Présentation du déploiement d'iOS en entreprise

L'iPad et l'iPhone peuvent transformer votre activité et le mode de travail de vos employés. Ils peuvent stimuler de façon significative la productivité et donner à vos employés la liberté et la flexibilité de mettre en œuvre de nouvelles méthodes de travail. Adopter cette nouvelle façon 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. En gérant iOS, les services informatiques peuvent offrir aux utilisateurs un accès aux outils les mieux adaptés à leur travail, tout en protégeant les données de l'entreprise. En fin de compte, tout le monde en profite : le personnel est remotivé et les nouvelles opportunités professionnelles se multiplient.

Ce document propose des conseils sur les facteurs à prendre en considération pour optimiser votre déploiement iOS. Il traite les sujets suivants :

- Modèles de déploiement
- Préparer votre infrastructure
- Configuration initiale
- Configurer et gérer
- Distribuer des apps et des livres
- Gestion continue
- Options d'assistance

Modèles de déploiement

Évaluer les modèles de déploiement et choisir le mieux adapté à votre entreprise constitue une première étape importante. Vous pouvez aborder le déploiement de diverses manières, en fonction de qui est propriétaire de l'appareil et de votre scénario préféré. Commencez par évaluer et identifier les modèles de déploiement les mieux adaptés à votre entreprise.

Il existe trois scénarios courants de déploiement d'appareils iOS au sein de l'entreprise :

- Appareil personnalisé (BYOD)
- Appareil personnalisé (détenu par l'entreprise)
- Appareil non personnalisé (partagé)

Bien que la plupart des entreprises privilégient un modèle plutôt qu'un autre, il est possible que votre propre environnement en utilise plusieurs. Par exemple, une société de vente au détail pourrait déployer une stratégie d'appareils personnalisés (BYOD) en autorisant les employés à configurer un iPad personnel tout en assurant la protection et la gestion des ressources sans affecter les données et apps personnelles de l'utilisateur. Les magasins de cette société pourraient toutefois aussi déployer une stratégie d'appareils non personnalisés (appareils partagés), en autorisant le partage d'iPad entre plusieurs employés pour le traitement des transactions clients.

Étudier ces modèles de déploiement de façon plus détaillée vous aidera à identifier le mieux adapté à votre propre environnement. Vous pourrez ensuite sélectionner les programmes et outils adaptés dans la Référence technique pour le déploiement d'iOS, disponible en ligne.

Référence technique pour le déploiement d'iOS : https://help.apple.com/deployment/ios

Appareil personnalisé (BYOD)

Dans le cadre d'un déploiement BYOD (Bring Your Own Device, Apportez vos appareils personnels), qui constitue le scénario le plus courant, les utilisateurs sont autorisés à configurer leurs appareils personnels avec leur identifiant Apple. Pour pouvoir accéder aux ressources de l'entreprise, les utilisateurs peuvent configurer manuellement les réglages, installer un profil de configuration ou, ce qui est plus courant, inscrire leurs appareils auprès d'une solution de gestion des appareils mobiles (MDM).

L'un des avantages que présente l'utilisation d'une solution MDM pour inscrire les appareils personnels est de permettre la gestion sécurisée des ressources et données de l'entreprise tout en respectant la vie privée, ainsi que les apps et données personnelles de l'utilisateur. Le service informatique peut appliquer des réglages, surveiller la conformité aux règles de l'entreprise et supprimer les données et apps professionnelles sans toucher aux données et apps personnelles de chaque appareil.

Le tableau ci-dessous illustre les responsabilités de l'administrateur et de l'utilisateur pour un déploiement d'appareils personnalisés (BYOD) :

