



Overview

iOS Deployment

Contents

[Overview](#)

[Ownership Models](#)

[Deployment Steps](#)

[Support Options](#)

[Summary](#)

Overview

iPhone and iPad can transform your business and how your employees work. They can significantly boost productivity and give your employees the freedom and flexibility to work in new ways, whether in the office or on the go. Embracing this modern way of working leads to benefits across the entire organization. Users have better access to information, so they feel empowered and are able to creatively solve problems. By supporting iOS, IT departments are viewed as shaping the business strategy and solving real-world problems, rather than just fixing technology and cutting costs. Ultimately everyone benefits, with an invigorated workforce and new business opportunities everywhere.

Setting up and deploying iPhone and iPad throughout your business has never been easier. With Apple Business Manager and a third-party mobile device management solution, your organization can easily deploy iOS devices and apps at scale.

- Mobile device management (MDM) allows you to configure and manage devices, and wirelessly distribute and manage apps.
- Apple Business Manager automates enrollment of Apple devices into your MDM solution to streamline deployment with zero-touch configuration for IT.
- Apple Business Manager also lets you purchase apps and books in bulk and distribute them to users wirelessly.

This document offers guidance on deploying iOS devices in your organization and helps you create a deployment plan that best suits your environment. These programs and tools, described in the Deployment Steps section of this overview, are covered in greater detail in the online iOS Deployment Reference:

help.apple.com/deployment/ios

Ownership Models

Evaluating ownership models and choosing the one that's right for your organization is an important first step to deployment. There are several ways to approach deployment, depending on who owns the device. Start by identifying what's best for your organization.

Two ownership models for iOS devices are commonly used in the enterprise:

- Organization owned
- User owned

While most organizations have a preferred model, you might encounter multiple models in your environment. For example, a corporate office might deploy a user-owned strategy by allowing employees to set up a personal iPad, while keeping corporate resources protected and managed without impacting the user's personal data and apps. However, the corporation's retail stores might deploy an organization-owned strategy that allows several employees to share iOS devices to process customer transactions.

Exploring these models will help you identify the best choices for your unique environment. Once you've identified the right model for your organization, your team can explore Apple's deployment and management capabilities in detail.

Organization-owned devices

With an organization-owned model, you can purchase devices from Apple or a participating Apple Authorized Reseller or carrier. In this case, you can provide a device to each user (a personally enabled deployment) or rotate devices among users (a nonpersonalized deployment). By using a combination of these models, key technologies from Apple, and an MDM solution, you can fully automate device setup and configuration.

Personally enabled. When using a personally enabled strategy, you can have each user choose their own device and enroll it with an MDM solution that provides organizational settings and apps over the air. For devices purchased directly from Apple or participating Apple Authorized Resellers or carriers, you can also take advantage of Apple Business Manager to automatically enroll new devices into your MDM solution. Once configured, these devices can be personalized by their user with their own apps and data, in addition to any corporate account or apps provided by your organization.

Nonpersonalized. When devices are shared by several people or used for a single purpose (for example, in a restaurant or a hotel), IT administrators typically configure and manage them centrally rather than relying on an individual user to perform the setup. With a nonpersonalized device deployment, users generally aren't permitted to install apps or save any personal data on the device. The following chart illustrates the actions required by both the administrator and the user during each step of an organization-owned strategy. Unless otherwise indicated, actions serve both *personally enabled* and *nonpersonalized* deployments.

	Administrator	User
Prepare	<ul style="list-style-type: none"> Evaluate your infrastructure Select an MDM solution Enroll in Apple Business Manager 	<ul style="list-style-type: none"> No user action necessary
Set up	<ul style="list-style-type: none"> Configure devices Distribute apps and books 	<ul style="list-style-type: none"> No user action necessary
Deploy	<ul style="list-style-type: none"> Distribute devices <p>Personally enabled only</p> <ul style="list-style-type: none"> Allow users to personalize 	<p>Personally enabled only</p> <ul style="list-style-type: none"> Download and install apps and books Use Apple ID, iTunes Store, and iCloud accounts, if applicable <p>Nonpersonalized only</p> <ul style="list-style-type: none"> No user action necessary
Manage	<ul style="list-style-type: none"> Administer devices Deploy and manage additional content 	<p>Personally enabled only</p> <ul style="list-style-type: none"> Discover additional apps to use <p>Nonpersonalized only</p> <ul style="list-style-type: none"> No user action necessary

User-owned devices

When devices are purchased and set up by the user—in what's commonly referred to as a BYOD, or bring-your-own-device deployment—you can still provide access to corporate services such as Wi-Fi, mail, and calendars with MDM. Users must opt in to enroll in your organization's MDM solution.

