What iOS 7 Means for the Enterprise

Version 1.3

MobileIron
415 East Middlefield Road
Mountain View, CA 94043 USA
Tel. +1.650.919.8100
Fax +1.650.919.8006
info@mobileiron.com

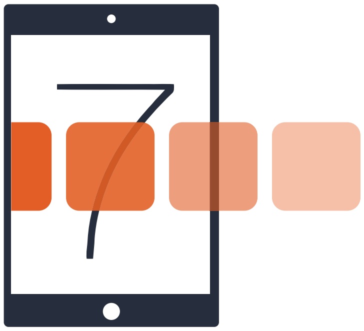
MOBILEIRON+ iOS 7

Introduction

Apple's iOS 7 brings over 200 new consumer and business features to iOS devices, including over 40 features that specifically enable or enhance key Enterprise Mobility Management (EMM) capabilities. These new EMM capabilities, such as per-app VPN, 'Open In' management, and a bulk app purchase program that includes license reclamation, respond to what enterprises need to fully embrace iOS devices as critical business tools. They also require a third-party EMM solution, like MobileIron, to function. These new EMM features, together with MobileIron's platform, empower enterprises to accelerate their adoption of mobile devices and apps, making mobile their primary computing platform and realizing all the benefits of being a Mobile First organization.

This document is intended to help you understand how these new EMM capabilities will impact your organization. We've organized them into two groups, Mobile Application Enhancements and Device Management Enhancements. We begin with Mobile Application Enhancements because we believe these capabilities will have the broadest impact.

1
iOS 7 Mobile Application Management Enhancements



The iOS 7 Big Picture Bottom Line for Enterprise:

The key iOS 7 Mobile Application Enhancements achieve four objectives:

- Enable easier enterprise-class mobile app development
- Enhance end user experience
- Provide more app security
- Allow easier IT app management

We believe that the first point, enabling easier enterprise-level mobile app development, will have the biggest impact on the enterprise, as it will foster an explosion of great mobile business apps, providing critical business processes at your employees' fingertips on devices that they love.

Previously, there were several barriers that limited enterprise app development. These barriers included authenticating a user with an enterprise identity provider, establishing a secure connection to the enterprise data source, auto-configuring apps, and preventing data loss. They created a high bar for entry for the majority of both third-party app developers and in-house developers. Now that these capabilities are available at the OS level, and may be managed and enforced by MobileIron, we expect to see a frenzy of new enterprise mobile apps in the next twelve to eighteen months.

FASTER APPLICATION DEVELOPMENT:

- App SSO, Per App VPN
- Managed Open-In, Application Configuration
- Default third-party data protection
- Managed Application Feedback.

These apps will not be designed by traditional desktop developers, but by mobile developers who cut their teeth making mobile consumer apps. They will bring design expertise focused on ease of use and a simple UI to enterprise workflows. When they do, business users will adopt quickly, as they've done for products like Dropbox, Evernote ®, and Box. Enterprise apps will be flooding in from two sides, the iTunes app store and in-house apps from the line of business. Mobile IT needs to be ready with an EMM platform purpose built to help businesses make the most of this faster, more agile way of working. One that covers the range of mobile devices from corporate owned to BYOD, with an advanced security and policy engine to manage and secure apps and content.

The table below outlines the key Mobile Application Enhancements that MobileIron is investing in to manage and enforce on iOS 7 devices, along with their primary benefits. Each will be explained in more detail below.

