Politiques - Android

Résumé

Les politiques Android sont les éléments centraux du système : elles définissent les règles qui sont appliquées et mises en œuvre sur les appareils gérés.

Vous pouvez consulter vos politiques et en créer de nouvelles dans la section **Politiques** du tableau de bord. Pour ouvrir une politique Android, cliquez sur la ligne correspondante dans le tableau : le système ouvre la page **Éditeur de politique**.

Une politique peut être associée à un jeton d'inscription, ce qui permet de l'appliquer automatiquement aux appareils pendant le processus de configuration. Vous pouvez également modifier la politique attribuée à un appareil après sa configuration.

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

> De nombreuses options de politique 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.

Mise en page de l'éditeur de politiques

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

- **Nom** (obligatoire)
- **Identifiant** (lecture seule)
- **Description** (facultative)

Les sections ci-dessous correspondent aux panneaux de l'éditeur de politiques (par exemple : gestion des applications, sécurité, réseau, système, utilisation personnelle, politiques multi-profils, etc.). Utilisez les pages de ce manuel pour comprendre chaque panneau en détail.

Enregistrer, supprimer et appareils associés

Utilisez **Enregistrer la politique** pour appliquer vos modifications. Le bouton est désactivé lorsqu'il n'y a pas de modifications en attente, ou lorsque la licence est expirée.

Si vous avez ouvert une politique existante (elle possède un identifiant), la page affiche une action "**Supprimer la politique** ainsi qu'une liste "**Appareils associés** en bas, afin que vous puissiez voir combien d'appareils utilisent actuellement cette politique.

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.

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 à une seule application et le mode kiosque à plusieurs applications dépend de vos objectifs commerciaux.

En **mode borne interactive monopropriétaire**, un appareil est configuré pour une seule application et n'autorise pas les utilisateurs finaux à accéder à d'autres applications sur 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** et définissez le **type d'installation** sur **borne interactive**.

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

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

Lanceur personnalisé pour le mode kiosque

Indique si le lanceur personnalisé pour le mode kiosque est activé. Cela remplace l'écran d'accueil par un lanceur qui verrouille l'appareil aux applications installées via le **Gestion des applications** . Les applications apparaissent sur une seule page, par ordre alphabétique.

Actions du bouton d'alimentation

Définit le comportement d'un appareil en mode kiosque lorsque l'utilisateur appuie longuement sur le bouton d'alimentation.

> **Disponible (par défaut)** : Le menu d’alimentation (par exemple, Éteindre, Redémarrer) s’affiche lorsque l’utilisateur appuie longuement sur le bouton d’alimentation d’un appareil en mode kiosque.
>
> **Bloqué** : Le menu d’alimentation (par exemple, Éteindre, Redémarrer) n’est pas affiché lorsque l’utilisateur appuie longuement sur le bouton d’alimentation d’un appareil en mode kiosque. Note : cela peut empêcher les utilisateurs d’éteindre l’appareil.

Avertissements d'erreurs système

Spécifie si les boîtes de dialogue d'erreurs système pour les applications qui se bloquent ou ne répondent pas sont bloquées en mode kiosque. Lorsqu'elles sont bloquées, le système force la fermeture de l'application, comme si l'utilisateur choisissait l'option "fermer l'application" dans l'interface utilisateur.

Bloqué (par défaut) : Tous les dialogues d'erreur système, tels que les plantages et les applications qui ne répondent pas (ANR), sont bloqués. Lorsqu'ils sont bloqués, le système force la fermeture de l'application, comme si l'utilisateur choisissait de la fermer via l'interface utilisateur.

Activé : Tous les dialogues d'erreur système, tels que les plantages et les applications qui ne répondent pas (ANR), sont affichés.

Navigation système

Spécifie quelles fonctionnalités 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.

Activés : Les boutons Accueil et Aperçu sont activés.

Barre d'état

Indique si les informations système et les notifications sont désactivés en mode kiosque.

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

Informations système uniquement : Seules les informations système sont affichées dans la barre d'état.

Activé : Les informations système et les notifications s'affichent dans la barre d'état en mode kiosque. Remarque : Pour que cette stratégie prenne effet, le bouton d'accueil de l'appareil doit être activé via kioskCustomization.systemNavigation.

Paramètres de l'appareil

Indique 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 politiques relatives à la sécurité.

Actions liées aux risques de sécurité

Choisissez ce qu'il faut faire lorsqu'un appareil signale un risque de sécurité dans les rapports d'état.

Types de risques de sécurité pris en charge :

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

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

L'évaluation basée sur le matériel a échoué : L'API Play Integrity détecte que l'appareil ne dispose pas d'une garantie forte de l'intégrité du système, si l'étiquette MEETS_STRONG_INTEGRITY n'apparaît pas dans le champ de l'intégrité de l'appareil.

Actions disponibles :

Effacer les données de l'entreprise (par défaut) : Désinscrire et effacer les données professionnelles (tout l'appareil si entièrement géré, ou uniquement le profil professionnel pour les appareils gérés par profil).

Aucune action : Ne pas désinscrire l'appareil et ne rien modifier automatiquement.

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

Conserver la protection de réinitialisation d'usine : Conservez les données de protection de réinitialisation d'usine (FRP) lors de l'effacement de l'appareil.

Effacer le stockage externe : Effacez 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. Pour les appareils personnels, cette option supprime les eSIM gérées (les eSIM ajoutées via la commande ADD_ESIM) sur les appareils, et aucune eSIM personnelle ne sera supprimée.

1. Durée maximale de verrouillage

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

2. Rester activé pendant la charge

Les modes de charge pour lesquels l'appareil reste allumé. Lorsque vous utilisez ce paramètre, il est recommandé de désactiver **le verrouillage automatique** afin que l'appareil ne se verrouille pas pendant qu'il est 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. Verrouillage d'écran désactivé

Si cette option est activée, elle désactive l'écran de verrouillage pour les écrans principaux et/ou secondaires. Cette stratégie est prise en charge uniquement en mode de gestion d'appareils dédié.

4. Exigences de mot de passe

Politiques de complexité des mots de passe.

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

Les exigences de mot de passe peuvent utiliser la portée **automatique** (une seule exigence) ou des portées distinctes **appareil**/**profil professionnel**. Les exigences basées sur la complexité doivent être combinées avec des exigences basées sur la qualité pour la même portée.

4.1. Portée

La portée à laquelle s'applique l'exigence de mot de passe.

Automatique : La portée n'est pas spécifiée. Les exigences de mot de passe s'appliquent au profil de travail pour les appareils avec profil de travail, 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. Une fois cette valeur définie, l'utilisateur ne pourra pas utiliser un nouveau mot de passe identique à un mot de passe présent dans l'historique. Une valeur de 0 signifie qu'il n'y a aucune restriction.

