon. Upload a custom icon using a .gif, .jpg, or .png format, for the application. For best results, provide a square image no larger than 400 pixels on each side and less than 1 MB when uncompressed. The graphic is automatically scaled and cropped to fit and converted to .png format, if necessary. Web Clip icons are 104 x 104 pixels for devices with a Retina display or 57 x 57 pixels for all other devices.
<b>Precomposed Icon</b>	Select this option to display the icon without any visual effects.
<b>Full Screen</b>	Select this option to run the Web page in full screen mode.

## SCEP/Credentials Profile for iOS

Even if you protect your corporate email, Wi-Fi and VPN with strong passcodes and other restrictions, your infrastructure may remain vulnerable to brute force and dictionary attacks, in addition to employee error. For greater security, you can implement digital certificates to protect corporate assets.

To assign certificates, you must first define a certificate authority. Then, configure a **Credentials** payload alongside your **Exchange ActiveSync (EAS)**, **Wi-Fi**, or **VPN** payload. Each of these payloads has settings for associating the certificate authority defined in the **Credentials** payload.

To push down certificates to devices, you must configure a **Credentials** or **SCEP** payload as part of the profiles you created for EAS, Wi-Fi, and VPN settings. Use the following instructions to create a certificate-enabled profile:

1. Navigate to **Resources > Profiles & Baselines > Profiles > Add** and select **iOS** from the platform list.
2. Configure the profile's **General** settings.
3. Select either the **EAS**, **Wi-Fi**, or **VPN** payload to configure. Fill out the necessary information, depending on the payload you selected.
4. Select the **Credentials** (or **SCEP**) payload.
5. Choose one option from the **Credentials Source** menu:
  - a. Choose to **Upload** a certificate and enter the **Certificate Name**.
  - b. Choose **Defined Certificate Authority** and select the appropriate **Certificate Authority** and **Certificate Template**.
  - c. Choose **User Certificate** and the use for the **S/MIME** certificate.

- d. Choose **Derived Credentials** and select the appropriate **Key Usage** based on how the certificate is used. Key Usage options are **Authentication**, **Signing**, and **Encryption**.
- 6 Navigate back to the previous payload for **EAS**, **Wi-Fi**, or **VPN**.
- 7 Specify the Identity Certificate in the payload:
  - a. **EAS** – Select the **Payload Certificate** under Login Information.
  - b. **Wi-Fi** – Select a compatible **Security Type** (WEP Enterprise, WPA/WPA2 Enterprise or Any (Enterprise)) and select the **Identity Certificate** under Authentication.
  - c. **VPN** – Select a compatible **Connection Type** (for example, CISCO AnyConnect, F5 SSL) and select **Certificate** from the User Authentication drop-down. Select the **Identity Certificate**.
- 8 Navigate back to **Credentials** (or **SCEP** ) payload.
- 9 Select **Save & Publish** after configuring any remaining settings.

## Global HTTP Proxy Profile for iOS

Configure a global HTTP proxy to direct all HTTP traffic from Supervised iOS 7 and higher devices through a designated proxy server. For example, a school can set a global proxy to ensure that all web browsing is routed through its Web content filter.

Configure Proxy settings including:

Setting	Description
<b>Proxy Type</b>	Choose <b>Auto</b> or to <b>Manual</b> for proxy configuration.
<b>Proxy Server</b>	Enter the URL of the proxy server. This text box displays when the <b>Proxy Type</b> is set to <b>Manual</b> .
<b>Proxy Server Port</b>	Enter the port used to communicate with the proxy. This text box displays when the <b>Proxy Type</b> is set to <b>Manual</b> .
<b>Proxy Username/ Password</b>	If the proxy requires credentials, you can use look-up values to define the authentication method. This text box displays when the <b>Proxy Type</b> is set to <b>Manual</b> .
<b>Allow bypassing proxy to access captive networks</b>	Select this check box to allow the device to bypass proxy settings to access a known network. This text box displays when the <b>Proxy Type</b> is set to <b>Manual</b> .
<b>Proxy PAC File URL</b>	Enter the URL of the Proxy PAC File to apply its settings automatically. This text box displays when the <b>Proxy Type</b> is set to <b>Auto</b> .
<b>Allow direct connection if PAC is unreachable</b>	Select this option to have iOS devices bypass the proxy server if the PAC file is unreachable. This text box displays when the <b>Proxy Type</b> is set to <b>Auto</b> .
<b>Allow bypassing proxy to access captive networks</b>	Select this check box to allow the device to bypass proxy settings to access a known network. This text box displays when the <b>Proxy Type</b> is set to <b>Auto</b> .

## Single App Mode Profile for iOS

Use Single App Mode to provision devices so they can only access a single app of choice. Single App Mode deactivates the home button and forces the device to boot directly into the designated app if the user attempts a manual restart.

This feature ensures that the device is not used for anything outside of the desired application and has no way of accessing unintended other apps, device settings, or an Internet browser. This feature is useful for restaurants and retail stores. For education, students can use devices that are locked access to a single game, eBook, or exercise.

An iOS 7 or higher device configured in Supervised mode. (iOS 7 and higher is required for extra options and autonomous single app mode.)

Configure Single App mode settings including:

Setting	Description
<b>Filter Type</b>	Choose a filter, either <b>Lock device into a single app</b> or <b>Permitted apps for autonomous single app mode</b> : <b>Lock device into a single app</b> – Lock devices into a single public, internal, purchased, or native application until the profile with this payload is removed. The home button is deactivated, and the device always returns to the specified application from a sleep state or reboot. <b>Permitted apps for autonomous single app mode</b> – Enable allowed applications to trigger Single App Mode based on an event that controls when to turn on and off Single App Mode on the device. This action happens within the app itself as determined by the app developer.
<b>Application Bundle ID</b>	Enter the bundle ID or select one from the drop-down menu. The bundle ID appears in the drop-down menu after the application has been uploaded to the UEM console. For example: com.air-watch.secure.browser.
<b>Optional Settings</b>	Choose optional settings for Supervised iOS 7 and higher devices.

Once you save the profile, each device provisioned with this profile enters Single App Mode.

### Restart a Device Operating in Single App Mode

The hard reset procedure is used to restart a device operating in Single App Mode.

- 1 Press and hold the Home button and the Sleep/Wake button simultaneously.
- 2 Continue holding both buttons until the device shuts off and begins to restart.
- 3 Let go when you see the silver Apple logo. It may take a while for the device to load from the Apple logo to the main screen.

### Exit Single App Mode on iOS Devices

End users cannot exit the app when Single App Mode is enabled. Workspace ONE UEM provides two options for exiting single app mode, depending on which Single App Mode you enable.

You can deactivate Single App Mode temporarily if you need to update the specified app to a new version or release. Deactivate Single App Mode using the instructions below, install the new app version, and enable Single App Mode again.

#### Procedure

- 1 Navigate to **Resources > Profiles & Baselines > Profiles**. In the row for the **Single App Mode** profile, select the **View Devices** icon.
- 2 Select **Remove Profile** for the device from which you want to remove the setting.
- 3 Update the application to the desired version.

#### 4 Re-install the profile using the steps under **Configure Single App Mode**

##### **Allow Device Admin to Exit Single App Mode from the Device**

You can allow an admin to exit Single App Mode with a passcode on the device itself. This option is only available if you enable autonomous single app mode as the Filter Type for the Single App Mode profile.

##### **Procedure**

- 1 Navigate to **Resources > Profiles & Baselines > Profiles > Add**. Select **Apple iOS**.
- 2 Configure the profile's **General** settings.
- 3 Select the **Single App Mode** payload.
- 4 With **Permitted apps for autonomous single app mode** selected, enter the bundle ID of an application that supports autonomous single app mode under **Permitted Applications**.
- 5 Select **Save & Publish** to push this profile to the assigned devices.
- 6 Navigate to **Resources > Apps > Native > Public** for public apps, or **Resources > Apps > Native > Purchased for apps managed through VPP**.
- 7 Locate the autonomous single app mode supported application and select the Edit Assignment icon. The Edit Application window displays.
- 8 Select the Assignment tab and expand the **Policies** section.
- 9 Select **Enabled** for **Send Application Configuration**, enter AdminPasscode as the **Configuration Key**, and set the **Value Type** to **String**.
- 10 Enter the passcode admins use to exit Single App Mode as the Configuration Value. The value can be numeric or alphanumeric. Select **Add**.
- 11 Select **Save and Publish** to push the application configuration.

## **Web Content Filter Profile for iOS**

You can allow or prevent end users from accessing specific URLs using a Web browser by configuring a Web content filter payload that is applied to devices. All URLs must begin with http:// or https://. If necessary, you must create separate entries for both the HTTP and HTTPS versions of the same URL. The Web content filter payload requires iOS 7+ supervised devices.

Select **Filter Type** drop-down menu:

- 1 Built-in: Allow Web sites
- 2 Built-in: Deny Web sites
- 3 Plug-in

##### **Built-in: Allow Web Sites**

Configure an allowlist of URLs to allow end users to access only these specific Web sites on the list and prevent them from accessing any other Web sites.

- 1 Select **Built-in: Allow Websites** in the **Filter Type** drop-down menu to choose what plug-ins can be accessed.
- 2 Select **Add** and configure a list of allowed Web sites:

Setting	Description
<b>Allowed URLs</b>	The URL of a allowed site.
<b>Title</b>	The bookmark title.
<b>Bookmark Path</b>	The folder into which the bookmark is added in Safari.

### Built-in: Deny Web Sites

Configure a denylist of URLs to prevent users from accessing the specified Web sites. However, all other Web sites remain available to end users. Also, Web sites with profanity are automatically filtered unless an exception is permitted.

Select **Built-in: Deny Website** in the **Filter Type** drop-down menu and configure denied Web sites:

Setting	Description
<b>Denied URLs</b>	Enter <b>Denied URLs</b> and separate with new lines, spaces, or commas.
<b>Automatically filter inappropriate Web sites</b>	Select to filter adult Web sites.
<b>Bookmark Path</b>	Enter the folder path into which the bookmark is added in Safari.
<b>Permitted URLs</b>	Enter any Web sites that may be allowed as exceptions to the automatic filter.

### Plug-ins

This payload allows you to integrate with a third-party Web content filtering plug-in with Safari.

If you want to integrate specifically with Forcepoint or Blue Coat content filters, see the appropriate sections in this guide.

- 1 Select **Plug-in** in the **Filter Type** drop-down menu to choose what plug-ins can be accessed. You must enable either Webkit or Socket traffic needs in order for the payload to work.

Setting	Description
<b>Filter Name</b>	Enter the name of filter that displays on the device.
<b>Identifier</b>	Enter the bundle ID of the identifier of the plug-in that provides filtering service.
<b>Service Address</b>	Enter the hostname, IP address, or URL for service.
<b>Organization</b>	Choose the organization string that is passed to the third party plug-in.

Setting	Description
<b>Filter WebKit Traffic</b>	Select to choose whether to filter Webkit traffic.
<b>Filter Socket Traffic</b>	Select to choose whether to filter Socket traffic.

- 2 Configure the **Authentication** information including:

Setting	Description
<b>Username</b>	Use look-up values to pull directly from the user account record. Ensure your Workspace ONE UEM user accounts have an email address and email user name defined.
<b>Password</b>	Enter the password for this account.
<b>Payload Certificate</b>	Choose the authentication certificate.

- 3 Add **Custom Data** which includes keys required by the third-party filtering service. This information goes into the vendor config dictionary.
- 4 Select **Save & Publish**.

## Managed Domains Profile for iOS

Managed domains are another way Workspace ONE UEM enhances Apple's "open in" security feature on iOS 8 devices. Using the "open in" feature with managed domains, you can protect corporate data by controlling what apps can open documents downloaded from enterprise domains using Safari.

Specify URLs or subdomains to manage how documents, attachments, and downloads from the browser are opened. Also, in managed email domains, a color-coded warning indicator can be displayed in email messages that are sent to unmanaged domains. These tools help end users quickly determine what documents can be opened with corporate apps and what documents are personal and may be opened in personal applications.

Setting	Description
<b>Managed Email Domains</b>	Enter domains to specify which email addresses are corporate domains. For example: <b>exchange.acme.com</b> . Emails sent to addresses not specified here are highlighted in the email app to indicate that the address is not part of the corporate domain.
<b>Managed Web Domains</b>	Enter domains to choose specific URLs or subdomains that can be considered managed. For example: <b>sharepoint.acme.com</b> . Any documents or attachments coming from those domains are considered managed.
<b>Safari Password Domains</b>	Enter password for the domains you specify for Safari to save. This option is applicable only for supervised devices.

## Network Usage Rules for iOS

Configure network usage rules to control which applications and SIM cards can access data based on the network connection type or when the device is roaming. This feature allows administrators to help manage data charges when employees are using devices for work. Use granular controls to apply different rules to different apps and SIMs as needed.

- 1 Under the App Usage Rules, enter the **Application Identifier** of any public, internal, or purchased applications.
- 2 Enable **Allow Cellular Data** and **Data Usage on Roaming**. Both options are selected by default.
- 3 Under the SIM Usage Rules, provide the **ICCID**s of SIM cards (physical and eSIM cards) and specify the type of **Wi-Fi Assist** capability, either **Default** or **Unlimited Cellular Data**.
- 4 Select **Save & Publish**.

## macOS Server Account Profile for iOS

Add an macOS server account directly from the UEM console to help manage your MDM framework. Use to provide the credentials to allow end users to access File Sharing on macOS.

Setting	Description
<b>Account Description</b>	Enter the display name for the account.
<b>Hostname</b>	Enter the server address.
<b>User Name</b>	Enter the user's login name.
<b>Password</b>	Enter the user's password.
<b>Port</b>	Designates the port number to use when contacting the server.

## Single Sign-On Profile for iOS

Enable single sign-on for corporate apps to allow seamless access without requiring authentication into each app. Push this profile to authenticate end users through Kerberos authentication instead of storing passwords on devices. For more information on single sign-on settings, refer to the **VMware Workspace ONE UEM Mobile Application Management Guide**.

- 1 Enter **Connection Info**:

Setting	Description
<b>Account Name</b>	Enter the name that appears on the device.
<b>Kerberos Principal Name</b>	Enter the Kerberos principal name.

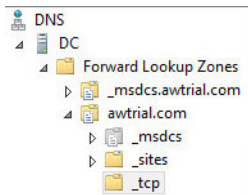
Setting	Description
Realm	Enter the Kerberos domain realm. This parameter must be fully capitalized.
Renewal Certificate	On iOS 8+ devices, select the certificate used to reauthenticate the user automatically without any need for user interaction when the user's single sign-on session expires. Configure a renewal certificate (for example: .pfx) using a credentials or SCEP payload.

- 2 Enter the **URL Prefixes** that must be matched to use this account for Kerberos authentication over HTTP. For example: **http://sharepoint.acme.com/**. If left empty, the account is eligible to match all HTTP and HTTPS URLs.
- 3 Enter the **Application Bundle ID** or select one from the drop-down menu. The bundle ID appears in this drop-down menu after the application has been uploaded to the UEM console. For example: **com.air-watch.secure.browser**. The applications specified must support Kerberos authentication.
- 4 Select **Save & Publish**.

In the example of a Web browser, when end users navigate to a Web site specified in the payload, they are prompted to enter the password of their domain account. Afterward, they do not have to enter credentials again to access any of the Web sites specified in the payload.

