
# iOS 10.3 + EMM

## Sécurité et contrôle accrus pour l'entreprise

### Table des matières



MobileIron

415 East Middlefield Road
Mountain View, CA 94043
États-Unis
info@mobileiron.com
www.mobileiron.com
Tél. : +1 877 819 3451
Fax : +1 650 919 8006

# iOS 10.3 : des fonctionnalités essentielles pour l'entreprise mobile moderne

Avec la récente sortie d'iOS 10.3, Apple poursuit sa stratégie axée sur le développement de fonctionnalités destinées aux entreprises, dans cette version qui apporte des changements majeurs. Pour cette mise à jour de printemps, Apple propose des fonctionnalités professionnelles à fort impact, avec les améliorations apportées à son application de messagerie native qui est à la fois plus conviviale et mieux sécurisée, et la possibilité de restreindre les réseaux Wi-Fi pour plus de sécurité. Certaines de ces nouvelles fonctionnalités, notamment l'arrêt et le redémarrage à distance des appareils, sont particulièrement adaptées aux environnements COSU (corporate-owned, single-use ; appareils appartenant à l'entreprise et dédiés à une utilisation spécifique) tels que les kiosques de magasin. En outre, Apple a intensifié ses investissements dans tvOS en y ajoutant des fonctionnalités de configuration et de contrôle EMM pour la quatrième génération d'appareils Apple TV. L'éducation fait également l'objet d'une attention particulière, puisqu'Apple continue de développer son programme d'iPad partagés pour l'enseignement avec des cas d'utilisation étendus à l'application En classe.

Les entreprises doivent cependant savoir que la plupart des nouvelles fonctionnalités ne sont disponibles que sur les appareils « supervisés » ou détenus par l'entreprise. Les organisations qui souhaitent profiter de ces nouvelles fonctionnalités devront superviser leurs appareils iOS à l'aide du programme d'inscription des appareils (DEP, Device Enrollment Program) et d'une plateforme de gestion de la mobilité en entreprise (EMM) telle que MobileIron.

## Performances accrues grâce au nouveau système de fichiers

Dans iOS 10.3, Apple a remplacé le système de fichiers actuellement utilisé sur tous les appareils iOS. Le précédent système de fichiers, HFS+, qui est présent sur les Mac depuis 1988, avait été repris pour iOS et tvOS depuis leur création. Le nouveau système de fichiers Apple (APFS) sera d'abord déployé sur iOS et il est optimisé pour les disques SSD modernes. Les utilisateurs devraient ainsi bénéficier de meilleures performances, car APFS est conçu pour réduire la latence. Ce système de fichiers permet non seulement de stocker largement plus de fichiers, mais aussi de prendre en charge les noms de fichiers 64 bits et de nouveaux schémas de chiffrement flexibles comprenant plusieurs clés pour offrir des options de chiffrement plus avancées. Nous recommandons à tous les développeurs dont les applications réalisent de nombreuses opérations sur le système de fichiers de tester leur code sur iOS 10.3 pour éviter tout conflit imprévu avec APFS.

## Contrôles Wi-Fi pour protéger les appareils des réseaux non approuvés

Grâce à une nouvelle restriction Wi-Fi applicable aux appareils supervisés, les administrateurs peuvent créer une liste blanche de réseaux Wi-Fi. Les réseaux ou SSID (service set identifier) qui ne figurent pas dans cette liste blanche ne seront pas visibles dans le menu des réglages Wi-Fi de l'appareil.

Cette nouvelle restriction Wi-Fi peut s'avérer particulièrement utile pour sécuriser des appareils COSU, par exemple un iPad servant de kiosque dans un magasin et qui se connecte exclusivement à un réseau de magasin préalablement autorisé. La liste blanche de réseaux Wi-Fi peut aussi servir à empêcher les collaborateurs de se connecter à des réseaux Wi-Fi non sécurisés, dans les aéroports ou les cafés par exemple, où de plus en plus de hackers parviennent à subtiliser des données en usurpant l'identité des réseaux existants.

## Sécurité de la messagerie renforcée avec OAuth 2.0

Dans la version 10.3 d'iOS, le client de messagerie natif a été optimisé de manière à prendre en charge OAuth 2.0 sur Office 365 lorsque la suite Microsoft est utilisée conjointement avec Exchange ActiveSync 16.1. OAuth 2.0 sécurise l'accès avec un jeton de sécurité, au lieu de recourir à un nom d'utilisateur et un mot de passe. Si OAuth n'est pas déployé, le client de messagerie utilise par défaut le précédent système de recherche automatique du domaine, qui consiste pour l'appareil à identifier le serveur de messagerie approprié à partir du domaine figurant dans l'adresse e-mail. Apple renforce également S/MIME avec des améliorations de la signature et du chiffrement. S/MIME est utilisé depuis de nombreuses années pour déployer des configurations ActiveSync sur la messagerie native d'iOS, mais les améliorations proposées aujourd'hui offrent davantage de flexibilité aux utilisateurs dans le choix des certificats à utiliser pour la signature et le chiffrement.


