# Gestion des applications

Dans cette section, vous pouvez définir des stratégies liées à la disponibilité, à l'installation, aux mises à jour et à la gestion des autorisations des applications.

> Les comptes Managed Google Play sont créés automatiquement lors du provisionnement des appareils.

## 1. Mode Play Store

Ce mode contrôle les applications disponibles pour l'utilisateur dans le Play Store ainsi que le comportement sur l'appareil lorsque des applications sont retirées de la stratégie.

**Liste blanche (par défaut)** : seules les applications présentes dans la stratégie sont disponibles et toute application absente de la stratégie est automatiquement désinstallée de l'appareil. Le Play Store n'affiche que les applications disponibles.

**Liste noire** : toutes les applications sont disponibles et toute application qui ne doit pas être sur l'appareil doit être explicitement marquée comme **bloquée** dans la stratégie d'applications. Le Play Store affiche toutes les applications, sauf celles qui sont bloquées.

## 2. Stratégie des applications non fiables

La stratégie relative aux applications non fiables (applications issues de sources inconnues) appliquée sur l'appareil. Cette option contrôle le paramètre du système Android qui détermine si un utilisateur peut installer des applications en dehors du Play Store (installation latérale).

**Interdire (par défaut)** : interdire l'installation d'applications non fiables sur l'ensemble de l'appareil.

**Profil personnel uniquement** : pour les appareils avec profils professionnels, autorisez l'installation d'applications non fiables uniquement dans le profil personnel de l'appareil.

**Autoriser** : autoriser l'installation d'applications non fiables sur l'ensemble de l'appareil.

## 3. Google Play Protect

Indique si la vérification des applications par Google Play Protect est appliquée.

**Appliquée (par défaut)** : active de force la vérification des applications.

**Choix de l'utilisateur** : permet à l'utilisateur de choisir d'activer ou non la vérification des applications.

## 4. Stratégie d'autorisations par défaut

La stratégie d'octroi des demandes d'autorisations d'exécution aux applications.

**Demander (par défaut)** : demander à l'utilisateur d'accorder une autorisation.

**Accorder** : accorder automatiquement une autorisation.

**Refuser** : refuser automatiquement une autorisation.

## 5. Fonctions des applications

Contrôle si les applications sur les appareils entièrement gérés ou dans les profils professionnels sont autorisées à exposer des fonctions d'application. Nécessite Android 16 ou version ultérieure.

**Autorisé (par défaut)** : les applications sur les appareils entièrement gérés ou dans les profils professionnels peuvent exposer des fonctions d'application.

**Non autorisé** : les applications sur les appareils entièrement gérés ou dans les profils professionnels ne peuvent pas exposer des fonctions d'application.

## 6. Installation d'applications désactivée

Indique si l'installation d'applications par l'utilisateur est désactivée.

## 7. Désinstallation d'applications désactivée

Indique si la désinstallation d'applications par l'utilisateur est désactivée.

## 8. Stratégies d'autorisations

Octrois ou refus explicites d'autorisations ou de groupes pour toutes les applications. Ces valeurs remplacent le paramètre **Stratégie d'autorisations par défaut**.

Utilisez **Ajouter une stratégie d'autorisations** pour créer des entrées et supprimez-les avec l'action de suppression.

Chaque entrée comprend :

> **Autorisation/groupe Android** : l'autorisation ou le groupe Android (requis), par exemple **android.permission.READ_CALENDAR** ou **android.permission_group.CALENDAR**.
>
> **Stratégie** : Accorder / Refuser / Demander (utilise les mêmes options de stratégie que **Stratégie d'autorisations par défaut**).

## 9. Applications

Liste des applications qui doivent être incluses dans la stratégie. Le comportement du contenu de la liste dépend de la valeur définie pour **Mode Play Store**.

Si **Mode Play Store** est défini sur **liste blanche**, seules les applications présentes dans la stratégie sont disponibles et toute application absente de la stratégie est automatiquement désinstallée de l'appareil.

Si **Mode Play Store** est défini sur **liste noire**, toutes les applications sont disponibles et toute application qui ne doit pas être sur l'appareil doit être explicitement marquée comme **bloquée** dans la stratégie d'applications.

Pour ajouter une application, cliquez sur le bouton **Ajouter des applications** (ou sur l'icône **Ajouter des applications**), sélectionnez **Depuis Managed Google Play**, puis choisissez l'application dans le Play Store et cliquez sur le bouton **Sélectionner** de la carte de l'application.

