A COMPREHENSIVE GUIDE

Mac Management

FOR BEGINNERS

jamf

According to a recent survey, 89% of respondents said that the ability to choose what type of device they use at work was important enough that they would take a salary cut.

And for the majority of those prioritizing device choice from their employers, the choice is clear — they're asking for Apple.**

As Apple device numbers rise in business and education environments around the globe, it's imperative that technology investments are maximized so that organizations can leverage Mac, iPad, iPhone and Apple TV to their full potential. This can put a heavy burden on IT staff that are now tasked with managing this influx of new devices – especially those in established Windows environments.

While some are very familiar with Apple already, many of you are diving into Mac hardware and macOS management for the first time. This guide is for the latter, and will help you build and master your Mac management skills by providing:

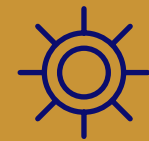**Introduction to Mac and macOS management**

Explanation of services and programs available for Mac

Outline of lifecycle management stages

Insight for infrastructure planning

Overview of the industry-leading Mac management solution

*** 2021 Global Survey: Employee Choice and its Impact on the Future of Work.*

Introduction to Mac and macOS management

When approaching Mac management, it's helpful to break the lifecycle down into common tasks you might do. These management tasks are the same regardless if you are managing a Mac or a PC.

How MDM works

Introduced in OS X 10.7 Lion or later, Mac computers gained the ability understand and apply settings such as remote wipe or passcode restrictions thanks to a built-in mobile device management (MDM) framework. Two core components to the MDM framework are **configuration profiles** and **management commands**.

These components communicate to the device via Apple Push Notification service (APNs), which is kept private to your organization through obtaining a secure certificate from Apple. Apple's server then maintains a constant connection to devices so you don't have to. Devices communicate back to your management server and receive commands, settings, configurations or apps you define.

Configuration profiles

… are XML files that define various settings for your Apple devices and tell that device how to behave. They can be used to automate configuring passcode settings, Wi-Fi passwords and VPN configurations. They can also be used to restrict items such as device features like the App Store, web browsers or the ability to rename a device. These profiles can all be specified and deployed leveraging Jamf and be set at the device or user level.

Management commands

…often referred to as "MDM commands" are singular commands that you can send to your managed devices to take specific actions. Has a device gone missing? Send a remote wipe command. Need to upgrade the OS? Send the command to download and install updates. These are just a few examples of the different actions you can take on a fully managed Mac computer.

MDM and client management

While Apple's MDM framework provides a baseline control over Mac computers, macOS is a more robust platform that may require more advanced functionality. Leveraging client management (only available for macOS), allows you to install a Mac agent, or binary, immediately after the device is enrolled into management.

This agent enables a hidden admin account to be added, allowing for remote root access to macOS and opens the door for more policies and scripts to be run on a computer. Since agent-based Mac management goes beyond the built-in MDM, you need third-party solution, like Jamf, to take full advantage of advanced Mac management.

