# Présentation du déploiement du Mac

# Introduction

Table des matières



Chez Apple, nous sommes convaincus que les professionnels donnent le meilleur d'eux-mêmes quand ils ont accès aux meilleurs outils et à la meilleure technologie. Tous nos produits sont conçus pour stimuler la créativité et la productivité, et pour favoriser l'émergence de nouvelles méthodes de travail, au bureau comme en déplacement. Cette approche est en parfaite adéquation avec la façon dont on souhaite travailler aujourd'hui, c'est-à-dire en bénéficiant d'un meilleur accès à l'information, en profitant d'une collaboration et d'échanges fluides, et en ayant la liberté de rester connecté et de travailler de n'importe où.

Jamais il n'a été aussi facile de déployer le Mac dans un environnement professionnel. Grâce à des services essentiels fournis par Apple et à une solution tierce de gestion des appareils mobiles (MDM), votre entreprise peut facilement déployer des Mac et en assurer la maintenance à grande échelle. Si votre entreprise a déjà déployé en interne des appareils iOS et iPadOS, il est probable que la plupart des adaptations de l'infrastructure nécessaires à la mise en œuvre de macOS aient déjà été réalisées.

De récentes améliorations de la sécurité, de la gestion et du déploiement du Mac permettent de passer de la création d'images monolithiques et de la liaison avec un service d'annuaire classique à un modèle d'approvisionnement homogène et à un processus de déploiement centré sur chaque utilisateur, reposant exclusivement sur des outils intégrés à macOS.

Ce document fournit des conseils sur tout ce qu'il vous faut pour déployer des Mac à l'échelle de votre entreprise, de la compréhension de votre infrastructure existante à la gestion des appareils, en passant par un approvisionnement rationalisé. Les sujets abordés dans ce document sont présentés plus en détail dans le document Référence pour le déploiement du Mac, disponible sur :
support.apple.com/guide/deployment-reference-macos

# Premiers pas

Au tout début du processus de déploiement, il est important d'élaborer une stratégie de déploiement et un plan de mise en œuvre et, s'il existe déjà des appareils macOS dans l'entreprise, d'évaluer la manière dont les employés les utilisent. Faites en sorte d'impliquer les équipes nécessaires très tôt dans le processus et de les mettre en phase avec votre vision du programme et vos objectifs. Certaines équipes commencent par une étude de faisabilité pour mettre au jour les éventuelles difficultés propres à leur environnement. Il est primordial de réaliser un projet pilote plus vaste auprès des utilisateurs existants afin de comprendre l'usage qui est fait des appareils dans l'ensemble de votre entreprise, et de savoir si votre équipe doit être informée de certains problèmes.

Les informations recueillies durant cette phase peuvent aider à déterminer quels rôles et fonctions au sein de l'entreprise bénéficieraient au maximum du Mac. Le service informatique peut ensuite décider s'il vaut mieux proposer macOS comme norme dans l'ensemble de l'organisation ou comme choix offert à certains postes.

Bien souvent, cette phase permet aussi de recenser les outils et apps internes devant être rendus compatibles avant le déploiement du Mac à grande échelle. Concentrez-vous d'abord sur les principales apps de productivité, de collaboration et de communication qui serviront à la majorité des utilisateurs. Les services internes stratégiques comme l'intranet de l'entreprise, les services d'annuaires et les logiciels de gestion des dépenses ont également une importance considérable pour la productivité d'une grande partie des employés.

Documentez toute solution alternative ou de remplacement d'outils internes, et communiquez à ce sujet, tout en encourageant les personnes propriétaires d'une application à la moderniser quand cela est nécessaire. Soyez transparent avec les utilisateurs sur les différentes apps métier qu'ils pourront utiliser en choisissant le Mac et laissez la demande des utilisateurs orienter l'ordre de priorité des actions de modernisation. Si nécessaire, élaborez avec les propriétaires d'applications un plan de mise à jour de leurs apps, en tirant parti à la fois du SDK macOS et de Swift ainsi que des divers partenaires professionnels spécialisés dans le développement et prêts à les aider.

Les ordinateurs Mac sont généralement fournis comme de l'équipement appartenant à l'entreprise. Certaines entreprises autorisent toutefois leurs employés à utiliser leur propre Mac dans le cadre de programmes BYOD (« Apportez vos appareils personnels »). Quel que soit le modèle de propriété de votre entreprise, donner le choix aux employés d'utiliser des produits Apple peut se révéler très bénéfique pour l'ensemble de l'entreprise et se traduire par un niveau supérieur de productivité, de créativité, d'implication et de satisfaction des collaborateurs, et par une baisse des coûts en termes de valeurs résiduelles et d'assistance. Les organisations peuvent également profiter de diverses options de crédit-bail et de financement pour réduire leurs frais immédiats. Il est possible de compenser les coûts en permettant aux employés de contribuer par des retenues sur salaire lorsqu'ils changent d'appareil ou de racheter leur équipement à la fin du crédit-bail ou du cycle de vie d'un appareil.