BYOD. A BYOD deployment allows users to set up and configure their own devices. Users can enroll their devices into your organization's MDM solution to gain access to corporate resources, configure various settings, install a configuration profile, or install corporate apps.

An advantage of using MDM to enroll personal devices is that it allows corporate resources and data to be managed in a way that is secure, yet also respectful of the user's personal privacy, data, and apps. IT can enforce settings, monitor corporate compliance, and remove corporate data and apps, while leaving personal data and apps on each user's device intact.

The following chart illustrates the actions required by both the administrator and the user during each step of a user-owned deployment.

	Administrator	User
Prepare	<ul style="list-style-type: none">• Evaluate your infrastructure• Select an MDM solution• Enroll in Apple Business Manager	<ul style="list-style-type: none">• Use Apple ID, iTunes Store, and iCloud accounts, if applicable
Set up	<ul style="list-style-type: none">• Configure devices• Distribute apps and books	<ul style="list-style-type: none">• Opt in to company's MDM solution• Download and install apps and books
Deploy	<ul style="list-style-type: none">• No administrator action necessary	<ul style="list-style-type: none">• No user action necessary
Manage	<ul style="list-style-type: none">• Administer devices• Deploy and manage additional content	<ul style="list-style-type: none">• Discover additional apps to use

Deployment Steps

This section provides a more detailed look at each of the four steps for deploying devices and content: preparing the environment, setting up devices, deploying them, and managing them. The steps you use will depend on whether the organization or the user owns the devices.

1. Prepare

After identifying the right deployment model for your organization, follow these steps to lay the groundwork for deployment; you can take these actions even before you have your devices in hand.

Evaluate your infrastructure

iPhone and iPad integrate seamlessly into most standard enterprise IT environments. It's important to assess your existing network infrastructure to make sure your organization takes full advantage of everything that iOS offers.

Wi-Fi and networking

Consistent and dependable access to a wireless network is critical to setting up and configuring iOS devices. Confirm that your company's Wi-Fi network can support multiple devices with simultaneous connections from all your users. You might need to configure your web proxy or firewall ports if devices are unable to access Apple's activation servers, iCloud, or the iTunes Store. Apple and Cisco have also optimized how iPhone and iPad communicate with a Cisco wireless network, paving the way for other advanced networking features such as fast roaming and Quality of Service (QoS) optimization for apps.

Evaluate your VPN infrastructure to make sure users are able to securely access company resources remotely via their iOS devices. Consider using the VPN On Demand or Per-App VPN feature of iOS so that a VPN connection is initiated only when needed. If you plan to use Per-App VPN, make sure your VPN gateways support these capabilities and you purchase sufficient licenses to cover the appropriate number of users and connections.

You should also make sure that your network infrastructure is set up to work correctly with Bonjour, Apple's standards-based, zero-configuration network protocol. Bonjour enables devices to find services on a network automatically. iOS devices use Bonjour to connect to AirPrint-compatible printers and AirPlay-compatible devices, such as Apple TV. Some apps also use Bonjour to discover other devices for collaboration and sharing.

For more detail on Wi-Fi and networking for enterprise deployments, see the iOS Deployment Reference: help.apple.com/deployment/ios

Learn more about Bonjour:
apple.com/support/bonjour

Mail, contacts, and calendars

If you use Microsoft Exchange, verify that the ActiveSync service is up to date and configured to support all users on the network. If you're using the cloud-based Office 365, ensure that you have sufficient licenses to support the anticipated number of iOS devices that will be connected. iOS also supports Office 365 modern authentication leveraging OAuth 2.0 and multi-factor authentication. If you don't use Exchange, iOS works with standards-based servers, including IMAP, POP, SMTP, CalDAV, CardDAV, and LDAP.

Content Caching

An integrated feature of macOS High Sierra or later, Content Caching stores a local copy of frequently requested content from Apple servers, helping to minimize the amount of bandwidth needed to download content on your network. Content Caching speeds up the download and delivery of software through the App Store, the Mac App Store, the iTunes Store, and Apple Books.

