



Aperçu du déploiement de Mac

Table des matières

[Introduction](#)

[Premiers pas](#)

[Étapes de déploiement](#)

[Options d'assistance](#)

[Conclusion](#)

Introduction

Chez Apple, nous croyons que les employés excellent quand ils ont accès aux meilleurs outils et technologies. Tous nos produits sont pensés pour favoriser la créativité, la productivité et les pratiques novatrices, au bureau comme à l'extérieur. Cette vision reflète la façon dont les employés d'aujourd'hui souhaitent travailler : avec un accès de pointe à l'information, des outils de collaboration et de partage simples, et la possibilité de garder le fil et d'être efficace partout.

Jamais configurer et déployer des ordinateurs Mac dans un contexte professionnel n'a été aussi simple. En associant des services clés d'Apple à une solution tierce de gestion des appareils mobiles (GAM), vous pouvez facilement déployer des appareils macOS et en assurer la maintenance à l'échelle de votre entreprise. Si votre organisation a déjà déployé des appareils iOS et iPadOS, le travail d'infrastructure nécessaire pour macOS est probablement fait en grande partie.

Les récentes améliorations apportées à Mac en matière de sécurité, de gestion et de déploiement permettent aux organisations de passer d'un modèle monolithique (avec images disque et association à un annuaire) à un modèle d'approvisionnement et à un processus de déploiement fluides, axés sur l'utilisateur et presque entièrement basés sur les outils intégrés à macOS.

Le présent document fournit des recommandations pour tous les aspects touchant au déploiement de Mac à l'échelle de votre entreprise, de l'évaluation de l'infrastructure actuelle à la gestion des appareils et à l'approvisionnement simplifié. Les sujets abordés ici sont expliqués plus en détail dans le document de référence pour le déploiement de Mac* :

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

* En anglais seulement.

Premiers pas

Pour entamer le processus de déploiement, il vous faut d'abord évaluer l'utilisation actuelle de macOS dans votre entreprise, puis élaborer une stratégie et un plan de mise en œuvre. Veillez à ce que les équipes pertinentes intègrent le projet dès le début et se rallient à la vision et aux objectifs de votre programme. Certaines équipes commenceront par une démonstration de faisabilité afin de déceler les défis propres à leur environnement. À cette étape, il est essentiel de discuter avec les utilisateurs actuels dans le cadre d'un projet pilote plus large pour comprendre l'utilisation des appareils dans votre organisation et cerner tout problème.

L'information ainsi recueillie peut contribuer à déterminer les rôles et fonctions auxquels Mac profiterait le plus, et aider le service des TI à évaluer si macOS devrait être offert par défaut dans toute l'entreprise, ou en option pour certains postes seulement.

Souvent, cette étape permet également d'établir une liste complète des apps et outils internes qui devront être compatibles avec Mac avant le déploiement. Concentrez-vous d'abord sur les apps clés de productivité, de collaboration et de communication qui comptent le plus d'utilisateurs. Les services internes critiques, comme l'intranet, l'annuaire et les logiciels de gestion des dépenses, sont aussi essentiels au fonctionnement de grands pans de l'entreprise.

Notez et communiquez les solutions de contournement ou substituts possibles pour les autres outils internes, tout en encourageant les gestionnaires d'application à moderniser leurs outils au besoin. Indiquez clairement aux utilisateurs quelles apps pour entreprises ils pourront utiliser s'ils choisissent Mac, et hiérarchisez les tâches de modernisation en fonction de la demande. Si nécessaire, avec les gestionnaires d'applications, créez un plan de mise à jour des apps qui fait appel à la trousse SDK macOS et Swift, ainsi qu'aux nombreux partenaires d'entreprise susceptibles de vous épauler dans le développement.

Les ordinateurs Mac fournis aux employés appartiennent habituellement à l'entreprise, mais certaines organisations permettent à leur personnel d'utiliser Mac dans le cadre d'un programme « Apportez votre appareil ». Peu importe le modèle de déploiement, donner le choix des produits Apple a le potentiel de générer des gains dans toutes les équipes : hausse de productivité, de créativité, d'engagement et de satisfaction, et réduction des coûts attribuable à une grande valeur résiduelle et à des besoins d'assistance restreints. Les entreprises ont également accès à diverses options de location et de financement pour réduire les coûts initiaux. Et elles peuvent compenser certains frais en proposant aux employés un rehaussement d'appareil par retenue salariale, ou un rachat en fin de location ou de cycle de vie.