Examples of Client Management Functions

Install PKG/DMG
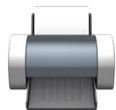
Enforce FileVault

Bind to Directory

Run Scripts

Customize Dock

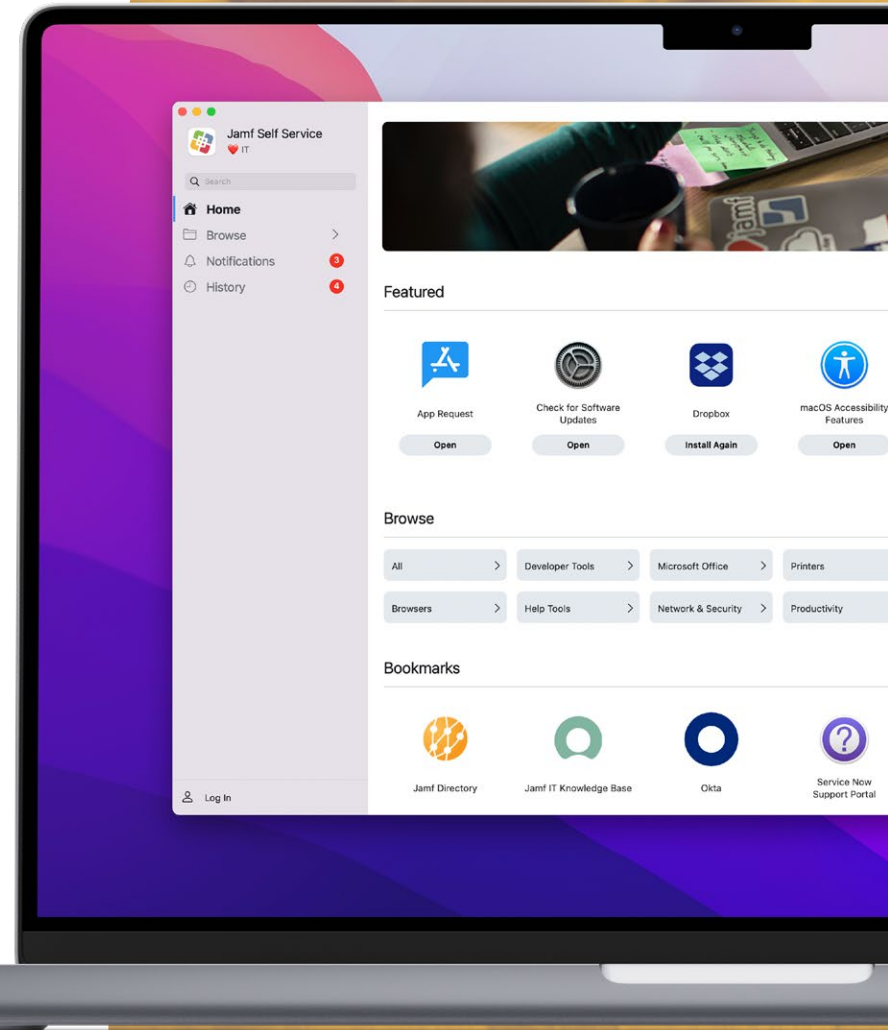**Set EFI Firmware Password**

Install Printers

Create Accounts

Set Software Update

Apple services and programs

As Mac became more popular in the enterprise and education, challenges arose about how to best deploy devices at scale, how to address Apple IDs and app purchasing. Apple introduced various programs and services to take device management one step further, address these challenges and make managing devices in bulk easier and more cost effective.

Not every third-party Apple device management solution supports Apple's programs and services. Check with your vendor to ensure they support these programs, as well as the incremental changes Apple makes throughout the year.

Zero Touch Deployment

Apple's automated MDM enrollment solution allows organizations of any size to pre-configure devices purchased from Apple or an authorized Apple reseller without ever having to touch the device. By leveraging the power of zero-touch deployments and user-initiated enrollment (formerly Apple's Device Enrollment Program or DEP), you no longer need to be the only person receiving, unboxing and configuring new hardware. Instead, you can ship new devices directly to individual employees and let them unbox it. The first time the device is turned on, it will automatically reach out to Apple and your mobile device management solution to pull down relevant configurations, settings and management.

Apps and Books

With Apps and Books from Apple (formerly Volume Purchase Program or VPP) you can purchase and license apps and books in bulk from Apple and distribute them to individuals via Apple ID or directly to devices without an Apple ID. Apps can be reassigned as deployment needs change. You can link your Apps and Books service token (received from Apple) to your Apple management solution for assignment and distribution.

Apple Business Manager

Apple Business Manager is a web-based portal for IT administrators that combines zero-touch deployments and Apps and Books so everything can be overseen from one central location. Apple Business Manager is available to all non-educational organizations. Organizations with existing DEP or VPP accounts can upgrade to Apple Business Manager within a few minutes, or organizations can sign up for the first time at **business.apple.com**

Apple School Manager

Apple School Manager is a web-based portal for IT administrators to oversee people, devices and content - all from one place. Exclusively for education, Apple School Manager combines zero-touch deployments as well as Apps and Books and other classroom management tools, like the Classroom app, in one portal. Apple School Manager enables Managed Apple IDs and Shared iPad and can be integrated with a school's student information system (SIS).

Apple IDs

Apple IDs are the personal account credentials users use to access Apple services such as the App Store, iTunes Store, iCloud, iMessage and more. Depending on the needs of your organization, your end users can leverage their Apple ID on the job, or you can avoid using Apple IDs altogether. If you're an education institution, your students will receive a different type of Apple ID.