It can also cache software updates for faster downloading to iOS devices. Content Caching includes the tethered caching service, which allows a Mac to share its Internet connection with many iOS devices connected via USB.

Learn more about Content Caching:

support.apple.com/HT208025

Learn more about tethered caching:

support.apple.com/HT207523

iTunes support

iTunes isn't required for devices using iOS 5 or later, but you might want to support it so users can activate devices, sync media, or back up their devices to a computer.

iTunes supports several deployment configuration options that are appropriate for enterprise use, including disabling access to explicit content, defining which network services users can access within iTunes, and enforcing encrypted backups.

Select an MDM solution

The Apple management framework for iOS gives organizations the ability to securely enroll devices in the corporate environment, wirelessly configure and update settings, monitor policy compliance, deploy apps and books, and remotely wipe or lock managed devices. These management features are enabled by third-party MDM solutions.

A variety of third-party MDM solutions are available to support different server platforms. Each solution offers different management consoles, features, and pricing. Before choosing a solution, review the resources listed below to evaluate which management features are most relevant to your organization. In addition to third-party MDM solutions, a solution from Apple is available called Profile Manager, a feature of macOS Server.

Learn more about managing devices and corporate data on iOS:

[images.apple.com/business/resources/docs/
Managing_Devices_and_Corporate_Data_on_iOS.pdf](https://images.apple.com/business/resources/docs/Managing_Devices_and_Corporate_Data_on_iOS.pdf)

Learn more about Profile Manager:

www.apple.com/macos/server/features/#profile-manager

Enroll in Apple Business Manager

Apple Business Manager is a new place for IT teams to automate device deployment, purchase and distribute content, and manage roles in their organizations. Working seamlessly with your mobile device management (MDM) solution, Apple Business Manager makes it easy to enroll devices, deploy content, and delegate administrative privileges.

The Device Enrollment Program (DEP) and the Volume Purchase Program (VPP) are seamlessly integrated into Apple Business Manager, so now you can bring together everything needed to deploy iOS devices, Mac computers, and Apple TV in your organization.

Devices

Device enrollment is now part of Apple Business Manager, giving you a fast, streamlined way to deploy corporate-owned Apple devices.

- Automatically enroll devices in MDM without having to physically touch or prep each device before users get them. This ensures that all users receive your organization's configurations immediately when they activate their device.
- Simplify the setup process for users by removing specific steps in Setup Assistant, so users are up and running quickly. And by using supervision, a higher level of device management options become available for iOS and tvOS devices, including non-removable MDM.
- More easily manage default MDM servers by setting a default server that's based on device type. And you can now manually enroll iOS devices and Apple TV using Apple Configurator 2, regardless of how you acquired them.

Content

The Apps and Books section of Apple Business Manager enables organizations to more easily buy content in volume. Whether your workforce uses iPhone, iPad, or Mac, you can provide great content that's ready for work with flexible and secure distribution options. Note: Book purchases in Apple Business Manager are not available in certain countries. To learn which features and purchasing methods are available where, visit support.apple.com/HT207867.

- Purchase apps, books, and custom apps in bulk. Easily transfer app licenses between locations and share licenses between purchasers within the same location. And see a unified listing of purchase history, including the current number of licenses in use via MDM.

Deployment Steps

- Distribute apps and books directly to managed devices or authorized users, and easily keep track of what content has been assigned to which user or device. With managed distribution, you control the entire distribution process, while retaining full ownership of apps. And apps that aren't needed by a device or user can be revoked and reassigned within your organization.
- Pay using multiple payment options, including credit cards and purchase orders. Organizations can buy Volume Credit (where available) directly from Apple or from an Apple Authorized Reseller in specific dollar amounts, which is delivered electronically to the account holder as store credit.
- Distribute an app to devices or users in any country where the app is available, enabling multinational distribution. Developers can make their apps available in multiple countries through the standard App Store publishing process.

Roles

Apple Business Manager allows you to create accounts that your organization owns and manages for additional administrators. It also introduces some changes to the roles you assign to your users.

- Add additional accounts for managing devices or content, delegate privileges, and easily transfer responsibility if someone leaves the organization.
- Designate roles within Apple Business Manager on a granular level, so you can assign privileges for managing devices or content to specific people or locations.
- Deactivate and delete user accounts so that the selected users can't sign in.

