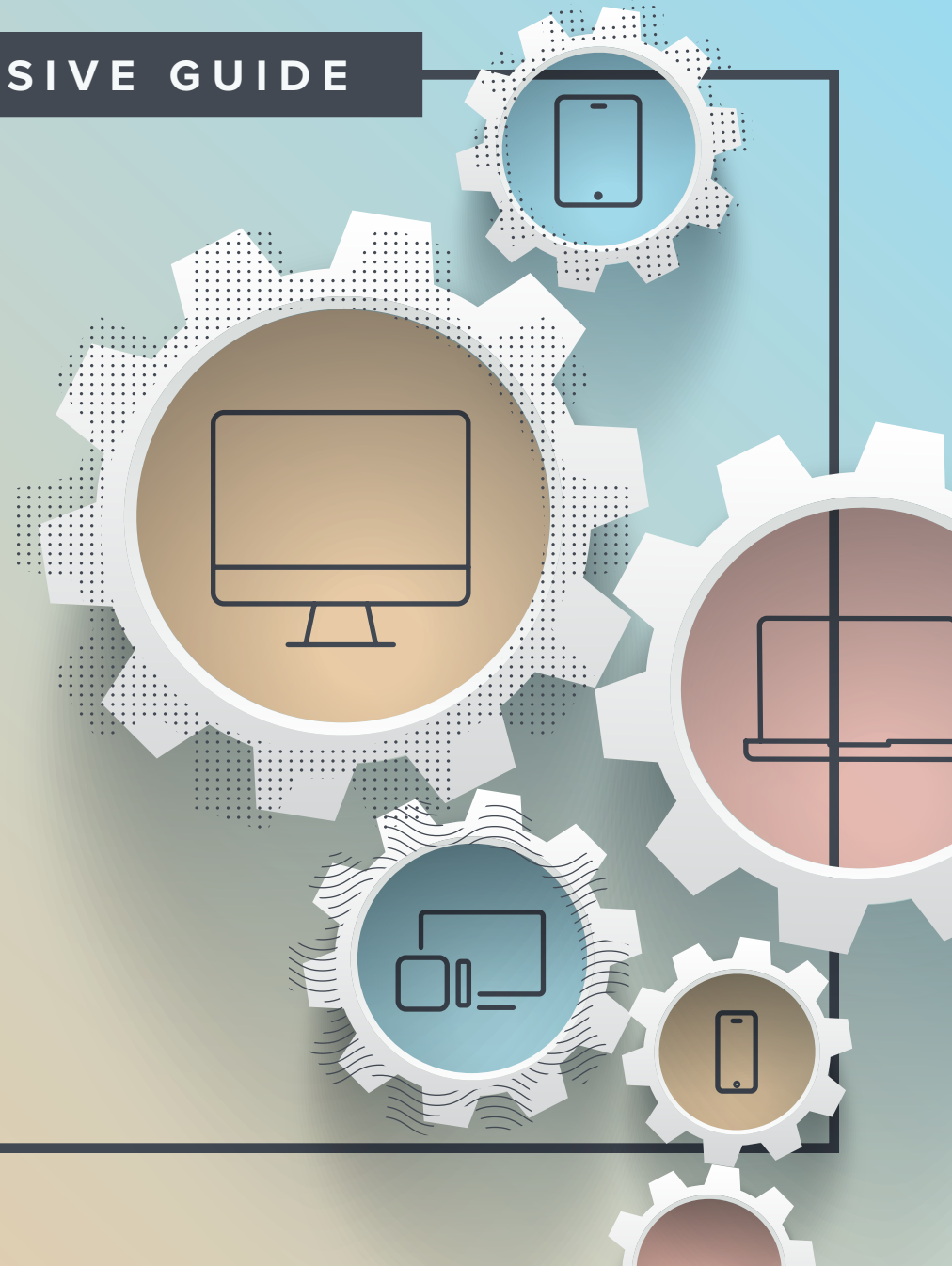


A COMPREHENSIVE GUIDE

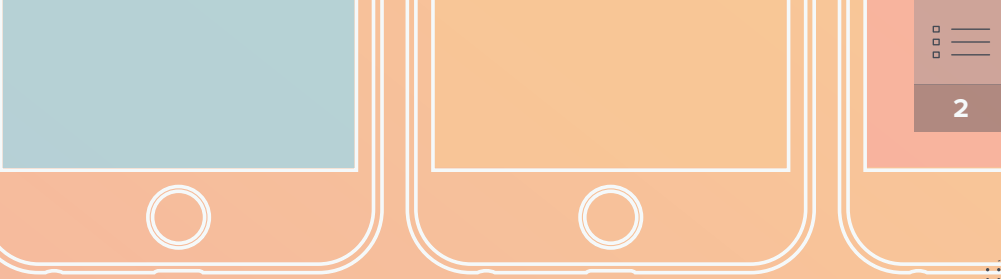
Apple Device Management

FOR BEGINNERS



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

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.



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

PAGE 3



Explanation of Apple services and programs available

PAGE 5



Outline of lifecycle management stages

PAGE 7



Insight for infrastructure planning

PAGE 24



Overview of the industry-leading Apple management solution

PAGE 25



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 if you are managing Apple, PCs, Android or all the above.

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.