Managed Apple IDs

Apple School Manager for education institutions enables Managed Apple IDs for students and can be integrated with your school's student information system (SIS). Managed Apple IDs are a special type of Apple ID for students. They don't require special permission, and they allow you, as an IT admin, to create and dynamically update user information. Managed Apple IDs are created in the Apple School Manager portal and can sync with Classroom data, as well as your school's SIS.

For businesses and government organizations, Managed Apple IDs are only used for administrative purposes within the forthcoming Apple Business Manager.

Classroom App

An instructional tool for educators, Apple's Classroom app empowers teachers to streamline classroom instruction, encourages interaction and collaboration, and supports productivity. A student's device can be limited to a specific app or webpage while teachers can monitor student devices for comprehension assessment.

Lifecycle management stages

Apple's device management framework, commonly referred to as the MDM framework, includes six key elements across the entire lifecycle of your Apple devices.

MDM is Apple's built-in management framework — available for macOS, iOS, iPadOS and tvOS — and aids with these functions:

1 Mac deployment and provisioning

Getting devices into the hands of end users.

2 Configuration management

Applying the correct settings to devices.

3 App management

Ensuring the correct software and apps are on each device and are up-to-date.

4 macOS Inventory

Reporting on the status of each device.

5 Mac security

Securing devices to organizational standards.

6 User empowerment

Allowing users to self-help when they require resources and services.

From initial deployment to the end-user experience, it's critical to understand, manage and support the entire lifecycle of the Mac computers in your environment. This ensures both the security and maximized potential of your devices.

Mac Deployment and Provisioning

Before configuring devices for end users, devices must be enrolled into management within an Apple management solution. There are several enrollment methods available, but the two highlighted below are recommended for enterprise and education institutions looking for a streamlined and positive end-user experience:
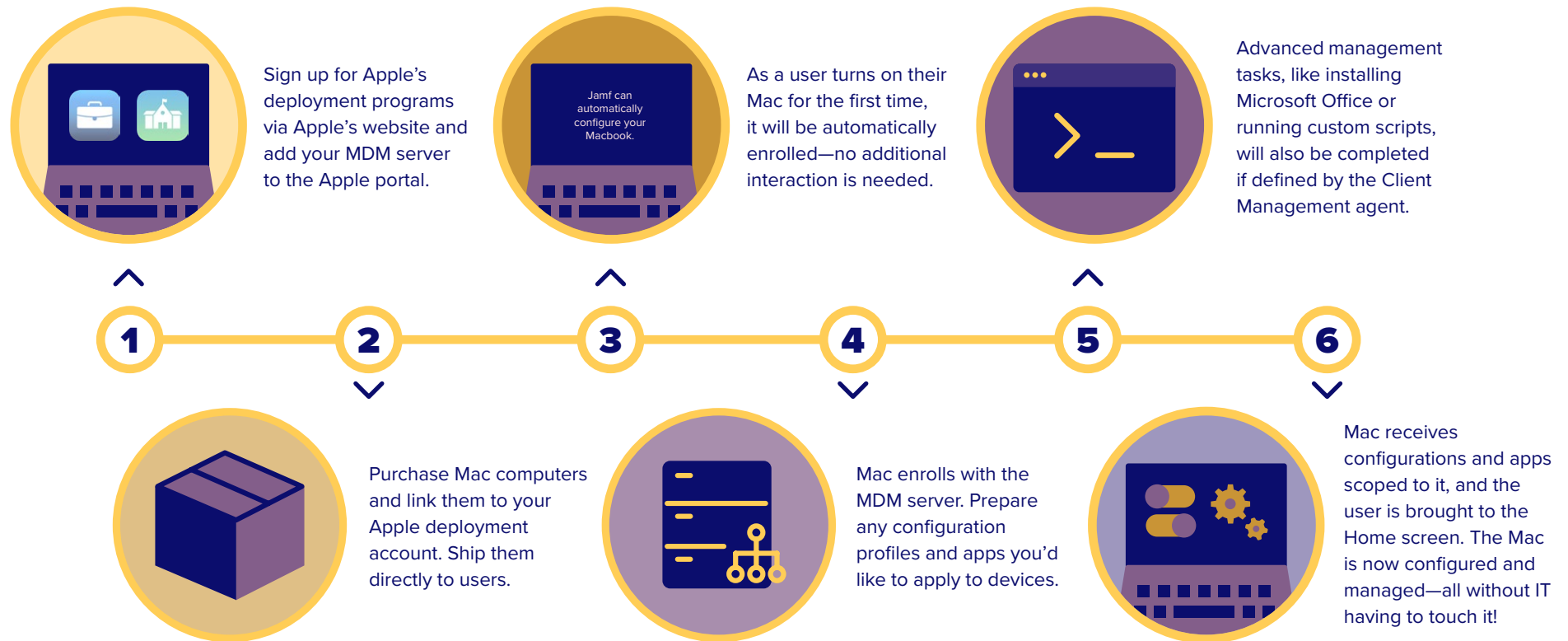
	Description	User Experience	Best For
Zero-Touch Deployment with Apple School Manager or Apple Business Manager	Automatic enrollment over the air	User receives shrink-wrapped box, and the device is automatically configured when turned on	Shipping devices to remote employees or to speed up the onboarding process. Providing users with an unboxing experience
User-initiated enrollment via URL	Manual enrollment over the air	User visits a specific URL to configure their device	Unmanaged devices currently in the field or devices that need to be reenrolled into a new MDM server

