Inscription pilotée par le compte Apple

Avec l’inscription pilotée par le compte, les utilisateurs inscrivent leur iPhone, iPad ou Mac en se connectant avec leur compte professionnel (un **compte Apple géré**, par exemple *name@company.com*) dans les réglages de l’appareil. Aucun profil à télécharger et aucun QR code : Cerberus Enterprise trouve l’utilisateur, applique la stratégie et définit lui-même la propriété.

Deux modes

- **Inscription utilisateur** (appareils personnels) : seules les applications, les comptes et les données professionnels sont gérés, dans une zone distincte de l’appareil. Cerberus ne peut pas voir les données personnelles, effacer l’appareil, le localiser ni lire son numéro de série. L’appareil est défini comme personnel. Nécessite iOS et iPadOS 15 ou macOS 14 ou version ultérieure.
- **Inscription d’appareil** (appareils d’entreprise qui ne figurent pas dans Apple Business) : l’appareil entier est géré, comme avec une inscription manuelle. Un Mac inscrit de cette manière est supervisé ; un iPhone ou un iPad ne l’est pas. L’appareil est défini comme appartenant à l’entreprise. Nécessite iOS et iPadOS 17.1 ou macOS 14.1 ou version ultérieure.

> Vous choisissez le mode pour iPhone et iPad et, séparément, pour Mac : par exemple l’inscription utilisateur pour les iPhone personnels et l’inscription d’appareil pour les Mac. Vous pouvez modifier ultérieurement la propriété d’un appareil sur la page de l’appareil.

> L’inscription pilotée par le compte est disponible lorsque Apple Management (APNs) est configuré. Si vous n’avez pas encore terminé la configuration APNs, consultez **Configuration d’Apple Management (APNs)**.

Configurer Apple Business

Les utilisateurs se connectent avec des comptes Apple gérés, créés dans Apple Business. Avant de commencer :

1. **Vérifiez votre domaine** (par exemple *company.com*) dans Apple Business, dans les domaines de votre organisation.
2. **Créez les comptes Apple gérés** de vos utilisateurs, ou connectez Apple Business à Google Workspace ou Microsoft Entra ID : le compte de chaque utilisateur correspond alors à son adresse e-mail professionnelle et il se connecte avec son mot de passe.
3. Pour l'inscription utilisateur, vérifiez dans les réglages de gestion des accès que les comptes Apple gérés peuvent se connecter sur des **appareils personnels** : lorsqu'ils ne peuvent se connecter que sur des appareils supervisés, l'inscription utilisateur échoue.
4. Uniquement pour l'option **Apple Business** ci-dessous : ouvrez **Appareils → Services de gestion → Attribution de l'appareil par défaut** (Modifier) et choisissez le service de gestion d'appareils Cerberus Enterprise pour iPhone, iPad et Mac.

> Conservez le service de gestion d'appareils Cerberus Enterprise et son jeton dans Apple Business tant que des appareils sont inscrits avec des comptes Apple gérés : leur suppression peut empêcher les comptes de fonctionner sur les appareils.

Configurer Cerberus Enterprise

Ouvrez la section **Inscription** du tableau de bord et sélectionnez l'onglet **Connexion au compte Apple**. Une liste de contrôle en haut indique ce qui manque encore. Seuls les administrateurs peuvent modifier les réglages.

- **Autoriser l'inscription en se connectant avec un compte professionnel** : active ou désactive l'inscription pilotée par le compte pour l'ensemble de l'organisation.
- **Domaines** : les domaines des comptes de vos utilisateurs (par exemple *company.com*), jusqu'à 20. Seuls les comptes de ces domaines peuvent s'inscrire, et uniquement après vérification du domaine (voir ci-dessous).
- **iPhone et iPad** et **Mac** : Désactivé, Inscription utilisateur ou Inscription d'appareil pour chaque famille d'appareils.
- **Stratégie** de chaque mode : appliquée aux appareils dès leur inscription. Sans stratégie, les appareils s'inscrivent sans stratégie. Une stratégie modifiée s'applique aux inscriptions suivantes.
- **Utilisateurs** : *Uniquement les utilisateurs existants* (l'adresse e-mail d'un utilisateur dans Cerberus Enterprise doit correspondre au compte saisi sur l'appareil), ou *Créer un utilisateur pour les comptes des domaines qui n'en ont pas*.

