Apple OS

Upgrades Guide For Beginners

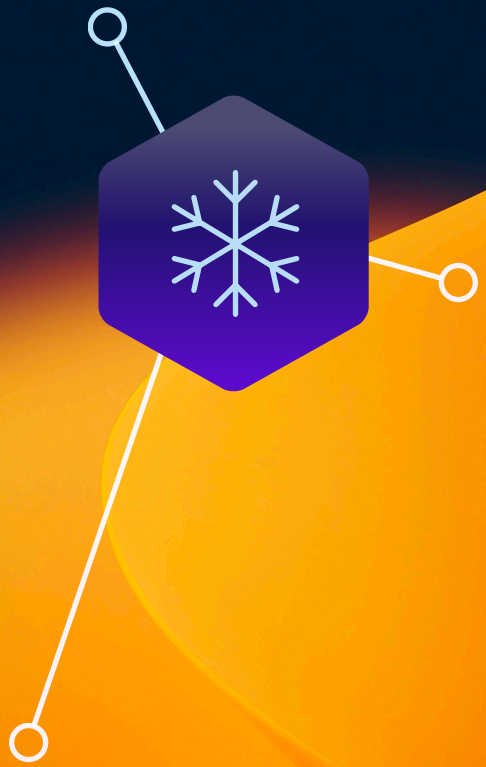
Everything you need to prepare for macOS Ventura, iPadOS 16, iOS 16 and tvOS 16

Apple OS upgrades are coming. Are you ready?

Exciting new versions of macOS (for Mac), iPadOS (for iPad), iOS (for iPhone) and tvOS (for Apple TV) are heading to a device near you. Your job is simple. Get the latest, most secure version of the OS with new features into the hands of users, all without disrupting workflows or slowing productivity.

As most IT organizations know, this can often be easier said than done, especially when factoring in the speed at which Apple users like to upgrade. Now for the good news. At Jamf, we've been doing this for more than 20 years, and are here to provide step-by-step guidance for successful Apple upgrades — regardless if it is your first OS season, or you are a seasoned professional.

Why an Apple upgrade is different



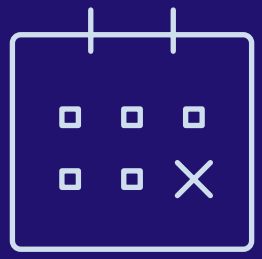
Contrary to other ecosystems, major new versions of Apple's operating systems, macOS, iOS, tvOS, and iPadOS, are released annually. A combination of the simple upgrade path and $0 cost help drive industry-leading adoption rates for consumers.

This trend is further accelerated by Apple's vertical integration of hardware and software: any new Mac, iPad, iPhone, Apple TV or Apple Watch will always ship with the latest OS version and can't be downgraded.

When devices are running old software, consistency, security and user experience are all compromised. And this is especially true when organizations attempt to support a variety of devices and OS platforms with a single management solution. Without the complications and cost of licensing, Apple's user-initiated upgrades are easy for end users to carry out autonomously. This is one of the reasons Apple's operating systems have the highest adoption rate of any ecosystem.

End users are so excited to access the new features; yet, you're responsible for maintaining security controls and an accurate systems inventory at all times.

This guide provides you with a thorough understanding of the new operating systems, and ways to carefully prepare for and implement an upgrade. You'll learn how to minimize disruptions and eliminate unplanned downtime, gaining the knowledge to deliver organizational value and walk users through their macOS Ventura, iPadOS 16, iOS 16 and tvOS 16 upgrades.



The business value of same-day readiness

There are four key reasons organizations should embrace upgrades and empower end users to update their device(s) when your environment, organization and team is ready:

1 Reduce security vulnerabilities

New operating system versions usually include improved security and privacy functionality. It's in your best interest to empower and encourage users to upgrade to the latest operating systems. This will help ensure your organization doesn't fall prey to data breaches and system vulnerabilities, all because devices are out of date.

2 Keep end users happy

New features and improvements mean end users eagerly anticipate new operating system versions. With more users adopting the full Apple ecosystem, they want all their devices upgraded and compatible for the features that allow multiple device types to work together.

