iOS and iPadOS Deployment Overview

Overview

Contents

iPhone and iPad, combined with iOS and iPadOS, enable employees to get their best work done from anywhere. And they allow IT departments to spend less time managing devices—empowering them to shape business strategy and focus on needs beyond fixing technology and cutting costs.

This document offers guidance on deploying iOS and iPadOS devices in your organization, and helps you lay the foundation for a deployment plan that best suits your environment.

These topics, including what's new in deploying with the latest iOS and iPadOS updates, are covered in greater detail in the online Apple Platform Deployment guide.

Ownership Models

These are the two ownership models for iOS and iPadOS devices that organizations commonly use:

- Organization-owned
- User-owned

Each model has its benefits, so it's important to choose the one that's best for your organization. While most organizations have a preferred model, you might use multiple models in your 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

In an organization-owned model, devices are purchased by your organization or a participating Apple Authorized Reseller or carrier. If a device is provided to each user, this is referred to as a one-to-one deployment. Devices can also be rotated among users, which is commonly referred to as a shared deployment. Shared iPad, an ownership model that enables multiple users to share an iPad device without sharing information, is an example of shared deployment. Organizations can use a combination of shared and one-to-one deployment models throughout their environments.

When using an organization-owned model, IT maintains a higher level of control with supervision and Automated Device Enrolment, which lets organizations configure and manage devices from the moment they're removed from the box.

Learn more about restrictions for supervised devices:
support.apple.com/guide/deployment/welcome/web

IT has more control when Apple devices are supervised.

- ✓ Configure accounts
- ✓ Configure global proxies
- ✓ Install, configure and remove apps
- ✓ Require a complex passcode
- ✓ Enforce all restrictions
- ✓ Access inventory of all apps
- ✓ Remotely erase the entire device
- ✓ Manage software updates
- ✓ Remove system apps
- ✓ Modify the wallpaper
- ✓ Lock into a single app
- ✓ Bypass Activation Lock
- ✓ Force Wi-Fi on
- ✓ Place device in Lost Mode

User-owned devices

In a user-owned model, users purchase, set up and configure the devices. These types of deployments are commonly referred to as BYOD, or bring your own device deployments. To use organizational services—such as Wi-Fi, mail and calendars—or to configure devices for specific education or business requirements, users typically enrol their devices in an organization's mobile device management (MDM) solution. They do this using an Apple feature called User Enrolment.

User Enrolment allows corporate resources and data to be managed securely while also respecting the user's privacy and personal data and apps. IT can enforce, access and manage specific functions, which are outlined in the table below.

To access corporate data on their devices, users leverage their Managed Apple IDs. A Managed Apple ID is part of the User Enrolment profile, and the user must successfully authenticate for enrolment to be completed. The Managed Apple ID can be used alongside the personal Apple ID that the user has already signed in with, and the two don't interact with each other. This creates data separation on the device. For organizations with iCloud storage space, a separate iCloud Drive will be created for all data managed under the Managed Apple ID.

Learn more about User Enrolment in MDM solutions:
support.apple.com/guide/deployment/welcome/web

MDM functions are limited on personal devices.

- ✓ Configure accounts
- ✓ Configure Per-App VPN
- ✓ Install and configure apps
- ✓ Require a passcode
- ✓ Enforce certain restrictions
- ✓ Access inventory of work apps
- ✓ Remove work data only
- ✗ Access personal information
- ✗ Access inventory of personal apps
- ✗ Remove any personal data
- ✗ Collect any logs on the device
- ✗ Take over personal apps
- ✗ Require a complex passcode
- ✗ Remotely wipe the entire device
- ✗ Access device location

Deployment Steps

This section provides an overview of the five 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 devices are owned by the organization or the users.

To view these steps in more detail, visit the online Apple Platform Deployment Guide.

1. Integration and setup

After identifying the right deployment model for your organization, it's important to lay the groundwork for deployment.

MDM solution. Apple's management framework for iOS and iPadOS gives organizations the ability to securely enrol 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.

Apple Business Manager. This web-based portal allows IT administrators to deploy iPhone, iPad, iPod touch, Apple TV and Mac all from one place. Apple Business Manager works seamlessly with your MDM solution, making it easy to automate device deployment, purchase apps and distribute content, and create Managed Apple IDs for employees.

Managed Apple IDs. Like personal Apple IDs, Managed Apple IDs are used to sign in to Apple devices and services—such as FaceTime, iMessage, the App Store, iCloud, iWork and Notes—giving users access to a wide range of content and features that can increase productivity and support collaboration. But Managed Apple IDs are owned by the organization, and they're an integral part of Apple device management. They allow your organization to manage things like password resets and role-based administration, and they have certain restricted settings.

