Politiques - Apple

- Stratégies Apple
- Apps et profils
- Mode kiosque et écran d'accueil
- Code d'accès
- Restrictions
- Réseau
- Mises à jour logicielles
- macOS
- Localisation et géorepérage
- Comptes
- Règles de conformité

Stratégies Apple

Les stratégies Apple définissent les paramètres de gestion que Cerberus Enterprise applique aux appareils Apple via MDM. Ces paramètres sont configurés depuis le tableau de bord dans l'éditeur de stratégie Apple.

Avant de commencer

La gestion des appareils Apple nécessite que Apple Management (APNs) soit configuré. Si nécessaire, consultez la page Configuration d'Apple Management (APNs).

Ouvrir l'éditeur de stratégie Apple

Dans le tableau de bord, ouvrez **Stratégies** et cliquez sur **Créer une stratégie Apple**. Pour modifier une stratégie Apple existante, cliquez sur sa ligne dans le tableau des stratégies.

Disposition de l'éditeur

L'éditeur de stratégie Apple est organisé en un ensemble de sections dépliables. En haut de la page, vous pouvez toujours modifier :

- **Nom** (requis)
- **Id** (en lecture seule)
- **Description** (facultatif)

Sections de la stratégie

Les sections ci-dessous correspondent aux panneaux actuellement disponibles dans l'éditeur de stratégie Apple. Lorsque vous ouvrez une stratégie enregistrée, les sections dont les réglages ont été modifiés sont déjà ouvertes et les autres restent fermées :

- **Gestion des applications** : configurez les restrictions liées aux applications, les applications gérées et les paramètres de l'application Cerberus Enterprise.

- **Kiosque et écran d'accueil** : mode application unique, applications autorisées et bloquées, disposition de l'écran d'accueil, clips web, paramètres de notification et message de l'écran verrouillé.
- **Sécurité** : contrôlez des fonctionnalités comme le déverrouillage automatique et le déverrouillage biométrique.
- **Paramètres du code d'accès** : configurez les exigences de code d'accès et les règles associées.
- **Multimédia** : autorisez ou interdisez l'appareil photo et les fonctionnalités associées.
- **Cellulaire** : contrôlez les réglages liés au cellulaire (réglages de données cellulaires des applications, eSIM, changements de forfait) et l'APN cellulaire.
- **Réseau** : réseaux Wi-Fi (y compris 802.1X d'entreprise), VPN, certificats, proxy global, DNS chiffré et filtre de contenu web, ainsi que les restrictions de connectivité telles qu'AirDrop et Bluetooth.
- **Système et interface utilisateur** : limitez les fonctionnalités système telles que Handoff, le nom de l'appareil et l'économiseur d'écran.
- **Mises à jour logicielles** : exigez une version du système avant une date limite et contrôlez le téléchargement et l'installation des mises à jour.
- **macOS** : pare-feu, Gatekeeper, économiseur d'écran et verrouillage, stockage externe et réseau, partage d'écran, autorisations de confidentialité et éléments d'ouverture des Mac.
- **Applications et services Apple** : limitez les applications et services Apple tels qu'iMessage, Game Center et Localiser.
- **Siri et Apple Intelligence** : limitez Siri, la dictée et les fonctionnalités Apple Intelligence.
- **iCloud** : autorisez ou interdisez des services iCloud spécifiques (sauvegarde, synchronisation du trousseau, relais privé, etc.).
- **Localisation et géorepérage** : zones dans lesquelles les iPhone et iPad équipés de l'application Cerberus Enterprise signalent leur entrée ou leur sortie, pour les règles d'événements.
- **Comptes** : limitez la modification des comptes et configurez les comptes Mail, Exchange, Google, calendrier, contacts et annuaire.
- **Règles de conformité** : exigences (code d'accès, version minimale du système, supervision, FileVault) qui rendent les appareils non conformes, avec blocage facultatif.

> De nombreuses options de l'éditeur de stratégie Apple incluent une info-bulle qui documente les exigences et les versions du système prises en charge.

Enregistrer, supprimer et appareils associés

Utilisez **Enregistrer la stratégie** pour appliquer vos modifications. Le bouton est désactivé lorsqu'il n'y a aucune modification en attente ou lorsque la licence est expirée.

Lors de la modification d'une stratégie existante, la page affiche également une action **Supprimer la stratégie**. L'éditeur peut afficher une liste **Appareils associés** en bas, afin que vous puissiez voir combien d'appareils utilisent actuellement la stratégie.

Pages suivantes

- Applications et profils : configurez les applications installées et les profils de configuration.
- Kiosque et écran d'accueil : mode application unique, applications autorisées, disposition de l'écran d'accueil et clips web.
- Code d'accès : configurez les exigences de code d'accès et les options de sécurité associées.
- Restrictions : définissez les fonctionnalités autorisées et les limitations au niveau du système.
- Réseau : réseaux Wi-Fi, VPN, certificats et restrictions de connectivité.
- Mises à jour logicielles : mises à jour requises du système et paramètres des mises à jour logicielles.
- macOS : pare-feu, Gatekeeper, verrouillage de l'écran, stockage, autorisations de confidentialité et éléments d'ouverture des Mac.
- Localisation et géorepérage : zones dont les iPhone et iPad signalent l'entrée et la sortie, et ce dont ils ont besoin pour fonctionner.
- Comptes : comptes mail, Exchange, Google, calendrier, contacts et annuaire.
- Règles de conformité : exigences pour les appareils et blocage des appareils non conformes.

Apps et profils

Cette section explique comment configurer les applications gérées et les charges utiles de compte pour les appareils Apple.

Gestion des applications

Le panneau **Gestion des applications** contient à la fois les restrictions générales liées aux applications et une liste d'applications gérées.

Restrictions générales des applications

- **Autoriser les App Clips**
- **Autoriser l'installation d'applications**
- **Autoriser la suppression d'applications**
- **Autoriser le téléchargement automatique des applications**
- **Autoriser le masquage des applications**
- **Autoriser le verrouillage des applications**
- **Autoriser les achats intégrés**
- **Autoriser la modification du navigateur par défaut**
- **Autoriser la confiance des applications d'entreprise**

Applications gérées

Utilisez **Ajouter une application** pour ajouter une application à la stratégie. Chaque application gérée est affichée sous forme de carte. Vous pouvez développer la carte pour modifier ses paramètres et supprimer l'application à l'aide de l'action de suppression.

- **ID App Store** : l'identifiant App Store de l'application gérée.
- **ID de bundle** : l'identifiant de bundle de l'application.
- **Comportement d'installation** : contrôle si l'application doit rester installée ou si l'utilisateur peut l'installer ou la supprimer.
- **Attribution** : le type de licence, choisi par Cerberus pour chaque appareil : une licence d'appareil sur les appareils d'entreprise, une licence utilisateur du Managed Apple Account sur les iPhone et iPad personnels (inscription utilisateur). Le champ ne peut pas être modifié.
- **Licence VPP** : type de licence VPP utilisé pour l'installation via l'App Store.

La liste de sélection des applications affiche les licences disponibles et totales de chaque application. Les applications gratuites affichent **Illimité** : Apple leur accorde des licences illimitées. Une application ne peut être ajoutée qu'une seule fois à une stratégie : une application ayant le même ID App Store ou ID de bundle qu'une application déjà présente dans la stratégie est refusée, tout comme une stratégie qui répertorie deux fois la même application lors de l'enregistrement.

La liste de sélection des applications affiche les applications de votre bibliothèque Apple Business. Pour ajouter une application, ouvrez dans Apple Business **Apps & Services → Apps & Books → App Store**, recherchez l'application et cliquez sur **View**. Pour une application gratuite, cliquez sur **Add**, sélectionnez **All current and future** (ou l'unité organisationnelle de votre jeton Apps and Books) dans **Organizational Units**, cliquez sur **Add**, puis sur **Review** et confirmez. Pour une application payante, cliquez sur son prix, choisissez **Managed Licenses** comme **License Type** (les codes d'échange ne peuvent pas être utilisés par Cerberus Enterprise), sélectionnez l' **Organizational Unit** de votre jeton Apps and Books, saisissez le nombre de **Licenses** (jusqu'à 1 000 par commande), puis **Review** et achetez. Un moyen de paiement doit d'abord être configuré dans **Settings → Payments & Billing → Apps & Services → Payment Methods**. Les applications apparaissent ensuite dans la liste de sélection des applications.

Applications sur les appareils personnels (inscription utilisateur)

Les iPhone et iPad personnels inscrits avec l'inscription utilisateur n'ont pas de numéro de série ; ils reçoivent donc les applications App Store de la stratégie avec une **licence utilisateur** du Managed Apple Account connecté sur l'appareil. Cerberus enregistre le compte auprès d'Apps and Books et attribue les licences automatiquement, applications gratuites comprises. Les Managed Apple Accounts et le jeton Apps and Books doivent appartenir à la même organisation Apple Business. Une application payante utilise une licence par compte, partagée par tous les appareils personnels de ce compte.

- **En attente d'une licence utilisateur** : l'application n'est envoyée à l'appareil qu'après confirmation de sa licence par Apple, généralement en quelques minutes. Le panneau **Applications** de l'appareil indique la raison.
- **Échec de la licence utilisateur** : Apple n'a pas pu attribuer la licence, par exemple parce qu'une application payante n'a plus de licence disponible. Ajoutez des licences dans Apple Business, puis utilisez **Demander à nouveau** ; Cerberus réessaie également automatiquement chaque jour.
- **Invite d'installation** : iOS demande l'accord de l'utilisateur avant d'installer chaque application. Si l'utilisateur annule, l'application affiche **En attente de l'approbation de l'installation par l'utilisateur** ; **Demander à nouveau** affiche à nouveau l'invite.
- **Libération** : retirer l'application de la stratégie, ou désinscrire le dernier appareil personnel du compte, supprime l'application et libère sa licence, sauf si un autre appareil inscrit du même compte en a encore besoin.

Pour plus de détails, consultez **Inscription pilotée par le compte Apple**.