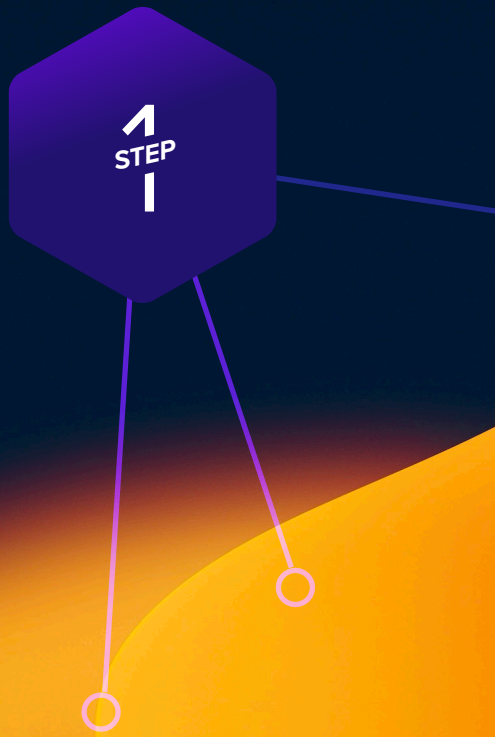
3 Keep users productive

The latest operating systems introduce new features that support greater efficiency and productivity. When users are unable to upgrade, they cannot take advantage of helpful functionality.

4 Access new IT management features

Gain access to a wealth of new management features. Not only will you have access to new capabilities for Apple ecosystem management, but you can also customize and configure new end-user features based on the unique needs of your environment.

Join the beta party



The best defense is a good offense. Arm yourself with previews of upcoming releases through AppleSeed for IT to get an early look at how new OS versions and features will impact your organization.

Apple updates its operating systems annually, which means participating in the beta program provides months of testing ahead of an operating system release. Apple offers AppleSeed for IT which provides free beta programs for macOS, iPadOS, iOS and tvOS. To join, sign up with your Managed Apple ID you use Apple Business Manager or Apple School Manager.

Why Beta?

1 The beta cycle for these operating systems typically occurs in multiple phases. Participating early and submitting feedback to Apple increases the likelihood that the features and issues that impact you most will be addressed before the update is generally released. And, when submitting feedback to Apple, you can use the Feedback Assistant app to have visibility to the issue's status and OS version where a potential resolution occurs.

2 Participating in the beta not only gives you early access to test new features and compatibility, but it also offers a deeper understanding of how the end-user experience will be impacted. Knowing which new settings have been added, any features that have moved, or changes to labels can inform necessary updates to your training materials, onboarding kits, etc. This helps your organization best prepare for changes to the end-user experience, so you can execute a more user-centric support model and communication plan accordingly.

3 Lastly, in addition to new OS settings and features, application, infrastructure and management compatibility testing is critical for continuity with current software offerings in your environment. We recommend you run Apple's betas to test their deployed apps for issues. Apple has various test plans available for organizations to validate how beta OS versions interact in numerous customer environments.

If you have not joined in Apple's Beta programs, you always can for free and you will get benefits for future OS testing.

