



# **Employee Choice for Higher Education**

Mac Deployment Overview

# Overview

## Contents

[Overview](#)

[Getting Started](#)

[Deployment Steps](#)

[Support Options](#)

[Summary](#)

At Apple, we believe employees can do their best work when they have access to the best tools and technology. All of our products are designed to enable employees to be more creative, productive, and work in new ways, whether in the office or on the go. This aligns with how employees want to work in today's world — with better access to information, frictionless collaboration and sharing, and the freedom to stay connected and work from anywhere.

Setting up and deploying Mac computers throughout your institution has never been easier. With key services from Apple, in concert with a third-party mobile device management (MDM) solution, your organisation can easily deploy and support Mac at scale. If your organisation has already deployed iOS devices internally, it's likely that most infrastructure work needed to implement macOS is already complete.

Recent improvements in macOS security, management and deployment allow an organisation to transition from monolithic imaging and traditional directory binding to a seamless provisioning model and deployment process that centres around each user and relies almost exclusively on tools that are built into macOS.

This document provides guidance on everything you need to deploy Mac at scale, from understanding your existing infrastructure to device management and streamlined provisioning. The topics covered in this document are described in greater detail in the online macOS Deployment Reference:

[help.apple.com/deployment/macos](https://help.apple.com/deployment/macos)

# Getting Started

Building a deployment strategy and rollout plan, and evaluating any existing macOS use by employees, are important initial steps in the deployment process. Ensure that necessary teams are engaged early and align with your programme's vision and goals. Some teams start with a small proof of concept to discover challenges unique to their environment. Engaging with existing users as part of a wider pilot is critical to gain an understanding of how devices are used across your organisation and if your team needs to be aware of any issues.

The information collected during this phase can help determine which employee roles and functions would gain the most from Mac. IT can then assess if macOS should be offered as a standard issue across the entire organisation or as a choice for specific job functions.

Often this phase will also reveal a comprehensive list of internal apps and tools that need to be compatible before Mac can be rolled out more widely. Focus primarily on the core productivity, collaboration and communication apps that will cover most users. Critical in-house services like the institution's intranet, directory and expense management software are also important for large portions of an organisation to be productive.

Document and communicate any workarounds or alternatives for other internal tools while encouraging each application owner to modernise as needed. Be transparent with users about all the different business apps that they will be able to use when they select Mac, and let user demand drive prioritisation for any modernisation efforts. When needed, create a plan with application owners for how they can update their apps, leveraging both the macOS SDK and Swift, as well as the wide variety of higher education institution partners that may be able to assist with development.

Mac computers are commonly issued as institution-owned devices. Some institutions may allow employees to use Mac at work through bring-your-own-device (BYOD) programmes. Embracing employee choice with Apple products can lead to benefits across the entire organisation: higher levels of employee productivity, creativity, engagement and job satisfaction, as well as lower costs when considering residual values and support. Organisations can also take advantage of various leasing and financing options to reduce up-front costs. And they can offset costs by allowing employees to contribute with payroll deductions during an upgrade, or by allowing employees to buy out the equipment at the end of a lease or device life cycle.

Institution policies, as well as the deployment, management and support processes described in this document, may differ depending on some of the information your team collects during a pilot. Not every user needs the exact same policies, settings and apps, as the requirements between the different groups or teams within an institution often vary dramatically.

# Deployment Steps

There are four main steps for deploying macOS: preparing your environment, setting up MDM, deploying devices to employees, and then completing ongoing management tasks.

## 1. Prepare

The first step in any deployment is to consider your existing environment. This phase includes a better understanding of your network and key infrastructure, as well as setting up the systems needed to deploy successfully.

### Evaluate your infrastructure

Although Mac integrates seamlessly into most standard institutional IT environments, it's still important to assess your existing infrastructure to make sure your organisation takes full advantage of everything that macOS offers. If your organisation needs help in this area, you can get assistance from Apple Professional Services as well as technical teams from your channel partner or reseller.

### Wi-Fi and networking

Consistent and dependable access to a wireless network is critical to setting up and configuring macOS devices. Confirm that your institution's Wi-Fi network is properly designed, including careful consideration of placement and power for access points, to ensure that roaming and capacity needs are met.