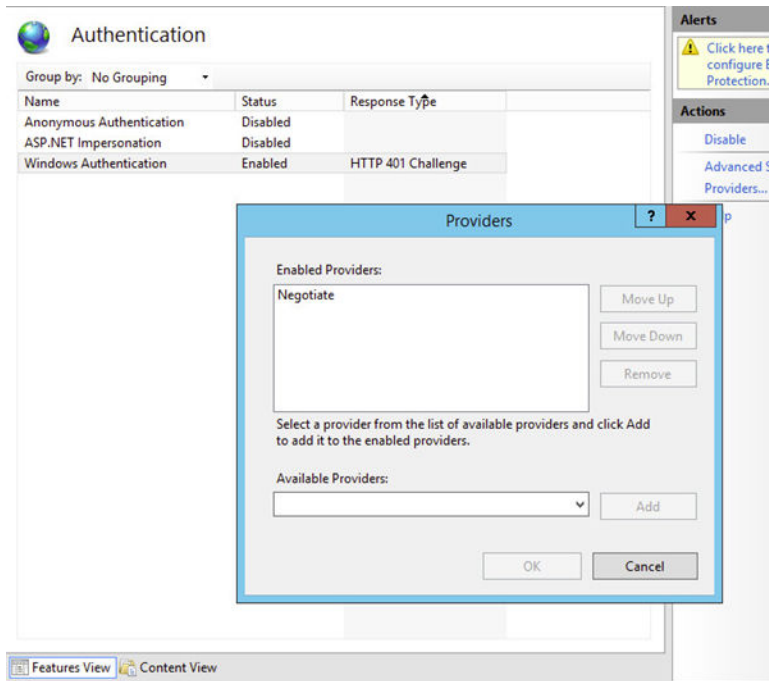
**Note:**

- Using Kerberos authentication, devices must be connected to the corporate network (either using corporate Wi-Fi or VPN).
- The DNS server must have a record of the Kerberos services (KDC server).



Name	Type	Timestamp
_gc	Service Location (SRV)	10/3/2013 6:00:00 AM
<b>_kerberos</b>	Service Location (SRV)	10/3/2013 6:00:00 AM
_kpasswd	Service Location (SRV)	10/3/2013 6:00:00 AM
_ldap	Service Location (SRV)	10/3/2013 6:00:00 AM

- Both the application on the mobile device and the Web site must support Kerberos/Negotiate authentication.



## SSO Extension Profile for iOS

To configure an application on device to perform single sign-on (SSO) with the Kerberos extension, configure the SSO Extension profile. With the SSO Extension profile, users do not have to provide their user name and password to access specific URLs. This profile is applicable only to iOS 13 and later devices.

Setting	Description
<b>Extension Type</b>	Select the type of the SSO extension for the application. If Generic is selected, provide the Bundle ID of the application extension that performs SSO for the specified URLs in the <b>Extension Identifier</b> field. If Kerberos is selected, provide the Active Directory Realm and Domains.
<b>Type</b>	Select either Credential or Redirect as extension type. Credentials extension is used for the challenge/response authentication. Redirect extension can use OpenID Connect, OAuth, and SAML authentication.
<b>Team Identifier</b>	Enter the Team Identifier of the application extension that performs SSO for the specified URLs.
<b>URLs</b>	Enter one or more URL prefixes of identity providers where the application extension performs SSO.
<b>Additional Settings</b>	Enter additional settings for the profile in XML code which is added to the ExtensionData node.
<b>Active Directory Realm</b>	This option appears only if Kerberos is selected as the Extension Type. Enter the name for the Kerberos Realm.
<b>Domains</b>	Enter the host names or the domain names which can be authenticated through the application extension.
<b>Use Site Auto-Discovery</b>	Enable the option to make the Kerberos extension to automatically use LDAP and DNS to determine the Active Directory site name.

Setting	Description
<b>Allow Automatic Login</b>	Enable the option to allow passwords to be saved to the keychain.
<b>Require User Touch ID or Password</b>	Enable the option to allow the user to provide Touch ID, FaceID, or passcode to access the keychain entry.
<b>Certificate</b>	Select the certificate to push down to the device which is in the same MDM profile.
<b>Allowed Bundle IDs</b>	Enter a list of application bundle IDs to allow access to the Kerberos Ticket Granting Ticket (TGT).

## AirPlay Profile for iOS

Configuring the AirPlay payload lets you allow a specific set of devices to receive broadcast privileges according to device ID. Also, if the display access to your Apple TV is password-protected, you can pre-enter the password to create a successful connection without revealing the PIN to unauthorized parties.

This payload works even if you do not enroll your Apple TVs with Workspace ONE UEM. For more information about tvOS capabilities, see **tvOS Management** guide.

**Note:** AirPlay allowlist currently only pertains to supervised iOS 7 and iOS 8 devices.

- 1 Configure **Passwords** settings for iOS 7 devices and **Allowlists** for iOS 7 + Supervised devices:

Setting	Description
<b>Device Name</b>	Enter the device name for the AirPlay destination.
<b>Password</b>	Enter the password for AirPlay destination. Select <b>Add</b> to include additional allowed devices.
<b>Display Name</b>	Enter the name of the destination display. The name must match the tvOS device name and is case-sensitive. The device name can be found on the tvOS device settings. (iOS 7 + Supervised)
<b>Device ID</b>	Enter the device ID (include the MAC address or Ethernet address formatted as XX:XX:XX:XX:XX:XX) for the destination display. Select <b>Add</b> to include additional allowed devices. (iOS 7 + Supervised)

- 2 Now that the AirPlay destination allowlist is established for iOS 7 + Supervised devices, use the Device Control Panel to activate or deactivate AirPlay manually:
  - a. Navigate to **Devices > List View** and locate the device intending to AirPlay, and select the device's Friendly Name.
  - b. Select **Support** and select **Start AirPlay** from the list of support options.
  - c. Choose the **Destination** created in the AirPlay profile, enter the **Password** if necessary and select the **Scan Time**. Optionally, select **Custom** from the Destination list to create a custom destination for this particular device.
  - d. Select **Save** and accept the prompt to enable AirPlay.

- 3 To deactivate AirPlay manually on the device, return to the device's Control Panel, select **Support** and select **Stop AirPlay**.

## AirPrint Profile for iOS

Configure an AirPrint payload for an Apple device to enable computers automatically to detect an AirPrint printer even if the device is on a different subnet than the AirPrint printer.

Setting	Description
IP address	Enter the IP address (XXX.XXX.XXX.XXX).
Resource Path	Enter the Resource Path associated with the AirPrint printer (ipp/printer or printers/Canon_MG5300_series). To find the Resource Path and IP address information of a printer, see the <i>Retrieve AirPrint Printer Information</i> section.

### Retrieve AirPrint Printer Information

To know the AirPrint printer's information such as IP address and Resource path, perform the steps mentioned in this section.

- 1 Connect an iOS device to the local network (subnet) where the AirPrint printers are located.
- 2 Open the Terminal window (located in /Applications/Utilities/), enter the following command and then press Return.

```
ippfind
```

**Note:** Make a note of the printer information that is fetched through the command. The first part is the name of your printer and the last part is the resource path.

```
ipp://myprinter.local.:XXX/ipp/portX
```

- 3 To get the IP address, enter the following command and the name of your printer.

```
ping myprinter.local.
```

**Note:** Make a note of the IP address information that is fetched through the command.

```
PING myprinter.local (XX.XX.XX.XX)
```

- 4 Enter the IP address (XX.XX.XX.XX) and resource path (/ipp/portX) obtained from the steps 2 and 3 into the AirPrint payload settings.

## Cellular Profile for iOS

Configure a cellular payload to configure cellular network settings on devices and determine how your device accesses the carrier's cellular data network.

Push this payload to use a different APN from the default point. If your APN settings are incorrect you may lose functionality, so find out the correct APN settings from your carrier. For more information on cellular settings, see [Apple's knowledge base article](#).

Setting	Description
<b>Access Point Name (APN)</b>	Enter the APN provided by your carrier (For example: come.moto.cellular).
<b>Authentication Type</b>	Select the authentication protocol.
<b>Access Point Username</b>	Enter the user name used for authentication.
<b>Access Point Password</b>	Enter the APN password used for authentication.
<b>Access Point Name</b>	Enter the APN provided by your carrier (For example: come.moto.cellular).
<b>Access Point Username</b>	Enter the user name used for authentication.
<b>Authentication Type</b>	Select the authentication protocol.
<b>Password</b>	Enter the APN password used for authentication.
<b>Proxy Server</b>	Enter the proxy server details.
<b>Proxy Server Port</b>	Enter the proxy server port for all traffic. Select <b>Add</b> to continue this process.

## Home Screen Layout Profile (iOS Supervised)

Use this payload to customize the Home Screen. Enabling this feature allows you to group applications in ways that meet your organization's needs.

When the payload is pushed to the device, the home screen is locked so users cannot change your custom configuration. This payload applies to iOS 9.3 + Supervised devices.

Setting	Description
<b>Dock</b>	Choose what applications you want to appear in the dock.
<b>Page</b>	Choose applications you want to add to the device. You can also add more pages for more groups of applications.
<b>Add Folder</b>	Configure a new folder to add to the device screen on the selected page. - Use the <b>pencil icon</b> in the gray bar to create or edit the name of the folder.

Select **Add Page** to add more pages to the device if needed and select **Save & Publish** to push this profile to devices.

## Lock Screen Message Profile for iOS

Customize the Lock Screen of your end users' devices with information that may help you retrieve devices that are lost.

Setting	Description
"If lost return to" Message	Display a name or organization to whom a found device should be returned. This field supports lookup values.
Asset Tag Information	Display the device asset tag information on the device lock screen. This asset tag may duplicate or replace a physical asset tag attached to the device. This field supports lookup values.

## Google Account Profile for iOS

Enable an end user to use their Google account on their iOS device Native Mail application. Add a Google Account directly from the UEM console.

Setting	Description
Account Name	The full user name for the Google account. This is the user name that appears when you send a mail message.
Account Description	A description of the Google account, which appears in Mail and Settings.
Email Address	The full Google email address for the account.
Default Audio Call App	Search and select an application that will be the default app for making any calls made from configured Google account.

## Custom Settings Profile for iOS

The **Custom Settings** payload can be used when Apple releases new iOS functionality or features that Workspace ONE UEM does not currently support through its native payloads. If you do not want to wait for the newest release of Workspace ONE UEM to control these settings, you can use the **Custom Settings** payload and XML code to enable or deactivate certain settings manually.

You might want to copy your profile and save it under a "test" organization group to avoid affecting users before you are ready to Save and Publish. Do not assign a profile to any smart group as it might give an encrypted value when viewing XML.

- 1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > iOS**.
- 2 Configure the profile's **General** settings.
- 3 Configure the appropriate payload (for example, Restrictions or Passcode).
- 4 Select **Save and Publish**.

**Note:** Ensure that the profile created in Steps 1–4 is not assigned to any smart group. Otherwise, the data might be encrypted when viewing xml.

- 5 Navigate back to the Profiles page and select a profile using the radio button next to the profile name. Menu options appear above the list.
- 6 Select **</> XML** from the menu choices. A **View Profile XML window** appears.

- Find and copy the section of text starting with <dict>...</dict> that you configured previously, for example, Restrictions or Passcode. This text contains a configuration type identifying its purpose, for example, restrictions. You must copy a single dictionary content inside the PayloadContent as shown in the example.

```
<plist version="1.0">
  <dict>
    <key>PayloadContent</key>
    <array>
      <dict>
        <key>safariAcceptCookies</key>
        <real>2</real>
        <key>safariAllowAutoFill</key>
        <true />
        <key>PayloadDisplayName</key>
        <string>Restrictions</string>
        <key>PayloadDescription</key>
        <string>RestrictionSettings</string>
        <key>PayloadIdentifier</key>
        <string>745714ad-e006-463d-8bc1-495fc99809d5.Restrictions</string>
        <key>PayloadOrganization</key>
        <string></string>
        <key>PayloadType</key>
        <string>com.apple.applicationaccess</string>
        <key>PayloadUUID</key>
        <string>9dd56416-dc94-4904-b60a-5518ae05ccde</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
      </dict>
    </array>
    <key>PayloadDescription</key>
    <string></string>
    <key>PayloadDisplayName</key>
    <string>Block Camera/V_1</string>
    <key>PayloadIdentifier</key>
    <string>745714ad-e006-463d-8bc1-495fc99809d5</string>
    <key>PayloadOrganization</key>
    <string></string>
    <key>PayloadRemovalDisallowed</key>
    <false />
    <key>PayloadType</key>
    <string>Configuration</string>
    <key>PayloadUUID</key>
    <string>86a02489-58ff-44ff-8cd0-faad7942f64a</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
  </dict>
</plist>
```

For more examples and information on the XML code, refer to the KB article [here](#).

- If you see encrypted text between dict tags in the XML window, you can generate the decrypted text by modifying the settings in the profiles page. To do this:

- a. Navigate to **Groups & Settings > All Settings > Devices > Users > Apple > Profiles**.
  - b. Override the custom settings option.
  - c. Deactivate Encrypt Profiles option and then Save.
- 9 Navigate back to **Custom Settings** profile and paste the XML you copied in the text box. The XML code you paste should contain the complete block of code, from <dict> to </dict>.
  - 10 Remove the original payload you configured by selecting the base payload section, for example, Restrictions, Passcode and selecting the minus [-] button. You can now enhance the profile by adding custom XML code for the new functionality.
  - 11 Select **Save and Publish**.

# Compliance Policies for iOS Devices

## 4

The compliance engine is an automated tool by Workspace ONE UEM powered by AirWatch that ensures all devices abide by your policies. These policies can include basic security settings such as requiring a passcode and having a minimum device lock period.

For certain platforms, you can also decide to set and enforce certain precautions. These precautions include setting password strength, denylisting certain apps, and requiring device check-in intervals to ensure that devices are safe and in-contact with Workspace ONE UEM. Once devices are determined to be out of compliance, the compliance engine warns users to address compliance errors to prevent disciplinary action on the device. For example, the compliance engine can trigger a message to notify the user that their device is out of compliance.

In addition, devices not in compliance cannot have device profiles assigned to it and cannot have apps installed on the device. If corrections are not made in the amount of time specified, the device loses access to certain content and functions that you define. The available compliance policies and actions vary by platform.

For more information about compliance policies, including which policies and actions are supported for a particular platform, see the **Managing Devices** documentation on [docs.vmware.com](https://docs.vmware.com).

# Apps for iOS Devices

# 5

Combine Workspace ONE UEM MDM features with Workspace ONE UEM apps to even further enhance security and functionality. Easily manage Workspace ONE UEM apps throughout the entire lifecycle across employee-owned, corporate-owned, and shared devices from the UEM console.

Workspace ONE UEM applications allow you and your end users to:

- Explore the VMware Workspace ONE Content to sync a personal content folder.
- Configure VMware Workspace ONE Web to secure Internet searches.
- Enable VMware Workspace ONE Boxer to configure email.
- Use the AirWatch Container as an alternative to MDM by providing separation of corporate and personal data on device, while maintaining employee privacy.

For more information about managing applications, see **Mobile Application Management**.

This chapter includes the following topics:

- [Workspace ONE Intelligent Hub for iOS](#)
- [Understanding the Certificate Exchange](#)
- [Securing the Data in Transit](#)
- [APIs and Application Functionality](#)
- [VMware Workspace ONE Content](#)
- [VMware Workspace ONE Web](#)
- [VMware Workspace ONE Boxer](#)
- [AirWatch Container for iOS](#)
- [Enforcing Application-Level Single Sign On Passcodes](#)
- [Apple Configurator Overview](#)

## Workspace ONE Intelligent Hub for iOS

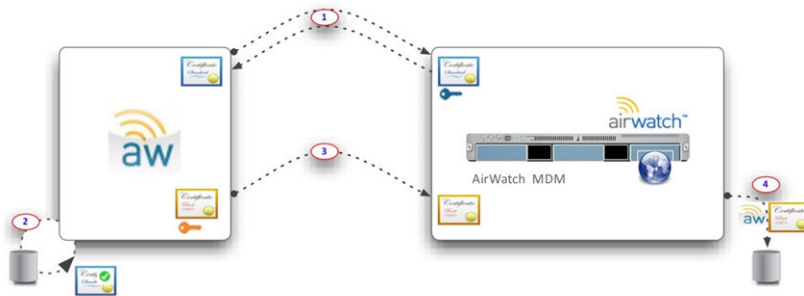
The Workspace ONE Intelligent Hub for iOS collects and delivers managed device information to the UEM console. Because this information may contain sensitive data, Workspace ONE UEM takes extensive measures to ensure that the information is encrypted and that it originates from a trusted source.