Configuration gérée

Une configuration gérée fournit à une application ses paramètres (par exemple une adresse de serveur ou un nom de compte), de la manière documentée par le fournisseur de l'application. Ouvrez l'application dans la stratégie et cliquez sur **Ajouter une configuration gérée**. Elle est envoyée aux iPhone et iPad sous **iOS ou iPadOS 18.4 ou version ultérieure** et aux Mac sous **macOS 27 ou version ultérieure** ; elle n'est pas encore envoyée à Apple Vision Pro. L'application doit prendre en charge la configuration gérée : une application qui ne la lit pas l'ignore. Le panneau de l'application affiche le nombre de clés à côté du nom de l'application.

- **Clés** : chaque ligne comporte une clé, un type et une valeur. Les types sont Texte, Entier, Nombre décimal, Booléen, Date, Liste de textes et Liste d'entiers. Les clés sont sensibles à la casse et doivent être uniques. **Ajouter une clé** ajoute une ligne ; **Supprimer la configuration** supprime toutes les clés.
- **Variables** : les valeurs Texte et Liste de textes peuvent contenir $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ et $UDID$, remplacées par les valeurs de chaque appareil et de son utilisateur. Une variable sans valeur (par exemple $EMAIL$ sur un appareil sans utilisateur) reste vide, et les journaux système l'indiquent. Lorsque les informations d'un utilisateur changent, les appareils reçoivent les nouvelles valeurs ; pour les utilisateurs synchronisés depuis Google Directory, les valeurs sont mises à jour lors de la prochaine modification de la stratégie ou de l'appareil.
- **Importer une configuration** : ouvrez ou collez le fichier que le fournisseur de l'application publie pour MDM, puis cliquez sur **Lire**. Un **specfile AppConfig** (specfile.xml) répertorie chaque clé prise en charge par l'application avec sa description, son type, sa valeur par défaut et ses valeurs autorisées : sélectionnez les clés à importer (celles ayant une valeur par défaut sont déjà sélectionnées) et renseignez les autres après l'import. Un avertissement apparaît lorsque le specfile concerne une autre application. Une **liste de propriétés** (une liste de propriétés complète ou seulement son <dict>) est importée telle quelle. Choisissez ensuite de remplacer les clés actuelles ou de les compléter. Les dictionnaires imbriqués, les valeurs de données et les listes contenant des types mixtes ou inconnus ne sont pas pris en charge et sont indiqués comme ignorés. Apple ne publie pas les clés de configuration des applications ; demandez donc le fichier au fournisseur lorsqu'il ne figure pas dans sa documentation. **Copier au format plist** copie la configuration telle que l'appareil la reçoit, avant le remplacement des variables.
- **Limites** : jusqu'à 200 clés par application ; clés jusqu'à 255 caractères ; valeurs de texte jusqu'à 4 096 caractères ; listes jusqu'à 200 éléments de 1 024 caractères chacun ; dates entre 1970 et 9999 ; 64 Ko par application au total.
- **Pas pour les mots de passe** : la configuration est envoyée uniquement à l'appareil pour lequel elle est conçue et les journaux n'affichent que les noms et types des clés, mais les administrateurs du tableau de bord peuvent lire les valeurs, et l'adresse depuis laquelle l'appareil la télécharge change selon les valeurs : une valeur facile à deviner (un booléen ou un petit nombre) pourrait donc en être déduite. Ne placez pas de mots de passe ni

d'autres secrets dans une configuration gérée.
- **État** : lorsque l'appareil signale que l'application n'a pas accepté sa configuration, le panneau Applications de l'appareil affiche **Configuration non acceptée** à côté de l'application. Cela ne rend pas l'appareil non conforme. Une configuration que l'appareil ne peut pas télécharger le rend en revanche non conforme.

Options des applications

Chaque application de la stratégie (App Store et applications personnalisées) dispose de ces options. **Valeur par défaut de l'appareil** laisse le choix à l'appareil. Les appareils qui ne prennent pas en charge une option ne la reçoivent pas ; l'application est tout de même installée.

- **Mises à jour automatiques** : réglage App Store, Toujours ou Jamais. iOS, iPadOS, macOS et visionOS 26 ou version ultérieure. Pour les applications personnalisées, le réglage App Store se comporte comme Jamais.
- **Téléchargements via le réseau cellulaire** : réglage App Store, Toujours ou Jamais, pour les installations et mises à jour automatiques. Uniquement sur les iPhone et iPad supervisés sous iOS ou iPadOS 26 ou version ultérieure.
- **Sauvegarder les données de l'application** : indique si les données de l'application sont incluses dans les sauvegardes de l'appareil. Non disponible sur Mac.
- **L'utilisateur peut masquer l'application** et **L'utilisateur peut verrouiller l'application** : iOS et iPadOS 18.1 ou version ultérieure, appliqué sur les appareils supervisés. Refuser le verrouillage empêche aussi le masquage. Les restrictions **Autoriser le masquage des applications** et **Autoriser le verrouillage des applications** s'appliquent à toutes les applications.
- **Verrouiller l'appareil après les transactions Tap to Pay nécessitant le code PIN du client** : iPhone uniquement.
- **Domaines associés** : les domaines auxquels l'application est associée (par exemple pour les liens universels ou le remplissage automatique des mots de passe), jusqu'à 50. Saisissez des noms d'hôte simples tels que www.example.com, sans applinks:, caractères génériques ni ?mode=. Non disponible sur Mac.
- **Vérifier les domaines directement** : l'appareil vérifie directement le fichier d'association de site des domaines au lieu de passer par les serveurs d'Apple. Activez cette option uniquement pour les domaines internes qui ne sont pas accessibles depuis Internet.
- **Suppression** : les applications installées comme **Obligatoires** ne peuvent pas être supprimées par l'utilisateur.

Applications du Mac App Store

La liste de sélection des applications affiche les plateformes de chaque application (iPhone/iPad, Mac, Apple TV, Vision) ; une application qui n'existe que pour Mac affiche son icône Mac. Une application qui n'existe que pour Mac s'applique aux Mac lorsque vous l'ajoutez. Une application

App Store sans version Mac n'est pas envoyée aux Mac : la stratégie affiche « Cette application n'a pas de version Mac : elle n'est pas envoyée aux Mac » sous **S'applique à**. Les Mac reçoivent les applications App Store par leur ID App Store, de sorte que les applications ayant un ID de bundle différent sur Mac sont installées correctement.

Application Cerberus Enterprise

Cerberus installe son application **Cerberus Enterprise** sur chaque iPhone et iPad sous **iOS ou iPadOS 18.4 ou version ultérieure**, avec ou sans stratégie. L'application partage la position de l'appareil et reçoit les notifications et les demandes de suivi en direct. Elle est installée comme **Obligatoire**, avec une licence d'appareil issue d'Apps and Books (une licence utilisateur sur les appareils personnels), de sorte que l'utilisateur ne peut pas la supprimer.

- **Configuration unique** : ajoutez l'application gratuite à votre bibliothèque une seule fois. Dans Apple Business, ouvrez **Apps & Services → Apps & Books → App Store**, recherchez « Cerberus Enterprise », cliquez sur **View**, puis sur **Add**, sélectionnez **All current and future** dans **Organizational Units**, cliquez sur **Add**, puis sur **Review** et confirmez. Si l'application affiche **Manage**, elle est déjà dans votre bibliothèque : ouvrez-la et vérifiez que ses unités organisationnelles sont **All current and future units**. D'ici là, le tableau de bord affiche une bannière et les appareils indiquent l'application comme non installée. Voir **Account settings**.
- **Non disponible dans les stratégies** : l'application ne peut pas être ajoutée à une stratégie. Elle est désactivée dans la liste de sélection des applications et refusée en tant qu'application personnalisée (même ID de bundle). Une stratégie qui la répertorie déjà voit son entrée supprimée à l'ouverture : enregistrez la stratégie pour confirmer.
- **Non installée sur** : les appareils sous iOS ou iPadOS antérieur à 18.4. L'iPad partagé est pris en charge pour l'installation, mais les fonctionnalités de l'application n'y sont pas vérifiées.
- **Appareils personnels** : sur les iPhone et iPad inscrits avec l'Inscription utilisateur, l'application est également installée, avec une invite d'installation et une licence utilisateur du Managed Apple Account. Elle reçoit les messages de votre organisation et n'accède pas à la position, sauf si la stratégie active **Localisation et géorepérage sur les appareils personnels** et que l'utilisateur l'autorise.
- **Maintenue installée** : si le jeton Apps and Books expire ou si l'application quitte votre bibliothèque, elle reste sur les appareils et la page de l'appareil indique que Apps and Books nécessite votre attention. Elle n'est supprimée que si l'application est toujours absente de votre bibliothèque 24 heures plus tard.

Applications personnalisées

Les applications personnalisées sont vos propres applications iPhone et iPad (fichiers .ipa), distribuées sans l'App Store. Dans Xcode, exportez l'application pour une distribution **Enterprise** (Apple Developer Enterprise Program : elle s'installe sur tous les appareils) ou **Ad Hoc** (elle

s'installe uniquement sur les appareils enregistrés dans son profil de provisionnement). Les versions App Store ne peuvent pas être importées.

Cliquez sur **Ajouter une application personnalisée** pour ouvrir les applications personnalisées de votre organisation. **Importer une application** ajoute un fichier .ipa (jusqu'à 2 Go). Sélectionnez une application et cliquez sur **Ajouter à la stratégie**. La liste affiche la version, le type de signature, le nombre d'appareils dans le profil des applications ad hoc et la date d'expiration du profil de provisionnement.