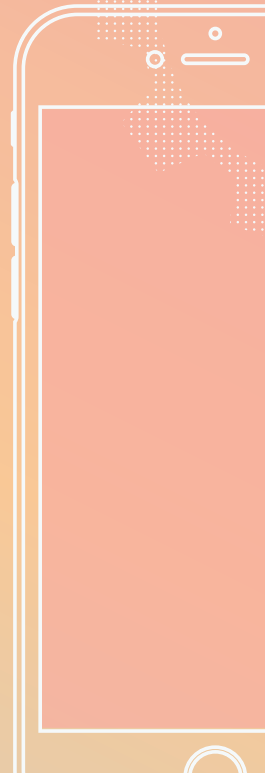
Configuration profiles

...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



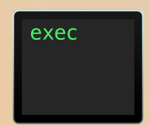
Install PKG/DMG



Enforce FileVault



Bind to Directory



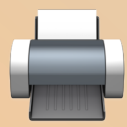
Run Scripts



Customize Dock



Set EFI Password



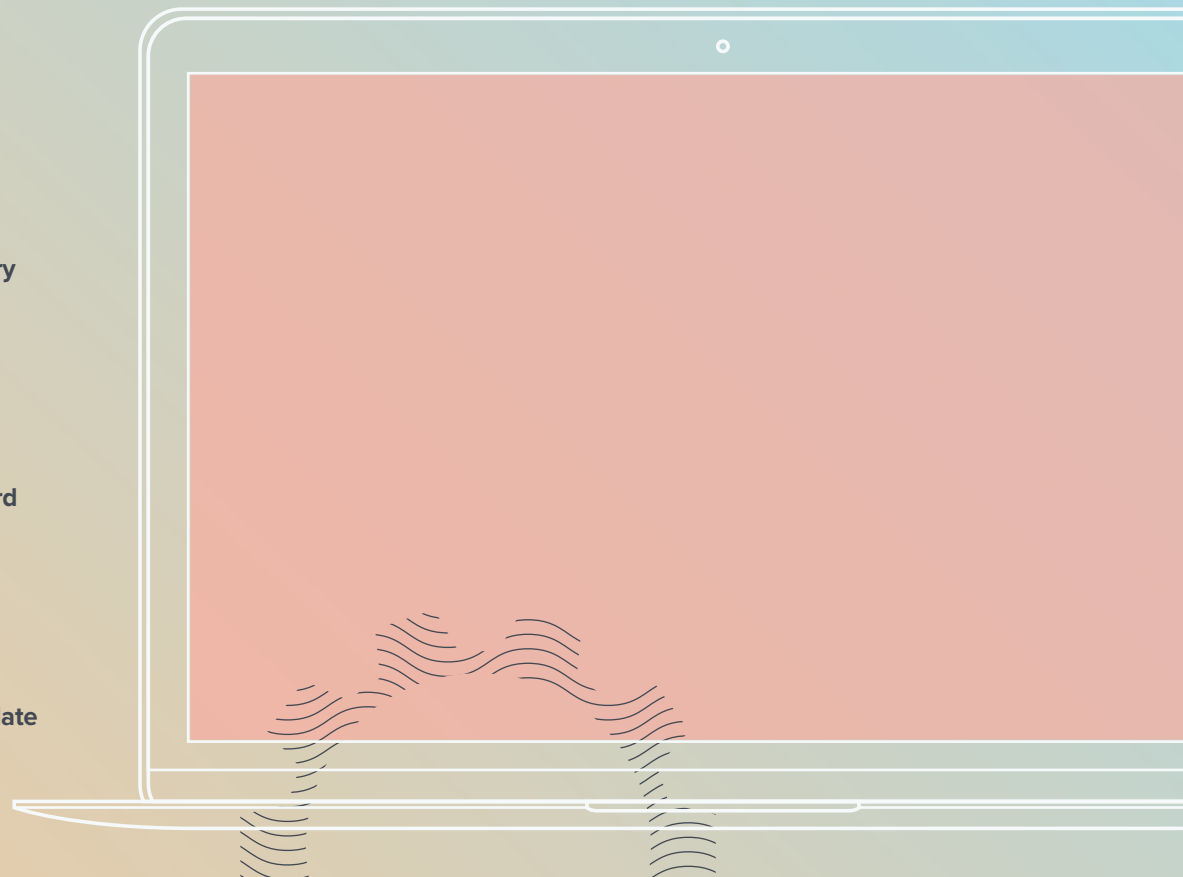
Install Printers



Create Accounts



Set Software Update





Apple services and programs

As Apple devices became more popular in 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.



Device Enrollment Program (DEP)

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 linked with DEP to automatically enroll a device into management under an Apple management solution. DEP 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 productive.