Zero-Touch Deployments

1 Sign up for Apple's deployment programs via Apple's website and add your MDM server to the Apple portal.

Jamf can automatically configure your Macbook.

3 As a user turns on their Mac for the first time, it will be automatically enrolled—no additional interaction is needed.

Advanced management tasks, like installing Microsoft Office or running custom scripts, will also be completed if defined by the Client Management agent.

1 — 2 — 3 — 4 — 5 — 6

2 Purchase Mac computers and link them to your Apple deployment account. Ship them directly to users.

4 Mac enrolls with the MDM server. Prepare any configuration profiles and apps you'd like to apply to devices.

6 Mac receives configurations and apps scoped to it, and the user is brought to the Home screen. The Mac is now configured and managed—all without IT having to touch it!

When it's not possible to use Apple's deployment programs, organizations can provision Mac via traditional imaging workflows (less preferred over zero-touch deployment) or use user-initiated enrollment workflows.

Configuration management

When it comes to configuring Mac computers, the world is your oyster. You can personalize and tailor individual devices or groups of devices based on the needs of your end users.

Configuration Profiles

Define settings within macOS by creating configuration profiles. These XML files can be distributed to devices utilizing a management solution. You can apply Wi-Fi, VPN, email settings and more so users can seamlessly connect to the resources they need.

Policies

Unique to macOS client management, policies go beyond the basic device management capabilities of MDM configuration profiles and help you install custom software and printers, manage local user accounts and conduct advanced management workflows. You can specify the tasks you want to automate, how often and when it should run, and to which users and/or devices.

Not all Apple management solutions offer policies and smart targeting. Check with your management vendor to ensure this functionality is available to you.

Don't know where to start? Check out a list of MDM configuration profiles **here**, or join the conversation on **Jamf Nation**.

Scripts

Part of policies, run shell scripts on macOS utilizing the Apple device management capabilities within your client management solution. Anything that can be executed in Terminal via the command line can be turned into a script. The ability to run scripts provides far more flexibility than standard configuration profiles, and opens the door to infinite device management capabilities.

Smart Targeting

Collect inventory details for all of your managed devices, including but not limited to, devices that require software updates, security hardening and custom inventory attributes that you define. If your device management solution allows, you can build groups based on inventory criteria and then trigger device management tasks automatically to specific individuals or groups, or make items available on demand to users with an enterprise app catalog.

App management

App fundamentals

Most organizations get their Mac software from the Mac App Store. Apple reviews the developer's code on the Mac App Store to ensure security and performance. This is one of the reasons why Apple enjoys a strong security reputation. For the Mac, however, you can also get software outside of the Mac App Store.

