Provisionnement des Appareils - Android

Appareils pris en charge

En général, tout appareil fonctionnant sous Android 6 ou une version ultérieure avec les services Google Play est compatible avec Cerberus Enterprise.

Pour une meilleure expérience utilisateur, nous suggérons d'utiliser des appareils qui répondent aux exigences Android Enterprise Recommended.

> Certaines fonctionnalités sont limitées à des versions spécifiques d'Android ou peuvent se comporter différemment selon les versions du système d'exploitation. Pour plus d'informations sur une fonctionnalité spécifique, consultez la section Policies de la documentation.

Cerberus Enterprise prend en charge les appareils appartenant à l'entreprise ainsi que les appareils personnels, et propose deux modes de gestion : le propriétaire de l'appareil (Device Owner) et le propriétaire du profil (Profile Owner).

Les appareils **personnels** peuvent être gérés via un **profil professionnel**. Cela permet une solution BYOD en séparant les données et applications professionnelles des données et applications personnelles, améliorant ainsi la sécurité et la confidentialité. Cette option est adaptée aux appareils déjà détenus par les employés que vous souhaitez enrôler dans votre organisation pour un usage professionnel.

Appartenant à l'entreprise : les appareils peuvent également être gérés via un profil professionnel, mais vous pouvez aussi choisir l'option **entièrement géré**, qui permet un contrôle plus strict de l'appareil. Les appareils appartenant à l'entreprise avec un profil professionnel sont adaptés lorsque vous fournissez des appareils d'entreprise aux employés pour le travail, tout en permettant un usage personnel. Les appareils entièrement gérés sont mieux adaptés aux appareils qui doivent être utilisés uniquement pour le travail, ou pour les **appareils dédiés** (COSU, single-use corporate-owned), tels que les bornes interactives.

Pour plus d'informations sur le provisionnement des appareils, consultez la page Aperçu du provisionnement des appareils).

Jetons d'enrôlement

Cerberus Enterprise utilise des jetons d'enrôlement pour lancer le processus d'enrôlement (provisionnement) des appareils Android. Le jeton que vous sélectionnez définit la politique initiale appliquée aux appareils enrôlés et influence les modes de provisionnement autorisés.

> L'onglet des jetons d'enrôlement Android n'est disponible qu'après avoir terminé la **configuration d'Android Management**.

Où trouver les jetons d'enrôlement

Dans le tableau de bord, ouvrez **Jetons d'enrôlement**. Selon la configuration de votre compte, la page peut afficher plusieurs onglets (jetons Android, enrôlement par connexion Google, enrôlement manuel Apple et enrôlement automatique des appareils Apple (ADE)).

> Si votre entreprise Android est associée à un domaine géré par Google (Google Workspace), le tableau de bord peut également afficher un onglet **Authentification via l'enrôlement Google**. Pour plus de détails sur l'activation et l'utilisation, consultez **Authentification via l'enrôlement Google**.

Liste des jetons d'enrôlement (Android)

L'onglet des jetons Android affiche un tableau de tous les jetons. Cliquer sur une ligne ouvre la page des détails du jeton.

Colonnes

- **ID** : identifiant interne du jeton.
- **Statut** : **Disponible**, **Utilisé** (jeton à usage unique déjà utilisé), ou **Expiré**.
- **Expiration** : date/heure d'expiration, ou **Jamais**.

- **Politique** : la politique assignée au jeton (l'info-bulle de l'interface utilisateur affiche également l'ID de la politique).
- **Usage personnel** : Autorisé / Interdit / Appareil dédié.
- **Usages autorisés** : Multiples ou Usage unique.
- **Utilisateur** : utilisateur optionnel préassigné aux appareils enrôlés avec le jeton.

Actions

- Chaque ligne dispose d'une action de suppression (**Supprimer le jeton d'enrôlement**). La suppression est désactivée lorsque la licence est expirée.
- Le tableau permet la sélection de plusieurs lignes : vous pouvez activer le mode de sélection, sélectionner plusieurs jetons et les supprimer avec **Supprimer les jetons sélectionnés**.
- Utilisez l'action d'actualisation pour recharger la liste. Le tableau est paginé (10/25/50 éléments par page).

Créer un nouveau jeton d'enrôlement

Dans l'onglet des jetons Android, cliquez sur **Nouveau jeton d'enrôlement** pour ouvrir la page de création de jeton. Si votre licence est expirée, le bouton de création est désactivé.

Options du jeton

1. Politique

Obligatoire. La politique appliquée automatiquement à tous les appareils enrôlés avec ce jeton.

Sélectionnez l'une de vos **politiques Android**. Si vous n'avez pas encore de politique, créez-en une d'abord.

