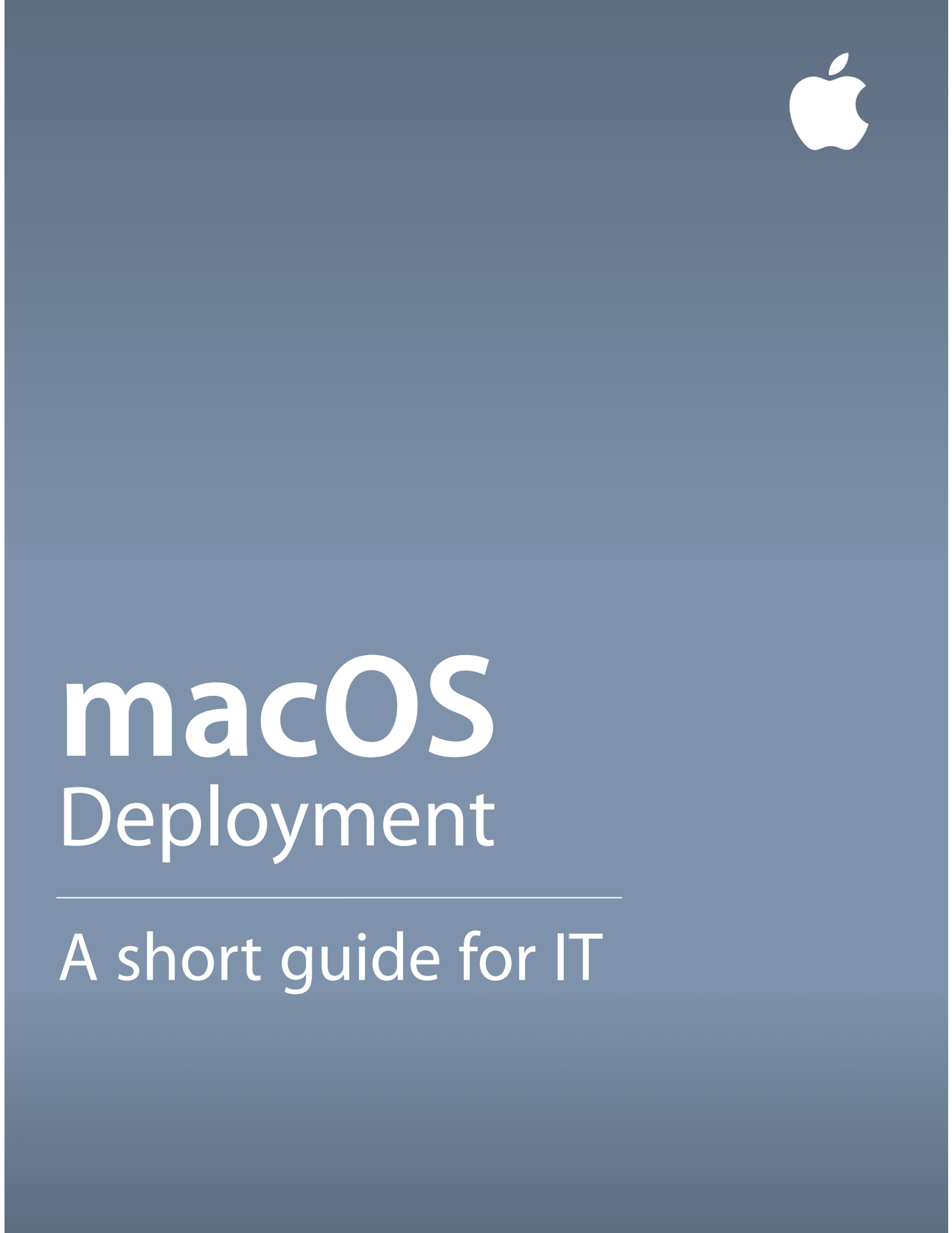


macOS Deployment

A short guide for IT

At Apple, we believe employees should use the tools that power their best work. We also understand the importance of making Mac deployments easy and efficient for IT.

With a complete set of resources from Apple and the right tools in place, your team can seamlessly deploy and manage macOS at scale. This short guide offers information on the four phases for implementing Mac in your environment. It also includes checklists, support information, and helpful links to support your macOS deployment.