> Le compte saisi sur l'appareil est mis en correspondance avec le champ **Compte Apple géré** des utilisateurs, puis avec leur adresse e-mail. Le code est toujours envoyé à l'adresse e-mail de l'utilisateur. Un compte Apple géré défini sur un utilisateur peut s'inscrire même lorsque son domaine n'est pas vérifié dans Cerberus, par exemple un compte du domaine réservé *org.appleid.com* d'Apple Business. Avec la découverte de service Apple Business, les

utilisateurs saisissent toujours leur compte Apple géré.

Vérifier les domaines

Une fois les réglages enregistrés, la section **Vérification du domaine** affiche un enregistrement TXT pour chaque domaine. Ajoutez-le au DNS du domaine, puis cliquez sur **Vérifier**. Les modifications DNS peuvent prendre un certain temps avant d'être visibles. Un domaine vérifié reste vérifié : vous pouvez supprimer l'enregistrement par la suite. Les utilisateurs d'un domaine non vérifié ne peuvent pas s'inscrire.

Découverte de service : comment les appareils trouvent Cerberus Enterprise

Lorsqu'un utilisateur se connecte, l'appareil demande au domaine du compte (par exemple *https://company.com*) quel serveur le gère. Configurez au moins l'une de ces trois options. La section **Découverte de service** de l'onglet affiche l'URL de découverte de votre organisation et le texte exact à copier pour chaque option.

Option 1 : Apple Business (recommandée)

Cliquez sur **S'inscrire dans Apple Business** : Cerberus Enterprise stocke son URL de découverte dans votre organisation Apple Business et rien ne doit être publié sur vos domaines. **Vérifier dans Apple Business** affiche l'URL qu'Apple Business possède actuellement, et **Supprimer d'Apple Business** la supprime.

- Nécessite iOS et iPadOS 18.2 ou macOS 15.2 ou version ultérieure. Les appareils plus anciens ont besoin de l'option 2 ou 3.
- Nécessite Apple Business connecté dans Cerberus Enterprise (jeton de service Automated Device Enrollment) et l'attribution d'appareil par défaut décrite ci-dessus.
- L'appareil n'interroge Apple Business que lorsque votre domaine ne répond pas : l'adresse *https://company.com/.well-known/com.apple.remotemanagement* ne doit pas exister (une erreur telle que « not found »). Si votre site web y répond par une page web, les appareils s'arrêtent là. Utilisez **Vérifier la configuration** pour voir ce qu'il répond.

> Apple Business conserve une seule URL de découverte par organisation : l'inscrire envoie tous les comptes Apple gérés de l'organisation vers cette organisation Cerberus Enterprise. Ne l'inscrivez pas depuis deux organisations Cerberus Enterprise qui utilisent la même organisation Apple Business.

Option 2 : redirection depuis votre site web

Sur le serveur web de chaque domaine, redirigez */.well-known/com.apple.remotemanagement* vers l'URL de découverte de votre organisation, **en conservant la chaîne de requête** (elle contient le compte saisi par l'utilisateur). Cela fonctionne avec toutes les versions du système qui prennent en charge l'inscription pilotée par le compte, et le mode peut être différent pour iPhone et Mac. Copiez le texte pour Apache ou nginx depuis l'onglet ; il ressemble à ceci, avec la clé de votre organisation :

Apache (.htaccess ou hôte virtuel) :

```
RewriteEngine On
RewriteRule ^\.well-known/com\.apple\.remotemanagement$
https://enterprise.cerberusapp.com/account-enroll/YOUR-KEY/discovery [R=302,L,QSA]
```

nginx :

```
location = /.well-known/com.apple.remotemanagement {
    return 302 https://enterprise.cerberusapp.com/account-enroll/YOUR-
KEY/discovery$is_args$args;
}
```

Sur d'autres serveurs ou services web (IIS, Cloudflare, panneaux de contrôle d'hébergement), créez une règle de redirection (302) depuis le même chemin vers l'URL de découverte avec l'option qui conserve ou transmet la chaîne de requête.

Option 3 : fichier statique sur votre site web

Si vous ne pouvez pas ajouter de redirection, publiez un fichier à l'adresse *https://company.com/.well-known/com.apple.remotemanagement* (sans extension de fichier), servi avec *Content-Type: application/json*. Copiez son contenu depuis l'onglet. Un fichier statique ne peut pas choisir le mode par appareil : il utilise le même mode pour iPhone, iPad et Mac. Pour

l’inscription utilisateur, il ressemble à ceci :

```
{"Servers":[{"Version":"mdm-byod","BaseURL":"https://enterprise.cerberusapp.com/account-enroll/YOUR-KEY/byod"}]}
```

et pour l’inscription d’appareil :

```
{"Servers":[{"Version":"mdm-adde","BaseURL":"https://enterprise.cerberusapp.com/account-enroll/YOUR-KEY/adde"}]}
```

> Le mode du fichier doit également être le mode défini dans l’onglet pour la famille d’appareils, sinon l’inscription est refusée.