Device Supervision

Supervision is a special mode iOS and tvOS devices are placed into when enrolled via DEP or Apple Configurator. Supervision gives institutions greater control over the iOS devices they own. 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.



Volume Purchase Program (VPP)

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



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 (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 DEP, VPP 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).



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.



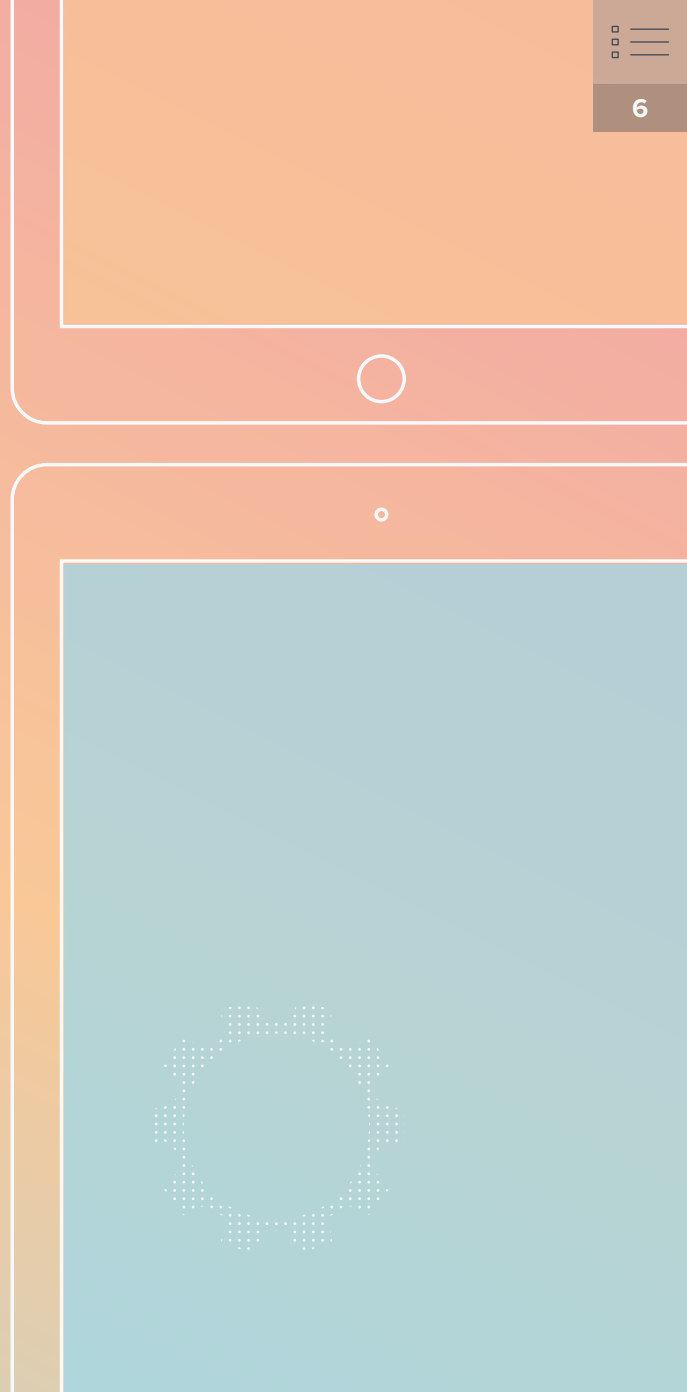
Managed Apple IDs

For education institutions, 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.



