



Aperçu du déploiement d'iOS et d'iPadOS

Table des matières

[Introduction](#)

[Modèles de déploiement](#)

[Étapes de déploiement](#)

[Options d'assistance](#)

[Conclusion](#)

Introduction

iPhone et iPad peuvent transformer votre entreprise et vos façons de faire. Ils favorisent grandement la productivité en donnant aux employés la liberté et les moyens de travailler autrement, au bureau comme à l'extérieur. Et ces outils modernes sont avantageux pour l'ensemble de l'entreprise. D'une part, en ayant un meilleur accès à l'information, les utilisateurs sont plus autonomes et peuvent trouver des solutions créatives à leurs problèmes.

D'autre part, en adoptant iOS et iPadOS, les services des TI montrent qu'ils façonnent la stratégie d'affaires et règlent des difficultés concrètes, plutôt que de s'en tenir au dépannage et à la réduction des coûts. Bref, tout le monde y gagne : l'équipe est motivée, et les occasions d'affaires se multiplient.

Configurer et déployer iPhone et iPad est plus facile que jamais. Avec Apple Business Manager et une solution de gestion des appareils mobiles (GAM) tierce, vous pouvez facilement implanter des apps et des appareils iOS et iPadOS à l'échelle de votre entreprise.

- La GAM vous aide à configurer et gérer les appareils, de même qu'à distribuer et gérer les apps à distance.
- Apple Business Manager automatise l'inscription de vos appareils Apple dans votre système de GAM et facilite leur déploiement – sans intervention de l'équipe des TI.
- Apple Business Manager facilite aussi l'achat d'apps et de livres en gros ainsi que la distribution sans fil aux utilisateurs.
- Apple Business Manager vous permet en outre de créer des identifiants Apple gérés pour les employés et d'utiliser l'authentification fédérée avec Microsoft Azure AD.

Ce document explique comment déployer des appareils iOS et iPadOS dans votre entreprise et vous aide à créer un plan de déploiement adapté à votre réalité. Les sujets abordés ici sont expliqués plus en détail dans le document de référence pour le déploiement d'iPhone et iPad* :

support.apple.com/guide/deployment-reference-ios

* En anglais seulement.

Modèles de déploiement

Avant le déploiement, il est important d'évaluer les modèles offerts et de choisir celui qui convient à votre entreprise. Il existe plusieurs approches, selon le modèle mis en œuvre. Commencez par cerner ce qui profiterait le plus à votre organisation.

Les entreprises utilisent généralement deux modèles de déploiement pour les appareils iOS et iPadOS :

- Appareils appartenant à l'organisation
- Appareils appartenant aux utilisateurs

Bien que la plupart des entreprises optent pour un seul modèle, il est possible d'en utiliser plusieurs. Par exemple, dans ses bureaux, une entreprise pourrait déployer un programme où les employés apportent et configurent leur propre iPad. Elle protégerait et gérerait ses ressources, sans toucher aux données et aux apps des utilisateurs. Et dans ses magasins, la même entreprise opérerait pour des appareils lui appartenant. Les employés se partageraient des appareils iOS servant à traiter les transactions.

Familiarisez-vous avec ces modèles de déploiement pour déterminer celui qui convient le mieux à votre environnement. Quand vous aurez fait votre choix, votre équipe pourra explorer en détail les fonctionnalités de gestion et de déploiement d'Apple.

Appareils appartenant à l'entreprise

Avec ce type de déploiement, vous pouvez attribuer des appareils aux employés pour leur travail quotidien, les partager entre plusieurs personnes pour des tâches communes, ou encore les configurer pour limiter leur utilisation à une seule app. Si les appareils attribués à une personne en particulier peuvent être personnalisés par l'utilisateur final, ce n'est généralement pas le cas pour les appareils réservés à une fonction précise ou partagés entre plusieurs utilisateurs. En combinant ces modèles, des technologies clés fournies par Apple et une solution de GAM, vous pouvez complètement automatiser la configuration des appareils.

Appareils individuels. En optant pour une activation individuelle, vous pouvez demander à chaque utilisateur de choisir son appareil et de l'inscrire à votre solution de GAM, qui fournit sans fil les apps et réglages de l'entreprise. Et si vous achetez vos appareils auprès d'Apple, d'un fournisseur de services ou d'un revendeur agréé Apple participant, vous pouvez tirer parti d'Apple Business Manager pour inscrire automatiquement vos nouveaux appareils à la GAM. C'est ce qu'on appelle l'inscription automatisée des appareils. Une fois les appareils configurés, les utilisateurs peuvent y ajouter leurs propres apps et données, en plus des comptes ou des apps fournis par l'entreprise.

Appareils partagés. Habituellement, quand les appareils sont partagés entre plusieurs personnes ou réservés à un usage unique (par exemple, dans un restaurant ou un hôtel), les administrateurs des TI les configurent et les gèrent de manière centralisée plutôt que de confier ces tâches aux utilisateurs. Dans le cadre d'un déploiement de ce type, les utilisateurs n'ont généralement pas la permission d'installer des apps ou d'enregistrer des données personnelles. L'inscription automatisée des appareils via Apple Business Manager permet aussi d'automatiser la configuration des appareils partagés. Le tableau ci-dessous présente les responsabilités des administrateurs et des utilisateurs à chaque étape d'un déploiement d'appareils appartenant à l'organisation. Sauf indication contraire, elles s'appliquent autant aux *appareils individuels* qu'aux *appareils partagés*.

| | Administrateur | Utilisateur |
|----------------------|--|--|
| Préparation | <ul style="list-style-type: none"> Évaluation de l'infrastructure Choix d'une solution de GAM Adhésion à Apple Business Manager | <ul style="list-style-type: none"> Aucune action requise |
| Configuration | <ul style="list-style-type: none"> Configuration des appareils Distribution d'apps et de livres | <ul style="list-style-type: none"> Aucune action requise |
| Déploiement | <ul style="list-style-type: none"> Distribution des appareils <p>Appareils individuels seulement</p> <ul style="list-style-type: none"> Autorisation de personnalisation par les utilisateurs | <p>Appareils individuels seulement</p> <ul style="list-style-type: none"> Téléchargement et installation des apps et des livres Utilisation de l'identifiant Apple ainsi que des comptes App Store et iCloud, le cas échéant <p>Appareils partagés seulement</p> <ul style="list-style-type: none"> Aucune action requise |
| Gestion | <ul style="list-style-type: none"> Gestion des appareils Déploiement et gestion de contenus supplémentaires | <p>Appareils individuels seulement</p> <ul style="list-style-type: none"> Découverte d'autres apps à utiliser <p>Appareils partagés seulement</p> <ul style="list-style-type: none"> Aucune action requise |