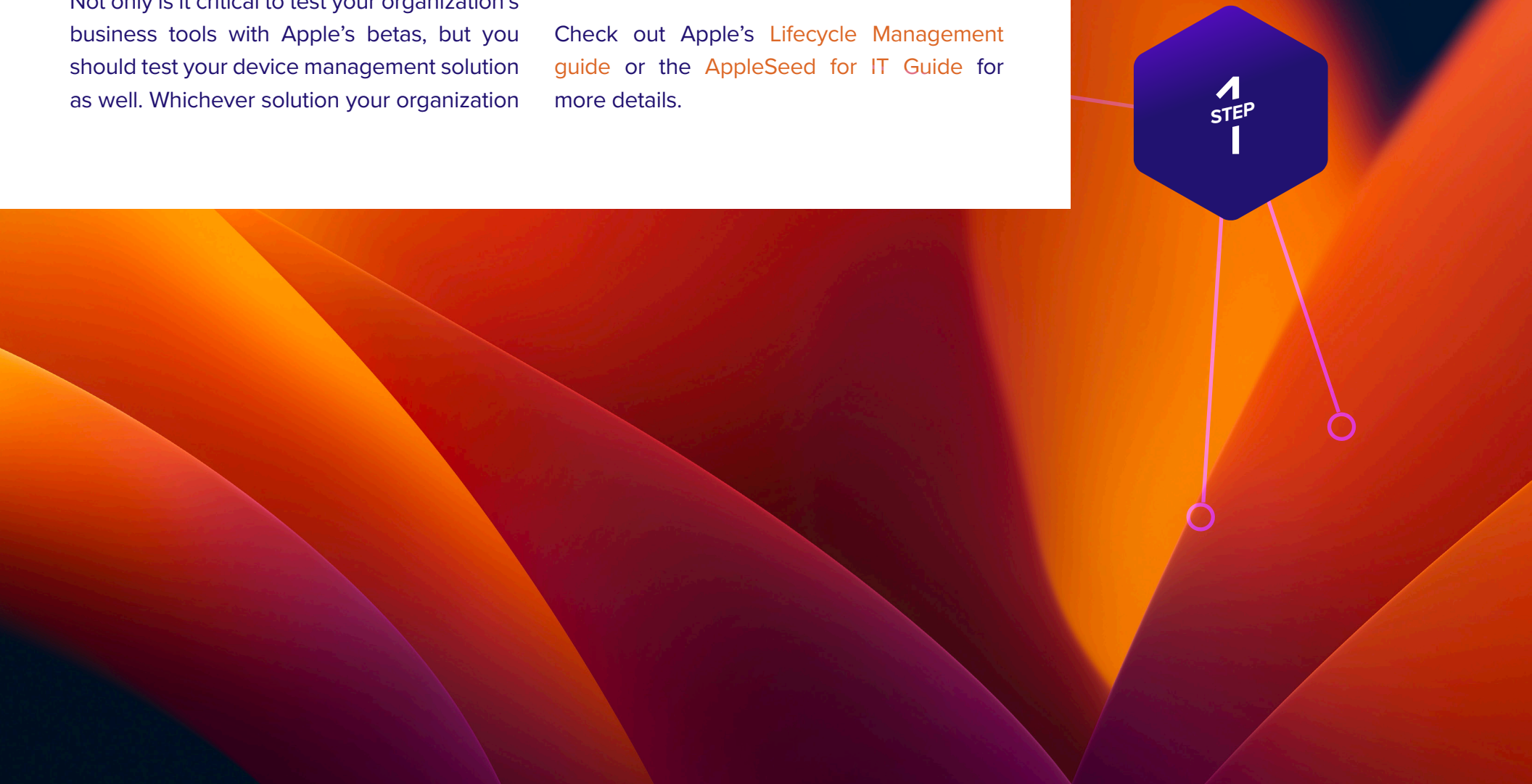
Join the beta party

Beta tips

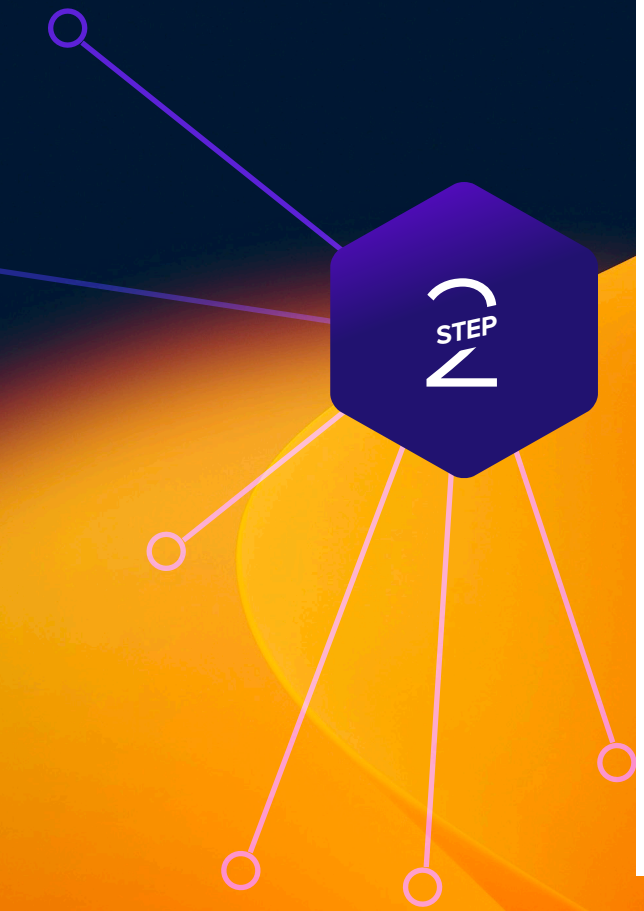
Use dedicated hardware for pre-release testing of Mac, iPad, iPhone and Apple TV devices. As always, avoid using personal or production hardware for beta testing.

Not only is it critical to test your organization's business tools with Apple's betas, but you should test your device management solution as well. Whichever solution your organization uses to manage and secure your Mac, iPad, iPhone or Apple TV devices should provide active beta programs year-round and demonstrate the ability to test compatibility with Apple's beta software on all of your devices.

