Aperçu du déploiement d’iOS et d’iPadOS

Introduction

Table des matières

Introduction
Modèles de déploiement
Étapes de déploiement
Sécurité des appareils
Options d’assistance
Conclusion et ressources

Alliés à iOS et iPadOS, iPhone et iPad donnent au personnel les moyens de se dépasser, quel que soit le lieu de travail. Et pour les équipes des TI, l’utilisation de ces appareils signifie moins de gestion du parc informatique – et donc plus de temps pour la stratégie d’entreprise et les enjeux autres que les bogues et la diminution des coûts.

Ce document explique comment déployer des appareils iOS et iPadOS en entreprise et vous aide à jeter les bases d’un plan adapté à votre réalité.

Ces sujets, ainsi que les nouveautés dans les dernières mises à jour d’iOS et iPadOS, sont abordés de manière plus détaillée dans le guide Déploiement des plateformes Apple.

Modèles de déploiement

En général, les entreprises utilisent l'un des deux modèles suivants pour déployer les appareils iOS et iPadOS :

- Appareils d'entreprise
- Appareils personnels

Chaque modèle présente des avantages, qui pourront vous aider à choisir la solution la mieux adaptée à votre organisation. Bien que la plupart des entreprises optent pour un seul modèle, il est possible d'en utiliser plusieurs.

Quand vous aurez fait votre choix, votre équipe pourra explorer en détail les fonctionnalités de gestion et de déploiement d'Apple.

Appareils d'entreprise

Dans ce modèle, les appareils sont achetés par votre organisation, ou par un revendeur ou un fournisseur de services agréé Apple participant. Quand chaque membre de l'entreprise reçoit un appareil, on parle d'accès individuel, et quand il y a une rotation au sein du personnel, il s'agit d'accès partagé. La mise en commun des iPad, où plusieurs personnes utilisent le même appareil sans accéder aux données des autres, est un exemple de déploiement d'appareils partagés. Il est aussi possible pour une entreprise de combiner les appareils partagés et individuels.

Dans le modèle des appareils d'entreprise, l'équipe des TI maintient un niveau de contrôle plus élevé grâce aux options de supervision et à l'inscription automatisée, qui permet de configurer et de gérer les machines dès l'instant où elles sortent de leur boîte.

En savoir plus sur les restrictions imposées aux appareils supervisés : support.apple.com/guide/deployment/welcome/web

Les équipes des TI ont un meilleur contrôle sur les appareils Apple supervisés.

- Configurer des comptes
- Configurer des serveurs mandataires
- Installer, configurer et supprimer des apps
- Exiger un code d'accès complexe
- Imposer toutes les restrictions voulues
- Voir la liste des apps installées
- Effacer à distance toutes les données de l'appareil
- Gérer les mises à jour logicielles
- Supprimer des apps système
- Modifier le fond d'écran
- Limiter l'utilisation à une seule app
- Contourner le verrouillage d'activation
- Forcer l'activation du Wi-Fi
- Activer le mode Perdu

Appareils personnels

Dans ce modèle, chaque personne achète et configure elle-même ses appareils. On dit que ce modèle de déploiement est de type « Apportez votre appareil ». Pour utiliser des services organisationnels, comme le Wi-Fi, les comptes de messagerie et les calendriers, ou pour adopter une configuration répondant à des besoins éducatifs ou professionnels précis, les utilisateurs et utilisatrices passent habituellement par la solution de gestion des appareils mobiles (GAM) de leur entreprise, au moyen de la fonctionnalité Apple d'inscription par l'utilisateur.

Cette solution assure une gestion sécurisée des ressources et des données de l'entreprise, mais aussi la protection de la vie privée, des informations et des apps personnelles. L'équipe des TI a des accès et des droits de gestion limités, qui sont décrits ci-dessous.

Les utilisateurs et utilisatrices accèdent aux données organisationnelles au moyen de leur identifiant Apple géré. Ce dernier est lié au profil d'inscription, et la personne doit s'authentifier pour s'inscrire. L'identifiant Apple géré peut être utilisé de pair avec l'identifiant Apple personnel qui a servi à la connexion – il n'y aura pas de recoupement entre les deux, et les données seront séparées sur l'appareil. Dans les organisations disposant d'espace de stockage sur iCloud, un iCloud Drive distinct sera créé pour toutes les données traitées avec l'identifiant Apple géré.

