Commandes

La page de l'appareil propose un panneau **Commandes** pour envoyer des commandes à distance à un appareil géré. Les commandes disponibles dépendent de la plateforme (Android ou Apple) et de l'état de l'appareil.

Les commandes ne peuvent être envoyées qu'à un appareil actuellement inscrit. Sur un appareil désinscrit, sur un appareil ADE qui n'est pas encore inscrit et sur l'historique d'une inscription passée, le panneau affiche uniquement l'historique des commandes.

> Si l'appareil n'est pas actuellement en ligne, la commande sera transmise et exécutée dès que l'appareil se connectera à Internet. Pour les commandes Android, vous pouvez définir le paramètre **Validité** afin de déterminer pendant combien de temps une commande non transmise reste valide.

Commandes Android (AMAPI)

Pour les appareils Android, le panneau Commandes comprend un champ **Validité** (valeur + unité) et un sélecteur **Commande**. Certaines commandes nécessitent des paramètres supplémentaires, qui apparaissent dynamiquement lorsque vous sélectionnez la commande.

Paramètres courants

- **Validité** : durée pendant laquelle la commande reste valide si elle ne peut pas être exécutée immédiatement.
- **Commande** : choisissez l'action à envoyer à l'appareil.

Commandes sans champs supplémentaires

- **Verrouiller l'appareil** : verrouille l'appareil.
- **Redémarrer l'appareil** : redémarre l'appareil. Nécessite Android 7.0 ou version ultérieure.
- **Désactiver le mode perdu** : sort l'appareil du mode perdu.

- **Renoncer à la propriété** : supprime le profil professionnel et toutes les stratégies d'un appareil d'entreprise sous Android 8.0 ou version ultérieure, et le laisse pour un usage personnel. Les applications et données du profil personnel sont conservées. L'appareil est supprimé du serveur après avoir accusé réception de la commande. Cette action est irréversible.

Commandes avec des champs supplémentaires

- **Réinitialiser le mot de passe** : nécessite **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**. Des options facultatives sont disponibles : **Verrouiller maintenant**, **Exiger la saisie** et **Ne pas demander d'identifiants au démarrage**.
- **Effacer les données de l'application** : nécessite le **Nom du package** cible.
- **Activer le mode perdu** : nécessite un **Message du mode perdu** et prend en charge des champs de contact facultatifs (adresse, organisation, numéro de téléphone, e-mail). Lorsque l'appareil le signale, son état devient **Perdu**, la page de l'appareil affiche une bannière et cette commande est masquée jusqu'à la désactivation du mode perdu.
- **Effacer l'appareil** : prend en charge un **Message de motif de réinitialisation** (affiché aux utilisateurs sur les appareils personnels) et des options de réinitialisation facultatives, notamment **Effacer les eSIM**.

> Les commandes eSIM (**Ajouter une eSIM**, **Supprimer une eSIM**, **Demander l'EID**) sont disponibles dans le panneau dédié **Gestion des SIM**.

Historique des commandes

Sous les commandes d'envoi, le tableau de bord affiche un tableau d'historique des commandes. Le tableau est triable et prend en charge la pagination. Certaines lignes peuvent être développées pour consulter des paramètres supplémentaires ou des détails d'exécution.

Colonnes de l'historique Android

- **Date de création**
- **Commande**
- **Validité**
- **État**
- **Erreur**
- **Date d'exécution**

Commandes Apple (MDM)

Pour les appareils Apple, le panneau Commandes fournit un sélecteur **Commande**. Certaines commandes nécessitent des saisies supplémentaires. Comme pour Android, un tableau d'historique des commandes est affiché ci-dessous.

Commandes avec des champs supplémentaires

- **Installer l'application** : nécessite le **Bundle ID** de l'application.
- **Envoyer une notification** : nécessite un **Message de notification** (200 caractères maximum).