For more information, including details on setting up a Mac pilot, contact your Apple Authorized Reseller or account representative.

“Our decision to offer Mac as a choice stemmed from the belief that employees would be more productive on the platform they choose.”

Tayloe Stansbury, Executive Vice President and Chief Technology Officer, Intuit

Getting started.

By following these four phases, you'll be able to quickly get employees up and running on Mac. Each phase is covered as a chapter in this guide. Links to additional resources are located in Resources and Support section in this book.

The first step in any deployment is to consider your existing environment. This phase includes preparing your network and setting up the systems needed to deploy successfully.

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

Deploying Mac includes distributing devices to employees, getting them up and running with Setup Assistant, and allowing for customization and personalization as needed.

Ongoing management includes remotely administering devices, deploying additional applications, and enabling self-support options for your employees.

Before you start, consider a pilot.

A well-executed pilot is a good place to start for any successful Mac deployment. Your internal IT team, an Apple Authorized Reseller or your account team can help you plan and implement a successful Mac evaluation.

Develop your Mac pilot charter

One of the first steps of a successful pilot is to select the team that will focus on the Mac evaluation and your eventual Mac implementation.

Developing a Mac pilot project charter, including success factors, milestones, and roles and responsibilities of your implementation team, will help ensure your pilot's success.

Mac evaluations can be designed to assess many metrics, including user satisfaction, support costs, productivity benefits, app compatibility, security needs, and other technical impacts.

As you plan your pilot, determine what metrics make sense for your organization.

For IT teams new to Mac, this is also a good time to explore technical training and certification programs provided by Apple and third-party providers.

Assess your environment

Two key components of a Mac evaluation are an employee workflow analysis and an app compatibility evaluation. This information will help determine which employee roles are best suited for Mac and your eventual deployment strategy.

When deciding which users will participate in your pilot, consider first selecting employees who request Mac and seem like a good fit, based on your app compatibility evaluation and employee workflow analysis.

It's also best if pilot participants align to the employee audiences who may eventually be using macOS full time.

Developing your device lifecycle management and user support strategies are additional elements of a successful evaluation and pilot.

When you are finished tracking and analyzing your pilot findings, evaluate which action items need to be prioritized, set the strategy for your deployment, and move forward with deploying Mac.

Decide on a deployment strategy.

Evaluating and choosing the deployment scenario that's right for your company is an important follow-up step after a successful pilot. Depending on your organization's needs, you may approach deploying Mac in several different ways.

Deployment options

As you evaluate tools to support corporate-owned Mac systems, it's important to determine your deployment strategy:

Mac as a choice. Mac is deployed as part of a choice program for all employees or subsets of employees.

Mac as a standard. Mac is issued as the standard personal computer to all employees, or an entire group or division.

Depending on how your organization is structured, you may want to consider supporting multiple scenarios at the same time.

Corporate-owned the is most common approach for Mac systems, yet some organizations may also want to support a BYOD option.

Here are a few examples of common deployment strategies:

- A large enterprise deploys Mac systems to corporate headquarters first, and later deploys Mac to its regional and international locations.
- A medium-size organization has a substantial number of existing Mac systems. IT decides to bring those systems under management.
- A large company with several hundred Mac users on its executive, marketing and engineering teams decides to offer Mac as a choice to all employees.
- A government agency has a large number of Mac computers and it decides to refresh those systems and deploy Mac as a choice to remote employees.
- A medium-size company offers Mac as a standard to all employees.

Your how-to checklist.

- Develop a Mac pilot charter.
- Explore Mac training and certification programs.
- Select your pilot participants.
- Complete an employee workflow study and application compatibility analysis.
- Implement your pilot, track your success, and analyze the data.
- Consider your device lifecycle management and user support options.
- Determine your deployment strategy.

CHAPTER ONE

Prepare

After identifying the right strategy for your deployment, follow these steps to lay the groundwork for your Mac implementation.

Evaluate your infrastructure.

Mac integrates seamlessly into most standard enterprise IT environments. It's important to assess your existing network infrastructure to make sure your employees can take full advantage of macOS capabilities.

