jamf

WHITE PAPER

Managing Apple OS Upgrades

Apple sets a high bar for Operating System (OS) upgrade frequency.

Exciting new versions of macOS (for Mac) and iOS (for iPhone and iPad) are heading to a device near you. macOS Sierra and iOS 10 offer new productivity, security and management capabilities to help you and the users you support get more done. Your job is to get these features into the hands of users and IT staff without disrupting workflows. Our job is to help you do it.

DON'T MISS A BEAT THIS UPGRADE SEASON

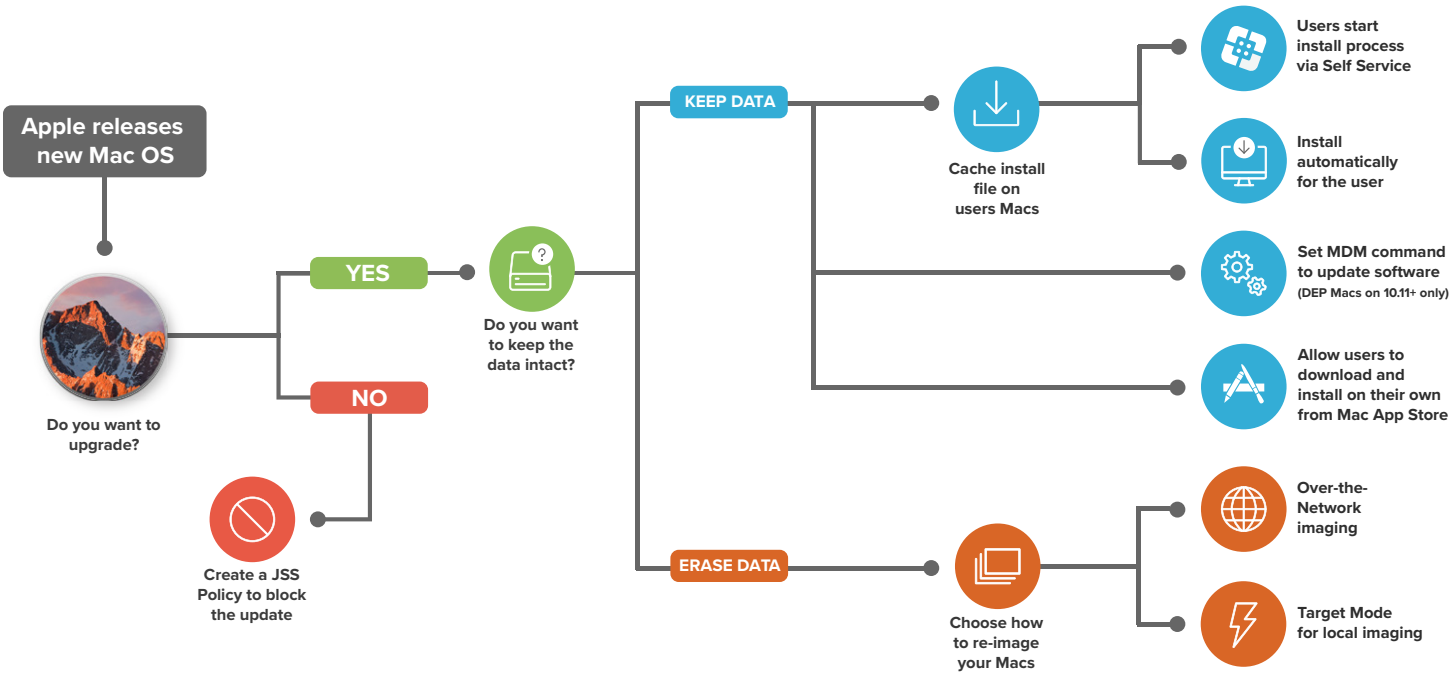
New versions of macOS and iOS are released each year. A combination of the simple upgrade path and $0 cost helps drive impressive adoption rates for consumers.

This trend is further accelerated by Apple's vertical integration of hardware and software: any new Mac, iPad or iPhone will always ship with the latest OS version—and can't be downgraded. This presents a stark contrast to Windows, where Windows XP and Windows 7 remain more popular than the newer Windows 10 release. The same can be said for Android, where a minority of devices are running on the latest Android OS. This level of fragmentation is a nightmare for IT staffs concerned with security, as it is nearly impossible to offer a consistent, protected device experience when all devices are different. And, since most PCs and Androids are not current, they are at a much higher risk for a security breach.

