iOS 10.3 + EMM

Expand Enterprise Control and Security

Table of Contents

MobileIron

415 East Middlefield Road
Mountain View, CA 94043
info@mobileiron.com
www.mobileiron.com
Tel: +1.877.819.3451
Fax :+1.650.919.8006

iOS 10.3 Delivers Key Features for the Modern Mobile Enterprise

With the recent release of iOS 10.3, Apple continues to follow an established pattern of delivering enterprise-focused features in a major point release. In the spring update, Apple has delivered some high-impact enterprise features, such as new email enhancements that make the native email app both easier to use and more secure, and the ability to restrict Wi-Fi networks to help improve security. Some of the new features, such as the ability to remotely shut down and restart devices, are particularly well-suited to corporate-owned, single-use (COSU) environments like retail kiosks. In addition, Apple has expanded its investment in tvOS by adding supported EMM configuration and control capabilities for the fourth-generation Apple TV. Education also remains in the spotlight as Apple continues to evolve the Shared iPad in Education program with expanded use cases for the Classroom app.

Enterprises should note that many of the new features are available only for "supervised" or institutionally owned devices. Organizations that want to leverage these new features will need to supervise iOS devices through the Device Enrollment Program (DEP) and an enterprise mobility management (EMM) platform like MobileIron.

New File System Improves Performance

In 10.3 Apple has replaced the current file system found on all iOS devices. The previous file system, HFS+, has existed on Macs since 1988 and has been the file system on both iOS and tvOS since their inception. The new Apple File System (APFS) will deploy first on iOS and is optimized for today's solid-state drives (SSDs). Users should experience improved performance since APFS is designed to reduce latency. In addition to dramatically increasing the number of files that can be stored, APFS includes support for 64-bit file names as well as new flexible encryption schemas with multiple keys to enable very granular encryption capabilities. Application developers who make heavy use of file system-level operations should thoroughly test their code against iOS 10.3 to avoid any unintended conflicts with APFS.

Wi-Fi Controls Protect Devices from Untrusted Networks

A new Wi-Fi restriction for supervised devices allows an administrator to create a whitelist of Wi-Fi networks. Networks or service set identifiers (SSIDs) that do not appear in the whitelist will not be visible from the device's Wi-Fi settings menu.

The new Wi-Fi restriction can be especially useful for securing COSU devices, such as an iPad in a retail kiosk that only connects to a pre-authorized store network. A Wi-Fi whitelist could also be used to prevent employees from joining untrusted Wi-Fi networks in airports or coffee shops, where hackers are increasingly spoofing existing networks to siphon data.

OAuth 2.0 Tightens Email Security

In 10.3, the native email client has been optimized to support OAuth 2.0 to Microsoft Office 365 when used with Exchange ActiveSync 16.1. OAuth 2.0 uses a secure token instead of relying on a username and password for secure access. If OAuth isn't deployed, the mail client will default to the previous domain auto-discovery behavior, in which a device will attempt to find the correct email server based on the domain configured in an email address. Apple is also improving S/MIME with enhancements to signing and encryption. Although S/MIME has been available for years when deploying ActiveSync configurations to native iOS email, the new enhancement will allow users greater flexibility in determining which certificates will be used for signing and encryption.

Expanded EMM Capabilities Simplify Device Management

Apple continues to demonstrate a strong commitment to securing iOS devices through DEP and EMM. New DEP enhancements allow administrators to skip the iCloud and Home setup screens on new devices. New management capabilities, most of which are available only on supervised, company-owned devices, include:

- **Admins can now remotely shut down and restart supervised iOS devices.** This feature would be particularly valuable to a school system finishing up classes at the end of the year. (Supervised devices only.)
- **Devices that are locked with a passcode can now be updated to the latest iOS version.** In the past, users had to enter a passcode to complete the update if the device was locked. Now the update can be completed even if users don't unlock the device. This feature may be useful when devices are updated overnight and no admin is available to unlock the device to complete the OS update. (Supervised devices only.)
- **A lost mode sound can be played on-demand for an iOS device.** This helps locate a device that does not have an Apple ID associated with it, such as a misplaced kiosk device in a retail store or an iPad that a student has lost in school. (Supervised devices only.)
- **Admins can now implement a new restriction on dictation.** This feature provides added security for organizations that want to prevent sensitive, dictated content, such as confidential healthcare or legal notes, from being lost or replicated to iCloud or other cloud services. (Supervised devices only.)

- **Check the posture of an iOS device if it is tethered to a network.** IT can now determine if an iOS device is physically connected to a network that may or may not be trusted by the organization.
- **Mobile admins can now specify whether a device should use the IPv4 or IPv6 protocol (or both) for voice, data, and roaming connections.** This will help organizations that have standardized on IPv6 extend the scope of their compliance to mobile environments.

