Présentation du déploiement d’iOS et d’iPadOS

Introduction

Table des matières

L'iPhone et l'iPad peuvent transformer votre activité et le mode de travail de vos employés. Ils peuvent optimiser la productivité de votre entreprise et donner à vos employés la liberté et la flexibilité de mettre en œuvre de nouvelles méthodes de travail, au bureau ou en déplacement. Adopter cette façon moderne de travailler profite à toute l'entreprise. Les utilisateurs disposent d'un meilleur accès aux informations. Ils se sentent de ce fait plus investis, et peuvent résoudre les problèmes de façon créative.

Les services informatiques qui prennent en charge iOS et iPadOS façonnent désormais la stratégie de l'entreprise et règlent des problèmes concrets ; leur rôle ne se limite plus à faire des réparations et à réduire les coûts. En fin de compte, tout le monde en profite : les collaborateurs s'impliquent davantage et les nouvelles opportunités se multiplient pour les entreprises.

Il est désormais très facile de configurer et de déployer des iPhone et des iPad dans votre entreprise. À l'aide d'Apple Business Manager et d'une solution tierce de gestion des appareils mobiles, votre organisation peut facilement déployer des appareils iOS et iPadOS et des apps à grande échelle.

- La gestion des appareils mobiles vous permet de configurer et de gérer les appareils, mais aussi de distribuer et de gérer les apps à distance.
- Apple Business Manager automatise l'inscription des appareils Apple auprès de votre solution MDM afin de simplifier le déploiement avec une configuration sans intervention pour le service informatique.
- Apple Business Manager vous permet d'acheter des apps et des livres en volume puis de les distribuer à distance aux utilisateurs.
- Apple Business Manager vous permet également de créer des identifiants Apple gérés pour les employés qui utilisent l'authentification fédérée avec Microsoft Azure AD.

Ce document vous guidera dans le déploiement d'appareils iOS et iPadOS au sein de votre entreprise et vous aidera à mettre en œuvre un plan de déploiement adapté à votre environnement. Les sujets abordés dans ce document sont présentés en détail dans la ressource Référence pour le déploiement d'iPhone et iPad, disponible sur : support.apple.com/guide/deployment-reference-ios

Modèles de propriété

Évaluer les modèles de propriété et choisir celui qui sera le mieux adapté à votre entreprise constitue une première étape importante du déploiement. Vous pouvez aborder le déploiement de diverses manières, en fonction du propriétaire de l'appareil. Commencez par déterminer ce qui convient le mieux à votre entreprise.

Deux modèles de propriété des appareils iOS et iPadOS sont fréquemment utilisés par les entreprises :

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

Bien que la plupart des entreprises privilégient un modèle plutôt qu'un autre, il est possible que plusieurs modèles conviennent à votre environnement. Par exemple, le siège social d'une entreprise peut déployer une stratégie d'appareils appartenant aux utilisateurs, en permettant aux employés de configurer un iPad personnel sans compromettre la protection et la gestion des ressources de l'entreprise, sans affecter les données et apps personnelles de l'utilisateur. En parallèle, les magasins de cette société peuvent déployer une stratégie d'appareils appartenant à l'entreprise, donnant la possibilité à plusieurs employés de partager des appareils iOS et iPadOS pour traiter les transactions des clients.

Explorez ces modèles pour identifier celui qui est le mieux adapté à votre environnement. Après cela, votre équipe pourra étudier en détail les options de déploiement et de gestion Apple.

Appareils appartenant à l'organisation

Dans le modèle où les appareils appartiennent à l'entreprise, vous pouvez mettre des appareils à la disposition des employés pour leur usage quotidien, en mettre en partage entre plusieurs employés pour les tâches courantes ou en configurer pour une tâche spécifique qui s'effectue dans une seule app. Les appareils fournis à un seul utilisateur peuvent être personnalisés par l'utilisateur final. En général, les appareils dont l'utilisation est limitée à une seule app ou partagée entre plusieurs utilisateurs ne sont pas personnalisés par les utilisateurs finaux. En utilisant une combinaison de ces différents modèles, des technologies clés Apple et une solution MDM, vous pouvez totalement automatiser l'installation et la configuration des appareils.

Déploiement personnalisé. En optant pour une stratégie de déploiement personnalisé, vous pouvez demander aux utilisateurs de choisir leur appareil et de l'inscrire auprès d'une solution MDM qui fournit à distance les réglages et les apps de l'entreprise. Si vous achetez des appareils directement auprès d'Apple ou de Revendeurs Agréés Apple et opérateurs participants, vous pouvez également tirer parti d'Apple Business Manager pour inscrire automatiquement les nouveaux appareils auprès de votre solution MDM : il s'agit de l'inscription automatisée des appareils. Une fois leur appareil configuré, les utilisateurs peuvent le personnaliser en y ajoutant leurs propres apps et données, en plus des comptes ou des apps fournis par l'entreprise.

Déploiement non personnalisé. Lorsque les appareils sont partagés par plusieurs personnes ou utilisés dans un seul but (par exemple, dans un restaurant ou un hôtel), les administrateurs informatiques les configurent et les gèrent généralement de façon centralisée au lieu de compter sur un utilisateur individuel pour effectuer la configuration. Dans un déploiement non personnalisé, les utilisateurs ne sont généralement pas autorisés à installer des apps sur les appareils ni à y enregistrer des données personnelles. L'inscription automatisée des appareils via Apple Business Manager peut également permettre d'automatiser la configuration des appareils non personnalisés. Le tableau suivant illustre les actions requises par l'administrateur et l'utilisateur pour chaque étape du déploiement lorsque les appareils appartiennent à l'entreprise. Sauf indication contraire, les actions requises s'appliquent aux déploiements *personnalisés* et aux déploiements *non personnalisés*.