Sur les iPhone et iPad, **Envoyer une notification** et le suivi en direct atteignent l'appareil via l'application **Cerberus Enterprise** : ils sont désactivés tant que l'application n'est pas installée et enregistrée pour les notifications (voir le champ **Application Cerberus Enterprise**). Le démarrage du suivi en direct affiche « Demande de suivi en direct envoyée à l'appareil » : le suivi commence lorsque l'appareil envoie sa première position. iOS peut retarder ou ne pas transmettre la demande, par exemple en mode Économie d'énergie ou sans connexion réseau : si aucune position n'arrive dans les 2 minutes, demandez à l'utilisateur d'ouvrir l'application une fois. En cas d'échec d'une demande, le message indique la raison, par exemple que l'application n'est pas encore enregistrée, que la clé de notification du serveur est absente ou que le jeton de notification de l'appareil n'est plus valide.

Actions sur l'appareil

Seules les commandes prises en charge par l'appareil sont répertoriées : certaines nécessitent un iPhone ou un iPad supervisé, d'autres ne sont pas disponibles sur un Mac. Les commandes perturbatrices demandent une confirmation.

- **Verrouiller l'appareil** : verrouille l'écran, avec un message et un numéro de téléphone facultatifs. Un Mac est redémarré et verrouillé avec un code PIN à six chiffres, affiché une fois après l'envoi de la commande et dans les détails de la commande. L'iPhone affiche le titre « iPhone perdu » au-dessus de votre message, même si cette commande n'active pas le mode perdu.
- **Activer le mode perdu** (iPhone et iPad supervisés) : verrouille l'appareil et affiche votre message, votre numéro de téléphone et votre note de bas de page sur l'écran verrouillé. Tant que le mode perdu est activé, la page affiche une bannière et les commandes **Localiser l'appareil** (la localisation apparaît sur la carte de localisation), **Lire un son** et **Désactiver le mode perdu**.

- L'appareil indique à la personne qui le tient qu'il a été localisé : après **Localiser l'appareil**, l'écran verrouillé affiche **iPhone localisé** avec l'heure et le nom du serveur qui a reçu la position, ainsi qu'un bouton **Continuer**. iOS affiche cet avis et il est impossible de le désactiver.
- **Effacer le code d'accès** : supprime le code d'accès d'un iPhone ou d'un iPad, par exemple lorsque l'utilisateur l'a oublié. Si la stratégie exige un code d'accès, l'utilisateur est invité à en définir un nouveau.
- **Actualiser les informations de l'appareil** : demande à l'appareil ses informations (supervision, version du système, état de sécurité, certificat MDM) et son inventaire.
- **Réglages de l'appareil** : ouvre une fenêtre pour modifier le nom de l'appareil, le nom d'hôte d'un Mac, le Bluetooth, l'itinérance des données, le partage de connexion, le fuseau horaire, le fond d'écran, l'autorisation du verrouillage d'activation et, sur un iPad partagé, ses réglages (voir ci-dessous). Seuls les réglages que vous modifiez sont envoyés ; ceux que l'appareil ne prend pas en charge sont désactivés avec la raison. Un appareil peut accuser réception de l'itinérance des données ou du partage de connexion sans les appliquer (par exemple lorsque le forfait SIM ne comprend pas le partage de connexion), c'est pourquoi Cerberus Enterprise les relit environ 30 secondes plus tard et écrit un avertissement dans les journaux système s'ils n'ont pas changé.
- **Redémarrer l'appareil** et **Éteindre l'appareil** : redémarrent ou éteignent l'appareil immédiatement, après confirmation.
- **Effacer l'appareil** : efface tout le contenu et les réglages et retire l'appareil de la gestion. Sur iPhone et iPad, vous pouvez conserver le forfait de données eSIM et ignorer la configuration de proximité ; un Mac reçoit un code PIN à six chiffres.
- **Retour au service** (option de **Effacer l'appareil**, iPhone et iPad avec iOS 17 ou ultérieur) : après l'effacement, l'appareil se configure à nouveau tout seul, sans intervention, et s'inscrit à nouveau avec sa stratégie, son utilisateur et son propriétaire actuels. Choisissez un réseau Wi-Fi de la stratégie de l'appareil pour la configuration, sauf si l'appareil dispose d'Ethernet ou de données cellulaires : seuls les réseaux personnels (avec un mot de passe, sans certificats) peuvent être utilisés, car l'appareil n'a encore ni utilisateur ni certificat. Le verrouillage d'activation doit être désactivé.
- **Actualiser les forfaits cellulaires** (iPhone et iPad cellulaire, iOS 13 ou ultérieur, hors User Enrollment) : saisissez l'**URL du serveur eSIM de l'opérateur** fournie par l'opérateur (une adresse https://, un nom d'hôte ou un code d'activation LPA, dont seul le serveur est utilisé) et l'appareil télécharge les forfaits eSIM que l'opérateur a associés à son EID. L'EID de l'appareil est affiché sous le champ pour l'envoyer à l'opérateur.

