Politiques - Android

Résumé

Les politiques Android sont les entités de base du système : elles définissent les règles qui sont appliquées et imposées sur les appareils gérés.

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

Une politique peut être associée à un jeton d'enrôlement, elle sera donc automatiquement appliquée aux appareils lors du processus de provisionnement. Vous pouvez également modifier la politique assignée à un appareil après le provisionnement.

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

> De nombreuses options de politique ne s'appliquent qu'à des types d'appareils spécifiques (gestion complète, dédié, profil de travail) et à certaines 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 sous forme d'un ensemble de sections extensibles. En haut de la page, vous pouvez toujours modifier :

- **Nom** (requis)
- **Id** (lecture seule)
- **Description** (facultatif)

Les sections ci-dessous correspondent aux panneaux de l'éditeur de politiques (par exemple : Gestion des applications, Sécurité, Réseau, Système, Usage personnel, Politiques inter-profils, et plus encore). Utilisez les pages des chapitres de ce manuel pour comprendre chaque panneau en détail.

Sauvegarde, suppression 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 Id), la page affiche une action **Supprimer la politique** et une liste des **Appareils associés** en bas, afin que vous puissiez voir combien d'appareils utilisent actuellement la politique.

Gestion des applications

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

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

1. Mode Play Store

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

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

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

2. Politique des applications non approuvées

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

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

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

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

3. Google Play Protect

Si la vérification des applications par Google Play Protect est appliquée.

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

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

4. Politique de permission par défaut

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

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

Accorder: Accorder automatiquement une permission.

Refuser: Refuser automatiquement une permission.

5. Fonctions d'application

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

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

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

6. Installation d'applications désactivée

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

7. Désinstallation des applications désactivée

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

8. Politiques de permissions

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

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

Chaque entrée comprend :

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

9. Applications

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

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

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

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

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

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

9.1. Type d'installation

Le type d'installation à effectuer pour une application.

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

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

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

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

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

Kiosque : L'application est installée automatiquement en mode kiosque : elle est définie comme l'intention d'accueil préférée et est ajoutée à la liste blanche pour le mode de verrouillage de tâche. La configuration de l'appareil ne sera pas terminée tant que l'application n'est pas installée. Après l'installation, les utilisateurs ne pourront pas supprimer l'application. Vous ne pouvez définir ce **type d'installation** que pour une seule application par politique. Lorsqu'il est présent dans la politique, la barre d'état sera automatiquement désactivée. Pour plus d'informations, veuillez consulter la page dédiée **Mode kiosque**.

9.2. Contraintes d'installation

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

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

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

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

Inactif : Installez l'application uniquement lorsque l'appareil est inactif.

9.3. Mode de mise à jour automatique

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

Par défaut : L'application est mise à jour automatiquement avec une priorité basse afin de minimiser l'impact sur l'utilisateur. L'application est mise à jour lorsque toutes les contraintes suivantes sont respectées : (1) l'appareil n'est pas utilisé activement, (2) l'appareil est

connecté à un réseau non limité, (3) l'appareil est en charge. L'appareil est notifié d'une nouvelle mise à jour dans les 24 heures suivant sa publication par le développeur, après quoi l'application est mise à jour la prochaine fois que les contraintes ci-dessus sont respectées.

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

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

9.4. Code de version minimum

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

9.5. Scopes délégués

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

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

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

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

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

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

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

9.6. Réseau préférentiel

Le service de réseau préférentiel à utiliser pour cette application. Si elle est définie, l'application utilisera le segment de réseau d'entreprise spécifié pour ses connexions lorsqu'il sera disponible.

Cela doit correspondre à un segment de réseau configuré dans la section **Configuration du découpage de réseau 5G** du panneau **Réseau cellulaire**.

9.7. Politique de permissions par défaut

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

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

Accorder : Accorder automatiquement une permission.

Refuser : Refuser automatiquement une permission.

9.8. Application connectée travail et personnel

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

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

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

9.9. Exemption du verrouillage VPN toujours actif

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

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

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

9.10. Widgets du profil de travail

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

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

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

9.11. Paramètres de contrôle utilisateur

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

> **Non spécifié** : Utilise le comportement par défaut de l'application pour déterminer si le contrôle utilisateur est autorisé ou interdit.
>
> **Autorisé** : Le contrôle utilisateur est autorisé pour l'application.
>
> **Interdit** : Le contrôle utilisateur est interdit pour l'application.

9.12. Désactivée

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

9.13. Autoriser le fournisseur d'identifiants

Indique si l'application est autorisée à agir comme fournisseur d'identifiants sur Android 14 et versions ultérieures.

9.14. Configuration gérée

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

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

9.15. Politiques de permissions

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

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

9.16. ID de canal

Liste des ID de canaux de test fermé de l'application auxquels un appareil peut accéder. Si plusieurs ID de canaux sont sélectionnés, les appareils reçoivent la version la plus récente parmi

tous les canaux accessibles. Si aucun ID de canal n'est sélectionné, les appareils ont uniquement accès au canal de production de l'application.

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

10. Paramètres d'application par défaut

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

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

10.1. Type d'application par défaut

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

10.2. Portées de l'application par défaut

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

> Si aucune des portées sélectionnées n'est applicable au mode de gestion de l'appareil, l'appareil signalera un détail de non-conformité.