- **Nouvelle version** : importez une application ayant le même ID de bundle. Elle remplace la version précédente et les appareils des stratégies qui l'utilisent mettent à jour l'application.
- **Prérequis** : iPhone et iPad sous iOS 17.2 ou version ultérieure. Les appareils qui ne peuvent pas installer l'application ne la reçoivent pas : une application réservée à l'iPad sur un iPhone, un iOS plus ancien que celui requis par l'application, un appareil absent du profil d'une application ad hoc ou un profil de provisionnement expiré.
- **Expiration** : lorsque le profil de provisionnement expire, l'application ne s'ouvre plus. Importez une version signée avec un nouveau profil avant la date d'expiration.
- **ID de bundle réservé** : une application personnalisée ayant l'ID de bundle de l'application Cerberus Enterprise (com.lsdroid.Cerberus.Enterprise) ne peut pas être ajoutée à une stratégie, car Cerberus installe cette application automatiquement.
- **Supprimer** : retirez d'abord l'application de ses stratégies ; les appareils la retirent ensuite.

Paquets Mac

Les applications personnalisées acceptent aussi les paquets d'installation Mac (fichiers .pkg). Le paquet doit être un paquet de distribution construit avec **productbuild** (un paquet de composants créé uniquement avec pkgbuild est refusé) et signé avec un certificat **Developer ID Installer**. Il est recommandé de le notariser et d'agrafer le ticket (**notarytool** et **stapler**). Les paquets non signés, les paquets modifiés après signature et les paquets signés avec d'autres certificats sont refusés.

Téléversez le fichier .pkg avec **Téléverser l'app** et ajoutez-le à la stratégie : il apparaît sous **Paquets Mac**. Les iPhone et iPad l'ignorent.

Les Mac avec **macOS 26 ou ultérieur** (supervisés, ce qui inclut les Mac inscrits manuellement, mais pas l'inscription utilisateur) reçoivent le paquet sous forme de **déclaration** : le Mac le télécharge, l'installe, réessaie et le met à jour de lui-même et signale son état. Les Mac plus anciens, et les paquets installés comme applications gérées, le reçoivent avec une **commande MDM**, sur toute version de macOS. Un Mac mis à niveau vers macOS 26 passe de lui-même à la déclaration ; il peut installer chaque paquet une fois de plus. Il peut en aller de même lorsqu'un Mac passe à une autre stratégie contenant le même paquet.

- **Nouvelle version** : téléversez un paquet avec le même identifiant de paquet. Il remplace la version précédente, et les Mac des stratégies qui l'utilisent installent la nouvelle.
- **Mac ignorés** : les Mac dont macOS est plus ancien que ce que le paquet permet, et les Mac Intel pour les paquets conçus uniquement pour Apple silicon. La page de l'appareil affiche le paquet comme Ignoré, avec la raison ; la version installée auparavant reste sur le Mac.
- **Installer** : **Obligatoire** (par défaut) installe le paquet sur le Mac ; **Facultatif** rend le paquet disponible sur le Mac sans l'installer. macOS 26 n'affiche pas les paquets facultatifs à l'utilisateur dans Réglages Système ni dans l'App Store (testé sur macOS 26.3), donc une app ou un script sur le Mac doit les installer ; ne choisissez Facultatif que si vous en avez un. Cela s'applique aux Mac avec macOS 26 ou ultérieur ; les Mac plus anciens installent toujours le paquet. Le choix n'est pas disponible pour les paquets installés comme applications gérées.
- **Supprimer les fichiers du paquet lorsqu'il quitte la stratégie (macOS 27 ou ultérieur)** : lorsque le paquet est retiré de la stratégie, les Mac avec macOS 27 ou ultérieur suppriment les fichiers qu'il a installés. Cette option est désactivée par défaut. Sur les Mac plus anciens, les fichiers restent. Non disponible pour les paquets installés comme applications gérées.
- **Installer comme application gérée** : activez cette option pour qu'un paquet de la stratégie installe son app comme application gérée (macOS 11 ou ultérieur, pas avec l'inscription utilisateur). macOS signale alors l'échec de l'installation, et le MDM peut supprimer l'app. L'app doit être installée directement dans le dossier Applications, signée avec un certificat **Developer ID Application** et notarisée ; sur macOS 11 à 13, le paquet ne doit contenir que cette app (aucun autre fichier ni script). Les applications personnalisées indiquent quels paquets sont admissibles. Lorsque l'option ne peut pas être appliquée sur un Mac, le paquet y est installé comme d'habitude et la page de l'appareil en explique la raison.
- **Options de suppression** d'une application gérée : **Supprimer l'app lorsque le paquet est retiré de la stratégie** (activé par défaut) et **Supprimer l'app lorsque le Mac quitte la gestion**. La suppression d'une app supprime aussi ses données. Si l'utilisateur avait déjà installé la même app, cette copie devient gérée et est également supprimée.
- **Suppression** : la commande MDM ne peut pas désinstaller un paquet. Pour un paquet installé comme application gérée, le retirer de la stratégie supprime l'app (lorsque l'option est activée) ; ses autres fichiers et le reçu du paquet restent. Les paquets dont l'option **Supprimer les fichiers du paquet** est activée sont supprimés des Mac avec macOS 27 ou ultérieur. Autres paquets : les retirer de la stratégie ne fait qu'arrêter les nouvelles installations, les fichiers restent sur les Mac. Un Mac ignoré (par exemple après une nouvelle version nécessitant un macOS plus récent) conserve l'app tant que le paquet est dans la stratégie ; le retrait du paquet de la stratégie le supprime alors aussi. Supprimez les fichiers restants sur le Mac (par exemple avec le désinstalleur du paquet) et exécutez `sudo pkgutil --forget <identifier>` pour oublier le reçu du paquet.
- **État sur l'appareil** : le panneau Applications du Mac affiche chaque paquet de la stratégie comme En file d'attente, Accepté (le Mac a accepté la commande), Téléchargé, Installé (uniquement pour les paquets contenant des apps, lorsque les apps sont trouvées

sur le Mac) ou Échec (avec l'erreur). macOS ne signale pas l'installation d'un paquet envoyé avec la commande, donc Téléchargé est le dernier état pour les paquets sans app. Un paquet installé comme application gérée passe aussi à Échec lorsque macOS signale que l'app n'a pas pu être installée ou a été supprimée du Mac. **Réinstaller** renvoie le paquet au Mac.
- **État avec la déclaration** : les paquets livrés sous forme de déclaration affichent la puce **Déclaration** et l'état signalé par le Mac : En file d'attente, Disponible (un paquet facultatif que l'utilisateur n'a pas installé), En attente de l'utilisateur, Téléchargement, Installation, Installé ou Échec (avec la raison, par exemple un téléchargement ou une installation échoués, ou une déclaration rejetée par le Mac). La puce **Fichiers supprimés avec la stratégie** signale les paquets dont les fichiers sont supprimés par un Mac sous macOS 27 lorsqu'ils quittent la stratégie. **Réinstaller** n'apparaît qu'après un échec et demande au Mac de réessayer ; elle n'est pas proposée lorsque le Mac a rejeté la déclaration.

Comptes

Le panneau **Comptes** vous permet de configurer les comptes appliqués aux appareils gérés. Il comprend également une option de restriction pour la modification des comptes.

Restriction

- **Autoriser la modification des comptes** : lorsqu'elle est désactivée, les utilisateurs ne peuvent pas modifier les comptes tels que les comptes Apple et les comptes Internet.

Ajouter des comptes

Utilisez **Ajouter un compte Google** ou **Ajouter un compte de messagerie** pour ajouter des charges utiles de compte à la stratégie. Chaque compte apparaît sous forme de carte avec ses champs de configuration.

Identifiants de compte fournis par les utilisateurs

Les cartes de compte Google et de compte de messagerie proposent toutes deux une option **Identifiants de compte fournis par les utilisateurs**. Lorsqu'elle est activée, le système applique les identifiants de compte pour chaque utilisateur. Lorsqu'elle est désactivée, vous saisissez l'identité du compte dans la stratégie.

Champs du compte Google

- **Nom visible** : le nom présenté à l'utilisateur pour le compte.
- **Adresse e-mail Google** : l'adresse e-mail de l'utilisateur.
- **Nom complet** : le nom complet de l'utilisateur.

Champs du compte de messagerie

Les comptes de messagerie comprennent des champs d'identité ainsi que la configuration des serveurs entrants et sortants. Les noms d'hôte sont obligatoires.

- **Nom visible** : le nom présenté à l'utilisateur pour le compte de messagerie.
- **Adresse e-mail** : l'adresse e-mail de l'utilisateur.
- **Nom complet** : le nom complet de l'utilisateur.

Serveur entrant

- **Type de serveur** : protocole de messagerie (par exemple IMAP ou POP).
- **Méthode d'authentification** : méthode d'authentification du serveur.
- **Préfixe de chemin IMAP** : affiché uniquement lorsque le type de serveur est IMAP.
- **Nom d'hôte** : obligatoire.
- **Port** : port du serveur (1–65535).

Serveur sortant

- **Méthode d'authentification**
- **Nom d'hôte** : obligatoire.
- **Port** : port du serveur (1–65535).

Options S/MIME

Pour les comptes de messagerie, vous pouvez également configurer le comportement de chiffrement et de signature S/MIME.

Chiffrement

- **Chiffrement S/MIME**
- **Identité modifiable par l'utilisateur**
- **Choix par message activé**
- **Modifiable par l'utilisateur**

Signature

- **Signature S/MIME**
- **Identité modifiable par l'utilisateur**
- **Modifiable par l'utilisateur**

> Les options de compte et de restriction comprennent dans le tableau de bord des infobulles documentant les prérequis et les versions de système d'exploitation prises en charge.

Mode kiosque et écran d'accueil

La section **Mode kiosque et écran d'accueil** de l'éditeur de stratégie Apple verrouille les appareils sur une seule app, choisit les apps qui peuvent être ouvertes, organise l'écran d'accueil et ajoute des icônes de site web. Chaque paramètre est installé sur les appareils sous forme de profil de configuration.

> Apple applique la plupart de ces réglages uniquement aux iPhone et iPad supervisés (appareils inscrits avec l'inscription automatique des appareils ou préparés avec Apple Configurator). Les autres appareils ne les reçoivent pas. Les clips web fonctionnent aussi sur les iPhone et iPad non supervisés. Les Mac ne reçoivent aucun de ces réglages.