You may also need to adjust configurations on web proxies or firewall ports if devices are unable to access Apple servers, the Apple Push Notification service (APNs), iCloud or the iTunes Store. Just like with iOS, certain parts of the macOS deployment process — especially with newer Mac hardware — require access to these services for things like updating firmware during installation.

Apple and Cisco have optimised 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 make sure Mac will be able to optimise critical traffic.

Companies also need to evaluate VPN infrastructure to make sure users can securely access institutional 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 enough licences to cover the appropriate number of users and connections.

Make sure your network infrastructure is set up correctly to work with Bonjour, the standards-based, zero-configuration network protocol made by Apple. Bonjour enables devices to find services on a network automatically. macOS uses Bonjour to connect to AirPrint-compatible printers, as well as to AirPlay-compatible devices such as Apple TV. Some apps and built-in macOS features also use Bonjour to discover other devices for collaboration and sharing.

Learn more about Wi-Fi network design: [help.apple.com/deployment/macOS](https://help.apple.com/deployment/macOS)

Learn more about configuring your network for MDM:  
[help.apple.com/deployment/macOS](https://help.apple.com/deployment/macOS)

Learn more about Bonjour: [help.apple.com/deployment/macOS](https://help.apple.com/deployment/macOS)

### Managing identities

macOS can access directory services for managing identities and other user data, including 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 Enterprise Connect from Apple Professional Services or Jamf Connect (formerly NoMAD) allow for integration with Active Directory policies and functionality without requiring a traditional bind and mobile account. Various types of certificates from both internal and external certificate authorities (CA) can also be managed by your MDM solution so that identities are automatically trusted.

Learn more about directory integration: [help.apple.com/deployment/macOS](https://help.apple.com/deployment/macOS)

Learn more about managing certificates: [help.apple.com/deployment/macOS](https://help.apple.com/deployment/macOS)

### 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 higher education productivity and collaboration software that will cover the highest percentage of critical daily workflows for users.

Learn more about configuring Microsoft Exchange:  
[help.apple.com/deployment/macOS](https://help.apple.com/deployment/macOS)

Learn more about standards-based services: [help.apple.com/deployment/macOS](https://help.apple.com/deployment/macOS)

### Caching

The caching service built into macOS stores a local copy of frequently requested content from Apple servers, helping to minimise 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, the iTunes Store and Apple Books. It can also cache software updates for faster downloading to your organisation's devices, whether macOS or iOS. Additional content can be cached with solutions from Cisco and Akamai.

Learn more about caching: [help.apple.com/deployment/macOS](https://help.apple.com/deployment/macOS)

### Establish a management solution

MDM lets organisations securely enrol Mac in the institution environment, wirelessly configure and update settings, deploy apps, monitor policy compliance, query devices, and remotely wipe or lock managed devices. IT can easily create profiles to manage user accounts, configure system settings, enforce restrictions and set password policies — all from the same mobile device management solution they use today for iPhone and iPad.

Behind the scenes, both macOS and iOS use a common management framework from Apple, which enables customers to work with various MDM solutions from third parties. A broad range of device management solutions exist from third-party companies like Jamf, VMware and MobileIron. As macOS and iOS share many of the same frameworks for device management, these solutions differ slightly in admin functionality, operating system support, pricing structures and hosting model. They may also offer different levels of services for integration, training and support. Before choosing a solution, evaluate which management features are most relevant to your organisation.

Once you have selected which MDM to use and have begun to configure it, you'll need to visit the Apple Push Certificates Portal and log in to create a new MDM push certificate.

Learn more about deploying MDM: [help.apple.com/deployment/macos](https://help.apple.com/deployment/macos)

Visit the Apple Push Certificates Portal: [identity.apple.com/pushcert](https://identity.apple.com/pushcert)

### Enrol in Apple School Manager

Apple School Manager is a free web-based portal for IT teams to automate device deployment, purchase and distribute content, and manage roles in their organisations. Working seamlessly with your mobile device management (MDM) solution, Apple School Manager makes it easy to enrol devices, deploy content and delegate administrative privileges.

Device enrolment and volume purchasing are seamlessly integrated into Apple School Manager, so now you can bring together everything needed to deploy iOS devices, Mac computers and Apple TV in your institution.

