A COMPREHENSIVE GUIDE

Apple Device Management in Education

jamf

As Apple device adoption rises in 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 of you in established Windows or Google environments.

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

Introduction to Apple device management

Apple Education services and programs overview

Understanding Apple lifecycle management

Insight for infrastructure planning

**Management and Security for Apple in Education**

Introduction to Apple device management

When thinking about how to manage Apple devices, it's helpful to break the lifecycle down into common tasks you might do. These tasks are the same regardless of whether you are managing Apple devices, non-Apple devices or a combination of both.

How MDM works

Most Apple devices are able to 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's 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.
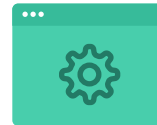
Configuration profiles

... 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 (virtual private network) 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

...are singular commands that you can send to your managed devices to take specific actions. Has a device gone missing? Put it into Lost Mode or 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 actions you can take on a fully managed Apple device.

MDM and client management

While Apple's MDM framework provides the necessary control over iPadOS, iOS and tvOS devices, macOS is a 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 a third-party solution, like Jamf, to take advantage of advanced Mac management.
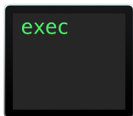
Examples of Client Management Functions

Install PKG/DMG

Enforce FileVault
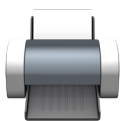
Bind to Directory

Run Scripts

Customize Dock

Set EFI Password

Install Printers

Create Accounts

Set Software Update

Apple services and programs

As Apple devices became more popular in the enterprise and education, challenges arose about how to best deploy devices at scale, how to address Apple IDs and the purchasing of apps. Apple, of course, looked to solve these issues and introduced various programs and services to take device management one step further, making it easier and more cost effective to manage devices in bulk.

Not every 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

This automated enrollment process allows you to configure any Mac, iPad, iPhone or Apple TV purchased from Apple or an Apple authorized reseller and customize each device for your users – all without ever having to touch the device. Hardware purchases are associated with your Apple customer number or reseller ID and automatically enroll a device into management under an Apple management solution. Automated Device Enrollment enables you to provide a great zero-touch experience for end users. They simply open up the box, turn on the device and get to work — regardless of if your employees is on-site or remote.

Apps and Books

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 later reassigned as deployment needs change. You can link a token (received from Apple) to your MDM solution for assignment and distribution. If you're an education institution, your instance is built directly within Apple School Manager.

Device Supervision

Supervision is a special mode of iPadOS, iOS and tvOS management where IT is granted greater control over devices they own when enrolled via Automated Device Enrollment, User Approved MDM or Apple Configurator. A large number of management features including Managed Lost Mode, blocking apps and silently installing apps all require supervision. It is recommended that corporate-owned and school-owned devices be put into supervision mode.

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. If you're an education institution, your students will receive a different type of Apple ID (see next page).

Apple School Manager

Launched in 2017, 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 Automated Device Enrollment and volume purchasing of Apps and Books and other classroom management tools, such as the Classroom app, in one portal. Apple School Manager enables Managed Apple IDs and Shared iPad and can be integrated with your school's Student Information Systems (SISs).

Managed Apple IDs

Apple School Manager enable Managed Apple IDs for users. Managed Apple IDs are created in the Apple School Manager portal, and can be integrated with a school's student information systems (SISs). They do not require special permission and, because they are owned by your organization, they allow IT admins to create and dynamically update user information or even assign apps and other services to the the user or device.

Shared iPad

Shared iPad extends the value of an iPad device by providing multiple users access to the device. Each user, with their own Managed Apple ID, can log in and out while their apps, content and work stay intact (requires Apple School Manager or Apple Business Manager.)

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 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 Inventory management

Reporting on the status of each device.

