Mac Deployment Overview

Introduction

Contents

Mac, combined with macOS, enables employees to get their best work done from anywhere. And it allows IT departments to spend less time managing devices — empowering them to shape business strategy and focus beyond fixing technology and cutting costs.

This document offers guidance on deploying macOS 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 macOS updates, are covered in greater detail in the online Apple Platform Deployment guide.

Ownership Models

These are the two ownership models for macOS devices that organizations commonly use:

- Organization-owned
- User-owned

Each model has its own benefits, so it's important to choose the one that's best for your organization. While most organizations have a preferred model, you might encounter 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 Enrollment, 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/mdm

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. BYOD deployments are less common for macOS devices, but still may be used in your organization. To use organizational services — such as Wi-Fi, mail, and calendars — or to configure devices for specific education or business requirements, users typically enroll their devices in an organization's mobile device management (MDM) solution. This is called User Enrollment.

User Enrollment 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 will leverage their Managed Apple IDs. A Managed Apple ID is part of the User Enrollment profile, and the user must successfully authenticate for enrollment 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 Enrollment in MDM solutions:
support.apple.com/guide/mdm

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 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 devices are owned by the organization or the users.

To view these steps in more detail, visit the online Apple 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 macOS 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.

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. An Apple ID enables a user to sign in to Apple services such as FaceTime, iMessage, the App Store, and iCloud, accessing a wide range of content and services that can increase productivity and support collaboration. Like any Apple ID, Managed Apple IDs are used to sign in to a personal device, and they're an integral part of Apple device management. Managed Apple IDs enable access to Apple services — including iCloud and collaboration with iWork and Notes — the same way a personal Apple ID does. Managed Apple IDs, however, are owned and managed by your organization for things like password resets and role-based administration. Managed Apple IDs 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. Apple and Cisco have optimized how Mac computers communicate with a Cisco wireless network, with support for advanced networking features in macOS like Quality of Service (QoS). If you have Cisco networking equipment, work with your internal teams to ensure that Mac will be able to optimize critical traffic. 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. macOS uses Bonjour to connect to AirPrint-compatible printers and to AirPlay-compatible devices such as Apple TV. And some apps and built-in macOS features use Bonjour to discover other devices for collaboration and sharing.

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

Learn more about configuring your network for MDM:
support.apple.com/HT210060

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

VPN. Evaluate VPN infrastructure to make sure users can securely access company resources remotely. Consider using the VPN On Demand feature of macOS so that a VPN connection is initiated only when needed. If you plan to use Per-App VPN, check that your VPN gateways support these capabilities and that you purchase sufficient licenses 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 G Suite, 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 licenses to support the anticipated number of macOS devices that will be connected.

Managing identities. To manage identities and other user data, macOS can access directory services that include Active Directory, Open Directory, and LDAP. Some MDM vendors provide tools to integrate their management solutions with Active Directory and LDAP directories out of the box. Additional tools like the Kerberos Single Sign-on extension in macOS Catalina allow for integration with Active Directory policies and functionality without requiring a traditional bind and mobile account. And your MDM solution can manage various types of certificates from both internal and external certificate authorities (CA) so that identities are automatically trusted.

Learn more about the new Kerberos Single Sign-on extension:
support.apple.com/guide/deployment

Learn more about directory integration:
support.apple.com/guide/deployment

Core employee services. Verify that your Microsoft Exchange service is up to date and configured to support all users on the network. If you don't use Exchange, macOS also works with standards-based servers, including IMAP, POP, SMTP, CalDAV, CardDAV, and LDAP. Test basic workflows for email, contacts, and calendars, as well as other enterprise productivity and collaboration software that will cover the highest percentage of critical daily workflows for users.

Learn more about configuring Microsoft Exchange:
support.apple.com/guide/deployment

Learn more about standards-based services:
support.apple.com/guide/deployment

Content caching. The caching service built into macOS stores a local copy of frequently requested content from Apple servers, helping minimize the amount of bandwidth needed to download content on your network. You can use caching to speed up the download and delivery of software through the Mac App Store. It can also cache software updates for faster downloading to your organization's devices, whether they're using macOS, iOS or iPadOS. Additional content can also be cached with third-party solutions from Cisco and Akamai.

Learn more about content caching:
support.apple.com/guide/deployment

2. 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 and Apple Business Manager or through MDM and Apple Configurator 2.

Automated Device Enrollment

This enrollment method is a fast, streamlined way to deploy corporate-owned Apple devices and enroll 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 receive the right configurations immediately upon activation. Only devices purchased directly from Apple or from participating Apple Authorized Resellers or carriers can be deployed through Automated Device Enrollment. However, there may be some Mac computers that were purchased or donated from outside of the normal channels that support Automated Device Enrollment. For these scenarios, Apple has introduced the new app Apple Configurator for iPhone. Apple Configurator for iPhone makes it easy to assign any supported Mac running macOS Monterey to your organization's Apple Business Manager account, allowing IT teams to take advantage of all the great device management features that automated device enrollment enables.

