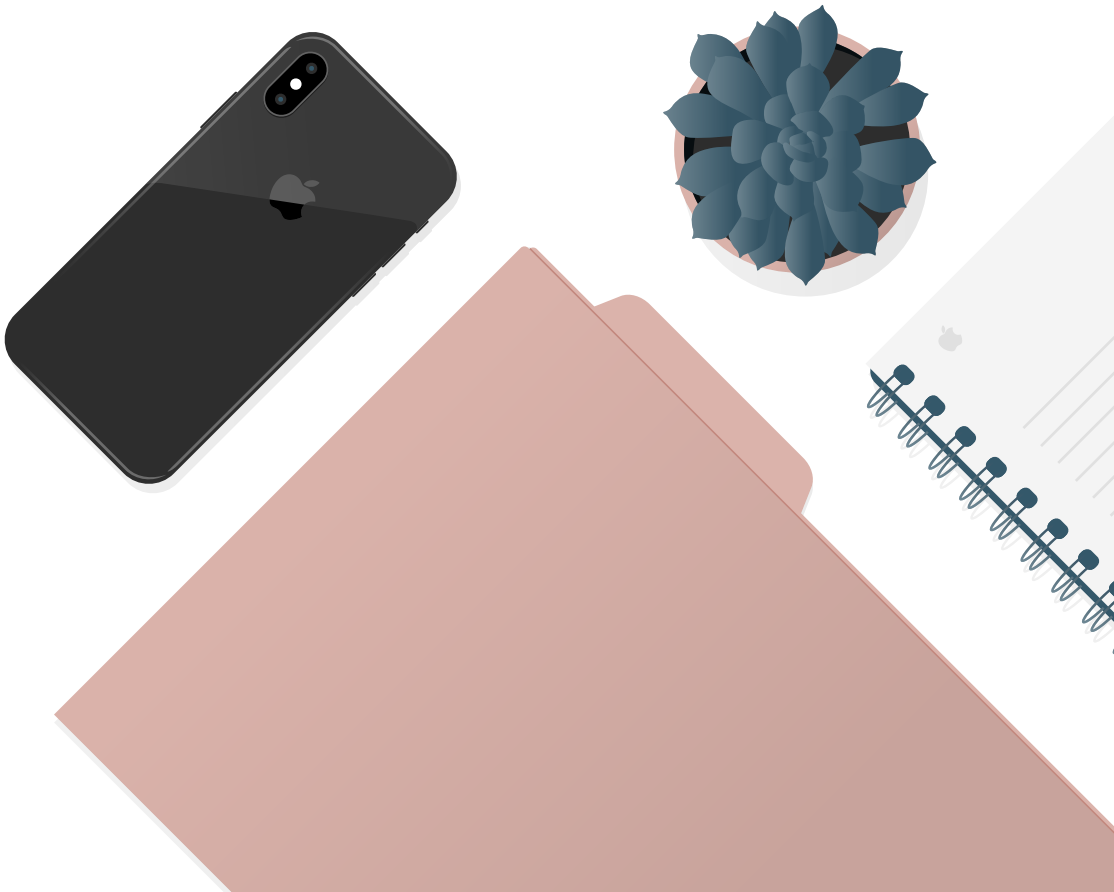
Guide de démarrage

Gestion d’appareils et de données d’entreprise sous iOS



Aperçu

Contenu

Partout dans le monde, des entreprises autonomisent leurs employés avec iPhone et iPad.

Une stratégie mobile efficace repose sur l'atteinte d'un équilibre entre le contrôle des TI et l'indépendance des utilisateurs. En personnalisant les appareils iOS avec leurs propres apps et contenus, les utilisateurs augmentent leur degré d'implication et de responsabilité et, par la même occasion, leur engagement et leur productivité. Le cadre de gestion d'Apple favorise cette personnalisation en proposant des moyens ingénieux de gérer discrètement les données et apps d'entreprise, et en séparant les données personnelles des données professionnelles. Et comme le processus de gestion des appareils est facile à comprendre, les utilisateurs n'ont aucun doute quant à la protection de leur vie privée.