Shared iPad

By offering students a personalized learning experience, Shared iPad extends the value of an iPad device. Several students, each with their own unique ID, can log in and out while their apps, content and work stay intact. Shared iPad is only available for education institutions and requires Apple School 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 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.

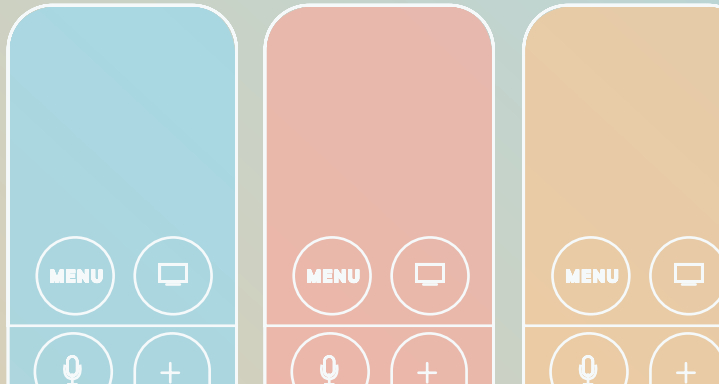
5 Security

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.





1

Deployment and Provisioning

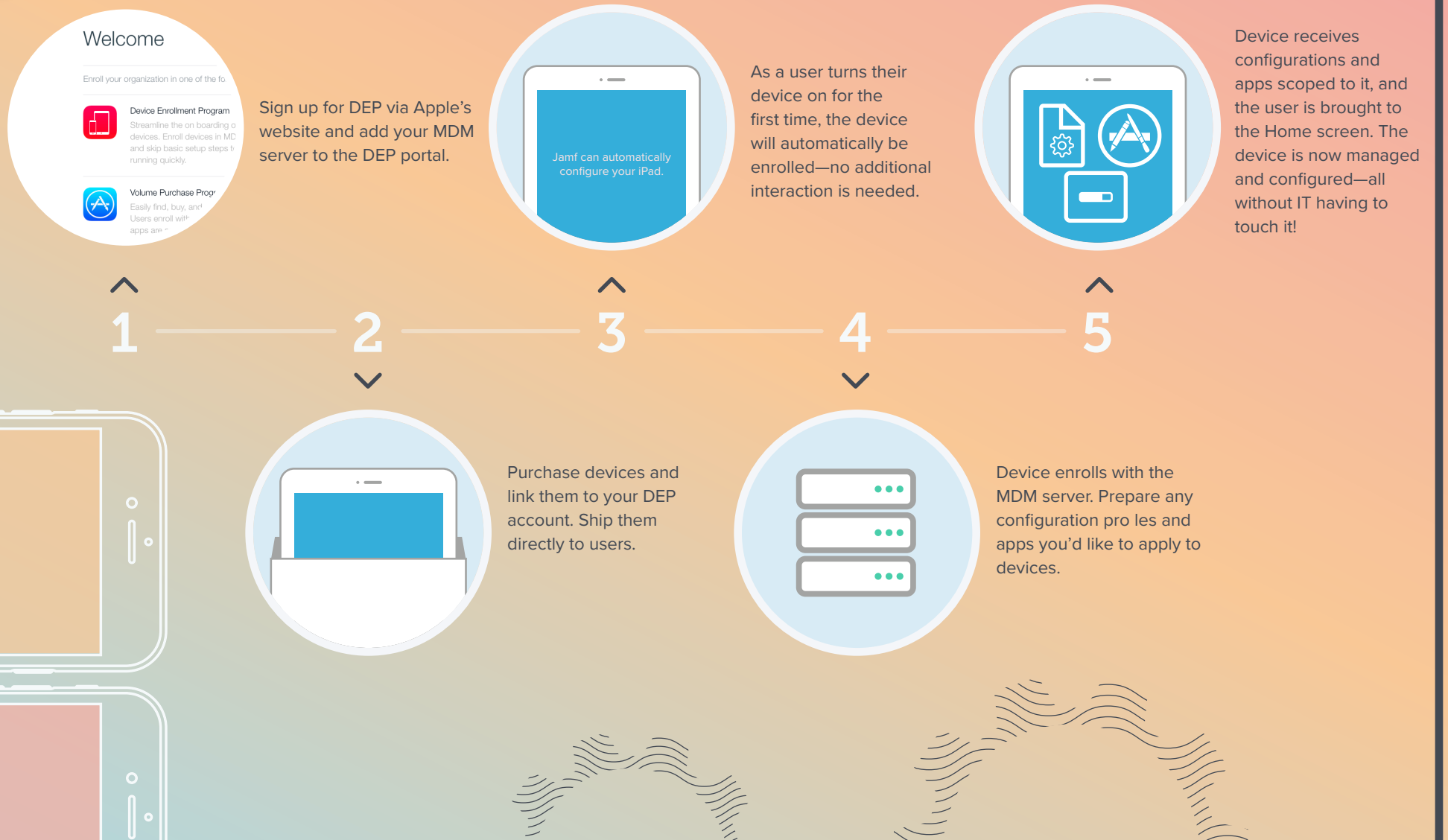
Before configuring devices for end users, devices must be enrolled into management within an MDM solution. There are several enrollment methods available, but the two highlighted below are recommended for enterprise and education institutions looking for a streamlined and positive end user experience:



	Description	User Experience	Supervision (iOS only)	Best For
Device Enrollment Program (DEP)	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 employees or to speed up the onboarding process. Providing users an out-of-box experience.
Automated deployment with Apple School Manager (Education only)	Automatic enrollment over the air	User receives shrink-wrapped box, and the device is automatically configured when turned on	Yes—wirelessly	K-12 schools with iPad programs. Providing students with an out-of-box experience.
Apple Configurator (iOS and tvOS only)	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
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

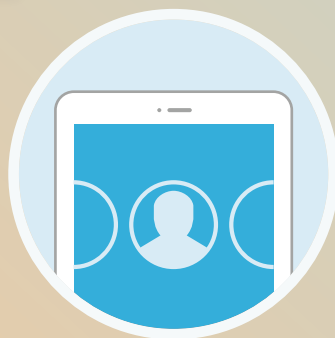
BEST PRACTICE

Zero-Touch Deployments with Device Enrollment Program



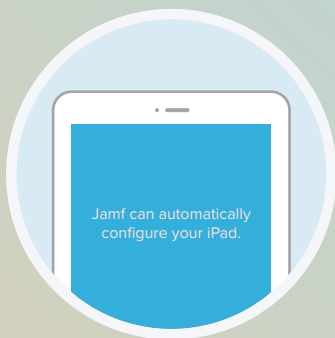
BEST PRACTICE

Zero-Touch Deployments with Apple School Manager



Sign up for Apple School Manager via <https://school.apple.com/> and add your MDM server to the Apple School Manager portal.

1



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

3



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

2

4



Purchase devices and link them to your DEP account. Ship them directly to users.



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

When DEP or Apple School Manager are not possible, organizations can provision Macs via traditional imaging workflows (less preferred over DEP), leverage Apple Configurator to enroll iOS and tvOS devices, or use user-initiated enrollments for Mac and iOS devices.

2 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.

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



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.

3 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.

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.

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



Deploy Apps
with VPP for the
Enterprise



Deploy Apps with
Apple School
Manager for
Education

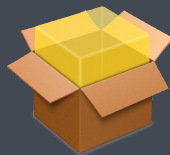


App Deployment
for Apple TV

SOFTWARE INSTALLS AND PATCHING



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.

3 App management

When deploying App Store apps via VPP or 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.