10.3. Applications par défaut

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

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

11. Sélection de la clé privée

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

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

12. Choisir les règles de clé privée

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

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

12.1. Alias de clé privée

L'alias de la clé privée à utiliser.

12.2. Modèle d'URL

Le modèle d'URL à comparer avec l'URL de la requête. S'il n'est pas défini ou s'il est vide, il correspond à toutes les URL. Cela utilise la syntaxe d'expression régulière de java.util.regex.Pattern.

12.3. Noms de package

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

KeyChain.choosePrivateKeyAlias.

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

> Pour supprimer une application, cliquez sur l'icône **poubelle** au bas de la fiche de l'application.

Mode kiosque

Avec le mode kiosque, vous pouvez restreindre les fonctionnalités d'un appareil à une seule application ou à plusieurs applications. Le choix entre le mode kiosque à application unique et celui à applications multiples dépend de vos objectifs commerciaux.

Dans le **mode kiosque à application unique**, l'appareil est configuré pour une seule application et ne permet pas aux utilisateurs finaux d'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** avec le **Type d'installation** défini sur **Kiosque**.

Dans le **mode kiosque à applications multiples**, les appareils permettent l'accès à plusieurs applications. Les utilisateurs finaux peuvent naviguer entre plusieurs applications via un lanceur personnalisé. Pour activer ce mode, activez l'option **Lanceur personnalisé kiosque**.

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 du système et la barre d'état.

Lanceur personnalisé kiosque

Détermine si le lanceur personnalisé kiosque est activé. Cela remplace l'écran d'accueil par un lanceur qui verrouille l'appareil sur les applications installées via le paramètre de la **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 lorsqu'un utilisateur effectue un appui prolongé sur le bouton d'alimentation.

> **Disponible (par défaut)** : Le menu d'alimentation (par exemple : Éteindre, Redémarrer) s'affiche lorsqu'un utilisateur effectue un appui prolongé sur 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 effectue un appui prolongé sur 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 plus sont bloquées en mode kiosque. Lorsqu'elles sont bloquées, le système arrêtera de force l'application comme si l'utilisateur choisissait l'option « fermer l'application » sur l'interface utilisateur.

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

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

Navigation système

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

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

Accueil uniquement : Seul le bouton d'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 politique prenne effet, le bouton d'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 politiques relatives à la sécurité.

Actions liées aux risques de sécurité

Choisissez l'action à entreprendre lorsqu'un appareil signale un risque de sécurité (SecurityRisk) dans les rapports d'état.

Types de risques de sécurité (SecurityRisk) pris en charge :

OS inconnu : l'API Play Integrity détecte que l'appareil exécute un OS inconnu (la vérification basicIntegrity réussit mais ctsProfileMatch échoue).

OS compromis : l'API Play Integrity détecte que l'appareil exécute un OS compromis (la vérification basicIntegrity échoue).

Échec de l'évaluation basée sur le matériel : l'API Play Integrity détecte que l'appareil ne dispose pas d'une garantie solide de l'intégrité du système, si le libellé MEETS_STRONG_INTEGRITY ne s'affiche pas dans le champ d'intégrité de l'appareil.

Actions disponibles :

Supprimer les données de l'entreprise (par défaut) : désenrôler l'appareil et supprimer les données de travail (l'appareil complet s'il est en gestion complète, ou uniquement le profil de travail pour les profils gérés).

Aucune action : laisser l'appareil enrôlé et ne rien faire automatiquement.

Lorsque vous sélectionnez **Supprimer les données de l'entreprise**, vous pouvez également configurer les options de suppression :

Conserver la protection contre la réinitialisation d'usine : préserver les données de protection contre la réinitialisation d'usine (FRP) lors de la suppression des données de l'appareil.

Supprimer le stockage externe : supprimer également le stockage externe de l'appareil (tel que les cartes SD) lors de la suppression des données.

Supprimer les eSIM : pour les appareils appartenant à l'entreprise, cela supprime toutes les eSIM de l'appareil lors de la suppression des données. Sur les appareils appartenant à des particuliers, cela supprimera les eSIM gérées (les eSIM ajoutées via la commande ADD_ESIM) sur l'appareil, et aucune eSIM personnelle ne sera supprimée.

1. Temps maximal avant verrouillage

Temps maximal (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 lors de la charge

Les modes de branchement sur secteur pour lesquels l'appareil reste activé. Lors de l'utilisation de ce paramètre, il est recommandé de vider **Temps maximal avant verrouillage** afin que l'appareil ne se verrouille pas tout en restant activé.

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. Désactivation de l'écran de verrouillage (Keyguard)

Si activé, cela désactive l'écran de verrouillage pour les écrans principaux et/ou secondaires. Cette politique est prise en charge uniquement en mode de gestion d'appareil dédié.

4. Exigences relatives au mot de passe

Politiques d'exigences relatives au 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 de travail**. Les exigences basées sur la complexité doivent être couplées à des exigences basées sur la qualité pour la même portée.

4.1. Portée

La 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 de travail pour les appareils avec profil de travail, et à l'appareil complet pour les appareils en gestion complète ou dédiés.
>
> **Appareil** : les exigences de mot de passe s'appliquent uniquement à l'appareil.
>
> **Profil de travail** : les exigences de mot de passe s'appliquent uniquement au profil de travail.