5 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 devices in your environment. This ensures both the security and maximized potential of your Apple devices.
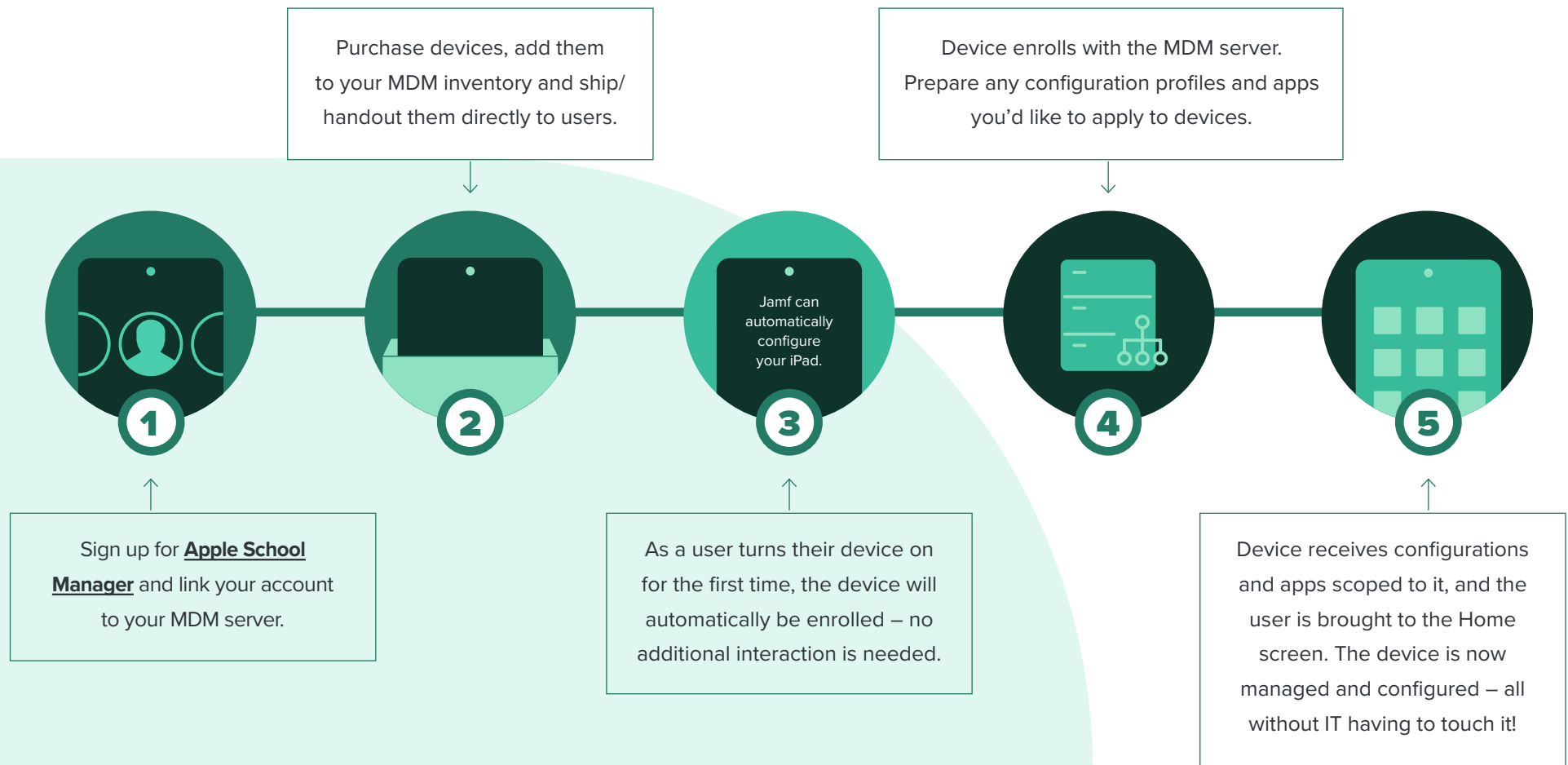
Deployment and Provisioning

1

Before configuring devices for end users, devices must be enrolled into management within an MDM solution. There are several enrollment methods available, but highlighted below are recommended for education institutions looking for a streamlined and positive end-user experience:

	Description	User Experience	Supervision (iOS only)	Best For
Automated Device Enrollment with Apple School Manager	Automatic enrollment over the air	User receives shrink-wrapped box, and the device is automatically configured when turned on	Yes—wirelessly	Shipping devices to remote faculty, students or to speed up the onboarding process. Providing users with an out-of-box experience
Account-driven User Enrollment	Manual enrollment over the air via Settings App	Users install the MDM profile by visiting the enrollment portal in the Settings app of their device	No	Unmanaged, personally owned devices that need to be enrolled into a new MDM server
User-initiated enrollment	Manual enrollment over the air or over the air via URL	User visits a specific URL to configure their device	No	Unmanaged devices currently in the field or devices that need to be reenrolled into a new MDM server
Apple Configurator	Enrollment through a Mac app to deploy iPad, iPhone or Apple TV devices, or Mac enrollment through an iOS app)	IT manages the setup process and hands devices to users	Yes—wired	Shared and cart-device models, labs

Automated Device Enrollments with Apple School Manager

Purchase devices, add them to your MDM inventory and ship/ handout them directly to users.

