Guide de démarrage

Déploiement Mac

Présentation

Table des matières

Présentation
Se lancer
Étapes du déploiement
Options d'assistance
Synthèse

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 adaptés fournis par Apple et à une solution tierce de gestion des appareils mobiles (Mobile Device Management, MDM), votre entreprise peut facilement déployer des appareils macOS et en assurer la maintenance à l'échelle de toute l'entreprise. Si votre entreprise a déjà déployé en interne des appareils iOS, 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 de macOS 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 et reposant exclusivement sur des outils intégrés à macOS.

Ce document fournit des conseils sur tout ce qu'il vous faut pour déployer macOS 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 thèmes abordés dans ce document sont détaillés dans la ressource Référence pour le déploiement macOS, disponible en ligne : help.apple.com/deployment/macos

Se lancer

L'élaboration d'une stratégie de déploiement et d'un plan de mise en œuvre, mais aussi l'évaluation de toute utilisation existante de macOS par les employés, sont des étapes initiales fondamentales du processus de déploiement. Vérifiez que les équipes nécessaires sont impliquées très tôt dans le processus et qu'elles adhèrent à votre vision du programme et à vos objectifs. Certaines équipes commencent par un modeste projet pilote ou une étude de faisabilité pour mettre au jour les éventuelles difficultés propres à leur environnement. À ce stade, il est primordial de comprendre auprès des utilisateurs existants l'usage qui est fait des appareils sur le réseau et de savoir si votre équipe doit être informée de certains problèmes.

Les informations recueillies durant cette phase peuvent contribuer 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'entreprise ou comme choix offert à certaines fonctions.

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'annuaire 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 chaque possesseur d'applications à se moderniser. 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 des priorités pour tout effort de modernisation envisagé. Si nécessaire, élaborez avec les possesseurs 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 de la diversité des partenaires professionnels spécialisés dans le développement et prêts à les aider.

Les ordinateurs Mac sont généralement la propriété de l'entreprise. Certaines entreprises autorisent toutefois leurs employés à utiliser leur propre Mac dans le cadre de programmes BYOD (Bring Your Own Device, « Apportez vos appareils personnels »). Respecter le choix des employés par rapport aux produits Apple peut se révéler très bénéfique à l'ensemble de l'entreprise et se traduire par un niveau accru de productivité, de créativité et d'implication des employés, par un taux de satisfaction plus élevé et par une baisse des coûts en termes de valeurs résiduelles et d'assistance. Les entreprises 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 pendant une mise à niveau ou d'acquérir 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 que recueille votre équipe pendant un projet pilote. Les utilisateurs n'ont pas tous les mêmes besoins en termes de règles, de réglages et d'apps. Ainsi, les exigences varient souvent considérablement entre les différents groupes ou équipes d'une même entreprise.

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 n'en est pas moins essentiel d'évaluer votre infrastructure existante pour vous assurer que votre entreprise tire le meilleur parti des possibilités qu'offre macOS. Si votre entreprise 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 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 d'Apple (APNs), à iCloud ou à l'iTunes Store. Tout comme avec iOS, certains aspects du processus de déploiement de macOS, en particulier avec les Mac récents, nécessitent un accès stable à ces services.

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 High Sierra, 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 réclame 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 des réseaux Wi-Fi :
help.apple.com/deployment/macos

En savoir plus sur la configuration de votre réseau pour la MDM :
help.apple.com/deployment/macos

En savoir plus sur Bonjour :
help.apple.com/deployment/macos

Gérer les identités
Pour la gestion des identités et d'autres informations sur les utilisateurs, macOS peut accéder à des services d'annuaire, 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 Enterprise Connect (un des Services professionnels Apple) ou NoMAD d'Orchard & Grove, assurent l'intégration avec les règles et fonctionnalités Active Directory sans nécessiter une liaison traditionnelle. 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 l'intégration des annuaires : help.apple.com/deployment/macos

En savoir plus sur la gestion des certificats : help.apple.com/deployment/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 :
help.apple.com/deployment/macos

En savoir plus sur les services basés sur des normes standard :
help.apple.com/deployment/macos

Mise en cache
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 booster le téléchargement et la distribution de logiciels via le Mac App Store, l'iTunes Store et l'iBooks Store.

Vous pouvez également mettre en cache les mises à jour logicielles pour en accélérer le téléchargement sur les appareils de votre entreprise, qu'il s'agisse d'appareils macOS ou iOS.

En savoir plus sur la mise en cache : help.apple.com/deployment/macos

Mettre en place une solution de gestion

La gestion des appareils mobiles (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 solution MDM que ce service utilise aujourd'hui pour l'iPhone et l'iPad.

En coulisses, macOS et iOS 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. Comme macOS et iOS partagent un grand nombre d'environnements pour la gestion des appareils, ces solutions 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 de gestion les plus pertinentes pour votre entreprise.