4.2. Longueur de l'historique des mots de passe

La 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 l'un des mots de passe présents dans l'historique. Une valeur de 0 signifie qu'il n'y a aucune restriction.

4.3. Nombre maximal d'échecs de mot de passe avant réinitialisation

Nombre de mots de passe de déverrouillage incorrects pouvant être saisis avant que l'appareil ne soit réinitialisé. 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 mettre à jour périodiquement son mot de passe, après le nombre de jours spécifié.

4.5. Exiger le déverrouillage par mot de passe

La durée pendant laquelle, après qu'un appareil ou un profil de travail a été déverrouillé à l'aide d'une forme d'authentification forte (mot de passe, code PIN, schéma), il peut être déverrouillé à l'aide de toute autre méthode d'authentification (ex. : empreinte digitale, agents de confiance, reconnaissance faciale). Une fois la période spécifiée écoulée, seules les formes d'authentification fortes pourront être utilisées pour déverrouiller l'appareil ou le profil de travail.

> **Par défaut de l'appareil** : la période de délai d'expiration est définie sur le paramètre par défaut de l'appareil.
>
> **Tous les jours** : la période de délai d'expiration est fixée à 24 heures.

4.6. Qualité du mot de passe

La qualité requise du mot de passe.

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

Complexité moyenne : définit la bande de complexité moyenne du mot de passe comme suit : code PIN sans séquences répétitives (4444) ou ordonnées (1234, 4321, 2468), longueur d'au moins 4 caractères ; alphabétique, longueur d'au moins 4 caractères ; alphanumérique, longueur d'au moins 4 caractères.

Complexité faible : définit la bande de complexité faible du mot de passe 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 sécurité. Cela inclut les technologies capables de reconnaître l'identité d'un individu et qui sont approximativement équivalentes à un code PIN à 3 chiffres (le taux de fausse détection est inférieur à 1 sur 1 000).

N'importe lequel : un mot de passe est requis, mais il n'y a aucune restriction sur son contenu.

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) ou 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 respecter les exigences minimales spécifiées dans passwordMinimumLength, passwordMinimumLetters, passwordMinimumSymbols, etc. Par exemple, si passwordMinimumSymbols est de 2, le mot de passe doit contenir au moins deux symboles.

4.7. Longueur minimale

La 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 autres que des lettres

Nombre minimal de caractères autres que des lettres (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 de travail, sur les appareils fonctionnant sous Android 9 et versions ultérieures avec un profil de travail. Cela n'a aucun effet sur les autres appareils.

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

5. Désactivation de la réinitialisation d'usine

Indique si la réinitialisation d'usine via les paramètres est désactivée. S'applique uniquement aux appareils en gestion complète.

6. Protection contre la réinitialisation d'usine

Adresses e-mail des administrateurs de l'appareil pour la protection contre la réinitialisation d'usine. Si l'appareil subit une réinitialisation d'usine non autorisée, il exigera que l'un de ces administrateurs se connecte avec son adresse e-mail et son mot de passe de compte Google pour déverrouiller l'appareil. Si aucun administrateur n'est spécifié, l'appareil ne proposera pas de protection contre la réinitialisation d'usine. S'applique uniquement aux appareils en gestion complète.

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

7. Fonctionnalités de l'écran de verrouillage (Keyguard)

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

7.1. Tout désactiver

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

7.2. Désactiver l'appareil photo

Désactive l'appareil photo sur les écrans de verrouillage sécurisés (ex. : 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 l'affichage du contenu des notifications 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'empreinte digitale 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 faciale

Désactive l'authentification 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 toute l'authentification biométrique

Désactive toute l'authentification biométrique 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 l'appareil photo/microphone, l'accès aux données USB, l'impression et les restrictions liées à l'affichage.

1. Accès à l'appareil photo

Contrôle l'utilisation de l'appareil photo et si l'utilisateur peut accéder au commutateur d'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 en gestion complète, et uniquement au sein du profil professionnel sur les appareils avec profil professionnel.

> **Choix de l'utilisateur (par défaut)** : Comportement par défaut de l'appareil. Les appareils photo sont disponibles et (Android 12+) l'utilisateur peut activer ou désactiver l'accès à l'appareil photo.
>
> **Désactivé** : Tous les appareils photo sont désactivés (gestion complète : sur tout l'appareil ; profil professionnel : uniquement pour les applications du profil professionnel). Le commutateur d'accès à l'appareil photo n'a aucun effet dans la portée gérée.
>
> **Appliqué** : Les appareils photo sont disponibles. Sur les appareils en gestion complète sous Android 12+, l'utilisateur ne peut pas activer ou désactiver l'accès à l'appareil photo. Sur les autres appareils/versions, cela se comporte comme le choix de l'utilisateur.

2. Accès au microphone

Sur les appareils en gestion complète, contrôle l'utilisation du microphone et si l'utilisateur peut accéder au commutateur d'accès au microphone (Android 12+). Ce paramètre n'a aucun effet sur les appareils qui ne sont pas en gestion complète.