Les règles de l'entreprise ainsi que les processus de déploiement, de gestion et d'assistance décrits dans ce document peuvent varier en fonction des informations recueillies par votre équipe pendant un projet pilote. Les utilisateurs n'ont pas tous les mêmes besoins en termes de règles, de réglages et d'apps car souvent, les exigences varient considérablement d'un groupe à l'autre ou d'une équipe à l'autre dans une société.

# Étapes du déploiement

Le déploiement de macOS s'organise en quatre grandes étapes : la préparation de l'environnement, la configuration de la solution MDM, le déploiement des appareils auprès des employés et la réalisation des tâches de gestion continue.

## 1. Préparation

La première étape de tout déploiement consiste à évaluer votre environnement existant. Il s'agit, dans cette phase, de mieux comprendre votre réseau et vos infrastructures clés, et d'installer les systèmes nécessaires à un déploiement réussi.

### Évaluer votre infrastructure

Bien que le Mac s'intègre sans problème dans la plupart des environnements informatiques d'entreprise standard, il est toujours essentiel d'évaluer votre infrastructure existante pour vous assurer que votre entreprise tire le meilleur parti des possibilités offertes par macOS. Si votre organisation a besoin d'aide dans ce domaine, vous pouvez faire appel aux Services professionnels Apple ou vous adresser aux équipes techniques de votre revendeur ou de votre partenaire du réseau de distribution.

#### Wi-Fi et réseau

Un accès stable et fiable à un réseau sans fil est essentiel pour l'installation et la configuration des appareils macOS. Vérifiez que le réseau Wi-Fi de votre entreprise est correctement conçu, en veillant à ce que l'emplacement et l'alimentation des points d'accès répondent aux besoins de capacité et d'itinérance.

Vous devrez peut-être adapter la configuration de vos proxies web ou des ports de coupe-feu si les appareils ne parviennent pas à accéder aux serveurs Apple, au service de notification push Apple (APNs), à iCloud ou à l'iTunes Store. Tout comme avec l'iPad et l'iPhone, certains aspects du processus de déploiement du Mac, en particulier avec les Mac récents, nécessitent un accès à ces services pour des opérations telles que la mise à niveau du programme interne lors de l'installation.

Apple et Cisco ont à cet effet optimisé la façon dont les Mac communiquent sur les réseaux sans fil Cisco, en prenant en charge des fonctionnalités avancées de mise en réseau de macOS, comme la qualité de service (QoS). Si vous êtes équipé d'un matériel réseau Cisco, collaborez avec vos équipes internes pour vous assurer que le Mac sera bien en mesure d'optimiser le trafic stratégique.

Les entreprises doivent également évaluer leur infrastructure VPN pour s'assurer que les utilisateurs pourront accéder à distance et de façon sécurisée aux ressources de l'entreprise. Envisagez d'utiliser la fonctionnalité VPN à la demande de macOS pour que les connexions VPN ne soient initiées que lorsqu'elles sont nécessaires. Si vous prévoyez d'utiliser le VPN via l'app, vérifiez que vos passerelles VPN prennent en charge cette fonctionnalité et que vous disposez d'un nombre suffisant de licences pour couvrir le nombre approprié d'utilisateurs et de connexions.

Assurez-vous que votre infrastructure réseau est configurée pour fonctionner avec Bonjour, le protocole réseau standard d'Apple qui ne nécessite aucune configuration. Bonjour permet aux appareils de trouver automatiquement des services sur un réseau. macOS utilise Bonjour pour se connecter aux imprimantes compatibles AirPrint et aux appareils compatibles AirPlay, comme l'Apple TV. Certaines apps et fonctionnalités intégrées à macOS utilisent également Bonjour pour découvrir d'autres appareils à des fins de collaboration et de partage.

En savoir plus sur la conception d'un réseau Wi-Fi :
support.apple.com/guide/deployment-reference-macos

En savoir plus sur la configuration d'un réseau pour une solution MDM :
support.apple.com/HT210060

En savoir plus sur Bonjour :
support.apple.com/guide/deployment-reference-macos

**Gérer les identités**
Pour la gestion des identités et d'autres informations sur les utilisateurs, macOS peut accéder à des services d'annuaires, notamment Active Directory, Open Directory et LDAP. Certains éditeurs de solutions MDM fournissent des outils permettant d'intégrer directement leurs solutions de gestion avec les annuaires Active Directory et LDAP. D'autres outils, comme l'extension d'authentification unique Kerberos de macOS Catalina, assurent l'intégration avec les règles et fonctionnalités Active Directory sans nécessiter de liaison traditionnelle ou de compte mobile. Divers types de certificats émanant d'autorités de certification (AC) internes et externes peuvent également être gérés par votre solution MDM afin que les identités soient automatiquement vérifiées.