Ce document renferme des indications sur la façon d'assurer un contrôle efficace des TI tout en autonomisant les utilisateurs à l'aide d'outils de travail optimaux. Il sert de complément au guide Référence pour le déploiement iOS, une ressource web complète sur la mise en service et la gestion d'appareils iOS en entreprise.

Pour consulter le guide Référence pour le déploiement iOS, visitez help.apple.com/deployment/ios/?lang=fr-ca.

Bases de la gestion

iOS simplifie le déploiement d'iPhone et d'iPad grâce à une gamme de fonctions intégrées qui facilitent la configuration des comptes, l'établissement de règles, la distribution d'apps et l'application de restrictions, le tout à distance.

Notre stratégie de gestion

Le processus de gestion des appareils iOS repose sur le cadre de gestion d'Apple. Comme ce dernier est intégré à iOS, les entreprises peuvent exécuter des tâches ciblées plutôt que de verrouiller ou de désactiver des fonctionnalités. Ainsi, à l'aide de solutions tierces de gestion des appareils mobiles, ou GAM, vous pouvez gérer avec précision vos appareils, apps et données. Et surtout, vous disposez du contrôle nécessaire sans compromettre l'expérience utilisateur ou la vie privée de vos employés.

D'autres termes, comme « gestion de la mobilité d'entreprise » (ou EMM) et « gestion des applications mobiles » (ou MAM), sont employés pour désigner les fonctionnalités de GAM sur le marché. Peu importe leur appellation, ces solutions partagent le même objectif : permettre la gestion à distance des apps et des données de votre entreprise. Et comme le cadre de gestion d'Apple est intégré à iOS, vous n'avez pas besoin d'agent logiciel distinct provenant de votre fournisseur de solution de GAM.

Séparation des données professionnelles et personnelles

Que votre organisation prenne en charge ses propres appareils ou ceux des employés, vous pouvez atteindre vos objectifs en matière de gestion des TI tout en veillant à la productivité des utilisateurs. Les données professionnelles et personnelles sont gérées séparément, sans segmentation de l'expérience utilisateur. Ainsi, les apps de productivité populaires peuvent cohabiter avec vos apps d'entreprise sur les appareils des utilisateurs, pour une liberté de travail accrue. iOS y parvient sans recourir à des solutions tierces, par exemple des conteneurs, qui détériorent l'expérience utilisateur et engendrent des frustrations.

Explication des différents modèles de gestion

Les conteneurs servent généralement à résoudre les problèmes propres à d'autres plateformes, qui ne touchent pas les appareils iOS. Certains appliquent une stratégie à double profil, qui crée deux environnements distincts sur un même appareil. D'autres conteneurisent les apps à l'aide d'une intégration fondée sur le code ou de solutions d'encapsulation. Toutes ces méthodes représentent des obstacles à la productivité. Par exemple, elles peuvent nécessiter une connexion à plusieurs espaces de travail, ou encore ajouter une dépendance à un code propriétaire – et ainsi causer une incompatibilité entre les apps et les mises à jour du système d'exploitation.

Les entreprises qui ont renoncé aux conteneurs remarquent que les contrôles de gestion natifs d'iOS favorisent la productivité des employés en optimisant leur expérience personnelle. Ainsi, plutôt que de compliquer la tâche aux personnes qui utilisent leurs appareils à des fins professionnelles et personnelles, vous pouvez appliquer des contrôles de règles qui gèrent le flux de données avec discrétion et transparence.

Gestion des données d'entreprise

Avec iOS, il n'est plus nécessaire de verrouiller vos appareils. Des technologies clés contrôlent le flux de données d'entreprise entre les apps, et préviennent tout transfert dans les apps personnelles ou les services infonuagiques des utilisateurs.