Choix des apps

Les apps sont identifiées par leur identifiant de bundle. Saisissez le nom d'une app pour la choisir parmi les apps Apple intégrées et les apps de la stratégie, ou saisissez un identifiant de bundle quelconque, par exemple `com.example.app`.

Mode app unique

L'appareil exécute uniquement l'app choisie : les utilisateurs ne peuvent pas revenir à l'écran d'accueil ni ouvrir d'autres apps. Installez d'abord l'app avec la stratégie. L'appareil quitte le mode app unique lorsque vous désactivez le paramètre ou retirez l'app.

- **Options** : désactivez l'écran tactile, la rotation, les boutons de volume, le commutateur Sonnerie/Silencieux, le bouton latéral ou le verrouillage automatique, et activez des fonctions d'accessibilité telles que VoiceOver ou Zoom.
- **Fonctions d'accessibilité que l'utilisateur peut activer** : fonctions que l'utilisateur peut activer en appuyant trois fois sur le bouton latéral.

Apps autorisées et bloquées

- **Applications bloquées** : les appareils masquent ces applications et ne les ouvrent pas. `com.apple.webapp` bloque tous les clips web. Réglages et, sur iPhone, Téléphone ne peuvent pas être bloqués.
- **Autoriser uniquement certaines apps** : les appareils affichent uniquement ces apps. Laissez la liste vide pour autoriser toutes les apps. **Apps de la stratégie** ajoute les apps installées par la stratégie ; `com.apple.webapp` autorise tous les clips web.
- **Apps pouvant démarrer le mode app unique** : apps qui peuvent verrouiller l'appareil sur elles-mêmes pendant qu'elles en ont besoin, par exemple pendant un examen.

> Avec **Autoriser uniquement certaines apps**, chaque application absente de la liste disparaît des appareils, y compris les applications de la stratégie. Réglages et, sur iPhone, Téléphone restent toujours.

Disposition de l'écran d'accueil

Organisez le Dock et les pages de l'écran d'accueil. Ajoutez des apps, des dossiers d'apps et les clips web de la stratégie, en choisissant l'emplacement avec **Ajouter à**, puis faites glisser les icônes pour les déplacer entre le Dock et les pages. Cliquez sur un dossier pour modifier son nom et ses apps.

Les utilisateurs ne peuvent pas déplacer les icônes ni supprimer des applications de l'écran d'accueil. Les applications absentes de la disposition vont sur les pages suivant celles que vous avez définies. Un iPhone affiche quatre icônes dans le Dock. Les utilisateurs peuvent toujours supprimer les applications qui ne sont pas Obligatoires dans l'écran de stockage des Réglages. Pour l'empêcher, désactivez **Autoriser la suppression d'applications** dans Gestion des applications.

Clips web

Un clip web est une icône sur l'écran d'accueil qui ouvre un site web. Définissez le libellé et l'URL, et éventuellement une image (PNG ou JPEG, recadrée en carré).

- **Les utilisateurs peuvent le supprimer** : désactivez cette option pour conserver l'icône sur les appareils.
- **Plein écran** : le site web s'ouvre comme une app web, sans la barre d'adresse de Safari. **Rester en plein écran sur les autres sites web** ouvre également les liens vers d'autres sites web dans l'app web.
- **Ouvrir avec cette app** : une app qui ouvre l'URL à la place de Safari.

Paramètres de notification

Choisissez comment les appareils affichent les notifications de certaines apps : si elles sont autorisées, où elles apparaissent (écran verrouillé, centre de notifications, CarPlay), les badges, les sons, les alertes critiques, le style de bannière, le regroupement et les aperçus. Les utilisateurs ne peuvent pas modifier ces paramètres.

Message de l'écran verrouillé

Un message affiché en bas de l'écran verrouillé, par exemple qui appeler si l'appareil est retrouvé, et une étiquette d'inventaire. Les deux peuvent contenir les variables $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ et $UDID$: une variable sans valeur pour l'appareil reste vide.

Code d'accès

La section **Réglages du code d'accès** contrôle les exigences de code d'accès de l'appareil et les règles de sécurité associées (par exemple, la longueur minimale et la complexité). Sur un Mac (macOS 13 ou version ultérieure, pas avec l'inscription utilisateur), les règles s'appliquent au mot de passe de connexion des utilisateurs.

Options

Dans l'éditeur de stratégie Apple, les options de code d'accès sont configurées à l'aide d'un mélange de commutateurs et de champs numériques. De nombreux champs comportent des infobulles qui indiquent les versions de système d'exploitation prises en charge et les exigences de supervision.

Commutateurs de code d'accès

- **Modifier à la prochaine authentification** : impose une réinitialisation du code d'accès la prochaine fois que l'utilisateur s'authentifie.
- **Exiger un code d'accès alphanumérique** : exige au moins un caractère alphabétique et un chiffre.
- **Exiger un code d'accès complexe** : exige un code d'accès « complexe » (sans motifs répétitifs ou séquentiels et avec au moins un caractère non alphanumérique).
- **Exiger un code d'accès** : exige un code d'accès sans exigences supplémentaires de longueur ou de qualité. Remarque : la définition d'autres clés de code d'accès impose implicitement un code d'accès.

Champs numériques

- **Réinitialisation des tentatives échouées (minutes)** : nombre de minutes avant la réinitialisation du compteur de tentatives échouées (nécessite Nombre maximal de tentatives échouées).
- **Nombre maximal de tentatives échouées** : tentatives échouées autorisées avant l'effacement d'un iPhone ou d'un iPad, ou le verrouillage d'un Mac (plage : 2–11).
- **Délai de grâce maximal (minutes)** : durée pendant laquelle l'appareil peut rester déverrouillé sans demander le code d'accès (0 = aucun).
- **Inactivité maximale (minutes)** : temps d'inactivité avant le verrouillage de l'appareil (plage : 0–15).

- **Âge maximal du code d'accès (jours)** : âge maximal du code d'accès avant un changement forcé (plage : 0–730).
- **Nombre minimal de caractères complexes** : nombre minimal de caractères « complexes » (plage : 0–4).
- **Longueur minimale** : longueur minimale du code d'accès (plage : 0–16).
- **Limite de réutilisation du code d'accès** : nombre de codes d'accès précédents conservés pour empêcher la réutilisation d'anciens codes (plage : 1–50).

Restrictions

Les sections Restrictions contrôlent les fonctionnalités du système d'exploitation autorisées sur les appareils Apple gérés. Dans l'éditeur de stratégie Apple, ces options sont présentées sous forme de panneaux groupés avec plusieurs commutateurs.

Les options des panneaux **Gestion des apps** et **Réseau** sont décrites dans les pages Apps et profils et Réseau des stratégies Apple.

> De nombreuses restrictions ne sont prises en charge que sur certaines versions du système d'exploitation et peuvent nécessiter des appareils supervisés. Utilisez les infobulles du tableau de bord pour connaître les exigences faisant foi.

> Sur les appareils en inscription utilisateur (appareils personnels inscrits en se connectant avec un compte professionnel), les restrictions qu'Apple n'autorise pas dans ce cas ne sont pas envoyées. Si aucune des restrictions de la stratégie ne s'applique, ces appareils ne reçoivent aucun profil de restrictions. L'éditeur de stratégie indique combien de restrictions ne s'appliquent pas aux appareils en inscription utilisateur.

Sécurité

- **Autoriser le déverrouillage automatique**
- **Autoriser l'empreinte digitale pour le déverrouillage**
- **Autoriser la modification de l'empreinte digitale**
- **Autoriser l'effacement du contenu et des réglages**
- **Autoriser l'activation des restrictions**
- **Autoriser l'installation de profils par les utilisateurs**
- **Autoriser l'appairage avec un hôte**
- **Autoriser l'envoi de diagnostics**
- **Autoriser la modification de l'envoi de diagnostics**
- **Autoriser la publicité personnalisée Apple**
- **Autoriser la modification de la gestion à distance**

Multimédia

- **Autoriser l'appareil photo**
- **Autoriser la modification du partage de fichiers**
- **Autoriser l'accès aux lecteurs USB dans Fichiers**
- **Autoriser l'enregistrement des appels**
- **Autoriser AirPrint**
- **Autoriser le stockage des identifiants AirPrint**
- **Autoriser la découverte iBeacon pour AirPrint**

Cellulaire

- **Autoriser la modification des données cellulaires des applications**
- **Autoriser la modification du forfait cellulaire**
- **Autoriser la modification de l'eSIM**
- **Autoriser les transferts sortants d'eSIM**
- **Conserver l'eSIM lorsque l'appareil est effacé**
- **Autoriser l'actualisation en arrière-plan en itinérance**

APN cellulaire

APN cellulaire définit le nom du point d'accès (APN) fourni par votre opérateur, par exemple pour un réseau mobile privé ou professionnel. Définissez le **nom du point d'accès** et, si l'opérateur les demande, l'authentification (PAP ou CHAP), le nom d'utilisateur (les variables comme $EMAIL$ sont autorisées), le mot de passe, les versions IP (aussi en itinérance), un serveur proxy avec son port et XLAT464. Activez **Joindre l'APN** uniquement si l'opérateur vous fournit un APN distinct pour la connexion au réseau.

- Seuls les iPhone et les iPad cellulaires le reçoivent, même sans supervision. Les appareils inscrits avec l'inscription utilisateur (appareils personnels) ne le reçoivent pas.
- Il s'applique uniquement à la SIM utilisée pour les données cellulaires. Un appareil qui possède déjà un profil APN installé d'une autre manière ne l'installe pas.
- Le mot de passe est protégé comme les autres mots de passe réseau : le profil est envoyé uniquement à l'appareil pour lequel il a été créé et le mot de passe n'est pas écrit dans les journaux.

> Un APN incorrect laisse les appareils sans données cellulaires : essayez d'abord les paramètres sur un appareil de test avec une SIM de l'opérateur.