Pour ajouter une application qui n'est pas publiée sur Google Play mais qui est déjà présente sur l'appareil (par exemple, une application système ou d'un fabricant), cliquez sur **Ajouter des applications**, sélectionnez **Par nom de package (applications préinstallées)**, saisissez le nom de package de l'application (par ex. **com.example.app**) et cliquez sur **Ajouter**.L'application est ajoutée avec le type d'installation **Installation forcée**. Pour afficher l'application dans le lanceur personnalisé du kiosque, son **Type d'installation** doit être **Préinstallée** ou **Installation forcée** : avec **Disponible**, l'application n'est pas affichée.

> Les applications qui ne sont pas disponibles sur Managed Google Play sont signalées par une icône Android dans la liste des applications. Elles ne peuvent pas être installées depuis Google Play ; elles doivent donc déjà être présentes sur l'appareil : les appareils qui ne disposent pas de l'application ne peuvent pas l'installer.

> 

> Toutes les applications publiées sur le Play Store dans votre pays sont disponibles à la sélection par défaut. Pour sélectionner vos propres applications privées ou web, vous devez d'abord les importer dans le système. Pour plus d'informations, consultez la page **Applications privées**.

Chaque application peut être configurée avec ses propres paramètres, regroupés visuellement dans une carte :

## 9.1. Type d'installation

Le type d'installation à effectuer pour une application.

**Disponible** : l'application peut être installée.

**Préinstallée** : l'application est installée automatiquement et peut être supprimée par l'utilisateur.

**Installation forcée** : l'application est installée automatiquement et ne peut pas être supprimée par l'utilisateur.

**Bloquée** : l'application est bloquée et ne peut pas être installée. Si l'application a été installée sous une stratégie précédente, elle sera désinstallée.

**Requise pour la configuration** : l'application est installée automatiquement, ne peut pas être supprimée par l'utilisateur et empêche la configuration de se terminer tant que l'installation n'est pas achevée.

**Kiosque** : l'application est installée automatiquement en mode kiosque : elle est définie comme intention d'accueil préférée et ajoutée à la liste blanche pour le mode de verrouillage des tâches. La configuration de l'appareil ne se terminera pas tant que l'application n'est pas installée. Après l'installation, les utilisateurs ne pourront pas supprimer l'application. Vous ne pouvez définir ce **type d'installation** que pour une seule application par stratégie. Lorsque cette option est présente dans la stratégie, la barre d'état est automatiquement désactivée.

Pour plus d'informations, consultez la page dédiée **Mode kiosque**.

## 9.2. Contraintes d'installation

Définit un ensemble de restrictions pour l'installation de l'application. Lorsque plusieurs contraintes sont sélectionnées, elles doivent toutes être satisfaites pour que l'application soit installée.

> Cette option n'est affichée que lorsque le **Type d'installation** est **Préinstallée** ou **Installation forcée**.

**Réseau non mesuré** : installez l'application uniquement lorsque l'appareil est connecté à un réseau non mesuré (par ex. Wi-Fi).

**En charge** : installez l'application uniquement lorsque l'appareil est en charge.

**Inactif** : installez l'application uniquement lorsque l'appareil est inactif.

## 9.3. Mode de mise à jour automatique

Contrôle le mode de mise à jour automatique de l'application.

**Par défaut** : l'application est mise à jour automatiquement avec une priorité faible afin de minimiser l'impact sur l'utilisateur. L'application est mise à jour lorsque toutes les contraintes suivantes sont remplies : (1) l'appareil n'est pas activement utilisé, (2) l'appareil est connecté à un réseau non mesuré, (3) l'appareil est en charge. L'appareil est informé d'une nouvelle mise à jour dans les 24 heures suivant sa publication par le développeur, puis l'application est mise à jour la prochaine fois que les contraintes ci-dessus sont remplies.

**Reportée** : l'application n'est pas mise à jour automatiquement pendant un maximum de 90 jours après qu'elle est devenue obsolète. 90 jours après que l'application est devenue obsolète, la dernière version disponible est installée automatiquement avec une priorité faible (voir **Par défaut** dans le mode de mise à jour automatique). Une fois l'application mise à jour, elle n'est plus mise à jour automatiquement avant 90 jours après qu'elle est redevenue obsolète. L'utilisateur peut toujours mettre à jour l'application manuellement depuis le Play Store à tout moment.

**Priorité élevée** : l'application est mise à jour dès que possible. Aucune contrainte n'est appliquée. L'appareil est informé immédiatement d'une nouvelle mise à jour dès qu'elle est disponible.

## 9.4. Code de version minimal

La version minimale de l'application qui s'exécute sur l'appareil. Si elle est définie, l'appareil tente de mettre à jour l'application vers au moins ce code de version. Si l'application n'est pas à jour, l'appareil contiendra un **Détail de non-conformité** avec **Motif de non-conformité** défini sur **APP_NOT_UPDATED**. L'application doit déjà être publiée sur Google Play avec un code de version supérieur ou égal à cette valeur. Au maximum 20 applications peuvent spécifier un code de version minimal par stratégie.