Au même titre que les processus de déploiement, de gestion et de soutien décrits dans ce document, les politiques d'entreprise peuvent varier selon l'information recueillie lors d'un projet pilote. Et comme les besoins sont propres à chaque groupe ou équipe, les mêmes politiques, réglages et apps ne s'appliquent généralement pas à tous les utilisateurs d'une organisation.

Étapes de déploiement

Le déploiement de macOS compte quatre grandes étapes : préparation de l'environnement, configuration de la GAM, distribution des appareils et gestion continue.

1. Préparation

La première étape de tout déploiement consiste à examiner l'environnement actuel. Cette phase comprend l'étude du réseau et de l'infrastructure, ainsi que la mise en place des systèmes requis pour un déploiement réussi.

Évaluer l'infrastructure

Même si Mac s'intègre facilement à la plupart des environnements TI standards en entreprise, il est important d'évaluer l'infrastructure en place pour que votre organisation puisse tirer pleinement parti de tout ce que macOS a à offrir. N'hésitez pas à faire appel aux services professionnels Apple ou aux équipes techniques de votre fournisseur ou revendeur si vous avez besoin d'aide.

Wi-Fi et réseautique

Une connexion sans fil fiable et constante est nécessaire à l'installation et à la configuration d'appareils macOS. Vérifiez le réseau Wi-Fi de votre entreprise. Assurez-vous notamment que l'emplacement et la bande passante de vos points d'accès répondent aux besoins d'itinérance et de capacité.

Vous devrez peut-être reconfigurer vos serveurs mandataires ou pare-feu si des appareils ne peuvent accéder aux serveurs d'Apple, au service de notification Push d'Apple (APN), à iCloud ou à l'iTunes Store. Comme pour iPad et iPhone, certains aspects du déploiement de Mac – surtout avec des Mac récents – requièrent un accès à ces services, par exemple pour la mise à jour micrologicielle durant l'installation.

Apple et Cisco ont optimisé les méthodes de communication de Mac sur les réseaux sans fil Cisco, en prenant en charge des fonctionnalités réseau avancées de macOS, comme la qualité de service (QS). Si vous utilisez de l'équipement réseautique Cisco, collaborez avec vos équipes internes pour veiller à ce que Mac optimise le trafic des données clés.

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

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

Pour en savoir plus sur la conception de réseaux Wi-Fi* :
support.apple.com/guide/deployment-reference-macos

Pour en savoir plus sur la configuration du réseau pour la GAM :
support.apple.com/HT210060

Pour en savoir plus sur Bonjour* :
support.apple.com/guide/deployment-reference-macos

Gestion des identités

macOS peut accéder à des services d'annuaire comme Active Directory, Open Directory et LDAP pour gérer les identités et d'autres données d'utilisateurs. Certains fournisseurs de solutions de GAM proposent des outils qui servent à lier leurs solutions à un annuaire Active Directory ou LDAP sans configuration. D'autres outils – par exemple l'extension d'authentification unique Kerberos sous macOS Catalina – permettent d'intégrer les politiques et fonctionnalités d'Active Directory sans associer l'appareil. Votre solution de GAM peut aussi gérer divers types de certificats délivrés par des autorités de certification internes et externes afin que les identités soient automatiquement certifiées.

Pour en savoir plus sur l'extension d'authentification unique Kerberos* :
support.apple.com/guide/deployment-reference-macos

Pour en savoir plus sur l'intégration à un annuaire* :
support.apple.com/guide/deployment-reference-macos

Services clés pour employés

Vérifiez que votre service Microsoft Exchange est à jour et configuré pour prendre en charge tous les utilisateurs du réseau. Si vous n'employez pas Exchange, macOS fonctionne également avec les serveurs normalisés, dont IMAP, POP, SMTP, CalDAV, CardDAV et LDAP. Testez les flux de travail de base pour les courriels, les contacts et les calendriers, ainsi que les autres logiciels de productivité et de collaboration les plus utilisés pour les tâches quotidiennes clés.