En savoir plus sur l'inscription par l'utilisateur aux solutions de GAM : support.apple.com/guide/deployment/welcome/web

Les fonctionnalités de GAM sont restreintes sur les appareils personnels.

- ✓ Configurer des comptes
- ✓ Configurer le VPN par app
- ✓ Installer et configurer des apps
- ✓ Exiger un code d'accès
- ✓ Imposer certaines restrictions
- ✓ Voir la liste des apps professionnelles
- ✓ Effacer des données d'entreprise
- ✗ Accéder aux données personnelles
- ✗ Voir la liste des apps personnelles
- ✗ Effacer des données personnelles
- ✗ Recueillir des fichiers journaux
- ✗ Prendre le contrôle d'apps personnelles
- ✗ Exiger un code d'accès complexe
- ✗ Effacer à distance toutes les données de l'appareil
- ✗ Connaître la position de l'appareil

Étapes de déploiement

Cette section présente les cinq étapes du déploiement d'appareils et de contenus, de la préparation de l'environnement jusqu'à la gestion, en passant par la configuration des appareils et la distribution. Les étapes à suivre changent selon que les appareils appartiennent à l'organisation ou aux personnes.

Pour obtenir plus de détails, consultez le guide Déploiement des plateformes Apple.

1. Intégration et configuration

Une fois que vous savez quel modèle convient à votre entreprise, il est important de préparer le déploiement.

Solution de GAM. Grâce au cadre de gestion d'Apple intégré à iOS et iPadOS, les entreprises peuvent inscrire les appareils de façon sécurisée dans leur environnement, configurer et mettre à jour les réglages à distance, vérifier la conformité avec les politiques, distribuer des apps et des livres, et même verrouiller à distance les machines gérées ou effacer leur contenu. Ces fonctionnalités sont offertes par des solutions de GAM tierces. Afin de prendre en charge les différentes plateformes de serveur, divers produits de GAM tiers sont à votre disposition. Chacun propose plusieurs types de consoles d'administration, de fonctionnalités et de structures de tarification.

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

Identifiants Apple gérés. Tout comme les identifiants Apple personnels, les identifiants gérés servent à ouvrir une session sur les appareils et les services Apple, tels que FaceTime, iMessage, l'App Store, iCloud, iWork et Notes. Ils donnent ainsi accès à une vaste gamme de contenus et de fonctionnalités qui favorisent la productivité et la collaboration. Les identifiants Apple gérés appartiennent toutefois à l'organisation et font partie intégrante de la gestion des appareils Apple. Ils permettent de réinitialiser les mots de passe, d'administrer les systèmes en fonction des rôles ou encore d'imposer certaines restrictions.

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

Wi-Fi et réseautique. Tous les appareils Apple sont dotés d'une connectivité réseau sans fil sécurisée. Vérifiez que le réseau Wi-Fi de votre entreprise prend en charge un grand nombre d'appareils et offre une connexion à tout le personnel simultanément. Assurez-vous également que votre infrastructure réseau est réglée pour fonctionner avec Bonjour, le protocole réseau normalisé sans configuration d'Apple. Celui-ci permet aux appareils de trouver automatiquement des services sur un réseau. iOS et iPadOS utilisent Bonjour pour se connecter aux imprimantes AirPrint et aux appareils AirPlay comme Apple TV. Et certaines apps s'en servent afin de détecter des appareils pour le partage et la collaboration.

En savoir plus sur le Wi-Fi et la réseautique :
support.apple.com/guide/deployment/welcome/web

En savoir plus sur Bonjour (en anglais) :
developer.apple.com/bonjour

VPN. Déterminez si votre infrastructure VPN permet aux membres du personnel d'accéder aux ressources d'entreprise à distance de façon sécurisée sur leurs appareils iOS et iPadOS. Songez à utiliser le VPN sur demande ou le VPN par app d'iOS et d'iPadOS pour que la connexion à un réseau privé virtuel ne soit activée qu'au besoin. Si vous prévoyez utiliser le VPN par app, vérifiez que vos passerelles VPN prennent en charge cette fonctionnalité et que vous avez suffisamment de licences pour le nombre de personnes et de connexions.