4.3. Nombre maximum de tentatives de mot de passe échouées avant suppression

Nombre maximal de mots de passe incorrects pour le déverrouillage de l'appareil avant effacement. Une valeur de 0 signifie qu'il n'y a aucune restriction.

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

Ce paramètre oblige l'utilisateur à modifier régulièrement son mot de passe, après le nombre de jours spécifié.

4.5. Nécessite un déverrouillage par mot de passe

La durée après le déverrouillage d'un appareil ou d'un profil professionnel à l'aide d'une méthode d'authentification forte (mot de passe, code PIN, schéma) pendant laquelle il peut être déverrouillé à l'aide de toute autre méthode d'authentification (par exemple, empreinte digitale, agents de confiance, reconnaissance faciale). Une fois la période spécifiée écoulée, seules les méthodes d'authentification fortes peuvent être utilisées pour déverrouiller l'appareil ou le profil professionnel.

Paramètres par défaut de l’appareil : La période d’attente est définie sur les paramètres par défaut de l’appareil.

Chaque jour : La période de délai d'attente est définie sur 24 heures.

4.6. Qualité du mot de passe

La qualité du mot de passe requise.

Complexité élevée: Définissez la plage de complexité élevée des mots de passe comme suit : Sur Android 12 et versions ultérieures : code PIN sans répétitions (4444) ni séquences

ordonnées (1234, 4321, 2468), longueur minimale de 8 caractères ; alphabétique, longueur minimale de 6 caractères ; alphanumérique, longueur minimale de 6 caractères.

Complexité moyenne : Définissez la plage de complexité moyenne des mots de passe comme suit : code PIN sans répétitions (4444) ni séquences ordonnées (1234, 4321, 2468), longueur minimale de 4 caractères ; alphabétique, longueur minimale de 4 caractères ; alphanumérique, longueur minimale de 4 caractères.

Faible complexité: Définissez la plage de faible complexité des mots de passe comme suit : motif ; code PIN avec répétitions (4444) ou séquences ordonnées (1234, 4321, 2468).

Aucun : Aucune exigence de mot de passe n'est définie.

Faible: L'appareil doit être sécurisé avec une technologie de reconnaissance biométrique de faible sécurité, au minimum. Cela inclut les technologies capables de reconnaître l'identité d'une personne, et qui sont approximativement équivalentes à un code PIN à 3 chiffres (le taux de fausses détections est inférieur à 1 sur 1 000).

N'importe quel: Un mot de passe est requis, mais il n'y a aucune restriction quant au contenu du mot de passe.

Chiffres : Le mot de passe doit contenir des caractères numériques.

Chiffres complexes : Le mot de passe doit contenir des caractères numériques sans séquences répétées (par exemple, 4444) ou ordonnées (par exemple, 1234, 4321, 2468).

Alphabétiques : Le mot de passe doit contenir des caractères alphabétiques (ou des symboles).

Alphanumériques : Le mot de passe doit contenir à la fois des chiffres et des caractères alphabétiques (ou des symboles).

Complexe : Le mot de passe doit répondre aux exigences minimales spécifiées dans passwordMinimumLength, passwordMinimumLetters, passwordMinimumSymbols, etc. Par exemple, si passwordMinimumSymbols est égal à 2, le mot de passe doit contenir au moins deux symboles.

4.7. Longueur minimale

La longueur minimale autorisée pour le mot de passe. Une valeur de 0 signifie qu'il n'y a aucune restriction.

4.8. Minimum de lettres

Nombre minimum de caractères requis pour le mot de passe.

4.9. Minimum de lettres minuscules

Minimum de lettres minuscules requises dans le mot de passe.

4.10. Minimum de lettres majuscules

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

4.11. Nombre minimum de caractères non alphabétiques requis

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

4.12. Nombre minimum de chiffres

Nombre minimum de chiffres requis dans le mot de passe.

4.13. Nombre minimum de symboles

Nombre minimum de symboles requis dans le mot de passe.

4.14. Verrouillage unifié

Activez ou désactivez le verrouillage unifié pour l'appareil et le profil professionnel, sur les appareils Android 9 et versions ultérieures disposant d'un profil professionnel. Cette option n'a aucun effet sur les autres appareils.

> **Autoriser le verrouillage unifié** : Permet d'utiliser un même verrouillage pour l'appareil et le profil professionnel.
>
> **Exiger un verrouillage distinct pour le profil professionnel** : Un verrouillage distinct est requis pour le profil professionnel.

5. Réinitialisation aux paramètres d'usine désactivée

La possibilité de réinitialiser aux paramètres d'usine depuis les paramètres est désactivée. Ceci ne s'applique qu'aux appareils entièrement gérés.

6. Protection contre la réinitialisation aux paramètres d'usine

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

Adresses e-mail des administrateurs : utilisez **Activer la protection contre la réinitialisation d'usine** pour commencer à configurer les administrateurs. Ensuite, utilisez **Ajouter une adresse e-mail d'administrateur** pour ajouter des adresses et les supprimer avec l'action de suppression.

7. Fonctionnalités de Keyguard

Fonctionnalités de l'écran de verrouillage (Keyguard) qui peuvent être désactivées.

7.1. Désactiver tout

Désactiver toutes les personnalisations actuelles et futures de l'écran de verrouillage.

7.2. Désactiver la caméra

Désactiver la caméra sur les écrans de verrouillage sécurisés (par exemple, code PIN).

7.3. Désactiver les notifications

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

7.4. Désactiver les notifications sans censure

Désactiver les notifications non censurées sur les écrans de verrouillage sécurisés.

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

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

7.6. Désactiver l'empreinte digitale

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

7.7. Désactiver la saisie de texte dans les notifications

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

7.8. Désactiver l'authentification par reconnaissance faciale

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

7.9. Désactiver l'authentification par reconnaissance de l'iris

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

7.10. Désactiver toutes les méthodes d'authentification biométrique

Désactiver toutes les méthodes d'authentification biométrique sur les écrans de verrouillage sécurisés.

7.11. Désactiver tous les raccourcis

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

Multimédia

Dans cette section, vous pouvez configurer le comportement de l'appareil photo/du microphone, l'accès aux données USB, l'impression et les restrictions relatives à l'affichage.

1. Accès à l'appareil photo

Contrôle l'utilisation de l'appareil photo et permet à l'utilisateur d'activer ou de désactiver l'accès à l'appareil photo (Android 12+). En général, la désactivation de l'appareil photo 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 accessibles, et (Android 12+) l'utilisateur peut activer ou désactiver l'accès à la caméra.
>
> **Désactivé** : Toutes les caméras sont désactivées (mode entièrement géré : à l'échelle de l'appareil ; profil professionnel : uniquement pour les applications du profil professionnel). Le commutateur d'accès à la caméra n'a aucun effet dans le contexte géré.
>
> **Autorisé** : Les caméras sont accessibles. Sur les appareils entièrement gérés exécutant Android 12 ou supérieur, l'utilisateur ne peut pas activer ou désactiver l'accès à la caméra. Sur les autres appareils/versions, le comportement est similaire au choix de l'utilisateur.

