Gérer les appareils et les données d'entreprise sur iOS

Présentation

Les entreprises du monde entier équipent leurs employés d'iPhone et d'iPad.

Table des matières

Pour une stratégie mobile réussie, il est essentiel de trouver un équilibre entre contrôle du service informatique et liberté des utilisateurs. En personnalisant les appareils iOS avec leurs propres apps et contenus, les utilisateurs se sentent plus investis et responsables, ce qui accroît leurs niveaux d'implication et de productivité. Cette personnalisation est rendue possible par la structure de gestion d'Apple, qui propose des solutions intelligentes pour gérer les données et les apps d'entreprise de manière discrète, en séparant les données professionnelles des données personnelles. En outre, les utilisateurs comprennent la manière dont leur appareil est géré et savent que leur vie privée est respectée.

Ce document explique comment confier les contrôles essentiels au service informatique tout en laissant à disposition des utilisateurs les outils les plus performants pour leur activité. Il vient compléter le document Référence pour le déploiement iOS, une référence technique complète en ligne pour le déploiement et la gestion des appareils iOS dans votre entreprise.

Pour accéder à Référence pour le déploiement iOS, consultez help.apple.com/deployment/ios.

Bases de la gestion

Avec iOS, vous pouvez faciliter les déploiements d'iPad et d'iPhone à l'aide de techniques intégrées qui vous permettent de simplifier la configuration des comptes, de configurer des règles, de distribuer des apps et d'appliquer des restrictions aux appareils à distance.

Notre approche de la gestion

La structure de gestion d'Apple constitue la base de la gestion des appareils mobiles. Cette structure est intégrée à iOS, ce qui permet aux entreprises de gérer juste ce qu'il faut d'éléments importants, au lieu de se contenter de verrouiller ou de désactiver des fonctionnalités. Ainsi, la structure de gestion d'Apple permet aux solutions de gestion des appareils mobiles (MDM) d'exercer un contrôle plus précis sur vos appareils, apps et données. Et, point essentiel, vous bénéficiez d'un grand contrôle sans nuire à l'expérience utilisateur ni compromettre la confidentialité de vos employés.

Les autres méthodes de gestion des appareils disponibles sur le marché emploient différents termes pour décrire la fonctionnalité MDM : par exemple, gestion de la mobilité en entreprise (EMM) ou gestion des applications mobiles (MAM). Ces solutions tendent vers le même objectif : gérer les appareils et les données professionnelles de votre entreprise à distance. Et comme la structure de gestion d'Apple est intégrée à iOS, il n'est pas nécessaire de se procurer une application agent distincte auprès du fournisseur de votre solution MDM.

Séparer les données professionnelles des données personnelles

Que votre entreprise prenne en charge les appareils personnels des utilisateurs ou des appareils lui appartenant, vous pouvez atteindre vos objectifs de gestion informatique tout en garantissant la productivité de vos employés. Les données personnelles et professionnelles sont gérées séparément sans nuire à la fluidité de l'expérience utilisateur. Les apps de productivité les plus performantes peuvent donc côtoyer vos apps d'entreprise sur l'appareil des utilisateurs, ce qui permet aux employés de bénéficier d'une plus grande liberté de travail. Sans compter qu'iOS n'a pas recours à des solutions tierces telles que des conteneurs, lesquelles modifient l'expérience utilisateur et frustrent les utilisateurs.

Comprendre les différents modèles de gestion

Les conteneurs sont souvent conçus pour résoudre des problèmes que l'on trouve sur des plates-formes tierces mais qui n'existent pas sous iOS. Certains conteneurs utilisent une stratégie « dual persona », qui consiste à créer deux environnements distincts sur le même appareil. D'autres se concentrent sur la conteneurisation des apps à travers une intégration basée sur le code ou des solutions d'enveloppement d'app. Toutes ces méthodes constituent des obstacles à la productivité des utilisateurs, qu'il s'agisse de se connecter et de se déconnecter de plusieurs espaces de travail ou d'introduire une dépendance à un code propriétaire résultant souvent en une incompatibilité des apps avec les mises à jour du système d'exploitation.