2. Utilisateur

Optionnel. Si configuré, les nouveaux appareils enrôlés seront automatiquement associés à cet utilisateur.

3. Usage personnel

Contrôle si l'usage personnel est autorisé sur un appareil provisionné avec ce jeton d'enrôlement :

- **Autorisé** : convient aux appareils personnels (profil professionnel) et aux appareils appartenant à l'entreprise pour un usage professionnel et personnel.
- **Interdit** : convient aux appareils appartenant à l'entreprise pour un usage professionnel uniquement (entièrement gérés).
- **Appareil dédié** : convient aux appareils de type kiosque ou dédiés (l'appareil n'est pas associé à un utilisateur unique).

4. Usages autorisés

Sélectionnez si le jeton peut être utilisé plusieurs fois (**Multiples**) ou une seule fois (**Usage unique**).

5. Expiration

Sélectionnez l'unité d'expiration (**Minutes**, **Heures**, **Jours**, ou **Jamais**). Si l'option n'est pas réglée sur Jamais, saisissez la valeur d'expiration. La plage autorisée dépend de l'unité sélectionnée et peut aller jusqu'à 10 000 jours.

Options de provisionnement (code QR uniquement)

Ces options supplémentaires sont intégrées au code QR et sont appliquées lors du provisionnement des appareils entièrement gérés enrôlés par balayage du code QR. Elles ne s'appliquent pas aux profils professionnels ni aux appareils enrôlés via l'URL ou le jeton d'enrôlement.

Configuration Wi-Fi

Utilisez cette option pour permettre à un appareil de se connecter automatiquement au Wi-Fi pendant le provisionnement, afin qu'il puisse télécharger et initialiser l'application de gestion. Les champs disponibles incluent le **SSID**, le **SSID masqué**, la **Sécurité**, et (si nécessaire) le **Mot de passe**.

Vous pouvez également configurer un proxy HTTP (**Proxy**) et, selon le mode, définir l'**Hôte**/**Port**, l'**URI PAC**, et l'**Hôte de contournement du proxy**.

Autres options

Les options supplémentaires incluent la **Localisation**, le **Fuseau horaire**, et le **Saut de l'étape de chiffrement**.

Détails du jeton d'enrôlement

Lorsque vous ouvrez un jeton, la page de détails affiche la configuration du jeton et les informations d'utilisation :

- **Statut**, **Expiration**, **Usage**, **Usage personnel**, et **Usages autorisés**.
- **Jeton** : la valeur brute du jeton d'enrôlement (copiable).
- **URL d'enrôlement** : une URL d'enrôlement Google Android Enterprise (copiable et envoyable par e-mail).
- **Code QR** : affiché sur le côté droit de la page, utilisé pour enrôler les appareils entièrement gérés.

> Pour les procédures de provisionnement étape par étape, suivez les guides d'enrôlement Android : **Appareils personnels**, **Appareils appartenant à l'entreprise pour usage professionnel et personnel**, **Appareils appartenant à l'entreprise pour usage professionnel uniquement**, et **Zero-touch**.

Appareils personnels

Les appareils appartenant aux employés peuvent être configurés avec un **profil professionnel**. Un profil professionnel offre un espace autonome pour les applications et les données professionnelles, séparé des applications et des données personnelles. La plupart des politiques de gestion des applications, des données et autres s'appliquent uniquement au profil professionnel, tandis que les applications et les données personnelles des employés restent privées.
Pour configurer un profil professionnel sur un appareil personnel, utilisez l'une des méthodes de provisionnement suivantes (assurez-vous que le jeton d'enrôlement a l'option ***Usage personnel*** définie sur **Autorisé**) :

Lien de jeton d'enrôlement

Version Android
6.0+

Vous pouvez fournir l'URL d'enrôlement aux utilisateurs finaux. Lorsqu'un utilisateur final ouvre le lien depuis son appareil, il sera guidé à travers la configuration du profil professionnel.

Ajouter un profil professionnel depuis les « *Paramètres* »

Version Android
6.0+

Pour configurer un profil professionnel sur son appareil, un utilisateur peut ouvrir l'application ***Paramètres*** de l'appareil, puis utiliser la barre de recherche pour trouver et appuyer sur l'option ***Configurer votre profil professionnel***.

Si la recherche ne donne rien, l'emplacement de cette option peut varier. Voici quelques possibilités :

- *Paramètres -> Services et préférences Google -> Tous les services -> Configurer votre profil professionnel*.
- *Paramètres -> Google -> Configurer et restaurer -> Configurer votre profil professionnel*.

