Introduction to the iOS Platform Guide

Overview

AirWatch provides you with a robust set of mobility management solutions for enrolling, securing, configuring and managing your iOS device deployment. Through the AirWatch Admin Console you have several tools and features for managing the entire lifecycle of corporate and employee owned devices. You can also enable end users to perform tasks themselves, for example, through the Self-Service Portal and user self-enrollment, which will save you vital time and resources.

Ensuring devices are compliant and secure is also an important part of managing a device fleet, and you can do this by ensuring compliance policies and security profiles are assigned to specific groups and individuals in your organization. Finally, custom reporting tools and a searchable, customizable Dashboard make it easy for you to perform ongoing maintenance and management of your device fleet.

In This Guide

- **Before You Begin** – Details useful background information and things to keep in mind before diving into AirWatch and iOS device management, including prerequisites and suggested reading.
- **iOS Device Enrollment** – Walks through AirWatch’s recommended enrollment process for iOS devices.
- **iOS Device Profiles** – Details the available profiles for securing and configuring iOS devices.
- **Compliance** – Explains how the AirWatch Compliance Engine works and how to create compliance policies.
- **Apps for iOS Devices** – Covers the available AirWatch applications for iOS devices and options for configuring the AirWatch Agent.
- **Apple Configurator** – Gives a general over of Apple Configurator and its integration with AirWatch.
- **Shared Devices** – Explains how to enable and use shared device mode for iOS devices.
- **Mobile Kiosks** – Explains how to configure mobile kiosks, which are devices set to run only a specific set of apps.
- **Managing iOS Devices** – Explains how you can manage your iOS Devices from the AirWatch Admin Console and Self-Service Portal.
- **Appendix A – iOS Functionality: Supervised vs. Unsupervised** – Lists all available securing, configuring and managing profiles and actions available for iOS devices and the software version and/or supervision status required for each.
Before You Begin

Overview

Before configuring and deploying your iOS device deployment, you should consider the following prerequisites, requirements, supporting materials, and helpful suggestions from the AirWatch team. Familiarizing yourself with the information available in this section will help prepare you for deploying iOS devices with AirWatch.

In This Section

- **Prerequisites** – Details prerequisites for a successful deployment.
- **Supported Devices** – Provides a comprehensive list of supported devices.
- **Recommended Reading** – Lists helpful background and supporting information available from other AirWatch guides.

Prerequisites

Before reading this guide, it is recommended you have the following materials ready:

- **Active Environment** – This is your active AirWatch environment and access to the AirWatch Admin Console.
- **Appropriate Admin Permissions** – This type of permission allows you to create profiles, policies and manage devices within the AirWatch Admin Console.
- **Enrollment URL** – This URL is unique to your organization’s enrollment environment and takes you directly to the enrollment screen. For example, mdm.acme.com.
- **Group ID** – This Group ID associates your device with your corporate role and is defined in the AirWatch Admin Console.
- **Credentials** – This username and password allow you to access your AirWatch environment. These credentials may be the same as your network directory services or may be uniquely defined in the AirWatch Admin Console.
- **Apple ID** – This Apple ID is needed for each user performing agent-based enrollment.
- **Apple Push Notification service (APNs) Certificate** – This is the certificate issued to your organization to authorize use of Apple’s cloud messaging services.

Enabling iOS MDM Support

If you are planning on managing iOS devices, you must first obtain an Apple Push Notification Service (APNs) certificate. An APNs certificate allows AirWatch to securely communicate to Apple devices and report information back to AirWatch. You will therefore need the APNs certificate that was issued to your organization to manage iOS devices. Refer to the [Generating an APNs Certificate for MDM](#) document for detailed instructions on generating an APNs certificate and uploading it to AirWatch.
**Note:** Per Apple's Enterprise Developer Program, an APNs certificate is valid for one year and then must be renewed.

**Note:** Your current certificate will be revoked as soon as you renew from the Apple Development Portal, which prevents device management until you upload the new one. You should therefore plan to immediately upload your certificate after it is renewed. In addition, it is recommended you use a different certificate for each environment if you use separate production and test environments. For additional information, refer to the *Generating an APNs Certificate for MDM* document.

---

**Supported Devices**

AirWatch supports iPhone, iPad, and iPod Touch devices running iOS v.4.3 and higher.

---

**Recommended Reading**

This guide touches on aspects of mobile device management and iOS device management. For an extensive background on these topics, please refer to the following guides:

- Mobile Device Management (MDM) Guide
iOS Device Enrollment

Overview

Each iOS device in your organization’s deployment must be enrolled before it can communicate with AirWatch and access internal content and features. This is facilitated with the AirWatch Agent. You can enroll iOS devices using one of three methods. You can use an agent-based process leveraging the AirWatch Agent; you can enroll using an agentless process using the device’s built-in Safari browser; or you can use the Apple Configurator utility. The following sections provide a background on the AirWatch Agent and its uses, then cover the enrollment capabilities of both agent-based versus agentless enrollment.

Requirements

Before you can enroll an iOS device, you (or end users) need the following information:

If an email domain is associated to your environment

- **Email address** – This is your email address associated to your organization. For example, JohnDoe@acme.com.
- **Credentials** – This username and password allow you to access your AirWatch environment. These credentials may be the same as your network directory services or may be uniquely defined in the AirWatch Admin Console.

If an email domain is not associated to your environment

If a domain is not associated to your environment, you will still be prompted to enter your email address. Since auto discovery is not enabled, you will then be prompted for the following information:

- **Enrollment URL** – This URL is unique to your organization’s enrollment environment and takes you directly to the enrollment screen. For example, mdm.acme.com.
- **Group ID** – This Group ID associates your device with your corporate role and is defined in the AirWatch Admin Console.
- **Credentials** – This username and password allow you to access your AirWatch environment. These credentials may be the same as your network directory services or may be uniquely defined in the AirWatch Admin Console.

In This Section

- **Capabilities Based on Enrollment Type** – Displays a comparison between agent-based and agentless enrollment for iOS devices.
- **Enrolling an iOS Device with the AirWatch Agent** – Covers how to enroll an iOS device using the AirWatch Agent application.
- **Enroll an iOS Device with the Safari Browser** – Covers how to perform agentless enrollment using the Safari browser on your iOS device.
- **Enroll an iOS Devices in Bulk using Apple Configurator** – Provides an overview of enrolling using the Apple Configurator utility.
### Capabilities Based on Enrollment Type

The following capabilities matrix lists supported features for agent-based and agentless enrollment types.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Agent-Based</th>
<th>Agentless</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enrollment</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requires Apple ID</td>
<td>Required</td>
<td>Optional</td>
</tr>
<tr>
<td>Force EULA/Terms of Use Acceptance</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Active Directory/LDAP/SAML Integration</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Two Factor Authentication</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>BYOD Support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Device Staging Support</td>
<td>Yes⁰</td>
<td>Yes</td>
</tr>
<tr>
<td>Branding</td>
<td>Partial</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Configuration Profile Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and Manage Profiles</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security Settings (Data Encryption, Password Policy, etc.)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Device Restrictions</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Certificate Management</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Email and Exchange ActiveSync management</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Device Information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Information (model, serial number, IMEI number, etc.)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>GPS Tracking</td>
<td>Yes</td>
<td>Yes†</td>
</tr>
<tr>
<td>Phone Number</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Memory Information</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Battery Information</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>UDID</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Compromised/Jailbreak Detection</td>
<td>Yes</td>
<td>Yes†</td>
</tr>
<tr>
<td><strong>Network Information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Agent-Based</td>
<td>Agentless</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Cellular Information (MCC/MNC, SIM card info, etc.)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Telecom Roaming Information</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Telecom Usage Information</td>
<td>Yes</td>
<td>Yes†</td>
</tr>
<tr>
<td>IP Address</td>
<td>Yes</td>
<td>Yes†</td>
</tr>
<tr>
<td>Bluetooth MAC address</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Wi-Fi MAC address</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Management Commands</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Device Wipe</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Enterprise Wipe</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Lock Device</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Clear Passcode</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Email Messaging</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SMS Messaging</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>APNs Push Messaging</td>
<td>Yes</td>
<td>Yes†</td>
</tr>
<tr>
<td><strong>Application Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and Manage Applications</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Volume Purchase Program (VPP)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Application List</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Number Badging for App Updates</td>
<td>Yes</td>
<td>Yes†</td>
</tr>
<tr>
<td><strong>Content Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content Management</td>
<td>Yes*</td>
<td>Yes*</td>
</tr>
</tbody>
</table>

⁰ Requires end user to transfer purchases when syncing for first time.
† Requires AirWatch SDK embedded application to be present on device.
* Requires AirWatch Secure Content Locker App from iTunes.
Enrolling an iOS Device with the AirWatch Agent

The agent-based enrollment process secures a connection between iOS devices and your AirWatch environment. The AirWatch Agent is the application that facilitates enrollment and allows for real-time management and access to relevant device information. Use the following instructions to install the AirWatch Agent and enroll with your credentials.

1. Navigate to AWAgent.com from the Safari browser.
   AirWatch will automatically detect if the AirWatch Agent is installed on your device and, if it is not, it will redirect you to the App Store to download it.

   **Note:** An Apple ID is required to download the AirWatch Agent from the iTunes store.

2. Download and install the AirWatch Agent from the App Store, if needed.

3. Launch the AirWatch Agent or return to your browser session to continue enrollment. Enter one of the following:
   - Select **Continue Without Email Address** and you will be prompted for the Enrollment URL and your Group ID. Click **Continue**. The My Device screen displays.

4. Enter your Group ID, username and password credentials.

5. Follow the remaining prompts to complete enrollment.
   You may be notified at this time if your user account is not allowed or blocked because your account is blacklisted and not approved for enrollment.

Enroll an iOS Device with the Safari Browser

You can enroll devices using an agentless process that leverages the iOS device's built-in Safari browser. This approach is best suited for deployments where security is not a top priority and where users do not have an available Apple ID to download the AirWatch Agent. To perform agentless enrollment:

1. Open Safari on the iOS device.

2. Navigate to **https://<environment name>.com/enroll**.

3. Enter the required information, depending on your environment’s enrollment options. For example, this could be a Group ID and credentials.

4. Accept the terms of use.

5. Follow any install prompts until enrollment is complete.

Enroll an iOS Devices in Bulk using Apple Configurator

You can enroll devices by using Apple Configurator for Mac OS X, which is a tool that lets you configure and deploy iOS devices for your organization via USB connection. For example, you could use this tool to conduct a scaled deployment of iOS devices with ease. By integrating Configurator with AirWatch, you can benefit from maintained management visibility of devices and continued life-cycle management beyond the initial configuration. In addition, you can take advantage of the unique setup capabilities offered by Configurator, such as iOS versioning enforcement and complete backup prevention.
With Configurator, you can:

- Prepare a single, central backup “image” to consistently mass configure devices.
- Install the AirWatch 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 AirWatch Admin Console before enrolling with Configurator.
- Configure and update corporate device settings and apps over-the-air in AirWatch.

For additional information on the additional security features Configurator provides for supervised devices, see iOS Device Profiles.

**Note:** For steps to integrate Apple Configurator with AirWatch or for more information, refer to the AirWatch Integration with Apple Configurator document.
Overview

Create iOS device profiles to ensure proper usage of devices, protection of sensitive data, and workplace functionality. Profiles serve many different purposes, from letting you enforce corporate rules and procedures to tailoring and preparing iOS devices for how they will be used. The individual settings you configure, such as those for passcodes, Wi-Fi, VPN and email, are referred to as payloads. In most cases it is recommended that you only configure one payload per profile, which means you will have multiple profiles for the different settings you wish to push to devices. For example, you can create a profile to integrate with your email server and another to connect devices to your workplace Wi-Fi network.

Supervised Mode

Certain profile settings have an icon displayed to the right, which indicates the minimum iOS requirement needed to enforce that setting or restriction. For example, in the following graphic, to disallow end users from using AirDrop to share files with other Mac computers and iOS devices you would uncheck the box next to Allow AirDrop. The iOS 7 + Supervised icon means only devices running iOS 7 that are also set to run in Supervised mode via Apple Configurator will be affected by this restriction. For more information about configuring Apple Configurator, please see the AirWatch Integration with Apple Configurator Guide.

To see a complete list of iOS version and supervised requirements, see Appendix A – iOS Functionality: Supervised vs. Unsupervised.

In This Section

- Configuring General Profile Settings – Covers how to set up a profile's general settings.
- Enforcing a Passcode Policy – Covers the multiple fields and levels of complexity for a passcode policy in the AirWatch Admin Console.
- Enforcing Device Restrictions – Details the restriction payloads used to secure and protect iOS devices available in the AirWatch Admin Console.
- Configuring Wi-Fi Access – Details the steps required to configure a device with your organization's Wi-Fi network.
- Configuring Virtual Private Network (VPN) Access – Details the steps required to configure a device with your organization's VPN client.
- Configuring VPN On Demand for iOS Devices – Details the steps required to enable VPN On Demand, which automatically establishes a VPN connection for specific domains.
- Configuring Per-App VPN for iOS Devices – Covers how to set up Per App VPN for iOS 7+ devices, which forces all traffic for certain apps through your VPN provider.
• **Deploying Email Account Settings** – Explains how to create an Email profile for iOS devices to configure email settings on the device.

• **Enabling Exchange ActiveSync (EAS) Mail for iOS Devices** – Outlines the process for configuring EAS for accessing mail on iOS devices.

• **Deploying EAS Mail via Native Mail Client** – Details deploying an EAS payload leveraging the native iOS email client.

• **Deploying EAS Mail via NitroDesk's TouchDown Client** – Details deploying an EAS payload leveraging the NitroDesk TouchDown email client.

• **Deploying EAS Mail via AirWatch Inbox** – Details deploying an EAS payload leveraging the AirWatch Inbox email client.

• **Configuring LDAP Settings** – Explains how to create an LDAP profile to allow end users to access and integrate with your corporate LDAPv3 directory information.

• **Syncing Calendars and Contacts with CalDAV/CardDAV** – Describes how to create a CalDAV or CardDAV profile to allow end users to sync corporate calendar items and contact.

• **Subscribed Calendars** – Explains how to push calendar subscriptions made using the Calendar app in OS X to your iOS devices.

• **Deploying Web Clips** – Covers how to deploy Web Clips to devices, which serve as bookmarks/hyperlinks pointing to commonly used or recommended web resources.

