Provisionnement des Appareils - Android

Appareils pris en charge

En général, tout appareil exécutant Android 6+ avec les services Google Play est compatible avec Cerberus Enterprise.

Pour une meilleure expérience utilisateur, nous vous recommandons d'utiliser des appareils répondant aux exigences des appareils recommandés par Android Enterprise.

> 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 Politiques de la documentation.

Cerberus Enterprise prend en charge les appareils appartenant à l'entreprise et les appareils personnels, ainsi que deux modes de gestion : propriétaire de l'appareil et propriétaire du profil.

Les appareils personnels peuvent être gérés via un **profil professionnel**. Cela permet une solution BYOD (Bring Your Own Device) en séparant les données et applications professionnelles des employés de leurs données et applications personnelles, améliorant ainsi la sécurité et la confidentialité. Cette option convient aux appareils déjà détenus par les employés que vous souhaitez inscrire auprès de votre organisation pour un usage professionnel.

Les appareils appartenant à l'entreprise peuvent également être gérés via un profil professionnel, mais vous pouvez également choisir l'option "**entièrement gérée**, qui permet un contrôle plus strict de l'appareil. Les appareils appartenant à l'entreprise et dotés d'un profil professionnel sont adaptés lorsque vous fournissez des appareils professionnels à vos employés tout en leur permettant de les utiliser pour un usage personnel. Les appareils entièrement gérés conviennent mieux aux appareils qui doivent être utilisés uniquement pour le travail, ou aux **appareils dédiés** (COSU, appareils uniques appartenant à l'entreprise), tels que les bornes interactives.

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

Jetons d'inscription

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

> L'onglet des jetons d'inscription Android est disponible uniquement après avoir effectué la **configuration Android Management**.

Où trouver les jetons d'inscription

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

> Si votre environnement Android Enterprise est associé à un domaine Google géré (Google Workspace), le tableau de bord peut également afficher un onglet "**Authentification via Google**". Pour plus de détails sur l'activation et l'utilisation de cette fonctionnalité, consultez **Authentification via Google**.

Liste des jetons d'inscription (Android)

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

Colonnes

- **Identifiant** : identifiant de jeton interne.
- **Statut**: **Disponible**, **Utilisé** (jeton unique déjà utilisé), ou **Expiré**.
- **Expiration** : date et heure d'expiration, ou **Jamais**.
- **Stratégie** : la stratégie attribuée au jeton (l'info-bulle de l'interface utilisateur affiche également l'identifiant de la stratégie).
- **Utilisation personnelle** : Autorisé / Interdit / Appareil dédié.
- **Utilisations autorisées** : Usage unique ou multiple.
- **Utilisateur** : utilisateur optionnel, pré-affecté aux appareils inscrits avec le jeton.

Actions

- Chaque ligne comporte une action de suppression (**Supprimer le jeton d'inscription**). La suppression est désactivée lorsque la licence est expirée.
- Le tableau prend en charge 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 "Actualiser" pour recharger la liste. Le tableau est paginé (10/25/50 éléments par page).

Créez un nouveau jeton d'inscription

Dans l'onglet "Jetons Android", cliquez sur **Nouveau jeton d'inscription** pour ouvrir la page de création du jeton. Si votre licence est expirée, le bouton de création est désactivé.

Options de jetons

1. Politique

Obligatoire. La politique est automatiquement appliquée à tous les appareils inscrits en utilisant ce jeton. Sélectionnez l'une de vos **politiques Android**. Si vous n'avez pas encore de politique, créez-en une en premier.

2. Utilisateur

Facultatif. Si défini, les appareils nouvellement inscrits sont automatiquement associés à cet utilisateur.

3. Utilisation personnelle

Contrôle si l'utilisation personnelle est autorisée sur un appareil provisionné avec ce jeton d'inscription :

- **Autorisé** : adapté aux appareils personnels (profil professionnel) et aux appareils appartenant à l'entreprise, utilisés pour le travail et les usages personnels.
- **Non autorisé** : compatible avec les appareils appartenant à l'entreprise, utilisés uniquement pour le travail (gestion complète).
- **Appareil dédié** : adapté aux terminaux de caisse ou aux appareils dédiés (l'appareil n'est pas associé à un utilisateur unique).

4. Utilisations autorisées

Sélectionnez si le jeton peut être utilisé plusieurs fois (**Plusieurs**) ou une seule fois (**Une seule fois**).

