Managing Devices and Corporate Data on iOS

Contents

Overview

Businesses everywhere are empowering their employees with iPhone and iPad.

The key to a successful mobile strategy is balancing IT control with user enablement. By personalizing iOS devices with their own apps and content, users take greater ownership and responsibility, leading to higher levels of engagement and increased productivity. This is enabled by Apple's management framework, which provides smart ways to manage corporate data and apps discretely, seamlessly separating work data from personal data. Additionally, users understand how their devices are being managed and trust that their privacy is protected.

This document offers guidance on how essential IT control can be achieved while at the same time keeping users enabled with the best tools for their job. It complements the iOS Deployment Reference, a comprehensive online technical reference for deploying and managing iOS devices in your enterprise.

To refer to the iOS Deployment Reference, visit help.apple.com/deployment/ios.

Management Basics

With iOS, you can streamline iPhone and iPad deployments using a range of built-in techniques that allow you to simplify account setup, configure policies, distribute apps, and apply device restrictions remotely.

Our management approach

Apple's management framework is the foundation for managing mobile devices. This framework is built into iOS, allowing organizations to manage what they must—with a light touch—and not by simply locking down features or disabling functionality. As a result, Apple's management framework enables granular control by third-party mobile device management (MDM) solutions of your devices, apps, and data. And most important, you get the control you need without degrading the user experience or compromising your employees' privacy.

Other device management methods in the market may use different names to describe MDM functionality, such as enterprise mobility management (EMM) or mobile application management (MAM). These solutions have the same goal in mind—to manage your organization's devices and corporate data over the air. And because Apple's management framework is built into iOS, you don't need a separate agent application from your MDM solution provider.

Separating Work and Personal Data

Whether your organization supports user-owned or company-owned devices, you can meet your IT management goals while at the same time keeping users fully productive in their tasks. Work and personal data are managed separately, without segmenting the user experience. This allows the hottest productivity app to sit next to your corporate apps on a user's device—giving employees more freedom to work. iOS achieves this without the use of third-party solutions such as containers, which impact the user experience and frustrate users.

Understanding different management models

Often containers have been built to solve issues on other platforms—issues not found with iOS. Some containers use a dual-persona strategy, which creates two separate environments running on the same device. Others focus on containerizing the apps themselves through code-based integration or app wrapping solutions. All of these methodologies present productivity obstacles for users, whether it's logging in and out of multiple workspaces or adding a dependency on proprietary code that often causes app incompatibility with operating system updates.

Organizations that no longer use containers are seeing that the native management controls in iOS enable an optimal personal experience for users and increase their productivity. Rather than making it hard for users to use their devices for both work and personal, you can use policy controls that manage the data flow seamlessly behind the scenes.

Managing corporate data

With iOS, you don't have to lock down your devices. Key technologies control the flow of corporate data between apps and prevent its leakage to the user's personal apps or cloud services.

Managed content

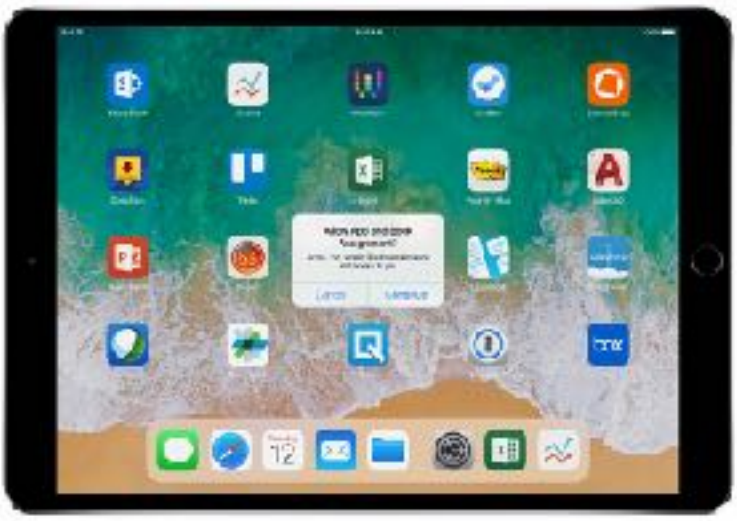
Managed content covers the installation, configuration, management, and removal of App Store and custom in-house apps, accounts, books, and domains.