Learn more about Managed Apple IDs:
support.apple.com/guide/apple-business-manager

Wi-Fi and networking. Apple devices have secure wireless network connectivity built in. Confirm that your company's Wi-Fi network can support multiple devices with simultaneous connections from all your users. And ensure that your network infrastructure is set up to work correctly with Bonjour, Apple's standards-based, zero-configuration network protocol. Bonjour enables devices to automatically find services on a network. iOS and iPadOS devices use Bonjour to connect to AirPrint-compatible printers and AirPlay-compatible devices, such as Apple TV. And some apps use Bonjour to discover other devices for collaboration and sharing.

Learn more about Wi-Fi and networking:
support.apple.com/guide/deployment/welcome/web

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

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

Mail, content and calendars. iPhone, iPad and Mac work with Microsoft Exchange, Office 365 and other popular email services, like Google Workspace, for instant access to push email, calendar, contacts and tasks over an encrypted SSL connection. 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 licences to support the anticipated number of iOS and iPadOS devices that will be connected. iOS and iPadOS also support Office 365 modern authentication leveraging OAuth 2.0 and multifactor authentication. If you don't use Exchange, iOS and iPadOS work with standards-based servers, including IMAP, POP, SMTP, CalDAV, CardDAV and LDAP.

2. Identity management

In addition to preparing your environment, IT teams will need to further lay the groundwork for deployment by choosing the way they'd like to manage authentication and authorization. This helps ensure that devices and data are kept secure.

Authentication. There are many methods of authentication. Using single sign-on and Apple services such as Managed Apple ID, iCloud, iMessage and more let users communicate securely, create documents online and back up personal data—all without compromising an organization's data. Each service uses its own security architecture, which ensures the following: secure handling of data (whether it's on an Apple device or in transit over a wireless network), protection of users' personal information, and threat protection against malicious or unauthorized access to information and services. MDM solutions can be used to restrict and manage access to specific services on Apple devices.

Learn more about single sign-on:
support.apple.com/guide/deployment/depfdbf18f55/1/web/1.0

Learn more about Kerberos single sign-on:
support.apple.com/guide/deployment/depe6a1cda64/1/web/1.0

Authorization. Authorization is different from authentication. Authentication proves who you are, whereas authorization defines what you are allowed to do. For example, this could be done by providing a user name and password to an IdP. In this example, the authority is your Identity Provider or Active Directory, the assertion is the user name and password, and the token is the data received after a successful sign in. Other assertions can be used including certificates, smart cards or other multi-factor devices.

Identity federation. Identity federation requires that domains are set up by administrators to trust each other and agree on the method to identify users. A common example is using your enterprise account to sign in to a cloud identity provider. IT teams can enable federation between Microsoft Azure Active Directory (Azure AD) and Apple Business Manager to streamline the creation of Managed Apple IDs for their organization, for example. The users will then use their existing Azure AD credentials to sign in to iCloud or on Apple devices associated with Apple Business Manager.

3. Deployment planning and provisioning

Once you've laid the groundwork, it's time to configure your devices and prepare to distribute your content. All ownership and deployment models work best when used with an MDM solution along with Apple Business Manager or Apple Configurator 2.

Automated Device Enrolment

This enrolment method is a fast, streamlined way to deploy corporate-owned Apple devices and enrol in MDM without having to physically touch or prepare each device. For end users, IT teams can simplify the setup process by streamlining steps in Setup Assistant, ensuring employees immediately receive the right configurations when their devices are activated. Only devices purchased directly from Apple or from participating Apple Authorized Resellers or carriers can be deployed through Automated Device Enrolment.

Device Enrolment

Devices can also be manually deployed through Apple Configurator 2 and your organization's MDM solution. Both corporate-owned and user-owned devices can be deployed through Device Enrolment. Devices that are managed manually behave like any other assigned device, with mandatory supervision and MDM enrolment. This deployment method is great for IT teams that will manage devices that weren't purchased directly from Apple or through participating Apple Authorized Resellers or carriers.

Learn more about Apple Configurator 2:
support.apple.com/apple-configurator

User Enrolment

User-owned devices can be configured and deployed through User Enrolment, which enables IT to protect corporate data without locking down the devices. Refer to the Ownership Models section for more information about User Enrolment.

Whether a device is owned by the organization or user, IT teams can retain control over the setup experience when distributing devices through Setup Assistant. Setup Assistant is configured by your MDM solution, and it enables users to start working on their devices right away.

After enrolling a device, an administrator can initiate an MDM policy, option or command; the management actions available for a device will vary depending on the supervision and enrolment method. The iOS or iPadOS device then receives notification of the administrator's action through the Apple Push Notification service (APNs) so that it can communicate directly with its MDM server over a secure connection. With a network connection, APNs can send commands to devices anywhere in the world. APNS doesn't, however, transmit any confidential or proprietary information.

4. Configuration management

Apple devices have a built-in, secure management framework that enables IT to manage devices using a wide range of administrative capabilities. This management framework can be broken down into four sections:

Configuration profiles

Configuration profiles consist of payloads that load settings and authorization information onto Apple devices. Configuration profiles automate the configuration of settings, accounts, restrictions and credentials. Depending on the MDM solution provider and integration with your internal systems, account payloads can be prepopulated with a user's name, mailing address and, where applicable, certificate identities for authentication and signing.