Pour en savoir plus sur la configuration de Microsoft Exchange* :
support.apple.com/guide/deployment-reference-macos

Pour en savoir plus sur les services normalisés* :
support.apple.com/guide/deployment-reference-macos

Mise en cache de contenu

Le service de mise en cache intégré à macOS conserve une copie locale des contenus fréquemment demandés aux serveurs Apple, ce qui réduit la bande passante utilisée par votre réseau pour les télécharger. Cette fonctionnalité accélère le téléchargement et la distribution de contenus à partir du Mac App Store. Elle peut aussi mettre en cache les mises à jour logicielles pour un téléchargement plus rapide sur les appareils macOS, iOS et iPadOS de votre organisation. Et d'autres types de contenus peuvent être mis en cache avec des solutions de Cisco et d'Akamai.

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

* En anglais seulement.

Choisir une solution de gestion

Avec la GAM, les organisations peuvent inscrire les ordinateurs Mac de leur environnement, en configurer et mettre à jour les réglages à distance, distribuer des apps, vérifier le respect des politiques, ainsi qu'interroger, verrouiller ou effacer à distance les appareils gérés – toujours de façon sécurisée. Le service des TI peut aisément créer des profils pour gérer les comptes d'utilisateur, configurer des réglages système, imposer des restrictions et fixer des politiques de mots de passe avec la solution de gestion des appareils mobiles déjà en place pour iPhone et iPad.

Toutes les plateformes Apple reposent sur le même cadre de gestion. Ainsi, les clients ont accès à toute une gamme de solutions de GAM offertes par des fournisseurs tiers comme Jamf, VMware et MobileIron. Même si les cadres de gestion des appareils sont principalement les mêmes pour macOS, iOS et iPadOS, ces solutions diffèrent légèrement les unes des autres quant aux fonctionnalités d'administration, à la prise en charge des systèmes d'exploitation, à la structure de tarification et au modèle d'hébergement. Elles offrent aussi différents niveaux de service pour l'intégration, la formation et le soutien. Avant d'arrêter votre choix, déterminez les fonctionnalités dont votre entreprise a le plus besoin.

Une fois la solution de GAM sélectionnée, vous devrez vous rendre sur le portail de certificats Push d'Apple et ouvrir une session pour créer un nouveau certificat Push de GAM.

Pour en savoir plus sur le déploiement d'une solution de GAM* :
support.apple.com/guide/deployment-reference-macos

Portail de certificats Push d'Apple* :
identity.apple.com/pushcert/

Adhérer à Apple Business Manager

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

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

Appareils

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

- Facilitez le processus de configuration en simplifiant les étapes dans l'Assistant réglages pour que les appareils des employés soient configurés convenablement dès leur activation. Les équipes des TI peuvent personnaliser encore plus cette expérience en présentant aux employés une entente d'utilisation, le logo de l'entreprise et des méthodes d'authentification de pointe.

* En anglais seulement.

- Élargissez le contrôle des appareils détenus par l'entreprise grâce à la supervision, qui comprend des options de gestion que vous ne trouverez pas dans d'autres modèles de déploiement, comme l'inscription irrévocable à la solution de GAM.
- Gérez plus facilement les serveurs de GAM en choisissant un serveur par défaut selon le type d'appareil. Et inscrivez manuellement vos iPhone, iPad et Apple TV à l'aide d'Apple Configurator 2, quelle que soit la manière dont vous les avez achetés.

Contenus

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

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

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

Utilisateurs

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

- Les employés se servent de leur identifiant Apple géré pour collaborer dans les apps et les services Apple, et même pour accéder aux données dont ils ont besoin dans des apps gérées compatibles avec iCloud Drive. Ces comptes sont détenus et gérés par l'entreprise.
- Grâce à l'authentification fédérée, vous pouvez lier Apple Business Manager à Microsoft Azure Active Directory. Un identifiant Apple géré sera créé automatiquement lorsque l'employé ouvrira une session sur un appareil Apple compatible à l'aide de son identifiant actuel.
- L'identifiant Apple géré peut être utilisé conjointement avec un identifiant Apple personnel sur un appareil appartenant à l'employé grâce à la nouvelle fonctionnalité d'inscription par l'utilisateur, offerte sous iOS 13, iPadOS et

macOS Catalina. Il est aussi possible d'utiliser un identifiant Apple géré sur n'importe quel appareil en tant qu'identifiant Apple principal (et unique).

L'identifiant Apple géré donne également accès à iCloud en ligne dès la première ouverture de session sur un appareil Apple.