• **Associating a SCEP/Credentials Payload with a Profile** – Details certificate-based authentication for iOS devices and the configuration options available in the AirWatch Admin Console.

• **Configuring a Global HTTP Proxy** – Describes how to define a global HTTP proxy for all traffic for iOS 6+ supervised devices.

• **Configuring Single App Mode** – Explains how to configure single app mode to place your devices in single app mode.

• **Implementing a Web Content Filter** – Details how to set up a web content filter through website whitelists and blacklists.

• **Enabling Single Sign On for Apps** – Describes the process for enabling Kerberos-based single sign on authentication for your apps.

• **Whitelisting AirPlay Destinations** – Explains how to whitelist devices to control which devices can broadcast over AirPlay.

• **Configuring AirPrint for iOS Devices** – Details how to set up automatic detection of AirPrint printers.

• **Profile Advanced** – Details how to configure customized advanced APNs settings.

• **Using Custom Settings** – Explains how to input custom settings payloads with iOS devices.

• **Time Schedules** – Details time schedules and how they are created and applied to profiles.
Configuring General Profile Settings

The process for creating a profile consists of two parts. First, you must specify the General settings for the profile. The General settings determine how the profile is deployed and who receives it as well as other overall settings. Next, you must specify the payload for the profile. The payload is the type of restriction or setting applied to the device when the profile is installed. The general settings listed below apply to any profile:

1. Navigate to Devices ▶ Profiles ▶ List View and select Add.
2. Select the appropriate platform for the profile you wish to deploy.
3. Configure General settings on the applicable tab. These include:
   - **Name** – Name of the profile to be displayed in the AirWatch Admin Console.
   - **Description** – A brief description of the profile that indicates its purpose.
   - **Deployment** – Determines if the profile will be automatically removed upon unenrollment:
     - **Managed** – The profile is removed.
     - **Manual** – The profile remains installed until removed by the end user.
   - **Assignment Type** – Determines how the profile is deployed to devices:
     - **Auto** – The profile is deployed to all devices automatically.
     - **Optional** – The end user can optionally install the profile from the Self-Service Portal (SSP) or can be deployed to individual devices at the administrator's discretion.
     - **Interactive** – This is a unique assignment type in which the profile integrates with third-party systems to deploy a specific payload to a device.
     - **Compliance** – The profile is deployed when the end user violates a compliance policy applicable to the device.
   - **Minimum Operating System** – The minimum operating system required to receive the profile.
   - **Model** – The type of device to receive the profile.
   - **Ownership** – Determines which ownership category receives the profile:
   - **Allow Removal** – Determines if the profile can be removed by the device's end user:
     - **Always** – The end user can manually remove the profile at any time.
     - **With Authorization** – The end user can remove the profile with the authorization of the administrator.
     - **Never** – The end user cannot remove the profile from the device.
   - **Managed By** – The Organization Group with administrative access to the profile.
   - **Assigned Organization Groups** – The Organization Groups that receive the profile.
   - **Additional Assignment Criteria** – These check boxes enable additional restrictions for the profile:
     - **Publish only to users in selected User Groups** – Specify one or more User Groups to receive the profile.
Enable Scheduling and install only during selected time periods – Specify a configured time schedule in which devices receive the profile only within that time-frame. See Time Schedules for more information.

4. Configure a payload for the device platform.

Note: For step-by-step instructions on configuring a specific payload for a particular platform, please refer to the applicable Platform Guide.

5. Select Save & Publish.

Enforcing a Device Passcode Policy

Device passcode profiles present a simple use case for securing iOS devices. For example, you may require your executives to have more complex passcodes on their devices compared to other employees. In addition, you may decide that while corporate-owned devices should have a maximum number of failed passcode attempts before blocking access, it may not be appropriate to apply the same profile to personal devices enrolled as part of a BYOD program. In addition, a passcode, when set on an iOS device, provides hardware encryption for the device.

When creating a passcode, you can configure:

- **Complexity** – Allow simple values for quick access or require alphanumeric passcodes for security. You can also require X number of complex characters (@, #, &, !, ?) in the passcode. For example, users with access to extremely sensitive content can be required to use more stringent passcodes.

- **Maximum Number of Failed Attempts** – Prevent unauthorized access by blocking access after X attempts. This helps prevent illegitimate users from attempting to repeatedly access content for which they do not have permission. For example, if set to 11 then if a user were to enter a wrong passcode 11 times in a row the device will automatically perform a full device wipe. If set to None, the Erase Data option is turned off, and after six failed attempts the device will be disabled for some 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)** – Locks the device automatically after the time period elapses. This can help ensure content on the device is not compromised if an end user accidentally leaves their phone somewhere.

To create a passcode profile

1. Navigate to Devices ➤Profiles ➤List View ➤Add. Select Apple iOS.
2. Configure General profile settings as appropriate.
3. Select the Passcode payload from the list.
4. Configure Passcode settings, including:
   - **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 must have.
• **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 device lock (min)** – Select the amount of time in minutes that must pass while a device is locked before an end user must re-enter their passcode.

• **Maximum Number of Failed Attempts** – Select the number of attempts allowed. If the end user enters an incorrect passcode for the set number of times, the device performs a factory reset.

5. Select **Save & Publish**.

### Enforcing Device Restrictions

One of the major challenges of managing mobile devices is that end users can use their devices in limitless ways, which can make it difficult to keep sensitive corporate information protected. **Restriction profiles** limit how employees can use their iOS devices and provide the control needed to effectively lock down a device if necessary. Restrictions profiles can lock down native functionality of iOS devices to help protect corporate information and enforce data-loss prevention.

**Note:** Certain restriction options on the Restrictions profile page will have an icon displayed to the right, which indicates the minimum iOS requirement needed to enforce that restriction. For example, in the following graphic, to disallow end users from using AirDrop to share files with other Mac computers and iOS devices you would uncheck the box next to **Allow AirDrop**. The **iOS 7 + Supervised** icon means only devices running iOS 7 that are also set to run in Supervised mode via Apple Configurator will be affected by this restriction.

![iOS 7 + Supervised](image)

**Note:** The step-by-step instructions below only list some 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**.

To create a restrictions profile:

1. Navigate to **Devices ►Profiles ►List View ►Add**. Select **Apple iOS**.

2. Configure **General profile settings** as appropriate.

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

4. Configure **Restrictions** settings, including:

   • **Device Functionality**
     
     Device-level restrictions can disable core device functionality such as the camera, FaceTime, Siri and in-app purchases to help improve productivity and security. For example:
     
     o Prohibiting device screen captures helps protect the confidentiality of corporate content on the device.
     
     o Disabling use of Siri even when the device is locked to prevent access to email, phone and notes without the secure passcode. *(iOS 5.1+)*
Note: For convenience, end users can hold down the Home button to use Siri even when a device is in a locked state. This could give others an opportunity to gain access to sensitive information and perform actions on a device they do not own. If your organization has strict security requirements, then consider deploying a Restrictions profile that restricts the use of Siri while a device is in a locked state.

- Preventing automatic syncing while roaming helps reduce data charges.
- Various iOS 7 restrictions, including:
  - Disallowing the ability to open managed app documents in unmanaged apps (and vice versa).
  - Disallowing AirDrop, which can be used to share files with other Mac computers and iOS devices.
  - Preventing fingerprint unlock for iPhone 5s devices.
  - Limiting ad tracking.
  - Disallowing account modifications.
  - Preventing certain information (Control Center, notifications) from appearing on the lock screen when the device is locked.

• Applications

Application-level restrictions can disable certain applications such as YouTube, iTunes Music Store and Safari, which enables you to enforce adherence to corporate policies for device usage. For example:

- Disabling Autofill ensures sensitive information does not automatically appear on certain forms.
- Enabling the Force Fraud Warning feature ensures Safari displays a warning when end users visit suspected phishing websites.
- Restricting Safari from accepting cookies ensures it does not accept any cookies or accepts cookies only from specific sites.
- Forbidding access to the Game Center and multiplayer gaming helps enforce corporate policies for device usage while at work.

• iCloud

For devices running iOS 5 and higher, end users can back up the data on their devices to the iCloud, a collection of Apple servers. This data includes photos, videos, device settings, app data, messages, ringtones and other data.

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

The iCloud enables data to be easily restored to a new or wiped device. Data backed up to Apple servers are encrypted in transit. Data on an iOS device that are stored in the iCloud can be accessed by Apple, and depending on your business sector, there may be rules and regulations that would prevent against storing enterprise data in the cloud. The iCloud-level restrictions apply only to iOS 5 and higher devices and can disable certain iCloud functionality such as backup, sync and photo stream. For example:

- Disabling document syncing so sensitive corporate content remains secure on the device.
- Disabling key sync value so app data such as a user's account passwords on a corporate device are not backed up to the iCloud and accessible from the user's other personal devices.
- Disabling photo stream so confidential image data on a corporate device cannot automatically sync to a user's unmanaged personal devices.
iCloud backups will only take place when:
- No restriction exists on iCloud backup.
- The iCloud toggle setting is enabled in Settings ► iCloud on the device.
- Wi-Fi is enabled.
- The device is connected to a power source and locked.

- Security and Privacy
  Security and privacy-based restrictions can prohibit end users from performing certain actions that might violate corporate policy or otherwise compromise their device. For example:
  - Preventing diagnostic data, which can include location information and usage data, to be sent to Apple to help them improve the iOS software.
  - Preventing users from accepting untrusted TLS certificates, which would prevent them from accessing websites with invalid SSL certificates; if allowed, users still would be notified of invalid certificates but could proceed if they wished.
  - Forcing encrypted backups, which ensures all personal information such as email account passwords or contact information is encrypted when backups are created and stored on devices.

- Media Content
  Ratings-based restrictions can prevent access to certain content based on its rating, which is managed by region. For example:
  - Restricting device access to adult or mature content on corporate-owned devices as part of a corporate policy.
  - Prohibiting device access to apps with a 17+ age restriction during normal business hours.
  - Blocking device access to inappropriate or explicit iBook content on corporate-owned devices.

5. Select Save & Publish.

Configuring Wi-Fi Access for iOS Devices

Configuring a Wi-Fi profile lets devices connect to corporate networks, even if they are hidden, encrypted, or password protected. This can be useful for end users who travel to various office locations that have their own unique wireless networks or for automatically configuring devices to connect to the appropriate wireless network while in an office. To create a Wi-Fi profile:

1. Navigate to Devices ► Profiles ► List View ► Add. Select Apple iOS.
2. Configure General profile settings as appropriate.
3. Select the Wi-Fi payload from the list.
4. Configure Wi-Fi settings, including:
   - **Service Set Identifier** – This is the name of the network the device connects to.
   - **Auto-Join** – This determines whether the device automatically connects to the network.
   - **Security Type** – This is the type of access protocol used and whether certificates are required.
• Wi-Fi Hotspot 2.0 – This enables Wi-Fi Hotspot 2.0 functionality and is only available to iOS 7 devices. Hotspot 2.0 is a type of public-access Wi-Fi that allows devices to seamlessly identify and connect to the best match access point. It can then authenticate without user input. Note that carrier plans must support Hotspot 2.0 for it to function correctly. Enabling this checkbox reveals the following additional options for configuring a Wi-Fi Hotspot 2.0:
  o Displayed Operator Name – Enter the name of the Wi-Fi hotspot service provider.
  o Domain Name – Enter the domain name of the Passpoint service provider.
  o Roaming Consortium Organization ID – Enter the roaming consortium organization identifiers.
  o Network Access ID – Enter the Network Access ID realm names.
  o MCC/MNC – Enter the Mobile Country Code/Mobile Network Configuration, formatted as a 6-digit number.
• Proxy – This enables an automatic or manual proxy that you can configure for your Wi-Fi profile.
• Protocols – These are the protocols that apply to your Wi-Fi network.
• Authentication – These are the credentials used to connect to the Wi-Fi network. If using certificate-based authentication, select an Identity Certificate after configuring a Credentials payload.
• Trust – This are the trusted server certificates for your Wi-Fi network.

5. Select Save & Publish.

Configuring Virtual Private Network (VPN) Access for iOS Devices

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 the on-site network. Configuring a VPN profile ensures end users have seamless access to email, files and content. To create a base VPN profile:

1. Navigate to Devices ►Profiles ►List View ►Add. Select Apple iOS.
2. Configure General profile settings as appropriate.
3. Select the VPN payload.
4. Configure VPN settings, including:
  o Connection Name – Enter the name of the connection name to be displayed.
  o Connection Type – Use the drop-down menu to select the network connection method.
    If you are using Websense or Blue Coat for content filtering, please see Creating a Websense Content Filter Profile and Creating a Blue Coat Content Filter Profile.
  o Server – Enter the hostname or IP address of the server to which to connect.
  o Account – Enter the name of the VPN account.
  o Send All Traffic – Select this check box to force all traffic through the specified network.
  o Per App VPN – Select this to enable Per App VPN. For more information, see Configuring Per-App VPN for iOS Devices.
- **User Authentication** – Select the radio button to indicate which method end users are authenticated. If you want to enable VPN On Demand to use certificates to automatically establish VPN connections, see [Configuring VPN On Demand for iOS Devices](#).

- **Shared Secret** – Enter the Shared Secret key to be provided to authorize end users for VPN access.

- **Proxy** – Use the drop-down menu to select either Manual or Auto Proxy.

5. **Select Save & Publish.**

End users will now have access to permitted sites based on your Blue Coat content filtering rules.

**Creating a Websense Content Filter Profile for iOS Devices**

AirWatch integration with Websense lets you leverage your existing content filtering categories in Websense and apply those to devices you manage within the AirWatch Admin Console. Allow or block access to websites according to the rules you configure in Websense and then deploy a VPN payload to force devices to comply with those rules. Directory users enrolled in AirWatch will be validated against Websense to determine which content filtering rules to apply based on the specific end user.

**Note:** You can enforce content filtering with Websense in one of two ways: through a VPN profile, which will apply to all web traffic using browsers other than the AirWatch Browser, or through the Settings and Policies page, which will apply to all web traffic using the AirWatch Browser. The first method is described below. For detailed instructions on configuring your Websense for use in the Content Filtering setting in Settings and Policies, please refer to the [AirWatch Browser Guide](#).

1. Navigate to **Devices ➤Profiles ➤List View ➤Add**. Select **Apple iOS**.

2. Configure **General profile settings** as appropriate.

3. Select **Websense** as the **Connection Type**.

4. Enter your Websense **Server** and **Username/Password** details.
   
   You can also optionally **Test Connection**.

