Managing Apple Devices in a Windows World

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Ivanti

April 2017

EMA™

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Executive Summary

While Windows PCs continue to comprise the core of business end user computing solutions, Apple macOS computers and iOS mobile devices are increasingly being adopted to satisfy evolving workforce requirements and preferences. This accelerating environment heterogeneity has exponentially amplified administration challenges for device provisioning, maintenance, and problem management. To meet the growing end user requirements, processes and solutions must be adopted that provide a unified approach to endpoint management while also addressing the unique requirements specific to Apple devices.

The State of Apple in the Enterprise

Few vendor rivalries have had as profound an effect on business productivity as the contentious relationship between Apple and Microsoft. Among many business professionals, the ideological differences between the two vendors' development directions have evolved into something of a religious war. As a result, workers often have strong opinions on which hardware and software platforms empower them with the greatest productivity boost. Historically, however, enterprises have broadly adopted Windows-based PCs as their system of choice for the vast majority of their workforces. Much to the chagrin of Apple enthusiasts, the lower cost of Windows PCs, coupled with a broader availability of business software for Windows platforms, made the platform much more attractive to the enterprise market. Apple did not help matters either, as it focused its marketing and incentive programs on the home and education markets.

The disproportional strength of Windows adoption in the enterprise, however, has started to shift. Organizations are increasingly allowing employees to select their own devices, opening the door to an increased adoption of Apple products in the enterprise. According to EMA primary research, enterprise adoption of Mac desktops and laptops has increased 27% in the past three years. That's an impressive improvement for Apple, but still only accounts for less than 10% of the total enterprise PC market, so there remain broad opportunities for increased Mac use in business environments. Nonetheless, as Apple slowly chips away at Microsoft's control of the enterprise PC market, organizations are increasingly supporting heterogeneous end user computing environments. In fact, today, roughly one-third of all businesses support both Mac and Windows PCs, and this increased presence of Macs is no longer restricted to traditional Apple verticals (such as education and advertising) but now extends to a broad range of industries including healthcare, finance, high-technology, and government.

According to EMA primary research, enterprise adoption of Mac desktops and laptops has increased 27% in the past three years.

Apple's most significant headway into the enterprise market is in the adoption of its mobile devices. Following the release of the iPhone in 2007, Apple's smartphone device almost immediately replaced Blackberry as the mobile platform of choice for business environments. This position was greatly enhanced with the release of the iPad, and Apple continues to garner the lion's share of the market, supplying 37% of enterprise smartphones and 41% of enterprise tablets (edging out both Android and Windows devices). Currently, about 20% of all workers regularly employ an iOS device to perform job tasks. Apple's success in the mobile market can be directly attributed to the "consumerization of IT," as users more frequently selected and purchased their own devices and then brought them into their workplaces. In fact, 71% of iOS devices used to perform business tasks are employee-owned.

