iOS 10.3 + EMM

Mehr Kontrolle und Sicherheit im Unternehmen

Inhalt

MobileIron

415 East Middlefield Road
Mountain View, CA 94043, USA
info@mobileiron.com
www.mobileiron.com
Tel.: +1 877 819 3451
Fax: +1.650.919.8006

iOS 10.3 bringt wichtige Funktionen für moderne mobile Unternehmen

Mit der aktuellen Freigabe von iOS 10.3 setzt Apple seine bewährte Politik fort. Unternehmensfunktionen in einem Haupt-Release bereitzustellen. In dem Frühlings-Update lieferte Apple einige wichtige Unternehmensfunktionen, beispielsweise neue E-Mail-Erweiterungen, die die native E-Mail-App benutzerfreundlicher und sicherer machen, und Sicherheitsfunktionen zur Beschränkung der Rechte in WLANs. Einige der neuen Funktionen, beispielsweise die Möglichkeit, Geräte aus der Ferne herunterzufahren und neu zu starten, sind insbesondere für Umgebungen geeignet, in denen beispielsweise unternehmenseigene Einzweck-Geräte im Kiosk-Modus genutzt werden. Darüber hinaus erweitert Apple seine Investitionen in tvOS durch eine unterstützte EMM-Konfiguration mit Kontrollfunktionen für die vierte Generation von Apple TV. Apple Education bleibt ebenfalls im Rampenlicht, da Apple das Programm „Shared iPad in Education" mit der erweiterten Nutzung für die Classroom-App weiterentwickelt.

Unternehmen seien darauf hingewiesen, dass viele der neuen Funktionen nur für unternehmenseigene bzw. „überwachte" Geräte verfügbar sind. Unternehmen, die diese neuen Funktionen umfassend nutzen wollen, müssen iOS-Geräte mit dem Geräte-Registrierungs-programm DEP und einer Enterprise Mobility Management-Plattform (EMM) wie MobileIron überwachen.

Höhere Leistung durch neues Dateisystem

In Release 10.3 ersetzte Apple das aktuelle Dateisystem, das bisher auf allen iOS-Geräten verwendet wurde. Das bisherige Dateisystem HFS+ gibt es auf Macintosh-Computern seit 1988. Es war von Anfang an das Dateisystem für iOS und tvOS. Das neue Apple-File-System (APFS) wird zunächst in iOS eingeführt und ist für moderne SSD-Laufwerke optimiert. Für die Benutzer bedeutet das eine Verbesserung der Eigenschaften, da APFS die Latenz reduziert. Neben der deutlichen Erhöhung der Anzahl der Dateien, die gespeichert werden können, unterstützt APFS 64-Bit-Dateinamen sowie neue, flexible Verschlüsselrungsschemata mit mehreren Schlüsseln, die sehr detaillierte Verschlüsselungsfunktionen ermöglichen. Anwendungsentwickler, die Anwendungen mit häufigem Zugriff auf das Dateisystem entwickeln, sollten ihren Programmcode mit iOS 10.3 intensiv testen, um unerwünschte Konflikte mit APFS auszuschließen.

WLAN-Kontrollen schützen Geräte vor nicht vertrauenswürdigen Netzwerken

Mit einer neuen WLAN-Beschränkung für überwachte Geräte kann ein Administrator eine Whitelist für WLANs erstellen. Netzwerke bzw. Dienst-IDs (SSIDs), die nicht in der Whitelist eingetragen sind, werden im WLAN-Einstellungsmenü des Geräts nicht angezeigt.

Die neue WLAN-Beschränkungsfunktion kann besonders zur Absicherung so genannter COSU-Geräte nützlich sein, beispielsweise für ein iPad in einem Kiosk-System, das nur eine Verbindung zu einem vorher autorisierten Netzwerk aufbaut. Mit einer WLAN-Whitelist ließe sich auch verhindern, dass Mitarbeiter nicht vertrauens-würdige WLANs auf Flughäfen oder in Cafés nutzen, den Orten, an denen Hacker zunehmend durch Spoofing vorhandener Netzwerke versuchen, Daten abzusaugen.