5. **Select Save & Publish.**

Directory-based end users will now have access to permitted sites based on your Websense categories.

**Creating a Blue Coat Content Filter Profile for iOS Devices**

AirWatch integration with Blue Coat lets you leverage your existing content filtering rules in Blue Coat and apply those to devices you manage within the AirWatch Admin Console. Allow or block access to websites 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 ➤List View ➤Add**. Select **Apple iOS**.

2. Configure **General profile settings** as appropriate.

3. Select **Blue Coat** as the **Connection Type**.
4. Enter your **Blue Coat Customer ID**, which you can access by logging in to the Blue Coat website and accessing the API Tokens & Keys section, which lets you add an MDM partner and obtain the identifier. Please contact Blue Coat for additional information or assistance.

5. Optionally select **Per-App VPN** to enable Per App VPN. For more information, see [Configuring Per-App VPN for iOS Devices](#).
   
   You can also optionally **Test Connection**.

6. Select **Save & Publish**.

   End users will now have access to permitted sites based on your Blue Coat content filtering rules.

---

**Configuring VPN On Demand for iOS Devices**

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 leverages certificates for authentication instead of simple passcodes. Use the following instructions to distribute certificates through the AirWatch Admin Console during configuration and set up VPN On Demand.

1. Ensure your certificate authority and certificate templates in AirWatch 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 ▶ List View ▶ Add**, then **iOS**. Select the **VPN** payload from the list.

4. Configure your [base VPN profile](#) accordingly.

5. Select **Certificate** from the User Authentication dropdown, then click the **Credentials** payload.

6. Select **Defined Certificate Authority** from the Credential Source dropdown and select the **Certificate Authority** and **Certificate Template** from their respective drop down menus. Navigate back to the **VPN** payload.

7. Select the **Identity Certificate** from the dropdown as specified through the Credentials payload.

8. Check the Enable **VPN On Demand** box, specify the relevant **Domains** and choose the **On-Demand Action**:
   
   - **Always Establish** – Initiates a VPN connection regardless of whether the page can be accessed directly or not.
   
   - **Never Establish** – Does not initiate a VPN connection for addresses that match the specified the domain. However, if the VPN is already active, it may be used.
   
   - **Establish if Needed** – Initiates a VPN connection only if the specified page cannot be reached directly.

   **Note:** For wildcard characters, do not use the asterisk (*) symbol; use a dot in front of the domain. For example, *.air-watch.com.

9. Click **Save and Publish**.

   Once the profile installs on a user's device, a VPN connection prompt will automatically display whenever the user navigates to a site that requires it, such as SharePoint.
Configuring Per-App VPN for iOS Devices

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

1. Navigate to Devices ➤Profiles ➤List View ➤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 and is used to configure apps so they always use the Per-App VPN service for all of their network communication.
5. Select Connect Automatically to display fields for the Safari Domains that will trigger the automatic connection.
6. Select Save & Publish.

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

7. Navigate to Apps & Books ➤List View and select Add Application.
8. Access the Deployment tab and select Per-App VPN to enable the app for VPN.

Deploying Email Account Settings

Create an Email profile for iOS devices to configure email settings on the device. To create an Email profile:

1. Navigate to Devices ➤Profiles ➤List View and select Add. Select Apple iOS.
2. General settings for the profile.
3. Select the Email payload.
4. Configure Email account settings, including:
   - **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 this check box to block the user from forwarding email or opening in third-party apps.
   - **Disable recent contact sync** – Select this check box to restrict the user from syncing email contacts to their personal device. (iOS 6)
5. Configuring the user’s incoming email settings.
   - **Host Name** – Enter the name of the email server.
• **Port** – Enter the number of the port assigned to incoming mail traffic.
• **Username** – Enter the username 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.
• **Show Characters** – Select this check box if you want users to see characters as they type.
• **Use SSL** – Select this check box to enable Secure Socket Layer usage for incoming email traffic.

6. Configuring the user’s outgoing email settings.

• **Host Name** – The name of the email server.
• **Port** – Enter the number of the port assigned to incoming mail traffic.
• **Username** – Enter the username 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 this to auto-populate the Password field.
• **Password** – Enter the password required to authenticate the end user.
• **Show Characters** – Select this check box if you want users to see characters as they type.
• **Use SSL** – Select this check box to enable Secure Socket Layer usage for incoming email traffic.
• **Prevent Use in 3rd Party Apps** – Select this check box to prevent users from moving corporate email into other email clients.
• **Use S/MIME** – Select this check box to use additional encryption certificates.

### Enabling 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 username, email address and password. If you integrate AirWatch with Active Directory services, then this user information is automatically populated for the user and can be specified in the EAS profile through the use of look-up values.

### Create a Generic EAS Profile for Multiple Users

Before you create an EAS profile that will automatically enable devices to pull data from your mail server, you must first ensure 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** fields.
- You can prompt users to enter this information during enrollment by navigating to **Devices ►Settings ►General ►Enrollment** and under the **Optional Prompt** tab, checking the **Enable Enrollment Email Prompt** box.
Deploying EAS Mail via Native Mail Client for iOS Devices

1. Navigate to Devices ►Profiles ►List View ►Add. Select Apple iOS.
2. Configure General profile settings as appropriate.
3. Select the Exchange ActiveSync payload.
4. Select Native Mail Client for the Mail Client. Fill in the Account Name field with a description of this mail account. Fill in the Exchange ActiveSync Host with the external URL of your company’s ActiveSync server.

   **Note:** 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. Fill in the Username, Email Address and Email Domain Name using look-up values. Look-up values pull directly from the user account record. To use the {EmailUserName} and {EmailDomain} look-up values, ensure your AirWatch user accounts have an email address and email username defined.
6. Leave the Password field empty to prompt the user to enter a password.
7. Set the following optional settings, as necessary:
   - Payload Certificate – Define a certificate for cert-based authentication after the certificate is added to the Credentials payload.
   - 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 messages.
   - Disable recent contact sync – Prevent the automatic sync of recent contacts to devices.
8. Select Save and Publish to push the profile to available devices.

Deploying EAS Mail via NitroDesk's TouchDown Client for iOS Devices

The NitroDesk TouchDown mail application provides additional email security flexibility for iOS devices. It is a paid application available from the App Store. NitroDesk TouchDown integration with iOS devices requires the AirWatch Agent v4.4 or higher and the TouchDown mail client v1.8.1 or higher. You can create an EAS profile to leverage NitroDesk TouchDown with the following steps:

1. Navigate to Devices ►Profiles ►List View ►Add. Select Apple iOS.
2. Configure General profile settings as appropriate.
3. Select the Exchange ActiveSync payload.
4. Select NitroDesk TouchDown for the Mail Client. Fill in the Exchange ActiveSync Host with the external URL of your company’s EAS server.

   **Note:** The EAS server can be any mail server that implements the EAS protocol, such as Lotus Notes Traveler, Novell Data Synchronizer and Microsoft Exchange.
5. Fill in the **Username** and **Email Address** using look-up values. Look-up values pull directly from the user account record. To use the `{EmailUserName}` and `{EmailDomain}` look-up values, ensure your AirWatch user accounts have an email address and email username defined.

6. Leave the **Password** field empty to prompt the user to enter a password.

7. Set the additional NitroDesk TouchDown settings, such as sync settings, passcode requirements and security restrictions. Key settings include:

   - **Past Days of Mail/Calendar to Sync** – Set the amount of past days of Mail/Calendar TouchDown should sync and display.
   - **Require Manual Sync While Roaming** – Suppress automatic data sync when a device is on a roaming network. This can help reduce roaming charges.
   - **Enable HTML Email** – Enable to display all emails in HTML format.
   - **Maximum Email Truncation Size** – Set the maximum allowed email size (in KB) that can be received.
   - **Email Signature** – Specify an email signature to be used on the application.
   - **Enable Email Signature Editing** – Allow users to change the email signature.
   - **Passcode** – Enable this setting and configure various passcode complexity parameters.
   - **Enable Security Restrictions** – Enable this setting to enable or allow functionality that TouchDown may natively restrict. The following list details some of the key settings you can apply to your EAS profile to allow certain functionality:
     - **Allow Copy-paste** – Allow the copying and pasting of data from the TouchDown client.
     - **Enable Copy to Phonebook** – Enable this setting to cause TouchDown to copy contacts to the device phonebook.
     - **Allow Attachments** – Allow users to download email attachments.
     - **Maximum Attachment Size** – Sets the maximum attachment size (in MB) that can be received.
     - **Allow Data Export** – Enable this setting to allow export of calendar/email to native apps.
     - **Show Email/Calendar/Task Info on Notification Bar** – Enable TouchDown to show information (for example, the first few lines of an email) as a notification when email/calendar/task information is received.
     - **Allow Printing** – Allows users to print email.
     - **Show Data On Lock Screen Widgets** – Enable this setting to allow lock screen widgets to display email/calendar/task data.

8. Select **Save & Publish**.

   **Note:** For iOS devices, you do not enter License Key information in the EAS Profile for NitroDesk TouchDown. You can deploy it as a Volume Purchase Program (VPP) application from the AirWatch Admin Console. Alternatively, you may tell users to purchase and download it themselves.

After deploying TouchDown as a recommended app, all profile configurations are applied to the app automatically. When the user first opens the TouchDown application the AirWatch Agent will launch and prompt the user to authorize the TouchDown application. Once authorized, TouchDown will re-open and the settings will be automatically applied.
Deploying EAS Mail via AirWatch Inbox for iOS Devices

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

1. Navigate to Device ►Profiles ►List View.
2. Click Add and select iOS as the platform.
3. Configure General profile settings as appropriate.
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.airwatchmdm.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. Prior to enabling this option, ensure you have uploaded necessary certificates under Credentials profile settings.
     
   Note: 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 field.
   - Select the certificate/smart card to both sign and encrypt email messages in the S/MIME Encryption Certificate field.
   - 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, which is the information used to authenticate user connections to your EAS Host. The profile supports lookup fields for inserting enrollment user’s information and login information. See Username and Password for more information.

7. Configure Settings, such as:
   - Enable Email
   - Enable Calendar
   - Enable Contacts
   - Sync Interval – The frequency with which the AirWatch Inbox app syncs with the email server.
   - Email Notifications – Configure how end users can be notified of new emails. Disabled means they will 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
   - Email Size (default is unlimited)
   - Email Signature
   - Enable Signature Editing
8. Configure a Passcode for AirWatch Inbox. You can require an end user to enter a passcode when the AirWatch Inbox is opened. This is not the email account password, but the passcode the user will have to enter to access the application. The following passcode settings are available:

- **Authentication Type**
  To allow iOS users to log in using their AirWatch credentials, select **Username and Password** as the **Authentication Type** under the **Passcode** section.

- **Complexity**, including whether to allow simple passcodes (e.g. 1111).

- **Minimum Length**

- **Minimum Number of Complex Characters**, if your **Complexity** is set to **Alphanumeric**.

- **Maximum Passcode Age** (days)

- **Passcode History**

- **Auto-Lock Timeout** (min)

- **Maximum Number of Failed Attempts**

9. Configure additional 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 AirWatch Browser app only.**

- **Restrict attachments to open only in other apps of your choosing.**

- **Set a Maximum Attachment Size** (MB).

- **Allow Printing.**

10. Select **Save & Publish** when you are done.

**Username and Password**

You can define the username that is used for users to log in to the AirWatch Inbox. This could be their actual email address or an email username that is different from their actual email address. When configuring the Exchange ActiveSync (EAS) payload in the AirWatch Inbox profile settings, there is a **User** field under **Login Information** that you can set to a predefined lookup value.

If you have email usernames that are different than users' email addresses, you can use the {{EmailUserName}} field, which corresponds to the email usernames imported during directory service integration. If your users' email usernames are same as their email addresses, you would still use the {{EmailUserName}} field, which would use their email addresses as they were imported during directory service integration.

**Removing Profile or Enterprise Wiping**

If the profile is removed via the remove profile command, compliance policies, or through an enterprise wipe, all email data gets deleted, including:
- User account/login information.
- Email message data.
- Contacts and calendar information.
- Attachments that were saved to the internal application storage.

**Note:** Attachments saved outside of AirWatch Inbox will **not** be deleted.

### Configuring LDAP Settings

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

1. Navigate to **Devices ➤ Profiles ➤ List View** and select **Add**. Select **Apple iOS**.
2. Configure **General profile settings** as appropriate.
3. Select the **LDAP** payload.
4. Configure LDAP settings, including:
   - **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 username 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 usage.
   - **Search Settings** – Click **Add** and enter settings for Active Directory searches executed from the device.
5. Select **Save & Publish**.

### Syncing Calendars and Contacts with CalDAV/CardDAV

Create 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 ➤ List View** and select **Add**. Select **Apple iOS**.
2. Configure **General profile settings** as appropriate.
3. Select the **CalDAV or CardDAV** payload.
4. Configure CalDAV or CardDAV settings, including:
   - **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 username 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 usage for communication with the server.

5. Select **Save & Publish**.

### Configuring Subscribed Calendars

Push calendar subscriptions made using the Calendar app in OS X to your iOS devices by configuring a Subscribed Calendars payload.

1. Navigate to **Devices ➤Profiles ➤List View** and select **Add**. Select **Apple iOS**.

2. Configure **General profile settings** as appropriate.

3. Select the **Subscribed Calendars** payload.

4. Configure Subscribed Calendars settings, including:
   
   • **Description** – Enter a brief description of the subscribed calendars.
   
   • **URL** – Enter the URL of the calendar to which you are subscribing.
   
   • **Username** – Enter the username 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**.

### Deploying Web Clips

Web Clips are web bookmarks that you can push to devices that will display as apps on the device or in your App Catalog. In fact, you can deploy the Self-Service Portal, App Catalog, and Book Catalog as Web Clips. To create a Web Clip:

1. Navigate to **Devices ➤Profiles ➤List View ➤Add**. Select **Apple iOS**.

2. Configure **General profile settings** as appropriate.

3. Select the **Web Clips** payload from the list.

4. Configure **Web Clip** settings, including:

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

   • **URL** – Enter the URL the Web Clip that will display. Below are some examples for AirWatch pages:
     
     o For the SSP, use: **https://<AirWatchEnvironment>/mydevice/**.
     
     o For the App Catalog, use:
       
       Unencrypted – **https://<Environment>/Catalog/AppCatalog?uid={DeviceUid}**
Encrypted – https://<Environment>/Catalog/AppCatalog?uid={SecureDeviceUdid}
  o For the Book Catalog, use: https://<Environment>/Catalog/BookCatalog?uid={DeviceUid}
• Removable – Select this option to allow end users to remove the Web Clip.
• Icon – Upload the custom icon, in .gif, .jpg, or .png format, for the application.
  o For best results, provide a square image no larger than 400 pixels on each side and less than 1 MB in size when uncompressed. The graphic will be automatically scaled and cropped to fit, if necessary and converted to png format. 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 launch the webpage in full screen mode.
• Show in App Catalog/Workspace – Select this option to list the application in your Enterprise App Catalog. You might use this setting if you do not set the profile to deploy automatically.
5. Select Save & Publish.