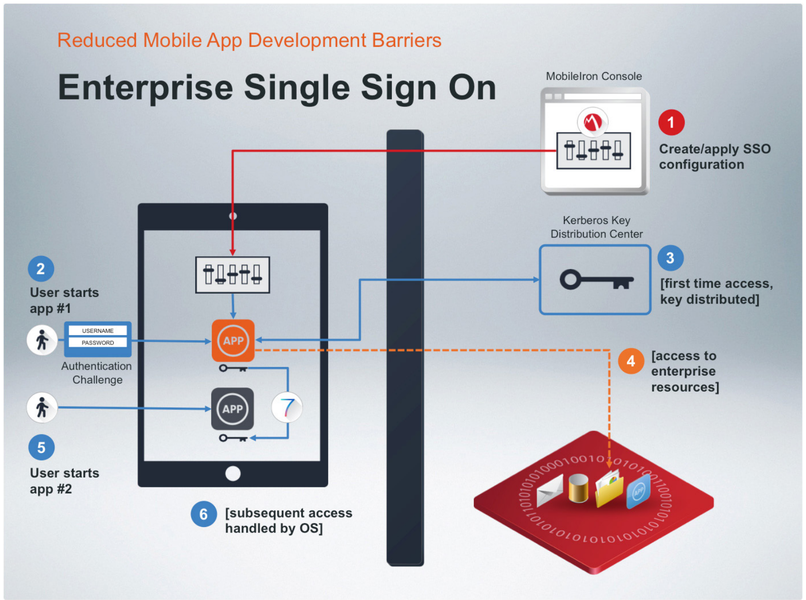
CAPABILITY	APP DEVELOPMENT	USER EXPERIENCE	SECURITY	MANAGEMENT
Enhancements to accelerate enterprise app development and use				
Enterprise single sign on (SSO)	x	x	x	x
Per app VPN and VPN-on-demand enhancements	x	x	x	x
Managed application configuration	x	x		x
Application Open in management	x	x	x	x
Default third-party application data protection	x		x	x
Managed application feedback	x	x		x
Enhancements to streamline IT administration				
Volume Purchase Program (VPP) app license reclamation				x
Silent app update and Install		x		x
App downloads from local caching server		x		x

Enhancements to Accelerate Enterprise Application Development and Use

The iOS 7 enhancements described below bring enterprise-level features to app development and use.

Enterprise Application Single Sign On (SSO)

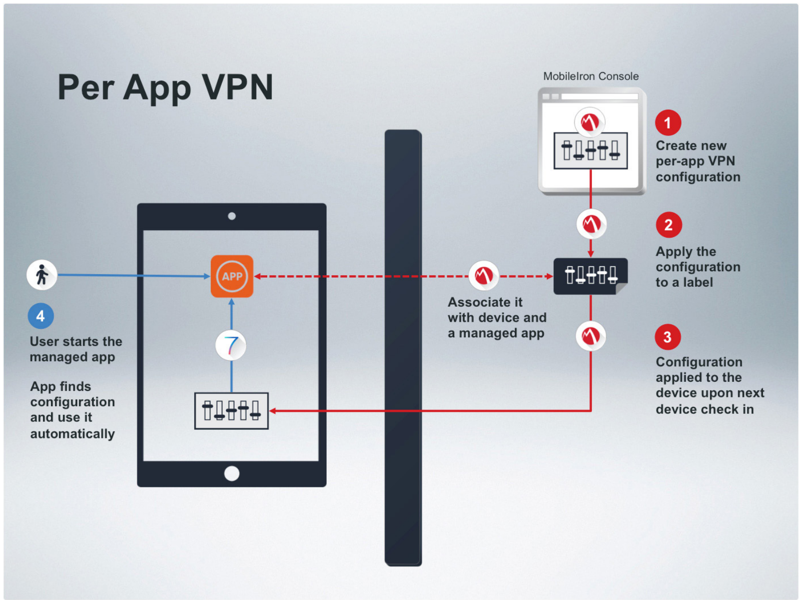
Applications can now share enterprise credentials across apps. That means users only have to authenticate once with their corporate credentials, then they can automatically be logged in to other business apps without entering the same password over and over. This both improves user experience and reduces potential help desk calls. The MobileIron administrator creates and distributes the SSO configurations through the EMM console. The configuration is then consumed and used by the device for ongoing authentication by applications.


