A COMPREHENSIVE GUIDE

Apple Device Management
FOR BEGINNERS
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 of you in established Windows environments.

Forbes recently reported Apple device growth at 20 percent in the enterprise and that’s on track to double by 2020.

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

- Introduction to Apple device management
- Explanation of Apple services and programs available
- Outline of lifecycle management stages
- Insight for infrastructure planning
- Overview of the industry-leading Apple management solution
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 Server (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**

...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 an MDM solution such as Jamf Pro.

**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 the different actions you can take on a fully managed Apple device.
MDM and client management

While Apple’s MDM framework provides the necessary control over iOS and tvOS devices, 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 a third-party solution, such as Jamf Pro, 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 schools and the enterprise, questions about how to best deploy devices at scale, how to address Apple IDs and the purchasing of apps arose. 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.

### 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.

### 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 (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.

### 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 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 system (SIS).
Managed Apple IDs

Apple School Manager for educational 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. Additionally, managed Apple IDs are created in the Apple School Manager portal and can sync with Classroom data.

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

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 personal Apple ID on the job, or you can avoid using Apple IDs altogether thanks to the ability to deploy Apps and Books to devices directly without an Apple ID. If you’re an education institution, your students will receive a different type of Apple ID.

Classroom App

An instructional tool for iPad, Apple’s Classroom app empowers teachers to streamline classroom instruction, encourage interaction and collaboration, focus student iPad devices on a specific app or webpage, and view student devices to check for understanding. New with macOS Mojave, the Classroom App is now available for Mac education customers as well.

Device Supervision

Supervision is a special mode iOS and tvOS devices are placed into when enrolled via Apple Business Manager, Apple School Manager or Apple Configurator. Supervision gives institutions greater control over the iOS devices they own. A larger number of management features including Managed Lost Mode, blocking apps and silently installing apps all require supervision. It is recommended that institutionally-owned devices be put into Supervision mode.
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 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.

4. **Inventory**
   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**

Before configuring devices for end users, devices must be enrolled into management within an MDM solution. There are several enrollment methods available, but Zero-Touch Deployments with Apple Business Manager and Apple School Manager are recommended for enterprise and education institutions looking for a streamlined and positive end user experience:

<table>
<thead>
<tr>
<th>Description</th>
<th>User Experience</th>
<th>Supervision</th>
<th>Best For</th>
</tr>
</thead>
</table>
| **Zero-Touch Deployment with Apple Business Manager and Apple School Manager** | Automatic enrollment over the air | User receives shrink-wrapped box, and the device is automatically configured when turned on | Yes—wirelessly | Providing users an out-of-box experience. With Zero-Touch Deployment you can:  
- Ship devices to remote employees  
- Speed up the onboarding process  
- Support education institutions with iPad programs |
| **Apple Configurator** | Enrollment through a Mac app that connects to devices via USB (does not apply to Apple TV 4K) | IT manages the setup process and hands devices to users | Yes—wired | • Shared and cart-device models, labs  
• Devices purchased through a retailer such as Best Buy |
| **User-initiated enrollment via URL** | Manual enrollment over the air | 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 |
For education customers:
sign up for Apple School Manager
For non-education customers: sign up for Apple Business manager and add your MDM server to the portal.

1. Purchase devices and assign them to your MDM server within Apple School Manager or Apple Business Manager. Ship them directly to users.

2. Jamf can automatically configure your iPad.

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

4. 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!

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

BEST PRACTICE
Deploy Apps and Books with Apple Business Manager and Apple School Manager
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 iOS, macOS 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.

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.

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.

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.

Don’t know where to start? Check out a list of MDM configuration profiles here, or join the conversation on Jamf Nation.
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 Microsoft Office and Adobe Creative Suite, so it’s important to have a Mac client management tools that’s able to deploy custom software. Some management tools, like Jamf Pro, 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.