	Administrateur	Utilisateur
Préparation	• Évaluer votre infrastructure • Choisir une solution MDM • S'inscrire à Apple Business Manager	• Aucune action requise de la part de l'utilisateur
Configuration	• Configurer des appareils • Distribuer des apps et des livres	• Aucune action requise de la part de l'utilisateur
Déploiement	• Distribuer les appareils **Déploiement personnalisé uniquement** • Permettre aux utilisateurs de personnaliser l'appareil	**Déploiement personnalisé uniquement** • Télécharger et installer les apps et les livres • Utiliser un identifiant Apple, ainsi que des comptes App Store et iCloud, le cas échéant **Déploiement non personnalisé uniquement** • Aucune action requise de la part de l'utilisateur
Gestion	• Gérer les appareils • Déployer et gérer le contenu supplémentaire	**Déploiement personnalisé uniquement** • Découvrir des apps complémentaires à utiliser **Déploiement non personnalisé uniquement** • Aucune action requise de la part de l'utilisateur

Appareils appartenant aux utilisateurs

Lorsque les appareils sont achetés et paramétrés par l'utilisateur, dans le cadre d'un déploiement communément appelé BYOD (Bring Your Own Device, « Apportez vos appareils personnels »), vous pouvez toujours fournir un accès aux services de l'entreprise comme le Wi-Fi, les e-mails et les calendriers par le biais de la solution MDM, grâce à la nouvelle option Inscription d'utilisateurs intégrée à iOS 13 et iPadOS.

Le déploiement BYOD permet aux utilisateurs d'installer et de configurer leurs propres appareils. Les utilisateurs peuvent inscrire leurs appareils auprès de la solution MDM de votre entreprise afin d'accéder aux ressources que celle-ci met à leur disposition, de configurer différents réglages et d'installer un profil

de configuration ou des apps d'entreprise. Les utilisateurs doivent alors s'inscrire auprès de la solution MDM de votre entreprise.

L'inscription d'utilisateurs pour les appareils personnels permet de gérer les ressources et les données de l'entreprise de façon sécurisée, tout en respectant la vie privée des utilisateurs, ainsi que la confidentialité de leurs données et apps personnelles. Le service informatique peut appliquer uniquement des réglages spécifiques, surveiller la conformité aux règles de l'entreprise et supprimer uniquement les données et apps de l'entreprise, sans toucher aux données et apps personnelles des appareils.

L'inscription d'utilisateurs inclut les éléments suivants :

- **Identifiants Apple gérés.** L'inscription d'utilisateurs intègre un identifiant Apple géré permettant d'établir l'identité de l'utilisateur sur l'appareil et de lui donner accès aux services Apple. L'identifiant Apple géré peut être utilisé en même temps que l'identifiant Apple personnel avec lequel l'utilisateur est déjà connecté. Les identifiants Apple gérés sont créés au sein d'Apple Business Manager et fournis à Microsoft Azure Active Directory par le biais de l'authentification fédérée.
- **Séparation des données.** L'inscription d'utilisateurs crée un volume APFS distinct pour les comptes gérés, les apps et les données sur l'appareil. Ce volume géré est séparé du reste de l'appareil par chiffrement.
- **Gestion spécifique des appareils BYOD.** L'inscription d'utilisateurs a été conçue pour les appareils appartenant aux utilisateurs. Elle permet au service informatique de gérer un sous-ensemble de configurations et de règles tout en limitant certaines tâches de gestion, comme l'effacement à distance d'un appareil ou la collecte d'informations personnelles.

Le tableau suivant illustre les actions requises par l'administrateur et l'utilisateur pour chaque étape du déploiement d'un appareil appartenant à l'utilisateur.

	Administrateur	Utilisateur
Préparation	• Évaluer votre infrastructure • Choisir une solution MDM • S'inscrire à Apple Business Manager	• Utiliser un identifiant Apple personnel et un identifiant Apple géré, ainsi que des comptes App Store et iCloud, le cas échéant
Configuration	• Configurer les réglages des appareils • Distribuer des apps et des livres	• S'inscrire auprès de la solution MDM • Télécharger et installer les apps et les livres
Déploiement	• Aucune action requise de la part de l'administrateur	• Aucune action requise de la part de l'utilisateur
Gestion	• Gérer les appareils • Déployer et gérer le contenu supplémentaire	• Découvrir des apps complémentaires à utiliser

En savoir plus sur l'option Inscription d'utilisateurs avec une solution MDM : support.apple.com/guide/mdm

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

Étapes du déploiement

Cette section présente de façon plus détaillée chacune des quatre étapes du déploiement d'appareils et de contenus : préparer l'environnement, configurer les appareils, les déployer et les gérer. Les étapes dépendront du choix de l'organisation d'avoir recours à des appareils lui appartenant ou appartenant aux utilisateurs.

1. Préparation

Après avoir déterminé quel modèle de déploiement convient le mieux à votre entreprise, suivez les étapes ci-après afin de préparer le terrain pour le déploiement. Vous pouvez effectuer ces actions avant d'avoir les appareils à disposition.

Évaluer votre infrastructure

L'iPhone et l'iPad s'intègrent parfaitement à la plupart des environnements informatiques d'entreprise standard. Il est primordial d'évaluer votre infrastructure réseau existante pour vous assurer que votre organisation tire le meilleur parti des possibilités qu'offrent iOS et iPadOS.

Wi-Fi et réseau

L'installation et la configuration des appareils iOS et iPadOS nécessitent un accès stable et fiable à un réseau sans fil. Vérifiez que le réseau Wi-Fi de votre entreprise peut prendre en charge plusieurs appareils avec connexion simultanée de tous les utilisateurs. Vous devrez peut-être configurer votre proxy web ou les ports de coupe-feu si les appareils ne parviennent pas à accéder aux serveurs d'activation d'Apple, à iCloud ou à l'App Store. Apple et Cisco ont par ailleurs optimisé la façon dont l'iPhone et l'iPad communiquent sur les réseaux sans fil Cisco, ouvrant la voie à d'autres fonctionnalités avancées de mise en réseau, comme l'itinérance rapide et l'optimisation de la qualité de service (QoS) pour les apps.