En savoir plus sur la nouvelle extension d'authentification unique Kerberos :
support.apple.com/guide/deployment-reference-macos

En savoir plus sur l'intégration des services d'annuaire :
support.apple.com/guide/deployment-reference-macos

**Services essentiels destinés aux employés**
Vérifiez que votre service Microsoft Exchange est à jour et configuré de façon à prendre en charge tous les utilisateurs du réseau. Si vous n'utilisez pas Exchange, macOS est également compatible avec des serveurs standard, notamment IMAP, POP, SMTP, CalDAV, CardDAV et LDAP. Testez les processus de base pour les e-mails, les contacts et les calendriers ainsi que d'autres logiciels de productivité et de collaboration couvrant le pourcentage le plus élevé des besoins stratégiques quotidiens des utilisateurs.

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

En savoir plus sur les services standard :
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 du contenu fréquemment demandé auprès des serveurs Apple, ce qui contribue à réduire la bande passante requise pour télécharger du contenu sur votre réseau. Vous pouvez utiliser la mise en cache pour accélérer le téléchargement et la distribution de logiciels via le Mac App Store. Vous pouvez également mettre en cache les mises à jour de logiciels pour en accélérer le téléchargement sur les appareils de votre entreprise, qu'il s'agisse d'appareils macOS, iOS ou iPadOS. Les autres contenus peuvent également être mis en cache grâce à des solutions tierces de Cisco et d'Akamai.

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

## Mettre en place une solution de gestion

La MDM permet aux entreprises d'inscrire les Mac en toute sécurité dans leur environnement professionnel, de configurer et d'actualiser sans fil les réglages, de déployer des apps, de vérifier le respect des règles, d'interroger les appareils et d'effacer ou de verrouiller à distance des appareils gérés. Le service informatique peut ainsi facilement créer des profils pour gérer les comptes utilisateur, configurer les réglages système, appliquer des restrictions et définir des règles de mots de passe. Le tout, depuis la même solution de gestion des appareils mobiles que ce service utilise aujourd'hui pour l'iPhone et l'iPad.

En coulisses, toutes les plateformes Apple utilisent une même structure de gestion signée Apple, qui permet aux clients d'utiliser diverses solutions MDM provenant de fournisseurs tiers. Des sociétés telles que Jamf, VMware et MobileIron proposent une large gamme de solutions de gestion des appareils. Bien que macOS, iOS et iPadOS aient en commun un grand nombre de structures pour la gestion des appareils, ces solutions MDM tierces diffèrent légèrement en termes de fonctionnalités d'administration, de prise en charge du système d'exploitation, de grilles tarifaires et de modèles d'hébergement. Elles peuvent également proposer différents niveaux de service pour l'intégration, la formation et l'assistance. Avant de choisir une solution, déterminez quelles sont les fonctionnalités les plus pertinentes pour votre entreprise.

Une fois que vous aurez sélectionné votre solution MDM, vous devrez vous connecter au portail des certificats push d'Apple (Apple Push Certificates Portal) pour créer un nouveau certificat push de MDM.

En savoir plus sur le déploiement des solutions MDM :
support.apple.com/guide/deployment-reference-macos

Consulter le portail Apple Push Certificates :
identity.apple.com/pushcert/

## S'inscrire à Apple Business Manager

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

Le Programme d'inscription des appareils (Device Enrolment Program, DEP) et le Programme d'achat en volume (Volume Purchase Program, VPP) sont désormais entièrement intégrés à Apple Business Manager. Les organisations disposent donc de tout ce dont elles ont besoin pour déployer des appareils Apple. La disponibilité de ces programmes prendra fin au 1er décembre 2019.

## Appareils

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

- Simplifiez les étapes de l'Assistant réglages pour optimiser le processus de configuration et vous assurer que les appareils des employés sont correctement configurés dès leur activation. Les équipes informatiques peuvent maintenant personnaliser davantage ce processus en proposant aux utilisateurs un texte de consentement, une image de marque personnalisée ou encore une méthode d'authentification moderne.

- Augmentez le niveau de contrôle des appareils appartenant à l'organisation grâce à la supervision, qui propose des commandes de gestion de l'appareil supplémentaires indisponibles avec les autres modèles de déploiement, y compris l'irrévocabilité de la solution MDM.
- Gérez plus facilement les serveurs MDM par défaut en paramétrant un serveur par défaut en fonction du type d'appareil. Enfin, vous pouvez désormais inscrire manuellement des iPhone, iPad et Apple TV à l'aide d'Apple Configurator 2, quelle que soit la manière dont vous les avez acquis.

## Contenu

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

- Achetez des apps, des livres et des apps personnalisées en volume, y compris les apps que vous avez développées en interne. Transférez facilement des licences d'applications d'un site à l'autre et partagez les licences entre acheteurs situés au même endroit. Consultez une liste consolidée de l'historique des achats, avec notamment le nombre actuel de licences utilisées avec la MDM.
- Distribuez les apps et les livres directement aux appareils gérés ou aux utilisateurs autorisés et vérifiez facilement quel contenu a été attribué à quel utilisateur ou appareil. Grâce à la distribution gérée, vous contrôlez tout le processus de distribution tout en restant entièrement propriétaire des apps. Et si une app n'est plus utilisée par un appareil ou un utilisateur, elle peut être révoquée et réattribuée à un autre appareil ou utilisateur au sein de votre organisation.
- Plusieurs options de paiement sont disponibles, notamment par carte bancaire ou sur bon de commande. Les organisations peuvent acheter du crédit VPP (dans les pays où cela est proposé) d'un montant spécifique en devise locale auprès d'Apple ou d'un Revendeur Agréé Apple. Ce montant est transféré de manière électronique au titulaire du compte sous forme d'avoir.
- Distribuez une app aux appareils ou utilisateurs dans tous les pays où l'app est disponible, pour une distribution internationale. Les développeurs peuvent proposer leurs apps dans plusieurs pays via le processus standard de publication sur l'App Store.

