# السياسات - Android


- الملخص
- إدارة التطبيقات
- وضع الكشك
- الأمان
- الوسائط المتعددة
- الشبكة الخلوية
- الشبكات
- النظام
- الموقع والنطاقات الجغرافية
- إدارة المستخدمين
- الاستخدام الشخصي
- السياسات العابرة لملفات التعريف
- الإبلاغ عن الحالة
- متفرقات
- قواعد الامتثال

# الملخص

سياسات Android هي الكيانات الأساسية للنظام: فهي تحدد القواعد التي تُطبّق وتُفرض على الأجهزة المُدارة.

يمكنك تصفح سياساتك وإنشاء سياسات جديدة من قسم **السياسات** في لوحة التحكم. لفتح سياسة Android، انقر على صف السياسة في الجدول: يفتح النظام صفحة **محرر السياسات**.

يمكن ربط سياسة بـرمز تسجيل، بحيث تُطبّق تلقائيًا على الأجهزة أثناء عملية التجهيز. يمكنك أيضًا تغيير السياسة المعيّنة لجهاز بعد التجهيز.

> يمكن ربط كل جهاز بسياسة واحدة فقط في كل مرة.

> تسري العديد من خيارات السياسة على أنواع أجهزة محددة فقط (مُدارة بالكامل، مخصصة، ملف تعريف عمل) وإصدارات Android. قد يتجاهل الجهاز الإعدادات غير المدعومة، أو يُبلغ عنها على أنها غير ممتثلة.

# تخطيط محرر السياسات

ينظّم محرر السياسات كمجموعة من الأقسام القابلة للتوسيع. في أعلى الصفحة يمكنك دائمًا تعديل:

- **الاسم** (مطلوب)
- **المعرّف** (للقراءة فقط)
- **الوصف** (اختياري)

تتوافق الأقسام أدناه مع لوحات محرّر السياسة (مثل: إدارة التطبيقات، والأمان، والشبكات، والنظام، والاستخدام الشخصي، وسياسات الملفات المتقاطعة، والمزيد). عند فتح سياسة محفوظة، تكون الأقسام التي غيّرت إعداداتها مفتوحة بالفعل وتبقى الأخرى مغلقة. استخدم صفحات الفصول في هذا الدليل لفهم كل لوحة بالتفصيل.

# الحفظ والحذف والأجهزة المرتبطة

استخدم **حفظ السياسة** لتطبيق التغييرات. يكون الزر معطّلًا عند عدم وجود تعديلات معلّقة، أو عند انتهاء صلاحية الترخيص.

إذا فتحت سياسة موجودة (لها معرّف)، فتعرض الصفحة إجراء **حذف السياسة** وقائمة **الأجهزة المرتبطة** في الأسفل، حتى تتمكن من رؤية عدد الأجهزة التي تستخدم السياسة حاليًا.

# إدارة التطبيقات

في هذا القسم، يمكنك تعيين سياسات تتعلق بتوفر التطبيقات وتثبيتها وتحديثاتها وإدارة الأذونات.

> تُنشأ حسابات Managed Google Play تلقائيًا عند تجهيز الأجهزة.

## 1. وضع Play Store

يتحكم هذا الوضع في التطبيقات المتاحة للمستخدم في Play Store وفي السلوك على الجهاز عند إزالة التطبيقات من السياسة.

**القائمة البيضاء (الافتراضي)**: لا تتوفر إلا التطبيقات الموجودة في السياسة، وأي تطبيق غير موجود فيها ستتم إزالته تلقائيًا من الجهاز. لن يعرض Play Store إلا التطبيقات المتاحة.

**القائمة السوداء**: تتوفر جميع التطبيقات، وأي تطبيق لا يجب أن يكون على الجهاز ينبغي وضع علامة **محظور** عليه صراحةً في سياسة التطبيقات. سيعرض Play Store جميع التطبيقات باستثناء المحظورة.

## 2. سياسة التطبيقات غير الموثوقة

السياسة الخاصة بالتطبيقات غير الموثوقة (التطبيقات من مصادر غير معروفة) التي تُفرض على الجهاز. يتحكم هذا الخيار في إعداد نظام Android الذي يحدد ما إذا كان المستخدم يستطيع تثبيت تطبيقات من خارج Play Store (التثبيت الجانبي).

**عدم السماح (الافتراضي)**: عدم السماح بتثبيت تطبيقات غير موثوقة على الجهاز بأكمله.

**الملف الشخصي فقط**: بالنسبة للأجهزة التي تحتوي على ملفات تعريف عمل، اسمح بتثبيت التطبيقات غير الموثوقة في الملف الشخصي للجهاز فقط.

**السماح**: السماح بتثبيت تطبيقات غير موثوقة على الجهاز بأكمله.

## 3. Google Play Protect

ام إذا كان التحقق من التطبيقات عبر Google Play Protect مفروضًا.

**مفروض (الافتراضي)**: يفعّل التحقق من التطبيقات قسرًا.

**اختيار المستخدم**: يسمح للمستخدم باختيار ما إذا كان سيفعّل التحقق من التطبيقات.

## 4. سياسة الأذونات الافتراضية

السياسة الخاصة بمنح طلبات أذونات وقت التشغيل للتطبيقات.

**المطالبة (الافتراضي)**: مطالبة المستخدم بمنح إذن.

**المنح**: منح إذن تلقائيًا.

**الرفض**: رفض إذن تلقائيًا.

## 5. وظائف التطبيقات

يتحكم في ما إذا كان يُسمح للتطبيقات على الأجهزة المدُارة بالكامل أو في ملفات تعريف العمل بكشف وظائف التطبيقات. يتطلب Android 16 أو أحدث.

**مسموح (الافتراضي)**: يمكن للتطبيقات على الأجهزة المدُارة بالكامل أو في ملفات تعريف العمل كشف وظائف التطبيقات.

**غير مسموح**: لا يمكن للتطبيقات على الأجهزة المدُارة بالكامل أو في ملفات تعريف العمل كشف وظائف التطبيقات.

## 6. تثبيت التطبيقات معطّل

ما إذا كان تثبيت المستخدم للتطبيقات معطّلًا.

## 7. إلغاء تثبيت التطبيقات معطّل

ما إذا كان إلغاء المستخدم لتثبيت التطبيقات معطّلًا.

## 8. سياسات الأذونات

منح أو رفض صريح للأذونات أو المجموعات لجميع التطبيقات. تتجاوز هذه القيم إعداد **سياسة الأذونات الافتراضية**.

استخدم **إضافة سياسة أذونات** لإنشاء إدخالات، وأزلها باستخدام إجراء الحذف.

يتضمن كل إدخال:

> **إذن/مجموعة Android**: إذن أو مجموعة Android (مطلوب)، مثل **android.permission.READ_CALENDAR** أو **android.permission_group.CALENDAR**.
>
> **السياسة**: منح / رفض / مطالبة (تستخدم خيارات السياسة نفسها كـ**سياسة الأذونات الافتراضية**).

## 9. التطبيقات

قائمة التطبيقات التي يجب تضمينها في السياسة. يعتمد سلوك محتوى القائمة على القيمة المحددة في **وضع Play Store**.

إذا كان **وضع Play Store** مضبوطاً على **القائمة البيضاء**، فلا تتوفر إلا التطبيقات الموجودة في السياسة، وأي تطبيق غير موجود فيها ستتم إزالته تلقائياً من الجهاز.

إذا كان **وضع Play Store** مضبوطاً على **القائمة السوداء**، تتوفر جميع التطبيقات، وأي تطبيق لا يجب أن يكون على الجهاز ينبغي وضع علامة **محظور** عليه صراحةً في سياسة التطبيقات.

لإضافة تطبيق جديد، انقر على زر **إضافة تطبيقات** (أو أيقونة **إضافة تطبيقات**)، واختر **من Managed Google Play**، ثم اختر التطبيق من Play Store وانقر على زر **تحديد** في بطاقة التطبيق.

لإضافة تطبيق غير منشور على Google Play لكنه موجود بالفعل على الجهاز (مثل تطبيق نظام أو تطبيق من الشركة المصنعة)، انقر على **إضافة تطبيقات**، واختر **حسب اسم الحزمة (التطبيقات المثبتة مسبقاً)**، واكتب اسم حزمة التطبيق (مثل **com.example.app**) ثم انقر على **إضافة**.يُضاف التطبيق بنوع التثبيت **مثبّت قسراً**. لإظهار التطبيق في مشغّل Kiosk المخصص، يجب أن يكون **نوع التثبيت** الخاص به **مثبّتاً مسبقاً** أو **مثبّتاً قسراً**: مع **متاح** لا يظهر التطبيق.

> تُوسم التطبيقات غير المتاحة على Managed Google Play بأيقونة Android في قائمة التطبيقات. لا يمكن تثبيتها من Google Play، لذا يجب أن تكون موجودة بالفعل على الجهاز: الأجهزة التي لا تحتوي على التطبيق لا تستطيع تثبيته.

> جميع التطبيقات المنشورة على Play Store في بلدك متاحة للاختيار افتراضياً. لتحديد تطبيقاتك الخاصة أو تطبيقات الويب، يجب رفعها إلى النظام أولاً. لمزيد من المعلومات، اقرأ صفحة

> **التطبيقات الخاصة**.

يمكن تهيئة كل تطبيق بإعداداته الخاصة، التي تظهر داخل بطاقة:

## 9.1. نوع التثبيت

نوع التثبيت الذي سيُجرى للتطبيق.

**متاح**: التطبيق متاح للتثبيت.

**مثبّت مسبقاً**: يُثبّت التطبيق تلقائياً ويمكن للمستخدم إزالته.

**مثبّت قسراً**: يُثبّت التطبيق تلقائياً ولا يمكن للمستخدم إزالته.

**محظور**: التطبيق محظور ولا يمكن تثبيته. إذا كان التطبيق مثبّتاً بموجب سياسة سابقة، فستتم إزالته.

**مطلوب للإعداد**: يُثبّت التطبيق تلقائياً ولا يمكن للمستخدم إزالته، وسيمنع اكتمال الإعداد حتى يكتمل التثبيت.

**Kiosk**: يُثبّت التطبيق تلقائياً في وضع Kiosk: يُضبط كنية الشاشة الرئيسية المفضلة ويُدرج في القائمة البيضاء وضع مهمة القفل. لن يكتمل إعداد الجهاز حتى يُثبّت التطبيق. بعد التثبيت، لن يتمكن المستخدمون من إزالة التطبيق. يمكنك ضبط **نوع التثبيت** هذا لتطبيق واحد فقط لكل سياسة. عند وجوده في السياسة، سيُعطّل شريط الحالة تلقائياً. لمزيد من المعلومات، يرجى قراءة صفحة **وضع Kiosk** المخصصة.

## 9.2. قيود التثبيت

يحدد مجموعة من القيود لتثبيت التطبيق. عند تحديد عدة قيود، يجب استيفاؤها جميعاً ليُثبّت التطبيق.

> يظهر هذا الخيار فقط عندما يكون **نوع التثبيت مثبّتاً مسبقاً** أو **مثبّتاً قسراً**.