Comptes de messagerie, contenus et calendriers. Grâce à la compatibilité d'iPhone, iPad et Mac avec Microsoft Exchange, Office 365 et d'autres services de messagerie comme Google Workspace, vous avez instantanément accès à la transmission automatique de vos courriels, événements de calendrier, contacts et tâches via une connexion SSL chiffrée. Si vous utilisez Microsoft Exchange, vérifiez que le service ActiveSync est à jour et configuré pour prendre en charge l'ensemble des utilisateurs et utilisatrices du réseau. Et si vous avez recours à Office 365 dans le nuage, veillez à avoir suffisamment de licences pour prendre en charge le nombre prévu d'appareils iOS et iPadOS qui se connecteront à votre réseau. iOS et iPadOS sont aussi compatibles avec l'authentification moderne Office 365, qui tire parti du protocole OAuth 2.0 et de l'authentification multifactorielle. Si vous n'employez pas Exchange, iOS et iPadOS fonctionnent avec les serveurs normalisés, dont IMAP, POP, SMTP, CalDAV, CardDAV et LDAP.

2. Gestion des identités

Pour aller plus loin dans la préparation du déploiement, les équipes des TI, une fois qu'elles seront intervenues sur l'environnement, devront choisir la façon dont elles géreront l'authentification et les autorisations. Cela contribuera à la protection des appareils et des données.

Authentification. Il existe de multiples méthodes d'authentification. L'authentification unique et les services Apple tels que les identifiants Apple gérés, iCloud ou iMessage permettent de communiquer de manière sécurisée, de créer des documents en ligne et de sauvegarder du contenu personnel, sans compromettre les données de l'organisation. Chaque service utilise sa propre architecture de sécurité, ce qui garantit un traitement sûr des données (que ce soit sur un appareil Apple ou en transit sur un réseau sans fil), la protection des renseignements personnels et la prévention des accès non autorisés ou malveillants à l'information et aux services. Les solutions de GAM peuvent servir à encadrer les accès à des services précis sur les appareils Apple.

En savoir plus sur l'authentification unique :
support.apple.com/guide/deployment/depfdbf18f55/1/web/1.0

En savoir plus sur l'authentification unique Kerberos :
support.apple.com/guide/deployment/depe6a1cda64/1/web/1.0

Autorisation. L'autorisation diffère de l'authentification. L'authentification prouve l'identité d'une personne, tandis que l'autorisation définit ce que cette personne peut accomplir. Elle peut par exemple reposer sur la communication d'un nom d'utilisateur et d'un mot de passe à un fournisseur d'identités. Dans cet exemple, l'autorité est le fournisseur d'identités ou Active Directory, l'assertion est le nom d'utilisateur et le mot de passe, et le jeton est constitué des données reçues après l'ouverture de session. D'autres assertions peuvent être utilisées, comme des certificats, des cartes intelligentes ou d'autres dispositifs à facteurs multiples.

Fédération d'identités. La fédération d'identités implique que des administrateurs et administratrices inscrivent plusieurs domaines dans un même cercle de confiance et s'entendent sur une méthode d'identification des membres du personnel. Par exemple, il peut s'agir d'ouvrir une session auprès d'un fournisseur d'identités infonuagique en se connectant à un compte d'entreprise. Les équipes des TI peuvent notamment activer la fédération entre Microsoft Azure Active Directory (Azure AD) et Apple Business Manager pour simplifier la création d'identifiants Apple gérés dans leur organisation. Les membres du personnel utiliseront ensuite leurs identifiants Azure AD pour ouvrir une session dans iCloud ou sur un appareil Apple associé à Apple Business Manager.

3. Planification du déploiement et approvisionnement

Après l'étape de préparation, il est temps de configurer les appareils et d'organiser la distribution du contenu. Tous les modèles de déploiement fonctionnent mieux lorsqu'ils s'appuient sur une solution de GAM en plus d'Apple Business Manager ou d'Apple Configurator 2.

Inscription automatisée des appareils

Grâce à cette méthode, les entreprises peuvent déployer les appareils Apple qui leur appartiennent et les inscrire dans leur solution de GAM facilement, rapidement et sans avoir à les manipuler ou à les préparer. Les équipes des TI sont en mesure d'alléger le processus de configuration en simplifiant les étapes dans l'Assistant réglages. Ainsi, le personnel obtient une configuration optimale dès l'activation des appareils. Seules les machines achetées directement auprès d'Apple ou d'un revendeur ou fournisseur de services agréé Apple participant peuvent être déployées au moyen de l'inscription automatisée.