- Attribuez d'autres rôles aux équipes des TI de votre entreprise pour gérer les appareils, les apps et les comptes efficacement dans Apple Business Manager. Le rôle d'administrateur permet d'accepter les modalités d'utilisation et de transférer les responsabilités facilement quand un employé quitte l'entreprise.

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

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

Adhérer au programme Apple pour développeurs en entreprise

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

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

2. Configuration

En vue de votre déploiement, vous devez établir des politiques d'entreprise et préparer votre solution de GAM afin qu'elle soit prête à configurer Mac pour vos employés.

Comprendre la sécurité sous macOS

La sécurité et la confidentialité sont au cœur de la conception de tous les appareils, logiciels et services Apple. Nous protégeons la vie privée de nos clients à l'aide de puissants outils de chiffrement et de politiques rigoureuses en matière de gestion des données. Sécuriser une plateforme informatique pour appareils Apple comporte plusieurs facteurs :

- Des méthodes qui préviennent toute utilisation non autorisée des appareils;
- La protection des données au repos, même en cas de perte ou de vol d'un appareil;
- Des protocoles réseau et le chiffrement des données en cours de transmission;
- Un moyen d'exécuter les apps en toute sécurité sans compromettre l'intégrité de la plateforme.

Comme plusieurs couches de sécurité sont incluses dans les appareils Apple, ceux-ci peuvent accéder aux services réseau de façon sécurisée et protéger les données importantes. macOS, iOS et iPadOS offrent aussi une sécurité renforcée grâce au verrouillage par mot de passe et à des politiques de mot de passe qui peuvent être assignées et imposées avec la GAM. Et si un appareil tombe entre de mauvaises mains, l'utilisateur ou l'administrateur est en mesure d'effacer son contenu confidentiel à distance.

* En anglais seulement.

Le service des TI peut faire appel à la GAM afin de déployer des politiques visant à sécuriser les appareils. Par exemple, la GAM permet d'imposer FileVault, une clé de secours, une politique de mot de passe, le verrouillage à l'activation de l'économiseur d'écran ou l'activation du pare-feu intégré.

Pour en savoir plus sur la sécurité des plateformes Apple* : apple.com/security/

Définir les politiques d'entreprise

Pour élaborer vos politiques d'entreprise, commencez par établir des règles générales s'appliquant à la majorité de vos utilisateurs Mac. Votre solution de GAM vous permettra de personnaliser des éléments selon les utilisateurs, par exemple les comptes ou l'accès à certaines apps. Vous pouvez aussi appliquer des politiques propres à des services ou à d'autres sous-groupes d'utilisateurs, par exemple pour le déploiement de logiciels ou de réglages destinés à des équipes en particulier.

Collaborez avec vos équipes internes afin de mettre à jour les politiques d'entreprise pour tenir compte de l'utilisation de Mac. Certaines politiques sont les mêmes pour toutes les plateformes, notamment celles touchant à la complexité et à la fréquence de changement des mots de passe, à la vitesse d'activation de l'économiseur d'écran et aux utilisations acceptables des appareils.

Si votre politique d'entreprise nécessite le recours à une technologie exclusive à une autre plateforme, partez du problème sous-jacent et repensez la politique en fonction des technologies intégrées à macOS. Plutôt que d'imposer une solution tierce pour le chiffrement du stockage, envisagez la création d'une politique exigeant que les données d'entreprise soient chiffrées au repos avec FileVault. Si la politique requiert des logiciels précis pour la protection contre les logiciels malveillants, formez les équipes au sujet de fonctionnalités intégrées comme Gatekeeper, puis mettez la politique à jour pour autoriser leur utilisation.

Configurer les réglages dans la solution de GAM

Pour permettre la gestion des politiques d'entreprise et donner aux employés un accès aux ressources dont ils ont besoin, vous devez inscrire chaque Mac de façon sécurisée à votre solution de GAM. Celle-ci appliquera ensuite les politiques et réglages au moyen des profils de configuration. Créés par votre solution de GAM, les profils de configuration sont des fichiers XML qui permettent l'envoi des réglages aux appareils. Ils automatisent la configuration des réglages, des comptes, des politiques, des restrictions et des renseignements d'identification. Pour renforcer la sécurité de vos systèmes, vous pouvez signer et chiffrer les profils.