Workspace ONE UEM uses a unique certificate pair to sign and encrypt all communication between Workspace ONE Intelligent Hub for iOS and the server. These certificates also allow the server to verify the identity and authenticity of each device enrolled in Workspace ONE UEM. This overview details the benefits and necessities of both security enhancements.



## Understanding the Certificate Exchange

Before any data is transferred, the Workspace ONE Intelligent Hub application and the server trade personalized certificates. This relationship is established when Workspace ONE Intelligent Hub for iOS checks into the Workspace ONE UEM server for the first time during enrollment.



- 1 Workspace ONE Intelligent Hub for iOS communicates with the Workspace ONE UEM server to obtain the server's certificate public key. Both Workspace ONE Intelligent Hub for iOS and the Workspace ONE UEM server trust the public key of the Workspace ONE UEM Root certificate, which verifies the authenticity of all certificates involved in the enrollment exchange.
- 2 Workspace ONE Intelligent Hub for iOS validates the server's certificate against the Workspace ONE UEM Root CA certificate.
- 3 Workspace ONE Intelligent Hub for iOS sends a unique certificate public key to the Workspace ONE UEM server.
- 4 The Workspace ONE UEM server associates the Workspace ONE Intelligent Hub's certificate with that device in the database.

## Securing the Data in Transit

After the initial exchange of certificates, all data sent to the UEM console is encrypted from that point forward. The following table shows the two certificates involved and their responsibility in the transaction.

	Hub Certificate	Server Certificate
Workspace ONE Intelligent Hub	Sign the Data	Encrypt the Data
Workspace ONE UEM Server	Verify the Data Origin	Decrypt the Data

## APIs and Application Functionality

There are two categories of APIs that Workspace ONE UEM uses with iOS devices for management and tracking capabilities:

- **Over-the-Air (OTA) MDM APIs** are activated through the enrollment process regardless if Workspace ONE Intelligent Hub for iOS is used or not.
- **Native iOS SDK APIs** are available to any third-party application, including Workspace ONE Intelligent Hub applications and any other application using the Workspace ONE UEM Software Development Kit (SDK).

The Workspace ONE Intelligent Hub for iOS acts as the broker application that integrates with the Native iOS SDK API layer of management. When using Workspace ONE Intelligent Hub for iOS combined with the Workspace ONE UEM SDK for iOS, administrators can take advantage of more MDM features for applications, more so than what is offered in the Over-the-Air (OTA) MDM API layer.

- **Configure Workspace ONE Intelligent Hub Settings for iOS Devices** You can customize the Workspace ONE Intelligent Hub settings in the UEM console. For example, specify an SDK Profile to use with the Workspace ONE Intelligent Hub to harness Workspace ONE UEM functionality.
- **Workspace ONE Intelligent Hub Mobile Application for iOS** After enrolling the Workspace ONE Intelligent Hub, the application defaults to a **My Device** screen. Here you can view real-time information about your device, sync the device, re-enroll the device, and read messages that have been sent from the UEM console.

## Configure Workspace ONE Intelligent Hub Settings for iOS Devices\*\*

You can customize the Workspace ONE Intelligent Hub settings in the UEM console. For example, specify an SDK Profile to use with the Workspace ONE Intelligent Hub to harness Workspace ONE UEM functionality.

### Procedure

- 1 Navigate to **Devices > Device Settings > Apple > Apple iOS > Hub Settings**.

## 2 Configure the following settings for the Workspace ONE Intelligent Hub:

Setting	Description
<b>Disable Un-Enroll in Hub</b>	This setting deactivates the user's ability to unenroll from Workspace ONE UEM MDM using the Workspace ONE Intelligent Hub. This setting is only available in the Workspace ONE Intelligent Hub v4.9.2 and higher.
<b>Background App Refresh</b>	This setting tells the Workspace ONE Intelligent Hub the maximum allowed time interval to refresh app content. Some applications run for a brief period before reaching a suspended state. Background App Refresh is a feature in iOS where the application itself wakes from this suspended state. During this refresh, the Workspace ONE Intelligent Hub reports information, such as compromised detection, hardware details, GPS, iBeacon, and telecom, to the UEM console. The frequency at which the Workspace ONE Intelligent Hub refreshes is controlled by the OS and only completed during efficient times, such as when the device is plugged into a power source, frequency of use, or connected to Wi-Fi. To take advantage of the Background App Refresh feature, this setting must be enabled in the UEM console, the Workspace ONE Intelligent Hub cannot be stopped on the device, and Background App Refresh must be enabled on the device for the Workspace ONE Intelligent Hub under <b>Settings &gt; General &gt; Background App Refresh</b> .
<b>Minimum Refresh Interval</b>	Select the minimum amount of time that must pass before the device attempts to refresh app content.
<b>Transmit on Wi-Fi only</b>	Enable background refresh to occur over Wi-Fi connections only.

- 1 Customize the following extra configurations for the Workspace ONE Intelligent Hub from the **Settings and Policies** page in the UEM console for **Single Sign On** in this guide.

### What to do next

For information about offline access, branding, and other Settings and Policies, refer to the **VMware AirWatch Mobile Application Management Guide**.

### Workspace ONE Intelligent Hub Mobile Application for iOS

After enrolling the Workspace ONE Intelligent Hub, the application defaults to a **My Device** screen. Here you can view real-time information about your device, sync the device, re-enroll the device, and read messages that have been sent from the UEM console.

The **Self Service Enabled** check box must be selected in the **Hub Settings** in the UEM console to see all the status information.

**Note:** If the **Disable Un-enroll Hub** option is not checked in **Hub Settings**, select **Un-enroll Device** before re-enrolling with the Workspace ONE Intelligent Hub v4.9.2.

### My Device Functionality

- Tap the **Status** menu to view various statuses and self-service diagnostic options:
  - **Sync Device** – Tap this action to send a request to resync the device with the UEM console.
  - **Current Status** – Use the menus to find information about enrollment, re-enroll the device, view accounts, and compliance.

- **Diagnostics** – Use these menus to test connectivity, view Internet access, connectivity issues, server information, and view and send Hub and Device logs.
- Tap the **Device Details** menu to view various status options:
  - **Network** – View network adapters and IP addresses.
  - **Advanced** – Use these menus to find information about the device's battery, memory, and disk space.
  - **Location**– View GPS coordinates for your device for the current and previous time periods
  - **iBeacon** – View the name of the iBeacon region. If iBeacon is configured but location data is not configured, then the device displays only the iBeacon area. If iBeacon and location data are enabled, then the device displays the iBeacon region and the map with the location on the device.
- Use the **dock** at the bottom of the screen to find additional information including:
  - **Messages**– Read notifications from the UEM console. For example, you may receive notifications in the message center to complete a required compliance check to ensure that your device can be successfully monitored.
  - **About** – Find information about the Workspace ONE Intelligent Hub application and legal information.

## VMware Workspace ONE Content

VMware Workspace ONE Content is an application that enables your end users to access important content on their devices while ensuring file safety for your organization.

From the Workspace ONE Content, end users can access content you upload in the UEM console, content from synced corporate repositories, or their own personal content.

Use the UEM console to add content, sync repositories and configure the actions that end users can take on content opened within the application. These configurations prevent content from being copied, shared, or saved without approval.

For more information about MCM and configuring the VMware Workspace ONE Content, see the **VMware Workspace ONE UEM Mobile Content Management Guide**.

## VMware Workspace ONE Web

VMware Workspace ONE Web is an application that provides a manageable and secure alternative to native Web browsers. You can secure the browsing experience on an application, tunnel, and Web site level.

You can configure the Workspace ONE Web to meet unique business needs by restricting Web access to Web sites and providing a secure Internet portal for mobile point-of-sale devices. Provide users with a standard browsing experience, including support of multi-tabbed browsing and JavaScript dialog box. For maximum security on your Android and iOS devices, consider deploying the Workspace ONE Web with a Restrictions profile blocking the native browser.

For additional information about preparing and configuring the Workspace ONE Web for deployment, see the **VMware Workspace ONE Web Admin Guide**.

## VMware Workspace ONE Boxer

VMware Workspace ONE Boxer is an email application that offers a consumer-centric focus on mobile productivity with enterprise-grade security in the form of AES 256-bit encryption. This app containerizes business data from personal data, providing frictionless access to enterprise email, calendar, and contacts across corporate-owned and employee owned.

Workspace ONE Boxer allows users to personalize the app to meet their needs with features like custom swipe gestures, contact avatars, custom smart folders, and account color preferences. The all-in-one email, calendar, and contacts app provides an intuitive user experience following native design paradigms on devices.

For more information on VMware Workspace ONE Boxer, see the **VMware Workspace ONE Boxer Admin Guide**.

## AirWatch Container for iOS

AirWatch Container offers a flexible approach to Bring Your Own Device (BYOD) management by pushing a secure work space to a personal device. Businesses can distribute Workspace ONE UEM applications and internal applications to the AirWatch Container for employees to use on their mobile devices.

Applications are visible inside and outside the AirWatch Container, but the enterprise applications are secure through a common SDK framework and a container passcode. These apps can interact seamlessly using single sign on authentication and can connect securely to the Internet through an app tunnel VPN.

For more information about the AirWatch Container, refer to the **VMware AirWatch Container Admin Guide**.

## Enforcing Application-Level Single Sign On Passcodes

Single sign on (SSO) allows end users to access Workspace ONE UEM apps, wrapped apps, and SDK-enabled apps without entering credentials for each application. Using the Workspace ONE Intelligent Hub or the AirWatch Container as a "broker application," end users authenticate once per session using their normal credentials or an SSO Passcode.

Enable SSO as part of the **Security Policies** that you configure to apply to all Workspace ONE UEM apps, wrapped apps, and SDK-enabled apps using a Default SDK Profile.

- 1 Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.
- 2 Set **Single Sign On** to **Enabled** to allow end users to access all Workspace ONE UEM applications and maintain a persistent login.
- 3 **Authentication Type** to **Passcode** and set the **Passcode Mode** to either **Numeric** or **Alphanumeric** to require an SSO Passcode on the device. If you enable SSO but do not enable an Authentication Type, end users use their normal credentials (either directory service or Workspace ONE UEM account) to authenticate, and an SSO Passcode does not exist.

Once an end user authenticates with an application participating in SSO, a session establishes. The session is active until the **Authentication Timeout** defined in the SDK profile is reached or if the user manually locks the application.

## Apple Configurator Overview

Workspace ONE UEM integrates with Apple Configurator to enable you to supervise and manage scaled deployments of Apple iOS devices. Administrators can create configuration profiles, import existing profiles from the iPhone Configuration Utility, install specific operating system versions and enforce iOS device security policies.

Install and run Apple Configurator 2 from a macOS laptop to integrate with the Workspace ONE UEM console to supervise and configure one or many devices at the same time.

- Install the Workspace ONE UEM MDM profile as part of the configuration to enroll devices silently.
- Supervise dedicated line-of-business devices that are shared among different users.
- Create configuration profiles to change device settings for Wi-Fi networks, preconfigure mail and Microsoft Exchange settings, and more.
- Distribute public apps without entering an Apple ID on the device using Configurator.
- Create blueprints to automate device management. Use blueprints as templates to configure profiles and application and push them quickly to devices
- Add Supervision to devices and take advantage of even more management capabilities including showing or hiding applications, modifying the device name, wall paper, passcodes, keyboard short cuts and more.
- Back up user settings and app data, including new user-created data using Configurator.

Apple Configurator 2 also works with Apple's Device Enrollment Program (DEP) to automate Mobile Device Management (MDM) enrollment and the Volume Purchase Program (VPP) by assigning managed licenses apps to devices.

For a complete list of features and functionality available to supervised and unsupervised devices, refer to the iOS Functionality appendix.

For information on enrolling iOS devices with Apple Configurator, see *Enrolling iOS Devices in Bulk using Apple Configurator* and the **Integration with Apple Configurator** guide.

### Upload a Signed Apple Configurator Profile to the UEM console

You can export a signed profile from Apple Configurator (or IPCU) directly to the UEM console.

- 1 Configure supervision and management settings in Apple Configurator (or IPCU).
- 2 Export and save the newly created profile to somewhere easily accessible on your computer.
- 3 Navigate to **Resources > Profiles & Baselines > Profiles** within the UEM console and select **Upload**.
- 4 Enter the **Managed By** group and select **Upload** to locate and upload the profile exported from Apple Configurator (or IPCU). Click **Continue**.
- 5 Enter the general profile description, including name, description, and assigned organization groups.
- 6 Click **Save & Publish** to send the profile down to assigned devices.

# Configure iOS Devices

# 6

Workspace ONE UEM helps you configure key elements to manage your end users' device experience to meet your enterprise objectives. The functionality detailed in this section provides granular detail of the interface and experience of your managed devices.

Many of these configurations are available only with certain types of deployments, such as Apple DEP deployments or Apple School Manager deployments.

This chapter includes the following topics:

- [Apple Industry Templates](#)
- [Working with Profiles and Compliance Policies for Industry Templates](#)
- [Create an Apple Industry Template](#)
- [Edit Application Lists in Apple Industry Templates](#)
- [Delete an Apple Industry Template](#)

## Apple Industry Templates

Choose industry templates to expedite your deployment process.

Apple Industry templates automatically bundle recommended mobile apps, profiles, and compliance policies so that they can be pushed simultaneously to the required organization group.

- Industry templates available on the UEM console v8.2.2 include Healthcare and Retail.
- Industry templates available on the UEM console v8.3+ include Healthcare, Retail, Education, Hospitality, and Field Services.

### Types of Templates

Use the following table to determine what kind of template and initiative best describes the type of mobile configuration you need. Each template includes recommended applications and security policies based on expert research industry standards and best practices.

Industry	Initiative	Description
Healthcare	Clinical Collaboration	Deliver timely communication to medical staff and patients to ensure the best care without sacrificing security. (UEM console v8.2.2+)
Mobile Clinician Workflows	Allow physicians, nurses, pharmacists, and others to use real-time communication to deliver care to patients if they are at home or located in another medical facility. (UEM console v8.2.2+)	
Patient Care	Improve medical outcomes and patient satisfaction by using iPads and mobile applications to enhance the patient experience. (UEM console v8.2.2+)	
Education	Digital Classroom	Use iPads and mobile applications to communicate with teachers, students and parents about assignments, student behavior, and more. (UEM console v8.3+)
Making Learning Fun	Keep students engaged and focused through digital learning and collaboration. (UEM console v8.3+)	
Mobile Cash Register	Authorize employees to become points of sale from any location, such as a bookstore or in an administrative office. (UEM console v8.3+)	
Hospitality	Guest Experience	Create memorable guest experiences to foster loyalty and ensure guests return by allowing them to schedule their own services, look for attractions, or redeem loyalty bonuses. (UEM console v8.3+)
Hotel Management	Manage bookings and reservations and track staff schedules, shift responsibilities, and special requests in real time. (UEM console v8.3+)	
Mobile Payment	Integrate mobile payment solutions into POS systems so guests may take advantage of fast payment options or authorize employees to become points of sale wherever needed. (UEM console v8.3+)	
<b>Retail</b>	Mobile In Store Experience	Serve customers from anywhere in the store by browsing products, providing product information, performing a price check, or making a sale. (UEM console v8.3+)
Mobile Cash Register	Create mobile points of sale and free up floor space for merchandise. (UEM console v8.2.2+)	
Store Managers	Give managers the freedom to work on reports, employee schedules, and payroll from anywhere in the store. (UEM console v8.2.2+)	

Industry	Initiative	Description
Field Services	Field Employee	Increase efficiency for sales reps, service technicians, and others to deliver improved paperless services and real-time data to customers. (UEM console v8.3+)
Field Manager	Provide dynamic scheduling and real-time reporting capabilities to managers to communicate with employees, identify locations, edit schedules, and assign tasks. (UEM console v8.3+)	

## Working with Profiles and Compliance Policies for Industry Templates

- **Profiles** - The ability to add or edit profiles is supported in the UEM console from the **List View** page only. Any changes made on the **List View** page are not reflected in the industry template UI under **Hub**.
- **Compliance Policies** - The only compliance policy that is seeded and available for viewing within industry templates is Compromised Status in the UEM console 8.2.2+. Similar to profiles, the ability to add or edit compliance policies is supported from the **List View** page only. Any changes made on the **List View** page are not reflected in the industry template UI under **Hub**.

