Managing Devices and Corporate Data

Overview

Data is one of a company's most important assets. Separating personal from corporate data is a great way to keep it protected from both attacks and user missteps, whether your users access corporate data on personal or company-provided devices. Apple has made it easy for IT to support varying levels of device management while helping users stay fully productive at their tasks.

With corporate-owned devices, IT teams can use Apple Business Manager to automate device enrollment — quickly and easily providing devices to users without having to physically touch or prepare each device. By using supervision, IT can access controls unavailable for other deployment models. That includes additional security configurations, nonremovable MDM, and software update management,

For personal devices managed under User Enrollment, corporate and personal data are separated through a Managed Apple ID and a personal Apple ID, respectively. This ensures corporate data is kept safe and separate from any personal data. And when an employee leaves the organization or no longer requires access to an app, the corporate data is removed.

Managing Apple devices

Apple gives IT teams the tools to be successful and have the control they need without compromising usability. This is achieved through the tight integration of Apple's management framework and your mobile device management (MDM) solution.

Apple's approach to device management

Apple builds a management framework into iOS, iPadOS, tvOS, and macOS to enable IT teams to configure and update settings, deploy apps, monitor compliance, query devices, and remotely wipe or lock devices. This framework, which supports both corporate-owned and employee-owned devices, is the foundation for device deployment and management. Because this framework is built into Apple's operating systems, it allows organizations to manage what they need — with a light touch — and not by simply locking down features or disabling functionality. So IT teams have the control they require without degrading the user experience or compromising privacy.

What is MDM?

Together, Apple and your MDM solution make it easy for IT to deploy devices, distribute apps, configure settings, and ensure the security of devices.

MDM supports configuration for apps, accounts, and data on each device. This includes integrated features such as password and policy enforcement. Controls remain transparent to employees while ensuring that their personal information stays private. And if devices ever go missing, IT teams can remotely and securely erase them.

Whether a business uses a cloud-based or on-premise server, MDM solutions are available from a wide range of vendors who offer a variety of features and pricing for ultimate flexibility.

Other device management methods in the market may use different names to describe MDM functionality, such as enterprise mobility management (EMM) or unified endpoint management (UEM). These solutions have the same goal in mind — to manage your organization's devices and corporate data over the air.

How MDM impacts your users

Apple enables IT teams to deploy and manage devices without compromising employee privacy or disrupting their daily work. This means that features and devices aren't locked down or disabled across the board and that data use and collection are limited, whether the device is owned by your organization or the employee.

This works because Apple separates apps and data by corporate and personal use. And tight integrations with most third-party MDM solutions allow IT to interact with an Apple device but limit the exposure of certain information and settings. Regardless of your deployment model, the MDM framework can never access personal information, including email, messages, and browser history.

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

Device ownership methods

Devices are owned by either the organization or the employees. Corporate-owned devices are most often distributed one-to-one, meaning each user is assigned a dedicated device with controls implemented by IT. But corporate-owned devices can also be shared by multiple employees. Examples of shared distribution include shift workers sharing devices between shifts or retail employees using one device as a handheld point of sale (POS). Corporate-owned devices can be managed through supervision, which provides additional control over configuration and restrictions without locking down the devices.

User-owned devices, also known as “bring your own device” (BYOD), are managed through User Enrollment. This management method enables employees to use their personal devices for business uses.

In both cases, Apple supports varying levels of management while respecting privacy, security, and data separation.

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

Corporate-owned devices

Corporate-owned devices can be configured by IT to only have the data, apps, and settings that employees need to complete their job functions. These devices can be deployed automatically through your MDM solution. Devices purchased directly from Apple or from an Apple Authorized Reseller can be automatically enrolled in Apple Business Manager and deployed through zero-touch deployment — eliminating the need for IT teams to handle each device individually.

With corporate-owned devices, organizations gain a higher level of control without sacrificing users’ privacy and usability. Enrolling a corporate-owned device means the IT team can set Wi-Fi, VPN, mail, and calendar settings, in addition to configuring and installing accounts and restrictions. And restrictions can be put in place to prevent users from adding their accounts to the devices.

While users can use either a Managed Apple ID, their personal Apple ID, or none at all on a corporate-owned device, it’s recommended that they use a Managed Apple ID. Managed Apple IDs are unique to your company and separate from Apple IDs that you can create for yourself. Unlike with personal Apple IDs, IT administrators manage the services that your Managed Apple ID can access. Additionally, supervision gives IT access to controls that aren’t available for other deployment models. These include additional security configurations, nonremovable MDM, and software update management.