Appareils appartenant aux utilisateurs

Quand les appareils sont achetés et configurés par les utilisateurs (modèle de type « Apportez votre appareil »), vous pouvez quand même utiliser la GAM pour autoriser l'accès aux services de l'entreprise, comme le Wi-Fi, la messagerie et les calendriers, grâce à la nouvelle fonctionnalité d'inscription par l'utilisateur sous iOS 13 et iPadOS.

Ce type de déploiement permet aux utilisateurs de configurer leur appareil personnel. Ils peuvent l'inscrire à la solution de GAM pour accéder aux ressources de l'organisation, modifier différents réglages, installer un profil de configuration ou installer des apps d'entreprise. Dans ce cas, les utilisateurs doivent s'inscrire eux-mêmes à la solution de GAM de l'entreprise.

L'inscription par l'utilisateur permet de gérer les ressources et les données de l'entreprise de façon sécuritaire, sans aucune incidence sur les contenus et les renseignements personnels de l'employé. Ainsi, le service des TI peut appliquer certains réglages, surveiller le respect des politiques et supprimer des données et apps d'entreprise, tandis que les apps et données personnelles présentes sur les appareils restent intactes.

L'inscription par l'utilisateur comprend les éléments suivants :

- **Identifiant Apple géré.** L'identifiant Apple géré permet de définir l'identité d'un utilisateur sur un appareil et de fournir l'accès aux services Apple. Il peut être utilisé de pair avec l'identifiant Apple personnel dont l'utilisateur s'est servi pour se connecter. D'abord créé dans Apple Business Manager, l'identifiant Apple géré est ensuite envoyé à Microsoft Azure Active Directory via l'authentification fédérée.
- **Séparation des données.** Lors de l'inscription par l'utilisateur, un volume APFS distinct est créé pour les données, les apps et les comptes gérés sur l'appareil. Ce volume géré est séparé de manière cryptographique du reste de l'appareil.
- **Gestion sur mesure pour le déploiement d'appareils appartenant aux utilisateurs.** L'inscription par l'utilisateur a été conçue pour les appareils personnels, de manière à pouvoir confier aux TI la gestion d'un sous-ensemble de configurations et de politiques tout en empêchant l'exécution de certaines tâches comme l'effacement d'un appareil à distance ou la collecte de renseignements personnels.

Le tableau ci-dessous présente les responsabilités des administrateurs et des utilisateurs à chaque étape d'un déploiement d'appareils personnels.

| | Administrateur | Utilisateur |
|--------------------|--|---|
| Préparation | <ul style="list-style-type: none"> • Évaluation de l'infrastructure • Choix d'une solution de GAM • Adhésion à Apple Business Manager | <ul style="list-style-type: none"> • Utilisation de l'identifiant Apple personnel et de l'identifiant Apple géré ainsi que des comptes App Store et iCloud, le cas échéant |
| Préparation | <ul style="list-style-type: none"> • Configuration des réglages • Distribution d'apps et de livres | <ul style="list-style-type: none"> • Inscription à la solution de GAM de l'entreprise • Téléchargement et installation des apps et des livres |
| Déploiement | <ul style="list-style-type: none"> • Aucune action requise | <ul style="list-style-type: none"> • Aucune action requise |
| Gestion | <ul style="list-style-type: none"> • Gestion des appareils • Déploiement et gestion de contenus supplémentaires | <ul style="list-style-type: none"> • Découverte d'autres apps à utiliser |

Pour en savoir plus sur l'inscription par l'utilisateur : support.apple.com/guide/mdm

Pour en savoir plus sur l'authentification fédérée : support.apple.com/guide/apple-business-manager

Étapes de déploiement

Cette section aborde plus en détail les quatre étapes du déploiement d'appareils et de contenus : la préparation de l'environnement, la configuration des appareils, le déploiement et la gestion. Les étapes à suivre changent selon que les appareils appartiennent à l'organisation ou aux utilisateurs.

1. Préparation

Une fois que vous savez quel modèle convient à votre entreprise, suivez les étapes ci-dessous pour préparer le déploiement. Vous pouvez entamer le processus avant même d'avoir reçu les appareils.

Évaluer l'infrastructure

iPhone et iPad s'intègrent naturellement à l'environnement informatique de la plupart des entreprises. Il est important d'évaluer l'infrastructure actuelle de votre réseau pour vous assurer que votre organisation tire pleinement parti de tous les avantages d'iOS et d'iPadOS.

Wi-Fi et réseautique

Une connexion sans fil fiable et constante est nécessaire à l'installation et à la configuration d'appareils iOS et iPadOS. Vérifiez que le réseau Wi-Fi de votre entreprise peut prendre en charge plusieurs appareils et offrir la connexion simultanée à tous vos utilisateurs. Vous devrez peut-être reconfigurer vos serveurs mandataires ou pare-feu si des appareils ne peuvent accéder aux serveurs d'activation d'Apple, à iCloud ou à l'App Store. De plus, Apple et Cisco ont optimisé les méthodes de communication d'iPhone et d'iPad sur les réseaux sans fil Cisco. D'autres fonctionnalités réseau avancées peuvent ainsi être mises en place, comme l'itinérance rapide et l'optimisation de la qualité de service (QS) des apps.

Évaluez votre infrastructure VPN afin que les utilisateurs puissent accéder à leurs ressources de travail à distance de façon sécurisée sur leurs appareils iOS et iPadOS. Pensez à utiliser le VPN sur demande ou le VPN par app d'iOS et d'iPadOS pour que la connexion à un réseau privé virtuel ne soit activée qu'au besoin. Si vous prévoyez utiliser le VPN par app, vérifiez que vos passerelles VPN prennent en charge cette fonctionnalité et que vous avez suffisamment de licences pour votre nombre d'utilisateurs et de connexions.

