Gestion des applications

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

> Les comptes Google Play gérés sont créés automatiquement lors de l'inscription des appareils.

1. Mode Google Play

Ce mode contrôle les applications disponibles pour l'utilisateur dans le Google Play Store et le comportement de 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 Google Play Store n'affichera que les applications disponibles.

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

2. Stratégie concernant les applications non approuvées

La politique concernant les applications non approuvées (applications provenant de sources inconnues) appliquée à 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 manuelle).

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

Profil personnel uniquement : Pour les appareils avec profils professionnels, autoriser 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

Que la vérification des applications Google Play Protect soit appliquée ou non.

Activé (par défaut) : Active la vérification des applications.

Choix de l'utilisateur : Permet à l'utilisateur de choisir si la vérification des applications doit être activée.

4. Stratégie de permissions par défaut

La stratégie pour accorder les demandes d'autorisations en cours d'exécution aux applications.

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

Autoriser : Accorder automatiquement une autorisation.

Refuser : Refuser automatiquement une autorisation.

5. Fonctions de l'application

Permet de contrôler si les applications installées sur les appareils entièrement gérés ou dans les profils professionnels peuvent exposer leurs fonctionnalités. Nécessite Android 16 ou version ultérieure.

Autorisé (par défaut) : Les applications installées sur les appareils entièrement gérés ou dans les profils professionnels peuvent exposer leurs fonctionnalités.

Non autorisé : Les applications installées sur les appareils entièrement gérés ou dans les profils professionnels ne peuvent pas exposer leurs fonctionnalités.

6. Installation des applications désactivée

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

7. Désactivation de la désinstallation des applications

La désinstallation des applications par l'utilisateur est-elle désactivée ?

8. Politiques de permissions

Attribution de permissions explicites, ou octroi/refus de permissions par groupe, 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 les supprimer avec l'action de suppression.

Chaque entrée comprend :

> **Autorisation/groupe Android** : L'autorisation ou le groupe Android (obligatoire), par exemple **android.permission.READ_CALENDAR** ou **android.permission_group.CALENDAR**.
>
> **Politique** : Autoriser / Refuser / Demander (utilise les mêmes options de politique que la **politique de permissions par défaut**).

9. Applications

Liste des applications qui doivent être incluses dans la politique. Le comportement du contenu de cette liste dépend de la valeur définie pour le mode **Google Play**.

Si le **mode Play Store** est configuré en mode **liste blanche**, seules les applications figurant dans la politique sont disponibles, et toute application non présente dans la politique sera automatiquement désinstallée de l'appareil.

Si le mode **Play Store** est configuré en mode **liste noire**, toutes les applications sont disponibles, et toute application qui ne devrait pas être présente 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 l'icône "**Ajouter des applications**"), puis sélectionnez l'application depuis le Play Store et cliquez sur le bouton "**Sélectionner**" dans la fiche de l'application.

> Toutes les applications disponibles sur le Play Store dans votre pays sont sélectionnables 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, qui sont regroupés visuellement dans une carte :

9.1. Type d'installation

Le type d'installation à effectuer pour une application.

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

Préinstallé : L'application est installée automatiquement et peut être supprimée par l'utilisateur.

Installé de force : 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 était installée via une politique précédente, elle sera désinstallée.

Nécessaire pour la configuration : L'application est installée automatiquement et ne peut pas être supprimée par l'utilisateur. Elle empêchera la finalisation de la configuration jusqu'à ce que l'installation soit terminée.

Mode kiosque : L'application est installée automatiquement en mode kiosque. Elle est définie comme l'intention d'accueil par défaut et est autorisée pour le mode de verrouillage. La configuration de l'appareil ne sera pas finalisée tant que l'application n'est pas installée. Une fois installée, les utilisateurs ne pourront pas désinstaller l'application. Vous ne pouvez définir ce **type d'installation** que pour une seule application par politique. Lorsque cette option est présente dans la politique, la barre de statut est 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, toutes doivent être satisfaites pour que l'application puisse être installée.