**شبكة غير محدودة**: ثبّت التطبيق فقط عندما يكون الجهاز متصلاً بشبكة غير محدودة (مثل Wi-Fi).

**الشحن**: ثبّت التطبيق فقط عندما يكون الجهاز قيد الشحن.

**خامل**: ثبّت التطبيق فقط عندما يكون الجهاز خاملاً.

## 9.3. وضع التحديث التلقائي

يتحكم في وضع التحديث التلقائي للتطبيق.

**الافتراضي**: يُحدّث التطبيق تلقائيًا بأولوية منخفضة لتقليل التأثير على المستخدم. يُحدّث التطبيق عند استيفاء جميع القيود التالية: (1) الجهاز غير مستخدم بشكل نشط، (2) الجهاز متصل بشبكة غير محدودة، (3) الجهاز قيد الشحن. يُبلَّغ الجهاز عن تحديث جديد خلال 24 ساعة بعد نشره من المطوّر، ثم يُحدّث التطبيق في المرة التالية التي تُستوفى فيها القيود أعلاه.

**مؤجّل**: لا يُحدّث التطبيق تلقائيًا لمدة أقصاها 90 يومًا بعد أن يصبح قديمًا. بعد 90 يومًا من أن يصبح التطبيق قديمًا، يُثبّت أحدث إصدار متاح تلقائيًا بأولوية منخفضة (انظر **الافتراضي** وضع التحديث التلقائي). بعد تحديث التطبيق، لا يُحدّث تلقائيًا مرة أخرى حتى 90 يومًا بعد أن يصبح قديمًا مجددًا. ولا يزال بإمكان المستخدم تحديث التطبيق يدويًا من Play Store في أي وقت.

**أولوية عالية**: يُحدّث التطبيق في أقرب وقت ممكن. لا تُطبّق أي قيود. يُبلَّغ الجهاز فورًا عن تحديث جديد بعد أن يصبح متاحًا.

## 9.4. الحد الأدنى لرمز الإصدار

الحد الأدنى لإصدار التطبيق الذي يعمل على الجهاز. إذا تم تعيينه، يحاول الجهاز تحديث التطبيق إلى رمز الإصدار هذا على الأقل. إذا لم يكن التطبيق محدّثًا، سيحتوي الجهاز على **تفصيل عدم الامتثال** مع **سبب عدم الامتثال** مضبوطًا على **APP_NOT_UPDATED**. يجب أن يكون التطبيق منشورًا بالفعل على Google Play برمز إصدار أكبر من أو يساوي هذه القيمة. يمكن لـ20 تطبيقًا كحد أقصى تحديد رمز إصدار أدنى لكل سياسة.

## 9.5. النطاقات المفوّضة

النطاقات المفوّضة إلى التطبيق من Android Device Policy. يمكنك منح تطبيقات أخرى مجموعة مختارة من أذونات Android الخاصة:

**تثبيت الشهادات**: يمنح الوصول إلى تثبيت الشهادات وإدارتها.

**التكوينات المُدارة**: يمنح الوصول إلى إدارة التكوينات المُدارة.

**حظر إلغاء التثبيت**: يمنح الوصول إلى حظر إلغاء التثبيت.

**الأذونات**: يمنح الوصول إلى سياسة الأذونات وحالة منح الأذونات.

**الوصول إلى الحزم**: يمنح الوصول إلى حالة الوصول إلى الحزم.

**تطبيق النظام**: يمنح الوصول لتفعيل تطبيقات النظام.

## 9.6. الشبكة التفضيلية

خدمة الشبكة التفضيلية التي ستُستخدم لهذا التطبيق. إذا تم ضبطها، سيستخدم التطبيق شريحة الشبكة المؤسسية المحددة لاتصالاته عند توفرها. يجب أن تتطابق هذه مع شريحة شبكة مهيأة في قسم **تكوين تقطيع شبكة 5G** في لوحة **الشبكة الخلوية**.

## 9.7. سياسة الأذونات الافتراضية

السياسة الافتراضية لجميع الأذونات التي يطلبها التطبيق. إذا تم تحديدها، فإنها تتجاوز **سياسة الأذونات الافتراضية** على مستوى السياسة التي تنطبق على جميع التطبيقات. وهي ال تتجاوز **سياسات الأذونات** التي تنطبق على جميع التطبيقات.

**المطالبة (الافتراضي)**: مطالبة المستخدم بمنح إذن.

**المنح**: منح إذن تلقائياً.

**الرفض**: رفض إذن تلقائياً.

## 9.8. تطبيق العمل والشخصي المتصل

يتحكم في ما إذا كان التطبيق يستطيع التواصل مع نفسه عبر ملفي تعريف العمل والشخصي على الجهاز، وفقاً لموافقة المستخدم (Android 11+).

**غير مسموح (الافتراضي)**: يمنع التطبيق من التواصل عبر ملفات التعريف.

**مسموح**: يسمح للتطبيق بالتواصل عبر ملفات التعريف بعد تلقي موافقة المستخدم.

## 9.9. إعفاء من قفل Always On VPN

يحدد ما إذا كان يُسمح للتطبيق بالشبكات عندما ال يكون VPN متصلاً ويكون **تفعيل القفل** نشطاً. مدعوم فقط على الأجهزة التي تعمل بنظام Android 10 أو أحدث.

**مفروض (الافتراضي)**: يحترم التطبيق إعداد قفل Always On VPN.

**معفى**: التطبيق معفى من إعداد قفل Always On VPN.

## 9.10. أدوات ملف تعريف العمل

يحدد ما إذا كان يُسمح للتطبيق المثبّت في ملف تعريف العمل بإضافة أدوات إلى الشاشة الرئيسية.

**مسموح**: يمكن للتطبيق إضافة أدوات إلى الشاشة الرئيسية.

**غير مسموح**: ال يمكن للتطبيق إضافة أدوات إلى الشاشة الرئيسية.

## 9.11. إعدادات تحكم المستخدم

يحدد ما إذا كان تحكم المستخدم مسموحاً لتطبيق معين. يشمل تحكم المستخدم إجراءات مثل إيقاف التطبيق قسراً ومسح بيانات التطبيق (Android 11+). إذا كانت **extensionConfig** مفعّلة لتطبيق، فإن تحكم المستخدم غير مسموح بغض النظر عن هذا الإعداد. لتطبيقات Kiosk، يمكن استخدام **مسموح** للسماح بتحكم المستخدم.

**غير محدد**: يستخدم السلوك الافتراضي للتطبيق لتحديد ما إذا كان تحكم المستخدم مسموحاً أو غير مسموح.

**مسموح**: تحكم المستخدم مسموح للتطبيق.

**غير مسموح**: تحكم المستخدم غير مسموح للتطبيق.

## 9.12. معطّل

ما إذا كان التطبيق معطّلاً. عند التعطيل، تظل بيانات التطبيق محفوظة.

## 9.13. السماح بمزوّد بيانات الاعتماد

ما إذا كان يُسمح للتطبيق بالعمل كمزوّد بيانات اعتماد على Android 14 أو أحدث.

## 9.14. التكوين المُدار

لتهيئة الإعدادات المُدارة للتطبيق، انقر على زر **تفعيل التكوين المُدار**. إذا كان قد تم ضبط تكوين مُدار للتطبيق بالفعل، يمكنك تعديل التكوين بزر **التكوين المُدار**، أو حذفه بزر **إزالة التكوين**.

> **التكوين المُدار** متاح فقط للتطبيقات التي تدعم هذه الوظيفة.

## 9.15. سياسات الأذونات

منح أو رفض صريح للأذونات للتطبيق. تتجاوز هذه القيم **سياسة الأذونات الافتراضية** و **سياسات الأذونات** التي تنطبق على جميع التطبيقات.

استخدم **إضافة سياسة أذونات** لإضافة قاعدة أذونات واحدة أو أكثر لبطاقة التطبيق، وأزلها باستخدام إجراء الحذف.

## 9.16. معرّفات المسارات

قائمة معرّفات مسارات الاختبار المغلق للتطبيق التي يمكن للجهاز الوصول إليها. إذا تم تحديد عدة معرّفات مسارات، تتلقى الأجهزة أحدث إصدار من بين جميع المسارات المتاحة. إذا لم يتم تحديد أي معرّف مسار، فلا يمكن للأجهزة الوصول إلا إلى مسار الإنتاج للتطبيق.

> خيار **معرّفات المسارات** متاح فقط للتطبيقات التي لديها معرّف مسار واحد على الأقل متاح لمؤسستك. لمزيد من التفاصيل حول كيفية إضافة مؤسستك إلى مسار اختبار مغلق لتطبيق معين، يرجى القراءة هنا.

# 10. إعدادات التطبيقات الافتراضية

عيّن تطبيقات افتراضية للأنواع المدعومة. عند تعيين تطبيق افتراضي لنوع واحد على الأقل، يُمنع المستخدمون من تغيير التطبيقات الافتراضية في ملف التعريف ذلك.

> 

يُسمح بإعداد تطبيق افتراضي واحد فقط لكل**نوع تطبيق افتراضي**. يجب ألا تحتوي قائمة التطبيقات الافتراضية على تكرارات.

### 10.1. نوع التطبيق الافتراضي

اختر فئة التطبيق لتهيئتها (مثل المتصفح أو تطبيق الاتصال أو الرسائل النصية أو المحفظة أو المساعد). يعتمد التوفر على إصدار Android ووضع الإدارة.

### 10.2. نطاقات التطبيق الافتراضي

حدّد المكان الذي ينطبق فيه التطبيق الافتراضي (مُدار بالكامل، ملف تعريف العمل، أو الملف الشخصي). لا يمكن اختيار إلا النطاقات المدعومة من النوع المحدد.

إذا لم يكن أي من النطاقات المحددة قابلاً للتطبيق على وضع إدارة الجهاز، فسيُبلغ الجهاز بتفصيل عدم امتثال.

### 10.3. التطبيقات الافتراضية

قائمة التطبيقات التي يمكن تعيينها كافتراضية للنوع المحدد. يُعيّن أول تطبيق مثبّت ومؤهل كتطبيق افتراضي.

إذا كانت النطاقات تشمل **مُدار بالكامل** أو **ملف تعريف العمل**، فيجب أن يكون كل تطبيق موجوداً أيضاً في قائمة **التطبيقات** مع **نوع تثبيت** غير مضبوط على **محظور**.

## 11. اختيار المفاتيح الخاص

يسمح بعرض واجهة على الجهاز ليختار المستخدم اسماً مستعاراً لمفاتيح خاص إذا لم تكن هناك قواعد مطابقة في **اختيار قواعد المفاتيح الخاصة**.

بالنسبة للأجهزة الأقدم من Android P، قد يؤدي ضبط هذا إلى ترك مفاتيح المؤسسة عرضة للخطر.