Associating a SCEP/Credentials Payload with a Profile

Even if you protect your corporate email, Wi-Fi and VPN with strong passcodes and other restrictions, your infrastructure still remains 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 do this, 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 certificates down to devices, you need to 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 ►List View ►Add and select iOS from the platform list.
2. Configure General profile settings as appropriate.
3. Select either an 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 and Upload a certificate. Or, select Defined Certificate Authority from the Credential Source drop-down menu and select the Certificate Authority and Certificate Template from their respective drop-down menu. Or, select User Certificate and the intended use for the S/MIME certificate.
5. Navigate back to the previous payload for EAS, Wi-Fi or VPN.
6. 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 dropdown. Select the Identity Certificate.
7. Select Save & Publish when you are done configuring any remaining settings.
Configuring a Global HTTP Proxy

You can configure a global HTTP proxy that directs traffic from Supervised iOS 6 and higher devices through a designated proxy server for all Wi-Fi connections. For example, a school can set a global proxy to ensure all web browsing is routed through its web content filter. To create a global HTTP proxy profile:

1. Navigate to Devices ►Profiles ►List View ►Add. Select Apple iOS.
2. Configure General profile settings as appropriate.
3. Select the Global HTTP Proxy payload from the list.
4. Configure Global HTTP Proxy settings, including:
   - Proxy Server – Enter the URL of the Proxy Server.
   - Proxy Server Port – Enter the port used to communicate with the proxy.
   - Proxy Username/Password – If the proxy requires credentials, you can use look-up values to define the authentication method.
   - Proxy PAC File URL – If you selected Auto as the Proxy Type, you can enter the URL of the Proxy PAC File to automatically apply its settings.
5. Select Save & Publish.

Configuring Single App Mode

Single App Mode provides enterprises a convenient way to provision devices so they can only access a single app of their 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 ensures the device is not used for anything outside of the desired application and will have no way of accessing unintended entertainment apps, device settings or an Internet browser.

This feature is particularly useful for restaurants and retail stores, where customers can place orders, make reservations, browse current inventory, or pay for their order. In the education industry, students can utilize devices with locked access to a single education game, eBook or exercise. Using this feature is easy; it can be dynamically enabled, adjusted or disabled from the AirWatch Admin Console, right next to the rest of the devices in your fleet.

Requirements

- An iOS 6 or higher device configured in Supervised mode. (iOS 7 required for additional options and autonomous single app mode).

Enable Single App Mode

Single App Mode is an available payload that can be selected as part of a device profile. Use the following instructions to enable it:

1. Ensure the application of choice is installed on the device.
2. Locate the application's unique Bundle ID. This can be found through either the:
   - Dashboard – Select a device, choose the Apps & Books tab and find the ID listed for any installed apps.
• **Public App Search** – Search for a specific app directly from the AirWatch Admin Console. For example: com.airwatch.browser.

3. Navigate to **Devices ▶ Profiles ▶ List View ▶ Add.** Select **Apple iOS.**

4. Configure [General profile settings](#) as appropriate.

5. Select the **Single App Mode** payload.

6. Select one of the following single app lock modes:

   • Select **Lock device into a single app** to lock devices into a single application until the profile with this payload is removed. The home button will be disabled, and the device will always return to the specified application from a sleep state or reboot. Enter the application's Bundle ID.

     With this setting, for Supervised iOS 7 devices, you can configure the following optional settings:

     ![Optional Settings](image)

     • Select **Permitted apps for autonomous single app mode** to allow applications to enable or disable Single App Mode on their own. Add the Application Bundle IDs that are permitted to place themselves into and out of a Single App Mode lock state.

7. Select **Save and publish.** Each device provisioned with this profile will enter Single App Mode.

### Exit Single App Mode

By design, end users cannot exit the app when Single App Mode is enabled. The home button is disabled and manually restarting the device will reboot directly into the specified app. You may want to temporarily disable Single App Mode if you want to update the specified app to a new version or release. To do this, you would disable Single App Mode using the instructions below, install the new app version, and enable Single App Mode again.

1. Navigate to **Devices ▶ Profiles ▶ List View.** In the row for the Single App Mode profile, click the **View Devices** icon.

2. In the row for the device from which you want to remove the setting, click **Remove Profile.**
Restart a Device Operating in Single App Mode

Follow the hard reset procedures below 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.

Implementing a Web Content Filter

You can allow or prevent end users from accessing specific URLs from the Safari web browser by configuring a web content filter payload. All URLs should 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 Supervised iOS 7+ devices.

Add URLs to Whitelist

If you add whitelisted URLs to the payload, then end users will not be able to access any other websites than the ones you specify. In addition, for multiple whitelists, only URLs that appear in every whitelist are accessible. The sites are added to Safari as bookmarks.

1. Navigate to Devices ►Profiles ►List View ►Add. Select iOS.
2. Configure General profile settings as appropriate.
3. Select the Web Content Filter payload.
4. Select Allow URLs if it is not already selected.
5. Select Add and enter the following information:
   - Allowed URL – The URL of a whitelisted site.
   - Title – The bookmark title.
   - Bookmark Path – The folder into which the bookmark will be added in Safari.

Add URLs to Blacklist

If you add blacklisted URLs to the payload, then end users will be able to access any site other than the ones you specify, which will be blocked. For multiple blacklists, any URL that appears in any blacklist will be inaccessible. Also, websites with profanity will be automatically filtered. URLs can be specified in a permitted list if you want to make exceptions to these automatically filtered sites.

1. Navigate to Devices ►Profiles ►List View ►Add. Select iOS.
2. Configure General profile settings as appropriate.
3. Select the **Web Content Filter** payload.

4. Select **Deny URLs** if it is not already selected.

5. Enter **Blacklisted URLs** and separate with new lines, spaces or commas. All URLs should begin with `http://` or `https://`.

6. Select whether or not to **Automatically filter inappropriate websites** (for example, adult websites).

7. Enter **Permitted URLs** if you want to add an exception to the automatic filter.

---

### Enabling Single Sign On for Apps

Enabling Single Sign On lets your end users access native device apps and web applications without having to enter username and password credentials each and every time. End users of iOS 7 devices will not store passwords on their devices and instead authenticate using Kerberos authentication. Note that these Single Sign On settings differ from those used for the AirWatch Workspace and internal AirWatch apps, which are set under **Apps & Books ➤ Settings ➤ Settings and Policies ➤ Security Policies**. For more information on these Single Sign On settings, refer to the AirWatch Mobile Application Management Guide.

To create a profile for iOS single sign on:

1. Navigate to **Devices ➤ Profiles ➤ List View ➤ Add** and select **iOS**.

2. Configure **General profile settings** as appropriate.

3. Select the **Single Sign On** payload.

4. Enter **Connection Info**, which includes Account Name, Kerberos Principal Name, and Realm.

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 blank, the account is eligible to match all HTTP and HTTPS URLs.

6. Enter the **Application Bundle IDs** that are allowed to leverage this login information. For example: `com.apple.mobilesafari`.

7. Select **Save and Publish**.

---

### Whitelisting AirPlay Destinations

Configuring the AirPlay payload lets you whitelist a specific set of devices to receive broadcast privileges according to device ID. Additionally, 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 will work even if you do not enroll your Apple TVs with AirWatch. For more information about Apple TV capabilities, please see the AirWatch Apple TV Guide.

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

To configure an AirPlay destination whitelist:

1. Navigate to **Devices ➤ Profiles ➤ List View**

2. Click **Add** and choose **Apple iOS** from the platform list.

3. Configure **General profile settings** as appropriate.
4. Select the **AirPlay Mirroring** payload tab.
5. Click **Add** under Whitelisted AirPlay Destinations.
6. Enter the destination and device information, including:
   - **Destination Name** – This is the name of the destination display. The name must match the Apple TV device name and is case-sensitive. The device name can be found on the Apple TV device settings.
   - **Allowed Destination Device ID** – This is the device ID for the destination display. Device IDs include the MAC address or Ethernet address formatted as XX:XX:XX:XX:XX:XX)
   - **Password** – This is the password that shows on the user’s device when attempting to mirror to the destination. This password is only required if a password is required to mirror to the Apple TV.
7. Select **Add** to create additional destinations and corresponding device whitelists.
8. Click **Save and Publish** when you are done configuring AirPlay settings.

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

1. Navigate to **Devices ►List View**, locate the device intending to AirPlay, and select the device’s Friendly Name.
2. Select **Support** and select **Play AirPlay** from the list of support options.
3. Choose the Destination created in the AirPlay profile, enter 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 manually disable AirPlay on the device, return to the device’s Control Panel, select **Support** and select **Stop AirPlay**.

### Configuring AirPrint for iOS Devices

Configuring the AirPrint payload for iOS devices enables devices 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 **Profiles ►Device Profiles** and select **Add**, then **iOS**.
2. Configure **General profile settings** as appropriate.
3. Select the **AirPrint** payload tab.
4. Enter the IP address (XXX.XXX.XXX.XXX) and Resource Path ( for example, ipp/printer or printers/Canon_MG5300_series) associated with the AirPrint printer. Select **Add** to include additional AirPrint printers or use the **Remove** button to delete existing AirPrint printers.
5. Select **Save and Publish**.

### Configuring Advanced APN Settings

An Access Point Name (APN) defines the network path for all cellular data connectivity, and APN settings dictate how your iOS devices access your carrier’s network. If you need to use a different APN from the default then you can create and push an Advanced payload to devices. Note that if your APN settings are incorrect you may lose functionality, so be
sure to check with your carrier as to the correct APN settings to use. For more information on the subject, see Apple’s knowledge base article.

1. Navigate to Devices ➤Profiles ➤List View and select Add. Select Apple iOS.
2. Configure General profile settings as appropriate.
3. Select the Advanced payload.
4. Configure Advanced settings, including:
   - **Access Point Name (APN)** – Enter the APN provided by your carrier.
   - **Access Point Username** – Enter the username used for authentication.
   - **Access Point 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.
5. Select Save & Publish.

Using Custom Settings

The Custom Settings payload can be used when Apple releases new iOS functionality or features that AirWatch does not currently support through its native payloads. If you do not want to wait for the newest release of AirWatch to be able to control these settings, you can use the Custom Settings payload and XML code to manually enable or disable certain settings. To do this you would use the following instructions:

1. Navigate to Devices ➤Profiles ➤List View ➤Add. Select iOS.
2. Complete General information as necessary and then configure the appropriate payload (for example, Restrictions or Passcode).
   You can work on a copy of your profile, saved under a "test" Organization Group, to avoid affecting users before you are ready to Save and Publish.
3. Save, but do not publish, your profile.
4. Select View XML from the actions menu in the Profiles List View for the row of the profile you wish to customize.

5. Find the section of text starting with `<dict>` ... </dict> that you configured previously, for example, Restrictions or Passcode. The section will contain a configuration type identifying its purpose, for example, restrictions.
6. Copy this section of text and close the XML View. Open your profile.
7. Select the Custom Settings payload and click Configure. Paste the XML you copied in the text box. The XML code you paste should contain the complete block of code, from `<dict>` to `</dict>`.
8. Remove the original payload you configured by selecting the base payload section, for example, Restrictions, Passcode and clicking the minus [-] button.

You can now enhance the profile by adding custom XML code for the new functionality. Note that:

- Any device not upgraded to the latest iOS version will ignore the enhancements you create.
- Since the code is now custom, you should test the profile devices with older iOS versions to verify expected behavior.
Time Schedules

In addition to simply assigning applicable profiles, you have the ability to enhance device management further by controlling when each profile assigned to the device is active. Configure and apply time schedules to restrict when profiles are active on the device. Applying time schedules to profiles secures your corporate resources by only allowing employees access during the specific days and time frames. Conversely, applying time schedules can also limit personal content and access during work hours.

In This Section

- **Defining Time Schedules** – See how to create a time schedule, which allows or denies access to internal content and features based on the day and time.
- **Applying a Time Schedule to a Profile** – See how to apply a time schedule to a profile, which lets you control when and how a particular profile is activated.

**Defining Time Schedules**

To create a time schedule:

1. Navigate to Devices ▶ Profiles ▶ Settings ▶ Time Schedules.
2. Select Add Schedule to launch the Add Schedule window.
3. Enter a name for the schedule in the Schedule Name field.
4. Select the applicable Time Zone using the drop-down menu.
5. Select the Add Schedule hyperlink.
6. Select the Day of the Week, Start Time and End Time using the applicable drop-down menus. You can also select the All Day check box to disable start and end times for the schedule. To remove a day from the schedule, select the applicable X under Actions.
7. Repeat steps 5 and 6 as many times as is necessary to add additional days to the schedule.

8. Select **Save**.

**Applying a Time Schedule to a Profile**

Once you have defined a time schedule, you can apply it to a profile and combine it with other payloads to create more robust profiles. For example, you can define time schedules for the normal work hours of different organization groups and add a Restrictions payload that denies access to the Game Center, multiplayer gaming or YouTube content based on ratings and other settings.

Once activated, the employees of the Organization Group to whom the profile was applied will no longer have access to these functions during the specified times.

1. Navigate to **Devices ➤ Profiles ➤ List View ➤ Add** and select your platform.

2. Select **Enable Scheduling and install only during selected time periods** on the **General** tab. An **Assigned Schedules** box displays.

3. Enter one or multiple Time Schedules to this profile.

4. Configure a payload, such as Passcode, Restrictions or Wi-Fi that you want to apply only while devices are inside the time frames.

5. Select **Save & Publish**.
**Compliance**

The **Compliance Engine** is an automated tool by AirWatch that ensures all devices abide by your policies. Your policies may include basic security settings such as requiring a passcode and having a minimum device lock period. You may also decide to set password strength, blacklist certain apps and require device check-in intervals to ensure devices are safe and in-contact with the AirWatch servers.

