VMware AirWatch iOS Platform Guide

Deploying and managing iOS devices

Workspace ONE UEM v9.7

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Table of Contents

Chapter 1:
Introduction to Workspace ONE UEM for iOS

Overview

Workspace ONE UEM 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.

Supported iOS Devices

Workspace ONE UEM supports iPhone, iPad, and iPod Touch devices running iOS v.5.0 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.

iOS Admin Task Prerequisites

You need the following information to perform many of the tasks in this guide. 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.

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 Workspace ONE UEM 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.

Chapter 2:
iOS Device Enrollment Overview

Overview

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.

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, see iOS Device Enrollment Requirements on page 8.

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 agent-based and agentless enrollment types. Use this matrix to determine what type of enrollment meets your organization's needs.

For a comparison between agent-based and browser-based enrollments, see Capabilities Based on Enrollment Type for iOS Devices on page 9.

Agent-Based Enrollment

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

For more information, see AirWatch Agent for iOS on page 57 and Enroll an iOS Device with the AirWatch Agent on page 11.

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 AirWatch Agent.

For more information, see Enroll an iOS Device with the Safari Browser on page 12.

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 Apple Configurator 2 and the Apple 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, see Bulk Enrollment of iOS Devices Using Apple Configurator on page 12.

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, see Device Enrollment with the Apple Device Enrollment Program (DEP) on page 12.

iOS Device Enrollment Requirements

To enroll an iOS device, you or your end users need the following information. The information the users need depends on whether you associated 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.
- **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 agent-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://<environment name>.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 agent-based enrollment.

Capabilities Based on Enrollment Type for iOS Devices

The following matrix lists supported features for agent-based and agentless enrollment types. Use this matrix to determine what type of enrollment meets your organization's needs.

Feature	Agent-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°	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
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

Feature	Agent-Based	Agentless
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†
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*

º 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 AirWatch Agent

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

If you want to take full advantage of AirWatch Agent capabilities while also allowing Web enrollment, You can require that users enroll through the AirWatch Agent. This setting prevents end users from enrolling if they have not downloaded the AirWatch Agent.

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

To enroll an iOS device:

1. Navigate to **AWAgent.com** from the Safari browser. Workspace ONE UEM automatically prompts end users to go to the App Store to download the AirWatch Agent app. Follow the download prompts. An Apple ID is required to download the AirWatch Agent from the iTunes store.
2. Tap the AirWatch Agent application to start it. Select one of the following authentication methods:
   - **Email Address** – Select if autodiscovery is configured in your environment. In addition, you may be prompted to select a Group from a drop-down menu.
   - **Server Details** – Select to enroll using the server URL, which is the network location of your organization's Workspace ONE UEM instance and the Group ID of the group associated with your device.
   - **QR Code** – Select and use the device to scan the QR code that was distributed by email.
3. Enter credentials, which may include either a **username** and **password**, or a **token** or a combination of both to authenticate the device.
   - If the end user enters 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. Tap **Next** after you complete each page.
   - Accept your organization's **Terms of Use**, if applicable.
   - Select your **Device Ownership** type, if applicable.
   - Enter the device **Asset Number**, if applicable.
5. Select **Redirect & Enable** to allow for mobile device management.
6. Tap **Install** to allow the MDM profile to install.
7. Tap **Open** to open the page in "Agent."
8. Tap **Done** to complete enrollment. A "Success" message is displayed. Enrollment into Workspace ONE UEM is now complete.
   - 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.
   - Optionally, choose to tap **Open** to see AirWatch Agent 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 AirWatch Agent.

If you do not want to require the AirWatch Agent for web-based enrollment (as a result performing "agentless" enrollment), then navigate to **Groups & Settings > All Settings > Devices & Users > General.** Make sure that the **Require Agent Enrollment for iOS** check box is not selected.

To perform web-based enrollment:

1. Open Safari on the iOS device.
2. Navigate to **https://<Environment_URL>.com/enroll**.
3. Select whether to authenticate using your **Email Address** (if autodiscovery has been set up for your environment) or **Group ID**. Select **Next**.
4. Enter the required information, depending on which authentication method you selected.
5. Enter your user name and password, if applicable.
6. Accept the **Terms of Use**, if applicable.
7. Install the MDM profile when prompted and accept the MDM warning message by selecting **Install**. Accept any prompts for trust, if applicable.

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 Device Enrollment Program (DEP)

To maximize the benefits of Apple devices enrolled in Mobile Device Management (MDM), Apple has introduced the Device Enrollment Program (DEP). 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 OS updates for all end users.

For more information, see the Apple Business Support Portal portal or the Apple Device Enrollment Program Guide, or contact your Apple representative.

Chapter 3:
iOS Device Profiles

Overview

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.

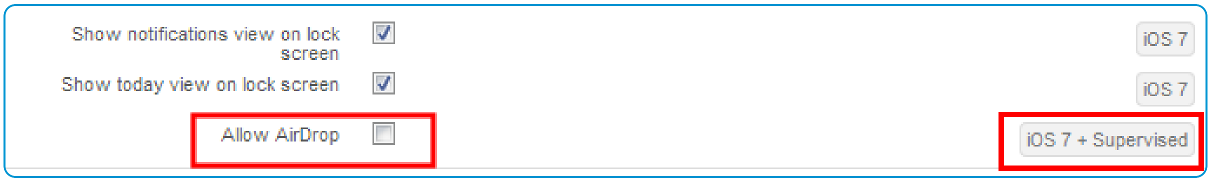
A profile consists of the general profile settings and a specific payload. Profiles work best when they contain only a single payload.

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.



Show notifications view on lock screen ☑ iOS 7

Show today view on lock screen ☑ iOS 7

Allow AirDrop ☐ iOS 7 + Supervised

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, please see the **VMware Workspace ONE UEM Integration with Apple Configurator** or the **Workspace ONE UEM Guide for Apple Device Enrollment Program**. To see a complete list of the iOS system requirements and supervision options, see Appendix – iOS Functionality: Supervised vs. Unsupervised.

Device Access

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

Some examples of device access profiles include:

- Secure a device with a Passcode profile. For more information, see Configure a Device Passcode Profile (iOS) on page 17
- Limit the device to a single application with a Single App Mode profile. For more information, see Configure a Single App Mode Profile (iOS) on page 43.

Device Security

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

Some examples of device security profiles include:

- Use a Wi-Fi profile to connect enrolled devices to your corporate Wi-Fi without sending the network credentials to users. For more information, see Configure a Wi-Fi Profile (iOS) on page 23.
- Implement digital certificates to protect corporate assets. For more information, see Configure a SCEP/Credentials Profile (iOS) on page 41
- Ensure access to internal resources for your devices with the VPN profile. For more information, see Configure a Virtual Private Network (VPN) Profile (iOS) on page 26.

Device Configuration

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

Some examples of device configuration profiles include:

- Set up an Exchange account on a device with an Exchange ActiveSync profile. For more information, see Configure an EAS Mail Profile using Native Mail Client (iOS) on page 35.
- Whitelist a specific set of devices to receive Apple TV broadcast privileges with the AirPlay profile. For more information, see Configure a AirPlay Whitelist Profile (iOS) on page 50.
- Ensure that the devices remain up to date with the iOS Updates profile. For more information, see Configure iOS Updates for iOS Devices on page 83.

iOS Device Profiles

Overview

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.

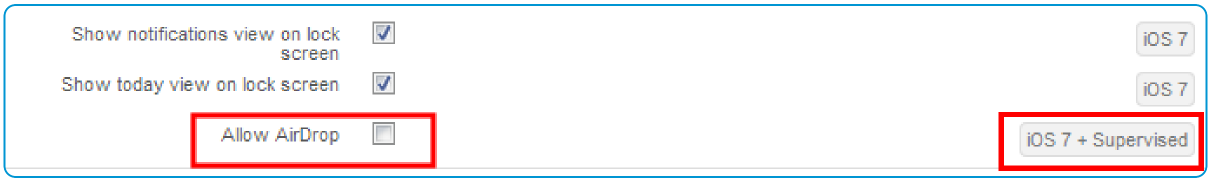
A profile consists of the general profile settings and a specific payload. Profiles work best when they contain only a single payload.

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.



Show notifications view on lock screen ☑ iOS 7

Show today view on lock screen ☑ iOS 7

Allow AirDrop ☐ iOS 7 + Supervised

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, please see the **VMware Workspace ONE UEM Integration with Apple Configurator** or the **Workspace ONE UEM Guide for Apple Device Enrollment Program**. To see a complete list of the iOS system requirements and supervision options, see Appendix – iOS Functionality: Supervised vs. Unsupervised.

Device Access

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

Some examples of device access profiles include:

- Secure a device with a Passcode profile. For more information, see Configure a Device Passcode Profile (iOS) on page 17
- Limit the device to a single application with a Single App Mode profile. For more information, see Configure a Single App Mode Profile (iOS) on page 43.

Device Security

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

Some examples of device security profiles include:

- Use a Wi-Fi profile to connect enrolled devices to your corporate Wi-Fi without sending the network credentials to users. For more information, see Configure a Wi-Fi Profile (iOS) on page 23.
- Implement digital certificates to protect corporate assets. For more information, see Configure a SCEP/Credentials Profile (iOS) on page 41

- Ensure access to internal resources for your devices with the VPN profile. For more information, see Configure a Virtual Private Network (VPN) Profile (iOS) on page 26.

Device Configuration

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

Some examples of device configuration profiles include:

- Set up an Exchange account on a device with an Exchange ActiveSync profile. For more information, see Configure an EAS Mail Profile using Native Mail Client (iOS) on page 35.
- Whitelist a specific set of devices to receive Apple TV broadcast privileges with the AirPlay profile. For more information, see Configure a AirPlay Whitelist Profile (iOS) on page 50.
- Ensure that the devices remain up to date with the iOS Updates profile. For more information, see Configure iOS Updates for iOS Devices on page 83.