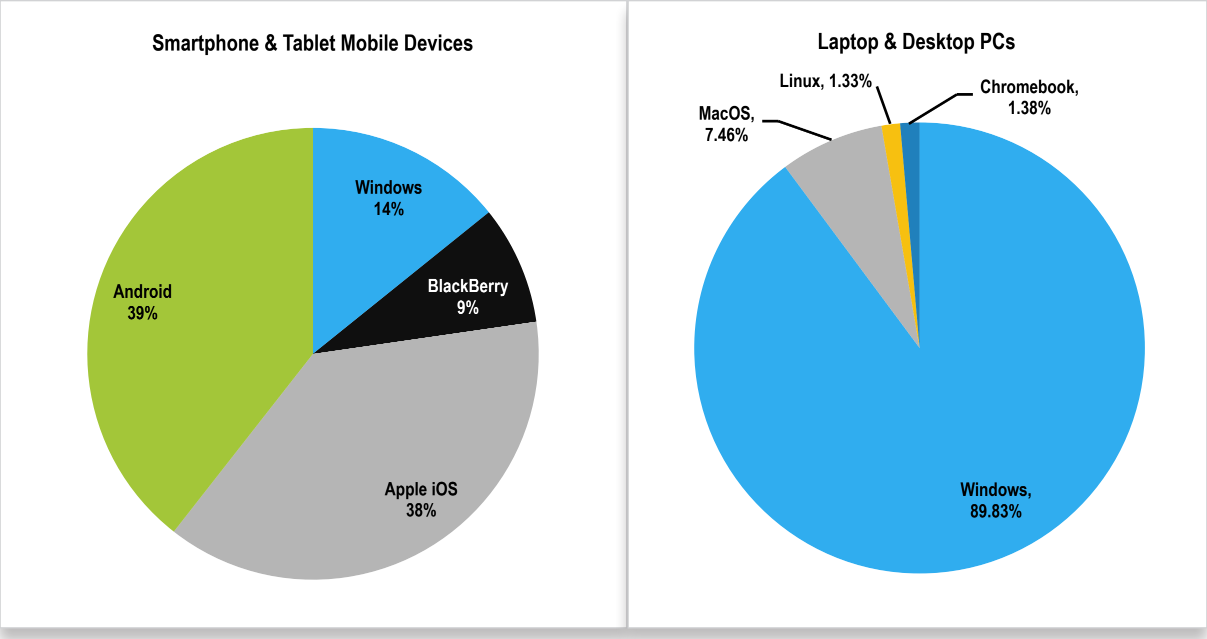


Figure 1. Enterprise adoption of mobile and PC device platforms

In total, 52% of organizations currently rely on a mix of both Apple and non-Apple devices for their end user productivity. This number is only expected to increase as user choice increasingly becomes a factor in business device adoption. For its part, Apple has finally started actively courting the business community by introducing a series of enterprise-focused programs. For instance, the Apple Volume Purchase Program (VPP) reduces the cost of bulk purchases of Apple software licenses, and AppleCare for Enterprise provides 24x7 help desk support and a dedicated account manager to personalize the support experience and ensure Apple products are scalable to large deployment stacks. Additionally, the Apple Device Enrollment Program (DEP) allows organizations to set up configuration profiles before deploying iOS and Mac devices, which encourages organizations to purchase devices directly through Apple, or authorized Apple resellers, and simplifies the onboarding of new devices through integration with third-party management platforms. Through the Apple Developer Enterprise Program, app development tools for coding, testing, and distribution are offered for a bundled discount price to business adopters, encouraging the creation of iOS and Mac business applications. The combination of broad user preference for Apple devices, along with the promotion of business incentives from Apple, suggests the adoption of iOS and Mac devices will significantly grow over the next few years. Organizations must be prepared to support these devices with the same level of performance and reliability that was traditionally reserved for Windows PCs.

Challenges of Managing Apple Devices in a Windows World

It is not surprising that most organizations resisted supporting non-Windows platforms for as long as they did. Managing heterogeneous environments becomes exponentially complex in relation to the number of platforms in the support stack. Every operating system has a unique set of configuration requirements and administration processes. Patches and updates must be continuously and rapidly deployed on all supported endpoint types to ensure peak performance and prevent "zero day attacks," which occur when hackers take advantage of the delay between the discovery of a security hole and its remediation on endpoint devices. Additionally, comprehensive, centralized reporting must be enabled for each managed platform to aid in correlating endpoint states and problems as well as providing continuous compliance assurance. Further, every group of users with a common job function that are actively using each platform will have their own unique set of business requirements. Management complexity and efforts compound with each additional architecture added to the business environment.

Requirements for increased workforce mobility have only compounded challenges in heterogeneous endpoint management support. Currently, 68% of business professionals regularly employ a desktop or laptop PC and at least one mobile device (i.e., smartphone or tablet) to perform job tasks. In addition to iOS and Windows endpoints, Android and Blackberry mobile devices are also commonly used in the workplace. While brand loyalty does play a part in device selection, users are not always consistent with platforms across all devices they adopt. For instance, 85% of iPhone users also regularly use a Windows PC—most likely because they chose the phone while the business provided the PC. This means heterogeneous support must be provided for individual users as well as across the business as a whole, and common applications and data must be accessible on a variety of mobile and PC endpoint architectures to ensure workforce productivity. Moreover, any device used to perform both business and non-business tasks, regardless of the true device owner, must be supported with "bring your own device" practices that deliver and secure business apps and data without limiting any personal use of the PC or mobile device. Supporting a mobile workforce also means enabling broad user self-service functionality, since today's more tech-savvy users increasingly have the skills and expectation to be able to provision and manage their own devices.