Assurez-vous également que votre infrastructure réseau est réglée pour fonctionner avec Bonjour, le protocole réseau normalisé sans configuration d'Apple. Bonjour permet aux appareils de trouver automatiquement des services sur un réseau. iOS et iPadOS l'utilisent pour se connecter aux imprimantes AirPrint et aux appareils AirPlay comme Apple TV. Et certaines apps s'en servent afin de détecter des appareils pour le partage et la collaboration.

Pour en savoir plus sur le Wi-Fi et la réseautique* :

support.apple.com/guide/deployment-reference-ios

Pour en savoir plus sur Bonjour* :

developer.apple.com/library

Courriels, contacts et calendriers

Si vous utilisez Microsoft Exchange, vérifiez que le service ActiveSync est à jour et configuré pour prendre en charge tous les utilisateurs du réseau. Et si vous avez recours à Office 365 dans le nuage, assurez-vous d'avoir suffisamment de licences pour prendre en charge le nombre prévu d'appareils iOS et iPadOS qui se connecteront à votre réseau. iOS et iPadOS sont aussi compatibles avec l'authentification moderne Office 365, qui tire parti du protocole OAuth 2.0 et de l'authentification multifactorielle. Si vous n'employez pas Exchange, iOS et iPadOS fonctionnent avec les serveurs normalisés, dont IMAP, POP, SMTP, CalDAV, CardDAV et LDAP.

Mise en cache de contenu

Le service de mise en cache, une fonctionnalité intégrée à macOS High Sierra et aux versions ultérieures, conserve une copie locale des contenus fréquemment demandés sur les serveurs Apple, et contribue ainsi à réduire la quantité de bande passante nécessaire pour les télécharger sur votre réseau. Cette fonctionnalité accélère le téléchargement et la distribution de contenus à partir de l'App Store, du Mac App Store et d'Apple Books.

Elle peut aussi mettre en cache les mises à jour logicielles pour un téléchargement plus rapide sur les appareils iOS et iPadOS. Par ailleurs, la mise en cache de contenu comprend la mise en cache connectée, qui permet à Mac de partager sa connexion Internet avec plusieurs appareils iOS et iPadOS connectés par câble USB.

Pour en savoir plus sur la mise en cache de contenu* :

support.apple.com/guide/deployment-reference-macos

Pour en savoir plus sur la mise en cache connectée :

support.apple.com/HT207523

Choisir une solution de GAM

Grâce au cadre de gestion d'Apple intégré à iOS et à iPadOS, les entreprises peuvent inscrire les appareils de façon sécurisée dans leur environnement, configurer et mettre à jour les réglages à distance, vérifier la conformité avec les politiques, distribuer des apps et des livres, et même effacer ou verrouiller à distance les appareils gérés. Ces fonctionnalités sont offertes par des solutions de GAM tierces.

* En anglais seulement.

Afin de prendre en charge les différentes plateformes de serveur, divers produits de GAM tiers sont à votre disposition. Chacun propose plusieurs types de consoles d'administration, de fonctionnalités et de structures de tarification. Avant d'arrêter votre choix, consultez les ressources ci-dessous afin de déterminer les fonctionnalités de gestion dont votre entreprise a le plus besoin. En plus des solutions de GAM tierces, Apple propose le Gestionnaire de profils, un outil intégré à macOS Server.

Pour en savoir plus sur la gestion des appareils et des données d'entreprise :
apple.com/ca/fr/business/docs/resources/Managing_Devices_and_Corporate_Data_on_iOS.pdf

Adhérer à Apple Business Manager

Apple Business Manager est un portail web qui permet aux administrateurs des TI de déployer des appareils iPhone, iPad, iPod touch, Apple TV et Mac à partir d'un seul et même endroit. Parce qu'il fonctionne main dans la main avec votre solution de GAM, il facilite le déploiement automatisé des appareils, l'achat d'apps, la distribution de contenus et la création d'identifiants Apple gérés pour les employés.

Le Programme d'inscription des appareils et le Programme de licences multipostes sont désormais parfaitement intégrés à Apple Business Manager. Ainsi, tout ce dont les entreprises ont besoin pour déployer des appareils Apple se retrouve à un seul endroit. Ces deux programmes ne seront plus disponibles après le 1^{er} décembre 2019.

Appareils

Avec la fonction d'inscription automatisée des appareils d'Apple Business Manager, les entreprises peuvent déployer les appareils Apple qui leur appartiennent et les inscrire dans leur solution de GAM facilement, rapidement et sans avoir à les manipuler ou à les préparer.

- Facilitez le processus de configuration en simplifiant les étapes dans l'Assistant réglages pour que les appareils des employés soient configurés convenablement dès leur activation. Les équipes des TI peuvent personnaliser encore plus cette expérience en présentant aux employés une entente d'utilisation, le logo de l'entreprise et des méthodes d'authentification de pointe.
- Élargissez le contrôle des appareils détenus par l'entreprise grâce à la supervision, qui comprend des options de gestion que vous ne trouverez pas dans d'autres modèles de déploiement, comme l'inscription irrévocable à la solution de GAM.
- Gérez plus facilement les serveurs de GAM en choisissant un serveur par défaut selon le type d'appareil. Et inscrivez manuellement vos iPhone, iPad et Apple TV à l'aide d'Apple Configurator 2, quelle que soit la manière dont vous les avez achetés.

Contenus

Apple Business Manager simplifie l'achat de contenus en gros pour les entreprises. Que vos employés utilisent iPhone, iPad ou Mac, équipez-les d'apps de travail géniales grâce aux options de distribution sécuritaires et flexibles.