  Consultez la page **Gestion des SIM**.
- **Conserver le forfait de données eSIM** désactivé supprime toutes les eSIM lors de l'effacement. La restriction de stratégie **Conserver l'eSIM lors de l'effacement de l'appareil** (appareils supervisés, iOS 17.2 ou ultérieur) s'applique aux effacements lancés sur l'appareil (trop de tentatives de code d'accès échouées, Effacer tout le contenu et les réglages) : Apple ne documente pas son effet sur cette commande.
- **Déconnecter l'utilisateur** (iPad partagé) : déconnecte l'utilisateur actuel et revient à l'écran de connexion. Les données non encore synchronisées avec iCloud restent sur l'iPad.

iPad partagé

Un iPad partagé est utilisé par plusieurs personnes, chacune avec son propre Managed Apple Account, ou par des invités avec des sessions temporaires. Il est configuré avec un profil ADE qui active l'iPad partagé (voir la page **Apple Automated Device Enrollment**), et son champ **Type d'inscription** indique **iPad partagé**.

- **Utilisateurs de l'iPad partagé** : les utilisateurs de l'iPad, avec l'utilisateur connecté, l'espace de stockage qu'ils utilisent et si certaines données ne sont pas encore synchronisées avec iCloud. Utilisez **Actualiser** pour demander à nouveau la liste à l'iPad. Un utilisateur peut être supprimé avec ses données, sauf l'utilisateur connecté (déconnectez-le d'abord) ; **Supprimer tous les utilisateurs** nécessite iPadOS 14 ou ultérieur. Lorsque les données ne sont pas encore synchronisées, la confirmation avertit qu'elles seront perdues.
- **Réglages de l'appareil** : le stockage de chaque utilisateur, le nombre d'utilisateurs attendu, le délai d'inactivité après lequel les utilisateurs et les sessions invité sont déconnectés, les sessions invité uniquement, les domaines Managed Apple Account suggérés sur l'écran de connexion, le nombre de jours pendant lesquels un utilisateur peut se connecter sans vérifier le mot de passe en ligne, et l'ignorance de la configuration de la langue et de la région pour les nouveaux utilisateurs. Les champs vides conservent leur valeur actuelle ; les réglages nécessitant une version plus récente d'iPadOS sont désactivés.

Utilisateurs du Mac

Sur un Mac, le panneau **Utilisateurs du Mac** répertorie les utilisateurs inscrits à la gestion, généralement l'utilisateur qui a inscrit le Mac. Les comptes de la stratégie sont installés dans leurs sessions. Pour chaque utilisateur, il indique quand il a été inscrit, le dernier rapport de sa session et l'état des comptes : **À jour**, **En attente de l'utilisateur** (le Mac les installe lorsque l'utilisateur est connecté), **Non appliqué** avec les raisons signalées par le Mac, ou **Aucun compte** lorsque la stratégie n'en contient aucun. Utilisez **Recharger** pour relire la liste.

Verrouillage d'activation

Le champ **Verrouillage d'activation** indique si le verrouillage d'activation est activé. Lorsqu'il est activé, un appareil effacé ne peut être configuré à nouveau qu'avec le compte Apple de l'utilisateur ou avec le code de contournement de l'appareil. Les appareils supervisés n'activent le verrouillage d'activation que s'il est autorisé dans **Réglages de l'appareil**. Cerberus Enterprise demande aux appareils supervisés leur code de contournement et le stocke : utilisez **Afficher le code de contournement** dans le menu du champ pour le consulter (seuls les administrateurs le peuvent, et chaque consultation est enregistrée dans le journal système), puis saisissez-le comme mot de passe sur l'écran de verrouillage d'activation de l'appareil, en laissant le compte Apple vide.