It should also be recognized that Apple device architectures have some very unique management requirements, and administration processes designed to support other platforms, such as Windows, will not translate well to delivering comprehensive support on Apple devices. While all operating systems have their own unique characteristics, Apple is substantially more restrictive than other vendors in how its platform can be used. For instance, third-party agent-based software is not permitted to be used on iOS devices, so any management software or processes used to support the devices must operate through Apple's own approved management services. Additionally, to ensure proper application installations, all software deployment processes should work through Apple's Software Update Service (SUS).

Faced with the need to provide comprehensive support for multiple architectures, many organizations have adopted multiple independent management platforms. For example, a business may adopt one platform to support Windows devices, a second to support Macs, and a third to support mobile devices. This results in inefficient "swivel-chair management," where multiple interfaces must be utilized to support a common set of user requirements. These environments lack standardization, requiring different administrative practices for each supported architecture and resulting in duplicate efforts for collecting asset information. Software provisioning is also a challenge since it is difficult to maintain consistent patch and update versions across the disparate devices. Additionally, the use of multiple management platforms is inherently inefficient. Administrators need to be trained on multiple interfaces, and any environment changes need to be entered in multiple locations. Environment failures or performance problems that may affect multiple device types may also be difficult to correlate through independent reporting systems. Lacking a consolidated management platform, organizations often are unable to control their critical end user devices and fail to provide their employees with the service reliability essential to enabling their productivity.

Empowering Apple Users with Unified Endpoint Management

To bestow Apple users with the same high level of support typically provided for Windows devices requires a targeted approach at enabling processes specifically attuned to the unique requirement of Apple devices. A "best of breed" Apple management platform will deliver full lifecycle management support for Mac and iOS devices from initial deployment through final retirement. Administration should be automated as much as possible to minimize support efforts, and management interfaces should be centralized so that operating systems and application configurations can be standardized. Ideally, profiles should be created for individual users and/or groups of users (for instance, segmented by user roles, departments, device types, etc.) so that user environments and policies are customized to meet specific user requirements but also logically grouped so multiple endpoints can be managed simultaneously.

To be considered a "best of breed" Apple management solution, the platform must directly integrate with Apple's management ecosystem.

To be considered a "best of breed" Apple management solution, the platform must directly integrate with Apple's management ecosystem. For instance, integration with Apple's Device Enrollment Program will allow newly purchased iOS or Mac devices to be preconfigured to meet profile settings identified in the centralized platform, eliminating both administrator and end user onboarding activities. When a user first activates their new device, it automatically installs and configures account settings, applications, and remote accessibility to business systems. With this approach, administrators no longer need to employ costly and time-consuming imaging and packaging solutions to provision devices. Similarly, asset management with the centralized solution should be able to track software licenses acquired through the Apple Volume Purchase Program, and Apple SUS should be leveraged for all software deployment processes to ensure proper application, patch, and update installations. It is highly advised that organizations only work with Apple-authorized developers to ensure agents and other management software elements operate in a manner approved for use on Apple architectures. Common third-party applications, such as those offered by Adobe (Acrobat, Flash, etc.), sometimes require unique installation processes, so these should be included in the manage platform. The management platform should also integrate directly with Apple's Global Service Exchange (GSX) to provide an entry point for delivering service information to AppleCare. Further, a "best of breed" Apple management solution provider must have an established business partnership with Apple. A strong relationship between the vendors ensures the management platform is rapidly able to adapt to new software versions and features.

New software is available for your computer.

Installing this software may take some time. If you're not ready to install now, you can choose Software Update from the Apple menu later.

Install	Name	Version	Size
□	iDVD Update	7.0.2	21.9 MB
□	iWeb Update	2.0.4	36.3 MB
□	iMovie Update	7.1.4	39.8 MB
□	Digital Camera Raw Compatib...	2.2	4.1 MB
□	Remote Desktop Client Update	3.2.2	4.4 MB
□	Front Row Update	2.1.6	13.1 MB
□	Java For Mac OS X 10.5 Update 2	1.0	136 MB
☑	Security Update 2008-007	1.0	31.1 MB

Security Update 2008-007 is recommended for all users and improves the security of Mac OS X. Previous security updates have been incorporated into this security update.

For information on the security content of this update, please visit this website: http://support.apple.com/kb/HT1222.

Note: Use of this software is subject to the original Software License Agreement(s) that accompanied the software being updated. A list of Apple SLAs may be found here: http://www.apple.com/legal/sla/.