Préparer votre infrastructure	
Administrateur : • Évaluer votre infrastructure existante, notamment le Wi-Fi, le VPN, et les serveurs de messagerie et de calendriers. • Étudier, obtenir et déployer une solution MDM comme le Gestionnaire de profils. • S'inscrire au Programme d'achats en volume (VPP).	**Utilisateurs :** • Déballer et activer l'appareil. • Créer un identifiant Apple, ainsi que des comptes iTunes Store et iCloud, le cas échéant.
Configurer	
Administrateur : • Inscrire les appareils en utilisant le libre-service. Configurer les comptes, réglages et restrictions sans fil via une solution MDM en se basant sur les règles d'utilisateur/de groupe définies par votre établissement. • Les sociétés peuvent également fournir aux utilisateurs des réglages pour des comptes individuels. Les règles peuvent en outre être transmises avec Exchange ou installées via un profil de configuration.	**Utilisateurs :** • Inscrire l'appareil auprès du serveur MDM. • La MDM transmet automatiquement les réglages et la configuration de l'appareil. • Les utilisateurs peuvent aussi installer manuellement les profils de configuration ou configurer les réglages que vous leur aurez fournis.
Distribuer des apps et des livres	
Administrateur : • Acheter des apps et des livres par le biais du Programme d'achats en volume (VPP) et les attribuer aux utilisateurs via votre solution MDM. • Envoyer aux utilisateurs une invitation au Programme d'achats en volume. Si vous utilisez des codes de téléchargement, les distribuer par e-mail ou via un site web interne. • Distribuer des apps internes du Programme pour développeurs iOS en entreprise (iDEP, iOS Developer Enterprise Program) et des livres internes en les hébergeant sur un serveur web ou sur votre solution MDM. • Installer Caching Server pour accélérer la distribution de contenu sur le réseau local.	**Utilisateurs :** • Accepter l'invitation au Programme d'achats en volume (VPP). • Télécharger et installer les apps et livres attribués par l'établissement.
Gestion continue	
Administrateur : • Utiliser votre solution MDM pour révoquer des apps et les réattribuer à d'autres utilisateurs, en fonction des besoins. • Un administrateur peut utiliser une solution MDM pour interroger les appareils gérés afin de surveiller la conformité, ou déclencher des alertes si un utilisateur ajoute des apps ou du contenu non approuvés. • Une solution MDM permet également de verrouiller les appareils ou de réinitialiser leur mot de passe, d'effacer à distance les comptes ou données gérés, ou d'effacer complètement un appareil.	**Utilisateurs :** • Sauvegarder l'appareil sur iTunes ou iCloud, pour préserver des documents et autres contenus personnels. • Si l'appareil est perdu ou volé, l'utilisateur peut connaître sa position avec Localiser mon iPhone. • Lorsque la relation MDM est supprimée, les comptes et données gérés sont supprimés, mais les apps, les livres, les données et le contenu personnels sont conservés.

Appareil personnalisé (détenu par l'entreprise)

Vous pouvez également utiliser le modèle d'appareil personnalisé lorsque vous déployez des appareils iOS qui appartiennent à votre entreprise. Le service informatique peut configurer les réglages de base sur les appareils avant de confier ceux-ci aux utilisateurs ou, comme avec le modèle BYOD, fournir des instructions ou des profils de configuration qui seront appliqués par les utilisateurs eux-mêmes.

Autre option, vous pouvez demander aux utilisateurs d'inscrire l'appareil auprès d'une solution MDM qui fournit à distance les réglages et apps propres à l'entreprise. Pour les appareils achetés directement auprès d'Apple ou d'un opérateur ou Revendeur agréé Apple participant, vous pouvez également tirer profit du Programme d'inscription des appareils (DEP) pour inscrire automatiquement les nouveaux appareils auprès de votre solution MDM. 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.

Le tableau ci-dessous illustre les responsabilités de l'administrateur et de l'utilisateur pour un déploiement d'appareils personnalisés (détenus par l'entreprise) :

Préparer votre infrastructure	
Administrateur : • Évaluer votre infrastructure existante, notamment le Wi-Fi, le VPN, et les serveurs de messagerie et de calendriers. • Étudier, obtenir et déployer une solution MDM comme le Gestionnaire de profils. • S'inscrire aux programmes DEP et VPP.	**Utilisateurs :** • Créer un identifiant Apple, ainsi que des comptes iTunes Store et iCloud, le cas échéant.

Configurer	
Administrateur : • Depuis le site web du Programme d'inscription des appareils (DEP), lier vos serveurs virtuels à votre solution MDM. • Rationaliser l'inscription via le Programme d'inscription des appareils en attribuant des appareils à vos serveurs MDM virtuels par numéro de commande ou numéro de série. • Attribuer des appareils dans le programme DEP pour assurer leur supervision et simplifier leur inscription auprès du serveur MDM. • Utiliser Apple Configurator pour configurer et superviser l'appareil (alternative à l'option ci-dessus). • Utiliser votre solution MDM pour configurer et installer des comptes, réglages et restrictions sans fil, ou utiliser une connexion USB avec Apple Configurator.	**Utilisateurs :** • Un appareil iOS est fourni à l'utilisateur. Si cet appareil a été configuré via Apple Configurator, l'utilisateur n'a pas à se préoccuper de la configuration. • Saisir les informations d'identification de l'établissement dans l'Assistant réglages du programme DEP (facultatif). • Utiliser l'Assistant réglages pour personnaliser l'appareil et saisir un identifiant Apple personnel. • Inscrire l'appareil auprès du serveur MDM. • La MDM transmet automatiquement les réglages et la configuration de l'appareil.