In Apple Deployment Programs, the highest level of administrative access was an Agent. The Agent was able to accept terms and conditions on behalf of your organization. This role is now called Administrator. Your organization can have up to five Administrators in Apple Business Manager.

Apple Deployment Programs included Admins for DEP and VPP. Admins are now called Managers in Apple Business Manager. Upon upgrading, DEP Admins are converted to Device Managers and VPP Admins are converted to Content Managers. Any Apple Deployment Programs Admin who was able to create other Admins becomes a People Manager.

A user can have multiple roles in Apple Business Manager. Any of your users who were Admins for more than one program will be assigned all roles that apply in Apple Business Manager. The Administrator can add, remove, or change Manager roles after you upgrade. People Managers can also make changes to other Manager roles, but not to Administrators.

When your previous Agent and Admins sign in to Apple Business Manager for the first time, their Apple IDs are converted to Managed Apple IDs. If their accounts weren't previously set up with two-factor authentication, they will now be required to set up two-factor authentication.

Managed Apple IDs are for use primarily by IT administrators to manage functionality within Apple Business Manager. They shouldn't be used for services like iCloud or by standard employees who don't manage functions in Apple Business Manager.

Learn more about the Apple Business Manager:

www.apple.com/business/it

Enroll in the Apple Developer Enterprise Program

Develop in-house iOS apps for use by your company using the Apple Developer Enterprise Program. This program offers a complete and integrated process for developing, testing, and distributing your iOS apps to employees within your organization. In-house apps are not submitted to the App Store and are not reviewed, approved, or hosted by Apple.

Distribute your in-house apps either by hosting your app on a simple internal web server or by using a third-party MDM solution. The benefits of managing in-house apps with MDM include the ability to configure apps remotely; manage versions; configure single sign-on; set policies for network access, such as Per-App VPN; and control which apps can export documents. Your specific requirements, infrastructure, and level of app management will dictate which solution makes the most sense for you.

Learn more about the Apple Developer Enterprise Program:

developer.apple.com/programs/enterprise

2. Set up

In this step, configure your devices and distribute your content by leveraging Apple Business Manager, an MDM solution, or optionally Apple Configurator 2. There are several ways to approach your setup, depending on who owns the devices and your preferred type of deployment.

Configure your devices

Multiple options are available for configuring user access to corporate services. IT can set up devices by distributing configuration profiles. Additional configuration options are available for supervised devices.

Configuring devices with MDM

Once your devices are securely enrolled into an MDM server, management is enabled using configuration profiles—an XML file containing configuration information to an iOS device. These profiles automate the configuration of settings, accounts, restrictions, and credentials. They can be delivered from your MDM solution over-the-air, which is ideal for low-touch configuration of multiple devices. Profiles can also be sent as an email attachment, downloaded from a web page, or installed on devices through Apple Configurator 2.

- **Organization-owned devices.** Use Apple Business Manager to enable automatic MDM enrollment of your users' devices upon activation. All iOS devices added to Apple Business Manager are always supervised with mandatory MDM enrollment.

- **User-owned devices.** Employees can decide whether or not to enroll their device in MDM. And to disassociate from MDM at any time, they simply remove the configuration profile from their device, which also removes corporate data and settings. But you should consider incentives for users to remain managed. For example, you might require users to enroll in MDM to get Wi-Fi network access—using your MDM solution to automatically provide the wireless credentials.

Once a device is enrolled, an administrator can initiate an MDM policy, option, or command. Then the iOS device receives notification of the administrator's action via the Apple Push Notification service (APNs), so it can communicate directly with its MDM server over a secure connection. With a network connection, devices can receive APNs commands anywhere in the world. However, no confidential or proprietary information is transmitted via APNs.

Configuring devices with Apple Configurator 2 (optional)

For local initial deployments of multiple devices, organizations can use Apple Configurator 2. This free macOS application allows you to connect iOS devices to a Mac computer over USB and update iOS devices to the latest version of iOS, configure device settings and restrictions, and install apps and other content. After initial setup, you can continue to manage everything over the air using MDM.