Verrouillage de récupération et mot de passe du microprogramme (Mac)

Un Mac avec Apple silicon affiche le champ **Verrouillage de récupération**, un Mac à processeur Intel le champ **Mot de passe du microprogramme**. Les deux protègent le Mac au démarrage : avec le verrouillage de récupération, recoveryOS demande le mot de passe ; avec un mot de passe du microprogramme, le Mac le demande pour démarrer depuis un autre disque ou depuis la récupération. Le champ indique si le Mac signale un mot de passe et, dans son infobulle, quand Cerberus Enterprise l'a stocké et quand il a été vérifié pour la dernière fois.

- **Définir ou modifier le mot de passe** : Cerberus Enterprise génère un mot de passe de 20 lettres situées sur les mêmes touches quel que soit la disposition du clavier, ou un administrateur le saisit (8 à 64 caractères sans accents ; les autres rôles peuvent uniquement en générer un, car ils ne peuvent pas voir les mots de passe stockés). Le mot de passe est stocké chiffré avant d'être envoyé et ne remplace celui qui est stocké que lorsque le Mac le confirme. Si le Mac possède déjà un mot de passe défini en dehors de Cerberus Enterprise, saisissez-le comme mot de passe actuel : il est utilisé une seule fois et n'est pas stocké.
- **Vérifier le mot de passe** : demande au Mac si le mot de passe stocké est correct. Le résultat figure dans l'infobulle et dans le journal système.
- **Afficher le mot de passe** : seuls les administrateurs peuvent voir le mot de passe stocké, et chaque consultation est enregistrée dans le journal système. Les mots de passe générés sont affichés par groupes de quatre lettres : saisissez-les sans espaces.
- **Effacer le mot de passe** : supprime le mot de passe du Mac.

Un Mac à processeur Intel redémarre pour appliquer une modification du mot de passe du microprogramme : jusque-là, l'ancien mot de passe reste nécessaire (Afficher le mot de passe l'indique) et aucune autre modification ne peut être envoyée. Apple n'accepte également qu'une seule commande de mot de passe du microprogramme toutes les 30 secondes. Les mots de passe sont masqués dans l'historique des commandes.

Lorsqu'un Mac quitte la gestion (désinscrit, retiré par l'utilisateur ou effacé), macOS supprime le verrouillage de récupération de lui-même et Cerberus Enterprise abandonne le mot de passe de verrouillage de récupération stocké ; il fait de même lorsque le Mac signale qu'il n'a pas de verrouillage de récupération, par exemple après une nouvelle inscription. Lorsque vous désinscrivez un Mac (ou supprimez sa stratégie), un mot de passe du microprogramme stocké est d'abord effacé, le Mac redémarre puis quitte la gestion. Si l'effacement échoue, le Mac quitte la gestion malgré tout et le mot de passe reste stocké afin que vous puissiez encore le consulter. Un Mac retiré de la gestion par l'utilisateur, ou effacé, conserve son mot de passe du microprogramme : Cerberus Enterprise le conserve aussi. La suppression de l'enregistrement de l'appareil supprime le mot de passe stocké ; il vous est donc demandé de confirmer au préalable : notez le mot de passe, car sans lui, seul Apple peut le supprimer.

FileVault (Mac)

Le champ **FileVault** indique si le disque du Mac est chiffré et, dans son infobulle, si Cerberus Enterprise conserve sa clé de récupération personnelle. Un Mac envoie la clé lorsque FileVault est activé après avoir reçu le réglage FileVault de sa stratégie (voir la page **macOS** des stratégies Apple).