Wi-Fi and networking

Consistent and dependable access to a wireless network is important to successfully setting up and configuring Mac. macOS supports both 802.11n and 802.11ac so Mac can take advantage of modern wireless technologies. Confirm your Wi-Fi network is properly designed, including careful consideration of placement and power for access points for effective roaming and capacity needs.

Evaluate your VPN infrastructure to make sure users can securely access company resources remotely. Consider using VPN On Demand so that a VPN connection is initiated only when needed.

You will also want to make sure that your network infrastructure is set up to work correctly with Bonjour, Apple's standards-based, zero-configuration network protocol. Bonjour allows devices to find services on a network automatically, and can enable features like AirPrint, AirPlay and AirDrop. Some apps also use Bonjour to discover other devices for collaboration and sharing.

Mail, contacts, and calendars

If you use Microsoft Exchange, verify that everything is up to date and configured to support all users on the network. If you use the cloud-based Office 365, be sure that you have sufficient licenses to support the number of Mac systems that will be connected.

If you don't use Exchange, macOS also works with standards-based servers, including IMAP, POP, SMTP, CalDAV, CardDAV, and LDAP.

Directory integration

macOS can access directory servers for user information and other administrative data, including Open Directory, Active Directory, and LDAP. Decide what will work best based on your existing environment and plan accordingly.

Caching Server

An integrated feature of macOS Server, Caching Server stores a local copy of frequently requested content from Apple servers, helping to minimize the amount of bandwidth needed to download content on your network. Consider enabling Caching Server for your users.

Select an MDM solution.

MDM 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.

If your team is currently managing iOS devices, you can manage macOS in much the same way you are managing iPhone and iPad today. macOS provides a built-in set of management features that are enabled and controlled by third-party MDM solutions.

A variety of third-party MDM solutions are available to support different platforms. Each solution offers different management consoles, features, and pricing. Before choosing a solution, evaluate which management features are appropriate for your environment.

Your Apple Authorized Reseller can offer guidance on which solution is best for your organization.

Enroll in Apple Programs.

Apple Programs are a suite of services that make it easy to streamline your deployment. While preparing for your deployment, learn what each program has to offer and enroll in the programs that make sense for your organization.

Device Enrollment Program

The Device Enrollment Program (DEP) provides a fast, streamlined way to deploy organization-owned Mac systems that are purchased directly from Apple or participating Apple Authorized Resellers.

You can simplify initial Mac setup by automating MDM enrollment so you don't have to physically touch each Mac.

DEP enables you to skip specific steps in Setup Assistant, and together with MDM, automatically configure each Mac as needed for your employees.

Learn more >

Volume Purchase Program

The Volume Purchase Program (VPP) allows businesses to purchase macOS apps and books in volume and distribute them to employees.

You can pay with a corporate credit card or with VPP Credit that you've procured using a purchase order (PO).

MDM solutions integrate with VPP and can be used to distribute apps and books to devices and users in any country where the apps and books are available.

Learn more >

Developer Enterprise Program

The Apple Developer Enterprise Program 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 become signed with your developer ID. This ensures compatibility with Gatekeeper, which is built into macOS and helps protect your Mac from malware.

Learn more >

Your how-to checklist.

- Evaluate your networking infrastructure.
- Confirm that Microsoft Exchange is configured to support your users.
- Ensure that all relevant applications are up to date and licenses are procured.
- Review the benefits of Caching Server.
- Select an MDM solution.
- Enroll in Apple Programs.

CHAPTER TWO

Set Up

Decide how to configure devices with MDM, define corporate policies, and distribute apps and other content to employees.

Configure your devices.

Multiple options are available for configuring employee access to corporate services. IT can set up devices by controlling settings through Mobile Device Management or distributing configuration profiles.

Define your corporate policies

Developing corporate policies for your Mac computers, including password policies, Gatekeeper settings, full volume encryption and screensaver policies, is another important preparation step.

You can develop general policies, as well as policies for subsets of users. This is also a good time to determine configurations. Set user-specific customizations, such as mail accounts. Determine group policies, such as deploying software that's specific to a particular business unit.

Configuring devices with MDM

To enable management and ensure employee access to corporate resources, you can enroll your Mac systems securely using an MDM solution. An MDM solution can apply policies and settings using configuration profiles.