Système et interface utilisateur

- **Autoriser Handoff**
- **Autoriser la correction automatique**
- **Autoriser l'assombrissement automatique de l'écran**
- **Autoriser l'économiseur d'écran automatique**
- **Autoriser le clavier QuickPath**
- **Autoriser la recherche de définitions**
- **Autoriser la modification du nom de l'appareil**
- **Autoriser la mise en veille de l'appareil**
- **Autoriser la mise en miroir de l'iPhone**
- **Autoriser les widgets iPhone sur Mac**
- **Autoriser les raccourcis clavier**

Applications et services Apple

- **Autoriser iMessage**
- **Autoriser Game Center**
- **Autoriser l'ajout d'amis Game Center**
- **Autoriser Localiser mon appareil**
- **Autoriser Localiser mes amis**
- **Autoriser la modification de Localiser mes amis**
- **Autoriser la Librairie**
- **Autoriser les contenus érotiques de la Librairie**
- **Autoriser la sauvegarde des livres d'entreprise**
- **Autoriser la synchronisation des métadonnées des livres d'entreprise**
- **Autoriser l'iTunes Store**
- **Autoriser le contenu explicite**

Siri et Apple Intelligence

- **Autoriser Siri**
- **Autoriser le contenu généré par les utilisateurs pour Siri**
- **Autoriser Siri lorsque l'appareil est verrouillé**
- **Autoriser la dictée**
- **Autoriser les intégrations d'intelligence externe**
- **Autoriser la connexion à une intelligence externe**
- **Autoriser Genmoji**
- **Autoriser Image Playground**
- **Autoriser Image Wand**

iCloud

- **Autoriser le carnet d'adresses iCloud**
- **Autoriser la sauvegarde iCloud**
- **Autoriser les signets iCloud**
- **Autoriser le calendrier iCloud**
- **Autoriser le bureau et les documents iCloud**
- **Autoriser la synchronisation des documents iCloud**
- **Autoriser iCloud Freeform**
- **Autoriser la synchronisation du trousseau iCloud**
- **Autoriser iCloud Mail**
- **Autoriser Notes iCloud**
- **Autoriser la photothèque iCloud**
- **Autoriser le relais privé iCloud**
- **Autoriser Rappels iCloud**

Comptes (restriction)

Le panneau Comptes contient à la fois une restriction et (facultativement) une configuration de comptes. L'option de restriction contrôle si l'utilisateur peut modifier les comptes système.

- **Autoriser la modification des comptes**

Réseau

La section **Réseau** de l'éditeur de stratégie Apple configure les réseaux Wi-Fi et les VPN sur les appareils, installe des certificats et restreint les fonctions de connectivité comme AirDrop et Bluetooth. Chaque réseau Wi-Fi, VPN et certificat est installé sous forme de profil de configuration distinct, que vous pouvez voir sur l'appareil dans **Réglages > Général > VPN et gestion de l'appareil** (Mac : **Réglages Système > Général > Gestion de l'appareil**, ou **Confidentialité et sécurité > Profils** sur macOS 13 et 14) et dans le panneau **Profils, certificats et sécurité** de la page de l'appareil.

> Les certificats proviennent de la page **Certificats** : importez-les d'abord à cet endroit. La stratégie ne fait que les référencer, ainsi un certificat n'est jamais copié dans la stratégie.

Restrictions

- **Autoriser AirDrop**
- **Autoriser les demandes AirPlay entrantes**
- **Autoriser la modification de Bluetooth**
- **Autoriser la modification du partage Bluetooth**
- **Autoriser l'accès aux lecteurs réseau dans Fichiers**
- **Autoriser la modification du partage Internet**
- **Autoriser la mise en cache du contenu**
- **Autoriser le partage de fichiers iTunes**

Réseaux Wi-Fi

Cliquez sur **Ajouter un réseau Wi-Fi** et renseignez :

- **Nom du réseau (SSID)** : le nom du réseau, jusqu'à 32 caractères.
- **Sécurité** : aucune (réseau ouvert), WEP, WPA ou WPA2, WPA2 ou WPA3, WPA3 uniquement, ou indifférent.
- **Mot de passe** : le mot de passe d'un réseau personnel.
- **Rejoindre automatiquement** et **Réseau masqué** (pour les réseaux qui ne diffusent pas leur nom).
- **Proxy** : aucun, manuel (serveur et port) ou automatique (une URL de fichier PAC, ou vide pour trouver les réglages sur le réseau avec WPAD).

- **Nom du profil** (facultatif) et **S'applique à**, pour limiter le réseau à certains types d'appareils.

Réseaux d'entreprise (802.1X)

Activez **Entreprise (802.1X)** lorsque les utilisateurs s'authentifient avec leurs propres identifiants ou un certificat au lieu d'un mot de passe partagé.

- **Authentification** : PEAP, TTLS (avec son authentification interne, par exemple MSCHAPv2) ou TLS (certificat uniquement).
- **Identifiants de l'utilisateur de l'appareil** : chaque appareil utilise l'identité EAP, l'identité anonyme et le mot de passe de son utilisateur, définis dans la page Utilisateurs. Les appareils sans utilisateur ne reçoivent pas le réseau.
- **Identité**, **Identité anonyme** et **Mot de passe** : les mêmes pour chaque appareil. L'identité peut contenir les variables $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ et $UDID$. Laissez le mot de passe vide pour que l'utilisateur le saisisse sur l'appareil.
- **Certificat d'identité** : le certificat client que l'appareil présente (obligatoire pour TLS). Voir les options de certificat ci-dessous.
- **Certificats de confiance** : les certificats CA qui ont émis le certificat de votre serveur RADIUS. Ils sont installés avec le réseau.
- **Noms de serveur de confiance** : les noms des certificats du serveur RADIUS que les appareils acceptent, par exemple radius.example.com ou *.example.com.

VPN

Cliquez sur **Ajouter un VPN** pour configurer un VPN IKEv2 ou Cisco IPSec, intégré à iOS, iPadOS et macOS (aucune app VPN nécessaire).

- **Type** et **Serveur**. Pour IKEv2 également l'**Identifiant distant** (l'identité du serveur, vide signifie l'adresse du serveur) et l'**Identifiant local**, qui peut contenir les variables $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ et $UDID$.
- **Authentification** de l'appareil : un certificat (depuis la page Certificats, le certificat de l'utilisateur de l'appareil, ou demandé à un serveur SCEP), un secret partagé (avec le nom de groupe facultatif pour IPSec), ou aucune pour les serveurs IKEv2 qui vérifient uniquement le nom d'utilisateur et le mot de passe.
- **Certificats de confiance** : les certificats CA de votre serveur VPN, installés avec le VPN. Pour IKEv2, vous pouvez aussi définir l'émetteur et le nom attendus du certificat du serveur.
- **Nom d'utilisateur et mot de passe** : l'utilisateur s'authentifie aussi avec un nom d'utilisateur (variables autorisées) et un mot de passe (EAP pour IKEv2, XAuth pour IPSec). Laissez le mot de passe vide pour que l'utilisateur le saisisse sur l'appareil.
- **Nom du VPN** (affiché dans Réglages) et **S'applique à**.

Connexion

- **L'utilisateur se connecte dans Réglages** : le VPN est installé et l'utilisateur l'active lorsqu'il en a besoin.
- **À la demande** : l'appareil connecte automatiquement le VPN. Avec **sauf sur les Wi-Fi de confiance**, le VPN n'est pas utilisé sur les réseaux Wi-Fi que vous listez, par exemple le réseau du bureau.
- **Toujours actif** (IKEv2, iPhone et iPad supervisés uniquement) : tout le trafic passe par le VPN en cellulaire et en Wi-Fi et l'utilisateur ne peut pas le désactiver. Les autres appareils ne reçoivent pas ce VPN. Si le VPN utilise un nom d'utilisateur, le mot de passe doit être défini dans la stratégie.
- **VPN par app** : seules certaines apps utilisent le VPN. Choisissez le VPN pour chaque app dans la section **Gestion des apps** (champ **VPN** de l'app, non disponible sur Mac), et listez éventuellement les domaines Safari qui l'utilisent.

> Testez d'abord un VPN Toujours actif ou à la demande sur un appareil de test : si le serveur est inaccessible, l'appareil peut ne plus avoir de connexion.

Proxy global, DNS chiffré et filtre de contenu web

Ces paramètres s'appliquent à tout le trafic de l'appareil. Activez-les avec leur commutateur.

- **Proxy HTTP global** (iPhone et iPad supervisés, Mac) : tout le trafic HTTP passe par le proxy, sur chaque réseau. Définissez le serveur et le port (avec un nom d'utilisateur et un mot de passe facultatifs) ou une configuration automatique (URL de fichier PAC, ou vide pour la trouver sur le réseau). **Autoriser les pages de connexion Wi-Fi** permet à l'utilisateur de se connecter aux réseaux Wi-Fi publics sans le proxy.
- **DNS chiffré** : l'appareil résout les noms avec votre serveur DNS via DNS over HTTPS (URL du serveur) ou DNS over TLS (nom du serveur), éventuellement uniquement pour certains domaines. Sur les appareils supervisés, vous pouvez empêcher l'utilisateur de le désactiver.
- **Filtre de contenu web** (iPhone et iPad supervisés) : le filtre intégré à iOS limite les sites pour adultes, avec des listes de sites toujours autorisés ou toujours bloqués, ou autorise uniquement une liste de sites, affichés comme favoris dans Safari.

> Un proxy ou un serveur DNS incorrect peut laisser les appareils sans connexion : essayez d'abord les paramètres sur un appareil de test.

Certificats

Cliquez sur **Ajouter un certificat** pour installer un certificat seul : une autorité de certification à laquelle Safari et les apps doivent faire confiance, ou une identité utilisée par des apps. Les certificats d'un réseau Wi-Fi ou d'un VPN n'ont pas besoin d'être ajoutés ici.

