Politiques - Android

- Résumé
- Gestion des applications
- Mode kiosque
- Sécurité
- Multimédia
- Cellulaire
- Réseau
- Système
- Localisation et géorepérage
- Gestion des utilisateurs
- Usage personnel
- Stratégies inter-profils
- Rapports d'état
- Divers
- Règles de conformité

Résumé

Les stratégies Android sont les entités centrales du système : elles définissent les règles appliquées et imposées sur les appareils gérés.

Vous pouvez parcourir vos stratégies et en créer de nouvelles depuis la section **Stratégies** du tableau de bord. Pour ouvrir une stratégie Android, cliquez sur la ligne de la stratégie dans le tableau : le système ouvre la page **Éditeur de stratégie**.

Une stratégie peut être associée à un jeton d'inscription, afin qu'elle soit automatiquement appliquée aux appareils pendant le processus d'approvisionnement. Vous pouvez également modifier la stratégie attribuée à un appareil après l'approvisionnement.

> Chaque appareil ne peut être associé qu'à une seule stratégie à la fois.

> De nombreuses options de stratégie ne s'appliquent qu'à certains types d'appareils (entièrement gérés, dédiés, profil professionnel) et versions d'Android. Les paramètres non pris en charge peuvent être ignorés par l'appareil ou signalés comme non conformes.

Disposition de l'éditeur de stratégie

L'éditeur de stratégie est organisé en un ensemble de sections extensibles. En haut de la page, vous pouvez toujours modifier :

- **Nom** (obligatoire)
- **Id** (en lecture seule)
- **Description** (facultatif)

Les sections ci-dessous correspondent aux panneaux de l'éditeur de stratégie (par exemple : Gestion des applications, Sécurité, Réseau, Système, Usage personnel, Stratégies inter-profils, etc.). Lorsque vous ouvrez une stratégie enregistrée, les sections dont les réglages ont été modifiés sont déjà ouvertes et les autres restent fermées. Utilisez les pages de chapitre de ce manuel pour comprendre chaque panneau en détail.

Enregistrer, supprimer et appareils associés

Utilisez **Enregistrer la stratégie** pour appliquer vos modifications. Le bouton est désactivé lorsqu'il n'y a aucune modification en attente ou lorsque la licence est expirée.

Si vous avez ouvert une stratégie existante (elle possède un Id), la page affiche une action **Supprimer la stratégie** et une liste **Appareils associés** en bas, afin que vous puissiez voir combien d'appareils utilisent actuellement la stratégie.

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.

Mode kiosque

Avec le mode kiosque, vous pouvez limiter les fonctionnalités d'un appareil à une seule application ou à plusieurs applications. Le choix entre le mode kiosque mono-application et multi-application dépend de vos objectifs professionnels.

En **mode kiosque mono-application**, un appareil est configuré pour une seule application et ne permet pas aux utilisateurs finaux d'accéder aux autres applications de l'appareil. Ils ne peuvent pas non plus quitter l'application, ce qui en fait un appareil dédié à cette application spécifique.

Pour activer ce mode, spécifiez une application dans la section **Gestion des applications** avec le **Type d'installation** défini sur **Kiosque**.

En **mode kiosque multi-application**, les appareils peuvent accéder à plusieurs applications. Les utilisateurs finaux peuvent naviguer entre plusieurs applications via un lanceur personnalisé. Pour activer ce mode, activez l'option **Lanceur personnalisé de kiosque**.

Lorsque le mode kiosque est activé, vous pouvez également configurer si les utilisateurs finaux peuvent accéder à certaines fonctions système, telles que les paramètres système et la barre d'état.

Lanceur personnalisé de kiosque

Indique si le lanceur personnalisé de kiosque est activé. Il remplace l'écran d'accueil par un lanceur qui verrouille l'appareil sur les applications installées via le paramètre **Gestion des applications**. Les applications s'affichent sur une seule page par ordre alphabétique.

Actions du bouton d'alimentation

Définit le comportement d'un appareil en mode kiosque lorsqu'un utilisateur maintient enfoncé le bouton d'alimentation.

> **Disponible (par défaut)** : le menu d'alimentation (par exemple Éteindre, Redémarrer) s'affiche lorsqu'un utilisateur maintient enfoncé le bouton d'alimentation d'un appareil en mode kiosque.
>
> **Bloqué** : le menu d'alimentation (par exemple Éteindre, Redémarrer) ne s'affiche pas lorsqu'un utilisateur maintient enfoncé le bouton d'alimentation d'un appareil en mode kiosque. Remarque : cela peut empêcher les utilisateurs d'éteindre l'appareil.

Avertissements d'erreur système

Spécifie si les boîtes de dialogue d'erreur système pour les applications plantées ou ne répondant pas sont bloquées en mode kiosque. Lorsqu'elles sont bloquées, le système force l'arrêt de l'application comme si l'utilisateur choisissait l'option « fermer l'application » dans l'interface.

Bloqué (par défaut) : toutes les boîtes de dialogue d'erreur système, telles que les plantages et les applications ne répondant pas (ANR), sont bloquées. Lorsqu'elles sont bloquées, le système force l'arrêt de l'application comme si l'utilisateur fermait l'application depuis l'interface.

Activé : toutes les boîtes de dialogue d'erreur système, telles que les plantages et les applications ne répondant pas (ANR), sont affichées.

Navigation système

Spécifie quelles fonctions de navigation sont activées (par exemple les boutons Accueil et Aperçu) en mode kiosque.

Désactivé (par défaut) : les boutons Accueil et Aperçu ne sont pas accessibles.

Accueil uniquement : seul le bouton Accueil est activé.

Activé : les boutons Accueil et Aperçu sont activés.

Barre d'état

Spécifie si les informations système et les notifications sont désactivées en mode kiosque.

Désactivé (par défaut) : les informations système et les notifications sont désactivées en mode kiosque.

Système uniquement : seules les informations système sont affichées dans la barre d'état.

Activé : les informations système et les notifications sont affichées dans la barre d'état en mode kiosque. Remarque : pour que cette stratégie prenne effet, le bouton Accueil de l'appareil doit être activé via kioskCustomization.systemNavigation.

Paramètres de l'appareil

Spécifie si l'application Paramètres est autorisée en mode kiosque.

Autorisé (par défaut) : l'accès à l'application Paramètres est autorisé en mode kiosque.

Bloqué : l'accès à l'application Paramètres n'est pas autorisé en mode kiosque.

Sécurité

Dans cette section, vous pouvez configurer les stratégies liées à la sécurité.

Actions en cas de risque de sécurité

Choisissez l'action à effectuer lorsqu'un appareil signale un SecurityRisk dans les rapports d'état.

Types de SecurityRisk pris en charge :

Système d'exploitation inconnu : Play Integrity API détecte que l'appareil exécute un système d'exploitation inconnu (la vérification basicIntegrity réussit, mais ctsProfileMatch échoue).

Système d'exploitation compromis : Play Integrity API détecte que l'appareil exécute un système d'exploitation compromis (la vérification basicIntegrity échoue).

Échec de l'évaluation matérielle : Play Integrity API détecte que l'appareil ne présente pas une garantie solide d'intégrité du système, si le libellé MEETS_STRONG_INTEGRITY n'apparaît pas dans le champ d'intégrité de l'appareil.

Actions disponibles :

Effacer les données d'entreprise (par défaut) : désinscrire et effacer les données professionnelles (l'appareil entier s'il est entièrement géré, ou uniquement le profil professionnel pour les appareils avec profil professionnel).

Aucune action : laissez l'appareil inscrit et n'effectuez aucune action automatiquement.

Lorsque vous sélectionnez **Effacer les données d'entreprise**, vous pouvez également configurer les options d'effacement :

Conserver la protection contre la réinitialisation d'usine : conserver les données de Factory Reset Protection (FRP) lors de l'effacement de l'appareil.

Effacer le stockage externe : effacer également le stockage externe de l'appareil (comme les cartes SD) lors de l'effacement.

Effacer les eSIM : pour les appareils appartenant à l'entreprise, cette option supprime toutes les eSIM de l'appareil lors de l'effacement. Sur les appareils appartenant à des particuliers, elle supprime les eSIM gérées (eSIM ajoutées via la commande ADD_ESIM) et aucune eSIM personnelle n'est supprimée.

1. Délai maximal avant verrouillage

Durée maximale (en secondes) d'activité de l'utilisateur avant le verrouillage de l'appareil. Une valeur de 0 signifie qu'il n'y a aucune restriction.

2. Rester allumé pendant la charge

Modes de branchement de la batterie pour lesquels l'appareil reste allumé. Lorsque vous utilisez ce paramètre, il est recommandé de désactiver **Délai maximal avant verrouillage** afin que l'appareil ne se verrouille pas de lui-même tant qu'il reste allumé.