## Gestion simplifiée des appareils avec des fonctionnalités EMM étendues

Apple continue d'honorer ses engagements forts visant à sécuriser les appareils iOS via le programme DEP et les solutions EMM. Grâce aux améliorations apportées au programme DEP, les administrateurs peuvent désormais désactiver les écrans de configuration d'iCloud et de l'écran d'accueil sur les nouveaux appareils. Les nouvelles fonctionnalités de gestion qui suivent sont, pour la plupart, disponibles uniquement sur les appareils supervisés détenus par l'entreprise.

- **Les administrateurs peuvent à présent éteindre et redémarrer à distance des appareils iOS supervisés.** Cette fonctionnalité sera particulièrement utile aux établissements scolaires qui clôturent les cours en fin d'année (appareils supervisés uniquement).
- **Les mises à jour d'iOS peuvent maintenant être installées sur les appareils, même s'ils sont verrouillés avec un code d'accès.** Auparavant, les utilisateurs devaient déverrouiller leur appareil en saisissant leur code d'accès pour terminer la mise à jour. Aujourd'hui, la mise à jour aboutit, même si l'utilisateur ne déverrouille pas son appareil. Cette fonctionnalité s'avère utile lorsque les appareils sont mis à jour pendant la nuit, alors qu'aucun administrateur n'est disponible pour les déverrouiller et permettre ainsi la mise à jour du système d'exploitation (appareils supervisés uniquement).
- **Lorsqu'un appareil iOS est perdu, il est possible de le faire jouer une sonnerie spécifique.** Cela permet de localiser des appareils dépourvus d'identifiant Apple, par exemple un appareil kiosque égaré dans un magasin ou un iPad perdu par un élève dans son établissement (appareils supervisés uniquement).
- **Les administrateurs peuvent maintenant restreindre la saisie vocale.** Cette fonctionnalité renforce la sécurité pour les organisations qui souhaitent éviter que des contenus dictés sensibles (notes juridiques ou médicales confidentielles, par exemple) soient perdus ou répliqués sur iCloud ou sur d'autres services cloud (appareils supervisés uniquement).

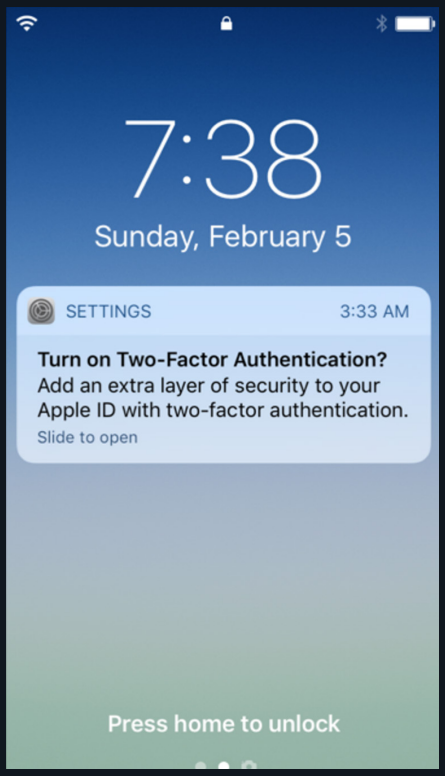
- **Il est possible de vérifier le statut des appareils iOS lorsqu'ils sont connectés par câble à un réseau.** À présent, le service informatique peut déterminer si un appareil iOS est connecté physiquement à un réseau et si ce dernier est approuvé ou non par l'organisation.
- **Les administrateurs de mobiles peuvent maintenant spécifier si un appareil donné doit utiliser le protocole IPv4 ou IPv6 (ou les deux) pour les connexions en modes voix, données et itinérance.** Ainsi, les organisations qui ont adopté le protocole IPv6 pourront étendre l'utilisation de ce protocole aux environnements mobiles.

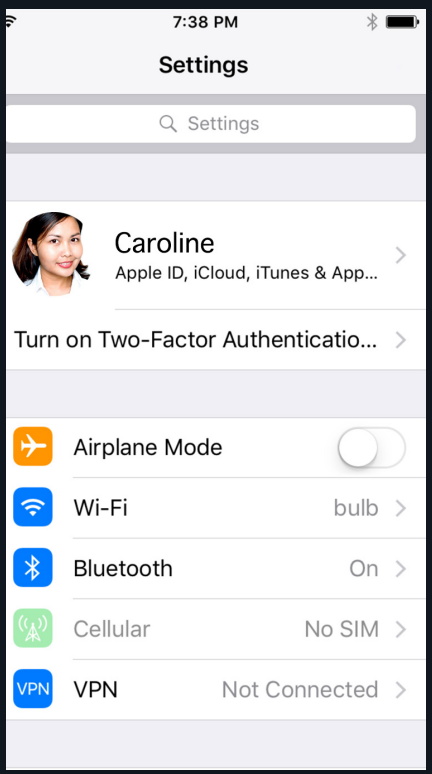
## Sécurité des appareils renforcée avec l'authentification à deux facteurs

Apple prend en charge l'authentification à deux facteurs depuis quelque temps, mais la version 10.3 d'iOS vient compléter cette prise en charge. En effet, les utilisateurs d'appareils équipés d'iOS 10.3 seront désormais invités à configurer l'authentification à deux facteurs si leur identifiant Apple ne prévoit que l'authentification par mot de passe. Il est également possible d'afficher une notification dans l'application Réglages afin de proposer à l'utilisateur de configurer l'authentification à deux facteurs. Enfin, dans iOS 10.3, l'identifiant Apple est présenté de façon plus évidente en haut du menu Réglages, afin que les utilisateurs puissent le trouver rapidement (pour configurer l'authentification à deux facteurs, par exemple) sans avoir à le chercher.