Évaluez votre infrastructure VPN pour vous assurer que les utilisateurs pourront se servir de leurs appareils iOS et iPadOS afin d'accéder à distance et de façon sécurisée aux ressources de l'entreprise. Envisagez d'utiliser la fonctionnalité VPN à la demande ou VPN via l'app disponibles sur iOS et iPadOS pour que les connexions VPN ne soient initiées que lorsqu'elles sont nécessaires. Si vous prévoyez d'utiliser le VPN via l'app, vérifiez que vos passerelles VPN prennent en charge cette fonctionnalité et que vous disposez d'un nombre suffisant de licences pour couvrir le nombre approprié d'utilisateurs et de connexions.

Vous devrez aussi vous assurer que votre infrastructure réseau est configurée de façon à fonctionner correctement avec Bonjour, le protocole réseau standard d'Apple sans configuration. Bonjour permet aux appareils de trouver automatiquement des services sur un réseau. Les appareils iOS et iPadOS utilisent Bonjour pour se connecter aux imprimantes compatibles AirPrint et aux appareils compatibles AirPlay, comme l'Apple TV. Certaines apps utilisent aussi Bonjour pour détecter d'autres appareils en vue d'une collaboration ou d'un partage.

En savoir plus sur le Wi-Fi et les réseaux :
support.apple.com/guide/deployment-reference-ios

En savoir plus sur Bonjour :
developer.apple.com/library

Mail, contacts et calendriers
Si vous utilisez Microsoft Exchange, vérifiez que le service ActiveSync est à jour et configuré de façon à prendre en charge tous les utilisateurs du réseau. Si vous utilisez le service Office 365 sur le cloud, vérifiez que vous avez un nombre suffisant de licences pour prendre en charge le nombre prévu d'appareils iOS et iPadOS qui seront connectés. iOS et iPadOS prennent aussi en charge l'authentification moderne d'Office 365 en tirant parti d'OAuth 2.0 et de l'authentification à plusieurs facteurs. Si vous n'utilisez pas Exchange, iOS et iPadOS sont également compatibles avec des serveurs standard, notamment IMAP, POP, SMTP, CalDAV, CardDAV et LDAP.

Mise en cache de contenu
La mise en cache de contenu, une fonctionnalité intégrée à macOS High Sierra et versions ultérieures, stocke une copie locale du contenu fréquemment demandé auprès des serveurs Apple, permettant ainsi de réduire la bande passante requise pour télécharger du contenu sur votre réseau. La mise en cache de contenu accélère le téléchargement et la diffusion de logiciels via l'App Store, le Mac App Store et Apple Books.

Elle peut également mettre en cache les mises à jour logicielles pour accélérer leur téléchargement sur les appareils iOS et iPadOS. La mise en cache de contenu comprend la mise en cache connectée, qui permet à un Mac de partager sa connexion Internet avec plusieurs appareils iOS et iPadOS connectés par USB.

En savoir plus sur la mise en cache de contenu :
support.apple.com/guide/deployment-reference-macos

En savoir plus sur la mise en cache connectée :
support.apple.com/HT207523

Choisir une solution MDM

La structure de gestion d'Apple pour iOS et iPadOS permet d'inscrire des appareils dans l'environnement de l'entreprise de façon sécurisée, de configurer et de mettre à jour les réglages à distance, de surveiller la conformité aux règles, de déployer des apps et des livres, et d'effacer ou de verrouiller à distance les appareils gérés. Ces fonctionnalités de gestion sont activées par des solutions MDM tierces.

Il existe différentes solutions MDM tierces compatibles avec différentes plateformes serveur. Chaque solution propose des consoles de gestion, des fonctionnalités et des tarifs différents. Avant de choisir une solution, étudiez les ressources ci-dessous pour déterminer les fonctionnalités de gestion les plus pertinentes pour votre organisation. En complément des solutions MDM tierces, Apple propose une solution appelée Gestionnaire de profils, intégrée à macOS Server.

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

S'inscrire à Apple Business Manager

Apple Business Manager est un portail web destiné aux administrateurs informatiques qui permet de déployer l'iPhone, l'iPad, l'iPod touch, l'Apple TV et le Mac depuis un même endroit. Apple Business Manager fonctionne en parfaite synergie avec votre solution de gestion des appareils mobiles (Mobile Device Management, MDM) et simplifie le déploiement automatisé des appareils, l'achat d'apps et la distribution de contenus, ainsi que la création d'identifiants Apple gérés pour les employés.

Le Programme d'inscription des appareils (Device Enrolment Program, DEP) et le Programme d'achat en volume (Volume Purchase Program, VPP) sont désormais entièrement intégrés à Apple Business Manager. Les entreprises disposent donc de tout ce dont elles ont besoin pour déployer des appareils Apple. Ces programmes ne seront plus disponibles à partir du 1er décembre 2019.

Appareils

Apple Business Manager offre plusieurs avantages aux entreprises, notamment l'inscription automatisée des appareils, le déploiement simple et rapide des appareils Apple appartenant à l'entreprise et l'inscription à la solution MDM sans intervention sur les appareils ni préparation de ceux-ci.

- Simplifiez les étapes de l'Assistant réglages pour optimiser le processus de configuration et vous assurer que les appareils des employés sont correctement configurés dès leur activation. Les équipes informatiques peuvent maintenant personnaliser davantage ce processus en proposant aux utilisateurs un texte de consentement, une image de marque personnalisée ou encore une méthode d'authentification moderne.
- Augmentez le niveau de contrôle des appareils appartenant à l'organisation grâce à la supervision, qui propose des commandes de gestion de l'appareil supplémentaires indisponibles avec les autres modèles de déploiement, y compris l'irrévocabilité de la solution MDM.
- Gérez plus facilement les serveurs MDM par défaut en paramétrant un serveur par défaut en fonction du type d'appareil. Enfin, vous pouvez désormais inscrire manuellement des iPhone, iPad et Apple TV à l'aide d'Apple Configurator 2, quelle que soit la manière dont vous les avez acquis.

Contenus

Apple Business Manager permet aux entreprises de se procurer plus facilement des contenus en volume. Que vos employés utilisent des iPhone, des iPad ou des Mac, vous pouvez leur fournir des contenus de qualité prêts à l'emploi avec des options de distribution souples et sécurisées.