2. Accès au microphone

Sur les appareils entièrement gérés, contrôle l'utilisation du microphone et indique si l'utilisateur peut activer ou désactiver l'accès au microphone (Android 12 et versions ultérieures). Ce paramètre n'a aucun effet sur les appareils qui ne sont pas entièrement gérés.

> **Choix utilisateur (par défaut)** : Comportement par défaut. Le microphone est accessible et (Android 12+) l'utilisateur peut activer ou désactiver l'accès au microphone.
>
> **Désactivé** : Le microphone est désactivé (au niveau de l'appareil). Le commutateur d'accès au microphone n'a aucun effet.
>
> **Appliquée** : Le microphone est accessible. Sur Android 12 et versions ultérieures, l'utilisateur ne peut pas activer ou désactiver l'accès au microphone. Sur Android 11 et versions antérieures, le comportement est identique à celui d'un choix de l'utilisateur.

3. Accès aux données via USB

Contrôle les fichiers et/ou les données qui peuvent être transférés via USB. Disponible uniquement sur les appareils appartenant à l'entreprise.

Interdire le transfert de fichiers (par défaut) : Le transfert de fichiers est désactivé, mais d'autres connexions USB (par exemple, souris/clavier) restent 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 fonctionnalité n'est pas prise en charge, l'appareil revient à l'option "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.

Non autorisé: L'impression n'est pas autorisée (Android 9 et versions ultérieures).

5. Paramètres de luminosité de l'écran

Contrôle le mode de luminosité de l'écran et (facultativement) la valeur de luminosité.

Mode de luminosité de l'écran :

Choix utilisateur (par défaut): L'utilisateur peut configurer la luminosité de l'écran.

Automatique : La luminosité est réglée automatiquement et l'utilisateur ne peut pas la modifier. Vous pouvez toujours définir une valeur de luminosité, qui est utilisée dans le cadre du réglage automatique (Android 9+ avec gestion complète ; profils professionnels sur les appareils Android 15+ appartenant à l'entreprise).

Fixe : La luminosité est réglée sur la valeur configurée et l'utilisateur ne peut pas la modifier. La valeur de luminosité est obligatoire (Android 9+ avec gestion complète ; profils professionnels sur les appareils Android 15+ appartenant à l'entreprise).

Luminosité de l'écran : la valeur est fixée et ne peut être modifiée par l'utilisateur. La valeur de luminosité est obligatoire (Android 9+ avec gestion complète ; profils professionnels sur les appareils Android 15+ appartenant à l'entreprise)

Valeur comprise entre 1 et 255 (1 = minimum, 255 = maximum). Une valeur de 0 indique qu'aucune luminosité n'est définie.

6. Paramètres du délai d'inactivité de l'écran

Contrôle si l'utilisateur peut configurer le délai d'inactivité de l'écran et, si cette option est imposée, la valeur du délai.

Le champ **Mode de délai d'inactivité 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 peut configurer le délai d'inactivité de l'écran.

Imposé : Le délai d'inactivité de l'écran est défini sur la valeur configurée et l'utilisateur ne peut pas le modifier (Android 9+ avec gestion complète ; profils professionnels sur les appareils Android 15+ appartenant à l'entreprise).

Temps d'attente avant extinction de l'écran : la valeur est définie par configuration et ne peut pas être modifiée par l'utilisateur (Android 9+ avec gestion complète ; profils professionnels sur les appareils Android 15+ appartenant à l'entreprise)

Durée du délai en secondes. La valeur doit être supérieure à 0. Si elle est supérieure à **durée maximale de verrouillage**, le système peut la limiter et signaler une non-conformité.

7. La capture d'écran est désactivée

La capture d'écran est-elle désactivée ?

8. Ajustement du volume désactivé

Que l'ajustement du volume principal soit désactivé.

9. Montage des supports physiques désactivé

Le montage des supports externes physiques est-il désactivé ?

Cellulaire

Dans cette section, vous pouvez configurer les politiques relatives à la connectivité cellulaire.

Mode avion

Permet de contrôler si l'utilisateur peut activer ou désactiver le mode avion.

Choix utilisateur (par défaut) : L'utilisateur peut activer ou désactiver le mode avion.

Désactivé : Le mode avion est désactivé. L'utilisateur ne peut pas activer ou désactiver le mode avion. Compatible avec Android 9 et versions ultérieures.

2. Cellulaire 2G

Permet de contrôler si l'utilisateur peut activer ou désactiver le paramètre cellulaire 2G.

Choix utilisateur (par défaut): L'utilisateur peut activer ou désactiver la connexion cellulaire 2G.

Désactivé : La connexion cellulaire 2G est désactivée. L'utilisateur ne peut pas activer la connexion cellulaire 2G via les paramètres. Disponible sur Android 14 et versions ultérieures.

3. Ignorer les APNs

Activez ou désactivez l'utilisation des APNs personnalisés. Lorsque cette option est activée, seuls les APNs personnalisés configurés sont utilisés, et tous les autres APNs sur l'appareil sont ignorés.

Désactivé (par défaut) : Tous les paramètres APN configurés sont enregistrés sur l'appareil, mais ils sont désactivés et n'ont aucun effet. Tous les autres APN sur l'appareil restent actifs.

Activé : Seuls les profils APN définis dans cette configuration sont utilisés, tous les autres profils APN sont ignorés. Ce paramètre ne peut être configuré que sur les appareils entièrement gérés avec Android 10 et versions ultérieures.

4. Paramètres APN

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

Chaque APN possède 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 utilisateur.

Champs APN facultatifs :

Type d'authentification, **Nom d'utilisateur**, **Mot de passe** : Configurez l'authentification du transporteur (si nécessaire).

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

Types de réseau : Limitez les technologies cellulaires que le profil APN peut utiliser (par exemple, LTE/5G NR).

Adresse du proxy et **Port du proxy** : Serveur proxy HTTP pour le trafic de données (si applicable).

Adresse du serveur proxy MMS, **Port du serveur proxy MMS**, **MMSC (URI du centre MMS)** : Paramètres liés à MMS.

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

Paramètre Toujours Actif : Indique si la session PDU activée par ce APN doit être maintenue active en permanence. Supporté sur Android 15 et versions ultérieures.

Type d'opérateur virtuel : Type d'identifiant de l'opérateur de réseau virtuel mobile.

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

5. La configuration de la diffusion cellulaire est désactivée

Que la configuration de la diffusion cellulaire est désactivée.

6. Configuration des réseaux mobiles : désactivé

La configuration des réseaux mobiles est-elle désactivée ?

7. Les données en itinérance sont désactivées

Si les services de données en itinérance sont désactivés.

