# Chicago Public Schools

## Mobile Device Management Settings

Version 1.0

May 21, 2019

# Contents

**MDM overview** 3

**Payload best practices** 5

**MDM Restrictions** 6

Functionality restrictions

iOS app restrictions

iOS media restrictions

Lists of available trusted root certificates in iOS

Allow USB accessories while locked

Manage software updates

**Sources** 15

**Change Log** 16

# MDM overview

This document is designed for IT and MDM administrators. It contains all aspects of mobile device management (MDM) settings as defined by Apple.

## What is mobile device management (MDM)?

iOS devices with iOS 5 or later, tvOS devices with tvOS 9 or later, and Mac computers with OS X 10.7 or later have a built-in framework that supports mobile device management (MDM). MDM lets you securely and wirelessly configure devices owned by your organization. MDM includes updating software and device settings, monitoring compliance with organizational policies, and remotely wiping or locking devices. Users can enroll their own devices in MDM, and organization-owned devices can be enrolled in MDM automatically using Apple School Manager.

After enrolled, you can wirelessly distribute, manage, and configure apps and books purchased through Apple School Manager, or enterprise apps developed in-house. Users can install apps themselves, or apps can be installed automatically depending on the type of app it is, how it's assigned, and whether the device is supervised.

There are a few concepts to understand if you're going to use MDM, so see next how MDM uses configuration profiles and payloads.

## How does MDM work?

Mobile device management is enabled when an MDM solution sends a properly configured enrollment profile to an Apple device. After the enrollment profile is approved, either by the device or the user, configuration profiles containing payloads are delivered to the device. The settings in the payloads determine how the device will function.

## What are configuration profiles?

A configuration profile is an XML file that consists of payloads that load settings and authorization information onto Apple devices. Configuration profiles automate the configuration of settings, accounts, restrictions, and credentials. These files can be created by an MDM solution or Apple Configurator 2, or they can be created manually.

Because configuration profiles can be encrypted and signed, you can restrict their use to a specific Apple device and—with the exception of user names and passwords—prevent anyone from changing the settings. You can also mark a configuration profile as being locked to the device. The configuration profile can be removed only by wiping the device of all data or by entering the password associated with the configuration profile. Accounts that are configured by a profile, such as Microsoft Exchange accounts, can be removed only by deleting the configuration profile.

## Why are there two types of configuration profiles?

Configuration profiles can be sent to users or devices, or groups of users or groups of devices.

You may also want to create separate configuration profiles for specific devices or a group of users (such as students). For information, see Payload best practices.

Note: You can use Apple Configurator 2 to add device configuration profiles (automatically or manually) to iOS and tvOS devices. To add device or user configuration profiles containing macOS-specific settings, use a third-party mobile device management (MDM) solution or Profile Manager, part of the macOS Server app.

## What is a payload?

A payload can be configured to manage specific settings on Apple devices. For example, you can have different payloads to require a complex passcode, populate an Exchange account with all the Exchange server information, and add a VPN configuration to a device. Even though each payload has its own unique settings, all payloads are defined by the following:

- The operating system or systems that the payload supports.
- The channel that does the payload work.
- Whether the payload requires the Apple device to be supervised.
- Whether the payload is exclusive or whether it can be combined with other payloads of the same type.
- Whether the payload can have duplicates.
- After payloads are configured, they are saved in a configuration profile.

# Payload best practices

Configuration profile and payload planning helps reduce complexity. Keep the following in mind:

- A configuration profile can have more than one payload.
- A device can have more than one configuration profile.
- On macOS, you can combine user configuration profiles with device configuration profiles.
- If you have multiple configuration profiles containing similar payloads with different settings, the resulting behavior is undefined. In iOS, if there are conflicting restrictions, the more restrictive restriction wins.
- Some payloads can have more than one unique payload. For example, a Certificates payload often involves more than one certificate, and a VPN payload may involve more than one VPN setting.

Here are some examples of optimized payload management:

- If you want to manage iOS and macOS devices, use the same payloads for all the devices.
- If you want to manage only iOS devices or users of iOS devices, focus on iOS payloads.
- If you want to manage only macOS devices or users of macOS devices, focus on macOS payloads, then decide if your management should be at the device or user level.