- Achetez des apps, des livres et des apps personnalisées en volume, y compris les apps que vous avez développées en interne. Transférez facilement des licences d'applications d'un site à l'autre et partagez les licences entre acheteurs situés au même endroit. Consultez une liste consolidée de l'historique des achats, avec notamment le nombre actuel de licences utilisées avec la MDM.
- Distribuez les apps et les livres directement aux appareils gérés ou aux utilisateurs autorisés et vérifiez facilement quel contenu a été attribué à quel utilisateur ou appareil. Grâce à la distribution gérée, vous contrôlez tout le processus de distribution tout en restant entièrement propriétaire des apps. Et si une app n'est

plus utilisée par un appareil ou un utilisateur, elle peut être révoquée et réattribuée à un autre appareil ou utilisateur au sein de votre organisation.

- Plusieurs options de paiement sont disponibles, notamment par carte bancaire ou sur bon de commande. Les organisations peuvent acheter du crédit VPP (dans les pays où cela est proposé) d'un montant spécifique en devise locale auprès d'Apple ou d'un Revendeur Agréé Apple. Ce montant est transféré de manière électronique directement au titulaire du compte sous forme d'avoir.
- Distribuez une app aux appareils ou utilisateurs dans tous les pays où l'app est disponible, pour une distribution internationale. Les développeurs peuvent proposer leurs apps dans plusieurs pays via le processus standard de publication sur l'App Store.

Remarque : les achats de livres dans Apple Business Manager ne sont pas disponibles dans tous les pays et régions. Pour connaître la disponibilité des fonctionnalités et des modes de paiement selon les pays et régions, consultez support.apple.com/HT207305/

Personnes

Apple Business Manager permet aux entreprises de créer et de gérer des comptes pour les employés. Ces comptes sont en mesure de s'intégrer à l'infrastructure existante et d'accéder aux apps Apple, aux services Apple et à Apple Business Manager.

- Créez des identifiants Apple gérés pour que les employés collaborent dans les apps et les services Apple, et accèdent aux données de l'entreprise dans les apps gérées utilisant iCloud Drive. Ce sont les entreprises qui détiennent et contrôlent ces comptes.
- Associez Apple Business Manager avec Microsoft Azure Active Directory pour tirer parti de l'authentification fédérée. Un identifiant Apple géré est automatiquement créé à chaque fois qu'un employé se connecte pour la première fois avec ses identifiants sur un appareil Apple compatible.
- Avec la nouvelle fonctionnalité Inscription d'utilisateurs disponible sur iOS 13, iPadOS et macOS Catalina, les appareils appartenant aux utilisateurs peuvent simultanément accueillir un identifiant Apple géré et un identifiant Apple personnel. Il est également possible d'utiliser un identifiant Apple géré en tant qu'identifiant Apple principal (et unique) sur n'importe quel appareil. Et après s'être connecté un appareil Apple avec un identifiant Apple géré une première fois, l'utilisateur pourra s'en servir pour accéder à iCloud sur le Web.
- Vous pouvez désigner des rôles spécifiques dans les équipes informatiques de votre entreprise afin de gérer plus efficacement les appareils, les apps et les comptes intégrés à Apple Business Manager. Le rôle Administrateur permet par exemple d'accepter des conditions générales d'utilisation si cela est nécessaire, et de facilement transférer des responsabilités si un employé quitte l'organisation.

Remarque : pour le moment, l'option Inscription d'utilisateurs ne prend pas en charge iCloud Drive. iCloud Drive est uniquement compatible avec les appareils utilisant un identifiant Apple géré s'il s'agit de l'unique identifiant Apple de l'appareil.

En savoir plus sur Apple Business Manager : www.apple.com/fr/business/it/

S’inscrire à l’Apple Developer Enterprise Program

L’Apple Developer Enterprise Program propose tout un ensemble d’outils pour développer et tester des apps puis les distribuer aux utilisateurs. Vous pouvez distribuer des apps soit en les hébergeant sur un serveur web, soit à l’aide d’une solution MDM. Vous pouvez également signer et notarier les apps et programmes d’installation Mac à l’aide d’un Developer ID pour Gatekeeper, afin de protéger macOS contre les logiciels malveillants.

En savoir plus sur l’Apple Developer Enterprise Program :
developer.apple.com/programs/enterprise

2. Configuration

Dans cette étape, vous configurez vos appareils et distribuez vos contenus en vous servant d’Apple Business Manager, d’une solution MDM ou éventuellement d’Apple Configurator 2. Vous pouvez aborder la configuration de diverses manières, en fonction du propriétaire des appareils et du type de déploiement qui répond à vos besoins.

Configurer vos appareils

Vous disposez de plusieurs options pour configurer l’accès des utilisateurs aux services de l’entreprise. Le service informatique peut configurer les appareils en distribuant des profils de configuration. D’autres options de configuration sont disponibles pour les appareils supervisés.

Configurer les appareils avec une solution MDM

Une fois vos appareils inscrits de façon sécurisée auprès d’un serveur MDM, chacun est géré grâce à un profil de configuration, c’est-à-dire un fichier XML contenant des informations de configuration destinées à un appareil iOS ou iPadOS. Ces profils automatisent la configuration des réglages, comptes, restrictions et identifiants. Ils peuvent être fournis à distance depuis votre solution MDM, ce qui est idéal pour configurer plusieurs appareils avec peu de manipulation. Les profils peuvent aussi être envoyés sous forme de pièce jointe à un e-mail, téléchargés depuis une page web ou installés sur les appareils via Apple Configurator 2.

- **Appareils appartenant à l’entreprise.** Utilisez Apple Business Manager pour activer l’inscription automatique des appareils auprès de la solution MDM dès leur activation. Les appareils iOS et iPadOS ajoutés à Apple Business Manager sont toujours supervisés et obligatoirement inscrits auprès de la MDM.
- **Appareils appartenant aux utilisateurs.** Les employés peuvent choisir d’inscrire ou non leur appareil auprès de la solution MDM. Et ils peuvent à tout moment les dissocier en supprimant le profil de configuration de leur appareil, ce qui efface aussi les données et réglages d’entreprise. Envisagez cependant de recourir à des mesures incitatives pour encourager les utilisateurs à rester inscrits. Vous pouvez par exemple leur demander d’inscrire leur appareil auprès de la solution MDM pour obtenir un accès au réseau Wi-Fi, votre solution MDM fournissant alors automatiquement les identifiants de connexion.