Les entreprises ayant renoncé à l'utilisation de conteneurs constatent que les commandes de gestion intégrées à iOS offrent une meilleure expérience aux utilisateurs et améliorent leur productivité. Il est préférable d'utiliser les contrôles des règles pour gérer les flux de données de manière discrète et fluide plutôt que de rendre plus compliquée l'utilisation à la fois professionnelle et personnelle des appareils.

Gestion des données d'entreprise

Avec iOS, inutile de verrouiller vos appareils. Les technologies majeures contrôlent le flux des données d'entreprise entre les apps et les empêchent de fuir dans les apps ou services cloud personnels de l'utilisateur.

Contenu géré

Le contenu géré couvre l'installation, la configuration, la gestion et la suppression d'apps de l'App Store et d'apps personnalisées développées en interne, de comptes ainsi que de livres et de domaines.

- **Apps gérées.** Les apps installées à l'aide d'une solution MDM sont appelées apps gérées. Il peut s'agir d'apps gratuites ou payantes de l'App Store ou d'apps personnalisées développées en interne, et toutes peuvent être installées à distance avec la MDM. Les apps gérées comportent souvent des données sensibles et offrent davantage de contrôle que les apps téléchargées par les utilisateurs. Le serveur MDM peut supprimer à la demande des apps gérées et les données associées ou préciser si les apps doivent être supprimées lors de la suppression du profil MDM. En outre, le serveur MDM peut empêcher la sauvegarde sur iTunes et iCloud des données de l'app gérée.
- **Comptes gérés.** La MDM peut aider les utilisateurs à être rapidement opérationnels en configurant automatiquement leurs comptes de messagerie et autres. En fonction du fournisseur de la solution MDM et de l'intégration avec vos systèmes internes, les entités de compte peuvent aussi être pré-renseignées avec le nom de l'utilisateur, l'adresse électronique et, le cas échéant, les identités de certificat pour l'authentification et la signature. La MDM peut configurer les types de comptes suivants : IMAP/POP, CalDAV, Calendriers par abonnement, CardDAV, Exchange ActiveSync et LDAP.

- **Livres gérés.** Avec la MDM, les livres, livres ePub et documents PDF peuvent directement être transférés sur les appareils, de sorte que les employés disposent toujours des ressources dont ils ont besoin. Les livres gérés peuvent uniquement être partagés avec d'autres apps gérées ou envoyés par e-mail depuis des comptes gérés. Les ressources obsolètes peuvent être supprimées à distance.
- **Domaines gérés.** Les téléchargements effectués depuis Safari sont considérés comme des documents gérés s'ils proviennent d'un domaine géré. Des URL et sous-domaines spécifiques peuvent être gérés. Si, par exemple, un utilisateur télécharge un fichier PDF depuis un domaine géré, ce dernier s'assure que le fichier est conforme aux réglages appliqués aux documents gérés. Les chemins suivant le domaine sont gérés par défaut.

Distribution gérée

La distribution gérée vous permet d'utiliser votre solution MDM ou Apple Configurator 2 pour gérer les apps et les livres achetés via le Programme d'achats en volume (VPP). Pour activer la distribution gérée, vous devez tout d'abord associer votre solution MDM à votre compte VPP à l'aide d'un jeton sécurisé. Lorsque votre serveur MDM est connecté au VPP, vous pouvez attribuer des apps directement à un appareil, même si l'utilisateur ne possède pas d'identifiant Apple. L'utilisateur est averti lorsque les apps sont prêtes à être installées sur son appareil. Sur les appareils supervisés, les apps sont installées en arrière-plan et l'utilisateur n'est pas averti.

Pour conserver le contrôle total des apps avec une solution MDM, attribuez directement les apps à un appareil.

Configuration des apps gérées

Avec la configuration des apps gérées, la MDM s'appuie sur la structure de gestion native d'iOS pour configurer les apps pendant ou après le déploiement. Cette structure permet aux développeurs d'identifier les réglages de configuration devant être appliqués lorsque leurs apps sont installées en tant qu'apps gérées. Les apps configurées de cette manière sont immédiatement utilisables par les employés, sans qu'aucune autre configuration ne soit requise. L'équipe informatique est assurée que les données d'entreprise présentes au sein des apps sont sécurisées et ne nécessitent ni SDK propriétaire ni enveloppement d'app.