Popular titles not in the Mac App Store include Google Chrome, Microsoft Office and Adobe Creative Suite, , so it's important to have a Mac client management tool that's able to deploy custom software. Some Apple management solutions have the ability to build custom .pkg or .dmg (Mac software install file types) by creating a before and after snapshot of an installation. That software package can then be deployed to managed Mac computers – all without users needing to be admins.

Mac computers are wildly popular among consumers because of the native communication, learning and productivity tools available right out of the box and also the rich ecosystem of applications available. With a device management solution in place to manage your app deployments, you ensure users have the apps they need — configured for their use case and secured for your environment. Whether your organization is choosing to utilize Apple's built-in apps, one of the apps from the Mac App Store, a third-party app or creating your own in-house custom apps, you need to ensure users have all the apps they need and are properly secured within your environment.

Take snapshots of software installs > Create a custom .pkg or .dmg > Push install via the Jamf Agent

For software that is in the Mac App Store, you can use Apple deployment programs to license and distribute apps to devices all without needing Apple IDs.

Software Installs and Patching

Jamf Title Editor extends the patch management capabilities of Jamf Pro for macOS devices to provide custom software titles, override existing patch definitions and create custom patch definitions. Better yet, App Installers are Jamf-provided installer packages that streamline deployment of third-party apps.
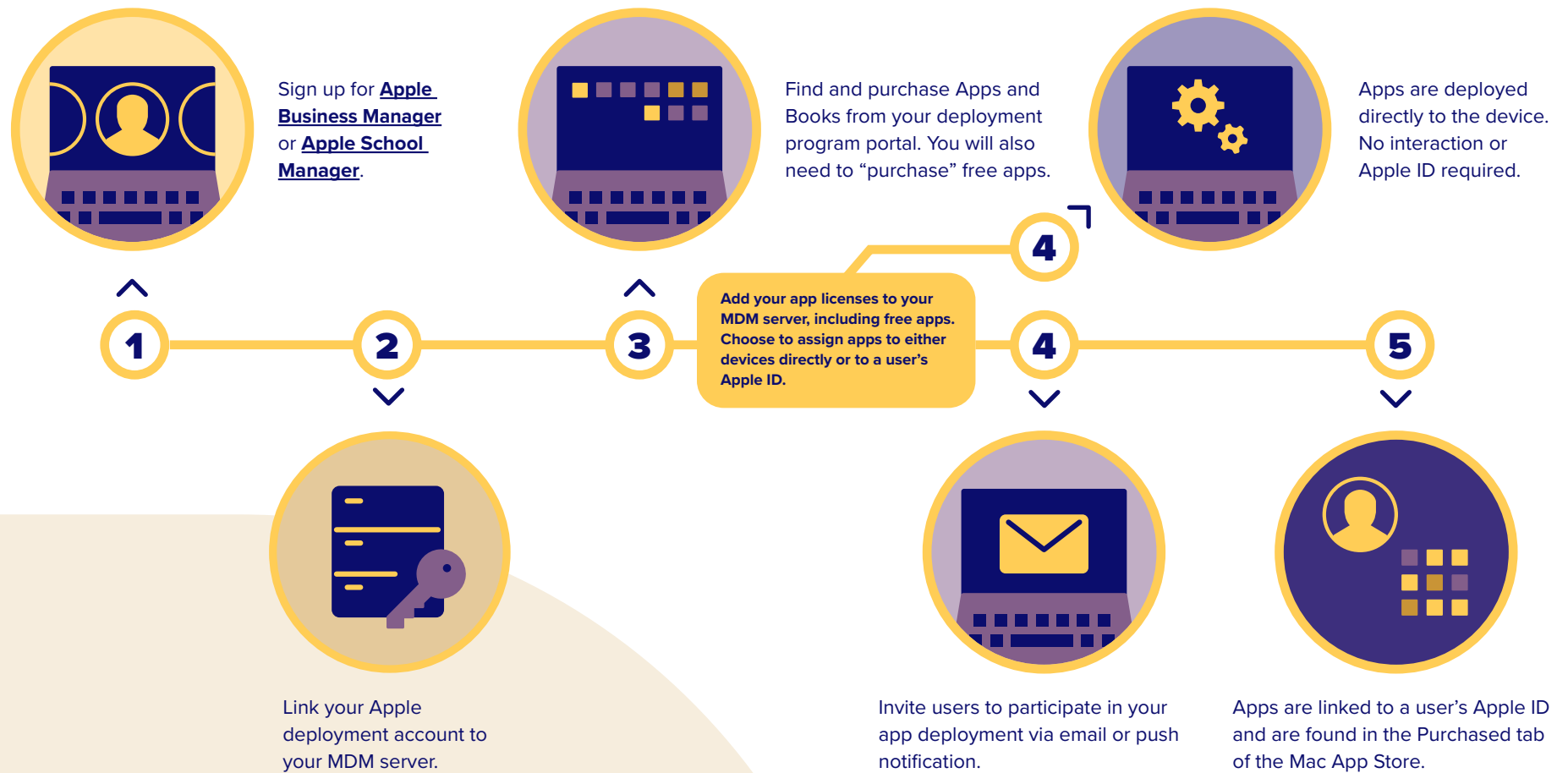
Custom Package Deployment

