APPLE OS 2017

Upgrades Guide

Everything you need to prepare for macOS High Sierra, iOS 11 and tvOS 11

Apple OS upgrades are coming. Are you ready?

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

As most, if not all, 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 15 years, and are here to provide step-by-step guidance for successful Apple upgrades — regardless if it is your first, fifth or 15th OS season.

Why an Apple upgrade is different

Contrary to other ecosystems, major new versions of Apple's operating systems, macOS, iOS and now tvOS, are released annually. A combination of the simple upgrade path and $0 cost help drive impressive 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. This is a stark contrast to Windows, where Windows 7 still remains more popular than the newer Windows 10 release. The same can be said for Android, where only a minority of devices are running the latest Android OS.

This level of fragmentation is a challenge for organizations concerned with security, and makes it nearly impossible to offer a consistent, protected device experience when attempting to support a wide variety of devices and OS platforms. And, since most Windows and Androids are often not current, they are at a much higher risk for a security breach.

Without the complications 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 poses a unique challenge**, especially in the case of iOS, which does not allow administrators to block end-user upgrades.

This guide will provide 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 High Sierra, iOS 11 and tvOS 11 upgrades.

The case for zero-day upgrades

There are four key reasons organizations should embrace upgrades and allow end users to update their device(s) the day new operating systems are released:

1 Reduce security vulnerabilities

Old versions of software are always less secure. 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

Apple trains users to keep their software up to date. In turn, Apple users expect to be able to successfully update their device(s) the day a new operating system becomes available. Zero-day upgrades ensure this expectation is met.

3 Keep users productive

The latest operating systems introduce new features that support greater efficiency and productivity. When zero-day upgrades are discouraged, users are unable to take advantage of helpful functionality, such as better multi-tasking with a new dock and the ability to drag and drop content between apps in iOS 11.

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

By participating in the Apple Beta Software Program, you can check compatibility with your existing applications, test the new features of the OS, and make sure it meets organizational needs prior to upgrading. After all, the last thing you want is downtime and compatibility issues mid-upgrade.

Apple is regularly updating its operating systems, which means participating in the beta program provides months of testing ahead of an operating system release.

Apple offers both paid developer and free public beta programs for macOS, iOS and tvOS. The paid developer account typically costs $100 annually, but provides access to additional resources, such as release notes. Additionally, Apple also offers the AppleSeed for IT programs for enterprise and education customers at no cost and by Invite only.

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. And, if you are the first to submit a bug report to Apple, you'll have visibility into the status of your ticket. Otherwise, duplicate bugs are closed, and you won't have insight into Apple's progress.

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 communications 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. A recommendation is for IT administrators to run Apple's betas to test their deployed apps for issues. Reporting any issues to the associated vendors upon discovery will help ensure the apps work upon Apple's official release.

Join the beta party

STEP 1

Beta tips

Use dedicated hardware for pre-release testing of Mac, iPad, iPhone and Apple TV devices. As always, avoid using personal or business-critical 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 iOS Lifecycle Management white paper for more details.

An upgrade story

When the MacBook Pro with Touch Bar introduced Touch ID to macOS for the first time, this new authentication method impacted organizations worldwide. Why? Because organizations did not discuss how they would categorize this new authentication method. How would it impact end users? How does it work within a security policy?

By participating in Apple's betas and submitting feedback to Apple, organizations can have these discussions months prior to an upgrade. This also allows them to better adapt their security policies to categorize and embrace new tech, which eliminates leaving users in ambiguous spots.

Conduct strategic testing

STEP 2

To aid in your planning, categorize testing into three buckets:

1 Infrastructure

Includes anything outside your application stack, such as testing 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. For example, those using Dropbox, as opposed to a file server, won't need to test those connections.

2 Applications

Includes both web and non-web based applications. VPN software is frequently the first of the application stack to be tested, since it's one of the most common to break upon upgrade. If you don't have time to test all apps, prioritize based on an application vendor's statements related to compatibility. For vendors who don't proactively promote planned compatibility on their website, in documentation or within direct communications, it is best to validate the apps yourself.

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. For example, new Skip Step options added to Apple's Device Enrollment Program (DEP) Setup Assistant in macOS High Sierra will alter any customizations you have made to the end user enrollment experience if your management solution does not support them.