Although you can create a single configuration profile that contains all payloads for your organization, consider creating separate profiles based on functionality. This will ensure that changes made to one configuration profile don't inadvertently affect another. Settings that rarely change may include device restrictions, Wi-Fi, security and privacy, LDAP, mail, and calendar. Settings that may change often include VPN, certificates, Web Clips, and Home screen settings.

Users generally can't change settings that are defined in a configuration profile. You can also set configuration profiles to expire on a specific date. Accounts configured by a configuration profile can be removed only by deleting the profile. Doing so may prevent the device from being used in your organization until the profile is reinstalled. For example, removing a configuration profile may prevent the user from accessing the network, receiving mail, and creating events using their Calendar app. You can also supervise iOS and tvOS devices, to prevent any user from removing the configuration profile.

**Important:** If the user knows the passcode, iOS devices that aren't supervised can have configuration profiles removed, even if the option is set to Never in the General settings. macOS configuration profiles can be removed if the user knows an administrator's user name and password.

# MDM Restrictions

### Restrictions overview

Restrictions can be enabled, or in some cases disabled, to prevent users from accessing a specific app, service, or function of the device. Restrictions are sent to devices in a restrictions payload, which is attached to a configuration profile. For example, a restriction can be enabled that prevents an iOS device from using the camera to take pictures or videos. Another restriction can be added to prevent FaceTime video and audio calls on the iOS device or Mac.

## Functionality restrictions

| Setting | JAMF Pro Expression | Definition | Supervision Required | OS Introduced | Enabled Districtwide |
|---|---|---|---|---|---|
| Use of cameras | Allow use of camera | Cameras are enabled and Users can take photographs or videos. The Camera icon is removed from the Home screen in iOS when disabled. | No | 2.0 | ✓ |
| FaceTime | Allow FaceTime (supervised only) | Users can place or receive FaceTime audio or video calls. | No | 4.0 | ✓ |
| Screenshots and screen recordings | Allow screenshots and screen recording | Users can save a screenshot or recording of the screen. | No | 3.1 | ✓ |
| AirPlay, View Screen by Classroom, and screen sharing | Allow screen observation by Classroom app (Apple Education Support enabled, supervised only) | Teachers using Classroom can use AirPlay with, view, students' screens, or share a student's screen. | Yes | 9.3 | ✓ |
| Classroom to perform AirPlay and View Screen without prompting | Allow modifying the AirPlay and View Screen permission for managed classes (supervised only) | Students in managed classes are prompted when the teacher uses AirPlay or View Screen. | Yes | 11.0 | - |
| AirDrop | Allow AirDrop (supervised only) | Users can use AirDrop. | Yes | 7.0 | ✓ |
| iMessage | Allow iMessage (supervised only) | For Wi-Fi–only devices, the Messages app is hidden when disabled. For devices with Wi-Fi and cellular, the Messages app is still available, but only the SMS/MMS service can be used. | Yes | 5.0 | ✓ |
| Voice dialing while device is locked | Allow voice dialing while device is locked | Users can use voice commands to dial their phone when it's locked. | No | 4.0 | ✓ |
| Siri | Allow Siri | Siri can be used. | No | 5.0 | ✓ |
| Siri while device locked | Allow Siri while device locked | Siri responds when the device is locked. | No | 5.1 | ✓ |
| User-generated content in Siri | Allow user-generated content in Siri (supervised only) | Siri can access content from sources that allow user-generated content, such as Wikipedia. | Yes | 7.0 | ✓ |
| Siri Suggestions | Allow Siri Suggestions | During search, Siri can offer suggestions for apps, people, locations, and more. | No | 7.0 | ✓ |
| Setup a nearby Apple device | Allow proximity setup to new device (iOS 11 or later, supervised only) | Users can use their Apple devices to set up and configure other Apple devices. | Yes | 11.0 | ✓ |
| Install apps | Allow installing apps using Apple Configurator and iTunes (iOS 9 or later) / Allow installing apps using App Store (iOS 5–iOS 8 only) | Users can install apps. | No | 2.0 | ✓ |
| Install apps using App Store | Allow installing apps using App Store (iOS 9 or later, supervised only) | App Store is enabled and its icon is available from the Home screen. Users can install or update apps from the App Store using iTunes or MDM. In-house enterprise apps can still be installed and updated when disabled. *Note:* If native iOS system apps are removed, they can be reinstalled. | Yes | 9.0 | ✓ |