Configuration profiles are XML files created by your MDM solution that allow IT to distribute configuration information to macOS and iOS devices.

These profiles automate the configuration of settings, accounts, policies, restrictions, and credentials. They can be signed and encrypted in order to help increase the security of your systems.

Once a device is enrolled, an admin can initiate an MDM policy, query, or command. The device then receives notification of the admin's action via the Apple Push Notification service (APNs) so it can communicate directly with its MDM server over a secure connection.

With a network connection, devices can receive APNs commands anywhere in the world. APNs will not transmit confidential or proprietary information.

MDM enrollment

Corporate-owned Mac systems can be enrolled in the Device Enrollment Program by your Apple Authorized reseller at the time of purchase. These systems can then become automatically enrolled in MDM during user setup.

Employees who bring in their own devices, or who have Mac systems that are already owned by the organization, can opt in to enroll in MDM to gain access

to corporate resources. If at any point an employee decides to opt out of management, or if the device falls out of compliance, all corporate configurations, settings, and access to resources are removed. Note that BYOD devices are not able to be enrolled in DEP.

Active Directory

Some organizations join their MDM server to their existing directory services, such as Active Directory. MDM can prompt users to log in with their directory service credentials upon enrollment. This way, MDM can customize configurations and accounts specific to individual users or by the groups they belong to. For example, a user's individual Microsoft Exchange account can be automatically provisioned during enrollment. It's also possible to enroll certificate identities with Active Directory Certification Services, which can then be then used with technologies such as 802.1x, VPN, and more.

Distribute apps and books

Apple offers extensive programs to help your organization take advantage of the great apps and content available for macOS. With VPP, you can purchase and distribute apps and books in volume, so that your users have everything they need to be productive when they set up their Mac. MDM can also distribute apps and install packages for software not available on the Mac App Store.

Your how-to checklist.

- Define your corporate policies.
- Configure your devices with MDM and the Device Enrollment Program.
- Consider integration with your organization's directory service.
- Take advantage of Apple's Volume Purchase Program to distribute apps and books to employees.

CHAPTER THREE

Deploy

Distribute your devices to employees, run through Setup Assistant and personalize settings.

Distribute your devices.

Mac is now ready to distribute to your organization. Give employees their Mac and allow them to use the streamlined Setup Assistant for further personalization and customization.

Setup Assistant

At startup, employees can use the Setup Assistant utility in macOS 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.

During this process, devices that are enrolled in DEP can be automatically enrolled in MDM. DEP-enrolled Mac systems can also be configured to skip certain screens, such as Terms and Conditions, Apple ID sign-in, Location Services windows, and more.

You can manage a wide variety of settings upon initial configuration through MDM. And you can also define whether or not a user will have full administrative privileges over their computer.

Allow users to personalize

Enabling your users to personalize their devices with an Apple ID can increase productivity because users choose which apps and content will allow them to best accomplish their tasks and goals.