Les développeurs d'apps peuvent utiliser certaines capacités pouvant être activées avec la configuration des apps gérées, par exemple configurer des apps, empêcher la sauvegarde des apps, désactiver la capture d'écran et effacer les apps à distance.

L'objectif de la communauté AppConfig est de partager des outils et des bonnes pratiques en rapport avec les capacités intégrées des systèmes d'exploitation mobiles. Les principaux

fournisseurs de solutions MDM appartenant à cette communauté ont mis au point une structure normalisée compatible avec la configuration des apps gérées et exploitable par tous les développeurs. En mettant à disposition une manière plus cohérente, plus libre et plus simple de configurer et de sécuriser les apps mobiles, cette communauté permet d'augmenter l'adoption de la mobilité en entreprise.

Pour en savoir plus sur la communauté AppConfig, consultez www.appconfig.org.

Flux de données gérés

Les solutions MDM offrent des fonctionnalités spécifiques permettant de gérer les données d'entreprise plus précisément afin d'éviter leur fuite dans les apps ou services cloud personnels de l'utilisateur.

- **Gestion des autorisations d'ouverture.** La gestion des autorisations d'ouverture s'appuie sur un ensemble de restrictions empêchant l'ouverture de pièces jointes ou de documents provenant de sources gérées dans des destinations non gérées, et inversement.

  Il est par exemple possible d'empêcher l'ouverture d'une pièce jointe confidentielle reçue sur un compte de messagerie professionnel géré dans une app personnelle de l'utilisateur. Seules les apps installées et gérées par la solution MDM peuvent ouvrir ce document de travail. Les apps personnelles non gérées de l'utilisateur ne figurent pas dans la liste des apps disponibles pour ouvrir la pièce jointe. En plus des apps, comptes, livres et domaines gérés, plusieurs extensions appliquent ces restrictions d'ouverture gérées.

Pour protéger les données d'entreprise, seules les apps qui ont été installées et gérées par la solution MDM peuvent ouvrir ce document de travail.

- **Extensions gérées.** Les extensions d'apps permettent aux développeurs tiers d'apporter une fonctionnalité à d'autres apps, voire à des systèmes essentiels intégrés à iOS comme le Centre de notifications, donnant lieu à de nouveaux processus professionnels entre les apps. Les ouvertures gérées empêchent les fonctionnalités d'extensions non gérées d'interagir avec des apps gérées. Les exemples suivants montrent différents types d'extensions :
  - **Les extensions de fournisseurs de documents** permettent aux apps de productivité d'ouvrir des documents à partir d'un grand nombre de services cloud sans créer de copies inutiles.
  - **Les extensions d'actions** permettent aux utilisateurs de manipuler ou de visualiser des contenus dans le contexte d'une autre app. Les utilisateurs peuvent, par exemple, utiliser une action pour traduire du texte depuis une autre langue directement dans Safari.

– **Les extensions de claviers personnalisés** fournissent des claviers différents de ceux déjà intégrés à iOS. Les ouvertures gérées peuvent empêcher l'affichage de claviers non autorisés dans vos apps d'entreprise.

– **Les extensions,** aujourd'hui également appelées Widgets, permettent de fournir directement des informations dans la vue Aujourd'hui du Centre de notifications. Cela permet aux utilisateurs d'obtenir immédiatement des informations à jour depuis une app, avec des interactions simplifiées pour lancer l'app complète et obtenir plus d'informations.

– **Les extensions de partage** offrent un moyen pratique de partager du contenu avec d'autres entités, comme des sites de réseaux sociaux ou des services de chargement. Par exemple, si une app prévoit un bouton Partager, les utilisateurs peuvent sélectionner une extension de partage représentant un site de réseaux sociaux et l'utiliser pour publier un commentaire ou un contenu.

