What iOS 9 Means for the Enterprise

v 1.2

MobileIron

Executive Summary

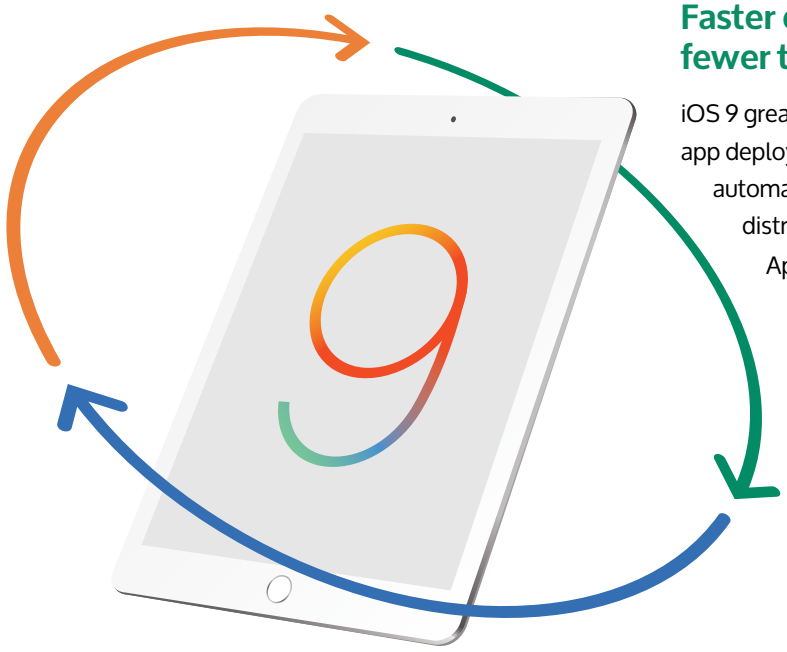
The release of iOS 9 offers much more than just new features for consumers and enterprise users. It further simplifies the complex challenges that IT organizations face when securely deploying iOS devices and apps across the enterprise. Combined with enterprise mobility management (EMM), iOS 9 provides an advanced set of tools to enable faster device configuration, easier app distribution, and more robust security for enterprise data. In just a few touches, IT admins can configure thousands of devices for employees, who are then ready to go as soon as they power on their new devices.

iOS 9 will not just help IT admins do their jobs faster and more efficiently, it will also help them accelerate their careers as mobility experts. iOS 9 combined with EMM gives IT admins the tools needed to improve employee productivity and support business goals.

The key upgrades in iOS 9 include:

Advanced enterprise security:

New security features for apps, devices, network configurations, and user experience help IT address critical security gaps.



Faster deployments with fewer touches:

iOS 9 greatly simplifies device and app deployment with features such as automated enrollment and the ability to distribute apps without enabling the App Store on end-user devices.

Enhanced productivity:

New features such as Mail upgrades, iPad multitasking capabilities, and predictive Calendar suggestions will help employees work more seamlessly on their iOS devices.

To better understand what iOS 9 means for the enterprise, this white paper provides a technical overview of these and other new features in the latest release. It also provides recommendations for developers and IT admins, who will need to evaluate how some of the new capabilities will impact their processes going forward.

iOS 9: Greater than the Sum of its Parts

iOS devices exploded into the enterprise seemingly overnight. Once users fell in love with their iPhones and iPads, they wanted to use them for everything, including work. The expectations and demands from mobile employees forced IT to quickly learn how to securely enable those devices without compromising the iOS user experience — all while juggling their other IT responsibilities. Resourceful admins ultimately secured and managed corporate email and calendar features with early mobile device management (MDM), but the adoption of advanced mobility solutions hasn't kept pace.

For IT organizations that haven't fully embraced what EMM can do for their business, now is the time to do it. The introduction of iOS 9, combined with EMM, gives IT a far more seamless and unified way to deploy, secure, and manage iOS devices and apps from start to finish. Together, iOS 9 and EMM further simplify all the complex, backend security and management work for IT. Admins can quickly configure and deploy devices with fewer touches so end users can be productive from the minute they get their devices.

> *iOS 9 and EMM further simplify all the complex, backend security and management work for IT.*

While many of the new features are impressive on their own, the true value of iOS 9 is much greater than the sum of its parts. Combined with EMM, iOS 9 enables IT to quickly unlock the real business potential of iOS devices to support their company's mission and goals. iOS 9 also gives IT admins the leverage they need to advance their own careers as enterprise mobility experts. For example, they can deploy thousands of devices without ever tapping on those devices to configure them. With just a few clicks, they can set up hundreds of kiosk devices so they are ready to go right out of the box. All users have to do is power on the device to access the secure apps and content they need.