Apple Configurator 2 has a user interface focused on your devices and the discrete tasks you want to perform on them. The application integrates with Apple Business Manager, enabling devices to automatically enroll in MDM using your organization's settings. Custom workflows can be created within Apple Configurator 2 using Blueprints to combine discrete tasks.

Learn more about Apple Configurator 2:

support.apple.com/apple-configurator

Supervised devices

Supervision provides additional management capabilities for iOS devices owned by your organization, allowing restrictions such as disabling AirDrop or placing the device in Single App Mode. It also provides 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 many more. By default, all iOS devices are nonsupervised. You can use Apple Business Manager to enable supervision or you can manually enable supervision using Apple Configurator 2.

Even if you don't plan to use any supervised-only features now, consider supervising your devices when you set them up, so you can 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 enhances company-owned devices 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](#).

Distribute apps and books

Apple offers extensive programs to help your organization take advantage of the great apps and content available for iOS. With these capabilities, you can distribute apps and books purchased through Apple Business Manager or apps you've developed in-house to devices and users, so your users have everything they need to be productive. At the time of purchase, you'll need to determine your distribution method: managed distribution or redemption codes.

Managed distribution

With managed distribution, use your MDM solution or Apple Configurator 2 to manage apps and books purchased from the Apple Business Manager store in any country where the app is available. To enable managed distribution, you must first link your MDM solution to your Apple Business Manager account using a secure token. Once you're connected to your MDM server, you can assign Apple Business Manager apps and books, even if the App Store on the device is disabled.

- **Assign apps to devices.** Using your MDM solution or Apple Configurator 2, assign apps directly to devices. This method saves several steps in the initial rollout, making your deployment significantly easier and faster, while giving you full control over managed devices and content. After an app is assigned to a device, the app is pushed to that device via MDM and no user invitation is required. Anyone using that device has access to the app.
- **Assign apps and books to users.** An alternative method is to use your MDM solution to invite users to download apps and books through an email or a push notification message. To accept the invitation, users sign in on their devices with a personal Apple ID. The Apple ID is registered with the Apple Business Manager service, but remains completely private and not visible to the administrator. Once users agree to the invitation, they're connected to your MDM server so they can start receiving assigned apps and books. Apps are automatically available for download on all of a user's devices, with no additional effort or cost to you.

When apps you've assigned are no longer needed by a device or a user, they can be revoked and reassigned to different devices and users, so your organization retains full ownership and control of purchased apps. However, once distributed, books remain the property of the recipient and cannot be revoked or reassigned.

Redemption codes

You can also distribute content using redemption codes. This is helpful when your organization cannot use MDM on the end user's device. For example, in a franchise business scenario. This method permanently transfers an app or a book to the user who redeems the code. Redemption codes are delivered in a spreadsheet format. A unique code is provided for each app or book in the quantity purchased. Each time a code is redeemed, the spreadsheet is updated in the Apple Business Manager store, allowing you to view the number of redeemed codes at any time. Distribute the codes using MDM, Apple Configurator 2, email, or an internal website.

Installing apps and content with Apple Configurator 2 (optional)

In addition to basic setup and configuration, Apple Configurator 2 can be used to install apps and content for devices you want to set up on behalf of the user. For personally enabled deployments, you can preinstall apps, saving time and network bandwidth. And for nonpersonalized deployments, you can fully set up your devices all the way to the Home screen. When you configure devices with Apple Configurator 2, you can install App Store apps, in-house apps, and documents. App Store apps require Apple Business Manager. Documents are available for apps that support iTunes file sharing. To review or retrieve documents from iOS devices, connect them to a Mac running Apple Configurator 2.

3. Deploy

iOS makes it simple for employees to start using their devices right out of the box, without requiring help from IT.

Distribute your devices

Once devices have been prepared and set up in the first two steps, they are ready for distribution. For personally enabled deployments, give devices to users who can use the streamlined Setup Assistant for further personalization and to finalize setup. For nonpersonalized deployments, distribute devices to your shift employees or place devices in kiosks designed to charge and secure the devices.

Setup Assistant

Out of the box, users can activate their devices, configure basic settings, and start working right away with Setup Assistant in iOS. After initial setup, users can also customize their personal preferences, such as language, location, Siri, iCloud, and Find My iPhone. Devices that are enrolled in Apple Business Manager are automatically enrolled in MDM right within the Setup Assistant.

