État de l'Appareil

- Présentation de l’appareil
- Carte de localisation
- Gestion des SIM
- Commandes

Présentation de l’appareil

Ouvrez un appareil depuis **Tableau de bord** → **Appareils** en cliquant sur la ligne de l’appareil. Le titre de la page affiche le **Modèle** de l’appareil (lorsqu’il est disponible) et l’**ID** interne.

Données historiques et inscription actuelle

Lorsqu’un appareil a plusieurs inscriptions, Cerberus Enterprise peut afficher un enregistrement historique en lecture seule. Dans ce cas, la page affiche une bannière **Données historiques** et un bouton pour revenir aux données de l’inscription actuelle.

Champs principaux

La section supérieure résume l’identité, l’attribution et l’état de gestion de l’appareil. Certains champs sont spécifiques à la plateforme et n’apparaissent que pour les appareils Android ou Apple.

- **ID** et **Modèle** : identifiants en lecture seule.
- **Utilisateur** : affiche l’utilisateur actuellement attribué (le cas échéant). Depuis le menu utilisateur, vous pouvez **Ouvrir l’utilisateur** ou **Changer d’utilisateur**, ou attribuer un utilisateur lorsqu’aucun n’est défini.
- **Mode de gestion** et **Propriété** : affichés avec des info-bulles dans l’interface.
- **État** : état actuel de l'appareil (avec l'icône et les détails dans l'infobulle). Un appareil en mode perdu affiche **Perdu** sur Android comme sur Apple, et une bannière en haut de la page indique la marche à suivre.
- **Profil ADE** (Apple uniquement) : affiche le profil Automated Device Enrollment attribué (le cas échéant) et vous permet de l’ouvrir ou de le modifier.
- **Stratégie** : affiche la stratégie attribuée et vous permet de l’ouvrir ou de la modifier, ou d’en attribuer une lorsqu’aucune n’est définie.
- **Statut de conformité de la stratégie** (lorsqu’une stratégie est attribuée) : indique si l’appareil est conforme.
- **Version de la stratégie** (lorsqu’une stratégie est attribuée) : indique si la dernière version de la stratégie a été appliquée sur l’appareil.
- **Application Cerberus Enterprise** (iPhone et iPad uniquement) : l'état de l'application Cerberus Enterprise que Cerberus installe sur l'appareil. **Non disponible** (iOS ou iPadOS antérieur à 18.4, absence de numéro de série sur un appareil d'entreprise ou absence de

Managed Apple Account sur un appareil personnel) ; **Pas encore disponible sur les appareils personnels** ; **En attente des informations de l'appareil** ; **En attente de la licence utilisateur du Managed Apple Account** (appareils personnels, pendant qu'Apple confirme la licence) ; **Non installée** (l'application n'est pas dans votre bibliothèque Apple Business ou Apps and Books n'est pas configuré, avec un lien vers **Paramètres du compte**) ; **Installée · Apps and Books nécessite votre attention** (le jeton a expiré ou l'application a quitté votre bibliothèque : l'application reste installée) ; **Configuration indisponible** ; **Installation…** (si l'appareil n'envoie aucun rapport d'état pendant 30 minutes, l'infobulle suggère de vérifier qu'il est en ligne et de le redémarrer, ce qui relance généralement l'installation) ; **En attente de l'approbation de l'utilisateur** ; **L'utilisateur a refusé** et **Échec de l'installation** (les deux avec **Réessayer**, qui interroge à nouveau l'appareil) ; **Installée · en attente du démarrage de l'application** (l'application n'a pas encore été ouverte) ; **Installée · configuration non acceptée** ; et, une fois l'application enregistrée, sa version, son dernier contact et l'état des notifications.

- **Inscrit le** et **Dernier rapport de statut** : horodatages de l'inscription et du dernier statut signalé.
- **Désinscrit le** : affiché lorsque l'appareil a été désinscrit.

