Sécurité

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

Actions en cas de risque de sécurité

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

Types de SecurityRisk pris en charge :

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

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

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

Actions disponibles :

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

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

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

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

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

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

1. Délai maximal avant verrouillage

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

2. Rester allumé pendant la charge

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

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

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

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

3. Keyguard désactivé

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

4. Exigences relatives aux mots de passe

Stratégies relatives aux exigences de mot de passe.

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

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

4.1. Portée

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

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

4.2. Longueur de l'historique des mots de passe

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

4.3. Nombre maximal de mots de passe erronés avant effacement

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

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

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

4.5. Exiger le déverrouillage par mot de passe

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

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

4.6. Qualité du mot de passe

Qualité de mot de passe requise.

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

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

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

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

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

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

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

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

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

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

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

4.7. Longueur minimale

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

4.8. Nombre minimal de lettres

Nombre minimal de lettres requis dans le mot de passe.

4.9. Nombre minimal de lettres minuscules

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

4.10. Nombre minimal de lettres majuscules

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

4.11. Nombre minimal de caractères non alphabétiques

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

4.12. Nombre minimal de chiffres

Nombre minimal de chiffres requis dans le mot de passe.

4.13. Nombre minimal de symboles

Nombre minimal de symboles requis dans le mot de passe.

4.14. Verrouillage unifié

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

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

5. Réinitialisation d'usine désactivée

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

6. Protection contre la réinitialisation d'usine

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

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

7. Fonctionnalités de Keyguard

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

7.1. Tout désactiver

Désactive toutes les personnalisations actuelles et futures de Keyguard.

7.2. Désactiver l'appareil photo

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

7.3. Désactiver les notifications

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

7.4. Désactiver les notifications non masquées

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

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

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

7.6. Désactiver l'empreinte digitale

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

7.7. Désactiver la saisie de texte dans les notifications

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

7.8. Désactiver l'authentification par reconnaissance faciale

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

7.9. Désactiver l'authentification par iris

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

7.10. Désactiver toutes les authentifications biométriques

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

7.11. Désactiver tous les raccourcis

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

Revision #56
Created 2025-12-17 09:33:36 UTC by Admin
Updated 2026-11-12 09:55:17 UTC by Admin