Contenu géré
Le contenu géré comprend l'installation, la configuration, la gestion et la suppression d'apps de l'App Store et d'apps maison, de même que de comptes, de livres et de domaines.

- **Apps gérées.** Les apps installées à l'aide d'une solution de GAM sont appelées « apps gérées ». Qu'il s'agisse d'apps gratuites ou payantes de l'App Store ou encore d'apps maison, elles peuvent toutes être installées à distance avec une solution de GAM. En général, elles contiennent des renseignements confidentiels et permettent un contrôle plus étroit que les apps téléchargées par les utilisateurs. Le serveur de GAM peut supprimer sur demande les apps gérées et leurs données, ou spécifier les apps à désinstaller si le profil de GAM est supprimé. Il peut aussi empêcher la sauvegarde sur iTunes et iCloud des données des apps gérées.
- **Comptes gérés.** La GAM peut aider vos utilisateurs à être rapidement opérationnels en configurant automatiquement leur messagerie et d'autres comptes. Selon le fournisseur de la GAM et l'intégration de celle-ci à vos systèmes internes, les champs de données des comptes peuvent aussi être préremplis avec le nom de l'utilisateur, son adresse courriel et, s'il y a lieu, les identités de certificat pour l'authentification et la signature. La GAM permet de configurer les types de comptes suivants : IMAP/POP, CalDAV, calendriers par abonnement, CardDAV, Exchange ActiveSync et LDAP.
- **Livres gérés.** La GAM pousse automatiquement les livres électroniques et les documents ePub et PDF vers les appareils des utilisateurs, qui disposent ainsi d'un accès constant au matériel nécessaire. Les livres gérés ne peuvent être partagés qu'avec des apps gérées ou transmis par courriel à partir de comptes gérés. Quand ils ne servent plus, tous ces contenus peuvent être retirés à distance.
- **Domaines gérés.** Les téléchargements de Safari sont considérés comme des documents gérés s'ils proviennent d'un domaine géré. Il est possible de gérer des URL et des sous-domaines précis. Par exemple, quand un utilisateur télécharge un PDF dans un domaine géré, celui-ci exige que tous les réglages du PDF soient conformes à ceux d'un document géré. Les chemins empruntés par le domaine sont gérés par défaut.

Distribution gérée

La distribution gérée vous permet d'utiliser votre solution de GAM ou Apple Configurator 2 pour gérer les apps et les livres achetés par l'entremise du Programme de licences multipostes (PLM). Pour l'activer, vous devez lier votre solution de GAM à votre compte du PLM à l'aide d'un jeton sécurisé. Par la suite, des apps peuvent être assignées directement à un appareil, sans saisie d'un identifiant Apple par l'utilisateur. Celui-ci est avisé lorsque des apps sont prêtes à être installées sur son appareil. Dans le cas d'un appareil supervisé, les apps y sont poussées sans que l'utilisateur en soit informé.

Avec une solution de GAM, vous pouvez assigner les apps directement aux appareils pour en garder le plein contrôle.

Configuration des apps gérées

Avec la configuration des apps gérées, la solution de GAM se sert du cadre de gestion natif d'iOS pour configurer les apps pendant et après le déploiement. Ce cadre permet aux développeurs de déterminer les paramètres qui s'appliquent quand leur app est installée en tant qu'application gérée. Les employés peuvent immédiatement utiliser les apps ainsi configurées, sans devoir personnaliser les réglages. Les spécialistes des TI, eux, ont la certitude que les données d'entreprise contenues dans les apps sont en sécurité, sans qu'aucune solution d'encapsulation d'apps ni trousse SDK d'entreprise ne soit nécessaire.

Certaines fonctionnalités accessibles aux développeurs peuvent être activées avec la configuration des apps gérées. Il est notamment possible de régler les paramètres des apps, d'empêcher leur sauvegarde, de désactiver la saisie d'écran et d'effacer des apps à distance.