> Cette option est affichée uniquement lorsque le **type d'installation** est **préinstallé** ou **installé de force**.

Réseau non limité : Installez l'application uniquement lorsque l'appareil est connecté à un réseau non limité (par exemple, Wi-Fi).

Chargement : Installez l'application uniquement lorsque l'appareil est en cours de chargement.

En veille : Installez l'application uniquement lorsque l'appareil est en mode veille.

9.3. Mode de mise à jour automatique

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

Par défaut : L'application est automatiquement mise à jour avec une faible priorité afin de minimiser l'impact sur l'utilisateur. L'application est mise à jour lorsque toutes les conditions suivantes sont remplies : (1) l'appareil n'est pas activement utilisé, (2) l'appareil est connecté à un réseau non facturé, (3) l'appareil est en charge. L'utilisateur est informé 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 conditions ci-dessus sont remplies.

Reporté : L'application n'est pas mise à jour automatiquement pendant un maximum de 90 jours après qu'elle soit devenue obsolète. 90 jours après qu'elle soit redevenue obsolète, la dernière version disponible est installée automatiquement avec une priorité faible (voir le mode de mise à jour automatique **par défaut**). Une fois l'application mise à jour, elle ne sera pas automatiquement mise à jour à nouveau avant 90 jours après qu'elle soit redevenue obsolète. L'utilisateur peut toujours mettre à jour manuellement l'application 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 immédiatement notifié de la disponibilité d'une nouvelle mise à jour.

9.4. Version minimale requise

La version minimale de l'application qui peut fonctionner sur l'appareil. Si cette valeur est définie, l'appareil tente de mettre à jour l'application vers au moins cette version. Si l'application n'est pas à jour, l'appareil affichera un **détail de non-conformité** avec une **raison de non-conformité** définie 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 minimale par politique.

9.5. Portées déléguées

Les autorisations déléguées à l'application depuis la politique de l'appareil Android. Vous pouvez accorder à d'autres applications une sélection de permissions Android spéciales :

Installation des certificats : Permet d'accéder à l'installation et à la gestion des certificats.

Configurations gérées : Permet d'accéder à la gestion des configurations gérées.

Bloquer la désinstallation : Permet d'accéder à la fonctionnalité de blocage de la désinstallation.

Autorisations : Accorde l'accès à la politique des autorisations et à l'état d'octroi des autorisations.

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

Application système : Autorise l'activation des applications système.

9.6. Réseau privilégié

Le réseau privilégié à utiliser pour cette application. Si ce paramètre est défini, l'application utilisera le segment de réseau d'entreprise spécifié pour ses connexions, lorsque cela est possible. Il doit correspondre à un segment de réseau configuré dans la section **Configuration du découpage de réseau 5G** du panneau **Cellulaire**.

9.7. Stratégie de permissions par défaut

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

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

Autoriser : Accorder automatiquement une autorisation.

Refuser : Refuser automatiquement une autorisation.

9.8. Travail connecté et applications personnelles

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 et versions ultérieures).

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

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

9.9. Exemption du verrouillage VPN "Always On"

Indique si l'application est autorisée à utiliser le réseau lorsque le VPN n'est pas connecté et que le **mode verrouillage** est activé. Cette fonctionnalité est prise en charge uniquement sur les appareils exécutant Android 10 et versions ultérieures.

Activé (par défaut) : L'application respecte le paramètre de verrouillage VPN permanent.

Exclu : L'application ne prend pas en compte le paramètre de verrouillage VPN permanent.

