

A close-up photograph of a person's hands typing on a silver laptop keyboard. The background is blurred, showing other laptops and office equipment.

## Best-of-Breed Enterprise Mac Management

Choose the right tool for the job.

---

A decade ago, Mac was an uncommon sight in many businesses and routinely ignored by corporate IT — but times have changed. Today, employee-choice programs are driving Mac growth in enterprises with 72 percent of employees choosing Mac over PC when given the chance. Now, the need to properly deploy, manage and secure Apple is at an all-time high. This white paper examines how purpose-built management solutions are essential to a successful Apple strategy.







## CURRENT STATE OF ENTERPRISE MANAGEMENT SOLUTIONS

The legacy view of device management fell into two classes: desktop and mobile.

Desktop tools, historically referred to as client management, are specifically designed for PC and Mac management. On the other hand, mobile device management (MDM) or enterprise mobility management (EMM) are tailored to manage iOS and Android devices.

A misleading approach that many in the industry have taken is to consolidate all mobile and desktop management into one solution. This is often referred to as unified endpoint management (UEM).

While, on the surface, this may be appealing. But issues quickly arise when organizations use solutions that attempt to support cross-platform, as the lack of commonalities is immediately apparent.

|                             |  |  |  |  |  |  |
|-----------------------------|---|---|---|--|---|---|
| <b>Provisioning</b>         | Device Enrollment Program   |   | Dynamic Provisioning via Azure AD   |  | Manual Enrollment into G Suite  | No Device Enrollment Program equivalent   |
| <b>Encryption</b>           | FileVault   | Enable with password  | Bitlocker   |  | Encryption via cloud storage  | Built-in encryption on new devices, turned off by default                           |
| <b>Management Framework</b> | MDM via Apple Push Notification Service   |   | SCCM + MDM via Windows Push Notification Service                                  | MDM via Windows Push Notification Service  | Chrome Management   | MDM via Google push notifications   |
| <b>Settings Management</b>  | Configuration profiles  |   | Group policy object   | Configuration policy   | Chrome policy   | Android (formerly Android for Work)   |
| <b>Software Licensing</b>   | Volume Purchase Program   |   | Windows Store for Business  |  | Chrome Web Store  | Google Play Volume Purchase (US & Canada only)                                      |

## MANAGEMENT THROUGH AN ECOSYSTEM LENS

Apple, Microsoft and Google did not intend for their platforms to be managed alongside their competitor with one solution. With each ecosystem having its own method of deployment, operating system release cycle, security features and overall device management — just to name a few — this approach prohibits IT from delivering the seamless technology experience that modern workers are now demanding.

Turning to purpose-built, best-of-breed solutions for each ecosystem is the only way to truly get the most out of a technology initiative.

## BEST-OF-BREED APPLE MANAGEMENT

From initial deployment to maximizing user productivity, organizations need a full lifecycle management solution catered to every stage of an Apple program. Best-of-breed solution feature sets include:

1. **Deployment and provisioning**
2. **Configuration management**
3. **App management**
4. **Inventory**
5. **Security**
6. **User empowerment**

### 1. DEPLOYMENT AND PROVISIONING

Prior to configuring Apple devices for users, devices must be enrolled into management. Jamf offers several enrollment options to ensure the unique needs of each organization are met.

#### Zero-touch enrollment

The ideal method to enroll devices is by using Apple's Device Enrollment Program (DEP) — soon to be a part of Apple Business Manager. DEP enables automatic enrollment, meaning Apple devices can be shipped to users, and when turned on for the first time, configured and immediately ready for use. No physical hands-on work ever needs to be performed by IT.

#### User-initiated enrollment

This is a manual process that requires users to visit a specific URL set up by IT to enroll and configure their device. Best used when unmanaged devices are in the field or the device needs to be re-enrolled into management.

#### User Approved MDM (UAMDM)

UAMDM is a special mode of management for macOS; similar to supervision for iOS and tvOS devices. This advanced management state ensures users are aware their Mac is being managed by IT and is required for managing sensitive security settings, like kernel

extensions. No matter how devices are enrolled with Jamf, they become UAMDM and allow you to approve which kernel extensions can run on managed Macs. Future management settings may require UAMDM.