Device Passcode Profiles 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**. After five failed attempts, the device is disabled for a determined time.
- **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 (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.

To create a passcode profile:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add**. Select **Apple iOS**.
2. Configure the profile's **General** settings.
3. Select the **Passcode** payload from the list.
4. Configure **Passcode** settings, including:

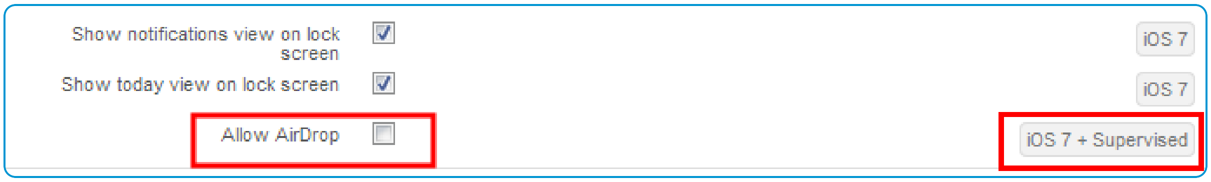
Setting	Description
Require passcode on device	Enable mandatory passcode protection.
Allow simple value	Allow the end user to apply a simple numeric passcode.
Require Alphanumeric Value	Restrict the end user from using spaces or non-alphanumeric characters in their passcode.
Minimum Passcode Length	Select 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.

5. Select **Save & Publish**.

Device 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.



Show notifications view on lock screen ☑ iOS 7

Show today view on lock screen ☑ iOS 7

Allow AirDrop □ iOS 7 + Supervised

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 Appendix A – iOS Functionality: Supervised vs. Unsupervised.

Restriction Profile Configurations for iOS Devices

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 (iOS) on page 23.

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

OS Update Restrictions

OS level software delay restriction allows you to perform a force delay in updating OS especially from updates being visible to end user for the 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+ 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 disable core device functionality such as the camera, FaceTime, Siri, and in-app purchases to help improve productivity and security. Available restrictions include:

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

  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 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 higher)

Featured iOS 8 Device Restrictions

- Disable Handoff, which can be used to start an activity on one device, locate other devices and resume activities on shared apps.
- Disable Internet search results in Spotlight. This restriction prevents suggested Web sites from appearing when searching using Spotlight. (iOS 8+ supervised)
- Disable configuration of the Restrictions setting. This permission allows administrators to override configuration of personal restrictions through the device's Settings menu. (iOS 8 + supervised)

- Prevent the end user from erasing all content and settings on the device. This restriction prevents users from wiping and unenrolling the device. (iOS 8+ supervised)
- Disable local data storage by backing up managed apps with iCloud.
- Disable backup of enterprise books with iCloud.
- Prevent users from syncing notes and highlights in enterprise books with iCloud.
- Disable adding or removing existing Touch ID information (iOS 8.1.3 + supervised)
- Disable Podcasts.This restriction prevents access to Apple's podcasts application. (Supervised only)

Featured iOS 9 Restrictions

- Disable passcode modification, which prevents a device passcode from being added, changed or removed. (Supervised only)
- Hide the App Store. This restriction disables 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)
- Disable 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)
- Disable device name modification. This restriction prevents end users from changing the device name. Consider this restriction for shared and staged device deployments.(Supervised only)
- Disable wallpaper modification. This restriction prevents the user from changing the device wallpaper. (Supervised only)
- Disable 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.
- Disable keyboard shortcuts to prevent users from creating and using keyboard shortcuts. (Supervised only)
- Disable News to prevent access to Apple's News application. (Supervised only)
- Disable iCloud Photo Library. This restriction prevents photos that are not fully downloaded from the library from being stored locally.
- Disable 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.
- Disable video recording by restricting screen capture to prevent end users from capturing the device display.
- Disable Music service, which restricts the Music app from installing. (8.3.3+, Supervised only)

Featured iOS 9.3 Restrictions

- Disable 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

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

Application-Level Restrictions

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

- Disable 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 Web sites.
- 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.
- Enable or disable individual native and other applications by adding them to whitelists or blacklists. This restriction allows you to show or hide applications as needed. (iOS 9.3+ Supervised only)
  - Whitelist webclips by adding the webclip to the `com.apple.webapp` list.

iCloud Restrictions

For devices running iOS 7 and higher, 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 higher devices that can disable 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 Disabled on Device
Restrict iCloud Configuration (device functionality restriction)		
Restrict the ability to sign into and configure iCloud settings	Allow Account Modification (requires Supervision)	Disables iCloud option under device Settings (iOS 7+ 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)

Administrative Requirement	Restriction	Setting Disabled on Device
Prevent users of managed applications from storing documents to iCloud	Allow managed apps to store data	Disables managed applications from storing documents within iCloud drive (iOS 8)
Prevent users from backing up Enterprise books to iCloud	Allow backing up Enterprise books	Disables 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	Disables 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	Disables "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+ Supervised 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 Web sites 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+ devices from connecting t to unknown or malicious networks. Devices enabled with this restriction can only connect to managed Wifi networks. Select **Force WiFi Whitelisting** 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.

Configure a Device Restriction Profile (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.

To create a restrictions profile:

1. Navigate to **Devices > Profiles & Resources > 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 Configurations for iOS Devices on page 19.
5. Select **Save & Publish**.

Configure a Wi-Fi Profile (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.

To create a Wi-Fi profile:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add**. Select **Apple iOS**.
2. Configure the profile's **General** settings.
3. Select the **Wi-Fi** payload from the list.
4. Configure **Wi-Fi** settings.

Setting	Description
Service Set Identifier	Enter the name of the network where the device connects.

Setting	Description
Hidden network	Enter a connection to a network that is not open or broadcasting.
Auto-Join	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.
Security Type	Select the type of access protocol to be used. Enter the **Password** or select the **Protocols** that apply to your Wi-Fi network.
Protocols	Choose protocols for network access. • This option appears when **WiFi** and **Security Type** is any of the **Enterprise** choices. This option also appears when **Ethernet** is selected.
Passpoint	
Wi-Fi Hotspot 2.0	Enable Wi-Fi Hotspot 2.0 functionality and is only available for iOS 7 and higher devices. Hotspot 2.0 is a type of public-access Wi-Fi that allows devices to identify and connect seamlessly to the best match access point. Carrier plans must support Hotspot 2.0 for it to function correctly.
Domain Name	Enter the domain name of the Passpoint service provider.
Allow connecting to roaming partner Passpoint networks	Enable roaming to partner Passpoint networks.
Displayed Operator Name	Enter the name of the Wi-Fi hotspot service provider.
Roaming Consortium Organization ID	Enter the roaming consortium organization identifiers.
Network Access ID	Enter the Network Access ID realm names.
MCC/MNC	Enter the Mobile Country Code/Mobile Network Configuration formatted as a 6-digit number.
Authentication	
Configure **Authentication** settings that vary by protocol.	
User name	Enter the username for the account.

Setting	Description
User Per-Connection Password	Request the password during the connection and send with authentication.
Password	Enter the password for the connection.
Identity Certificate	Select the certificate for authentication.
Outer Identity	Select the external authentication method.
TLS Minimum Version	Select the minimum TLS version 1.0, 1.1, and 1.2. If no value is selected, the minimum TLS version defaults to 1.0 **Note:** Minimum and Maximum TLS versions can be configured only for TLS , TTLS, EAP-Fast, and PEAP protocol types.
TLS Maximum Version	Select the maximum TLS version 1.0, 1.1, and 1.2. If no value is selected, he maximum TLS version defaults to 1.2
Trust	
Trusted Certificates	These are the trusted server certificates for your Wi-Fi network.
Trusted Server Certificate Names	Enter the trusted server certificate names
Allow Trust Exceptions	Allow end users to make trust decisions.

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

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

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

7. (Optional) Configure **Captivate Portal** to bypass the portal.

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

Configure a Virtual Private Network (VPN) Profile (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 seamless access to email, files, and content.

To create a base VPN profile:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add**. Select **Apple iOS**.
2. Configure the profile's **General** settings.
3. Select the **VPN** payload.
4. Configure **Connection** information, including:

   The settings that you see may vary depending on the **Connection Type** you choose. If you are using Forcepoint or Blue Coat for content filtering, see Creating a Forcepoint Content Filter Profile and Creating a Blue Coat Content Filter Profile.

Settings	Description
Connection Name	Enter the name of the connection to be displayed on the device.
Connection Type	Use the drop-down menu to select the network connection method.
Server	Enter the hostname or IP address of the server for connection.
Account	Enter the name of the VPN account.
Send All Traffic	Select to force all traffic through the specified network.
Disconnect on Idle	Allow the VPN to auto-disconnect after a specific amount of time. Support for this value depends on the VPN provider.
Per App VPN Rules	Select to enable Per App VPN. For more information, see Configuring Per-App VPN for iOS Devices.
Connect Automatically	Select to allow the VPN to connect automatically to chosen Safari Domains. This option appears when **Per App VPN** is selected.
Provider Type	Select the provider type either AppProxy, or Packet Tunnel, or None.
Authentication	Choose the method to authenticate to end users. Follow the related prompts to upload an **Identity Certificate**, or enter a **Password** information, or the **Shared Secret** key to be provided to authorize end users for VPN access.
Enable VPN On Demand	Enable VPN On Demand to use certificates to establish VPN connections automatically using the Configuring VPN On Demand for iOS Devices section in this guide.
Proxy	
Proxy	Select either **Manual** or **Auto** proxy type to configure with this VPN connection.

Settings	Description
Server	Enter the URL of the proxy server.
Port	Enter the port used to communicate with the proxy
Username	Enter the user name to connect to the proxy server.
Password	Enter the password for authentication.
Vendor Configurations	
Vendor Keys	Select to create custom keys to go into the vendor config dictionary.
Key	Enter the specific key provided by the vendor.
Value	Enter the VPN value for each key.