| Setting | JAMF Pro Expression | Definition | Supervision Required | OS Introduced | Enabled Districtwide |
|---|---|---|---|---|---|
| Automatic app downloads | Allow automatic app downloads (iOS 9 or later, supervised only) | The App Store will automatically download apps. | Yes | 9.0 | ✓ |
| Remove apps | Allow removing apps (supervised only) | Users can remove installed apps. | Yes | 4.2.1 | ✓ |
| Remove system apps | Allow removing system apps (iOS 11 or later, supervised only) | Users can remove iOS-native apps. | Yes | 11.0 | ✓ |
| Apple Music | Allow Apple Music (supervised only) | Users can use Apple Music. | Yes | 9.3 | ✓ |
| Radio | Allow Radio (supervised only) | Users can listen to the radio with Apple Music. | Yes | 9.3 | ✓ |
| Require iTunes Store password for all purchases | Require iTunes Store password for all purchases | In-app purchases and iTunes Store purchases prompt for the account password. | No | 6.0 | - |
| iCloud backup | Allow iCloud backup | Device backup is performed only in iTunes when disabled. | No | 5.0 | ✓ |
| iCloud Drive | Allow iCloud documents & data (supervised only) | iCloud Drive can be used to store any data. | No | iOS 5.0 | ✓ |
| iCloud Keychain | Allow iCloud keychain | iCloud Keychain can be used. | No | 7.0 | ✓ |
| Managed apps store data in iCloud | Allow managed apps to store data in iCloud | Users can store data from managed apps in iCloud. | No | 8.0 | ✓ |
| Backup enterprise books | Allow backup of enterprise books | Users can back up books distributed by their organization to iCloud or iTunes. | No | 8.0 | ✓ |
| Notes and highlights sync for enterprise books | Allow notes and highlights sync for enterprise books | Users can sync notes or highlights to other devices using iCloud. | No | 8.0 | ✓ |
| Shared Albums | Allow iCloud Photo Sharing | Users can subscribe to or publish shared photo albums. | No | 5.0 | ✓ |
| iCloud Photos | Allow iCloud Photo Library | Users can use their iCloud Photos. | No | 9.0 | ✓ |
| My Photo Stream | Allow My Photo Stream (disallowing can cause data loss) | When disabled, Photos in My Photo Stream are erased from the device, photos from the Camera Roll aren't sent to My Photo Stream, and photos and videos in shared streams can no longer be viewed on the device.<br>*Important*: If there are no other copies of these photos and videos, they may be lost when disabled. | No | 5.0 | ✓ |
| Automatic sync while roaming | Allow automatic sync while roaming | Devices that are roaming sync only when an account is accessed by the user. | No | 4.0 | ✓ |
| Force encrypted backups | Force encrypted backups | Users can't choose whether device backups performed in iTunes are stored in encrypted format on the user's Mac. If any profile is encrypted and this option is turned off, encryption of backups is required and enforced by iTunes.<br>Profiles installed on the device by Profile Manager are never encrypted. | No | 4.0 | - |
| Force limited ad tracking | Force limited ad tracking | Apps can't use the Advertising Identifier (a nonpermanent device identifier) to serve the user-targeted ads. | No | 7.0 | ✓ |
| Erase All Content and Settings | Allow Erase All Content and Settings (supervised only) | Users can erase their device and reset it to factory defaults. | Yes | 8.0 | ✓ |
| Users accept untrusted TLS certificates | Allow users to accept untrusted TLS certificates | Users are asked if they want to trust certificates that can't be verified. This setting applies to Safari, Mail, Contacts, and Calendar accounts. When this option is on, only certificates with trusted root certificates are accepted without a prompt. To view the root CAs accepted by iOS, see the Apple Support article Lists of available trusted root certificates in iOS. | No | 5.0 | ✓ |