L'AppConfig Community propose des outils et des pratiques exemplaires mettant à profit les fonctionnalités natives des systèmes d'exploitation mobiles. Les principaux fournisseurs de solutions de GAM de ce groupe ont établi un schéma standard sur lequel les développeurs peuvent s'appuyer pour la configuration des apps gérées. En proposant une façon uniforme, ouverte et simple de configurer et de sécuriser les apps mobiles, le groupe contribue à renforcer l'adoption de la mobilité en entreprise.

Pour en savoir plus sur l'AppConfig Community, visitez le www.appconfig.org.

Flux de données gérés

Les solutions de GAM comprennent des fonctionnalités servant à gérer les données d'entreprise avec précision, de manière à prévenir tout transfert dans les apps ou les services infonuagiques personnels des utilisateurs.

Pour protéger vos données d'entreprise, seules les apps installées et gérées par une solution de GAM peuvent ouvrir ce document de travail.

- **Autorisations d'ouverture gérées.** Cette fonctionnalité fait appel à un ensemble de restrictions qui empêchent les pièces jointes ou les documents provenant de sources gérées d'être ouverts à partir d'une destination non gérée, et vice-versa.

  Par exemple, vous pouvez empêcher les pièces jointes confidentielles liées à un compte de messagerie géré de s'ouvrir dans les apps personnelles de l'utilisateur. Seules les apps installées et gérées par la GAM peuvent ouvrir ce document, et 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, des comptes, des livres et des domaines gérés, plusieurs extensions sont soumises aux restrictions des autorisations d'ouverture gérées.

  Extensions gérées. Les extensions d'apps offrent aux développeurs tiers un moyen de fournir des fonctionnalités à d'autres apps et même à des systèmes clés intégrés à iOS, comme le Centre de notifications, et d'établir ainsi de nouveaux flux de travail entre les applications. Les autorisations d'ouverture gérées empêchent les extensions non gérées d'interagir avec les apps gérées. Voici différents exemples d'extensions :

  – **Les extensions qui fournissent des documents (Document Provider)** permettent aux apps de productivité d'ouvrir des fichiers à partir de plusieurs services infonuagiques sans créer de copies inutiles.

  – **Les extensions d'action (Action)** permettent aux utilisateurs de manipuler ou d'afficher du contenu dans le contexte d'une autre app. Par exemple, une action peut servir à traduire du texte directement dans Safari.

  – **Les extensions de clavier personnalisé (Custom Keyboard)** permettent d'utiliser d'autres claviers que ceux intégrés à iOS. Les autorisations d'ouverture gérées peuvent empêcher les claviers non autorisés de s'afficher dans vos apps d'entreprise.

– **Les extensions de l'affichage Aujourd'hui (Today),** aussi appelées « widgets », fournissent un résumé d'information dans l'affichage Aujourd'hui du Centre de notifications. Les utilisateurs ont ainsi accès à des renseignements à jour en un coup d'œil, et peuvent en savoir plus en lançant l'app complète grâce à des interactions simplifiées.

– **Les extensions de partage (Share)** offrent aux utilisateurs un moyen pratique de partager du contenu avec d'autres entités, comme des sites de partage social ou des services de téléversement. Par exemple, dans une app dotée d'un bouton de partage, l'utilisateur peut sélectionner l'extension se rapportant à un site de partage social, puis l'utiliser pour publier un commentaire ou du contenu.