- **Afficher la clé de récupération** : seuls les administrateurs peuvent voir la clé, et chaque consultation est enregistrée dans le journal système. Utilisez-la à la fenêtre de connexion du Mac pour réinitialiser le mot de passe de l'utilisateur, ou en mode récupération pour déverrouiller le disque. Elle reste disponible après que le Mac a quitté la gestion ; la suppression de l'enregistrement de l'appareil la supprime.
- **Modifier la clé de récupération** : le Mac remplace sa clé de récupération personnelle et envoie la nouvelle, chiffrée ; l'ancienne clé cesse de fonctionner. Cela n'est possible que lorsque la clé stockée peut être lue : le Mac est déverrouillé avec celle-ci et aucun mot de passe utilisateur n'est nécessaire. La clé stockée est masquée dans l'historique des commandes et supprimée du serveur dès que le Mac répond (ou après 7 jours sans réponse).

Bootstrap Token (Mac)

Un Mac avec macOS 10.15 ou ultérieur envoie son **Bootstrap Token** au serveur de gestion lorsqu'un utilisateur disposant d'un jeton sécurisé se connecte. Le serveur le conserve et le renvoie uniquement à ce Mac, qui l'utilise pour attribuer un jeton sécurisé aux nouveaux utilisateurs et, sur un Mac avec Apple silicon, pour installer des mises à jour logicielles et approuver des extensions de noyau sans demander de mot de passe administrateur. Personne ne peut voir le jeton, ni dans le tableau de bord ni ailleurs. Le champ **Bootstrap Token** indique son état :

- **Séquestré** : le serveur possède le jeton ; l'infobulle indique quand le Mac l'a envoyé.
- **Séquestré auparavant** : le jeton stocké a été envoyé avant la dernière inscription ou le dernier renouvellement du certificat MDM du Mac. Après un renouvellement, c'est normal : le jeton est conservé et le Mac ne l'envoie plus. Après une nouvelle inscription, il peut ne plus être valide : exécutez `sudo profiles install -type bootstraptoken` dans Terminal sur le Mac.
- **Non séquestré** : le Mac n'a pas encore envoyé de jeton. Pour l'envoyer maintenant, un administrateur du Mac exécute `sudo profiles install -type bootstraptoken` dans Terminal (`sudo profiles status -type bootstraptoken` indique s'il est séquestré).

L'infobulle indique également si le Mac autorise le jeton pour l'authentification. Les Mac configurés avec Automated Device Enrollment l'autorisent automatiquement ; sur les autres Mac avec Apple silicon, un utilisateur peut l'autoriser dans l'Utilitaire de sécurité au démarrage de recoveryOS. Les Mac Intel ne peuvent pas utiliser le jeton pour l'authentification (**Non pris en charge**), mais un jeton séquestré attribue tout de même un jeton sécurisé aux nouveaux utilisateurs. Chaque fois

qu'un Mac envoie, supprime ou demande son jeton, cela est enregistré dans le journal système.

État de l'appareil et mises à jour du système

Le panneau **État de l'appareil** affiche ce que l'appareil signale à son sujet : la version et la compilation du système, la progression d'une mise à jour logicielle (version en attente, échéance, origine du déclenchement, échecs), la présence d'un code d'accès et sa conformité à la stratégie, FileVault sur un Mac, l'état de la batterie et les comptes configurés sur l'appareil.

La liste **Mises à jour disponibles** affiche les mises à jour du système que l'appareil peut installer, collectées lors de l'inscription et chaque semaine. Utilisez **Rechercher des mises à jour** pour les demander maintenant, et **Installer** pour installer immédiatement une mise à jour (l'appareil redémarre, après confirmation) ou seulement la télécharger et laisser l'utilisateur l'installer. Cela fonctionne sur les iPhone et iPad supervisés et sur les Mac, jusqu'à iOS, iPadOS et macOS 26 : sur les versions ultérieures, et pour mettre à jour de nombreux appareils, utilisez les mises à jour obligatoires de la stratégie (voir la page **Mises à jour logicielles** des stratégies Apple).