Once configuration is complete and devices are out of compliance, the Compliance Engine begins to warn the user to fix compliance errors to prevent disciplinary action on the device. For example, if a user loads blacklisted games or social media apps onto their device, the Compliance Engine sends a message to notify the user that their device is out of compliance. If the errors are not corrected in the amount of time specified, the device loses access to certain content and applications.

You may even automate the escalation process if corrections are not made. Lock down the device and notify the user to contact you to unlock the device. These escalation steps, disciplinary actions, grace periods and messages are all completely customizable with the AirWatch Admin Console.

Enforcing mobile security policies is as easy as:

- **Building your policies** – Customize your policy to cover everything from application list, compromised status, encryption, model and OS version, passcode and roaming.

- **Defining escalation** – Configure time-based actions in minutes, hours or days and take a tiered approach to those actions.

- **Specifying actions** – Send SMS, email or push notifications to the user's device or send an email only to an Administrator. Request device check-in, remove or block specific profiles, install compliance profiles, remove or block apps and perform an enterprise wipe.

**In This Section**

- [Enforcing Device Compliance](#) – Details the general process for setting up Compliance policies and the Compliance Engine.
Enforcing Device Compliance

Follow the steps below to set up and initiate the Compliance Engine complete with profiles and automated escalations:

1. Navigate to Devices ◀Compliance Policies ◀List View and select Add. Match Any or All rules to detect conditions. Select Next when rule definition is complete. The supported compliance policies by Platform are as follows:

<table>
<thead>
<tr>
<th>Compliance Policy</th>
<th>Apple iOS</th>
<th>Android</th>
<th>Mac OS X</th>
<th>Windows Mobile (Motorola)</th>
<th>Windows Phone 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application List</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compromised Status</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Device Last Seen</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Interactive Certificate Profile Expiry</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Compromised Scan</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDM Terms of Use Acceptance</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Model</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS Version</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passcode</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roaming</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIM Card Change</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Application List** – Detect specific, blacklisted apps that are installed on a device, or detect all apps that are not whitelisted.
  
  You can either specifically prohibit certain apps, such as social media or entertainment apps, or specifically permit only the apps you specify, such as internal applications for business use.

- **Compromised Status** – Select if the device is non-compliant when compromised.
  
  Prohibit the use of jailbroken devices that are enrolled with AirWatch. Jailbroken devices strip away integral security settings and may introduce malware in your network and provide access to your enterprise resources. Monitoring for compromised device status is especially important in BYOD environments where employees have various versions of devices and operating systems. For more information, refer to the Detecting Compromised Devices document available on the AirWatch Resources Portal.

- **Device Last Seen** – Select if the device is non-compliant when the device fails to check in within an allotted time window.

- **Encryption** – Select if the device is non-compliant when Encryption is not enabled.
- **Interactive Profile Expiry** – Select if the device is non-compliant when an installed profile expires within the specified length of time.

- **Last Compromised Scan** – Select if the device is non-compliant when AirWatch is unable to successfully query the device on schedule.

- **MDM Terms of Use Acceptance** – Select if the device is non-compliant when the current MDM Terms of Use have not been accepted by the end user within a specified length of time.

- **Model** – Select if the device is non-compliant based on a specific platform.

- **OS Version** – Select if the device should be marked as non-compliant when it is within a certain window of OS versions that you configure.

- **Passcode** – Select if the device is non-compliant when a passcode is not present.

- **Roaming** – Detect if the device is roaming.

- **SIM Card Change** – Select if the device is non-compliant when the SIM Card has been replaced.

2. Specify **Actions** and **Escalations** that occur. Select the type of action to perform: **Application**, **Command**, **Notify**, **Profile**, or **Email**.

   **Note:** Block Email applies if you are using Mobile Email Management and the Email Compliance Engine, which is accessed by navigating to Email ►Compliance Policies ►Email Policies. This lets you use Device Compliance policies such as blacklisted apps in conjunction with any Email Compliance Engine policies you configure. With this Action selected, email compliance is triggered with a single device policy update if the device falls out of compliance.

   Increase security of actions over time by adding Escalations. Select **Next** when all actions and escalations are added.
3. Configure **Assignment** and **Activate Policy**. Define the devices, Organization Groups and user groups to receive the policy. Enter a policy name, view a snapshot and select **Finish & Activate** to launch the new rule.

**Note:** Query non-compliant iOS 7 devices to decrease the delay between when a user has taken action to make their device compliant and when AirWatch detects that action. Set this sample by navigating to **Groups & Settings ►Settings ►Devices & Users ►Apple ►MDM Sample Schedule** and setting the **Non-Compliant Device Sample**.

You can enforce application compliance as well by establishing a whitelist, blacklist or required list of applications. For more information on establishing a robust and effective Mobile Application Management (MAM) plan, please see the AirWatch MAM Guide.
Apps for iOS Devices

You can use AirWatch applications in addition to AirWatch MDM features to further secure devices and configure them with added functionality.

For more information about deploying public, internal, and purchased applications, please see the comprehensive AirWatch Mobile Application Management Guide.

In This Section

- **Using the AirWatch MDM Agent for iOS** – Learn more about how the AirWatch Agent is used to secure devices and how to configure its settings.
- **Using the AirWatch Browser for iOS** – Learn more about the AirWatch Browser for iOS devices.
- **Using the AirWatch Inbox for iOS** – Learn more about the AirWatch Inbox for iOS devices.
- **Using AirWatch Workspace for iOS** – Learn more about the AirWatch Workspace for iOS devices.
- **Enforcing Application-Level Single Sign On Passcodes** – Learn more about how you can apply a single app-level SSO passcode for end users to access applications without having to authenticate each time.

Using the AirWatch MDM Agent for iOS

**Overview**

The AirWatch Agent is an application installed on managed devices that collects and delivers device information to the AirWatch Admin Console. The information the Agent transmits may contain sensitive data such as GPS coordinates or compromised device status. Therefore, AirWatch takes extensive measures to secure this data and ensure the information is protected and that it originates from a trusted source.

AirWatch utilizes a unique certificate pair – one on the Agent and one on the server – to sign and encrypt all communication between the two endpoints. These certificates add an additional layer of encryption between the Agent and the server and also allow the server to verify the identity and authenticity of each device’s Agent. This overview details the benefits and necessities of both security enhancements.

**The Certificate Exchange**

Before any data is transferred, the Agent and server will trade personalized certificates. This relationship is established on the Agent’s first check-in to the AirWatch server.
1. The Agent reaches out to the AirWatch server to obtain the server’s certificate public key.
2. The Agent validates the server’s certificate against the AirWatch Root CA certificate, which has been hard-coded.
3. The Agent sends a unique certificate public key to the AirWatch server.
4. The AirWatch server associates the Agent’s certificate to that device in the database.

Note: Both the Agent and the AirWatch server trust the public key of the AirWatch Root certificate, which they use to verify the authenticity of all certificates involved in the enrollment exchange.

Securing the Data in Transit

Once the certificates are in place from the initial exchange, all data sent to the AirWatch console will be encrypted. Below is a table showing the two certificates involved and their responsibility in the transaction.

<table>
<thead>
<tr>
<th></th>
<th>Agent Certificate</th>
<th>Server Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirWatch Agent</td>
<td>Sign the Data</td>
<td>Encrypt the Data</td>
</tr>
<tr>
<td>AirWatch Server</td>
<td>Verify the Data Origin</td>
<td>Decrypt the Data</td>
</tr>
</tbody>
</table>

APIs and Functionality

There are two categories of APIs that AirWatch leverages on iOS devices for management and tracking capabilities:

- **Over-the-Air (OTA) MDM APIs** are activated through the enrollment process regardless if an agent is used or not.
- **Native iOS SDK APIs** are available to any third-party application, including the AirWatch MDM Agent and any other application using the AirWatch Software Development Kit (SDK).

The **AirWatch MDM Agent for iOS** refers to the application that enables the **Native iOS SDK API** layer of management that AirWatch hooks into. Primarily, these applications have been developed with AirWatch. With the AirWatch SDK, applications can take advantage of key MDM features that are available above what is offered in the **Over-the-Air (OTA) MDM API** layer, such as:

- Compromised Device Detection
- Additional Telecom Detail
- Additional Network Details such as IP address
- Additional Battery and Memory statistics
Native number badging

APNs Push Messaging

Configuring AirWatch Agent Settings

You can customize the AirWatch Agent from the System Configuration of the AirWatch Admin Console. For example, you can specify an SDK Profile to use with the AirWatch Agent to leverage AirWatch functionality.

1. Navigate to Devices ▶ Settings ▶ Apple ▶ Apple iOS ▶ Agent Settings.

2. Configure the following settings for the AirWatch Agent:

   **General Tab**
   - **Disable Un-Enroll in Agent** – This setting disables the user’s ability to un-enroll from AirWatch MDM via the Agent. This setting is only available in the AirWatch MDM Agent v4.9.2 and higher.
   - **Background App Refresh** – This setting tells the Agent when to refresh app content through the Console. Apps are refreshed based on the Console’s settings and through learned patterns of the app’s use in iOS.
   - **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 ▶ Settings ▶ General ▶ Privacy.
   - **Collect Cellular Data Usage** – This setting enables the AirWatch Agent to collect cellular data usage from devices. Whether or not data is actually collected depends on the privacy settings set in Devices ▶ Settings ▶ General ▶ Privacy.
   - **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.
   - **SDK Profile** – 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. For more information on SDK profiles, refer to the iOS SDK Guide.

   **Notification Tab**
   - **Notification** – These notification settings ensure the AirWatch Agent can send push notifications.

Configuring AirWatch Agent via Settings and Policies

Customize the following additional configurations for the AirWatch Agent from the Settings and Policies page in the AirWatch Admin Console:

   - **Single Sign On**
   - **Offline Access**
   - **Branding**

**Note:** For more information about Settings and Policies, please refer to the AirWatch Mobile Application Management Guide.
Using the AirWatch Agent

Once you have enrolled and configured the AirWatch Agent for your device, you can view snapshot information about your enrollment. For example, if you install an application your organization has blacklisted, you may receive a compliance message that can be viewed from the Agent's Message Center. In addition, you can view the real-time status of your compliance, user account, and connectivity to ensure your device is operating as expected. Through the AirWatch Admin Console you can also send APNs messages to the Agent and use the Find Device feature to make the Agent play an audible tone, which can be used to physically locate the device if it is nearby.

My Device

When you first launch the AirWatch Agent, the application defaults to the My Device tab. This tab provides a centralized resource for viewing useful information about your device.

The Status section lists various statuses for device enrollment, compliance, and connectivity. Tap the Status box to view various self-service diagnostic options, such as:

- View overall compliance status (if Self Service Enabled is checked in the AirWatch Admin Console under Agent Settings).
- View current device status.
  - Select Re-Enroll Device to restart the enrollment process. If you are using the AirWatch MDM Agent v4.9.2 or higher, select Un-Enroll Device (if the Disable Un-enroll Agent option is not checked in the AirWatch Admin Console under Agent Settings) to un-enroll your device.
- View connectivity status for Internet, APNs and the AirWatch Server.

The Device Details section lets users view additional device information, such as:

- Location to view GPS coordinates for your device for the current and previous time periods.
- Network to view Cellular and Wi-Fi information in addition to any additional network interfaces.
- Advanced to see battery life, free memory and free disk space.

Messages

The Messages tab displays notifications from the AirWatch Admin Console. For example, you may receive notifications in the message center to complete a required compliance check to ensure your device can be successfully monitored.

About

The About tab displays App Version and Privacy Policy information about the Agent.

Offline Access

The following step-by-step instructions explain how to configure this profile as part of the default settings that apply to all applications. For more information about default versus custom profiles, refer to the "Default or Custom Settings for Profiles" section of the AirWatch Mobile Application Management Guide.

Configuring Offline Access

Select Offline Access to allow access using the SSO identity to applications when the device is offline.

2. Select Enabled and then choose an acceptable time frame for offline access before the device requires re-authentication to the network and applications in the Maximum Period Allowed Offline field.
Devices should return online periodically so the system can check device compliance and security status.

3. **Save** your settings.

**Branding**

The following step-by-step instructions explain how to configure this profile as part of the default settings that apply to all applications. For more information about default versus custom profiles, refer to the "Default or Custom Settings for Profiles" section of the *AirWatch Mobile Application Management Guide*.

**Configuring Branding**

Change the look and feel of applications to reflect your company's unique brand by configuring images and colors through the use of *Branding* settings.

1. Navigate to **Groups & Settings ▶ All Settings ▶ Apps ▶ Settings and Policies ▶ Settings**.
2. Select **Enabled** for **Branding** and then complete the following options:
   - Reflect your company colors by choosing the **Toolbar**, **Toolbar Text**, **Primary**, **Primary Text**, **Secondary**, and **Secondary Text** colors from a color palette.
   - Enter in your **Organization Name**.
   - Upload a custom **Background Image**.
   - Rebrand the following iOS devices: **iPhone**, **iPhone (Retina)**, **iPhone 5 (Retina)**, **iPad**, and **iPad (Retina)**.
   - Rebrand Android devices by uploading the following sizes: **Small**, **Medium**, **Large**, and **Extra Large**.
   - Upload a **Company Logo** for your **Phone**, or **Tablet** in regular or **High Resolution**.
3. **Save** your settings.

**Using the AirWatch Browser for iOS**

The AirWatch Browser is a safe, accessible and manageable Internet browser for your devices. You can customize and configure the AirWatch Browser to meet unique business and end user needs, restrict web access to certain websites, provide a secure Internet portal for devices used as a mobile point-of-sale, and more. Provide users with a standard browsing experience, including support of multi-tabbed browsing and Javascript pop-ups. For maximum security on your Android and iOS devices, AirWatch recommends deploying the AirWatch browser in conjunction with a Restrictions profile blocking the native browser.

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

**Using the AirWatch Inbox for iOS**

AirWatch Inbox is a fully containerized email management solution for iOS and Android devices. The AirWatch Inbox enables administrators to remotely configure and manage enterprise email accounts while keeping personal and enterprise data separate for end users. The application features support for Exchange ActiveSync and offers encryption for email messages and attachments. Some of its data loss prevention features include:
- Setting a passcode to access the application.
- Configuring restrictions such as disable copy/paste.
- Removing email messages and attachments upon an enterprise wipe.

For more information on AirWatch Inbox, please see the AirWatch Inbox Guide.

