



# IBM MaaS360 Mobile Device Management for iOS

*Approvisionnez, gérez et protégez les derniers appareils iOS, les applications et le contenu*

---

## Principaux avantages

- Approvisionnez, protégez et gérez vos appareils, vos applications et votre contenu depuis une seule console
- Configurez la messagerie, les calendriers, les contacts, le Wi-Fi et les profils VPN avec la technologie sans fil pour l'accueil et l'intégration rapide des utilisateurs
- Bénéficiez d'une prise en charge dès le jour de lancement des derniers systèmes d'exploitation mobiles pour les appareils iOS
- Créez des règles de sécurité et mettez-les en œuvre au moyen d'actions automatisées de conformité (par ex. code d'accès et blocage d'un appareil compromis)
- Utilisez des tableaux de bord et des rapports rigoureux pour gérer à la fois les terminaux d'entreprise et personnels

## Apple + IBM® MaaS360® = meilleurs ensemble

Apple continue d'innover sur les technologies d'entreprise pour faire d'iOS 9 une plateforme de productivité plus puissante. Et MaaS360 offre une prise en charge rapide et robuste d'iOS 9 et des versions précédentes. En travaillant ensemble, Apple et IBM aident les entreprises à réaliser le potentiel inexploité de la mobilité avec leurs employés, leurs clients et leurs partenaires.

Inscrivez et mettez à jour les appareils à la dernière version d'iOS instantanément et en toute transparence le jour du lancement par Apple sans aucune perturbation de l'utilisateur ni aucun mal de tête pour le service informatique. Ne restez pas derrière avec d'autres fournisseurs de gestion d'appareils mobiles (MDM) ; découvrez les nouvelles caractéristiques du nouvel iOS 9 avec MaaS360 dès aujourd'hui !

## Gestion instantanée d'Apple iOS

IBM MaaS360 for iOS offre une visibilité et un contrôle étendus pour prendre en charge les iPhone et les iPad dans l'entreprise, en prenant en charge les versions iOS 4.3 et ultérieures. Il prend aujourd'hui en charge iOS9 et fournit des outils que vous pouvez utiliser pour gagner en perspicacité, prendre des mesures, établir et distribuer des règles, gérer des applications et des documents, et bien plus encore.

La solution offre une manière rapide et facile de protéger ces appareils et les données d'entreprise qu'ils contiennent. Vous pouvez les inscrire à distance et utiliser les règles de sécurité et de conformité pour appliquer des codes d'accès et de cryptage, détecter et limiter les appareils débridés, mettre sur liste blanche ou noire des applications, contrôler les sauvegardes de fichiers, et bien plus encore.

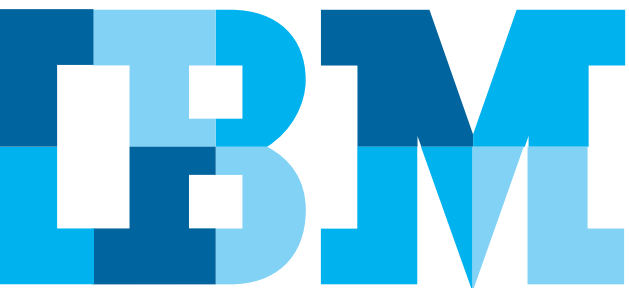




Figure 1 : Déployez simplement des applications et du contenu vers les appareils iOS de votre entreprise

## Gagnez en profondeur

- Modèle, numéro de série, système d'exploitation
- Réseau local / réseau actuel
  - Statut d'itinérance, adresse MAC
- Capacité de stockage gratuit
- Version et taille des applications
- Référence de l'appareil (numéro de téléphone, IMEI, adresse e-mail)
  - Niveau de cryptage, détection du débridage, statut du code d'accès, limitations de l'appareil, profils installés, règles de sécurité, et bien plus encore
- Utilisez le programme d'inscription des appareils d'Apple pour inscrire automatiquement les appareils appartenant à l'entreprise lors de l'activation avec vos configurations et règles.
- Le verrou d'activation dans Localiser mon iPhone est activé, verrouillant l'appareil pour la référence Apple de l'utilisateur
- Rapport si un compte iTunes existe sur un appareil
- Affichez en détail des rapports sur les documents, les utilisateurs, les appareils, les applications, et bien plus encore

## Prenez des mesures

- Configurez le Wi-Fi, le VPN et les paramètres et profils de messagerie
- Repérez, verrouillez un appareil ou réinitialisez les codes d'accès oubliés
- Nettoyez sélectivement les données d'entreprise tout en conservant les données personnelles sur un appareil appartenant à un employé
- Réalisez le nettoyage complet d'un appareil perdu ou volé
- Changez les règles d'iOS
- Activez ou désactivez la voix et les contrôles d'itinérance des données