5. Date d'expiration

Sélectionnez l'unité de temps d'expiration (**Minutes**, **Heures**, **Jours**, ou **Jamais**). Lorsque l'option "Jamais" n'est pas sélectionnée, 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 dans le code QR et sont appliquées lors de la configuration des appareils entièrement gérés, inscrits en scannant le code QR. Elles ne s'appliquent pas aux profils professionnels ou aux appareils inscrits à l'aide de l'URL d'inscription ou du jeton.

Configuration Wi-Fi

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

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

Autres options

Les options supplémentaires incluent **la langue**, **le fuseau horaire** et **l'option de passer outre le chiffrement**.

Détails du jeton d'inscription

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

- **Statut**, **Expiration**, **Utilisation**, **Utilisation personnelle**, et **Utilisations autorisées**.
- **Jeton** : la valeur brute du jeton d'inscription (copiable).
- **URL d'inscription** : une URL d'inscription Google Android Enterprise (copiable et pouvant être envoyée par e-mail).
- **Code QR** : affiché sur le côté droit de la page, utilisé pour inscrire les appareils entièrement gérés.

> Pour connaître les procédures d'installation étape par étape, consultez les guides d'inscription Android : **Appareils personnels**, **Appareils appartenant à l'entreprise**

pour un usage professionnel et personnel, **Appareils appartenant à l'entreprise pour un usage strictement professionnel**, et **Inscription automatique**.

Appareils personnels

Les appareils appartenant aux employés peuvent être configurés avec un **profil professionnel**. Un profil professionnel offre un espace isolé 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'inscription est configuré avec ***Utilisation personnelle*** sur **Autorisé**) :

Lien du jeton d'inscription

Version Android
6.0+

Vous pouvez fournir l'URL d'inscription aux utilisateurs finaux. Lorsqu'un utilisateur final ouvre le lien depuis son appareil, il sera guidé tout au long de la configuration du profil professionnel.

Ajouter le profil professionnel depuis "*Paramètres*"

Version Android
6.0+

Pour configurer un profil professionnel sur leur appareil, un utilisateur peut :

1. Allez dans *Paramètres > Google > Configuration et restauration*.
2. Appuyez sur "*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 entrer manuellement un jeton d'inscription pour terminer la configuration du profil professionnel.

Télécharger Android Device Policy

Version Android
6.0+

Pour configurer un profil professionnel sur leur appareil, l'utilisateur peut télécharger l'application 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'inscription pour finaliser la configuration du profil professionnel.

Appareils fournis par l'entreprise pour un usage professionnel et personnel

La configuration d'un appareil appartenant à l'entreprise avec un **profil professionnel** permet d'utiliser l'appareil à la fois pour le travail et pour un usage personnel. Sur les appareils appartenant à l'entreprise et dotés d'un profil professionnel :

- La plupart des politiques de gestion des applications, des données et autres paramètres s'appliquent uniquement au profil professionnel.
- Les profils personnels des employés restent privés. Toutefois, les entreprises peuvent appliquer certaines politiques générales de l'appareil et des politiques d'utilisation personnelle.
- Les entreprises peuvent utiliser les *portées de bloc* pour appliquer des actions de conformité à tout un appareil ou uniquement à son profil professionnel.
- La désinscription de l'appareil et les commandes de l'appareil s'appliquent à l'ensemble de l'appareil.

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'inscription a l'option **Utilisation personnelle** définie sur **Autorisée**):

Méthode par code QR

Version Android
8.0+

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

Appareils fournis par l'entreprise, réservés à un usage professionnel

La gestion complète de l'appareil est adaptée aux appareils appartenant à l'entreprise et 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'Android Management API.
Il est également possible de verrouiller un appareil (via une politique) à une seule application ou à un ensemble limité d'applications, afin de lui attribuer une fonction ou un usage spécifique. Cet 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'inscription a l'option **Utilisation personnelle** définie sur **Interdite**) :

Méthode par code QR

Version Android
7.0+

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

Méthode d'identification du DPC

Version Android
5.1+

Si la politique d'appareil Android ne peut pas être ajoutée via un code QR, un utilisateur ou un administrateur informatique peut suivre ces étapes pour configurer un appareil entièrement géré ou un appareil dédié :

1. Suivez l'assistant de configuration sur un nouvel appareil ou un appareil réinitialisé aux paramètres d'usine.
2. Entrez les informations de connexion Wi-Fi pour connecter l'appareil à Internet.
3. Lorsque vous êtes invité à vous connecter, saisissez **afw#setup**, ce qui permet de télécharger la stratégie d'appareil Android.
4. Analysez un code QR ou saisissez manuellement un jeton d'inscription pour configurer l'appareil.