Höhere E-Mail-Sicherheit durch OAuth 2.0

In Release 10.3 wurde der native E-Mail-Client für die Unterstützung von OAuth 2.0 für Microsoft Office 365 optimiert, wenn gleichzeitig Exchange ActiveSync 16.1 verwendet wird. OAuth 2.0 nutzt statt des Benutzernamens und Passworts ein sicheres Token für den sicheren Zugriff. Wenn OAuth nicht installiert ist, nutzt der E-Mail-Client standardmäßig die bisherige automatische Erkennung der Domain, d. h. ein Gerät versucht, den korrekten E-Mail-Server anhand der in einer E-Mail-Adresse enthaltenen Domain zu finden. Apple verbessert außerdem S/MIME mit Erweiterungen für Signaturen und Verschlüsselung. S/MIME ist seit Jahren durch ActiveSync-Konfigurationen für die native iOS E-Mail-App verfügbar, mit der neuen Erweiterung können die Benutzer jedoch flexibler entscheiden, welche Zertifikate für Signierung und Verschlüsselung verwendet werden sollen.

Erweiterte EMM-Funktionen vereinfachen die Geräteverwaltung

Apple unterstreicht erneut sein starkes Engagement zur Absicherung der iOS-Geräte mit DEP und EMM. Mit den neuen DEP-Erweiterungen können Administratoren die Konfigurationsbildschirme für die iCloud und den Startbildschirm auf neuen Geräten überspringen. Es sind neue Verwaltungsfunktionen (meist nur für überwachte unternehmenseigene Geräte) verfügbar:

- **Administratoren können jetzt überwachte iOS-Geräte aus der Ferne herunterfahren und neu starten.** Nützlich wäre diese Funktion insbesondere in einem Schulsystem, bei dem die Klassen zum Jahresende enden. (Nur überwachte Geräte.)
- **Geräte, die mit einem Passcode gesperrt sind, können nicht auf die neue iOS-Version aktualisiert werden.** In der Vergangenheit mussten die Benutzer einen Passcode eingeben, um das Update abzuschließen, wenn das Gerät gesperrt war. Jetzt kann das Update selbst dann abgeschlossen werden, wenn Benutzer das Gerät nicht entsperren. Diese Funktion ist insbesondere zweckmäßig bei Geräten, die über Nacht aktualisiert werden und bei denen kein Administrator das Gerät nach dem Betriebssystem-Update entsperren kann. (Nur überwachte Geräte.)
- **Auf Anforderung kann auf jedem iOS-Gerät ein Klang abgespielt werden, wenn das Gerät als verloren gemeldet ist.** Dies hilft dabei, ein Gerät zu finden, dem keine Apple-ID zugeordnet ist, beispielsweise ein verlegtes Kiosk-Gerät in einem Einzelhandelsgeschäft oder einen iPad, den ein Schüler in der Schule vergessen hat. (Nur überwachte Geräte.)
- **Administratoren können jetzt für Diktate eine neue Einschränkung implementieren.** Diese Funktion erhöht die Sicherheit für Unternehmen, die verhindern wollen, dass sensibler diktierter Content, beispielsweise vertrauliche Notizen im Gesundheitswesen oder Rechtswesen, verloren gehen oder in der iCloud oder anderen Cloud-Diensten repliziert werden. (Nur überwachte Geräte.)