Chargeur secteur : la source d'alimentation est un chargeur secteur.

Port USB : la source d'alimentation est un port USB.

Chargeur sans fil : la source d'alimentation est sans fil.

3. Keyguard désactivé

Si cette option est activée, elle désactive l'écran de verrouillage pour les écrans principal et/ou secondaire. Cette stratégie n'est prise en charge qu'en mode de gestion d'appareil dédié.

4. Exigences relatives aux mots de passe

Stratégies relatives aux exigences de mot de passe.

Utilisez **Configurer les exigences de mot de passe** pour ajouter un ou plusieurs blocs d'exigences de mot de passe. Utilisez **Tout effacer** pour supprimer toutes les exigences de mot de passe configurées.

Les exigences de mot de passe peuvent utiliser la portée **Auto** (exigence unique) ou des portées distinctes **Appareil**/**Profil professionnel**. Les exigences basées sur la complexité doivent être associées à des exigences basées sur la qualité pour la même portée.

4.1. Portée

Portée à laquelle l'exigence de mot de passe s'applique.

> **Auto** : la portée n'est pas spécifiée. Les exigences de mot de passe s'appliquent au profil professionnel pour les appareils avec profil professionnel, et à l'ensemble de l'appareil pour les appareils entièrement gérés ou dédiés.
>
> **Appareil** : les exigences de mot de passe s'appliquent uniquement à l'appareil.
>
> **Profil professionnel** : les exigences de mot de passe s'appliquent uniquement au profil professionnel.

4.2. Longueur de l'historique des mots de passe

Longueur de l'historique des mots de passe. Après avoir défini ce champ, l'utilisateur ne pourra pas saisir un nouveau mot de passe identique à un mot de passe de l'historique. Une valeur de 0 signifie qu'il n'y a aucune restriction.

4.3. Nombre maximal de mots de passe erronés avant effacement

Nombre de mots de passe de déverrouillage incorrects pouvant être saisis avant l'effacement de l'appareil. Une valeur de 0 signifie qu'il n'y a aucune restriction.

4.4. Délai d'expiration du mot de passe (jours)

Ce paramètre oblige l'utilisateur à mettre à jour périodiquement son mot de passe après le nombre de jours spécifié.

4.5. Exiger le déverrouillage par mot de passe

Durée après laquelle un appareil ou un profil professionnel déverrouillé à l'aide d'une forme d'authentification forte (mot de passe, code PIN, schéma) peut être déverrouillé à l'aide de toute autre méthode d'authentification (par exemple empreinte digitale, agents de confiance, visage). Une fois ce délai écoulé, seules les formes d'authentification fortes peuvent être utilisées pour déverrouiller l'appareil ou le profil professionnel.

> **Valeur par défaut de l'appareil** : le délai est défini sur la valeur par défaut de l'appareil.
>
> **Chaque jour** : le délai est défini sur 24 heures.

4.6. Qualité du mot de passe

Qualité de mot de passe requise.

Complexité élevée : définit la bande de complexité de mot de passe élevée comme suit : sur Android 12 et versions ultérieures : code PIN sans séquences répétitives (4444) ni ordonnées (1234, 4321, 2468), longueur minimale de 8 ; alphabétique, longueur minimale de 6 ; alphanumérique, longueur minimale de 6.

Complexité moyenne : définit la bande de complexité de mot de passe moyenne comme suit : code PIN sans séquences répétitives (4444) ni ordonnées (1234, 4321, 2468), longueur minimale de 4 ; alphabétique, longueur minimale de 4 ; alphanumérique, longueur minimale de 4.

Complexité faible : définit la bande de complexité de mot de passe faible comme suit : schéma ; code PIN avec séquences répétitives (4444) ou ordonnées (1234, 4321, 2468).

Aucune : il n'y a aucune exigence de mot de passe.

Faible : l'appareil doit être sécurisé au minimum par une technologie de reconnaissance biométrique à faible niveau de sécurité. Cela inclut les technologies capables de reconnaître l'identité d'une personne, à peu près équivalentes à un code PIN à 3 chiffres (taux de fausse détection inférieur à 1 sur 1 000).

Quelconque : un mot de passe est requis, mais son contenu n'est soumis à aucune restriction.

Numérique : le mot de passe doit contenir des caractères numériques.

Numérique complexe : le mot de passe doit contenir des caractères numériques sans séquences répétitives (4444) ni ordonnées (1234, 4321, 2468).

Alphabétique : le mot de passe doit contenir des caractères alphabétiques (ou des symboles).

Alphanumérique : le mot de passe doit contenir à la fois des caractères numériques et alphabétiques (ou des symboles).

Complexe : le mot de passe doit satisfaire aux exigences minimales spécifiées dans passwordMinimumLength, passwordMinimumLetters, passwordMinimumSymbols, etc. Par exemple, si passwordMinimumSymbols vaut 2, le mot de passe doit contenir au moins deux symboles.

4.7. Longueur minimale

Longueur minimale autorisée du mot de passe. Une valeur de 0 signifie qu'il n'y a aucune restriction.

4.8. Nombre minimal de lettres

Nombre minimal de lettres requis dans le mot de passe.

4.9. Nombre minimal de lettres minuscules

Nombre minimal de lettres minuscules requis dans le mot de passe.

4.10. Nombre minimal de lettres majuscules

Nombre minimal de lettres majuscules requis dans le mot de passe.

4.11. Nombre minimal de caractères non alphabétiques

Nombre minimal de caractères non alphabétiques (chiffres ou symboles) requis dans le mot de passe.

4.12. Nombre minimal de chiffres

Nombre minimal de chiffres requis dans le mot de passe.

4.13. Nombre minimal de symboles

Nombre minimal de symboles requis dans le mot de passe.

4.14. Verrouillage unifié

Contrôle si un verrouillage unifié est autorisé pour l'appareil et le profil professionnel, sur les appareils exécutant Android 9 et versions ultérieures avec un profil professionnel. Cela n'a aucun effet sur les autres appareils.

> **Autoriser le verrouillage unifié** : un verrou commun pour l'appareil et le profil professionnel est autorisé.
>
> **Exiger un verrou professionnel séparé** : un verrou distinct pour le profil professionnel est requis.

5. Réinitialisation d'usine désactivée

Indique si la réinitialisation d'usine depuis les paramètres est désactivée. S'applique uniquement aux appareils entièrement gérés.

6. Protection contre la réinitialisation d'usine

Adresses e-mail des administrateurs de l'appareil pour la protection contre la réinitialisation d'usine. Lorsque l'appareil subit une réinitialisation d'usine non autorisée, l'un de ces administrateurs devra se connecter avec l'e-mail et le mot de passe du compte Google pour déverrouiller l'appareil. Si aucun administrateur n'est spécifié, l'appareil ne fournira pas de protection contre la réinitialisation d'usine. S'applique uniquement aux appareils entièrement gérés.

E-mails des administrateurs : utilisez **Activer la protection contre la réinitialisation d'usine** pour commencer à configurer les administrateurs. Utilisez ensuite **Ajouter l'e-mail d'un administrateur** pour ajouter des adresses et les supprimer avec l'action de suppression.

7. Fonctionnalités de Keyguard

Fonctionnalités de Keyguard (écran de verrouillage) pouvant être désactivées.

7.1. Tout désactiver

Désactive toutes les personnalisations actuelles et futures de Keyguard.

7.2. Désactiver l'appareil photo

Désactive l'appareil photo sur les écrans de verrouillage sécurisés (par exemple, code PIN).

7.3. Désactiver les notifications

Désactive l'affichage de toutes les notifications sur les écrans de verrouillage sécurisés.

7.4. Désactiver les notifications non masquées

Désactive les notifications non masquées sur les écrans de verrouillage sécurisés.

7.5. Ignorer l'état de l'agent de confiance

Ignore l'état de l'agent de confiance sur les écrans de verrouillage sécurisés.

7.6. Désactiver l'empreinte digitale

Désactive le capteur d'empreintes digitales sur les écrans de verrouillage sécurisés.

7.7. Désactiver la saisie de texte dans les notifications

Désactive la saisie de texte dans les notifications sur les écrans de verrouillage sécurisés.

7.8. Désactiver l'authentification par reconnaissance faciale

Désactive l'authentification par reconnaissance faciale sur les écrans de verrouillage sécurisés.

7.9. Désactiver l'authentification par iris

Désactive l'authentification par iris sur les écrans de verrouillage sécurisés.

7.10. Désactiver toutes les authentifications biométriques

Désactive toutes les authentifications biométriques sur les écrans de verrouillage sécurisés.