## 12. اختيار قواعد المفاتيح الخاصة

يتحكم في وصول التطبيقات إلى المفاتيح الخاصة. تحدد القاعدة المفتاح الخاص، إن وُجد، الذي يمنحه Android Device Policy للتطبيق المحدد. يُمنح الوصول إما عندما يستدعي التطبيق KeyChain.choosePrivateKeyAlias (أو أي نسخ محمّلة) لطلب اسم مستعار لمفتاح خاص لعنوان URL معين، أو للقواعد غير الخاصة بعنوان URL (أي إذا لم يتم ضبط urlPattern، أو تم ضبطه على سلسلة فارغة أو .*) على Android 11 وأحدث، مباشرةً بحيث يمكن للتطبيق استدعاء

KeyChain.getPrivateKey دون الحاجة أولاً إلى استدعاء KeyChain.choosePrivateKeyAlias. عندما يستدعي تطبيق KeyChain.choosePrivateKeyAlias وكانت أكثر من قاعدة choosePrivateKeyRules متطابقة، تحدد آخر قاعدة متطابقة اسم المفتاح المستعار الذي يُعاد.

استخدم **إضافة قاعدة مفتاح خاص** لإنشاء إدخالات، وأزلها باستخدام إجراء الحذف.

## 12.1. اسم المفتاح الخاص المستعار

الاسم المستعار للمفتاح الخاص المراد استخدامه.

## 12.2. نمط URL

نمط URL المطلوب مطابقته مع عنوان URL للطلب. إذا لم يتم ضبطه أو كان فارغاً، فإنه يطابق جميع عناوين URL. يستخدم هذا صيغة التعبيرات النمطية الخاصة بـ java.util.regex.Pattern.

## 12.3. أسماء الحزم

أسماء الحزم التي تنطبق عليها هذه القاعدة. يتم التحقق من تجزئة شهادة توقيع كل تطبيق مقابل التجزئة المقدمة من Play. إذا لم تُحدد أسماء حزم، فيُقدّم الاسم المستعار لجميع التطبيقات التي تستدعي KeyChain.choosePrivateKeyAlias أو أي نسخ محمّلة (ولكن ليس دون استدعاء KeyChain.choosePrivateKeyAlias، حتى على Android 11 وأحدث). أي تطبيق يحمل معرّف Android UID نفسه لحزمة محددة هنا سيكون لديه وصول عند استدعاء KeyChain.choosePrivateKeyAlias.

استخدم **إضافة اسم حزمة** لإضافة إدخالات، وأزلها باستخدام إجراء الحذف.

> لحذف تطبيق، انقر على أيقونة **سلة المهملات** في أسفل بطاقة التطبيق.

# وضع الكشك

باستخدام وضع الكشك، يمكنك تقييد وظائف الجهاز بتطبيق واحد أو عدة تطبيقات. يعتمد الاختيار بين وضع الكشك أحادي التطبيق ومتعدد التطبيقات على أهداف عملك.

في **وضع الكشك أحادي التطبيق**، يُكوّن الجهاز لتطبيق واحد ولا يسمح للمستخدمين النهائيين بالوصول إلى تطبيقات أخرى على الجهاز. كما لا يمكنهم الخروج من التطبيق، مما يجعله جهازاً مخصصاً لذلك التطبيق تحديداً. لتمكين هذا الوضع، حدّد تطبيقاً في قسم **إدارة التطبيقات** مع ضبط **نوع التثبيت** على **كشك**.

في **وضع الكشك متعدد التطبيقات**، يُسمح للأجهزة بالوصول إلى عدة تطبيقات. يمكن للمستخدمين النهائيين التنقل بين تطبيقات متعددة عبر مشغّل مخصص. لتمكين هذا الوضع، فعّل خيار **مشغّل الكشك المخصص**.

عند تمكين وضع الكشك، يمكنك أيضاً تكوين ما إذا كان يمكن للمستخدمين النهائيين الوصول إلى ميزات نظام معينة، مثل إعدادات النظام وشريط الحالة.

## مشغّل الكشك المخصص

ما إذا كان مشغّل الكشك المخصص ممكّناً. يستبدل هذا الشاشة الرئيسية بمشغّل يقفل الجهاز على التطبيقات المثبّتة عبر إعداد **إدارة التطبيقات**. تظهر التطبيقات في صفحة واحدة بترتيب أبجدي.

## إجراءات زر الطاقة

يضبط سلوك الجهاز في وضع الكشك عندما يضغط المستخدم مع الاستمرار (ضغطاً مطوّلاً) على زر الطاقة.

> **متاح (الافتراضي)**: تُعرض قائمة الطاقة (مثل إيقاف التشغيل، إعادة التشغيل) عندما يضغط المستخدم ضغطاً مطوّلاً على زر الطاقة لجهاز في وضع الكشك.
>
> **محظور**: لا تُعرض قائمة الطاقة (مثل إيقاف التشغيل، إعادة التشغيل) عندما يضغط المستخدم ضغطاً مطوّلاً على زر الطاقة لجهاز في وضع الكشك. ملاحظة: قد يمنع هذا المستخدمين من إيقاف تشغيل الجهاز.

## تحذيرات أخطاء النظام

يحدد ما إذا كانت مربعات حوار أخطاء النظام للتطبيقات المتعطلة أو غير المستجيبة محظورة في وضع الكشك. عند الحظر، سيوقف النظام التطبيق قسرًا كما لو اختار المستخدم خيار "إغلاق التطبيق" في واجهة المستخدم.

**محظور (الافتراضي)**: تُحظر جميع مربعات حوار أخطاء النظام، مثل التعطل وعدم استجابة التطبيق (ANR). عند الحظر، يوقف النظام التطبيق قسرًا كما لو أغلق المستخدم التطبيق من واجهة المستخدم.

**مفعّل**: تُعرض جميع مربعات حوار أخطاء النظام مثل التعطل وعدم استجابة التطبيق (ANR).

## تنقل النظام

يحدد ميزات التنقل المتاحة (مثل زرَي Home وOverview) في وضع الكشك.

**معطّل (الافتراضي)**: زرّا الصفحة الرئيسية وOverview غير متاحين.

**الصفحة الرئيسية فقط**: يُفعّل زر الصفحة الرئيسية فقط.

**مفعّل**: يُفعّل زر الصفحة الرئيسية وOverview.

## شريط الحالة

يحدد ما إذا كانت معلومات النظام والإشعارات معطّلة في وضع الكشك.

**معطّل (الافتراضي)**: معلومات النظام والإشعارات معطّلة في وضع الكشك.

**النظام فقط**: تُعرض معلومات النظام فقط على شريط الحالة.

**مفعّل**: تُعرض معلومات النظام والإشعارات على شريط الحالة في وضع الكشك. ملاحظة: لكي تسري هذه السياسة، يجب تمكين زر الصفحة الرئيسية للجهاز باستخدام kioskCustomization.systemNavigation.

## إعدادات الجهاز

يحدد ما إذا كان تطبيق الإعدادات مسموحًا في وضع الكشك.

**مسموح (الافتراضي)**: الوصول إلى تطبيق الإعدادات مسموح في وضع الكشك.

**محظور**: الوصول إلى تطبيق الإعدادات غير مسموح في وضع الكشك.

# الأمان

في هذا القسم، يمكنك تهيئة السياسات المتعلقة بالأمان.

## إجراءات المخاطر الأمنية

اختر ما يجب فعله عندما يُبلغ جهاز عن SecurityRisk في تقارير الحالة.

أنواع SecurityRisk المدعومة:

**نظام تشغيل غير معروف**: تكتشف واجهة Play Integrity API أن الجهاز يعمل بنظام تشغيل غير معروف (تنجح عملية فحص basicIntegrity لكن يفشل ctsProfileMatch).

**نظام تشغيل مخترق**: تكتشف واجهة Play Integrity API أن الجهاز يعمل بنظام تشغيل مخترق (يفشل فحص basicIntegrity).

**فشل التقييم المدعوم بالعتاد**: تكتشف واجهة Play Integrity API أن الجهاز ال يملك ضمانًا قويًا لسلامة النظام، إذا لم تظهر التسمية MEETS_STRONG_INTEGRITY في حقل سلامة الجهاز.

الإجراءات المتاحة:

**محو بيانات الشركة (افتراضي)**: إلغاء التسجيل ومحو بيانات العمل (الجهاز بأكمله إذا كان مُدارًا بالكامل، أو ملف تعريف العمل فقط إذا كان مملوكًا لملف تعريف).

**لا إجراء**: اترك الجهاز مسجّلًا ولا تفعل شيئًا تلقائيًا.

عند تحديد **محو بيانات الشركة**، يمكنك أيضًا تهيئة خيارات المحو:

**الحفاظ على حماية إعادة ضبط المصنع**: الحفاظ على بيانات حماية إعادة ضبط المصنع (FRP) عند محو الجهاز.

**محو التخزين الخارجي**: محو التخزين الخارجي للجهاز (مثل بطاقات SD) أيضًا عند تنفيذ المحو.

**محو شرائح eSIM**: بالنسبة إلى الأجهزة المملوكة للشركة، يزيل هذا جميع شرائح eSIM من الجهاز عند محو الجهاز. أما في الأجهزة المملوكة شخصيًا، فسيزيل شرائح eSIM المُدارة (شرائح eSIM التي تُضاف عبر الأمر ADD_ESIM) على الأجهزة، ولن تتم إزالة أي شرائح eSIM مملوكة شخصيًا.

# 1. الحد الأقصى لوقت القفل

الحد الأقصى للوقت (بالثواني) لنشاط المستخدم حتى يقفل الجهاز. تعني القيمة 0 عدم وجود قيود.

# 2. البقاء قيد التشغيل أثناء الشحن

أوضاع توصيل البطارية التي يبقى فيها الجهاز قيد التشغيل. عند استخدام هذا الإعداد، يُوصى بمسح **الحد الأقصى لوقت القفل** حتى لا يقفل الجهاز نفسه أثناء بقائه قيد التشغيل.

**شاحن AC**: مصدر الطاقة هو شاحن AC.

**منفذ USB**: مصدر الطاقة هو منفذ USB.

**شاحن لاسلكي**: مصدر الطاقة لاسلكي.

# 3. شاشة القفل معطّلة

إذا كانت القيمة صحيحة، يعطّل هذا شاشة القفل للشاشات الأساسية و/أو الثانوية. تُدعم هذه السياسة فقط في وضع إدارة الأجهزة المخصصة.

# 4. متطلبات كلمة المرور

سياسات متطلبات كلمة المرور.

استخدم **تهيئة متطلبات كلمة المرور** لإضافة كتلة أو أكثر من كتل متطلبات كلمة المرور. استخدم **مسح الكل** لإزالة جميع متطلبات كلمة المرور المكوّنة.

يمكن لمتطلبات كلمة المرور استخدام نطاق **تلقائي** (متطلب واحد) أو نطاقات منفصلة **الجهاز/ملف تعريف العمل**. يجب أن تقترن المتطلبات القائمة على التعقيد بمتطلبات قائمة على الجودة للنطاق نفسه.

## 4.1. النطاق

النطاق الذي ينطبق عليه متطلب كلمة المرور.

**تلقائي**: النطاق غير محدد. تُطبّق متطلبات كلمة المرور على ملف تعريف العمل في أجهزة ملف تعريف العمل، وعلى الجهاز بأكمله في الأجهزة المُدارة بالكامل أو المخصصة.

**الجهاز**: تُطبّق متطلبات كلمة المرور على الجهاز فقط.

**ملف تعريف العمل**: تُطبّق متطلبات كلمة المرور على ملف تعريف العمل فقط.

## 4.2. طول سجل كلمات المرور

طول سجل كلمات المرور. بعد تعيين هذا الحقل، لن يتمكن المستخدم من إدخال كلمة مرور جديدة مماثلة لأي كلمة مرور في السجل. تعني القيمة 0 عدم وجود قيود.