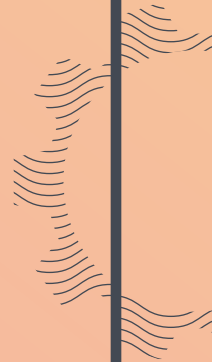
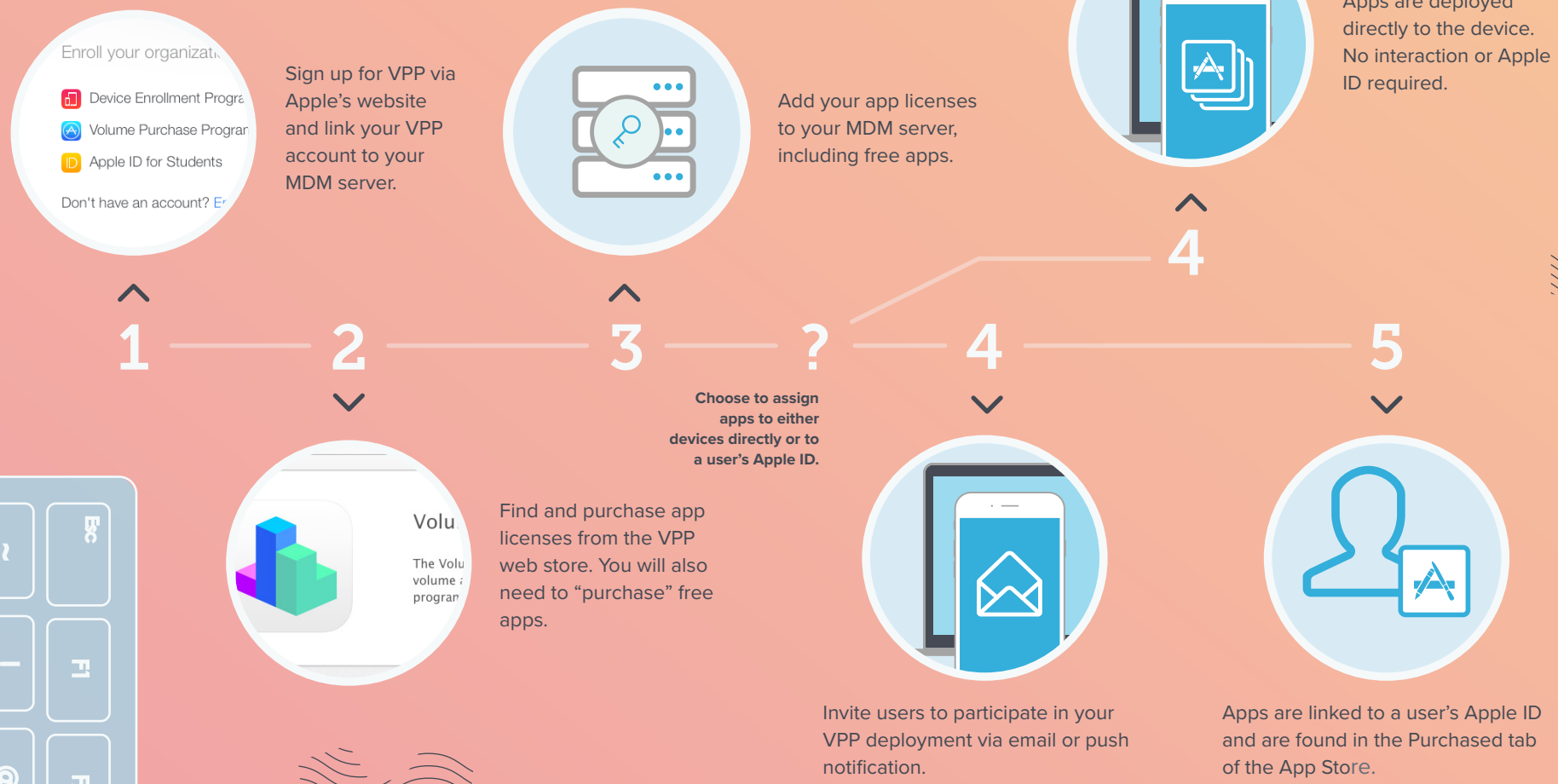
App Configurations

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

BEST PRACTICE

Deploys Apps with VPP for the Enterprise

VPP for the enterprise (soon to be Apple Business Manager): The ability to purchase apps in bulk and automatically distribute them.



BEST PRACTICE

Deploy Apps with Apple School Manager for Education

Apple School Manager for education: A web portal to set up Apple IDs, manage device enrollment and distribute apps – all from one location.



Sign up for Apple School Manager via <https://school.apple.com/> and add your MDM server to the Apple School Manager portal.