Remarque : les achats de livres dans Apple Business Manager ne sont pas disponibles dans tous les pays et régions. Pour connaître les fonctionnalités et méthodes d'achat disponibles, consultez consultez support.apple.com/HT207305.

## Personnes

Apple Business Manager permet aux organisations de créer et de gérer des comptes pour les employés. Ces comptes s'intègrent à l'infrastructure existante et donnent accès aux apps Apple, aux services Apple et à Apple Business Manager.

- Créez des identifiants Apple gérés pour que les employés collaborent dans les apps et les services Apple, et accèdent aux données de l'entreprise dans les apps gérées utilisant iCloud Drive. Ces comptes sont détenus et gérés par chaque organisation.

- Associez Apple Business Manager avec Microsoft Azure Active Directory pour tirer parti de l'authentification fédérée. Les identifiants Apple gérés seront automatiquement créés à chaque fois qu'un employé se connectera pour la première fois avec ses identifiants sur un appareil Apple compatible.
- Avec la nouvelle fonctionnalité Inscription d'utilisateurs disponible sous iOS 13, iPadOS et macOS Catalina, les appareils appartenant aux utilisateurs peuvent simultanément accueillir un identifiant Apple géré et un identifiant Apple personnel. Un identifiant Apple géré peut aussi être utilisé sur n'importe quel appareil en tant qu'identifiant Apple principal (et unique). Et après une première connexion à un appareil Apple avec un identifiant Apple géré, l'utilisateur pourra s'en servir pour accéder à iCloud sur le Web.
- Vous pouvez désigner des rôles spécifiques dans les équipes informatiques de votre entreprise afin de gérer plus efficacement les appareils, les apps et les comptes intégrés à Apple Business Manager. Le rôle Administrateur permet par exemple d'accepter des conditions générales d'utilisation si cela est nécessaire, et de facilement transférer des responsabilités si un employé quitte l'entreprise.

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

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

### S'inscrire à l'Apple Developer Enterprise Program

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

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

## 2. Configuration

Pour mener à bien votre déploiement et configurer les Mac de vos employés, vous devez définir des règles d'entreprise et préparer votre solution de gestion des appareils mobiles.

### Comprendre la sécurité de macOS

La sécurité et la confidentialité sont au cœur même de la conception de tous les matériels, logiciels et services Apple. Nous préservons la confidentialité de nos clients grâce à un chiffrement fort et à des règles strictes régissant la manière dont les données sont gérées. La sécurisation de votre plateforme informatique pour les appareils Apple passe par :

- des méthodes empêchant toute utilisation non autorisée des appareils ;
- la protection des données au repos, notamment en cas de perte ou de vol d'un appareil ;
- des protocoles réseau et le chiffrement des données transmises ;
- la possibilité d'exécuter des apps en toute sécurité, sans compromettre l'intégrité de la plateforme.

Tous les appareils Apple intègrent plusieurs niveaux de sécurité, ce qui leur permet d'accéder aux services réseau en toute sécurité et de protéger les données importantes. macOS, iOS et iPadOS assurent également la sécurité grâce à des règles de codes et de mots de passe pouvant être diffusées et appliquées avec la MDM. Si un appareil tombe entre de mauvaises mains, un utilisateur ou un administrateur peut utiliser une commande à distance pour en supprimer toutes les informations privées.

Le service informatique peut utiliser la solution MDM pour déployer toute une gamme de règles visant à sécuriser les appareils. Il peut s'agir, par exemple, de mettre en œuvre FileVault et un séquestre de clés de secours avec la MDM, d'imposer une règle de mot de passe spécifique ou le verrouillage par économiseur d'écran, ou encore d'activer le coupe-feu intégré.

En savoir plus sur la sécurité de la plateforme Apple : apple.com/security/

### Définir les règles de l'entreprise

Initiez le développement de votre politique d'entreprise en établissant des règles générales concernant la majorité des utilisateurs Mac de votre entreprise. Votre solution MDM vous permettra de définir des personnalisations propres à l'utilisateur, comme des comptes ou l'accès à certaines apps. Vous pouvez aussi définir des règles spécifiques pour des entités ou des groupes plus restreints d'utilisateurs : par exemple, déployer des logiciels ou des réglages propres à un service.

Collaborez avec vos équipes internes pour actualiser les règles existant dans l'entreprise afin d'y intégrer l'utilisation des ordinateurs Mac. Certaines règles essentielles sont communes à l'ensemble des plateformes, telles que la complexité des mots de passe et les exigences en matière de rotation, les délais d'attente de l'économiseur d'écran et l'utilisation acceptable.