Infrastructure Investment

As Apple makes strides in infrastructure integrations by partnering with Cisco, upgrade season is the ideal time to evaluate your infrastructure investments. If you're on the fence, there are great motivating factors to choose one technology over another given Apple's integration efforts. For example, the Cisco and Apple partnership delivers unique enterprise solutions with Fast Lane for iOS and macOS.

Incorporate a user-centric test process.

STEP 2

Prioritization is essential, especially in resource-strapped organizations. Take inventory of all applications used across your organization and rank them by critical-business nature (financial software, CRM software, ERP software, etc.). Start with high-level business apps and 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).

While you may have automated hardware and software inventory information at your disposal, there is no replacement for human interaction. Do not forget to identify the key functional business units in your organization and interview them.

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 iOS and tvOS apps, light testing might be more appropriate for these platforms. Consider leveraging automated testing tools such as **Sellenium**, **TestPlant** or **Sikuli**, which automate point and click tasks to execute a task and test it. For more information on testing frameworks, check out ITIL certification.

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

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 High Sierra	Yes

Understand the new operating systems

3
STEP

In addition to the testing guidance above, macOS High Sierra, iOS 11 and tvOS 11 have differing sets of new features and unique impact on your environment.

Below you will find important information for what you need to know when upgrading to each operating system. For a comprehensive list, please review Apple's online resources, including articles on their support site.

Upgrading to macOS High Sierra

There are several ways to accomplish upgrades on a Mac. The most common upgrade path for macOS is an in-place upgrade. An in-place upgrade involves installing the operating system while keeping user data intact.

One method for conducting an in-place upgrade is to send an MDM command to Macs enrolled in Apple's DEP. Like iOS, this MDM command will trigger your Macs to download the new OS from Apple and automatically install it on devices. However, this method will only work for Macs enrolled in DEP.

For Macs not enrolled in DEP, Jamf customers typically accomplish in-place upgrades by pre-packaging the macOS installer for the user. The macOS installer is then either installed automatically by IT or initiated by the end user through Jamf Self Service (an enterprise app catalog). To save on network bandwidth and maximize user productivity, the macOS installer can be pre-cached on the systems that are eligible for an upgrade. Additional software updates and configuration changes can be combined with the update to ensure a smooth transition.

But what about imaging? Imaging, a set of technologies that are used in a variety of deployment scenarios, is being replaced with native Apple technologies. Long-term, imaging options will continue to become less and less relevant when it comes to managing a Mac deployment. **Apple does not recommend or support monolithic system imaging when updating or upgrading to macOS High Sierra. See this article on Apple's support site for more details.**

Understand the new operating systems

STEP 3

For the first time, you must also be connected to the internet when you upgrade macOS. This is due to firmware updates Apple installs on the Mac, further strengthening the security of your devices. Only the macOS installer can download and install these firmware updates, which validates Apple as the source of the critical firmware. **In fact, installing macOS High Sierra on a Mac connected by Target Disk Mode is no longer a supported installation method.**

The only supported imaging upgrade workflow for macOS High Sierra leverages System Image Utility to create a NetInstall image. While this can be a more labor-intensive process, Apple supports this method.

Here are some other areas to consider as you prepare to upgrade to macOS High Sierra:

Apple File System (APFS)

APFS, Apple's next generation file system, will ship with macOS High Sierra. APFS will be the standard file system for devices with solid-state drives. Revisit any imaging workflows in your environment, as they may no longer be supported. See Jamf's APFS white paper for more information.

Cisco Fast Lane QOS for macOS

macOS High Sierra introduces Cisco Fast Lane for macOS. Cisco Fast Lane enables you to optimize network traffic for business-critical apps. Organizations using Cisco networks can define what iOS, and now Mac, apps get priority on the network. Inventory your most critical Mac apps and confirm that your device management provider supports the new Cisco Fast Lane QOS features for macOS.

Customer Quote

> “ Being able to deploy a Mac operating system upgrade without having to visit each machine is huge. Jamf Self Service allows us to put the power into our end users' hands, allowing them to kick off a system upgrade on their time.”