- Achetez des apps de l'App Store, des livres et des apps sur mesure en gros, et distribuez les apps que vous avez conçues à l'interne. Transférez les licences d'app d'un établissement à l'autre et partagez-les entre plusieurs acheteurs au même endroit. Et consultez l'historique global des achats, y compris le nombre de licences actuellement utilisées avec votre solution de GAM.
- Distribuez des apps et des livres directement aux appareils gérés ou aux utilisateurs autorisés tout en suivant le fil des utilisateurs ou appareils auxquels les contenus sont assignés. Avec la distribution gérée, supervisez le processus de A à Z tout en conservant les droits de propriété sur les apps. Quand une app n'est plus utile sur un appareil ou pour un utilisateur, vous pouvez la retirer et la réattribuer à un autre appareil ou utilisateur de l'entreprise.
- Choisissez parmi divers modes de paiement, y compris la carte de crédit et les bons de commande. Les entreprises peuvent se procurer un crédit d'achat en gros (si disponible) auprès d'Apple ou d'un revendeur agréé Apple. Le crédit est établi pour un montant précis dans la devise locale et délivré par voie électronique à la personne titulaire du compte.
- Pour un déploiement international, distribuez des apps aux appareils ou utilisateurs dans tout pays où elles sont offertes. Les développeurs peuvent rendre leurs apps disponibles dans divers pays en suivant le processus de publication habituel de l'App Store.

Remarque : L'achat de livres dans Apple Business Manager n'est pas possible dans tous les pays. Pour savoir quels programmes et modes de paiement sont disponibles dans votre région, visitez support.apple.com/HT207305.

Utilisateurs

Avec Apple Business Manager, les entreprises peuvent créer et gérer des comptes qui s'intègrent à leur infrastructure pour permettre aux employés d'accéder aux apps et aux services Apple ainsi qu'à Apple Business Manager.

- Les employés se servent de leur identifiant Apple géré pour collaborer dans les apps et les services Apple, et même pour accéder aux données dont ils ont besoin dans des apps gérées compatibles avec iCloud Drive. Ces comptes sont détenus et gérés par l'entreprise.
- Grâce à l'authentification fédérée, vous pouvez lier Apple Business Manager à Microsoft Azure Active Directory. Un identifiant Apple géré sera créé automatiquement lorsque l'employé ouvrira une session sur un appareil Apple compatible à l'aide de son identifiant actuel.

- L'identifiant Apple géré peut être utilisé conjointement avec un identifiant Apple personnel sur un appareil appartenant à l'employé grâce à la nouvelle fonctionnalité d'inscription par l'utilisateur, offerte sous iOS 13, iPadOS et macOS Catalina. Il est aussi possible d'utiliser un identifiant Apple géré sur n'importe quel appareil en tant qu'identifiant Apple principal (et unique). L'identifiant Apple géré donne également accès à iCloud en ligne dès la première ouverture de session sur un appareil Apple.
- Attribuez d'autres rôles aux équipes des TI de votre entreprise pour gérer les appareils, les apps et les comptes efficacement dans Apple Business Manager. Le rôle d'administrateur permet d'accepter les modalités d'utilisation et de transférer les responsabilités facilement quand un employé quitte l'entreprise.

Remarque : À l'heure actuelle, iCloud Drive n'est pas compatible avec l'inscription par l'utilisateur. iCloud Drive peut être utilisé avec un identifiant Apple géré si aucun autre identifiant Apple n'est enregistré dans l'appareil.

Pour en savoir plus sur Apple Business Manager : apple.com/ca/fr/business/it

Adhérer au programme Apple pour développeurs en entreprise

Le programme Apple pour développeurs en entreprise (Developer Enterprise Program) offre un ensemble complet d'outils pour développer, tester et distribuer des apps. Vous pouvez distribuer les apps en les hébergeant sur un serveur web, ou en employant une solution de GAM. Et vous pouvez signer et notariser les apps et programmes d'installation Mac avec votre identifiant de développeur pour Gatekeeper, une fonctionnalité qui protège macOS des logiciels malveillants.

Pour en savoir plus sur le programme pour développeurs en entreprise* : developer.apple.com/programs/enterprise

2. Configuration

Pour configurer vos appareils et distribuer vos contenus, vous pouvez utiliser Apple Business Manager, une solution de GAM ou Apple Configurator 2. Il existe plusieurs façons d'aborder un processus de déploiement, et elles varient en fonction des propriétaires des appareils et du modèle privilégié.

Configurer les appareils

L'accès des utilisateurs aux services de l'entreprise peut être configuré de plusieurs façons. Les TI peuvent choisir de distribuer des profils de configuration. Des options supplémentaires sont disponibles pour les appareils supervisés.

* En anglais seulement.

Configuration des appareils avec la GAM

Une fois vos appareils inscrits de manière sécurisée à un serveur de GAM, la gestion est exécutée à l'aide de profils de configuration – des fichiers XML qui envoient des renseignements de configuration aux appareils iOS et iPadOS. Ces profils automatisent la configuration des réglages, des comptes, des restrictions et des renseignements d'identification. Ils peuvent être envoyés sans fil par votre solution de GAM, ce qui convient parfaitement au déploiement d'appareils multiples avec intervention minimale. Pour être ajoutés à des appareils, les profils peuvent aussi être reçus sous forme de pièce jointe dans un courriel, téléchargés depuis une page web ou installés à l'aide d'Apple Configurator 2.

- **Appareils appartenant à l'entreprise.** Utilisez Apple Business Manager pour automatiser l'inscription des appareils activés à la solution de GAM. Les appareils iOS et iPadOS ajoutés à Apple Business Manager sont supervisés en tout temps et obligatoirement inscrits à la GAM.
- **Appareils appartenant aux utilisateurs.** Les utilisateurs décident d'inscrire ou non leurs appareils à la solution de GAM. Ils peuvent se désinscrire à tout moment en supprimant le profil de configuration de leur appareil, y compris les données et réglages d'entreprise. Vous devriez toutefois penser à mettre en place des mesures encourageant les utilisateurs à rester inscrits. Vous pourriez par exemple exiger que les utilisateurs s'inscrivent à la solution de GAM pour accéder au réseau Wi-Fi en utilisant la GAM pour fournir automatiquement les identifiants de connexion.