Options de gestion flexibles

La structure de gestion d'Apple est flexible et permet de trouver une méthode de gestion équilibrée entre les appareils personnels des utilisateurs et les appareils appartenant à l'entreprise. Lorsque vous utilisez une solution MDM tierce avec iOS, vos options de gestion des appareils forment un ensemble allant de l'utilisation d'une méthode hautement ouverte à l'utilisation d'une méthode aussi précise que nécessaire.

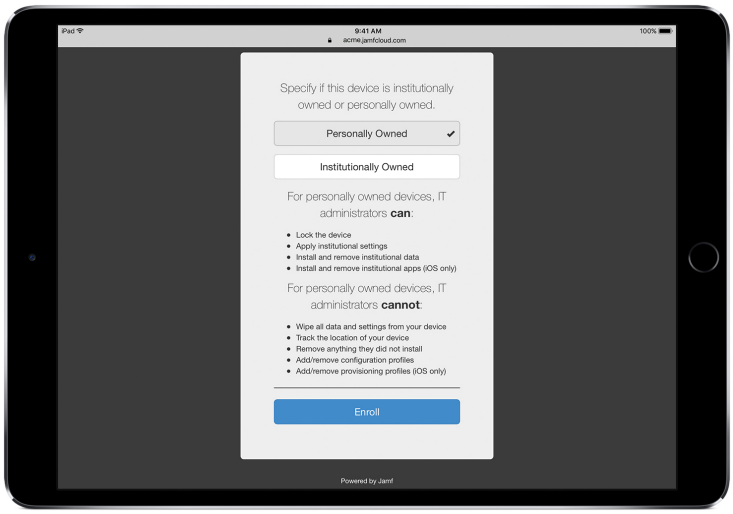
Modèles de propriété

Selon le modèle de propriété de votre entreprise, la gestion des appareils et des apps pourra varier. Les deux modèles de propriété pour appareils iOS les plus utilisés en entreprise distinguent les appareils appartenant à l'entreprise des appareils appartenant aux utilisateurs.

Appareils appartenant à l'utilisateur

Dans le cas du déploiement d'appareils appartenant aux utilisateurs, iOS propose une installation personnalisée et garantit la transparence sur la manière dont les appareils sont configurés. Elle garantit également aux utilisateurs que leurs données personnelles ne pourront pas être consultées par l'entreprise.

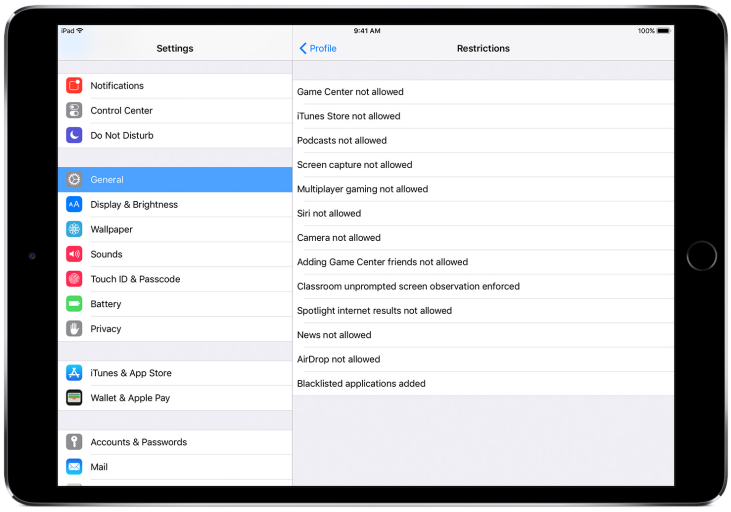
• **Abonnement et désabonnement.** Lorsque les appareils sont achetés et configurés par les utilisateurs (appareils personnalisés ou BYOD), il est toujours possible de leur donner accès aux services fournis par l'entreprise, comme le Wi-Fi, la messagerie et le calendrier. Pour ce faire, il suffit aux utilisateurs de s'inscrire auprès de la solution MDM de votre entreprise. Lorsqu'un utilisateur inscrit son appareil iOS auprès du serveur MDM pour la première fois, il reçoit des informations concernant les données auxquelles le serveur MDM pourra accéder et les fonctionnalités qu'il configurera. Cela permet aux utilisateurs de savoir exactement quels éléments sont gérés et instaure une relation de confiance entre les utilisateurs et vous. Il est important de préciser aux utilisateurs que si cette méthode de gestion leur pose un quelconque problème, ils pourront se désinscrire en supprimant le profil de gestion de leur appareil. Cela entraînera la suppression de tous les comptes et apps d'entreprise installés via MDM.