- **Managed apps.** Apps installed using MDM are called managed apps. They may be free or paid apps from the App Store, or custom in-house apps, and all can be installed over the air using MDM. Managed apps often contain sensitive information, and provide more control than apps downloaded by the user. The MDM server can remove managed apps and their associated data on demand, or specify whether the apps should be removed when the MDM profile is removed. Additionally, the MDM server can prevent managed app data from being backed up to iTunes and iCloud.
- **Managed accounts.** MDM can help your users get up and running quickly by setting up their mail and other accounts automatically. Depending on the MDM solution provider and integration with your internal systems, account payloads can also be pre-populated with a user's name, mail address, and, where applicable, certificate identities for authentication and signing. MDM can configure the following types of accounts: IMAP/POP, CalDAV, subscribed Calendars, CardDAV, Exchange ActiveSync, and LDAP.
- **Managed books.** Using MDM, books, ePub books, and PDF documents can be automatically pushed to user devices, so employees always have what they need. Managed books can be shared only with other managed apps or mailed using managed accounts. When no longer necessary, the materials can be removed remotely.

- **Managed domains.** Downloads from Safari are considered managed documents if they originate from a managed domain. Specific URLs and subdomains can be managed. For example, if a user downloads a PDF from a managed domain, the domain requires that the PDF comply with all managed document settings. Paths following the domain are managed by default.

Managed distribution

Managed distribution lets you use your MDM solution or Apple Configurator 2 to manage apps purchased from the Volume Purchase Program (VPP). To enable managed distribution, you'll need to first link your MDM solution to your VPP account using a secure token. Once your MDM server is connected to VPP, assign apps directly to a device without the user even needing an Apple ID. A user is prompted when apps are ready to be installed on their device. If a device is supervised, apps are silently pushed to that device without prompting the user.



To retain full control over apps with an MDM solution, assign apps directly to a device.

Managed app configuration

With managed app configuration, MDM uses the native iOS management framework to configure apps during or after deployment. This framework enables developers to identify the configuration settings that should be implemented when their app is installed as a managed app. Employees can start using apps that have been configured this way right away, without requiring custom setup. IT gets the assurance that corporate data within apps is handled securely, with no need for proprietary SDKs or app wrapping.

There are capabilities available to app developers that can be enabled using managed app configuration such as app configuration, prevent app backup, disable screen capture, and remotely wipe app.

The AppConfig Community is focused on providing tools and best practices around native capabilities in mobile operating systems. Leading MDM solution providers from this community have established a standard schema that all app developers can use to support managed app configuration. By enabling a more consistent, open, and simple way to configure and secure mobile apps, the community helps increase mobile adoption in business.

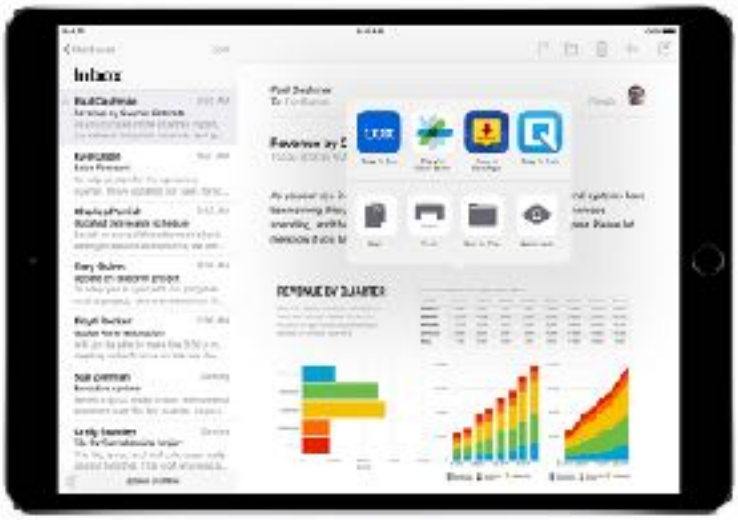
To learn more about the AppConfig Community, visit www.appconfig.org.

Managed data flow

MDM solutions provide specific features that enable corporate data to be managed at a granular level so that it does not leak out to the users' personal apps and cloud services.

- **Managed Open In.** Open In management uses a set of restrictions that prevent attachments or documents from managed sources from being opened in unmanaged destinations, and vice versa.

  For example, you can prevent a confidential email attachment in your organization's managed mail account from being opened in any user's personal apps. Only apps installed and managed by MDM can open this work document. The user's unmanaged personal apps do not appear in the list of apps available to open the attachment. In addition to managed apps, accounts, books, and domains, several extensions respect managed Open In restrictions.