Une fois qu'un appareil est inscrit, l'administrateur peut lui envoyer une politique, une option ou une commande de GAM; les fonctions de gestion disponibles pour un appareil en particulier varient selon la méthode d'inscription et le niveau de supervision. L'appareil iOS ou iPadOS reçoit alors une notification envoyée par le service de notification Push d'Apple afin qu'il puisse communiquer directement avec le serveur de GAM via une connexion sécurisée. Avec une connexion réseau, les appareils peuvent recevoir les commandes APN partout dans le monde. Toutefois, le service APN ne transmet pas de renseignements d'identification ni de données confidentielles.

Configuration des appareils avec Apple Configurator 2 (facultatif)

Pour un premier déploiement d'appareils multiples à l'échelle locale, les organisations peuvent utiliser Apple Configurator 2. Cette application macOS gratuite vous permet de connecter vos appareils iOS et iPadOS à un ordinateur Mac par port USB et de les faire passer à la plus récente version logicielle, de modifier leurs réglages et restrictions, et d'installer apps et autres contenus. Après la configuration initiale, toute la gestion se fait à distance à l'aide de la GAM.

L'interface utilisateur d'Apple Configurator 2 met l'accent sur vos appareils et sur les tâches précises que vous souhaitez exécuter. L'app s'intègre parfaitement à Apple Business Manager, ce qui permet l'inscription automatique d'appareils à votre solution de GAM avec vos réglages d'entreprise. Vous pouvez créer des processus personnalisés dans Apple Configurator 2 en jumelant des tâches distinctes à l'aide de Blueprints.

Pour en savoir plus sur Apple Configurator 2 :

support.apple.com/apple-configurator

Appareils supervisés

La supervision offre des possibilités supplémentaires pour gérer les appareils iOS et iPadOS appartenant à l'entreprise, y compris l'imposition de restrictions comme la désactivation d'AirDrop ou l'activation du mode App individuelle. Vous pouvez également activer un filtre de connexion web via un serveur mandataire pour vous assurer que la navigation des utilisateurs respecte les politiques de l'organisation, empêcher les utilisateurs de rétablir les réglages d'origine de leur appareil, et bien plus. Par défaut, les appareils iOS et iPadOS ne sont pas supervisés. Pour activer le mode supervision, vous pouvez recourir à Apple Business Manager ou le faire manuellement à l'aide d'Apple Configurator 2.

Même si vous n'envisagez pas d'utiliser les fonctions propres au mode supervisé dans l'immédiat, songez-y lors de la configuration de vos appareils, car elles pourraient vous profiter 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 fonctions 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 en savoir plus sur les restrictions pouvant être imposées aux appareils supervisés :

support.apple.com/guide/mdm

Distribuer des apps et des livres

Apple propose des programmes complets pour aider votre entreprise à tirer profit des apps et contenus formidables conçus pour iOS et iPadOS. Ces outils vous permettent de distribuer tant les apps et les livres achetés avec Apple Business Manager que vos apps maison, de sorte que vos utilisateurs aient tout le nécessaire pour travailler. Au moment de l'achat, vous devrez choisir votre méthode de distribution : gérée ou par codes de téléchargement.

Distribution gérée

Avec la distribution gérée, utilisez votre solution de GAM ou Apple Configurator 2 pour gérer les apps et livres achetés avec Apple Business Manager dans tout pays où ils sont offerts. Pour l'activer, vous devez lier votre solution de GAM à votre compte Apple Business Manager à l'aide d'un jeton sécurisé. Dès que c'est fait, vous pouvez attribuer des apps et des livres même si l'App Store de l'appareil est désactivé.

- **Attribuez des apps aux appareils.** Vous pouvez assigner des apps directement aux appareils avec votre système de GAM ou Apple Configurator 2. Cette méthode vous épargne plusieurs étapes lors du déploiement initial, ce qui facilite et accélère le processus tout en vous permettant de garder le plein contrôle des appareils et des contenus gérés. Lors de l'attribution d'une app, celle-ci est transmise à l'appareil par le système de GAM, sans qu'il soit nécessaire d'envoyer une invitation aux utilisateurs. Par la suite, toute personne qui utilise l'appareil peut accéder à l'app.
- **Attribuez des apps et des livres à des utilisateurs.** Une autre méthode consiste à utiliser votre solution de GAM pour inviter les utilisateurs à télécharger des apps et des livres par courriel ou notification Push. Pour accepter l'invitation, les utilisateurs se connectent sur leur appareil avec leur identifiant Apple personnel. L'identifiant Apple est enregistré auprès du service Apple Business Manager, mais il demeure entièrement confidentiel et n'est pas divulgué aux administrateurs. Une fois que les utilisateurs acceptent l'invitation, ils sont connectés à votre serveur de GAM et peuvent télécharger les apps et les livres que vous leur avez attribués. Les apps sont automatiquement téléchargeables sur tous les appareils de l'utilisateur, sans que vous ayez à faire quoi que ce soit ni à déboursier de frais supplémentaires.

Lorsqu'une app n'est plus utile sur un appareil ou pour un utilisateur, vous pouvez la retirer et l'attribuer à un autre appareil ou à un autre utilisateur. Votre entreprise conserve la propriété exclusive des apps achetées et en dispose à sa convenance. Une fois distribués, les livres demeurent toutefois la propriété de leur destinataire et ne peuvent être ni retirés ni réattribués.

Codes de téléchargement

Vous pouvez aussi distribuer les contenus en employant des codes de téléchargement. C'est une solution pratique si votre entreprise ne peut utiliser la GAM sur les appareils des utilisateurs – par exemple s'il s'agit d'une entreprise franchisée. Avec cette méthode, vous transférez l'app ou le livre de façon permanente à l'utilisateur qui active le code. La liste des codes de téléchargement est livrée sous forme de feuille de calcul. Un code unique est fourni pour chaque app ou chaque livre; il y a autant de codes que de licences achetées. Chaque fois qu'un code est activé, votre feuille de calcul est mise à jour dans la boutique Apple Business Manager. Vous avez donc toujours accès au nombre de codes de téléchargement utilisés. Vous pouvez distribuer les codes avec votre solution de GAM, Apple Configurator 2 ou votre site web interne, ou encore par courriel.