#### Devices

Device enrolment is part of Apple School Manager, giving you a fast and streamlined way to deploy institution-owned Apple devices.

- Automatically enrol devices in MDM without having to physically touch or prep each device before users get them. This ensures that all users receive your organisation's configurations immediately after they activate their device.
- Simplify the setup process for users by removing specific steps in Setup Assistant, so users are up and running quickly.
- Manage default MDM servers more easily by setting a default server that's based on device type.

### Content

The Apps and Books section of Apple School Manager enables organisations to 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 School Manager are not available in certain countries. To learn which features and purchasing methods are available where, visit [support.apple.com/HT207305](https://support.apple.com/HT207305).

- Purchase apps, books and custom apps in bulk. When you buy apps, you can access special pricing for 20 or more copies if you're an eligible education organisation. For books, special pricing is not available. Easily transfer app licences between locations and share licences between purchasers within the same location. And see a unified listing of purchase history, including the current number of licences in use via MDM.
- Distribute apps and books directly to managed devices or authorised 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 organisation.
- Pay using multiple payment options, including credit cards and purchase orders. Organisations can buy Volume Credit (where available) directly from Apple or from an Apple Authorised Reseller in specific 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 School Manager allows you to create accounts that your organisation 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 organisation.
- Designate roles within Apple School Manager on a granular level, so you can assign privileges for 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 Programmes, the highest level of administrative access was an Agent. The Agent was able to accept terms and conditions on behalf of your organisation. This role is now called Administrator. Your organisation can have up to five Administrators in Apple School Manager.

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

A user can have multiple roles in Apple School Manager. Any of your users who were Admins for more than one programme will be assigned all roles that apply in Apple School 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 School 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 School Manager. They shouldn't be used for services like iCloud or by standard employees who don't manage functions in Apple School Manager.

Higher education institutions can also use Managed Apple IDs to provide students with access to Apple services. Student Managed Apple IDs are designed to meet the privacy and security needs of primary and secondary schools, including limitations on purchasing and communications. Students in higher education who want access to Apple services can create personal Apple IDs instead.

Learn more about Apple School Manager: [help.apple.com/schoolmanager](https://help.apple.com/schoolmanager)

### **Enrol in the Apple Developer Enterprise Programme**

The Apple Developer Enterprise Programme offers a complete set of tools for developing, testing and distributing macOS or iOS apps to users. You can distribute apps either by hosting them on a web server or with an MDM solution. Mac apps and installers can be signed with your Developer ID for Gatekeeper compatibility, which is built into macOS to help protect Mac from malware.

Learn more about the Developer Enterprise Programme:  
[developer.apple.com/programs/enterprise](https://developer.apple.com/programs/enterprise)

## **2. Set up**

Setting up your deployment involves defining institution policies and getting your mobile device management solution ready to configure Mac for employees.

### **Understand macOS security**

Security and privacy are fundamental to the design of all Apple hardware, software and services. We protect our customers' privacy with strong encryption and strict policies that govern how all data is handled. Providing a secure computing platform for Apple devices involves:

- Methods that prevent unauthorised use of devices
- Protecting data at rest, even when a device is lost or stolen
- Networking protocols and the encryption of data in transmission
- Enabling apps to run securely without compromising platform integrity



macOS and iOS are built with multiple layers of security so that Apple devices can securely access network services and protect important data. macOS and iOS also provide security through passcode and password policies that can be delivered and enforced with MDM. A user or administrator can use a remote command to erase all private information if a device falls into the wrong hands.

IT can use MDM to deploy a range of policies to keep devices secure. Examples include enforcing FileVault and recovery key escrow with MDM, forcing a specific password policy or screen saver lock and enabling the built-in firewall.

Understand how security is built into macOS: [www.apple.com/uk/macOS/security](http://www.apple.com/uk/macOS/security)

Learn about macOS security features:

[apple.com/uk/business/resources/docs/macOS\\_Security\\_Overview.pdf](http://apple.com/uk/business/resources/docs/macOS_Security_Overview.pdf)

Learn about the Apple T2 Security Chip:

[apple.com/mac/docs/Apple\\_T2\\_Security\\_Chip\\_Overview.pdf](http://apple.com/mac/docs/Apple_T2_Security_Chip_Overview.pdf)

### Define institution policies

Start your institution policy development by establishing general policies that cover the majority of Mac users at your institution. Your MDM solution will let you define user-specific customisations, such as accounts or access to certain apps. You can also set specific policies for organisations or other smaller subsets of users, such as deploying department-specific software or settings.