Si vos règles d'entreprise requièrent une technologie spécifique mise en œuvre sur une autre plateforme, identifiez le problème sous-jacent et redéfinissez les règles afin qu'elles prennent en compte les technologies intégrées à macOS. Au lieu d'exiger que tous les ordinateurs utilisent une solution tierce spécifique pour chiffrer tout un disque, envisagez de mettre au point une règle exigeant que les données d'entreprise soient chiffrées au repos et faites accomplir cette tâche par FileVault. Si la règle exige un logiciel particulier pour la protection contre les logiciels malveillants, informez les équipes sur les fonctionnalités intégrées telles que Gatekeeper, puis actualisez la règle pour en permettre l'utilisation.

### Configurer les réglages dans la MDM

Pour permettre la gestion des règles d'entreprise et veiller à ce que les employés aient accès aux ressources nécessaires, chaque Mac sera inscrit de façon sécurisée auprès de votre solution MDM. Les solutions MDM appliquent ensuite les règles et les réglages à l'aide de profils de configuration. Les profils de configuration sont des fichiers XML créés par votre solution MDM qui permettent la distribution des réglages aux appareils. Ces profils automatisent la configuration des réglages, comptes, règles, restrictions et identifiants. Ils peuvent être signés et chiffrés afin de renforcer la sécurité de vos systèmes.

Une fois qu'un appareil est inscrit auprès de la MDM, un administrateur peut mettre en place une règle et lancer une requête ou une commande MDM. Avec une connexion réseau, l'appareil reçoit ensuite une notification via le service de notification push d'Apple (APNs) lui donnant l'ordre de communiquer directement avec son serveur MDM par le biais d'une connexion sécurisée pour traiter l'action de l'administrateur. Comme la communication n'est établie qu'entre la solution MDM et l'appareil, le service APNs ne transmettra aucune information confidentielle ou privée. Si un appareil est supprimé de la gestion, les règles et réglages contrôlés par ce profil de configuration seront également supprimés. En cas de besoin, l'entreprise peut également effacer à distance le contenu d'un appareil.

Nombre d'organisations lient leur solution MDM à leurs services d'annuaires existants. L'Assistant réglages de macOS peut demander aux utilisateurs de se connecter à l'aide de leur identifiant du service d'annuaire lors de l'inscription automatisée des appareils. Dans macOS Catalina, les nouvelles options de personnalisation de l'inscription permettent à l'Assistant réglages d'afficher l'authentification des fournisseurs d'identités utilisant un service dans le nuage. Une fois l'appareil attribué à un utilisateur spécifique, la MDM peut personnaliser les configurations et les comptes propres à une personne ou un groupe. Par exemple, le compte Microsoft Exchange d'un utilisateur peut être mis automatiquement à disposition lors de l'inscription. Il est également possible d'utiliser des identités de certificat pour des technologies telles que 802.1x, VPN, etc.

Étant donné le contrôle que procurent ces systèmes, les entreprises se sentent souvent fondées à accorder à un utilisateur un accès administrateur complet à son Mac, lui permettant ainsi de personnaliser pleinement ses réglages, d'installer des apps et de résoudre des problèmes tout en restant dans le cadre de la politique d'entreprise via la MDM. Ce modèle suit le type de privilèges et de contrôles dont disposent les utilisateurs sur leur iPhone ou iPad lorsqu'ils sont soumis à une politique de gestion.

En savoir plus sur les profils de configuration :
support.apple.com/guide/deployment-reference-macos

### Préparer l'inscription automatisée des appareils

La méthode la plus simple pour inscrire un appareil auprès de la MDM consiste à utiliser l'Assistant réglages avec les fonctionnalités d'inscription automatisée des appareils d'Apple Business Manager. Cette méthode permet d'inscrire les appareils sans intervention du service informatique et de simplifier certains écrans de l'Assistant réglages afin d'accélérer le processus pour les utilisateurs.

Pour configurer l'inscription automatisée des appareils, vous devez lier votre solution MDM à votre compte Apple Business Manager via un jeton sécurisé. L'autorisation sécurisée d'une solution MDM s'effectue via un processus de vérification en deux étapes. Votre fournisseur de solution MDM peut vous donner des informations sur les conditions requises pour mettre en œuvre ce processus.

Si les appareils sont déjà utilisés par les employés ou leur appartiennent, un seul profil de configuration peut être ouvert par l'utilisateur et vérifié dans les Préférences Système pour finaliser l'inscription. C'est ce qu'on appelle l'inscription à la MDM « approuvée par l'utilisateur ». L'inscription doit s'effectuer soit par le biais de l'inscription des appareils, soit par le biais de l'inscription à la MDM approuvée par l'utilisateur pour gérer certains réglages sensibles à la sécurité, comme les règles s'appliquant aux extensions de noyau ou le contrôle des règles de préférence de confidentialité.