> **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 (sur tout l'appareil). Le commutateur d'accès au microphone n'a aucun effet.
>
> **Appliqué** : Le microphone est disponible. Sur Android 12+, l'utilisateur ne peut pas activer ou désactiver l'accès au microphone. Sur Android 11 ou versions antérieures, 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 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.

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

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 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, qui est utilisée dans le cadre du réglage automatique (Android 9+ en gestion complète ; profils professionnels sur 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 requise (Android 9+ en gestion complète ; profils professionnels sur Android 15+ appartenant à l'entreprise).

Luminosité de l'écran :

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

6. Paramètres de mise en veille de l'écran

Contrôle si l'utilisateur peut configurer la mise en veille de l'écran et, lorsqu'elle est imposée, la valeur de la mise en veille.

Le champ **Mode de mise en veille 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 la mise en veille de l'écran.
>
> **Appliqué** : La mise en veille de l'écran est réglée sur la valeur configurée et l'utilisateur ne peut pas la modifier (Android 9+ en gestion complète ; profils professionnels sur Android 15+ appartenant à l'entreprise).

Mise en veille de l'écran :

> Durée de la mise en veille en secondes. La valeur doit être supérieure à 0. Si elle est supérieure au **temps de verrouillage maximal**, le système peut la limiter et signaler une non-conformité.

7. Capture d'écran désactivée

Détermine si la capture d'écran est désactivée.

8. Ajustement du volume désactivé

Détermine si l'ajustement du volume principal est désactivé.

9. Montage de supports physiques désactivé

Détermine si le montage de supports physiques externes est désactivé.

Cellulaire

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

1. Mode avion

Contrôle si le mode avion peut être activé ou désactivé par l'utilisateur.

> **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 le paramètre cellulaire 2G peut être activé ou désactivé par l'utilisateur.

> **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 le remplacement des APN est activé ou désactivé. Lorsqu'il est activé, seuls les APN de remplacement configurés sont utilisés et tous les autres APN sur l'appareil sont ignorés.

> **Désactivé (par défaut)** : Tous les paramètres d'APN configurés sont enregistrés sur l'appareil, mais ils sont désactivés et n'ont aucun effet. Tous les autres APN sur l'appareil restent en usage.
>
> **Activé** : Seuls les APN de remplacement sont utilisés, tous les autres APN sont ignorés. Ce paramètre ne peut être configuré que sur les appareils en gestion complète avec Android 10 et versions ultérieures.

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 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 de l'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 de l'opérateur (si nécessaire).

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

Types de réseau : Restreignez 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 relatifs aux MMS.

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

Paramètre Toujours activé : Détermine si la session PDU activée par cet APN doit être toujours active. Pris en charge sur Android 15 et versions ultérieures.

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

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

5. Configuration de la diffusion cellulaire désactivée

Détermine si la configuration de la diffusion cellulaire est désactivée.

6. Configuration des réseaux mobiles désactivée

Détermine si la configuration des réseaux mobiles est désactivée.

7. Données en itinérance désactivées

Détermine si les services de données en itinérance sont désactivés.

8. Appels sortants désactivés

Détermine si les appels sortants sont désactivés.

9. SMS désactivés

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

10. Configuration du découpage de réseau 5G

Configurez les paramètres de service réseau préférentiels pour activer le découpage de réseau 5G d'entreprise. Vous pouvez configurer jusqu'à 5 tranches d'entreprise et assigner des applications à des réseaux spécifiques pour un routage optimisé du trafic.

10.1. Réseau préférentiel par défaut

Identifiant du 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. Doit comporter une configuration pour l'identifiant de réseau spécifié (sauf s'il est défini sur **Aucun réseau préférentiel**).

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 tranche. Vous pouvez ajouter jusqu'à 5 configurations. Chaque configuration comprend :

Identifiant du réseau préférentiel (assigné automatiquement) : L'identifiant du réseau est assigné automatiquement et ne peut pas être modifié.

Repli sur la connexion par défaut : Détermine si le repli sur le réseau par défaut de l'appareil est autorisé. Si ce n'est pas autorisé, les applications ne pourront pas accéder à Internet si la tranche 5G est indisponible.

Réseaux non correspondants : Détermine si les applications soumises à cette configuration peuvent utiliser des réseaux autres que le service préférentiel. Si défini sur **Interdit**, le **Repli sur la connexion par défaut** doit également être sur **Interdit**. Nécessite Android 14 et versions ultérieures.

Réseautage

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

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

État de la radio de l'appareil

1. État du Wi-Fi

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

Le niveau de sécurité minimal requis des réseaux Wi-Fi auxquels l'appareil peut se connecter. Pris en charge sur Android 13 et versions ultérieures, pour les appareils en gestion complète 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 ; nécessite au moins une sécurité de type personnel (par exemple WPA2-PSK).
>
> **Réseau d'entreprise** : Nécessite des réseaux EAP d'entreprise ; interdit les réseaux Wi-Fi dont le niveau de sécurité est inférieur.

Réseau d'entreprise 192 bits : Nécessite des réseaux d'entreprise 192 bits ; l'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 en gestion complète, 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 config. Wi-Fi : L'ajout de nouvelles configurations Wi-Fi est interdit. L'utilisateur peut basculer entre les réseaux déjà configurés (Android 13+ ; appareils en

gestion complète et profils professionnels sur appareils appartenant à l'entreprise).