1



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



3



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



2



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



4

BEST PRACTICE

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 deployment?

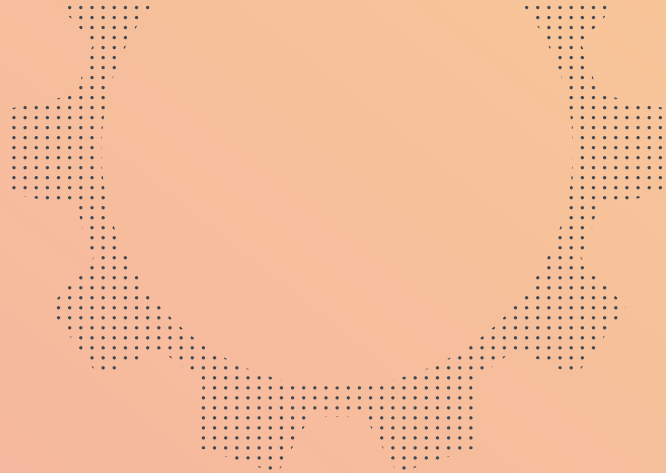


Check out our
[Apple TV Management white paper](#)

MENU



4 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



4 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

Apply a Profile or Policy



Smart Groups

Find all Macs with 8GB RAM, with 80% full hard drives, running 10.12.2 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.

5 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, iOS and tvOS.

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



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



5 Security

MDM security commands for macOS, iOS and tvOS



macOS

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



iOS

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



tvOS

- Remote wipe
- Restart device
- Single App Mode
- Delete restricted apps



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

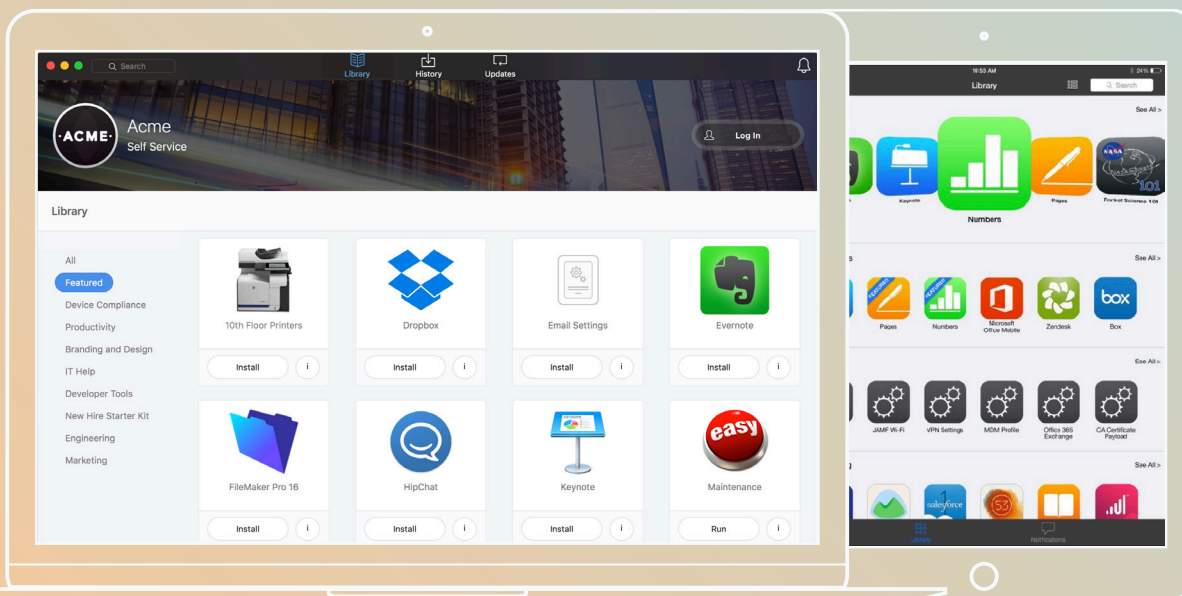
By developing major versions of macOS, iOS and tvOS annually, Apple has set the pace of innovation. Each year, Apple unveils new and great consumer features, but also adds layers of security and fixes vulnerabilities. These updates can be critical for devices used by employees or students in order to 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.

6 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.

App catalog for Mac

App catalog for mobile



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.

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

6 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.



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 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](#)