Work with your internal teams to update existing institution policies to incorporate the use of Mac computers. Some core policies remain the same across all platforms, such as password complexity and rotation requirements, screen saver timeouts and acceptable use.

If your institution policy mandates a specific technology that's used on another platform, understand the underlying issue and work to reframe the policy to cover built-in technologies on macOS. Rather than mandate that all computers use a specific third-party solution to encrypt an entire disk, consider creating a policy that states institution data must be encrypted at rest and accomplish that with FileVault. If the policy requires a specific software title to protect against malware, educate teams on built-in features like Gatekeeper and then update the policy to allow it.

### Configure settings in MDM

To enable management of institution policies and ensure employee access to necessary resources, each Mac will become securely enrolled with your MDM solution. MDM solutions then apply policies and settings using configuration profiles. Configuration profiles are XML files, created by your MDM solution, that allow distribution of settings to macOS and iOS devices. These profiles automate the configuration of settings, accounts, policies, restrictions and credentials. They can be signed and encrypted to help increase the security of your systems.

Once a device is enrolled in MDM, an administrator can initiate an MDM policy, query or command. With a network connection, the device then receives a notification via the Apple Push Notification service (APNs) that instructs it to communicate directly with its MDM solution over a secure connection to process the administrator's action. As communication is only between the MDM solution and the device, APNs will not transmit confidential or proprietary information. If a device is removed from management, settings and policies controlled by that configuration profile will be removed. An institution can also remotely wipe a device if needed.

Many organisations join their MDM solution to their existing directory services. Setup Assistant in macOS can prompt users to log in with their directory service credentials upon initial enrolment. Once the device is assigned to a specific user, MDM can customise configurations and accounts specific to an individual or group. For example, a user's individual Microsoft Exchange account can be automatically provisioned during enrolment. It's also possible to use certificate identities for technologies such as 802.1x, VPN and more.

Given the control these systems provide, often institutions are comfortable giving a user admin access to their Mac, enabling them to fully personalise settings, install apps and troubleshoot issues while still staying within the control of institutional policy via MDM. This model follows the types of privileges and controls that users have over their iOS device when under management.

Learn more about configuration profiles: [help.apple.com/deployment/macOS](https://help.apple.com/deployment/macOS)

### **Prepare for device enrolment**

The easiest method for enrolling a device in MDM is during Setup Assistant with the device enrolment features of Apple School Manager. This enables enrolment without interaction by IT and can streamline certain screens of Setup Assistant to make the process quicker for users.

To configure device enrolment, you'll link your MDM solution to your Apple School Manager account via a secure token. A two-step verification process securely authorises an MDM solution. Your MDM vendor can provide documentation on the specifics of its particular implementation.

If devices are already in use by employees or are owned by individuals, a single configuration profile can be opened by the user and verified in System Preferences to complete enrolment. This is known as User Approved MDM enrolment. Enrolment must take place either through device enrolment or through User Approved MDM enrolment to manage certain security-sensitive settings, like the Kernel Extension Policy and Privacy Preferences Policy Control.

Learn more about kernel extensions and User Approved MDM:

[support.apple.com/HT208019](https://support.apple.com/HT208019)

Learn more about the Privacy Preferences Policy Control:

[help.apple.com/deployment/mdm](https://help.apple.com/deployment/mdm)

### Get ready to distribute apps and books

Apple offers extensive programmes to help your organisation take advantage of the great apps and content available for macOS. With these capabilities, you can distribute apps and books purchased through Apple School Manager as well as your own in-house applications to employees so that they have everything they need to be productive. MDM can also distribute apps and install packages for software that isn't available in the Mac App Store.

Your MDM solution can use managed distribution to distribute apps and books purchased from Apple School Manager in any country where the app is available. To enable managed distribution, you must first link your MDM solution to your Apple School Manager account using a secure token. Once you're connected to your MDM solution, you can assign apps and books to users, even if the App Store on the device is disabled. You can also assign apps directly to devices, which makes your deployment significantly easier as any user on that device will have access to each app.