> Certaines données et certains panneaux ne sont disponibles que si la catégorie correspondante est activée dans la stratégie de l'appareil. Pour plus d'informations, consultez les pages **Signalement de l'état** et **Localisation et géorepérage**.

Panneaux

La page de l'appareil est organisée en sections extensibles. Selon la plateforme et l'état, vous pouvez voir un ou plusieurs des panneaux suivants :

- **Carte de localisation** : un panneau à onglets présentant l'historique de **Localisation** de l'appareil actuel et, sur les appareils Android, les iPhone et les iPad, un onglet **Zones géographiques** pour les transitions de zones géographiques.
- **Gestion des SIM** : EID de l'appareil et SIM et eSIM installées. Sur Android également les commandes eSIM et leur historique ; sur les iPhone et les iPad cellulaires appartenant à l'entreprise également l'itinérance des données, le partage de connexion et **Actualiser les forfaits cellulaires**. Consultez la page **Gestion des SIM** dédiée.
- **Commandes** : envoyez des commandes à l'appareil et consultez l'historique des commandes (selon la plateforme).
- **Posture de sécurité** : l'état de sécurité de l'appareil et ses risques. Sur Android également, le verdict Play Integrity. Tant que l'appareil ne l'a pas signalé, il indique **Non spécifié**, ou **Pas encore signalé** sur un appareil Android qui n'a envoyé aucune donnée de sécurité.

- **Pourquoi l'appareil est non conforme** : affiché uniquement lorsque l'appareil est non conforme, avec une icône d'alerte rouge ; ouvrez-le pour voir les raisons. Sur Android, il liste les paramètres de stratégie non conformes ; sur Apple, il indique aussi si une règle de conformité a bloqué l'appareil.
- **État de l’appareil** (Apple uniquement) : version du système, progression de la mise à jour logicielle, code d’accès, FileVault, batterie et comptes signalés par l’appareil, ainsi que les mises à jour du système disponibles pour celui-ci. Consultez la page **Commandes** .
- **Applications** (Android) : applications installées et leurs commentaires et rapports d'erreur.
- **Applications** (Apple uniquement) : les applications installées par la stratégie, les applications installées avec des commandes et les applications installées par l’utilisateur, avec leur état d’installation, leurs erreurs et leurs actions (réessayer, supprimer). Sur les Mac, elle répertorie également les paquets installés par la stratégie, avec leur état et **Réinstaller** ; les paquets installés comme applications gérées portent une puce **Géré**, et une note indique quand un paquet a été installé sans gestion et pourquoi, ou quand son application n’a pas été trouvée une heure après le téléchargement. Sur les iPhone et les iPad, l’application Cerberus Enterprise porte la puce **Installée par Cerberus** ; elle n’est pas répertoriée sous le filtre **Stratégie**. Une application dont la configuration gérée n’a pas été acceptée par l’appareil porte la puce **Configuration non acceptée**. Sur les iPhone et les iPad personnels (inscription utilisateur), une ligne indique le compte Apple géré dont les licences utilisateur sont utilisées par les applications App Store, les applications en attente de leur licence affichent **En attente d’une licence utilisateur** ou **Échec de la licence utilisateur**, une application dont l’utilisateur a annulé l’invite d’installation affiche **En attente de l’approbation de l’installation par l’utilisateur**, et **Redemander** demande à nouveau la licence à Apple ou réaffiche l’invite. Consultez la page **Commandes**.
- **Profils, certificats et sécurité** (Apple uniquement) : profils de configuration, certificats et état de sécurité signalés par l’appareil.
- **Modifications de l’inventaire** (Apple uniquement) : une chronologie des applications, profils et certificats installés, supprimés ou mis à jour sur l’appareil, avec recherche et filtres par type et par modification. Consultez la page **Commandes**.
- **Utilisateurs de l'iPad partagé** et **Utilisateurs du Mac** (Apple uniquement) : les utilisateurs d'un iPad partagé et les utilisateurs d'un Mac. Consultez la page **Commandes**.
- **Rapports de statut** : données supplémentaires signalées par l’appareil, affichées sous forme d’arborescence de catégories et de valeurs.
- **Historique des inscriptions** : inscriptions précédentes pour ce même appareil physique, affichées sous forme de liste.