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

Jamf can automatically configure your iPad.

1

2

3

4

5

Sign up for **Apple School Manager** and link your account to your MDM server.

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

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

Configuration management

When it comes to configuring Apple devices, 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, iOS, iPadOS and tvOS by creating configuration profiles. These small XML files can be distributed to devices utilizing a managed solution. You can apply Wi-Fi, VPN, email settings and more so users can seamlessly connect to the resources they need.

Smart Targeting

Collect inventory details, including custom inventory attributes you define, for all of your managed devices, to identify which ones require software updates, security hardening or other management actions. 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.

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

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.

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.

App management

App fundamentals

Today, we are all familiar with the App Store on our iPhone, iPad and Apple TV devices. They are the only way for consumers to get apps on their devices. Apple reviews the developer's code 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 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 management tools, like Jamf Pro or Jamf School, 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 Macs — all without users needing to be admins.

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

For software that is in the App Store, we can use an Apple program to license and distribute apps to devices all without needing Apple IDs.

Apple devices are wildly popular among consumers because of the native communication, learning and productivity tools available right out of the box, but the rich library of apps in the App Store are what set the Apple ecosystem apart. 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 (or many) of the millions of apps from the App Store 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.

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.

Here are three app management options you can utilize for your devices.

Deploy Apps with Apple School Manager or Apple Business Manager

Place Apps in an on-demand self service catalog with Jamf Pro (more below)

App Deployment for Apple TV

App management

When deploying App Store apps via Apple School Manager, you gain extra security and configurations for that app (iOS only).

Here's what's possible:

What is a Managed App?

Introduced in iOS 5, managed apps differ from a standard app because they are flagged as owned by an organization. Specifically, managed apps are distributed via MDM technology and can be configured and reassigned by MDM.

Managed Open In

Managed Open In takes the concept of managed apps a step further by controlling the flow of data from one app to another. With MDM, organizations can restrict what apps are presented in the iOS share sheet for opening documents. This allows for truly native data management without the need for a container.
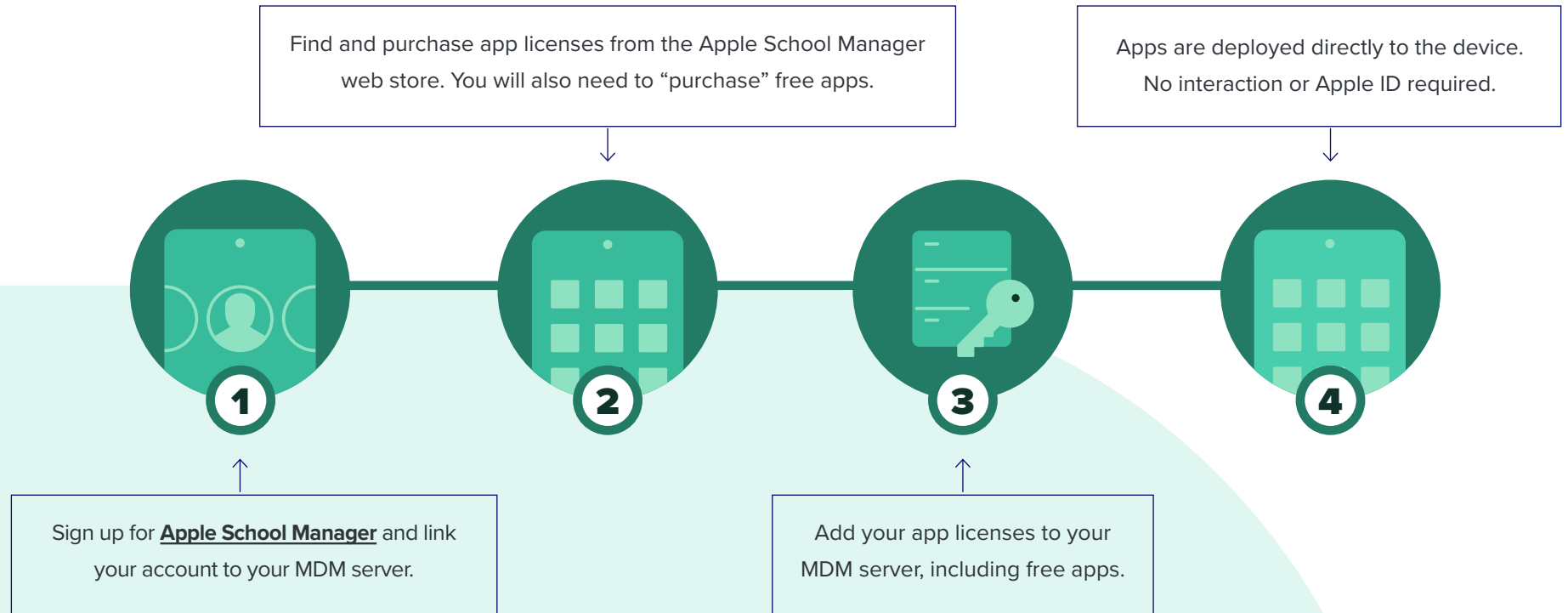
App Configurations