Options de certificat

- **Un certificat de la page Certificats** : le même certificat sur chaque appareil. Cliquez sur **Choisir un certificat** pour le sélectionner.
- **Le certificat de l'utilisateur de l'appareil** : chaque appareil reçoit le certificat client lié à son utilisateur. Les appareils dont l'utilisateur n'a pas de certificat ne le reçoivent pas. Lorsque vous liez un autre certificat à l'utilisateur, les appareils sont mis à jour.
- **Demandé à un serveur SCEP** : chaque appareil demande son propre certificat à votre serveur SCEP (par exemple Microsoft NDES), de sorte que la clé privée ne quitte jamais l'appareil. Définissez l'URL du serveur, le défi si le serveur en exige un, le sujet (par exemple CN=$EMAIL$), les noms alternatifs, la taille de clé et l'usage de la clé.

> Les certificats client (.p12) protégés par l'ancien chiffrement RC2 ne peuvent pas être installés sur les appareils Apple. Exportez-les de nouveau avec le chiffrement 3DES ou AES avant de les importer.

Sécurité

Les profils qui contiennent des mots de passe ou des clés privées sont envoyés uniquement à l'appareil pour lequel ils ont été créés : l'appareil doit signer sa demande avec son certificat de gestion. Les mots de passe et les certificats ne sont pas écrits dans les journaux.

Mises à jour logicielles

La section **Mises à jour logicielles** de l'éditeur de stratégie Apple permet de maintenir les appareils à jour : elle peut exiger une version spécifique du système d'exploitation avant une date limite et contrôler la façon dont les appareils téléchargent et installent les mises à jour.

Mises à jour requises du système

Cliquez sur **Ajouter une mise à jour requise** pour exiger une version du système. L'appareil télécharge la mise à jour, informe l'utilisateur de la date limite et l'installe à cette date si l'utilisateur ne l'a pas déjà fait. Les appareils qui exécutent déjà cette version ou une version ultérieure l'ignorent. Nécessite iOS et iPadOS 17 ou macOS 14.

- **S'applique à** (requis) : iPhone et iPad, ou Mac. Chaque système a ses propres numéros de version, ajoutez donc une mise à jour requise pour chacun.
- **Version du système** : la version à installer, par exemple 18.5 ou 15.4.1.
- **Build** (facultatif) : une version de compilation spécifique, par exemple une bêta ou une amélioration de sécurité en arrière-plan.
- **Installer avant** : la date limite, dans l'heure locale de chaque appareil. Une date passée incite les appareils à installer la mise à jour dès que possible.
- **URL des détails** (facultatif) : une page web sur la mise à jour, affichée à l'utilisateur.

> L'appareil signale la progression de la mise à jour (téléchargement, installation, échecs) dans le panneau **État de l'appareil** de la page de l'appareil.

Paramètres des mises à jour logicielles

Activez **Paramètres des mises à jour logicielles pour iPhone et iPad** ou **Paramètres des mises à jour logicielles pour Mac** pour contrôler les mises à jour sur ces appareils. Lorsqu'une option est désactivée, les appareils conservent leurs propres paramètres. Nécessite iOS et iPadOS 18 ou macOS 15 : les appareils plus anciens ignorent ces paramètres.

- **Différer les mises à jour** : les nouvelles mises à jour ne sont présentées à l'utilisateur qu'après le nombre de jours indiqué (1 à 90). Sur un Mac, vous pouvez définir des périodes différentes pour les mises à jour majeures, les mises à jour mineures et les autres mises à jour du système.
- **Mises à jour présentées à l'utilisateur** (iPhone et iPad) : lorsque plusieurs mises à jour sont disponibles, affichez-les toutes, uniquement la plus ancienne mise à jour mineure ou uniquement la plus récente.
- **Les utilisateurs standard peuvent installer les mises à jour** (Mac) : les utilisateurs sans droits d'administrateur peuvent installer les mises à jour macOS.
- **Notifier l'utilisateur des mises à jour requises** : afficher les notifications concernant les mises à jour requises et leur date limite.
- **Téléchargement automatique**, **Installation automatique** et **Mises à jour de sécurité automatiques** : laissez l'utilisateur décider (valeur par défaut d'Apple), ou maintenez-les toujours activés ou toujours désactivés.
- **Améliorations de sécurité en arrière-plan** : proposez à l'utilisateur les correctifs de sécurité rapides d'Apple et choisissez si l'utilisateur peut les supprimer.
- **Programmes bêta** : laissez l'utilisateur rejoindre les programmes bêta d'Apple, ou retirez l'appareil de ces programmes et bloquez-les (sur iPhone et iPad, appareils supervisés uniquement).

Installer une mise à jour depuis la page de l'appareil

Le panneau **État de l'appareil** d'un appareil répertorie les mises à jour disponibles. Utilisez **Rechercher les mises à jour** pour demander la liste à l'appareil et **Installer** pour en installer une immédiatement ou pour la télécharger et laisser l'utilisateur l'installer. Cela fonctionne sur les iPhone et iPad supervisés et sur les Mac. Apple supprime ces commandes dans iOS, iPadOS et macOS 27 : sur ces versions, utilisez les mises à jour requises de la stratégie.

macOS

La section **macOS** de l'éditeur de stratégie Apple gère les paramètres de sécurité, de confidentialité et de connexion des Mac : FileVault, pare-feu, Gatekeeper, économiseur d'écran et verrouillage, stockage externe et réseau, partage d'écran, autorisations de confidentialité, éléments de connexion, et extensions système et noyau autorisées à se charger. Elle installe aussi des fichiers de configuration de services système et de tâches en arrière-plan. Les autres appareils de la stratégie ne reçoivent pas ces paramètres. Activez un paramètre pour le gérer ; tant qu'il est désactivé, les utilisateurs conservent leurs propres choix.

> La plupart des paramètres sont installés sur le Mac sous forme de profils de configuration, visibles dans Réglages Système > Général > Gestion de l'appareil. FileVault, les autorisations de confidentialité, les éléments de connexion et les paramètres d'extension nécessitent un MDM approuvé par l'utilisateur : sur un Mac inscrit avec l'URL d'inscription ou le code QR, l'utilisateur approuve le profil d'inscription dans Réglages Système. La page de l'appareil l'indique dans le champ **MDM approuvé par l'utilisateur**. Lorsque l'utilisateur l'approuve plus tard, le Mac reçoit ces paramètres automatiquement.

FileVault

FileVault chiffre le disque du Mac. Lorsque ce paramètre est activé, les utilisateurs sont invités à activer FileVault avec leur mot de passe, et le Mac envoie sa clé de récupération personnelle à Cerberus Enterprise, chiffrée avec une clé qui appartient uniquement à votre organisation. La clé est affichée et modifiée depuis le champ **FileVault** de la page de l'appareil (voir Commandes de l'appareil). Le paramètre nécessite macOS 13 ou ultérieur et un MDM approuvé par l'utilisateur ; sans MDM approuvé par l'utilisateur, le Mac n'est pas invité à activer FileVault, mais si un utilisateur l'active, sa clé est stockée.

- **Obligatoire à la connexion** : à la prochaine connexion, après un certain nombre de reports (l'utilisateur est invité de nouveau à chaque connexion et à la déconnexion), ou uniquement lorsque l'utilisateur se déconnecte.
- **Ne pas demander à la déconnexion** : l'utilisateur est invité uniquement à la connexion. Cette option ne peut pas être combinée avec « Uniquement demandé à la déconnexion ».
- **Afficher la clé de récupération à l'utilisateur** : désactivé par défaut, de sorte que seuls les administrateurs connaissent la clé, depuis la page de l'appareil.
- **Empêcher la désactivation de FileVault** : activé par défaut.
- **Supprimer la clé de la mémoire en veille** : l'utilisateur saisit de nouveau le mot de passe lorsque le Mac sort de veille.

- **Où la clé est conservée** : texte affiché à l'utilisateur à l'écran de connexion, par exemple qui appeler pour récupérer le Mac (par défaut « Cerberus Enterprise »).

> Un Mac déjà chiffré lorsqu'il a reçu le paramètre conserve sa clé actuelle, que Cerberus Enterprise ne reçoit pas : la clé est stockée uniquement après que l'utilisateur a désactivé puis réactivé FileVault (avec « Empêcher la désactivation de FileVault » désactivé). La désactivation du paramètre, ou le retrait du Mac de la gestion, ne désactive pas FileVault, et la clé stockée continue de fonctionner. Le paramètre ne peut pas être enregistré lorsque le serveur n'est pas configuré pour stocker les clés de récupération.

Pare-feu

- **Activer le pare-feu** : lorsqu'il est désactivé, le pare-feu reste désactivé et les utilisateurs ne peuvent pas l'activer.
- **Bloquer toutes les connexions entrantes** : seuls les services réseau de base (DHCP, Bonjour, IPSec) peuvent recevoir des connexions.
- **Mode furtif** : le Mac ne répond pas aux requêtes ping ni aux connexions vers des ports fermés.
- **Autoriser les logiciels intégrés** et **Autoriser les apps signées téléchargées** à recevoir des connexions sans demander à l'utilisateur (macOS 12.3 ou ultérieur).
- **Règles pour des apps spécifiques** : autorisez ou bloquez les connexions entrantes d'une app, par identifiant de bundle.

Gatekeeper

Gatekeeper vérifie les apps avant qu'elles ne s'ouvrent. Choisissez si les Mac ouvrent uniquement les apps de l'App Store, ou aussi les apps de développeurs identifiés. Avec Gatekeeper désactivé, toute app peut être ouverte, y compris les apps non signées ou endommagées. Sur macOS 15 ou ultérieur, vous pouvez aussi choisir si les utilisateurs sont invités à envoyer les logiciels malveillants bloqués à Apple.

Économiseur d'écran et verrouillage

Démarrez l'économiseur d'écran après une période d'inactivité et demandez le mot de passe lorsque l'économiseur d'écran démarre ou que l'écran s'éteint, immédiatement ou après un délai.

Un paramètre laissé sur **Non géré** reste au choix de l'utilisateur.