### 2. CONFIGURATION MANAGEMENT

After devices are enrolled and in the hands of users, IT must next configure each device with the appropriate access, settings, software and apps users will need to be successful. Once again, Jamf offers several paths to customize one or thousands of Apple devices.

#### Configuration profiles

These small XML files can be created and distributed to define settings for macOS, iOS and tvOS. Examples include Wi-Fi, VPN and email settings. These profiles are built within Jamf and distributed over the air to managed devices.

#### Policies

Unique to macOS management, policies go beyond the scope of configuration profiles and allow for custom software and printer installs, local user account management and advanced management workflows. Only Apple-focused management solutions offer this extended client management functionality.

#### Scripts

Part of policies, scripts open the door to infinite device management capabilities. Anything that can be executed in Terminal via the command line can be turned into a script. A best-of-breed solution will provide a library of existing scripts for organizations to use, along with a community where script creators can share and connect with each other.

#### Smart Targeting

Based on inventory data, Jamf empowers IT to create Smart Groups which automatically trigger device management capabilities to specific devices or groups that meet IT-defined criteria. Unlike so-called "UEM" solutions, Smart Targeting is dynamic and the backbone of personalizing the technology experience for end users.

### 3. APP MANAGEMENT

For iPad, iPhone and Apple TV devices, the App Store is the only way for consumers to get apps on their devices. Apple reviews the developer's code to ensure security and performance. For Mac, however, software is made available outside of the App Store.

Popular titles such as Microsoft Office and Adobe Creative Suite are not available via the App Store. But, Jamf offers the ability to deploy custom software by building a custom .pkg or .dmg. That software package can then be deployed to managed Macs, all without users needing to be admins.

Apple offers a robust SDK and powerful development tools for their operating systems. Organizations can develop custom in-house apps to help solve business problems or workflows by leveraging the native APIs available. Additionally, organizations can take advantage of the enterprise partnerships Apple has made with IBM, SAP, Deloitte and GE to deploy industry-specific app solutions.

#### Apple deployment integration

Jamf also integrates seamlessly with Apple's Volume Purchase Program (VPP) to empower organizations to purchase and license apps in bulk and distribute them directly to individuals with an Apple ID or directly to devices without an Apple ID. Apps can later be reassigned if needs change.

#### Custom app configurations

If simply purchasing and deploying an app is not enough, you can also pre-customize app settings to tailor the app to a specific user or group of users. For example, pre-configure the Box app with your server info, or populate the Salesforce app with the correct info for your domain. Jamf is a founding member of AppConfig.org, where IT admins can find app configuration examples for popular business apps.

### 4. INVENTORY

Management solutions are capable of querying devices to collect a large amount of inventory data, ensuring IT has a clear view of the entire environment. This also ensures that informed decisions are being made if a device displays out of date software or lapsed security settings. Inventory can be collected from a device at various intervals and include serial number, OS version, apps installed and much more.

Jamf goes beyond basic inventory collection and allows IT to see custom inventory data about specific hardware or software add-ons.

#### Scoping and Targeting

IT often will deploy different settings to different groups of users. For example, only the marketing team needs Photoshop or only the finance team needs Excel. With the inventory collected via Jamf, IT can dynamically target devices and deploy configuration profiles and restrictions to those devices. Depending on needs and desires, two targeting methods are available: Static Groups and Smart Groups.

#### Static Groups

Static Groups are a set of devices that are defined, like a department or floor. IT can then apply a management policy to that group.

#### Smart Groups

Smart Groups are dynamic and always changing based on inventory data. This enables IT to group devices and deploy configuration profiles and restrictions based on a large set of criteria. Example: Find all Macs with 8GB RAM, 80 percent full hard drives, running 10.12.2 or higher.

#### Extension attributes

Extension attributes allow you to collect extra inventory from computers and mobile devices. By leveraging the free library of extension attributes found on Jamf Nation, IT admins can report on things like the backup status of their Code42 instance, battery health information or what version of Java is installed. The possibilities are endless by adding extension attributes to your Jamf Pro server.

## 5. SECURITY

Apple includes powerful native security features with every device. When paired with Jamf, IT can ensure that these security features are turned on, enforced and working properly for hardware, apps and the entire network — no need for additional third-party software or complexities.

### Restrictions

Not all consumer features of Apple's operating system are designed for enterprise use. That's why IT admins can restrict certain features based on security needs. Disable the camera, turn off iCloud, prevent changes to System Preferences, and even blacklist specific applications.