To protect corporate data, only apps installed and managed by MDM can open this work document.

- **Managed extensions.** App extensions give third-party developers a way to provide functionality to other apps or even to key systems built into iOS like Notification Center, enabling new business workflows between apps. Using managed Open In prevents unmanaged extension functionality from interacting with managed apps. The following examples show different types of extensions:
  - **Document Provider extensions** allow productivity apps to open documents from a variety of cloud services, without having to make unnecessary copies.
  - **Action extensions** let users manipulate or view content within the context of another app. For example, users can use an action to translate text from another language right in Safari.
  - **Custom Keyboard extensions** provide keyboards beyond the ones already built into iOS. Managed Open In can prevent unauthorized keyboards from appearing in your corporate apps.
  - **Today extensions,** also known as Widgets, are used to deliver glanceable information in the Today view in the Notification Center. This becomes a great way for users to get immediate, up-to-date information from an app, with simplified interactions that launch into the full app for more information.
  - **Share extensions** give users a convenient way to share content with other entities, such as social sharing websites or upload services. For example, in an app that includes a Share button, users can choose a Share extension that represents a social sharing website, then use it to post a comment or other content.

Flexible Management Options

Apple's management framework is flexible and offers a balanced approach to the way you manage user-owned as well as company-owned devices in your enterprise. When you use a third-party MDM solution with iOS, your device management options are on a continuum that ranges from applying a highly open methodology to getting as granular as needed.

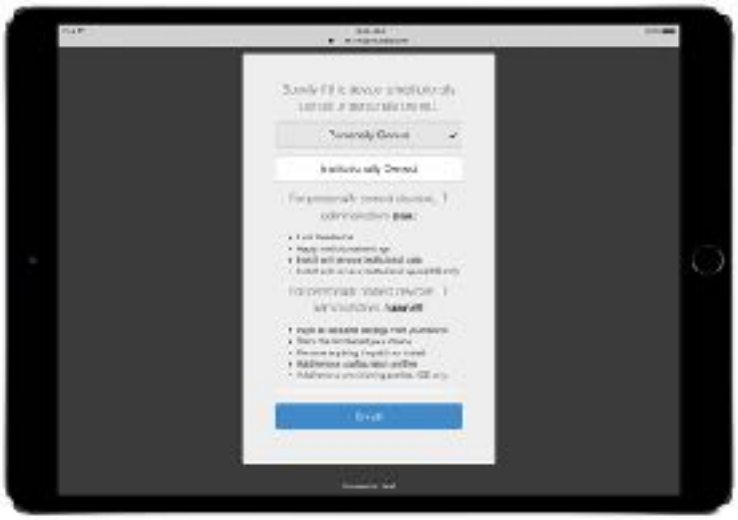
Ownership models

Depending on the device ownership model—or models—in your organization, you'll manage devices and apps differently. The two ownership models for iOS devices that are commonly used in the enterprise are user owned and organization owned.

User-owned devices

With a user-owned deployment, iOS offers personalized setup by users and transparency around how devices are configured, along with the assurance that users' personal data won't be accessed by your organization.

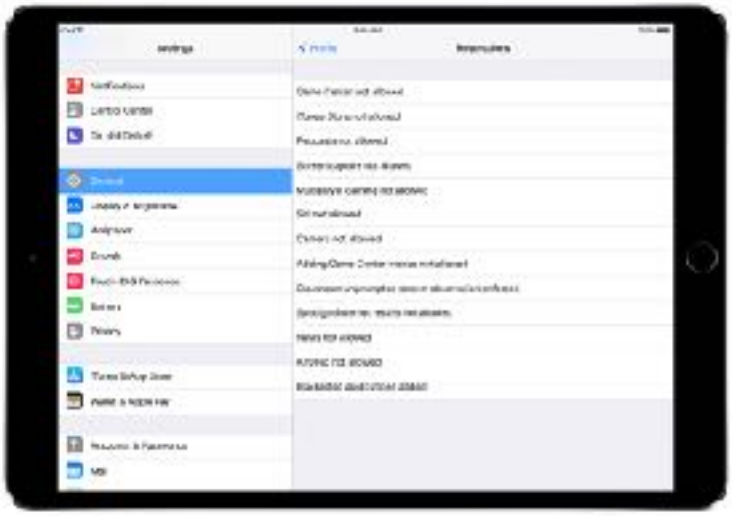
- **Opt-in and opt-out enrollment.** When devices are purchased and set up by the users—commonly referred to as BYOD—you can still provide access to corporate services such as Wi-Fi, mail, and calendar. Users simply opt in to enroll in your organization's MDM solution. When users enroll in MDM for the first time on an iOS device, they are provided with information about what the MDM server can access on their devices and the features it will configure. This provides transparency to users about what is being managed, and establishes trust between you and the users. It's important to let your users know that if at any time they are not comfortable with this management, they can opt out of the enrollment by removing the management profile from their device. When they do, all corporate accounts and apps installed by MDM are removed.



