Gestion des applications

Dans cette section, vous pouvez définir des politiques relatives à la disponibilité des applications, à l'installation, aux mises à jour et à la gestion des permissions.

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

1. Mode Play Store

Ce mode contrôle quelles applications sont disponibles pour l'utilisateur dans le Play Store et le comportement sur l'appareil lorsque des applications sont supprimées de la politique.

Liste blanche (par défaut) : seules les applications présentes dans la politique sont disponibles, et toute application non présente dans la politique sera automatiquement désinstallée de l'appareil. Le Play Store n'affichera que les applications disponibles.

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

2. Politique des applications non approuvées

La politique relative aux applications non approuvées (applications provenant 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 (sideloading).

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

Profil personnel uniquement : Pour les appareils avec profils de travail, autorise l'installation d'applications non approuvées uniquement dans le profil personnel de l'appareil.

Autoriser: Autoriser l'installation d'applications non approuvées sur l'ensemble de l'appareil.

3. Google Play Protect

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. Politique de permission par défaut

La politique relative à l'octroi des demandes de permissions d'exécution aux applications.

Demander (par défaut) : Demander à l'utilisateur d'accorder une permission.

Accorder: Accorder automatiquement une permission.

Refuser: Refuser automatiquement une permission.

5. Fonctions d'application

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

Autorisé (par défaut) : Les applications sur des appareils entièrement gérés ou dans des profils de travail peuvent exposer des fonctions d'application.

Interdit : Les applications sur des appareils entièrement gérés ou dans des profils de travail ne peuvent pas exposer de fonctions d'application.

6. Installation d'applications désactivée

Si l'installation d'applications par l'utilisateur est désactivée.

7. Désinstallation des applications désactivée

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

8. Politiques de permissions

Attributions ou refus explicites de permissions ou de groupes pour toutes les applications. Ces valeurs remplacent le paramètre **Politique de permissions par défaut**.

Utilisez **Ajouter une politique de permissions** pour créer des entrées et supprimez-les avec l'action de suppression.

Chaque entrée comprend :

> **Permission/groupe Android** : La permission ou le groupe Android (requis), par exemple **android.permission.READ_CALENDAR** ou **android.permission_group.CALENDAR**.
>
> **Politique** : Accorder / Refuser / Demander (utilise les mêmes options de politique que **Politique de permissions par défaut**).

9. Applications

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

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

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

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

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

Chaque application peut être configurée avec ses propres paramètres, qui sont regroupés visuellement dans une fiche :

9.1. Type d'installation

Le type d'installation à effectuer pour une application.

> **Disponible** : L'application est disponible pour l'installation.

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 politique précédente, elle sera désinstallée.

Requise pour la configuration : L'application est installée automatiquement, ne peut pas être supprimée par l'utilisateur et empêchera la fin de la configuration tant que l'installation n'est pas terminée.

Kiosque : L'application est installée automatiquement en mode kiosque : elle est définie comme l'intention d'accueil préférée et est ajoutée à la liste blanche pour le mode de verrouillage de tâche. La configuration de l'appareil ne sera pas terminée 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 politique. Lorsqu'il est présent dans la politique, la barre d'état sera automatiquement désactivée. Pour plus d'informations, veuillez consulter 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 respectées pour que l'application puisse être installée.

> Cette option ne s'affiche que lorsque le **Type d'installation** est **Préinstallée** ou **Installation forcée**.

Réseau non limité : Installez l'application uniquement lorsque l'appareil est connecté à un réseau non limité (par exemple, 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 basse afin de minimiser l'impact sur l'utilisateur. L'application est mise à jour lorsque toutes les contraintes suivantes sont respectées : (1) l'appareil n'est pas utilisé activement, (2) l'appareil est connecté à un réseau non limité, (3) l'appareil est en charge. L'appareil est notifié d'une nouvelle mise à jour dans les 24 heures suivant sa publication par le développeur, après quoi l'application est mise à jour la prochaine fois que les contraintes ci-dessus sont respectées.

Reporté : L'application n'est pas mise à jour automatiquement pendant une période maximale 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 basse (voir le mode **Mise à jour automatique par défaut**). Une fois l'application mise à jour, elle ne sera plus mise à jour automatiquement avant un délai de 90 jours après qu'elle soit redevenue obsolète. L'utilisateur peut toujours mettre à jour l'application manuellement depuis le Play Store à tout moment.

Priorité haute : L'application est mise à jour dès que possible. Aucune contrainte n'est appliquée. L'appareil est immédiatement notifié d'une nouvelle mise à jour dès qu'elle devient disponible.

9.4. Code de version minimum

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 affichera un **Détail de non-conformité** avec le **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 minimum par politique.

9.5. Scopes délégués

Les scopes délégués à l'application par Android Device Policy. Vous pouvez accorder une sélection de permissions Android spéciales à d'autres applications :

Installation de certificat : Accorde l'accès à l'installation et à la gestion des certificats.

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

Bloquer la désinstallation : Accorde l'accès au blocage de la désinstallation.

Permissions : Accorde l'accès à la politique de permissions et à l'état d'attribution des permissions.

Accès aux packages : Accorde l'accès à l'état d'accès aux packages.

Application système : Accorde l'accès pour l'activation des applications système.