Reduced Mobile App Development Barriers
Enterprise Single Sign On
MobileIron Console
1 Create/apply SSO configuration
Kerberos Key Distribution Center
3 [first time access, key distributed]
2 User starts app #1
USERNAME
PASSWORD
Authentication Challenge
APP
4 [access to enterprise resources]
APP
5 User starts app #2
6 [subsequent access handled by OS]

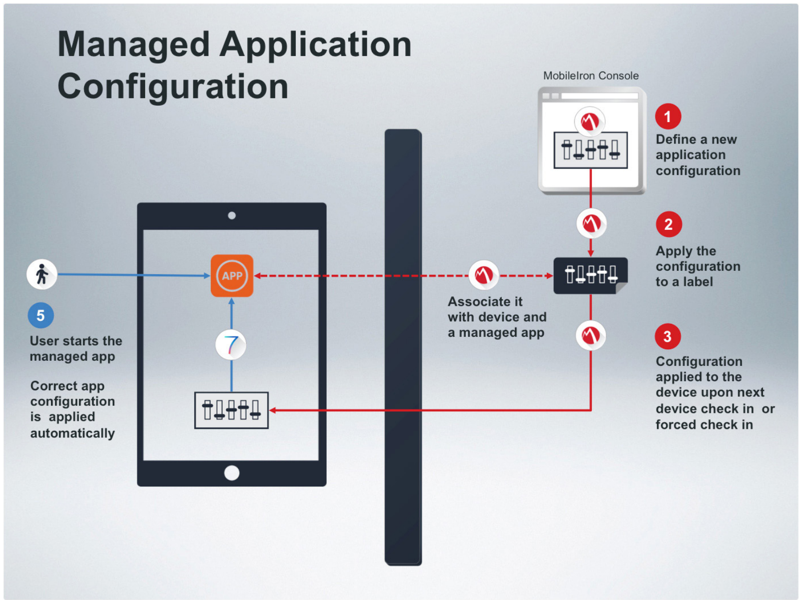
It is important to note that iOS 7's implementation of SSO will only work on a trusted network with a Key Distribution Center. Therefore it will most likely be realized in coordination with a device wide VPN so as to establish a connection to the trusted network. Because of this limitation, it is recommended that customers review MobileIron's AppConnect and AppTunnel solution for utilizing SSO outside of a trusted network.

Per App VPN and VPN on Demand Enhancements

For enterprise mobile app development to take off, apps need a fast and secure way to easily connect and transmit data from a backend corporate resource. Users want to get the information they need quickly, without complicated setup and multiple authentication prompts. IT prefers the greater security and control of allowing a single app, rather than the whole device, access to the network only when needed. To implement this capability, a MobileIron administrator creates a per app VPN configuration in our EMM console, then associates that configuration with specific apps. The MobileIron administrator can also create a list of URL's that, when opened in Safari, will trigger a VPN on demand connection.


Per App VPN
MobileIron Console
1 Create new per-app VPN configuration
2 Apply the configuration to a label
3 Configuration applied to the device upon next device check in
Associate it with device and a managed app
APP
4 User starts the managed app
App finds configuration and use it automatically

Managed Application Configuration

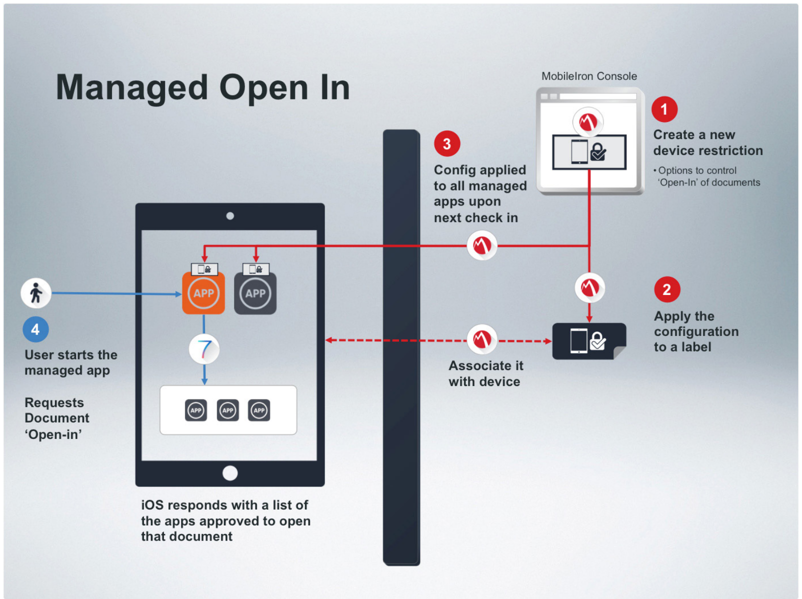

Managed Application Configuration
MobileIron Console
1
Define a new application configuration
2
Apply the configuration to a label
Associate it with device and a managed app
3
Configuration applied to the device upon next device check in or forced check in
APP
5
User starts the managed app
Correct app configuration is applied automatically