Steve Wood
Endpoint Services Manager, Omnicom Group

Understand the new operating systems

Software update deferral

For the first time, a new configuration profile is available for IT admins who want to defer software updates on a Mac for up to 90 days. Evaluate your software update timelines and determine whether you need to defer future software updates for end users.

Kernel extension management

As Apple strengthens macOS security, there are new user consent requirements to load kernel extensions with or after the installation of macOS High Sierra. End users will only need to approve kernel extensions on their Mac if A) they were not on the Mac before the upgrade to macOS High Sierra, or B) the kernel extensions are not replacing previously approved extensions. Review any existing kernel extensions (for example, with anti-virus software and virtualization software), and apply them prior to any upgrades. User Approved Kernel Extension Loading is disabled when a Mac is automatically enrolled in MDM. See Apple's article for more information.

Enhancements to certificate security

Similar to requirements implemented in iOS 10.3, user-initiated enrollments on macOS now require trusted third-party certificates. If you are not already, this update introduces another reason to use trusted third-party certificates to deliver the best experience.

FileVault

A new FileVault redirect recovery key payload will be available for macOS High Sierra.

New local user management

Local user account data can now be collected via mobile device management (MDM). Additionally, IT can send a command to remove a local user or unlock an account if the user has entered an incorrect password too many times. However, these new MDM capabilities are not as robust as leveraging agents from device management solutions like Jamf.

STEP 3

Understand the new operating systems

Upgrading to iOS 11

Unlike macOS upgrades, there is only one workflow for iOS upgrades. They are made available by Apple and then installed by the end user. While organizations cannot block end users from upgrading, they can mass upgrade end users on supervised devices (running iOS 10.3 or later) leveraging the upgrade MDM command.. Here are some other areas to consider as you prepare for upgrades to iOS 11:

Setup Assistant

iOS 11 includes DEP enrollment skip steps for Keyboard chooser and Apple Watch migration. These options allow for a customized, streamlined enrollment experience for end users. DEP enrollment Skip Steps are always an important area to consider with each upgrade. The ability for a device management provider to support new Skip Step options makes or breaks their ability to offer a streamlined enrollment experience.

DEP and Apple Configurator

For the first time, organizations gain the ability to manually enroll iOS and Apple TV devices regardless of how you purchased them. This is made possible by using Apple Configurator to retroactively add devices into DEP. To prepare your iOS devices, inventory and collect iOS devices, wipe them, and preserve them within DEP for the new 30-day grace period. Keep in mind that you may need to work backward in time from when you plan to deploy these iOS devices and factor in a 30-day window.

Supervision requirements

During DEP enrollment, MDM is no longer optional, and all iOS devices will now be supervised. While this may not impact your workflows, consider the potential impact to the end-user experience and setup process, and keep in mind that supervision and DEP now go hand in hand.

Understand the new operating systems

STEP 3

Preserve cellular data plans

For organizations with shared-use field iOS devices, a new option is available to preserve a data plan when erasing iOS 11 devices. This will be helpful for those who frequently need to wipe and re-deploy cellular devices.

Restrict system app removal

iOS 11 introduces a new restriction to keep end users from deleting system apps. Earlier releases of iOS introduced the ability for end users to delete system apps, such as Tips or Weather. However, if end users deleted a critical app, like Mail, they were not able to remotely reinstall this app. You can now rest easy knowing business-critical system apps will stay intact.

VPN and network security

You can restrict managed iOS devices from manually setting up and connecting to unapproved VPN networks. This reduces workarounds for content filters and network security, and strengthens your ability to maintain compliance — an especially crucial component for your InfoSec team.