## 9.5. Portées déléguées

Les portées déléguées à l'application depuis Android Device Policy. Vous pouvez accorder à d'autres applications une sélection d'autorisations Android spéciales :

**Installation de certificats** : accorde l'accès à l'installation et à la gestion des certificats.

**Configurations gérées** : accorde l'accès à la gestion des configurations gérées.

**Blocage de la désinstallation** : accorde l'accès au blocage de la désinstallation.

**Autorisations** : accorde l'accès à la stratégie d'autorisations et à l'état d'octroi des autorisations.

**Accès aux packages** : accorde l'accès à l'état d'accès aux packages.

**Application système** : accorde l'accès à l'activation des applications système.

## 9.6. Réseau préférentiel

Le service de réseau préférentiel à utiliser pour cette application. S'il est défini, l'application utilisera la tranche de réseau d'entreprise spécifiée pour ses connexions lorsqu'elle est disponible. Cela doit correspondre à une tranche de réseau configurée dans la section **Configuration de découpage réseau 5G** du panneau **Cellulaire**.

## 9.7. Stratégie d'autorisations par défaut

La stratégie par défaut pour toutes les autorisations demandées par l'application. Si elle est spécifiée, elle remplace la **Stratégie d'autorisations par défaut** au niveau de la stratégie qui s'applique à toutes les applications. Elle ne remplace pas les **Stratégies d'autorisations** qui s'appliquent à toutes les applications.

**Demander (par défaut)** : demander à l'utilisateur d'accorder une autorisation.

**Accorder** : accorder automatiquement une autorisation.

**Refuser** : refuser automatiquement une autorisation.

## 9.8. Application professionnelle et personnelle connectée

Contrôle si l'application peut communiquer avec elle-même entre les profils professionnel et personnel d'un appareil, sous réserve du consentement de l'utilisateur (Android 11+).

**Non autorisé (par défaut)** : empêche l'application de communiquer entre profils.

**Autorisé** : permet à l'application de communiquer entre profils après avoir reçu le consentement de l'utilisateur.

## 9.9. Exemption du verrouillage du VPN Always On

Indique si l'application est autorisée à accéder au réseau lorsque le VPN n'est pas connecté et que le **verrouillage est activé**. Pris en charge uniquement sur les appareils exécutant Android 10 ou version ultérieure.

**Appliquée (par défaut)** : l'application respecte le paramètre de verrouillage du VPN Always On.

**Exemptée** : l'application est exemptée du paramètre de verrouillage du VPN Always On.

## 9.10. Widgets du profil professionnel

Indique si l'application installée dans le profil professionnel est autorisée à ajouter des widgets à l'écran d'accueil.

**Autorisé** : l'application peut ajouter des widgets à l'écran d'accueil.

**Non autorisé** : l'application ne peut pas ajouter de widgets à l'écran d'accueil.

## 9.11. Paramètres de contrôle utilisateur

Indique si le contrôle utilisateur est autorisé pour une application donnée. Le contrôle utilisateur inclut des actions comme l'arrêt forcé et l'effacement des données de l'application (Android 11+). Si **extensionConfig** est activé pour une application, le contrôle utilisateur est interdit quel que soit ce paramètre. Pour les applications de kiosque, vous pouvez utiliser **Autorisé** pour autoriser le contrôle utilisateur.

**Non spécifié** : utilise le comportement par défaut de l'application pour déterminer si le contrôle utilisateur est autorisé ou interdit.

**Autorisé** : le contrôle utilisateur est autorisé pour l'application.

**Non autorisé** : le contrôle utilisateur est interdit pour l'application.

## 9.12. Désactivée

Indique si l'application est désactivée. Lorsqu'elle est désactivée, les données de l'application sont toujours conservées.

## 9.13. Autoriser le fournisseur d'identifiants

Indique si l'application est autorisée à agir comme fournisseur d'identifiants sur Android 14 ou version ultérieure.

## 9.14. Configuration gérée

Pour configurer les paramètres gérés de l'application, cliquez sur le bouton **Activer la configuration gérée**. Si une configuration gérée est déjà définie pour l'application, vous pouvez modifier la configuration avec le bouton **Configuration gérée**, ou la supprimer avec le bouton **Supprimer la configuration**.

> L'option **Configuration gérée** n'est disponible que pour les applications qui prennent en charge cette fonctionnalité.

## 9.15. Stratégies d'autorisations

Octrois ou refus explicites d'autorisations pour l'application. Ces valeurs remplacent la **Stratégie d'autorisations par défaut** et les **Stratégies d'autorisations** qui s'appliquent à toutes les applications.