En savoir plus sur le chargement des extensions de noyau :
support.apple.com/guide/deployment-reference-macos

En savoir plus sur le Contrôle de politique de préférences Confidentialité :
support.apple.com/guide/mdm

### Préparer la distribution d'apps et de livres

Apple propose des programmes complets pour aider votre entreprise à tirer parti des apps et des contenus de qualité disponibles pour macOS. Ces fonctionnalités vous permettent de distribuer les apps et les livres achetés via Apple Business Manager ainsi que les apps développées en interne, afin que vos employés aient tous les outils dont ils ont besoin pour être productifs. La solution MDM peut également distribuer des apps et installer des paquets logiciels non disponibles sur le Mac App Store.

Votre solution MDM peut utiliser la distribution gérée pour distribuer les apps et les livres achetés sur Apple Business Manager dans tous les pays où les apps en question sont disponibles. Pour activer la distribution gérée, vous devez tout d'abord associer votre solution MDM à votre compte Apple Business Manager à l'aide d'un jeton sécurisé. Une fois connecté à votre solution MDM, vous pouvez attribuer des apps et des livres à des utilisateurs même si l'App Store est désactivé sur l'appareil. Vous pouvez également attribuer des apps directement à un appareil, ce qui simplifie considérablement le déploiement puisque n'importe quel utilisateur de cet appareil aura accès à ces apps.

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

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

### Préparer les contenus supplémentaires

Votre solution MDM peut vous aider à distribuer des paquets logiciels supplémentaires, dont le contenu ne provient pas du Mac App Store. C'est une approche courante pour de nombreux paquets logiciels d'entreprise, tels que les applications internes personnalisées ou des apps comme Chrome ou Firefox. Les logiciels requis peuvent être « poussés » à l'aide de cette méthode et installés automatiquement après finalisation de l'inscription. Les polices, scripts et autres éléments peuvent également être installés et exécutés via des paquets. Veillez à ce que ces paquets soient correctement signés avec votre identifiant de développeur de l'Apple Developer Enterprise Program.

En savoir plus sur l'installation des contenus supplémentaires :
support.apple.com/guide/deployment-reference-macos

## 3. Déploiement

Avec macOS, il est facile de déployer des appareils auprès des employés, de les personnaliser en fonction des besoins et d'être opérationnel sans recours au service informatique.

## Utiliser l'Assistant réglages

Au démarrage, les employés peuvent utiliser l'utilitaire Assistant réglages de macOS pour définir leurs préférences de langue et de région, et se connecter à un réseau. Une fois connectés à Internet, les utilisateurs accéderont à différentes fenêtres de l'Assistant réglages, lequel les guidera étape par étape dans la configuration de leur nouveau Mac. Les appareils inscrits à Apple Business Manager peuvent être automatiquement inscrits à la MDM au cours de ce processus. Les systèmes Mac inscrits peuvent aussi être configurés de manière à sauter certaines étapes, telles que les Conditions générales, la connexion à l'aide d'un identifiant Apple et le service de localisation.

Une fois les étapes de l'Assistant réglages effectuées, la MDM peut servir à déployer toute une variété de réglages lors de la configuration initiale, notamment pour déterminer si un utilisateur doit bénéficier de privilèges administratifs complets sur son ordinateur. Comme sur iPhone et iPad, cette option permet à l'utilisateur de contrôler son appareil tout en respectant les règles de l'entreprise et les réglages gérés par la MDM. Pour permettre aux utilisateurs d'être productifs dès que l'Assistant réglages a terminé la configuration, seuls les applications et paquets logiciels stratégiques doivent commencer à se télécharger et à s'installer en arrière-plan, sans empêcher l'employé de se mettre au travail. Les applications plus volumineuses peuvent être programmées pour être téléchargées et installées en arrière-plan ou à un stade ultérieur par l'utilisateur dans l'outil de libre-service de votre solution MDM.

## Configurer les comptes d'entreprise

La solution MDM peut configurer automatiquement la messagerie électronique et les autres comptes utilisateur. En fonction de la solution MDM que vous utilisez et de son intégration à vos systèmes internes, les données utiles de compte peuvent également être pré-renseignées avec un nom d'utilisateur, une adresse e-mail et des identités de certificat à des fins d'authentification et de signature.

## Autoriser la personnalisation par les utilisateurs

Permettre aux utilisateurs de personnaliser leurs appareils est susceptible d'accroître la productivité, car ce sont les utilisateurs qui choisissent les apps et les contenus qui leur permettront de gagner en efficacité pour réaliser leurs tâches et leurs objectifs. Dorénavant, avec les identifiants Apple gérés et la fonctionnalité Inscription d'utilisateurs de macOS Catalina, les entreprises disposent de nouvelles options pour rendre les services Apple accessibles aux employés, qui peuvent simultanément utiliser leur appareil avec un identifiant Apple appartenant à l'entreprise ou un identifiant Apple personnel.