Distribuer des apps et des livres	
Administrateur : • Acheter des apps et des livres par le biais du Programme d'achats en volume (VPP) et les attribuer aux utilisateurs via votre solution MDM. • Télécharger votre jeton du Store du Programme d'achats en volume et le lier à votre solution MDM. • Envoyer aux utilisateurs une invitation au Programme d'achats en volume. Si vous utilisez des codes de téléchargement, les distribuer par e-mail ou via un site web interne. • Distribuer des apps internes du Programme pour développeurs iOS en entreprise (iDEP, iOS Developer Enterprise Program) et des livres internes en les hébergeant sur un serveur web ou sur votre solution MDM. • Installer Caching Server pour accélérer la distribution de contenu sur le réseau local.	**Utilisateurs :** • Accepter l'invitation au Programme d'achats en volume. • Télécharger et installer les apps et livres attribués par l'entreprise. • Les apps peuvent être installées automatiquement sur l'appareil de l'utilisateur.

Gestion continue	
Administrateur : • Utiliser votre solution MDM pour révoquer des apps et les réattribuer à d'autres utilisateurs, en fonction des besoins. • Un administrateur peut utiliser une solution MDM pour interroger les appareils gérés afin de surveiller la conformité, ou déclencher des alertes si un utilisateur ajoute des apps ou du contenu non approuvés. • Une solution MDM permet également de verrouiller les appareils ou de réinitialiser leur mot de passe, d'effacer à distance les comptes ou données gérés, ou d'effacer complètement un appareil.	**Utilisateurs :** • Sauvegarder l'appareil sur iTunes ou iCloud, pour préserver des documents et autres contenus personnels. • Si l'appareil est perdu ou volé, l'utilisateur peut le localiser avec Localiser mon iPhone.

Appareil non personnalisé (partagé)

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 d'appareils non personnalisés, les utilisateurs ne sont généralement pas autorisés à installer des apps sur les appareils ni à y stocker des données personnelles.

Les appareils non personnalisés sont généralement inscrits auprès d'une solution MDM et supervisés avec Apple Configurator. Cela permet d'actualiser ou de restaurer le contenu figurant sur l'appareil si un utilisateur le modifie.

Le tableau ci-dessous illustre les responsabilités de l'administrateur et de l'utilisateur pour un déploiement d'appareils non personnalisés (partagés) :

Préparer votre infrastructure	
Administrateur : • Évaluer votre infrastructure existante, notamment le Wi-Fi, le VPN, et les serveurs de messagerie et de calendriers. • Étudier, obtenir et déployer une solution MDM comme le Gestionnaire de profils. • S'inscrire au Programme d'achats en volume (VPP).	**Utilisateurs :** • Aucune action n'est requise à ce stade.

Configurer	
Administrateur : • Déballer l'appareil et (éventuellement) le marquer pour inventaire. • Utiliser Apple Configurator pour configurer et superviser les appareils. • Utiliser Apple Configurator pour inscrire les appareils auprès du serveur MDM (facultatif). • Utiliser Apple Configurator ou votre solution MDM pour installer des comptes, réglages et restrictions.	**Utilisateurs :** • Aucune action n'est requise à ce stade.

Distribuer des apps et des livres	
Administrateur : • Acheter des apps et des livres avec le Programme d'achats en volume et les déployer en utilisant des codes de téléchargement pour assurer leur installation et leur gestion via Apple Configurator. • Distribuer des apps internes du Programme pour développeurs iOS en entreprise (iDEP, iOS Developer Enterprise Program) via Apple Configurator. • Distribuer des livres internes en les hébergeant sur un serveur web ou sur votre solution MDM. • Ajouter Apple Configurator pour les apps comme pour les livres.	**Utilisateurs :** • Aucune action n'est requise à ce stade.

Gestion continue

Administrateur :

- Utiliser Apple Configurator pour mettre à jour iOS sur l'appareil.
- Utiliser Apple Configurator pour rétablir régulièrement la configuration standard des appareils.
- Vous pouvez utiliser une solution MDM pour interroger les appareils gérés afin de surveiller la conformité, ou déclencher des alertes si un utilisateur ajoute des apps ou du contenu non approuvés.
- Une solution MDM permet également de verrouiller les appareils ou de réinitialiser leur mot de passe, d'effacer à distance les comptes ou données gérés, ou d'effacer complètement un appareil.
- Une sauvegarde régulière du Mac exécutant Apple Configurator est nécessaire, les achats du Programme d'achats en volume étant gérés au niveau local.
- Une solution MDM peut superviser les appareils en utilisant le mode app individuelle.

Utilisateurs :

- Aucune action n'est requise à ce stade.

Préparer votre infrastructure

Après avoir choisi les modèles de déploiement appropriés, étudiez votre infrastructure existante pour vous assurer que votre entreprise pourra profiter pleinement de tout ce qu'iOS a à offrir. L'iPhone et l'iPad s'intègrent sans problème dans la plupart des environnements informatiques d'entreprise standard. Toutefois, il peut y avoir des moyens d'optimiser votre environnement réseau pour la prise en charge des technologies essentielles d'iOS.