Vérifier la configuration

Dans **Vérifier la configuration**, choisissez un domaine et un appareil (iPhone ou Mac), puis cliquez sur **Vérifier** : Cerberus Enterprise interroge le domaine comme le ferait un appareil et affiche la réponse, chaque redirection et un verdict. Un domaine qui pointe vers Cerberus Enterprise signifie que les options 2 ou 3 fonctionnent ; une réponse d’erreur (telle que « not found ») convient pour l’option 1 ; une page web ou un fichier pointant ailleurs arrête les appareils. La vérification avertit également lorsqu’une redirection perd la chaîne de requête ou que le fichier n’est pas servi en *application/json*.

Clé d’inscription

Les URL de découverte et d’inscription contiennent une clé de votre organisation. Si les URL ont été publiées par erreur, cliquez sur **Régénérer la clé** : les anciennes URL cessent immédiatement de fonctionner, alors mettez à jour les redirections et les fichiers statiques sur vos sites web. Cerberus Enterprise enregistre lui-même la nouvelle URL dans Apple Business lorsque l’option 1 est utilisée.

Comment les utilisateurs s’inscrivent

1. iPhone et iPad : ouvrez *Réglages → Général → VPN et gestion de l'appareil → Se connecter à un compte professionnel ou scolaire*. Mac : *Réglages Système → Général → Gestion de l'appareil → Se connecter* (sur macOS 14 : *Confidentialité et sécurité → Profils → Se connecter*).

2. Saisissez le compte Apple géré, ou l’adresse e-mail professionnelle de l’utilisateur dans Cerberus (par exemple *name@company.com*). Lorsque le compte Apple géré de l’utilisateur diffère de ce qui a été saisi, l’appareil demande ensuite de se connecter avec ce compte.
3. Une page Cerberus Enterprise s’ouvre : appuyez sur *Envoyer le code*, puis saisissez le code à 6 chiffres reçu par e-mail. Le code expire après 10 minutes ; après 5 codes erronés, l’utilisateur doit fermer la page et se reconnecter.
4. Connectez-vous avec le mot de passe du compte Apple géré (ou avec la page de connexion de l’entreprise lorsque Apple Business est connecté à Google Workspace ou Microsoft Entra ID), puis autorisez la gestion de l’appareil.

> Les comptes qui ne peuvent pas s’inscrire (domaine non vérifié, aucun utilisateur correspondant lorsque les utilisateurs ne sont pas créés automatiquement, plusieurs utilisateurs avec la même adresse e-mail) voient le message « Ce compte n’est pas configuré pour l’inscription. Contactez votre administrateur informatique. » Les événements figurent dans les journaux système du tableau de bord.

Après l’inscription

- La page de l’appareil affiche le **compte Apple géré** utilisé pour l’inscription et le type d’inscription (Inscription utilisateur ou Inscription d’appareil pilotée par le compte). Dans la liste des appareils, les appareils en inscription utilisateur affichent « Inscription utilisateur ».
- Sur les appareils en inscription utilisateur, les commandes et les paramètres de stratégie qu’Apple n’autorise pas (effacement, localisation, mode perdu, mises à jour du système, nombreuses restrictions) ne sont pas proposés ou ne sont pas envoyés. Les applications App Store de la stratégie utilisent une licence utilisateur au lieu d’une licence d’appareil (voir **Applications sur les appareils personnels** ci-dessous).
- Sur les appareils en inscription utilisateur, les clips web apparaissent sur l’écran d’accueil mais ne sont pas répertoriés dans *Réglages → Général → VPN et gestion de l’appareil*.
- Le certificat MDM de ces appareils n’est pas renouvelé automatiquement et **Return to Service** n’est pas disponible : avant l’expiration du certificat MDM (un an après l’inscription, voir la page de l’appareil), demandez à l’utilisateur de réinscrire l’appareil.
- Pour quitter la gestion, l’utilisateur se déconnecte du compte professionnel au même endroit des réglages, ou vous désinscrivez l’appareil de Cerberus Enterprise. Avec l’inscription utilisateur, seules les applications, les comptes et les données professionnels sont supprimés ; les données personnelles restent. Un appareil qui s’inscrit à nouveau apparaît comme un nouvel appareil.