8. Appels sortants désactivés

Que les appels sortants soient désactivés ou non.

9. SMS désactivé

L'envoi et la réception des SMS sont-ils désactivés.

10. Configuration du découpage réseau 5G

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

10.1. Réseau prioritaire par défaut

Identifiant du réseau prioritaire par défaut pour les applications qui ne figurent pas dans la liste des applications, ou si le **Réseau prioritaire** d'une application n'est pas configuré. Une configuration pour l'identifiant de réseau spécifié est requise (sauf si elle est définie sur **Aucun réseau prioritaire**).

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

10.2. Configurations des services réseau

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

> **Identifiant de réseau préféré (attribué automatiquement)** : L'identifiant de réseau est attribué automatiquement et ne peut pas être modifié.

Revenir à la connexion par défaut : Indique si le système doit revenir à la connexion réseau par défaut de l'appareil. Si cette option est désactivée, les applications ne peuvent pas accéder à Internet si la tranche 5G n'est pas disponible.

Réseaux incompatibles : Indique si les applications soumises à cette configuration peuvent utiliser des réseaux autres que le service préféré. Si cette option est définie sur **Non autorisé**, l'option **Revenir à la connexion par défaut** doit également être définie sur **Non autorisé**. Nécessite Android 14 et versions ultérieures.

Réseau

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

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

État de la radio de l'appareil

1. État du Wi-Fi

Contrôle de l'état actuel du Wi-Fi et de la possibilité pour l'utilisateur de le modifier.

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

2. Niveau de sécurité Wi-Fi minimum

Le niveau de sécurité Wi-Fi minimum requis pour les réseaux auxquels l'appareil peut se connecter. Supporté sur 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 publics ; requiert au moins une sécurité de niveau personnel (par exemple, WPA2-PSK).
>
> **Réseau d'entreprise** : Nécessite des réseaux EAP d'entreprise ; interdit les réseaux Wi-Fi ayant un niveau de sécurité inférieur.

Réseau d'entreprise 192 bits : Nécessite des réseaux d'entreprise 192 bits ; option la plus sécurisée.

3. État de la technologie à très large bande (UWB)

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

Choix utilisateur (par défaut): L'utilisateur peut activer ou désactiver UWB.

Désactivé : UWB est désactivé et l'utilisateur ne peut pas le réactiver via les paramètres (Android 14 et versions ultérieures).

Gestion de la connectivité des appareils

4. Partage via Bluetooth

Activez ou désactivez le partage via Bluetooth.

Autorisé : Le partage via Bluetooth est autorisé (par défaut sur les appareils entièrement gérés, Android 8 et versions ultérieures).

Non autorisé : Le partage via Bluetooth est désactivé (par défaut pour les profils d'entreprise, Android 8 et versions ultérieures).

5. Configurez le Wi-Fi

Contrôle des privilèges de configuration Wi-Fi. Selon l'option sélectionnée, l'utilisateur dispose d'un contrôle total, limité ou inexistant 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 et versions ultérieures ; profils professionnels gérés et appartenant à l'entreprise).

Interdire la configuration du Wi-Fi : Empêche la configuration de réseaux Wi-Fi. Pour les appareils entièrement gérés, cela supprime les réseaux configurés par l'utilisateur et conserve uniquement les réseaux configurés via **les configurations Wi-Fi**. Pour les profils

professionnels d'entreprise, les réseaux existants ne sont pas affectés, mais les utilisateurs ne peuvent pas ajouter, supprimer ou modifier les réseaux Wi-Fi.

> Lorsque la configuration Wi-Fi est désactivée et que l'appareil ne peut pas se connecter au démarrage, le système peut afficher la **fonction de contournement réseau** pour permettre à l'utilisateur de se connecter temporairement et de rafraîchir la configuration.

6. Paramètres de la connexion Wi-Fi Direct

Paramètres de configuration et d'utilisation de la connexion Wi-Fi Direct. Supporté sur les appareils appartenant à l'entreprise et fonctionnant sous Android 13 et versions ultérieures.

Autoriser (par défaut) : L'utilisateur est autorisé à utiliser la connexion Wi-Fi Direct.

Interdire : L'utilisateur n'est pas autorisé à utiliser la connexion Wi-Fi Direct.

7. Paramètres du partage de connexion

Contrôle les paramètres du partage de connexion. En fonction de la valeur définie, l'utilisateur peut être partiellement ou totalement empêché d'utiliser différentes formes de partage de connexion.

Autoriser toutes les options de partage de connexion (par défaut) : Permet la configuration et l'utilisation de toutes les formes de partage de connexion.

Interdire le partage de connexion Wi-Fi : Empêche l'utilisateur d'utiliser le partage de connexion Wi-Fi (appareils Android 13 et versions ultérieures appartenant à l'entreprise).

Interdire tout le partage de connexion : Empêche toutes les formes de partage de connexion (appareils entièrement gérés et profils professionnels appartenant à l'entreprise).

8. Politique du 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). Disponible sur les appareils appartenant à l'entreprise et exécutant Android 13 et versions ultérieures.

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

Liste blanche des SSID : L'appareil ne peut se connecter qu'aux réseaux Wi-Fi dont le SSID figure dans cette liste. La liste des SSID ne doit pas être vide.

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

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 interdits** pour les listes de blocage.

9. Paramètres de compatibilité Wi?Fi

Configurez le mode de compatibilité Wi-Fi par SSID. Utilisez **Ajouter un paramètre de compatibilité Wi-Fi** pour créer des entrées.

Chaque entrée comprend :

> **SSID** : L'identifiant SSID auquel s'applique le paramètre de roaming (obligatoire).
>
> **Mode de roaming Wi-Fi** : Par défaut / Désactivé / Adaptatif. Les modes Désactivé et Adaptatif nécessitent Android 15 et ne sont pris en charge que sur les appareils entièrement gérés et les profils d'entreprise sur les appareils appartenant à l'entreprise.

Restrictions réseau

Bluetooth désactivé

Le Bluetooth est-il désactivé ? (Privilégiez ce paramètre plutôt que "Configuration Bluetooth désactivée", car cette dernière peut être contournée par l'utilisateur).

11. Le partage de contacts via Bluetooth est désactivé

Que le partage de contacts via Bluetooth est désactivé.

12. La configuration Bluetooth est désactivée

Que la configuration Bluetooth est désactivée.

13. Réinitialisation du réseau désactivée

Que la réinitialisation des paramètres réseau est désactivée.

14. Transmission en flux désactivée

L'utilisation de la technologie NFC pour transmettre des données depuis les applications est désactivée.

VPN

Application VPN toujours activée

Spécifiez un nom de package VPN permanent pour vous assurer que les données des applications gérées spécifiées transitent toujours par un VPN configuré.

> Note : Cette fonctionnalité nécessite le déploiement d'un client VPN prenant en charge à la fois les fonctionnalités VPN permanentes et VPN par application.