Using AirWatch Workspace for iOS

AirWatch Workspace offers a flexible new approach to BYOD through management by “containerization” within the device. The Workspace creates a virtual container where all corporate applications (AirWatch and internal) may be visible inside and outside the Workspace view but are secure through a shared container passcode. Productivity tools are granted to end users as apps in the container and can be managed by the administrator at the app-level rather than the device level.

Each app maintains security controls built in to prevent data leakage outside of the app. These apps include AirWatch Inbox, AirWatch Browser web app shortcuts on intranet sites that require connectivity. Multiple apps interact seamlessly via Single Sign On to avoid multiple authentication prompts, and an app-level intranet tunnel connects to any required backend services.

- **“Dual-Persona” separation between work and play** – Separates from a privacy perspective and does not allow AirWatch visibility into personal apps or the ability to wipe any personal items.
- **Passcode/Encryption enforced only within Workspace** – Sets complex passcodes that do not intrude on personal life; encryption is only enforced locally within the applications.
- **No MDM Required** – Avoids OS prompts.

All devices — whether MDM- or Workspace-enrolled — can be managed from a single pane of glass with hybrid deployments.

For more information about the AirWatch Workspace, please refer to the AirWatch Workspace Guide.

Enforcing Application-Level Single Sign On Passcodes

AirWatch’s single sign on (SSO) feature allows end users to access all AirWatch apps, wrapped apps, and SDK-enabled apps with a single SSO Passcode without having to enter login credentials for each application. Using either the AirWatch MDM Agent or the AirWatch Workspace as a "broker application", end users can authenticate once using either their normal credentials or an SSO Passcode and then gain access to other applications so long as the SSO session is active.

Enabling Single Sign On

Enable SSO as part of the Security Policies that you configure to apply to all AirWatch appsTo enable SSO:

2. Set Single Sign On to Enabled to allow end users to access all AirWatch applications and maintain a persistent login.
3. Optionally set Passcode Mode to either Numeric or Alphanumeric to require an SSO Passcode on the device. If you enable SSO but do not enable a Passcode Mode, end users will use their normal credentials (either directory service or AirWatch account) to authenticate, and an SSO Passcode will not exist.
**Apps / Settings And Policies / Security Policies**

![Settings and Policies](image)

**SSO Session**

Once an end user authenticates with either the Workspace or the Agent, an SSO session is opened. It lasts so long as the Workspace is running in the background or until the **Passcode Timeout** value defined in the **Passcode Mode** settings is exceeded. With an active session, end users can access managed applications without having to enter their SSO Passcode.

---

**Note:** Wrapped apps must have a passcode, either numeric or alphanumerical. Without this passcode, wrapped apps do not display true SSO functionality.
Apple Configurator

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

AirWatch integrates with Apple Configurator to enable you to efficiently 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.

With Configurator, you can:

- Supervise dedicated line of business devices that are shared among different users.
- Configure supervised devices in the Prepare process with an identical configuration.
- Install the AirWatch MDM profile as part of the configuration to silently enroll devices.
- Re-configure supervised devices after each use by reconnecting them to Configurator.
- Distribute public apps without entering an Apple ID on the device using Configurator.
- Assign a supervised device to a designated user in your organization for corporate use.
- Configure and update corporate device settings and apps over-the-air in AirWatch.
- Back up user settings and app data, including new user-created data using Configurator.

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

Upload a Signed Profile to the AirWatch Admin Console

You can export a signed profile from Apple Configurator (or IPCU) directly to the AirWatch Admin 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 ➤List View within the AirWatch Admin Console and select Upload.
4. Enter the **Managed By** group and click **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 Group(s).

6. Click **Save & Publish** to send the profile down to assigned devices.
Shared Devices

Overview

Issuing a device to every employee in your organization can be expensive. With AirWatch MDM, you can share mobile devices among end users using either a single fixed configuration for all end users or a unique configuration setting for each individual end user. AirWatch’s Shared Device/Multi-User Device functionality ensures security and authentication are in place for every unique end user, and if applicable, allows only specific end users to access sensitive information.

When administering shared devices, you must first provision devices with applicable settings and restrictions before deploying them to end users. Once deployed, AirWatch utilizes a simple Login/Logout process for shared devices in which end users simply enter their directory services or dedicated credentials to log in. The end user's role determines their level of access to corporate resources, including content, features, and applications. This ensures the automatic configuration of features and resources that are available after the user logs in. The Login/Logout functions are self-contained within the AirWatch Agent, so the device's enrollment status is never affected, and the device can be managed in the AirWatch Admin Console whether it is in use or not.

System Capabilities

Functionality

- Configure a single managed device which can be used by multiple end users.
- Personalize each end user’s experience without losing corporate-wide settings.
- Configure corporate access, apps, files, and device privileges based on user or Organization Group.
- Allow for a seamless login/logout process that is self-contained in the AirWatch Agent.

Security

- Provision devices with the shared device settings before providing devices to end users.
- Login and Logout devices without affecting device enrollment in AirWatch.
- Authenticate end users during device login with directory services or dedicated AirWatch credentials.
- Manage devices even when a device is not logged in.

Supported Platforms

Android 2.3+ and iOS devices with AirWatch MDM Agent v4.2+ support shared device/multi-user device functionality.
In This Section

This document discusses the detailed setup and configuration of Shared Device mode. It is divided into the following sections:

- Organizing Shared Devices – Talks about how and where to create organization hierarchy to organize devices in the AirWatch Admin Console.
- Configuring Shared Devices – Details the multiple ways to configure shared device functionality on to the devices.
- Using Shared Devices – Explains how to use shared device functionality on the device.

Organizing Shared Devices

The easiest way to manage your mobile fleet is to organize the devices you administer based on your corporate hierarchy and geographic location, if applicable. Because employee permissions, device restrictions and corporate access are often based on defined roles within the hierarchy, it is both logical and beneficial for you to mirror this structure when organizing groups within the AirWatch Admin Console for the first time.

Defining the Device Hierarchy

In most cases, when you first log in to the AirWatch Admin Console, you will see a single Organization Group that has been created for you with the name of your organization. This group serves as your top-level Organization Group, and you will create subgroups underneath it to build out your company's hierarchical structure.

To define the device hierarchy:

1. Navigate to Groups & Settings ➤Groups ➤Organization Groups ➤Organization Group Details. Here, you can see an Organization Group representing your company.

2. Ensure the Organization Group Details displayed are accurate and then use the available data entry fields and drop-down menus to make any modifications, if necessary. If you make changes, click Save.


4. Enter the following information for the first Organization Group to reside within the top-level Organization Group:
   - **Organization Group Name** - Enter a name for the child Organization Group to be displayed within the AirWatch Admin Console.
   - **Group ID** - Enter an identifier for the Organization Group for the end users to use for device to log in.

   *Note: Ensure the end users who share devices receive the Group ID as it may be required for device to log in depending on your Shared Device configuration.*

   - **Organization Group Type** - Select the preconfigured Organization Group Type that reflects the category for the child Organization Group.
   - **Country** - Select the country where the Organization Group is based.
   - **Locale** - Select the language classification for selected country.
5. Create additional groups and subgroups in the same manner as needed to build out your corporate hierarchical structure. If configuring a **Fixed Organization Group**, then ensure you have created the single Organization Group for end user to log in or log out. If you configure **Prompt Users for Organization Group**, then ensure you have created the multiple Organization Groups that are required for your various end-user log in or log out roles. For more information, see Configuring Shared Devices.

6. Select **Save**.

**Configuring Shared Devices**

You can utilize Shared Device functionality by navigating to **Groups & Settings ► All Settings ► Devices & Users ► General ► Shared Device**. Configure devices in one of three ways:

- **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, for example, 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, the settings, applications, and content to which they have access are based on their specific role within the hierarchy. For example, if an end user is a member of the 'Sales' User Group, which is mapped to the 'Standard Access' Organization Group, then when that end user logs in to the device, the device will be configured with the settings, applications and content available to the 'Standard Access' Organization Group. Consider an other example, hospitals can utilize this method by configuring different device profiles for different employees. A doctor can log in to a device and have access to certain applications and information related to a patient’s personal information, treatment, and diagnosis. A nurse can log in to the same device and have access to an entirely different set of resources applicable to their role.

- **Select Prompt User for Organization Group** to have the end user enter a Group ID for an Organization Group each time they log in to a device.

  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.
Configuring Shared Device Settings

1. Navigate to **Groups & Settings ➤ All Settings ➤ Devices & Users ➤ General ➤ Shared Device**.

2. Select the **Override** radio button.

3. Select any one of the following applicable radio button to enable the **Group Assignment Mode** that meets your shared device requirements:
   - **Prompt User for Organization Group** – Select to prompt the end user to enter a valid Group ID and credentials to log in to a device, thereby allowing the device to leverage the settings, applications, and content of a particular Organization Group.
   - **Fixed Organization Group** – Select to restrict the end user to a particular Organization Group when they log in to a device. A Group ID is not required, but an end user may be prompted to enter credentials to log in to a device.
   - **User Group Organization Group** – Select to use the User Group-to-Organization Group mapping configured in the AirWatch Admin Console to determine access to settings, applications, and content.
   - **Always Prompt Terms of Use** – Select this checkbox to prompt the end user to accept **Terms of Use** agreement before logging in to a device.

4. Select the **Auto Logout Enabled** check box to configure automatic logout after a specific time period.

5. Select the **Enable Single App Mode** check box to configure Single App Mode, which locks the device into a single application when an end user logs into the device.

   **Note:** Single App Mode applies only to Supervised iOS devices.

6. Click **Save**.
Enabling Multi-User Device Staging

Similar to single-user device staging, multi-user device/shared device staging allows an IT administrator to provision devices intended to be used by more than one user. However, multi-user devices require configuration of the device to accept any allowed users to sign-in and use the device as necessary.

1. Navigate to Accounts ►Users ►List View and select Edit for the user account for which you want to enable device staging.
2. Select Enable Device Staging and then select the staging settings that will apply to this staging user.
   - Multi User Devices – Stages devices for use by multiple users.
3. Open a device's Internet browser, navigate to the enrollment URL and enter the proper Group ID.
4. Complete enrollment and install the Mobile Device Management (MDM) profile by following the prompts. Once you are done, the Login/Logout screen displays and prompts any users of the device to check out the device to access the applications, settings and content for their Organization Group, which is assigned based on the Group Assignment Mode settings you specify under Devices ►Settings ►Devices & Users ►General ►Shared Device.

The device is now staged and ready for use by the new users.

Using Shared Devices

Logging in a device automatically configures it with the specific settings, applications, and content based on the end-user's role. After the end user is done using the device and logging out of the device, the configuration settings of that session are wiped and the device is ready for login by another end user.
Logging In and Logging Out Devices

Login to a device:
1. Launch the AirWatch Agent on the device.
2. Enter your credentials. If the device is logged into the Agent, then you will be prompted to enter your SSO Passcode. If not, then you will be prompted to enter a username and password.

   **Note:** end users are required to enter a Group ID to log in to a device if Prompt User for Organization Group is enabled on the console. See Configuring and Enabling Shared Devices for more information.

3. Select Login and accept the Terms of Use.

Log out of a device:
1. Navigate to My Device.
2. Select Log out and then Yes, when prompted.

   **Note:** When the shared device is logged out, both the device’s passcode and Single Sign On passcode are cleared without any warning or notification. Thus, allowing the next user to configure another passcode.
Mobile Kiosks

Overview

AirWatch offers you the ability to utilize devices in your mobile fleet as kiosks. Mobile kiosks limit your employees to single website browsing, as well as to specify the applications allowed for use. Devices can act as electronic kiosks at different layers of mobile architecture based on your resources and needs:

- **Web Kiosks** restrict browsing to a specific website or web application and automatically revert to the configured home page after certain period of inactivity.
  - Enable browsing through AirWatch Browser app.
  - Remove all navigation.
  - Define cookies policy.
  - Assign a single homepage URL and force return to homepage at specified inactivity period.
  - Available for iOS and Android devices.

  **Note:** For more information about configuring a web kiosk, see the AirWatch Browser Guide.

- **Mobile Application Kiosks** restrict device usage to a single or multiple mobile application which prevents tampering of system functions and unauthorized use.
  - In-app lock down as an electronic kiosk.
  - Device remains only within one specific app.
  - Prevent use of home button from exiting app.
  - Supported on iOS devices.

  **Note:** For more information, see Configuring Single App Mode.

You can implement mobile kiosks in several ways. For example, an educational institution can deploy devices as web kiosks for use by students who need the ability to research a particular web resource, but should not be allowed to browse elsewhere. In the case of application kiosks, a transportation company can deploy iOS devices as application kiosks restricted to an internal app used by employees for specialized tasks like scheduling, booking and logistics. Finally, a retail establishment can deploy devices in device kiosk mode for use in store, utilizing corporate applications for in-store functionality like querying inventory and checking product pricing as well as custom branding to enhance the kiosk functionality.
Supported Devices

Kiosk mode availability differs based on the device platform and operating system version:

- Android and iOS devices support web kiosk functionality using the AirWatch Browser.
- Apple iOS 6+ devices support mobile application kiosks.

**Note:** Apple Configurator is required to place target iOS devices in Supervised mode, which is needed to deploy the Single App Mode payload used for application kiosks.
Managing Devices

Overview

You can manage all of your deployment’s devices from the AirWatch Dashboard. The Dashboard is a searchable, customizable view you can use to filter and find specific devices based on various criteria. This simplifies performing actions and administrative functions on a particular set of devices. In addition, you can set up the Self-Service Portal (SSP) to empower end users to manage their own devices and reduce the strain on Help Desk personnel.

In This Section

- Using the Device Dashboard — Explains how administrators can locate and manage iOS devices in the AirWatch Admin Console.
- Using the Device List View — Details how to use the Devices List View to search for, filter, and perform remote actions on multiple iOS devices.
- Using the Device Details Page — Walks through the ways you can manage iOS devices from using the Device Details Page in the AirWatch Admin Console.
- Utilizing Reports — Presents reports and collected data within the AirWatch Admin Console featuring detailed information on all aspects of your deployment.
- Using the Hub — Presents the data flow within AirWatch Hub and how to use the data within.
- Using the Self-Service Portal — Explains how users can manage their iOS devices from the Self-Service Portal.
- Controlling iOS 7+ Devices with Activation Lock — Covers the Activation Lock feature that is available to devices running iOS 7 and higher and how to clear the lock.
- Configuring Managed Settings for iOS Devices — Gives more information on additional iOS configuration options.
- Installing Fonts on iOS Devices — Details how to upload and install your own fonts on iOS devices.
Using the Device Dashboard

As devices are enrolled, view and manage them from the AirWatch Device Dashboard. The Device Dashboard provides a high-level view of your entire fleet of mobile devices while allowing a quick and easy way to drill down to individual devices and take MDM actions. View graphical representations of relevant statistics, including important device information for your fleet, such as device ownership type, compliance statistics and platform breakdown.