## 4.3. الحد الأقصى لكلمات المرور الفاشلة قبل المحو

عدد كلمات مرور فتح الجهاز غير الصحيحة التي يمكن إدخالها قبل محو الجهاز. تعني القيمة 0 عدم وجود قيود.

## 4.4. مهلة انتهاء صلاحية كلمة المرور (بالأيام)

يفرض هذا الإعداد على المستخدم تحديث كلمة المرور دورياً بعد عدد الأيام المحدد.

## 4.5. طلب فتح القفل بكلمة المرور

المدة الزمنية بعد فتح قفل جهاز أو ملف تعريف عمل باستخدام نموذج قوي للمصادقة (كلمة مرور، PIN، نمط) التي يمكن خلالها فتح القفل بأي طريقة مصادقة أخرى (مثل بصمة الإصبع، وكلاء الثقة، الوجه). بعد انقضاء المدة المحددة، لا يمكن استخدام سوى النماذج القوية للمصادقة لفتح قفل الجهاز أو ملف تعريف العمل.

**افتراضي الجهاز**: تُعيّن فترة المهلة على القيمة الافتراضية للجهاز.

**كل يوم**: تُعيّن فترة المهلة على 24 ساعة.

## 4.6. جودة كلمة المرور

جودة كلمة المرور المطلوبة.

**تعقيد عالٍ**: حدّد نطاق التعقيد العالي لكلمة المرور على النحو التالي: في Android 12 وما فوق: PIN بدون تسلسلات متكررة (4444) أو مرتبة (1234، 4321، 2468)، بطول 8 على الأقل؛ أبجدي، بطول 6 على الأقل؛ أبجدي رقمي، بطول 6 على الأقل.

**تعقيد متوسط**: حدّد نطاق التعقيد المتوسط لكلمة المرور على النحو التالي: PIN بدون تسلسلات متكررة (4444) أو مرتبة (1234، 4321، 2468)، بطول 4 على الأقل؛ أبجدي، بطول 4 على الأقل؛ أبجدي رقمي، بطول 4 على الأقل.

**تعقيد منخفض**: حدّد نطاق التعقيد المنخفض لكلمة المرور على النحو التالي: نمط؛ PIN بتسلسلات متكررة (4444) أو مرتبة (1234، 4321، 2468).

**بلا**: لا توجد متطلبات لكلمة المرور.

**ضعيف**: يجب تأمين الجهاز بتقنية تعرّف حيوي منخفضة الأمان على الأقل. يشمل ذلك التقنيات التي يمكنها التعرف على وجوه الفردا والتي تعادل تقريبًا PIN مكوّنًا من 3 أرقام (الاكتشاف الخاطئ أقل من 1 من 1000).

**أي**: كلمة المرور مطلوبة، ولكن لا توجد قيود على ما يجب أن تحتويه.

**رقمي**: يجب أن تحتوي كلمة المرور على أحرف رقمية.

**رقمي معقد**: يجب أن تحتوي كلمة المرور على أحرف رقمية بدون تسلسلات متكررة (4444) أو مرتبة (1234، 4321، 2468).

**أبجدي**: يجب أن تحتوي كلمة المرور على أحرف أبجدية (أو رموز).

**أبجدي رقمي**: يجب أن تحتوي كلمة المرور على أحرف رقمية وأبجدية (أو رموز) معًا.

**معقد**: يجب أن تستوفي كلمة المرور الحد الأدنى من المتطلبات المحددة في passwordMinimumLength وpasswordMinimumLetters وpasswordMinimumSymbols وغيرها. على سبيل المثال، إذا كانت passwordMinimumSymbols هي 2، فيجب أن تحتوي كلمة المرور على رمزين على الأقل.

## 4.7. الحد الأدنى للطول

الحد الأدنى المسموح به لطول كلمة المرور. تعني القيمة 0 عدم وجود قيود.

## 4.8. الحد الأدنى للأحرف

الحد الأدنى لعدد الأحرف المطلوبة في كلمة المرور.

## 4.9. الحد الأدنى للأحرف الصغيرة

الحد الأدنى لعدد الأحرف الصغيرة المطلوبة في كلمة المرور.

## 4.10. الحد الأدنى للأحرف الكبيرة

الحد الأدنى لعدد الأحرف الكبيرة المطلوبة في كلمة المرور.

## 4.11. الحد الأدنى للأحرف غير الأبجدية

الحد الأدنى لعدد الأحرف غير الأبجدية (الأرقام أو الرموز) المطلوبة في كلمة المرور.

## 4.12. الحد الأدنى للأرقام

الحد الأدنى لعدد الأرقام المطلوبة في كلمة المرور.

### 4.13. الحد الأدنى للرموز

الحد الأدنى لعدد الرموز المطلوبة في كلمة المرور.

### 4.14. قفل موحّد

يتحكم في السماح بقفل موحّد للجهاز وملف تعريف العمل، في الأجهزة التي تعمل بنظام Android 9 وما فوق وتحتوي على ملف تعريف عمل. لا يكون له أي تأثير على الأجهزة الأخرى.

**السماح بقفل موحّد**: يُسمح بقفل مشترك للجهاز وملف تعريف العمل.

**طلب قفل عمل منفصل**: يُطلب قفل منفصل لملف تعريف العمل.

## 5. إعادة ضبط المصنع معطّلة

ما إذا كانت إعادة الضبط إلى إعدادات المصنع من الإعدادات معطّلة. لا ينطبق إلا على الأجهزة المُدارة بالكامل.

## 6. حماية إعادة ضبط المصنع

عناوين البريد الإلكتروني لمسؤولي الجهاز من أجل حماية إعادة ضبط المصنع. عند تعرّض الجهاز لإعادة ضبط غير مصرّح بها إلى إعدادات المصنع، سيتطلب من أحد هؤلاء المسؤولين تسجيل الدخول باستخدام بريد حساب Google وكلمة المرور لفتح قفل الجهاز. إذا لم يتم تحديد أي مسؤول، فلن يوفّر الجهاز حماية إعادة ضبط المصنع. لا ينطبق إلا على الأجهزة المُدارة بالكامل.

**بريد المسؤول الإلكتروني**: استخدم **تمكين حماية إعادة ضبط المصنع** لبدء تهيئة المسؤولين. ثم استخدم **إضافة بريد مسؤول إلكتروني** لإضافة عناوين وإزالتها باستخدام إجراء الحذف.

## 7. ميزات شاشة القفل

ميزات Keyguard (شاشة القفل) التي يمكن تعطيلها.

### 7.1. تعطيل الكل

تعطيل جميع تخصيصات شاشة القفل الحالية والمستقبلية.

### 7.2. تعطيل الكاميرا

تعطيل الكاميرا على شاشات القفل الآمنة (مثل PIN).

## 7.3. تعطيل الإشعارات

تعطيل عرض جميع الإشعارات على شاشات القفل الآمنة.

## 7.4. تعطيل الإشعارات غير المحجوبة

تعطيل الإشعارات غير المحجوبة على شاشات القفل الآمنة.

## 7.5. تجاهل حالة وكيل الثقة

تجاهل حالة وكيل الثقة على شاشات القفل الآمنة.

## 7.6. تعطيل بصمة الإصبع

تعطيل مستشعر بصمة الإصبع على شاشات القفل الآمنة.

## 7.7. تعطيل إدخال النص في الإشعارات

تعطيل إدخال النص في الإشعارات على شاشات القفل الآمنة.

## 7.8. تعطيل مصادقة الوجه

تعطيل مصادقة الوجه على شاشات القفل الآمنة.

## 7.9. تعطيل مصادقة قزحية العين

تعطيل مصادقة قزحية العين على شاشات القفل الآمنة.

## 7.10. تعطيل جميع أشكال المصادقة الحيوية

تعطيل جميع أشكال المصادقة الحيوية على شاشات القفل الآمنة.

## 7.11. تعطيل جميع الاختصارات

تعطيل جميع الاختصارات على شاشة القفل الآمنة في Android 14 وما فوق.

# الوسائط المتعددة

في هذا القسم، يمكنك تكوين سلوك الكاميرا/الميكروفون والوصول إلى بيانات USB والطباعة والقيود المتعلقة بالعرض.

## 1. الوصول إلى الكاميرا

يتحكم في استخدام الكاميرا وما إذا كان يمكن للمستخدم الوصول إلى مفتاح الوصول إلى الكاميرا (Android 12+). بشكل عام، يُنطبق تعطيل الكاميرا على مستوى الجهاز بالكامل في الأجهزة المُدارة بالكامل، ودخل ملف تعريف العمل فقط في أجهزة ملف تعريف العمل.

**اختيار المستخدم (الافتراضي)**: سلوك الجهاز الافتراضي. الكاميرات متاحة و(Android 12+) يمكن للمستخدم تبديل الوصول إلى الكاميرا.

**معطّل**: جميع الكاميرات معطّلة (الإدارة الكاملة: على مستوى الجهاز؛ ملف تعريف العمل: لتطبيقات ملف تعريف العمل فقط). لا يكون لمفتاح الوصول إلى الكاميرا أي تأثير في النطاق المُدار.

**مفروض**: الكاميرات متاحة. على الأجهزة المُدارة بالكامل التي تعمل بنظام Android 12+، لا يمكن للمستخدم تبديل الوصول إلى الكاميرا. على الأجهزة/الإصدارات الأخرى، يتصرف هذا مثل اختيار المستخدم.

## 2. الوصول إلى الميكروفون

على الأجهزة المُدارة بالكامل، يتحكم في استخدام الميكروفون وما إذا كان يمكن للمستخدم الوصول إلى مفتاح الوصول إلى الميكروفون (Android 12+). ليس لهذا الإعداد أي تأثير على الأجهزة غير المُدارة بالكامل.

**اختيار المستخدم (الافتراضي)**: السلوك الافتراضي. الميكروفون متاح و(Android 12+) يمكن للمستخدم تبديل الوصول إلى الميكروفون.

**معطّل**: الميكروفون معطّل (على مستوى الجهاز). لا يكون لمفتاح الوصول إلى الميكروفون أي تأثير.

**مفروض**: الميكروفون متاح. على Android 12+، لا يمكن للمستخدم تبديل الوصول إلى الميكروفون. على Android 11 وأقدم، يتصرف هذا مثل اختيار المستخدم.

# 3. الوصول إلى بيانات USB

يتحكم في الملفات و/أو البيانات التي يمكن نقلها عبر USB. مدعوم فقط على الأجهزة المملوكة للشركة.

**عدم السماح بنقل الملفات (الافتراضي)**: نقل الملفات غير مسموح، لكن اتصالات بيانات USB الأخرى (مثل الفأرة/لوحة المفاتيح) مسموحة.

**عدم السماح بنقل البيانات**: جميع أنواع نقل بيانات USB محظورة (Android 12+ مع USB HAL 1.3+). إذا لم يكن مدعومًا، يعود الجهاز إلى خيار عدم السماح بنقل الملفات.