Interdire la configuration du Wi-Fi : Interdit la configuration des réseaux Wi-Fi. Pour les appareils en gestion complète, cela supprime les réseaux configurés par l'utilisateur et ne conserve que les réseaux configurés via les **configurations Wi-Fi**. Pour les profils professionnels sur appareils appartenant à l'entreprise, les réseaux existants ne sont pas affectés, mais les utilisateurs ne peuvent ni ajouter, ni supprimer, ni 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 la **soupape de sécurité réseau** pour permettre à l'utilisateur de se connecter temporairement et d'actualiser la politique.

6. Paramètres 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 de différentes formes de partage de connexion.

Autoriser tout le 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+ appartenant à l'entreprise).

Interdire tout le partage de connexion : empêche toutes les formes de partage de connexion (gestion complète + profils de travail appartenant à l'entreprise).

8. Politique de SSID Wi-Fi

Restrictions sur les SSID Wi-Fi auxquels l'appareil peut se connecter (cela n'affecte pas les réseaux pouvant être configurés sur l'appareil). Pris en charge sur les appareils appartenant à l'entreprise

fonctionnant sous Android 13 et versions ultérieures.

Liste d'exclusion de SSID (par défaut) : l'appareil ne peut se connecter à aucun réseau Wi-Fi dont le SSID est répertorié, mais peut se connecter aux autres réseaux.

Liste d'autorisation de 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 politique sélectionné, la liste est interprétée comme des SSID autorisés ou refusés.

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

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 s'applique le paramètre d'itinérance (requis).

Mode d'itinérance Wi-Fi : Par défaut / Désactivé / Agressif. Les modes Désactivé et Agressif nécessitent Android 15+ et sont pris en charge uniquement sur les appareils en gestion complète ainsi que sur les profils de travail des appareils appartenant à l'entreprise.

Restrictions réseau

10. Désactivation du Bluetooth

Indique si le Bluetooth est désactivé. Privilégiez ce paramètre par rapport à la désactivation de la configuration Bluetooth, car cette dernière peut être contournée par l'utilisateur.

11. Désactivation du partage de contacts via Bluetooth

Indique si le partage de contacts via Bluetooth est désactivé.

12. Désactivation de la configuration Bluetooth

Indique si la configuration du Bluetooth est désactivée.

13. Désactivation de la réinitialisation du réseau

Indique si la réinitialisation des paramètres réseau est désactivée.

14. Désactivation du partage par Android Beam (sortant)

Indique si l'utilisation du NFC pour le partage de données via Beam est désactivée.

VPN

15. Application VPN toujours activé (Always On)

Spécifiez le nom du package de l'application VPN toujours activé (Always On) pour garantir que les données des applications gérées spécifiées passeront toujours par un VPN configuré.

> Remarque : Cette fonctionnalité nécessite le déploiement d'un client VPN prenant en charge à la fois les fonctions « Always On » (toujours activé) et le VPN par application.

16. Verrouillage VPN (VPN lockdown)

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

17. Désactivation de la configuration VPN

Indique si la configuration du VPN est désactivée.

Proxy et services réseau

18. Service de réseau préférentiel

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

Désactivé : le service de réseau préférentiel est désactivé sur le profil de travail.

Activé : le service de réseau préférentiel est activé sur le profil de travail.

> Si vous utilisez le découpage de réseau (network slicing) d'entreprise, configurez également la **Configuration du découpage de réseau 5G** dans le panneau de politique **Réseau cellulaire** et assignez les applications à une tranche en utilisant leur paramètre **Réseau préférentiel**.

19. Proxy global recommandé

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

Désactivé

Proxy direct

Proxy auto-config (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'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 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 : Requis.

SSID : Requis.

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

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

SSID caché : indique si le SSID sera diffusé.

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

20.1. Sécurité

Options de sécurité Wi-Fi :

WEP-PSK : WEP (clé pré-partagée).

WPA-PSK : WPA/WPA2/WPA3-Personnel (clé pré-partagée).

WPA-EAP : WPA/WPA2/WPA3-Entreprise (Extensible Authentication Protocol).

Mode WPA3 192 bits : réseau WPA-EAP n'autorisant que le mode WPA3 192 bits.

20.2. Mot de passe (clé pré-partagée)

Affiché lorsque la sécurité est **WEP-PSK** ou **WPA-PSK**. Le mot de passe est requis.

20.3. Méthode EAP (Entreprise)

Affiché lorsque la sécurité est **WPA-EAP** ou **Mode WPA3 192 bits**. 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 à tunnel (**EAP-TTLS** et **PEAP**).

MSCHAPv2

PAP

20.5. Identifiants EAP des utilisateurs

Lorsqu'elle 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 assigner un certificat client utilisé pour l'authentification Wi-Fi. Pour plus d'informations, consultez la page **Gestion des certificats**.

Si un certificat est déjà assigné, 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 tous deux configurés, l'alias de la paire de clés est ignoré.

20.7. Identité

Identité de l'utilisateur. Pour les protocoles externes à tunnel (PEAP, EAP-TTLS), celle-ci est utilisée 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 sans tunnel, elle est utilisée pour l'identité EAP.