Installation d'apps et de contenu avec Apple Configurator 2 (facultatif)

Apple Configurator 2 vous permet non seulement d'accéder aux fonctions d'installation et de configuration de base, mais aussi d'installer des apps et des contenus sur les appareils que vous configurez pour un utilisateur. Pour les déploiements d'appareils individuels, vous pouvez préinstaller les apps pour économiser du temps et de la bande passante. Et pour les déploiements d'appareils partagés, vous pouvez configurer vos appareils de A à Z, jusqu'à l'écran d'accueil. Apple Configurator 2 vous donne la possibilité d'installer des apps de l'App Store, des apps maison et des documents sur les appareils. Les apps de l'App Store nécessitent Apple Business Manager, et les documents sont accessibles aux apps qui prennent en charge le partage de fichiers. Pour consulter ou récupérer des documents sur des appareils iOS ou iPadOS, associez-les à un Mac équipé d'Apple Configurator 2.

3. Distribution

Les employés peuvent facilement utiliser iPhone et iPad sitôt déballés, sans l'aide du service des TI.

Distribuer les appareils

Une fois les étapes de préparation et de configuration terminées, les appareils peuvent être distribués. S'il s'agit d'un déploiement d'appareils individuels, distribuez-les aux utilisateurs. Ceux-ci pourront personnaliser leur appareil et terminer la configuration avec l'Assistant réglages simplifié. S'il s'agit d'un déploiement d'appareils partagés, distribuez-les aux employés au début des quarts de travail, ou prévoyez des postes où les appareils seront conservés en sécurité et rechargés au besoin.

Assistant réglages

Aussitôt les appareils déballés, les utilisateurs peuvent les activer, configurer les réglages de base et se mettre au travail grâce à l'Assistant réglages. Au-delà du choix des réglages de base, ils peuvent personnaliser d'autres paramètres en fonction de leurs préférences, comme la langue, les services de localisation, Siri, iCloud et Localiser mon iPhone. Une fois les appareils inscrits à Apple Business Manager, ils sont automatiquement inscrits à la solution de GAM dans l'Assistant réglages.

Autorisation de personnalisation par les utilisateurs

Les déploiements sur des appareils individuels ou sur des appareils appartenant aux utilisateurs se traduisent par un gain en productivité : munis de leur propre identifiant Apple, les utilisateurs choisissent les apps et les contenus dont ils ont besoin pour optimiser leur travail.

Identifiant Apple et identifiant Apple géré

Quand les employés se servent d'un identifiant Apple pour se connecter à des services tels que FaceTime, iMessage, l'App Store et iCloud, ils ont accès à une vaste gamme de ressources qui simplifient le travail, favorisent la productivité et encouragent la collaboration.

À l'instar de l'identifiant Apple standard, l'identifiant Apple géré sert à se connecter à un appareil personnel. Il donne aussi accès aux services Apple, y compris iCloud et les fonctionnalités de collaboration d'iWork et de Notes, ainsi qu'à Apple Business Manager. Toutefois, contrairement à l'identifiant Apple standard, il est détenu et géré par l'entreprise, qui s'occupe entre autres de la réinitialisation des mots de passe et de l'administration basée sur les rôles. L'identifiant Apple géré est également assorti de certaines restrictions.

L'inscription par l'utilisateur requiert quant à elle un identifiant Apple géré qui peut aussi être utilisé de pair avec un identifiant personnel. Les autres options nécessitent soit un identifiant Apple personnel, soit un identifiant Apple géré. Seule l'inscription par l'utilisateur fonctionne avec plus d'un identifiant.

Pour profiter pleinement des services, les utilisateurs doivent employer leur propre identifiant Apple ou l'identifiant Apple géré qui leur a été fourni. Ceux qui n'ont pas d'identifiant Apple peuvent en créer un avant même de recevoir leur appareil. L'Assistant réglages permet également de créer un identifiant Apple personnel si ce n'est déjà fait. Aucune carte de crédit n'est requise.

Pour en savoir plus sur les identifiants Apple gérés :
support.apple.com/guide/apple-business-manager

iCloud

Avec iCloud, les utilisateurs peuvent automatiquement synchroniser leurs contenus personnels (contacts, calendriers, documents, photos, etc.) et les garder à jour sur tous leurs appareils. Le service Localiser, quant à lui, les aide à retrouver un Mac, un iPhone, un iPad ou un iPod touch perdu ou volé. Vous pouvez désactiver certains services (comme iCloud Keychain et iCloud Drive) par l'intermédiaire de la GAM ou en configurant manuellement des restrictions sur l'appareil. Ceci permet aux entreprises de mieux contrôler le type de données stockées sur chaque compte.

Pour en savoir plus sur la gestion d'iCloud* :
support.apple.com/guide/deployment-reference-ios

4. Gestion

Une fois le déploiement terminé, vous disposez d'un vaste éventail de fonctionnalités pour la gestion et la maintenance de vos appareils et contenus.

Contrôler les appareils

Pour les appareils gérés, vous pouvez faire appel à votre serveur de GAM afin d'exécuter un ensemble de tâches précises. Par exemple, vous pouvez interroger les appareils pour obtenir de l'information, ainsi qu'exécuter des tâches à distance en cas de vol, de perte ou de non-respect des politiques.

* En anglais seulement.

Requêtes

Le serveur de GAM peut demander divers renseignements aux appareils, comme le numéro de série, l'identifiant UDID ou l'adresse MAC du Wi-Fi, ou de l'information logicielle, comme la version d'iOS ou d'iPadOS et une liste détaillée de toutes les apps installées sur l'appareil. Ces données peuvent être utilisées par votre solution de GAM pour mettre à jour votre inventaire, guider la prise de décisions et automatiser des tâches de gestion, comme vérifier que les utilisateurs se servent des apps appropriées.

Tâches de gestion

Le serveur de GAM peut effectuer diverses tâches administratives sur les appareils gérés, comme modifier les réglages de configuration sans intervention de l'utilisateur, faire une mise à jour logicielle 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 iPhone ou à un iPad de lancer la copie vidéo AirPlay vers une destination précise, ou de l'interrompre.