Onglets du panneau de localisation

Le panneau **Carte de localisation** utilise des onglets pour séparer l'historique des positions et les transitions de géorepérage.

- **Localisation** : affiche les filtres d’historique, une recherche par plage de dates, les repères de localisation, le cercle de précision et les commandes de suivi en direct pour l’appareil actuel.
- **Zones géographiques** (Android, iPhone et iPad) : affiche l’historique des transitions de zones géographiques sur une carte dédiée, avec des filtres de période, une option pour inclure les zones archivées et une liste latérale des transitions. Sur les iPhone et les iPad, une ligne d’état indique également quand la géolocalisation par zones ne peut pas fonctionner sur l’appareil.

Pour connaître le comportement complet de ces onglets, consultez **Carte de localisation**.

Actions

En bas de la page, vous pouvez actualiser les données et effectuer des actions selon la plateforme, l’état de l’appareil et le statut de la licence.

- **Actualiser les données** : recharge l’enregistrement de l’appareil.
- **Désactiver l’appareil** / **Activer l’appareil** (Android uniquement) : disponible dans les états pris en charge.
- **Désinscrire l’appareil** : retire la gestion de l’appareil. Le comportement exact dépend de la plateforme et de la propriété (par exemple, Android peut effacer un profil professionnel ou réinitialiser l’appareil).
- **Supprimer l’appareil** : disponible lorsque l’appareil est déjà désinscrit et que son enregistrement peut être supprimé.

Carte de localisation

Cette page documente les outils de localisation propres à l'appareil disponibles dans **Présentation de l'appareil**. Le panneau contient un onglet **Localisation** pour l'historique des positions et, sur les appareils Android, les iPhone et iPad, un onglet **Geofencing** pour les transitions de geofencing.

Prérequis

Sur Android, les données de localisation de l'appareil ne sont affichées que si le signalement de la localisation est activé dans la stratégie de l'appareil. Pour l'activer, ouvrez la stratégie et activez **Localisation et géorepérage → Signaler la localisation**. Pour plus de détails, consultez **Localisation et géorepérage**.

Sur les iPhone et iPad, la position provient de l'application Cerberus Enterprise, une fois que l'utilisateur l'autorise, ou de la commande **Localiser l'appareil** lorsque l'appareil est en mode perdu. Les Mac et les autres appareils Apple ne signalent pas leur position.

> Sur les appareils qui ne sont pas entièrement gérés, les données de localisation peuvent encore dépendre de l'autorisation de localisation accordée à l'application Cerberus Enterprise et de l'activation des services de localisation sur l'appareil.

> Sur les appareils personnels (User Enrollment), la localisation et le geofencing ne sont disponibles que lorsque la stratégie Apple a l'option **Localisation et geofencing sur les appareils personnels** activée, et uniquement si l'utilisateur autorise la localisation pour l'application Cerberus Enterprise. Sinon, la page de leur appareil n'affiche pas les actions de localisation ni le suivi en direct. Le mode perdu n'est jamais disponible sur les appareils personnels.

> Pour la carte globale multi-appareils disponible depuis le tableau de bord, consultez **Carte de localisation du tableau de bord**.

État de chargement et d'absence de données

- Pendant le chargement des données de localisation, le panneau affiche une superposition de chargement sur la carte.
- Si l'appareil n'a aucune donnée de localisation disponible, le panneau affiche un message indiquant **Aucune donnée de localisation disponible**. Sur Android, il ajoute un rappel pour activer la transmission de la localisation dans la stratégie attribuée lorsqu'elle est désactivée. Sur Apple, il indique d'où provient la position ou que ce type d'appareil ne la signale pas.
- Si un filtre de date est actif et qu'aucun échantillon ne correspond, le panneau affiche **Aucune donnée disponible dans la plage de dates sélectionnée**.