Stockage externe et réseau

Autorisez, rendez accessible en lecture seule ou bloquez le stockage externe (clés USB, cartes SD, disques externes) et le stockage réseau (partages de fichiers) des Mac. Nécessite macOS 15 ou ultérieur.

Partage d'écran

Limites des personnes qui se connectent à ces Mac avec le partage d'écran : copie de fichiers depuis ou vers le Mac, connexions hautes performances et nombre d'écrans virtuels. L'activation du partage d'écran reste au choix de l'utilisateur. Nécessite macOS 14 ou ultérieur.

Autorisations de confidentialité

Accordez ou refusez aux apps l'accès que les utilisateurs autoriseraient autrement dans Réglages Système > Confidentialité et sécurité, par exemple l'accès complet au disque pour une app de sauvegarde, ou refusez la caméra à une app. Pour chaque autorisation, choisissez :

- **Autorisation** : Accès complet au disque, Accessibilité, Automatisation, les dossiers, contacts, calendriers, photos, caméra, microphone, enregistrement de l'écran et les autres autorisations de Confidentialité et sécurité.
- **Accès** : autoriser ou refuser. La caméra, le microphone, l'enregistrement de l'écran et la surveillance des entrées ne peuvent pas être autorisés par un profil, seulement refusés ; pour l'enregistrement de l'écran et la surveillance des entrées, vous pouvez permettre aux utilisateurs de les autoriser aussi sans droits d'administrateur.
- **App** : l'identifiant de bundle d'une app, ou le chemin d'un programme (par exemple un outil en ligne de commande).
- **Exigence de code** : identifie l'app par sa signature. Obtenez-la dans Terminal avec `codesign -dr - /Applications/Example.app` et copiez le texte après `designated =>`.
- **Automatisation** nécessite aussi l'app contrôlée (par exemple le Finder) et son exigence de code.

Éléments de connexion et d'arrière-plan

Les éléments de connexion et d'arrière-plan qui correspondent aux règles sont gérés : ils s'exécutent sans demander et les utilisateurs ne peuvent pas les désactiver dans Réglages Système > Général > Éléments de connexion. Une règle correspond à l'identifiant d'équipe de développeur d'une app, à son identifiant de bundle ou au libellé d'un démon ou agent de lancement (aussi par leur première partie). Nécessite macOS 13 ou ultérieur.

Extensions système

Les extensions système sont le moyen moderne pour les apps d'étendre macOS : filtres réseau et VPN, agents et pilotes de sécurité des points de terminaison. Lorsque ce paramètre est activé, les extensions système des équipes de développeurs listées se chargent sans demander à l'utilisateur. Nécessite macOS 10.15 ou ultérieur et un MDM approuvé par l'utilisateur.

- **ID d'équipe** : l'ID d'équipe de 10 caractères du développeur (par exemple dans les détails « Signé par » de l'app, ou avec `codesign -dv`). Chaque équipe ne peut apparaître qu'une fois.
- **Autoriser** : toutes les extensions de l'équipe, ou uniquement les extensions dont les identifiants de bundle sont listés.
- **Types** : limite l'équipe aux pilotes, aux extensions réseau ou de sécurité des points de terminaison. Si aucun type n'est choisi, tous les types sont autorisés.
- **Suppression** (uniquement pour les extensions listées) : l'app peut supprimer son extension sans administrateur (macOS 12 ou ultérieur), l'extension ne peut pas être désactivée ni supprimée tant que la protection de l'intégrité du système est activée, ou elle ne peut pas être supprimée dans Réglages Système et le Finder (macOS 15 ou ultérieur). Les Mac avec un macOS plus ancien autorisent toujours l'extension, sans l'option de suppression.
- **Les utilisateurs peuvent approuver d'autres extensions système** : activé par défaut. Lorsque cette option est désactivée, seules les extensions autorisées par un profil peuvent se charger ; si un profil du Mac la désactive, elle est désactivée.

> Sur macOS 11.3 ou ultérieur, la suppression de ce paramètre désactive les extensions système qu'il autorisait, par exemple un agent de sécurité ou un filtre réseau. Cela se produit lorsque le paramètre est désactivé, lorsque la stratégie est supprimée et lorsque le Mac passe à une stratégie qui ne le contient pas. L'éditeur demande une confirmation avant de désactiver le paramètre.

Extensions de noyau (héritées)

Les extensions de noyau sont l'ancien moyen, obsolète, d'étendre macOS : préférez les extensions système lorsque l'éditeur les propose. Les extensions de noyau des équipes listées (toutes les extensions d'une équipe, ou uniquement les identifiants de bundle listés) se chargent sans demander à l'utilisateur, après un redémarrage. Nécessite macOS 10.13.2 ou ultérieur et un MDM approuvé par l'utilisateur.

- **Les utilisateurs peuvent approuver d'autres extensions de noyau** : désactivé par défaut, de sorte que seules les équipes listées peuvent charger des extensions de noyau.
- **Les utilisateurs standard peuvent aussi les approuver** : lorsque les approbations par les utilisateurs sont activées, les utilisateurs sans droits d'administrateur peuvent aussi les approuver (macOS 11 ou ultérieur).

> Sur les Mac avec Apple silicon, un profil seul ne suffit pas : quelqu'un doit démarrer le Mac en recoveryOS, choisir Sécurité réduite dans l'Utilitaire de sécurité au démarrage et autoriser la gestion des extensions de noyau par les utilisateurs pour les développeurs identifiés. Le Mac peut aussi avoir besoin d'un Bootstrap Token déposé dans Cerberus Enterprise pour les approuver (voir le champ Bootstrap Token de la page de l'appareil).

Fichiers Mac

Les fichiers de configuration de service et les tâches en arrière-plan utilisent des fichiers que vous téléversez dans les **Fichiers Mac** de votre organisation : archives zip et listes de propriétés (.plist) jusqu'à 20 Mo. Téléversez-les, vérifiez où ils sont utilisés ou supprimez-les avec le bouton **Fichiers Mac** de la section macOS, ou avec **Choisir un fichier** dans un paramètre. Un fichier utilisé par une stratégie ne peut pas être supprimé. Pour modifier un fichier, téléversez la nouvelle version et choisissez-la dans la stratégie : les Mac la téléchargent de nouveau.

Fichiers de configuration de service

Installe les fichiers de configuration d'un service système à partir d'une archive zip. Les services intégrés sont le serveur SSH (sshd), sudo, PAM, l'impression (CUPS), le serveur web Apache, bash, zsh, la connexion par carte à puce et l'autorisation. Vous pouvez aussi utiliser votre propre service, avec un identifiant DNS inversé comme `com.example.service` : il trouve les fichiers avec la bibliothèque de fichiers de configuration gérés de macOS. Chaque service peut avoir un seul

paramètre. Nécessite macOS 14 ou ultérieur.

> Un service intégré utilise uniquement les fichiers de l'archive et ignore ses propres fichiers, par exemple /etc/ssh pour sshd : placez toute la configuration dans l'archive, dans des dossiers qui partent de la racine du disque (par exemple `etc/ssh/sshd_config`). Les fichiers sont en lecture seule sur le Mac et sont supprimés avec le paramètre. Testez d'abord l'archive sur un Mac : une mauvaise configuration de sudo ou de PAM peut empêcher les utilisateurs de se connecter ou d'utiliser les droits d'administrateur.

Tâches en arrière-plan

Programmes et scripts qui s'exécutent en arrière-plan, lancés par launchd. Les utilisateurs ne peuvent pas les désactiver, et ils sont supprimés avec le paramètre. Nécessite macOS 15 ou ultérieur. Pour chaque tâche, choisissez :

- **Identifiant de tâche** : un identifiant DNS inversé, comme `com.example.task`, différent pour chaque tâche.
- **Programmes et scripts** (facultatif) : une archive zip que le Mac décompresse dans `/var/db/ManagedConfigurationFiles/BackgroundTaskServices/Services/` suivi de l'identifiant de tâche. Conservez le droit d'exécution des fichiers et n'y placez pas de listes de propriétés.
- **Listes de propriétés launchd** : les tâches qui démarrent les programmes, chargées comme démon (pour tout le système, en tant que root) ou comme agent (dans chaque session utilisateur). Référez-vous aux programmes avec leur chemin dans le dossier ci-dessus.

Une tâche nécessite les programmes ou au moins une liste de propriétés. Lorsque les fichiers changent, les Mac redémarrent la tâche.

Localisation et géorepérage

La section **Localisation et géorepérage** de l'éditeur de stratégie Apple définit des zones, par exemple un site ou un entrepôt. Les iPhone et iPad avec l'app Cerberus Enterprise signalent lorsqu'ils entrent dans l'une de ces zones ou en sortent, et les règles d'événement peuvent y réagir : envoyer un e-mail, verrouiller ou désactiver l'appareil, ou le réactiver. Les Mac n'utilisent pas le géorepérage.

Champs de la zone géographique

Utilisez **Ajouter une zone géographique** pour créer une nouvelle entrée. Une stratégie peut contenir jusqu'à **10 zones géographiques**, et leurs noms doivent être uniques au sein de la stratégie. Chaque zone géographique contient les champs suivants :

- **Nom** : obligatoire et unique.
- **Latitude** et **Longitude** : le centre de la zone. Vous pouvez également cliquer sur la carte pour le définir.
- **Rayon (m)** : obligatoire, de **200** à **10 000** mètres.
- **Description** : notes facultatives pour les administrateurs.
- **Signaler l'entrée** et **Signaler la sortie** : choisissez les événements à générer. Au moins l'un d'eux doit rester activé.
- **Active** : active ou désactive la zone géographique sans la supprimer.

Chaque zone géographique dispose d'un aperçu de carte. Le centre et le rayon d'une zone géographique enregistrée sont verrouillés : utilisez le bouton de verrouillage sur la carte pour les modifier. Les autres boutons centrent la carte sur la zone ou sur votre position actuelle.

Lorsque vous enregistrez la stratégie, Cerberus Enterprise demande aux iPhone et iPad de la stratégie de récupérer les nouvelles zones géographiques. Cela prend généralement quelques minutes, mais iOS peut le retarder, par exemple en mode Économie d'énergie ou sans connexion réseau. La page de l'appareil indique lorsque l'app n'a pas encore appliqué les dernières zones géographiques.