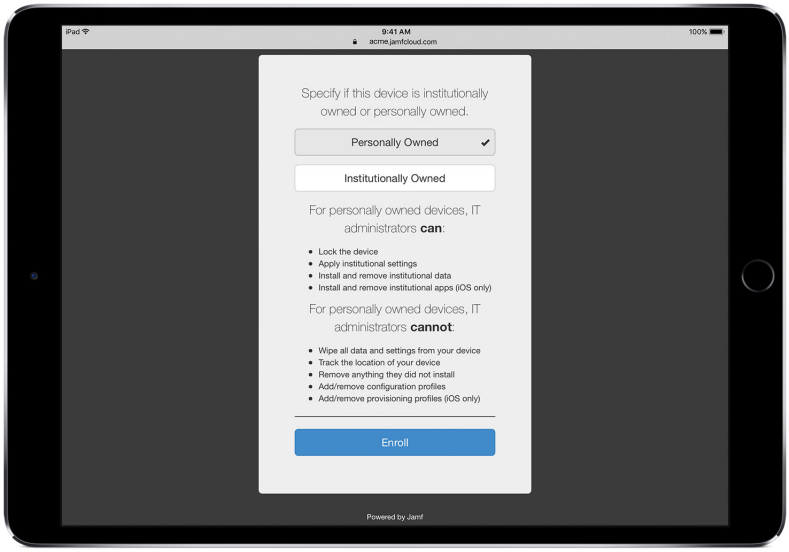
Options de gestion flexibles

Le cadre de gestion d'Apple est polyvalent et propose une approche de gestion équilibrée, tant pour les appareils des utilisateurs que pour ceux de l'entreprise. Lorsque vous choisissez une solution de GAM tierce sous iOS, vos options sont aussi nombreuses que variées, qu'il s'agisse d'appliquer une méthodologie très ouverte ou d'assurer un contrôle aussi précis que nécessaire.

Modèles de déploiement

La façon dont vous gérez les appareils et les apps variera en fonction du modèle – ou des modèles – de déploiement en vigueur dans votre organisation. Il existe généralement deux modèles possibles en entreprise : les appareils appartiennent aux utilisateurs, ou bien ils sont fournis par l'entreprise.

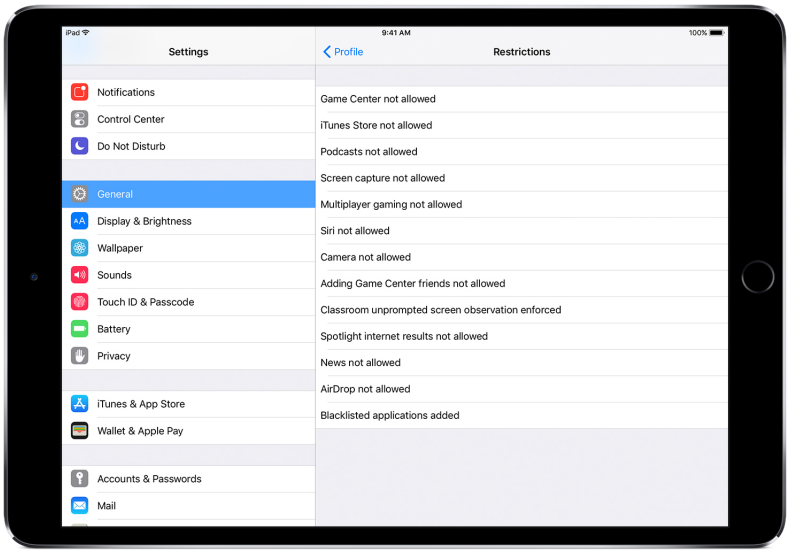
Appareils des utilisateurs
Dans ce type de déploiement, iOS offre une configuration personnalisée par l'utilisateur et une transparence complète quant au paramétrage de l'appareil, avec la garantie que l'entreprise n'accédera pas aux données personnelles.



Les solutions de GAM tierces proposent généralement une interface conviviale pour inciter les employés à s'inscrire le moment venu*.

* L'image de l'écran est une gracieuseté de Jamf.