**السماح بنقل البيانات**: جميع أنواع نقل بيانات USB مسموحة.

# 4. الطباعة

يتحكم في ما إذا كانت الطباعة مسموحة (Android 9+).

**مسموح (الافتراضي)**: الطباعة مسموحة.

**غير مسموح**: الطباعة غير مسموحة (Android 9+).

# 5. إعدادات سطوع الشاشة

يتحكم في وضع سطوع الشاشة و(اختياريًا) قيمة السطوع.

وضع سطوع الشاشة:

**اختيار المستخدم (الافتراضي)**: يُسمح للمستخدم بتكوين سطوع الشاشة.

**تلقائي**: السطوع تلقائي ولا يمكن للمستخدم تغييره. لا يزال بإمكانك تعيين قيمة سطوع تُستخدم كجزء من الضبط التلقائي (الأجهزة المُدارة بالكامل على Android 9+؛ ملفات تعريف العمل على Android 15+ المملوكة للشركة).

**ثابت**: يُضبط السطوع على القيمة المكوّنة ولا يمكن للمستخدم تغييره. قيمة السطوع مطلوبة (الأجهزة المُدارة بالكامل على Android 9+؛ ملفات تعريف العمل على Android 15+ المملوكة للشركة).

سطوع الشاشة:

قيمة من 1 إلى 255 (1 = الأدنى، 255 = الأعلى). تعني القيمة 0 عدم تعيين قيمة سطوع.

## 6. إعدادات مهلة الشاشة

يتحكم في ما إذا كان يمكن للمستخدم تكوين مهلة الشاشة، وعند الفرض، قيمة المهلة.

يحدد حقل **وضع مهلة الشاشة** بين السلوك الذي يتحكم فيه المستخدم والسلوك المفروض.

> **اختيار المستخدم (الافتراضي)**: يُسمح للمستخدم بتكوين مهلة الشاشة.
>
> **مفروض**: تُضبط مهلة الشاشة على القيمة المكوّنة ولا يمكن للمستخدم تغييرها (الأجهزة المُدارة بالكامل على Android 9+؛ ملفات تعريف العمل على Android 15+ المملوكة للشركة).

مهلة الشاشة:

> مدة المهلة بالثواني. يجب أن تكون القيمة أكبر من 0. إذا كانت أكبر من **الحد الأقصى لوقت القفل**، فقد يقيّدها النظام ويبلّغ عن عدم الامتثال.

## 7. التقاط الشاشة معطّل

ما إذا كان التقاط الشاشة معطّلًا.

## 8. ضبط مستوى الصوت معطّل

ما إذا كان ضبط مستوى الصوت الرئيسي معطّلًا.

## 9. تركيب الوسائط الفعلية معطّل

ما إذا كان تركيب الوسائط الخارجية الفعلية معطّلًا.

# الشبكة الخلوية

في هذا القسم، يمكنك تهيئة السياسات المتعلقة بالشبكة الخلوية.

## 1. وضع الطيران

يتحكم في ما إذا كان يمكن للمستخدم تبديل وضع الطيران أم لا.

> **اختيار المستخدم (الافتراضي)**: يُسمح للمستخدم بتشغيل وضع الطيران أو إيقافه.
>
> **معطّل**: وضع الطيران معطّل. لا يُسمح للمستخدم بتشغيل وضع الطيران. مدعوم على Android 9 وأحدث.

## 2. الشبكة الخلوية 2G

يتحكم في ما إذا كان يمكن للمستخدم تبديل إعداد الشبكة الخلوية 2G أم لا.

> **اختيار المستخدم (الافتراضي)**: يُسمح للمستخدم بتشغيل الشبكة الخلوية 2G أو إيقافها.
>
> **معطّل**: الشبكة الخلوية 2G معطّلة. لا يُسمح للمستخدم بتشغيل الشبكة الخلوية 2G عبر الإعدادات. مدعوم على Android 14 وأحدث.

## 3. تجاوز APNs

يتحكم في تفعيل APNs المتجاوزة أو تعطيلها. عند التفعيل، لا تُستخدم إلا APNs المتجاوزة المهيأة وتُتجاهل جميع APNs الأخرى على الجهاز.

> **معطّل (الافتراضي)**: تُحفظ جميع إعدادات APN التي تم تكوينها على الجهاز، لكنها معطّلة وليس لها أي تأثير. تظل جميع نقاط APN الأخرى على الجهاز قيد الاستخدام.
>
> **مفعّل**: تُستخدم نقاط APN للتجاوز فقط، ويتم تجاهل جميع نقاط APN الأخرى. لا يمكن تكوين هذا الإعداد إلا على الأجهزة المُدارة بالكامل التي تعمل بنظام Android 10 فما فوق.

## 4. إعدادات APN

كوّن إدخال APN واحدًا أو أكثر. استخدم **إضافة APN** لإنشاء إدخال و**إزالة APN** لحذفه.

يتضمّن كل APN حقولًا مطلوبة:

**أنواع APN**: حدّد نوعًا واحدًا أو أكثر من أنواع حركة البيانات لهذا APN (يتوقف التوفر على وضع الإدارة وإصدار Android).

**اسم APN**: معرّف APN الذي يقدّمه مشغّل الشبكة لديك.

**الاسم المعروض**: اسم ودّي يظهر في واجهة المستخدم.

حقول APN الاختيارية:

**نوع المصادقة، اسم المستخدم، كلمة المرور**: كوّن مصادقة مشغّل الشبكة (إذا لزم الأمر).

**البروتوكول** و**بروتوكول التجوال**: تكوين بروتوكول IP.

**أنواع الشبكات**: قيّد تقنيات الشبكة الخلوية التي يجوز لـ APN استخدامها (على سبيل المثال LTE/5G NR).

**عنوان الوكيل** و**منفذ الوكيل**: وكيل HTTP لحركة البيانات (إن وُجد).

**عنوان وكيل MMS، منفذ وكيل MMS، MMSC (معرّف URI لمركز MMS)**: إعدادات مرتبطة بـ MMS.

**معرّف المشغّل الرقمي (MCC+MNC)** و**معرّف مشغّل الشبكة**: حقول تعريف مشغّل الشبكة.

**إعداد التشغيل الدائم**: ما إذا كان يجب أن تكون جلسة PDU التي ينشّطها هذا APN قيد التشغيل دائمًا. مدعوم على Android 15 فما فوق.

**نوع MVNO**: نوع معرّف مشغّل الشبكة الافتراضية للهاتف المحمول.

**MTU IPv4** و**MTU IPv6**: وحدة الإرسال القصوى لمسارات IPv4/IPv6. مدعومة على Android 13 فما فوق.

## 5. تكوين بث الخلية معطّل

ما إذا كان تكوين بث الخلية معطّلًا.

## 6. تكوين شبكات الهاتف المحمول معطّل

ما إذا كان تكوين شبكات الهاتف المحمول معطّلاً.

## 7. بيانات التجوال معطّلة

ما إذا كانت خدمات بيانات التجوال معطّلة.

## 8. المكالمات الصادرة معطّلة

ما إذا كانت المكالمات الصادرة معطّلة.

## 9. رسائل SMS معطّلة

ما إذا كان إرسال رسائل SMS واستقبالها معطّلاً.

## 10. تكوين تقسيم شبكة 5G

كوّن إعدادات خدمة الشبكة التفضيلية لتمكين تقسيم شبكة 5G للمؤسسات. يمكنك إعداد ما يصل إلى 5 شرائح للمؤسسات وتعيين التطبيقات لشبكات محددة لتحسين توجيه حركة البيانات.

### 10.1. الشبكة التفضيلية الافتراضية

عرّف الشبكة التفضيلية الافتراضية للتطبيقات غير المدرجة في قائمة التطبيقات، وأ إذا لم يتم تعيين **الشبكة التفضيلية** لأحد التطبيقات. يجب أن يوجد تكوين لمعرّف الشبكة المحدد (ما لم يتم الضبط على **لا توجد شبكة تفضيلية**).

ملاحظة: تُستثنى التطبيقات المهمة مثل **com.google.android.apps.work.clouddpc** و **com.google.android.gms** من هذا الإعداد الافتراضي.

### 10.2. تكوينات خدمة الشبكة

استخدم **إضافة تكوين شبكة** لإنشاء تكوين شريحة. يمكنك إضافة ما يصل إلى 5 تكوينات. يتضمّن كل تكوين:

**معرّف الشبكة التفضيلية (يُعيّن تلقائياً)**: يُعيّن معرّف الشبكة تلقائياً والا يمكن تغييره.

**الرجوع إلى الاتصال الافتراضي**: ما إذا كان الرجوع إلى الشبكة الافتراضية على مستوى الجهاز مسموحاً. إذا لم يكن مسموحاً، فلا يمكن للتطبيقات الوصول إلى الإنترنت إذا كانت شريحة 5G غير متاحة.

**الشبكات غير المطابقة**: ما إذا كان يمكن للتطبيقات الخاضعة لهذا التكوين استخدام شبكات غير الخدمة التفضيلية. إذا تم الضبط على **غير مسموح**، فيجب أن يكون **الرجوع إلى الاتصال الافتراضي** أيضاً **غير مسموح**. يتطلب Android 14 فما فوق.

# الشبكات

في هذا القسم، يمكنك تكوين السياسات المتعلقة بالشبكات.

> يمكن توفير تكوينات Wi-Fi وإدارتها بواسطة النظام عبر **تكوينات WiFi**. وفقاً للقيمة المعيّنة في **تكوين Wi-Fi**، قد يمتلك المستخدمون تحكماً محدوداً أو لا تحكم في إضافة الشبكات/تعديلها.

# حالة راديو الجهاز

## 1. حالة Wi-Fi

يتحكم في الحالة الحالية لـ Wi-Fi وما إذا كان يمكن للمستخدم تغيير حالتها.

**اختيار المستخدم (الافتراضي)**: يُسمح للمستخدم بتمكين/تعطيل Wi-Fi.

**مفعّل**: Wi-Fi قيد التشغيل ولا يُسمح للمستخدم بإيقافها (Android 13+).

**معطّل**: Wi-Fi متوقفة ولا يُسمح للمستخدم بتشغيلها (Android 13+).

## 2. الحد الأدنى لمستوى أمان Wi-Fi

الحد الأدنى المطلوب لمستوى أمان شبكات Wi-Fi التي يمكن للجهاز الاتصال بها. مدعوم على Android 13 فما فوق، للأجهزة المُدارة بالكامل وملفات تعريف العمل على الأجهزة المملوكة للشركة.

**شبكة مفتوحة (الافتراضي)**: يمكن للجهاز الاتصال بجميع أنواع شبكات Wi-Fi.

**شبكة شخصية**: تمنع شبكات Wi-Fi المفتوحة؛ تتطلب أماناً شخصياً على الأقل (على سبيل المثال WPA2-PSK).

**شبكة مؤسسة**: تتطلب شبكات EAP للمؤسسات؛ تمنع شبكات Wi-Fi الأقل من مستوى الأمان هذا.

**شبكة مؤسسة 192-بت**: تتطلب شبكات مؤسسة 192-بت؛ الخيار الأكثر صرامة.

## 3. حالة النطاق العريض الفائق (UWB)

يتحكم في حالة إعداد النطاق العريض الفائق وما إذا كان يمكن للمستخدم تبديله تشغيلاً وإيقافاً.