Learn more about purchasing content in Apple School Manager:

[help.apple.com/deployment/macos](https://help.apple.com/deployment/macos)

Learn more about distributing apps and books:

[help.apple.com/deployment/macos](https://help.apple.com/deployment/macos)

### Prepare additional content

Your MDM solution can help you distribute additional packages with content that does not originate from the Mac App Store. This is a common approach for many institutional software packages, such as internal custom applications or apps like Microsoft Office. Required software can be pushed out through this method and installed automatically after completing enrolment. 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 programme.

Learn more about installing additional content:

[help.apple.com/deployment/macos](https://help.apple.com/deployment/macos)

## 3. Deploy

macOS makes it easy to deploy devices to employees, personalise as needed, and get up and running without the need for any IT intervention.

### Utilise Setup Assistant

Employees can use the Setup Assistant utility in macOS upon startup to set their language and region preferences, and connect to a network. Upon connecting to the Internet, users will be presented with a series of Setup Assistant windows that lead them through the basic steps of setting up a new Mac. Devices that are enrolled in Apple School Manager can be automatically enrolled in MDM during this process. Device enrolled Mac systems can also be configured to skip certain screens, such as Terms and Conditions, Apple ID sign-in, Location Services and more.

MDM can then be used after Setup Assistant to deploy a wide variety of settings upon initial configuration, including defining whether a user will have full administrative privileges over their computer. Just like on iOS devices, this enables them to have control over their device while still conforming to institution policies and settings that are managed by MDM. To enable users to be immediately productive after Setup Assistant completes, only the most critical applications and packages should begin downloading and installing in the background, without disrupting the employee from beginning their work. Larger applications can be scheduled to download and install in the background or at a later point by the user in your MDM solution's self-service tool.

Learn more about configuring Setup Assistant through device enrolment: [help.apple.com/deployment/macOS](https://help.apple.com/deployment/macOS)

### **Configure institution accounts**

MDM can set up email and other user accounts automatically. Depending on the MDM solution you use and its integration with internal systems, account payloads can also be pre-populated with a user's name, email address and certificate identities for authentication and signing.

### **Allow user personalisation**

Enabling your users to personalise their devices can increase productivity because users choose which apps and content will allow them to best accomplish their tasks and goals.

### **Apple ID**

An Apple ID is an identity for logging 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 higher education institution 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 more about Apple IDs: [help.apple.com/deployment/macOS](https://help.apple.com/deployment/macOS)

### **iCloud**

With iCloud, users can automatically sync documents and personal content — such as contacts, calendars, documents and photos — and keep them up to date among multiple devices. Find My iPhone lets users locate a lost or stolen Mac, iPhone, iPad or iPod touch. Specific parts of iCloud — such as iCloud Keychain and iCloud Drive — can be disabled through restrictions entered manually on the device or set via MDM. This gives users the benefits of iCloud for personal data, while preventing the institution's data from being stored in iCloud.

Learn more about managing iCloud: [help.apple.com/deployment/macOS](https://help.apple.com/deployment/macOS)

## 4. Manage

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

### Administer devices

MDM solutions can administer a managed device through a set of specific tasks. These tasks include querying devices for information, as well as initiating tasks that allow you to manage devices that are out of policy, lost or stolen.

### Queries

An MDM solution can query devices for a range of information to help ensure users maintain the appropriate set of applications and settings. The queries may pertain to hardware, such as the serial number or the device model, or to software, such as the macOS version or a list of installed applications. Additionally, MDM can query the state of key security features such as FileVault or the built-in firewall.

### Management tasks

When a device is managed, an MDM solution may 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. These portals can do everything from install software purchased from the App Store through Apple School Manager or non-App Store apps, scripts, and other utilities.

See the full list of management tasks: [help.apple.com/deployment/macos](https://help.apple.com/deployment/macos)

### Manage software updates

IT can give users the choice to upgrade to the latest operating system when it's made available. By testing a pre-release 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 Programme 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 are not ready. Users will be unable 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 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.

### Manage additional software

Organisations often need to distribute additional apps to their users beyond the initial set. 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 install software purchased from the App Store through Apple School Manager or 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 can be managed by MDM.