Deploying enterprise apps at scale often means configuring them to work with parameters specific to geographic regions, divisions, and/or security requirements. That means sending the correct first time startup parameters, to the right user, the right app, on the right device, with little to no user intervention for seamless initial app launch. A MobileIron administrator can now push configurations such as server name, username, and email address, to managed apps on iOS 7 devices to significantly improve user experience and decrease help desk calls.

The configuration cannot be encrypted, and so it should not contain any secrets (e.g. certificates). If you need to provide configuration information that should be encrypted, MobileIron's AppConnect solution can provide an encrypted configuration to the app.

Additionally, apps must be programmed to support configuration by iOS 7. We expect a significant increase in updates to existing apps incorporating this functionality over the next several months.

Application Open in Management


Managed Open In
MobileIron Console
1
Create a new device restriction
• Options to control 'Open-In' of documents
3
Config applied to all managed apps upon next check in
2
Apply the configuration to a label
Associate it with device
APP
APP
4
User starts the managed app
Requests Document 'Open-in'
iOS responds with a list of the apps approved to open that document

The benefit of thousands of mobile apps often lies in their specialization in specific tasks. Instagram took an average photo from amateur to awesome, then allowed us to pass it to Twitter for widespread acclaim. That's great for public information, but internal corporate information needs to stay private. That means preventing managed (business) apps from sharing data with unmanaged (personal) apps. This is often referred to as Data Loss Prevention, or DLP.

The MobileIron administrator can now control this feature through the EMM console with the following options:

- **DISALLOW OPEN IN FROM MANAGED TO UNMANAGED -** This prevents business documents from being shared from managed (business) apps to potentially insecure unmanaged (personal) apps
- **DISALLOW OPEN IN FROM UNMANAGED TO MANAGED -** This prevents personal documents in unmanaged apps from being opened in managed apps.

A MobileIron administrator can set either or both of these settings depending on the security needs of the enterprise. The Open in management capabilities extend beyond applications to accounts as well. For example, a managed email account will inherit the Open In restrictions specified in the EMM console.

Third Party App Data Protection On by Default

Previously, the only way third party app developers could use the encryption capabilities in iOS was by explicitly enabling them. Depending on developer practices, some might encrypt data while others might not, leading to inconsistent protection of business data. With iOS 7, third- party apps use the iOS 7 encryption capabilities by default, through an encryption key derived from the device passcode. For enterprises, this means that as long as there is a policy in MobileIron's EMM console that requires a device passcode, information in third-party apps will be protected by default.

It is important to note that this iOS 7 enhancement alone will not secure the data in a BYOD environment where a passcode policy is not enforced. For these environments, MobileIron AppConnect is recommended to secure enterprise app data with an app passcode and standalone encryption.

Managed Application Feedback

Developers need app usage and reporting information to make exceptional apps, and business owners need it to measure an apps' ROI. iOS 7 now provides a metaphorical pipe from an application to MobileIron's EMM console. Information like usage statistics, error messages, and other data can be sent through that pipe to the EMM console, where it can be displayed and reported on. Data written to this pipe is not encrypted, so sensitive information should not be included.

Enhancements to Streamline IT Administration

With the expected increase in enterprise app development and use, efficient app management will become more critical. iOS 7 brings the following enhancements to help streamline app administration.

Volume Purchasing Program (VPP) App License Reclamation

Prior to iOS 7, when a company distributed a licensed app to an employee, the license became associated with the employee's Apple ID, and could not be reclaimed or reused by the company that paid for it. This has been a big barrier preventing many enterprises from fully adopting commercial business apps for their employees. With iOS 7, the enterprise owns the app license. MobileIron administrators can not only distribute, but also reclaim and reassign those licenses over the air. That means when an employee leaves the company, they don't take the app with them as they did with the prior VPP structure. The administrator can instead reclaim that app license and issue it to a new employee, saving the company money.