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

5. Select **Save & Publish**. End users now have access to permitted sites.

Configure a Forcepoint Content Filter Profile (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**.

1. Navigate to **Devices > Profiles & Resources > Profiles > Add**. Select **Apple iOS**.
2. Configure the profile's **General** settings.
3. Select the **VPN** payload.
4. Select **Websense (Forcepoint)** as the **Connection Type**.
5. Configure **Connection** Info including:

Settings	Description
Connection Name	Enter the name of the connection name to be displayed.

Settings	Description
Username	Enter the user name to connect to the proxy server.
Password	Enter the password for connection.

6. Optionally, you can also **Test Connection**.

7. Configure **Vendor Configurations** settings.

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

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

Configure a Blue Coat Content Filter Profile (iOS)

Workspace ONE UEM integration with Blue Coat lets you use your existing content filtering rules in Blue Coat. Allow or block access to Web sites according to the rules you configure in Blue Coat and then deploy a VPN payload to force devices to comply with those rules.

1. Navigate to **Devices > Profiles & Resources > Profiles > Add**. Select **Apple iOS**.

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

3. Select the **VPN** payload.

4. Select **Blue Coat** as the **Connection Type**.

Setting	Description
Blue Coat Customer ID	Access this value by logging in to the Blue Coat Web site and accessing the API Tokens & Keys section, which lets you add an MDM partner and obtain the identifier. Contact Blue Coat for additional information or assistance.
Per-App VPN	Optionally enable Per App VPN. For more information, see Configuring Per-App VPN for iOS Devices.

5. You can also optionally select **Test Connection**.

6. Configure **Vendor Configurations**:

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

7. Select **Save & Publish**. End users now have access to permitted sites based on your Blue Coat content filtering rules.

Configure a VPN On Demand (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.

Use the following instructions to distribute certificates through the UEM console during configuration and set up VPN On Demand.

1. Ensure your certificate authority and certificate templates in Workspace ONE UEM are properly configured for certificate distribution.
2. 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.
3. Navigate to **Devices > Profiles & Resources > Profiles > Add**, then **iOS**.
4. Select the **VPN** payload from the list.
5. Configure your base VPN profile accordingly.
6. Select **Certificate** from the **User Authentication** drop-down menu.
   - Navigate to the **Credentials** payload.
     - From the **Credential Source** drop-down menu, select **Defined Certificate Authority**.
     - Select the **Certificate Authority** and **Certificate Template** from the respective drop-down menus.
   - Navigate back to the **VPN** payload.
7. Select the **Identity Certificate** as specified through the **Credentials** payload if you are applying certificate authentication to the VPN profile.
8. Select the **Enable VPN On Demand** box.
9. 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
Use new On Demand Keys (iOS 7 and higher)	Select to use the new syntax that allows for specifying more granular VPN rules.
On Demand Rule/Action	Choose an **Action** to define VPN behavior to apply to the VPN connection based on the definedcriteria. If the criterion is true, then the action specified takes place. • **Evaluate Connection**: 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. • **Connect**: Automatically establish the VPN tunnel connection on the next network attempt if the network criteria met. • **Disconnect**: Automatically disable the VPN tunnel connection and do not reconnect on demand if the network criteria are met. • **Ignore**: Leave the existing VPN connection, but do not reconnect on demand if the network criteria are met.
Action Parameter	Configure **Action Parameters** 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 **Evaluate Connection**, these options appear: • Choose **Connect If Needed/Never Connect** and enter additional information: ◦ **Domains** – Enter the domains for which this evaluation applies. ◦ **URL Probe** – 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. ◦ **DNS Servers** – 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)

Setting	Description
Criteria/Value for Parameter	- **Interface Match** – Select the type of connection that matches device's network current adapter. Values available are **any**, **Wifi**, **Ethernet**, and **Cellular**. - **URL Probe** – 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). - **SSID Match** – 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. - **DNS Domain Match** – Enter the device's current network search domain. A wildcard is supported (*.example.com). - **DNS Address Match** – 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.*).

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

Setting	Description
Match Domain or Host	On Demand Action - **Establish if Needed** or **Always Establish** – Initiates a VPN connection only if the specified page cannot be reached directly. - **Never Establish** – 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.

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

11. Choose a **Proxy** type:

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

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

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

13. 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.

Configure a Per-App VPN Profile (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.

Configure the Per-App VPN Profile

1. Navigate to **Devices > Profiles & Resources > Profiles > Add** and select **iOS**.
2. Select the **VPN** payload from the list.
3. Configure your base VPN profile accordingly.
4. 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.
5. Select **Connect Automatically** to display text boxes for the **Safari Domains**, which are internal sites that trigger an automatic VPN connection.
6. Choose a **Provider Type** to determine how to tunnel traffic, either through an application layer or IP layer.
7. 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 that application to use the defined VPN profile when establishing connections.

1. Navigate to **Apps & Books > Applications > Native**.
2. Select the **Public** tab.
3. Select **Add Application** to add an app or **Edit** an existing app.

   For iOS apps, only public or internal apps built with the Cocoa Framework are supported.
4. On the Deployment tab, select **Use VPN** and then select the profile you created.
5. Select **Save** and publish your changes.

For additional instructions on adding or editing apps, please see the **VMware Workspace ONE UEM 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 that application to use the defined VPN profile when establishing connections.

1. Navigate to **Apps & Books > Applications > Native**.
2. Select the **Internal** tab.
3. Select **Add Application** and add an app.

   For iOS apps, only public or internal apps built with the Cocoa Framework are supported.
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 additional instructions on adding or editing apps, please see the **VMware Workspace ONE UEM Mobile Application Management Guide**.

Configure an Email Account Profile (iOS)

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

To create an email profile:

1. Navigate to **Devices > Profiles & Resources > Profiles and select Add**. Select **Apple iOS**.
2. Configure the profile's **General** settings.
3. Select the **Email** payload.
4. Configure email account settings, including:

Settings	Descriptions
Account Description	Enter a brief description of the email account.
Account Type	Use the drop-down menu to select either IMAP or POP.
Path Prefix	Enter the name of the root folder for the email account (IMAP only).
User Display Name	Enter the name of the end user.
Email Address	Enter the address for the email account.
Prevent moving messages	Select to block the user from forwarding email or opening in third-party apps.
Prevent Recent Address syncing	Select to restrict the user from syncing email contacts to their personal device.
Prevent use in third party apps	Select to prevent users from moving corporate email into other email clients.
Prevent Mail Drop	Select to prevent users from using Apple's Mail Drop feature.
Use S/MIME	Select to use more encryption certificates.

Settings	Descriptions
Incoming Mail	
Host Name	Enter the name of the email server.
Port	Enter the number of the port assigned to incoming mail traffic.
Username	Enter the user name for the email account.
Authentication Type	Use the drop-down menu to select how the email account holder is authenticated.
Password	Enter the password required to authenticate the end user.
Use SSL	Select to enable Secure Socket Layer use for incoming email traffic.
Outgoing Mail	
Host Name	Enter the name of the email server.
Port	Enter the number of the port assigned to outgoing mail traffic.
Username	Enter the user name for the email account.
Authentication Type	Use the drop-down menu to select how the email account holder is authenticated.
Outgoing Password Same As Incoming	Select to auto-populate the password text box.
Password	Enter the password required to authenticate the end user.
Use SSL	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 using Native Mail Client (iOS)

Use the following steps to create an email configuration profile for the native mail client on iOS devices.

1. Navigate to **Devices > Profiles & Resources > 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.
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.
   - Select the **S/MIME Certificate** to sign email messages.
   - Select the **S/MIME Encryption Certificate** to both sign and encrypt email messages.
   - 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. 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.
8. Leave the **Password** field empty to prompt the user to enter a password.
9. Select the **Payload Certificate** to define a certificate for cert-based authentication after the certificate is added to the **Credentials** payload.
10. Configure the following **Settings and Security** optional settings, as necessary:
    - **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.
    - **Prevent Moving Messages** – Disallows moving mail from an Exchange mailbox to another mailbox on the device.
    - **Prevent Use in 3rd Party Apps** – Disallows other apps from using the Exchange mailbox to send message.
    - **Prevent Recent Address Syncing** – Disables suggestions for contacts when sending mail in Exchange.
    - **Prevent Mail Drop** – Disables use of Apple's Mail Drop feature.
11. 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.
12. Select **Save and Publish** to push the profile to available devices.

Configure an EAS Mail Profile using AirWatch Inbox (iOS)

Use the following steps to create a configuration profile for the AirWatch Inbox. For more information about AirWatch Inbox, see the **VMware AirWatch Inbox Guide**.

1. Navigate to **Devices > Profiles & Resources > Profiles.**
2. Select **Add** and select **iOS** as the platform.
3. Configure the profile's **General** settings.
4. Select the **Exchange ActiveSync** payload and then select the **AirWatch Inbox** from the **Mail Client** drop-down.
5. Enter the **Exchange ActiveSync Host,** which is the information of your EAS server. For example: **webmail.Workspace ONE UEMmdm.com**.
   - Enable **Ignore SSL Errors** to allow the devices to ignore Secure Socket Layer errors from agent processes.
   - Enable **Use S/MIME** to select the certificate/smart card for signing and encrypting email messages. Before enabling this option, ensure that you have uploaded necessary certificates under **the Credentials** profile settings.