| Setting | JAMF Pro Expression | Definition | Supervision Required | OS Introduced | Enabled Districtwide |
|---|---|---|---|---|---|
| Automatic updates to certificate trust settings | Allow automatic updates to certificate trust settings | Automatic updates to certificate trust settings can occur. | No | 7.0 | ✓ |
| Trust new enterprise app authors | Allow trusting new enterprise app authors | Users can allow new enterprise app authors to be trusted, which prohibits apps from those authors from launching. | No | 9.0 | ✓ |
| Install configuration profiles | Allow installing configuration profiles (supervised only) | Configuration profiles can be manually installed by users. | Yes | 6.0 | ✓ |
| Add VPN configurations | Allow adding VPN configurations (iOS 11 or later, supervised only) | Users can create and add VPN configurations. | Yes | 11.0 | ✓ |
| Classroom can focus students on a single app and lock the device without prompting | Allow Classroom app to lock student devices to an app and lock device screens without prompting (iOS 11 or later, supervised only) | Teachers can lock an app open or lock the device without first prompting the user. | Yes | 11.0 | ✓ |
| Require teacher permission to leave Classroom teacher-created classes | Require teacher permission to leave Classroom unmanaged classes (iOS 11.3 or later, supervised only) | Students must request permission before they can leave a teacher-created class. | Yes | 11.3 | ✓ |
| Automatic joining of Classroom classes without prompting | Automatically join Classroom classes without prompting (iOS 11 or later, supervised only) | Students can join a class without prompting the teacher. | Yes | 11.0 | ✓ |
| Modify account settings | Allow modifying account settings (supervised only) | Users can create new accounts or change their user name, password, or other settings associated with their account. | Yes | 7.0 | ✓ |
| Modify Bluetooth settings | Allow modifying Bluetooth settings (supervised only) | Users can modify the Bluetooth setting. | Yes | 11.0 | ✓ |
| Modify cellular data app settings | Allow modifying cellular data app settings (supervised only) | Users can change any settings for apps that use cellular data. | Yes | 7.0 | ✓ |
| Modify Find My Friends settings | Allow modifying Find My Friends settings (supervised only) | Users can change any settings in the Find My Friends app. | Yes | 7.0 | ✓ |
| Modify Notifications settings | Allow modifying notifications settings (supervised only) | Users can change the configuration of any Notifications settings. | Yes | 9.3 | ✓ |
| Modify passcode | Allow modifying passcode (supervised only) | Users can change the set passcode. | Yes | 9.0 | ✓ |
| Modify Touch ID fingerprints and Face ID faces | Allow modifying Touch ID fingerprints (supervised only) | Users can add or remove existing biometric information. | Yes | 8.3 (Touch ID) 11.0 (Face ID) | ✓ |
| Modify restrictions or Screen Time settings | Allow modifying restrictions (supervised only) | Users can set their own restrictions on their device for iOS 11.4.1 and earlier. Users can set their own Screen Time settings on their device for iOS 12 or later. | Yes | 8.0 (Restrictions) 12.0 (Screen Time) | ✓ |
| Modify Wallpaper | Allow modifying Wallpaper (supervised only) | Users can modify the wallpaper for the Lock screen or Home screen. | Yes | 9.0 | ✓ |
| Turn on "Set Automatically" in Date and Time settings | Force automatic date and time (iOS 12 or later, supervised only) | Set Automatically is turned on, and users can't turn it off. | Yes | 12.0 | - |
| Pair with non-Apple Configurator 2 hosts | Allow pairing with non-Configurator hosts (supervised only) | Users can pair their iOS device with anything but the Mac with Apple Configurator 2 installed, where the device was first supervised. | Yes | 7.0 | ✓ |
| Documents from managed sources appear in unmanaged destinations | Allow documents from managed sources in unmanaged destinations | Documents created or downloaded from managed sources can be opened in unmanaged destinations. | No | 7.0 | ✓ |