Onglet Localisation

Ouvrez l'onglet **Localisation** pour consulter l'historique d'un seul appareil. Les filtres disponibles incluent la dernière position connue, des plages d'historique récentes, une plage de dates personnalisée et le suivi en direct.

- **Dernière** : affiche la dernière position connue.
- **Aujourd'hui**, **7 derniers jours** et **30 derniers jours** : affichent les positions enregistrées pour la période sélectionnée.
- **Rechercher** : permet de choisir une plage de dates personnalisée.
- **Direct** : démarre ou arrête le suivi en direct de l'appareil actuel.

> Les positions sont conservées **90 jours** : les plus anciennes sont supprimées automatiquement chaque nuit. La dernière position de chaque appareil inscrit est toujours conservée, de sorte que l'appareil reste sur les cartes même s'il n'a pas envoyé de position depuis longtemps. Pour les appareils supprimés et les inscriptions passées, toutes les positions de plus de 90 jours sont supprimées. C'est pourquoi la plage de dates du filtre **Rechercher** ne peut pas commencer il y a plus de 90 jours.

Détails du marqueur

Lorsque vous cliquez sur un marqueur de localisation, une fenêtre d'informations s'ouvre avec :

- Horodatage de l’enregistrement de localisation.
- La **précision** signalée (en mètres).
- La **vitesse** signalée, lorsque l’appareil la fournit.
- Le **cap** ou le relèvement signalé, lorsque l’appareil le fournit.

Cercle de précision

Lorsque la fenêtre d’informations est ouverte, un cercle de précision s’affiche autour du repère. Le rayon du cercle correspond à la précision signalée (en mètres). La fermeture de la fenêtre d’informations masque le cercle.

Suivi en direct

Dans la vue de l’historique de l’appareil, la sélection du filtre **En direct** démarre une demande de suivi en temps réel pour cet appareil spécifique. Cerberus Enterprise demande une confirmation avant de démarrer la demande.

- Le suivi en direct dure jusqu’à **15 minutes**.
- Pendant le suivi en direct, les appareils Android affichent une notification et les iPhone et les iPad affichent l’indicateur de localisation.
- Pendant le suivi en direct, le panneau actualise en continu la dernière position et l’indicateur en direct reste visible.
- Sélectionner à nouveau le filtre En direct vous permet d’arrêter le suivi en direct avant la fin du délai.
- Sur **iPhone et iPad**, le suivi en direct s’effectue via l’application Cerberus Enterprise, avec l’accès à la localisation réglé sur **Toujours**. La demande réveille normalement l’application même lorsqu’elle n’est pas ouverte, et l’application envoie ensuite les positions pendant toute la session. iOS ne garantit pas ces demandes : il peut les retarder ou ne pas les livrer, par exemple en mode Économie d’énergie ou sans connexion réseau. Si aucune position n’arrive dans les 2 minutes, le tableau de bord annule la demande : demandez à l’utilisateur d’ouvrir l’application une fois, puis réessayez.

Onglet Zones géographiques

Sur les appareils Android, les iPhone et les iPad, le deuxième onglet affiche les transitions de zones géographiques générées à partir des zones géographiques définies dans la stratégie attribuée.

- La carte affiche les zones géographiques actuelles ainsi que les points de transition enregistrés.

- La liste des transitions à droite vous permet d’examiner les événements **d’entrée** et **de sortie**.
- Les filtres disponibles sont **Aujourd’hui**, **7 derniers jours**, **30 derniers jours** et une recherche personnalisée par plage de dates.
- **Inclure les archives** affiche également les transitions liées à d’anciennes définitions de zones géographiques qui ne sont plus présentes dans la stratégie actuelle.
- Les transitions de zones géographiques sont conservées **90 jours** et les plus anciennes sont supprimées automatiquement chaque nuit : la recherche par plage de dates personnalisée ne peut donc pas commencer il y a plus de 90 jours.