Whether a corporate-owned device is provided to each employee or shared among many for common tasks, all data on it can be easily secured and protected.

User-owned devices

Employees who use their personal devices for work can have their corporate data managed through User Enrollment. Designed specifically for BYOD programs, User Enrollment allows employees to protect their privacy while keeping corporate data safe, separate, and protected — enabling device personalization that wasn't previously possible. IT can enforce only specific settings, monitor corporate compliance, and remove only corporate data and apps. IT teams can't remotely wipe a device, access device location, or access personal information or apps on the device. Users can remove the MDM profile — which removes all corporate apps and data — whenever they want, and they have greater abilities over updates and other configurations than they would on corporate-owned devices.

User Enrollment requires users to opt in to enroll their devices into the organization's MDM solution. This gives them access to corporate resources, configures various settings, installs a configuration profile, and installs corporate apps.

User Enrollment allows for a personal and a Managed Apple ID to exist on the same device. The existing personal Apple ID is used for all of the user's personal iCloud data. The Managed Apple ID provided by the organization stores all of the organization's corporate iCloud data in the company's managed iCloud Drive and Notes.

With iOS 15 and iPadOS 15, users can now enroll their devices right from the Settings app. In Settings, they'll choose General, choose VPN & Device Management, then tap Sign in to Work or School Account. Once they enter their Managed Apple ID username and password, the authentication process will begin.

Managing data this way gives users more autonomy over their own devices while increasing the security of enterprise data by storing it on a separate, cryptographically protected Apple File System (APFS) volume with Notes and the iCloud Drive app. This provides a better balance of security, privacy, and user experience for BYOD programs. And if a user changes their managed device or leaves the organization, all APFS volume data is destroyed as soon as their device is unenrolled.

Tools for separating corporate data

Apple has a variety of tools that make it simple to separate corporate and personal data on devices, regardless of the ownership model you use. In this section, you'll learn how to manage data in managed apps, settings, accounts, and more.

Managed apps

To receive assigned apps from your organization, devices must be enrolled in your MDM solution. After an app is assigned to a device, it's pushed to that device through MDM. On corporate-owned devices managed through supervision, apps are installed silently without user interaction or an Apple ID.

Data stored in a managed app — whether devices are owned by the company or the users — will be deleted when a device is unenrolled from MDM either by IT or the user. And IT teams can prevent managed apps from backing up data to the Finder, iTunes, or iCloud. Disallowing backup helps prevent managed app data from being recovered if the app is removed using an MDM solution but later reinstalled by the user.

Managed settings

Once users are enrolled in MDM, users can easily view in Settings which apps, and accounts are being managed and which restrictions have been implemented. All enterprise settings, accounts, and content installed by MDM are flagged as managed. This includes Wi-Fi and VPN configurations and password requirements. All settings can be updated or removed at any time.

Restrictions

Restricting access to sharing options or downloading certain apps is one way that IT teams can keep corporate data secure. With Apple and your MDM solution, IT can enable a higher level of control for corporate-owned devices by using supervision. This provides additional device management controls that aren't available for other deployment models, including nonremovable MDM. Additionally, teams can implement various restrictions such as disabling the camera on iPhone, disabling iCloud, disabling Siri, and more.

Managed accounts

IT teams can manage the corporate email, calendar, and contacts on the device, helping users get up and running more quickly. Managing accounts prevents users from adding their personal email, calendar, and contacts — preventing user personalization but giving IT greater ability over protecting data on the device.

Managed extensions

App extensions give third-party developers a way to provide functionality to other apps or even to key systems built into the operating systems, enabling new business workflows between apps. Managing extensions prevents unmanaged extension functionality from interacting with managed apps. Examples of extensions include document provider extensions, which allow productivity apps to open documents from a variety of cloud services; share extensions, which give users a convenient way to share content with other entities; and action extensions, which let users manipulate or view content within the context of another app.

Managed Open In for iOS and iPadOS

Managed Open In uses three separate functions to protect corporate data:

- **Allow documents from unmanaged sources in managed destinations.** Enforcing this restriction helps prevent a user's personal sources and accounts from opening documents in your organization's managed destinations. For example, this restriction could prevent the user from opening a PDF from a random website in your organization's PDF app.

- **Allow documents from managed sources in unmanaged destinations.** Enforcing this restriction helps prevent an organization's managed sources and accounts from opening documents in a user's personal destinations. This restriction could prevent a confidential email attachment in your organization's managed mail account from being opened in any of the user's personal apps.