With the release of iOS 9, Apple is empowering both enterprise IT and app developers to take the mobile user experience and enterprise security to a new level. In this white paper, we'll discuss what these enhancements mean for the enterprise and provide recommendations for going forward.

Enhanced Enterprise Security: Simpler for IT, More Transparent for Users

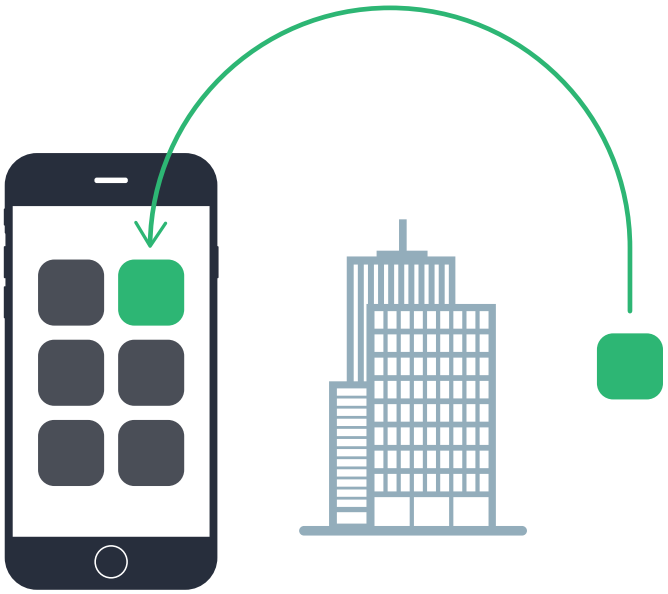
The new security features in iOS 9 make it much easier for IT to protect devices and apps without impacting the user experience. Through an EMM, IT can now close several iOS security gaps while allowing employees to access the apps and content they need with fewer touches and interruptions. iOS 9 includes enhancements to app security, device security, network security, and the user experience, which are covered in more detail below.

App Security

Distribute and Update Apps without the App Store

Before iOS 9, IT organizations that wanted to distribute corporate apps without enabling the App Store on corporate devices faced several challenges. Typically, an admin would enable the App Store just long enough to deploy the necessary business apps (in the middle of the night, for instance). The admin would then run a report to make sure all the required employees received the app. Once the app deployment was complete, the admin could disable the App Store. Not only was this a time-consuming process, it also created a security gap because users could install unauthorized apps from the App Store while it was enabled on the device.

iOS 9 includes enhancements to app security, device security, network security, and the user experience.



iOS 9 eliminates this problem by allowing IT to completely disable the App Store and instead deploy apps through the EMM server or Apple Configurator 2 (the new version released with iOS 9). IT can silently push apps through the EMM server via "Send Message" on supervised devices or assign apps to the device for the end user to install.

This allows mobile administrators to more easily maintain a standard deployment blueprint and not worry about end users installing personal apps on supervised devices. IT can easily manage curated apps, whitelists, and blacklists in an EMM app store and prevent users from installing unauthorized apps.

These new app security capabilities are especially advantageous for managing kiosk devices and fleet deployments. For example, many resorts offer iPads to guests so they can learn about daily events and excursions, create personal itineraries, view menus, order room service, access the Internet and more. With iOS 9, IT admins can easily update the apps on all of the iPads without worrying about guests downloading unauthorized and potentially malicious apps on supervised devices.

New IPv6 App Requirements

Apple is making IPv6 an App Store submission requirement in iOS 9, which means that developers will need to resubmit their code to get their apps approved. See the "Notes for Developers" section at the end of this paper to learn more.

> *By disabling the App Store on supervised devices, IT can manage curated apps, whitelists, and blacklists in the EMM app store and prevent users from installing unauthorized apps.*

Managed vs. Supervised Devices

Managed device: A managed device can be owned by either the employee or the company. With a managed device, IT can secure and manage corporate data and apps separately from the employee's personal data and apps by installing an MDM profile. Corporate content and apps can be wiped if the device is lost, stolen, or falls out of compliance, while personal information remains untouched.

Supervised device: Supervision is typically reserved for corporate-owned devices and provides IT with greater control than a managed device. In supervised mode, an iOS device can be secured with several management features, including single-app mode and always-on VPN. IT can also restrict features such as the iCloud Photo Library and automatic app downloads — restrictions that the user can't modify. Supervision is typically initiated during device setup through Apple's Device Enrollment Program (DEP).