The enhanced VPP also enables licenses to be distributed worldwide. This overcomes a prior limitation where VPP participation was limited to ten countries. Now, as long as an application is available in the App Store for that user's country, they may receive and redeem a VPP license.

Silent App Updates & Installation

It is not uncommon for the number of installed apps on a mobile device to reach into the high double digits. The ethos of app development is to iterate often, delivering incremental improvements, which often address security issues, on schedules that work for the app developer. The high volume of apps, which we expect to increase even more, compounded with multiple devices and frequent app updates makes staying up to date with the latest versions a tremendous challenge for IT. iOS 7 eliminates this challenge by enabling apps to automatically update without user intervention. The enterprise can avoid the headaches caused by app version fragmentation, including administration overhead, increased help desk calls, longer call resolution times, frustrated users, and security holes.

> With iOS 7 and MobileIron, enterprises can manage app licenses like they manage software licenses: distributing, reclaiming, and re-distributing them to employees as needed.

MobileIron administrators also now have the ability to silently install apps on corporate-owned devices supervised through Apple Configurator. Administrators select the apps in the EMM console and then MobileIron sends instructions to the device for the applications to be installed. Users will not be prompted to install the app, the app just appears on their device ready for use.

App Downloads from Local Caching Server

Now instead of downloading every new app and update directly from Apple, enterprises can set up a local caching server and iOS 7 clients can download them from there. This saves bandwidth and accelerates the download and delivery of content from the App Store, Mac App Store, iTunes Store, and iBookstore.

2
iOS 7 Device Management Enhancements

User Simplicity and Ease of Use

Apple has always focused on the user to make a fantastic experience that is simple and intuitive. And while ease-of-use is important to the enterprise, security is often a more critical concern. Previously, many desired security and management controls were either cumbersome as they had to be implemented manually on the device, or they were not possible at all. Now, with iOS 7, more of these configurations will be provisioned directly from the MobileIron EMM console, and managed by IT. Users will find their devices just work, without complicated setup or calls to the help desk. Not only do the devices work, but it will feel like magic as users roam to hot spots and conference rooms projecting their presentations and videos on screens throughout their organization. And with the additional management controls available, IT can confidently support iOS devices as essential business tools.

The key device level enhancements in iOS 7 achieve the following objectives:

- Enhance end user experience
- Allow easier IT management
- Improve security
- Protect employee privacy

The table below outlines the key Device Management Enhancements that MobileIron can manage and enforce on iOS 7 devices, along with their primary benefits. Each will be explained in more detail below.

CAPABILITY	MANAGEMENT	USER EXPERIENCE	SECURITY	PRIVACY
Simplifying the Enterprise User Experience				
Touch ID	x	x	x	
AirPrint and AirPlay configuration	x	x		
Wi-Fi configuration enhancements		x		
Font distribution	x	x		
Improving IT Management Controls				
Web content filtering		x	x	
Apple TV Management		x	x	
Device restrictions enhancements		x	x	
Single App Mode Enhancements		x	x	
Filtered app inventory	x	x		x

Simplifying the Enterprise User Experience

These enhancements are focused on improving the enterprise user experience - whether that user is in the business unit or an IT administrator - and helping ensure that devices just work.

Touch ID

Unlocking your device is now as simple as touching your finger to the home button. Touch ID is a marquis feature introduced on the new iPhone 5S. It incorporates a high-resolution sensor in the home button as well as a conductive ring that senses a finger. The information captured by the sensor is used to authenticate the user and unlock the phone. The fingerprint data is encrypted directly in the device’s A7 processor and is accessible only by the Touch ID sensor. The device does not store an actual photo of the fingerprint, it only stores the data. The data is not accessible by other software and does not leave the device, nor is it backed up to iTunes or the cloud.

Users that want to use Touch ID will also have to create a device passcode as a backup. Only that passcode, not a finger, can unlock the phone if the phone is rebooted or hasn't been unlocked in 48 hours.