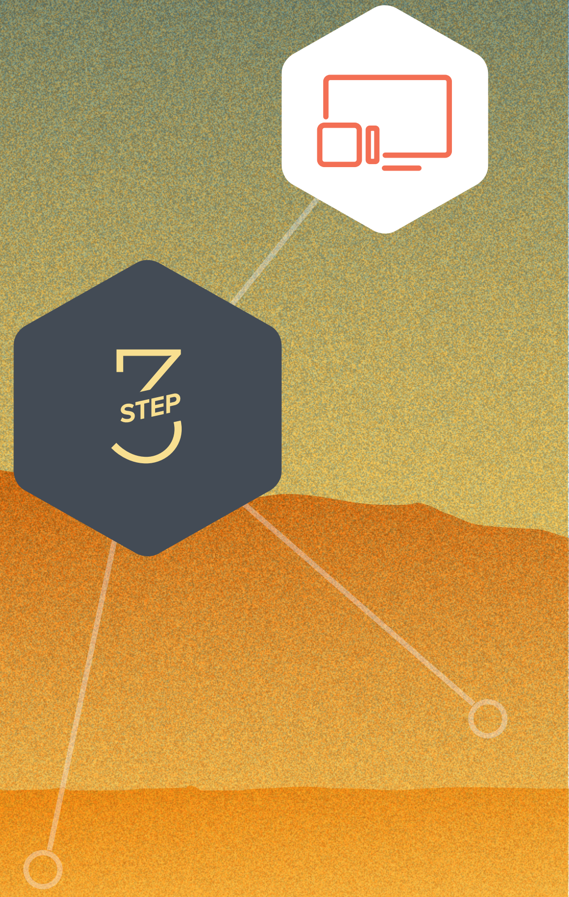
AirPrint

The future of printer drivers, AirPrint, allows end users to connect and print without a driver. New management options around AirPrint drivers are available in iOS 11, providing an opportunity to revisit your printer strategy.

32-bit applications

iOS 11 doesn't support 32-bit applications, so anything under 64-bit will not work. Because bit size isn't a common inventory field, many organizations will need to take stock of all apps in their environment and install them on a test iOS device to determine which applications won't be compatible. To see which apps fall out of compatibility, go to Settings>General>About>Applications>App Compatibility on a test device running iOS 10.3.1. Create a group of the 32-bit apps to remove within your device management solution, and inform end users which apps will no longer work after the upgrade. For more information, join the conversation on Jamf Nation.

Understand the new operating systems



Upgrading to tvOS 11

A recent Jamf Nation survey found that 95 percent of respondents report leveraging Apple TV devices in their environment, and for good reason. They 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. But until recently, they haven't necessarily been easy to set up and manage. That all changed with tvOS 10.2, and now tvOS 11 gives organizations even more control over the Apple TV experience.

Organizations can leverage Apple Configurator with a Mac to upgrade Apple TV devices to tvOS 11 or use the Apple TV remote to navigate to the software update settings and run the upgrade. Here are some other areas to consider as you prepare for upgrades to tvOS 11:

Apple TV device name modification

Organizations were delighted to be able to apply an Apple TV device name en masse with tvOS 10.2. Now with tvOS 11, you can prevent Apple TV devices from being renamed by end users in the Apple TV settings.

Apple TV configuration

With new features to show or hide specific Apple TV apps, and the ability to configure the Home screen layout with folders, organizations can prepare for tvOS 11 by outlining their desired Apple TV display experience for each use case in their environment.

Restrict media content

tvOS 11 also brings the ability to restrict certain media content. You should begin taking stock of which media content you want to restrict, and add it to any internal content policies shared with end users.

AirPlay for Apple TV, iPad and iPhone

In addition to the new management features, you can further secure AirPlay for Apple TV by defining specific passwords for individual Apple TV devices and automatically sharing that password with specific iOS devices. This eliminates accidental sharing of private data to different rooms. To prepare, organizations can begin outlining which Apple TV devices pair with each iOS device in their environments.

Upgrades communications plan

A deep understanding of the new operating systems, careful planning and insight into the potential impact for end users ahead of an upgrade can minimize disruption, help desk calls and unhappy end users. Next, consider the following stakeholders and conversations ahead of your upgrade.

Loop in InfoSec

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 block 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. By participating in Apple's betas (if your device management solution supports them), you can preemptively block any features that concern your InfoSec team before they are available to end users on managed devices.

Steps to preparing end users

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 like Crashplan 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.)

Go forth and conquer

Apple's upcoming operating systems, macOS High Sierra, iOS 11 and tvOS 11 bring great capabilities to all organizations.

A streamlined approach to Apple upgrades ensures security measures are met, accurate system inventory is maintained and downtime is eliminated. 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 committed to helping organizations succeed with Apple. We've offered zero-day support for all Apple releases for more than a decade, ensuring organizations can take advantage of new Apple technology as it becomes available.

Let Us Prove It