Une fois que vous aurez sélectionné votre solution MDM et commencé à la configurer, 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 de la MDM : help.apple.com/deployment/macos

Visiter l'Apple Push Certificates Portal : identity.apple.com/pushcert/

S'inscrire aux services Apple

Apple propose une suite de services conçus pour simplifier votre déploiement. Si vous découvrez les services Apple, le compte créé au moment de l'inscription sera l'administrateur le plus important de ces services et disposera d'un contrôle administratif complet sur chaque service de votre entreprise. Ce même compte pourra être utilisé pour s'inscrire à d'autres services Apple.

Programme d'inscription des appareils

Le Programme d'inscription des appareils (Device Enrollment Program, DEP) d'Apple offre un moyen simple et rapide de déployer les Mac appartenant à l'entreprise, qu'ils aient été achetés directement auprès d'Apple ou auprès d'un Revendeur

Agréé Apple participant. Vous pouvez simplifier la configuration initiale des Mac en automatisant l'inscription auprès de la solution MDM, sans avoir à manipuler ou à préparer chacun des Mac avant de les remettre aux utilisateurs. Le processus de configuration peut encore être simplifié pour les utilisateurs en supprimant certaines étapes de l'Assistant réglages.

En savoir plus sur le Programme d'inscription des appareils :
www.apple.com/fr/business/dep/

Programme d'achat en volume
Le Programme d'achat en volume (VPP) d'Apple permet aux entreprises d'acheter des livres et des apps macOS en grand nombre et de les distribuer aux employés. Vous pouvez payer à l'aide d'une carte bancaire d'entreprise ou d'un crédit VPP obtenu à l'aide d'un bon de commande. Les solutions MDM s'intègrent avec le Programme d'achat en volume et peuvent être utilisées pour distribuer des apps et des livres dans tous les pays où ils sont disponibles. Grâce à la distribution gérée, les licences individuelles peuvent être révoquées et réattribuées à d'autres employés en fonction des besoins.

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

Developer Enterprise Program
L'Apple Developer Enterprise Program propose tout un ensemble d'outils pour développer, tester et distribuer des apps macOS ou iOS aux utilisateurs. Vous pouvez distribuer des apps soit en les hébergeant sur un serveur web, soit à l'aide d'une solution MDM. Les apps et programmes d'installation pour Mac peuvent être signés à l'aide de votre identifiant de développeur pour être compatibles avec Gatekeeper, fonction intégrée à macOS qui permet de protéger le Mac des 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.

macOS et iOS intègrent plusieurs niveaux de sécurité, ce qui permet aux appareils Apple d'accéder aux services réseau en toute sécurité et de protéger les données importantes. macOS et iOS 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 Apple 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 systèmes Mac. 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.

Comprendre l'intégration de la sécurité dans macOS :
www.apple.com/fr/macos/security/

En savoir plus sur les fonctionnalités de sécurité de macOS :
help.apple.com/deployment/macos

Définir les règles de l'entreprise

Initiez le développement de votre politique d'entreprise en établissant des règles générales qui couvrent la majorité des utilisateurs Mac de votre environnement. 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 réclament 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 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 macOS et iOS. 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'annuaire existants. L'Assistant réglages de macOS peut demander aux utilisateurs de se connecter à l'aide de leurs identifiants du service d'annuaire lors de l'inscription. Une fois l'appareil attribué à un utilisateur spécifique, la MDM peut personnaliser les configurations et les comptes propres à un individu ou à 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 leurs appareils iOS lorsqu'ils sont soumis à une politique de gestion.

En savoir plus sur les profils de configuration : help.apple.com/deployment/macos

Préparer l'inscription des appareils

La méthode la plus simple pour inscrire un appareil auprès de la MDM consiste à utiliser l'Assistant réglages avec le Programme d'inscription des appareils (DEP). 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 le Programme d'inscription des appareils (DEP), vous devez lier votre solution MDM à votre compte DEP via un jeton sécurisé. L'autorisation sécurisée d'une solution MDM s'effectue via un processus de validation en deux étapes. Votre

éditeur de solution MDM peut vous fournir des informations sur les caractéristiques spécifiques nécessaires 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 du Programme d'inscription des appareils (DEP), soit par le biais de l'inscription à la MDM approuvée par l'utilisateur pour gérer certains réglages sensibles de sécurité (comme les règles s'appliquant aux extensions de noyau) sous macOS High Sierra.