Third-party MDM solutions typically offer a user-friendly interface for employees so they feel comfortable opting in during enrollment.*

*Screen image courtesy of Jamf.

- **Greater transparency.** Once users are enrolled in MDM, employees can easily view in Settings which apps, books, and accounts are being managed and which restrictions have been implemented. All enterprise settings, accounts, and content installed by MDM are flagged by iOS as "managed."



The user interface for configuration profiles in Settings show users exactly what has been configured on their device.

- **User privacy.** While an MDM server lets you interact with iOS devices, not all settings and account information are exposed. You can manage corporate accounts, settings, and information provisioned via MDM, but the user's personal accounts cannot be accessed. In fact, the same features that keep data secure in corporate-managed apps also protect a user's personal content from entering the corporate data stream.

  The following examples show what a third-party MDM server can and cannot see on a personal iOS device:

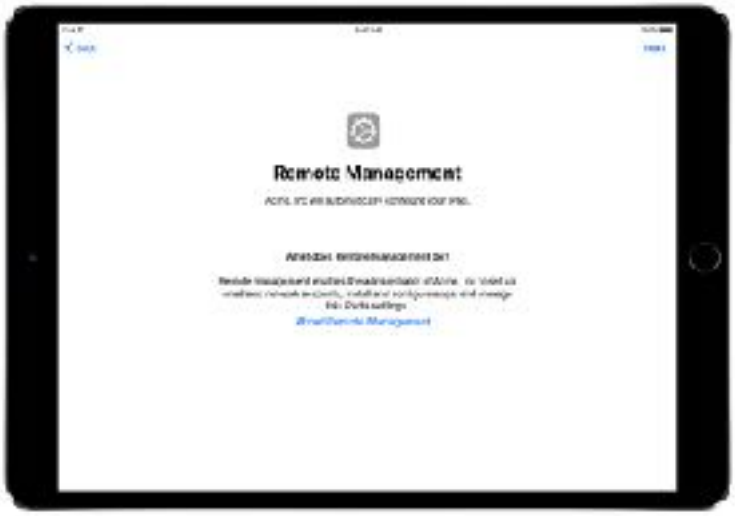
MDM can see:	MDM cannot see personal data such as:
Device name	Personal or work mail, calendars, contacts
Phone number	SMS or iMessages
Serial number	Safari browser history
Model name and number	FaceTime or phone call logs
Capacity and space available	Personal reminders and notes
iOS version number	Frequency of app use
Installed apps	Device location

- **Personalizing devices.** Businesses have found that allowing users to personalize a device with their own Apple ID leads to greater levels of ownership and responsibility among users, and their productivity increases because they're now able to choose which apps and content they need to best accomplish their jobs.

Organization-owned devices

With an organization-owned deployment, you can provide a device to each user, referred to as a personally enabled deployment, or another option is to rotate devices among users, referred to as a nonpersonalized deployment. iOS features such as automated enrollment, lockable MDM settings, device supervision, and always-on VPN ensure that devices are configured based on your organization's specific requirements, providing increased control while ensuring that corporate data is protected.

- **Automated enrollment.** The Device Enrollment Program (DEP) allows you to automate MDM enrollment during the initial setup of the iPhone and iPad devices and Mac systems that your organization owns. You can make the enrollment mandatory and nonremovable. You can also put devices into supervised mode during the enrollment process, and allow users to skip some of the basic setup steps.



With DEP, your MDM solution will automatically configure your iOS devices during the Setup Assistant.

- **Supervised devices.** Supervision provides additional management capabilities for iOS devices owned by your organization. These include the ability to enable a web filter via a global proxy to ensure that the users' web traffic stays within the organization's guidelines, prevent users from resetting their device to factory defaults, and much more. By default, all iOS devices are unsupervised. Use DEP to enable supervised mode automatically, or you can use Apple Configurator 2 to enable supervision manually.