     You do not need to upload any certificates if a smart card is selected as the credential source in the **Credentials** profile settings.
   - Select the certificate/smart card to sign only email messages in the **S/MIME Certificate** text box.
   - Select the certificate/smart card to both sign and encrypt email messages in the **S/MIME Encryption Certificate** text box.
   - If the smart card is selected, default information populates the **Smart Card Reader Type** and **Smart Card Type**.
   - Choose the **Smart Card Timeout** interval.
6. Enter **Login Information** to authenticate user connections to your EAS Host. The profile supports lookup values for inserting enrollment user’s information and login information.
7. Configure Settings, such as:
   - **Enable Calendar**
   - **Enable Contacts**
   - **Caller ID**
   - **Sync Interval** – The frequency with which the Workspace ONE UEM Inbox app syncs with the email server.
   - **Email Notifications** – Configure how end users can be notified of new emails. **Disabled** means they do not receive a notification. You can also trigger the device to play an alert sound, or allow the device to display specific email message details such as the sender, subject, and message preview.
   - **Past Days of Mail to Sync**
   - **Past Days of Calendar to Sync**
   - **Enable HTML Email**

- **Email Signature**
- **Enable Signature Editing**

8. Configure a Passcode for Workspace ONE UEM Inbox. You can require an end user to enter a passcode when the Workspace ONE UEM Inbox is opened. This is not the email account password, but the passcode the user enters to access the application. The following passcode settings are available:
   - **Authentication Type**

     To allow iOS users to log in using their Workspace ONE UEM credentials, select **Username and Password** as the **Authentication Type** under the **Passcode** section.
   - **Passcode Complexity** – Determine whether the password is simple or complex.
   - **Minimum Length** – Set the minimum number of characters allowed for the passcode.
   - **Minimum Number of Complex Characters**, if the **Complexity** is set to **Alphanumeric**.
   - **Maximum Passcode Age (days)** – Limit the number of days allowed before passcode has to be reset.
   - **Passcode History** – Determine the history of passcodes used to prevent the user from reusing passcodes.
   - **Auto-Lock Timeout (min)** – Set the number of minutes before the device automatically locks.
   - **Maximum Number of Failed Attempts** – Determine the number of passcode entry attempts allowed before the data in Workspace ONE UEM Inbox are erased.
9. Configure more restrictions and security settings. The following restrictions are available:
   - **Allow/Disable Copy and Paste**
     - Disable user's ability to long press email text and copy it to the clipboard.
     - Disable user's ability to copy text from outside of the email client and paste it into a mail message.
   - **Restrict all links to open in the VMware Browser app only**
   - **Restrict attachments to open only in the VMware Content Locker**
   - **Set a Maximum Attachment Size (MB)**
   - **Allow Printing**
10. Select **Save & Publish**.

Username and Password

You can define the user name that is assigned for users to log in to the Workspace ONE UEM Inbox. The user name can be their actual email address or an email user name that is different from their actual email address. When configuring the **Exchange ActiveSync (EAS)** payload in the Workspace ONE UEM **Inbox** profile settings, there is a **User** text box under **Login Information** that you can set to a predefined lookup value.

If you have email user names that are different than user email addresses, you can use the **{EmailUserName}** text box, which corresponds to the email user names imported during directory service integration. Even if your user user names are the same as their email addresses, use the **{EmailUserName}** text box, because it uses email addresses imported through the directory service integration.

Removing Profile or Enterprise Wiping

If the profile is removed by using remove profile command, enforcing compliance policies, or through an enterprise wipe, the following email data gets deleted:

- User account/login information.
  - Email message data.
- Contacts and calendar information.
- Attachments that were saved to the internal application storage.

  Attachments saved outside of Workspace ONE UEM Inbox are **not**deleted.

Configure a Notifications Profile (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. Navigate to **Profiles > List View > Add**. Select **Apple iOS**.
2. Configure the profile's **General** settings.
3. Select the **Notifications** payload from the list.
4. Choose **Select App.** A new window appears.

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

5. Select **Save** to push the payload to the device.

Configure an LDAP Settings Profile (iOS)

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

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select **Apple iOS.**
2. Configure the profile's **General** settings.
3. Select the **LDAP** payload.
4. Configure LDAP settings, including:

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

5. Select **Save & Publish.**

Configure a CalDAV or CardDAV Profile (iOS)

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

To create these profiles:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select **Apple iOS**.
2. Configure the profile's **General** settings.
3. Select the **CalDAV or CardDAV** payload.
4. Configure **CalDAV** or **CardDAV** settings, including:

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

5. Select **Save & Publish.**

Configure a Subscribed Calendar Profile (iOS)

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

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select **Apple iOS**.
2. Configure the profile's **General** settings.
3. Select the **Subscribed Calendars** payload.
4. Configure the calendar settings, including:

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

5. Select **Save & Publish.**

Configure Web Clips Profile

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

To create a Web Clip:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add**. Select **Apple iOS**.
2. Configure the profile's **General** settings.
3. Select the **Web Clips** payload from the list.
4. Configure **Web Clip** settings, including:

Setting	Description
Label	Enter the text displayed beneath the Web Clip icon on an end user's device. For example: "AirWatch Self-Service Portal."

Setting	Description
URL	Enter the URL of the Web Clip that displays. Here are some examples for Workspace ONE UEM pages: • For the SSP, use: **https://<AirWatch Environment>/mydevice/** • For the app catalog, use: **https://<Environment>/Catalog/ViewCatalog/{SecureDeviceUdid}/{DevicePlatform}** • For the book catalog, use: **https://<Environment>/Catalog/BookCatalog?uid={SecureDeviceUdid}**
Removable	Enable device users to use the long press feature to remove the Web Clip off their devices.
Icon	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.
Precomposed Icon	Select this option to display the icon without any visual effects.
Full Screen	Select this option to run the Web page in full screen mode.

5. Select **Save & Publish**.

Configure a SCEP/Credentials Profile (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 **Devices > Profiles & Resources > 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:
   - Choose to **Upload** a certificate and enter the **Certificate Name**
   - Choose **Defined Certificate Authority** and select the appropriate **Certificate Authority** and **Certificate Template**

- Choose **User Certificate** and the intended use for the **S/MIME** certificate.
- 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:
   - **EAS** – Select the **Payload Certificate** under Login Information.
   - **Wi-Fi** – Select a compatible **Security Type** (WEP Enterprise, WPA/WPA2 Enterprise or Any (Enterprise)) and select the **Identity Certificate** under Authentication.
   - **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.

Configure a Global HTTP Proxy Profile (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.

To create a global HTTP proxy profile:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add**. Select **Apple iOS**.
2. Configure the profile's **General** settings.
3. Select the **Global HTTP Proxy** payload from the list.

4. Configure Proxy settings including:

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

5. Select **Save & Publish**.

Configure a Single App Mode Profile (iOS)

Use Single App Mode to provision devices so they can only access a single app of choice. Single App Mode disables 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.

Single App Mode Requirements

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

Enable Single App Mode

Configure Single App Mode using the instructions listed here:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add.** Select **Apple iOS**.
2. Configure the profile's **General** settings.
3. Select the **Single App Mode** payload.

4. Configure Single App mode settings including:

Setting	Description
Filter Type	Choose a filter, either **Lock device into a single app** or **Permitted apps for autonomous single app mode**: • **Lock device into a single app** – Lock devices into a single public, internal, purchased, or native application until the profile with this payload is removed. The home button is disabled, and the device always returns to the specified application from a sleep state or reboot. • **Permitted apps for autonomous single app mode** – Enable whitelisted 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.
Application Bundle ID	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**.
Optional Settings	Choose optional settings for Supervised iOS 7 and higher devices.

5. Select **Save & Publish**. Each device provisioned with this profile enters Single App Mode.

Restart a Device Operating in Single App Mode

Follow the hard reset procedures 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.

Disable Single App Mode Temporarily

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

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

1. Navigate to **Devices > Profiles & Resources > 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 **com.air-watch.agent** under **Permitted Applications**.
5. Select **Save & Publish** to push this profile to the assigned devices.
6. Navigate to **Apps & Books > Applications > Native > Public** for public apps, or **Apps & Books > Applications > Native > Purchased** for apps managed through VPP.
7. Locate the iOS version of the AirWatch Agent, 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.

Configure a Web Content Filter Profile (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.

1. Navigate to **Devices > Profiles & Resources > Profiles > Add.** Select **iOS**.
2. Configure the profile's **General** settings.
3. Select the **Content Filter** payload.
4. Select **Filter Type** drop-down menu:
   - Built-in: Allow Web sites
   - Built-in: Deny Web sites
   - Plug-in

Built-in: Allow Web sites

Configure a whitelist 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
Allowed URLs	The URL of a whitelisted site.
Title	The bookmark title.
Bookmark Path	The folder into which the bookmark is added in Safari.

Built-in: Deny Web sites

Configure a blacklist 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.

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

Setting	Description
Blacklisted URLs	Enter **Blacklisted URLs** and separate with new lines, spaces, or commas.
Automatically filter inappropriate Web sites	Select to filter adult Web sites.
Bookmark Path	Enter the folder path into which the bookmark is added in Safari.
Permitted URLs	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
Filter Name	Enter the name of filter that displays on the device.
Identifier	Enter the bundle ID of the identifier of the plug-in that provides filtering service.
Service Address	Enter the hostname, IP address, or URL for service.
Organization	Choose the organization string that is passed to the third party plug-in.
Filter WebKit Traffic	Select to choose whether to filter Webkit traffic.
Filter Socket Traffic	Select to choose whether to filter SocKet traffic.

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

Setting	Description
Username	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.
Password	Enter the password for this account.
Payload Certificate	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**.

Configure a Managed Domains Profile (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.

1. **Profiles > List View > Add**. Select **Apple iOS**.

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

3. Select the **Managed Domains** payload from the list.

Setting	Description
Managed Email Domains	Enter domains to specify which email addresses are corporate domains. For example: **exchange.acme.com**. 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.
Managed Web Domains	Enter domains to choose specific URLs or subdomains that can be considered managed. For example: **sharepoint.acme.com**. Any documents or attachments coming from those domains are considered managed.

4. Select **Save & Publish**.

Configure a Network Usage Rules Profile (iOS)

Configure network usage rules to control which applications 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 as needed.