La majeure partie des solutions MDM tierces dispose d'une interface conviviale pour mettre à l'aise les employés lors de leur inscription*.

* Capture d'écran utilisée avec l'aimable autorisation de Jamf.

Une plus grande transparence. Une fois inscrits à la MDM, les employés peuvent aller dans Réglages pour voir les apps, les livres et les comptes gérés ainsi que les restrictions appliquées. iOS identifie comme étant « gérés » tous les réglages, comptes et contenus de l'entreprise installés via la MDM.



Dans Réglages, l'interface utilisateur pour les profils de configuration montre précisément aux utilisateurs les éléments ayant été configurés sur leur appareil.

- **Vie privée de l'utilisateur.** Le serveur MDM vous permet d'interagir avec les appareils iOS sans pour autant donner accès à l'intégralité des réglages et des informations associés au compte. Il est possible de gérer les comptes, les réglages et les informations d'entreprise mis à disposition via la MDM, mais les comptes personnels des utilisateurs restent toujours inaccessibles. En fait, les fonctionnalités qui assurent la sécurité des données dans les apps gérées par l'entreprise empêchent également que le contenu personnel d'un utilisateur entre dans le flux de données de l'entreprise.

  Les exemples suivants montrent à quelles informations un serveur MDM tiers peut avoir accès sur un appareil iOS personnel :

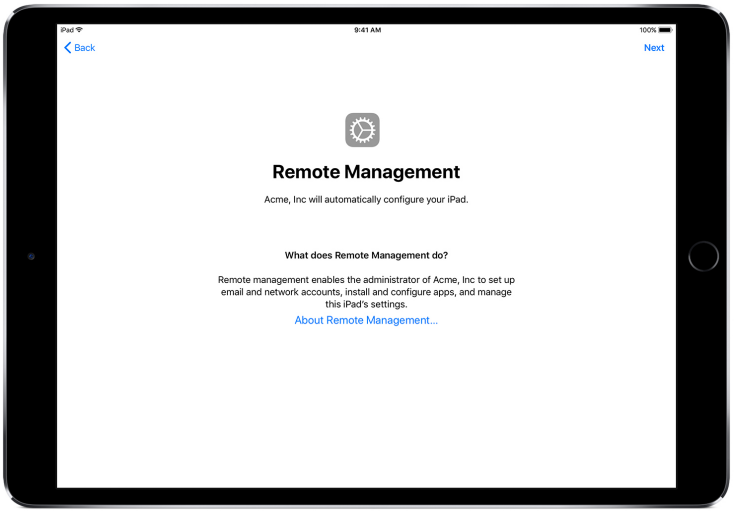
Ce qu'un serveur MDM peut voir :	Un serveur MDM ne peut pas voir les données personnelles telles que :
Nom de l'appareil	E-mails, calendriers, contacts personnels ou professionnels
Numéro de téléphone	SMS ou messages iMessage
Numéro de série	Historique du navigateur Safari
Nom et numéro du modèle	Journaux des appels FaceTime ou téléphoniques
Capacité et espace disponible	Rappels et notes personnels
Numéro de version iOS	Fréquence d'utilisation des apps
Apps installées	Localisation de l'appareil

- **Personnalisation des appareils.** Les entreprises ont remarqué qu'en autorisant les utilisateurs à personnaliser un appareil à l'aide de leur propre identifiant Apple, ceux-ci se sentent plus investis et responsables. De plus, ils gagnent en productivité, car ils peuvent choisir les apps et les contenus dont ils ont besoin pour accomplir leurs tâches au mieux.