Sometimes deploying an app isn't enough and you'd like to pre-customize some of the settings. This is the premise for App configurations. App developers can define what settings can be pre-configured by an MDM server for their app. For example, you could deploy the Box app with the server URL pre-populated so users only need to enter their username and password to get the app up and running. Check that your Apple management vendor offers functionality to package and deploy software customizations to your Mac computers.

Deploy Mac Apps and Books with Apple Deployment Programs

With Apple deployment programs, organizations gain the ability to purchase apps in bulk and automatically distribute them to end users and devices.

1 Sign up for **Apple Business Manager** or **Apple School Manager**.

2 Link your Apple deployment account to your MDM server.

3 Find and purchase Apps and Books from your deployment program portal. You will also need to "purchase" free apps.

Add your app licenses to your MDM server, including free apps. Choose to assign apps to either devices directly or to a user's Apple ID.

4 Apps are deployed directly to the device. No interaction or Apple ID required.

4 Invite users to participate in your app deployment via email or push notification.

5 Apps are linked to a user's Apple ID and are found in the Purchased tab of the Mac App Store.

macOS Inventory

Best-in-class Apple management solutions are capable of querying an Apple device to collect a large amount of inventory data, ensuring you always have up to date device information and can make informed management decisions. Inventory can be collected from a device at various intervals and include serial number, OS version, apps installed and much more.

Examples of data collected with an Apple management solution using both MDM and Client Management functionality:

Hardware Details

- Device Type
- Device Model
- Device Name
- Serial Number
- UDID
- Battery Level

Software Details

- OS Version
- List of Apps Installed
- Storage Capacity
- Available Space
- iTunes Store Status

Management Details

- Managed Status
- Supervised Status
- IP Address
- Enrollment Method
- Security Status

Additional Details

- Profiles Installed
- Certificates Installed
- Activation Lock Status
- Purchasing Information
- Last Inventory Update

macOS Inventory

Why does inventory matter?

You can't manage what you can't measure. The inventory data your Apple management solution collects can be used for a wide range of business needs and empower you to answer common questions like:

> **?**
>
> **Are all my devices secure?**
>
> **How many apps do we have deployed?**
>
> **What version of macOS are certain devices running?**

Some management solutions even allow you to collect extra (custom) inventory about specific hardware and software add-ons. For example, you can figure out when a third-party backup utility last ran or what printer drivers are installed.

Check that your Apple management solution collects the **widest range of inventory available**.

Smart targeting

By leveraging inventory data, smart targeting enables you to dynamically group devices and deploy configuration profiles and restrictions to those devices. At Jamf, this is referred to as:
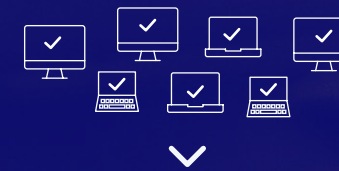
Static Groups

Apply a Profile or Policy

⌄

| 1 | 2 | 3 |
| 4 | 5 | 6 |

Patented Smart Groups

🔍 Find all Macs wtih 8GB RAM, with 80% full hard drives, running 12.2.1 or higher

⌄

Apply a Profile or Policy

Static vs. Smart groups

Static Groups are a set of devices that are defined, like a classroom or a lab. You can apply a management policy to that entire group.