For more information on setting up profiles and compliance policies, refer to the **VMware Workspace ONE UEM Mobile Device Management Guide**, [available on Workspace ONE UEM Resources](#).

## Create an Apple Industry Template

Configure initiative-specific settings using a template. Then create a Patient Care template to push to patients. For example, you can create a Clinical Collaboration template to push to a user group of doctors and a user group of nurses.

### Prerequisites

Consider creating your User Groups before you begin this process.

### Procedure

- 1 Navigate to **Hub > Industry Templates > List View > Add Template**. An **Add Template** window appears.
- 2 Select the appropriate Industry category. A **Getting Started with Industry Templates** window appears.
  - a. If you want to select another industry and pick different initiatives, select **Choose Another Industry** at the bottom of the window to override the current industry if needed.
- 3 Choose the business initiative to configure and select **Setup**.

- 4 Select **Next** after reviewing the template overview. A new window appears where you can customize the template.
- 5 Set the **Friendly Name** that appears in the UEM console.
- 6 Choose what **Applications** to push to your users by selecting and deselecting apps. All the seeded apps are recommended and pre-selected by default. Alternatively, select **Add App** to search the app store for public applications or to upload internal applications.
  - a. Choose **More Options** to push the application in **Auto** mode or **On-Demand** and create a custom **Application Configuration** to enter the key value pairs.

If you choose the Mobile In Store Experience template and select VMware Browser in single app mode, configure the URL before pushing the template to devices by navigating to **Groups & Settings > All Settings > Apps > Browser > Mode > Home Page URL**. These devices must be configured in supervised mode.

- 7 Review **Policies** that apply to the selected template.
- 8 Assign **Users** or user groups for deployment, or create users. Directory services must already be configured to add directory users. If a new user or group is created, it appears on the **Accounts > List View** page in UEM console, even if the industry template is not yet deployed.
- 9 Select **Next** after confirming your selections.
- 10 Select **Publish**. The new template creates a smart group to which all apps, profiles, policies, users, and user groups are assigned. The new template now appears in the **Industry Templates > List View**.

Consider assigning one template to one group of devices, so that only one business initiative is assigned to each device. However, if you assign more than one template to the same group, then all the apps from both templates install and the most restrictive policies are sent to the device.

## Edit Application Lists in Apple Industry Templates

You can customize the industry templates you create with specific app deployment configurations.

- 1 Quickly remove a public application and push the updated application list to users immediately.
  - a. Navigate to **Hub > Industry Templates > List View**.
  - b. Select the **pencil button** or template name to edit the template.
  - c. Deselect the application. The check mark in the corner disappears.
  - d. Select **Next > Publish** to save and republish the template.
- 2 Upload a new application version of an internal app after deleting the old version.
  - a. Select the **pencil button** or template link to edit the template.
  - b. Select **More Options**. A trash can icon appears on the internal application.

- c. Select **Remove** and follow the prompt to delete the application from the list.
- d. Select **Add App** to upload the updated application.
- e. Select **Next** > **Publish** to save and republish the template with new application version.

Consider editing applications only within the industry template. However, applications can also be edited from the **Resources** > **Apps** > **Native** in the UEM console. Any changes made to applications from the Native List View page are not reflected in the industry template UI.

## Delete an Apple Industry Template

You can edit and delete templates at the current or parent Organization Group level only. You cannot edit or delete templates that were created at a higher Organization Group, you can only view them.

- 1 Navigate to **Hub** > **Industry Templates** > **List View**.
- 2 Select the **radio button**. A **Delete** button appears at the top of list.
- 3 Select **Delete** and follow the prompt to delete the template. Deleting a template also deletes the corresponding applications and policies from assigned devices.

Deleting a template does not remove the application from **Applications** > **Native** or remove the smart group from **Groups** > **List View**.

# Apple iBeacon Overview

# 7

Apple iBeacon with Workspace ONE Intelligent Hub v5.1+ helps manage location awareness for devices. Using Bluetooth Low Energy (BLE), iBeacons provide a more efficient way to track devices than using geofencing.

Bluetooth Low Energy does not drain the battery life of a device, and you can establish iBeacons to observe multiple regions simultaneously, providing more precise monitoring. This functionality also allows more privacy for end users because devices are only tracked when the device enters or exits specific locations, instead of being constantly monitored.

After setting up a third-party iBeacon, configure the iBeacon in the UEM console. Next, create iBeacon regions to monitor. Last, push device profiles with iBeacon functionality to manage iBeacons within the configured regions using the Workspace ONE Intelligent Hub. Detect when the device enters these regions and use device event logs to find changes in iBeacon ranges.

This chapter includes the following topics:

- [Requirements for iBeacon](#)
- [iBeacon Operations Details](#)
- [Enable iBeacon for iOS Devices](#)
- [Assign iBeacon Groups to Device Profiles](#)
- [Add Compliance Policies for iBeacon Groups](#)

## Requirements for iBeacon

- Workspace ONE UEM console v8.1+
- iBeacons from a third-party vendor
- Workspace ONE Intelligent Hub v5.1 + for iOS
- Location services on the device must be enabled
- Bluetooth must be enabled
- iPhone 4S+, iPad mini+, iPad 3rd Generation+, iPod touch 5th Generation+

## iBeacon Operations Details

- A maximum of 20 regions, including geofencing and iBeacon groups may be assigned to the device. This is the maximum amount that Apple allows. A high number of iBeacon groups assigned to the device increases battery consumption on the device.
- The Workspace ONE Intelligent Hub monitors iBeacons only. It does not use the ranging technique that determines the proximity of the device to iBeacon transmitter.
- If the Workspace ONE Intelligent Hub is stopped before a device exits the iBeacon group, the device is not detected until the Workspace ONE Intelligent Hub is launched again.

## Enable iBeacon for iOS Devices

To configure iBeacon, first enable the Workspace ONE Intelligent Hub to detect iBeacon groups that receive broadcasts. Then, add a set of iBeacon groups for the device to monitor.

- 1 Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Apple iOS > Hub Settings**.
- 2 Scroll to **Area** and select **Detect iBeacon Area** to enable an iBeacon for the organization group.
- 3 Select **Save**.
- 4 Navigate to **Resources > Profile & Baselines > Settings > Areas**.
- 5 Select **Add > iBeacon Group**. Choose **Add > Add Profile** or **Edit** an existing profile using the pencil button on the left-side of the profile. A **General** profile window appears.
- 6 Configure the **iBeacon Group** settings.

Setting	Description
<b>Group Name</b>	Enter the name for the specific iBeacon group.
<b>iBeacon Name</b>	Enter the name of the iBeacon.
<b>UUID</b>	Enter a unique identifier for the iBeacon deployment to share.
<b>Major Value</b>	Enter an identifier to subdivide the area of the iBeacon.
<b>Minor Value</b>	Enter an extra identifier to subdivide the area of the iBeacon.

- 7 Select **Save**. Return to **Area** and edit and delete iBeacon groups as needed using the menu buttons on the left.

## Assign iBeacon Groups to Device Profiles

Once the iBeacon group is established, you can assign the group to a device profile. This profile is then installed on the device when it enters the iBeacon group and is removed when it exits the group.

- 1 Navigate to **Resources > Profiles & Baselines > Profiles**. Choose **Add > Add Profile** or **Edit** an existing profile using the pencil button on the left-side of the profile. A **General** profile window appears.
- 2 Scroll to **Additional Assignment Criteria** on the **General** profile.
- 3 Select **Install only on devices inside selected areas** and select the iBeacon from **Assigned Geofence Areas**.
- 4 Continue to configure the payload as needed.
- 5 Select **Save & Publish**. You can now manage devices in the iBeacon group with the Workspace ONE Intelligent Hub.

## Add Compliance Policies for iBeacon Groups

Once the iBeacon group is established, add compliance policies to enforce actions on the device when it enters or exits the iBeacon group.

- 1 Navigate to **Devices > Compliance Policies > List View**, and select **Add** and then **Apple iOS**.
- 2 Choose **Any** or **All** of the rules to match.
- 3 Select **iBeacon Area** and choose **within/not within** for a specific iBeacon group and select **Next**.
- 4 Choose the **Actions** tab and select actions that can occur in the iBeacon group. For detailed information on the applicable actions on Apple iOS, see the *Compliance Policies Actions by Platform* section of the *Managing Devices* documentation.
- 5 Select **Finish and Activate** when you have completed the compliance policy configuration. Verify that the policy is available on the Device Details page in the UEM console.

# Activation Lock Overview



Activation Lock is a security feature for devices running iOS 7 and higher that uses Apple's Find My iPhone functionality. This feature makes it difficult for unauthorized persons to use a lost or stolen device.

When Activation Lock is enabled, an end user's Apple ID and password are required to unlock a device even if the device is wiped or factory reset, including through DFU mode. For more information about Activation Lock as an iOS feature, read the Apple Support article [Find My iPhone Activation Lock](#).

## Prerequisites

To use the Activation Lock feature, devices must have the following:

- A valid Apple ID and password assigned
- Find My iPhone enabled

This chapter includes the following topics:

- [Activation Lock for Unsupervised vs. Supervised Devices](#)
- [Enable Activation Lock for iOS Devices](#)
- [Viewing Activation Lock Status](#)
- [Clear Activation Lock on iOS Devices](#)
- [Use the Clear Activation Lock Command](#)
- [Enter an Activation Lock Bypass Code](#)
- [Perform a Device Wipe Command](#)
- [Activation Lock - Wipe Command Workflow Matrix](#)

## Activation Lock for Unsupervised vs. Supervised Devices

The extent to which you can manage devices with Activation Lock depends on whether the devices are supervised or unsupervised. The following table outlines the differences:

Unsupervised	Supervised
End user must enable <b>Find My iPhone</b> setting. Administrator can view whether Activation Lock is enabled on a particular device. Administrator must accept a notification when performing a device wipe command, which warns that a device with Activation Lock enabled cannot be reactivated without the original Apple ID and password*.	Administrator can enable Activation Lock. This will automatically activate the Find My iPhone setting. Administrator can view whether Activation Lock is enabled on a particular device. Administrator can clear the Activation Lock using one of three methods.
To learn how to remove a previous owner's Apple ID in order to reactivate a device, read the Apple Support article <a href="#">Find My iPhone Activation Lock</a> .	

## Enable Activation Lock for iOS Devices

For supervised devices running iOS 7 and higher, you can configure Activation Lock and force it to be enabled.

### Procedure

- 1 Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Apple iOS > Managed Settings**.
- 2 Select the **Activation Lock** setting.
- 3 Select **Save**.

## Viewing Activation Lock Status

For both unsupervised and supervised devices running iOS 7 and higher, you can view whether Activation Lock is enabled on the device. **Procedure**

- 1 Navigate to **Devices > List View**.
- 2 Select an iOS device.

Under the **Security** section, you can see whether Activation Lock is activated or deactivated.

## Clear Activation Lock on iOS Devices

For supervised devices running iOS 7 and later, you can clear the Activation Lock using one of three methods.

### Procedure

- 1 Use the Clear Activation Lock command
- 2 Enter an Activation Lock Bypass Code directly onto the device.
- 3 Perform a Device Wipe Command and select an option to clear the Activation Lock.

## Use the Clear Activation Lock Command

Using the Clear Activation Lock command you can clear the Activation Lock on a device without performing a device wipe. This command is useful if you know the whereabouts of the device and do not want to wipe its contents completely to clear the lock.

This command also works if the device is unenrolled from Workspace ONE UEM MDM.

- 1 Navigate to **Devices > List View**.
- 2 Select an iOS device.
- 3 The Device Details page displays. Select the **More** drop-down to see a list of available remote commands.
- 4 Select **Clear Activation Lock**.
- 5 Select **Deactivate**.

## Enter an Activation Lock Bypass Code

Entering an Activation Lock Bypass Code can be useful if the device has been unenrolled from Workspace ONE UEM MDM and you have no means by which to perform a Clear Activation Lock command or device wipe.

- 1 Navigate to **Devices > List View**.
- 2 Select an iOS device. The Device Details page displays.
- 3 Select the **More** drop-down to see a list of available remote commands.
- 4 Select **Clear Activation Lock**. The Activation Lock Bypass Code displays on the screen.

Reactivate the device once factory wiped using MDM. When you reach the Activate iPhone pane in the Setup Assistant, enter the bypass code as the Activation Lock password and leave the Apple ID text box empty.

## Perform a Device Wipe Command

When performing a device wipe command, you also have the option of clearing the Activation Lock on a device.

- 1 Navigate to **Devices > List View**.
- 2 Select an iOS device. The Device Details page displays.
- 3 Select the **More** drop-down to see a list of available remote commands.
- 4 Select **Device Wipe**. The Device Wipe page displays.
- 5 Select **Clear Activation Lock**. Enter your **Security PIN**, and the device is wiped.

## Activation Lock - Wipe Command Workflow Matrix

The following matrix shows the workflow to check the activation lock bypass code before issuing the wipe command from the UEM console to the device. The bypass code check can be initiated from the Device **List View** page or the **Device Details** page.

Command	Activation Lock Bypass Code Workflow	
	Device List View	Device Details page
<b>Device Wipe</b>	Not applicable	Sends query to the device for fetching the activation lock bypass code. Device marked as <b>Device Wipe Initiated</b> in the UEM console. If the wipe protection is turned off on the device, the device responds with the bypass code to the UEM console. The UEM console sends the device wipe command to the device. Device responds with the successful wipe message to the UEM console. Device is marked as Unenrolled in the UEM console.
<b>Enterprise Wipe</b>	Sends query to the device for fetching the activation lock bypass code. Device is marked as <b>Enterprise Wipe Initiated</b> in the UEM console. If the wipe protection is turned off on the device, the device responds with the bypass code to the UEM console. The UEM console sends the enterprise wipe command to the device. Device responds with the successful wipe message to the UEM console. Device marked as <b>Unenrolled</b> in the UEM console.	Sends query to the device for fetching the activation lock bypass code. Device marked as <b>Enterprise Wipe Initiated</b> in the UEM console. If the wipe protection is turned off on the device, the device responds with the bypass code to the UEM console. The UEM console sends the enterprise wipe command to the device. Device responds with the successful wipe message to the UEM console. Device marked as Unenrolled in the UEM console.

# Remote View

# 9

With the Remote View feature, administrators can easily assist with troubleshooting by viewing an MDM managed end user's device from the UEM console that is integrated with the partner system. Integration of the partner system with the UEM console offers a complete remote management suite with Remote View capabilities.