**اختيار المستخدم (الافتراضي)**: يُسمح للمستخدم بتبديل UWB تشغيلاً وإيقافاً.

**معطّل**: UWB معطّل ولا يُسمح للمستخدم بتبديله عبر الإعدادات (Android 14+).

# إدارة اتصال الجهاز

## 4. مشاركة Bluetooth

يتحكم في ما إذا كانت مشاركة Bluetooth مسموحة.

**مسموح**: مشاركة Bluetooth مسموحة (الافتراضي على الأجهزة المُدارة بالكامل، Android 8+).

**غير مسموح**: مشاركة Bluetooth غير مسموحة (الافتراضي على ملفات تعريف العمل، Android 8+).

## 5. تكوين Wi-Fi

يتحكم في صلاحيات تكوين Wi-Fi. وفقاً للخيار المحدد، يمتلك المستخدم تحكماً كاملاً أو محدوداً أو لا تحكم في تكوين شبكات Wi-Fi.

**السماح بتكوين Wi-Fi (الافتراضي)**: يُسمح للمستخدم بتكوين Wi-Fi.

**عدم السماح بإضافة تكوين Wi-Fi**: إضافة تكوينات Wi-Fi جديدة غير مسموحة. يمكن للمستخدم التبديل بين الشبكات المكوّنة بالفعل (Android 13+؛ الأجهزة المُدارة بالكامل وملفات تعريف العمل المملوكة للشركة).

**عدم السماح بتكوين Wi-Fi**: يمنع تكوين شبكات Wi-Fi. بالنسبة للأجهزة المُدارة بالكامل، يزيل هذا الشبكات التي كوّنها المستخدم ويحتفظ فقط بالشبكات المكوّنة عبر **تكوينات WiFi**. بالنسبة لملفات تعريف العمل المملوكة للشركة، لا تتأثر الشبكات الحالية لكن لا يمكن للمستخدمين إضافة شبكات Wi-Fi أو إزالتها أو تعديلها.

عند تعطيل تكوين Wi-Fi والسماح للجهاز بالاتصال وقت بدء التشغيل، يمكن للنظام عرض **مخرج الشبكة البديل** لتمكين المستخدم من الاتصال مؤقتاً وتحديث السياسة.

## 6. إعدادات Wi-Fi Direct

يتحكم في تكوين إعدادات Wi-Fi Direct واستخدامها. مدعوم على الأجهزة المملوكة للشركة التي تعمل بنظام Android 13 فما فوق.

**السماح (الافتراضي)**: يُسمح للمستخدم باستخدام Wi-Fi Direct.

**عدم السماح**: لا يُسمح للمستخدم باستخدام Wi-Fi Direct.

## 7. إعدادات المشاركة عبر نقطة الاتصال

يتحكم في إعدادات المشاركة عبر نقطة الاتصال. بناءً على القيمة المعيّنة، يُمنع المستخدم جزئياً أو كلياً من استخدام أشكال مختلفة من المشاركة عبر نقطة الاتصال.

**السماح بجميع أشكال المشاركة عبر نقطة الاتصال (الافتراضي)**: يسمح بتكوين واستخدام جميع أشكال المشاركة عبر نقطة الاتصال.

**عدم السماح بالمشاركة عبر نقطة اتصال Wi-Fi**: يمنع المستخدم من استخدام المشاركة عبر نقطة اتصال Wi-Fi (الأجهزة المملوكة للشركة على Android 13+).

**عدم السماح بجميع أشكال المشاركة عبر نقطة الاتصال**: يمنع جميع أشكال المشاركة عبر نقطة الاتصال (الأجهزة المُدارة بالكامل + ملفات تعريف العمل المملوكة للشركة).

## 8. سياسة SSID لـ Wi-Fi

قيود على معرّفات SSID لـ Wi-Fi التي يمكن للجهاز الاتصال بها (لا يؤثر هذا في الشبكات التي يمكن تكوينها على الجهاز). مدعوم على الأجهزة المملوكة للشركة التي تعمل بنظام Android 13 فما فوق.

**قائمة حظر SSID (الافتراضي)**: لا يمكن للجهاز الاتصال بأي شبكة Wi-Fi مدرج معرّف SSID الخاص بها، لكن يمكنه الاتصال بشبكات أخرى.

**قائمة سماح SSID**: يمكن للجهاز الاتصال بمعرّفات SSID المدرجة فقط. يجب ألا تكون قائمة SSID فارغة.

استخدم **إضافة SSID** لإضافة إدخالات. وفقًا لنوع السياسة المحدد، تُفسّر القائمة على أنها معرّفات SSID مسموحة أو محظورة.

في واجهة محرر السياسات، تُسمّى قائمة SSID **معرّفات SSID المسموحة لـ Wi-Fi** لقوائم السماح و**معرّفات SSID المحظورة لـ Wi-Fi** لقوائم الحظر.

## 9. إعدادات تجوال Wi-Fi

كوّن وضع تجوال Wi-Fi لكل SSID. استخدم **إضافة إعداد تجوال Wi-Fi** لإنشاء إدخالات.

يتضمن كل إدخال:

> **SSID**: معرّف SSID الذي ينطبق عليه إعداد التجوال (مطلوب).
>
> **وضع تجوال Wi-Fi**: الافتراضي / معطّل / عدواني. يتطلب المعطّل والعدواني Android 15+ وهما مدعومان فقط على الأجهزة المُدارة بالكامل وملفات تعريف العمل على الأجهزة المملوكة للشركة.

# قيود الشبكة

## 10. Bluetooth معطّل

ما إذا كان Bluetooth معطّلًا. فضّل هذا الإعداد على خيار تكوين Bluetooth معطّل لأن المستخدم يمكنه تجاوز خيار تكوين Bluetooth معطّل.

## 11. مشاركة جهات الاتصال عبر Bluetooth معطّلة

ما إذا كانت مشاركة جهات الاتصال عبر Bluetooth معطّلة.

## 12. تكوين Bluetooth معطّل

ما إذا كان تكوين Bluetooth معطّلًا.

## 13. إعادة تعيين الشبكة معطّلة

ما إذا كانت إعادة تعيين إعدادات الشبكة معطّلة.

## 14. البث الصادر معطّل

ما إذا كان استخدام NFC لبث البيانات من التطبيقات معطّلاً.

# VPN

## 15. تطبيق Always On VPN

حدد اسم حزمة Always On VPN لضمان أن بيانات التطبيقات المُدارة المحددة ستمر دائماً عبر VPN مكوّن.

> ملاحظة: تتطلب هذه الميزة نشر عميل VPN يدعم ميزتي Always On وVPN لكل تطبيق.

## 16. قفل VPN

يمنع الشبكات عندما لا يكون VPN متصلاً.

## 17. تكوين VPN معطّل

ما إذا كان تكوين VPN معطّلاً.

# الوكيل وخدمات الشبكة

## 18. خدمة الشبكة التفضيلية

يتحكم في ما إذا كانت خدمة الشبكة التفضيلية ممكّنة على ملف تعريف العمل. على سبيل المثال، قد تكون لدى المؤسسة اتفاقية مع مشغّل شبكة تُرسَل بموجبها بيانات العمل عبر خدمة شبكة مخصّصة لاستخدام المؤسسات (على سبيل المثال، شريحة مؤسسة على شبكات

5G). ليس لهذا أي تأثير على الأجهزة المُدارة بالكامل.

**معطّل**: خدمة الشبكة التفضيلية معطّلة على ملف تعريف العمل.

**مفعّل**: خدمة الشبكة التفضيلية ممكّنة على ملف تعريف العمل.

> إذا كنت تستخدم تقسيم شبكة المؤسسات، فكوّن أيضاً **تكوين تقسيم شبكة 5G** ضمن لوحة سياسة **الشبكة الخلوية** وعيّن التطبيقات إلى شريحة باستخدام إعداد **الشبكة التفضيلية** الخاص بها.

# 19. الوكيل العام الموصى به

وكيل HTTP العام المستقل عن الشبكة. عادةً، ينبغي تكوين الوكلاء لكل شبكة في تكوينات WiFi. قد يكون الوكيل العام مفيداً للتكوينات غير المعتادة مثل التصفية الداخلية العامة. الوكيل العام مجرد توصية وقد تتجاهله بعض التطبيقات.

**معطّل**

**الوكيل المباشر**

**التهيئة التلقائية للوكيل (PAC)**

## 19.1. المضيف

مضيف الوكيل المباشر.

## 19.2. المنفذ

منفذ الوكيل المباشر.

## 19.3. عنوان URI لـ PAC

عنوان URI لنص PAC المستخدم لتهيئة الوكيل.

## 19.4. المضيفون المستثنون

في الوكيل المباشر، المضيفون الذين يتم تجاوز الوكيل لهم. قد تحتوي أسماء المضيفين على أحرف بدل مثل ***.example.com**.

استخدم **إضافة مضيف مستثنى** لإضافة إدخالات (متاح للوكيل المباشر فقط).

# تهيئات Wi-Fi

حدّد تهيئات شبكات Wi-Fi التي سيطبّقها النظام على الأجهزة. استخدم **إضافة تهيئة Wi-Fi** لإنشاء إدخال، وأزله باستخدام إجراء الحذف.

## 20. حقول تهيئة Wi-Fi

تتضمن كل تهيئة:

**اسم التهيئة**: مطلوب.

**SSID**: مطلوب.

**الاتصال التلقائي**: ما إذا كان يجب الاتصال بالشبكة تلقائيًا عند توفرها.

**الانتقال السريع**: ما إذا كان يجب على العميل محاولة استخدام الانتقال السريع (IEEE 802.11r-2008) مع الشبكة.

**SSID مخفي**: ما إذا كان سيتم بث SSID.

**وضع عشوائية MAC**: الأجهزة أو تلقائي (Android 13+).

### 20.1. الأمان

خيارات أمان Wi-Fi:

**WEP-PSK**: WEP (مفتاح مشترك مسبقًا).

**WPA-PSK**: WPA/WPA2/WPA3-Personal (مفتاح مشترك مسبقًا).

**WPA-EAP**: WPA/WPA2/WPA3-Enterprise (بروتوكول المصادقة القابل للتوسيع).

**وضع WPA3 192 بت**: شبكة WPA-EAP تسمح بوضع WPA3 192 بت فقط.

### 20.2. عبارة المرور (المفتاح المشترك مسبقًا)

يظهر عندما يكون الأمان **WEP-PSK** أو **WPA-PSK**. عبارة المرور مطلوبة.

### 20.3. طريقة EAP (المؤسسة)

يظهر عندما يكون الأمان **WPA-EAP** أو **وضع WPA3 192 بت**. اختر طريقة EAP خارجية واحدة:

**EAP-TLS**

**EAP-TTLS**

**PEAP**

**EAP-SIM**

**EAP-AKA**

## 20.4. مصادقة المرحلة 2

يظهر لطرق النفق الخارجية (**EAP-TTLS** و**PEAP**).

**MSCHAPv2**

**PAP**

## 20.5. بيانات اعتماد EAP من المستخدمين

عند التمكين، يطبّق النظام بيانات اعتماد EAP على الأجهزة تلقائيًا لكل مستخدم. يمكنك تهيئة بيانات اعتماد المستخدمين في قسم **المستخدمون**.