Wi-Fi et réseau

Un accès stable et fiable à un réseau sans fil est essentiel pour la configuration des appareils iOS. Vérifiez que le réseau Wi-Fi de votre entreprise peut prendre en charge plusieurs appareils avec connexion simultanée de tous vos employés. 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'iTunes Store.

Évaluez votre infrastructure VPN pour vous assurer que les utilisateurs pourront se servir de leurs appareils iOS pour accéder à distance et de façon sécurisée aux ressources de l'entreprise. Envisagez d'utiliser la fonctionnalité VPN à la demande d'iOS 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 possibilité 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 pour fonctionner correctement avec Bonjour, le protocole réseau standard d'Apple ne réclamant aucune configuration. Bonjour permet aux appareils de trouver automatiquement des services sur un réseau. Les appareils iOS 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.

Pour plus de détails sur le Wi-Fi et la configuration réseau pour les déploiements en entreprises, reportez-vous au document Référence technique pour le déploiement d'iOS. L'Annexe A, « Infrastructure Wi-Fi », explique les technologies et normes sans fil exploitées par les appareils iOS et fournit des informations sur la conception de réseaux sans fil.

Accédez en ligne à la Référence technique pour le déploiement d'iOS : www.help.apple.com/deployment/ios

Pour en savoir plus sur Bonjour : www.apple.com/fr/support/bonjour

E-mails, 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 basé sur le nuage, vérifiez que vous avez un nombre suffisant de licences pour prendre en charge le nombre prévu d'appareils iOS qui seront connectés. Si vous n'utilisez pas Exchange, iOS est également compatible avec des serveurs standard, notamment IMAP, POP, SMTP, CalDAV, CardDAV et LDAP.

La gestion des appareils mobiles (MDM)

Pour configurer et gérer sans fil des appareils iOS, il vous faudra une solution de gestion des appareils mobiles (MDM). La gestion des appareils mobiles permet aux entreprises d'inscrire de façon sécurisée des appareils dans l'environnement de l'entreprise, de configurer et de mettre à jour sans fil les réglages, de surveiller la conformité aux règles, de déployer des apps et des livres, et d'effacer ou de verrouiller à distance les appareils gérés.

Il existe différentes solutions MDM tierces compatibles avec différentes plates-formes serveur. Chaque solution offre 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 entreprise.

En plus des solutions tierces, Apple offre une solution MDM appelée Gestionnaire de profils, intégrée à OS X Server. Le Gestionnaire de profils facilite la configuration des appareils iOS en fonction des spécifications de votre entreprise. Il fournit trois composants : un outil d'administration en ligne, un portail utilisateur en libre-service pour l'inscription des appareils et un serveur MDM.

Pour en savoir plus sur la gestion des appareils mobiles : www.apple.com/ipad/business/it/management.html

Pour en savoir plus sur le Gestionnaire de profils : www.apple.com/fr/osx/server/features/#profile-manager

Caching Server

Caching Server, une fonctionnalité intégrée à OS X Server, 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. Caching Server accélère le téléchargement et la diffusion de logiciels via l'App Store, le Mac App Store, l'iTunes Store et l'iBooks Store. Et Caching Server peut également mettre en cache les mises à jour de logiciels pour accélérer leur téléchargement sur les appareils iOS.

Pour en savoir plus sur Caching Server : www.apple.com/fr/osx/server/features/#caching-server

Prise en charge d'iTunes

iTunes n'est pas nécessaire pour les appareils équipés d'iOS 5 (ou version ultérieure), mais il peut être utile de le prendre en charge afin que les utilisateurs puissent activer leurs appareils, synchroniser des médias ou sauvegarder le contenu de leurs appareils sur un ordinateur.

iTunes prend en charge plusieurs options de configuration de déploiement adaptées à un usage en entreprise. Cela inclut notamment la désactivation de l'accès à des contenus explicites, la définition des services réseau auxquels les utilisateurs peuvent accéder à partir d'iTunes et la détermination des dernières mises à jour logicielles que peuvent installer les utilisateurs.

Pour en savoir plus sur le déploiement d'iTunes : help.apple.com/iosdeployment/itunes

Configuration initiale

Une fois votre infrastructure préparée, vous devrez déployer vos appareils iOS auprès de vos utilisateurs. Vous pouvez aborder la configuration initiale des appareils de diverses manières, en fonction de qui est propriétaire de l'appareil et de votre modèle de déploiement préféré. Explorez ces diverses possibilités avant de vous lancer.

