Provisionnement des Appareils - Android

- Appareils pris en charge
- Jetons d'inscription
- Appareils personnels
- Appareils d'entreprise pour usage professionnel et personnel
- Appareils d'entreprise pour usage professionnel uniquement
- Zero-touch
- S'authentifier avec Google Enrollment

Appareils pris en charge

En général, tout appareil exécutant Android 6 ou version ultérieure avec Google Play Services est compatible avec Cerberus Enterprise.

Pour une meilleure expérience utilisateur, nous vous 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 la version du système d'exploitation. Pour plus d'informations sur une fonctionnalité spécifique, consultez la section Stratégies de la documentation.

Cerberus Enterprise prend en charge les appareils d'entreprise et les appareils personnels, ainsi que deux modes de gestion : propriétaire de l'appareil (device owner) et propriétaire du profil (profile owner).

Les **appareils personnels** peuvent être gérés au moyen d'un **profil professionnel**. Cela permet une solution BYOD en séparant les données et apps professionnelles des employés de leurs données et apps personnelles, ce qui améliore à la fois la sécurité et la confidentialité. Cette option convient aux appareils déjà possédés par les employés que vous souhaitez inscrire dans votre organisation pour un usage professionnel.

Les **appareils d'entreprise** peuvent également être gérés au moyen d'un profil professionnel, mais vous pouvez aussi choisir l'option **entièrement gérée**, qui offre un contrôle plus strict de l'appareil. Les appareils d'entreprise dotés d'un profil professionnel conviennent lorsque vous fournissez des appareils à vos employés pour le travail tout en autorisant un usage personnel. Les appareils entièrement gérés sont plus adaptés aux appareils qui doivent être utilisés uniquement pour le travail, ou aux **appareils dédiés** (COSU, corporate-owned single-use), comme les bornes interactives.

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

Jetons d'inscription

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

> L'onglet des jetons d'inscription Android n'est disponible qu'après avoir terminé la **configuration d'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 par connexion Google, inscription manuelle Apple et Apple Automated Device Enrollment).

> Si votre environnement Android enterprise repose sur un domaine Google géré (Google Workspace), le tableau de bord peut également afficher un onglet **S'authentifier avec Google Enrollment**. Pour en savoir plus sur son activation et son utilisation, consultez **S'authentifier avec Google Enrollment**.

Liste des jetons d'inscription (Android)

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

Colonnes

- **Statut** : **Actif** (les appareils peuvent s'inscrire avec le jeton), **Expiré** (la date d'expiration est passée) ou **Épuisé** (un jeton à usage unique déjà utilisé).
- **Stratégie** : la stratégie attribuée au jeton (l'infobulle affiche l'id de la stratégie). **Stratégie supprimée** signifie que la stratégie a été supprimée après la création du

jeton.

- **Utilisateur** : utilisateur facultatif préattribué aux appareils inscrits avec le jeton. **Utilisateur supprimé** signifie que l'utilisateur a été supprimé après la création du jeton.
- **Inscriptions** : combien d'appareils se sont inscrits avec le jeton, affiché sous la forme **n / 1** pour un jeton à usage unique.
- **Usage personnel** : Autorisé / Non autorisé / Appareil dédié.
- **Création** : date de création du jeton. Le tableau affiche les jetons les plus récents en premier.
- **Expiration** : date et heure d'expiration, ou **Jamais**.
- **Code d'inscription** : le code du jeton, celui que vous saisissez sur l'appareil lorsque vous l'inscrivez sans code QR.

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 d'actualisation pour recharger la liste. Le tableau est paginé (10/25/50 éléments par page).

Créer un jeton d'inscription

Dans l'onglet des 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 du jeton

1. Stratégie

Obligatoire. Stratégie appliquée automatiquement à tous les appareils inscrits avec ce jeton.

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

2. Utilisateur

Facultatif. S'il est défini, les appareils nouvellement inscrits sont automatiquement associés à cet utilisateur.

3. Usage personnel

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

- **Autorisé** : adapté aux appareils personnels (profil professionnel) et aux appareils d'entreprise destinés à un usage professionnel et personnel.
- **Non autorisé** : adapté aux appareils d'entreprise destinés à un usage professionnel uniquement (entièrement gérés).
- **Appareil dédié** : adapté aux appareils de type kiosque/dédié (l'appareil n'est pas associé à un utilisateur unique).