16. Blocage VPN

Empêche l'accès au réseau lorsque le VPN n'est pas connecté.

17. Configuration VPN désactivée

Que la configuration VPN soit désactivée.

Services proxy et réseau

18. Service réseau prioritaire

Activez ou désactivez le service réseau prioritaire sur le profil professionnel. Par exemple, une entreprise peut avoir un accord avec un opérateur qui prévoit que les données professionnelles sont envoyées via un service réseau dédié aux entreprises (par exemple, une tranche réservée aux entreprises sur les réseaux 5G). Cela n'a aucun effet sur les appareils entièrement gérés.

Désactivé : Le service réseau prioritaire est désactivé sur le profil professionnel.

Activé : Le service réseau prioritaire est activé sur le profil professionnel.

> Si vous utilisez le découpage de réseau entreprise, configurez également **Configuration du découpage réseau 5G** dans le panneau de la politique **Cellulaire** et attribuez des applications à un segment en utilisant leur paramètre **Réseau Prioritaire**.

19. Proxy global recommandé

Le proxy HTTP global indépendant du réseau. En général, les proxies doivent être configurés pour chaque réseau dans les paramètres WiFi. Un proxy global peut être utile pour des configurations inhabituelles, comme le 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, ce sont les hôtes pour lesquels le proxy est contourné. Les noms d'hôtes 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 réseau Wi-Fi que le système appliquera aux 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.

Nom du réseau : Obligatoire.

Connexion automatique : Indique si le réseau doit se connecter automatiquement lorsque vous êtes dans sa portée.

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

SSID masqué : Indique si le SSID doit être diffusé.

Mode de randomisation de l'adresse MAC : Matériel ou Automatique (Android 13 et versions ultérieures).

20.1. Sécurité

Options de sécurité Wi-Fi :

WEP-PSK : WEP (clé prépartagée).

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

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

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

20.2. Phrase de passe (clé pré-partagée)

Affiché lorsque la sécurité est **WEP-PSK** ou **WPA-PSK**. La phrase de passe est requise.

20.3. Méthode EAP (Entreprise)

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

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Authentification, phase 2

Affiché pour le tunneling des méthodes externes (**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 aux appareils, par utilisateur. Vous pouvez configurer les identifiants utilisateur 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 **Modifier le certificat** pour en sélectionner un autre.

Alternativement, vous pouvez spécifier **l'alias de la paire de clés du certificat client**, qui fait référence à un certificat client stocké dans le trousseau Android et autorisé pour l'authentification Wi-Fi.

> Si le **certificat client** et l'alias de la paire de clés du **certificat client** sont spécifiés, l'alias de la paire de clés est ignoré.

20.7. Identité

Identité de l'utilisateur. Pour le tunneling des protocoles externes (PEAP, EAP-TTLS), ceci est utilisé pour l'authentification à l'intérieur du tunnel, et **l'identité anonyme** est utilisée pour l'identité EAP à l'extérieur du tunnel. Pour les protocoles externes non utilisant le tunneling, ceci est utilisé pour l'identité EAP.

20.8. Identité anonyme

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

20.9. Mot de passe

Mot de passe de l'utilisateur. Si non spécifié, le système invite l'utilisateur à le saisir.

20.10. Certificats CA du serveur

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

Utilisez **l'option Ajouter le certificat CA du serveur** pour ajouter des entrées et les supprimer à l'aide de l'action supprimer.

20.11. Le suffixe de domaine correspond

Une liste de contraintes pour le nom de domaine du serveur. Ces entrées sont utilisées comme exigences de correspondance de suffixe par rapport au(x) nom(s) DNS du nom de sujet alternatif d'un certificat de serveur d'authentification.

Système

Dans cette section, vous pouvez configurer les politiques relatives au système.

1. Niveau d'API minimum

Le niveau d'API Android minimum autorisé.

2. Politique 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**: Le chiffrement est requis, mais aucun mot de passe n'est nécessaire pour le démarrage.
>
> **Activé avec mot de passe**: Le chiffrement est requis et un mot de passe est nécessaire pour le démarrage.

3. Date et heure automatiques

Indique si la synchronisation automatique de la date, de l'heure et du fuseau horaire est activée sur un appareil appartenant à l'entreprise.

> **Choix de l'utilisateur (par défaut)**: La synchronisation automatique de la date, de l'heure et du fuseau horaire est laissée au choix de l'utilisateur.
>
> **Obligatoire**: Activer la synchronisation automatique de la date, de l'heure et du fuseau horaire sur l'appareil.

4. Paramètres pour les développeurs

Contrôle l'accès aux paramètres développeur : options pour les développeurs et démarrage sécurisé.

Désactivé (par défaut) : Désactive tous les paramètres pour développeurs et empêche l'utilisateur d'y accéder.

Autorisé : Permet l'accès à tous les paramètres pour développeurs. L'utilisateur peut accéder et, éventuellement, configurer ces paramètres.

5. Mode de conformité aux critères communs

Modes de sécurité standard : normes de sécurité définies dans le référentiel Common Criteria pour l'évaluation de la sécurité des technologies de l'information. L'activation du mode Common Criteria renforce certains composants de sécurité d'un appareil (par exemple, le chiffrement AES-GCM des clés à long terme Bluetooth, une validation supplémentaire pour certains certificats réseau et des vérifications de l'intégrité des politiques cryptographiques). Le mode Common Criteria est pris en charge uniquement sur les appareils appartenant à l'entreprise et exécutant Android 11 ou une version ultérieure. Attention : le mode Common Criteria applique un modèle de sécurité strict, généralement requis uniquement pour les organisations traitant des informations très sensibles. L'utilisation normale de l'appareil peut être affectée ; activez-le uniquement si nécessaire.

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

Activé : Active le mode Common Criteria.

6. Extension de marquage de la mémoire (MTE)

Active ou désactive l'extension de marquage de la mémoire (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).

Obligatoire : MTE est activé et l'utilisateur ne peut pas le désactiver (Android 14 et versions ultérieures ; pris en charge sur les appareils entièrement gérés et les profils professionnels sur les appareils appartenant à l'entreprise).

Désactivé : MTE est désactivé et l'utilisateur ne peut pas le modifier (Android 14 et versions ultérieures ; pris en charge uniquement sur les appareils entièrement gérés).

7. Protection du contenu

Active ou désactive la protection du contenu (qui analyse la présence d'applications potentiellement malveillantes). 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 modifier ce paramètre.

Activée (obligatoire): La protection du contenu est activée et l'utilisateur ne peut pas modifier ce paramètre (Android 15 et versions ultérieures).

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

8. Assistance au contenu

Permet de déterminer si l'envoi de contenu d'assistance à une application privilégiée, telle qu'une application d'assistance (par exemple, Circle to Search), est autorisé. Le contenu d'assistance comprend des captures d'écran et des informations sur une application, telles que le nom du package. Cette fonctionnalité est prise en charge sur Android 15 et versions ultérieures.