- **Managed pasteboard.** In iOS 15 and iPadOS 15 or later, this restriction helps control the pasting of content between managed and unmanaged destinations. When the restrictions above are enforced, pasting of content is designed to respect the Managed Open In boundary between third-party or Apple apps like Calendar, Files, Mail, and Notes. And with this restriction, apps can't request items from the pasteboard when the content crosses the managed boundary.

On the most basic level, these three functions help divide the managed device into two environments: one for managed corporate apps and data and one for unmanaged personal apps and data.

Using Managed Open In to separate data helps create a much more positive user experience. Instead of locking down an entire device, Apple's more user-friendly approach gives IT teams the necessary visibility to manage the data source and destination without the traditional heavy-handedness.

Managed domains for iOS and iPadOS

IT can manage specific URLs and subdomains on iPhone and iPad**.** For example, if a user downloads a PDF from a managed domain, the domain requires that the PDF comply with all manage document settings. Paths following the domain are managed by default.

Lost or stolen devices

Devices can, unfortunately, be lost or stolen. With Apple and your MDM solution, missing devices won't give individuals unfettered access to corporate data. Your MDM solution can set up data protection that's automatically turned on with a passcode. Additionally, managed settings can ensure that your users have difficult-to-crack passcodes on all managed devices.

It's easy for IT teams to remotely lock a missing macOS device or to turn on Lost Mode for a missing iOS or iPadOS device. In both cases, the device is locked until the correct password or passcode is entered. If the device can't be located, your MDM solution can remotely lock and wipe it. This ensures that no one else can access your sensitive corporate data.

Identity management

For organizations that deploy Apple devices at any scale, identity is the centerpiece of how users authenticate to devices, websites, apps, and services. Identity is tightly integrated into all operating systems. This provides a seamless, nearly invisible experience to users. And it enables them to work from anywhere while giving IT teams the visibility and control they need. With strong identity management practices, IT teams can prevent data leaks before they even happen and have a clear path for follow-up if they do. Apple has built a number of tools and technologies that enable this experience, including the ones described below.

Device authentication

Identity management in Apple devices starts with device authentication — the Lock Screen or login window — and is in effect throughout the device. Whether your employees are using a shared iPad or a shared Mac, they can select their account, enter their credentials, and get a personalized experience. Through device authentication, IT teams have a clear view into the data chain of command — such as who accessed what files and who they shared them with. Device authentication on a shared iPad is enabled by a Managed Apple ID; and on a shared Mac, accounts can be local or come from the network.

Single Sign-on extensions

Single Sign-on (SSO) extensions are configured through your MDM solution and enable native apps and WebKit to provide a more seamless single sign-on experience. This means that your users are able to leverage existing credentials to securely access apps, without needing to create individual logins and passwords. With macOS Big Sur and iPadOS 14, IT teams can configure SSO extensions on both macOS and iPadOS with Shared iPad. In macOS, additional tools such as the Kerberos Single Sign-on extension allow for integration with Active Directory policies and functionality without requiring a traditional bind and mobile account. And your MDM solution can manage certificates from internal and external certificate authorities (CA) so that client certificates can be used to transparently authenticate to secure, administratively trusted services.

Managed Apple IDs

IT teams use Managed Apple IDs to manage their organization's devices and app purchases in Apple Business Manager. With a Managed Apple ID, IT teams can also leverage federated authentication, a simple and secure identity management architecture. Federated authentication with Managed Apple IDs allows organizations that are enrolled in Apple Business Manager to connect to their existing identity system. This automatically sets users up with access to Apple services, so they don't need new sign-in credentials. This means that when a user first signs in to their Apple device using federated authentication, the Managed Apple ID needed to access Apple services is automatically created. Federated authentication reduces account-related overheads for IT teams and users, and it ensures that identity management policies are consistently enforced across all apps and services used within the organization.

Summary

Your data goes where your employees go, and it's crucial to make sure it's protected. With Apple's management framework and your MDM solution, Apple empowers your users to do great work no matter where they are.

As you continue to manage your fleet and build your data separation framework, don't forget these critical points:

- Corporate-owned devices give the most control and protections over corporate data.
- User-owned devices managed through User Enrollment keep corporate data protected without accessing personal data, thereby protecting user privacy.
- User privacy and security are just as critical as protecting corporate data.
- Managing devices and data is a shared exercise, and the best IT teams employ a user-friendly approach.

Additional resources

Learn about deploying Apple devices:
support.apple.com/zh-hk/guide/deployment/welcome/web

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

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

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

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

Learn about Apple platform security:
apple.com/security

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

Discover Apple Training and Certification:
training.apple.com