Un Mac avec Apple silicon n'installe une mise à jour sans demander de mot de passe administrateur que lorsqu'il autorise son Bootstrap Token pour l'authentification et que le jeton est séquestré (voir Bootstrap Token ci-dessus). Sinon, la confirmation indique qu'un utilisateur devra peut-être saisir un mot de passe administrateur avant l'installation de la mise à jour.

Applications et inventaire

Le panneau **Applications** répertorie toutes les applications de l'appareil dans un seul tableau. L'état d'installation des applications installées par la stratégie ou par une commande est signalé en direct par l'appareil ; les versions, les tailles et les applications installées par l'utilisateur proviennent de la dernière liste d'applications, collectée lors de l'inscription et chaque semaine. Utilisez **Interroger l'appareil** pour la demander maintenant.

- **Gestion** : **Stratégie** pour les applications installées par la stratégie de l'appareil, **Géré** pour les applications installées avec une commande telle que **Installer l'application**, **Non géré** pour celles installées par l'utilisateur. L'application Cerberus Enterprise porte la puce **Installé par Cerberus**.
- **Nécessite votre attention** : applications dont l'installation a échoué, qui ont été refusées ou supprimées par l'utilisateur, ou qui attendent l'utilisateur. Ouvrez une ligne pour voir l'erreur ; les applications de stratégie en échec peuvent être réinstallées avec le bouton de nouvelle tentative. Les applications intégrées et les applications App Store que l'appareil signale comme non validées ne sont pas comptabilisées.
- **Supprimer l'application** : les applications gérées peuvent être supprimées, avec leurs données. Pour supprimer une application installée par la stratégie, retirez-la de la

stratégie. La stratégie envoie également cette commande d'elle-même lorsqu'un paquet Mac installé comme application gérée est retiré de la stratégie.

Le panneau **Profils, certificats et sécurité** affiche les profils de configuration, les certificats et l'état de sécurité (code d'accès, chiffrement, FileVault et pare-feu sur un Mac) signalés par l'appareil.

> Sur les appareils personnels, les applications installées par l'utilisateur ne sont pas collectées et seuls les profils et certificats gérés par Cerberus Enterprise sont répertoriés.

Le panneau **Modifications de l'inventaire** affiche ce qui a changé entre deux listes envoyées par l'appareil : applications installées, supprimées ou mises à jour (avec l'ancienne et la nouvelle version), profils installés, supprimés ou mis à jour, et certificats ajoutés ou supprimés. Une modification est détectée lorsque l'appareil envoie une nouvelle liste, chaque semaine pour les applications et les profils, chaque jour pour les certificats, ou lorsque vous utilisez **Interroger l'appareil** : la date affichée correspond au moment de la détection, la modification ayant eu lieu entre la liste précédente et celle-ci. La première liste d'un appareil, ainsi que la première après une nouvelle inscription ou un changement de propriétaire, est uniquement enregistrée comme point de départ. Recherchez par nom ou identifiant, et filtrez par type et par modification. Les modifications sont conservées pendant 365 jours.

> Lorsqu'une mise à jour du système remplace plusieurs applications Apple à la fois, elles sont affichées sur une seule ligne (par exemple "23 applications Apple mises à jour") que vous pouvez développer. Le renouvellement du certificat MDM est affiché comme **Certificat MDM renouvelé**. Sur les appareils personnels, seules les modifications des éléments gérés par Cerberus Enterprise sont affichées.

Colonnes de l'historique Apple

- **Date de création**
- **Commande**
- **Statut** : **Envoyé** (en attente de l'appareil, remis dès qu'il se connecte), **Réussi**, **Répondu** (ouvrez la ligne pour voir le résultat), **En attente de l'appareil** (l'appareil ne peut pas exécuter la commande pour le moment), **Échoué** (ouvrez la ligne pour voir la raison) ou **Annulé** (la file de commandes de l'appareil a été vidée, par exemple lors d'une nouvelle inscription).
- **Date d'exécution**

Actualiser

Utilisez l'action d'actualisation dans le panneau Commandes pour recharger l'historique des commandes.

Revision #53
Created 2025-12-18 17:34:03 UTC by Admin
Updated 2026-11-12 09:55:25 UTC by Admin