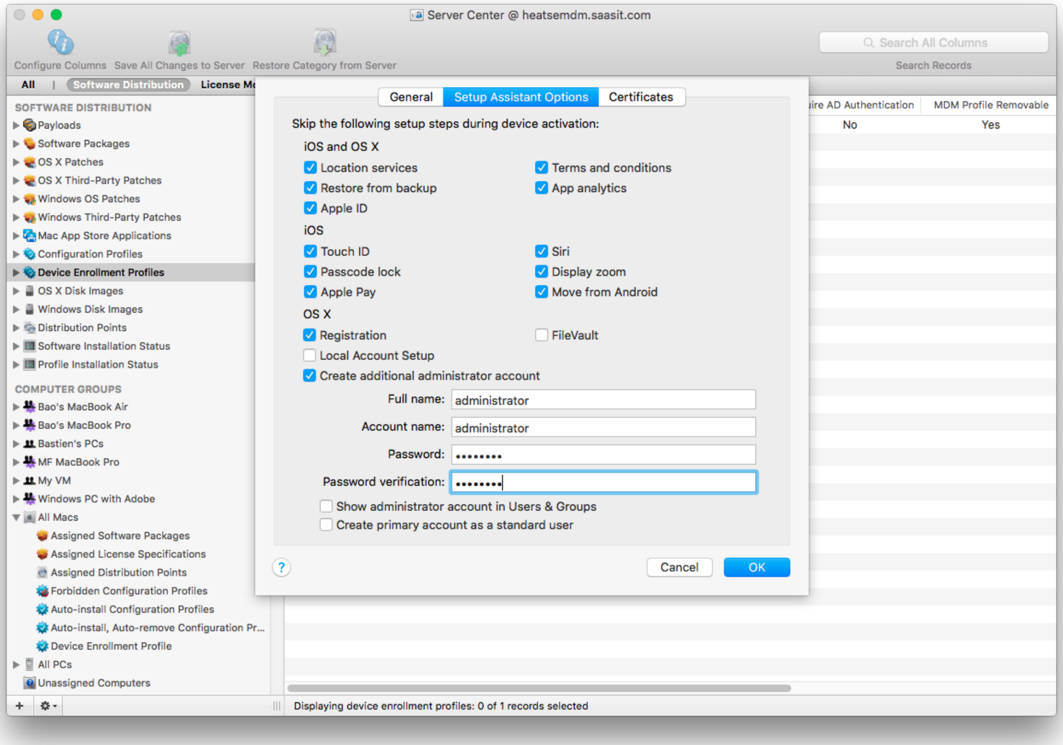
Restart will be required.

While support of Apple-specific requirements is essential for providing comprehensive support for Mac and iOS devices, it is a mistake to consider a "best of breed" solution as synonymous with a point solution. Unless the user environment is 100% Apple-based (a rare occurrence, indeed), administrative functionality supporting all endpoint devices must be consolidated onto a single management interface in order to prevent swivel-chair management. Unified endpoint management solutions are purpose-built to provide centralized management of all devices in a support stack with a common asset database, a single set of user profile definitions, and consolidated data analysis and reporting engine. Management tasks are performed in essentially the same way, regardless of the endpoint type, to create consistent administration experiences. For the majority of modern enterprises, therefore, an ideal unified endpoint management platform should provide "best of breed" functionality for all Apple and Windows devices in use in the organization. Additionally, a unified endpoint management platform should provide self-service capabilities that are consistent, allowing end users to provision applications and perform tasks in the same way regardless of the devices they choose to use. In this way, unified endpoint management enhances user experiences.

Security assurance is also an essential component of a unified endpoint management platform, particularly when supporting a mobile workforce that will be utilizing their devices in locations outside the control of the enterprise. All business data must be protected from unauthorized access and distribution on all devices employed by end users. Data loss prevention practices limit access to business content with the use of multi-factor authentication and encryption. These security processes should be managed from the unified console consistently and with the same effectiveness for all supported platforms, and the status of authentication and encryption services should be continuously monitored to rapidly identify any breaches or potential problems. Security monitoring is also essential for achieving compliance objectives. All supported endpoints must meet the same stringent compliance requirements regardless of the operating platform, and a unified endpoint management solution can provide the centralized reporting necessary to deliver the proof of compliance or to rapidly identify out of compliance elements before performing an official audit.