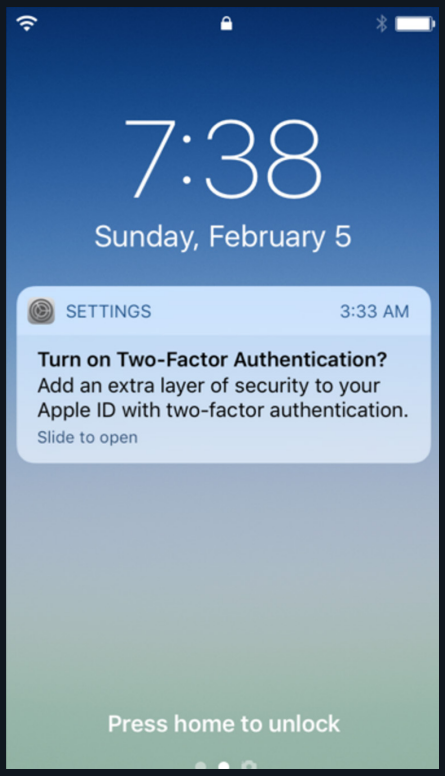
- **Risikostatusprüfung eines iOS-Geräts, wenn es mit einem Netzwerk verbunden ist.** Die IT kann jetzt ermitteln, ob ein iOS-Gerät physisch mit einem Netzwerk verbunden ist, das von dem Unternehmen als vertrauenswürdig oder nicht vertrauenswürdig eingestuft wurde.
- **Mobile Administratoren können jetzt festlegen, ob ein Gerät das Protokoll IPv4 oder IPv6 oder beide für Voice-Daten und Roaming-Verbindungen verwenden darf.** Unternehmen können damit leichter auf IPv6 standardisieren und ihre Compliance für mobile Umgebungen verbessern.

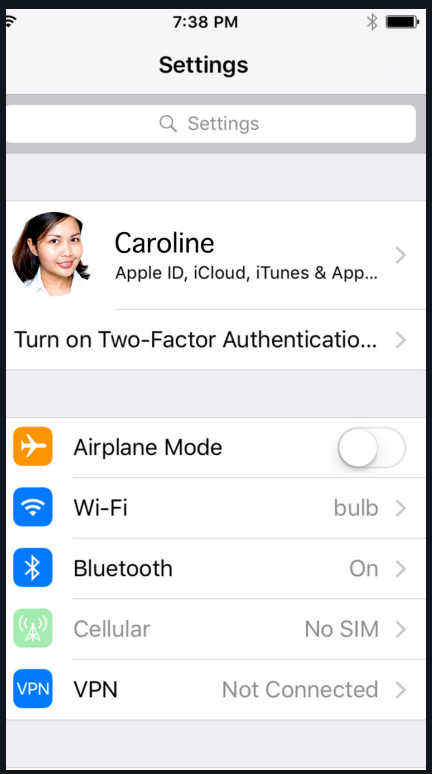
Höhere Gerätesicherheit durch zweistufige Authentifizierung

Apple unterstützt seit einiger Zeit die zweistufige Authentifizierung (2FA) und geht mit Release 10.3 noch einen Schritt weiter. In iOS 10.3 fordert das Gerät die Benutzer auf, 2FA zu konfigurieren, wenn eine Apple-ID nur für die Passwort-Authentifizierung konfiguriert ist. Die Einstellungs-App Kann auch ein „Badge" mit einer Benachrichtigung erhalten, die den Benutzer auffordert, 2FA zu konfigurieren. Nicht zuletzt wird in iOS 10.3 die Apple-ID an besser sichtbarer Stelle am oberen Rand des Einstellungsmenüs angezeigt, sodass die Benutzer sie schneller finden und Änderungen an der Apple-ID (beispielsweise mit 2FA) vornehmen können, ohne erst die Apple-ID zu suchen.

Mac Tethered Caching beschleunigt Updates von App und iOS

Mac-Geräte können jetzt als temporäre Caching-Server zur Aktualisierung von iOS und zur Bereitstellung von Apps auf Geräten konfiguriert werden. Beispielsweise kann ein Gerät mit einem kürzlich aktualisierten Gerät mit Mac OS Sierra verbunden werden. Wenn eine App oder das iOS-Update bereits auf diesem Mac bereitgestellt wurden, kann das angeschlossene iOS-Gerät das Update herunterladen, ohne dass die Datei erneut aus dem Internet geladen werden muss.





Apple empfiehlt die Nutzung von 2FA zum Schutz der Apple-IDs.