Check out Apple's Lifecycle Management guide or the AppleSeed for IT Guide for more details.



Conduct strategic testing



For best results, and to ensure the upgrade won't impact any unforeseen aspects of your end users' workflows, be sure to test your entire tech stack including:

1 Infrastructure

Includes anything outside your application stack, such as VPN or printer drivers (which should always be tested with new operating systems). Testing infrastructure is less of a concern for organizations moving toward cloud hosting and services.

2 Applications

Includes both web and non-web based applications. If you don't have time to test all apps, prioritize based on an application vendor's statements related to compatibility.

In 2021, macOS Monterey included changes to legacy kernel extenstions. Consult your vendor(s) to see if they support Apple's modern System Extensions framework.

3 Management

Includes device deployment and management solutions (MDM, EMM, UEM, etc.). Check that your device management solution offers the ability to test new restrictions, management capabilities and features.

4 Security

Includes identity and access, endpoint protection, threat prevention and content filtering. Similar to your management provider, check that your security solution offers the ability to test new security capabilities and features.

Incorporate a user-centric test process.

Prioritization is essential. Take inventory of all applications used across your organization and rank them by critical-business nature. Start with high-level business apps, move to mid-level apps, browsers and low-level apps.

Many organizations choose to prioritize based on automated inventory information from their device management provider, as well as frequency of use (most commonly used to least commonly used).

Consider recruiting end-user liaisons from each department you support (Finance, Marketing, Sales, Technology, HR, etc.) to discuss their daily business processes. Ask them to walk you through their workflows and which tools they use most. Then, document each item in a spreadsheet format for testing.

Due to the architecture of iPadOS, iOS and tvOS apps, light testing might be more appropriate for these platforms. Consider leveraging automated testing tools which automate point-and-click tasks to execute a task and test it. For more information on testing frameworks, check out ITIL certification.

For additional OS testing support, Apple has "test plans" that suggest areas of each OS and features to test and validate. This can be found within the AppleSeed portal.

When documenting use cases, lay out the key business units, critical level, applications, user tasks and whether you validated compatibility.

Business Unit	Critical	Apps	User Task	Operating System	Validate
Marketing	Mid-Level	Word	*"I want to create a Word document on a machine that was just upgraded, choose the Copperplate font, then print on a printer."*	macOS Ventura	Yes

Understand the new operating systems

Options for Upgrading Operating Systems

With the options below, consider using the caching service within macOS to help reduce network traffic during the upgrade process, which can increase software download speeds for computers.

Updating macOS by sending a mass action command

You can use a mass action command to upgrade an individual computer or group of computers that are supervised or enrolled via a PreStage enrollment in Jamf Pro. Jamf Pro will send a ScheduleOSUpdate command. Then select the Download and Install command to update and restart computers after the installation action. For more information, see Updating macOS by Sending a Mass Action Command. Note: For computers with Apple silicon, no user interaction is required to authorize the update when Bootstrap Token is escrowed with Jamf Pro, which is the recommended update method.

Packaging the macOS installer and installing macOS

If you want to automate the upgrade process, you can package the macOS installer and install it automatically or allow users to install it via Self Service. Additionally, you have the option of using a script to customize the end user experience. This method is recommended for major macOS releases. For more information, see Packaging and Deploying the macOS Installer. Note: Jamf recommends using a Download and Install command to install major macOS versions on target computers with Apple silicon.

Learn more about Deploying macOS Upgrades and Updates with Jamf

Understand the new operating systems

Options for Upgrading Operating Systems

Erasing data with the macOS upgrade

If you decide to erase any data on the existing Mac when you decide to upgrade, rather than choose an option form the previous page, you can utilize the following method to complete your upgrade.

--eraseinstall is a command to install macOS and erase the hard drive at the same time. Simply download the macOS Ventura installer and upload via your MDM solution. Deploy macOS Ventura via policies:

1. Stage the installer on a client Mac
2. Run start to install with the --eraseinstall flag
3. Choose to start the installation automatically or via Self Service Applications

Note: User credentials are required to use starttoinstall and macOS installer apps with Apple silicon machines.