Une fois qu'un appareil est inscrit à la GAM, l'administrateur peut lui envoyer une politique, une requête ou une commande de GAM. Si l'appareil est connecté au réseau, il reçoit alors une notification via le service de notification Push d'Apple (APN) lui donnant l'instruction de communiquer avec la solution de GAM par connexion sécurisée pour exécuter l'action de l'administrateur. Comme la communication se fait exclusivement entre l'appareil et la solution de GAM, le service APN ne transmet pas de données ou d'informations confidentielles. Lorsqu'un appareil est retiré de la solution de GAM, les réglages et les politiques liés à son profil de configuration sont supprimés. Au besoin, l'entreprise peut aussi effacer à distance le contenu d'un appareil.

De nombreuses organisations lient leur solution de GAM à leurs services d'annuaire existants. Durant l'inscription automatisée des appareils, l'Assistant réglages de macOS peut demander aux utilisateurs d'ouvrir une session avec leurs identifiants du service d'annuaire. Sous macOS Catalina, de nouvelles options

* En anglais seulement.

d'inscription permettent de recourir au processus d'authentification de fournisseurs d'identités infonuagiques dans l'Assistant réglages. Une fois l'appareil assigné à un utilisateur donné, la GAM peut personnaliser la configuration et les comptes en fonction de l'employé ou du groupe. Par exemple, l'information sur le compte Microsoft Exchange d'un utilisateur peut être obtenue automatiquement durant l'inscription. Vous pouvez également utiliser des identités de certificat pour certaines technologies, par exemple 802.1X et VPN.

Compte tenu du niveau de contrôle qu'offrent ces systèmes, beaucoup d'entreprises n'hésitent pas à donner aux utilisateurs un accès administrateur complet à Mac. Les employés peuvent ainsi personnaliser les réglages, installer des apps et dépanner les problèmes en restant dans le cadre des politiques d'entreprise imposées par la GAM. Avec ce modèle, les utilisateurs de Mac profitent des mêmes privilèges et commandes que sur leur iPhone ou iPad géré.

Pour en savoir plus sur les profils de configuration* :

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

Se préparer à l'inscription automatisée des appareils

La façon la plus simple d'inscrire les appareils à la GAM est d'utiliser les fonctionnalités d'inscription automatisée d'Apple Business Manager durant la configuration avec l'Assistant réglages. Ainsi, l'inscription se fait sans l'intervention des TI, et certaines étapes de l'Assistant réglages peuvent être simplifiées afin d'accélérer le processus pour les utilisateurs.

Pour configurer l'inscription automatisée des appareils, vous devez lier votre compte Apple Business Manager à votre solution de GAM au moyen d'un jeton sécurisé. Votre solution de GAM est autorisée de façon sécuritaire grâce à un processus de vérification en deux étapes. Votre fournisseur de solution de GAM peut vous renseigner sur la marche à suivre propre à son logiciel.

Si les appareils sont déjà utilisés ou appartiennent aux employés, un profil de configuration unique peut être ouvert. L'utilisateur n'a alors qu'à se rendre dans Préférences Système pour le faire vérifier et conclure le processus. On parle alors d'inscription à la GAM approuvée par l'utilisateur. La gestion de certains réglages critiques (par exemple la politique des extensions de noyau ou le contrôle de politique des préférences de confidentialité) exige le recours à l'inscription des appareils ou à l'inscription approuvée par l'utilisateur.

Pour en savoir plus sur le chargement d'extensions de noyau* :

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

Pour en savoir plus sur le contrôle de politique des préférences de confidentialité :

support.apple.com/guide/mdm

Se préparer à distribuer des apps et des livres

Apple propose des programmes complets pour aider votre entreprise à tirer profit des apps et contenus formidables conçus pour macOS. Ces outils vous permettent de distribuer tant les apps et les livres achetés avec Apple Business Manager que vos apps maison, de sorte que vos employés aient tout le nécessaire pour travailler. Votre solution de GAM peut aussi distribuer des apps et installer des progiciels qui ne sont pas offerts par le Mac App Store.

La fonction de distribution gérée intégrée à la GAM permet en outre de distribuer les apps et livres achetés avec Apple Business Manager dans tout pays où ils sont offerts. Pour l'activer, vous devez lier votre solution de GAM à votre compte

* En anglais seulement.

Apple Business Manager à l'aide d'un jeton sécurisé. Dès que c'est fait, vous pouvez assigner des apps et des livres aux utilisateurs même si l'App Store est désactivé sur leur appareil. Vous pouvez aussi assigner des apps directement à un appareil si vous souhaitez que tous les utilisateurs de cet appareil y aient accès, une fonctionnalité qui simplifie grandement le déploiement.