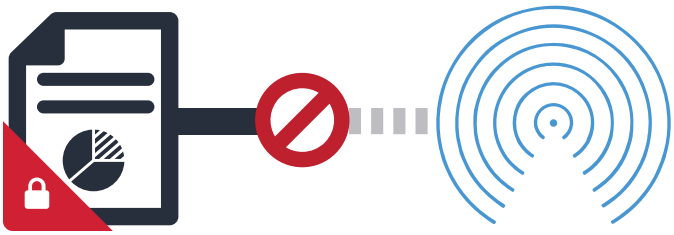
MobileIron

Device Security

New Device Restrictions

In iOS 9, Apple added new device restrictions to help IT admins close some of the main security gaps on iOS devices. For example, AirDrop, which is Apple's tool for wirelessly transferring data between devices, was a potential source of data loss in previous iOS versions. In iOS 9, AirDrop can be treated as an unmanaged destination so employees can't use it to transfer corporate data from managed apps. The chart below includes some of the key device restrictions in iOS 9:

Feature	Security Restriction	Supervised Mode Only
AirDrop	AirDrop can be treated as an unmanaged location so managed apps like email can't share content or files, such as attachments, through AirDrop.	
Automatic app downloads	The EMM admin can toggle this switch to enable or disable automatic app downloads. This helps avoid the mass distribution of faulty apps by allowing IT to ensure that only tested and approved apps are intentionally distributed to end users. Note: A user can still manually download apps even if the automatic feature is turned off.	✓
iCloud Photo Library	The EMM admin can enable or disable iCloud Photo Library sync on the entire device.	✓
News app	Depending on corporate policies, IT organizations can choose to enable or disable News, a new app in iOS 9.	✓
Pair with Apple Watch	This allows or disallows the pairing of Apple Watch to iPhone.	✓
Screen recording	Along with screenshots, screen recordings can be restricted on any managed device regardless of supervision.	
Keyboard shortcuts	IT can restrict the creation or use of keyboard shortcuts, which allow users to create their own text substitutions. For example, a user could create a keyboard shortcut that instructs iOS to automatically replace "np" for "No Problem." So anywhere the user types "np", iOS would automatically replace it with "No Problem." Restricting keyboard shortcuts can help prevent supervised devices from being compromised by pranksters, who could create distracting and potentially embarrassing shortcuts on a user's device.	✓
Trust UI	This closes a security loophole that can be exploited by rogue enterprise developers, who might socially engineer apps to install malware on iOS devices. In iOS 9, any app distributed via EMM is implicitly trusted and does not require users to authorize the download on supervised devices. Users who try to download apps on managed devices will receive a prompt that tells the user whether or not the developer is trusted before downloading the app. See the "Trust UI" section below for more information.	
Modify device name, setting a passcode, wallpaper	These restrictions prevent employees from altering these preset configurations, such as branded wallpaper, which is especially useful in kiosk or fleet deployments.	✓



AirDrop can be treated as an unmanaged location so managed apps like email can't share content or files, such as attachments, through AirDrop.

Six-digit Passcode

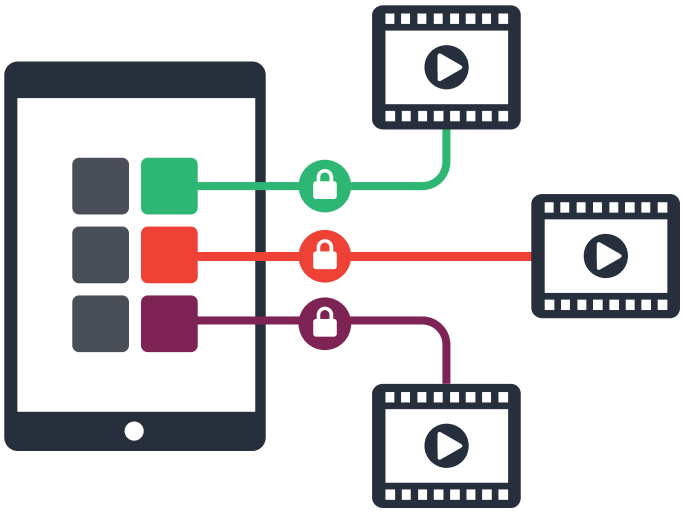
Apple has started to move to six-digit passcodes for iPhones and iPads equipped with a Touch ID sensor. Note that only the Simple Passcode feature changes in iOS 9; IT can still require a more complex passcode. The passcode requirement can also be turned off, but if it is enabled, it will have to contain six digits going forward. While this feature is great for overall device security, IT should expect questions from mobile employees accustomed to four-digit passcodes.

Networking Security

Per-app VPN and Networking Improvements

Apple announced new per-app VPN enhancements, which are designed to give enterprise IT more control over network traffic. They include:

1. **Support for UDP traffic.** UDP traffic will now be supported with the current per-app VPN implementation. This should benefit apps that require UDP in order to stream audio or video.
2. **A per-app VPN connection can be established at layer 3.** Prior to iOS 9, the per-app VPN network connection was determined by the underlying network settings that were already established. In iOS 9, a network or EMM admin can now define specific network routes and domain name server (DNS) settings that a managed app will use when making the per-app VPN connection. This security enhancement provides an EMM admin with far more control over the network traffic that a managed app uses.