For more information on configuration and integration of Remote Management services using the partner system with the UEM console, refer **VMware AirWatch Advanced Remote Management Guide** found on docs.vmware.com.

This chapter includes the following topics:

- [Prerequisites to initiate a Remote View](#)
- [Remote View Device Requirements](#)

## Prerequisites to initiate a Remote View

- UEM console provisioned with proper partner hostname and all required certificates.
- End User devices registered with partner by the Workspace ONE Intelligent Hub.

## Remote View Device Requirements

- Devices must have the Workspace ONE Intelligent Hub v5.8 or higher installed and in the foreground when you attempt to initiate remote view.
- iOS 11 and higher devices are required to run the **Start Remote View** command.
- iOS 11 and higher Supervised devices are required for administrators to run the **Stop Remote View** command. This command appears on the partner console.

## Configure the UEM Console with Remote View

For On-premises deployments, provision the site URLs with proper hostname for the partner system at the Global organization group in the Site URLs page.

- 1 Navigate to **Groups & Settings > All Settings > System > AdvancedSite > URLItem**
- 2 In the **Workspace ONE Assist** section, configure the Remote Management settings.

Settings	Description
Console Connection Hostname	Enter the Remote Management server fully qualified domain name (FQDN) plus "/t10". For example: <a href="https://rmstage01.awmdm.com/t10">https://rmstage01.awmdm.com/t10</a>
Device Connection Hostname	Enter the ARM server fully qualified domain name (FQDN). For example: <a href="https://rmstage01.awmdm.com">https://rmstage01.awmdm.com</a> The Device Hostname is the only URL used for device registration and gets delivered to all the devices in the organization group when the partner is provisioned.

3. Select **Save**.

## Configure End-User Devices

Now that the console is configured, you must install the iOS-specific Hub on the devices so that they can be remotely managed.

- 1 Visit the my Workspace ONE™ page that lists all the device agents. <https://my.workspaceone.com/products/AirWatch-Agent>.
- 2 Download Workspace ONE Intelligent Hub from the iOS App store for your deployment.  
For more information about App Management, see **Mobile Application Management** guide on [VMware AirWatch documentation](#).
- 3 Customize control center for initiating screen broadcasting:
  - a. Navigate to **Settings > Control Center > Customize Controls**.
  - b. Add **Screen Recording**.

## Initiate a Remote View Session

Use the Remote View session to easily assist the troubleshooting issues by viewing an end user's device from the UEM console.

- 1 Navigate to **Devices > List View > Select Device > More Actions > Support > Start Remote View**

The **Remote Support** window appears. The UEM console verifies the device's abilities before initiating the broadcast. Simultaneously, a push notification is sent to the end user device through Workspace ONE Intelligent Hub to start the broadcast. The user must access the device control center and force touch on the Screen Recording. Select **Hub Broadcast > Start Broadcast** to initiate broadcasting the device's screen. The device begins capturing the UI and shares it to the Workspace ONE Intelligent Hub which in turn is linked to the Advanced Remote Management server.

## Remote Support

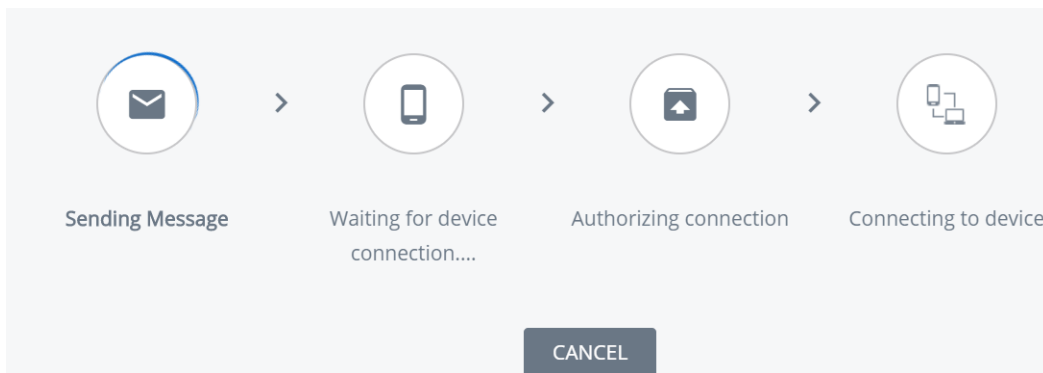


Remote Management Session Available

Step	Status
Checking Device Registration	Success
Queuing Remote Management Command	Success
Creating Remote Management Session	Success

LAUNCH SESSION

- In the Remote Support window, select **Launch Session** to initiate the remote view session. Once the connection is made, the remote management client opens on the console and then the mirrored device screen is shown up.



**Note:** The UEM console displays a four-digit PIN which you must direct the customer to enter into their device. This action provides customer authorization to manage their device remotely.

- Select **Cancel**, if required to end the session.

### Request AirPlay for an iOS Device

Using the AirPlay command, administrators can easily mirror screens from a macOS computer to an tvOS on the same subnet as an end user's iOS 7 + device.

If an end user needs assistance, simply send an AirPlay request from the UEM console to the device to share your screen on an end user's device.

- Navigate to **Devices > List View > Select Device > Support > More > Start AirPlay**. An **AirPlay** window appears.
- Select **Add a Destination** to start adding destinations to view. An **Add New AirPlay Destination** window appears.
- Enter the **Destination Name**, which is the friendly name for the device.
- Enter the **Destination Address**, which is the MAC address of the device to view.
- Enter the **Password** for the destination.

- 6 Determine the **Scan Time**, which is the length of time that the device searches for the destination. The default value is 30 seconds.
- 7 Select the **Set as Default** check box to make the current destination the default destination. The next time AirPlay is used, the default destination appears as the **Destination Name**. It does not have to be entered again.
- 8 Select **Save and Start** to send the AirPlay request to the device.
  - a. This destination is saved for the next request in the **Destination Name** drop-down menu.
- 9 To **Stop AirPlay** on iOS 7+ supervised devices, navigate back to the UEM console. Go to **Devices > List View > Select Device > Support > More > Stop AirPlay**.
- 10 To **Edit AirPlay Destination**
  - a. Navigate to **Devices > List View > Select Device > Support > More > AirPlay**. An **AirPlay** window appears.
  - b. Choose the **Device Destination** to edit from the drop-down menu.
  - c. Select **Edit** to start editing the destination settings. An **Edit AirPlay Destination** window appears.
  - d. Select **Save and Start** to send the AirPlay request to the device.

# Configure Managed Settings for iOS Devices

# 10

The Managed Settings page in the UEM console lets you configure a few extra settings related to the Workspace ONE Intelligent Hub and managing iOS devices.

- 1 Navigate to **Devices > Device Settings > Devices & Users > Apple > Apple iOS > Managed Settings > Default Managed Settings**.
- 2 Configure which devices the settings affect according to ownership type, including Corporate - Dedicated, Corporate - Shared, Employee Owned, and Unknown.
- 3 Activate or deactivate:
  - a. Voice Roaming (iOS 5+)
  - b. Data Roaming (iOS 5+)
  - c. Personal Hotspot (iOS 7)
  - d. Activation Lock (iOS 7 and Supervised)
  - e. (iOS 11.3+ Supervised)
- 4 Select **Save** to save the settings to devices in the current organization group.

This chapter includes the following topics:

- [Configure Organization Settings](#)
- [Override Default Roaming Settings \(iOS\)](#)
- [Set a Default Wallpaper](#)
- [Set Default Organization Information](#)
- [Install Fonts on iOS Devices](#)
- [Cisco QOS Marking for iOS Applications](#)

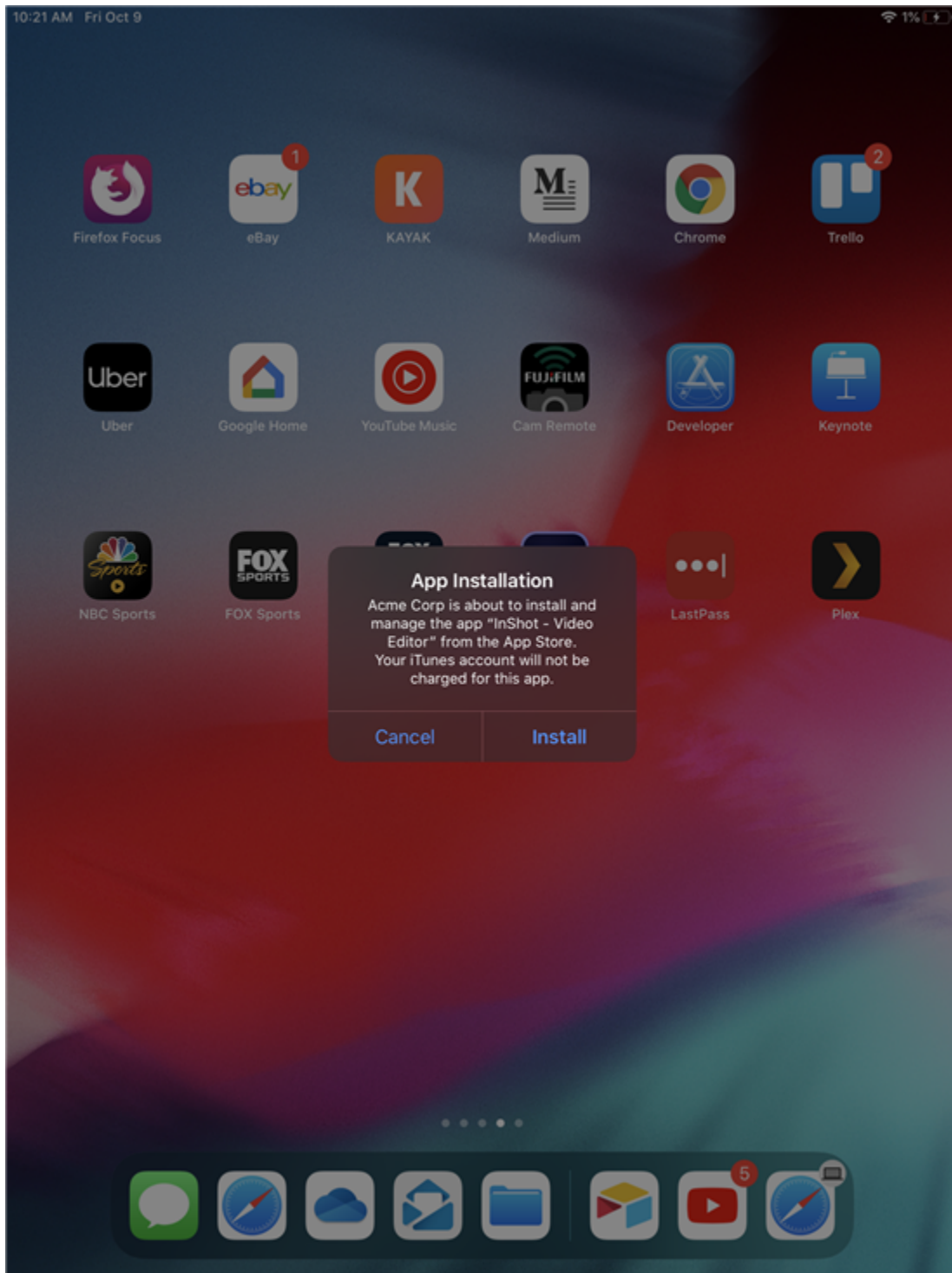
## Configure Organization Settings

The Managed Settings Requested page in the UEM console lets you configure settings related to branding in Workspace ONE Intelligent Hub and managing iOS devices. Change the settings including default wallpaper, home screen image, organizational settings and so on.

- 1 Navigate to **Devices > Settings > Devices & Users > Apple > Apple iOS > Managed Settings Requested**.
- 2 Navigate to **Organization Information > Organization Name**. Enter the Organization name.

The screenshot displays the 'Settings' interface with a sidebar on the left containing a tree view of settings categories. The main content area is titled 'Settings' and includes a dropdown menu for 'Global / naeventest'. The 'Managed Settings Requested' section is active, showing various configuration options. The 'Organization Information' section is expanded, revealing input fields for 'Organization Name' (containing 'Acme Corp'), 'Organization Phone Number', and 'Organization Email'. The 'Child Permission' section at the bottom shows 'Inherit or Override' as the selected option. A 'SAVE' button is located in the bottom right corner.

- 3 Click **Save**.
- 4 Install and manage any app for the same device. The organization name that you have entered is included in the installation screen.



## Override Default Roaming Settings (iOS)

Override default settings in order to modify roaming permissions for an individual iOS device.

Modify settings to manage roaming status that does not require a permanent restriction.

- 1 Navigate to **Devices > List View**. Filter by **Platform** to locate your desired device. Select its **Friendly Name** to launch the Device Control Panel.
- 2 Select **More > Managed Settings**.
- 3 Select the **Enable** or **Disable** radio button to override current **Voice Roaming Allowed**, **Data Roaming Allowed**, and **Personal Hotspot Allowed** settings. Click **Save**.

## Set a Default Wallpaper

Set a default Lock Screen image or Home Screen image for iOS 7 + Supervised devices to match your corporate branding policies.

- 1 Navigate to **Devices > Device Settings > Devices & Users > Apple > Apple iOS > Managed Settings**. Scroll down to the Default Wallpaper section.
- 2 Upload a **Lock Screen Image** or **Home Screen Image**.
- 3 Select **Save**.

## Set Default Organization Information

Set up custom organization information for MDM prompts for iOS 7+ devices.

- 1 Navigate to **Devices > Device Settings > Apple > Apple iOS > Managed Settings** and scroll down to the **Default Organization Information** section.
- 2 Enter your organization information, including name, phone number, and email.
- 3 Select **Save**.

## Install Fonts on iOS Devices

Available to macOS Yosemite and devices running iOS 7 and higher, the UEM console provides a means to upload fonts and install them onto devices. Installing specific fonts allows users to view and read text that is not supported by standard means.

Compatible font file types include .ttf or .otf. There is no limit to the number of fonts you are can install on devices and you can remove a font at any time.

### Procedure

To install and deploy fonts:

- 1 Navigate to **Devices > Device Settings > Apple > Install Fonts**.
- 2 Drag and drop a supported font file type (.ttf or .otf) onto the screen.
- 3 Locate the font file and select **Save** to send the font to all devices enrolled in the current organization group.

## Cisco QOS Marking for iOS Applications

Apple and Cisco have partnered to deliver a better app and voice experience for iOS devices on corporate networks through Cisco's QOS fast lane network. Workspace ONE UEM allows you to select audio and video applications to receive prioritized data allocations.

With Workspace ONE UEM MDM, customers with the Cisco infrastructure can:

- Activate or Deactivate use of Cisco QoS fast lane network
- Allowlist Applications to benefit from L2 and L3 marking
- Enable Audio and Video traffic for built-in services such as FaceTime and Wi-Fi calling for L2 and L3 marking for traffic sent to Wi-Fi network

To configure Cisco QOS Marking for applications, see **Create a Wifi Profile** in this guide..

# Apple Push Notification Service (APNs)

# 11

Apple Push Notification service (APNs) is the MDM protocol created by Apple to manage their devices. It requires the MDM provider to have a valid APNs certificate configured and routes all commands through Apple's central cloud messaging servers.

Initiating an APNs command leads to the following:

- When an iOS device is enrolled, an APNs token is generated that is connected to a specific device. The generated token is known to both Workspace ONE UEM console and the APNs servers.
- Once enrolled, a device always (connectivity permitting) exhibits an active connection to Apple's APNs servers.
- When a command is initiated in the UEM console (such as a profile push or a device lock command), the following steps occur:
  - An entry is stored in the Device Command Queue in the UEM database. The entry contains a specific ID attached to the type of command initiated.
  - The UEM server (either console or device services depending on where the command initiated), reaches out to the APNs servers with the APNs token tied to that specific device.
- The APNs server validates the token and informs the device to connect to the MDM server to receive a command.
- The device connects to the device services server. Upon establishing this connection, the device receives all pending commands from the Device Command Queue.