1. Navigate to **Profiles > List View > Add**. Select **Apple iOS**.
2. Configure the profile's **General** settings.
3. Select the **Network Usage Rules** payload from the list.
4. Add or select the public, internal, or purchased **applications**.
5. Choose to **Allow Cellular Data** and **Allow Data Roaming**. Both options are selected by default.
6. Select **Save & Publish**.

Configure a macOS Server Account Profile (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.

To configure an macOS Server Account:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add**. Select **Apple iOS**.
2. Configure the profile's **General** settings.
3. Select the **macOS Server Account** payload from the list.

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

4. Select **Save & Publish**.

Configure a Single Sign-On Profile (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. Navigate to **Devices > Profiles & Resources > Profiles > Add** and select **iOS.**
2. Configure the profile's **General** settings.
3. Select the **Single Sign On** payload.
4. Enter **Connection Info**:

Setting	Description
Account Name	Enter the name that appears on the device.
Kerberos Principal name	Enter the Kerberos principal name.
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

5. 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.

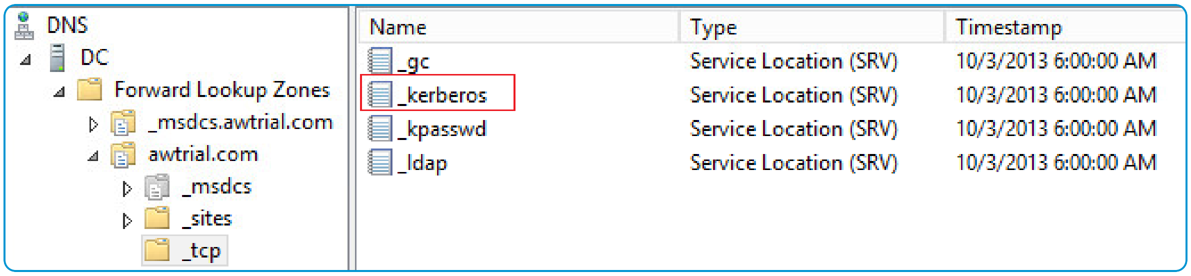
6. Enter the **Application Bundle ID** or select one from the drop-down menu. The bundle ID appears in this drop-down menu after the application has been uploaded to the UEM console. For example: **com.air-watch.secure.browser**. The applications specified must support Kerberos authentication.

7. 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.

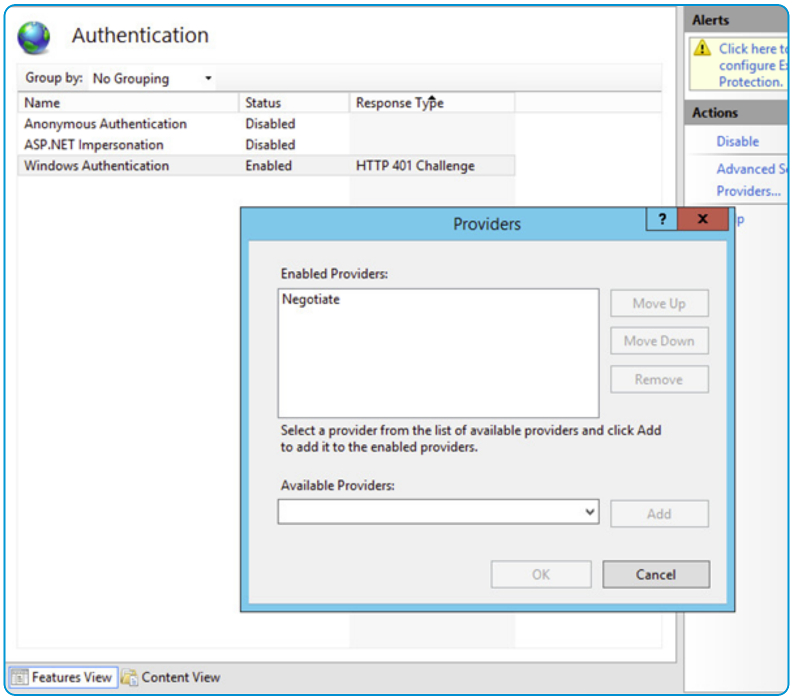
Notes

- 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
_kerberos	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.



Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Windows Authentication	Enabled	HTTP 401 Challenge

Select a provider from the list of available providers and click Add to add it to the enabled providers.

Configure a AirPlay Whitelist Profile (iOS)

Configuring the AirPlay payload lets you whitelist 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 the **VMware Workspace ONE UEM tvOS Guide**.

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

To configure an AirPlay destination whitelist:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add**. Choose **Apple iOS** from the platform list.
2. Configure the profile's **General** settings.
3. Select the **AirPlay Mirroring** payload tab.
4. Configure **Passwords** settings for iOS 7 devices and **Whitelists** for iOS 7 + Supervised devices:

Setting	Description
Device Name	Enter the device name for the AirPlay destination
Password	Enter the password for AirPlay destination. Select **Add** to include additional whitelisted devices.

Setting	Description
Display Name	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)
Device ID	Enter the device ID (include the MAC address or Ethernet address formatted as XX:XX:XX:XX:XX:XX) for the destination display. Select **Add** to include additional whitelisted devices. (iOS 7 + Supervised)

Using AirPlay in the UEM console with iOS 7 + Supervised devices

Now that the AirPlay destination whitelist is established for iOS 7 + Supervised devices, use the Device Control Panel to enable or disable AirPlay manually:

1. Navigate to **Devices > List View** and locate the device intending to AirPlay, and select the device's Friendly Name.
2. Select **Support** and select **Start AirPlay** from the list of support options.
3. 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.
4. Select **Save** and accept the prompt to enable AirPlay.

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

Configure AirPrint Profile (iOS)

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

To configure the AirPrint payload:

1. Navigate to **Devices > Profiles > List View > Add** and then **Add** the appropriate platform. If you select Apple macOS, then select whether this profile will apply to only the enrollment user on the device (**User Profile**), or the entire device (**Device Profile**).
2. Configure the profile's **General** settings.
3. Select the **AirPrint** payload tab.

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).

4. Select **Save & Publish**.

Configure a Cellular Settings Profile (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.

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select **Apple iOS**.
2. Configure the profile's **General** settings.
3. Choose a **Cellular** payload for devices using iOS 7 and higher.
4. Configure the Cellular payload settings.

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

5. Select **Save & Publish.**

Configure a 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.

1. Navigate to **Profiles > List View > Add**. Select **Apple iOS**.
2. Configure the profile's **General** settings.
3. Select the **Home Screen Layout** payload from the list.

Setting	Description
Dock	Choose what applications you want to appear in the dock.
Page	Choose applications you want to add to the device. You can also add more pages for more groups of applications.

Setting	Description
Add Folder	Configure a new folder to add to the device screen on the selected page. • Use the **pencil icon** in the gray bar to create or edit the name of the folder.

4. Select **Add Page** to add more pages to the device if needed.

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

Create a Lock Screen Message Profile (iOS)

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

To create a Lock Screen Message profile:

1. Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**. Select **Apple iOS**.

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

3. Configure the Lock Screen Message:

Setting	Description
"If lost return to" Message (optional)	Display a name or organization to whom a found device should be returned. This field supports lookup values.
Asset Tag Information (optional)	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.

4. Select **Save & Publish**.

Configure a Google Account Support Profile (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.

To configure a Google Account:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add**. Select **Apple iOS** as the platform.

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

3. Configure the user's account information:

Setting	Description
Account Name (optional)	The full user name for the Google account. This is the user name that appears when you send a mail message.
Account Description (optional)	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 (Optional)	Search and select an application that will be the default app for making any calls made from configured Google account.

4. Select **Save & Publish**.

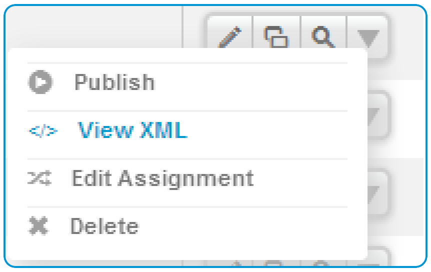
Configure a Custom Settings Profile (iOS)

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 disable certain settings manually.

You may 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.

To create custom settings:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add.** Select **iOS**.
2. Configure the profile's **General** settings.
3. Configure the appropriate payload (for example, Restrictions or Passcode).
4. Select **Save and Publish**.
5. Select the profile using the radio button next to the profile name. Menu buttons appears about the Profile Details.



6. Select **XML** from the menu choices. A **View Profile XML window** appears.
7. 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.
8. Navigate back to **the Custom Settings** profile and paste the XML you copied in the text box. The XML code you paste must contain the complete block of code, from <dict> to </dict>.

9. 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.

> **Note:** Any device not upgraded to the latest iOS version ignores the enhancements you create. Since the code is now customized, test the profile devices with older iOS versions to verify expected behavior.

Chapter 4:
Compliance Policies

The compliance engine is an automated tool by Workspace ONE ™ UEM 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, blacklisting 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, refer to the **VMware AirWatch Mobile Device Management Guide**, available on docs.vmware.com.

Chapter 5:
Apps for iOS

Overview

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 Content Locker to sync a personal content folder.
- Configure VMware Browser to secure Internet searches.
- Enable VMware 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.