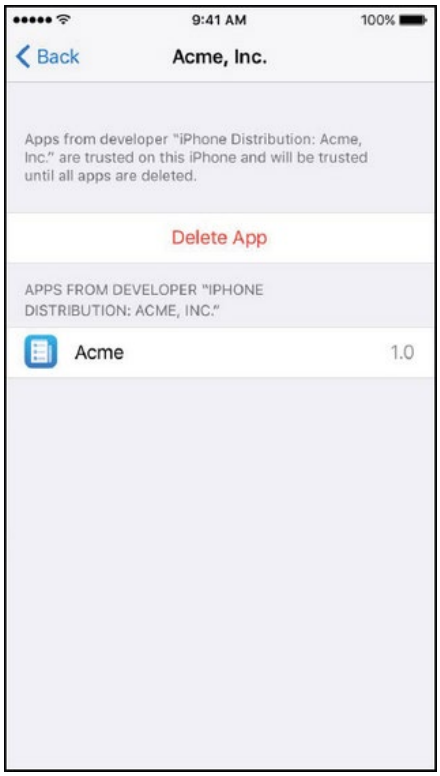
New Network Usage Rules

iOS 9 gives admins greater control to define how managed apps can use the network. For example, network usage rules allow IT to specify how managed apps use networks, such as cellular data networks, by restricting the app's ability to connect over cellular when roaming on other networks. This capability is only available on supervised devices.

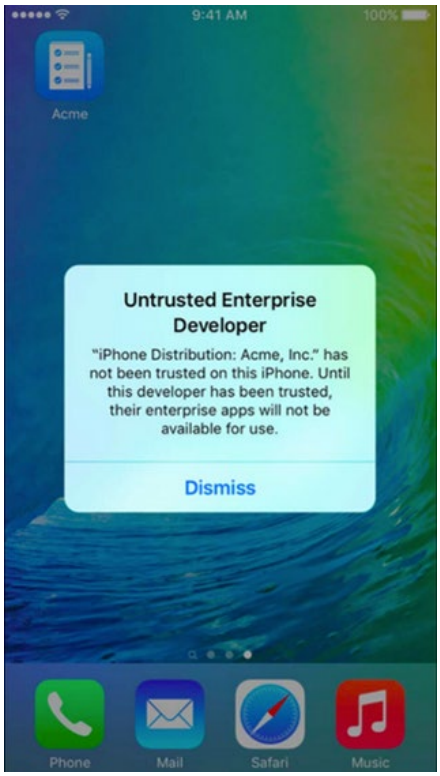
Secure User Experience

Trust UI

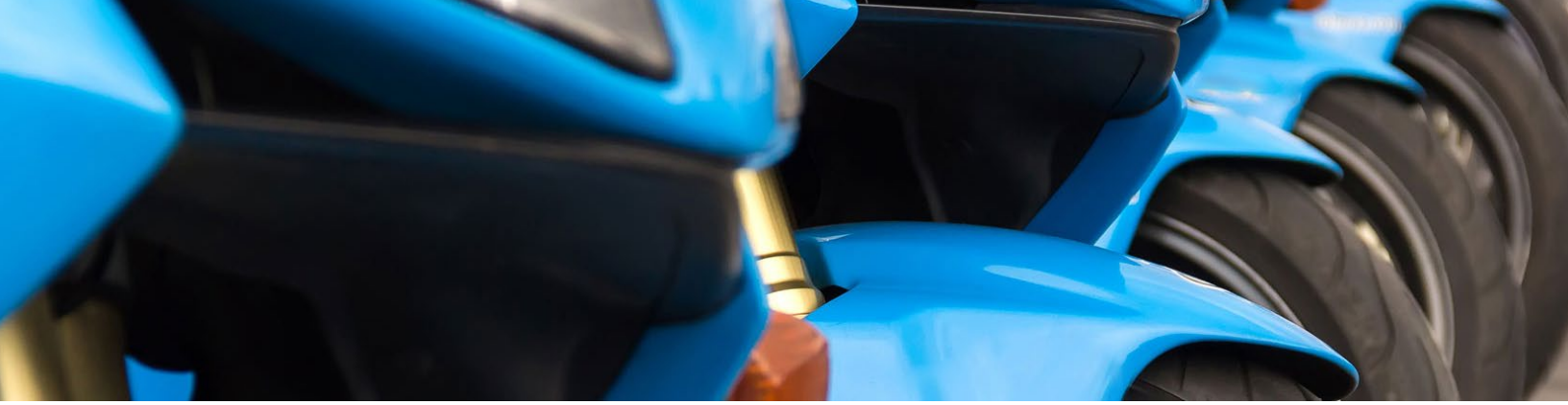
iOS 9 introduces a new trust UI that makes it easy for users on managed devices to know when they are installing an app from an authorized or unauthorized enterprise developer. This new interface allows end users to trust the certificate used to digitally sign in-house apps, shown in the image below:



The new trust UI also prevents users from installing apps from unauthorized developers on managed devices. Although IT won't be able to block unmanaged apps on employee-owned devices, iOS 9 will allow IT to prompt users with this warning about downloading apps from untrusted developers:



In-house apps distributed via an EMM server to managed devices will not show the trust UI prompt. These apps will be implicitly trusted because the device is already managed by the EMM server trying to distribute the app. If the device is supervised, the app will install silently. If the device is not supervised, the end user will be prompted to install the app.