- **Inscription et désinscription.** Dans le cas d'appareils achetés et configurés par les utilisateurs, il demeure possible d'autoriser l'accès aux services de l'entreprise, comme le Wi-Fi, la messagerie et les calendriers. Les utilisateurs n'ont qu'à s'inscrire à la GAM. Lorsqu'ils accèdent pour la première fois à la GAM sur un appareil iOS, ils sont informés des données auxquelles le serveur de GAM peut accéder et des fonctionnalités qui seront configurées par ce dernier. Cette transparence renforce le lien de confiance entre les utilisateurs et l'entreprise. Prenez soin d'informer les utilisateurs qu'à tout moment, s'ils ne sont pas à l'aise avec ce type de gestion, ils peuvent se désinscrire en supprimant le profil de gestion de leur appareil. Dans ce cas, tous les comptes d'entreprise et toutes les apps installées par la GAM seront supprimés.
- **Transparence accrue.** Une fois inscrits à la GAM, les employés peuvent facilement voir dans Réglages leurs apps, livres et comptes gérés, ainsi que les restrictions qui s'y appliquent. Tous les réglages, comptes et contenus d'entreprise installés avec une solution de GAM sont définis comme étant « gérés ».



L'interface de configuration des profils dans Réglages montre aux utilisateurs tout ce qui a été configuré sur leur appareil.

- **Vie privée des utilisateurs.** Un serveur de GAM permet d'interagir avec les appareils iOS, sans pour autant donner accès à tous les réglages et renseignements de compte. Vous pouvez gérer les comptes, réglages et renseignements d'entreprise fournis par la GAM, mais les comptes personnels des utilisateurs demeurent inaccessibles. En fait, les fonctionnalités qui sécurisent les données des apps gérées par l'entreprise empêchent aussi la diffusion des contenus personnels dans le flux de données de l'entreprise.

  Voici des exemples de données auxquelles un serveur de GAM tiers peut ou ne peut pas accéder sur les appareils iOS personnels.

Éléments accessibles :

Nom de l'appareil

Numéro de téléphone

Numéro de série

Nom et numéro de modèle

Capacité et espace disponible

Numéro de version iOS

Apps installées

Exemples de données personnelles inaccessibles :

Courriels, calendriers et contacts personnels ou professionnels

Textos et iMessages

Historique de Safari

Registre des appels téléphoniques et FaceTime

Notes et rappels personnels

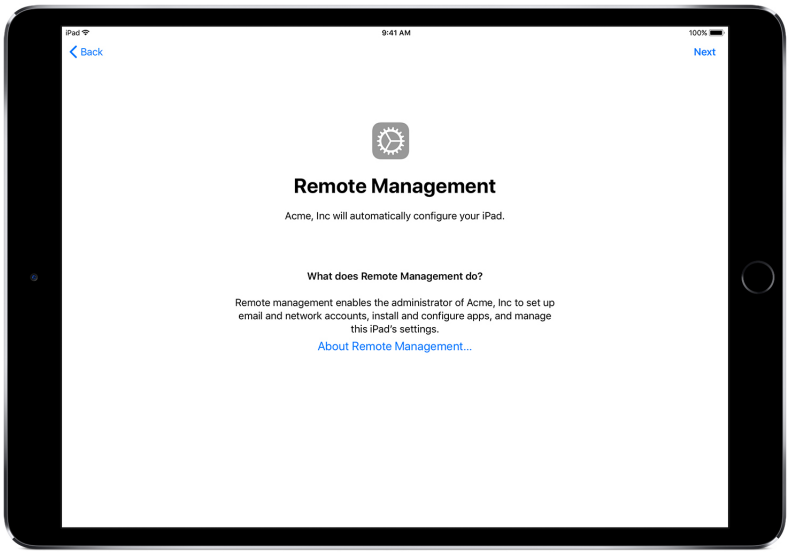
Fréquence d'utilisation des apps

Localisation de l'appareil

- **Personnalisation des appareils.** Bon nombre d'entreprises constatent que les utilisateurs, quand ils peuvent personnaliser les appareils avec leur propre identifiant Apple, ont un plus grand sentiment d'appropriation et de responsabilité. Ils sont également plus productifs, car ils peuvent eux-mêmes choisir les apps et les contenus qui leur seront les plus utiles au travail.