Inscription des appareils

Le déploiement des appareils peut aussi se faire manuellement au moyen d'Apple Configurator 2 et de la solution de GAM de votre entreprise. Cette option fonctionne aussi bien avec les machines appartenant à l'organisation que les machines personnelles. Tout comme le reste du parc, les appareils gérés manuellement sont inscrits à la GAM et soumis à une supervision obligatoire. Cette méthode de déploiement est parfaite pour les équipes des TI qui doivent gérer des appareils n'ayant pas été achetés directement auprès d'Apple ou d'un revendeur ou fournisseur de services agréé Apple participant.

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

Inscription par l'utilisateur

Les appareils personnels peuvent être configurés et déployés au moyen de l'inscription par l'utilisateur, qui permet aux équipes des TI de protéger les données de l'entreprise sans verrouiller les machines. Consultez la section Modèles de déploiement pour en savoir plus sur cette méthode d'inscription.

Qu'un appareil appartienne ou non à l'organisation, les équipes des TI peuvent garder le contrôle sur le processus de configuration lors du déploiement grâce à l'Assistant réglages. Ce dernier est paramétré au moyen de la solution de GAM et permet aux gens de commencer à travailler avec leurs appareils sans délai.

Une fois qu'un appareil est inscrit, l'administrateur ou administratrice peut envoyer une option, une commande ou une politique de GAM; les fonctions de gestion disponibles pour une machine varient selon la méthode d'inscription et le niveau de supervision. L'appareil iOS ou iPadOS reçoit alors une notification envoyée par le service de notification Push d'Apple (APN) pour pouvoir communiquer directement avec le serveur de GAM via une connexion sécurisée. Avec une connexion réseau, les appareils peuvent recevoir des commandes du service APN partout dans le monde. Les notifications ne contiennent toutefois aucun renseignement confidentiel ou exclusif.

4. Gestion de la configuration

Les appareils Apple intègrent un cadre de gestion sécurisé qui permet aux équipes des TI d'administrer leur parc au moyen d'un grand nombre de fonctionnalités. Ce cadre comporte quatre volets :

Profils de configuration

Les profils de configuration sont des entités qui chargent les paramètres et les renseignements d'autorisation sur les appareils Apple. Ils automatisent la configuration des réglages, comptes, restrictions et renseignements d'identification. Selon votre solution de GAM et son intégration dans vos systèmes internes, les champs de données des comptes peuvent être préremplis avec le nom de la personne, son adresse courriel et, s'il y a lieu, les identités de certificat pour l'authentification et la signature.

Restrictions

Les restrictions permettent d'appliquer des politiques de sécurité et de favoriser la concentration du personnel sans avoir à verrouiller les appareils. Parmi elles, la gestion des autorisations d'ouverture bloque la consultation de pièces jointes ou de documents provenant de sources gérées dans des destinations non gérées; le mode App individuelle limite l'accès à une seule app sur un appareil; et la prévention de la sauvegarde empêche des apps gérées de sauvegarder des données sur iCloud ou sur l'appareil.

Tâches de gestion

Le serveur de GAM peut effectuer diverses tâches administratives sur les appareils gérés, comme modifier les réglages de configuration sans intervention de l'utilisateur ou de l'utilisatrice, faire une mise à jour logicielle sur un appareil protégé par mot de passe, verrouiller un appareil ou effacer son contenu à distance, et réinitialiser un code d'accès en cas d'oubli. Le serveur de GAM peut aussi demander à un iPhone ou à un iPad de lancer la recopie vidéo AirPlay vers une destination précise, ou de l'interrompre. Il est par ailleurs possible d'empêcher la mise à jour manuelle des appareils supervisés à distance pour une période allant jusqu'à 90 jours. La solution de GAM permet également de planifier les mises à jour logicielles sur les machines supervisées.