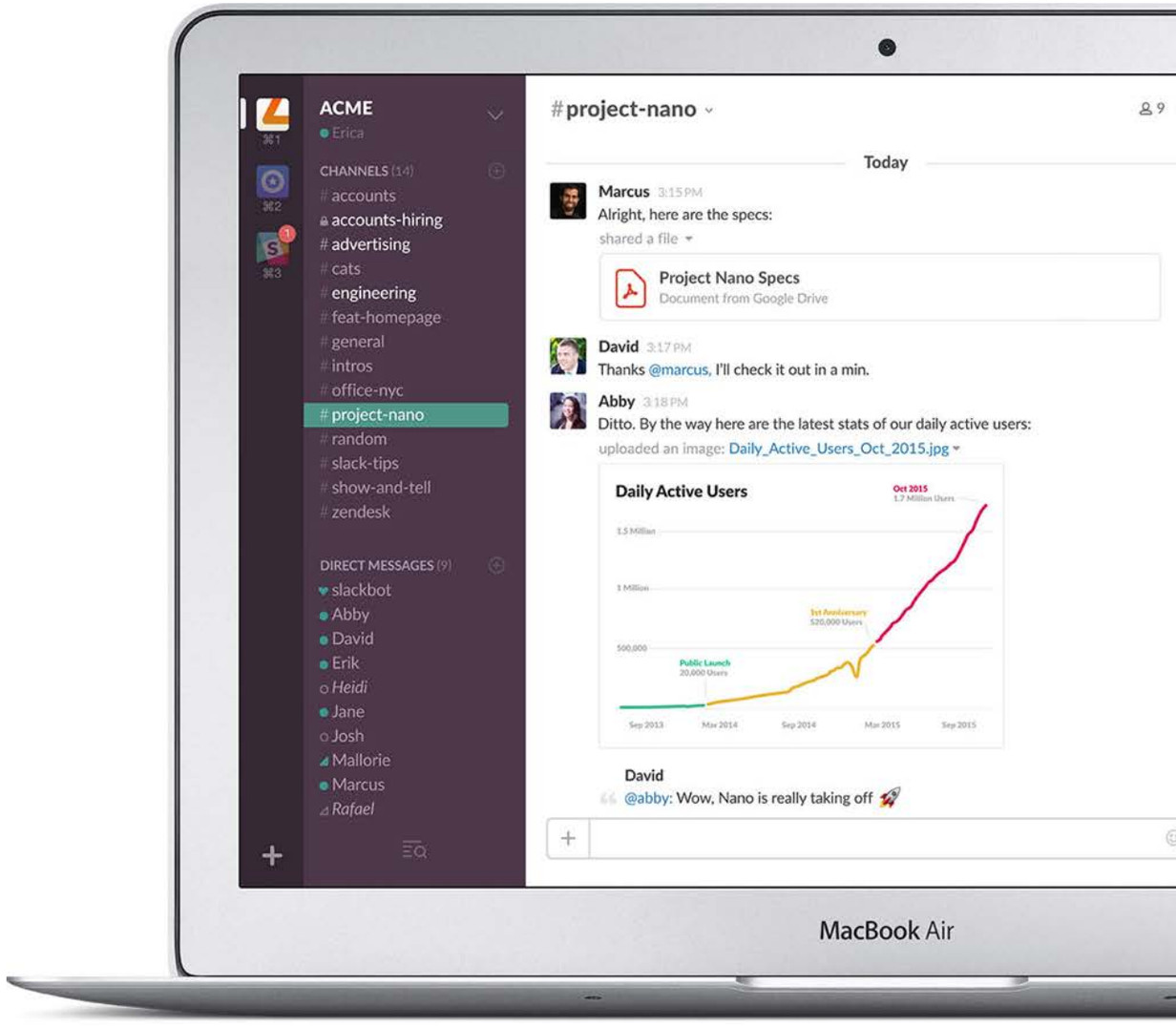
An Apple ID is an identity that's used to log in to various Apple services such as FaceTime, iMessage, the iTunes Store, the App Store, the iBooks Store, and iCloud. These services give users access to a wide range of content for streamlining business tasks, increasing productivity, and supporting collaboration.

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

Some services—such as Photo Stream, iCloud Keychain, iCloud Drive, and backup —can be disabled through restrictions either entered manually on the device or set via your MDM.

Your how-to checklist.

- Streamline Setup Assistant with DEP.
- Consider appropriate levels of user personalization.
- Distribute Mac systems to your employees.



CHAPTER FOUR

Manage

Administer deployed devices with queries and commands. Enable self-service options for employees.

Administer your devices.

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

Queries

An MDM server can query devices for a variety of information, including hardware information, such as serial number or MAC address. It can also query software information, such as the macOS version or a list of installed applications.

This information helps to ensure that users maintain the appropriate set of applications and settings.

Commands

When a device is managed, an MDM server can perform a wide variety of administrative commands, including changing configuration settings automatically without user interaction, locking or wiping a Mac remotely, or clearing the passcode lock so users can reset forgotten passwords.

Additional commands that can be administered by MDM include:

- Locking a Mac with a password
- Renaming a Mac
- Requesting AirPlay mirroring
- Removing a device from MDM

Installing macOS updates can be administered by MDM if the Mac is DEP enabled. Also, some MDM solutions enable employees to manage certain functions themselves, including the ability to run routine maintenance tasks on their Mac or install software.