Ces étapes lancent un assistant de configuration qui télécharge *Android Device Policy* sur l'appareil. Ensuite, l'utilisateur sera invité à scanner un code QR ou à saisir manuellement un jeton d'enrôlement pour terminer la configuration du profil professionnel.

Télécharger Android Device Policy

Version Android
6.0+

Pour configurer un profil professionnel sur son appareil, un utilisateur peut télécharger Android Device Policy depuis le Google Play Store. Une fois l'application installée, l'utilisateur sera invité à scanner un code QR ou à saisir manuellement un jeton d'enrôlement pour terminer la configuration du profil professionnel.

Appareils appartenant à l'entreprise pour usage professionnel et personnel

La configuration d'un appareil appartenant à l'entreprise avec un **profil professionnel** permet d'utiliser l'appareil pour un usage professionnel et personnel. Sur les appareils appartenant à l'entreprise avec des profils professionnels :

- La plupart des politiques relatives aux applications, aux données et à la gestion s'appliquent uniquement au profil professionnel.
- Les profils personnels des employés restent privés. Toutefois, les entreprises peuvent appliquer certaines politiques globales sur l'appareil ainsi que des politiques d'utilisation personnelle.
- Les entreprises peuvent utiliser la *portée de blocage* pour appliquer des actions de conformité sur l'appareil entier ou uniquement sur son profil professionnel.
- Le désenrôlement de l'appareil et les commandes d'appareil s'appliquent à l'appareil entier.

Pour configurer un appareil appartenant à l'entreprise avec un profil professionnel, utilisez l'une des méthodes de provisionnement suivantes (assurez-vous que le jeton d'enrôlement a l'option **Usage personnel** réglée sur **Autorisé**) :

Méthode par code QR

Version Android
8.0+

Sur un appareil neuf ou réinitialisé aux paramètres d'usine, l'utilisateur (généralement un administrateur informatique) tapote six fois sur le même endroit de l'écran. Cela déclenche une invite sur l'appareil demandant à l'utilisateur de scanner un code QR.

Appareils appartenant à l'entreprise pour usage professionnel uniquement

La gestion complète de l'appareil est adaptée aux appareils appartenant à l'entreprise destinés exclusivement à un usage professionnel. Les entreprises peuvent gérer toutes les applications de l'appareil et appliquer l'ensemble des politiques et commandes de l'API Android Management.
Il est également possible de verrouiller un appareil (via une politique) sur une seule application ou un petit ensemble d'applications pour répondre à un usage ou un cas d'utilisation spécifique. Ce sous-ensemble d'appareils entièrement gérés est appelé **appareils dédiés**.
Pour configurer une gestion complète sur un appareil appartenant à l'entreprise, utilisez l'une des méthodes de provisionnement suivantes (assurez-vous que le jeton d'enrôlement a l'option **Usage personnel** réglée sur **Interdit**) :

Méthode par code QR

Version Android
7.0+

Sur un appareil neuf ou réinitialisé aux paramètres d'usine, l'utilisateur (généralement un administrateur informatique) tapote six fois sur le même endroit de l'écran. Cela déclenche une invite sur l'appareil demandant à l'utilisateur de scanner un code QR.

Méthode par identifiant DPC

Version Android
5.1+

Si l'application Android Device Policy ne peut pas être ajoutée via un code QR, un utilisateur ou un administrateur informatique peut suivre ces étapes pour provisionner un appareil entièrement géré ou dédié :

1. Suivez l'assistant de configuration sur un appareil neuf ou réinitialisé aux paramètres d'usine.
2. Saisissez les informations de connexion Wi-Fi pour connecter l'appareil à Internet.
3. Lorsque l'on vous demande de vous connecter, saisissez **afw#setup**, ce qui téléchargera Android Device Policy.

4. Scannez un code QR ou saisissez manuellement un jeton d'enrôlement pour provisionner l'appareil.

Zero-touch

Les administrateurs informatiques peuvent provisionner les appareils appartenant à l'entreprise en utilisant la méthode d'enrôlement zero-touch, décrite dans l'enrôlement zero-touch pour les administrateurs informatiques. Lorsqu'un appareil est allumé pour la première fois, il est automatiquement contraint d'appliquer les paramètres définis par l'administrateur informatique.

Les administrateurs informatiques peuvent préconfigurer des appareils achetés auprès de revendeurs agréés et les gérer à l'aide du tableau de bord Cerberus Enterprise. Pour lier votre compte Zero-touch, accédez à la section **Zero-touch** du tableau de bord, puis suivez les instructions.

Version Android	Profil professionnel	Appareil entièrement géré	Appareil dédié
8.0+ (Pixel 7.1+)	✓	✓	✓

Authentification via l'enrôlement Google

L'authentification via l'enrôlement Google (également appelée **Authentification Google pour l'enrôlement**) permet aux utilisateurs de s'authentifier avec leur compte Google Workspace lors de l'enrôlement d'un appareil Android.