Together with MobileIron's platform, enterprise administrators will have the ability to disable Touch ID for managed devices. Supervision of the device is not required to disable the feature. Touch ID is a compelling end user features that combines ease of use with better device security. We recommend that administrators continue to allow Touch ID.

AirPrint and AirPlay Configurations

The ecosystem of corporate assets that include AirPlay and AirPrint destinations are now more valuable and

simpler to use. Everyday workflows that include printing and delivering presentations work wirelessly without hunting for cables and compatible connectors.

- **AIRPLAY DESTINATIONS** - A MobileIron administrator can send a list of AirPlay destinations and passcodes to an iOS 7 supported device, enabling employees to easily connect to appropriate display resources, without needing to know or enter the passcode. Whitelisting of AirPlay destinations can be enforced for devices that are supervised by the Apple Configurator.
- **AIRPRINT DESTINATIONS** - A MobileIron administrator can send a list of AirPrint destinations to an iOS 7 supported device, enabling employees to easily print to appropriate printers.

> It's important to note that Safari is an unmanaged app. Therefore, business documents downloaded via Safari cannot be restricted to only managed (business) apps. For organizations that have more stringent security requirements, MobileIron Web@Work can be used to containerize web content and documents downloaded from the organization's web sites.

Wi-Fi Configuration Enhancements

MobileIron administrators now will have the ability to set priorities for WiFi profiles, enabling them to deploy additional network configurations to devices, and automatically migrate users to the new configurations. Administrators will also have the ability to prevent users from making changes to their Wi-Fi configuration from the lock screen by disabling the feature on the lock screen. Employees will find it easier than ever to connect to the most appropriate Wi-Fi network.

Font Distribution

A great user experience, all the way down to beautiful typography, is embedded deep in Apple's history. It originates from a calligraphy class Steve Jobs took in college that left a lasting impression. Corporations often have custom fonts that communicate their brand and persona. These custom fonts appear in a variety of materials from documents to a presentations. If iOS doesn't have those custom fonts, it will attempt to do a conversion, which may change the look of the document. The MobileIron administrator will be able to distribute the appropriate fonts in a configuration profile through the EMM console, preserving the end user experience.

Improving IT Management Controls

The remaining Device Management Enhancements focus on increasing IT control over devices and associated data to protect both enterprise data and employee privacy.

Web Content Filtering

iOS 7 will include a powerful new capability to filter access to urls across the entire device. Together with MobilelIron, administrators can now apply website whitelist/blacklist policies to Safari as well as other web browsers, including MobileIron's Web@Work.

This allows security administrators to enforce select corporate web browsing guidelines , without having to run all internet traffic from a mobile device through a proxy.

MobileIron's EMM console will use the Web Content Filter configuration to define allowed and disallowed urls. Filters can be set to allow access only to specified websites, to limit access to adult content, and to prevent access to specific websites. Mobileiron will support distributing multiple web content filter profiles on a single device. iOS 7 will parse the rules and apply them at the device level. This capability is available only for corporate-owned supervised devices, and is particularly useful for fleet deployments.

Apple TV Management

Apple TVs also run iOS and can now be deployed as a managed device, similar to an iPhone or iPad, although with limited options. Together with MobileIron's platform, administrators will be able to set the language, locale, and WiFi network profiles on managed Apple TV's.

Device Restriction Enhancements

With MobileIron's EMM console and iOS 7, administrators will be able to enforce more restrictions on corporate-owned or BYOD devices. Some of the new restrictions require the device to be supervised by the Apple Configurator, which is only appropriate for corporate-owned devices.

For unsupervised devices, which may be corporate-owned or BYOD devices, administrators will be able to:

- **DISABLE TOUCH ID UNLOCK** - Prevent the user from enabling the Touch ID unlock feature on the device.
- **DISABLE PERSONAL HOTSPOT** - Prevent the user from enabling the device as a personal hotspot.