Assistant réglages

Leur appareil à peine sorti de l'emballage, les utilisateurs peuvent l'activer, configurer les réglages de base et se mettre à travailler dans la foulée grâce à l'Assistant réglages d'iOS. En plus de pouvoir choisir les réglages de base, les employés peuvent également personnaliser leurs préférences personnelles, comme la langue, le lieu, Siri, iCloud et Localiser mon iPhone. L'Assistant réglages permet également aux utilisateurs de se créer un identifiant Apple personnel, s'ils n'en ont pas déjà un. Lorsque des appareils sont inscrits au Programme d'inscription des appareils (DEP), ils peuvent être automatiquement inscrits auprès du serveur MDM, directement depuis l'Assistant réglages.

Configurer les appareils avec Apple Configurator

Si les appareils de votre entreprise sont gérés de façon centralisée par le service informatique et ne sont pas configurés par les utilisateurs eux-mêmes, utilisez Apple Configurator pour activer rapidement les appareils, définir et appliquer les configurations, superviser les appareils, installer des apps et mettre à jour les appareils avec la dernière version d'iOS. Apple Configurator est une application gratuite pour OS X, disponible en téléchargement sur le Mac App Store. Les appareils doivent être connectés à un Mac via USB pour effectuer ces tâches. Vous pouvez aussi restaurer une sauvegarde sur des appareils. Cette restauration installera les données d'apps, et appliquera les réglages de l'appareil ainsi que la disposition des écrans d'accueil.

Identifiant Apple

Un identifiant Apple est une identité servant à se connecter à différents services Apple comme FaceTime, iMessage, l'iTunes Store, l'App Store, l'iBooks Store et iCloud. Ces services permettent aux utilisateurs d'accéder à un large éventail de contenus pour rationaliser les tâches professionnelles, augmenter la productivité et favoriser la collaboration.

Pour profiter au maximum de ces services, les utilisateurs doivent utiliser leur propre identifiant Apple. S'ils n'en ont pas, ils peuvent s'en créer un avant même de recevoir un appareil ou utiliser l'Assistant réglages intégré à iOS. Cet assistant permet aux utilisateurs de créer aisément un identifiant Apple directement depuis leurs appareils iOS. Aucun numéro de carte bancaire ne leur sera demandé.

Lorsque les appareils ne sont pas personnalisés par les utilisateurs, comme dans un déploiement d'appareils partagés, Apple Configurator peut utiliser un même identifiant Apple d'administrateur pour installer des apps et du contenu sur plusieurs appareils.

Découvrez comment créer un identifiant Apple : appleid.apple.com

iCloud

iCloud permet aux utilisateurs de synchroniser automatiquement documents et contenus personnels tels que les contacts, calendriers, documents et photos, et de les actualiser sur plusieurs appareils*. Les utilisateurs peuvent également sauvegarder automatiquement un appareil iOS lorsque celui-ci est connecté à un réseau Wi-Fi et utiliser Localiser mon iPhone pour localiser un iPhone, iPad, iPod touch ou Mac égaré ou volé.

Certains services, comme Flux de photos, Trousseau iCloud, iCloud Drive et Sauvegarde, peuvent être désactivés par l'utilisation de restrictions programmées soit manuellement sur l'appareil, soit via des profils de configuration. Une solution MDM peut également permettre d'éviter que des apps gérées soient sauvegardées sur iCloud. Ainsi, les utilisateurs peuvent profiter de tous les avantages d'iCloud pour gérer leurs données personnelles sans que les données de l'entreprise soient stockées sur iCloud. Les données des comptes d'entreprise tels qu'Exchange ou les données stockées dans des apps internes à l'entreprise ne sont pas sauvegardées sur iCloud.

Remarque : iCloud n'est pas disponible dans tous les pays, et les fonctionnalités d'iCloud varient en fonction des zones géographiques.

Pour en savoir plus sur iCloud : www.apple.com/fr/icloud

Configurer et gérer

Une fois les appareils configurés pour une utilisation initiale, il existe différentes options de configuration et de gestion de l'accès aux services de l'entreprise. Le service informatique peut distribuer des profils de configuration ou configurer les appareils à distance via une solution MDM. Des options de configuration supplémentaires sont disponibles pour les appareils supervisés.

Profils de configuration

Un profil de configuration est un fichier XML qui vous permet de distribuer des informations de configuration à un appareil iOS. Les profils de configuration automatisent la configuration des réglages, comptes, restrictions et informations d'identification. Les profils de configuration peuvent être installés via une pièce jointe à un e-mail, téléchargés depuis une page web ou installés sur les appareils via Apple Configurator. Si vous avez besoin de configurer un grand nombre d'appareils ou que vous préférez tout simplement un modèle de déploiement à distance limitant les interventions, vous pouvez distribuer les profils de configuration via votre solution MDM.