> Cette fonctionnalité est disponible uniquement pour les entreprises Android associées à un domaine géré par Google (Google Workspace).

Où le trouver

Dans le tableau de bord, ouvrez **Jetons d'enrôlement** et sélectionnez l'onglet **Authentification via l'enrôlement Google**. L'onglet ne s'affiche que lorsque la gestion Android est configurée et que l'intégration Google Workspace est disponible pour votre entreprise.

Activer (ou désactiver) l'authentification Google

L'authentification Google est activée depuis la **console d'administration Google**. Après avoir modifié le paramètre, retournez dans Cerberus Enterprise et utilisez **Actualiser le statut** pour recharger la configuration actuelle.

1. Connectez-vous à votre **console d'administration Google** avec un compte administrateur.
2. Ouvrez **Appareils**.
3. Allez dans **Appareils mobiles et points de terminaison** → **Paramètres** → **Intégrations tierces**.
4. Trouvez l'**Intégration Android EMM** pour Cerberus Enterprise et ouvrez-la.
5. Cliquez sur **Gérer les fournisseurs EMM**.

6. Activez ou désactivez **Authentification via l'enrôlement Google** pour activer ou désactiver l'authentification Google pour l'enrôlement.
7. Cliquez sur **Enregistrer**.
8. Retournez sur le tableau de bord Cerberus Enterprise et cliquez sur **Actualiser le statut** dans l'onglet **Authentification via l'enrôlement Google**.

Jeton d'enrôlement par authentification Google

Lorsque l'authentification Google est activée, le tableau de bord affiche un jeton d'enrôlement dédié utilisé pour ce mode d'enrôlement. La page peut afficher un **code QR**, une valeur de **jeton d'enrôlement** et une **URL d'enrôlement** (copiable et envoyable par e-mail).

Options clés

- **Autoriser l'usage personnel** : contrôle si le jeton peut enrôler des appareils pour un usage professionnel et personnel (scénarios de profil professionnel) ou uniquement pour un usage professionnel (scénarios d'appareils entièrement gérés / dédiés).
- **Politique par défaut de repli** : la politique appliquée lorsque l'utilisateur enrôlé n'a pas de politique par défaut d'authentification Google spécifique assignée.

Interaction avec la politique

Le paramètre de stratégie **Work account setup authentication** (workAccountSetupConfig.authenticationType) contrôle la manière dont les utilisateurs s'authentifient lors de la configuration du compte professionnel, mais le paramètre de la console d'administration Google **Authenticate Using Google** ainsi que le type de jeton d'enrôlement peuvent toujours exiger une authentification.

Pour les appareils déjà enrôlés, cette stratégie ne s'applique que si l'appareil est géré par un compte Google Play géré (c'est-à-dire enrôlé sans **Authenticate Using Google Enrollment**).

> Certaines actions (par exemple, la modification des options de jeton) peuvent être désactivées lorsque la licence est expirée.

Enrôler un appareil

Lors de l'enrôlement, l'utilisateur est invité à s'authentifier avec son compte Google Workspace. Une fois l'enrôlement réussi, l'appareil est associé à l'utilisateur authentifié.

Profil professionnel (appareils personnels)

- Partagez l'**URL d'enrôlement** avec l'utilisateur. Lorsqu'il l'ouvre sur son appareil Android, il est guidé à travers la configuration du profil professionnel et l'authentification Google.
- Alternativement, l'utilisateur peut démarrer depuis les paramètres Android et choisir le flux de configuration du profil professionnel, puis scanner le code QR ou saisir le jeton d'enrôlement lorsqu'il est invité à le faire.

Appareils appartenant à l'entreprise

- **Méthode par code QR** : sur un appareil neuf ou réinitialisé aux paramètres d'usine, appuyez plusieurs fois au même endroit sur l'écran jusqu'à ce que l'invite de code QR apparaisse, puis scannez le code QR affiché dans le tableau de bord.
- **Méthode par identifiant DPC** (lorsque le scan de code QR n'est pas disponible) : suivez l'assistant de configuration, connectez-vous au Wi-Fi, puis lorsqu'on vous demande de vous connecter, saisissez **afw#setup** et procédez en scannant le code QR ou en saisissant le jeton d'enrôlement. Lorsqu'on vous le demande, authentifiez-vous avec votre compte Google Workspace.

Pour les procédures générales de provisionnement Android (profil professionnel vs appareil entièrement géré), consultez les pages d'enrôlement Android standard dans ce manuel.