Smart Groups, on the other hand, are dynamic and always changing based on inventory data. This enables you to dynamically group devices and deploy configuration profiles and restrictions to those devices automatically.

Mac Security

The security and privacy of devices and access to corporate resources are a top priority for any organization. To address these worries, Apple has a number of security features built right into macOS. Coupled with an Apple management solution, you can ensure that your devices are not only secure, but your apps and network are as well.
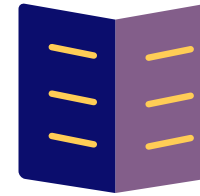
Check out our beginner's guide for detials on macOS security features and Mac-focused endpoint protection.

macOS Security Features

Software Updates

System Integrity Protection (SIP)

Gatekeeper

App Store

FileVault Encryption

XProtect

App Sandboxing

Privacy

Mac Security

Unix is the foundation for Apple's operating systems (OSs), providing a strong kernel at the core. Apple's OSs are built with security in mind and have unique security settings added. Those settings can be managed via an Apple management solution.

Additionally, utilizing Apple's deployment programs with an Apple management solution allow for even more management of those settings within your environment.
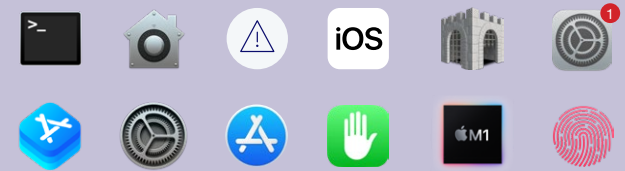
Apple's deployment programs

Management

Apple security features

Apple OSs

Foundation for Apple's OSs UNIX

Mac Security

MDM security commands for macOS

- Enforce FileVault
- Enforce Gatekeeper settings
- Set software update
- Lock and wipe a computer
- Delete restricted apps
- Remove MDM
- Restrict password sharing via AirDrop

Conditional access

The shift in traditional business hours and workspaces has created the modern, mobile workforce. The days of IT simply building a "wall" to protect people, devices and sensitive data are a thing of the past as employees continue to work offsite, outside of traditional business hours and require access to resources stored in the cloud. To accommodate cloud organizations and those that offer choice in computer, it's critical to implement a conditional access path for Mac devices. For organizations leveraging Windows Azure AD and Office 365, best-of-breed Apple management solutions offer built-in conditional access integrations. For more information on macOS and conditional access, read about the **Jamf and Microsoft Enterprise Mobility + Security (EMS) partnership**, which provides an automated compliance management solution for Mac devices accessing applications set up with Azure AD authentication. This collaboration leverages conditional access to ensure that only trusted users on compliant devices, using approved apps, are accessing company data.
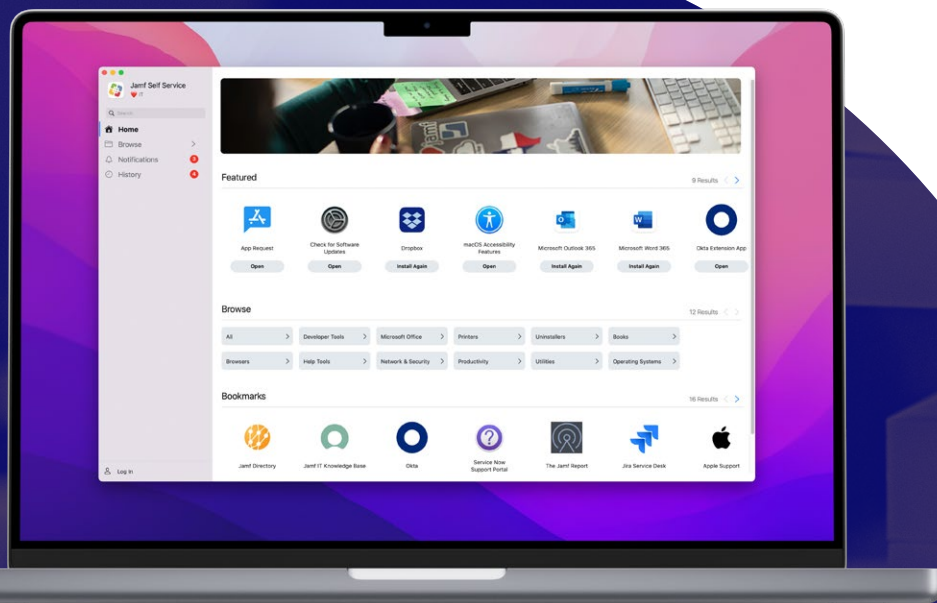
Software upgrades