Autorisé (par défaut) : L'envoi de contenu d'assistance à une application privilégiée (Android 15 et versions ultérieures) est autorisé.

Interdit : L'envoi de contenu d'assistance à une application privilégiée est bloqué (Android 15 et versions ultérieures).

9. Créez des fenêtres désactivées

Que la création de fenêtres en dehors des fenêtres d'application soit désactivée. Cette option empêche l'affichage des éléments d'interface système suivants : notifications et barres de notification, activités du téléphone (telles que les appels entrants) et activités téléphoniques prioritaires (telles que les appels en cours), alertes système, erreurs système et superpositions système.

10. Porte de sortie réseau

Indique si la fonctionnalité de secours réseau est activée. Si une connexion réseau ne peut pas être établie au démarrage, la fonctionnalité de secours invite l'utilisateur à se connecter temporairement à un réseau afin de mettre à jour la configuration de l'appareil. Une fois la configuration appliquée, la connexion temporaire est oubliée et l'appareil continue de démarrer. Cela permet d'éviter l'impossibilité de se connecter à un réseau si aucun réseau approprié n'est défini dans la configuration et que l'appareil démarre dans une application en mode "lock task", ou si l'utilisateur ne peut pas accéder aux paramètres de l'appareil.

11. Activités par défaut

Une liste des activités par défaut pour gérer les intentions qui correspondent à un filtre d'intention spécifique. Par exemple, cette fonctionnalité permettrait aux administrateurs informatiques de choisir quelle application de navigateur s'ouvre automatiquement pour les liens web, ou quelle application de lanceur est utilisée lorsqu'on 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 définir le filtre d'intention.

11.1. Activité du récepteur

L'activité qui doit être le gestionnaire d'intent par défaut. Il s'agit d'un nom de composant Android, par exemple com.android.enterprise.app/.MainActivity. Alternativement, la valeur peut être le nom du package d'une application, ce qui permet à Android Device Policy de choisir une activité appropriée dans cette application pour gérer l'intent.

11.2. Action

Les actions à faire correspondre dans le filtre. Si des actions sont incluses dans le filtre, l'action de l'intent doit correspondre à l'une de ces valeurs pour qu'il soit pris en compte. S'il n'y a pas d'actions incluses, l'action de l'intent est ignorée.

11.3. Catégorie

Les catégories d'intentions à prendre en compte dans le filtre. Une intention inclut les catégories qu'elle requiert, et toutes doivent être incluses dans le filtre pour qu'il corresponde. En d'autres termes, ajouter une catégorie au filtre n'a aucun impact sur la correspondance, sauf si cette catégorie est spécifiée dans l'intention.

12. Méthodes de saisie autorisées

Spécifie les méthodes de saisie autorisées.

> **Autorisées :** Aucune restriction n'est appliquée. Toutes les méthodes de saisie sont autorisées.
>
> **Uniquement les méthodes de saisie** du système : Seules les méthodes de saisie intégrées au système sont autorisées.
>
> **Seules les méthodes de saisie** intégrées au système et celles fournies sont autorisées.

12.1. Méthodes de saisie autorisées

Noms de packages de méthodes de saisie autorisés. S'applique uniquement lorsque **Méthodes de saisie autorisées** est défini sur **Uniquement les méthodes du système et celles fournies**.

Utilisez **l'option Ajouter une méthode de saisie** pour ajouter des éléments 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.
>
> **Seuls les services** : Seuls les services d'accessibilité intégrés au système peuvent être utilisés.
>
> **Seuls les services** : Seuls les services d'accessibilité intégrés au système et ceux fournis peuvent être utilisés.

13.1. Services d'accessibilité autorisés

Services d'accessibilité autorisés. S'applique uniquement lorsque **Services d'accessibilité autorisés** est défini sur **Uniquement les services système et fournis**.

Utilisez **l'option Ajouter un service d'accessibilité** pour ajouter des éléments et les supprimer avec l'action de suppression.

14. Stratégie de mise à jour du système

Configuration pour gérer les mises à jour du système.

> **Par défaut**: Suivez le comportement par défaut des mises à jour pour l'appareil, ce qui nécessite généralement que l'utilisateur accepte les mises à jour du système.
>
> **Automatique**: Installer automatiquement dès qu'une mise à jour est disponible.
>
> **Mode fenêtré** : Installation automatique pendant une plage horaire de maintenance quotidienne. Cela configure également les applications Play pour qu'elles soient mises à jour pendant cette plage horaire. Il est fortement recommandé pour les appareils en mode kiosque, car c'est la seule façon pour les applications épinglées en permanence au premier plan de pouvoir être mises à jour via Play.
>
> **Reporter** : Reportez l'installation automatique jusqu'à un maximum de 30 jours.

14.1. Fenêtre de maintenance (Uniquement fenêtré)

Lorsque la **politique de mise à jour du système** est définie sur **Mode graphique**, vous pouvez définir la fenêtre de maintenance quotidienne à l'aide des champs **depuis** et **jusqu'à**.

14.2. Périodes de suspension des mises à jour système

Une période annuelle pendant laquelle les mises à jour système sans fil (OTA) sont reportées afin de figer la version du système d'exploitation exécutée sur un appareil. Pour éviter de bloquer définitivement l'appareil, chaque période de suspension doit être séparée d'au moins 60 jours. Chaque période de suspension ne doit pas dépasser 90 jours.

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

15. Fournisseurs de crédentiels par défaut

Contrôle les applications autorisées à agir en tant que fournisseurs de crédentiels sur Android 14 et versions ultérieures.

> **Non autorisées (par défaut)**: Les applications dont la politique de fournisseur de crédentiels n'est pas spécifiée ne sont pas autorisées à agir en tant que fournisseur de crédentiels.
>
> **Non autorisées, sauf pour le système**: Les applications dont la politique de fournisseur de crédentiels n'est pas spécifiée ne sont pas autorisées à agir en tant que fournisseur de crédentiels, sauf pour les fournisseurs de crédentiels par défaut du fabricant de l'appareil.

Emplacement et périmètre géographique

Ce panneau regroupe les paramètres de stratégie Android qui contrôlent l’envoi des données de localisation, l’application des règles de géolocalisation et la définition des périmètres. Utilisez-le lorsque vous souhaitez que Cerberus Enterprise collecte les positions des appareils ou détecte quand ils entrent ou sortent de zones configurées.

Rapports de localisation

Signaler la position

Active la déclaration géolocalisation de l’appareil. Les données de localisation collectées via ce paramètre sont utilisées par le **tableau de bord des emplacements**, l’historique des emplacements dans la vue d’ensemble de l’appareil et le traitement des géofences.