### Lock, wipe and restart

If a device is ever lost, stolen or compromised, IT can leverage Jamf to send a command to the device to lock, wipe and/or restart it. This is done without compromising privacy through ongoing tracking.

### Software upgrades

Each year, Apple unveils new features with its annual macOS, iOS and tvOS releases. These updates are critical for devices and their users to remain protected and productive, so it's imperative that your management solution be in lockstep with Apple's release cycle. Jamf has and will continue to support Apple releases on the day (or before) they become generally available.

### Patch management

Security breaches are on the rise. And to alleviate risk, devices must remain up to date with the latest software installed. Patch management is the key, and Jamf is the only solution with automated patch alerts for macOS updates and third-party apps built right into the platform. Jamf includes patch notifications, patch packaging, patch distribution and patch reporting — taking the guesswork out of software and device security.

### Active Directory binding

Jamf automates Active Directory binding for secure user authentication and password compliance. With deep Apple integration, Jamf can manage local user accounts for complete user security. As an additional safety measure, local management account passwords can be randomized to nullify the chances of unauthorized access.

## 6. USER EMPOWERMENT

Today's employees are no longer willing to wait for the resources they want and need. To save on endless help desk tickets for app installs, printer mapping, software updates and email configurations, IT can create its own app catalog where employees can get what they need, when they need it.

Jamf Self Service is an on-demand app and resource catalog where IT can pre-populate assets and resources they want to make available to users. Instead of reaching out to IT, users simply navigate to Self Service, download and be on their way.

Most importantly, best-of-breed solutions should offer the ability to brand a self service app to seamlessly integrate to existing intranets or other HR/technology portals. Jamf lets you do just that by customizing the app icon, name and the banner image within Self Service.

### Third-party integrations

Take empowerment even further by extending your ecosystem through third-party integrations like those offered 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 organizations and their users. Examples include integration with Cisco ISE and FastLane, ServiceNow, Tableau, Splunk and more.

### Dedicated Apple support

Exclusively focused on Apple device management, Jamf provides nearly two decades worth of experience supporting those who support others. If IT or their end users run into issues, a dedicated Jamf and Apple expert will be available to ensure the problem is solved. From strategic initiatives to emergency responses, no other management solution is as versed at providing the best Apple experience possible.

## THE BEST-OF-BREED SOLUTION: JAMF AND MICROSOFT INTEGRATION

While Apple has gained significant traction in the enterprise, many organizations will still need to support Windows PCs right alongside Mac. To accommodate these organizations, Jamf integrates with Microsoft's best-of-breed Windows management solution, Intune, to deliver the answer to the challenge of cross-platform management.

This integration provides an automated compliance management solution for Macs accessing applications set up with Azure Active Directory. Through the industry's only proxy-free conditional access, this partnership ensures that only trusted users, from compliant Mac computers, using approved apps are accessing Office 365 and other cloud and on-premises resources.

Microsoft enables Jamf to report Mac information to Intune and provide a simple process to remediate non-compliant devices.

For more information on the Jamf and Intune integration, [read our full white paper](#).

### Co-management with SCCM

For traditional Windows organizations not ready to move to the modern management philosophies of Intune, Jamf offers a plug-in for Microsoft's Systems Center Configuration Manager (SCCM). This allows Windows admins to view and share Mac inventory, providing a single pane of glass view for all devices in the environment.

## Don't settle for the pitfalls of unified endpoint management

---

The one-size fits all approach is never the best option and often forces severe trade-offs. Multi-platform tools only address the basic needs of IT and have limited inventory, deployment and security capabilities, while also failing to adequately support each operating system in a timely manner.

With Jamf, IT admins have a tool that is built for Apple by those who know Apple management best, and one that seamlessly integrates with Windows environments.

Join more than 15,000 organizations that rely on Jamf to manage over 10 million Apple devices and see why 98 percent of our customers stick with us year over year. Put our best-of-breed features to the test today with a free trial.



[www.jamf.com](http://www.jamf.com)

© 2002-2018 Jamf, LLC. All rights reserved.  
Created 11/2016. Modified 05/2018.

See how you can achieve Apple success by taking Jamf for a free test drive. [Request a trial.](#)