Restrictions

Restrictions enable you to enforce security policies and help users stay focused without locking down devices. Examples of restrictions include features like Managed Open In, which can prevent attachments or documents from managed sources from being opened in unmanaged destinations; Single App Mode, which limits the device to a single app; and Prevent Backup, which prevents managed apps from backing up data to iCloud or the device.

Management tasks

When a device is managed, an MDM server can perform a wide variety of administrative tasks, including changing configuration settings automatically without user interaction, performing a software update on a passcode-locked device, locking or wiping a device remotely, or clearing the passcode lock so a user can reset a forgotten password. An MDM server can also request an iPhone or iPad to begin AirPlay mirroring to a specific destination or to end a current AirPlay session. And you can prevent users from manually updating a supervised device over the air for up to 90 days. Software updates for supervised devices can also be scheduled using your MDM solution.

Queries

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

5. Content distribution

After enrollment, the administrator can now also use managed distribution. This allows the MDM solution or Apple Configurator 2 to manage all apps and books purchased from the Apple Business Manager store in any country where those apps and books are 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.

There are two types of content that can be distributed to users: managed apps, and managed books and documents. Managed apps can be deployed and removed by an MDM server or when users remove their own devices from MDM. Removing an app also removes the data associated with it. Managed books and documents can be automatically pushed to user devices, and they can only be shared with other managed apps or mailed using managed accounts. Managed documents can be removed automatically, but managed books can't be revoked or reassigned, even if they're assigned through Apple Business Manager.

The two ways that content can be distributed to users include:

Assigning apps to devices. You can use your MDM solution or Apple Configurator 2 to 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, it's pushed to that device through MDM and no user invitation is required. Anyone using that device has access to the app.

Assigning apps and books to users. The other 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 it 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.

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

Device Security

Apple builds advanced security into devices from the ground up. After devices are set up, IT teams can manage and protect corporate data thanks to built-in security features and additional controls made available through MDM. Common frameworks across apps enable configuration and ongoing management of settings.

Learn more about Apple platform security:
support.apple.com/guide/security/welcome/web

Protecting work data. IT can enforce and monitor security policies through MDM. For example, requiring a passcode on an iOS and iPadOS device automatically enables Data Protection, providing file encryption for the device. And MDM can be used to configure Wi-Fi and VPN and deploy certificates for added security.

MDM solutions allow device management at a granular level without the need for containers, keeping corporate data safe. With Managed Open In, IT can set restrictions to keep attachments or documents from being opened in unmanaged destinations.

Locking, locating and wiping. When a device goes missing, your corporate data doesn't have to go with it. For iOS and iPadOS devices, IT can remotely lock and erase all sensitive data to protect your company's information. For supervised iOS and iPadOS devices, IT can enable Lost Mode to see a device's location. IT also has the tools to manage corporate apps, which can be instantly removed from a device without erasing personal data.

Apps. Thanks to a common framework and controlled ecosystem, apps on Apple platforms are secure by design. Our developer programs verify the identity of every developer, and apps are verified by the system before they're launched on the App Store. Apple provides developers with frameworks for features—including signing, app extensions, entitlements and sandboxing—to ensure even greater levels of security.

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 display 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 to be enabled.

Activation Lock. You can use MDM to enable Activation Lock when a user turns on Find My on a supervised device. This lets your organization benefit from the theft-deterrent functionality of Activation Lock while allowing you to bypass the feature if a user is unable to authenticate with their Apple ID.

Support Options

Apple provides a variety of programs and support resources.

AppleCare for Enterprise

For companies looking for complete coverage, AppleCare for Enterprise can help reduce the load on your internal help desk. It provides 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 and iPadOS 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 and iPadOS devices.

AppleCare+ for iPad, AppleCare+ for iPhone and AppleCare+ for iPod touch

Every iOS and iPadOS 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 original purchase date with AppleCare+ for iPhone, AppleCare+ for iPad or AppleCare+ 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, the plans offer up to two incidents of accidental damage coverage, each subject to a service fee.

iOS Direct Service Program

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

Learn more about AppleCare programs:
apple.com/ca/support/professional

Summary and Resources

Whether your company deploys iPhone or iPad 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 about iOS and iPadOS deployment, management and security features:
support.apple.com/guide/deployment/welcome/web

Learn about Apple Business Manager:
support.apple.com/guide/apple-business-manager

Learn about Managed Apple IDs for business:
apple.com/ca/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Learn about Apple at Work:
apple.com/ca/business

Learn about IT features:
apple.com/ca/business/it

Learn about Apple platform security:
support.apple.com/guide/security/welcome/web

Browse available AppleCare programs:
apple.com/ca/support/professional

Discover Apple training and certification:
training.apple.com

Engage with Apple Professional Services:
consultingservices@apple.com

Test beta software, access test plans and provide feedback:
appleseed.apple.com/sp/welcome