7.11. Désactiver tous les raccourcis

Désactive tous les raccourcis sur l'écran de verrouillage sécurisé sous Android 14 et versions ultérieures.

Multimédia

Dans cette section, vous pouvez configurer le comportement de la caméra et du microphone, l'accès aux données USB, l'impression et les restrictions liées à l'affichage.

1. Accès à la caméra

Contrôle l'utilisation de la caméra et si l'utilisateur peut accéder à l'option d'activation de la caméra (Android 12+). En général, la désactivation de la caméra s'applique à l'ensemble de l'appareil sur les appareils entièrement gérés, et uniquement dans le profil professionnel sur les appareils avec profil professionnel.

> **Choix de l'utilisateur (par défaut)** : comportement par défaut de l'appareil. Les caméras sont disponibles et (Android 12+) l'utilisateur peut activer ou désactiver l'accès à la caméra.
>
> **Désactivé** : toutes les caméras sont désactivées (entièrement géré : ensemble de l'appareil ; profil professionnel : uniquement pour les applications du profil professionnel). L'option d'accès à la caméra n'a aucun effet dans le périmètre géré.
>
> **Imposé** : les caméras sont disponibles. Sur les appareils entièrement gérés sous Android 12+, l'utilisateur ne peut pas activer ou désactiver l'accès à la caméra. Sur les autres appareils ou versions, cela se comporte comme le choix de l'utilisateur.

2. Accès au microphone

Sur les appareils entièrement gérés, contrôle l'utilisation du microphone et si l'utilisateur peut accéder à l'option d'activation du microphone (Android 12+). Ce paramètre n'a aucun effet sur les appareils qui ne sont pas entièrement gérés.

> **Choix de l'utilisateur (par défaut)** : comportement par défaut. Le microphone est disponible et (Android 12+) l'utilisateur peut activer ou désactiver l'accès au microphone.
>
> **Désactivé** : le microphone est désactivé (ensemble de l'appareil). L'option d'accès au microphone n'a aucun effet.
>
> **Imposé** : le microphone est disponible. Sous Android 12+, l'utilisateur ne peut pas activer ou désactiver l'accès au microphone. Sous Android 11 ou antérieur, cela se comporte comme le choix de l'utilisateur.

3. Accès aux données USB

Contrôle quels fichiers et/ou données peuvent être transférés via USB. Pris en charge uniquement sur les appareils appartenant à l'entreprise.

Interdire le transfert de fichiers (par défaut) : les transferts de fichiers sont interdits, mais les autres connexions de données USB (par exemple souris/clavier) sont autorisées.

Interdire le transfert de données : tous les types de transferts de données USB sont interdits (Android 12+ avec USB HAL 1.3+). Si cette option n'est pas prise en charge, l'appareil revient à Interdire le transfert de fichiers.

Autoriser le transfert de données : tous les types de transferts de données USB sont autorisés.

4. Impression

Contrôle si l'impression est autorisée (Android 9+).

Autorisé (par défaut) : l'impression est autorisée.

Interdit : l'impression est interdite (Android 9+).

5. Paramètres de luminosité de l'écran

Contrôle le mode de luminosité de l'écran et, éventuellement, la valeur de luminosité.

Mode de luminosité de l'écran :

Choix de l'utilisateur (par défaut) : l'utilisateur est autorisé à configurer la luminosité de l'écran.

Automatique : la luminosité est automatique et l'utilisateur ne peut pas la modifier. Vous pouvez toujours définir une valeur de luminosité, utilisée dans le cadre du réglage automatique (entièrement géré Android 9+ ; profils professionnels sur appareils d'entreprise Android 15+).

Fixe : la luminosité est définie sur la valeur configurée et l'utilisateur ne peut pas la modifier. La valeur de luminosité est obligatoire (entièrement géré Android 9+ ; profils professionnels sur appareils d'entreprise Android 15+).

Luminosité de l'écran :

> Valeur de 1 à 255 (1 = la plus faible, 255 = la plus élevée). Une valeur de 0 signifie qu'aucune valeur de luminosité n'est définie.

6. Paramètres de délai d'expiration de l'écran

Contrôle si l'utilisateur peut configurer le délai d'expiration de l'écran et, lorsque ce délai est imposé, sa valeur.

Le champ **Mode de délai d'expiration de l'écran** permet de choisir entre un comportement contrôlé par l'utilisateur et un comportement imposé.

> **Choix de l'utilisateur (par défaut)** : l'utilisateur est autorisé à configurer le délai d'expiration de l'écran.
>
> **Imposé** : le délai d'expiration de l'écran est défini sur la valeur configurée et l'utilisateur ne peut pas le modifier (entièrement géré Android 9+ ; profils professionnels sur appareils d'entreprise Android 15+).

Délai d'expiration de l'écran :

> Durée d'expiration en secondes. La valeur doit être supérieure à 0. Si elle est supérieure à **Durée maximale avant verrouillage**, le système peut la plafonner et signaler une non-conformité.

7. Capture d'écran désactivée

Indique si la capture d'écran est désactivée.

8. Réglage du volume désactivé

Indique si le réglage du volume principal est désactivé.

9. Montage de supports physiques désactivé

Indique si le montage de supports externes physiques est désactivé.

Cellulaire

Dans cette section, vous pouvez configurer les stratégies liées au cellulaire.

1. Mode avion

Contrôle si l'utilisateur peut activer ou désactiver le mode avion.

> **Choix de l'utilisateur (par défaut)** : l'utilisateur est autorisé à activer ou désactiver le mode avion.
>
> **Désactivé** : le mode avion est désactivé. L'utilisateur n'est pas autorisé à activer le mode avion. Pris en charge sur Android 9 et versions ultérieures.

2. Cellulaire 2G

Contrôle si l'utilisateur peut activer ou désactiver le paramètre Cellulaire 2G.

> **Choix de l'utilisateur (par défaut)** : l'utilisateur est autorisé à activer ou désactiver le cellulaire 2G.
>
> **Désactivé** : le cellulaire 2G est désactivé. L'utilisateur n'est pas autorisé à activer le cellulaire 2G via les paramètres. Pris en charge sur Android 14 et versions ultérieures.

3. Remplacer les APN

Contrôle si les APN de remplacement sont activés ou désactivés. Lorsqu'ils sont activés, seuls les APN de remplacement configurés sont utilisés et tous les autres APN de l'appareil sont ignorés.

> **Désactivé (par défaut)** : tous les réglages APN configurés sont enregistrés sur l'appareil, mais ils sont désactivés et n'ont aucun effet. Tous les autres APN de l'appareil restent utilisés.
>
> **Activé** : seuls les APN de remplacement sont utilisés, tous les autres APN sont ignorés. Ce paramètre ne peut être configuré que sur les appareils entièrement gérés sous Android 10 ou version ultérieure.

4. Paramètres APN

Configurez une ou plusieurs entrées APN. Utilisez **Ajouter un APN** pour créer une entrée et **Supprimer l'APN** pour la supprimer.

Chaque APN comporte des champs obligatoires :

Types d'APN : sélectionnez un ou plusieurs types de trafic pour cet APN (la disponibilité dépend du mode de gestion et de la version d'Android).

Nom de l'APN : l'identifiant APN fourni par votre opérateur.

Nom d'affichage : nom convivial affiché dans l'interface.

Champs APN facultatifs :

Type d'authentification, **Nom d'utilisateur**, **Mot de passe** : configurez l'authentification auprès de l'opérateur (si nécessaire).

Protocole et **Protocole d'itinérance** : configuration du protocole IP.

Types de réseau : limitez les technologies cellulaires que l'APN peut utiliser (par exemple LTE/5G NR).

Adresse du proxy et **Port du proxy** : proxy HTTP pour le trafic de données (le cas échéant).

Adresse du proxy MMS, **Port du proxy MMS**, **MMSC (URI du centre MMS)** : paramètres liés aux MMS.

ID d'opérateur numérique (MCC+MNC) et **ID d'opérateur** : champs d'identification de l'opérateur.

Réglage toujours actif : indique si la session PDU activée par cet APN doit être toujours active. Pris en charge sous Android 15 et versions ultérieures.

Type de MVNO : type d'identifiant d'opérateur de réseau mobile virtuel.

MTU IPv4 et **MTU IPv6** : unité de transmission maximale pour les routes IPv4/IPv6. Pris en charge sous Android 13 et versions ultérieures.

5. Configuration de la diffusion cellulaire désactivée

Indique si la configuration de la diffusion cellulaire est désactivée.

6. Configuration des réseaux mobiles désactivée

Indique si la configuration des réseaux mobiles est désactivée.

7. Données en itinérance désactivées

Indique si les services de données en itinérance sont désactivés.