Appareils appartenant à l'entreprise

Dans le cas du déploiement d'appareils appartenant à l'entreprise, vous pouvez fournir un appareil à chaque utilisateur (appelé déploiement personnalisé) ou bien choisir de partager des appareils entre plusieurs utilisateurs (déploiement non personnalisé). Les fonctionnalités iOS telles que l'inscription automatique, les réglages MDM verrouillables, la supervision des appareils et le VPN permanent garantissent que les appareils sont configurés selon les exigences de votre entreprise, ce qui permet un contrôle accru tout en assurant la protection des données de l'entreprise.

- **Inscription automatisée.** Le Programme d'inscription des appareils (DEP) vous permet d'automatiser l'inscription MDM pendant la configuration initiale des iPhone, iPad et Mac appartenant à votre entreprise. Vous pouvez rendre l'inscription obligatoire et non révocable. Vous pouvez également régler les appareils en mode supervisé pendant le processus d'inscription et permettre aux utilisateurs de passer certaines étapes de configuration de base.



Avec le DEP, votre solution MDM configurera automatiquement vos appareils iOS pendant les étapes de l'Assistant réglages.

- **Appareils supervisés.** La supervision propose des capacités de gestion supplémentaires pour les appareils iOS appartenant à l'entreprise. Cela comprend, entre autres, la capacité à activer un filtre web via un proxy global pour vous assurer que le trafic web des utilisateurs respecte les consignes de l'entreprise, ou encore l'impossibilité pour l'utilisateur de rétablir les réglages d'usine de l'appareil. Par défaut, tous les appareils iOS sont non supervisés. Utilisez le DEP pour

activer automatiquement le mode supervisé, ou Apple Configurator 2 pour activer manuellement la supervision.

Si vous n'avez pas prévu d'utiliser les fonctionnalités spécifiques du mode supervisé pour le moment, vous pouvez tout de même envisager d'activer la supervision de vos appareils pendant la configuration afin de pouvoir en tirer parti à l'avenir. Autrement, vous devrez effacer des appareils ayant déjà été déployés. Le rôle de la supervision n'est pas de verrouiller l'appareil, il s'agit plutôt d'optimiser les appareils appartenant à l'entreprise en améliorant les capacités de gestion. À long terme, la supervision offre davantage de possibilités à votre entreprise.

Pour voir une liste complète des réglages supervisés, consultez le document Référence pour le déploiement iOS.

Restrictions

iOS prend en charge les catégories de restrictions suivantes, que vous pouvez configurer à distance pour répondre aux besoins de votre entreprise sans nuire à l'expérience des utilisateurs :

- AirPrint
- Installation d'applications
- Utilisation des apps
- App En classe
- Appareil
- Page d'accueil
- Restrictions relatives aux utilisateurs et groupes d'utilisateurs de Gestionnaire de profils
- Safari
- Réglages de sécurité et de confidentialité
- Siri

Les catégories suivantes proposent également des options qui peuvent être configurées par votre solution MDM :

- Réglages d'inscription MDM automatisée
- Écrans de l'Assistant réglages

Capacités de gestion supplémentaires

Interrogation des appareils

Outre la configuration des appareils, un serveur MDM peut également interroger les appareils afin de récupérer diverses informations, comme des détails sur l'appareil, le réseau, les applications ainsi que les données de conformité et de sécurité. Ces informations permettent de vérifier que l'appareil est toujours en conformité avec les règles fixées par l'entreprise. Le serveur MDM détermine la fréquence à laquelle il collecte les informations.