Une fois qu'un appareil est inscrit, un administrateur peut lancer l'application d'une règle, option ou commande MDM. Les actions proposées pour gérer un appareil dépendent du mode de supervision et d'inscription de celui-ci. L'appareil iOS ou iPadOS reçoit ensuite une notification de l'action de l'administrateur via le service de notification push d'Apple (APNS), lui permettant de communiquer directement avec son serveur MDM par le biais d'une connexion sécurisée. Avec une connexion réseau, les appareils peuvent recevoir les commandes APNS n'importe où dans le monde. Cependant, le service de notification push d'Apple ne transmet aucune information de nature confidentielle ou propriétaire.

Configurer les appareils avec Apple Configurator 2 (facultatif)
Pour les déploiements initiaux de plusieurs appareils en local, les organisations peuvent utiliser Apple Configurator 2. Cette app macOS gratuite vous permet de connecter vos appareils iOS et iPadOS à un ordinateur Mac via USB et d'installer la dernière version d'iOS ou d'iPadOS sur vos appareils, de configurer les réglages et restrictions, et d'installer des apps et autres contenus. Une fois la configuration initiale effectuée, vous pouvez toujours gérer les appareils à distance à l'aide de votre solution MDM.

L'interface utilisateur d'Apple Configurator 2 est centrée sur vos appareils et les tâches distinctes que vous souhaitez y effectuer. Comme l'app s'intègre avec Apple Business Manager, les appareils s'inscrivent automatiquement auprès de la solution MDM en exploitant les réglages de votre entreprise. Vous pouvez créer des processus personnalisés avec Apple Configurator 2 à l'aide de schémas permettant de combiner plusieurs tâches distinctes.

En savoir plus sur Apple Configurator 2 :
support.apple.com/fr-fr/apple-configurator

Appareils supervisés
La supervision offre des options de gestion supplémentaires pour les appareils iOS et iPadOS qui appartiennent à votre organisation, et permet d'appliquer des restrictions telles que désactiver AirDrop ou placer l'appareil en mode App individuelle. Elle permet également d'activer un filtre web via un proxy global pour, entre autres, s'assurer que le trafic web des utilisateurs respecte les consignes de l'entreprise ou empêcher l'utilisateur de rétablir les réglages par défaut de l'appareil. Par défaut, tous les appareils iOS et iPadOS sont non supervisés. Vous pouvez utiliser Apple Business Manager pour activer la supervision ou bien l'activer manuellement à l'aide d'Apple Configurator 2.

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 ultérieurement. Sinon, 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.

En savoir plus sur les restrictions pour les appareils supervisés :
support.apple.com/guide/mdm

Distribuer des apps et des livres

Apple propose des programmes complets pour aider votre entreprise à tirer parti des apps et des contenus de qualité disponibles pour iOS et iPadOS. Ces fonctionnalités vous permettent de distribuer les apps et les livres achetés via Apple Business Manager ou les apps développées en interne aux appareils et aux utilisateurs. Vos utilisateurs ont ainsi tous les outils à disposition pour gagner en productivité. Au moment de l'achat, vous devrez préciser votre méthode de distribution : distribution gérée ou codes de téléchargement.

Distribution gérée

La distribution gérée vous permet d'utiliser votre solution MDM ou Apple Configurator 2 pour gérer les apps et les livres achetés sur le Store Apple Business Manager dans tous les pays où l'app est disponible. Pour activer la distribution gérée, vous devez tout d'abord associer votre solution MDM à votre compte Apple Business Manager à l'aide d'un jeton sécurisé. Une fois connecté à votre serveur MDM, vous pouvez attribuer des apps et des livres achetés sur Apple Business Manager, même si l'App Store est désactivé sur l'appareil.

- **Attribuer des apps à des appareils.** À l'aide de votre solution MDM ou d'Apple Configurator 2, vous pouvez attribuer directement des apps aux appareils. Cette méthode élimine plusieurs étapes du déploiement initial, le rendant plus simple et plus rapide, et vous donne le contrôle complet des appareils et des contenus gérés. Lorsqu'une app est attribuée à un appareil, elle est envoyée en mode push vers l'appareil par le biais de la solution MDM. Aucune invitation n'est requise. Tous les utilisateurs de l'appareil ont accès à l'app concernée.
- **Attribuer des apps et des livres aux utilisateurs.** Une autre méthode consiste à utiliser votre solution MDM pour inviter les utilisateurs à télécharger des apps et des livres, en leur envoyant un e-mail ou une notification push. Pour accepter l'invitation, les utilisateurs se connectent sur leur appareil en utilisant leur identifiant Apple personnel. L'identifiant Apple est enregistré auprès du service Apple Business Manager, mais reste néanmoins complètement privé. Même l'administrateur ne peut pas le consulter. Une fois que les utilisateurs ont accepté l'invitation, ils sont immédiatement connectés à votre serveur MDM et peuvent commencer à recevoir les apps et les livres attribués. Les apps sont automatiquement disponibles au téléchargement sur tous les appareils de l'utilisateur, sans coûts ni efforts supplémentaires de votre part.

Lorsque l'appareil ou l'utilisateur n'a plus besoin des apps que vous lui avez attribuées, celles-ci peuvent être révoquées et réattribuées à des appareils et utilisateurs différents, de sorte que votre entreprise conserve la propriété et le contrôle total des apps achetées. Cependant, une fois que des livres ont été distribués, ils restent la propriété de leur destinataire et ne peuvent être ni révoqués ni réassignés.