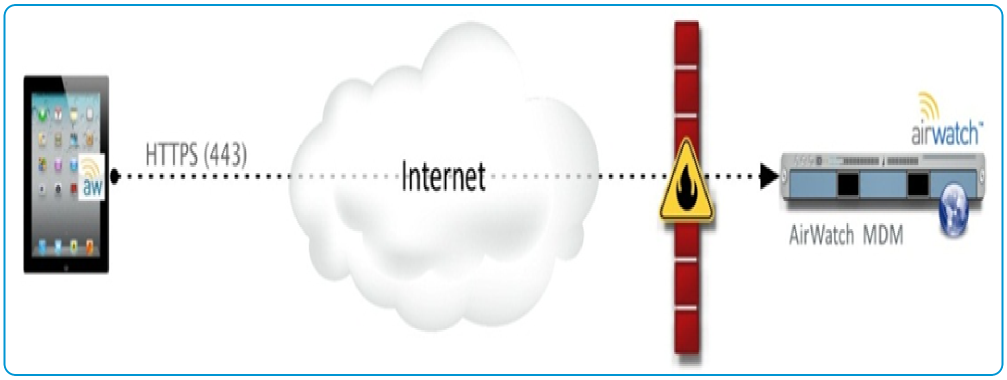
For more information about managing applications, refer to the **VMware AirWatch Mobile Application Management Guide**.

AirWatch Agent for iOS

The AirWatch Agent 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.

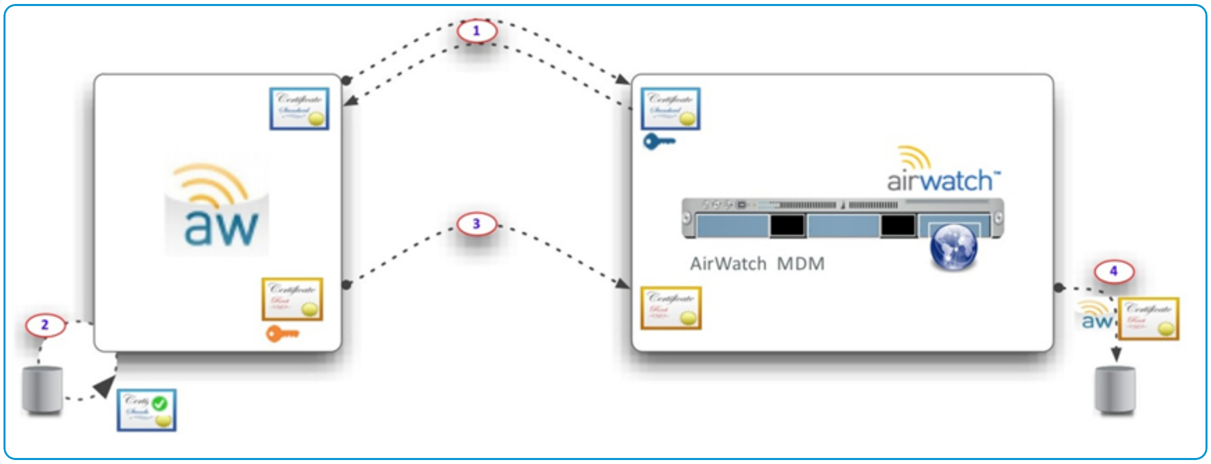
Workspace ONE UEM uses a unique certificate pair to sign and encrypt all communication between AirWatch Agent for iOS and the server. These certificates also allow the server to verify the identity and authenticity of each device enrolled in

Workspace ONE UEM. This overview details the benefits and necessities of both security enhancements.



Understanding the Certificate Exchange

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



1. AirWatch Agent for iOS communicates with the Workspace ONE UEM server to obtain the server's certificate public key. Both AirWatch Agent 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. AirWatch Agent for iOS validates the server's certificate against the Workspace ONE UEM Root CA certificate.

3. AirWatch Agent for iOS sends a unique certificate public key to the Workspace ONE UEM server.

4. The Workspace ONE UEM server associates the AirWatch Agent'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.

	Agent Certificate	Server Certificate
AirWatch Agent	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 AirWatch Agent for iOS is used or not.
- **Native iOS SDK APIs** are available to any third-party application, including AirWatch Agent applications and any other application using the Workspace ONE UEM Software Development Kit (SDK).

The AirWatch Agent for iOS acts as the broker application that integrates with the Native iOS SDK API layer of management. When using AirWatch Agent 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 AirWatch Agent Settings for iOS Devices

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

To configure the AirWatch Agent Settings:

1. Navigate to **Devices > Device Settings > Apple > Apple iOS > Agent Settings**.
2. Configure the following settings for the AirWatch Agent:

Setting	Description
General	
Disable Un-Enroll in Agent	This setting disables the user's ability to unenroll from Workspace ONE UEM MDM using the Agent. This setting is only available in the AirWatch Agent v4.9.2 and higher.
Background App Refresh	This setting tells the AirWatch Agent 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 AirWatch Agent reports information, such as compromised detection, hardware details, GPS, iBeacon, and telecom, to the UEM console. The frequency at which the Agent 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 AirWatch Agent cannot be killed on the device, and Background App Refresh must be enabled on the device for the AirWatch Agent under **Settings > General > Background App Refresh**.
Minimum Refresh Interval	Select the minimum amount of time that must pass before the device attempts to refresh app content.
Transmit on Wi-Fi only	Enable background refresh to occur over Wi-Fi connections only.

Setting	Description
Area	
Collect Location Data	This setting enables the AirWatch Agent to collect GPS data from devices. Whether or not data is actually collected depends on the privacy settings set in **Devices > Device Settings > General > Privacy**.
Detect iBeacon Region	This setting enables the AirWatch Agent to listen to iBeacon information in regions where the device is located.
Telecom	
Collect Cellular Data Usage	This setting enables the AirWatch Agent to collect cellular data use from devices. Whether or not data is actually collected depends on the privacy settings set in **Devices > Device Settings > General > Privacy**.
Self Service Setting	
Self Service Enabled	This setting allows users to view their user account status, device compliance status, and assigned compliance policies from within the AirWatch Agent. If enabled, users can see if their devices are compliant. For more information about enabling users to sync their devices to check for compliance status, see the following Workspace ONE UEM Knowledge Base article: https://support.air-watch.com/articles/115001662408.
SDK Profile	
SDK Profile (Legacy)	This setting specifies the SDK profile you want to apply to the AirWatch Agent. SDK profiles can be used to enforce geofencing, create custom branding for the Agent and more.
SDK Profile V2	This setting specifies the SDK V2 profile you want to apply to the AirWatch Agent. SDK profiles can be used to enforce geofencing, create custom branding for the Agent and more.

Configuring AirWatch Agent using Settings and Policies

Customize the following extra configurations for the AirWatch Agent from the **Settings and Policies** page in the UEM console for Single Sign On in this guide. For information about offline access, branding, and other Settings and Polices, refer to the **VMWare AirWatch Mobile Application Management Guide**.

AirWatch Agent Mobile Application for iOS

After enrolling the AirWatch Agent, 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 **Agent Settings** in the UEM console to see all the status information.

Note: If the **Disable Un-enroll Agent** option is not checked in **Agent Settings**, select **Un-enroll Device** before re-enrolling with the AirWatch Agent 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 Agent 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 AirWatch Agent application and legal information.

VMware Content Locker for iOS

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

From the VMware Content Locker, 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 Content Locker, refer to the **VMware Workspace ONE UEM Mobile Content Management Guide**.

VMware Browser for iOS

VMware Browser 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 VMware Browser 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 VMware Browser with a Restrictions profile blocking the native browser.

For additional information about preparing and configuring the VMware Browser for deployment, refer to the **VMware AirWatch Browser Guide**.

VMware Boxer for iOS

VMware 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.

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 iOS devices.

For more information on VMware Boxer, see the **VMware 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 instructions on how to use the AirWatch Container on a device, see the **VMware AirWatch Container User Guide for iOS** or the **VMware AirWatch Container User Guide for Android.**

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 AirWatch Agent 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. To enable SSO:

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. Optionally set **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 **VMware Workspace ONE UEM 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.

To upload a profile:

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 **Devices** > **Profiles & Resources** > **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.

Chapter 6:
iOS Device Configurations

Overview

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.

iOS Device Configurations

Overview

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.

Apple Industry Templates

Choose industry templates to expedite your deployment process. These templates, or single entities, 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+)	

Industry	Initiative	Description
Retail	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+)	
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**.

Create an Apple Industry Template

Configure initiative-specific settings using a template. Then create a Patient Care template to push to patients. Consider creating your User Groups before you begin this process.

For example, you can create a Clinical Collaboration template to push to a user group of doctors and a user group of nurses.

To create an industry template:

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.
   - 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.
   - 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.

   > **Note:** 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. Use the following best practices to edit your application list for each template.

Remove a Public Application

Quickly remove a public application and push the updated application list to users immediately.

1. Navigate to **Hub > Industry Templates > List View**.
2. Select the **pencil button** or template name to edit the template.
3. Deselect the application. The check mark in the corner disappears.
4. Select **Next > Publish** to save and republish the template.

Add an Updated Version of an Internal Application

Upload a new application version of an internal app after deleting the old version.

1. Select the **pencil button** or template link to edit the template.
2. Select **More Options**. A trash can icon appears on the internal application.
3. Select **Remove** and follow the prompt to delete the application from the list.
4. Select **Add App** to upload the updated application.
5. 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 **Apps & Books > Applications > 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.

To delete an industry template:

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

Apple iBeacon with AirWatch Agent 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 AirWatch Agent. Detect when the device enters these regions and use device event logs to find changes in iBeacon ranges.

Requirements for iBeacon

- Workspace ONE UEM console v8.1+
- iBeacons from a third-party vendor

- AirWatch Agent 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 AirWatch Agent monitors iBeacons only. It does not use the ranging technique that determines the proximity of the device to iBeacon transmitter.
- If the AirWatch Agent is killed before a device exits the iBeacon group, the device is not detected until the AirWatch Agent is launched again.

Enable iBeacon for iOS Devices

To configure iBeacon, first enable the AirWatch Agent to detect iBeacon groups that receive broadcasts. Then, add a set of iBeacon groups for the device to monitor.

For more information on iBeacon technology, see the Apple article iBeacon for Developers.