Device and App Deployments: iOS 9 Delivers a Seamless Experience from Purchase to Productivity

iOS 9 includes several updates that directly respond to enterprise customer needs by greatly simplifying both device and app deployment processes for IT admins and end users. Now IT can accelerate deployments by setting up a fleet of iPads with just a few touches, which allows employees to start using them with no additional configuration required.

Device Management: Accelerating the Rollout Process

iOS 9 builds on the enterprise enhancements in iOS 8 by adding several key features that make it faster and easier for IT to configure, enroll, and manage iOS device deployments.

iOS 9 is compatible with iPhone 4s, iPad 2, iPad mini, iPod touch fifth generation and later models.

Deployment through the Device Enrollment Program (DEP)

Enrollment optimization

Prior to iOS 9, the profile setup process could cause problems for the end user. For example, devices could be distributed to employees without confirming that all the proper policies and restrictions were in place. iOS 9 eliminates this problem by enabling the MDM server that manages the device to keep the device in Setup Assistant until it is fully configured and ready for the end user. (Admins will be able to remove the Setup Assistant panes for Apple Pay, Touch ID, Zoom, and the new Android Migration option.)

Once the device is fully configured and enrolled in the MDM server, it can exit the Setup Assistant. This ensures that the device contains all of the required policies and restrictions before an end user even touches it. This also eliminates the need for IT to force device check-ins to make sure nothing was missed, and helps reduce support tickets. Once enrolled, DEP devices can be forced to update to the latest version of iOS, and admins can command managed devices to all update at the same time.

Automated enrollment

This new feature in iOS 9 enables devices to be enrolled in the MDM server through the DEP without anyone tapping on the actual device, which greatly simplifies the DEP process. Here's how it works:

IT admins can force DEP devices to update to the latest version of iOS.

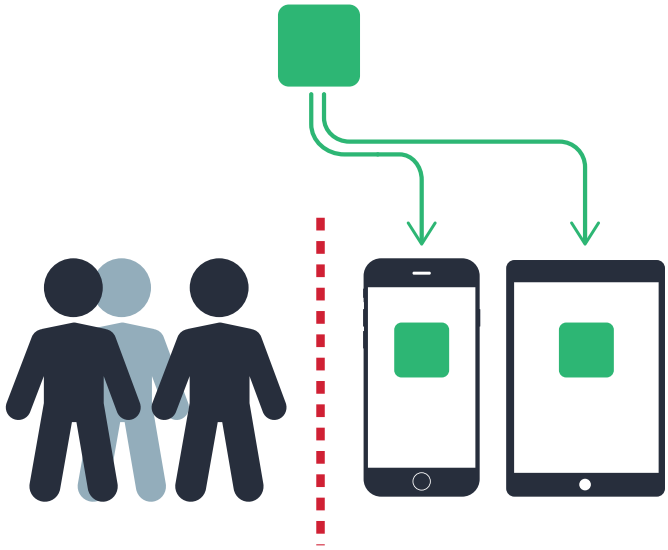
The admin configures the DEP settings, but instead of the user walking through Setup Assistant to configure the device, the admin connects the device to Apple Configurator 2 to complete the configuration setup for the user. The device is then ready to go without requiring any user interaction. Multiple iOS 9 devices can also be configured and enrolled by connecting them via USB cable to Apple Configurator 2, eliminating the need to configure each device separately.

App Distribution and Management: Fewer Touches, Faster Deployment

iOS 9 greatly simplifies app deployment and management processes for IT admins and creates a more seamless enterprise workflow for employees. Now IT can perform more "behind the scenes" app installation and management work that is transparent to the end user. This eliminates many unnecessary touches for users to securely get to the apps and content they need on their devices. Fewer prompts and notifications mean less frustration for employees. This section covers some of the essential new app distribution and management capabilities in iOS 9.

Device-based Licensing Eliminates the Apple ID Requirement

One of the biggest changes in iOS 9 is device-based licensing, an app distribution model that eliminates the need for an Apple ID. Prior to iOS 9, installing an app from the App Store required the end user to have an Apple ID, which often caused problems for enterprise users. To meet this requirement, IT would generate Apple IDs on behalf of employees, and expect them to use these separate IDs to access managed apps. This created ongoing headaches for the help desk because users were frequently confused about which ID to use.