Allow users to personalize

For personally enabled and BYOD deployments, allowing users to personalize their devices with their own Apple IDs increases productivity, because users choose which apps and content will allow them to best accomplish their tasks and goals. Corporate data remains separate from personal data in iOS.

Apple ID

An Apple ID is an identity that's used to log in to various Apple services such as FaceTime, iMessage, the iTunes Store, the App Store, Apple Books, and iCloud. These services give users access to a wide range of content for streamlining business tasks, increasing productivity, and supporting collaboration.

To get the most out of these services, users should use their own Apple IDs. Users who don't have an Apple ID can create one even before they receive a device. Setup Assistant also enables users to create a personal Apple ID if they don't already have one. Users do not need a credit card to create an Apple ID.

Learn how to create an Apple ID without a credit card:

support.apple.com/ht204034

Sign up for an Apple ID:

support.apple.com/ht204316

iCloud

iCloud allows users to automatically sync documents and personal content—such as contacts, calendars, documents, and photos—and keep them up to date between multiple devices. Users can also back up an iOS device automatically when connected to Wi-Fi, and use Find My iPhone to locate a lost or stolen iPhone, iPad, iPod touch, or Mac.

Some services—such as Photo Stream, iCloud Keychain, iCloud Drive, and iCloud Backup—can be disabled through the use of restrictions, either entered manually on the device or set via configuration profiles. In addition, an MDM solution can prevent managed apps from being backed up to iCloud. This capability gives users the benefits of using iCloud for personal data while preventing corporate information from being stored in iCloud. Data from corporate accounts, such as Exchange, or data stored within enterprise in-house apps are not backed up to iCloud.

Learn more about iCloud:

www.apple.com/icloud

4. Manage

Once your users are up and running, a wide range of administrative capabilities are available for managing and maintaining your devices and content over time.

Administer your devices

A managed device can be administered by the MDM server through a set of specific tasks. These tasks include querying devices for information, as well as initiating management tasks that allow you to manage devices that are out of policy, lost, or stolen.

Queries

An MDM server can query devices for a variety of information, including hardware details such as serial number, device UDID, or Wi-Fi MAC address, as well as software details such as the iOS version and a detailed list of all apps installed on the device. This information can be used by your MDM solution to maintain up-to-date inventory information, make informed management decisions, and automate management tasks like ensuring that users maintain the appropriate set of apps.

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.

Managed Software Updates

You can prevent users from manually updating a supervised 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 iOS update. However, you can change the default number of days you prevent updates, anywhere from one to 90 days. You can also schedule software updates on supervised devices using your mobile device management (MDM) solution.

Lost Mode

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.

Activation Lock

With iOS 7.1 or later, you can 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 a user is unable to authenticate with their Apple ID.

Deploy and manage additional content

Organizations often need to distribute apps so their users are productive. At the same time, organizations need to control how apps connect to internal resources or how data is securely handled when a user transitions out of the organization—all while coexisting alongside the user's personal apps and data.

Internal app portals

Most MDM servers offer internal app portals as part of their solution or you can create your own internal app portal for your employees, where they can easily find apps for their iOS devices. In-house apps, App Store app URLs or Apple Business Manager codes, or custom B2B Apple Business Manager codes can be linked from this portal, making it a single destination for users. You can manage and secure this site centrally. An internal app portal makes it easy for employees to find approved resources they need without having to contact IT.

Managed content

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

- **Managed apps.** In iOS, managed apps allow an organization to distribute free, paid, and enterprise apps over the air using MDM, while also providing the right balance of protecting corporate data and respecting user privacy. Managed apps can be removed remotely by an MDM server or when users remove their own devices from MDM. Removing the app also removes the data associated with the app. If an app remains assigned to a user through Apple Business Manager, or if the user redeemed an app code using a personal Apple ID, the app can be downloaded again from the App Store, but it will not be managed by MDM.
- **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.
- **Managed books and documents.** MDM tools, books, ePub books, and PDF documents can be automatically pushed to user devices, so employees always have what they need. At the same time, managed books can be shared only with other managed apps or mailed using managed accounts. When the materials are no longer necessary, they can be removed remotely. Books purchased through Apple Business Manager can be distributed through managed book distribution, but cannot be revoked and reassigned. A book already purchased by the user cannot be managed unless the book is explicitly assigned to the user by Apple Business Manager.