8. Appels sortants désactivés

Indique si les appels sortants sont désactivés.

9. SMS désactivés

Indique si l'envoi et la réception de SMS sont désactivés.

10. Configuration du découpage réseau 5G

Configurez les paramètres du service réseau préférentiel pour activer le découpage réseau 5G d'entreprise. Vous pouvez configurer jusqu'à 5 tranches d'entreprise et affecter des applications à des réseaux spécifiques pour optimiser le routage du trafic.

10.1. Réseau préférentiel par défaut

ID de réseau préférentiel par défaut pour les applications qui ne figurent pas dans la liste des applications, ou si le **réseau préférentiel** d'une application n'est pas défini. Une configuration doit exister pour l'ID de réseau spécifié (sauf s'il est défini sur **Aucun réseau préférentiel**).

Remarque : les applications critiques comme **com.google.android.apps.work.clouddpc** et **com.google.android.gms** sont exclues de ce paramètre par défaut.

10.2. Configurations du service réseau

Utilisez **Ajouter une configuration réseau** pour créer une configuration de tranche. Vous pouvez ajouter jusqu'à 5 configurations. Chaque configuration comporte :

ID de réseau préférentiel (attribué automatiquement) : l'ID de réseau est attribué automatiquement et ne peut pas être modifié.

Repli vers la connexion par défaut : indique si le repli vers le réseau par défaut de l'appareil est autorisé. S'il est interdit, les applications ne peuvent pas accéder à Internet si la tranche 5G est indisponible.

Réseaux non correspondants : indique si les applications soumises à cette configuration peuvent utiliser des réseaux autres que le service préférentiel. Si cette option est définie sur **Interdit**, **Repli vers la connexion par défaut** doit également être défini sur **Interdit**. Nécessite Android 14 ou version ultérieure.

Réseau

Dans cette section, vous pouvez configurer les stratégies liées au réseau.

> Les configurations Wi-Fi peuvent être provisionnées et gérées par le système via **Configurations Wi-Fi**. Selon la valeur définie pour **Configurer le Wi-Fi**, les utilisateurs peuvent avoir un contrôle limité ou nul sur l'ajout et la modification des réseaux.

État des radios de l'appareil

1. État du Wi-Fi

Contrôle l'état actuel du Wi-Fi et si l'utilisateur peut modifier cet état.

> **Choix de l'utilisateur (par défaut)** : l'utilisateur est autorisé à activer ou désactiver le Wi-Fi.
>
> **Activé** : le Wi-Fi est activé et l'utilisateur n'est pas autorisé à le désactiver (Android 13+).
>
> **Désactivé** : le Wi-Fi est désactivé et l'utilisateur n'est pas autorisé à l'activer (Android 13+).

2. Niveau de sécurité Wi-Fi minimal

Niveau de sécurité minimal requis des réseaux Wi-Fi auxquels l'appareil peut se connecter. Pris en charge sous Android 13 et versions ultérieures, pour les appareils entièrement gérés et les profils professionnels sur les appareils appartenant à l'entreprise.

> **Réseau ouvert (par défaut)** : l'appareil peut se connecter à tous les types de réseaux Wi-Fi.
>
> **Réseau personnel** : interdit les réseaux Wi-Fi ouverts ; exige au moins une sécurité personnelle (par exemple WPA2-PSK).
>
> **Réseau d'entreprise** : exige des réseaux EAP d'entreprise ; interdit les réseaux Wi-Fi inférieurs à ce niveau de sécurité.

Réseau d'entreprise 192 bits : exige des réseaux d'entreprise 192 bits ; option la plus stricte.

3. État de l'ultra large bande (UWB)

Contrôle l'état du paramètre ultra large bande et si l'utilisateur peut l'activer ou le désactiver.

Choix de l'utilisateur (par défaut) : l'utilisateur est autorisé à activer ou désactiver l'UWB.

Désactivé : l'UWB est désactivé et l'utilisateur n'est pas autorisé à l'activer via les paramètres (Android 14+).

Gestion de la connectivité de l'appareil

4. Partage Bluetooth

Contrôle si le partage Bluetooth est autorisé.

Autorisé : le partage Bluetooth est autorisé (par défaut sur les appareils entièrement gérés, Android 8+).

Interdit : le partage Bluetooth est interdit (par défaut sur les profils professionnels, Android 8+).

5. Configurer le Wi-Fi

Contrôle les privilèges de configuration du Wi-Fi. Selon l'option sélectionnée, l'utilisateur dispose d'un contrôle total, limité ou nul sur la configuration des réseaux Wi-Fi.

Autoriser la configuration du Wi-Fi (par défaut) : l'utilisateur est autorisé à configurer le Wi-Fi.

Interdire l'ajout de configurations Wi-Fi : l'ajout de nouvelles configurations Wi-Fi est interdit. L'utilisateur peut basculer entre les réseaux déjà configurés (Android 13+ ; appareils entièrement gérés et profils professionnels sur appareils d'entreprise).

Interdire la configuration du Wi-Fi : interdit la configuration des réseaux Wi-Fi. Pour les appareils entièrement gérés, cela supprime les réseaux configurés par l'utilisateur et conserve uniquement les réseaux configurés via **Configurations Wi-Fi**. Pour les profils professionnels sur appareils d'entreprise, les réseaux existants ne sont pas affectés, mais les utilisateurs ne peuvent pas ajouter, supprimer ou modifier de réseaux Wi-Fi.

> Lorsque la configuration du Wi-Fi est désactivée et que l'appareil ne peut pas se connecter au démarrage, le système peut afficher le **moyen de secours réseau** pour permettre à l'utilisateur de se connecter temporairement et d'actualiser la stratégie.

6. Paramètres du Wi-Fi Direct

Contrôle la configuration et l'utilisation des paramètres Wi-Fi Direct. Pris en charge sur les appareils appartenant à l'entreprise sous Android 13 et versions ultérieures.

Autoriser (par défaut) : l'utilisateur est autorisé à utiliser le Wi-Fi Direct.

Interdire : l'utilisateur n'est pas autorisé à utiliser le Wi-Fi Direct.

7. Paramètres de partage de connexion

Contrôle les paramètres de partage de connexion. Selon la valeur définie, l'utilisateur se voit partiellement ou totalement interdire l'utilisation des différentes formes de partage de connexion.

Autoriser tous les partages de connexion (par défaut) : autorise la configuration et l'utilisation de toutes les formes de partage de connexion.

Interdire le partage de connexion Wi-Fi : interdit à l'utilisateur d'utiliser le partage de connexion Wi-Fi (appareils d'entreprise Android 13+).

Interdire tous les partages de connexion : interdit toutes les formes de partage de connexion (appareils entièrement gérés + profils professionnels sur appareils d'entreprise).

8. Stratégie de SSID Wi-Fi

Restrictions sur les SSID Wi-Fi auxquels l'appareil peut se connecter (cela n'affecte pas les réseaux qui peuvent être configurés sur l'appareil). Pris en charge sur les appareils appartenant à l'entreprise sous Android 13 et versions ultérieures.

Liste de refus des SSID (par défaut) : l'appareil ne peut se connecter à aucun réseau Wi-Fi dont le SSID figure dans la liste, mais peut se connecter à d'autres réseaux.

Liste d'autorisation des SSID : l'appareil peut se connecter uniquement aux SSID répertoriés. La liste des SSID ne doit pas être vide.

Utilisez **Ajouter un SSID** pour ajouter des entrées. Selon le type de stratégie sélectionné, la liste est interprétée comme des SSID autorisés ou refusés.

Dans l'interface de l'éditeur de stratégie, la liste des SSID est intitulée **SSID Wi-Fi autorisés** pour les listes d'autorisation et **SSID Wi-Fi refusés** pour les listes de refus.

9. Paramètres d'itinérance Wi-Fi

Configurez le mode d'itinérance Wi-Fi par SSID. Utilisez **Ajouter un paramètre d'itinérance Wi-Fi** pour créer des entrées.

Chaque entrée comprend :

SSID : le SSID auquel le paramètre d'itinérance s'applique (obligatoire).

Mode d'itinérance Wi-Fi : Par défaut / Désactivé / Agressif. Les modes Désactivé et Agressif nécessitent Android 15+ et ne sont pris en charge que sur les appareils entièrement gérés et les profils professionnels sur les appareils appartenant à l'entreprise.

Restrictions réseau

10. Bluetooth désactivé

Indique si le Bluetooth est désactivé. Préférez ce paramètre à Configuration Bluetooth désactivée, car celle-ci peut être contournée par l'utilisateur.

11. Partage de contacts Bluetooth désactivé

Indique si le partage de contacts Bluetooth est désactivé.