Mobile devices that are permitted to perform non-business tasks (such as devices personally owned by employees) must be supported with BYOD management practices on all endpoints. Principally, this requires business apps and data to be completely isolated from a user's personal resources. Containerization is the common method employed for achieving resource isolation, but whatever method is used must be consistent for all supported mobile devices so that users are able to access business services in the same way, regardless of the device they choose to use. Some users are not comfortable with their business performing any management or security activities on their personal devices, so users must have the ability to opt into any BYOD services provided. Of course, users who decide not to opt in will simply not be able to access business resources on their devices.

The common denominator for enabling comprehensive multi-platform support is the adoption of a unified endpoint management platform designed to deliver full administrative support to meet both Apple and Windows device management requirements. As an example, Ivanti offers the LANrev management platform, a complete lifecycle management platform for Apple and Windows management and includes a common asset inventory, a centralized software provisioning solution, and multi-platform configuration management functionality. All administration is performed from a centralized console interface with built-in role-based access and a policy-based approach to security and configuration management. Ivanti LANrev is directly integrated with Apple's management services. For instance, the Apple DEP setup wizard can enforce enrollment through LANrev, authenticate users via a local Active Directory, and restrict the availability of unapproved and unsecure features. Direct integration is also included for tracking software licenses in Apple's Volume Purchase Program and to provide status information to AppleCare through Apple GSX. Ivanti PatchLink is also integrated with LANrev to rapidly deploy patches on Mac OS, Windows, Unix, and Linux endpoints, eliminating zero-day vulnerabilities.



Skip the following setup steps during device activation:

iOS and OS X

☑ Location services ☑ Terms and conditions
☑ Restore from backup ☑ App analytics
☑ Apple ID

iOS

☑ Touch ID ☑ Siri
☑ Passcode lock ☑ Display zoom
☑ Apple Pay ☑ Move from Android

OS X

☑ Registration □ FileVault
□ Local Account Setup
☑ Create additional administrator account

Full name: administrator
Account name: administrator
Password: ••••••••
Password verification: ••••••••

□ Show administrator account in Users & Groups
□ Create primary account as a standard user

Displaying device enrollment profiles: 0 of 1 records selected

Figure 2: Ivanti LANrev Apple device enrollment profile setup

EMA Perspective

Until recently, there was no question that we lived in a Windows world. This was especially true in the business market, where Windows-based devices dominated the vast majority of desktop computing solutions. It's not surprise, then, that IT management solution providers responded by delivering platforms that were almost entirely Windows focused. "Best of breed" Windows management platforms have become almost commonplace, with most solution suites offering the majority of key capabilities essential to successfully provisioning and supporting Windows endpoints. As Macs, iOS, and other devices entered workplaces, management solution providers extended a few capabilities of their Windows-focused management platform to support other devices. However, the functionality was still principally Windows-centric in design and functionality. As a result, Apple devices were traditionally second-class citizens in endpoint management, and apple users had to take a backseat to Windows users in the availability of support services.

Conversely, solutions that exclusively support Apple devices (most notably, those offered by JAMF Software) are point solutions that are not able to extend support to non-Apple devices. To effectively empower end user productivity, organizations must adopt a unified endpoint management platform that provides "best of breed" functionality for all supported endpoint platforms. Even in environments that principally support Apple devices, some Windows devices may be in use but will not be supported by an Apple-only solution and may go unsupported or require the adoption of a completely separate management solution. Alternatively, organizations can restrict the devices employees may use to perform job tasks, but this unnecessarily restricts the freedom of users to choose the devices they prefer and that will best optimize their productivity.

Only a unified endpoint management platform that includes comprehensive support for Apple devices, such as Ivanti LANrev, enables organizations to fully support Mac and iOS users while still delivering extensible Windows support in a way that is easy to manage and cost-effective. Moreover, a single, consolidated management platform reduces administrative efforts while enhancing security and improving the performance and reliability of IT investments.

About Ivanti

Ivanti is IT *evolved*. By integrating and automating critical IT tasks, Ivanti helps IT organizations secure the digital workplace. For more than three decades, Ivanti has helped IT professionals address security threats, manage devices and optimize their user experience. From traditional PCs, to mobile devices, virtual machines and the data center, Ivanti helps discover and manage your IT assets wherever they are located, improving IT service delivery and reducing risk. Ivanti also ensures that supply chain and warehouse teams are effectively leveraging the most up-to-date technology to improve productivity throughout their operation. Ivanti is headquartered in Salt Lake City, Utah, and has offices all over the world. For more information, visit www.ivanti.com.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
3451.040417