Sur les iPhone et les iPad, lorsque la stratégie comporte des zones géographiques actives, une ligne d’état en haut de l’onglet indique si la géolocalisation par zones fonctionne sur l’appareil. Elle vous informe lorsque cela ne peut pas fonctionner : l’application Cerberus Enterprise n’a pas contacté le serveur ou doit être mise à jour, l’accès à la localisation n’est pas réglé sur **Toujours**, **Position précise** ou **Actualisation des apps en arrière-plan** est désactivé, **Mode économie d’énergie** était activé lors du dernier rapport de réglages de l’application (les événements et changements de zones peuvent alors être retardés de plusieurs heures), ou l’application n’a pas encore appliqué les dernières zones géographiques. Lorsque tout fonctionne, elle indique combien de zones géographiques l’application surveille.

Détails de la transition de zone géographique

La sélection d’une transition ouvre ses détails sur la carte et met en évidence l’entrée correspondante dans la liste. Lorsqu’elles sont disponibles, Cerberus Enterprise affiche également les coordonnées de l’appareil et la précision signalée pour cette transition.

Gestion des SIM

La page de l'appareil propose un panneau **Gestion des SIM**. Sur les appareils Android, il gère les SIM et les profils eSIM installés sur l'appareil, ajoute ou supprime des profils eSIM et affiche l'historique des commandes eSIM envoyées à l'appareil. Sur les iPhone et iPad cellulaires d'entreprise, il affiche les SIM et les forfaits eSIM signalés par l'appareil et permet à l'appareil de télécharger les forfaits eSIM préparés par l'opérateur : voir **iPhone et iPad** ci-dessous.

> Les informations SIM sont signalées par les appareils entièrement gérés lorsque la communication des **Informations réseau** est activée dans la stratégie de l'appareil (cette option est toujours activée par Cerberus Enterprise). Consultez la page **Communication du statut**.

EID de l'appareil

L'EID (eUICC Identifier) identifie le matériel eSIM de l'appareil. Les opérateurs l'utilisent pour associer les profils eSIM à l'appareil ; sa récupération constitue donc généralement la première étape d'un flux de provisionnement eSIM.

- **Appareils appartenant à l'entreprise** (Android 13 et versions ultérieures) : l'EID est signalé automatiquement avec l'état de l'appareil et aucune interaction de l'utilisateur n'est requise.
- **Appareils personnels** (Android 13 et versions ultérieures) : utilisez le bouton **Demander l'EID**. L'utilisateur verra une notification sur l'appareil lui demandant de partager l'EID et pourra approuver ou refuser la demande. L'EID n'est affiché que si l'utilisateur approuve. Tant que la demande est en attente, le bouton reste désactivé.

> L'envoi d'une demande d'EID affiche d'abord une boîte de dialogue de confirmation, car l'utilisateur verra une notification sur l'appareil.

SIM installées

Le tableau **SIM installées** répertorie les SIM actuellement connues pour l'appareil, y compris les SIM physiques et les profils eSIM. Sur les appareils personnels, les profils eSIM installés avec la commande **Ajouter une eSIM** sont affichés même lorsque l'appareil ne signale pas les

informations SIM.

- **Opérateur** : le nom de l’opérateur associé à la SIM (lorsqu’il est signalé).
- **Numéro de téléphone** : le numéro de téléphone associé à la SIM (lorsqu’il est signalé).
- **ICCID** : l’identifiant de carte à circuit intégré de la SIM.
- **État d’activation** : indique si l’eSIM est activée ou non. Signalé uniquement pour les eSIM sous Android 15 et versions ultérieures.
- **Mode de configuration** : indique si l’eSIM a été configurée par un administrateur ou par l’utilisateur. Signalé uniquement pour les eSIM sous Android 15 et versions ultérieures.
- **Type de SIM** : indique si l’appareil signale l’entrée comme une eSIM.

