Sécurité

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

Actions liées aux risques de sécurité

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

Types de risques de sécurité pris en charge :

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

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

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

Actions disponibles :

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

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

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

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

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

Effacer les eSIM : Pour les appareils appartenant à l'entreprise, cette option supprime toutes les eSIM de l'appareil lors de l'effacement. Pour les appareils personnels, cette option supprime les eSIM gérées (les eSIM ajoutées via la commande ADD_ESIM) sur les appareils, et aucune eSIM personnelle ne sera supprimée.

1. Durée maximale de verrouillage

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

2. Rester activé pendant la charge

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

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

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

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

3. Verrouillage d'écran désactivé

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

4. Exigences de mot de passe

Politiques de complexité des mots de passe.

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

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

doivent être combinées avec des exigences basées sur la qualité pour la même portée.

4.1. Portée

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

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

4.2. Longueur de l'historique des mots de passe

Longueur de l'historique des mots de passe. Une fois cette valeur définie, l'utilisateur ne pourra pas utiliser un nouveau mot de passe identique à un mot de passe présent dans l'historique. Une valeur de 0 signifie qu'il n'y a aucune restriction.

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

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

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

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

4.5. Nécessite un déverrouillage par mot de passe

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

> **Paramètres par défaut de l’appareil** : La période d’attente est définie sur les paramètres par défaut de l’appareil.
>
> **Chaque jour** : La période de délai d'attente est définie sur 24 heures.

4.6. Qualité du mot de passe

La qualité du mot de passe requise.

Complexité élevée: Définissez la plage de complexité élevée des mots de passe comme suit : Sur Android 12 et versions ultérieures : code PIN sans répétitions (4444) ni séquences ordonnées (1234, 4321, 2468), longueur minimale de 8 caractères ; alphabétique, longueur minimale de 6 caractères ; alphanumérique, longueur minimale de 6 caractères.

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

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

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

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

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

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

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

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

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

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

4.7. Longueur minimale

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

4.8. Minimum de lettres

Nombre minimum de caractères requis pour le mot de passe.

4.9. Minimum de lettres minuscules

Minimum de lettres minuscules requises dans le mot de passe.

4.10. Minimum de lettres majuscules

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

4.11. Nombre minimum de caractères non alphabétiques requis

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

4.12. Nombre minimum de chiffres

Nombre minimum de chiffres requis dans le mot de passe.

4.13. Nombre minimum de symboles

Nombre minimum de symboles requis dans le mot de passe.

4.14. Verrouillage unifié

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

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

5. Réinitialisation aux paramètres d'usine désactivée

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

6. Protection contre la réinitialisation aux paramètres d'usine

Adresses e-mail des administrateurs de l'appareil pour la protection contre la réinitialisation aux paramètres d'usine. Lorsqu'un appareil subit une réinitialisation aux paramètres d'usine non autorisée, l'un de ces administrateurs devra se connecter avec l'adresse e-mail et le mot de passe

du compte Google pour déverrouiller l'appareil. Si aucun administrateur n'est spécifié, l'appareil ne bénéficiera pas de la protection contre la réinitialisation aux paramètres d'usine. S'applique uniquement aux appareils entièrement gérés.

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

7. Fonctionnalités de Keyguard

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

7.1. Désactiver tout

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

7.2. Désactiver la caméra

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

7.3. Désactiver les notifications

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

7.4. Désactiver les notifications sans censure

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

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

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

7.6. Désactiver l'empreinte digitale

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

7.7. Désactiver la saisie de texte dans les notifications

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

7.8. Désactiver l'authentification par reconnaissance faciale

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

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

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

7.10. Désactiver toutes les méthodes d'authentification biométrique

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

7.11. Désactiver tous les raccourcis

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

Revision #38
Created 2025-12-17 09:33:36 UTC by Admin
Updated 2026-06-23 17:14:39 UTC by Admin