## Mises à jour plus rapides d'iOS et des applications par connexion filaire sur un Mac

Il est maintenant possible de configurer les appareils Mac comme des serveurs de mémoire cache temporaires pour effectuer les mises à jour d'iOS et déployer des applications sur des appareils. Par exemple, un appareil peut être branché sur n'importe quel appareil utilisant une version à jour de macOS Sierra et, si une mise à jour d'application ou d'iOS a déjà été déployée à l'aide de ce Mac, l'appareil iOS connecté peut récupérer la mise à jour sans avoir à télécharger de fichiers via Internet.




*Apple encourage l'utilisation de l'authentification à deux facteurs pour protéger les identifiants Apple.*

Cette fonctionnalité sera particulièrement utile aux entreprises qui doivent préparer un grand nombre d'appareils. Ainsi, un hôpital qui souhaite préparer 100 nouveaux iPad, en y installant une application de 2 Go et la dernière version d'iOS, n'aura besoin de télécharger ces fichiers volumineux qu'une seule fois pour le premier appareil. Il lui suffira de brancher les appareils suivants à un port ou un hub USB sur ce Mac, et ceux-ci pourront récupérer l'application et le système d'exploitation requis par liaison filaire, ce qui réduira considérablement le temps de préparation. Cette fonctionnalité filaire vient compléter l'option de serveur de mémoire cache des serveurs macOS, une solution OTA (over-the-air) qui fonctionne sur le réseau local de l'entreprise.

## tvOS arrivé à maturité professionnelle

Apple lance la gestion de tvOS pour les appareils Apple TV de quatrième génération. Avec tvOS 10.2, Apple transpose de nombreuses fonctionnalités précédemment disponibles sur les appareils iOS traditionnels vers les appareils Apple TV. Désormais, il est possible de configurer et de déployer des certificats, de configurer des réseaux d'entreprise sécurisés et de réinitialiser à distance un appareil Apple TV. Point plus important encore, les appareils Apple TV peuvent maintenant être inscrits à DEP et supervisés OTA lorsqu'ils sont acquis auprès d'un revendeur DEP agréé. Cela représente une extension considérable du rôle que joue tvOS dans la stratégie d'Apple sur les segments de l'éducation et des entreprises.

## EMM et iOS 10.3 pour un enseignement numérique avancé

Le programme iPad partagés pour l'enseignement comprend Apple School Manager (ASM), l'application En classe pour les enseignants et les élèves, ainsi que la possibilité de créer des identifiants gérés au nom des élèves.

iOS 10.3 inclut une version actualisée de En classe 2.0 qui complète et améliore les précédentes fonctionnalités de gestion des classes, et prend également en charge les classes non gérées. Lorsque l'application En classe 2.0 est déployée dans des classes gérées, les enseignants peuvent maintenant couper le son sur les appareils des élèves, et ces derniers peuvent partager des contenus tels que des documents et des URL avec un enseignant. Lorsque la version non gérée de l'application En classe 2.0 est déployée, les utilisateurs ne sont pas tenus de s'inscrire dans ASM ni de disposer d'un profil de configuration EMM sur leur appareil. Dans ce cas, ce sont les enseignants qui invitent les élèves à rejoindre une classe non gérée en saisissant un code d'accès à quatre chiffres. Les élèves peuvent rejoindre la classe, à condition de n'être inscrits dans aucune classe gérée.

# iOS et MobileIron, le choix des entreprises modernes

Avec iOS 10.3, Apple montre clairement sa volonté de poursuivre sa stratégie en faveur de l'enseignement et de l'entreprise mobiles modernes. Si la plupart des nouvelles fonctionnalités d'iOS 10.3 ne sont exploitables que sur des appareils supervisés et détenus par une organisation, il est évident qu'Apple donne de nouveau la priorité au contrôle du service informatique et à la sécurité, sans faire de compromis sur l'expérience native hautement productive à laquelle les utilisateurs d'iOS sont habitués.

En associant leurs appareils iOS à la plateforme de sécurité cloud et mobile unifiée de MobileIron, les organisations peuvent disposer d'une infrastructure encore plus solide pour déployer des applications de façon sécurisée, faire évoluer leur capacité de gestion et de déploiement d'appareils, et protéger leurs applications et données cloud sur n'importe quel réseau. Pour en savoir plus sur les avantages de la solution EMM de MobileIron dans le cadre d'un déploiement iOS, consultez notre site Web.