20.8. Identité anonyme

Pour les protocoles à tunnel uniquement, cela 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 d'autorité de certification (CA) du serveur

Liste des certificats d'autorité de certification (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 d'autorité de certification (CA) du serveur** pour ajouter des entrées et supprimez-les avec l'action de suppression.

20.11. Correspondances de suffixes de domaine

Une liste de contraintes pour le nom de domaine du serveur. Les 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 minimal

Le niveau d'API Android minimal 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 avec un mot de passe nécessaire pour le 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 développement

Contrôle l'accès aux paramètres de développement : options pour développeurs et mode sans échec.

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

Autorisé : permet tous les paramètres de développement. L'utilisateur peut y accéder et, si nécessaire, configurer les paramètres.

5. Mode Critères Communs (Common Criteria)

Contrôle le mode Critères Communs (Common Criteria) — des normes de sécurité définies dans les Critères Communs pour l'évaluation de la sécurité de l'informatique (CC). L'activation du mode Critères Communs renforce certains composants de sécurité sur l'appareil (par exemple : le chiffrement AES-GCM des clés à long terme Bluetooth, une validation supplémentaire pour certains certificats réseau et des contrôles d'intégrité de la politique cryptographique). Le mode Critères Communs est pris en charge uniquement sur les appareils appartenant à l'entreprise fonctionnant sous Android 11 ou versions ultérieures. Avertissement : le mode Critères Commuliers impose un modèle de sécurité strict, généralement requis uniquement 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 Critères Communs.

Activé : Active le mode Common Criteria.

6. Memory Tagging Extension (MTE)

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

Choix de l'utilisateur (par défaut) : L'utilisateur peut choisir d'activer ou de désactiver le MTE sur l'appareil (si l'appareil est compatible).

Appliqué : Le MTE est activé et l'utilisateur ne peut pas le modifier (Android 14+ ; pris en charge sur les appareils entièrement gérés et les profils de travail sur les appareils appartenant à l'entreprise).

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

7. Protection du contenu

Contrôle si la protection du contenu (qui recherche 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 modifier ce paramètre.

Appliqué : La protection du contenu est activée et l'utilisateur ne peut pas modifier ce paramètre (Android 15+).

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

8. Contenu d'assistance

Contrôle si l'envoi de AssistContent est autorisé à une application privilégiée, telle qu'une application d'assistance (par exemple, Circle to Search). AssistContent inclut des 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) : L'envoi du contenu d'assistance à une application privilégiée est autorisé (Android 15+).

Interdit : L'envoi du contenu d'assistance à une application privilégiée est bloqué (Android 15+).

9. Désactivation de la création de fenêtres

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

10. Soupape de sécurité réseau

Indique si la soupape de sécurité réseau est activée. Si aucune connexion réseau ne peut être établie au démarrage, la soupape de sécurité invite l'utilisateur à se connecter temporairement à un réseau afin d'actualiser la politique de l'appareil. Après l'application de la politique, le réseau temporaire sera oublié et l'appareil poursuivra son démarrage. Cela permet d'éviter de se retrouver dans l'impossibilité de se connecter à un réseau si aucun réseau approprié n'était disponible dans la dernière politique et que l'appareil démarre sur une application en mode verrouillage (lock task), ou si l'utilisateur est autrement incapable d'accéder aux paramètres de l'appareil.

11. Activités par défaut

Une liste d'activités par défaut pour la gestion des intents correspondant à un filtre d'intent spécifique. Par exemple, cette fonctionnalité permettrait aux administrateurs informatiques de choisir quelle application de navigateur ouvre automatiquement les liens web, ou quelle application de lanceur est utilisée lors de l'appui 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

L'activité qui doit servir de 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 amène Android Device Policy à choisir une activité appropriée au sein de l'application pour gérer l'intent.

11.2. Action

Les actions d'intent à faire correspondre dans le filtre. Si des actions sont incluses dans le filtre, l'action de l'intent doit être l'une de ces valeurs pour qu'il y ait correspondance. Si aucune action n'est incluse, l'action de l'intent est ignorée.

11.3. Catégorie

Les catégories d'intent à faire correspondre dans le filtre. Un intent inclut les catégories dont il a besoin, et toutes celles-ci doivent être incluses dans le filtre pour qu'il y ait correspondance. En d'autres termes, l'ajout d'une catégorie au filtre n'a aucun impact sur la correspondance, à moins que cette catégorie ne soit spécifiée dans l'intent.

12. Méthodes de saisie autorisées

Spécifie les méthodes de saisie autorisées.

> **Tout est autorisé** : 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 packages des méthodes de saisie autorisés. 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.

> **Tout est autorisé** : N'importe quel service d'accessibilité peut être utilisé.
>
> **Système uniquement** : Seuls les services d'accessibilité intégrés au système peuvent être utilisés.
>
> **Système et fournies 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 fournies uniquement**.

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

14. Politique de mise à jour du système

Configuration pour la gestion des mises à jour du système.

> **Par défaut** : Suit le comportement de mise à jour par défaut de l'appareil, ce qui nécessite généralement que l'utilisateur accepte les mises à jour du système.
>
> **Automatique** : Installe automatiquement dès qu'une mise à jour est disponible.
>
> **Fenêtre de maintenance** : Installe automatiquement au sein d'une fenêtre de maintenance quotidienne. Cela configure également les applications Play pour qu'elles soient mises à jour pendant cette fenêtre. Cette option est fortement recommandée pour les appareils de type kiosque, car c'est le seul moyen de mettre à jour via Play les applications épinglées de manière persistante au premier plan.