Configurer les appareils grâce à la gestion des appareils mobiles (MDM)

La gestion des appareils mobiles permet aux entreprises d'inscrire et de configurer de façon sécurisée des appareils appartenant aux employés ou à l'entreprise dans un environnement professionnel. Une solution MDM permet aux administrateurs informatiques de configurer et de mettre à jour les réglages, de surveiller la conformité aux règles de l'entreprise, et d'effacer ou de verrouiller à distance les appareils gérés. La gestion des appareils mobiles permet également de distribuer, de gérer et de configurer les apps et livres achetés via le Programme d'achats en volume ou développés en interne.

Pour permettre leur gestion, les appareils sont inscrits auprès d'un serveur MDM à l'aide d'un profil de configuration d'inscription. Les utilisateurs peuvent s'inscrire eux-mêmes directement ou, pour les appareils appartenant à l'entreprise, vous pouvez automatiser l'inscription au serveur MDM via le Programme d'inscription des appareils. Lorsqu'un administrateur initie une règle, option ou commande MDM, l'appareil iOS est informé de cette action par le biais du service de notification push d'Apple (Apple Push Notification service ou APNs). Il peut ainsi communiquer directement avec le serveur MDM via 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.

Appareils supervisés

La supervision offre un niveau supérieur de gestion pour les appareils qui appartiennent à votre organisation. Elle permet en effet d'appliquer d'autres restrictions comme la désactivation d'iMessage ou de Game Center, ou d'empêcher les utilisateurs de modifier les réglages des comptes. Par défaut, tous les appareils iOS sont non supervisés. Vous pouvez associer la supervision à la gestion à distance via une solution MDM pour gérer les réglages et restrictions supplémentaires. Grâce au Programme d'inscription des appareils, la supervision peut être activée sans fil sur l'appareil, dans le cadre du processus de configuration, ou par le biais d'Apple Configurator.

Programme d'inscription des appareils

Avec le Programme d'inscription des appareils (DEP), les entreprises ayant acheté des appareils iOS directement auprès d'Apple ou d'un opérateur ou Revendeur agréé Apple participant peuvent inscrire aisément les appareils auprès du serveur MDM, et configurer et superviser ces appareils sans fil. Avec le Programme d'inscription des appareils, tous vos appareils peuvent être configurés sans avoir à toucher physiquement chacun d'eux.

Le processus est simple : après s'être inscrits au programme, les administrateurs se connectent à son site web, puis ils lient le programme à leur serveur MDM et attribuent des appareils aux utilisateurs. Une fois que des appareils ont été attribués aux utilisateurs, ceux-ci peuvent suivre les étapes de l'Assistant réglages de leur appareil pour installer automatiquement toutes les configurations, restrictions ou commandes spécifiées par la MDM.

Pour en savoir plus sur le Programme d'inscription des appareils (DEP) : www.apple.com/business/dep

Apple Configurator

Apple Configurator, une application OS X gratuite disponible sur le Mac App Store, permet aux administrateurs de configurer via USB plusieurs appareils iOS à la fois avant de les fournir aux utilisateurs. Avec cet outil, votre personnel informatique peut rapidement configurer et mettre à jour plusieurs appareils avec la dernière version d'iOS, configurer les réglages et restrictions des appareils, et installer des apps et du contenu.

Apple Configurator est idéal lorsque les utilisateurs partagent des appareils iOS qui doivent être actualisés et disposer de réglages, règles, apps et données appropriés à jour. Avant d'utiliser votre solution MDM pour gérer les réglages, règles et apps, vous pouvez vous servir d'Apple Configurator pour activer la supervision des appareils, et ainsi disposer de restrictions et de commandes supplémentaires.

Pour en savoir plus sur Apple Configurator : help.apple.com/configurator/mac

Distribuer des apps et des livres

Apple propose des programmes complets pour aider votre entreprise à tirer profit des apps et du contenu de qualité disponibles pour iOS. Ces programmes vous permettent de distribuer à distance des apps et du contenu directement sur les appareils des employés, et de leur fournir tout ce dont ils ont besoin pour être productifs.

Programme d'achats en volume

Le Programme d'achats en volume (VPP) permet aux entreprises d'acheter des livres et des apps iOS en volume et de les distribuer aux employés.

Et vous pouvez également obtenir des apps iOS B2B personnalisées, conçues sur mesure par des développeurs tiers et distribuées de façon privée via le Store du Programme d'achats en volume (VPP). Les développeurs inscrits au Programme pour développeurs iOS en entreprise peuvent soumettre des apps pour une distribution d'entreprise à entreprise à l'aide d'iTunes Connect. Le processus est identique à la soumission d'apps sur l'App Store.