Learn more about User Approved Kernel Extension Loading:

[help.apple.com/deployment/macOS](https://help.apple.com/deployment/macOS)

### Maintain device security

Beyond the initial set of security policies that were established before device deployment, your team will want to monitor machines for compliance and pull back as much reporting as possible through your MDM solution. This could include monitoring the security posture of each device or collecting information on the installation of software patches. Although most organisations are comfortable using native tools to encrypt and protect each Mac, some organisations may mandate the use of additional file sync and share services or data loss prevention tools to prevent institutional data leakage and provide in-depth reporting on any sensitive data.

The Find My Mac feature of iCloud can initiate a remote wipe that removes all data and deactivates a Mac if it is lost or stolen. IT teams can also perform a remote wipe with MDM.

### Reprovision devices

A Mac can easily be reprovisioned for another user when an employee leaves an organisation by using Internet Recovery and the local Recovery Partition. This enables the contents of the Mac to be wiped, and the latest version of the operating system installed. A device-enrolled Mac will automatically re-enrol with MDM during Setup Assistant, configure settings for the new user, apply institution policies, and deploy all appropriate software. Mac computers that aren't enrolled can be wiped and re-provisioned with the same process, then re-enrolled manually.

Learn more about Internet Recovery: [help.apple.com/deployment/macOS](https://help.apple.com/deployment/macOS)

# Support Options

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

As a best practice, institutions shouldn't require users to rely completely on themselves for support. Instead, take a collaborative approach to problem-solving and focus on enabling users to troubleshoot issues themselves before calling the help desk. Encourage users to have a shared stake in the process and get them to investigate issues themselves before they call for help.

Shared support responsibility enables reduced downtime for employees and a lower total footprint for support costs and staff.

For organisations that need more, AppleCare provides a variety of products that complement internal support structures for employees and IT.

## **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 senior technical Apple support staff. It also includes a suite of tools to diagnose and troubleshoot Apple hardware, which can help large organisations 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 Mac**

Every Mac computer comes with a one-year limited warranty and complimentary telephone technical support for 90 days after the purchase date. With AppleCare+, this coverage can be extended to three years from the AppleCare+ purchase date. 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 up to two incidents of accidental damage coverage, each subject to a service fee.

### **AppleCare for Enterprise**

For institutions 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 programme supports IT department-level integration scenarios, including MDM and Active Directory. AppleCare for Enterprise is available in volume-based price tiers starting from 1,000 and 5,000 covered devices.

Learn more about AppleCare support options:

[www.apple.com/uk/support/professional](http://www.apple.com/uk/support/professional)



# Summary

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

Learn more about macOS deployment, management and security features:

<https://help.apple.com/deployment/macOS/>

Learn about macOS security features:

[apple.com/uk/business/resources/docs/macOS\\_Security\\_Overview.pdf](https://apple.com/uk/business/resources/docs/macOS_Security_Overview.pdf)

Learn about the Apple T2 Security Chip:

[https://www.apple.com/mac/docs/Apple\\_T2\\_Security\\_Chip\\_Overview.pdf](https://www.apple.com/mac/docs/Apple_T2_Security_Chip_Overview.pdf)

Learn more about mobile device management settings for IT:

[help.apple.com/deployment/mdm](https://help.apple.com/deployment/mdm)

Browse available AppleCare programmes:

[www.apple.com/uk/support/professional/](https://www.apple.com/uk/support/professional/)

Discover Apple Training and Certification:

[training.apple.com](https://training.apple.com)

Engage with Apple Professional Services:

[consultingservices@apple.com](mailto:consultingservices@apple.com)

© 2019 Apple Inc. All rights reserved. Apple, the Apple logo, AirPlay, AirPrint, Apple TV, Bonjour, FaceTime, FileVault, iMessage, iPad, iPhone, iPod touch, iTunes, Mac and macOS are trademarks of Apple Inc., registered in the US and other countries. Swift is a trademark of Apple Inc. App Store, AppleCare, Apple Books, iCloud, iCloud Drive, iCloud Keychain and iTunes Store are service marks of Apple Inc., registered in the US and other countries. IOS is a trademark or registered trademark of Cisco in the US and other countries, and is used under licence. 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.