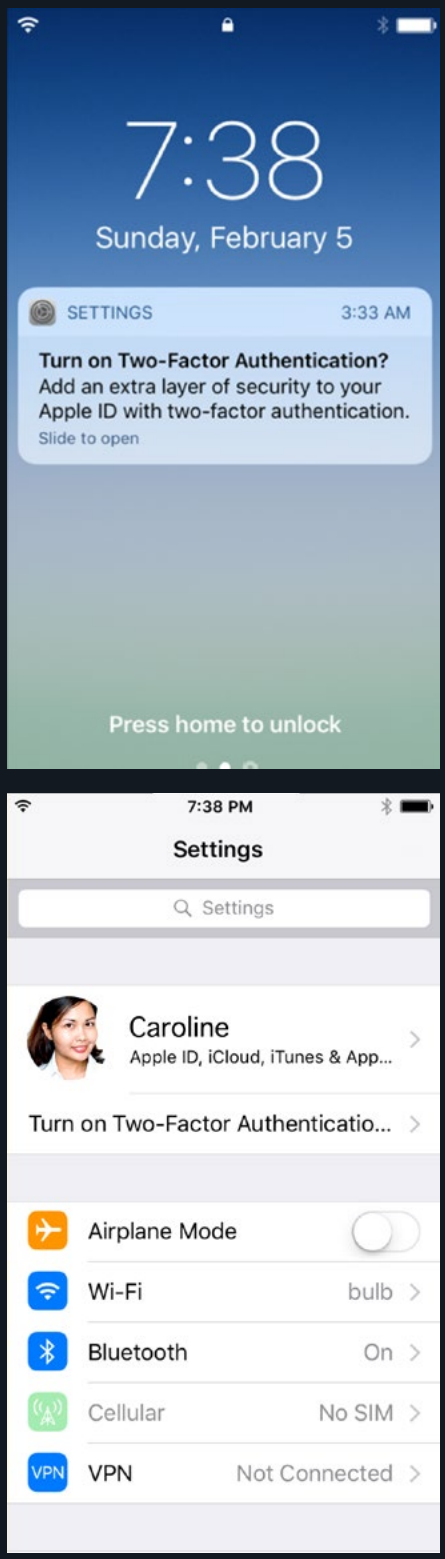
Two-factor Authentication Boosts Device Security

Apple has supported the use of two-factor authentication (2FA) for some time, and 10.3 takes it a step further. An iOS 10.3 device will now prompt users to set up 2FA when an Apple ID is configured only for password authentication. The Settings app may also be "badged" with a notification prompting the user to initiate the 2FA configuration. Lastly, in iOS 10.3 the Apple ID is displayed more prominently at the top of the Settings menu so users can quickly find and make changes to the Apple ID (like 2FA) without having to search for it.

Mac Tethered Caching Accelerates App and iOS Updates

Mac devices can now be configured as temporary caching servers for updating iOS and deploying apps to devices. For instance, a device can be plugged into any recently updated macOS Sierra device, and if an app or iOS update had already been deployed through that Mac, the attached iOS device can download the update without needing to download the file over the Internet.

This feature is particularly useful for companies staging a large number of devices. For instance, a hospital that needs to stage 100 new iPads and



Apple is encouraging the use of 2FA to protect Apple IDs.

deploy a 2GB app along with the latest version of iOS will only need to download these large files once for the first device. Subsequent devices, when attached to the Mac through USB or a USB hub, will download the app and OS over the wire, significantly reducing the amount of time it takes the hospital to stage the devices. The tethering capability augments the currently available caching server for macOS server, an over-the-air (OTA) solution that works on the local company network.

tvOS is Ready for the Enterprise

Apple is ramping up tvOS management for fourth-generation Apple TV devices. In the tvOS 10.2 release, Apple is extending many of the capabilities that were previously available only on traditional iOS devices to Apple TV devices. These features include the ability to configure and deploy certificates, configure secure corporate networks, and remotely erase an Apple TV. More importantly, an Apple TV can now be enrolled in DEP and supervised OTA when purchased from an approved DEP reseller. This is a significant expansion of Apple's vision of the role of tvOS in education and the enterprise.

EMM + iOS 10.3 Expand the Digital Classroom

The Shared iPad in Education program is made up of Apple School Manager (ASM), the Classroom app for teachers and students, and the ability to create Managed IDs on behalf of students.

iOS 10.3 includes an updated Classroom 2.0 app, which expands and improves previous managed class capabilities and also supports unmanaged classes. When the Classroom 2.0 app is deployed in managed classes, teachers can now mute student devices and students can share content such as documents and URLs with a teacher. When the unmanaged Classroom 2.0 app is deployed, users aren't required to be enrolled in ASM or have an EMM configuration profile installed on their devices. Instead, teachers can invite students to join unmanaged classes by entering a four-digit passcode. Students can join as long as they are not enrolled in any managed classes.

The Modern Enterprise Runs on iOS and MobileIron

Apple's continued commitment to enabling the modern mobile enterprise and classroom is clearly evident in the release of iOS 10.3. Although many of the new features can only be leveraged on supervised, institutionally owned devices, iOS 10.3 shows how Apple is continuing to prioritize IT control and security without sacrificing the highly productive native experience iOS users have come to expect.

Together with MobileIron's unified mobile and cloud security platform, organizations have an even more robust way to securely deploy apps, scale device deployment and management, and protect cloud-based apps and data on any network. To learn how MobileIron EMM can support your iOS deployment, please visit our website.