| Setting | JAMF Pro Expression | Definition | Supervision Required | OS Introduced | Enabled Districtwide |
|---|---|---|---|---|---|
| Documents from unmanaged sources appear in managed destinations | Allow documents from unmanaged sources in managed destinations | Documents created or downloaded from unmanaged sources can be opened in managed destinations. | No | 7.0 | ✓ |
| Treat AirDrop as unmanaged destination | Treat AirDrop as unmanaged destination | Users see AirDrop as an option from a managed app.<br>For this restriction to work when it's enabled, you must also disable "Allow documents from managed sources in unmanaged destinations." | No | 9.0 | - |
| Handoff | Allow Handoff | Users can use Handoff with their Apple devices. | No | 8.0 | ✓ |
| Send diagnostic and usage data to Apple | Allow sending diagnostic and usage data to Apple | Users can choose to send diagnostic information to Apple. | No | 6.0 | ✓ |
| Modify diagnostic settings | Allow modifying diagnostics settings (supervised only) | Modifying diagnostic data settings is permitted. | Yes | 9.3.2 | ✓ |
| Touch ID or Face ID to unlock device | Allow Touch ID/Face ID to unlock device | Users can use a passcode to unlock the device. | No | 7.0 (Touch ID)<br>11.0 (Face ID) | ✓ |
| Password AutoFill | Allow password AutoFill (iOS 12 or later, supervised only) | Users can use AutoFill Passwords, and no prompt is shown to pick a saved password from iCloud Keychain or third-party password managers. | Yes | 12.0 | ✓ |
| Require Face ID authentication for AutoFill | Require Face ID authentication before AutoFill (iOS 11.3 or later, supervised only) | Users can use Face ID authentication to AutoFill app data. | Yes | 11.0 | ✓ |
| Force Apple Watch wrist detection | Force Apple Watch wrist detection | Apple Watch locks automatically when it's removed from the user's wrist. It can be unlocked with its passcode or the paired iPhone. | No | 8.2 | - |
| Pair with Apple Watch | Allow pairing with Apple Watch (supervised only) | Users can pair their supervised iPhone with Apple Watch. | Yes | 9.0 | ✓ |
| Require passcode on first AirPlay pairing | Require passcode on first AirPlay pairing | A passcode is required when an iOS device or Apple TV is first paired for AirPlay. | No | 7.1 | - |
| Join only Wi-Fi networks installed by a Wi-Fi payload | Allow connection to unmanaged Wi-Fi networks (supervised only) | Devices that have this restriction can join any Wi-Fi network, not only those added to the Wi-Fi payload.<br>Important: If the Wi-Fi network isn't available, the device can't be managed. | Yes | 10.3 | ✓ |
| Share passwords over AirDrop. | Allow password sharing (iOS 12 or later, supervised only) | Users can share their passwords over AirDrop. | Yes | 12.0 | ✓ |
| AirPrint | Allow AirPrint (iOS 11 or later, supervised only) | Users can use AirPrint. | Yes | 11.0 | ✓ |
| AirPrint to destinations with untrusted certificates | Disallow AirPrint to destinations with untrusted certificates (iOS 11 or later, supervised only) | Users can't use AirPrint to print to printers with untrusted certificates. | Yes | 11.0 | - |
| Discover AirPrint printers using iBeacons | Allow discovery of AirPrint printers using iBeacons (iOS 11 or later, supervised only) | Users can discover AirPrint printers using nearby iBeacon-compatible hardware transmitters. | Yes | 11.0 | ✓ |
| Store AirPrint credentials in Keychain | Allow storage of AirPrint credentials in Keychain (iOS 11 or later, supervised only) | Users can save their AirPrint credentials to their Keychain. | Yes | 11.0 | ✓ |
| Predictive keyboard | Allow predictive keyboard (supervised only) | Users will see the predictive keyboard. | Yes | 8.1.3 | - |
| Keyboard shortcuts | Allow keyboard shortcuts (supervised only) | Users can use any keyboard shortcuts. | Yes | 9.0 | ✓ |
| Auto correction | Allow auto correction (supervised only) | Users will see any word correction suggestions. | Yes | 8.1.3 | - |
| Spell check | Allow spell check (supervised only) | Users will see potentially misspelled words underlined in red. | Yes | 8.1.3 | - |
| Define | Allow Define (supervised only) | Users can double-tap to search for a word's definition. | Yes | 8.1.3 | - |

