النظام

في هذا القسم، يمكنك تهيئة السياسات المتعلقة بالنظام.

1. الحد الأدنى لمستوى API

الحد الأدنى المسموح به لمستوى Android API.

2. سياسة التشفير

ما إذا كان التشفير ممكّناً.

افتراضي: تُتجاهل هذه القيمة، أي لا يُشترط التشفير.

ممكّن بدون كلمة مرور: التشفير مطلوب ولكن لا تُشترط كلمة مرور للإقلاع.

ممكّن مع كلمة مرور: التشفير مطلوب مع كلمة مرور مطلوبة للإقلاع.

3. التاريخ والوقت التلقائيان

ما إذا كان التاريخ والوقت والمنطقة الزمنية التلقائية ممكّنة على جهاز مملوك للشركة.

اختيار المستخدم (افتراضي): يُترك التاريخ والوقت والمنطقة الزمنية التلقائية لاختيار المستخدم.

مفروض: فرض التاريخ والوقت والمنطقة الزمنية التلقائية على الجهاز.

4. إعدادات المطوّر

يتحكم في الوصول إلى إعدادات المطوّر: خيارات المطوّر والتمهيد الآمن.

معطّل (افتراضي): يعطّل جميع إعدادات المطوّر ويمنع المستخدم من الوصول إليها.

مسموح: يسمح بجميع إعدادات المطوّر. يمكن للمستخدم الوصول إلى الإعدادات وتكوينها اختيارياً.

5. وضع المعايير المشتركة

يتحكم في وضع المعايير المشتركة — معايير الأمان المحددة في Common Criteria لتقييم أمن تكنولوجيا المعلومات (CC). يؤدي تفعيل وضع المعايير المشتركة إلى زيادة بعض مكوّنات الأمان على الجهاز (على سبيل المثال: تشفير AES-GCM لمفاتيح Bluetooth طويلة الأمد، والتحقق الإضافي من بعض شهادات الشبكة، وفحوص سلامة سياسة التشفير). وضع المعايير المشتركة مدعوم فقط على الأجهزة المملوكة للشركة التي تعمل بنظام Android 11 أو أحدث. تحذير: يفرض وضع المعايير المشتركة نموذج أمان صارمًا يُطلب عادةً للمؤسسات شديدة الحساسية. قد يتأثر الاستخدام العادي للجهاز؛ لا تفعّله إلا إذا كان مطلوبًا.

معطّل (افتراضي): يعطّل وضع المعايير المشتركة.

مفعّل: يفعّل وضع المعايير المشتركة.

6. Memory Tagging Extension (MTE)

يتحكم في Memory Tagging Extension (MTE) على الجهاز.

اختيار المستخدم (افتراضي): يمكن للمستخدم اختيار تفعيل MTE أو تعطيله على الجهاز (إذا كان الجهاز يدعم ذلك).

مفروض: يُفعّل MTE ولا يُسمح للمستخدم بتغييره (Android 14+؛ مدعوم على الأجهزة المملوكة للشركة المُدارة بالكامل وملفات تعريف العمل على الأجهزة المملوكة للشركة).

معطّل: يُعطّل MTE ولا يُسمح للمستخدم بتغييره (Android 14+؛ مدعوم على الأجهزة المُدارة بالكامل فقط).

7. حماية المحتوى

يتحكم في تفعيل حماية المحتوى (التي تفحص التطبيقات الخادعة). هذا مدعوم على Android 15 وما فوق.

معطّل (افتراضي): حماية المحتوى معطّلة ولا يمكن للمستخدم تغيير ذلك.

مفروض: حماية المحتوى مفعّلة ولا يمكن للمستخدم تغيير ذلك (Android 15+).

اختيار المستخدم: حماية المحتوى غير خاضعة للسياسة؛ يمكن للمستخدم الاختيار (Android 15+).