> Sur les appareils qui ne sont pas entièrement gérés, l’accès aux données de localisation peut toujours dépendre des autorisations de localisation requises pour l’application Cerberus Enterprise et de l’activation des services de localisation sur l’appareil.

Mode de géolocalisation

Contrôle le paramètre de localisation des appareils appartenant à l'entreprise.

- **Choix de l'utilisateur** : les services de localisation ne sont pas restreints par la politique.
- **Appliqué**: les services de localisation sont activés sur l'appareil.
- **Désactivé**: les services de localisation sont désactivés sur l'appareil.

Partage de la localisation désactivé

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

Comportement automatique avec des géosalles actives

Les géosalles actives nécessitent l'envoi de données de localisation pour fonctionner. Lorsqu'au moins une géosalle est active, Cerberus Enterprise maintient automatiquement les paramètres de localisation associés.

- **L'envoi de la position** est forcé lorsque des géosalles actives sont présentes.
- **Mode localisation** est forcé sur **Actif**.
- **Le partage de la position est désactivé** et forcé sur Off.

Si vous essayez de désactiver **Signaler la position** alors qu'une ou plusieurs clôtures géographiques sont actives, Cerberus Enterprise affiche une boîte de dialogue de confirmation. Si vous continuez, toutes les clôtures géographiques actives dans la stratégie sont désactivées.

Liste des clôtures géographiques

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

Utilisez **Ajouter une clôture géographique** pour créer une nouvelle entrée. Chaque clôture géographique contient les champs principaux suivants :

- **Nom** : requis et unique.
- **Latitude** et **Longitude** : le centre de la zone.
- **Rayon (m)**: requis, de **100** à **10000** mètres.
- **Description**: notes optionnelles pour les administrateurs.
- **Rapport d'entrée** et **Rapport de sortie** : sélectionnez les événements de transition à générer.
- **Actif** : active ou désactive la géoperimètre sans la supprimer.

> Au moins un des **Report d'entrée** ou **Report de sortie** doit rester activé pour chaque géoperimètre.

Outils de modification de la carte

Chaque carte de géofence inclut un aperçu cartographique de la zone. Vous pouvez modifier la géométrie directement sur la carte ou à partir des champs numériques.

- Cliquez sur la carte pour déplacer le centre de la géofence lorsque l'édition de zone est activée.
- Utilisez le bouton **Position actuelle** pour centrer la carte sur votre position de navigateur actuelle.
- Utilisez le bouton **Recentrer la carte** pour restaurer la vue préférée pour cette zone géographique.
- Utilisez le bouton de verrouillage pour éviter toute modification accidentelle de la géolocalisation.

Où apparaissent les données de géocage

Les transitions de géocage peuvent être consultées dans la page **Aperçu de l’appareil**, dans l’onglet **Géocage** du panneau de localisation. Cet onglet affiche les transitions sur une carte dédiée, ainsi que des outils de filtrage et la liste des transitions.

Gestion des utilisateurs

Ajouter un utilisateur désactivé

L'ajout de nouveaux utilisateurs et profils peut être désactivé. Pour les appareils où managementMode est **DEVICE_OWNER**, ce champ est ignoré et l'utilisateur n'a jamais la possibilité d'ajouter ou de supprimer des utilisateurs.

Modifier les comptes désactivés

Que l'ajout ou la suppression de comptes soit désactivé.

La configuration des identifiants utilisateur est désactivée

La configuration des identifiants utilisateur est-elle désactivée ?

Supprimer l'utilisateur désactivé

Que la suppression d'autres utilisateurs soit désactivée.

Définir l'icône utilisateur comme désactivée

Que le changement de l'icône utilisateur soit désactivé.

Définir le fond d'écran est désactivé

Que le changement de fond d'écran soit désactivé.

Authentification de la configuration du compte professionnel

Contrôle la méthode d'authentification des utilisateurs lors de la configuration du compte professionnel. Cette option est uniquement disponible pour les entreprises Android utilisant un domaine Google géré (Google Workspace).

Pendant la configuration/l'inscription de l'appareil, cette stratégie détermine si une authentification pour le compte professionnel est requise, mais le paramètre de la console d'administration Google **Authentification via Google** et le type de jeton d'inscription peuvent toujours nécessiter une authentification.

Pour les appareils déjà inscrits, cette stratégie s'applique uniquement si l'appareil est géré par un compte Google Play d'entreprise (c'est-à-dire, inscrit sans **authentification via Google**).

Pour plus de détails et pour résoudre les problèmes, consultez **Authentification via Google**.

Types de comptes bloqués

Types de comptes que l'utilisateur ne peut pas gérer. Cette option empêche les utilisateurs de l'appareil d'ajouter des comptes non autorisés.

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

Chaque entrée possède un champ "**Type de compte**" (obligatoire). Entrez une chaîne de caractères comme **com.google**. Supprimez une entrée en utilisant l'action de suppression.

Utilisation personnelle

Lorsque vous configurez un appareil de l'entreprise pour un usage professionnel et personnel, vous pouvez définir certaines règles pour limiter la manière dont l'utilisateur peut utiliser l'appareil pour un usage personnel, en dehors du profil professionnel.

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

1. Appareil photo désactivé

L'appareil photo est-il désactivé ?

2. La capture d'écran est désactivée

La capture d'écran est-elle désactivée ?

3. Nombre maximal de jours de congé

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

4. Partage via Bluetooth

Active ou désactive le partage Bluetooth dans le profil personnel d'un appareil appartenant à l'entreprise et disposant d'un profil professionnel.

5. Espace privé

Active ou désactive l'autorisation d'espaces privés sur l'appareil.

6. Mode Google Play

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

Liste bloquée (par défaut) : 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 section **Applications**.

Liste autorisée : Seules les applications spécifiées explicitement dans la section **Applications** et dont le **Type d'installation** est défini sur **Disponible** peuvent 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 cette 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 de profil personnel peut avoir.

Bloqué : L'application est bloquée et ne peut pas être installée dans le profil personnel.

Disponible : L'application est disponible pour l'installation dans le profil personnel.

8. Types de comptes bloqués

Types de comptes que l'utilisateur ne peut pas gérer. Cette option empêche les utilisateurs de l'appareil d'ajouter des comptes non autorisés à leur profil personnel.

Stratégies multi-profils

S'applique uniquement aux appareils disposant de profils personnels et professionnels.

Copier/coller entre les profils

Que le texte copié d'un profil (personnel ou professionnel) puisse être collé dans l'autre profil.

> **Non autorisé (par défaut)** : Empêche les utilisateurs de coller du texte dans le profil personnel à partir du profil professionnel. Le texte copié du profil personnel peut être collé dans le profil professionnel.
>
> **Autorisé** : Le texte copié dans n'importe quel profil peut être collé dans l'autre profil.