The new device-based licensing model solves this problem by offering an alternative to the existing user-based licensing model, which will still be available in iOS 9:

1. **Device-based licensing:** This deployment method is ideal for environments where multiple users share a device, such as in a retail store or shipping warehouse. In this licensing model, IT can assign apps to devices instead of users. There is no invitation process for the user because no Apple ID is required on the device in order to distribute and install apps. Even if there is an iTunes Apple ID configured on the device, these apps will not appear in the user's purchase history because they are not assigned to that user. The EMM admin has complete control over any changes or updates to the app — the user has no way to manage apps with a device-based license. Although it's more expensive, device-based licensing eliminates Apple ID management challenges.

   Note: Device-based licensing requires all apps to be acquired through Apple's Volume Purchase Program (VPP).

2. **User-based licensing:** If end users are given multiple corporate devices, assigning a license to the user may be preferred. An EMM provider can distribute a user license that works across all of the user's devices.

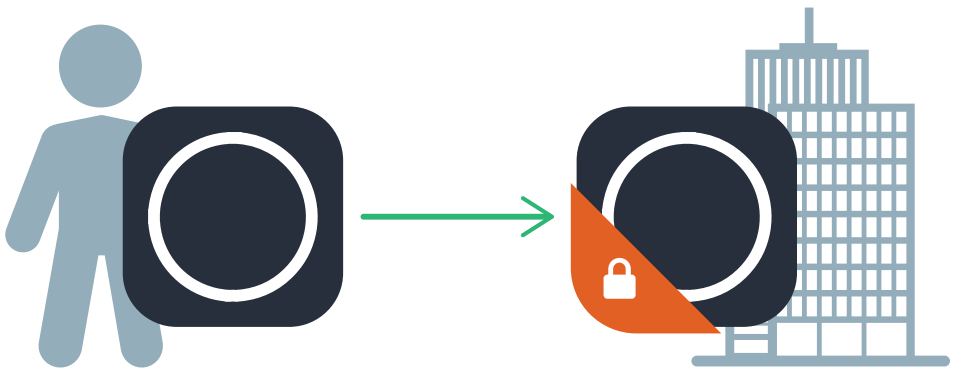
   Note: IT will still need to manage Apple IDs in order to issue user-based licenses for multiple devices.

IT should note that both of these methods work only within the domain of the VPP and not outside of it. Each enterprise will need to evaluate their needs before deciding which licensing model best meets their deployment requirements.

iOS 9 eliminates Apple ID management headaches by allowing app licenses to be assigned to the device instead of the user.

Convert Employee-installed Apps into Managed Apps

With iOS 9, an EMM vendor like Mobileiron can convert a user-installed app into a corporate-liable app, which can be done in the background with no loss of user data. Prior to iOS 9, this process required an end user to manually delete the app and then reinstall the same app through an EMM enterprise app store.



Once the app is converted to a managed app, users can benefit from enterprise security controls without having to reinstall the app. This conversion is invisible to the user on a supervised device, but on an unsupervised device the user will need to accept the change. IT admins should note that an app can't be both unmanaged and managed on the same device. In the event of a conflict IT will need to choose one and notify the end user.

Volume Purchase Program (VPP) Updates

By eliminating the Apple ID requirement to install apps on managed devices, iOS 9 also eliminates the app invitation process for device-based licenses. User-based licenses will still require an Apple ID, as in previous versions of iOS.

VPP Expands to 26 Countries

VPP has significantly expanded its global footprint to include 26 countries (up from eight prior to iOS 9). The new program includes a multinational app assignment, which allows an enterprise to purchase an app in any participating VPP country and distribute it in any country where that app is sold. For example, if a company is headquartered in the UK, it can buy an app and distribute it to users in the US, France, and South Africa as long as the app is available in the App Store in those countries — even if there is no VPP.

MobileIron

New APIs Improve B2B App Store Management

Introduced by Apple in 2013, the B2B App Store allows developers to offer custom B2B apps directly to business customers who have a VPP account. This enables developers to reach a wider business audience because they can build an app for one company and then customize and rebrand the same app for a different company. Once an app is created, the developer uploads it to the iTunes Connect Store for Apple to review. Business customers then login to their VPP account to access apps from that developer. Unlike the B2B App Store, an EMM enterprise app store primarily hosts company-specific apps that are available only to the employees of that company.[1]

In iOS 9, Apple is adding better EMM support features for apps in the B2B App Store. Prior to iOS 9, B2B metadata did not exist in iTunes, which meant there was no way to automatically import that information into the EMM app catalog. As a result, EMM providers had no easy way to stage apps from the B2B App Store. With iOS 9, B2B app metadata will be included in the iTunes metadata stream. This will allow EMM vendors to access that information so they can add B2B apps to an app catalog.