Pour en savoir plus sur l'achat de contenus avec Apple Business Manager :
support.apple.com/guide/apple-business-manager

Pour en savoir plus sur la distribution d'apps et de livres :
support.apple.com/guide/apple-business-manager

Préparer les contenus supplémentaires

La solution de GAM peut aussi vous aider à distribuer des paquets de contenu ne provenant pas du Mac App Store. Cette approche est couramment employée pour bon nombre de logiciels d'entreprise, par exemple des apps maison ou des apps comme Chrome ou Firefox. Les logiciels requis sont ainsi transmis et installés automatiquement une fois le processus d'inscription terminé. Les paquets permettent aussi l'installation et l'exécution d'éléments divers tels que polices et scripts. Veillez à ce que ces paquets soient signés comme il se doit avec votre certificat de développeur du programme pour développeurs en entreprise.

Pour en savoir plus sur l'installation de contenus supplémentaires* :
support.apple.com/guide/deployment-reference-macos

3. Distribution

macOS permet de déployer, de personnaliser et de configurer les appareils facilement, sans l'aide des TI.

Utiliser l'Assistant réglages

Dès le démarrage, les employés peuvent sélectionner une langue et un pays et se connecter à un réseau en suivant l'Assistant réglages. Une fois la connexion Internet établie, l'Assistant réglages affiche une série de fenêtres pour les guider tout au long de la configuration. Les appareils inscrits via Apple Business Manager peuvent être automatiquement inscrits à la GAM au cours de ce processus. Il est également possible de configurer les systèmes Mac via l'inscription des appareils de manière à sauter des étapes telles que l'acceptation des modalités, la connexion avec un identifiant Apple ou l'activation des services de localisation.

La GAM peut ensuite être utilisée pour déployer divers réglages dès la configuration initiale des appareils, par exemple pour donner aux utilisateurs des privilèges d'administrateur. Comme sur iPhone et iPad, les utilisateurs dotés de tels privilèges sont en mesure de gérer leur Mac tout en se conformant aux politiques d'entreprise et aux réglages gérés par la GAM. Ensuite, pour permettre aux utilisateurs d'être productifs dès la configuration terminée, seuls les apps et logiciels les plus importants devraient être téléchargés et installés en arrière-plan. Les applications plus volumineuses pourront être téléchargées et installées en arrière-plan ultérieurement selon les réglages choisis par les utilisateurs dans le portail libre-service de la solution de GAM.

* En anglais seulement.

Configurer les comptes d'entreprise

Une solution de GAM peut configurer automatiquement la messagerie et d'autres comptes d'utilisateur. Selon celle que vous employez et son intégration à vos systèmes internes, les champs de données des comptes peuvent aussi être préremplis avec le nom de l'utilisateur, son adresse courriel et les identités de certificat pour l'authentification et la signature.

Autoriser la personnalisation par l'utilisateur

Permettre aux utilisateurs de personnaliser leur appareil peut se traduire par un gain de productivité, car ils choisissent alors les apps et contenus qui les aident à travailler le plus efficacement. Et grâce aux identifiants Apple gérés et à l'inscription par l'utilisateur sous macOS Catalina, de nouvelles options s'offrent aux entreprises pour permettre l'accès aux services Apple avec un identifiant fourni par l'organisation, qui peut aussi être utilisé conjointement avec un identifiant personnel.

Identifiant Apple et identifiant Apple géré

Quand les employés se servent d'un identifiant Apple pour se connecter à des services tels que FaceTime, iMessage, l'App Store et iCloud, ils ont accès à une vaste gamme de ressources qui simplifient le travail, favorisent la productivité et encouragent la collaboration. À l'instar de l'identifiant Apple standard, l'identifiant Apple géré sert à se connecter à un appareil personnel. Il donne aussi accès aux services Apple, y compris iCloud et les fonctionnalités de collaboration d'iWork et de Notes, ainsi qu'à Apple Business Manager. Toutefois, contrairement à l'identifiant Apple standard, il est détenu et géré par l'entreprise, qui s'occupe entre autres de la réinitialisation des mots de passe et de l'administration basée sur les rôles. L'identifiant Apple géré est également assorti de certaines restrictions.