To enable iBeacon:

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Apple iOS > Agent Settings**,
2. Scroll to **Area** and select **Detect iBeaconArea** to enable an iBeacon for the organization group.
3. Select **Save**.
4. Navigate to **Devices > Profile & Resources > Profile 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
Group Name	Enter the name for the specific iBeacon group.
iBeacon Name	Enter the name of the iBeacon.
UUID	Enter a unique identifier for the iBeacon deployment to share.
Major Value	Enter an identifier to subdivide the area of the iBeacon.
Minor Value	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.

To assign an iBeacon group to a device profile:

1. Navigate to **Devices > Profiles & Resources > 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 AirWatch Agent.

Add Compliance Policies for iBeacon Groups

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

To add an iBeacon compliance policy:

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. Applicable actions are:
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

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 Find My iPhone 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 Turn off Find My iPhone Activation Lock.	

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. To enable this feature:

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. To view devices:

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

   Under the Security section, you can see whether Activation Lock is enabled or disabled.

Clear Activation Lock on iOS Devices

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

The available methods are:

- Use the Clear Activation Lock command.
- Enter an Activation Lock Bypass Code directly onto the device.
- Perform a Device Wipe command and selecting 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 even if the device is unenrolled from Workspace ONE UEM MDM.

To use the command:

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. To view the bypass code:

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

When performing a device wipe command, you also have the option clearing the Activation Lock on a device. To perform a 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 **Device Wipe**. The Device Wipe page displays.
5. Select **Clear Activation Lock**. Enter your **Security PIN**, and the device is wiped.

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.

1. Navigate to **Devices > List View > Select Device > Support > More > Start AirPlay.** An **AirPlay** window appears.
2. Select **Add a Destination** to start adding destinations to view. An **Add New AirPlay Destination** window appears.
3. Enter the **Destination Name**, which is the friendly name for the device.
4. Enter the **Destination Address**, which is the MAC address of the device to view.
5. 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.
   - 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.**

Edit an AirPlay Destination

1. Navigate to **Devices > List View > Select Device > Support > More > AirPlay.** An **AirPlay** window appears.
2. Choose the **Device Destination** to edit from the drop-down menu.
3. Select **Edit** to start editing the destination settings. An **Edit AirPlay Destination** window appears.
4. Select **Save and Start** to send the AirPlay request to the device.

Remote View

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.

Pre-requisites to initiate a Remote View

- UEM console provisioned with proper partner hostname and all required certificates.
- End User devices registered with partner by the AirWatch Agent.

Remote View Device Requirements

- Devices must have the AirWatch Agent 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 > Advanced > Site URLs**.
2. In the **External Remote Management** 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: `https://rmstage01.awmdm.com/t10`
Device Connection Hostname	Enter the ARM server fully qualified domain name (FQDN). For example: `https://rmstage01.awmdm.com` 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**.

   When the Site URLs page is saved, the Site URL along with the following data is pushed to the agent settings profile. The devices that are already enrolled with the agent start picking up the updated agent setting profile.

   - **Device HostName** — Hostname for the device to reach out to when a remote view session is initiated from the UEM console.
   - **Environment Name** — Environment name for the partner to put the device in the correct organization group when device reaches out to them for remote view.

Configure End-User Devices

Now that the console is configured, you must install the iOS-specific agent 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 AirWatch Agent from iOS App store for your deployment.

For more information about App Management, see the **VMware AirWatch Mobile Application Management Guide** found on docs.vmware.com.

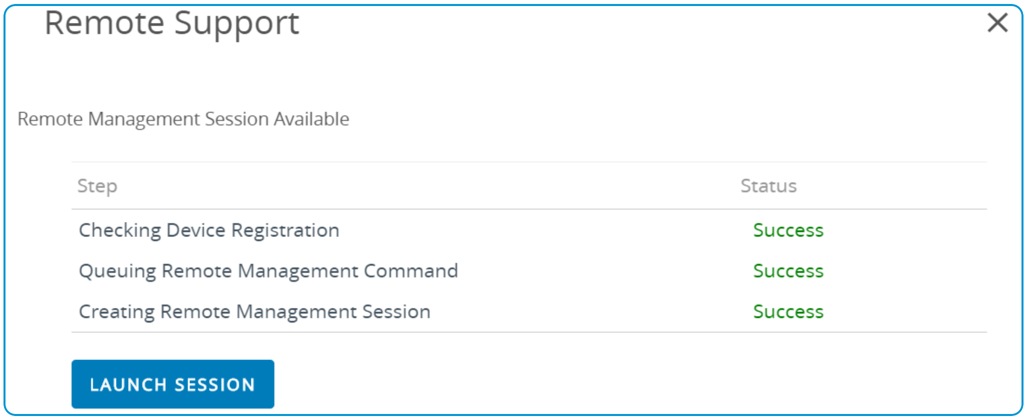
Initiate a Remote View Session

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 AirWatch Agent to start the broadcast.

   The user must access the iOS control center and select **Agent Broadcast** > **Start Broadcast** to initiate broadcasting the device's screen. The iOS device begins capturing the UI and shares it to the AirWatch agent which in turn is linked to the Advanced Remote Management server.

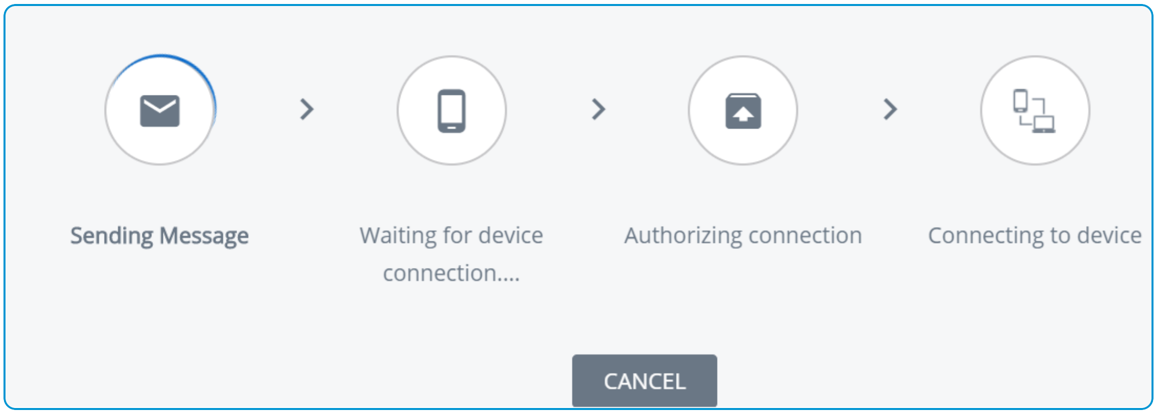


Remote Support

Remote Management Session Available

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

2. 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.

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

Configure Managed Settings for iOS Devices

The Managed Settings page in the UEM console lets you configure a few extra settings related to the AirWatch Agent and managing iOS devices.

To configure Managed Settings:

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. Enable or disable:
   - Voice Roaming (iOS 5+)
   - Data Roaming (iOS 5+)
   - Personal Hotspot (iOS 7)
   - Activation Lock (iOS 7 and Supervised)
   - Bluetooth (iOS 11.3+ Supervised)
4. Select **Save** to save the settings to devices in the current organization group.

Override Default Roaming Settings (iOS)

Modifying settings to manage roaming status that does not require a permanent restriction. To override default settings in order to modify roaming permissions for an individual iOS device:

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.
4. 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

To 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.

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:

- Enable or Disable use of Cisco QoS fast lane network
- Whitelist 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.

Chapter 7:
Device Management

Overview

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, AirWatch Agent 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.

Device Dashboard

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

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

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

Device List View

Select **Devices > List View** to see a full listing of all devices.

The **Last Seen** column displays an indicator showing the number of minutes elapsed since the device has checked-in.

Select a device in the **General Info** column at any time to open the details page for that device.

Sort by columns and configure information filters to review device 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. For instance, you can hide 'Asset Number' from the **Device List**.

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.

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.

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 with the UEM console.

View Device Information

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

- **Summary** – View general statistics on: compliance, enrollment status, last seen, platform, model, or 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, groups, serial number, UDID, asset number, power status, storage capacity, any available OS updates (iOS 9), 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 11.3+ devices, the UEM console displays on 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 via the App Store, distributed as a Beta app, signed adhoc by an enterprise account, or managed using a device based VPP license).
- **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 tab (More ▾).

- **Network** – View current network (Cellular, Wi-Fi, Bluetooth) status of a device.
- **Security** – View 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 issuant. 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 targets 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, and links for troubleshooting and other purposes without taking up space on the device itself.

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 apps (including AirWatch Agent, where applicable), books, certificates, device information, profiles and security measures.
- **Device Information (Query)** – Send an MDM query command to the device to return basic 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, etc.).
- **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 apps.
- **Certificates (Query)** – Send an MDM query command to the device to return a list of installed certificates.
- **Clear Passcode (Restrictions Setting)** – Clear the passcode that restricts device features such as app installation, Safari use, camera use and more.
- **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 apps.
- **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 will be required for Workspace ONE UEM to manage this device again. Includes options to prevent future re-enrollment and a **Note Description** field for you to add any noteworthy details about the action.
  - Enterprise Wipe is not supported for cloud domain-joined devices.
- **OS updates** - Select individual devices or devices in bulk to send updates to devices that are enrolled through DEP.
- **Managed Settings** – Enable or disable 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.

- 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 enable or disable 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.
- **Send Message** – Send a message to the user of the selected device. Choose between **Email**, **Push Notification** (through AirWatch Cloud Messaging), and **SMS**.
- **Find Device** – Send a text message to the applicable Workspace ONE UEM application together with an audible sound (with options to repeat the sound a configurable number of times and the length of the gap, in seconds, between sounds). This audible sound should help the user locate a misplaced device.
- **App Remote View** – Take a series of screenshots of an installed application and send them to the Remote View screen in the UEM console. You may choose the number of screenshots and the length of the gap, in seconds, between the screenshots.