Managed app configuration

App developers can identify app settings and capabilities that can be enabled when installed as a managed app. Install these configuration settings before or after the managed app is installed. For example, IT could establish a set of default preferences for a Sharepoint app, so the user doesn't need to manually configure server settings.

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

Learn more about the AppConfig Community:

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 users' personal apps and cloud services.

- **Managed Open In.** Open In management uses a set of restrictions that prevents 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.
- **Single App Mode.** This setting will limit the iOS device to a single app and is ideal for kiosks or single purpose devices, such as a retail point of sale or hospital check-in device. Developers can also enable this functionality within their apps to allow apps to enter and exit Single App Mode autonomously.
- **Prevent backup.** This restriction prevents managed apps from backing up data to iCloud or iTunes. Disallowing backup prevents managed app data from being recovered if the app is removed via MDM but later reinstalled by the user.

Support Options

Apple provides a variety of programs and support options for iOS users and IT administrators.

AppleCare for Enterprise

For companies looking for complete coverage, AppleCare for Enterprise can help reduce the load on your internal help desk by providing technical support for employees over the phone, 24/7, with one-hour response times for top-priority issues. The program provides IT department-level support for all Apple hardware and software, as well as support for complex deployment and integration scenarios, including MDM and Active Directory.

AppleCare OS Support

AppleCare OS Support provides your IT department with enterprise-level phone and email support for iOS, macOS, and macOS Server deployments. It offers up to 24/7 support and an assigned technical account manager, depending on the level of support you purchase. With direct access to technicians for questions on integration, migration, and advanced server operation issues, AppleCare OS Support can increase your IT staff's efficiency in deploying and managing devices and resolving issues.

AppleCare Help Desk Support

AppleCare Help Desk Support provides priority telephone access to Apple's senior technical support staff. It also includes a suite of tools to diagnose and troubleshoot Apple hardware, which can help large organizations manage their resources more efficiently, improve response time, and reduce training costs. AppleCare Help Desk Support covers an unlimited number of support incidents for hardware and software diagnosis, as well as troubleshooting and issue isolation for iOS devices.

AppleCare for iOS device users

Every iOS device comes with a one-year limited warranty and complimentary telephone technical support for 90 days after the purchase date. This service coverage can be extended to two years from the original purchase date with AppleCare+ for iPhone, AppleCare+ for iPad, or the AppleCare Protection Plan (APP) for iPod touch. You can call Apple's technical support experts as often as you like with questions. Apple also provides convenient service options when devices need to be repaired. In addition, AppleCare+ for iPhone and AppleCare+ for iPad offer up to two incidents of accidental damage coverage, each subject to a service fee.

iOS Direct Service Program

As a benefit of AppleCare+ and the AppleCare Protection Plan, the iOS Direct Service Program enables your help desk to screen devices for issues without calling AppleCare or visiting an Apple Store. If necessary, your organization can directly order a replacement iPhone, iPad, iPod touch, or in-box accessory.

Learn more about AppleCare programs:

www.apple.com/support/professional

Summary

Whether your company deploys iOS devices to a group of users or across the entire organization, you have many options for easily deploying and managing devices. Choosing the right strategies for your organization can help your employees be more productive and accomplish their work in entirely new ways.

Learn more about integrating iOS into enterprise IT environments:

www.apple.com/business/products-platform

¹Some apps and books might not be available subject to country or region and developer opt-in. [See program and content availability.](#)

²Some features require a Wi-Fi connection. Some features are not available in all countries. For minimum and recommended system requirements for iCloud, visit support.apple.com/HT204230.

© 2018 Apple Inc. All rights reserved. Apple, the Apple logo, AirDrop, AirPlay, AirPrint, Apple TV, Bonjour, FaceTime, iMessage, iPad, iPhone, iPod touch, iTunes, Mac, macOS, and Siri are trademarks of Apple Inc., registered in the U.S. and other countries. tvOS is a trademark of Apple Inc. App Store, AppleCare, Apple Store, Apple Books, iCloud, iCloud Drive, iCloud Keychain, and iTunes Store are service marks of Apple Inc., registered in the U.S. and other countries. IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license. Other product and company names mentioned herein may be trademarks of their respective companies. Product specifications are subject to change without notice. This material is provided for information purposes only; Apple assumes no liability related to its use.