## 20.6. شهادة العميل

بالنسبة إلى **EAP-TLS**، يمكنك تعيين شهادة عميل تُستخدم لمصادقة Wi-Fi. لمزيد من المعلومات، راجع صفحة **إدارة الشهادات**.

إذا كانت هناك شهادة معيّنة بالفعل، يمكنك استخدام **فتح الشهادة** لعرضها أو **تغيير الشهادة** لتحديد شهادة أخرى.

بدلًا من ذلك، يمكنك تحديد **الاسم المستعار لزوج مفاتيح شهادة العميل**، والذي يشير إلى شهادة عميل مخزّنة في سلسلة مفاتيح Android ومسموح بها لمصادقة Wi-Fi.

> إذا تم تعيين كل من **شهادة العميل** و**الاسم المستعار لزوج مفاتيح شهادة العميل**، يتم تجاهل الاسم المستعار لزوج المفاتيح.

## 20.7. الهوية

هوية المستخدم. بالنسبة إلى البروتوكولات الخارجية النفقية (PEAP، EAP-TTLS)، تُستخدم هذه للمصادقة داخل النفق، وتُستخدم **الهوية المجهولة** لهوية EAP خارج النفق. أما بالنسبة إلى البروتوكولات الخارجية غير النفقية، فتُستخدم هذه لهوية EAP.

## 20.8. الهوية المجهولة

للبروتوكولات النفقية فقط، يشير هذا إلى هوية المستخدم المعروضة على البروتوكول الخارجي.

## 20.9. كلمة المرور

كلمة مرور المستخدم. إذا لم تُحدّد، يكون الافتراضي هو مطالبة المستخدم.

## 20.10. شهادات CA للخادم

قائمة شهادات CA المستخدمة للتحقق من سلسلة شهادات المضيف. يجب أن تتطابق شهادة CA واحدة على الأقل. لمزيد من المعلومات، راجع صفحة **إدارة الشهادات**.

استخدم **إضافة شهادة CA للخادم** لإضافة إدخالات، وأزلها باستخدام إجراء الحذف.

## 20.11. مطابقات لاحقة النطاق

قائمة بقيود اسم نطاق الخادم. تُستخدم الإدخالات كمطالبات مطابقة اللاحقة مقابل اسم (أسماء) DNS للاسم الموضوعي البديل لشهادة خادم المصادقة.

# 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).

# الموقع والنطاقات الجغرافية

تجمع هذه اللوحة إعدادات سياسة Android التي تتحكم في الإبلاغ عن موقع الجهاز وفرض الموقع وتعريفات السياج الجغرافي. استخدمها عندما تريد أن تجمع Cerberus Enterprise مواقع الأجهزة أو تكتشف دخول الأجهزة إلى المناطق المكوّنة أو مغادرتها.

# الإبلاغ عن الموقع

## الإبلاغ عن الموقع

يمكّن الإبلاغ عن الموقع الجغرافي للجهاز. تُستخدم بيانات الموقع التي تُجمع عبر هذا الإعداد في **خريطة الموقع في لوحة التحكم**، وسجل مواقع نظرة عامة الجهاز، ومعالجة السياج الجغرافي.

> يُحفظ سجل المواقع وأحداث الأسيجة الجغرافية لمدة **90 يومًا** وتُحذف البيانات الأقدم تلقائيًا كل ليلة. ويُحفظ دائمًا آخر موقع لكل جهاز مسجّل، لذا يظل الجهاز على الخرائط.

> على الأجهزة غير المُدارة بالكامل، قد تظل بيانات الموقع تعتمد على امتلاك تطبيق Cerberus Enterprise لأذونات الموقع المطلوبة وعلى تفعيل خدمات الموقع على الجهاز.

> على أجهزة Apple الشخصية (تسجيل المستخدم)، يكون الموقع والسياج الجغرافي معطّلين افتراضيًا: لا يتوفران إلا عندما تكون سياسة Apple **الموقع والسياج الجغرافي على الأجهزة الشخصية** مفعّلة، وفقط إذا سمح المستخدم بالموقع لتطبيق Cerberus Enterprise.

# وضع الموقع

يتحكم في إعداد الموقع على الأجهزة المملوكة للشركة.

- **اختيار المستخدم**: لا تُقيّد خدمات الموقع بواسطة السياسة.

- **مفروض**: خدمات الموقع ممكّنة على الجهاز.
- **معطّل**: خدمات الموقع معطّلة على الجهاز.

# مشاركة الموقع معطّلة

يعطّل مشاركة الموقع لتطبيقات العمل. على الأجهزة التي يملكها مالك ملف التعريف، يؤثر هذا في ملف تعريف العمل. على الأجهزة المُدارة بالكامل، يعطّل الموقع للجهاز بأكمله ويتجاوز وضع موقع الجهاز.

# السلوك التلقائي مع الأسيجة الجغرافية النشطة

تتطلب الأسيجة الجغرافية النشطة عمل الإبلاغ عن الموقع. عندما يكون سياج جغرافي واحد على الأقل نشطاً، تحافظ Cerberus Enterprise تلقائياً على اتساق إعدادات الموقع ذات الصلة.

- يُفرض تشغيل **الإبلاغ عن الموقع** ما دامت هناك أسيجة جغرافية نشطة.
- يُفرض ضبط **وضع الموقع** على **مفروض**.
- يُفرض إيقاف **مشاركة الموقع معطّلة**.

إذا حاولت تعطيل **الإبلاغ عن الموقع** أثناء وجود سياج جغرافي واحد أو أكثر نشطاً، تعرض Cerberus Enterprise مربع حوار تأكيد. إذا تابعت، يتم تعطيل جميع الأسيجة الجغرافية النشطة في السياسة.

# قائمة الأسيجة الجغرافية

يمكن أن تحتوي السياسة على ما يصل إلى **10 أسيجة جغرافية**. يجب أن تكون أسماء الأسيجة الجغرافية فريدة داخل السياسة.

استخدم **إضافة سياج جغرافي** لإنشاء إدخال جديد. يتضمّن كل سياج جغرافي هذه الحقول الرئيسية:

- **الاسم**: مطلوب وفريد.
- **خط العرض** و**خط الطول**: مركز المنطقة.
- **نصف القطر (م)**: مطلوب، من **200** إلى **10000** متر.
- **الوصف**: ملاحظات اختيارية للمسؤولين.
- **الإبلاغ عن الدخول** و**الإبلاغ عن الخروج**: اختر أحداث الانتقال التي يجب إنشاؤها.
- **نشط**: يمكّن السياج الجغرافي أو يعطّله دون حذفه.

> يجب أن يبقى أحد الخياريين على الأقل **الإبلاغ عن الدخول** أو **الإبلاغ عن الخروج** ممكّنًا لكل سياج جغرافي.

> كان الحد الأدنى لنصف القطر 100 متر سابقًا. تستمر الأسيجة الجغرافية الحالية الأصغر من 200 متر في العمل وتُحفظ كما هي عند حفظ السياسة، حتى إذا نقلتها أو أعدت تسميتها. إذا غيّرت نصف قطرها، فيجب أن يكون 200 متر على الأقل.

# أدوات تحرير الخريطة

تتضمّن كل بطاقة سياج جغرافي معاينة للخريطة للمنطقة. يمكنك تحرير الشكل الهندسي من الخريطة أو من الحقول الرقمية.

- انقر على الخريطة لنقل مركز السياج الجغرافي عند إلغاء قفل تحرير المنطقة.
- استخدم زر **الموقع الحالي** لتوسيط الخريطة على موقع المتصفح الحالي.
- استخدم زر **إعادة توسيط الخريطة** لاستعادة منفذ العرض المفضل لذلك السياج الجغرافي.
- استخدم زر القفل لمنع التغييرات العرضية في الشكل الهندسي للسياج الجغرافي.

# أين تظهر بيانات السياج الجغرافي

يمكن مراجعة انتقالات السياج الجغرافي في صفحة Android [نظرة عامة الجهاز](#)، داخل علامة التبويب **السياج الجغرافي** في لوحة الموقع. تعرض علامة التبويب تلك الانتقالات على خريطة مخصصة إلى جانب أدوات التصفية وقائمة الانتقالات.

# إدارة المستخدمين

## تعطيل إضافة مستخدم

هل إضافة مستخدمين وملفات تعريف جديدة معطّلة. بالنسبة للأجهزة التي يكون فيها managementMode هو **DEVICE_OWNER** يتم تجاهل هذا الحقل ولا يُسمح للمستخدم أبدًا بإضافة أو إزالة مستخدمين.

## تعطيل تعديل الحسابات

هل إضافة الحسابات أو إزالتها معطّلة.

## تعطيل تكوين بيانات اعتماد المستخدم

هل تكوين بيانات اعتماد المستخدم معطّل.

## تعطيل إزالة مستخدم

هل إزالة المستخدمين الآخرين معطّلة.

## تعطيل تعيين رمز المستخدم

هل تغيير رمز المستخدم معطّل.

## تعطيل تعيين خلفية الشاشة

هل تغيير خلفية الشاشة معطّل.

## مصادقة إعداد حساب العمل

يتحكم في كيفية مصادقة المستخدمين أثناء إعداد حساب العمل. هذا الخيار متاح فقط لمؤسسات Android المدعومة بنطاق Google مُدار (Google Workspace).

أثناء إعداد الجهاز/التسجيل، تؤثر هذه السياسة في ما إذا كان تسجيل الدخول إلى حساب العمل مطلوبًا، لكن إعداد **المصادقة باستخدام Google** في Google Admin Console ونوع رمز التسجيل قد يتطلبان المصادقة رغم ذلك.

بالنسبة للأجهزة المسجّلة مسبقًا، تنطبق هذه السياسة فقط إذا كان الجهاز مُدارًا بواسطة حساب Google Play مُدار (أي مسجّلًا بدون **المصادقة باستخدام Google Enrollment**).

لمزيد من التفاصيل واستكشاف الأخطاء وإصلاحها، راجع **المصادقة باستخدام Google Enrollment**.

## أنواع الحسابات المحظورة

أنواع الحسابات التي لا يمكن للمستخدم إدارتها. يمنع هذا الخيار مستخدمي الجهاز من إضافة حسابات غير معتمدة.

استخدم **إضافة نوع حساب محظور** لإضافة نوع حساب واحد أو أكثر.

يحتوي كل إدخال على حقل **نوع الحساب** (مطلوب). أدخل سلسلة مثل **com.google**. أزل إدخالًا باستخدام إجراء الحذف.

# الاستخدام الشخصي

عند تجهيز جهاز مملوك للشركة للعمل والاستخدام الشخصي، يمكنك تحديد بعض القواعد للحد من كيفية تشغيل المستخدم للجهاز للاستخدام الشخصي خارج ملف تعريف العمل.

> لا ينطبق هذا القسم إلا على الأجهزة المملوكة للشركة التي تحتوي على ملف تعريف عمل. لن يكون لها أي تأثير على الأجهزة المُدارة بالكامل أو المملوكة شخصيًا.

## 1. الكاميرا معطّلة

ما إذا كانت الكاميرا معطّلة.