4. Utilisations autorisées

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

5. Expiration

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

6. Authentification Google

Détermine si l'utilisateur doit s'authentifier avec un compte Google lors de l'inscription de l'appareil :

- **Non spécifié** : le paramètre d'authentification Google de l'entreprise est utilisé pour déterminer si l'utilisateur doit s'authentifier auprès de Google lors de l'inscription.
- **Facultatif** : l'utilisateur peut choisir d'ignorer l'authentification Google lors de l'inscription.
- **Obligatoire** : l'utilisateur doit s'authentifier avec un compte Google pour poursuivre l'inscription.

Lorsque **Obligatoire** est sélectionné, un champ facultatif **Adresse e-mail du compte requis** apparaît. S'il est défini, l'utilisateur doit s'authentifier avec ce compte Google spécifique lors de l'inscription.

Options de provisionnement (QR code uniquement)

Ces options supplémentaires sont intégrées au QR code et s'appliquent lors du provisionnement des appareils entièrement gérés inscrits en scannant le QR code. Elles ne s'appliquent pas aux profils professionnels ni aux appareils inscrits à l'aide de l'URL d'inscription ou du jeton.

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'app de gestion. Les champs disponibles incluent **SSID**, **SSID masqué**, **Sécurité** et (si nécessaire) **Phrase secrète**.

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

Autres options

Les options supplémentaires incluent **Paramètres régionaux**, **Fuseau horaire** et **Ignorer 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**, **Usage personnel**, **Utilisations autorisées** et (le cas échéant) **Authentification Google** avec le champ facultatif **Adresse e-mail du compte requis**.
- **Jeton** : la valeur brute du jeton d'inscription (copiable).
- **URL d'inscription** : une URL d'inscription Google Android Enterprise (copiable et envoyable par e-mail).
- **QR code** : affiché à droite de la page, utilisé pour inscrire les appareils entièrement gérés.

> Pour les procédures de provisionnement détaillées, suivez les guides d'inscription Android : **Appareils personnels**, **Appareils d'entreprise pour usage professionnel et personnel**, **Appareils d'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 apps et données professionnelles, séparé des apps et données personnelles. La plupart des stratégies de gestion des apps, des données et autres s'appliquent uniquement au profil professionnel, tandis que les apps et 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 a ***Usage personnel*** défini 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 est guidé tout au long de la configuration du profil professionnel.

Ajouter un profil professionnel depuis "*Paramètres*"

Version Android
6.0+

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

iPhone et iPad personnels

Les iPhone et iPad personnels (ainsi que les Mac) s'inscrivent avec l'**Inscription utilisateur** d'Apple : l'utilisateur se connecte avec son Managed Apple Account dans les réglages de l'appareil, et seules les applications, comptes et données professionnels sont gérés. Sur les iPhone et iPad, les applications de l'App Store de la stratégie et l'application **Cerberus Enterprise** sont installées avec une licence utilisateur de ce compte. La position des appareils personnels est collectée uniquement si leur stratégie active **Localisation et géorepérage sur les appareils personnels** et que l'utilisateur l'autorise. Consultez la page **Inscription Apple pilotée par le compte**.

Appareils d'entreprise pour usage professionnel et personnel

La configuration d'un appareil d'entreprise avec un **profil professionnel** permet de l'utiliser à des fins professionnelles et personnelles. Sur les appareils d'entreprise dotés d'un profil professionnel :

- La plupart des stratégies de gestion des apps, des données et autres s'appliquent uniquement au profil professionnel.
- Les profils personnels des employés restent privés. Toutefois, les entreprises peuvent appliquer certaines stratégies à l'échelle de l'appareil et des stratégies d'usage personnel.
- Les entreprises peuvent utiliser la *portée de blocage* pour appliquer des actions de conformité à un appareil entier ou uniquement à son profil professionnel.
- La désinscription d'un appareil et les commandes d'appareil s'appliquent à l'appareil entier.

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

Méthode par QR code

Version Android
8.0+

Sur un appareil neuf ou réinitialisé, l'utilisateur (généralement un administrateur informatique) appuie six fois au même endroit sur l'écran. L'appareil invite alors l'utilisateur à scanner un QR code.