> Les eSIM faisant l’objet d’une commande de suppression en cours ou exécutée (non échouée) affichent un état d’activation **Suppression en cours** temporaire. L’entrée disparaît de la liste lorsque l’appareil signale la liste de SIM mise à jour. Pendant une suppression en cours, le bouton de suppression n’est pas disponible, afin d’éviter d’envoyer deux fois la même commande.

Supprimer une eSIM

Utilisez le bouton de suppression à côté d’une eSIM installée pour supprimer son profil de l’appareil. Une boîte de dialogue de confirmation vous demande de confirmer l’ICCID de l’eSIM à supprimer avant l’envoi de la commande. La suppression d’une eSIM est prise en charge sous Android 15 et versions ultérieures.

Ajouter une eSIM

La section **Ajouter une eSIM** installe un nouveau profil eSIM sur l’appareil (prise en charge sous Android 15 et versions ultérieures). Elle nécessite :

- **Validité** : la durée pendant laquelle la commande est valide si elle ne peut pas être exécutée immédiatement.
- **Code d’activation** : le code d’activation du profil eSIM, fourni par l’opérateur. Vous pouvez saisir le code complet, ou uniquement l’adresse SM-DP+ pour permettre à l’appareil de découvrir un profil que l’opérateur a déjà associé à son EID.
- **État d’activation** : indique si le profil eSIM doit être activé automatiquement après le téléchargement, ou laissé désactivé pour une activation manuelle par l’utilisateur.

Historique des commandes

Sous la section Ajouter une eSIM, le panneau affiche l'historique des commandes eSIM envoyées à l'appareil : **Ajouter une eSIM**, **Supprimer une eSIM** et **Demander l'EID**. Le tableau est triable et prend en charge la pagination. Certaines lignes peuvent être développées pour consulter les paramètres de la commande (par exemple le code d'activation ou l'ICCID) et l'état d'exécution, y compris les détails de l'erreur eSIM lorsqu'une opération échoue sur l'appareil.

- **Date de création**
- **Commande**
- **Validité**
- **État**
- **Erreur** : affiche l'état d'erreur eSIM (par exemple *Utilisateur refusé*, *Code d'activation non valide* ou *ICCID introuvable*) lorsque l'exécution de la commande le signale.
- **Date d'exécution**

Effacer les eSIM lors de l'effacement et de la désinscription

Lorsque vous effacez l'appareil depuis le panneau Commandes, l'option **Effacer les eSIM** détermine si les profils eSIM sont supprimés lors de l'effacement. Sur les appareils personnels dotés d'un profil professionnel, cette option est activée par défaut (les eSIM gérées sont supprimées, les eSIM personnelles ne sont pas affectées). La même option est disponible dans la boîte de dialogue de confirmation **Désinscrire l'appareil**.

iPhone et iPad

Le panneau est affiché pour les iPhone et pour les iPad ayant signalé des données cellulaires (un iPad Wi-Fi uniquement n'en a aucune), uniquement lorsque l'appareil appartient à l'entreprise et ne relève pas d'une inscription utilisateur. Les informations cellulaires de l'appareil sont demandées avec les informations de l'appareil : lors de l'inscription, chaque jour, avec **Actualiser les informations de l'appareil**, lorsque son propriétaire devient l'entreprise, et quelques minutes après **Actualiser les forfaits cellulaires**.

- **EID de l'appareil** : l'EID signalé avec les SIM, avec un bouton pour le copier à l'intention de l'opérateur. Si l'appareil ne le signale pas, l'utilisateur le trouve dans Réglages > Général > À propos.
- **Signalé**, **Itinérance des données**, **Partage de connexion** et **Micrologiciel du modem** : la réponse de l'appareil et l'état qu'il a signalé. L'itinérance des données et le partage de connexion peuvent être modifiés avec **Réglages de l'appareil** dans le panneau Commandes, qui affiche également l'état actuel.