Codes de téléchargement

Il est également possible de distribuer des contenus à l'aide de codes de téléchargement, ce qui est particulièrement utile pour les entreprises ne pouvant pas utiliser de solution MDM sur l'appareil de l'utilisateur final, par exemple les sociétés franchisées. Cette méthode transfère de façon définitive la propriété d'une app ou d'un livre à l'utilisateur qui utilise le code de contenu. Les codes sont fournis dans une feuille de calcul et sont propres à chaque app ou livre, quelle que soit la quantité achetée. Dès qu'un code est utilisé, la feuille de calcul du Store Apple Business Manager est actualisée, ce qui vous permet de connaître à tout moment le nombre de codes utilisés. Distribuez les codes via une solution MDM, Apple Configurator 2, un e-mail ou un site web interne.

Installer des apps et des contenus avec Apple Configurator 2 (facultatif)
En plus de l'installation et de la configuration de base, Apple Configurator 2 vous permet d'installer des apps et des contenus sur les appareils que vous configurez pour un utilisateur. Lorsque vous effectuez des déploiements personnalisés, vous pouvez préinstaller les apps pour gagner du temps et économiser de la bande passante. Si vous optez pour des déploiements non personnalisés, vous pouvez entièrement configurer vos appareils, jusqu'à l'écran d'accueil. Configurer des appareils avec Apple Configurator 2 permet d'installer des apps de l'App Store, des apps développées en interne et des documents. Les apps de l'App Store nécessitent Apple Business Manager et les apps qui prennent en charge le partage de fichiers peuvent recevoir des documents. Pour consulter ou récupérer des documents sur des appareils iOS et iPadOS, connectez-les à un Mac exécutant Apple Configurator 2.

3. Déploiement

Avec l'iPhone et l'iPad, les employés peuvent commencer à utiliser leurs appareils dès la sortie de l'emballage, sans demande l'aide du service informatique.

Distribuer les appareils

Une fois que les appareils ont été préparés et configurés comme décrit dans les deux premières étapes, ils sont prêts à être distribués. Si vous effectuez un déploiement personnalisé, distribuez les appareils aux utilisateurs qui pourront utiliser l'Assistant réglages simplifié pour personnaliser et finaliser la configuration. Pour les déploiements non personnalisés, distribuez les appareils aux employés présents ou placez-les dans les bornes conçues pour recharger et sécuriser les appareils.

Assistant réglages
Grâce à l'Assistant réglages, les utilisateurs peuvent déballer leurs appareils et aussitôt les activer, configurer les réglages de base et se mettre au travail. Après la configuration initiale, ils peuvent également personnaliser des options selon leurs préférences, comme la langue, le lieu, Siri, iCloud et Localiser mon iPhone. Les appareils inscrits à Apple Business Manager sont automatiquement inscrits auprès de la solution MDM directement depuis l'Assistant réglages.

Permettre aux utilisateurs de personnaliser l'appareil
Dans le cadre de déploiements personnalisés et BYOD, les utilisateurs peuvent personnaliser leurs appareils avec leur propre identifiant Apple pour améliorer leur productivité. En effet, ils pourront choisir eux-mêmes les apps et les contenus qui leur permettront de gagner en efficacité pour réaliser leurs tâches et leurs objectifs.

Identifiant Apple et identifiant Apple géré
Lorsque les employés se connectent à des services Apple comme FaceTime, iMessage, l'App Store et iCloud avec leur identifiant Apple, ils ont accès à un vaste éventail de contenus conçus pour simplifier leurs tâches professionnelles, améliorer leur productivité et les aider à mieux collaborer.

Comme tous les identifiants Apple, les identifiants Apple gérés permettent de se connecter à un appareil personnel. Ils sont aussi utilisés pour accéder à des services Apple comme iCloud, pour collaborer avec iWork et Notes, et pour se connecter à Apple Business Manager. Contrairement aux identifiants Apple, les identifiants Apple sont détenus et gérés par votre entreprise. Elle peut ainsi, par exemple, réinitialiser les mots de passe de ces identifiants et appliquer une administration basée sur les rôles. Certains réglages des identifiants Apple gérés sont restreints.

Les appareils inscrits via la fonctionnalité Inscription d'utilisateurs nécessitent un identifiant Apple géré. L'inscription d'utilisateurs permet d'utiliser un identifiant Apple personnel en complément, tandis que les autres options d'inscription prennent en charge soit un identifiant Apple personnel, soit un identifiant Apple géré. Seule l'option Inscription d'utilisateurs permet de gérer plusieurs identifiants Apple.

Pour profiter au maximum de ces services, les utilisateurs doivent utiliser leur propre identifiant Apple ou l'identifiant Apple géré créé pour eux. Les utilisateurs ne possédant pas d'identifiant Apple peuvent en créer un avant même de recevoir un appareil. L'Assistant réglages permet également aux utilisateurs de se créer un identifiant Apple personnel, s'ils n'en ont pas déjà un. La création d'un identifiant Apple ne nécessite aucune Information bancaire.

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

iCloud

Grâce à iCloud, les utilisateurs peuvent synchroniser automatiquement des contenus personnels, comme des contacts, calendriers, documents et photos, et les actualiser en permanence sur plusieurs appareils. Localiser mon permet aux utilisateurs de localiser un Mac, iPhone, iPad ou iPod touch égaré ou volé. Certains éléments d'iCloud, comme le trousseau iCloud et iCloud Drive, peuvent être désactivés grâce à des restrictions saisies manuellement sur l'appareil ou définies via la MDM. Les entreprises peuvent ainsi mieux contrôler quelles données sont stockées et sur quels comptes.

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

4. Gestion

Une fois vos utilisateurs opérationnels, une vaste gamme de fonctionnalités administratives est à votre disposition pour gérer et assurer la maintenance de vos appareils et contenus sur le long terme.

Administrer vos appareils

Les appareils gérés peuvent être administrés par le serveur MDM à travers une gamme de tâches spécifiques. Il s'agit notamment d'interroger des appareils pour recueillir des informations ou encore de mettre en place des tâches permettant de gérer les appareils perdus, volés ou qui ne respectent pas les règles.