Mises à jour logicielles gérées

Pour une période déterminée, vous pouvez empêcher les utilisateurs de mettre à jour manuellement et à distance des appareils iOS et iPadOS supervisés. Par défaut, la période de report est de 30 jours à partir de la parution d'une mise à jour d'iOS ou d'iPadOS. Vous pouvez modifier la durée par défaut de la période (de 1 à 90 jours). Vous pouvez également planifier les mises à jour des appareils supervisés au moyen de votre solution de GAM.

Mode Perdu

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.

Verrouillage d'activation

Sous iOS 7.1 et les versions ultérieures, il est possible d'utiliser la GAM pour activer l'option Verrouillage d'activation quand un utilisateur active la fonction Localiser sur un appareil supervisé. Ainsi, votre entreprise peut profiter de la fonctionnalité antivol du verrouillage d'activation tout en conservant la possibilité de la contourner si un utilisateur n'arrive pas à s'authentifier avec son identifiant Apple.

Déploiement et gestion de contenus supplémentaires

Les entreprises doivent souvent distribuer des apps pour aider les utilisateurs à être productifs. Elles doivent également contrôler la façon dont les apps se connectent aux ressources internes ou dont la sécurité des données est gérée quand des utilisateurs quittent l'organisation, tout en assurant la coexistence avec les apps et les données personnelles des utilisateurs.

Portail d'apps interne

La plupart des serveurs de GAM offrent des portails internes. Sinon, vous pouvez créer votre propre portail afin d'aider vos employés à trouver facilement des apps pour leur iPhone ou leur iPad. Les apps maison, les URL des apps de l'App Store, les codes de téléchargement d'Apple Business Manager et les apps sur mesure peuvent tous être accessibles dans ce portail interne, qui devient un guichet unique pour vos utilisateurs. La gestion et la sécurisation de ce site sont centralisées. Et le portail permet aux employés d'accéder aux ressources approuvées dont ils ont besoin en moins de deux, sans faire appel aux TI.

Contenu géré

Le contenu géré comprend l'installation, la configuration, la gestion et la suppression des apps de l'App Store, des apps maison, des comptes, des livres et des autres documents.

- **Apps gérées.** En choisissant de gérer les apps sous iOS et iPadOS, les entreprises peuvent distribuer à distance des apps gratuites, payantes et internes au moyen d'une solution de GAM, tout en offrant le bon équilibre entre protection des données de l'entreprise et protection des données personnelles de l'utilisateur. Les apps gérées peuvent être supprimées à distance par le serveur de GAM ou lorsque l'utilisateur désinscrit son appareil du serveur. La suppression d'une app a pour effet de supprimer les données qui lui sont associées. Si une app demeure attribuée à un utilisateur dans Apple Business Manager ou si l'utilisateur s'est servi d'un code avec son identifiant Apple personnel, l'app pourra de nouveau être téléchargée sur l'App Store, mais elle ne sera pas gérée par la solution de GAM.
- **Comptes gérés.** La GAM peut aider vos utilisateurs à être rapidement opérationnels en configurant automatiquement leur messagerie et d'autres comptes. Selon votre solution de GAM et son intégration dans 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.
- **Livres et documents gérés.** Les outils de GAM, les livres électroniques et les documents ePub et PDF sont automatiquement poussés vers les appareils des utilisateurs, qui disposent ainsi en tout temps du matériel qu'il leur faut. Toutefois, les livres gérés ne peuvent être partagés qu'avec des apps gérées ou transmis par courriel à partir de comptes gérés. Enfin, quand les contenus ne servent plus, il est possible de les retirer à distance. Les livres achetés par l'intermédiaire d'Apple Business Manager peuvent être distribués de manière gérée, mais ne peuvent être ni retirés ni réassignés. Il est impossible de gérer un livre déjà acheté par l'utilisateur, à moins qu'il n'ait été spécifiquement assigné par Apple Business Manager.

Configurer les apps gérées

Les développeurs peuvent déterminer les paramètres et fonctionnalités activables d'une app gérée. Vous avez le choix de définir ces paramètres de configuration avant ou après l'installation de l'app gérée. Par exemple, les TI pourraient créer un ensemble de préférences par défaut pour l'app SharePoint de façon à ce que l'utilisateur n'ait pas à configurer manuellement les paramètres de serveur.

D'importants fournisseurs de solutions de GAM ont mis sur pied l'AppConfig Community et établi un schéma standard pour aider les développeurs d'apps à configurer des apps gérées. Le groupe AppConfig Community propose des outils et des pratiques exemplaires mettant à profit les fonctionnalités natives des systèmes d'exploitation mobiles. Il contribue également à définir une méthode uniforme, ouverte et accessible pour configurer et sécuriser les apps mobiles et ainsi accroître l'intégration des technologies mobiles dans les entreprises.

Pour en savoir plus sur le groupe AppConfig Community* :
appconfig.org

Gérer les flux de données

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.

- **Gestion des autorisations d'ouverture.** 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 une pièce jointe confidentielle liée 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 le fichier, et les apps personnelles non gérées de l'utilisateur ne figurent même pas dans la liste des apps disponibles. En plus des comptes, livres, domaines et apps gérés, plusieurs extensions respectent les restrictions de gestion des autorisations d'ouverture.
- **Mode App individuelle.** Limitant l'utilisation d'iOS ou d'iPadOS à une seule app, ce réglage est parfait pour les appareils ayant une fonction unique, par exemple dans les kiosques, les points de vente et les comptoirs d'accueil. Les développeurs peuvent activer cette fonctionnalité dans leurs apps afin qu'elles puissent entrer et sortir du mode App individuelle de manière autonome.
- **Prévention de la sauvegarde.** Cette restriction empêche les apps gérées de sauvegarder des données sur iCloud ou sur un ordinateur. En interdisant la sauvegarde, vous évitez que les données des apps gérées ne soient récupérées si l'app est supprimée via la GAM, puis réinstallée par l'utilisateur.

* En anglais seulement.

Options d'assistance

Apple propose un éventail de programmes et d'options de soutien aux utilisateurs d'iOS et d'iPadOS ainsi qu'aux administrateurs des TI.