Even if you don't plan to use any supervised-only features now, consider supervising your devices when you set them up, enabling you to take advantage of supervised-only features in the future. Otherwise, you'll need to wipe devices that have already been deployed. Supervision isn't about locking down a device; rather, it makes company-owned devices better by extending management capabilities. In the long run, supervision provides even more options for your enterprise.

For a complete list of supervised settings, see the iOS Deployment Reference.

Restrictions

iOS supports the following categories of restrictions, which you can configure over the air to meet the needs of your organization, without impacting users:

- AirPrint
- App installation
- App usage
- Classroom app
- Device
- iCloud
- Profile Manager user and user group restrictions

- Safari
- Security and privacy settings
- Siri

The following categories also have options that can be configured by your MDM solution:

- Automated MDM Enrollment settings
- Setup Assistant screens

Additional management capabilities

Querying devices

In addition to configuring devices, an MDM server has the ability to query devices for a variety of information, such as details on devices, network, applications, and compliance and security data. This information helps ensure that devices continue to comply with required policies. The MDM server determines the frequency at which it gathers information.

The following are examples of information that can be queried on an iOS device:

- Device details (name)
- Model, iOS version, serial number
- Network information
- Roaming status, MAC addresses
- Installed applications
- App name, version, size
- Compliance and security data
- Installed settings, policies, certificates
- Encryption status

Management tasks

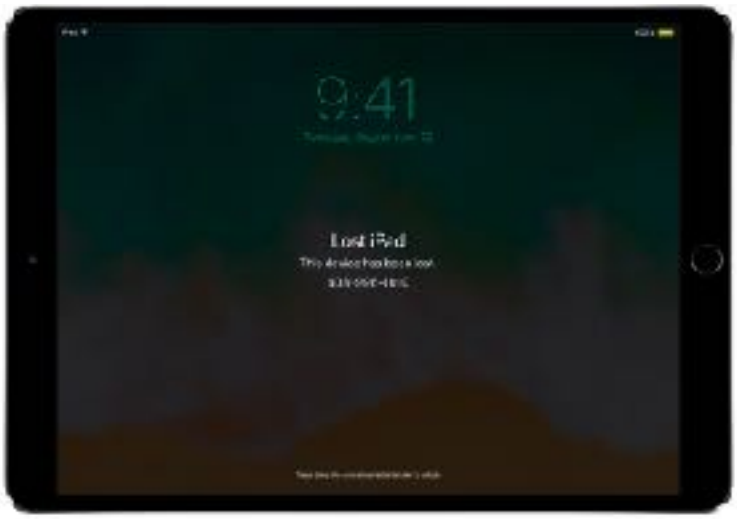
When a device is managed, an MDM server may perform a wide variety of administrative tasks, including changing configuration settings automatically without user interaction, performing an iOS update on passcode-locked devices, locking or wiping a device remotely, or clearing the passcode lock so users can reset forgotten passwords. An MDM server may also request an iOS device to begin AirPlay mirroring to a specific destination or end a current AirPlay session.

Lost Mode

With iOS 9.3 or later, your MDM solution can place a supervised device in Lost Mode remotely. This action locks the device and allows a message with a phone number to be displayed on the Lock screen.

With Lost Mode, supervised devices that are lost or stolen can be located, because MDM remotely queries for their location the last time they were online. Lost Mode doesn’t require Find My iPhone to be enabled.

If MDM remotely disables Lost Mode, the device is unlocked and its location is collected. To maintain transparency, the user is notified that Lost Mode is turned off.



When MDM puts a missing device in Lost Mode, it locks the device, allows messages to be displayed onscreen, and determines its location.

Activation Lock

With iOS 7.1 or later, use MDM to enable Activation Lock when a user turns on Find My iPhone on a supervised device. This allows your organization to benefit from the theft-deterrent functionality of Activation Lock, while still allowing you to bypass the feature if, for instance, a user leaves your organization without first removing Activation Lock using their Apple ID.

Your MDM solution can retrieve a bypass code and permit the user to enable Activation Lock on the device based on the following:

- If Find My iPhone is turned on when your MDM solution allows Activation Lock, Activation Lock is enabled at that point.
- If Find My iPhone is turned off when your MDM solution allows Activation Lock, Activation Lock is enabled the next time the user activates Find My iPhone.

Summary

The iOS management framework gives you the best of both worlds: IT is able to configure, manage, and secure devices and control the corporate data flowing through them, while at the same time users are empowered to do great work with the devices they love to use.