Partage de données entre les 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 les intents. La gestion des autres canaux de communication inter-profils, tels que la recherche de contacts, la copie/colle,
ou les applications professionnelles et personnelles connectées, est configurée séparément.

> **Interdit** : Empêche le partage de données entre le profil personnel et le profil professionnel, et inversement.
>
> **Interdit le partage de données** (par défaut) : Empêche les utilisateurs de partager des données du profil professionnel vers les applications du profil personnel. Les données personnelles peuvent être partagées avec les applications professionnelles.
>
> **Autorisé** : Les données de n'importe quel profil peuvent être partagées avec l'autre profil.

Les widgets du profil de travail sont configurés par défaut

Comportement par défaut des widgets du profil de travail. Si une application spécifique ne définit pas de politique pour les widgets, elle utilise les paramètres par défaut définis ici.

Fonctions des applications inter-profils

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

> Ce paramètre dépend de l'option de **fonctions d'application** définie au niveau de la politique (dans la section Gestion des applications). Si l'option Fonctions d'application est définie sur **Non autorisées**, l'API rejettera les fonctions d'application inter-profil définies sur **Autorisées**.

Contacts professionnels dans le profil personnel

Si les contacts enregistrés dans le profil professionnel peuvent être affichés dans les recherches de contacts du profil personnel et dans les appels entrants.

Autorisé (par défaut) : Permet aux contacts du profil professionnel de s'afficher dans le profil personnel.

Non autorisé : Empêche les applications personnelles d'accéder aux contacts du profil professionnel et de rechercher des contacts professionnels.

Non autorisé, sauf pour les applications système : Empêche la plupart des applications personnelles d'accéder aux contacts du profil professionnel, à l'exception des applications Dialer, Messages et Contacts par défaut du fabricant (Android 14 et versions ultérieures).

Lorsque les contacts professionnels sont configurés dans le profil personnel, vous pouvez éventuellement définir une liste de **noms de paquets exclus**. Selon le mode sélectionné, ces exclusions fonctionnent comme une liste blanche ou une liste noire pour les applications personnelles.

Rapport 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 de tableau de bord **État de l'appareil**.

Rapports d'application

Si les rapports d'application sont activés. (Informations rapportées concernant 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'applications.

Paramètres de l'appareil

Indique si l'enregistrement des paramètres de l'appareil est activé. (Informations sur les paramètres de sécurité de l'appareil.)

Informations sur le logiciel

L'affichage des informations sur le logiciel est-il activé ? (Informations sur le logiciel de l'appareil.)

Informations sur la mémoire

Indique si le reporting de la mémoire est activé. (Un événement lié aux mesures de mémoire et de stockage.)

Informations réseau

Indique si l'envoi des informations réseau est activé. (Informations réseau de l'appareil.)

Afficher les informations

L'affichage des informations de l'appareil est activé ou non. Les données de reporting ne sont pas disponibles pour les appareils personnels avec des profils professionnels. (Informations d'affichage de l'appareil.)

Événements de gestion de l'alimentation

Indique si l'enregistrement des événements de gestion de l'alimentation est activé. Les données ne sont pas disponibles pour les appareils personnels avec des profils professionnels.

État du matériel

Indique si le reporting de l'état du matériel est activé. Les données de reporting ne sont pas disponibles pour les appareils personnels équipés d'un profil professionnel.

Propriétés du système

Indique si l'enregistrement des propriétés du système est activé.

Mode de conformité aux critères communs

Indique si le mode de conformité aux critères communs est activé.

Divers

1. Jeu de "cloclo" désactivé

Le jeu de "cloclo" dans les paramètres est-il désactivé ?

2. Ignorer les conseils pour la première utilisation

Indiquer si l'on doit ignorer les conseils lors de la première utilisation. L'administrateur Enterprise peut activer la recommandation système pour que les applications n'affichent pas leur tutoriel utilisateur ni d'autres conseils d'introduction lors du premier lancement.

3. Court message d'assistance

Message affiché à l'utilisateur dans l'écran des paramètres, indiquant que la fonctionnalité a été désactivée par l'administrateur. Si le message est plus long que 200 caractères, il peut être tronqué.

4. Message de support détaillé

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

5. Informations affichées sur l'écran de verrouillage du propriétaire

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

6. Actions de configuration

Actions à effectuer pendant le processus de configuration. Pendant l'inscription, vous pouvez demander à l'utilisateur d'ouvrir une ou plusieurs applications nécessaires à la configuration de l'appareil.

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

6.1. Lancer l'application

Nom du package de l'application à lancer

6.2. Titre

Affiche un message destiné à l'utilisateur, expliquant pourquoi l'application doit être lancée.

6.3. Description

Affiche un message destiné à l'utilisateur, expliquant pourquoi l'application doit être lancée.

7. Visibilité du nom d'affichage pour les entreprises

Contrôle la visibilité du nom d'affichage de l'entreprise sur l'appareil (par exemple, en tant que 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 pour Android 7+ et les appareils entièrement gérés sur Android 8+).

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

Règles d'application des politiques

Si un appareil ou un profil professionnel ne respecte pas l'une des règles de configuration indiquées ci-dessous, Android Device Policy bloque automatiquement l'utilisation de l'appareil ou du profil professionnel

- **Exigences de mot de passe**
- **Politique de chiffrement**
- **Verrouillage d'écran désactivé**
- **Méthodes de saisie autorisées**
- **Services d'accessibilité autorisés**

Si l'appareil ou le profil professionnel reste non conforme après 10 jours, la stratégie de gestion des appareils Android réinitialisera l'appareil aux paramètres d'usine ou supprimera le profil professionnel.

Dans cette section, vous pouvez modifier les règles de conformité par défaut ou en ajouter de nouvelles.

Règles

Liste des règles qui définissent le comportement lorsqu'une politique 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 politique de niveau supérieur à appliquer. Par exemple, les **applications** ou les **exigences de mot de passe**.

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

Bloquer après un nombre de jours

Nombre de jours pendant lesquels la stratégie n'est pas conforme avant que l'appareil ou le profil professionnel ne soit bloqué. Pour bloquer l'accès immédiatement, réglez sur 0. **Bloquer après un certain nombre de jours** doit être inférieur à **Effacer après un certain nombre de jours**. Applicable uniquement aux appareils appartenant à l'entreprise.

Plage autorisée : 0 à 300.

Portée de bloc

Définit la portée de l'action de blocage. S'applique 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 les applications du profil personnel.

Effacer après un nombre de jours

Nombre de jours pendant lesquels la règle est non conforme avant que l'appareil ou le profil professionnel ne soit effacé.
Nombre de jours avant effacement doit être supérieur à la valeur de **Bloquer après un nombre de jours**. S'applique uniquement aux appareils appartenant à l'entreprise.

Obligatoire. Valeur par défaut (nouvelle règle) : **1**.

Plage autorisée : de 1 à 300.

Conserver la protection de 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.