This chapter includes the following topics:

- [Apple Push Notification Service \(APNs\) Certificate](#)
- [Apple Push Notification Service Workflow](#)

## Apple Push Notification Service (APNs) Certificate

To manage iOS devices, you must first obtain an Apple Push Notification Service (APNs) certificate. An APNs certificate allows the UEM console to communicate securely to Apple devices and report information back to the UEM console.

Per Apple's Enterprise Developer Program, an APNs certificate is valid for one year and then must be renewed. The UEM console sends reminders through Notifications as the expiration date nears. Your current certificate is revoked when you renew from the Apple Development Portal, which prevents device management until you upload the new one. Plan to upload your certificate immediately after it is renewed. Consider using a different certificate for each environment if you use separate production and test environments.

## Apple Push Notification Service Workflow

Understand the backend workflow of the Apple Push Notification Service before initiating the MDM management on Apple devices.

- 1 System Administrator remotely performs MDM actions such as lock device, clear device passcode, device wipe, and break MDM from the UEM console.

A notification will be queued in **FastLaneAPNsOutBound** queue which is picked up by **Workspace ONE Messaging Service** and sent to APNs server. Later, a command is queued in **AWEventLog** queue and then picked up by **EntityChangeQueueMonitor** service. This service queues the command in Workspace ONE Database server.

- 2 The device always has an active connection to APNs. All communication to APNs is inbound and is constantly checking with APNs. The servers let the device know when there's a command waiting for the device by MDM.
- 3 Once the device receives the push notification, it checks-in to the Workspace ONE device services server.
- 4 Device services server checks whether any command is queued for that particular device (based on DeviceID) in the Workspace ONE database server.
- 5 Device services server pulls the command which is already queued for that device from the Workspace ONE database server.
- 6 Device services generates an XML and sends it to the device. Native MDM Agent (MDM profile installed on device) then performs required action on the device.

# Device Management

# 12

After your devices are enrolled and configured, manage the devices using the Workspace ONE™ UEM console. The management tools and functions enable you to keep an eye on your devices and remotely perform administrative functions.

You can manage all your devices from the UEM console. The Dashboard is a searchable, customizable view that you can use to filter and find specific devices. This feature makes it easier to perform administrative functions on a particular set of devices. The Device List View displays all the devices currently enrolled in your Workspace ONE UEM environment and their status. The **Device Details** page provides device-specific information such as profiles, apps, Workspace ONE Intelligent Hub version and which version of any applicable OEM service currently installed on the device. You can also perform remote actions on the device from the Device Details page that are platform-specific.

This chapter includes the following topics:

- [Device Dashboard](#)
- [Device List View](#)
- [Customize Device List View Layout](#)
- [Exporting List View](#)
- [Search in Device List View](#)
- [Device List View Action Button Cluster](#)
- [Remote Assist](#)
- [Using the Device Details Page for iOS Devices](#)
- [Configure and Deploy a Custom Command to a Managed Device](#)

## Device Dashboard

As devices are enrolled, you can manage them from the **Device Dashboard** in Workspace ONE UEM powered by AirWatch.

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.

- **Security** – View the top causes of security issues in your device fleet. Selecting any of the doughnut charts displays a filtered **Device List** view comprised of devices affected by the selected security issue. If supported by the platform, you can configure a compliance policy to act on these devices.
  - **Compromised** – The number and percentage of compromised devices (jailbroken or rooted) in your deployment.
  - **No Passcode** – The number and percentage of devices without a passcode configured for security.
  - **Not Encrypted** – The number and percentage of devices that are not encrypted for security. This reported figure excludes Android SD Card encryption. Only those Android devices lacking disc encryption are reported in the donut graph.
- **Ownership** – View the total number of devices in each ownership category. Selecting any of the bar graph segments displays a filtered **Device List** view comprised of devices affected by the selected ownership type.
- **Last Seen Overview/Breakdown** – View the number and percentage of devices that have recently communicated with the Workspace ONE UEM MDM server. For example, if several devices have not been seen in over 30 days, select the corresponding bar graph to display only those devices. You can then select all these filtered devices and send out a query command so that the devices can check in.
- **Platforms** – View the total number of devices in each device platform category. Selecting any of the graphs displays a filtered **Device List** view comprised of devices under the selected platform.
- **Enrollment** – View the total number of devices in each enrollment category. Selecting any of the graphs displays a filtered **Device List** view comprised of devices with the selected enrollment status.
- **Operating System Breakdown** – View devices in your fleet based on operating system. There are separate charts for each supported OS. Selecting any of the graphs displays a filtered **Device List** view comprised of devices running the selected OS version.

## 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.

Device List View, UEM, Workspace ONE, device list, friendly name, device status

Devices  
List View

Filters < ADD DEVICE LAYOUT EXPORT Search List

Management	Last Seen	General Info	Platform	User	Enrollment	Compliance Status	Tags
Ownership	18m	swamyg MacBook Pro macOS 10.15.0 GSWN Global / VMwareT MDM   Corporate - Dedicated	Apple macOS MacBook Pro "Core i7" 15" Retina (Mid-2015) 10.15.0	swamyg G S	Enrolled	Compliant	
Smart Groups	23m	6HTD4C2 - AW Migration Testing Global / Arun_Chrome MDM   Corporate - Dedicated	Chrome OS		Unenrolled	Not Available	
User Groups	1h	wsuser2 Desktop Windows Desktop 10.0.17134 ... Global / stg12 MDM   Corporate - Dedicated	Windows Desktop VMware Virtual Platform 10.0.17134		Unenrolled	Not Available	
Device Type	2h	a Desktop Windows Desktop 10.0.18362.6TQ2 1... Global / sachin MDM   Corporate - Dedicated	Windows Desktop Precision 5530 10.0.18362	a@a.com a	Enrolled	Compliant	
Security	2h	sakshis MacBook Pro macOS 10.14.6 FD58 Global / cdvi UEM Managed   Corporate - Dedicated	Apple macOS MacBook Pro "Core i7" 15" Retina (Late 2015) 10.14.6	sakshis Sakshis ss	Enrolled	Compliant	
Status	2h	preetu Ubuntu Linux 4.15 Global / Preetu MDM   Unassigned	Linux Ubuntu 4.15.0		Unenrolled	Not Available	
Advanced	2h	preetu WindowsMobile WindowsMobile 5.2.2123... Global / Preetu MDM   Unassigned	Windows Rugged microsoft deviceemulator 5.2.21234	preetu	Enrolled	Not Available	
	3h	sakshis iPhone iOS 12.2.0 HG6X Global / cdvi UEM Managed   Corporate - Dedicated	Apple iOS iPhone 7 (32 GB Silver) 12.2.0	sakshis Sakshis ss	Enrolled	Compliant	
		m iPhone iOS 13.0.0 KXKN	Apple iOS	m@m.com			

Items 1 - 50 of 33731 Page Size: 50

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.

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.

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.

## 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.

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.

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

## 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, 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

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.

For more information, see the **Workspace ONE Assist** guide, available on [docs.vmware.com](https://docs.vmware.com).

## Using the Device Details Page for iOS Devices

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

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

**View Device Information** Use the Device Details menu tabs to access specific device information, including:

- **Summary** – View general statistics such as:
  - Compliance
  - Enrollment status
  - Last seen
  - Platform/model/OS
  - Management
  - Supervision
  - Activation Lock
  - Find My iPhone
  - iCloud Backup (use the mouse to hover over iCloud Backup status to see Last Backup status)
  - Data protection
  - Encryption
  - Contact information
  - Organization group and smart group

- Phone number (for the devices such as iPhone XS, XR, or XS Max that supports multiple SIM cards including eSIM, displays the phone numbers of all the SIMs associated with the device)
- Serial number, UDID, and asset number
- Power status
- Storage capacity
- Available OS updates (iOS 11 and later devices)
- Physical memory and virtual memory and warranty information

If Apple's Global Service Exchange information is accessible, select the warranty link to see when the status was last updated. Then, use the **Refresh** button to get the latest information

- An enterprise or factory wipe queries an Activation Lock bypass code and then go into wipe pending mode on supervised devices.
- If the Find my iPhone Activation Lock option is enabled for iOS 7+ devices, then a warning will appear when performing a device wipe command on an unsupervised device, notifying you that a device with Activation Lock enabled cannot be reactivated without the original Apple ID and password. This is true even if you perform a full device wipe. For more information, see Activation Lock Overview.
- **Compliance** – Display the status, policy name, date of the previous and forthcoming compliance check and the actions already taken on the device.
- **Profiles** – View all MDM profiles currently installed on a device.
- **Apps** – View the app status, app name, type of the app (whether public or internal), app version and identifier, and the size of the app. For iOS 11.+ devices, the UEM console displays available app updates (whether the installed version is the latest version or if an update is available) and app source (whether the app is installed through the App Store, distributed as a Beta app, signed adhoc by an enterprise account, or managed using a device based VPP license).

**Note:** Due to the way application status is reported on iOS devices, an application achieves Installed status only after the installation process is fully completed. Which means when the Workspace ONE UEM console queries the device for its application list sample, and if the application is still downloading, then the application returns a status of Installing. On a successful application installation, the device returns the application status as Installed which is marked the same in the Workspace ONE UEM console.

- **Updates** – View the iOS updates available for the device including the OS version, product key, build version, last update, download percentage, and progress status.
- **Content** – View the status, type, name, priority, deployment, last update, and date and time of views, and provides a toolbar for administrative action (install or delete content).
- **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.

The menu tabs below are accessed by selecting More from the main Device Details page:

- **Network** – View the current network (Cellular, Wi-Fi, Bluetooth) status of a device. For iOS 12.1 and later devices such as iPhone XS, XR, or XS Max that supports multiple SIMs and eSIM, you can view and track the network status of the SIMs on the UEM console.
- **Security** – View the current security status of a device based on security settings.
- **Restrictions** – View the types of restrictions that currently apply to the device.
- **Telecom** – View all amounts of calls, data and messages sent and received involving 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 issuer. This tab also provides information about certificate expiration.
- **Terms of Use** – View a list of End User License Agreements (EULAs) which have been accepted during device enrollment.
- **Alerts** – View all alerts associated with the device.
- **Books** – View all internal books on the device.
- **Shared Device Log** – View the history of the shared device including past check-ins and check-outs and status.
- **Restrictions** – 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.
- **Targeted Logging** – View the logs for the Console, Catalog, Device Services, Device Management, and Self Service Portal. You must enable Targeted Logging in settings and a link is provided for this purpose. You must then select the Create New Log button and select a length of time the log is collected.
- **Troubleshooting** – View Event Log and Commands logging information. This page features export and search functions, enabling you to perform targeted searches and analysis
  - **Event Log** – View detailed debug information and server check-ins, including a Filter by Event Group Type, Date Range, Severity, Module, and Category.

In the Event Log listing, the Event Data column may display hypertext links that open a separate screen with even more detail surrounding the specific event. This information enables you to perform advanced troubleshooting such as determining why a profile fails to install.

- **Commands** – View detailed listing of pending, queued, and completed commands sent to the device. Includes a Filter enabling you to filter commands by Category, Status, and specific Command.

- **Attachments** – Use this storage space on the server for screenshots, documents, display Hub logs sent from the Intelligent Hub, and links for troubleshooting and other purposes without taking up space on the device

**Perform Remote Actions** The **More Actions** drop-down on the Device Details page enables you to perform remote actions over-the-air to the selected device. See below for detailed information about each remote action. The actions listed below will vary depending on factors such as device platform, UEM console settings, and enrollment status.

- **Query All** – Send a query command to the device to return a list of installed applications (including Workspace ONE Intelligent Hub, where applicable), books, certificates, device information, profiles, and security measures.
- **Device Information (Query)** – Send an MDM query command to the device to return information on the device such as friendly name, platform, model, organization group, operating system version, and ownership status.
- **Security (Query)** – Send an MDM query command to the device to return the list of active security measures (device manager, encryption, passcode, certificates, and so on).
- **Profiles (Query)** – Send an MDM query command to the device to return a list of installed device profiles.
- **Apps (Query)** – Send an MDM query command to the device to return a list of installed applications.
- **Certificates (Query)** – Send an MDM query command to the device to return a list of installed certificates.
- **Clear Passcode (Restrictions Setting)** – Clear the passcode command clears the login passcode on the device. The device needs to be supervised.
- **User Lists (Query)** - Send a query command to the device to return a list of users who have logged into the device (for shared devices only).
- **Lock Device** – Send an MDM command to lock a selected device, rendering it unusable until it is unlocked.
- **Lock SSO** – Lock the device user out of Workspace ONE UEM Container and all participating applications.
- **Enterprise Wipe** – Enterprise Wipe a device to unenroll and remove all managed enterprise resources including applications and profiles. This action cannot be undone and re-enrollment is required before Workspace ONE UEM can manage this device again. This device action includes options to prevent future re-enrollment and a Note Description text box for you to add information about the action.
  - Enterprise Wipe is not supported for cloud domain-joined devices.
- **iOS updates** - Select individual devices or devices in bulk to send updates to devices that are enrolled through Apple Business Manager.

- **Managed Settings** – Activate or deactivate voice roaming, data roaming, and personal hotspots.
- **Device Wipe** – Send an MDM command to wipe a device clear of all data and operating system. This puts the device in a state where recovery partition will be needed to reinstall the OS. This action cannot be undone. The recovery partition is only needed on Mac devices and not in iOS devices.
  - **iOS Device Wipe Considerations**
    - For iOS 11 and below devices, the device wipe command would also wipe the Apple SIM data associated with the devices.
    - For iOS 11+ devices, you have the option to preserve the Apple SIM data plan (if existed on the devices). To do this, select the Preserve Data Plan checkbox on the Device Wipe page before sending the device wipe command.
    - For iOS 11.3+ devices, you have an additional option to activate or deactivate to skip the Proximity Setup screen while sending down the device wipe command. When the option is enabled, the Proximity Setup screen will be skipped in the Setup Assistant and thus preventing the device user from seeing the Proximity Setup option

For more information about troubleshooting device wipes, related permissions, and when device wipe actions appear in the UEM console, refer to the following Workspace ONE UEM Knowledge Base article <https://support.workspaceone.com/articles/115012396488>.

- **Schedule iOS Updates** – Push an iOS update to a device that is not enrolled through DEP. For more information, see Configure iOS Updates.
- **Refresh eSIM** – Send a query to a carrier eSIM server URL to refresh the active eSIM cellular plan profiles on the device.
- **Send Message** – Send a message to the user of the selected device. Select between Email, Push Notification (through AirWatch Cloud Messaging), and SMS. Push notification requires Airwatch applications like Hub, Boxer etc which must have been launched at least once.
- **Find Device** – Send a text message to the applicable Workspace ONE UEM application together with an audible sound designed to help the user locate a misplaced device. The audible sound options include playing the sound a configurable number of times and the length of the gap, in seconds, between sounds.
- **Request Device Check-In** – Request the selected device to check-in itself in to the UEM console and updates the Last column status. This action also resets the device enrollment to the staging user.
- **Sync Device** – Synchronize the selected device with the UEM console, aligning its Last Seen status.
- **Remote View** – Enable an active stream of the device's output to a destination of your choice, allowing you to see what the user sees as they operate the device. The destination parameters include IP address, port, audio port, password, and scan time.