8. محتوى المساعدة

يتحكم في السماح بإرسال AssistContent إلى تطبيق ذي امتيازات مثل تطبيق مساعد (على سبيل المثال، Circle to Search). يتضمن AssistContent لقطات شاشة ومعلومات عن التطبيق، مثل اسم الحزمة. هذا مدعوم على Android 15 وما فوق.

> **مسموح (افتراضي)**: يُسمح بإرسال محتوى المساعدة إلى تطبيق ذي امتيازات (Android 15+).
>
> **غير مسموح**: يُحظر إرسال محتوى المساعدة إلى تطبيق ذي امتيازات (Android 15+).

9. تعطيل إنشاء النوافذ

هل إنشاء نوافذ غير نوافذ التطبيقات معطّل. يمنع هذا الخيار عرض واجهات النظام التالية: الإشعارات المنبثقة (toasts) والأشرطة السريعة (snackbars)، وأنشطة الهاتف (مثل المكالمات الواردة) وأنشطة الهاتف ذات الأولوية (مثل المكالمات الجارية)، وتنبيهات النظام، وأخطاء النظام، وطبقات النظام العلوية.

10. منفذ الشبكة الاحتياطي

هل منفذ الشبكة الاحتياطي مفعّل. إذا تعذّر إنشاء اتصال بالشبكة عند التمهيد، يطلب المنفذ الاحتياطي من المستخدم الاتصال بشبكة مؤقتاً لتحديث سياسة الجهاز. بعد تطبيق السياسة، تُنسى الشبكة المؤقتة ويستمر الجهاز في التمهيد. يمنع ذلك عدم القدرة على الاتصال بالشبكة إذا لم تكن هناك شبكة مناسبة في آخر سياسة وكان الجهاز يبدأ التشغيل في تطبيق وضع تثبيت المهام، أو إذا لم يتمكن المستخدم من الوصول إلى إعدادات الجهاز.

11. الأنشطة الافتراضية

قائمة بالأنشطة الافتراضية لمعالجة النوايا (intents) التي تطابق مرشح نوايا معيناً. على سبيل المثال، تتيح هذه الميزة لمسؤولي تقنية المعلومات اختيار تطبيق المتصفح الذي يفتح روابط الويب تلقائياً، أو تطبيق مشغّل التشغيل المستخدم عند الضغط على زر الصفحة الرئيسية.

استخدم **إضافة نشاط افتراضي** لإنشاء إدخالات. داخل الإدخال، استخدم **إضافة إجراء** و**إضافة فئة** لإنشاء مرشح النوايا.

11.1. نشاط الاستقبال

النشاط الذي يجب أن يكون معالج النوايا الافتراضي. يجب أن يكون هذا اسم مكوّن Android، مثل com.android.enterprise.app/.MainActivity. بدلاً من ذلك، يمكن أن تكون القيمة اسم حزمة تطبيق،

مما يجعل Android Device Policy يختار نشاطاً مناسباً من التطبيق لمعالجة النية.

11.2. الإجراء

إجراءات النوايا المطلوب مطابقتها في المرشح. إذا تم تضمين أي إجراءات في المرشح، فيجب أن يكون إجراء النية أحد تلك القيم لكي تتطابق. إذا لم يتم تضمين أي إجراءات، يتم تجاهل إجراء النية.

11.3. الفئة

فئات النوايا المطلوب مطابقتها في المرشح. تتضمن النية الفئات التي تتطلبها، ويجب تضمينها جميعاً في المرشح لكي تتطابق. بعبارة أخرى، إضافة فئة إلى المرشح ليس لها تأثير على المطابقة ما لم تُحدّد تلك الفئة في النية.

12. طرق الإدخال المسموح بها

يحدد طرق الإدخال المسموح بها.

> **الكل مسموح**: لم يتم تطبيق أي قيود. جميع طرق الإدخال مسموح بها.
>
> **أنظمة النظام فقط**: طرق الإدخال المدمجة في النظام فقط مسموح بها.
>
> **أنظمة النظام والمقدمة فقط**: طرق الإدخال المقدمة والمدمجة في النظام فقط مسموح بها.