9.6. Réseau préférentiel

Le service de réseau préférentiel à utiliser pour cette application. Si elle est définie, l'application utilisera le segment de réseau d'entreprise spécifié pour ses connexions lorsqu'il sera disponible. Cela doit correspondre à un segment de réseau configuré dans la section **Configuration du découpage de réseau 5G** du panneau **Réseau cellulaire**.

9.7. Politique de permissions par défaut

La politique par défaut pour toutes les permissions demandées par l'application. Si elle est spécifiée, elle remplace la **Politique de permissions par défaut** au niveau de la politique qui s'applique à toutes les applications. Elle ne remplace pas les **Politiques de permissions** qui s'appliquent à toutes les applications.

Demander (par défaut) : Demander à l'utilisateur d'accorder une permission.

Accorder : Accorder automatiquement une permission.

Refuser : Refuser automatiquement une permission.

9.8. Application connectée travail et personnel

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

Interdit (par défaut) : Empêche l'application de communiquer entre les profils.

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

9.9. Exemption du verrouillage VPN toujours actif

Spécifie si l'application est autorisée à utiliser le réseau lorsque le VPN n'est pas connecté et que le **verrouillage activé** est actif. Pris en charge uniquement sur les appareils fonctionnant sous Android 10 et versions ultérieures.

Appliqué (par défaut) : L'application respecte le paramètre de verrouillage VPN toujours actif.

Exemptée : L'application est exemptée du paramètre de verrouillage VPN toujours actif.

9.10. Widgets du profil de travail

Spécifie si l'application installée dans le profil de travail est autorisée à ajouter des widgets sur l'écran d'accueil.

Autorisé : L'application peut ajouter des widgets sur l'écran d'accueil.

Interdit : L'application ne peut pas ajouter de widgets sur l'écran d'accueil.

9.11. Paramètres de contrôle utilisateur

Spécifie si le contrôle utilisateur est autorisé pour une application donnée. Le contrôle utilisateur comprend des actions de l'utilisateur telles que 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 en mode kiosque, vous

pouvez utiliser **Autorisé** pour permettre 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.

Interdit : 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 et versions ultérieures.

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 la modifier avec le bouton **Configuration gérée**, ou la supprimer avec le bouton **Supprimer la configuration**.

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

9.15. Politiques de permissions

Attributions ou refus explicites de permissions pour l'application. Ces valeurs remplacent la **Politique de permissions par défaut** et les **Politiques de permissions** qui s'appliquent à toutes les applications.

Utilisez **Ajouter une politique de permissions** pour ajouter une ou plusieurs règles de permission à la fiche de l'application et supprimez-les avec l'action de suppression.

9.16. ID de canal

Liste des ID de canaux de test fermé de l'application auxquels un appareil peut accéder. Si plusieurs ID de canaux sont sélectionnés, les appareils reçoivent la version la plus récente parmi tous les canaux accessibles. Si aucun ID de canal n'est sélectionné, les appareils ont uniquement accès au canal de production de l'application.

>

> **L'option Identifiants de suivi** n'est disponible que pour les applications disposant d'au moins un identifiant de suivi pour votre organisation. Pour plus de détails sur la manière d'ajouter votre organisation à une piste de test fermé pour une application spécifique, veuillez lire ici.

10. Paramètres d'application par défaut

Définissez les 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 plus 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 de l'application par défaut

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

> Si aucune des portées sélectionnées n'est applicable au mode de gestion de l'appareil, l'appareil signalera 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 comme application par défaut.

> Si les portées incluent **Gestion complète** ou **Profil professionnel**, chaque application doit également figurer dans la liste **Applications** avec un **Type d'installation** qui n'est pas défini sur **Bloqué**.

11. Sélection de la clé privée

Permet d'afficher l'interface utilisateur sur un appareil pour qu'un utilisateur puisse choisir un alias de clé privée s'il n'y a pas de règles correspondantes dans **Choisir les règles de clé privée**.

> Pour les appareils antérieurs à Android P, le réglage de 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 une chaîne vide ou .*) sur Android 11 et versions ultérieures, directement afin que l'application puisse appeler KeyChain.getPrivateKey sans avoir à appeler préalablement KeyChain.choosePrivateKeyAlias. Lorsqu'une application appelle KeyChain.choosePrivateKeyAlias et que plus d'une règle de type choosePrivateKeyRules correspond, 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 comparer avec 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 d'expression régulière de java.util.regex.Pattern.

12.3. Noms de package

Les noms de package auxquels cette règle s'applique. L'empreinte du certificat de signature de chaque application est vérifiée par rapport à l'empreinte fournie par Play. Si aucun nom de package n'est spécifié, l'alias est fourni à toutes les applications qui appellent KeyChain.choosePrivateKeyAlias ou ses surcharges (mais pas sans appeler KeyChain.choosePrivateKeyAlias, même sur Android 11 et versions ultérieures). Toute application possédant le même UID Android qu'un package spécifié ici aura accès à l'alias lorsqu'elle appellera 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 **poubelle** au bas de la fiche de l'application.

Revision #47
Created 2025-12-17 09:33:41 UTC by Admin
Updated 2026-07-07 10:55:06 UTC by Admin