## Catalogue des applications d'entreprise

- Facilité de gestion des applications d'entreprise : les applications mobiles distribuées par MaaS360 pour les appareils iOS sont entièrement gérées, vous permettant de simplifier le déploiement des applications tout en augmentant la sécurité.
  - Recommandez l'application iTunes pour les employés
  - Distribuez des applications « faites maison » et publiez des mises à jour
  - Poussez à distance une application sur un appareil, installez automatiquement si l'appareil est supervisé
  - Gérez les contrôles d'ouverture pour limiter les ouvertures de fichiers d'entreprise dans des applications personnelles et vice-versa
  - Connectez les applications gérées au VPN pour avoir un accès protégé au réseau
  - Activez la connexion unique à travers des applications pour l'authentification
  - Appliquez le cryptage des données d'applications tierces automatiquement
- Support VPP Apple
  - Distribuez et installez des applications prépayées sans visiter le magasin d'applications Apple App Store
  - Économisez de l'argent en conservant la pleine propriété et le contrôle des licences VPP des applications et des livres lorsque les utilisateurs n'ont plus besoin d'elles

## Mettez en place et distribuez des règles

- Appliquez les exigences des codes d'accès
- Configurez les limitations des appareils
  - Appliquez les sauvegardes cryptées
  - Restreignez l'utilisation de l'appareil photo, de FaceTime et de Touch ID, et bien plus encore
  - Restreignez l'installation des applications, des Photo Stream partagés, et bien plus encore
  - Forcez le trafic Internet via un serveur proxy global HTTP
  - Distribuez le Wi-Fi, le VPN et les profils de messagerie tels que les paramètres d'Exchange ActiveSync
- Gérez les contrôles d'iCloud
  - Gérez les documents, les données d'application, la sauvegarde de l'appareil photo et la synchronisation avec iCloud pour l'utilisateur, un groupe ou tous les appareils
- Augmentez la sécurité de la messagerie
  - Limitez les déplacements d'e-mails entre différents comptes pour protéger des fuites de données d'entreprise
  - Empêchez les applications tierces d'envoyer des e-mails.
- Configuration Wi-Fi avancée
  - Gérez et poussez automatiquement les paramètres du proxy et le SSID
- Renforcement du mot de passe iTunes
  - Nécessite que les utilisateurs entrent leurs mots de passe iTunes pour accéder au contenu, aux applications et aux données stockées dans iTunes
- Envoyez un message et un numéro sur l'écran de verrouillage si l'appareil est perdu
- Autorisez la fonction Handoff qui permet la continuité, les résultats internet dans Spotlight et une synchronisation iCloud pour les applications gérées



### Prise en charge le jour du lancement

Ensemble, iOS 9 et MaaS360 sont prêts à offrir un nouveau niveau de sécurité, de productivité, et des fonctions de gestion des appareils et des données pour aider votre entreprise à franchir l'étape suivante dans son voyage vers la mobilité.

### Fonctions de sécurité pour l'entreprise du nouvel iOS 9

- Limitez l'usage de la fonction Airdrop pour les applications gérées et l'iCloud Photo Library
- Définissez de nouvelles restrictions pour l'App Store, de nouveaux raccourcis clavier, Apple Watch, la modification du mot de passe, les téléchargements automatiques d'applications, et bien plus encore
- Permet une installation directe les appareils supervisés

### Caractéristiques de distribution d'applications du nouvel iOS 9

- La distribution d'applications basée sur l'appareil Désactivez la fonction « confiance » pour les applications d'entreprise sur en utilisant le programme de volume d'achat (PVA) et MaaS360 pour affecter des applications directement à un appareil avec le numéro de série, sans avoir besoin d'un identifiant Apple
- Poussez ou tirez des applications publiques sans avoir besoin que l'utilisateur accède à l'App Store
- Les applications d'entreprise installées avec MaaS360 sont explicitement considérées comme étant de confiance, l'utilisateur n'ayant plus à le confirmer
- Si un appareil a une application avant d'être supervisé, cette application sera automatiquement gérée quand il sera supervisé
- Les applications achetées et distribuées via le VPP peuvent être assignées à des appareils ou à des utilisateurs n'importe où dans le monde où l'application est disponible