- **Change Organization Group** – Change the device's home organization group to another existing OG. Includes an option to select a static or dynamic OG.
  - If you want to change the organization group for multiple devices at a time, you must select devices for the bulk action using the Block selection method (using the shift-key) instead of the Global check box (next to the Last Seen column heading in the device list view).
- **Add Tag** – Assign a customizable tag to a device, which can be used to identify a special device in your fleet.
- **Edit Device** – Edit device information such as Friendly Name, Asset Number, Device Ownership, Device Group Device Category.
- **Delete Device** – Delete and unenroll a device from the console. Sends the enterprise wipe command to the device that gets wiped on the next check-in and marks the device as Delete In Progress on the console. If the wipe protection is turned off on the device, the issued command immediately performs an enterprise wipe and removes the device representation in the console.
- **Clear Activation Lock** – Clear the Activation Lock on an iOS device. With the Activation Lock enabled, the user requires an Apple ID and password before taking the following actions: disabling Find My iPhone, factory wipe, and reactivate to use the device.
- **Device Configured** - Send this command if a device is stuck in an Awaiting Configuration state.
- **Enable/Disable Lost Mode** – Use this device action to lock a device and send a message, phone number, or text to the lock screen. The device end user cannot deactivate Lost Mode. When an admin deactivates Lost Mode, the device returns to normal functionality. Users receive a message that tells them that the location of the device was shared. (iOS 9.3 + Supervised)
  - **Request Device Location** – Query a device when in Lost Mode and then use the Location tab to find the device. (iOS 9.3 + Supervised)
- **Log out user** - Log out the current user of the device if needed.

## 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

### Procedure

- 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.
- 5 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.

# OS Update Management

# 13

With the OS update management system, admins can block and require iOS updates on their supervised iOS devices to keep all devices on a common iOS version for a consistent management experience. Maintaining the OS ensures that the device security issues are addressed with minor iOS updates and the devices are always up to date.

OS update management offers an ideal solution for admins to:

- Block end-user devices from detecting new iOS updates released by Apple. For more information on configuring the restriction profile to block end-users, refer *Restriction Profile Configurations* in [Device Profiles](#).
- Get information on current available patches/updates available for devices.
- Publish iOS updates to end-user devices.

This chapter includes the following topics:

- [iOS Update Management Features](#)
- [iOS Update Management Prerequisites](#)
- [Supported Devices](#)
- [Network Requirements](#)
- [View the Available iOS Updates](#)
- [Assign and Publish iOS Updates](#)
- [Pause and Unpause iOS Updates](#)
- [Monitor iOS Update Assignments](#)
- [Manage iOS Updates for Individual Devices](#)
- [Delay iOS Updates](#)
- [Set the Device Name for a Supervised iOS Device](#)

## iOS Update Management Features

The major features available are:

- **Block Update** – Configure the device not to detect an update for up to 90 days from the release date of the update by Apple. For more information on configuring the restriction profile to block the updates, refer [Restriction Profile Configurations](#)
- **List available updates** – Lists all the available updates from Apple and lists out the devices that are eligible for the respective updates.
- **OS Update Action** – Define the OS update action; download only, install only, or download and install immediately.
- **Monitor** – Display the status of an OS update on assigned devices.

## iOS Update Management Prerequisites

Ensure to have the minimum requirements explained in this section before initiating the OS update management on managed devices from the UEM console.

### Supported Devices

- Supervised iOS 11.3 and later
- Device must have at least 50 percent battery
- Device must have enough storage space available to download the update
- Device must have a network connection Apple's update servers

### Network Requirements

For information on network architecture and its requirements, refer to the **Recommended Architecture** guide.

## View the Available iOS Updates

View the snapshot of the list of latest or active iOS updates available from Apple for all your managed and eligible devices.

Navigate to the **Resources > Device Updates > iOS** page to view the available OS updates and other related details, including:

- **Update** – Name of the update.
- **Version** – Version of the update.
- **Release Date** – Date when the update is released.
- **Expiration Date** – Date when the update expires.

- **Update Status** – Status of the iOS update if available or not available from Apple.
- **Assignments** – Number of assignments applied to an update.
- **Assignment Status** – Status of the assignments applied to the update such as Assigned, Not Assigned, or Paused.

The list of iOS update details is pulled from the Apple using the Sync Device Updates scheduler job at the specified interval which runs at an interval of 6-24 hours (that pulls data from Apple).

**Note:** The Update Status shows the OS versions that are not available in <https://gdmf.apple.com/v2/pmv>. Whenever there is any change in the Expiry Date, the sync job inserts new records or updates the records accordingly. The update becomes unavailable only if the Expiry Date is over. To overcome this issue, the job must be fixed to update the Expiry Date of missing updates to one day less than the job runs so that the updates can be displayed as not available in UEM.

Select an OS Update from the **Device Updates > iOS** page to view additional information. The Details section shows the details of the OS update (such as version details, supported devices and so on). The graphs beneath the Details section, shows:

- **Device Readiness** – Provides information related to the update and the devices enrolled at the organization group and below. This includes devices that are eligible to receive the update, devices that are not eligible to receive the update (e.g. unsupervised, incompatible hardware, etc.), devices that are on higher version, or devices already on the selected version.
- **Device Status** – Provides information on the status of the iOS update on the assigned, eligible devices. This includes the devices that downloaded the update, installed the update, or failed with a specified error code.
- **Devices** – The table shows the status of the iOS updates on eligible and non-eligible devices that are triggered from an assignment.

Updates to the devices are assigned using Smart Groups with preferred deployment parameters by selecting **Manage Assignments**. For more information on assignment, refer *Assign OS Updates*.

## Assign and Publish iOS Updates

To deploy an OS Update, assign one or more smart groups to an iOS update and publish to the device.

To assign smart groups and deploy the iOS updates:

- 1 Navigate to the **Resources > Device Updates > iOS** page.
- 2 Select an iOS Update by selecting the corresponding radio button. The **Manage Assignments** option appears on top of the page.
- 3 Select **Manage Assignments** for the assignment page to display.
- 4 Select **New Assignment** under the **Assignment** section. The **Add Assignment** page appears.

- 5 In the **Definition** tab, enter the assignment name and select one or more smart groups. Select **Next**.
- 6 In the **Deployment** tab, enter the date and time for the deployment to begin and select one deployment method. The available deployment methods are:

Method	Description
<b>Download and Install</b>	The iOS update gets downloaded and installed on the device.
<b>Download Only</b>	The iOS update only gets downloaded but not installed on the device.
<b>Install Only</b>	The iOS updates gets installed on the device only if it is already downloaded through MDM or manually.

- 7 In the **Notification** tab, activate or deactivate the notification for the successful download or install status and enter the notification text in the **Push Notification** field.
- 8 Select **Save** to publish the iOS update.

When the assignment gets saved for the selected iOS update in the UEM console, any eligible, assigned devices will receive the update command on their next check in. Keep in mind a device may not immediately check in depending on your console's settings. After saving, the status of the iOS update will change to Assigned and the status for assigned devices can be monitored in the Update Details page.

**Note:** These settings can be changed at any time after the update has been published.

If devices have multiple iOS update assignments, the deployment settings and iOS version will be evaluated in the following priority:

- 1 Newest iOS version (e.g. iOS 13.3 be prioritized over iOS 13.1).
- 2 Closest assignment at or above the Organization Group where the device is enrolled (e.g. if a device is enrolled at a child Organization Group, the device will take the assignment at the child Organization Group rather than any at a parent level. This assumes the assignments are for the same iOS version).
- 3 Highest priority within the assignment selected based on the first two criteria with an ascending priority (e.g. priority of 1 is higher than a priority of 2).

## Pause and Unpause iOS Updates

As an admin, you can even pause any updates that have been assigned. This holds any updates that have not been sent to iOS devices until the update is unpaused.

To pause an iOS update:

- 1 Navigate to the **Resources > Device Updates > iOS** page.
- 2 Select an assigned iOS update.
- 3 Select the **PAUSE** option at the top of the page.

**Note:** Pausing does not stop the updates that have already been processed on the device such as already downloading the update. Pause only stops the assigned future downloads of the update.

## Monitor iOS Update Assignments

After assigning and publishing iOS updates to devices, the next step is to monitor their deployment.

To see the status of a deployment, select an iOS update from the **Resources > Device Updates > iOS** page to view additional information. The Details section shows the details of the iOS update (such as version details, supported devices and so on). The graphs beneath the Details section are for monitoring and taking action on the assigned devices. Those graphs show:

- **Device Readiness** – Provides information related to the update and the devices enrolled at the organization group and below. This includes devices that are eligible to receive the update, devices that are not eligible to receive the update (e.g. unsupervised, incompatible hardware, etc.), devices that are on higher version, or devices already on the selected version.
- **Device Status** – Provides information on the status of the iOS Update on the assigned, eligible devices. This includes the devices that downloaded the update, installed the update, or failed with a specified error code.
- **Devices** – The table shows the status of the iOS update on eligible and non-eligible devices that are triggered from an assignment. The values of this table are:

Values	Description
Last Seen	The last time the device communicated back to Workspace ONE UEM.
Device Name	The friendly name of the device.
User	The enrollment user's first and last name assigned to the device.
Status	The most recent status received for this iOS version's update.
Reason	Additional context for the status of an update if it was a failure.
Next Retry	An estimate of when the system retries to send the update to the device when a failure occurs. It can be more frequent than the time listed.

The table is also used to take action on devices for the selected update. The actions include:

- **Query** – Request latest information for the device related to the iOS update.
- **Override** – Trigger a Download and/or Install command for the device. It ignores any assignments made for the device previously.

## Manage iOS Updates for Individual Devices

Managing iOS Updates can be achieved at an individual device level for a more direct approach to ensure that the latest updates and their functionalities are applied across a managed device. These updates can be deployed and monitored for an individual device by navigating to **Devices > List View > Select Device > Updates**.

### Publish iOS Updates for a Device

To publish a specific update to a selected device:

- 1 Select **Updates** tab to view the snapshot of the available OS Updates details.
- 2 Select an OS Update name and then select **Publish**. The **Update** page appears.
- 3 Select the preferred **Device Installation Method**.

**Note:** **Download/Install** option for Update Assignments performs either download or install actions based on the status of the OS update on the device.

If the OS update has already been downloaded, then the command installs the OS update. However, if the OS update is not downloaded yet, then the command triggers a download instead. Send the command again after the download is completed to trigger the install.

- 4 Select **Send** to publish the OS Update to the device.
- 5 Select **Query Update Progress** to request the latest status on the update.

**Note:** This does not impact any iOS updates assigned to the device. Any assignments will continue to be published to devices until they are on or above the assigned iOS version.

### Track the Status for iOS Updates

The status for iOS updates are not shown until you schedule an update from the UEM console whether manually publishing or by assigning an update to the device. If an update is downloaded manually on an iOS device, the status of that update will not appear in the **Updates** list view. Once an admin schedules the update, the status on the console is updated. If an update installed manually, this is reflected in the Device Details Summary.

### Troubleshooting

All commands and responses can be seen in event data by navigating to **Device Details → More → Troubleshooting** tab.

## Delay iOS Updates

Admins can delay iOS updates for up to 90 days from when the update is released by Apple using a configuration profile.

To delay an iOS update:

- 1 Navigate to **Resources > Profiles & Baselines > Profiles > Add**.
- 2 Select **Apple > iOS** and configure **Restrictions** settings.

- 3 Select **Delay Updates (Days)** from the **OS Updates Restrictions** subsection.
- 4 Restrict Delay Updates and specify the number of days to delay the software update. Number of days range from 1 to 90. The number of days dictate the length of time after the release of the software update and not after the time of installation of the profile

**Note:** Any managed OS update command will bypass the delay OS updates restriction even if the OS version is within the restriction window of 90 or fewer days. However, if an update is downloaded while a restriction window is active, the update may still not be visible to the user. Once the restriction window expires, the update becomes visible to users.

## Set the Device Name for a Supervised iOS Device

Automatically or manually set an iOS 8+ supervised device name to match the Friendly Name in the UEM console. This feature is helpful when performing asset tracking from the device itself. The device name appears when the device is connected to iTunes and it can be edited in iTunes too.

- 1 Navigate to **Groups & Settings > All Settings > General > Devices & Users > Friendly Name**.
- 2 Select the **Enable Custom Smartphone Friendly Name** to set the device name as the friendly name.
- 3 Enter the **Smartphone Friendly Name Format** by entering the enrollment user, the device model, and device operating system information.
- 4 Select the **Set Device Name to Friendly Name** setting to set this name as the Device Name to match the Friendly Name.
- 5 Select **Save** to update the name.

Apple Global Service Exchange (GSX) allows administrators to look up device details related to the display model name, the device purchase and warranty status directly from the UEM console.

If any devices in an organization group are missing a display model name, then a time scheduler runs periodically to search and update these names using the GSX information that was configured for the devices at that organization group level.

Only authorized Apple employees or organizations that have registered with Apple's Self-Servicing Account Program can access GSX information.

This chapter includes the following topics:

- [Create a GSX Account](#)
- [Obtain an Apple Certificate to Integrate AppleCare GSX](#)
- [Configure AppleCare in the UEM console](#)
- [Obtain an Apple Certificate to Integrate AppleCare GSX](#)
- [Configure AppleCare GSX in the UEM Console](#)

## Create a GSX Account

Before you can integrate your deployment, you must create an Apple GSX account. To apply for a GSX account, you must have a service contract with Apple. Contact your Apple Account Executive to learn more about GSX.

To apply for a GSX account, visit <http://www.apple.com/support/programs/ssa/>.

## Obtain an Apple Certificate to Integrate AppleCare GSX

To integrate AppleCare GSX with your Workspace ONE UEM deployment, you must first obtain an Apple certificates and convert them to .p12 format.

For more information, see *Obtain an Apple Certificate to Integrate AppleCare GSX*.

## Configure AppleCare in the UEM console

Once you have obtained and configured an Apple Certificate, you must upload the certificate to the UEM console and configure your AppleCare instance.

For more information, see *Configure AppleCare GSX in the UEM console*.

## Obtain an Apple Certificate to Integrate AppleCare GSX

To integrate AppleCare GSX with your Workspace ONE UEM deployment, you must first obtain an Apple certificate and convert them to .p12 format.

- 1 Generate a certificate signing request (CSR) using OpenSSL or Java Keytool.
- 2 Send the CSR and the following GSX account information to Apple to receive Apple certificates (.pem files).
  - GSX Sold-To account number
  - Primary IT contact name
  - Primary IT contact email
  - Primary IT contact phone number
  - Outgoing static IP address of the server that sends requests to GSX Production

If your environment is hosted on the AW SaaS, refer to <https://support.air-watch.com/articles/115001662168> for the IP address. If the IP range for your environment is not listed, please open a support ticket to have our Network Operations team facilitate it.

Apple generates the Apple certificate(.pem) and returns a signed certificate and a chain certificate. For ease of use, rename the files “cert.pem” and “chain.pem” for use in subsequent steps.

You may also receive a file labeled “issuer” that is not needed for this process.

- 3 Convert the Apple certificates to .p12 format.
  - a. Create a .p12 file using the private key and Apple certificates by executing the following command: `sudo openssl pkcs12 -export -inkey privatekey.pem -in cert.pem -certfile chain.pem -out GSX_Cert.p12`
  - b. The certificate saves as a .p12 file in the location you specified.

If you do not specify a path before the file name when running the conversion command, the file saves to your working directory.

## Configure AppleCare GSX in the UEM Console

Once you have obtained and configured an Apple Certificate, you must upload the certificate to the UEM console and configure your AppleCare instance.

## Procedure

- 1 Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > AppleCare**.  
To configure a GSX connection with the UEM console, you must have a GSX account with manager-level access, access to web services, and access to coverage and warranty information.