Vous trouverez ci-dessous des exemples des informations pouvant être obtenues lors de l'interrogation d'un appareil iOS :

- Informations sur l'appareil (nom)
- Modèle, version d'iOS, numéro de série

• Informations réseau

• État de l'itinérance, adresses MAC

• Applications installées

• Nom, version, taille des apps

• Données de conformité et de sécurité

• Certificats, règles et paramètres installés

• État du chiffrement

Tâches de gestion

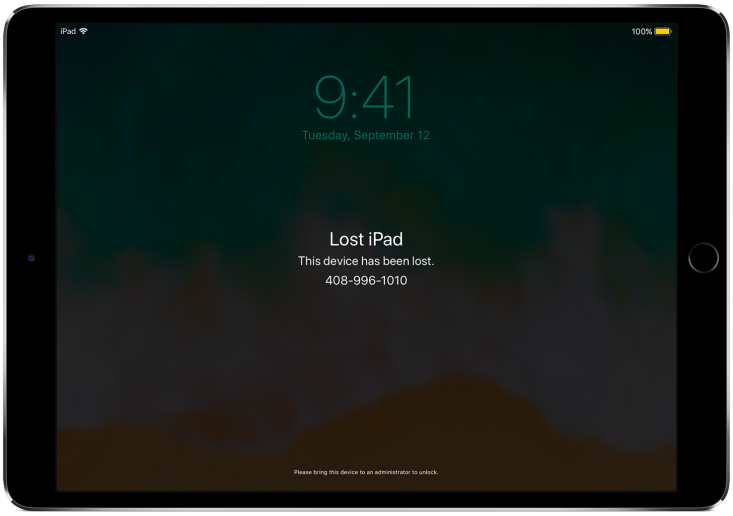
Lorsqu'un appareil est géré, un serveur MDM peut effectuer un large éventail de tâches administratives, notamment modifier automatiquement les réglages de configuration sans intervention de l'utilisateur, effectuer une mise à jour d'iOS sur les appareils verrouillés par code de sécurité, verrouiller ou effacer un appareil à distance, ou supprimer le code de verrouillage pour que les utilisateurs ayant oublié leur mot de passe puissent le réinitialiser. Un serveur MDM peut également demander à un appareil iOS de lancer la recopie vidéo AirPlay vers une destination spécifique, ou de mettre fin à une session AirPlay.

Mode Perdu

Avec iOS 9.3 et ultérieur, votre solution MDM peut mettre un appareil supervisé en mode Perdu à distance. Cette action verrouille l'appareil et permet d'afficher un message avec un numéro de téléphone sur l'écran de verrouillage.

Avec le mode Perdu, les appareils supervisés perdus ou volés peuvent être localisés, car la MDM leur demande à distance où ils se situaient la dernière fois qu'ils se sont connectés. Le mode Perdu ne nécessite pas l'activation de Localiser mon iPhone.

Si la MDM désactive le mode Perdu à distance, l'appareil est déverrouillé et sa position est enregistrée. Dans un souci de transparence, l'utilisateur est averti de la désactivation du mode Perdu.



Lorsque la MDM met un appareil en mode Perdu, elle verrouille l'appareil, autorise l'affichage de messages à l'écran et détermine sa position.

Verrouillage de l'activation

Avec iOS 7.1 et ultérieur, vous pouvez utiliser la MDM pour activer le Verrouillage de l'activation lorsqu'un utilisateur lance Localiser mon iPhone sur un appareil supervisé. Cela permet à votre entreprise de bénéficier de la capacité dissuasive du Verrouillage de l'activation, tout en vous permettant de la contourner si, par exemple, un utilisateur quitte votre entreprise sans préalablement désactiver le Verrouillage de l'activation avec son identifiant Apple.

Votre solution MDM peut récupérer un code de contournement et permettre à l'utilisateur d'activer le Verrouillage de l'activation sur l'appareil si les conditions suivantes sont remplies :

- Si Localiser mon iPhone est activé lorsque votre solution MDM autorise le Verrouillage de l'activation, ce dernier sera activé à partir de ce moment.
- Si Localiser mon iPhone est désactivé lorsque votre solution MDM autorise le Verrouillage de l'activation, ce dernier sera activé la prochaine fois où l'utilisateur activera Localiser mon iPhone.

Synthèse

La structure de gestion iOS vous offre le meilleur des deux mondes : l'équipe informatique peut configurer, gérer et sécuriser les appareils ainsi que contrôler les données d'entreprise y circulant, tandis que les utilisateurs ont la possibilité d'améliorer leurs performances en travaillant sur des appareils qu'ils adorent.