Configuration sans intervention

Les administrateurs informatiques peuvent configurer les appareils appartenant à l'entreprise en utilisant la méthode d'inscription sans intervention, décrite dans l'inscription sans intervention pour les administrateurs informatiques. Lors du premier démarrage d'un appareil, celui-ci est automatiquement configuré selon les paramètres définis par l'administrateur informatique.

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

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

Authentification via l'inscription Google

Authentifiez-vous via l'inscription Google (également appelée **Authentification Google pour l'inscription**), ce qui permet aux utilisateurs de s'authentifier avec leur compte Google Workspace lors de l'inscription de leur appareil Android.

> Cette fonctionnalité est disponible uniquement pour les appareils Android utilisés par les entreprises disposant d'un domaine Google géré (Google Workspace).

Où le trouver ?

Dans le tableau de bord, ouvrez **les jetons d'inscription** et sélectionnez l'onglet **Authentification via l'inscription Google**. L'onglet est visible uniquement lorsque la gestion Android est configurée et que l'intégration Google Workspace est disponible pour votre entreprise.

Activez (ou désactivez) l'authentification via Google

L'authentification via Google est activée depuis la **console d'administration Google**. Après avoir modifié ce paramètre, revenez à Cerberus Enterprise et utilisez **Actualiser l'état** pour recharger la configuration actuelle.

1. Connectez-vous à votre **console d'administration Google** avec un compte administrateur.
2. Ouvrez **Appareils**.
3. Accédez à **Appareils mobiles et terminaux** → **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 **l'authentification via Google** pour configurer l'authentification Google pour l'inscription.
7. Cliquez sur **Enregistrer**.
8. Retournez au tableau de bord de Cerberus Enterprise et cliquez sur **Actualiser l'état** dans l'onglet **Authentification via Google Enrollment**.

Mettre à jour l'état de l'onglet "Authentification via Google Enrollment"

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

Options principales

- **Autoriser l'utilisation personnelle** : contrôle si le jeton peut enregistrer des appareils pour un usage professionnel et personnel (scénarios de profil professionnel) ou uniquement pour un usage professionnel (scénarios entièrement gérés/dévolus).
- **Stratégie par défaut de secours** : la stratégie appliquée lorsque l'utilisateur qui s'inscrit n'a pas de stratégie par défaut Google Authentication spécifique attribuée.

Interaction avec les politiques

Le paramètre de stratégie **Authentification de la configuration du compte professionnel** (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 **Authentification via Google** et le type de jeton d'inscription peuvent toujours nécessiter une authentification.

Pour les appareils déjà inscrits, cette stratégie s'applique uniquement si l'appareil est géré par un compte Google Play professionnel (c'est-à-dire, inscrit sans **authentification via Google**).

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

Enregistrer un appareil

Pendant l'inscription, l'utilisateur est invité à s'authentifier avec son compte Google Workspace. Une fois l'inscription réussie, l'appareil est associé à l'utilisateur authentifié.

Profil professionnel (appareils personnels)

- Partagez l' **URL d'inscription** avec l'utilisateur. Lorsque l'utilisateur l'ouvre sur son appareil Android, il est guidé tout au long de la configuration du profil professionnel et de

l'authentification Google.
- Sinon, l'utilisateur peut commencer depuis les paramètres Android et choisir le processus de configuration du profil professionnel, puis scanner le code QR ou saisir le code d'inscription lorsqu'on lui demande.

Appareils appartenant à l'entreprise

- **Méthode du code QR** : sur un appareil neuf ou réinitialisé aux paramètres d'usine, appuyez plusieurs fois sur le même endroit de l'écran jusqu'à ce que l'invite du code QR apparaisse, puis scannez le code QR affiché dans le tableau de bord.
- **Méthode d'identification DPC** (lorsque le scan de QR code n'est pas disponible) : suivez l'assistant de configuration, connectez-vous au réseau Wi-Fi, puis, lorsque vous êtes invité à vous connecter, saisissez **afw#setup** et continuez en scannant le code QR ou en entrant le jeton d'inscription. Lorsque vous y êtes invité, authentifiez-vous avec le compte Google Workspace.

Pour connaître les procédures générales de configuration des appareils Android (profil professionnel par rapport à gestion complète), consultez les pages standard d'inscription Android de ce manuel.