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 prepopulated so users only need to enter their username and password to get the app up and running.

Deploy Apps with Apple School Manager for Education

Find and purchase app licenses from the Apple School Manager web store. You will also need to "purchase" free apps.

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

1

2

3

4

Sign up for **Apple School Manager** and link your account to your MDM server.

Add your app licenses to your MDM server, including free apps.

App Deployment for Apple TV

Apple TV provides support for enterprise apps (commonly referred to as in-house apps). These apps can be uploaded to your management server and pushed out to your Apple TV devices automatically and without Apple IDs, just like your iOS devices. Popular enterprise apps for Apple TV include digital signage, emergency alerts and more.

Configuration profiles

Using an MDM solution, IT can define settings with tvOS configuration profiles and distribute them to Apple TV devices. As a result, Wi-Fi, restrictions and AirPlay settings are more easily applied over the air. Further, Apple TV devices can be put in Single App Mode to customize the Apple TV experience by class or Conference Display Mode for an intuitive presentation workflow.

Smart targeting

With the ability to automatically collect inventory details, including Apple TV device names from all managed devices, IT can quickly and accurately identify which devices require action. Based on this inventory information, IT can build targeted groups to trigger automatic device management tasks. For example, IT can now find all Apple TV devices without AirPlay settings configured and then deploy that configuration.

Custom app and display support

If and when businesses create unique app experiences to deliver a customized full-screen experience, IT can leverage MDM to deploy these custom apps over the air. Additionally, with the latest tvOS, IT can now set a Home Screen layout, show/hide apps as well as restrict media content based on age guidance.

Want the ins and outs of Apple TV?

Check out our
Apple TV Management for Beginners e-book.

MENU

Inventory

MDM 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 MDM

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
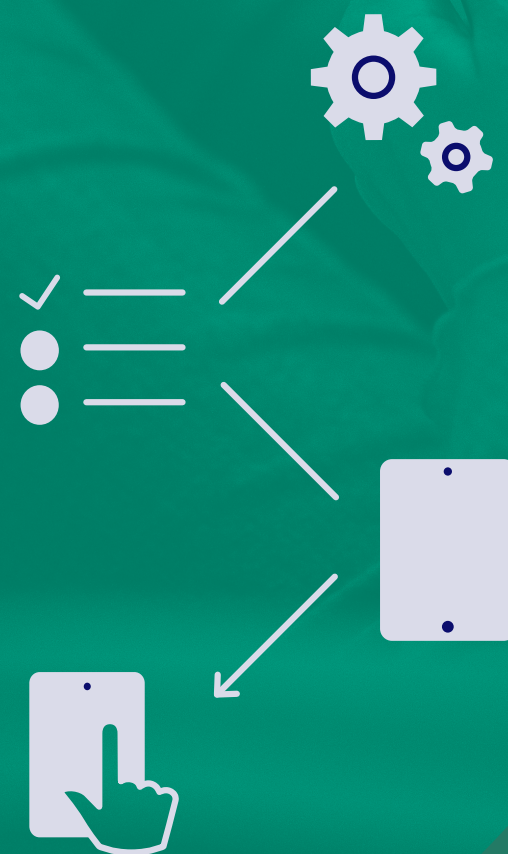
Inventory

Why does inventory matter?