Here are the most effective ways to manage and deploy apps to your devices:

For the enterprise:

Deploy Apps and Books with Apple Business Manager

For the education institutions:

Deploy Apps and Books with Apple School Manager

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.
When deploying Apps and Books via Apple Business Manager and Apple School Manager, you gain extra security and configurations for that app (iOS and tvOS only). Here’s what’s possible:

**What is a Managed App?**
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 pre-populated so users only need to enter their username and password to get the app up and running.
Deploy Apps and Books with Apple Business Manager and Apple School Manager

**BEST PRACTICE**

1. Sign up for Apps and Books via Apple School Manager or Apple Business Manager and add your MDM server to your portal.

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

3. 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.

5. Find and purchase app licenses from the Apps and Books section of Apple Business Manager or Apple School Manager. You will also need to “purchase” free apps.

6. Invite users to participate in your Apps and Books deployment via email or push notification.

7. Apps are linked to a user’s Apple ID and are found in the Purchased tab of the App Store.
App Deployment for Apple TV

Apple TV provides support for both App Store apps as well as 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.

App and display support

IT can leverage MDM to deploy both custom in-house and App Store apps directly to Apple TV devices. Additionally, IT can 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 deployment?

Check out our Apple TV Management white paper
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 utility 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

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

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.
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, iOS and tvOS.

**iOS Security Features**
- Touch ID
- Privacy
- Hardware Encryption
- App Sandboxing
- App Store

**macOS Security Features**
- Software Updates
- System Integrity Protection (SIP)
- Gatekeeper
- App Sandboxing
- Privacy
- FileVault Encryption

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

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.
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, utilizing Apple’s deployment programs with an MDM solution allow for even more management of those settings within your environment.
### MDM security commands for macOS, iOS and tvOS

<table>
<thead>
<tr>
<th>macOS</th>
<th>iOS</th>
<th>tvOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Enforce FileVault</td>
<td>• Restrict Autofill passwords</td>
<td>• Remote wipe</td>
</tr>
<tr>
<td>• Enforce Gatekeeper settings</td>
<td>• Enable Lost Mode</td>
<td>• Restart device</td>
</tr>
<tr>
<td>• Set software update</td>
<td>• Lock and wipe a device</td>
<td>• Single App Mode</td>
</tr>
<tr>
<td>• Lock, wipe and restart computer</td>
<td>• Remote wipe</td>
<td>• Delete restricted apps</td>
</tr>
<tr>
<td>• Delete restricted apps</td>
<td>• Update iOS</td>
<td>• Block passwords via proximity requests</td>
</tr>
<tr>
<td>• Remove MDM</td>
<td>• Clear restrictions and passcodes</td>
<td>• Block passwords via proximity requests</td>
</tr>
<tr>
<td>• Restrict Password sharing via AirDrop</td>
<td>• Remove MDM</td>
<td></td>
</tr>
</tbody>
</table>

**MDM Lost Mode for iOS**

By utilizing Apple’s Lost Mode with an MDM solution, you can lock, locate and recover lost or stolen iOS 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. For more information go here.

**Software upgrades**

By developing major versions of macOS, iOS 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 (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, Amazon Prime and WebMD, 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.

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

- App Store, B2B, 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

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

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.

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 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.
More and more organizations are moving to the cloud.

Below are just a few reasons why enterprise organizations like Eventbrite 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

Apple continues to build an interconnected ecosystem, with apps and services being cross compatible across devices. 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 and has proven from day one that helping people succeed with Apple is top priority.

As the gold standard in Apple management and with dedication to the Apple ecosystem since 2002, Jamf is the product most trusted by businesses and schools that want to offer Apple and provide a consistent management experience across the entire ecosystem.

By integrating with all Apple services and providing immediate support for Apple operating systems and features, Jamf empowers you with the tools necessary to address all support needs, and gives you the freedom to focus on strategic tasks so you can save your organization time and money.

Put our word to the test by taking a free test drive and you’ll see why 96 percent of Jamf customers stick with us year over year.

Start Trial