Learn more about Apple Configurator for iPhone:
support.apple.com/guide/apple-configurator/welcome/ios

Device Enrollment

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 Enrollment. Devices that are managed manually behave like any other assigned device, with mandatory supervision and MDM enrollment. 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 Enrollment

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

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 enrollment method. The macOS device then receives notification of the administrator's action through the Apple Push Notification service (APNs), so 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.

3. 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. Restrictions include features like erase all content and settings, which quickly resets a Mac to its current OS version, cryptographically removing all user data in the process.

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 macOS update, locking or wiping a device remotely, or managing passwords. 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 macOS 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. And MDM can query the state of key security features such as FileVault or the built-in firewall.

Managed software updates

IT can give users the choice to upgrade to the latest operating system when it's available. By testing a prerelease version of macOS, IT can ensure that application compatibility issues are identified early and are addressed with developers before the final release. IT can get involved with testing each release through the Apple Beta Software Program or AppleSeed for IT. Take a comprehensive approach to keeping Mac computers up to date in order to protect your users and their data. Update frequently — as soon as you've determined that your workflow is compatible with a new version of macOS.

MDM can push macOS updates automatically to a device-enrolled Mac. A device-enrolled Mac can also be configured to defer updates and notifications of updates for up to 90 days if critical systems aren't ready. Users won't be

able to initiate updates manually until the policy is removed or MDM sends an installation command.

Apple doesn't recommend or support monolithic system imaging for macOS upgrades. Like iPhone and iPad, Mac computers often rely on firmware updates that are specific to their model. Similarly, updates to the Mac operating system mandate that these firmware updates be installed directly from Apple. The most reliable strategy is to use the macOS Installer or MDM commands to update.

Managed additional software

Organizations often need to distribute additional apps beyond the initial set to their users. This can be handled automatically by MDM for critical applications and updates or on demand by enabling employees to request applications through a self-service portal provided by your MDM solution. These portals can do everything from installing software purchased from the App Store through Apple Business Manager to installing non–App Store apps, scripts, and other utilities.

While most software can be installed automatically, certain installations may require user interaction. To improve security, apps that require kernel extensions now require user consent to load. This is known as User Approved Kernel Extension Loading, and it can be managed by MDM.

4. Content distribution

After enrollment, the administrator can now also use managed distribution. This enables the MDM or Apple Configurator 2 to manage all apps and books purchased from the Apple Business Manager store in any country where those apps 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 via MDM and no user invitation is required. Anyone using that device has access to the app.

Assigning apps and books to users. Another 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 a 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've been distributed, and they can't be revoked or reassigned.

Preparing additional content. Your MDM solution can help you distribute additional packages with content that doesn't originate from the Mac App Store. This is a common approach for many enterprise software packages, such as internal custom applications or apps like Chrome or Firefox. Required software can be pushed out through this method and installed automatically after completing enrollment. Fonts, scripts, or other items can also be installed and executed via packages. Ensure that these packages are signed appropriately with your Developer ID from the Developer Enterprise program.

Device Security

Apple devices are secure by design. After devices are set up, manage and protect corporate data with the built-in security features and additional controls that are available through your MDM solution. IT 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 password via MDM on a macOS 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. Built-in security features let IT encrypt data, protect devices from malware, and enforce security settings without the need for third-party tools.

Locking, locating, and wiping. When a device goes missing, your corporate data doesn't have to go with it. For iOS, iPadOS, and macOS devices, IT can remotely lock and erase all sensitive data to protect your company's information. For supervised macOS devices, IT can enable Find My 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 provide 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. With macOS Catalina or later, 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

Many organizations find that Mac users require minimal support from IT. To encourage self-support, as well as to increase the quality of support, most IT teams develop self-support tools. Examples include creating a robust Mac support web page, offering self-help forums, and providing onsite tech help bars. And MDM solutions can enable users to perform support tasks, like installing or updating software from a self-service portal.

As a best practice, companies shouldn't make users rely completely on themselves for support — instead, companies should take a collaborative approach to problem-solving. Encourage users to have a shared stake in the process by enabling them to investigate and troubleshoot issues themselves before calling the help desk.

Sharing support responsibility helps reduce downtime for employees and lower the total footprint for support costs and staff. For organizations that need more, AppleCare provides a variety of programs and services that complement internal support structures for employees and IT.

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 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, iPadOS, 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 senior technical Apple 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 and AppleCare+ for Mac

Every Mac computer 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 three years from the original purchase date with AppleCare+ for Mac or the AppleCare Protection Plan. Employees can call Apple Support with Apple hardware or software questions. Apple also provides convenient service options when devices need to be repaired. In addition, AppleCare+ for Mac offers select incidents of accidental damage coverage, each subject to a service fee.

Learn more about AppleCare support options:
apple.com/support/professional

Summary and Resources

Whether your company deploys Mac computers 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 macOS deployment, management, and security features:
support.apple.com/guide/deployment/welcome/web

Apple Configurator User Guide:
support.apple.com/guide/apple-configurator/welcome/ios

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

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

Learn about Apple at Work:
apple.com/business

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

Learn about Apple platform security:
apple.com/security

Browse available AppleCare programs:
apple.com/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