Deploying and managing content

Beyond the initial set of apps, organizations often need to distribute additional apps to their users. At the same time, organizations need to control how apps connect to internal resources or how data security is handled when a user transitions out of the organization, all while coexisting alongside the user's personal apps and data.

You might consider a strategy for deploying additional apps to users as needed, or for enabling employees to request applications through a self-service portal.

Software updates

IT can give users the choice to upgrade to the latest operating system when it's made 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.

Self support

Many organizations 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 can also provide support info and enable users to perform support tasks from a self-service portal including:

- Installing software
- Offering self-help and training videos
- Obtaining organizational templates, documents, and software updates
- Adding printers
- Adding VPN and 802.1X (port-based Network Access Control) configurations
- Performing simple IT tasks, like checking disk integrity

Security best practices

macOS has many layers of advanced security technologies to help protect your systems, apps and data. IT can use MDM to deploy the following types of security policies to help keep Mac systems safe:

- Turning on a firewall to prevent other machines from accessing services
- Setting their Mac to lock the screen after a period of inactivity
- Setting up secure file sharing
- Securely deleting outdated sensitive files with the Secure Empty Trash command
- Using Password Assistant to create stronger passwords for local utilities, such as Uses & Groups
- Running only sharing services that are really needed

Device reprovisioning

A Mac can easily be reprovisioned for another user when an employee leaves an organization. If the Mac is DEP-enabled, it's as easy as erasing and restoring the operating system. The device will use DEP to automatically re-enroll with MDM, configure settings for the new user, apply any corporate policies, and deploy all appropriate software.

Your how-to checklist.

- Explore the queries and commands offered by your MDM solution
- Put a process in place to test prerelease versions of macOS.
- Consider offering self-support tools.
- Work with your MDM vendor on setting up a self-service portal.
- Develop security best practices.

CHAPTER FIVE

Resources and Support

Explore additional resources and get information on Apple Support offerings for business.

"Between lower support costs and higher residual values, every Mac we deploy makes and saves about $270 for IBM."

Fletcher Previn, VP of Workplace as a Service, IBM

AppleCare Solutions and Reseller Support

Apple and Apple Authorized Resellers offer several service and support programs for medium and large organizations. All AppleCare programs can be purchased directly from your Apple Authorized Reseller.

AppleCare Protection Plan

Every Mac comes with a one-year limited warranty and up to 90 days of complimentary telephone support. The AppleCare Protection Plan for Mac extends the hardware and software coverage to three years from the original purchase date of the Mac.

AppleCare OS Support

AppleCare OS Support provides assistance from experts to keep your IT operations running smoothly. It offers IT enterprise-level support for integration into heterogeneous environments, including support for system components, network configuration, and administration; professional software applications, web applications, and services; and technical issues requiring the use of command-line tools for resolution. It also includes AppleCare Help Desk Support to back up your help desk team.

AppleCare for Enterprise

AppleCare for Enterprise offers IT department–level support for complex deployments and integration questions, including MDM and Active Directory. Help desk backup for your IT team is also included. And AppleCare for Enterprise provides 24/7 technical support and next-day onsite service coverage for employees.[1]

Apple Self-Servicing Account Program

The Apple Self-Servicing Account Program for IT provides a quick and easy online process to obtain genuine Apple, Do-It-Yourself parts, which are customer installable and typically include replacement keyboards, mice, power cables, memory, and modem cables. Participation for qualifying organizations is free of charge.

1. Requires a deployment of 2000 units.

Deployment Resources

Explore resources on Apple Programs, leasing, trade-in, support and training.

Apple Programs

- Device Enrollment Program
- Volume Purchase Program
- Developer Enterprise Program
- Apple Deployment Programs Help

Leasing and trade-in

- Leasing
- Trade-in

Support

- Business support
- AppleCare OS Support
- AppleCare Protection Plan
- AppleCare for Enterprise
- Self-Servicing Account Program

Training

- Mac Basics for employees
- Mac Integration Basics for IT
- Training and Certification

Resources and Support

Technical Resources

These links links contain information relevant to the four phases of deploying macOS. For additional questions, contact your Apple Authorized Reseller or account representative.

