Système

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

1. Niveau d'API minimal

Niveau d'API Android minimal autorisé.

2. Stratégie de chiffrement

Indique si le chiffrement est activé.

> **Par défaut** : cette valeur est ignorée, c'est-à-dire qu'aucun chiffrement n'est requis.
>
> **Activé sans mot de passe** : chiffrement requis, mais aucun mot de passe requis au démarrage.
>
> **Activé avec mot de passe** : chiffrement requis avec mot de passe requis au démarrage.

3. Date et heure automatiques

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

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

4. Paramètres de développeur

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

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

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

5. Mode Common Criteria

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

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

Activé : active le mode Common Criteria.

6. Memory Tagging Extension (MTE)

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

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

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

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

7. Protection du contenu

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

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

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

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

8. Contenu d'assistance

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

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

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

9. Création de fenêtres désactivée

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

10. Connexion réseau de secours

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

11. Activités par défaut

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

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

11.1. Activité de réception

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

11.2. Action

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

11.3. Catégorie

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

12. Méthodes de saisie autorisées

Spécifie les méthodes de saisie autorisées.

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

12.1. Méthodes de saisie autorisées

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

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

13. Services d'accessibilité autorisés

Spécifie les services d'accessibilité autorisés.

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

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

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

13.1. Services d'accessibilité autorisés

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

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

14. Stratégie de mise à jour du système

Configuration de la gestion des mises à jour du système.

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

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

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

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

14.1. Fenêtre de maintenance (Fenêtre horaire uniquement)

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

14.2. Périodes de gel des mises à jour système

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

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

15. Fournisseurs d'identifiants par défaut

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

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

Revision #55
Created 2025-12-17 09:33:42 UTC by Admin
Updated 2026-11-12 09:55:07 UTC by Admin