12.1. طرق الإدخال المسموح بها

أسماء حزم طرق الإدخال المسموح بها. ينطبق فقط عندما تكون **طرق الإدخال المسموح بها** مضبوطة على **أنظمة النظام والمقدمة فقط**.

استخدم **إضافة طريقة إدخال** لإضافة الإدخالات وإزالتها باستخدام إجراء الحذف.

13. خدمات إمكانية الوصول المسموح بها

يحدد خدمات إمكانية الوصول المسموح بها.

> **الكل مسموح**: يمكن استخدام أي خدمة إمكانية وصول.
>
> **أنظمة النظام فقط**: يمكن استخدام خدمات إمكانية الوصول المدمجة في النظام فقط.
>
> **أنظمة النظام والمقدمة فقط**: يمكن استخدام خدمات إمكانية الوصول المقدمة والمدمجة في النظام فقط.

13.1. خدمات إمكانية الوصول المسموح بها

خدمات إمكانية الوصول المسموح بها. ينطبق فقط عندما تكون **خدمات إمكانية الوصول المسموح بها** مضبوطة على **أنظمة النظام والمقدمة فقط**.

استخدم **إضافة خدمة إمكانية وصول** لإضافة الإدخالات وإزالتها باستخدام إجراء الحذف.

14. سياسة تحديث النظام

تكوين لإدارة تحديثات النظام.

> **افتراضي**: اتبع سلوك التحديث الافتراضي للجهاز، والذي يتطلب عادةً من المستخدم قبول تحديثات النظام.
>
> **تلقائي**: التثبيت تلقائياً بمجرد توفر تحديث.
>
> **ضمن نافذة زمنية**: التثبيت تلقائياً ضمن نافذة صيانة يومية. يضبط هذا أيضاً تحديث تطبيقات Play ضمن النافذة. يُوصى بشدة بذلك لأجهزة الكشك لأنه الطريقة الوحيدة التي يمكن بها تحديث التطبيقات المثبتة في المقدمة بشكل دائم بواسطة Play.
>
> **تأجيل**: تأجيل التثبيت التلقائي لمدة أقصاها 30 يوماً.

14.1. نافذة الصيانة (ضمن نافذة زمنية فقط)

عندما تكون **سياسة تحديث النظام** مضبوطة على **ضمن نافذة زمنية**، يمكنك تحديد نافذة الصيانة اليومية باستخدام حقلي **من** و**إلى**.

14.2. فترات تجميد تحديث النظام

فترة زمنية متكررة سنوياً يتم فيها تأجيل تحديثات النظام اللاسلكية (OTA) لتجميد إصدار نظام التشغيل على الجهاز. لمنع تجميد الجهاز إلى ما لا نهاية، يجب أن تفصل بين كل فترة تجميد 60 يوماً على الأقل. ويجب ألا تتجاوز كل فترة تجميد 90 يوماً.

استخدم **إضافة فترة تجميد تحديث النظام** لإنشاء إدخالات.

15. موفّرو بيانات الاعتماد الافتراضيون

يتحكم في التطبيقات المسموح لها بالعمل كموفّري بيانات اعتماد على Android 14 وما فوق.

غير مسموح (افتراضي): التطبيقات التي تكون credentialProviderPolicy غير محددة ال يُسمح لها بالعمل كموفّر بيانات اعتماد.

غير مسموح باستثناء النظام: التطبيقات التي تكون credentialProviderPolicy غير محددة ال يُسمح لها بالعمل كموفّر بيانات اعتماد، باستثناء موفّري بيانات الاعتماد الافتراضيين من الشركة المصنعة (OEM).

Revision #58
Created 2025-12-17 09:32:28 UTC by Admin
Updated 2026-11-12 09:53:12 UTC by Admin