1 Rao, Arun. "What is Apple's B2B App Store and How Does It Work?" ChaiOne, July 29, 2014. http://chaione.com/what-is-apples-b2b-app-store-and-how-does-it-work/

Productivity: Enabling Contextual, Seamless, and Continuous Workflow

With iOS 9, Apple introduced several new features to boost enterprise productivity by helping employees access content in ways that are smarter and aware of the user's location, history, settings and more. Below is a summary of the features most relevant to business users and their benefits for the enterprise.

Mail Upgrades

- **Attachment markups:** PDF files and graphics attachments in an email can be marked up at the moment of sending them. For instance, a user can circle a typo on a document, draw arrows on a diagram, and add a signature to a contract. In addition, users can now add file attachments of any type to outgoing Mail messages (not just photos or videos). Users can also save any file attachment from Mail to iCloud Drive, unless the admin restricts this capability.[2]

- **Name suggestions:** When a user composes a new email message, iOS 9 suggests the names of other people usually copied on messages to the same recipient or with the same subject line such as, "Quarterly Sales Report." This is a great time-saver and helps ensure critical messages go to all relevant recipients.

- **Phone number lookup:** When a call is received from someone who is not in the user's address book, iOS 9 instantly searches the user's mail to try to find a match for that number so it can display a name as caller ID. For instance, if a sales manager gets a call in the middle of a meeting and sees that it's coming from an important customer, she may decide it's worth interrupting the meeting to leave the conference room and take the call.

2 Pogue, David. "iOS 9 Deep Plunge: The 57 Coolest Features." July 7, 2015. https://www.yahoo.com/tech/ios-9-deep-plunge-the-57-coolest-features-123432534089.html

iPad Multitasking Features

Multitasking in iOS 9 will completely change the way many employees work. Employees will be able to accomplish tasks that were once faster to do on a desktop or which required the ability to multitask. iOS 9 now makes many of these tasks just as easy (or easier) on an iPad.

The new iPad multitasking functions include Slide Over, Split View, and Picture in Picture:

- **Slide Over** can be activated in any supported app. Pulling from the right to left side of the screen opens up a second window, which takes up one-third of the screen. This allows the user to quickly send an email or answer an incoming email without the user having to stop the current task.

- **Split View** is available on iPad Air 2, and shows two apps at once by pulling the Slide Over view further to the left. A user can use both apps independently, with each taking up half the screen.

- **Picture in Picture** allows the user to minimize the video window to one corner of the iPad and continue to use other apps while watching a video or participating in a FaceTime call. This feature will make life much easier for enterprise users who need to pull up a presentation or other document during a FaceTime call.

For now, all of these features are compatible only with Apple's apps, but third-party app providers will likely want to take advantage of these new multitasking capabilities very soon.[3]

Predictive Calendar Suggestions

This feature tells users what time they should leave their current location to arrive at another location by a certain time. This is especially beneficial for attorneys, service technicians, real estate agents, and other business users who need to anticipate travel times between appointments and meetings.

3 Clover, Juli. June 12, 2015.

Notes Enhancements

iOS 9 has added some major enhancements to Notes that will transform it from a simple text-based app to a feature-rich, note-taking app. For example, a Notes page can now include a checklist of to-do's, photos, maps, Web links, and more. The new Attachments Browser lets the user view a palette of all the content added to notes, which can help enterprise users quickly repurpose this content for other projects. Notes also appears in the list of options when the user taps Share, so content can be added directly to a note from within another app. These new features require the user to upgrade to the new Notes format, which can only be opened with devices running iOS 9 or OS X El Capitan for the Mac.[4]

More Contextualized Siri Interaction

Users can now give Siri more elaborate spoken commands such as, "Show me the keynote video from last week's conference." If a user is looking at a text message on an iPhone, she can ask Siri to "Remind me about this message when I get to the office." When the employee arrives at the office, the device will offer a link to the page or message so the employee can continue working where she left off.

Extended Battery Life

With iOS 9, Apple designed several tweaks to squeeze more battery life out of every charge. For instance, if an iPhone is face-down on the table, the screen no longer lights up for incoming notifications. It also includes a new Low Power mode, which can be turned on on at any time. In Low Power mode, the phone ceases unnecessary actions such as animations and updating apps in the background. The processor also slows down, which means app switching will also run more slowly. Extended battery life is a great feature for companies that loan devices to customers and employees, because they can go longer between runs before having to recharge the device.[5]

4 Pogue, David. July 7, 2015.
5 Pogue, David. July 7, 2015.

iOS 9 Enhancements for Developers

iOS 9 includes several features and requirements that developers should be aware of for all iOS apps moving forward.