12. Configuration Bluetooth désactivée

Indique si la configuration du Bluetooth est désactivée.

13. Réinitialisation réseau désactivée

Indique si la réinitialisation des paramètres réseau est désactivée.

14. Émission sortante via Beam désactivée

Indique si l'utilisation du NFC pour envoyer des données depuis des applications est désactivée.

VPN

15. Application VPN Always On

Spécifiez un nom de package VPN Always On pour garantir que les données des applications gérées spécifiées passent toujours par un VPN configuré.

> Remarque : cette fonctionnalité nécessite le déploiement d'un client VPN compatible avec les fonctions Always On et VPN par application.

16. Verrouillage VPN

Interdit la mise en réseau lorsque le VPN n'est pas connecté.

17. Configuration VPN désactivée

Indique si la configuration du VPN est désactivée.

Proxy et services réseau

18. Service réseau préférentiel

Contrôle si le service réseau préférentiel est activé sur le profil professionnel. Par exemple, une organisation peut avoir un accord avec un opérateur pour que les données professionnelles soient envoyées via un service réseau de l'opérateur dédié à l'usage professionnel (par exemple, une tranche d'entreprise sur les réseaux 5G). Cela n'a aucun effet sur les appareils entièrement gérés.

Désactivé : le service réseau préférentiel est désactivé sur le profil professionnel.

Activé : le service réseau préférentiel est activé sur le profil professionnel.

> Si vous utilisez le découpage réseau d'entreprise, configurez également **Configuration du découpage réseau 5G** dans le panneau de stratégie **Cellulaire** et affectez les applications à une tranche via leur paramètre **Réseau préférentiel**.

19. Proxy global recommandé

Proxy HTTP global indépendant du réseau. En général, les proxys doivent être configurés par réseau dans les configurations Wi-Fi. Un proxy global peut être utile pour des configurations particulières, comme un filtrage interne général. Le proxy global n'est qu'une recommandation et certaines applications peuvent l'ignorer.

Désactivé

Proxy direct

Configuration automatique du proxy (PAC)

19.1. Hôte

L'hôte du proxy direct.

19.2. Port

Le port du proxy direct.

19.3. URI PAC

L'URI du script PAC utilisé pour configurer le proxy.

19.4. Hôtes exclus

Pour un proxy direct, les hôtes pour lesquels le proxy est contourné. Les noms d'hôte peuvent contenir des caractères génériques tels que ***.example.com**.

Utilisez **Ajouter un hôte exclu** pour ajouter des entrées (disponible uniquement pour le proxy direct).

Configurations Wi-Fi

Définissez les configurations de réseau Wi-Fi que le système appliquera sur les appareils. Utilisez **Ajouter une configuration Wi-Fi** pour créer une entrée et supprimez-la avec l'action de suppression.

20. Champs de configuration Wi-Fi

Chaque configuration comprend :

Nom de la configuration : Obligatoire.

SSID : Obligatoire.

Connexion automatique : Indique si le réseau doit être connecté automatiquement lorsqu'il est à portée.

Transition rapide : Indique si le client doit tenter d'utiliser la transition rapide (IEEE 802.11r-2008) avec le réseau.

SSID masqué : Indique si le SSID sera diffusé.

Mode de randomisation MAC : Matériel ou Automatique (Android 13+).

20.1. Sécurité

Options de sécurité Wi-Fi :

WEP-PSK : WEP (clé prépartagée).

WPA-PSK : WPA/WPA2/WPA3-Personal (clé prépartagée).

WPA-EAP : WPA/WPA2/WPA3-Enterprise (protocole d'authentification extensible).

Mode 192 bits WPA3 : réseau WPA-EAP autorisant uniquement le mode 192 bits WPA3.

20.2. Phrase secrète (clé prépartagée)

Affiché lorsque la sécurité est **WEP-PSK** ou **WPA-PSK**. La phrase secrète est obligatoire.

20.3. Méthode EAP (Enterprise)

Affiché lorsque la sécurité est **WPA-EAP** ou **Mode 192 bits WPA3**. Sélectionnez une méthode EAP externe :

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Authentification de phase 2

Affiché pour les méthodes externes utilisant un tunnel (**EAP-TTLS** et **PEAP**).

MSCHAPv2

PAP

20.5. Identifiants EAP fournis par les utilisateurs

Lorsque cette option est activée, le système applique automatiquement les identifiants EAP sur les appareils pour chaque utilisateur. Vous pouvez configurer les identifiants des utilisateurs dans la section **Utilisateurs**.

20.6. Certificat client

Pour **EAP-TLS**, vous pouvez attribuer un certificat client utilisé pour l'authentification Wi-Fi. Pour plus d'informations, consultez la page **Gestion des certificats**.

Si un certificat est déjà attribué, vous pouvez utiliser **Ouvrir le certificat** pour le consulter ou **Changer de certificat** pour en sélectionner un autre.

Vous pouvez également spécifier **Alias de paire de clés du certificat client**, qui référence un certificat client stocké dans le trousseau Android et autorisé pour l'authentification Wi-Fi.

> Si**Certificat client** et **Alias de paire de clés du certificat client** sont tous deux définis, l'alias de paire de clés est ignoré.

20.7. Identité

Identité de l'utilisateur. Pour les protocoles externes avec tunnel (PEAP, EAP-TTLS), elle est utilisée pour s'authentifier à l'intérieur du tunnel, et l'**Identité anonyme** est utilisée pour l'identité EAP à l'extérieur du tunnel. Pour les protocoles externes sans tunnel, elle est utilisée pour l'identité EAP.

20.8. Identité anonyme

Pour les protocoles avec tunnel uniquement, indique l'identité de l'utilisateur présentée au protocole externe.

20.9. Mot de passe

Mot de passe de l'utilisateur. S'il n'est pas spécifié, l'utilisateur sera invité à le saisir par défaut.

20.10. Certificats CA du serveur

Liste des certificats CA à utiliser pour vérifier la chaîne de certificats de l'hôte. Au moins un certificat CA doit correspondre. Pour plus d'informations, consultez la page **Gestion des certificats**.

Utilisez **Ajouter un certificat CA de serveur** pour ajouter des entrées et supprimez-les avec l'action de suppression.

20.11. Correspondances de suffixe de domaine

Liste de contraintes pour le nom de domaine du serveur. Les entrées sont utilisées comme exigences de correspondance de suffixe par rapport aux noms DNS du nom de sujet alternatif d'un certificat de serveur d'authentification.

Système

Dans cette section, vous pouvez configurer les stratégies liées au système.

1. Niveau d'API minimal

Niveau d'API Android minimal autorisé.

2. Stratégie de chiffrement

Indique si le chiffrement est activé.

Par défaut : cette valeur est ignorée, c'est-à-dire qu'aucun chiffrement n'est requis.

Activé sans mot de passe : chiffrement requis, mais aucun mot de passe requis au démarrage.

Activé avec mot de passe : chiffrement requis avec mot de passe requis au démarrage.

3. Date et heure automatiques

Indique si la date, l'heure et le fuseau horaire automatiques sont activés sur un appareil appartenant à l'entreprise.

Choix de l'utilisateur (par défaut) : la date, l'heure et le fuseau horaire automatiques sont laissés au choix de l'utilisateur.

Imposé : impose la date, l'heure et le fuseau horaire automatiques sur l'appareil.

4. Paramètres de développeur

Contrôle l'accès aux paramètres de développeur : options de développeur et démarrage sécurisé.

Désactivé (par défaut) : désactive tous les paramètres de développeur et empêche l'utilisateur d'y accéder.

Autorisé : autorise tous les paramètres de développeur. L'utilisateur peut y accéder et, s'il le souhaite, les configurer.

5. Mode Common Criteria

Contrôle le mode Common Criteria, à savoir les normes de sécurité définies dans les Common Criteria for Information Technology Security Evaluation (CC). L'activation du mode Common Criteria renforce certains composants de sécurité d'un appareil (par exemple : chiffrement AES-GCM des clés Bluetooth à long terme, validation supplémentaire de certains certificats réseau et contrôles d'intégrité de la stratégie cryptographique). Le mode Common Criteria n'est pris en charge que sur les appareils d'entreprise exécutant Android 11 ou une version ultérieure. Avertissement : le mode Common Criteria applique un modèle de sécurité strict qui n'est généralement requis que pour les organisations hautement sensibles. L'utilisation standard de l'appareil peut être affectée ; ne l'activez que si nécessaire.

Désactivé (par défaut) : désactive le mode Common Criteria.

Activé : active le mode Common Criteria.

6. Memory Tagging Extension (MTE)

Contrôle Memory Tagging Extension (MTE) sur l'appareil.