  VMware Content Locker must be installed on the device to execute **App Remote View**.
- **Request Device Check-In** – Request the selected device to check-in itself in to the UEM console and updates the **Last Seen** 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 choosing (including IP address, port, audio port, password and scan time), allowing you to see what the user sees as they operate the device.
- **Change Organization Group** – Change the device's home organization group to another pre-existing OG. Includes an option to select a static or dynamic OG.
- **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** and **Device Category**.
- **Delete Device** – Delete and unenroll a device from the UEM console. This action performs an Enterprise Wipe and remove its representation in the UEM 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 prior to 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 to lock a device and send a message, phone number or text to the lock screen. Lost Mode cannot be disabled by the user. When Lost Mode is disabled by an administrator, the device returns to normal functionality. Users are sent 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://support.air-watch.com/kb.

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.

To create and deploy a custom command:

1. In the UEM console, navigate to **Devices > List View**.
2. Select one or more macOS 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.

   Browse XML code for Custom Commands on the Workspace ONE UEM Knowledge Base at https://support.air-watch.com/kb.
5. Select **Send** to deploy the command to devices.

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.

Configure iOS Updates for iOS Devices

Configure iOS updates on iOS 9+ devices to ensure that end users are taking advantage of all the security and features offered on the latest iOS version. Administrators can query for available updates on iOS 9+ devices and force updates on iOS 9+ DEP+Supervised devices and iOS 10.3+ Supervised devices.

Query for iOS Updates (iOS 9+ devices)

1. Navigate to **Devices > List View > Select Device > More > Query > iOS Update**.
2. On the **Details View** page, select the **Summary** tab and find the **Device Info** box to determine if an update is available for the selected device. **Available iOS Updates** appears in the box if an update is available. If not, **None** indicates that there are no updates.

Configure iOS Updates (iOS 9+ DEP+Supervised devices and iOS 10.3+ Supervised devices)

1. Navigate to **Devices > List View > Select Device > More > iOS Update**. A message box appears.
2. Select **OK** to send the command to push the iOS update on the device.
3. View the **iOS Update Status** on the **Details View** page. Select **Refresh** as needed to update the **iOS Update Status** and **Download Percentage** of the update. When the update process is complete, **None** appears in the **Device Info** box.

> **Note:** On iOS 10.3 and later, supported Software Update commands require supervision but not DEP enrollment. If there is a passcode on the device, a user must enter it to start a software update. Prior to iOS 10.3, the supervised devices need to be DEP-enrolled and have no passcode.

Delay iOS Updates (iOS 11.3+ Supervised devices)

1. Navigate to **Devices > Profiles & Resources > Profiles > Add**. Select **Apple iOS**.
2. Configure **Restrictions** settings.
3. Select **Delay Updates (Days)** from the **OS Updates Restrictions** subsection.

   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.

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.

To set the device name:

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 **Enable for Device Name** setting to set this name as the Device Name to match the Friendly Name.
5. Select **Save** to update the name.

AppleCare GSX

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.

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 on page 85.

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 on page 86.

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.

To integrate, perform the following:

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).
    a. GSX Sold-To account number
    b. Primary IT contact name
    c. Primary IT contact email
    d. Primary IT contact phone number
    e. 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.

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	Description
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.

3. Select **Save** to complete the integration with AppleCare.

4. Navigate to the **List View**, select a device, and use the **More** menu to find **AppleCare** information in the UEM console.

Chapter 8:
Shared Devices

Overview

Issuing a device to every employee in certain organizations can be expensive. Workspace ONE ™ UEM 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.

Shared Device/Multi-User Device functionality ensures that security and authentication are in place for every unique end user. And if applicable, shared devices allow only specific end users to access sensitive information.

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 AirWatch Agent. Self-containment ensures that the enrollment status is never affected, and that the device is managed whether it is in use or not.

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 AirWatch Agent.
  - 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.
  - 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+,
- iOS devices with AirWatch Agent v4.2+,
- MacOS devices with AirWatch Agent v2.1+.

Define the Shared Device Hierarchy

When you first log in to Workspace ONE ™ UEM, you see a single organization group (OG) that has been created for you using the name of your organization. This group serves as your top-level OG. Below this top-level group you can create subgroups to build out your company hierarchical structure.

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. Use alphanumeric characters only. Ensure that users sharing devices receive the **Group ID** as it may be required for the device to log in depending on your Shared Device configuration.
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 **Type** is Customer. Select from the list of Customer Industries.

5. Build out your corporate hierarchical structure by creating more groups and subgroups in the same manner.
   - 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.
   - 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 on page 89.
6. 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
Group Assignment Mode	Configure devices in one of three ways: • Select **Prompt User for Organization Group** 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 **Fixed Organization Group** 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 **User Group Organization Group** 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 **Groups & Settings > All Settings > Devices & Users > General > Enrollment**. Select the **Grouping** tab and fill in the required details.

Setting	Description
Always Prompt for Terms of Use	Prompts the end users to accept your **Terms of Use** agreement before they log in to a device.

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

Setting	Description
Require Shared Device Passcode	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	**(For iOS devices only)** 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.
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 Log out Enabled	Configure an automatic log out after a specific time period.
Auto Log out After	Set the length of time that must elapse before the **Auto Log out** function activates in **Minutes**, **Hours**, or **Days**.

Setting	Description
Enable Single App Mode	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 a 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. Enabling Single App Mode also disables the Home button on the device. **Note:** Single App Mode applies only to Supervised iOS devices.
Clear Device Passcode on Logout (Android Only)	This setting controls whether the current device passcode is cleared when the user logs out (checks in) a multi-user shared device.
Clear App Data on Logout (Android Only)	Select this checkbox to clear the app data when the user logs out of a shared device (checks it in).

4. Click **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.

Log In to an iOS Device

1. Run the AirWatch Agent on the device.
2. Enter the end-user credentials.

   If the device is already logged in to the AirWatch Agent, 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 AirWatch Agent prompts users to change the passcode on the device. If users do not a change their passcode before it expires, users must return to the Self-Service Portal to create another passcode.

Log Out of an iOS Device

1. Run the AirWatch Agent.
2. Select **My Device** at the bottom.
3. Tap **Log out** under the **Shared Device** section.

> **Note:** When the shared device is logged out, both the device passcode and Single Sign On passcode are cleared without any warning or notification. The device in this state allows the next user to configure another passcode.

Appendix:
iOS Functionality Matrix: Supervised vs. Unsupervised

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
Passcode			
Passcode settings	✓		-
Wi-Fi			
Wi-Fi settings	✓		-
Auto-Join	✓		iOS 7
Wi-Fi Hotspot 2.0 settings	✓		iOS 7
Proxy settings	✓		iOS 7
QOS Marking Policy	✓		iOS 10
VPN			
VPN settings	✓		-
Per-App VPN	✓		iOS 7
Connect automatically	✓		iOS 7
Email			
Email settings	✓		-
Prevent Moving Messages	✓		iOS 7

Features and Functionality	Does Not Require Supervision	Requires Supervision	OS Notes
Disable recent contact sync	✓		iOS 7
Prevent Use In 3rd Party Apps	✓		iOS 7
Use S/MIME	✓		iOS 7
Exchange ActiveSync			
EAS settings	✓		-
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
LDAP			
LDAP settings	✓		-
CalDAV			
CalDAV settings	✓		-
Subscribed Calendars			
Subscribed Calendar settings	✓		-
CardDAV			

Features and Functionality	Does Not Require Supervision	Requires Supervision	OS Notes
CardDAV settings	✓		-
Web Clips			
Web Clip settings	✓		-
Credentials			
Credentials certificate settings	✓		-
SCEP			
SCEP settings for certificate authority	✓		-
Global HTTP Proxy			
Global HTTP Proxy settings		✓	iOS 7
Single App Mode			
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
Web Content Filter			
Web Content Filter settings (Whitelist, Blacklist, Permitted URLs)		✓	iOS 7
Web Content Filtering with 3rd Party Provider		✓	iOS 8
Managed Domains			
Managed Email Domains	✓		iOS 8
Managed Web Domains	✓		iOS 8

Features and Functionality	Does Not Require Supervision	Requires Supervision	OS Notes
Managed Safari Password Domains	✓		iOS 9.3
Network Usage Rules			
Network Usage Rules	✓		iOS 9
macOS Server Accounts			
macOS Server Accounts	✓		iOS 9
Single Sign On			
Single Sign On settings with Kerberos authentication	✓		iOS 7
Single Sign On settings with Renewal certificates	✓		iOS 8
AirPrint			
AirPrint destination settings	✓		iOS 7
AirPlay Mirroring			
AirPlay Destination settings (Whitelist)		✓	iOS 7
AirPlay Passwords	✓		
Access Point			
Advanced Access Point settings	✓		
App Installation Settings			
Silent App Installation		✓ +VPP	
Control Cellular Settings			
Voice Roaming	✓		iOS 7

Features and Functionality	Does Not Require Supervision	Requires Supervision	OS Notes
Data Roaming	✓		iOS 7
Personal Hotspot	✓		iOS 7
Wallpaper Settings			
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+
Notifications			
Notification settings		✓	iOS 9.3+
Queries and Commands			
Supervised status	✓		iOS 7
Personal Hotspot status	✓		iOS 7
Clear Activation Lock		✓	iOS 7
Clear Restrictions Passcode		✓	iOS 8
Query iOS Updates	✓		iOS 9
Configure iOS Updates		✓	iOS 9 Prior to iOS 10.3, DEP is also required
Delay iOS Updates		✓	iOS 11.3+
Custom Fonts and Messaging			

Features and Functionality	Does Not Require Supervision	Requires Supervision	OS Notes
Custom Font Installation	✓		iOS 7
Custom Enrollment Messages	✓		iOS 7
Custom MDM Prompts	✓		iOS 7
Activation Lock Warning	✓		iOS 7