| Setting | JAMF Pro Expression | Definition | Supervision Required | OS Introduced | Enabled Districtwide |
|---|---|---|---|---|---|
| Dictation | Allow dictation (supervised only) | Users can use dictation on their device. | Yes | 10.3 | ✓ |
| Wallet notifications in Lock screen | Allow Wallet notifications in Lock screen | Users mustn't unlock the device to use Wallet. | No | 6.0 | ✓ |
| Control Center in Lock screen | Show Control Center in Lock screen | Users can swipe up to view Control Center. | No | 7.0 | ✓ |
| Notification Center in Lock screen | Show Notification Center in Lock screen | Users can view the Notification history when the screen is locked. | No | 7.0 | ✓ |
| Today view in Lock screen | Show Today view in Lock screen | Users can swipe down to see Notification Center using Today View in the Lock screen. | No | 7.0 | ✓ |
| Manage software updates | Defer software update for n days (iOS 11.3 or later, supervised only) | There are two options when managing software updates:<br>• Hide iOS software updates.<br>• Force an iOS software update delay.<br>See Manage software updates. | Yes | 11.3 | - |
| Allow USB accessories while locked | Allow USB restricted mode (iOS 11.3 or later, supervised only) | Users can always connect USB accessories when the iOS device is locked.<br>See Allow USB accessories while locked. | Yes | 11.4.1 | ✓ |
| Modify device name | Allow modifying device name (supervised only) | Users can change the name of the device as shown in Settings > General > About. | Yes | 9.0 | ✓ |
| Siri profanity filter | Enable Siri profanity filter (supervised only) | The profanity filter in Siri can't be disabled. | Yes | 5.0 | ✓ |
| Apple Books | Allow iBooks Store (supervised only) | Apple Books is enabled, and users can access it from the Books app. | Yes | 6.0 | ✓ |
| In-app purchase | Allow in-app purchase | Users can make in-app purchases. | No | 4.0 | ✓ |
| Proximity AutoFill | Allow proximity based password sharing requests (iOS 12 or later, tvOS 12 or later, supervised only) | Users' devices will advertise themselves to nearby devices for passwords by use of Proximity AutoFill. In iOS and macOS this feature restricts only Wi-Fi Password requests. | Yes | 12.0 | ✓ |
| Modify personal Hotspot settings | Not Supported | Users can't modify personal Hotspot settings. | Yes | 12.2 | n/a |
| Modify cellular plan settings | Not Supported | Users can't change any settings for the cellular plan. | Yes | 11.0 | n/a |
| Modify eSIM settings | Not Supported | Users can't add or remove an eSIM plan for an iPhone that supports eSIM. | Yes | 12.1 | n/a |
| Managed apps to edit unmanaged contacts | Not Supported | Managed apps can edit contacts to unmanaged accounts, even if managed apps are prevented from editing unmanaged destinations. | No | 12.0 | n/a |
| Unmanaged apps to read managed contacts | Not Supported | Unmanaged apps can read contacts from managed accounts, even if unmanaged apps are prevented from reading to managed destinations. | No | 12.0 | n/a |
| Require Touch ID or Face ID authentication for AutoFill | Not Supported | Users can't use biometric authentication to AutoFill app data. | Yes | 11.0 | n/a |

# iOS app restrictions

| Setting | JAMF Pro Expression | Definition | Supervision Required | OS Introduced | Enabled Districtwide |
|---|---|---|---|---|---|
| iTunes Store | Allow use of iTunes Store (supervised only) | The iTunes Store is enabled and its icon is available from the Home screen. Users can preview, purchase, or download content. | Yes | 2.0 | ✓ |
| News | Allow use of News (supervised only) | Users can use the News app. | Yes | 9.0 | ✓ |
| Podcasts | Allow use of Podcasts (supervised only) | Users can download podcasts. | Yes | 8.0 | ✓ |
| Game Center | Allow use of Game Center (supervised only) | Users can use Game Center. | Yes | 6.0 | ✓ |
| Multiplayer gaming | Allow multiplayer gaming (supervised only) | Users can play multiplayer games in Game Center. | Yes | 4.1 | ✓ |
| Add Game Center friends | Allow adding Game Center friends (supervised only) | Users can find or add friends in Game Center. | Yes | 4.2.1 | ✓ |
| Use Safari | Allow use of Safari (supervised only) | The Safari web browser app is enabled and its icon is available from the Home screen. When disabled, this setting will prevent users from opening web clips.<br><br>*Note:* This restriction is deprecated on unsupervised devices. | Yes | 2.0 | ✓ |
| Safari AutoFill | Enable AutoFill | Safari can keep track of what users enter in web forms. | No | 4.0 | ✓ |
| Force fraud warning | Force fraud warning | Safari attempts to prevent the user from visiting websites identified as being fraudulent or compromised. | No | 4.0 | - |
| JavaScript | Enable JavaScript | Safari ignores all JavaScript on websites. | No | 4.0 | ✓ |
| Safari pop-ups | Block pop-ups | Pop-ups are blocked in Safari. | No | 4.0 | - |
| Block cookies | Block cookies | Sets the cookie policy in Safari.<br><br>See Manage Safari cookies. | No | 4.0 | Always Allow |
| Autonomous Single App Mode | Autonomous Single App Mode apps (supervised only) | Allows selected apps to be used in Autonomous Single App Mode. | Yes | 7.0 | - |
| Restrict app usage | Restrict App Usage (supervised only) | Allows any apps other than Settings or Phone (iPhone) to be placed in an approved list or in a disapproved list. | Yes | 9.3 | Allow All Apps |