Overall technical information

- macOS Deployment Reference

Prepare

- Wi-Fi and networking
- Bonjour
- Mail, contacts, and calendars
- Directory integration
- Active Directory Integration
- Caching Server
- Select an MDM solution
- Enroll in Apple Programs

Set Up

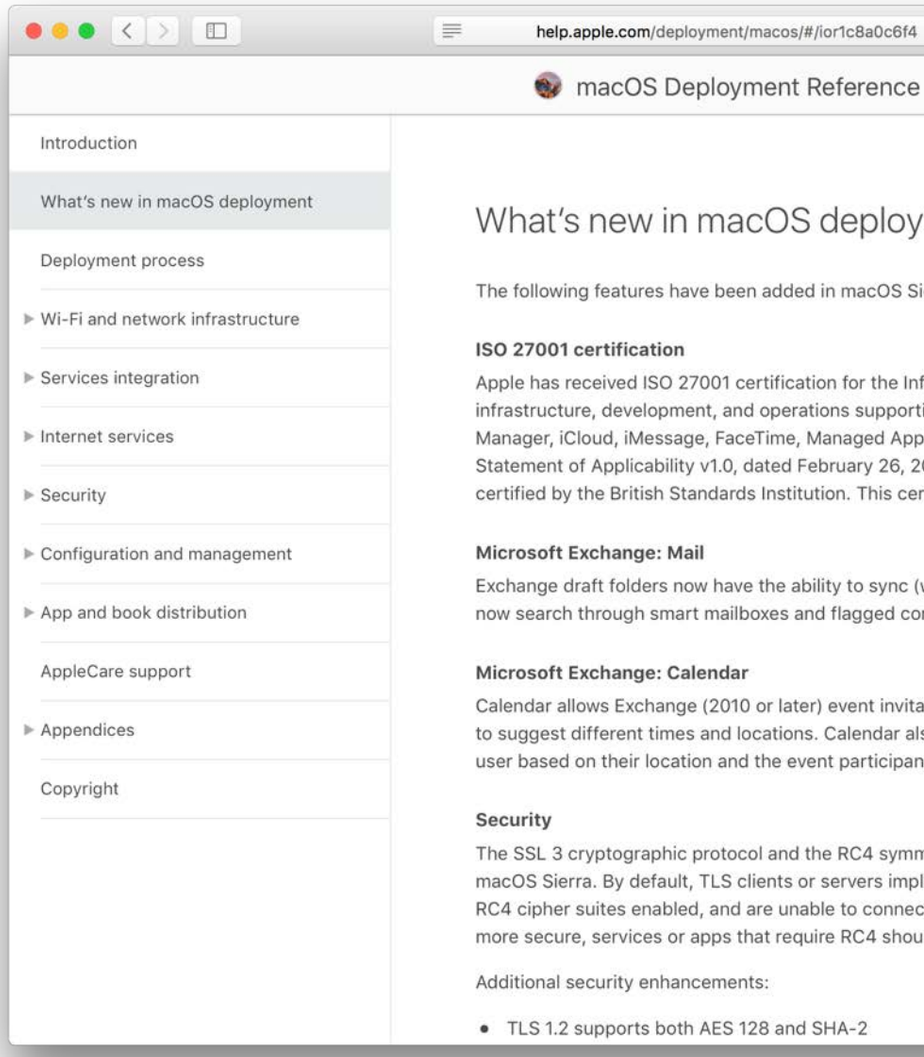
- Configuring devices with MDM
- MDM enrollment
- Distribute apps and books

Deploy

- Device Enrollment Program
- Setup Assistant
- Apple ID
- User personalization

Manage

- Queries
- Commands
- Security best practices



Additional resources

Read the real-world stories of organizations that are deploying Mac today.

Mac Customer Profiles

- BiblioTech Mac Customer Profile
- CareerBuilder Mac Customer Profile
- The CDM Group Mac Customer Profile
- Cisco Systems Mac Customer Profile
- Intuit Mac Customer Profile
- Kelly Services Mac Customer Profile

Some features may not be available for all countries or all areas. Click here to see complete list.
Some features require an Apple ID, compatible hardware, and compatible Internet access or cellular network; additional fees and terms may apply.