Les solutions MDM s'intègrent avec le Programme d'achats en volume et peuvent être utilisées pour attribuer des apps et des livres aux utilisateurs. Lorsqu'un utilisateur donné n'a plus besoin d'une app, vous pouvez utiliser votre solution MDM pour la révoquer et la réattribuer à un autre utilisateur. Chaque app est, en outre, automatiquement disponible au téléchargement sur tous les appareils de l'utilisateur, sans coûts ni efforts supplémentaires de votre part. Vous pouvez également acheter des codes de téléchargement via le Programme d'achats en volume pour les utiliser avec Apple Configurator, ou si la gestion des appareils mobiles ne s'applique pas.

Pour en savoir plus sur le Programme d'achats en volume : www.apple.com/fr/business/vpp

Programme pour développeurs iOS en entreprise

Développez des apps iOS internes à utiliser dans votre entreprise à l'aide du Programme pour développeurs iOS en entreprise. Ce programme propose un processus complet et intégré pour développer, tester et diffuser vos apps iOS auprès des employés de votre organisation. Les apps internes ne sont pas soumises à l'App Store et ne sont ni vérifiées, ni approuvées, ni hébergées par Apple.

Vous pouvez distribuer des apps internes soit en hébergeant votre app sur un simple serveur web interne, soit à l'aide d'une solution tierce de MDM ou de gestion des apps. Gérer les apps internes à l'aide d'une solution MDM présente plusieurs avantages, notamment la possibilité de configurer les apps à distance, de gérer les versions, de configurer l'authentification par signature unique (SSO), de définir des règles pour l'accès au réseau (comme le VPN via l'app), et de contrôler quelles apps peuvent exporter des documents. Ce sont vos exigences spécifiques, votre type d'infrastructure et le niveau désiré de gestion des apps qui détermineront la solution qui sera la plus appropriée à votre situation.

Pour développer et déployer des apps internes pour iOS, découvrez le Programme pour développeurs iOS en entreprise : developer.apple.com/programs/ios/enterprise/

Distribution gérée d'apps et de livres

Les serveurs MDM peuvent déployer à distance sur les appareils des apps de l'App Store ou des apps développées en interne. Qu'elles soient payantes ou gratuites, les apps de l'App Store peuvent être gérées par un serveur MDM à l'aide de la distribution gérée du Programme d'achats en volume (VPP). Pour plus d'informations sur la distribution gérée avec MDM, consultez la section « Programme d'achats en volume » ci-dessus.

Vous pouvez installer les apps achetées via le Programme d'achats en volume de trois façons différentes. Les utilisateurs ayant un appareil personnel sont invités par la solution MDM à utiliser leur identifiant Apple pour installer l'app depuis l'App Store. Avec un appareil supervisé inscrit auprès d'un serveur MDM, l'installation des apps s'effectue automatiquement. Et si un appareil n'est pas associé à une solution MDM, les utilisateurs utilisent des codes de téléchargement pour installer des apps payantes. Les apps sont alors associées à l'identifiant Apple personnel de chaque utilisateur.

Installer des apps et du contenu avec Apple Configurator

En plus de la configuration de base, vous pouvez utiliser Apple Configurator pour installer des apps et du contenu. Cela s'applique surtout aux cas où Apple Configurator supervise un appareil qui ne sera pas personnalisé par l'utilisateur. Lorsque vous utilisez Apple Configurator pour configurer des appareils, vous pouvez installer des apps gratuites, des apps payantes via des codes du Programme d'achats en volume (VPP), des apps internes et des documents. Vous pouvez aussi récupérer des documents depuis des appareils iOS attribués. La récupération et l'actualisation de documents suivent le même processus que le partage de documents par importation/exportation depuis/vers iTunes.

Gestion continue

Une fois que vos utilisateurs sont opérationnels, il existe un large éventail de fonctionnalités d'administration permettant de gérer les appareils tout au long de leur cycle de vie, notamment la possibilité d'interroger les appareils pour récupérer des informations, de lancer des commandes de sécurité (comme l'effacement à distance) et de réaliser des tâches spécifiques liées aux apps.

Interrogation

Un serveur MDM peut interroger les appareils afin de récupérer différentes informations. Il peut s'agir d'informations matérielles, comme le numéro de série, l'identifiant UDID ou l'adresse MAC du Wi-Fi, et d'informations logicielles, comme la version d'iOS et une liste détaillée des apps installées sur l'appareil. Ces informations permettent de vérifier que les utilisateurs utilisent les apps préconisées.

Commandes

Lorsqu'un appareil est géré, un serveur MDM peut effectuer un large éventail de commandes administratives, notamment modifier automatiquement les réglages de configuration sans intervention de l'utilisateur, verrouiller ou effacer un appareil à distance, ou supprimer le code de verrouillage pour que les utilisateurs puissent réinitialiser leur mot de passe en cas de perte. Un serveur MDM peut également demander à un appareil iOS de lancer la recopie vidéo AirPlay vers une destination spécifique, ou de mettre fin à une session AirPlay.