Choix de l'utilisateur (par défaut) : l'utilisateur peut choisir d'activer ou de désactiver MTE sur l'appareil (si l'appareil le prend en charge).

Imposé : MTE est activé et l'utilisateur n'est pas autorisé à le modifier (Android 14+ ; pris en charge sur les appareils entièrement gérés et les profils professionnels des appareils d'entreprise).

Désactivé : MTE est désactivé et l'utilisateur n'est pas autorisé à le modifier (Android 14+ ; pris en charge uniquement sur les appareils entièrement gérés).

7. Protection du contenu

Contrôle si la protection du contenu (qui détecte les applications trompeuses) est activée. Cette fonctionnalité est prise en charge sur Android 15 et versions ultérieures.

Désactivé (par défaut) : la protection du contenu est désactivée et l'utilisateur ne peut pas la modifier.

Imposé : la protection du contenu est activée et l'utilisateur ne peut pas la modifier (Android 15+).

Choix de l'utilisateur : la protection du contenu n'est pas contrôlée par la stratégie ; l'utilisateur peut choisir (Android 15+).

8. Contenu d'assistance

Contrôle si le contenu d'assistance (AssistContent) peut être envoyé à une application privilégiée telle qu'une application d'assistance (par exemple, Circle to Search). Le contenu d'assistance inclut les captures d'écran et des informations sur une application, comme le nom du package. Cette fonctionnalité est prise en charge sur Android 15 et versions ultérieures.

Autorisé (par défaut) : le contenu d'assistance peut être envoyé à une application privilégiée (Android 15+).

Non autorisé : l'envoi du contenu d'assistance à une application privilégiée est bloqué (Android 15+).

9. Création de fenêtres désactivée

Indique si la création de fenêtres autres que les fenêtres d'application est désactivée. Cette option empêche l'affichage des interfaces système suivantes : toasts et snackbars, activités téléphoniques (comme les appels entrants) et activités téléphoniques prioritaires (comme les appels en cours), alertes système, erreurs système et superpositions système.

10. Connexion réseau de secours

Indique si la connexion réseau de secours est activée. Si aucune connexion réseau ne peut être établie au démarrage, la connexion de secours invite l'utilisateur à se connecter temporairement à un réseau afin d'actualiser la stratégie de l'appareil. Une fois la stratégie appliquée, le réseau temporaire est oublié et l'appareil poursuit son démarrage. Cela évite de rester dans l'impossibilité de se connecter à un réseau s'il n'existe aucun réseau adapté dans la dernière stratégie et que l'appareil démarre dans une application en mode tâche verrouillée, ou si l'utilisateur ne peut pas accéder autrement aux paramètres de l'appareil.

11. Activités par défaut

Liste d'activités par défaut pour traiter les intents correspondant à un filtre d'intent particulier. Par exemple, cette fonctionnalité permet aux administrateurs informatiques de choisir l'application de navigation qui ouvre automatiquement les liens web, ou l'application de lancement utilisée lorsque l'utilisateur appuie sur le bouton d'accueil.

Utilisez **Ajouter une activité par défaut** pour créer des entrées. Dans une entrée, utilisez **Ajouter une action** et **Ajouter une catégorie** pour construire le filtre d'intent.

11.1. Activité de réception

Activité qui doit être le gestionnaire d'intent par défaut. Il doit s'agir d'un nom de composant Android, par exemple com.android.enterprise.app/.MainActivity. La valeur peut également être le nom de package d'une application, auquel cas Android Device Policy choisit une activité appropriée dans l'application pour traiter l'intent.

11.2. Action

Actions d'intent à faire correspondre dans le filtre. Si des actions sont incluses dans le filtre, l'action d'un intent doit être l'une de ces valeurs pour correspondre. Si aucune action n'est incluse, l'action de l'intent est ignorée.

11.3. Catégorie

Catégories d'intent à faire correspondre dans le filtre. Un intent inclut les catégories dont il a besoin, et toutes doivent être incluses dans le filtre pour correspondre. Autrement dit, l'ajout d'une catégorie au filtre n'a aucun effet sur la correspondance, sauf si cette catégorie est spécifiée dans l'intent.

12. Méthodes de saisie autorisées

Spécifie les méthodes de saisie autorisées.

> **Toutes autorisées** : aucune restriction appliquée. Toutes les méthodes de saisie sont autorisées.
>
> **Système uniquement** : seules les méthodes de saisie intégrées au système sont autorisées.
>
> **Système et fournies uniquement** : seules les méthodes de saisie fournies et celles intégrées au système sont autorisées.

12.1. Méthodes de saisie autorisées

Noms de package des méthodes de saisie autorisées. S'applique uniquement lorsque **Méthodes de saisie autorisées** est défini sur **Système et fournies uniquement**.

Utilisez **Ajouter une méthode de saisie** pour ajouter des entrées et supprimez-les avec l'action de suppression.

13. Services d'accessibilité autorisés

Spécifie les services d'accessibilité autorisés.

Tous autorisés : tout service d'accessibilité peut être utilisé.

Système uniquement : seuls les services d'accessibilité intégrés au système peuvent être utilisés.

Système et fournis uniquement : seuls les services d'accessibilité fournis et ceux intégrés au système peuvent être utilisés.

13.1. Services d'accessibilité autorisés

Services d'accessibilité autorisés. S'applique uniquement lorsque **Services d'accessibilité autorisés** est défini sur **Système et fournis uniquement**.

Utilisez **Ajouter un service d'accessibilité** pour ajouter des entrées et supprimez-les avec l'action de suppression.

14. Stratégie de mise à jour du système

Configuration de la gestion des mises à jour du système.

Par défaut : suivez le comportement de mise à jour par défaut de l'appareil, qui exige généralement que l'utilisateur accepte les mises à jour du système.

Automatique : installez automatiquement dès qu'une mise à jour est disponible.

Fenêtre horaire : installez automatiquement dans une fenêtre de maintenance quotidienne. Cela configure également les applications Play pour qu'elles soient mises à jour dans cette fenêtre. Cette option est vivement recommandée pour les appareils en mode kiosque, car c'est le seul moyen de mettre à jour via Play les applications épinglées en permanence au premier plan.

Reporter : reportez l'installation automatique jusqu'à 30 jours maximum.

14.1. Fenêtre de maintenance (Fenêtre horaire uniquement)

Lorsque **Stratégie de mise à jour du système** est défini sur **Fenêtre horaire**, vous pouvez définir la fenêtre de maintenance quotidienne à l'aide des champs **de** et **à**.

14.2. Périodes de gel des mises à jour système

Période récurrente chaque année pendant laquelle les mises à jour système over-the-air (OTA) sont reportées afin de figer la version du système d'exploitation exécutée sur un appareil. Pour éviter de figer l'appareil indéfiniment, chaque période de gel doit être séparée d'au moins 60 jours. Chaque période de gel ne doit pas dépasser 90 jours.

Utilisez **Ajouter une période de gel des mises à jour système** pour créer des entrées.

15. Fournisseurs d'identifiants par défaut

Contrôle quelles applications sont autorisées à agir comme fournisseurs d'identifiants sur Android 14 et versions ultérieures.

> **Non autorisé (par défaut)** : les applications dont credentialProviderPolicy n'est pas spécifié ne sont pas autorisées à agir comme fournisseur d'identifiants.
>
> **Non autorisé sauf système** : les applications dont credentialProviderPolicy n'est pas spécifié ne sont pas autorisées à agir comme fournisseur d'identifiants, à l'exception des fournisseurs d'identifiants par défaut de l'OEM.

Localisation et géorepérage

Ce panneau regroupe les paramètres de stratégie Android qui contrôlent la transmission de la localisation de l'appareil, l'application de la localisation et les définitions de géorepérage. Utilisez-le lorsque vous souhaitez que Cerberus Enterprise collecte la localisation des appareils ou détecte l'entrée ou la sortie des appareils dans les zones configurées.

Transmission de la localisation

Signaler la localisation

Active la transmission de la géolocalisation de l'appareil. Les données de localisation collectées via ce paramètre sont utilisées par la **carte de localisation du tableau de bord**, l'historique de localisation de la vue d'ensemble de l'appareil et le traitement du géorepérage.

> L'historique des positions et les événements de géorepérage sont conservés **90 jours** et les données plus anciennes sont supprimées automatiquement chaque nuit. La dernière position de chaque appareil inscrit est toujours conservée, de sorte qu'il reste sur les cartes.

> Sur les appareils qui ne sont pas entièrement gérés, les données de localisation peuvent encore dépendre de l'autorisation de localisation accordée à l'application Cerberus Enterprise et de l'activation des services de localisation sur l'appareil.