- **SIM** : une ligne par SIM ou forfait eSIM (les appareils double SIM en ont deux), avec l'emplacement tel que signalé par l'appareil, son libellé et son type (**eSIM** lorsque l'appareil signale l'EID avec, **Carte SIM** sinon), l'opérateur (l'opérateur d'origine dans une info-bulle lorsque l'appareil est en itinérance sur un autre réseau), le numéro de téléphone, l'ICCID, l'EID, l'IMEI, la SIM utilisée pour les données et pour les appels, et l'itinérance. Un emplacement eSIM sans forfait est affiché en grisé sous la forme **Aucun forfait**.
- **Cet appareil n'a signalé aucune SIM** signifie que l'appareil a répondu sans aucune SIM ; **Aucune information cellulaire pour l'instant** signifie qu'il n'a pas encore répondu : utilisez **Actualiser les informations de l'appareil**.

> Les numéros de téléphone, l'ICCID, l'IMEI et l'EID identifient la personne et la ligne : ils ne sont jamais demandés aux appareils personnels ni aux inscriptions utilisateur. Lorsqu'un appareil devient personnel, les informations sont supprimées immédiatement et masquées dans les résultats des anciennes commandes d'informations de l'appareil, dans l'historique des commandes. Elles ne sont pas exportées et ne sont pas écrites dans les journaux système.

Actualiser les forfaits cellulaires

Les iPhone et les iPad ne peuvent pas installer une eSIM à partir d'un code d'activation. L'opérateur associe (réserve) le forfait eSIM à l'EID de l'appareil sur son serveur eSIM (SM-DP+) et vous fournit l'adresse de ce serveur ; **Actualiser les forfaits cellulaires** demande alors à l'appareil de télécharger les forfaits qui l'attendent. Le bouton **Actualiser les forfaits cellulaires** du panneau sélectionne la commande dans le panneau Commandes, où vous saisissez l'**URL du serveur eSIM de l'opérateur** :

- **Une adresse https://**, envoyée telle quelle. Les adresses avec http://, un nom d'utilisateur ou un mot de passe, ou une partie # ne sont pas acceptées.
- **Un nom d'hôte**, par exemple *smdp.carrier.example*, envoyé sous la forme https://smdp.carrier.example.
- **Un code d'activation LPA** (LPA:1$server$code, le texte d'un QR code eSIM) : seul le serveur est utilisé, car la commande ne peut pas transporter le code. Le forfait doit être associé à l'EID de l'appareil par l'opérateur, sinon l'appareil ne trouve rien à télécharger.

L'appareil installe et active le forfait sans demander à l'utilisateur, y compris lorsqu'il n'est pas supervisé. Un succès dans l'historique des commandes signifie que l'appareil a accepté la demande, et non qu'un forfait a été installé : l'installation peut prendre jusqu'à trois minutes, et Cerberus Enterprise redemande ses SIM à l'appareil environ trois minutes plus tard, afin que le nouveau forfait apparaisse dans le panneau. Les erreurs 36001 (l'appareil n'a pas pu joindre son système cellulaire), 36002 (aucune prise en charge des eSIM) et 36003 (système cellulaire occupé, réessayez plus tard) sont expliquées dans les journaux système. Un forfait téléchargé une fois ne peut pas être téléchargé à nouveau : si l'installation échoue, contactez l'opérateur. La commande

est également disponible pour plusieurs appareils à la fois dans le menu **Actions pour appareils Apple** de la page Appareils.

Ce qu’Apple n’autorise pas

- **Ajouter une eSIM** à partir d’un code d’activation : impossible, utilisez **Actualiser les forfaits cellulaires** avec un forfait associé à l’EID.
- **Supprimer une eSIM** : une eSIM ne peut pas être supprimée à distance une par une. L’effacement de l’appareil avec l’option **Conserver le forfait de données eSIM** désactivée supprime toutes les eSIM. Pour arrêter un seul forfait, demandez à l’opérateur de le désactiver : le forfait reste sur l’appareil mais ne peut pas se connecter.
- **Demander l’EID** : inutile, l’EID est fourni avec les SIM des appareils appartenant à l’entreprise.
- **Les Mac** ne disposent d’aucune gestion cellulaire ou eSIM.

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.