Utilisez **Ajouter une stratégie d'autorisations** pour ajouter une ou plusieurs règles d'autorisations à la carte de l'application et supprimez-les avec l'action de suppression.

### 9.16. ID de piste

Liste des ID de piste de test fermé de l'application auxquels un appareil peut accéder. Si plusieurs ID de piste sont sélectionnés, les appareils reçoivent la dernière version parmi toutes les pistes accessibles. Si aucun ID de piste n'est sélectionné, les appareils n'ont accès qu'à la piste de production de l'application.

> L'option **ID de piste** n'est disponible que pour les applications qui disposent d'au moins un ID de piste pour votre organisation. Pour plus de détails sur la façon d'ajouter votre organisation à une piste de test fermé pour une application spécifique, veuillez lire ceci.

## 10. Paramètres d'application par défaut

Définissez des applications par défaut pour les types pris en charge. Lorsqu'une application par défaut est définie pour au moins un type, les utilisateurs ne peuvent pas modifier les applications par défaut dans ce profil.

> Un seul paramètre d'application par défaut est autorisé par **Type d'application par défaut** . La liste des applications par défaut ne doit pas contenir de doublons.

### 10.1. Type d'application par défaut

Sélectionnez la catégorie d'application à configurer (par exemple Navigateur, Téléphone, SMS, Portefeuille ou Assistant). La disponibilité dépend de la version d'Android et du mode de gestion.

### 10.2. Portées d'application par défaut

Sélectionnez l'emplacement où l'application par défaut doit s'appliquer (Entièrement géré, Profil professionnel ou Profil personnel). Seules les portées prises en charge par le type sélectionné peuvent être choisies.

> Si aucune des portées sélectionnées ne s'applique au mode de gestion de l'appareil, l'appareil signale un détail de non-conformité.

### 10.3. Applications par défaut

Liste des applications pouvant être définies par défaut pour le type sélectionné. La première application installée et éligible est définie par défaut.

> Si les portées incluent **Entièrement géré** ou **Profil professionnel**, chaque application doit également figurer dans la liste **Applications** avec un **Type d'installation** différent de **Bloquée**.

## 11. Sélection de clé privée

Permet d'afficher sur un appareil une interface permettant à l'utilisateur de choisir un alias de clé privée s'il n'existe aucune règle correspondante dans **Choisir les règles de clé privée**.

> Pour les appareils antérieurs à Android P, activer cette option peut rendre les clés d'entreprise vulnérables.

## 12. Choisir les règles de clé privée

Contrôle l'accès des applications aux clés privées. La règle détermine quelle clé privée, le cas échéant, Android Device Policy accorde à l'application spécifiée. L'accès est accordé soit lorsque l'application appelle KeyChain.choosePrivateKeyAlias (ou toute surcharge) pour demander un alias de clé privée pour une URL donnée, soit, pour les règles qui ne sont pas spécifiques à une URL (c'est-à-dire si urlPattern n'est pas défini, ou est défini sur la chaîne vide ou .*) sur Android 11 et versions ultérieures, directement afin que l'application puisse appeler KeyChain.getPrivateKey, sans devoir d'abord appeler KeyChain.choosePrivateKeyAlias. Lorsqu'une application appelle KeyChain.choosePrivateKeyAlias et que plusieurs choosePrivateKeyRules correspondent, la dernière règle correspondante définit l'alias de clé à renvoyer.

Utilisez **Ajouter une règle de clé privée** pour créer des entrées et supprimez-les avec l'action de suppression.

### 12.1. Alias de clé privée

L'alias de la clé privée à utiliser.

### 12.2. Modèle d'URL

Le modèle d'URL à faire correspondre à l'URL de la requête. S'il n'est pas défini ou s'il est vide, il correspond à toutes les URL. Cela utilise la syntaxe des expressions régulières de

java.util.regex.Pattern.

## 12.3. Noms de packages

Les noms de packages auxquels cette règle s'applique. Le hachage du certificat de signature de chaque application est vérifié par rapport au hachage fourni par Play. Si aucun nom de package n'est spécifié, l'alias est fourni à toutes les applications qui appellent KeyChain.choosePrivateKeyAlias ou toute surcharge (mais pas sans appeler KeyChain.choosePrivateKeyAlias, même sur Android 11 et versions ultérieures). Toute application ayant le même UID Android qu'un package spécifié ici y aura accès lorsqu'elle appelle KeyChain.choosePrivateKeyAlias.

Utilisez **Ajouter un nom de package** pour ajouter des entrées et supprimez-les avec l'action de suppression.

> Pour supprimer une application, cliquez sur l'icône **corbeille**, en bas de la carte de l'application.

Revision #55
Created 2025-12-17 09:33:41 UTC by Admin
Updated 2026-11-12 09:55:13 UTC by Admin