En savoir plus sur les extensions de noyau et la MDM approuvée par l'utilisateur : support.apple.com/HT208019

Préparer la distribution d'apps et de livres

Apple propose des programmes complets pour aider votre entreprise à tirer profit des apps et des contenus de qualité disponibles pour macOS. Ces fonctionnalités vous permettent de distribuer aux employés les apps et les livres achetés via le programme VPP ainsi que les apps développées en interne, afin que vos utilisateurs aient tous les outils à disposition pour gagner en productivité. 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 le Store VPP dans n'importe quel pays où l'app est disponible. Pour activer la distribution gérée, vous devez tout d'abord associer votre solution MDM à votre compte VPP à l'aide d'un jeton sécurisé. Une fois connecté à votre solution MDM, vous pouvez attribuer des apps et des livres achetés en volume, 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 en volume (VPP) : help.apple.com/deployment/macos

En savoir plus sur la distribution d'apps et de livres : help.apple.com/deployment/macos

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 Microsoft Office. 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 de contenus supplémentaires : help.apple.com/deployment/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 ajoutés au programme DEP peuvent être automatiquement inscrits à la MDM au cours de ce processus. Les systèmes Mac ajoutés au DEP peuvent aussi être configurés de manière à sauter certaines étapes, telles que les Conditions générales, la connexion à l'aide d'un identifiant Apple, le service de localisation, etc.

Après l'Assistant réglages, la MDM peut être utilisée pour 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. Tout comme avec les appareils iOS, 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.

En savoir plus sur la configuration de l'Assistant réglages via le programme DEP : help.apple.com/deployment/macos/

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 charges 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 réaliser au mieux leurs tâches et d'atteindre leurs objectifs.

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

Pour profiter au maximum de ces services, les utilisateurs doivent utiliser leur propre identifiant Apple. 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 possèdent pas déjà un. Aucun numéro de carte bancaire ne leur sera demandé.

En savoir plus sur les identifiants Apple : help.apple.com/deployment/macos

iCloud
Grâce à iCloud, les utilisateurs peuvent synchroniser automatiquement des contenus personnels, comme des contacts, calendriers, documents et photos, et les actualiser en permanence sur plusieurs appareils. Localiser mon iPhone 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 utilisateurs peuvent ainsi profiter de tous les avantages d'iCloud pour gérer leurs données personnelles tout en évitant que les données de l'entreprise soient stockées sur iCloud.

En savoir plus sur la gestion d'iCloud : help.apple.com/deployment/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

La solution MDM peut administrer un appareil géré grâce à 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 d'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.

Voir la liste complète des tâches de gestion : help.apple.com/deployment/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. Le service informatique peut s'impliquer dans les 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 rapidement à la mise à jour et mettez à niveau dès que vous avez déterminé que votre flux de travail est compatible avec une nouvelle version majeure de macOS.

La MDM peut « pousser » automatiquement les mises à jour de macOS sur un Mac inscrit au programme DEP. Un Mac inscrit au programme DEP 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 de déploiement la plus fiable consiste à utiliser le programme d'installation de macOS. Téléchargez le programme d'installation de macOS High Sierra et installez-le avec la fonctionnalité de récupération par Internet, un programme d'installation externe amorçable, ou avec NetInstall (qui fait partie de l'Utilitaire d'images système).

Gérer les logiciels supplémentaires

Au-delà de l'ensemble de base, les entreprises 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 le programme VPP, 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 qui nécessitent des extensions de noyau exigent désormais l'accord 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.

En savoir plus sur le chargement de l'extension de noyau approuvé par l'utilisateur : help.apple.com/deployment/macos

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 la fonctionnalité de récupération par 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. Un Mac inscrit au programme DEP pourra automatiquement se réinscrire auprès de la MDM pendant le processus effectué par l'Assistant réglages, configurer les réglages pour le nouvel utilisateur, appliquer les règles de l'entreprise et déployer tous les logiciels appropriés.

Pour les Mac qui ne sont pas inscrits au programme DEP, le même processus sera utilisé pour en effacer le contenu et les réapprovisionner, puis la réinscription se fera manuellement.

En savoir plus sur la fonctionnalité de récupération par Internet : help.apple.com/deployment/macos

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 allégera la charge de travail de leur service d’assistance interne en fournissant aux employés une assistance technique par téléphone 24 heures sur 24 et 7 jours sur 7, avec un temps de réponse d’une heure maximum pour les problèmes prioritaires. Ce programme 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, macOS et macOS Server. Il propose une assistance 24 heures sur 24 et 7 jours sur 7 et l’aide d’un responsable de compte technique, selon le niveau d’assistance souscrit. Offrant un accès direct à des techniciens pour toute question relative à l’intégration, la migration et les problèmes serveur avancés, l’AppleCare OS Support peut améliorer l’efficacité de votre personnel informatique au niveau du déploiement et de la gestion des appareils, et de la résolution des problèmes.

AppleCare Help Desk Support

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

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. Cette couverture peut être étendue à trois ans à compter de la date d’achat de l’appareil par la souscription de l’AppleCare+ ou de l’AppleCare Protection Plan. S’ils ont des questions sur le matériel ou les logiciels Apple, les employés peuvent appeler l’Assistance Apple. Apple propose 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 :
www.apple.com/fr/support/professional/

Synthèse

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

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

En savoir plus sur Apple en entreprise : www.apple.com/fr/business/

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

Découvrir la formation et la certification Apple : training.apple.com

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