App Licensing

iOS 9 will now offer device-based licensing, which requires an app license for each device. To enable device-based licensing, developers will need to go into iTunes Connect to make sure they approve their apps to be assigned to devices. Otherwise, in VPP, they will only be allowed to enable apps for users.

App Transport Security

App Transport Security (ATS) is a new feature of iOS 9 and OS X El Capitan that is designed to improve Apple OS and app security. ATS helps protect mobile data by imposing several security best practices to help keep data secure during network transmission. For example, ATS requires all network requests to be sent over a secure connection. When ATS is enabled, network requests are automatically made over HTTPS instead of HTTP.[6] iOS 9 requires app developers to adopt ATS as soon as possible for all new apps as well as upgrades to existing apps.

New IPv6 App Requirements

Apple is making IPv6 an App Store submission requirement in iOS 9, which means that developers will need to resubmit their code to get their apps approved going forward. IPv6 support helps ensure applications work for every employee and customer, anywhere in the world. IPv6 avoids the need for network address translation, provides faster routing through the network by using simplified headers, prevents network fragmentation, and avoids broadcasting for neighbor address resolution.

6 Jacobs, Bart. "Apple Tightens Security With App Transport Security." Tuts+. July 17, 2015. http://code.tutsplus.com/articles/apple-tightens-security-with-app-transport-security--cms-24420

App Thinning

Apps in iOS 9 will be designed to take up even less space on Apple devices. App thinning makes it easier for developers to design their apps so users only download the code they need. As a result, app installations and updates will run much faster, require less battery life, and provide a better user experience.[7] For more information about app thinning, visit https://developer.apple.com/ios/pre-release/

New Unified Apple Developer Program

Developers will no longer be required to maintain separate memberships to develop for Apple's Mac and iOS platforms. By creating a single developer program, Apple is helping to simplify iOS app development with a single place to develop, manage, and distribute apps across all Apple platforms.[8]

7 Heisler, Yoni. "'App Thinning' is the Best iOS 9 Feature You Haven't Yet Heard Of." BGR, June 10, 2015. http://bgr.com/2015/06/10/ios-9-app-thinning-iphone-ipad-storage/

8 AppleInsider, June 8, 2015. "Apple reveals new integrated developer program for Mac, Watch, and iOS" http://appleinsider.com/articles/15/06/08/apple-reveals-new-integrated-developer-program-for-mac-and-ios-

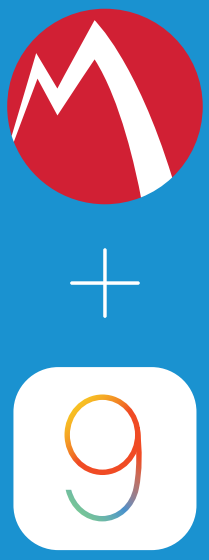
Conclusion

iOS 9 offers far more than just a collection of new features. Combined with EMM, it delivers advanced capabilities to enhance enterprise security, simplify device and app management, and take employee productivity to a whole new level. IT admins also gain management tools that can help accelerate their careers by making it easier to deliver the full value of iOS mobility to the enterprise.

One of the biggest advantages of iOS 9 is how much faster IT can deploy devices and apps and allow users to access them with fewer touches. To support the new features of iOS 9 in your enterprise, it's important to prepare both the IT organization and employees for all the updates coming their way. We recommend informing key stakeholders — including IT admins, security team members, developers, and end users — about what to expect, how to plan, and how they will benefit from iOS 9. The list of recommendations below should help you get started.

Enterprise Recommendations for iOS 9

1. Now is the time to reevaluate app deployments that have been stalled by complex distribution requirements. iOS 9 removes many deployment obstacles, such as the need for the App Store and Apple ID on iOS devices, which should greatly simplify and accelerate enterprise app distribution.
2. Apple is emphasizing device supervision, so IT should determine how to supervise all corporate-owned iOS devices as soon as possible. The good news is, DEP makes the process of setting up and managing supervised devices much easier and more robust with advanced management capabilities.
3. For organizations with a four-digit passcode policy, educate end users about the upcoming six-digit passcode requirement so they can prepare to transition.
4. Meet with line-of-business (LOB) managers and discuss ways to get the right devices, apps, and data into the hands of employees. This is an opportunity to educate functional business groups about the new productivity features in iOS 9 and how they can help accelerate the business.
5. Make sure all internal and external developers understand iOS 9's new app requirements. To summarize the key changes, you can forward them the section above, "iOS 9 Enhancements for Developers." Admins should also update the deployment and security strategy for internal apps to account for iOS 9's new security features, such as new device restrictions and VPN capabilities.



For More Information

To learn more about iOS 9 and what it means for the enterprise, please visit mobileiron.com/ios9

For questions regarding your iOS implementation, please contact MobileIron at globalsales@mobileiron.com

MobileIron