For supervised devices, which are always corporate-owned, administrators will be able to:

- **DISABLE AIRDROP** - Prevent the user from sharing content via Airdrop when the share button is accessed.
- **DISABLE MAIL ACCOUNT CHANGES** - Prevent the user from adding, changing, or deleting mail accounts.
- **WHITELIST AIRPLAY DESTINATIONS** - Allow AirPlay display only to destinations specified by the EMM administrator.

Single App Mode Enhancements

With MobileIron and iOS 7 administrators have more options to lock down the behavior of the device when in Single App Mode. The following features can be disabled by a MobileIron administrator through the EMM console:

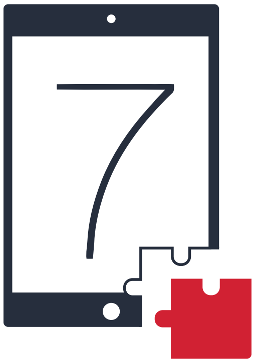
- Touch Screen
- Rotation Sensing
- Volume Buttons
- Ringer Button
- Sleep / Wake Button
- Auto Lock

Additionally, the MobileIron administrator can specify a list of apps that can autonomously enter single app mode when needed. For example, an exam app could prevent students from exiting to the home screen while a test is in progress. Once the test is over, the app could release single app mode and allow the student to exit to the home screen. This eliminates the need for a MobileIron administrator to manually initiate single app mode at the right moment.

Filtered App Inventory

Whitelist or blacklist rules cannot be enforced without an inventory of the apps installed on a device. But the apps a user chooses to install can be revealing to their personal life. Many enterprises want to limit their exposure to this kind of personal information, and many are required to do so to comply with local privacy laws. MobileIron, together with iOS 7, will provide the ability for a MobileIron administrator to view only managed (business) apps on a user's device and not every app on the device, to both protect employee privacy and limit potential liability.

CONCLUSION:
MobileIron + iOS 7 =
The Next Level of Mobile Productivity



All of the new iOS 7 features described in this paper require an EMM platform. Alone, the new EMM iOS 7 features are inaccessible to the enterprise. They are just a set of dormant API's in the OS. It is only together with an EMM platform like MobileIron that these features come alive. MobileIron has the most experience managing iOS devices and apps, including the largest iOS deployment in the industry. We are ready to help enterprises enable new employees in minutes with corporate-owned devices fully configured with apps and network access, protect Office 365 email attachments on corporate-owned or BYOD devices, help global enterprises ensure compliance with privacy laws, and many other use cases enabled through the combination of iOS and MobileIron. With 5+ years of enabling enterprises to take advantage of EMM innovations, both at the device/ OS level and through EMM software, MobileIron is committed to helping our customers make the most of iOS 7 and accelerate the next level of mobile productivity - through apps that streamline and speed existing business processes.

MobileIron will support iOS 7 devices at launch. Some new features, such as Per-App VPN, will be immediately supported by MobileIron, but rely on VPN vendors to release additional software to enable full implementation. If you are a current customer, more detail on upcoming releases is available in our Support Portal. Otherwise, please contact your MobileIron Sales Representative for more information.

Appendix

iOS 7 Hardware Support

The following devices can be updated to iOS 7:

- iPhone 4 & 4S
- iPhone 5, 5C, & 5S
- iPod Touch 5th Generation (16 GB, 32 GB, 64 GB)
- iPad 2
- iPad with Retina Display
- iPad Mini

MobileIron is Ready for iOS 7

Our generally available products below are compatible with newly registered iOS 7 Devices, as well as existing devices under management that are updated to iOS 7.

- VSP v5.7.1 or later
- Mobile@Work v5.7.4 or later
- Web@Work v1.1.2 or later
- AppConnect SDK v1.6 or later
- AppConnect-enabled Apps Wrapped with v1.6 or later

Recommendations:

- All MobileIron customers should upgrade to these versions or later ones
- All MobileIron customers should rewrap all AppConnect-enabled apps with v1.6 or later

For additional information on requirements for iOS 7 support, please visit our Customer Support Knowledge Base.

MobileIron®

415 East Middlefield Road
Mountain View, CA 94043 USA
Tel. +1.650.919.8100
Fax +1.650.919.8006
info@mobileiron.com

www.mobileiron.com