Additional considerations

- User credentials are required to use startosinstall and macOS installer apps
- Select “Include major updates, if available” option with a Jamf Pro Mass Action MDM command
- No user interaction is required when a Bootstrap Token is escrowed to Jamf Pro. macOS will request the token to authorize software updates

Understand the new operating systems

Features of macOS Ventura

Declarative Device Management
Declarative Device Management allows devices to act more proactively within the confines of policies from its management server. A device will discover its own state changes and take action based on defined criteria, rather than waiting to hear back from the management server. It supports modern, complex management strategies; enhances the overall user experience when using managed devices; relieves IT Administrators of performing tedious tasks; and, finally, permits devices to be the operator in their own management state.

Rapid Security Response
Rapid Security Response, brings security updates to devices and users faster than we have seen in the past. How? Because Rapid Security Response does not need to comply to the software update delay mechanism. This means that a response is included in the next minor update. On top of that, any update introduced by Rapid Security Response will not adjust the firmware of the device or need the device to reboot.

Platform Single Sign-On Extension
Users now have a faster, more secure way to access company resources. This is done through Platform Single Sign-On Extension. The Platform Single Sign-On Extension (PSSOe) builds on the SSOe configuration profile by tying the local user account on a Mac to the Single Sign-On application. From the macOS login window, the user is allowed to use their cloud identity provider (IdP) password to unlock that Mac. Once the user enters their credentials at the Mac login window, the PSSOe app will either update the local account password for the user or use a token stored in the secure element of the Mac to authenticate the user locally. After the user has successfully logged in, the local account password is kept in sync with the cloud identity password, meaning users can access any resources gated by the IdP and the SSOe app without additional password prompts.

Note: This will not be available at the initial launch and there must be a cloud identity provider that supports the Enrollment SSO workflow.

Upgrading to iPadOS 16 and iOS 16

When it comes to actually rolling out and executing the upgrade for iPad and iPhone devices, there are two options. You will simply determine if you want users or IT to be in charge of the upgrade.

Before we dive deeper into each upgrade option, note that if you are still testing or not ready to upgrade, you have the option to defer updates for up to 90 days if you are using a management solution such as Jamf. With the deferral in place, users won't be able to upgrade their device. Once you decide to update, you can choose to deploy a specific operating system version.

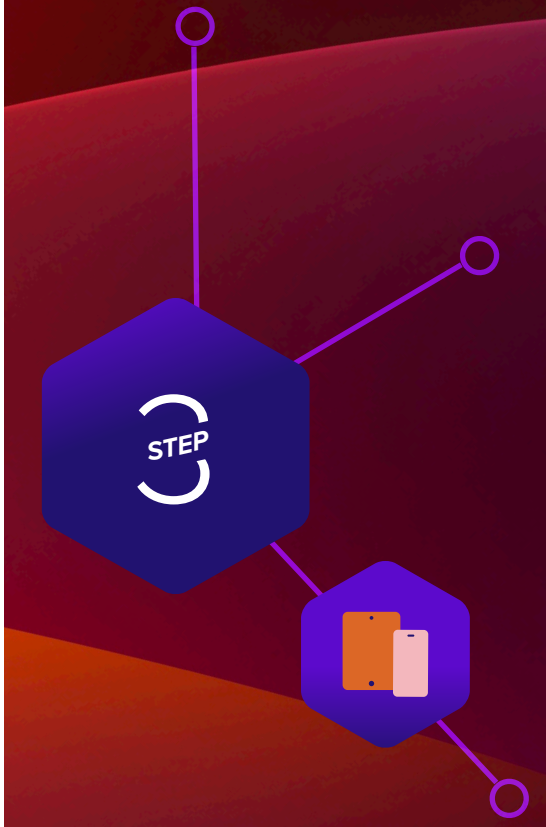
Ready to upgrade?
Once you have decided to move forward with an upgrade, you need to determine if you want users or IT to be in charge of the upgrade.

Upgrade by user
If you are having your users complete their upgrades, they will simply go to Settings on their device(s) and start the installation — no IT interaction required.

Upgrade by IT
If your devices are managed by Apple Business Manager or Apple School Manager, IT has the ability to send an MDM command to download and install a new operating system — no user interaction required. This command can be sent to individual devices or groups, giving you the control to match your customized upgrade plan.

Note: If there is no passcode, you can perform the installation automatically. If the device has a passcode, Jamf Pro or Jamf School queues the update and the user is prompted to enter their passcode in order to start the installation.