### Identifiant Apple et identifiant Apple géré

Lorsque les employés se connectent à des services Apple comme FaceTime, iMessage, l'App Store et iCloud avec leur identifiant Apple, ils ont accès à un vaste éventail de contenus conçus pour simplifier leurs tâches professionnelles, améliorer leur productivité et les aider à mieux collaborer. Comme tous les identifiants Apple, les identifiants Apple gérés permettent de se connecter à un appareil personnel. Ils sont aussi utilisés pour accéder à des services Apple comme iCloud, pour collaborer en utilisant iWork et Notes, et pour se connecter à Apple Business Manager. Contrairement aux identifiants Apple, les identifiants Apple gérés sont détenus et gérés par votre entreprise. Elle peut ainsi, par exemple, réinitialiser les mots de passe de ces identifiants et appliquer une administration basée sur les rôles. Certains réglages des identifiants Apple gérés sont restreints.

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

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

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

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

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

# 4. Gestion

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

## Gérer les appareils

Des solutions MDM peuvent administrer un appareil géré au moyen d'un ensemble de tâches spécifiques. Il s'agit notamment d'interroger des appareils pour recueillir des informations ou encore de mettre en place des tâches permettant de gérer les appareils perdus, volés ou qui ne respectent pas les règles.

**Requêtes**
Une solution MDM peut interroger des appareils pour leur demander toutes sortes d'informations afin de s'assurer que les utilisateurs disposent bien de l'ensemble approprié d'applications et de réglages. Les requêtes peuvent porter sur le matériel (par exemple, le numéro de série ou le modèle de l'appareil) ou sur les logiciels (par exemple, le numéro de version de macOS ou une liste des applications installées). Par ailleurs, la MDM peut se renseigner sur l'état des fonctionnalités de sécurité essentielles, comme FileVault ou le coupe-feu intégré.

**Tâches de gestion**
Lorsqu'un appareil est géré, la solution MDM peut effectuer un large éventail de tâches administratives : par exemple, modifier automatiquement des réglages de configuration sans interaction avec l'utilisateur, effectuer une mise à jour de macOS, verrouiller un appareil ou en effacer le contenu à distance, ou encore gérer les mots de passe.

En savoir plus sur les tâches de gestion :
support.apple.com/guide/deployment-reference-macos

## Gérer les mises à jour logicielles

Le service informatique peut laisser le choix aux utilisateurs d'installer la dernière version du système d'exploitation au moment de sa sortie. En testant une pré-version de macOS, le service informatique s'assure que les problèmes de compatibilité ont été identifiés et qu'ils seront résolus par les développeurs avant la sortie de la version finale. L'équipe informatique peut participer aux tests de chaque version grâce au Programme de logiciels bêta d'Apple ou au programme AppleSeed for IT. Adoptez une approche globale pour l'actualisation des ordinateurs Mac afin de protéger vos utilisateurs et leurs données. Procédez régulièrement à la mise à jour, dès que vous avez déterminé que votre flux de travail est compatible avec une nouvelle version de macOS.

La MDM peut « pousser » automatiquement les mises à jour de macOS sur un Mac inscrit. Un Mac inscrit peut également être configuré pour différer les mises à jour et les notifications de mises à jour sur une période allant jusqu'à 90 jours si les systèmes stratégiques ne sont pas prêts. Les utilisateurs ne seront pas en mesure de lancer les mises à jour de façon manuelle tant que la règle n'aura pas été supprimée ou que la MDM n'aura pas envoyé une commande d'installation.

Apple ne recommande ni ne prend en charge la création d'images système monolithiques pour les mises à jour de macOS. Comme les iPhone et iPad, les Mac reposent souvent sur des mises à jour du programme interne propres à leur modèle. De même, les mises à jour du système d'exploitation du Mac exigent que ces mises à jour du programme interne soient installées directement par Apple. La stratégie la plus fiable consiste à utiliser le programme d'installation de macOS ou les commandes MDM pour effectuer les mises à jour.

## Gérer les logiciels supplémentaires

Au-delà de l'ensemble de base, les organisations ont souvent besoin de distribuer à leurs utilisateurs des logiciels supplémentaires. Cela peut être effectué automatiquement par la MDM pour les applications et mises à jour stratégiques, ou à la demande en permettant aux utilisateurs de se procurer des applications via un portail de libre-service fourni par votre solution MDM. Ces portails peuvent se charger de tout, comme installer les logiciels achetés sur l'App Store via Apple Business Manager, mais aussi les apps ne provenant pas de l'App Store, les scripts et autres utilitaires.

Si la plupart des logiciels peuvent être installés automatiquement, certaines installations nécessitent toutefois une action de la part de l'utilisateur. Pour renforcer la sécurité, les apps ayant besoin d'extensions de noyau exigent désormais le consentement de l'utilisateur pour se charger. Ce processus, appelé chargement de l'extension de noyau approuvé par l'utilisateur, peut être géré par la MDM.

## Assurer la sécurité des appareils

Au-delà de l'ensemble initial de règles de sécurité établies avant le déploiement des appareils, votre équipe devra surveiller les machines pour vérifier qu'elles respectent les règles et obtenir le maximum d'informations à des fins de reporting via votre solution MDM. Il peut s'agir de surveiller l'état de chaque appareil en matière de sécurité ou de recueillir des informations sur l'installation de correctifs logiciels. Si la plupart des entreprises n'ont aucune difficulté à utiliser des outils natifs pour chiffrer et protéger chaque Mac, certaines peuvent néanmoins exiger l'utilisation de services complémentaires de synchronisation et de partage des fichiers ou d'outils de prévention des pertes de données pour éviter les fuites de données de l'entreprise et fournir des rapports approfondis sur des données sensibles, quelle qu'en soit la nature.