Appareils d'entreprise pour usage professionnel uniquement

Gestion complète de l'appareil convient aux appareils d'entreprise destinés exclusivement à un usage professionnel. Les entreprises peuvent gérer toutes les apps de l'appareil et appliquer l'ensemble des stratégies et commandes de l'API Android Management.
Il est également possible de verrouiller un appareil (via une stratégie) sur une seule app ou un petit ensemble d'apps afin de répondre à un usage ou à un cas d'utilisation dédié. Ce sous-ensemble d'appareils entièrement gérés est appelé **appareils dédiés**.
Pour configurer la gestion complète d'un appareil d'entreprise, utilisez l'une des méthodes de provisionnement suivantes (assurez-vous que le jeton d'inscription a **Usage personnel** défini sur **Non autorisé**) :

Méthode par QR code

Version Android
7.0+

Sur un appareil neuf ou réinitialisé, l'utilisateur (généralement un administrateur informatique) appuie six fois au même endroit sur l'écran. L'appareil invite alors l'utilisateur à scanner un QR code.

Méthode par identifiant DPC

Version Android
5.1+

Si Android Device Policy ne peut pas être ajouté via un QR code, 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.
2. Saisissez les identifiants Wi-Fi pour connecter l'appareil à Internet.
3. Lorsque vous êtes invité à vous connecter, saisissez **afw#setup**, ce qui télécharge Android Device Policy.
4. Scannez un QR code ou saisissez manuellement un jeton d'inscription pour provisionner l'appareil.

Zero-touch

Les administrateurs informatiques peuvent provisionner des appareils d'entreprise à l'aide de la méthode d'inscription Zero-touch, décrite dans Inscription Zero-touch pour les administrateurs informatiques. Lorsqu'un appareil est allumé pour la première fois, il est automatiquement soumis aux 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 associer 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+)	✓	✓	✓

S'authentifier avec Google Enrollment

S'authentifier avec Google Enrollment (également appelé **Authentification Google pour l'inscription**) permet aux utilisateurs de s'authentifier avec leur compte Google Workspace lors de l'inscription d'un appareil Android.

> Cette fonctionnalité est disponible uniquement pour les environnements Android enterprise reposant sur un domaine Google géré (Google Workspace).

Où la trouver

Dans le tableau de bord, ouvrez **Jetons d'inscription** et sélectionnez l'onglet **S'authentifier avec Google Enrollment**. Cet onglet n'apparaît que lorsque Android Management est configuré et que l'intégration Google Workspace est disponible pour votre entreprise.

Activer (ou désactiver) l'authentification Google

L'authentification Google s'active depuis la **Google Admin console**. Après avoir modifié le paramètre, revenez à Cerberus Enterprise et utilisez **Actualiser l'état** pour recharger la configuration actuelle.

1. Connectez-vous à la **Google Admin console** avec un compte administrateur.
2. Ouvrez **Appareils**.
3. Accédez à **Mobile et points de terminaison → Paramètres → Intégrations tierces**.
4. Recherchez l'**intégration Android EMM** de Cerberus Enterprise et ouvrez-la.
5. Cliquez sur **Gérer les fournisseurs EMM**.
6. Utilisez le bouton **S'authentifier avec Google** pour activer ou désactiver l'authentification Google lors de l'inscription.
7. Cliquez sur **Enregistrer**.

8. Revenez au tableau de bord Cerberus Enterprise et cliquez sur **Actualiser l'état** dans l'onglet **S'authentifier avec Google Enrollment**.

Jeton d'inscription avec authentification Google

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

Options clés

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

Interaction avec les stratégies

Le paramètre de stratégie **Authentification lors de la configuration du compte professionnel** (workAccountSetupConfig.authenticationType) détermine comment les utilisateurs s'authentifient lors de la configuration de leur compte professionnel, mais le paramètre **S'authentifier avec Google** de la Google Admin Console et le type de jeton d'inscription peuvent toujours exiger une authentification.

Pour les appareils déjà inscrits, cette stratégie ne s'applique que si l'appareil est géré par un compte Managed Google Play (c'est-à-dire inscrit sans **S'authentifier avec Google Enrollment**).

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

Inscrire un appareil

Lors de 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 celui-ci l'ouvre sur son appareil Android, il est guidé tout au long de la configuration du profil professionnel et de l'authentification Google.
- Vous pouvez également partir des Paramètres Android et choisir le flux de configuration du profil professionnel, puis scanner le QR code ou saisir le jeton d'inscription lorsque cela vous est demandé.

Appareils d'entreprise

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

Pour les procédures générales de provisionnement Android (profil professionnel ou entièrement géré), consultez les pages d'inscription Android standard de ce manuel.