Exigences

Les zones géographiques fonctionnent sur les iPhone et iPad équipés de l'app Cerberus Enterprise. Les Mac les ignorent. Sur l'appareil :

- l'app Cerberus Enterprise est installée (Cerberus l'installe) et l'utilisateur l'a ouverte au moins une fois ;
- l'accès à la position pour l'app est défini sur **Toujours** ;
- **Position précise** est activée pour l'app ;
- **Actualisation des apps en arrière-plan** est activée.

> **Position et zones géographiques sur les appareils personnels**, en haut de la section, est désactivé par défaut. Tant que cette option est désactivée, Cerberus ne collecte pas la position des appareils personnels (inscription utilisateur), leurs événements de zone géographique ne sont pas générés et leur page d'appareil ne propose ni Localiser ni le suivi en direct. Lorsque vous l'activez, les appareils personnels de la stratégie partagent leur position et leurs événements de zone géographique comme les appareils d'entreprise, mais uniquement si l'utilisateur autorise la localisation pour l'app Cerberus Enterprise ; l'app explique cela à l'utilisateur avant que iOS ne le demande. Votre organisation est responsable d'informer les utilisateurs et de respecter la réglementation locale sur la localisation des employés. Le mode Perdu et la demande de localisation MDM ne sont jamais disponibles sur les appareils personnels (Apple ne les autorise pas).

En **mode Économie d'énergie**, les zones géographiques continuent de fonctionner, mais iOS signale une sortie de zone plus tard et avec une position moins précise, et il peut retarder de plusieurs heures la récupération de nouvelles zones géographiques après une modification de stratégie, jusqu'à la prochaine exécution de l'app (par exemple au prochain franchissement ou lorsque l'utilisateur l'ouvre).

Comment arrivent les événements

iOS surveille les zones pour l'app et la réveille lorsque l'appareil franchit une limite, même lorsque l'app n'est pas ouverte. Les événements peuvent arriver quelques minutes après le franchissement, et une petite zone ou une visite courte peut être manquée : iOS exige que l'appareil parcoure une certaine distance au-delà de la limite et y reste un moment.

Si l'app ne peut pas s'exécuter, par exemple après un redémarrage avant le déverrouillage de l'appareil, le serveur détecte aussi le franchissement à partir des positions envoyées par l'app, plus tard. Chaque franchissement déclenche une seule fois les règles d'événement, que ce soit l'app ou le serveur qui le détecte.

Lorsque l'app n'a pas contacté le serveur depuis plusieurs heures, le serveur demande à iOS de la réveiller afin qu'elle puisse vérifier à nouveau ses zones géographiques. iOS ne garantit pas ces demandes.

Page de l'appareil

Sur la page de l'appareil, l'onglet **Zone géographique** du panneau **Carte de localisation** affiche les transitions de l'appareil. Lorsque la stratégie comporte des zones géographiques actives, une ligne d'état indique si le géorepérage fonctionne sur l'appareil, ou pourquoi il ne le peut pas : l'app n'a pas contacté le serveur ou doit être mise à jour, l'accès à la position n'est pas défini sur **Toujours**, **Position précise** ou **Actualisation des apps en arrière-plan** est désactivé, le **mode Économie d'énergie** était activé lors du dernier signalement des réglages par l'app, ou l'app n'a pas encore appliqué les dernières zones géographiques.

> Les transitions de zones géographiques et les positions sont conservées **90 jours** et les données plus anciennes sont supprimées automatiquement chaque nuit. La dernière position de chaque appareil inscrit est toujours conservée, de sorte qu'il reste sur les cartes.

Limites

- La copie d'une stratégie ne copie pas ses zones géographiques : ajoutez-les de nouveau dans la copie.
- Les événements de zone géographique sur iPhone et iPad sont fournis au mieux : iOS décide quand l'app peut s'exécuter.

> Pour réagir aux événements de zone géographique, créez une règle d'événement pour **L'appareil entre dans une zone géographique** ou **L'appareil sort d'une zone géographique**. Consultez **Règles d'événement**.

Comptes

La section **Comptes** de l'éditeur de stratégie Apple ajoute des comptes de messagerie, Exchange, Google, calendrier, contacts et annuaire aux iPhone, iPad et Mac. Cliquez sur **Ajouter un compte** et choisissez le type. La section contient également la restriction **Autoriser la modification du compte** (appareils supervisés).

> Sur un Mac (macOS 13 ou version ultérieure), les comptes sont installés dans la session des utilisateurs inscrits à la gestion, généralement l'utilisateur qui a inscrit le Mac, lorsqu'ils sont connectés. La page de l'appareil répertorie ces utilisateurs sous **Utilisateurs du Mac**, avec l'état de leurs comptes. Les comptes qui reprennent l'adresse e-mail de l'utilisateur de l'appareil utilisent l'utilisateur affecté au Mac dans Cerberus Enterprise.

Paramètres communs

- **Nom et e-mail de l'utilisateur de l'appareil** (Mail, Exchange, Google) : chaque appareil utilise le nom et l'adresse e-mail de son utilisateur, définis dans la page Utilisateurs (pour Google, le compte Google de l'utilisateur). Les appareils sans utilisateur, ou dont l'utilisateur n'a pas d'adresse e-mail, ne reçoivent pas le compte. Sinon, définissez une adresse e-mail et un nom complet fixes.
- **Nom du compte** (facultatif) : le nom du compte dans les Réglages et dans les applications.
- **Nom d'utilisateur** et **Mot de passe** (facultatifs) : le nom d'utilisateur peut contenir les variables $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ et $UDID$. Laissez le mot de passe vide pour que l'utilisateur le saisisse sur l'appareil, ou laissez les deux vides pour que l'utilisateur les saisisse.
- **S'applique à** : limitez le compte à certains types d'appareils.

Types de comptes

- **Compte de messagerie** : serveur entrant IMAP ou POP et serveur sortant, avec leurs ports et leur authentification. Le serveur sortant peut utiliser le même nom d'utilisateur et le même mot de passe que le serveur entrant.
- **Compte Exchange** (Exchange ActiveSync) : le serveur, ou vide pour le rechercher à partir de l'adresse e-mail. Choisissez les services (messagerie, contacts, calendriers, rappels, notes) et si l'utilisateur peut les modifier. Avec **l'authentification moderne**

(OAuth), l'utilisateur se connecte via la page de votre fournisseur d'identité, par exemple Microsoft 365. Un **certificat d'authentification** (iOS 17 ou version ultérieure) authentifie l'appareil avec un certificat.
- **Compte Google** : l'utilisateur se connecte au compte Google avec l'adresse e-mail indiquée.
- **Compte de calendrier (CalDAV)** et **Compte de contacts (CardDAV)** : le serveur, le port et le chemin.
- **Annuaire (LDAP)** : le serveur et le port, ainsi que les recherches (base de recherche, portée et description) utilisées pour rechercher des contacts.
- **Calendrier abonné** : l'URL du calendrier (https, http ou webcal).

S/MIME

Les comptes Mail et Exchange peuvent signer et chiffrer les messages avec S/MIME (iOS 17 ou version ultérieure). Pour chacun, choisissez le certificat : l'un de ceux de la page Certificats, le certificat de l'utilisateur de l'appareil ou un certificat demandé à un serveur SCEP. Vous pouvez autoriser l'utilisateur à le désactiver, à choisir un autre certificat et, pour le chiffrement, afficher un commutateur pour chaque message.

Sécurité

Les mots de passe et les certificats ne font pas partie des paramètres envoyés aux appareils : chaque appareil télécharge ses propres identifiants depuis Cerberus Enterprise en signant la demande avec son certificat de gestion. Ils ne sont pas écrits dans les journaux.

Règles de conformité

La section **Règles de conformité** de l'éditeur de stratégie Apple définit des exigences pour les appareils de la stratégie. Un appareil qui enfreint une règle est immédiatement non conforme : la page de l'appareil en explique la raison, dans **Pourquoi l'appareil est non conforme**, et la liste des appareils l'affiche comme non conforme. Un appareil est également non conforme lorsqu'un paramètre de la stratégie ne peut pas y être appliqué.

Règles

- **Code d'accès** : l'appareil possède un code d'accès et celui-ci respecte les paramètres de code d'accès de la stratégie.
- **Version minimale du système d'exploitation** : pour iPhone et iPad, ou pour Mac. Pour mettre à jour les appareils, ajoutez une mise à jour obligatoire dans Mises à jour logicielles.
- **Appareil supervisé** : les appareils inscrits avec le profil d'inscription ou avec l'inscription utilisateur ne sont pas supervisés.
- **FileVault activé (Mac)** : le disque du Mac est chiffré avec FileVault. Les autres appareils ne sont pas concernés.

Une règle est vérifiée lorsque l'appareil envoie son état, lorsque la stratégie est enregistrée et toutes les heures. Un appareil dont l'état est inconnu (par exemple un Mac qui n'a pas encore signalé FileVault) n'enfreint pas la règle.

Blocage de l'appareil

Activez **Bloquer l'appareil s'il est toujours non conforme** et définissez après combien de jours (0 bloque immédiatement). Les iPhone et iPad supervisés passent en mode Perdu avec le message que vous définissez. Les autres appareils sont verrouillés une fois ; un Mac redémarre et demande un code PIN, affiché dans les détails de la commande de l'historique des commandes.

- **Débloquer** : lorsque l'appareil est de nouveau conforme, le mode Perdu est désactivé automatiquement.
- **Désactiver vous-même le mode Perdu** : l'appareil n'est plus bloqué tant qu'il ne redevient pas conforme et n'enfreint pas de nouveau une règle. Utilisez cette option pour permettre à l'utilisateur de corriger l'appareil.

Pour être notifié ou réagir d'une autre manière, créez une règle d'événement pour **L'appareil devient non conforme** : elle reçoit aussi les raisons.