### Nouvelle gestion d'appareils et de données iOS 9

- MaaS360 peut déclencher des mises à jour de l'appareil pour des nouvelles versions d'iOS pour tout appareil du programme d'inscription des appareils d'Apple
- Le configurateur Apple vous permet de pré-déployer des applications et de diffuser des inscriptions d'appareils avec MaaS360 via le programme d'inscription d'Apple
- Les applications VPN prennent en charge les connexions UDP et TCP pour diffuser de l'audio ou de la vidéo

Pour plus d'informations sur IBM MaaS360 et pour commencer un essai gratuit de 30 jours, visitez <http://ibm.biz/EssayezMaaS360>



---

© Copyright IBM Corporation 2016

Compagnie IBM France  
17, avenue de l'Europe  
92275 BOIS COLOMBES CEDEX

Produit aux États-Unis d'Amérique  
Août 2016

IBM, le logo IBM, ibm.com et X-Force sont des marques d'International Business Machines Corp. déposées dans de nombreuses juridictions à travers le monde. BYOD360™, Cloud Extender™, Control360®, E360®, Fiberlink®, MaaS360®, MaaS360® et appareil, MaaS360 PRO™, MCM360™, MDM360™, MI360®, Mobile Context Management™, Mobile NAC®, Mobile360®, MaaS360 Productivity Suite™, MaaS360® Secure Mobile Mail, MaaS360® Mobile Document Sync, MaaS360® Mobile Document Editor, et MaaS360® Content Suite, Simple. Secure. Mobility.®, Trusted Workplace™, Visibility360®, et We do IT in the Cloud.™ et appareil sont des marques ou des marques déposées de Fiberlink Communications Corporation, une société IBM. D'autres noms de produits et services peuvent être des marques commerciales d'IBM ou d'autres sociétés. Une liste actualisée des marques IBM est disponible sur le Web à la section « Copyright and trademark information » sur [ibm.com/legal/copytrade.html](http://ibm.com/legal/copytrade.html)

Apple, iPhone, iPad, iPod touch et iOS sont des marques commerciales ou déposées d'Apple Inc. enregistrées aux États-Unis et dans d'autres pays. Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

Les informations contenues dans ce document sont correctes à la date de leur publication initiale et peuvent être modifiées par IBM à tout moment. Toutes les offres ne sont pas disponibles dans tous les pays.

Les données de performances et les exemples citant des clients ne sont présentés qu'à titre d'illustration. Les résultats de performances réels peuvent varier selon les configurations et les conditions de fonctionnement spécifiques. Il incombe à l'utilisateur d'évaluer et de vérifier le fonctionnement de tout autre produit ou programme avec les produits et programmes IBM.

LES INFORMATIONS CONTENUES DANS CE DOCUMENT SONT FOURNIES « EN L'ÉTAT », SANS AUCUNE GARANTIE, EXPRESSE OU TACITE, NOTAMMENT SANS AUCUNE GARANTIE OU CONDITION DE QUALITÉ MARCHANDE OU D'APTITUDE A UN EMPLOI SPÉCIFIQUE ET SANS AUCUNE GARANTIE DE NON-CONTREFAÇON. Les produits IBM sont garantis conformément aux conditions de leur contrat de vente.

Le client est tenu de s'assurer du respect des lois et réglementations en vigueur. IBM ne fournit aucun conseil juridique et ne garantit pas que ses produits ou services assurent la conformité du client aux lois et réglementations en vigueur.

Toutes les déclarations relatives aux orientations futures d'IBM sont sujettes à modification ou retrait sans préavis. Elles n'expriment que les intentions et les objectifs d'IBM.

Déclaration de bonnes pratiques en matière de sécurité : La sécurité des systèmes informatiques implique la protection des systèmes et des informations en prévenant, détectant et réagissant aux accès non autorisés, qu'ils proviennent de l'entreprise ou de l'extérieur. Les accès non autorisés peuvent entraîner l'altération, la destruction ou l'utilisation inappropriée des informations, et ainsi causer des dommages ou une utilisation abusive de vos systèmes, par exemple pour attaquer des tiers. Aucun système ou produit informatiques ne doit être considéré comme entièrement sécurisé. Aucun produit ni aucune mesure de sécurité ne peut être totalement efficace contre les accès non autorisés. Les systèmes et produits IBM s'inscrivent dans une approche de sécurité complète qui implique des procédures opérationnelles supplémentaires et peuvent demander aux autres systèmes, produits ou services d'être plus efficaces. IBM ne garantit pas que ses systèmes et ses produits sont invulnérables face aux comportements malveillants ou illégaux provenant de tiers.



Recyclable