Select any of the available data views from the Device Dashboard to quickly access each set of devices in the List View. From this List View, take administrative action, including send a message, lock devices, delete devices and change groups associated with the device.

Security

View security-related information related to your entire deployment, such as:

- **Compromised** – The number and percentage of compromised devices (i.e. jailbroken, rooted, etc.) in your deployment.
- **No Passcode** – The number and percentage of devices without a passcode configured for security.
- **No Encryption** – The number and percentage of devices that are not encrypted for security.

If supported by the platform, you can configure a compliance policy to take action on these devices.

Ownership
View the total number of devices in each ownership category.

**Last Seen Overview**

View the number and percentage of devices that have recently communicated with the AirWatch MDM server. For example, if several hundred devices have not been seen in over 30 days, you can select the corresponding bar graph to pull of a List View of those devices, add additional filters if needed (e.g. Corporate Dedicated), and follow-up with the employees accordingly.

**Platforms**

View the total number of devices in each device platform category.

**Enrollment**

View the total number of devices in each enrollment category.

---

**Using the Device List View**

Switch to List View (Devices ▶ List View) at any time to sort and manage devices by filtering the columns and fields available in the Device Dashboard, including:

- Last Seen
- Friendly Name
- Ownership
  - Corporate - Dedicated
  - Corporate - Shared
  - Employee-Owned
- Username
- Display Name
- Platform/OS/Model
- Organization Group
- Compliance Status

Select on a device Friendly Name at any time to open up the device details page for that device.

Sort columns and configure information filters to gain insight on device activity based on specific information you are curious about. For example, sort the Compliance Status column to view only devices that are currently out-of-compliance and take action or message only those specific devices. Search all devices for a friendly name or user’s name to isolate one device or user. Once you have sorted or filtered dashboard information, export, save and send the data for review.
Using the Search List, Filters, and Bulk Messaging

At times, you will need to search for a single device for quick access to its information and take remote action on the device. For example, search for a specific device, platform or user. Navigate to Devices ▶ List View ▶ Search List and search for all devices within the current Organization Group and all child groups.

You can also drill down to specific sets of devices by filtering device criteria, including by Platform, Ownership Type, Passcode, Last Seen, Enrollment, Encryption and Compromised status.

You can also search specific information across all fields associated with devices and users, allowing you to search user name ("John Doe") or device type.

Once you have applied a filter to show a specific set of devices, perform bulk actions to multiple, selected devices by clicking the check box for those devices and selecting an action from the Management tabs.

You can also select Send Message to All to send a message to all devices according to your current filters.

For example, if no filters are set, you will send a message to every device; but if you have filters set for Android Compromised devices, then you will only send a message to those devices.

This action is only available if enabled in the system settings (Groups & Settings ▶ All Settings ▶ System ▶ Security ▶ Restricted Actions) and requires a PIN to perform.

Using the Management Tabs

With the categorized devices displayed, take bulk action on specific devices by selecting the check box next to each device and using the top Control Panel to:

**Note:** The actions listed below will vary depending on factors such as device platform, AirWatch Admin Console settings, and enrollment status.
With the categorized devices displayed, take bulk action on specific devices by selecting the check box next to each device and using the top Control Panel to:

**Query** – Query all selected devices for current device info, including last seen, OS, model and compliance status.

**Send** – Access Send Message menu and compose message to send to selected devices.

**Lock** – Lock all selected devices and force users to re-enter device security PIN.

**More** – View commands that you can perform on all selected devices. For example:
- **Management** – Query, lock or perform Enterprise Wipe on all selected devices.
- **Support** – Send a message to a device with instructions or communication to end user. Locate current GPS location of all selected devices.
- **Admin** – Change AirWatch Admin Console settings, including changing Organization Group, Ownership type or device group of selected devices or deleting devices from AirWatch MDM.
- **Advanced** – Perform a warm boot on devices to remotely reboot those devices. Select Provision Now to perform a number of configuration for selected devices. Select Install Product to install a particular apps to selected devices.

You can perform additional remote actions to individual devices from the Device Details page.

### Using the Device Details Page

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 AirWatch Admin Console.
**Viewing Device Information**

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

- **Summary** – View general statistics such as enrollment status, compliance, last seen, platform/model/OS, Organization Group, contact information, serial number, power status, storage capacity, physical memory and virtual memory.

- **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 all apps currently installed or pending installation on the device.

- **Location** – View current location or location history of a device.

- **User** – Access details about the user of a device as well as the status of the other devices enrolled to this user.

The menu tabs below are accessed by clicking **More** from the main Device Details tab.

- **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 type s of restrictions that currently apply to the device.
• **Notes** – View and add notes regarding the device. For example, note the shipping status or if the device is in repair and out of commission.

• **Certificates** – Identify device certificates by name and issuant. This tab also provides information about certificate expiration.

• **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.

• **Shared Device Log** – View history of device in terms of Shared Device, including past check-ins and check-outs and current status.

• **Event Log** – View history of device in relation to MDM, including instances of debug, information and server check-ins.

• **Status History** – View history of device in relation to enrollment status.

• **Device Registration** – View all restrictions currently applied to a device. This tab also shows specific restrictions by Device, Apps, Ratings and Passcode.

• **Targeted Logging** – Enable and view logging for this device.

## Performing Remote Actions

The **More 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.

<table>
<thead>
<tr>
<th>Query</th>
<th>Clear Passcode</th>
<th>Management</th>
<th>Support</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query All</td>
<td>Device</td>
<td>Lock Device</td>
<td>Send Message</td>
<td>Change Org Group</td>
</tr>
<tr>
<td>Device Information</td>
<td>SSO</td>
<td>Lock SSO</td>
<td>Find Device</td>
<td>Edit Device</td>
</tr>
<tr>
<td>AirWatch MDM Agent</td>
<td></td>
<td>Enterprise Wipe</td>
<td>Remote View</td>
<td>Delete Device</td>
</tr>
<tr>
<td>Security</td>
<td>Profiles</td>
<td>Managed Settings</td>
<td>Request Device Check In</td>
<td></td>
</tr>
<tr>
<td>Apps</td>
<td>Certificates</td>
<td>Device Wipe</td>
<td>Sync Device</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The actions listed below will vary depending on factors such as device platform, AirWatch Admin Console settings, and enrollment status.

• **Query** – Query the device for all information or only specific information.

• **Clear Passcode** – Clear either the device-level passcode or the SSO Passcode.

• **Management** – Lock the device or SSO session or perform an enterprise or device wipe.

  **Note:** 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 for **unsupervised** devices, 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 [Controlling iOS 7+ Devices with Activation Lock](#).

• **Support** – Perform support actions such as sending the device a message, sending a message, finding the device by playing an audible tone, or syncing the device.
• **Admin** – Change AirWatch Admin Console settings, including changing Organization Group, and editing/deleting devices from AirWatch MDM.

**Utilizing Reports**

AirWatch has extensive reporting capabilities that provide administrators with actionable, result-driven statistics about their device fleets. IT administrators can leverage these pre-defined reports or create custom reports based on specific devices, User Groups, date ranges or file preferences.

In addition, the administrator can schedule any of these reports for automated distribution to a group of users and recipients on either a defined schedule or a recurring basis. For example, you can run reports to see the number of compromised devices, how many devices there are for a specific make or model, or the total amount of devices running a particular version of an operating system.

**Using the Hub**

Utilize the AirWatch Hub as your central portal for fast access to critical information. Quickly identify important issues or devices and take action from a single location in the AirWatch Admin Console. Select any metric to open the **Device List View** for that specific set of devices, where you can perform actions such as sending a message to those devices.

For more information about using the Hub to filter and view specific information, refer to the Managing Devices section of the [AirWatch Mobile Device Management Guide](#).
Using the Self-Service Portal (SSP)

The AirWatch Self-Service Portal (SSP) allows end users to remotely monitor and manage their smart devices. The Self-Service Portal lets you view relevant device information for enrolled devices and perform remote actions such as clear passcode, lock device, or device wipe.

Accessing the Self-Service Portal on Devices

Your end users will always be able to access the Self-Service Portal from their workstations or devices by navigating to https://<AirWatchEnvironment>/MyDevice. However, in many cases it is helpful to deploy SSP access as a Web Clip to managed devices. This gives your users the ability to easily monitor and track their device status within AirWatch without worrying about a URL. Giving end users the ability to perform such actions can simplify the administrative experience by reducing end-user support requests.

Deploying an SSP Web Clip is optional and allows users to access the SSP from their devices in addition to their computer's web browser. To deploy an SSP Web Clip, use the following instructions:

1. Navigate to Devices ►Profiles ►List View ►Add and select Apple iOS from the platform list.
2. Enter General information as necessary.
3. Select Web Clips from the payload list. Enter the following information:
   - **Label** – The text displayed beneath the Web Clip icon on an end-user's device. For example: "AirWatch Self-Service Portal."
   - **URL** – The URL the Web Clip will display.
     - For the SSP, use the following URL: https://<AirWatchEnvironment>/mydevice/.
   - **Removable** – The option to allow end users to remove the SSP Web Clip.
   - **Icon** – The custom icon, in .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 in size when uncompressed. The graphic will be automatically scaled and cropped to fit, if necessary and converted to png format. Web clip icons are 104 x 104 pixels for devices with a Retina display or 57 x 57 pixels for all other devices.

- **Full Screen** – The option to launch the SSP webpage in full screen mode.
- **Show As Web App In App Catalog** – The option to list the SSP as an application in your Enterprise App Catalog. You might use this setting if you do set the profile to deploy automatically.

4. Click **Save and Publish** when you are done to immediately send the profile to all appropriate devices.

**Note:** Access to information and Remote Actions in the Self-Service Portal is determined by both Privacy settings (Devices ▶ Settings ▶ General ▶ Privacy) and Role settings (Administrators ▶ Roles). If multiple settings are in place, the strictest policy is enforced.

### Using the SSP

#### Logging into the SSP

You can access the SSP in two possible ways:

- Log in through a browser and manage your devices remotely. To do this, navigate to the SSP website using the URL provided to you. It should look similar to this format: https://mdm.acme.com/mydevice.
- Access the SSP from your device by opening the SSP Web Clip, if one has been pushed to your device.

Once you launch the SSP, you can log in using the same credentials (**Group ID**, **username** and **password**) you used to enroll in AirWatch. Optionally, if Email Domain registration is configured, you can log in using your corporate email address.

#### Selecting a Device in the SSP

After logging in to the SSP, a list of all devices tied to your user account displays on the left. Select the device you want to manage. The **Device Details** screen displays.

#### Viewing Device Information

The following tabs display device-related information:

- **Security** – This tab displays the information specific to security controls currently in place for the device, including: enrollment status, assigned profile status, installed certificate status, certificates nearing expiry and installed applications.
- **Compliance** – This tab shows the compliance status of the device, including the name and level of all compliance policies that apply to the device. It is important for end users to take note of these policies to ensure devices remain compliant and operate as intended.
- **Profiles** – This tab shows all of the MDM profiles that have been sent to the devices enrolled under your user account and the status of each profile. From the Profiles view, you can select the install icon (➕) to install a profile or the delete icon (➖) to remove it from the device.
- **Apps** – This tab displays all applications that have been installed on the selected device and provides basic application information.
• **Certificates** – This tab displays a detailed listing of certificates currently assigned to and installed on the device. From the Certificates view, you can deactivate, renew or remove a certificate, if allowed.

• **Location** – This tab displays the coordinates of the selected device, if enabled.

• **Event Log** – This tab contains a comprehensive log of all interactions between the AirWatch Admin Console and the device.

• **Support** – This tab contains detailed device information and contact information for your organization’s support representatives.

### Perform Remote Actions

The **Remote Actions** enable you to perform remote actions over-the-air to the selected device. See below for detailed information about each remote action.

**Note:** All remote action permissions are determined by your administrator and therefore you may not be able to perform all listed actions.

• **Device Query** – Manually requests the device to send a comprehensive set of MDM information to the AirWatch Server.

• **Clear Passcode** – Clears the passcode on the selected device and will prompt for a new passcode. This is useful if you forget your device passcode and are locked out of your device.

• **Send Message** – Sends an Email, SMS (text) or Push Notification over-the-air to the selected device.

• **Lock Device** – Locks the selected device so that an unauthorized user cannot access it. This feature is useful if the device is lost or stolen (In this case, you may also want to use the GPS feature to locate the device.)

• **Enterprise Wipe** – Wipes all corporate data from the selected device and removes the device from AirWatch MDM. All of the enterprise data contained on the device is removed, including MDM profiles, policies and internal applications. The device will return to the state it was in prior to the installation of AirWatch MDM.

• **Device Wipe** – Wipes all data from the selected device, including all data, email, profiles and MDM capabilities and returns the device to factory default settings.

  **Note:** 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 for **unsupervised** devices, 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 Controlling iOS 7+ Devices with Activation Lock.

• **Find My Device** – Display a message along with an optional sound chime.

• **Set Roaming** – Enable or disable roaming settings.

• **Sync Device** – Sync the device with the AirWatch Admin Console.

### Controlling iOS 7+ Devices with Activation Lock

Activation Lock is a security feature for devices running iOS 7 and higher that leverages Apple's Find my iPhone functionality. Using this feature makes it difficult for anyone to use a lost or stolen device. This is because an end-user's Apple ID and password are required to unlock a device that has Activation Lock enabled, even if the device is wiped or factory reset, including through DFU mode. For more information about Activation Lock as an iOS feature, see Apple's [knowledge base article](#).
Unsupervised vs. Supervised

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:

<table>
<thead>
<tr>
<th>Unsupervised</th>
<th>Supervised</th>
</tr>
</thead>
<tbody>
<tr>
<td>• View if Activation Lock is enabled on a particular device.</td>
<td>• Enable an Activation Lock setting to enforce Activation Lock</td>
</tr>
<tr>
<td>• Accept a warning when performing a device wipe command, notifying you that a device with Activation Lock enabled cannot be reactivated without the original Apple ID and password.*</td>
<td>• View if Activation Lock is enabled on a particular device.</td>
</tr>
<tr>
<td></td>
<td>• Clear the Activation Lock using one of three methods, detailed below.</td>
</tr>
</tbody>
</table>

*See this [Apple knowledge base article](https://support.apple.com) for instructions on how to remove a device from a previous owner’s Apple ID so you can re-activate it for use.