Appareils de l'organisation

Dans le cas d'un déploiement d'appareils appartenant à l'entreprise, les utilisateurs reçoivent chacun un appareil (déploiement sur appareils individuels) ou se partagent des appareils (déploiement sur appareils partagés). Les fonctionnalités iOS telles que l'inscription automatisée, les paramètres de GAM verrouillables, la supervision d'appareils et le RPV permanent vous assurent que les appareils sont configurés selon les exigences de votre entreprise. Vous profitez ainsi d'un contrôle accru, tout en ayant la garantie que vos données sont protégées.



Avec le Programme d'inscription des appareils (PIA), votre solution de GAM configure automatiquement vos appareils iOS à l'étape de l'Assistant réglages.

- **Inscription automatisée.** Le PIA vous permet d'automatiser l'inscription à la GAM des iPhone, iPad et Mac appartenant à votre organisation pendant leur configuration initiale. Vous pouvez rendre l'inscription obligatoire et irrévocable. Vous pouvez même régler les appareils en mode supervisé au moment de l'inscription et autoriser les utilisateurs à sauter certaines étapes de configuration de base.

- **Appareils supervisés.** La supervision offre des possibilités supplémentaires pour gérer les appareils iOS de votre entreprise. Il est notamment possible d'activer un filtre web via un serveur mandataire pour que la navigation se limite au réseau de l'organisation, ou d'empêcher les utilisateurs de rétablir les réglages d'origine de leur appareil. Par défaut, les appareils iOS ne sont pas supervisés. Vous pouvez activer la supervision automatiquement avec le PIA, ou manuellement à l'aide d'Apple Configurator 2.

Même si vous ne pensez pas utiliser les fonctions propres au mode supervisé dans l'immédiat, songez-y lors de la configuration de vos appareils, car elles pourraient vous servir plus tard. Autrement, pour les ajouter, vous devrez effacer le contenu des appareils déjà déployés. Le but de la supervision n'est pas de verrouiller les appareils, mais d'élargir les capacités de gestion pour rendre les appareils de l'entreprise encore plus performants. Et à long terme, la supervision a encore plus d'options à offrir à votre entreprise.

Pour une liste exhaustive des réglages supervisés, consultez le guide 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 organisation, sans gêner les utilisateurs :

- AirPrint
- Installation d'apps
- Utilisation d'apps
- App En classe
- Appareil
- iCloud
- Gestionnaire de profils pour utilisateurs et groupes d'utilisateurs
- Safari
- Réglages de confidentialité et de sécurité
- Siri

Les catégories suivantes comportent aussi des éléments configurables avec votre solution de GAM :

- Paramètres d'inscription automatique à la solution de GAM
- Écrans de l'Assistant réglages

Fonctions de gestion supplémentaires

Interrogation d'appareils
En plus de configurer les appareils, le serveur de GAM peut les interroger pour obtenir divers renseignements sur les appareils eux-mêmes, le réseau, les applications et les données de conformité et de sécurité. Ces informations permettent de s'assurer que les appareils demeurent conformes aux politiques en vigueur. Le serveur de GAM détermine la fréquence à laquelle il recueille des données.

Voici quelques exemples d'informations pouvant être demandées à un appareil iOS :

- Renseignements sur l'appareil (nom)
- Modèle, version d'iOS, numéro de série
- Information sur le réseau

- Statut d'itinérance, adresses MAC
- Applications installées
- Nom, version et taille de l'app
- Données de conformité et de sécurité
- Réglages, politiques et certificats installés
- État du chiffrement