With Apple, users are so excited to access the new features that IT managers know they can't always prevent them from upgrading their devices, and yet they're responsible for maintaining IT security controls and accurate systems inventory. This presents a real challenge and makes it essential that their system management tools are updated in step with Apple.

With some advance planning and the right tools in place, these major OS updates are a great opportunity for IT managers to deliver business value by guiding users through the upgrade and leveraging new Apple technologies.

The Jamf Pro provides the tools to prepare, plan, and deploy OS upgrades.



How to make the transition to iOS 10 and macOS Sierra seamless

Upgrading your Mac and iOS devices offers employees, teachers and students access to the latest productivity and learning tools. It also gives IT the security capabilities they need to best protect their environment and prohibit costly data breaches from occurring. With the decision to upgrade made, the next step is to prepare.

1. LEVERAGE INVENTORY REPORTS

Careful planning ahead of an upgrade can minimize disruption and eliminate unplanned downtime. The Jamf Pro's dynamic inventory tools make it easy to identify which devices are eligible for the upgrade.

Each device sends an inventory report to the central Jamf Pro server on a daily basis, with inventory data including hardware details, software versions and security configurations. The inventory data can be used to create dynamic smart groups—device groups based on inventory attributes—that are used for reporting and to scope deployment activities. This work can be done before a new OS is released to avoid delays or surprises.

Any in-house or mission-critical commercial software should be tested for compatibility with the new OS. If gaps are identified, the Jamf Pro's software inventory will quickly identify which systems are affected. As needed, software updates can be deployed to those systems using the Jamf Pro software deployment tools.

Updates can be pushed to devices, scheduled for overnight installs, or users can initiate the install using the Self Service app. To aid in user communication regarding updates, the Jamf Pro can push notifications using Apple's Push Notification service.

When environments are not ready to make the upgrade the moment the operating system is released, IT can use the Jamf Pro to prevent users from updating. This ensures IT has ample time to test the environment and eliminate service interruptions, so they can roll out a consistency upgrade experience for all users

2. PLAN MULTIPLE PATHS FOR DEPLOYMENT

The most common path is the in-place upgrade, where the OS is updated without changing the other software or user data on the system. This is the default option for iOS upgrades and savvy Mac users can upgrade on their own, using Apple's built-in software update feature. Some organizations prefer to coordinate the upgrade process within the IT group to ensure consistency and compatibility with other systems.

The Jamf Pro software deployment, package caching and Self Service features make in-place upgrades painless for IT admins and users alike. Based on the smart groups described above, IT can make a communication plan and prepare upgrade paths for users.

On the Mac, the update software package can be cached on the systems that are eligible for an update, then later installed on a schedule, triggered by a system event, or initiated by the user through the Self Service app. Additional software updates or configuration changes can be combined with the update to ensure a smooth transition.

iOS updates can be initiated by the user or automatically deployed using an MDM command. This will work with any iOS device that has been enrolled using DEP and is running at least iOS 9. The Jamf Pro's breadth of management capabilities for both iOS and macOS offers IT groups the flexibility to develop the right workflow for their users.

In the case of new hardware or repurposed devices, the Jamf Pro imaging tools offer a simple, repeatable workflow to install the latest OS. The Casper Imaging tool for Mac can wipe and install a fresh OS along with

all the additional software and configurations required. This process is automated and scalable to support large, distributed organizations. By sharing a package library, the same preparation done for in-place upgrades is repurposed for imaging.

3. UTILIZE CONSISTENT SECURITY CONTROLS

Securing a Mac or mobile device is most effective using native controls. Unlike other solutions that require additional client software on the device to enforce security, the Jamf Pro can configure the native OS security features.

The native data encryption capabilities in both macOS and iOS, paired with Jamf Pro for configuration and key escrow, offer strong security for Apple devices. Because the encryption capabilities are part of the OS, upgrades are painless and the data encryption is preserved throughout the process.

Beyond data encryption, the Apple OS provides good security controls for network security, user authentication, application safety and others. These controls can be managed by the Jamf Pro using the native configuration profile technology and is consistent across OS upgrades.

Fully align with Apple

A streamlined approach to macOS and iOS upgrades ensures security measures are met, accurate system inventory is maintained and downtime is eliminated. As a best-of-breed Apple management solution, the Jamf Pro equips IT managers with the tools they need to take advantage of the latest Apple OS without negatively impacting end users or putting abundant strain on IT personnel.

jamf

www.jamf.com

To learn more about how Jamf Pro can make an impact on your Mac and iOS management, visit **jamf.com**.