Enabling Activation Lock

For supervised devices running iOS 7 and higher, you can force Activation Lock to be enabled. To do this:

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

**Devices & Users / Apple / Apple iOS / Managed Settings**

![DEFAULT MANAGED SETTINGS](image)

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 do this:
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.

![Device Security Screen]

**Clearing Activation Lock**

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

- **Using the Clear Activation Lock command.**
- **Entering an Activation Lock Bypass Code** directly onto the device.
- **Performing a Device Wipe command** and selecting an option to clear the Activation Lock.

**Using 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 could be useful if you know the whereabouts of the device and do not wish to completely wipe its contents to clear the lock. This command also works even if the device is unenrolled from AirWatch MDM. To use the command:

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**.

![Remote Command Menu]

5. Select **Deactivate**.
Entering an Activation Lock Bypass Code
Entering an Activation Lock Bypass Code can be useful if the device has been unenrolled from AirWatch 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.

Re-activate the device once factory wiped via 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 field empty.

Performing a Device Wipe
When performing a device wipe command you also have the option clearing the Activation Lock on a device. To do this:

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.
5. Select Clear Activation Lock. Enter your Security PIN, and the device will be wiped.
Configuring Managed Settings for iOS Devices

The Managed Settings page in the AirWatch Admin Console lets you configure a few additional settings related to the AirWatch Agent and managing iOS devices.

Configuring Managing Settings

Set the roaming and Hotspot settings for devices in your Organization Groups by managing the Default Cellular Settings in the AirWatch Admin Console. To set these default settings:

1. Navigate to Devices ►Settings ►Devices & Users ►Apple ►Apple iOS ►Managed Settings ►Default Managed Settings.

2. Configure which devices the settings will 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)
Overriding Default Roaming Settings (iOS)

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 and click 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.

**Note:** Modifying iOS settings to manage roaming status does not apply a permanent restriction. End users are able to make changes to these settings manually if needed in the event of an emergency, for example.
Setting 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 ►Settings ►Devices & Users ►Apple ►Apple iOS ►Managed Settings. Scroll down to the Default Wallpaper section.
2. Upload a Lock Screen Image and/or Home Screen Image.
3. Select Save.

Setting Default Organization Information

To set up custom organization information for MDM prompts for iOS 7+ devices:

1. Navigate to Devices ►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.

Installing Fonts on iOS Devices

Specifically available to devices running iOS 7 and higher, the AirWatch Admin 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. To install and deploy fonts:

1. Navigate to Devices ►Settings ►Apple ►Apple iOS ►Install Fonts.
2. Click Add Font and click Upload to browse your computer for the font file. Allowed file types include .ttf or .otf.
3. Locate the font file and select Save to send the font to all iOS devices enrolled in the current Organization Group.

There is no limit to the amount of fonts you’re able to install on iOS devices and you can remove a font at any time by selecting the remove button.
## Appendix A – iOS Functionality: Supervised vs. Unsupervised

The following table shows all of the available iOS profile functionality that you can control via the AirWatch Admin Console. It is organized by whether a supervised iOS device is required to configure a particular setting or feature. Also included are OS Notes that indicate the minimum iOS version that applies.

<table>
<thead>
<tr>
<th>Features and Functionality</th>
<th>Does Not Require Supervision</th>
<th>Requires Supervision</th>
<th>OS Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Passcode</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passcode settings</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Restrictions</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Device Functionality</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow use of camera</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow FaceTime</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow screen capture</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow Fingerprint for Unlock</td>
<td>✓</td>
<td></td>
<td>iOS 7 + iPhone 5s</td>
</tr>
<tr>
<td>Allow use of iMessage</td>
<td></td>
<td>✓</td>
<td>iOS 6 + Supervised</td>
</tr>
<tr>
<td>Allow installing public apps</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow app removal</td>
<td></td>
<td>✓</td>
<td>iOS 6 + Supervised</td>
</tr>
<tr>
<td>Allow in-app purchase</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Allow opening managed app documents in unmanaged apps</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
<tr>
<td>Allow opening unmanaged app documents in managed apps</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
<tr>
<td>Features and Functionality</td>
<td>Does Not Require Supervision</td>
<td>Requires Supervision</td>
<td>OS Notes</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------</td>
<td>----------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Limit ad tracking</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
<tr>
<td>Allow automatic sync while roaming</td>
<td>✓</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Allow voice dialing</td>
<td>✓</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Allow Siri</td>
<td>✓</td>
<td></td>
<td>iOS 5</td>
</tr>
<tr>
<td>Allow Siri while device locked</td>
<td>✓</td>
<td></td>
<td>iOS 5.1</td>
</tr>
<tr>
<td>Enable Siri Profanity Filter</td>
<td></td>
<td>✓</td>
<td>iOS 6 +Supervised</td>
</tr>
<tr>
<td>Allow Passbook while device locked</td>
<td>✓</td>
<td></td>
<td>iOS 6</td>
</tr>
<tr>
<td>Allow manual profile installation</td>
<td></td>
<td>✓</td>
<td>iOS 6 +Supervised</td>
</tr>
<tr>
<td>Allow account modification</td>
<td></td>
<td>✓</td>
<td>iOS 7 +Supervised</td>
</tr>
<tr>
<td>Show Control Center on lock screen</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
<tr>
<td>Show notifications view on lock screen</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
<tr>
<td>Show today view on lock screen</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
<tr>
<td>Allow AirDrop</td>
<td></td>
<td>✓</td>
<td>iOS 7 +Supervised</td>
</tr>
</tbody>
</table>

### Applications

<table>
<thead>
<tr>
<th>Applications</th>
<th>Does Not Require Supervision</th>
<th>Requires Supervision</th>
<th>OS Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow use of YouTube</td>
<td>✓</td>
<td></td>
<td>iOS 5 and below</td>
</tr>
<tr>
<td>Allow use of iTunes Music Store</td>
<td>✓</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Allow use of iBookstore</td>
<td></td>
<td>✓</td>
<td>iOS 6 +Supervised</td>
</tr>
<tr>
<td>Allow Game Center</td>
<td></td>
<td>✓</td>
<td>iOS 6</td>
</tr>
<tr>
<td>Features and Functionality</td>
<td>Does Not Require Supervision</td>
<td>Requires Supervision</td>
<td>OS Notes</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------</td>
<td>---------------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>+Supervised</td>
</tr>
<tr>
<td>Allow multiplayer gaming</td>
<td>✓</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Allow adding Game Center Friends</td>
<td>✓</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Allow changes to Find My Friends</td>
<td>✓</td>
<td>✓</td>
<td>iOS 7</td>
</tr>
<tr>
<td>Allow changes to cellular data usage for apps</td>
<td>✓</td>
<td>✓</td>
<td>iOS 7</td>
</tr>
<tr>
<td>Allow use of Safari</td>
<td>✓</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Enable autofill</td>
<td>✓</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Force fraud warning</td>
<td>✓</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Enable JavaScript</td>
<td>✓</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Enable plugins</td>
<td>✓</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Block pop-ups</td>
<td>✓</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Accept Cookies</td>
<td>✓</td>
<td></td>
<td>-</td>
</tr>
</tbody>
</table>

**iCloud**

| Allow backup                | ✓                           |                     | iOS 5    |
| Allow document sync         | ✓                           |                     | iOS 5    |
| Allow keychain sync         | ✓                           |                     | iOS 7    |
| Allow app settings sync (key value sync) | ✓                       |                     | iOS 5    |
| Allow Photo Stream          | ✓                           |                     | iOS 5    |
| Allow Shared Photo Stream   | ✓                           |                     | iOS 6    |

**Security and Privacy**

<p>| Force iTunes Store password entry | ✓                           |                     | iOS 5    |
| Allow diagnostic data to be sent to Apple | ✓                       |                     | iOS 5    |
| Allow user to accept untrusted TLS certificates | ✓                       |                     | iOS 5    |</p>
<table>
<thead>
<tr>
<th>Features and Functionality</th>
<th>Does Not Require Supervision</th>
<th>Requires Supervision</th>
<th>OS Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow over the air PKI updates</td>
<td></td>
<td>✓</td>
<td>iOS 7</td>
</tr>
<tr>
<td>Force encrypted backups</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow pairing with non-Configurator hosts</td>
<td></td>
<td>✓</td>
<td>iOS 7 +Supervised</td>
</tr>
<tr>
<td>Enable Activation Lock</td>
<td></td>
<td>✓</td>
<td>iOS 7 +Supervised</td>
</tr>
<tr>
<td>Clear Activation Lock</td>
<td></td>
<td>✓</td>
<td>iOS 7.1 +Supervised</td>
</tr>
<tr>
<td>Media Content</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ratings region/Movies/TV Shows/Apps</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iBooks</td>
<td></td>
<td>✓</td>
<td>iOS 6 +Supervised</td>
</tr>
<tr>
<td>Allow explicit music and podcasts</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wi-Fi</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wi-Fi settings</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto-Join</td>
<td>✓</td>
<td></td>
<td>iOS 5</td>
</tr>
<tr>
<td>Wi-Fi Hotspot 2.0 settings</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
<tr>
<td>Proxy settings</td>
<td>✓</td>
<td></td>
<td>iOS 5</td>
</tr>
<tr>
<td>VPN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN settings</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per-App VPN</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
<tr>
<td>Connect automatically</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
<tr>
<td>Features and Functionality</td>
<td>Does Not Require Supervision</td>
<td>Requires Supervision</td>
<td>OS Notes</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------</td>
<td>----------------------</td>
<td>----------</td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email settings</td>
<td>✓</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Prevent Moving Messages</td>
<td>✓</td>
<td></td>
<td>iOS 5</td>
</tr>
<tr>
<td>Disable recent contact sync</td>
<td>✓</td>
<td></td>
<td>iOS 6</td>
</tr>
<tr>
<td>Prevent Use In 3rd Party Apps</td>
<td>✓</td>
<td></td>
<td>iOS 5</td>
</tr>
<tr>
<td>Use S/MIME</td>
<td>✓</td>
<td></td>
<td>iOS 5</td>
</tr>
<tr>
<td><strong>Exchange ActiveSync</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EAS settings</td>
<td>✓</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Use S/MIME</td>
<td>✓</td>
<td></td>
<td>iOS 5</td>
</tr>
<tr>
<td>Prevent Moving Messages</td>
<td>✓</td>
<td></td>
<td>iOS 5</td>
</tr>
<tr>
<td>Prevent Use In 3rd Party Apps</td>
<td>✓</td>
<td></td>
<td>iOS 5</td>
</tr>
<tr>
<td>Disable recent contact sync</td>
<td>✓</td>
<td></td>
<td>iOS 6</td>
</tr>
<tr>
<td><strong>LDAP</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP settings</td>
<td>✓</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td><strong>CalDAV</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CalDAV settings</td>
<td>✓</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td><strong>Subscribed Calendars</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features and Functionality</td>
<td>Does Not Require Supervision</td>
<td>Requires Supervision</td>
<td>OS Notes</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>------------------------------</td>
<td>----------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Subscribed Calendar settings</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CardDAV</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CardDAV settings</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web Clips</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Clip settings</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Credentials</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credentials certificate settings</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SCEP</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCEP settings for certificate authority</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Global HTTP Proxy</strong></td>
<td></td>
<td>✓</td>
<td>iOS 7 +Supervised</td>
</tr>
<tr>
<td>Global HTTP Proxy settings</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Single App Mode</strong></td>
<td></td>
<td>✓</td>
<td>iOS 6 +Supervised</td>
</tr>
<tr>
<td>Single App Mode – Lock device into a single app</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optional settings for &quot;Lock device into a single app&quot;</td>
<td>✓</td>
<td></td>
<td>iOS 7 +Supervised</td>
</tr>
<tr>
<td>Autonomous single app mode</td>
<td>✓</td>
<td></td>
<td>iOS 7 +Supervised</td>
</tr>
<tr>
<td><strong>Web Content Filter</strong></td>
<td></td>
<td>✓</td>
<td>iOS 7 +Supervised</td>
</tr>
<tr>
<td>Web Content Filter settings (Whitelist, Blacklist, Permitted URLs)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features and Functionality</td>
<td>Does Not Require Supervision</td>
<td>Requires Supervision</td>
<td>OS Notes</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------------------</td>
<td>----------------------</td>
<td>----------</td>
</tr>
<tr>
<td><strong>Single Sign On</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Single Sign On settings with Kerberos authentication</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
<tr>
<td><strong>AirPrint</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AirPrint destination settings</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
<tr>
<td><strong>AirPlay Mirroring</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AirPlay Destination settings (Whitelist)</td>
<td></td>
<td>✓</td>
<td>iOS 7</td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced Access Point settings</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>App Installation Settings</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Silent App Installation</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Control Cellular Settings</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice Roaming</td>
<td>✓</td>
<td></td>
<td>iOS 5</td>
</tr>
<tr>
<td>Data Roaming</td>
<td>✓</td>
<td></td>
<td>iOS 5</td>
</tr>
<tr>
<td>Personal Hotspot</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
<tr>
<td><strong>Wallpaper Settings</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set Lockscreen Image</td>
<td></td>
<td>✓</td>
<td>iOS 7</td>
</tr>
<tr>
<td>Set Home Screen Image</td>
<td></td>
<td>✓</td>
<td>iOS 7</td>
</tr>
<tr>
<td>Features and Functionality</td>
<td>Does Not Require Supervision</td>
<td>Requires Supervision</td>
<td>OS Notes</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------</td>
<td>----------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Queries and Commands</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervised status</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
<tr>
<td>Location service status</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
<tr>
<td>Personal Hotspot status</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
<tr>
<td><strong>Custom Fonts and Messaging</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Font Installation</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
<tr>
<td>Custom Enrollment Messages</td>
<td>✓</td>
<td></td>
<td>iOS 6</td>
</tr>
<tr>
<td>Custom MDM Prompts</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
<tr>
<td>Activation Lock Warning</td>
<td>✓</td>
<td></td>
<td>iOS 7</td>
</tr>
</tbody>
</table>