You can't manage what you can't measure. The inventory data your MDM 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 iOS, macOS and tvOS 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 utilitiy last ran or what printer drivers are installed.

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 Smart Groups.
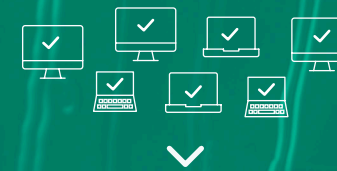
Static Groups

Apply a Profile or Policy

⌄

| 1 | 2 | 3 |
| 4 | 5 | 6 |
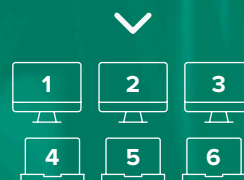
Patented Smart Groups

🔍 Find all Macs wtih 8GB RAM, with 80% full hard drives, running 15.1.1 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.

Security and privacy

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, iPadOS, iOS and tvOS.

Coupled with an MDM solution, you can ensure that not only your devices are secure, but your network, data and apps are as well.

iOS/iPadOS Security Features

Software Updates

Secure System

App Store

Touch ID

Hardware Encryption

App Sandboxing

Privacy

Supervision

macOS Security Features

Software Updates

System Integrity Protection (SIP)

Gatekeeper

App Store

FileVault Encryption

XProtect

App Sandboxing

Privacy

tvOS leverages many of the security features found in iOS, such as direct software updates from Apple, vetted and secure App Store apps, app data protection with App Sandboxing and deeper levels of management through supervision.

With management, Apple TV settings can be deployed to automate AirPlay security. This allows you to pair Apple devices with Apple TVs, so only the appropriate devices share their screens wirelessly.

5

Security

Unix is the foundation for Apple's operating systems, 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 MDM solution.

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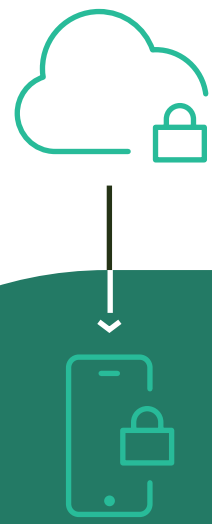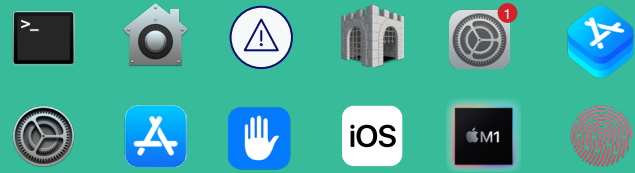
Apple's deployment programs

Management

Apple security features

Apple OSs

Foundation for Apple's OSs UNIX

Security

MDM security commands for macOS, iOS, iPadOS and tvOS

macOS

- Enforce FileVault
- Enforce Gatekeeper settings
- Set software update
- Lock, wipe and restart computer
- Delete restricted apps
- Remove MDM

iOS/iPadOS

- Enable Lost Mode
- Lock and wipe a device
- Remote wipe
- Update iOS
- Clear restrictions and passcodes
- Remove MDM

tvOS

- Enable Lost Mode
- Lock and wipe a device
- Remote wipe
- Update iOS
- Clear restrictions and passcodes
- Remove MDM

MDM Lost Mode for iOS/iPadOS

By utilizing Apple's Lost Mode with an MDM solution, you can lock, locate and recover lost or stolen iOS and iPadOS devices without compromising privacy through ongoing tracking. When Lost Mode is activated, iOS devices receive a customized lock screen message, are disabled from use and send the location to IT.

Conditional access

For organizations leveraging Windows Azure AD and Office 365, it's critical to implement a conditional access path for Mac devices. Best-of-breed MDM solutions offer built-in conditional access integrations.