Requêtes

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

5. Distribution de contenu

Après l'inscription, l'administrateur ou administratrice peut recourir à la distribution gérée. Celle-ci permet d'utiliser la solution de GAM ou Apple Configurator 2 pour gérer les apps et livres achetés avec Apple Business Manager dans tous les pays où ils sont offerts. Pour activer cette fonctionnalité, vous devez lier votre solution de GAM à votre compte Apple Business Manager à l'aide d'un jeton sécurisé. Dès que c'est fait, vous pouvez assigner des apps et des livres dans Apple Business Manager, même si l'App Store est désactivé sur les appareils.

Deux types de contenus peuvent être distribués : les apps gérées et les livres et documents gérés. Il est possible de passer par un serveur de GAM pour déployer et désinstaller les apps gérées, qui peuvent aussi être supprimées lors de la désinscription d'un appareil personnel de la GAM. La suppression d'une app entraîne l'effacement des données qui lui sont associées. Les livres et documents gérés, quant à eux, peuvent être automatiquement envoyés vers les appareils. Seuls le partage avec d'autres apps gérées et l'envoi par compte de messagerie géré sont autorisés pour ce contenu. Les documents gérés peuvent être supprimés automatiquement, mais il est impossible de retirer ou de réassigner des livres gérés, même s'ils ont été remis via Apple Business Manager.

La distribution de contenu se fait selon deux méthodes :

Attribution d'apps aux appareils. La solution de GAM et Apple Configurator 2 peuvent servir à attribuer des apps directement aux appareils. Cette méthode vous épargne plusieurs étapes lors du déploiement initial, ce qui facilite et accélère le processus, tout en vous permettant de garder le plein contrôle des appareils et des contenus gérés. Lors de l'attribution d'une app, celle-ci est transmise à l'appareil par le système de GAM, sans qu'il soit nécessaire d'envoyer une invitation. Par la suite, toute personne qui utilise l'appareil peut accéder à l'app.

Attribution d'apps et de livres aux comptes. La deuxième méthode consiste à utiliser la solution de GAM pour inviter les utilisateurs et utilisatrices à télécharger des apps et des livres par l'intermédiaire d'un courriel ou d'une notification Push. Pour accepter l'invitation, chaque personne doit se connecter sur son appareil avec son identifiant Apple personnel. L'identifiant Apple est enregistré auprès du service Apple Business Manager, mais il demeure entièrement confidentiel et n'est pas divulgué à l'administrateur ou administratrice. Une fois que les utilisateurs et utilisatrices acceptent l'invitation, ils sont connectés au serveur de GAM et peuvent se procurer les apps et les livres qui leur ont été attribués. Les apps sont automatiquement téléchargeables sur tous les appareils des membres du personnel, sans aucuns frais ni démarche supplémentaires.

Lorsqu'une app n'est plus utile sur une machine ou pour une personne, vous pouvez la retirer et l'attribuer à un autre appareil ou compte. Votre entreprise conserve ainsi la propriété et le contrôle exclusifs des apps achetées. Une fois distribués, les livres demeurent toutefois la propriété de leur destinataire et ne peuvent être ni retirés ni réattribués.

Sécurité des appareils

Apple place au cœur de ses produits les dernières innovations en matière de sécurité. Une fois les appareils configurés, les équipes des TI sont en mesure de gérer et de protéger les données d'entreprise grâce aux fonctionnalités de sécurité intégrées et à d'autres options offertes par la GAM. L'utilisation par les apps de cadres logiciels communs permet la configuration et la gestion continue des paramètres.

En savoir plus sur la sécurité des plateformes Apple :
support.apple.com/guide/security/welcome/web

Protection des données professionnelles. Les TI peuvent imposer des politiques de sécurité et vérifier qu'elles sont respectées par l'intermédiaire de la GAM. Par exemple, le fait d'imposer la saisie d'un code d'accès sur les appareils iOS et iPadOS active automatiquement la protection des données, ce qui chiffre les fichiers stockés sur les machines. La GAM peut aussi servir à configurer le Wi-Fi et le VPN, et à appliquer des certificats qui renforceront la sécurité.

Les solutions de GAM permettent de gérer les appareils de façon très précise sans recourir à des conteneurs, et d'ainsi protéger les données de l'entreprise. Avec la gestion des autorisations d'ouverture, les équipes des TI peuvent interdire la consultation de pièces jointes et de documents à partir de destinations non gérées.