> Sur les appareils Apple personnels (inscription utilisateur), la localisation et le géorepérage sont désactivés par défaut : ils ne sont disponibles que lorsque la stratégie Apple active l'option **Localisation et géorepérage sur les appareils personnels**, et uniquement si l'utilisateur autorise la localisation pour l'application Cerberus Enterprise.

Mode de localisation

Contrôle le paramètre de localisation de l'appareil sur les appareils appartenant à l'entreprise.

- **Choix de l'utilisateur** : les services de localisation ne sont pas restreints par la stratégie.
- **Imposé** : les services de localisation sont activés sur l'appareil.

- **Désactivé** : les services de localisation sont désactivés sur l'appareil.

Partage de localisation désactivé

Désactive le partage de localisation pour les applications professionnelles. Sur les appareils avec propriétaire de profil, cela affecte le profil professionnel. Sur les appareils entièrement gérés, cela désactive la localisation pour l'ensemble de l'appareil et remplace le mode de localisation de l'appareil.

Comportement automatique avec des géorepérages actifs

Les géorepérages actifs nécessitent la transmission de la localisation pour fonctionner. Lorsqu'au moins un géorepérage est actif, Cerberus Enterprise maintient automatiquement la cohérence des paramètres de localisation associés.

- **Signaler la localisation** est forcé à Activé tant que des géorepérages actifs existent.
- Le **mode de localisation** est forcé sur **Imposé**.
- **Partage de localisation désactivé** est forcé à Désactivé.

Si vous tentez de désactiver **Signaler la localisation** alors qu'un ou plusieurs géorepérages sont actifs, Cerberus Enterprise affiche une boîte de dialogue de confirmation. Si vous continuez, tous les géorepérages actifs de la stratégie sont désactivés.

Liste des géorepérages

Une stratégie peut contenir jusqu'à **10 géorepérages**. Les noms des géorepérages doivent être uniques au sein de la stratégie.

Utilisez **Ajouter un géorepérage** pour créer une nouvelle entrée. Chaque géorepérage contient ces champs principaux :

- **Nom** : obligatoire et unique.
- **Latitude** et **Longitude** : le centre de la zone.
- **Rayon (m)** : obligatoire, de **200** à **10000** mètres.
- **Description** : notes facultatives pour les administrateurs.
- **Signaler l'entrée** et **Signaler la sortie** : choisissez les événements de transition à générer.
- **Actif** : active ou désactive le géorepérage sans le supprimer.

> Au moins l'une des options**Signaler l'entrée** ou **Signaler la sortie** doit rester activée pour chaque géorepérage.

> Le rayon minimal était auparavant de 100 mètres. Les géorepérages existants de moins de 200 mètres continuent de fonctionner et sont conservés tels quels lorsque vous enregistrez la stratégie, même si vous les déplacez ou les renommez. Si vous modifiez leur rayon, celui-ci doit être d'au moins 200 mètres.

Outils de modification de la carte

Chaque carte de géorepérage inclut un aperçu cartographique de la zone. Vous pouvez modifier la géométrie depuis la carte ou depuis les champs numériques.

- Cliquez sur la carte pour déplacer le centre du géorepérage lorsque la modification de la zone est déverrouillée.
- Utilisez le bouton **Position actuelle** pour centrer la carte sur la position actuelle de votre navigateur.
- Utilisez le bouton **Recentrer la carte** pour restaurer la vue préférée de ce géorepérage.
- Utilisez le bouton de verrouillage pour éviter toute modification accidentelle de la géométrie du géorepérage.

Où apparaissent les données de géorepérage

Les transitions de géorepérage peuvent être consultées dans la page Android **Vue d'ensemble de l'appareil**, dans l'onglet **Géorepérage** du panneau de localisation. Cet onglet affiche les transitions sur une carte dédiée, ainsi que les outils de filtrage et la liste des transitions.

Gestion des utilisateurs

Ajout d'utilisateur désactivé

Indique si l'ajout de nouveaux utilisateurs et profils est désactivé. Pour les appareils dont managementMode est **DEVICE_OWNER**, ce champ est ignoré et l'utilisateur n'est jamais autorisé à ajouter ou supprimer des utilisateurs.

Modification des comptes désactivée

Indique si l'ajout ou la suppression de comptes est désactivé.

Configuration des identifiants utilisateur désactivée

Indique si la configuration des identifiants utilisateur est désactivée.

Suppression d'utilisateur désactivée

Indique si la suppression d'autres utilisateurs est désactivée.

Définition de l'icône utilisateur désactivée

Indique si la modification de l'icône utilisateur est désactivée.

Définition du fond d'écran désactivée

Indique si la modification du fond d'écran est désactivée.

Authentification lors de la configuration du compte professionnel

Contrôle la manière dont les utilisateurs s'authentifient lors de la configuration du compte professionnel. Cette option n'est disponible que pour les entreprises Android adossées à un domaine Google géré (Google Workspace).

Lors de la configuration ou de l'inscription de l'appareil, cette stratégie influence l'obligation de connexion à un compte professionnel, mais le paramètre **Authenticate Using 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 s'applique uniquement si l'appareil est géré par un compte Managed Google Play (c'est-à-dire inscrit sans **Authenticate Using Google Enrollment**).

Pour plus de détails et pour le dépannage, consultez **Authenticate Using Google enrollment**.

Types de comptes bloqués

Types de comptes qui ne peuvent pas être gérés par l'utilisateur. Cette option empêche les utilisateurs de l'appareil d'ajouter des comptes non approuvés.

Utilisez **Ajouter un type de compte bloqué** pour ajouter un ou plusieurs types de comptes.

Chaque entrée comporte un champ **Type de compte** (obligatoire). Saisissez une chaîne telle que **com.google**. Supprimez une entrée à l'aide de l'action de suppression.

Usage personnel

Lors de l'approvisionnement d'un appareil appartenant à l'entreprise pour un usage professionnel et personnel, vous pouvez spécifier certaines règles pour limiter la manière dont l'utilisateur peut utiliser l'appareil à des fins personnelles, en dehors du profil professionnel.

> Cette section ne s'applique qu'aux appareils appartenant à l'entreprise avec un profil professionnel. Elle n'a aucun effet sur les appareils entièrement gérés ou appartenant à des particuliers.

1. Appareil photo désactivé

Indique si l'appareil photo est désactivé.

2. Capture d'écran désactivée

Indique si la capture d'écran est désactivée.

3. Nombre maximal de jours avec le travail désactivé

Contrôle la durée pendant laquelle le profil professionnel peut rester désactivé.

4. Partage Bluetooth

Contrôle si le partage Bluetooth est autorisé dans le profil personnel d'un appareil appartenant à l'entreprise avec un profil professionnel.

5. Espace privé

Contrôle si un espace privé est autorisé sur l'appareil.

6. Mode Play Store

Ce mode contrôle les applications autorisées ou bloquées pour l'utilisateur dans le Play Store du profil personnel.

> **Liste de blocage (par défaut)** : toutes les applications sont disponibles et toute application qui ne doit pas se trouver sur l'appareil doit être explicitement marquée comme **Bloquée** dans la section **Applications**.
>
> **Liste d'autorisation** : seules les applications explicitement spécifiées dans la section **Applications** avec le **Type d'installation** défini sur **Disponible** sont autorisées à être installées dans le profil personnel.

7. Applications

Liste des applications qui doivent être autorisées ou bloquées sur le profil personnel. Le comportement du contenu de la liste dépend de la valeur définie pour le **Mode Play Store**.

Pour ajouter une nouvelle application depuis le Play Store, cliquez sur l'icône **+**.

7.1. Type d'installation

Types de comportements d'installation qu'une application du profil personnel peut avoir.

> **Bloquée** : l'application est bloquée et ne peut pas être installée dans le profil personnel.
>
> **Disponible** : l'application peut être installée dans le profil personnel.

8. Types de comptes bloqués

Types de comptes qui ne peuvent pas être gérés par l'utilisateur. Cette option empêche les utilisateurs d'appareil d'ajouter des comptes non approuvés sur leur profil personnel.

Stratégies inter-profils

S'applique uniquement aux appareils dotés de profils personnel et professionnel.

Copier/coller inter-profils

Indique si le texte copié dans un profil (personnel ou professionnel) peut être collé dans l'autre profil.

> **Interdit (par défaut)** : empêche les utilisateurs de coller dans le profil personnel du texte copié depuis le profil professionnel. Le texte copié depuis le profil personnel peut être collé dans le profil professionnel.
>
> **Autorisé** : le texte copié dans l'un ou l'autre profil peut être collé dans l'autre profil.

Partage de données inter-profils

Indique si les données d'un profil (personnel ou professionnel) peuvent être partagées avec les applications de l'autre profil. Contrôle spécifiquement le partage simple de données via des intents. La gestion des autres canaux de communication inter-profils, tels que la recherche de contacts, le copier/coller,
ou les applications professionnelles et personnelles connectées, se configure séparément.