AppleCare pour entreprises

Si vous cherchez une protection complète, AppleCare pour entreprises peut vous aider à réduire la charge de travail de votre service informatique en offrant à vos employés du soutien technique par téléphone 24 heures sur 24, 7 jours sur 7, et un délai de réponse d'au maximum une heure pour les problèmes majeurs. Avec ce programme, votre équipe des TI peut obtenir de l'aide pour tous les composants matériels et logiciels d'Apple, et de l'assistance pour les déploiements et les intégrations complexes, par exemple pour les solutions de GAM et Active Directory.

AppleCare OS Support

AppleCare OS Support procure à votre service des TI un soutien par téléphone et par courriel à l'échelle de l'entreprise relativement au déploiement d'iOS, d'iPadOS, de macOS et de macOS Server. Plusieurs niveaux sont proposés, de l'aide ponctuelle au soutien jour et nuit avec gestionnaire de compte affecté à votre entreprise. En vous permettant de communiquer directement avec des techniciens pour toutes vos questions sur l'intégration, la migration et le fonctionnement de votre serveur, AppleCare OS Support vous aide à améliorer l'efficacité de votre équipe des TI dans le déploiement et la gestion d'appareils et la résolution de problèmes.

Soutien AppleCare pour centres d'assistance

Le soutien AppleCare pour centres d'assistance offre un accès téléphonique prioritaire aux équipes de techniciens Apple chevronnés. Il comprend également une gamme d'outils pour le diagnostic des problèmes et le dépannage du matériel Apple, ce qui permet aux grandes entreprises de gérer plus efficacement leurs ressources, d'améliorer leur temps de réponse et de réduire leurs coûts de formation. Le soutien AppleCare pour centres d'assistance assure le diagnostic et le dépannage pour un nombre illimité d'incidents relatifs au matériel et aux logiciels, ainsi que le dépistage des problèmes liés aux appareils iOS et iPadOS.

AppleCare pour les utilisateurs d'appareils iOS et iPadOS

Chaque appareil iOS et iPadOS est assorti d'une garantie limitée d'un an et d'un service d'assistance téléphonique gratuit valable 90 jours à compter de la date d'achat. AppleCare+ pour iPhone, AppleCare+ pour iPad et AppleCare+ pour iPod touch vous permettent de prolonger la période de couverture à deux ans à compter de la date d'achat. Vous pouvez téléphoner aux experts du service d'assistance technique d'Apple aussi souvent que vous le voulez pour obtenir des réponses à vos questions. Apple met également à votre disposition des options pratiques si vos appareils doivent être réparés. De plus, les plans de protection offrent la prise en charge d'un maximum de deux réparations requises en raison de dommages accidentels, chacune entraînant des frais.

Programme d'assistance directe pour iOS

En complément d'AppleCare+, le programme d'assistance directe pour iOS permet à votre service de soutien de dépister les appareils présentant des défaillances matérielles sans avoir à appeler AppleCare ou à se rendre à l'Apple Store. Au besoin, votre entreprise peut commander directement un iPhone, un iPad, un iPod touch ou des accessoires de remplacement.

Pour en savoir plus sur les programmes AppleCare :

apple.com/ca/fr/support/professional

Conclusion

De nombreuses options s'offrent à vous pour faciliter le déploiement et la gestion d'iPhone et d'iPad dans votre entreprise, que vous visiez un groupe restreint d'utilisateurs ou l'ensemble de votre personnel. En choisissant les stratégies les mieux adaptées à votre entreprise, vous aiderez vos employés à gagner en productivité et à révolutionner leurs façons de travailler.

Pour en savoir plus sur le déploiement, la gestion et les fonctionnalités de sécurité d'iOS et d'iPadOS* :

support.apple.com/guide/deployment-reference-ios

Pour en savoir plus sur les réglages de la gestion des appareils mobiles pour les TI :

support.apple.com/guide/mdm

Pour en savoir plus sur Apple Business Manager :

support.apple.com/guide/apple-business-manager

Pour en savoir plus sur les identifiants Apple gérés en entreprise :

apple.com/ca/fr/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Pour en savoir plus sur Apple at Work :

www.apple.com/ca/fr/business/

Pour en savoir plus sur les fonctionnalités des TI :

www.apple.com/ca/fr/business/it/

Pour en savoir plus sur la sécurité des plateformes Apple* :

www.apple.com/security/

Pour en savoir plus sur les programmes AppleCare :

www.apple.com/ca/fr/support/professional/

Pour en savoir plus sur la formation et la certification Apple* :

training.apple.com

Pour en savoir plus sur les Services professionnels Apple :

consultingservices@apple.com

* En anglais seulement.

Certaines apps et certains livres peuvent ne pas être disponibles, selon le pays ou la région et les décisions du développeur; consultez [le programme et les contenus offerts](#). Certaines fonctionnalités nécessitent une connexion Wi-Fi. Certaines fonctionnalités ne sont pas offertes dans tous les pays. Pour connaître les exigences système minimales et recommandées pour iCloud, visitez support.apple.com/HT204230.

© 2019 Apple Inc. Tous droits réservés. Apple, le logo Apple, AirDrop, AirPlay, AirPrint, Apple TV, Bonjour, FaceTime, iMessage, iPad, iPhone, iPod touch, iWork, Mac, macOS et Siri sont des marques de commerce d'Apple Inc., déposées aux États-Unis et dans d'autres pays. iPadOS est une marque de commerce d'Apple Inc. App Store, AppleCare, Apple Store, Apple Books, iCloud, iCloud Drive et iCloud Keychain sont des marques de service d'Apple Inc., déposées aux États-Unis et dans d'autres pays. iOS est une marque de commerce ou une marque de commerce déposée de Cisco aux États-Unis et dans d'autres pays; elle est utilisée sous licence. Les autres produits et dénominations sociales mentionnés ici peuvent être des marques de commerce de leurs sociétés respectives. Les caractéristiques des produits peuvent changer sans préavis. Le présent document n'est fourni qu'à titre d'information; Apple se dégage de toute responsabilité quant à son utilisation.