9.10. Widgets du profil de travail

Indique si l'application installée dans le profil de travail 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 comprend les actions de l'utilisateur, telles que la force-arrêt et la suppression des données de l'application (Android 11 et versions ultérieures). Si **extensionConfig** est activé pour une application, le contrôle utilisateur est désactivé, quel que soit ce paramètre. Pour les applications en mode kiosk, 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 non.
>
> **Autorisé** : Le contrôle utilisateur est autorisé pour cette application.
>
> **Non autorisé** : Le contrôle utilisateur n'est pas autorisé pour cette application.

9.12. Désactivé

L'application est-elle désactivée ? Lorsque l'application est désactivée, ses données sont toujours conservées.

9.13. Autoriser le fournisseur d'identifiants

L'application est-elle autorisée à agir en tant que 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 modifier la configuration avec le bouton **Configuration gérée**, ou la supprimer avec le bouton **Supprimer la configuration**.

> **La configuration gérée** est disponible uniquement pour les applications qui prennent en charge cette fonctionnalité.

9.15. Politiques de permissions

Attribution explicite des autorisations ou refus 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 **la politique d'ajout des permissions** pour ajouter une ou plusieurs règles de permissions à la carte de l'application et pour les supprimer, utilisez l'action "supprimer".

9.16. Identifiants de suivi

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

> **L'option "Identifiants de test"** est disponible uniquement pour les applications qui disposent d'au moins un identifiant de test pour votre organisation. Pour plus de détails sur la façon d'ajouter votre organisation à un programme de test fermé pour une application spécifique, veuillez lire ici.

10. Paramètres d'application par défaut

Définir 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 pas modifier les applications par défaut dans ce profil.

> Une seule application par défaut est autorisée 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 où appliquer l'application par défaut (entièrement gérée, 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 étendues incluent **entièrement gérées** ou **profil de travail**, chaque application doit également exister dans la liste **Applications** avec le **type d'installation** non défini sur **bloqué**.

11. Sélection de la clé privée

Permet d'afficher une interface utilisateur sur un appareil pour qu'un utilisateur puisse choisir un alias de clé privée s'il n'existe aucune règle correspondante dans **Règles de sélection de la clé privée**.

> Pour les appareils utilisant une version d'Android antérieure à P, l'activation de cette option peut rendre les clés d'entreprise vulnérables.

12. Choisissez les règles relatives à la clé privée

Contrôle l'accès des applications aux clés privées. Cette règle détermine quelle clé privée, le cas échéant, la politique d'appareil Android accorde à l'application spécifiée. L'accès est accordé soit lorsque l'application appelle KeyChain.choosePrivateKeyAlias (ou l'une de ses variantes) 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 ".*") sur Android 11 et versions ultérieures, directement, afin que l'application puisse appeler KeyChain.getPrivateKey, sans avoir à appeler KeyChain.choosePrivateKeyAlias au préalable. Lorsqu'une application appelle KeyChain.choosePrivateKeyAlias et que plusieurs règles choosePrivateKeyRules correspondent, la dernière règle correspondante définit quel alias de clé à renvoyer.

Utilisez **la règle de clé privée** pour créer des entrées et les supprimer à l'aide de l'action de suppression.

12.1. Alias de la clé privée

L'alias de la clé privée à utiliser.

12.2. Modèle d'URL

Le modèle d'URL à utiliser pour comparer à l'URL de la requête. S'il n'est pas défini ou est vide, toutes les URL sont acceptées. Il utilise la syntaxe d'expressions régulières de java.util.regex.Pattern.

12.3. Noms des 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 l'une de ses variantes (mais uniquement après avoir appelé KeyChain.choosePrivateKeyAlias, même sur Android 11 et versions ultérieures). Toute application ayant le même UID Android qu'un package spécifié ici aura accès lorsqu'elle appelle

KeyChain.choosePrivateKeyAlias.

Utilisez **Ajouter le nom du package** pour ajouter des éléments et les supprimer avec l'action de suppression.

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

Revision #34
Created 2025-12-17 09:33:41 UTC by Admin
Updated 2026-04-22 15:50:30 UTC by Admin