La fonctionnalité Localiser mon Mac d'iCloud peut lancer un effacement à distance pour désactiver un Mac et en supprimer toutes les données, si celui-ci est perdu ou volé. Les équipes informatiques peuvent également effectuer un effacement à distance à l'aide de la MDM.

### Réapprovisionner les appareils

Il est facile de réapprovisionner un Mac pour un autre utilisateur lorsqu'un employé quitte l'entreprise, avec Récupération Internet et la partition de secours locale. Cette manipulation permet d'effacer le contenu du Mac et d'installer la dernière version du système d'exploitation. Les Mac associés à une solution MDM spécifique dans Apple Business Manager seront automatiquement réinscrits avec cette solution MDM au cours de l'exécution de l'Assistant réglages. La configuration des réglages du nouvel utilisateur, l'application des règles de l'entreprise et le déploiement des logiciels requis seront également effectués de manière automatique. Pour les Mac qui ne sont pas inscrits, le même processus sera utilisé pour en effacer le contenu et les réapprovisionner, puis la réinscription se fera manuellement.

# Options d’assistance

Bon nombre d’entreprises constatent que les utilisateurs Mac n’ont besoin que d’une assistance informatique minimale. Pour encourager l’assistance autonome et améliorer la qualité de l’assistance, la plupart des équipes informatiques développent des outils d’auto-assistance. Il peut s’agir de pages web d’assistance Mac, de forums d’auto-assistance et de comptoirs d’aide technique sur site. Les solutions MDM peuvent également permettre aux utilisateurs d’effectuer des tâches d’assistance comme l’installation et la mise à jour de logiciels depuis un portail de libre-service.

Conformément aux bonnes pratiques recommandées, les entreprises ne doivent pas obliger les utilisateurs à ne compter que sur eux-mêmes pour les besoins d’assistance. Adoptez plutôt une approche collaborative de la résolution de problèmes et attachez-vous à donner les moyens aux utilisateurs de se dépanner eux-mêmes avant de recourir au service d’assistance. Encouragez les utilisateurs à se sentir partie prenante du processus et incitez-les à tenter d’identifier par eux-mêmes les problèmes avant de demander de l’aide.

Le fait de partager les responsabilités en matière d’assistance permet de limiter le temps d’indisponibilité des employés et de réduire la mobilisation du personnel technique ainsi que les frais d’assistance. Pour les entreprises ayant plus de besoins, AppleCare propose toute une gamme de programmes et de services qui viennent compléter les structures d’assistance internes pour les employés et le service informatique.

### AppleCare for Enterprise

Les entreprises désirant une couverture complète peuvent opter pour AppleCare for Enterprise, qui allègera la charge de travail de leur service d’assistance interne en fournissant aux employés une assistance technique par téléphone 24 heures sur 24, 7 jours sur 7, avec un temps de réponse d’une heure maximum pour les problèmes prioritaires. Ce programme propose des scénarios d’intégration au niveau du service informatique, avec MDM et Active Directory.

### 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, iPadOS, macOS et macOS Server. Il propose différents niveaux d’assistance, allant jusqu’à une assistance 24 heures sur 24, 7 jours sur 7 et l’attribution d’un responsable de compte technique. L’AppleCare OS Support vous met directement en relation avec des techniciens pour toute question relative à des problèmes d’intégration, de migration et de fonctionnement avancé des serveurs, ce qui améliore l’efficacité de votre personnel informatique au niveau du déploiement et de la gestion des appareils, ainsi que de la résolution des problèmes.

### AppleCare Help Desk Support

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

## AppleCare et AppleCare+ pour Mac

Chaque Mac s’accompagne d’une garantie limitée d’un an et d’une assistance technique téléphonique gratuite valable pendant 90 jours à compter de la date d’achat. La couverture peut être étendue à trois ans à compter de la date d’achat de l’appareil par la souscription d’un contrat AppleCare+ ou AppleCare Protection Plan. S’ils ont des questions sur le matériel ou les logiciels Apple, les employés peuvent appeler l’Assistance Apple. Apple fournit également des options de service pratiques lorsque les appareils nécessitent une réparation. En outre, l’AppleCare+ pour Mac offre une couverture pour certains incidents ayant entraîné des dommages accidentels, chaque incident étant soumis à des frais d’intervention.

En savoir plus sur les options d’assistance AppleCare :
apple.com/fr/support/professional/

# Synthèse

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

En savoir plus sur le déploiement, la gestion et les fonctionnalités de sécurité de macOS :
support.apple.com/guide/deployment-reference-macos

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

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

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

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

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

En savoir plus sur la sécurité de la plateforme Apple :
www.apple.com/security/

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

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

Contacter les Services professionnels Apple :
consultingservices@apple.com