Reporter : Reporte l'installation automatique jusqu'à un maximum de 30 jours.

14.1. Fenêtre de maintenance (Mode fenêtre uniquement)

Lorsque la **Politique de mise à jour du système** est définie sur **Fenêtre de maintenance**, 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 du système

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

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

15. Fournisseurs d'identifiants par défaut

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

Interdit (par défaut) : Les applications dont la politique credentialProviderPolicy n'est pas spécifiée ne sont pas autorisées à agir en tant que fournisseur d'identifiants.

Interdit sauf système : Les applications dont la politique credentialProviderPolicy n'est pas spécifiée ne sont pas autorisées à agir en tant que fournisseur d'identifiants, sauf pour les fournisseurs d'identifiants par défaut du fabricant (OEM).

Localisation et géorepérage

Ce panneau regroupe les paramètres de la politique Android qui contrôlent le signalement de la position de l'appareil, l'application de la localisation et les définitions de géorepérage. Utilisez-le lorsque vous souhaitez que Cerberus Enterprise collecte la position des appareils ou détecte lorsqu'ils entrent ou sortent de zones configurées.

Signalement de la position

Signaler la position

Active le signalement 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 l'aperçu de l'appareil et le traitement du géorepérage.

> Sur les appareils qui ne sont pas entièrement gérés, la transmission des données de localisation peut toujours dépendre du fait que l'application Cerberus Enterprise possède les autorisations de localisation requises et que les services de localisation soient activés sur l'appareil.

Mode de localisation

Contrôle le paramètre de localisation sur les 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 position désactivé

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

Comportement automatique avec géorepérages actifs

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

- **Signaler la position** est activé de force tant que des géorepérages actifs existent.
- **Le mode de localisation** est forcé sur **Appliqué**.
- **Le partage de la position désactivé** est forcé sur désactivé.

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

Liste de géorepérages

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

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 **100** à **10000** mètres.
- **Description** : notes facultatives pour les administrateurs.
- **Signaler l'entrée** et **Signaler la sortie** : choisissez quels événements de transition doivent être générés.
- **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.

Outils d'édition de la carte

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

- Cliquez sur la carte pour déplacer le centre du géorepérage lorsque l'édition de la zone est déverrouillée.
- Utilisez le bouton **Position actuelle** pour centrer la carte sur votre position actuelle dans le navigateur.
- Utilisez le bouton **Recentrer la carte** pour restaurer la zone d'affichage préférée de ce géorepérage.
- Utilisez le bouton de verrouillage pour empêcher toute modification accidentelle de la géométrie du géorepérage.

Où les données de géorepérage apparaissent

Les transitions de géorepérage peuvent être consultées dans la page **Aperçu de l'appareil** de l'Android, dans l'onglet **Géorepérage** 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

Désactivation de l'ajout d'utilisateurs

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

Désactivation de la modification des comptes

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

Désactivation de la configuration des identifiants utilisateur

Indique si la configuration des identifiants utilisateur est désactivée.

Désactivation de la suppression d'utilisateurs

Indique si la suppression d'autres utilisateurs est désactivée.

Désactivation de la définition de l'icône utilisateur

Indique si le changement de l'icône utilisateur est désactivé.

Désactivation de la définition du fond d'écran

Indique si le changement de fond d'écran est désactivé.

Authentification lors de la configuration du compte de travail

Contrôle la manière dont les utilisateurs s'authentifient lors de la configuration du compte de travail. Cette option est disponible uniquement pour les entreprises Android gérées par un domaine Google (Google Workspace).

Lors de la configuration ou de l'enrôlement de l'appareil, cette politique influence si une connexion au compte de travail est requise, mais le paramètre **S'authentifier à l'aide de Google** de la console d'administration Google ainsi que le type de jeton d'enrôlement peuvent toujours exiger une authentification.

Pour les appareils déjà enrôlés, cette politique ne s'applique que si l'appareil est géré par un compte Google Play géré (c'est-à-dire enrôlé sans **enrôlement avec authentification via Google**).

Pour plus de détails et pour le dépannage, reportez-vous à **l'enrôlement avec authentification via Google**.

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

Usage personnel

Lors du provisionnement 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 de travail.

> Cette section s'applique uniquement aux appareils appartenant à l'entreprise avec un profil de travail. Elle n'aura aucun effet sur les appareils en gestion complète ou appartenant à des particuliers.

1. Désactivation de l'appareil photo

Indique si l'appareil photo est désactivé.

2. Désactivation de la capture d'écran

Indique si la capture d'écran est désactivée.

3. Nombre maximal de jours avec le profil de travail désactivé

Contrôle la durée pendant laquelle le profil de travail peut rester désactivé.

4. Partage via Bluetooth

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

5. Espace privé

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

6. Mode Play Store

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

> **Liste d'exclusion (par défaut)** : toutes les applications sont disponibles et toute application qui ne devrait pas être 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 dans 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 est disponible pour 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 de l'appareil d'ajouter des comptes non approuvés sur leur profil personnel.