> **Interdit** : empêche le partage de données du profil personnel vers le profil professionnel et du profil professionnel vers le profil personnel.
>
> **Professionnel vers personnel interdit (par défaut)** : empêche les utilisateurs de partager des données du profil professionnel avec les applications du profil personnel. Les données personnelles peuvent être partagées avec les applications professionnelles.
>
> **Autorisé** : les données de l'un ou l'autre profil peuvent être partagées avec l'autre profil.

Valeurs par défaut des widgets du profil professionnel

Comportement par défaut des widgets du profil professionnel. Si une application spécifique ne définit pas de stratégie de widgets, elle applique celle définie ici par défaut.

Fonctions d'application inter-profils

Contrôle si les applications du profil personnel peuvent invoquer les fonctions d'application des applications du profil professionnel. Nécessite Android 16 ou version ultérieure.

> Ce paramètre dépend de l'option **Fonctions d'application** au niveau de la stratégie (dans la section Gestion des applications). Si Fonctions d'application est défini sur **Interdit**, l'API rejettera les Fonctions d'application inter-profils définies sur **Autorisé**.

Contacts professionnels dans le profil personnel

Indique si les contacts stockés dans le profil professionnel peuvent apparaître dans les recherches de contacts et les appels entrants du profil personnel.

> **Autorisé (par défaut)** : autorise l'affichage des contacts du profil professionnel dans le profil personnel.
>
> **Interdit** : empêche les applications personnelles d'accéder aux contacts du profil professionnel et de rechercher des contacts professionnels.
>
> **Interdit sauf pour le système** : empêche la plupart des applications personnelles d'accéder aux contacts du profil professionnel, à l'exception des applications Téléphone, Messages et Contacts par défaut de l'OEM (Android 14+).

Lorsque l'option Contacts professionnels dans le profil personnel est configurée, vous pouvez éventuellement définir une liste d'entrées **Nom de package exempté**. Selon le mode sélectionné, ces exemptions se comportent comme une liste d'autorisation ou une liste de blocage pour les applications personnelles.

Rapports d'état

Dans cette section, vous pouvez configurer les données à récupérer depuis l'appareil. Les données d'état peuvent être consultées sur la page du tableau de bord **État de l'appareil**.

Rapports d'application

Indique si les rapports d'application sont activés. (Informations signalées sur une application installée.)

> Cette option est requise par le système (pour l'intégration avec l'application compagnon) et est toujours activée ; elle ne peut pas être désactivée.

Inclure les applications supprimées

Indique si les applications supprimées sont incluses dans les rapports d'application.

Paramètres de l'appareil

Indique si les rapports sur les paramètres de l'appareil sont activés. (Informations sur les paramètres de sécurité de l'appareil.)

Informations logicielles

Indique si les rapports sur les informations logicielles sont activés. (Informations sur le logiciel de l'appareil.)

Informations sur la mémoire

Indique si les rapports sur la mémoire sont activés. (Événement lié aux mesures de mémoire et de stockage.)

Informations réseau

Indique si les rapports sur les informations réseau sont activés. (Informations réseau de l'appareil.)

Informations sur l'écran

Indique si les rapports sur les écrans sont activés. Les données de rapport ne sont pas disponibles pour les appareils appartenant à des particuliers avec profil professionnel. (Informations sur l'écran de l'appareil.)

Événements de gestion de l'alimentation

Indique si les rapports sur les événements de gestion de l'alimentation sont activés. Les données de rapport ne sont pas disponibles pour les appareils appartenant à des particuliers avec profil professionnel.

État du matériel

Indique si les rapports sur l'état du matériel sont activés. Les données de rapport ne sont pas disponibles pour les appareils appartenant à des particuliers avec profil professionnel.

Propriétés système

Indique si les rapports sur les propriétés système sont activés.

Mode Common Criteria

Indique si les rapports sur le mode Common Criteria sont activés.

Divers

1. Jeu easter egg désactivé

Indique si le jeu easter egg des Paramètres est désactivé.

2. Ignorer les conseils de première utilisation

Indicateur permettant d'ignorer les conseils lors de la première utilisation. L'administrateur d'entreprise peut activer la recommandation système invitant les applications à ignorer leur tutoriel utilisateur et autres conseils d'introduction au premier démarrage.

3. Message d'assistance court

Message affiché à l'utilisateur dans l'écran des paramètres partout où une fonctionnalité a été désactivée par l'administrateur. Si le message dépasse 200 caractères, il peut être tronqué.

4. Message d'assistance long

Message affiché à l'utilisateur dans l'écran des paramètres des administrateurs de l'appareil.

5. Informations du propriétaire sur l'écran de verrouillage

Informations du propriétaire de l'appareil à afficher sur l'écran de verrouillage.

6. Actions de configuration

Actions à exécuter pendant le processus de configuration. Lors de l'inscription, vous pouvez exiger que l'utilisateur ouvre une ou plusieurs applications nécessaires à la configuration de l'appareil.

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

6.1. Lancer l'application

Nom de package de l'application à lancer

6.2. Titre

Fournit un message destiné à l'utilisateur pour lui expliquer pourquoi l'application doit être lancée.

6.3. Description

Fournit un message destiné à l'utilisateur pour lui expliquer pourquoi l'application doit être lancée.

7. Visibilité du nom d'affichage de l'entreprise

Contrôle si le nom d'affichage de l'entreprise est visible sur l'appareil (par exemple, sous forme de message sur l'écran de verrouillage des appareils appartenant à l'entreprise).

Visible (par défaut) : le nom d'affichage de l'entreprise est visible sur l'appareil (pris en charge sur les profils professionnels sous Android 7+ et les appareils entièrement gérés sous Android 8+).

Masqué : le nom d'affichage de l'entreprise est masqué sur l'appareil.

Règles de conformité

Si un appareil ou un profil professionnel ne respecte pas l'un des paramètres de stratégie répertoriés ci-dessous, Android Device Policy bloque immédiatement l'utilisation de l'appareil ou du profil professionnel par défaut :

- **Exigences relatives aux mots de passe**
- **Stratégie de chiffrement**
- **Keyguard désactivé**
- **Méthodes de saisie autorisées**
- **Services d'accessibilité autorisés**

Si l'appareil ou le profil professionnel reste non conforme après 10 jours, Android Device Policy réinitialisera l'appareil aux paramètres d'usine ou supprimera le profil professionnel.

Dans cette section, vous pouvez remplacer les règles d'application de conformité par défaut ou en ajouter de nouvelles.

Règles

Liste des règles qui définissent le comportement lorsqu'une stratégie particulière ne peut pas être appliquée à un appareil.

Utilisez **Ajouter une règle** pour créer une nouvelle règle. Chaque carte de règle peut être supprimée à l'aide de l'action de suppression.

Nom du paramètre

La stratégie de niveau supérieur à appliquer. Par exemple, **Applications** ou **Exigences relatives aux mots de passe**.

Obligatoire. La valeur doit correspondre à un nom de stratégie de niveau supérieur pris en charge ; sinon, le champ est marqué comme non valide.

Bloquer après (jours)

Nombre de jours pendant lesquels la stratégie est non conforme avant que l'appareil ou le profil professionnel ne soit bloqué. Pour bloquer l'accès immédiatement, définissez la valeur sur 0. **Bloquer après (jours)** doit être inférieur à **Effacer après (jours)**. Applicable uniquement aux appareils appartenant à l'entreprise.

Plage autorisée : 0–300.

Portée du blocage

Spécifie la portée de l'action de blocage. Applicable uniquement aux appareils appartenant à l'entreprise.

Par défaut (nouvelle règle) : **Profil professionnel**.

> **Profil professionnel** : l'action de blocage s'applique uniquement aux applications du profil professionnel. Les applications du profil personnel ne sont pas affectées.
>
> **Appareil entier** : l'action de blocage s'applique à l'ensemble de l'appareil, y compris aux applications du profil personnel.

Effacer après (jours)

Nombre de jours pendant lesquels la stratégie est non conforme avant que l'appareil ou le profil professionnel ne soit effacé.
Effacer après (jours) doit être supérieur à **Bloquer après (jours)**. Applicable uniquement aux appareils appartenant à l'entreprise.

Obligatoire. Par défaut (nouvelle règle) : **1**.

Plage autorisée : 1–300.

Conserver la protection contre la réinitialisation d'usine

Indique si les données de protection contre la réinitialisation d'usine sont conservées sur l'appareil. Ce paramètre ne s'applique pas aux profils professionnels.

Par défaut (nouvelle règle) : activé.