Requêtes

Un serveur MDM peut interroger les appareils pour recueillir une multitude d'informations d'un point de vue matériel (numéro de série, identifiant UDID de l'appareil, adresse MAC Wi-Fi, etc.) ou logiciel (version d'iOS ou d'iPadOS, liste détaillée de toutes les apps installées sur l'appareil, etc.). Ces informations pourront ensuite être utilisées par votre solution MDM pour tenir à jour l'inventaire des appareils, faciliter la prise de décisions et automatiser des tâches de gestion, pour s'assurer par exemple que les utilisateurs se servent des apps préconisées.

Tâches de gestion

Lorsqu'un appareil est géré, un serveur MDM peut effectuer nombre de tâches administratives : modifier automatiquement les réglages de configuration sans intervention de l'utilisateur, effectuer des mises à jour logicielles sur les appareils verrouillés par code, verrouiller ou effacer un appareil à distance, ou encore 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 iPhone ou iPad de lancer la recopie vidéo AirPlay vers une destination spécifique, ou de mettre fin à une session AirPlay.

Mises à jour logicielles gérées

Vous pouvez empêcher les utilisateurs de mettre à jour un appareil supervisé à distance et manuellement pendant un certain temps. Le délai par défaut de cette restriction est de 30 jours et elle se déclenche au moment où Apple publie une mise à jour d'iOS ou d'iPadOS. Vous pouvez toutefois modifier la durée pendant laquelle les mises à jour sont empêchées, pour la fixer entre un et 90 jours. Vous pouvez également planifier les mises à jour logicielles des appareils supervisés à l'aide de votre solution MDM.

Mode Perdu

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.

Verrouillage d'activation

Avec iOS 7.1 et versions ultérieures, vous pouvez utiliser la solution MDM pour activer le Verrouillage d'activation lorsqu'un utilisateur lance Localiser mon sur un appareil supervisé. Cela vous permet de profiter de la capacité dissuasive du Verrouillage d'activation, tout en ayant la possibilité de la contourner si un utilisateur ne parvient pas à s'authentifier avec son identifiant Apple.

Déployer et gérer des contenus supplémentaires

Les entreprises ont souvent besoin de distribuer des apps pour assurer la productivité des utilisateurs. Elles doivent aussi contrôler la connexion des apps aux ressources internes, ou encore la sécurité des données des employés quittant l'entreprise. Tout cela, sur des appareils qui renferment également les apps et données personnelles des utilisateurs.

Portails d'apps internes

La plupart des serveurs MDM proposent un portail d'apps interne dans le cadre de leur solution. Vous avez aussi la possibilité de créer un portail d'apps interne où vos employés trouveront facilement des apps pour leur iPhone ou iPad. Les apps développées en interne, les URL des apps de l'App Store ou les codes Apple Business Manager peuvent être mis à disposition sous forme de liens sur ce portail, qui sert de référentiel unique aux utilisateurs. Vous pouvez gérer et sécuriser ce site de manière centralisée. Grâce au portail d'apps interne, les employés trouvent facilement les ressources approuvées dont ils ont besoin sans avoir à contacter l'équipe informatique.

Contenu géré

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

- **Apps gérées.** Sous iOS et iPadOS, les apps gérées permettent à une organisation de distribuer à distance des apps gratuites, payantes ou développées en interne à l'aide d'une solution MDM, tout en offrant le juste équilibre entre la protection des données de l'entreprise et le respect de la vie privée des utilisateurs. Les apps gérées peuvent être supprimées à distance par un serveur MDM ou lorsque les utilisateurs désinscrivent leurs appareils de celui-ci. La suppression d'une app a pour effet de supprimer les données qui lui sont associées. Si l'app reste attribuée à un utilisateur via Apple Business Manager, ou si cet utilisateur s'est servi d'un code de téléchargement d'app avec son identifiant Apple personnel, l'app pourra de nouveau être téléchargée sur l'App Store, mais elle ne sera pas gérée via la solution MDM.
- **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 solution MDM et de son intégration avec vos systèmes internes, les données utiles de compte peuvent aussi être prérenseignées avec le nom de l'utilisateur, son adresse e-mail et, le cas échéant, les identités de certificat pour l'authentification et la signature.
- **Livres et documents gérés.** Les outils de la MDM, les livres, livres ePub et documents PDF peuvent être directement transférés sur les appareils, de sorte que les employés disposent toujours des ressources dont ils ont besoin. Parallèlement, les livres gérés peuvent être partagés uniquement avec d'autres apps gérées ou envoyés par e-mail en utilisant des comptes gérés. Lorsque ces documents ne sont plus utiles, ils peuvent être supprimés à distance. Les livres achetés via Apple Business Manager peuvent être distribués par le biais de la distribution gérée des livres, mais ne peuvent pas être révoqués ni réattribués. Un livre déjà acheté par l'utilisateur ne peut pas être géré, à moins de lui être explicitement attribué via Apple Business Manager.

Configuration des apps gérées

Les développeurs d'apps peuvent identifier les réglages et fonctionnalités pouvant être activés lorsqu'une app est installée en tant qu'app gérée. Ces réglages de configuration peuvent être appliqués avant ou après l'installation de l'app gérée. Le service informatique peut, par exemple, établir un ensemble de préférences par défaut pour une app SharePoint afin que l'utilisateur n'ait pas besoin de configurer manuellement les réglages du serveur.

Les principaux fournisseurs de solutions MDM ont fondé la communauté AppConfig et mis au point une structure normalisée compatible avec la configuration des apps gérées et exploitable par tous les développeurs. L'objectif de la communauté AppConfig est de partager des outils et des bonnes pratiques en rapport avec les capacités natives des systèmes d'exploitation mobiles. La communauté contribue à créer une manière plus simple, ouverte et cohérente de configurer et de sécuriser les apps mobiles, afin d'encourager l'adoption de la mobilité dans les entreprises.

En savoir plus sur la communauté AppConfig :
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 partage avec les apps ou les services dans le nuage propres aux utilisateurs.