Verrouillage, localisation et effacement du contenu. Les appareils peuvent se perdre, mais pas leurs données. Les équipes des TI ont la possibilité de verrouiller les appareils iOS et iPadOS à distance et d'en effacer toutes les données sensibles afin de protéger les renseignements de l'organisation. Elles peuvent activer le mode Perdu sur un appareil iOS ou iPadOS supervisé afin de le localiser, et disposent aussi d'outils permettant de désinstaller instantanément une app d'entreprise sans effacer de données personnelles.

Apps. Un cadre logiciel commun et un écosystème géré assurent d'emblée la sécurité des apps sur les plateformes Apple. Nos programmes pour développeurs contrôlent l'identité de chaque entité de conception, et le système vérifie les apps avant leur lancement dans l'App Store. Apple met à la disposition des équipes de développement des cadres pour certaines fonctionnalités, comme la signature, les extensions, les autorisations et la mise en bac à sable afin de renforcer encore plus la sécurité.

Mode Perdu. Votre solution de GAM peut activer à distance le mode Perdu sur un appareil supervisé. Cette fonction bloque l'appareil et permet d'afficher un message et un numéro de téléphone sur l'écran verrouillé. Grâce au mode Perdu, la GAM peut localiser un appareil supervisé perdu ou volé en produisant une requête qui détermine le lieu de la dernière connexion. Il n'est pas nécessaire d'activer l'app Localiser pour que le mode Perdu fonctionne.

Verrouillage d'activation. Il est possible d'utiliser la GAM pour activer l'option Verrouillage d'activation quand une personne met en fonction l'app Localiser sur un appareil supervisé. Ainsi, votre entreprise peut profiter de la fonctionnalité antivol du verrouillage d'activation tout en conservant la possibilité de la contourner si quelqu'un n'arrive pas à s'authentifier avec son identifiant Apple.

Options d’assistance

Apple offre une vaste gamme de programmes et de ressources d’assistance.

AppleCare pour entreprises

Cette solution convient aux organisations à la recherche d’une couverture complète et contribue à réduire la charge de travail de leur service des TI. Elle offre au personnel du soutien technique par téléphone 24 heures sur 24, 7 jours sur 7, et un délai de réponse d’au maximum une heure pour les problèmes majeurs. Ce programme fournit de l’assistance à l’échelle du service informatique, incluant de l’aide pour tous les appareils et logiciels Apple, et du soutien pour les déploiements et les intégrations complexes, par exemple pour les solutions de GAM et Active Directory.

AppleCare OS Support

AppleCare OS Support procure aux services des TI un soutien par téléphone et par courriel à l’échelle de l’entreprise pour les déploiements iOS et iPadOS. Plusieurs plans sont proposés, allant jusqu’au soutien technique jour et nuit avec une personne attitrée au compte de l’entreprise. En offrant un accès direct à des spécialistes pour les questions sur l’intégration, la migration et le fonctionnement des serveurs, AppleCare OS Support aide votre équipe des TI à déployer et gérer les appareils et résoudre les problèmes avec plus d’efficacité.

Soutien AppleCare pour centres d’assistance

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

AppleCare+ pour iPad, AppleCare+ pour iPhone et AppleCare+ pour iPod touch

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

Programme d’assistance directe pour iOS

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

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

Conclusion et ressources

De nombreuses options sont disponibles pour faciliter le déploiement et la gestion d'iPhone et d'iPad dans votre entreprise, que ce soit pour un groupe restreint de personnes ou l'ensemble des équipes. En choisissant les stratégies les mieux adaptées à votre organisation, vous pourrez aider le personnel à gagner en productivité et à révolutionner sa façon de travailler.

En savoir plus sur le déploiement, la gestion et les fonctionnalités de sécurité d'iOS et iPadOS :
support.apple.com/guide/deployment/welcome/web

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

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

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

En savoir plus sur les fonctionnalités pour les TI :
apple.com/ca/fr/business/it/

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

Parcourir les programmes AppleCare :
apple.com/ca/fr/support/professional/

En savoir plus sur les formations et les certifications Apple (en anglais) :
training.apple.com

Communiquer avec les Services professionnels Apple :
consultingservices@apple.com

Essayer les logiciels bêta, accéder à des plans de test et fournir des commentaires :
appleseed.apple.com/sp/welcome