- 2 Enter **GSX settings** including:

Setting	Action
GSX User ID	Enter the account user ID.
GSX Password	Enter the account password.
Sold-to Account Number	Enter the 10-digit service account number. This account number can be found in the GSX portal at the bottom of the web page.
Time Zone	Use the drop-down menu to select the appropriate time zone.
Language	Use the drop-down menu to choose a language.

- 1 Select **Save** to complete the integration with AppleCare.
- 2 Navigate to the **List View**, select a device, and use the **More** menu to find AppleCare information in the UEM console.
- 3 Navigate to **Accounts > Administrators** and pull the information from **Details** section.
- 4 In the **Add/Edit Admin** page, add the GSX User ID and click **SAVE**.

You can now make GSX API calls.

Shared Device/Multi-User Device functionality in Workspace ONE UEM powered by AirWatch ensures that security and authentication are in place for every unique end user. Shared devices can also allow only specific end users to access sensitive information.

Issuing a device to every employee in certain organizations can be expensive. Workspace ONE UEM powered by AirWatch lets you share a mobile device among end users in two ways: using a single fixed configuration for all end users, or using a unique configuration setting for individual end users.

When administering shared devices, you must first provision the devices with applicable settings and restrictions before deploying them to end users. Once deployed, Workspace ONE UEM uses a simple login or log-out process for shared devices in which end users simply enter their directory services or dedicated credentials to log in. The end-user role determines their level of access to corporate resources such as content, features, and applications. This role ensures the automatic configuration of features and resources that are available after the user logs in.

The login or log-out functions are self-contained within the Workspace ONE Intelligent Hub. Self-containment ensures that the enrollment status is never affected, and that the device is managed whether it is in use or not.

Shared Device capabilities are also possible natively on Apple iPads integrated with Apple Business Manager. This functionality called Shared iPads for Business leverages the user's Managed Apple ID for login and does not take place in the Workspace ONE Intelligent Hub for login and logout. To know more about configuring Shared iPads for Business with Apple Business Manager and steps to achieve this functionality, see **Shared iPads for Business** in *Introduction to Apple Business Manager Guide* available on [docs.vmware.com](https://docs.vmware.com).

## Shared Devices Capabilities

There are basic capabilities surrounding the functionality and security of devices that are shared across multiple users. These capabilities offer compelling reasons to consider shared devices as a cost-effective solution to making the most of enterprise mobility.

### Functionality

- Personalize each end-user experience without losing corporate settings.
- Logging in a device configures it with corporate access and specific settings, applications, and content based on the end-user role and organization group (OG).

- Allow for a log in/log out process that is self-contained in the Workspace ONE Intelligent Hub or Workspace ONE Access.
- After the end user logs out of the device, the configuration settings of that session are wiped. The device is then ready for login by another end user.

### Security

- Provision devices with the shared device settings before providing devices to end users.
- Log in and log out devices without affecting an enrollment in Workspace ONE UEM.
- Authenticate end users during a login with directory services or dedicated Workspace ONE UEM credentials.
- Authenticate end users using Workspace ONE Access.
- Manage devices even when a device is not logged in.

### Platforms That Support Shared Devices

The following devices support shared device/multi-user device functionality.

- Android 4.3 or later
- iOS devices with Workspace ONE Intelligent Hub 4.2 or later.
  - For details about logging in and out of shared iOS devices, see the topic *Log In and Log Out of Shared iOS Devices* in the **iOS Platform Guide**, available on [docs.vmware.com](https://docs.vmware.com).
- MacOS devices with Workspace ONE Intelligent Hub 2.1 or later.

This chapter includes the following topics:

- [Define the Shared Device Hierarchy](#)
- [Configure Shared Devices](#)

## Define the Shared Device Hierarchy

While strictly optional, making an organization group (OG) specific to shared devices offers many benefits due to multi-tenancy and inherited device settings.

If you have a large number of shared devices in your fleet and you want to manage them apart from single user devices, you can make a shared device-specific OG. Making a shared device hierarchy in your OG structure is optional. Features like smart groups and user groups mean you do not have to rely strictly on OG hierarchy design to simplify device management.

However, having a shared device OG (or nested OGs) simplifies device management by enabling you to standardize device functionality through profiles, policies, and device inheritance without the processing overhead required by a smart group or a user group.

- 1 Navigate to **Groups & Settings > Groups > Organization Groups > Organization Group Details**.

Here, you can see an OG representing your company.

- 2 Ensure the **Organization Group Details** displayed are accurate, and then use the available settings to make modifications, if necessary. If you make changes, select **Save**.
- 3 Select **Add Child Organization Group**.
- 4 Enter the following information for the first OG underneath the top-level OG.

Setting	Description
Name	Enter a name for the child organization group (OG) to be displayed. Use alphanumeric characters only. Do not use odd characters.
Group ID	Enter an identifier for the OG for the end users to use during the device login. Group IDs are used during the enrollment of group devices to the appropriate OG.

Ensure that users sharing devices receive the **Group ID** as it might be required for the device to log in depending on your Shared Device configuration. If you are not in an on-premises environment, the Group ID identifies your organization group across the entire shared SaaS environment. For this reason, all Group IDs must be uniquely named.

Setting	Description
Name	Enter a name for the child organization group (OG) to be displayed. Use alphanumeric characters only. Do not use odd characters.
GroupID	Enter an identifier for the OG for the end users to use during the device login. Group IDs are used during the enrollment of group devices to the appropriate OG. Ensure that users sharing devices receive the <b>Group ID</b> as it might be required for the device to log in depending on your Shared Device configuration. If you are not in an on-premises environment, the Group ID identifies your organization group across the entire shared SaaS environment. For this reason, all Group IDs must be uniquely named.
Type	Select the preconfigured OG type that reflects the category for the child OG.
Country	Select the country where the OG is based.
Locale	Select the language classification for the selected country.
Customer Industry	This setting is only available when <b>Type</b> is Customer. Select from the list of Customer Industries.
Time Zone	Select the time zone for the OG's location.

- 1 Build out your corporate hierarchical structure by creating more groups and subgroups in the same manner.
  - a. If you are configuring a **Fixed Organization Group**, then ensure that you create the single organization group for end users to log in or log out.
  - b. If you configure **Prompt Users for Organization Group**, then ensure that you have created the multiple OGs for end-user roles for logging in or logging out. For more information, see *Configure Shared Devices*.
- 2 Select **Save**.

## Configure Shared Devices

Similar to single-user device staging, multi-user staging (a "shared device") allows an IT administrator to provision devices to be used by more than one user.

- 1 Navigate to **Groups & Settings > All Settings > Devices & Users > General > Shared Device**.
- 2 Select **Override** and complete the **Grouping** section.

Setting	Description
<b>Group Assignment Mode</b>	Configure devices in one of three ways: Select <b>Prompt User for Organization Group</b> to have the end user enter a Group ID for an organization group upon login. With this method, you have the flexibility to provide access to the settings, applications, and content of the organization group entered. Using this approach, an end user is not restricted to accessing only the settings, applications, and content for the organization group to which they are enrolled. Select <b>Fixed Organization Group</b> to limit your managed devices to settings and content applicable to a single organization group. Each end user who logs in to a device has access to the same settings, applications, and content. This method can be beneficial in a retail use case where employees use shared devices for similar purposes such as checking inventory. Select <b>User Group Organization Group</b> to enable features based on both user groups and organization groups across your hierarchy. When an end user logs in to a device, they have access to specific settings, applications, and content based on their assigned role within the hierarchy. For example, an end user is a member of the 'Sales' user group, and that user group is mapped to the 'Standard Access' organization group. When that end user logs in to the device, the device is configured with the settings, applications, and content available to the 'Standard Access' organization group. You can map user groups to organization groups on the UEM console. Navigate to <b>Groups &amp; Settings &gt; All Settings &gt; Devices &amp; Users &gt; General &gt; Enrollment</b> . Select the <b>Grouping</b> tab and fill in the required details.
<b>Always Prompt for Terms of Use</b>	Prompts the end users to accept your <b>Terms of Use</b> agreement before they log in to a device.

- 3 Complete the **Security** section, as applicable.

Setting	Description
Require Shared Device Passcode	<b>(For iOS devices only)</b> Require users to create a Shared Device passcode in the Self-Service Portal to check out devices. This passcode is different from a Single Sign On passcode or a device-level passcode.
Require Special Characters	Require special characters in the shared device passcode, which includes characters such as @, %, &, and so forth.
Shared Device Passcode Minimum Length	Set the minimum character length of the shared passcode.
Shared Device Passcode Expiration Time (days)	Set the length of time (in days) the shared passcode expires.
Keep Shared device Passcode for minimum time (days)	Set the minimum amount of time (in days) the shared device passcode must be changed.
Prompt users to change their Shared Device Passcode x (days) before expiration	<b>(For iOS devices only)</b> Set the number of days the user is reminded to change their shared device passcode before it expires. For best results, set a value less than the difference between the Expiration Time and minimum time you can keep the Shared Device Passcode.

Setting	Description
Passcode History	Set the number of passcodes that are remembered by the system, providing a more secure environment by preventing the user from reusing old passcodes.
Auto Logout	Configure an automatic log out after a specific time period.
Auto Logout After	Set the length of time that must elapse before the <b>Auto Log out</b> function activates in <b>Minutes, Hours, or Days</b> .
iOS Single App Mode	<p>Select this check box to configure Single App Mode, which locks the device into a single application when an end user logs in to the device. To check out an iOS device in Single App Mode, end users log in using their credentials. When the device is checked in again, it returns to Single App Mode.</p> <p>Enabling Single App Mode also deactivates the Home button on the device. <b>Note:</b> Single App Mode applies only to Supervised iOS devices.</p>

Configure the **Logout Settings**, as applicable.

Setting	Description
Clear Android App Data	Clear the app data when the user logs out of a shared device (checks it in).
Reinstall Android Apps	Use the drop-down to select whether to Always reinstall app between users or never reinstall app between users. For Android (Legacy) deployments, you can opt to reinstall app if the Hub cannot clear app data between users.
Clear Android Device Passcode	This setting controls whether the current Android device passcode is cleared when the user logs out (checks in) a multi-user shared device.
Allow PIN at Startup	Activate or deactivate Android Secure Startup, which requires an initial PIN entry to boot up the device. If deactivated, users cannot enable Secure Startup during passcode setup. If Secure Startup is already deactivated on the device, the device must be factory reset to enable it. This feature applies only to Android devices that do not have file-based encryption.
Clear iOS Device Passcode	This setting controls whether the current iOS device passcode is cleared when the user logs out (checks in) a multi-user shared device.

Select **Save**.

## Log In and Log Out of Shared iOS Devices

You can log in to and out of an iOS device that is shared across multiple users.

- 1 Run the Workspace ONE Intelligent Hub on the device.
- 2 Enter the end-user credentials.

If the device is already logged in to Workspace ONE Intelligent Hub, then users are prompted to enter an SSO Passcode. If the device is not logged in, then users are prompted to enter a user name and password. The profiles assigned to each user are pushed down based on the smart group and user group association.

**Note:** If **Prompt User for Organization Group** is enabled, then end users are required to enter a **Group ID** to log in to a device.

3 Select **Login** and accept the **Terms of Use**.

**Note:** If prompted for a passcode, users can create one in the Self-Service Portal. These passcodes are subject to an expiration period. As the expiration period nears, the Workspace ONE Intelligent Hub prompts users to change the passcode on the device. If users do not change their passcode before it expires, users must return to the Self-Service Portal to create another passcode.

To log out of an iOS device, run the Workspace ONE Intelligent Hub and select **Log Out** at the bottom.

# iOS Functionality Matrix: Supervised vs. Unsupervised

16

The following table shows all the available iOS profile functionality that you can control using the UEM console and the minimum iOS version that applies.

Features and Functionality	Does Not Require Supervision	Requires Supervision	OS Notes
<b>Passcode</b>			
Passcode settings	✓		-
<b>Wi-Fi</b>			
Wi-Fi settings	✓		-
Auto-Join	✓		iOS 7
Wi-Fi Hotspot 2.0 settings	✓		iOS 7
Proxy settings	✓		iOS 7
QOS Marking Policy	✓		iOS 10
<b>VPN</b>			
VPN settings	✓		-
Per-App VPN	✓		iOS 7
Connect automatically	✓		iOS 7
<b>Email</b>			
Email settings	✓		-
Prevent Moving Messages	✓		iOS 7
Disable recent contact sync	✓		iOS 7
Prevent Use In 3rd Party Apps	✓		iOS 7
Use S/MIME	✓		iOS 7
<b>Exchange ActiveSync</b>			
EAS settings	✓		-

Features and Functionality	Does Not Require Supervision	Requires Supervision	OS Notes
Use S/MIME	✓		iOS 7
Per-Message S/MIME	✓		iOS 8
Prevent Moving Messages	✓		iOS 7
Prevent Use In 3rd Party Apps	✓		iOS 7
Disable recent contact sync	✓		iOS 7
Prevent Mail Drop	✓		iOS 9
Default Calling App	✓		iOS 10
<b>LDAP</b>			
LDAP settings	✓		-
<b>CalDAV</b>			
CalDAV settings	✓		-
<b>Subscribed Calendars</b>			
Subscribed Calendar settings	✓		-
<b>CardDAV</b>			
CardDAV settings	✓		-
<b>Web Clips</b>			
Web Clip settings	✓		-
<b>Credentials</b>			
Credentials certificate settings	✓		-
<b>SCEP</b>			
SCEP settings for certificate authority	✓		-
<b>Global HTTP Proxy</b>			
Global HTTP Proxy settings		✓	iOS 7
<b>Single App Mode</b>			
Single App Mode – Lock device into a single app		✓	iOS 7
Optional settings for "Lock device into a single app"		✓	iOS 7
Autonomous single app mode		✓	iOS 7
<b>Web Content Filter</b>			

Features and Functionality	Does Not Require Supervision	Requires Supervision	OS Notes
Web Content Filter settings (Allowlist, Denylist, Permitted URLs)		✓	iOS 7
Web Content Filtering with 3rd Party Provider		✓	iOS 8
<b>Managed Domains</b>			
Managed Email Domains	✓		iOS 8
Managed Web Domains	✓		iOS 8
Managed Safari Password Domains	✓		iOS 9.3
<b>Network Usage Rules</b>			
Network Usage Rules	✓		iOS 9
<b>macOS Server Accounts</b>			
macOS Server Accounts	✓		iOS 9
<b>Single Sign On</b>			
Single Sign On settings with Kerberos authentication	✓		iOS 7
Single Sign On settings with Renewal certificates	✓		iOS 8
<b>AirPrint</b>			
AirPrint destination settings	✓		iOS 7
<b>AirPlay Mirroring</b>			
AirPlay Destination settings (Allowlist)		✓	iOS 7
AirPlay Passwords	✓		
<b>Access Point</b>			
Advanced Access Point settings	✓		
<b>App Installation Settings</b>			
Silent App Installation		✓ +VPP	
Control Cellular Settings			
Voice Roaming	✓	✓	iOS 7
Data Roaming	✓	✓	iOS 7
Personal Hotspot	✓	✓	iOS 7
<b>Wallpaper Settings</b>			

Features and Functionality	Does Not Require Supervision	Requires Supervision	OS Notes
Set Lock Screen Image		✓	iOS 7
Set Lock Screen Message		✓	iOS 9.3+
Set Home Screen Image		✓	iOS 7
Set Home Screen Layout		✓	iOS 9.3+
<b>Notifications</b>			
Notification settings		✓	iOS 9.3+
<b>Queries and Commands</b>			
Supervised status	✓		iOS 7
Personal Hotspot status	✓		iOS 7
Clear Activation Lock		✓	iOS 7
Clear Restrictions Passcode		✓	iOS 8
Configure iOS Updates		✓	iOS 9 Prior to iOS 10.3, DEP is also required