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

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

Pour en savoir plus sur les identifiants Apple gérés* :
support.apple.com/guide/deployment-reference-macos

iCloud

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

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

* En anglais seulement.

4. Gestion

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

Contrôler les appareils

La solution de GAM veille sur les appareils gérés en exécutant un ensemble de tâches précises. Par exemple, vous pouvez interroger les appareils pour obtenir de l'information, ainsi qu'exécuter des tâches à distance en cas de vol, de perte ou de non-respect des politiques.

Requêtes

Une solution de GAM peut obtenir divers renseignements des appareils pour vérifier que les utilisateurs se servent des apps et réglages appropriés. L'information recueillie peut concerner les composants matériels (par exemple le numéro de série ou le modèle de l'appareil) ou logiciels (par exemple la version de macOS ou la liste des apps installées). De plus, la GAM peut obtenir des renseignements sur l'état des principales fonctionnalités de sécurité, comme FileVault ou le pare-feu intégré.

Tâches de gestion

Quand un appareil est géré, la solution de GAM peut exécuter tout un éventail de tâches administratives, comme modifier les réglages de configuration sans intervention des utilisateurs, mettre à jour macOS, bloquer ou effacer un appareil à distance, ou gérer les mots de passe.

Pour en savoir plus sur les tâches de gestion* :

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

Gérer les mises à jour logicielles

Les TI peuvent proposer aux utilisateurs de passer à la dernière version du système d'exploitation dès qu'elle est disponible. En testant une version préliminaire de macOS, ils sont à même de cibler vite fait les problèmes de compatibilité avec les apps – et d'aider les développeurs à les résoudre avant le lancement. Et par l'intermédiaire du programme de logiciels bêta d'Apple ou du programme AppleSeed pour les TI, ils peuvent aussi participer à la mise à l'essai de chaque nouvelle version. Adoptez une stratégie globale pour garder vos appareils Mac à jour et protéger les données de vos utilisateurs. Effectuez vos mises à jour fréquemment et passez à la toute dernière version de macOS dès que sa comptabilité avec votre flux de travail est vérifiée.

La GAM peut transmettre automatiquement les mises à jour de macOS aux ordinateurs Mac enregistrés via l'inscription des appareils. Ces derniers peuvent aussi être configurés de sorte que leurs mises à jour et les notifications connexes soient reportées jusqu'à concurrence de 90 jours si vos systèmes critiques ne sont pas prêts. Ainsi, les utilisateurs ne pourront lancer les mises à jour manuellement que si la politique est supprimée ou que la GAM envoie une commande d'installation.

Apple ne recommande ni ne prend en charge les solutions d'images système monolithiques pour les mises à niveau de macOS. Tout comme iPhone et iPad, les ordinateurs Mac reposent souvent sur des mises à jour micrologicielles propres au modèle. Les mises à jour du système d'exploitation de Mac exigent que ces mises à jour micrologicielles soient installées directement par Apple. La stratégie la plus fiable consiste à utiliser le programme d'installation de macOS ou les commandes de GAM.

* En anglais seulement.

Gérer des logiciels supplémentaires

Les organisations doivent souvent distribuer des apps supplémentaires aux utilisateurs après la configuration initiale. Pour les applications critiques et les mises à jour, ce peut être fait de façon automatique par la GAM. On peut aussi permettre aux employés de demander des apps via un portail libre-service intégré à la solution de GAM. Fort utiles, ces portails permettent notamment d'installer des logiciels achetés sur l'App Store au moyen d'Apple Business Manager, de même que des apps ne provenant pas de l'App Store, des scripts et d'autres utilitaires.

Bien que la plupart des logiciels puissent être installés automatiquement, certains d'entre eux nécessitent l'intervention des utilisateurs. Pour une sécurité renforcée, le téléchargement d'apps qui requièrent des extensions de noyau ne peut s'effectuer sans le consentement de l'utilisateur. C'est ce qu'on appelle le chargement d'extensions de noyau approuvées par l'utilisateur.

Maintenir la sécurité des appareils

En plus de respecter les politiques de sécurité établies avant le déploiement, votre équipe devra contrôler les appareils pour s'assurer du respect des politiques, et recueillir le plus de données possible avec votre solution de GAM. Ce contrôle pourrait comprendre une vérification de la posture de sécurité de chaque appareil ou la collecte d'information sur l'installation de correctifs logiciels. Bien que la plupart des organisations soient à l'aise d'utiliser les outils natifs pour sécuriser et chiffrer les données de Mac, certaines souhaitent aussi recourir à des services de synchronisation et de partage de fichiers, ou encore à des outils de prévention des pertes de données, pour empêcher les fuites de données d'entreprise et obtenir des rapports détaillés sur les données sensibles.