- **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.
- **Mode App individuelle.** Ce réglage permet de limiter l'appareil iOS ou iPadOS à une seule app, ce qui peut être très pratique pour des appareils servant de bornes ou utilisés pour une seule tâche, comme dans un magasin ou à l'hôpital pour l'enregistrement à l'arrivée. Les développeurs peuvent également activer cette fonctionnalité dans leurs apps afin que celles-ci puissent accéder au mode App individuelle et le quitter de façon indépendante.
- **Empêcher la sauvegarde.** Cette restriction empêche les apps gérées de sauvegarder des données sur iCloud ou sur un ordinateur. Ne pas autoriser la sauvegarde permet d'éviter que les données des apps gérées ne soient récupérées si l'app est supprimée via la MDM, mais réinstallée ensuite par l'utilisateur.

Options d’assistance

Apple propose toute une gamme de programmes et d’options d’assistance destinés aux utilisateurs iOS et iPadOS et aux administrateurs informatiques.

AppleCare for Enterprise

Les entreprises désirant une couverture complète peuvent opter pour AppleCare for Enterprise, qui allégera la charge de travail de leur service d’assistance interne en fournissant aux employés une assistance technique par téléphone 24 heures sur 24 et 7 jours sur 7, avec un temps de réponse d’une heure maximum pour les problèmes prioritaires. Ce programme offre toute l’assistance nécessaire aux services informatiques pour la totalité du matériel et des logiciels Apple, ainsi qu’une assistance pour les déploiements et scénarios d’intégration complexes, notamment la MDM et Active Directory.

AppleCare OS Support

AppleCare OS Support offre à votre service informatique une assistance par téléphone et e-mail de niveau entreprise pour les déploiements iOS, iPadOS, macOS et macOS Server. Il propose une assistance 24 heures sur 24 et 7 jours sur 7 et l’aide d’un responsable de compte technique, selon le niveau d’assistance souscrit. AppleCare OS Support vous met directement en relation avec des techniciens pour toute question relative à des problèmes d’intégration, de migration et de fonctionnement avancé des serveurs, améliorant l’efficacité de votre personnel informatique au niveau du déploiement et de la gestion des appareils, ainsi que de la résolution des problèmes.

AppleCare Help Desk Support

Le contrat d’assistance AppleCare Help Desk Support vous assure un accès téléphonique prioritaire aux équipes d’assistance technique d’Apple. Il comprend également un ensemble d’outils permettant de diagnostiquer et de résoudre les problèmes liés au matériel Apple, ce qui peut aider les organisations d’envergure à gérer plus efficacement leurs ressources, à améliorer les temps de réponse et à réduire les coûts de formation. AppleCare Help Desk Support comporte une assistance illimitée pour le diagnostic d’incidents matériels et logiciels ainsi que le dépannage et l’isolement des problèmes affectant les appareils iOS et iPadOS.

AppleCare pour les utilisateurs d’appareils iOS et iPadOS

Chaque appareil iOS ou iPadOS s’accompagne d’une garantie limitée d’un an et d’une assistance technique téléphonique gratuite valable pendant 90 jours à compter de la date d’achat. La couverture peut être étendue à deux ans à compter de la date d’achat de l’appareil par la souscription d’un contrat AppleCare+ pour iPhone, AppleCare+ pour iPad ou de AppleCare+ pour iPod touch. Vous pourrez alors appeler les experts de l’assistance technique Apple aussi souvent que vous le souhaitez et obtenir des réponses à toutes vos questions. Apple fournit également des options de service pratiques lorsque les appareils nécessitent une réparation. De plus, ces contrats incluent la prise en charge de deux incidents relevant de dégâts accidentels, chacun étant soumis à des frais supplémentaires.

Programme d’assistance directe iOS

Le Programme d’assistance directe iOS inclus dans votre contrat AppleCare+ permet à votre service d’assistance d’analyser les appareils pour détecter les problèmes sans contacter AppleCare ni se rendre dans un Apple Store.
Si nécessaire, votre entreprise peut commander directement un iPhone, iPad ou iPod touch de rechange ou un accessoire intégré.

En savoir plus sur les programmes AppleCare :
apple.com/fr/support/professional

Synthèse

Votre entreprise, qu'elle déploie des iPhone ou des iPad pour un groupe d'utilisateurs ou dans l'ensemble de sa structure, dispose de nombreuses options pour déployer et gérer facilement les appareils. En choisissant les bonnes stratégies pour votre organisation, vous pourrez aider vos collaborateurs à gagner en productivité et à renouveler leurs méthodes de travail.

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

En savoir plus sur les réglages de la gestion des appareils mobiles pour les administrateurs informatiques :
support.apple.com/guide/mdm

En savoir plus sur Apple Business Manager :
support.apple.com/guide/apple-business-manager

En savoir plus sur les identifiants Apple gérés pour les entreprises :
apple.com/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

En savoir plus sur Apple at Work :
www.apple.com/fr/business/

En savoir plus sur les fonctionnalités pour les administrateurs informatiques :
www.apple.com/fr/business/it/

En savoir plus sur la sécurité des plateformes Apple :
www.apple.com/security/

Découvrir les programmes AppleCare :
www.apple.com/fr/support/professional/

Découvrir les formations et certifications Apple :
training.apple.com

Contacter les Services professionnels Apple :
consultingservices@apple.com

La disponibilité des apps et des livres peut varier en fonction des pays ou régions et du choix des développeurs. Consultez la disponibilité des programmes et des contenus. Certaines fonctionnalités nécessitent une connexion Wi-Fi. Certaines fonctionnalités ne sont pas disponibles dans tous les pays. Pour connaître la configuration système minimale et recommandée pour iCloud, rendez-vous sur 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 d'Apple Inc., déposées aux États-Unis et dans d'autres pays. iPadOS est une marque d'Apple Inc. App Store, AppleCare, Apple Store, Apple Books, iCloud, iCloud Drive et le trousseau iCloud sont des marques de service d'Apple Inc., déposées aux États-Unis et dans d'autres pays. iOS est une marque ou une marque déposée de Cisco aux États-Unis et dans d'autres pays, utilisée ici sous licence. Les autres noms de produits et de sociétés mentionnés dans ce document appartiennent à leurs propriétaires respectifs. Les caractéristiques des produits sont susceptibles d'être modifiées sans préavis. Les informations contenues dans ce document sont fournies à titre indicatif uniquement ; Apple n'assume aucune responsabilité quant à leur utilisation.