Système

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

1. Niveau d'API minimum

Le niveau d'API Android minimum autorisé.

2. Politique de chiffrement

Indique si le chiffrement est activé.

Par défaut: cette valeur est ignorée, c'est-à-dire qu'aucun chiffrement n'est requis.

Activé sans mot de passe: Le chiffrement est requis, mais aucun mot de passe n'est nécessaire pour le démarrage.

Activé avec mot de passe: Le chiffrement est requis et un mot de passe est nécessaire pour le démarrage.

3. Date et heure automatiques

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

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

Obligatoire: Activer la synchronisation automatique de la date, de l'heure et du fuseau horaire sur l'appareil.

4. Paramètres pour les développeurs

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

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

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

5. Mode de conformité aux critères communs

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

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

Activé : Active le mode Common Criteria.

6. Extension de marquage de la mémoire (MTE)

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

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

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

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

7. Protection du contenu

Active ou désactive la protection du contenu (qui analyse la présence d'applications potentiellement malveillantes). Cette fonctionnalité est prise en charge sur Android 15 et versions ultérieures.

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

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

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

8. Assistance au contenu

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

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

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

9. Créez des fenêtres désactivées

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

10. Porte de sortie réseau

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

11. Activités par défaut

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

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

11.1. Activité du récepteur

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

11.2. Action

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

11.3. Catégorie

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

12. Méthodes de saisie autorisées

Spécifie les méthodes de saisie autorisées.

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

12.1. Méthodes de saisie autorisées

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

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

13. Services d'accessibilité autorisés

Spécifie les services d'accessibilité autorisés.

> **Tous autorisés** : Tout service d'accessibilité peut être utilisé.
>
> **Seuls les services** : Seuls les services d'accessibilité intégrés au système peuvent être utilisés.
>
> **Seuls les services** : Seuls les services d'accessibilité intégrés au système et ceux fournis peuvent être utilisés.

13.1. Services d'accessibilité autorisés

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

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

14. Stratégie de mise à jour du système

Configuration pour gérer les mises à jour du système.

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

14.1. Fenêtre de maintenance (Uniquement fenêtré)

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

14.2. Périodes de suspension des mises à jour système

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

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

15. Fournisseurs de crédentiels par défaut

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

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

Revision #34
Created 2025-12-17 09:33:42 UTC by Admin
Updated 2026-04-22 15:50:21 UTC by Admin