Software upgrades

By developing major versions of macOS, iOS, iPadOS and tvOS 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 all the new management features that come with them too.

User empowerment and adoption

With the rise in self-sufficiency tools like, Headspace and Duolingo, today's teachers and students expect to get the tools they want, when they need them. The Jamf School student app, or Self Service for Jamf Pro users, 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.
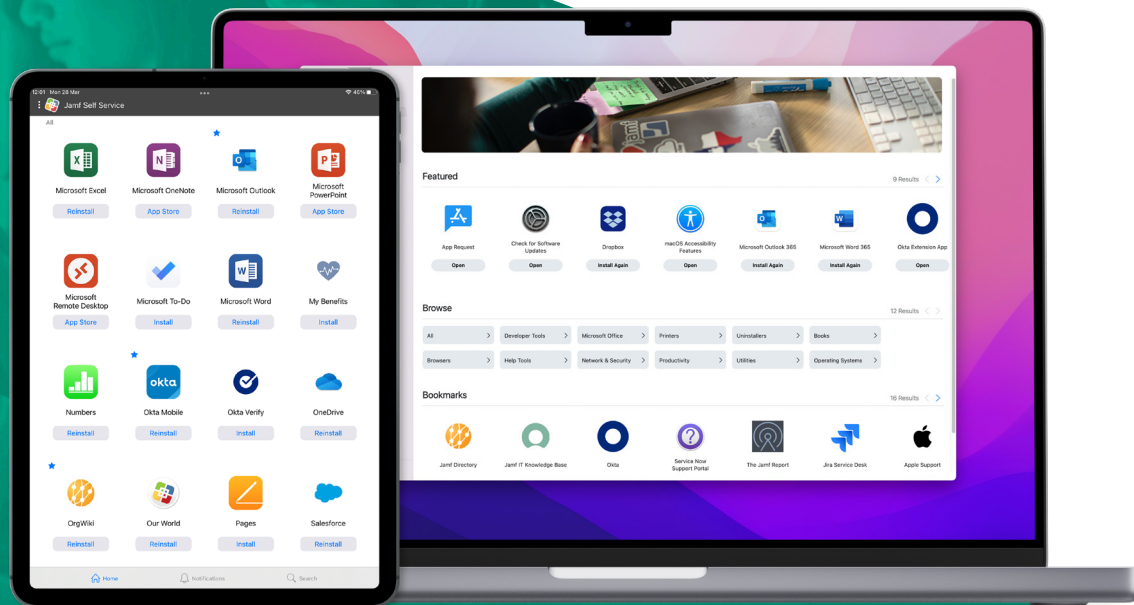
APP CATALOG FOR MOBILE

APP CATALOG FOR MAC

Jamf Self Service for Jamf Pro offers a branded app catalogue that can integrated seamlessly into any education environment. Jamf School's Student app offers even more powerful workflows for the student including access to apps, resources and profiles as well as messgaing with the teacher to enhance teaching and learning workflows and empower student success.

With education 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 for Jamf Pro or Jamf Teacher and Student apps for Jamf School on any managed Mac, iPad or iPhone

- 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 teachers, staff and students?

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

- Intuitive user interface personalized for local language and your own education environment

- Bookmark common web services such as learning portals, intranet sites, communication platforms or internal resources for an easy entry point to valuable information and learning resources

- Install education-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

Apple device 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 Incident IQ or an SSO authentication tool like Google or Microsoft, 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 IT, Teachers, Staff and Students.

Best-of-breed MDM solutions 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 schools and universities 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

Management and Security of Apple in Education

Apple continues to build an interconnected ecosystem, with apps and services being cross compatible across devices. Growing education partnerships (Shaw Acadmey Trust, Califonia State University, Oasis Horizons Project) and a boom in technology to enahnce learning and offer remote teaching and learning, Universites offering staff, faculty and student 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 need a management solution that matches Apple's intuition and has proven from day one that helping people succeed with Apple is top priority.

As the go-to platform for Apple management and security, Jamf is the product most trusted by schools that want to offer Apple and provide a consistent management experience across the entire ecosystem.

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

Request Trial

Or contact your preferred reseller of Apple devices.