### Manage Safari cookies

You can manage how cookies are handled in Safari. You can set the restriction to Always Allow or one of these options:

| Prevent cross-site tracking | Block all cookies | User action |
|---|---|---|
| Enabled | Enabled | Can't disable either setting |
| Enabled | Not enabled | Can manage only Block all cookies setting |
| Enabled | Not enabled | Can manage either setting |

# iOS media restrictions

| Setting | JAMF Pro Expression | Definition | Supervision Required | OS Introduced | Enabled Districtwide |
|---|---|---|---|---|---|
| Ratings region | Ratings region | Select from nine different regions. This setting can't be disabled. The default is United States. | No | 4.0 | United States |
| Define content ratings | Allowed content ratings | Select maximum allowed ratings for movies, TV shows, and apps. | No | 4.0 | Allow All |
| Explicit content in Apple Books | Allow explicit sexual content in iBooks Store | Explicit content purchased from Apple Books is hidden. Explicit content is flagged by content providers when sold through the Books app. | No | 6.0 | ✓ |
| Playback of explicit music, podcasts, and iTunes U content | Allow playback of explicit music, podcasts, and iTunes U (supervised only) | Explicit music or video content purchased from the iTunes Store or listed in iTunes U is hidden. Explicit content is flagged by content providers, such as record labels, when sold through the iTunes Store or distributed through iTunes U. | Yes | 2.0 | ✓ |

# Lists of available trusted root certificates in iOS

The iOS Trust Store contains trusted root certificates that are preinstalled with iOS.

**Blocking Trust for WoSign CA Free SSL Certificate G2**
Certificate Authority WoSign experienced multiple control failures in their certificate issuance processes for the WoSign CA Free SSL Certificate G2 intermediate CA. Although no WoSign root is in the list of Apple trusted roots, this intermediate CA used cross-signed certificate relationships with StartCom and Comodo to establish trust on Apple products.

In light of these findings, we took action to protect users in a security update. Apple products no longer trust the WoSign CA Free SSL Certificate G2 intermediate CA.

To avoid disruption to existing WoSign certificate holders and to allow their transition to trusted roots, Apple products trust individual existing certificates that were issued from this intermediate CA and published to public Certificate Transparency log servers by 2016-09-19. They will continue to be trusted until they expire, are revoked, or are untrusted at Apple's discretion.

As the investigation progresses, we will take further action on WoSign/StartCom trust anchors in Apple products as needed to protect users.

**Further steps for WoSign**
After further investigation, we have concluded that in addition to multiple control failures in the operation of the WoSign certificate authority (CA), WoSign did not disclose the acquisition of StartCom.

We are taking further actions to protect users in an upcoming security update. Apple products will block certificates from WoSign and StartCom root CAs if the "Not Before" date is on or after 1 Dec 2016 00:00:00 GMT/UTC.

**About trust and certificates**
Each iOS Trust Store listed below contains three categories of certificates:

- Trusted certificates establish a chain of trust that verifies other certificates signed by the trusted roots—for example, to establish a secure connection to a web server. When IT administrators create Configuration Profiles for iOS, these trusted root certificates don't need to be included.
- Always Ask certificates are untrusted but not blocked. When one of these certificates is used, you'll be prompted to choose whether or not to trust it.
- Blocked certificates are believed to be compromised and will never be trusted.