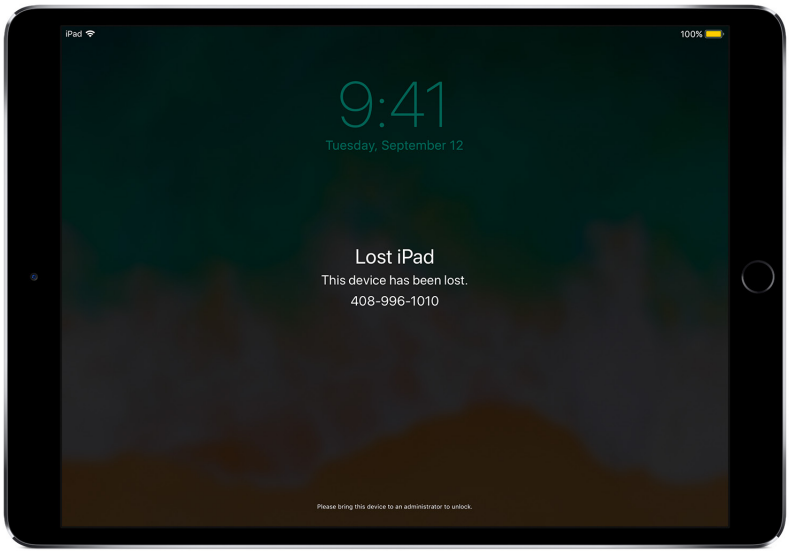
Tâches de gestion
Le serveur de GAM peut effectuer un vaste éventail de tâches administratives sur les appareils gérés, comme modifier les réglages de configuration sans intervention de l'utilisateur, faire la mise à jour d'iOS sur un appareil protégé par un mot de passe, bloquer ou effacer un appareil à distance, ou supprimer le code de sécurité pour permettre à un utilisateur de réinitialiser son mot de passe. Le serveur de GAM peut aussi demander à un appareil iOS de lancer la recopie vidéo AirPlay vers une destination précise, ou de l'interrompre.

Mode Perdu
Sous iOS 9.3 ou une version ultérieure, votre solution de GAM peut activer à distance le mode Perdu sur un appareil supervisé.

Ce mode verrouille l'appareil à distance et permet d'afficher un message et un numéro de téléphone sur l'écran verrouillé.

Grâce au mode Perdu, la GAM peut localiser un appareil supervisé perdu ou volé en produisant une requête visant à repérer l'endroit où il se trouvait la dernière fois qu'il était en ligne. Il n'est pas nécessaire d'activer la fonction Localiser mon iPhone pour utiliser le mode Perdu.

Si la GAM désactive à distance le mode Perdu, l'appareil se déverrouille, et ses données de localisation sont recueillies. Par souci de transparence, l'utilisateur est avisé que le mode Perdu a été désactivé.



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

Verrouillage d'activation
iOS 7.1 et les versions ultérieures permettent d'utiliser une solution de GAM pour activer le verrouillage d'activation lorsqu'un utilisateur se sert de Localiser mon iPhone sur un appareil supervisé. Ainsi, votre entreprise peut profiter de l'aspect antivol du verrouillage d'activation tout en conservant la possibilité de contourner cette fonctionnalité si, par exemple, un utilisateur quitte votre entreprise sans l'avoir préalablement désactivée avec son identifiant Apple.

Votre solution de GAM peut récupérer un code de contournement et permettre à l'utilisateur d'activer le verrouillage d'activation sur son appareil selon les conditions suivantes :

- Si la fonction Localiser mon iPhone est activée quand votre solution de GAM autorise le verrouillage d'activation, la fonctionnalité est mise en marche.
- Si la fonction Localiser mon iPhone n'est pas activée quand votre solution de GAM autorise le verrouillage d'activation, la fonctionnalité sera mise en marche la prochaine fois que l'utilisateur activera Localiser mon iPhone.

Conclusion

Le cadre de gestion d'iOS vous offre le meilleur des deux mondes. Grâce à lui, les TI peuvent configurer, gérer et sécuriser les appareils, en plus de contrôler le flux des données d'entreprise qui y transitent, et les utilisateurs réussissent à travailler encore mieux avec leurs appareils.