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.

Revision #6
Created 2026-11-10 15:15:28 UTC by Admin
Updated 2026-11-12 09:55:16 UTC by Admin