**iOS Trust Store**
- List of available trusted root certificates in iOS 12, macOS 10.14, watchOS 5, and tvOS 12
- List of available trusted root certificates in iOS 11
- List of available trusted root certificates in iOS 10
- List of available trusted root certificates in iOS 9
- List of available trusted root certificates in iOS 8
- List of available trusted root certificates in iOS 7

## Allow USB accessories while locked

To improve security while maintaining usability, iOS 11.4.1 or later requires Touch ID, Face ID, or passcode entry to activate the USB interface if USB hasn't been used recently. This eliminates attack surface against physically connected devices such as malicious chargers while still enabling usage of USB accessories within reasonable time constraints. If more than an hour has passed since the iOS device has locked or since a USB connection has been detached, the device won't allow any new connections to be established until the device is unlocked. This hour period:

- Ensures that frequent users of connections to a Mac or PC, to USB accessories, or wired to CarPlay won't need to input their passcodes every time they attach their device
- Is necessary because the USB accessory ecosystem doesn't provide a reliable way to identify accessories before establishing a data connection

In addition, in iOS 12 if it's been more than three days since a USB connection has been established, the device will disallow new USB connections immediately after it locks. This is to increase protection for users that don't often make use of such connections. USB connections are also disabled whenever the device is in a state where it requires a passcode to re-enable biometric authentication.

This behavior may be disabled by a profile on supervised devices to always allow USB connections while locked. If the device isn't supervised, the user can choose to re-enable always-on USB connections in devices:

- Without Touch ID or Face ID: Choose Settings > Passcode > Allow Access When Locked > USB Accessories
- With Face ID: Choose Settings > Face ID & Passcode > Allow Access When Locked > USB Accessories
- With Touch ID: Choose Settings > Touch ID & Passcode > Allow Access When Locked > USB Accessories

Setting up some assistive devices does this automatically.

## Manage software updates

There are two options when managing software updates:

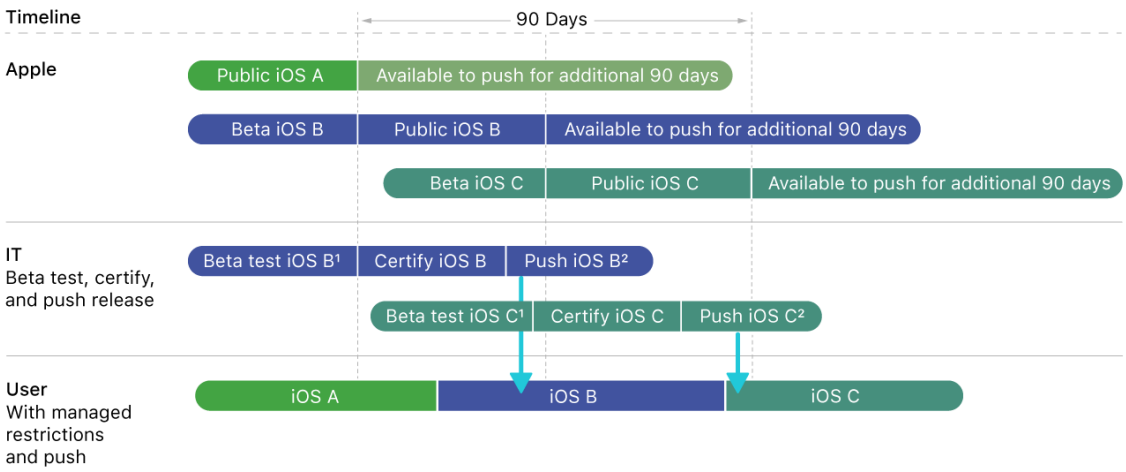
- Hide OS software updates
- Force an OS software update delay

You can prevent users from manually updating a device over-the-air for a specified time. When you implement this restriction, the default delay is 30 days and is triggered the moment Apple releases an OS update. However, you can change the default number of days you prevent updates, anywhere from 1 to 90 days. When the delay expires, users get a notification to update to the earliest version of OS that was available when the delay was triggered.

If the devices are enrolled in Apple School Manager or Apple Business Manager, the user won't need to review and accept updated OS terms and conditions on the device.

The following figure illustrates how you may manage iOS software updates:

If permitted, users can still update their devices with Apple Configurator or iTunes.




*Note:* If there is no passcode, you can perform the installation using your MDM solution. If the device has a passcode, MDM queues the update and the user is prompted to enter their passcode in order to start the installation.

# Sources

Mobile Device Management Settings: MDM for IT

# Change Log

20190517 - Original release