Diese Funktion ist besonders nützlich für Unternehmen, die eine Vielzahl von Geräten verwalten. Beispielsweise könnte es in einer Klinik notwendig sein, 100 neue iPads bereitzustellen und dafür eine 2 GB-App mit der aktuellen iOS-Version zu installieren. Jetzt müssen diese großen Dateien nur einmal für das erste Gerät heruntergeladen werden. Weitere Geräte werden mit dem Mac-Computer über USB oder einen USB-Hub verbunden und laden die App und das Betriebssystem per Kabel herunter. Damit verkürzt sich für die Klinik die Zeit zur Bereitstellung der Geräte deutlich. Die Tethering-Funktion erweitert den derzeit verfügbaren Caching-Server für Mac OS-Server, eine Over-the-Air-Lösung (OTA) im lokalen Netzwerk des Unternehmens.

tvOS ist für Unternehmen vorbereitet

Apple verbessert die tvOS-Verwaltung für die vierte Generation der Apple TV-Geräte. In der Version tvOS 10.2 erweitert Apple viele Funktionen, die bisher nur auf konventionellen iOS-Geräten verfügbaren waren, und bietet diese auch für Apple TV an. Solche Funktionen sind beispielsweise die Möglichkeit, Zertifikate zu konfigurieren und bereitzustellen, sichere Unternehmensnetzwerke zu konfigurieren und ein Apple-TV aus der Ferne zu löschen. Vor allem aber kann Apple TV jetzt in DEP registriert und durch überwachtes OTA bereitgestellt werden, wenn der Kauf über einen genehmigten DEP-Händler erfolgte. Dies ist eine deutliche Erweiterung der Vorstellungen von Apple über die Rolle von tvOS im Bildungswesen und im Unternehmen.

EMM + iOS 10.3 erweitern das digitale Klassenzimmer

Das Programm „Shared iPad in Education" besteht aus dem Apple School Manager (ASM), der Classroom-App für Lehrer und Schüler und der Möglichkeit, verwaltete IDs für die Schüler zu erstellen.

Version iOS 10.3 enthält eine aktualisierte Classroom-2.0-App, die die bisherigen Verwaltungsfunktionen für die Klasse erweitert und verbessert und auch nicht verwaltete Klassen unterstützt. Wenn die Classroom-2.0-App in verwalteten Klassen bereitgestellt wird, können die Lehrer jetzt die Schülergeräte stumm schalten und die Schüler Content, beispielsweise Dokumente und URLs, mit einem Lehrer teilen. Wenn die nicht verwaltete Classroom-2.0-App bereitgestellt wird, müssen die Benutzer sich nicht in ASM registrieren. Es muss kein EMM-Konfigurationsprofil auf ihren Geräten installiert werden. Stattdessen laden die Lehrer die Schüler ein, der nicht verwalteten Klassen beizutreten, indem sie einen vierstelligen Passcode eingeben. Die Schüler können der Klasse beitreten, solange sie nicht in verwalteten Klassen registriert sind.

Das moderne Unternehmen nutzt iOS und MobileIron

Mit der Freigabe von iOS 10.3 unterstreicht Apple nochmals sein Engagement für das moderne mobile Unternehmen und die Classroom-App. Obgleich viele der neuen Funktionen nur auf institutionseigenen verwalteten Geräten genutzt werden können, zeigt Apple mit iOS 10.3, dass die Kontrolle durch die IT und die Sicherheit ohne Abstriche an dem hochproduktiven, nativen Benutzererlebnis für iOS-Benutzer weiter Priorität haben.

Gemeinsam mit der vereinheitlichen Mobil- und Cloud-Sicherheitsplattform von MobileIron verfügen Unternehmen damit über eine noch robustere Möglichkeit, Apps sicher bereitzustellen, die Gerätebereitstellung und Geräteverwaltung zu skalieren sowie Apps und Daten in der Cloud in jedem Netzwerk zu schützen. Wenn Sie mehr über die Unterstützung von iOS-Bereitstellungen durch MobileIron EMM wissen wollen, besuchen Sie bitte unsere Website.