Politiques interprofils

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

Copier/coller interprofils

Détermine si le texte copié d'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 interprofils

Détermine 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 interprofils, tels que la recherche de contacts, le copier/coller,
ou les applications professionnelles et personnelles connectées, est configurée séparément.

> **Interdit** : Empêche le partage de données, que ce soit du profil personnel vers le profil professionnel ou du profil professionnel vers le profil personnel.
>
> **Partage professionnel vers personnel interdit (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 l'un ou l'autre profil peuvent être partagées avec l'autre profil.

Widgets du profil professionnel par défaut

Comportement par défaut des widgets du profil professionnel. Si une application spécifique ne définit pas de politique de widgets, elle suivra le paramètre défini ici.

Fonctions d'application interprofils

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

> Ce paramètre dépend de l'option **Fonctions d'application** au niveau de la politique (dans la section Gestion des applications). Si les fonctions d'application sont définies sur **Interdit**, l'API rejettera les fonctions d'application interprofils définies sur **Autorisé**.

Contacts professionnels dans le profil personnel

Détermine si les contacts enregistrés dans le profil professionnel peuvent être affichés lors des recherches de contacts et des appels entrants sur le profil personnel.

Autorisé (par défaut) : Permet aux contacts du profil professionnel d'apparaître dans le profil personnel.

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

Interdit sauf système : Empêche la plupart des applications personnelles d'accéder aux contacts du profil professionnel, à l'exception des applications par défaut de l'OEM (Téléphone, Messages et Contacts) (Android 14+).

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

Rapport d'état

Dans cette section, vous pouvez configurer les données qui doivent être récupérées sur l'appareil.

Les données d'état peuvent être consultées sur la page du tableau de bord **État de l'appareil**.

Rapports d'applications

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

> Cette option est requise par le système (pour l'intégration d'applications compagnons) 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 le rapport des paramètres de l'appareil est activé. (Informations sur les paramètres de l'appareil liés à la sécurité sur l'appareil.)

Informations sur le logiciel

Indique si le rapport des informations sur le logiciel est activé. (Informations sur le logiciel de l'appareil.)

Informations sur la mémoire

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

Informations sur le réseau

Indique si le rapport des informations sur le réseau est activé. (Informations sur le réseau de l'appareil.)

Informations sur l'affichage

Indique si le rapport de l'affichage est activé. Les données de rapport ne sont pas disponibles pour les appareils appartenant à des particuliers avec un profil de travail. (Informations sur l'affichage de l'appareil.)

Événements de gestion de l'alimentation

Indique si le rapport des événements de gestion de l'alimentation est activé. Les données de rapport ne sont pas disponibles pour les appareils appartenant à des particuliers avec un profil de travail.

État du matériel

Indique si le rapport de l'état du matériel est activé. Les données de rapport ne sont pas disponibles pour les appareils appartenant à des particuliers avec un profil de travail.

Propriétés du système

Indique si le rapport des propriétés du système est activé.

Mode Critères Communs (Common Criteria)

Indique si le rapport du mode Critères Communs est activé.

Divers

1. Jeu d'Easter egg désactivé

Détermine si le jeu d'Easter egg dans les Paramètres est désactivé.

2. Ignorer les conseils de première utilisation

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

3. Message d'assistance court

Un message affiché à l'utilisateur sur 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

Un message affiché à l'utilisateur sur l'écran des paramètres de l'administrateur de l'appareil.

5. Infos écran de verrouillage du propriétaire

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

6. Actions de configuration

Actions à effectuer pendant le processus de configuration. Lors de l'enrôlement, 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 le lancement de l'application est requis.

6.3. Description

Fournit un message destiné à l'utilisateur pour lui expliquer pourquoi le lancement de l'application est requis.

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 en gestion complète sous 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 de travail ne respecte pas l'un des paramètres de politique énumérés ci-dessous, la politique d'appareil Android bloque immédiatement l'utilisation de l'appareil ou du profil de travail par défaut :

- **Exigences relatives au mot de passe**
- **Politique de chiffrement**
- **Désactivation de l'écran de verrouillage (Keyguard)**
- **Méthodes de saisie autorisées**
- **Services d'accessibilité autorisés**

Si l'appareil ou le profil de travail reste non conforme après 10 jours, la politique d'appareil Android réinitialisera l'appareil aux paramètres d'usine ou supprimera le profil de travail.

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 politique particulière ne peut pas être appliquée à un appareil.

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

Nom du paramètre

La politique de premier niveau à appliquer. Par exemple, **Applications** ou **Exigences relatives au mot de passe**.

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

Bloquer après X jours

Nombre de jours pendant lesquels la politique est non conforme avant que l'appareil ou le profil de travail ne soit bloqué. Pour bloquer l'accès immédiatement, réglez sur 0. **Bloquer après X jours** doit être inférieur à **Réinitialisation après X 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 de travail**.

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

Réinitialisation après X jours

Nombre de jours pendant lesquels la politique est non conforme avant que l'appareil ou le profil de travail ne soit réinitialisé.
Réinitialisation après X jours doit être supérieur à **Bloquer après X jours**. Applicable uniquement aux appareils appartenant à l'entreprise.

Requis. 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 de travail.

Par défaut (nouvelle règle) : activé.