Understand the new operating systems



Understand the new operating systems

Features of iOS 16 and iPadOS 16

Enrollment Single Sign On
Apple continues to improve both the user experience and security of enrolling devices into MDM with Enrollment Single Sign-on (SSO). This method allows users to access company resources with a single authentication, using their Managed Apple ID and cloud identity provider credentials. What is needed for Enrollment SSO to work? An app that supports Enrollment SSO; a Managed Apple ID created in Apple Business Manager (ABM) or Apple School Manager (ASM); an MDM that is federated with a cloud identity provider; and, your MDM server configured to validate the end user by returning app information.

Let's break down how a user would sign in and use Enrollment SSO:

1 The user goes to the Settings app and enters their Managed Apple ID

2 They then download an app that is compatible with Enrollment SSO from the App Store, which contains the Enrollment Single Sign-on extension

3 The user signs in

4 The app then signs in where the user goes through the enrollment flow, never having to sign in again.

Important Note: Enrollment SSO will not be available at the initial launch but will be with a later update to iOS 16 and there must be a cloud identity provider that supports the Enrollment SSO workflow.

Managed Device Attestation Apple Managed Device Attestation makes sure that only genuine and approved devices can connect to an organization's server.

It ensures that the iOS/iPadOS identifier (UDID and Serial Number) is authentic; it also ensures that it hasn't been altered or misused by an attacker.

Rapid Security Response
Rapid Security Response, brings security updates to devices and users faster than we have seen in the past. How? Because Rapid Security Response does not need to comply to the software update delay mechanism. This means that a response is included in the next minor update. On top of that, any update introduced by Rapid Security Response will not adjust the firmware of the device or need the device to reboot.

Understand the new operating systems

Upgrading to tvOS 16

Apple TV devices enable wireless sharing without the need for adapters, all while delivering a modern conference room experience. Apple TV is also great for digital signage, wayfinding and specific industries, such as hospitality.

Building off the management functionality introduced with tvOS 16, tvOS 16 gives organizations even more control over the Apple TV experience.

Here are some areas to consider as you prepare for upgrades to tvOS 16:

MDM command upgrades

tvOS devices can be now upgraded by MDM command like iOS, including specifying which available tvOS version you want to update them to.

Automatic upgrades

tvOS will automatically and silently update itself to the latest OS release at its earliest convenience without interrupting users. This is unless updates are deferred by a configuration profile or the Apple TV is running in Single App Mode.

Next, consider the following stakeholders and conversations ahead of your upgrade.

Partner with InfoSec

If your organization has an information security (InfoSec) team, this is a great opportunity to partner with them. Keeping your organization secure and productive is not often a one-team task, so reach out proactively to make sure you consider their needs before OS upgrades.

Some consumer features released by Apple may not be approved for use by your InfoSec team. This is why the MDM specs are updated to disable these features. Get together with your InfoSec team now to discuss which features are appropriate for your organization.

Establish a test plan, and communicate these new features to your InfoSec team. If your organization is going to adopt new settings or restrictions available in a new OS version, consider using Smart Groups to intelligently target those configurations to eligible devices.

Preparing end users for upgrades

1 Not every end user is aware of the time it takes to upgrade a Mac. Inform users of the average upgrade time, and provide tips on the best time of day to upgrade.

2 Recommend that your end users back up their device(s) before they update. This applies to localized and iCloud backups.

* *If you use a centralized backup tool for macOS, consider sending a policy to run a backup before you do an upgrade.*

3 Implement a policy to require end users to update within 30 days, or let them know you will update for them. PCIDSS compliance requires 30 days.

When it comes to upgrades, err on the side of over communication. Use email, your company's intranet, or if your device management solution allows, your Jamf Self Service app catalog, to give users plenty of warning and recommendations prior to OS upgrades. They'll thank you for it (or if all goes well, they'll say nothing.)

Upgrades communications plan

Upgrade, enhance, enjoy

Apple's latest operating systems—macOS Ventura, iPadOS 16, iOS 16 and tvOS 16 — bring innovative capabilities to all organizations.

Providing a seamless upgrade process to your organization not only ensures security measures are met, accurate system inventory is maintained and downtime is eliminated, it will make IT look like the heroes they are. A purpose-built Apple ecosystem management solution equips you with the tools you need to take advantage of the latest Apple OSs without negatively impacting end users or putting abundant strain on IT personnel.

Jamf is the only management and security solution of scale that automates the entire lifecycle of Apple, including operating system upgrades without negatively impacting the end-user experience. Jamf hangs its hat on same-day support for Apple operating systems, going on 20 years of support and compatibility on the day the new OS is released.

Let Us Prove It

Or contact your preferred authorized reseller of Apple devices to take Jamf for a test drive.