By developing major versions of macOS annually, Apple has set the pace of innovation. Each year, Apple unveils new and great consumer features, but also adds layers of security and fixes vulnerabilities. These updates can be critical for devices used by employees or students in order to protect their data. Your management solution not only needs to be able to deploy updates from Apple, but also needs to quickly support (**ideally on day zero**) all the new management features that come with them too.

User empowerment and adoption

With the rise in self-sufficiency tools like Lyft, Headspace and Duolingo, today's workforce expects to get the tools they want, when they need them. Enterprise app catalogs meet the needs of users by empowering them with instant access to resources, content, tier one help and trusted apps through a single click from their device — all without submitting a help desk ticket to IT.

APP CATALOG FOR MAC

Example: Jamf Self Service for Mac offers a branded and customizable app catalog that can integrate seamlessly into any organization's internal resources or corporate intranet.

With enterprise app catalogs, users have the ability to access:

- App Store, in-house apps and third-party software

- Email, VPN and other configurations

- E-books, guides and videos

- Bookmarks and shortcuts

- Printer mapping and drivers

- Help desk ticketing and hardware requests

- Password resets and compliance information

- Basic maintenance and system diagnostics

- Software and OS upgrades

- Single Sign-on (SSO) integration

- Localized language support for English, French, German, Japanese and Simplified Chinese

User empowerment and adoption

Benefits of on-demand app and resource catalogs.

What's in it for IT?

- Reduce help desk tickets and support costs while maintaining control of your environment

- Automatically install an app catalog like Jamf Self Service on any managed Mac

- Integrate with directory services to personalize content based on department, user role, location and more

- Automate common IT tasks, such as password resets and system diagnostics, for tier-zero support

What's in it for users?

- Give end users instant access to a full-service, self-help destination of diversified resources

- Intuitive user interface personalized for local language and your environment

- Bookmark common web services such as HR tools, communication platforms or internal resources for an easy entry point to valuable company information

- Install organization-approved apps without IT help

- Fast resolution of common IT issues, such as printer installations and software updates

- Receive real-time notifications for available services and security enhancements

Bonus: Third-party integrations

Mac management is just one piece of your technology portfolio, but it's a critical and instrumental piece. Regardless of whether you use a help desk ticketing system like ServiceNow or an SSO authentication tool like Okta, your Apple device management solution must integrate seamlessly with your existing IT tools.

Amplify the power of what you have and extend the power of your ecosystem by leveraging third-party integrations like those seen in the **Jamf Marketplace**. From cross-industry integrations to specific solutions, integrations like these bridge IT teams and services, creating an integrated, secure and seamless experience for end users.

Your Apple managements solution should offer the ability to brand your app catalog to match your existing corporate resources. This seamlessly integrates your app catalog among existing internal properties, increasing familiarity and ease of use.

Infrastructure planning

Where you host your management environment is just as important as the management solution you choose. Not only does cloud hosting make upgrades a breeze, it takes the added pressure of server management, disaster recovery, and more off of IT.

More and more organizations are moving to the cloud.

Below are just a few reasons why enterprise organizations are going cloud:

Benefits of cloud hosting

Server provisioning, ongoing security and update management

Backup administration and testing

Storage infrastructure for global availability

Disaster recovery; offsite location

Database administration, ongoing security and updates

Server monitoring and response team

Industry-leading
Apple management

Growing enterprise partnerships (IBM, Cisco, SAP, etc.) and a boom in technology choice programs will only bring more Mac, iPad, iPhone and Apple TV devices to your doorstep.

To get the absolute most out of Apple and your technology investment, you require a management solution that matches Apple's intuition.

As the gold standard in Apple management, Jamf is the product most trusted by businesses and schools that want to provide a consistent management experience across the entire ecosystem.

Put our word to the test by taking a free test drive.

Start Trial

Or contact your preferred reseller of Apple devices to take Jamf for a spin.