> Juste après l'inscription, certains profils de la stratégie (certificats, réseaux Wi-Fi, clips web) peuvent être signalés comme ayant échoué avec une erreur inconnue, et l'appareil peut

apparaître comme **Non conforme** pendant un certain temps. L'appareil les réessaie de lui-même et ils s'installent après un moment, sans aucune action nécessaire. N'enregistrez pas à nouveau la stratégie et n'inscrivez pas à nouveau l'appareil pour cette raison.

Applications sur les appareils personnels

Les iPhone et les iPad inscrits avec l’inscription utilisateur n’ont pas de numéro de série, de sorte qu’Apps and Books ne peut pas leur attribuer de licence d’appareil. Cerberus Enterprise attribue à la place une **licence utilisateur** aux applications App Store de leur stratégie : la licence est attribuée au compte Apple géré connecté sur l’appareil. Rien ne change dans la stratégie : la même stratégie sert les appareils d’entreprise et personnels, et Cerberus choisit le type de licence pour chaque appareil.

- **Automatique** : lors de la première inscription, Cerberus enregistre le compte Apple géré auprès d’Apps and Books, puis demande à Apple une licence pour chaque application App Store de la stratégie. Les applications gratuites ont aussi besoin d’une licence ; Apple leur en accorde un nombre illimité. Une application payante utilise une licence par compte Apple géré, partagée par tous les appareils personnels de ce compte.
- **Même organisation** : les comptes Apple gérés et le jeton Apps and Books de Cerberus Enterprise doivent appartenir à la même organisation Apple Business, et les applications doivent figurer dans la bibliothèque de l’emplacement du jeton.
- **Licence d’abord** : une application n’est envoyée à l’appareil qu’après confirmation de sa licence par Apple, généralement en quelques minutes. Jusque-là, le panneau **Applications** de l’appareil l’affiche comme **En attente d’une licence utilisateur**, avec le motif.
- **Invite d'installation** : les appareils personnels ne sont jamais supervisés, iOS demande donc à l'utilisateur avant d'installer chaque application, y compris l'application **Cerberus Enterprise**, que Cerberus installe aussi sur ces appareils (**Installer** ou **Annuler**) ; aucune connexion à un compte Apple n'est nécessaire. Si l'utilisateur annule, l'application affiche **En attente de l'approbation de l'installation par l'utilisateur** : utilisez **Redemander** sur la page de l'appareil pour afficher à nouveau l'invite. Les applications installées comme **Obligatoires** ne peuvent pas être supprimées par l'utilisateur.
- **Applications installées avant l’inscription** : Apple ne permet pas à l’organisation de reprendre une application que l’utilisateur a installée personnellement sur un appareil inscrit avec l’inscription utilisateur. Demandez à l’utilisateur de supprimer sa propre copie avant l’inscription, ou supprimez-la puis utilisez **Redemander** sur la page de l’appareil : l’organisation installe alors la copie gérée.
- **Quitter la gestion** : lorsque l’appareil est désinscrit, iOS supprime les applications gérées et leurs données. Une licence est libérée lorsqu’aucun autre appareil inscrit du même compte Apple géré n’en a besoin, par exemple lorsque l’application quitte la

stratégie ou que le dernier appareil est désinscrit ; les licences dont plus personne n’a besoin sont libérées par la vérification quotidienne dans la journée.

> Lorsqu’Apple ne peut pas attribuer de licence, par exemple parce qu’une application payante n’a plus de licence disponible, l’application affiche **Échec de la licence utilisateur** avec le message d’Apple. Ajoutez des licences dans Apple Business, puis utilisez **Redemander** sur la page de l’appareil ; Cerberus réessaie également de lui-même lors de la vérification quotidienne. La ligne au-dessus de la liste des applications indique le compte Apple géré et l’état de son utilisateur Apps and Books ; le même état figure sur la page de l’utilisateur.

> Les licences utilisateur ne sont utilisées que sur les iPhone et iPad : sur les Mac inscrits avec l'inscription utilisateur, les apps App Store de la stratégie ne sont pas installées. Les livres et les comptes Apple personnels ne sont pas pris en charge.

Revision #6
Created 2026-11-10 15:15:45 UTC by Admin
Updated 2026-11-12 09:55:31 UTC by Admin