Apps gérées

Les entreprises ont souvent besoin de distribuer des apps pour assurer la productivité des utilisateurs. Mais elles doivent également contrôler la façon dont ces apps se connectent aux ressources internes ou dont la sécurité des données est gérée lorsque l'utilisateur quitte l'entreprise. Les apps gérées sous iOS permettent à une entreprise de distribuer à distance des apps gratuites, payantes et d'entreprise via une solution MDM, tout en trouvant le bon équilibre entre la protection des données de l'entreprise et la protection des apps et données personnelles de l'utilisateur.

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 le Programme d'achats en volume, ou si cet utilisateur s'est servi d'un code d'app avec son identifiant Apple personnel, l'app pourra de nouveau être téléchargée de l'App Store, mais elle ne sera pas gérée par MDM.

iOS et votre solution MDM offrent des fonctionnalités supplémentaires qui permettent de gérer les apps, d'améliorer la sécurité et d'offrir une meilleure expérience utilisateur :

- **Gestion des autorisations d'ouverture.** Cette restriction protège les données d'entreprise en contrôlant les apps et comptes utilisés pour ouvrir des documents et pièces jointes. Les sociétés informatiques peuvent configurer la liste des apps disponibles dans le panneau de partage afin de limiter les documents de travail aux apps de l'entreprise et d'éviter que des documents personnels ne soient ouverts dans des apps gérées. Cette règle s'applique également aux fournisseurs de documents tiers et apps de clavier tierces dans iOS 8.
- **Configuration des apps.** Les développeurs d'apps peuvent identifier les réglages pouvant être activés lorsqu'une app est installée en tant qu'app gérée. Ces réglages de configuration s'effectuent 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.
- **Mode app individuelle.** Aide l'utilisateur à rester concentré sur une tâche lorsqu'il utilise un appareil iOS. Ce réglage limite un appareil iOS à une seule app. 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 iTunes. Ne pas autoriser la sauvegarde permet d'éviter que les données des apps gérées ne soient récupérées si l'app est supprimée via la gestion des appareils mobiles 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 aux administrateurs informatiques.

AppleCare OS Support

L'AppleCare OS Support offre à votre service informatique une assistance par téléphone et e-mail de niveau entreprise pour les déploiements iOS, OS X et OS X Server. Offrant un accès direct à des techniciens pour toute question relative à l'intégration, la migration et les problèmes serveur avancés, AppleCare OS Support peut améliorer l'efficacité de votre personnel informatique au niveau du déploiement ainsi que de la gestion des appareils, et de la résolution des problèmes.

AppleCare Help Desk Support

L'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. L'assistance AppleCare Help Desk Support couvre un nombre illimité d'incidents concernant le diagnostic du matériel et des logiciels ainsi que l'identification des problèmes affectant les appareils iOS.

AppleCare pour les utilisateurs d'appareils iOS

Chaque appareil iOS s'accompagne d'une garantie limitée d'un an et d'une assistance technique téléphonique gratuite valable pendant 90 jours. La couverture peut être étendue à deux ans à compter de la date d'achat par la souscription de l'AppleCare+ pour iPhone, de l'AppleCare+ pour iPad ou de l'AppleCare Protection Plan (APP) 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. En outre, les contrats AppleCare+ pour iPhone et AppleCare+ pour iPad offrent la prise en charge de deux incidents liés à des dommages accidentels, chaque incident étant soumis à des frais d'intervention.

Programme d'assistance directe iOS

Avantage procuré par l'AppleCare+ et l'AppleCare Protection Plan, le Programme d'assistance directe iOS permet à votre propre service d'assistance de passer les appareils au crible pour détecter les problèmes sans appeler l'AppleCare ni se rendre dans un Apple Store. Si nécessaire, votre entreprise peut commander directement un iPhone, iPad ou iPod touch de rechange ou des accessoires intégrés.

Pour en savoir plus sur les programmes AppleCare : www.apple.com/fr/support/products

Récapitulatif

Que votre société déploie des appareils iOS auprès d'un groupe d'utilisateurs ou dans toute l'entreprise, il existe de nombreuses options pour déployer et gérer facilement les appareils. En choisissant les bonnes stratégies pour votre entreprise, vous pourrez aider vos collaborateurs à gagner en productivité et à renouveler leurs méthodes de travail.

Pour en savoir plus sur l'intégration d'iOS dans les environnements informatiques d'entreprise : www.apple.com/ipad/business/it

Pour obtenir des informations techniques plus détaillées sur le déploiement d'iOS, consultez le document Référence technique pour le déploiement d'iOS à l'adresse https://help.apple.com/deployment/ios

*Certaines fonctionnalités nécessitent une connexion Wi-Fi. Certaines fonctionnalités ne sont pas disponibles dans tous les pays. L'accès à certains services est limité à 10 appareils.