La fonctionnalité Localiser mon Mac d'iCloud permet d'effacer à distance un Mac perdu ou volé, ce qui entraînera la désactivation de l'appareil et la suppression de toutes les données. Les équipes des TI peuvent aussi exécuter un effacement à distance au moyen de la GAM.

Réassigner des appareils

Quand quelqu'un quitte l'organisation, son Mac peut aisément être réassigné à une autre personne à l'aide de la restauration par Internet et de la partition de secours locale. Les contenus de l'appareil seront alors effacés, et la dernière version du système d'exploitation sera installée. Tout ordinateur Mac assigné à une GAM dans Apple Business Manager sera réinscrit à la GAM à l'étape de l'Assistant réglages. Les paramètres du nouvel utilisateur seront configurés, les politiques d'entreprise seront appliquées et les logiciels appropriés seront installés – automatiquement. Les ordinateurs Mac qui ne sont pas inscrits peuvent être effacés et réassignés de la même manière, puis réinscrits manuellement.

Options d'assistance

Bon nombre d'organisations arrivent au même constat : les utilisateurs de Mac sollicitent peu l'aide des TI. Pour favoriser la débrouillardise et améliorer la qualité des services offerts, la plupart des équipes des TI conçoivent des ressources d'aide libre-service. Par exemple, elles créent des pages web consacrées à l'assistance Mac et des forums d'entraide, en plus d'offrir du soutien technique sur les lieux de travail. Les solutions de GAM permettent aussi aux utilisateurs d'exécuter des tâches de maintenance comme l'installation et la mise à jour de logiciels à partir d'un portail libre-service.

Idéalement, les entreprises ne devraient pas laisser les utilisateurs complètement à eux-mêmes. Il est plutôt recommandé d'adopter une approche collaborative en incitant les utilisateurs à diagnostiquer les problèmes avant de faire appel aux TI. Encouragez-les à prendre part au processus et à chercher à comprendre ce qui cloche avant de demander de l'aide.

La prise en charge partagée du soutien technique permet de limiter les interruptions de travail et de réduire les coûts liés à l'assistance et à la main-d'œuvre. Pour les organisations qui ont besoin de soutien additionnel, AppleCare offre une multitude de programmes et de services qui s'inscrivent en complément des services d'assistance internes pour les employés et les TI.

AppleCare pour entreprises

Si vous cherchez une protection complète, AppleCare pour entreprises peut vous aider à réduire la charge de travail de votre service informatique en offrant à vos employés du soutien technique par téléphone 24 heures sur 24, 7 jours sur 7, et un délai de réponse d'au maximum une heure pour les problèmes majeurs. Le programme offre des scénarios d'intégration destinés aux TI, y compris pour la GAM et Active Directory.

AppleCare OS Support

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

Soutien AppleCare pour centres d'assistance

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

AppleCare et AppleCare+ pour Mac

Chaque Mac 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. Avec AppleCare+ ou le Plan de protection AppleCare, vous pouvez prolonger la période de couverture à trois ans à compter de la date d'achat. Les employés sont invités à communiquer avec l'assistance Apple pour toute question relative aux équipements et logiciels Apple. Apple met également à votre disposition des options pratiques si vos appareils doivent être réparés. De plus, AppleCare+ pour Mac offre la prise en charge de réparations requises en raison de certains dommages accidentels, chaque incident entraînant des frais.

Pour en savoir plus sur les options d'assistance AppleCare :

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

Conclusion

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

Pour en savoir plus sur le déploiement, la gestion et les fonctionnalités de sécurité de macOS* :

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

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

support.apple.com/guide/mdm

Pour en savoir plus sur Apple Business Manager :

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

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

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

Pour en savoir plus sur Apple at Work :

www.apple.com/ca/fr/business

Pour en savoir plus sur les fonctionnalités des TI :

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

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

www.apple.com/security/

Pour en savoir plus sur les programmes AppleCare :

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

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

training.apple.com

Pour en savoir plus sur les Services professionnels Apple :

consultingservices@apple.com

* En anglais seulement.

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