## 2. التقاط الشاشة معطّل

ما إذا كان التقاط الشاشة معطّلًا.

## 3. الحد الأقصى للأيام مع إيقاف العمل

يتحكم في مدة بقاء ملف تعريف العمل متوقفًا.

## 4. مشاركة Bluetooth

يتحكم في السماح بمشاركة Bluetooth في ملف التعريف الشخصي لجهاز مملوك للشركة يحتوي على ملف تعريف عمل.

## 5. المساحة الخاصة

يتحكم في السماح بمساحة خاصة على الجهاز.

## 6. وضع Play Store

يتحكم هذا الوضع في التطبيقات المسموح بها أو المحظورة للمستخدم في متجر Play Store لملف التعريف الشخصي.

**القائمة المحظورة (افتراضي)**: جميع التطبيقات متاحة، وأي تطبيق يجب ألا يكون على الجهاز يجب وضع علامة **محظور** عليه صراحةً في قسم **التطبيقات**.

**القائمة المسموح بها**: لا يُسمح بتثبيت في ملف التعريف الشخصي سوى التطبيقات المحددة صراحةً في قسم **التطبيقات** مع تعيين **نوع التثبيت** على **متاح**.

# 7. التطبيقات

قائمة التطبيقات التي يجب السماح بها أو حظرها في ملف التعريف الشخصي. يعتمد سلوك محتوى القائمة على القيمة المعيّنة في **وضع Play Store**.

لإضافة تطبيق جديد من Play Store، انقر على أيقونة **+**.

## 7.1. نوع التثبيت

أنواع سلوكيات التثبيت التي يمكن أن يمتلكها تطبيق ملف التعريف الشخصي.

**محظور**: التطبيق محظور ولا يمكن تثبيته في ملف التعريف الشخصي.

**متاح**: التطبيق متاح للتثبيت في ملف التعريف الشخصي.

# 8. أنواع الحسابات المحظورة

أنواع الحسابات التي لا يمكن للمستخدم إدارتها. يمنع هذا الخيار مستخدمي الجهاز من إضافة حسابات غير معتمدة إلى ملف التعريف الشخصي الخاص بهم.

# السياسات العابرة لملفات التعريف

ينطبق فقط على الأجهزة التي تحتوي على ملف تعريف شخصي وملف تعريف عمل.

## النسخ واللصق العابران لملفات التعريف

ما إذا كان يمكن لصق النص المنسوخ من أحد ملفي التعريف (الشخصي أو العمل) في ملف التعريف الآخر.

> **غير مسموح (الافتراضي)**: يمنع المستخدمين من لصق النص المنسوخ من ملف تعريف العمل في ملف التعريف الشخصي. يمكن لصق النص المنسوخ من ملف التعريف الشخصي في ملف تعريف العمل.
>
> **مسموح**: يمكن لصق النص المنسوخ في أي من ملفي التعريف في ملف التعريف الآخر.

## مشاركة البيانات العابرة لملفات التعريف

ما إذا كان يمكن مشاركة البيانات من أحد ملفي التعريف (الشخصي أو العمل) مع التطبيقات في ملف التعريف الآخر. يتحكم هذا تحديدًا في مشاركة البيانات البسيطة عبر intents. تُكوّن قنوات الاتصال الأخرى العابرة لملفات التعريف، مثل البحث في جهات الاتصال والنسخ/اللصق،
أو التطبيقات المتصلة لملفَي العمل والشخصي، بشكل منفصل.

> **غير مسموح**: يمنع مشاركة البيانات من ملف التعريف الشخصي إلى ملف تعريف العمل ومن ملف تعريف العمل إلى ملف التعريف الشخصي.
>
> **من العمل إلى الشخصي غير مسموح (الافتراضي)**: يمنع المستخدمين من مشاركة البيانات من ملف تعريف العمل مع التطبيقات في ملف التعريف الشخصي. يمكن مشاركة البيانات الشخصية مع تطبيقات العمل.
>
> **مسموح**: يمكن مشاركة البيانات من أي من ملفي التعريف مع ملف التعريف الآخر.

## الإعداد الافتراضي لأدوات ملف تعريف العمل

السلوك الافتراضي لأدوات ملف تعريف العمل. إذا لم يحدد تطبيق معين سياسة للأدوات، فإنه يتبع الإعداد الافتراضي المحدد هنا.

## وظائف التطبيقات العابرة لملفات التعريف

يتحكم في ما إذا كان يمكن لتطبيقات ملف التعريف الشخصي استدعاء وظائف التطبيقات من تطبيقات ملف تعريف العمل. يتطلب ذلك Android 16 فما فوق.

> يعتمد هذا الإعداد على خيار **وظائف التطبيقات** على مستوى السياسة (في قسم إدارة التطبيقات). إذا تم ضبط وظائف التطبيقات على **غير مسموح**، فسترفض واجهة API وظائف التطبيقات العابرة لملفات التعريف المضبوطة على **مسموح**.

## جهات اتصال العمل في ملف التعريف الشخصي

ما إذا كان يمكن إظهار جهات الاتصال المخزّنة في ملف تعريف العمل في عمليات البحث عن جهات الاتصال في ملف التعريف الشخصي والمكالمات الواردة.

> **مسموح (الافتراضي)**: يسمح بظهور جهات اتصال ملف تعريف العمل في ملف التعريف الشخصي.
>
> **غير مسموح**: يمنع التطبيقات الشخصية من الوصول إلى جهات اتصال ملف تعريف العمل والبحث عنها.
>
> **غير مسموح باستثناء النظام**: يمنع معظم التطبيقات الشخصية من الوصول إلى جهات اتصال ملف تعريف العمل، باستثناء تطبيقات Dialer وMessages وContacts الافتراضية من OEM (Android 14+).

عند تكوين ميزة جهات اتصال العمل في ملف التعريف الشخصي، يمكنك اختياريًا تحديد قائمة من إدخالات **اسم الحزمة المستثنى**. وفقًا للوضع المحدد، تعمل هذه الاستثناءات كقائمة سماح أو قائمة حظر للتطبيقات الشخصية.

# الإبلاغ عن الحالة

في هذا القسم، يمكنك تهيئة البيانات التي يجب استردادها من الجهاز. يمكن عرض بيانات الحالة في لوحة **حالة الجهاز**.

## تقارير التطبيقات

ما إذا كانت تقارير التطبيقات ممكّنة. (المعلومات المُبلغ عنها حول تطبيق مثبّت.)

> هذا الخيار مطلوب من قبل النظام (لتكامل تطبيق الرفيق) وهو ممكّن دائماً؛ ولا يمكن تعطيله.

## تضمين التطبيقات المزالة

ما إذا كانت التطبيقات المزالة مضمنة في تقارير التطبيقات.

## إعدادات الجهاز

ما إذا كان الإبلاغ عن إعدادات الجهاز ممكّناً. (معلومات حول إعدادات الجهاز المتعلقة بالأمان على الجهاز.)

## معلومات البرنامج

ما إذا كان الإبلاغ عن معلومات البرنامج ممكّناً. (معلومات حول برنامج الجهاز.)

## معلومات الذاكرة

ما إذا كان الإبلاغ عن الذاكرة ممكّناً. (حدث متعلق بقياسات الذاكرة والتخزين.)

## معلومات الشبكة

ام إذا كان الإبلاغ عن معلومات الشبكة ممكّناً. (معلومات شبكة الجهاز.)

## معلومات العرض

ام إذا كان الإبلاغ عن شاشات العرض ممكّناً. بيانات التقرير غير متاحة للأجهزة المملوكة شخصياً التي تحتوي على ملفات تعريف عمل. (معلومات عرض الجهاز.)

## أحداث إدارة الطاقة

ام إذا كان الإبلاغ عن أحداث إدارة الطاقة ممكّناً. بيانات التقرير غير متاحة للأجهزة المملوكة شخصياً التي تحتوي على ملفات تعريف عمل.

## حالة العتاد

ام إذا كان الإبلاغ عن حالة العتاد ممكّناً. بيانات التقرير غير متاحة للأجهزة المملوكة شخصياً التي تحتوي على ملفات تعريف عمل.

## خصائص النظام

ام إذا كان الإبلاغ عن خصائص النظام ممكّناً.

## وضع Common Criteria

ام إذا كان الإبلاغ عن وضع Common Criteria ممكّناً.

# متفرقات

## 1. لعبة الإيستر إيغ معطّلة

ما إذا كانت لعبة الإيستر إيغ في الإعدادات معطّلة.

## 2. تخطي تلميحات الاستخدام الأول

عالمة لتخطي التلميحات عند الاستخدام الأول. يمكن لمسؤول المؤسسة تمكين توصية النظام للتطبيقات بتخطي دروس المستخدم والتلميحات التمهيدية الأخرى عند أول بدء تشغيل.

## 3. رسالة دعم قصيرة

رسالة تُعرض للمستخدم في شاشة الإعدادات حيثما عطّل المسؤول إحدى الوظائف. إذا كانت الرسالة أطول من 200 حرف، فقد يتم اقتطاعها.

## 4. رسالة دعم طويلة

رسالة تُعرض للمستخدم في شاشة إعدادات مسؤولي الجهاز.

## 5. معلومات المالك على شاشة القفل

معلومات مالك الجهاز التي ستُعرض على شاشة القفل.

## 6. إجراءات الإعداد

الإجراءات التي تُتخذ أثناء عملية الإعداد. أثناء التسجيل، يمكنك مطالبة المستخدم بفتح تطبيق واحد أو أكثر لازمة لإعداد الجهاز.

استخدم **إضافة إجراء إعداد** لإنشاء إدخالات وإزالتها باستخدام إجراء الحذف.

### 6.1. تشغيل التطبيق

اسم حزمة التطبيق المراد تشغيله

### 6.2. العنوان

يوفّر رسالة موجّهة للمستخدم لشرح سبب الحاجة إلى تشغيل التطبيق.

### 6.3. الوصف

يوفّر رسالة موجّهة للمستخدم لشرح سبب الحاجة إلى تشغيل التطبيق.

## 7. ظهور اسم عرض المؤسسة

يتحكم في ما إذا كان اسم عرض المؤسسة ظاهرًا على الجهاز (على سبيل المثال، كرسالة على شاشة القفل على الأجهزة المملوكة للشركة).

**ظاهر (الافتراضي)**: اسم عرض المؤسسة ظاهر على الجهاز (مدعوم في ملفات تعريف العمل على Android 7+ والأجهزة المُدارة بالكامل على Android 8+).

**مخفي**: اسم عرض المؤسسة مخفي على الجهاز.

# قواعد الامتثال

إذا فشل جهاز أو ملف تعريف عمل في الامتثال لأي من إعدادات السياسة المدرجة أدناه، فإن Android Device Policy يحظر فورًا استخدام الجهاز أو ملف تعريف العمل افتراضيًا:

- **متطلبات كلمة المرور**
- **سياسة التشفير**
- **شاشة القفل معطّلة**
- **طرق الإدخال المسموح بها**
- **خدمات إمكانية الوصول المسموح بها**

إذا بقي الجهاز أو ملف العمل غير ممتثل بعد 10 أيام، فسيُعيد Android Device Policy ضبط الجهاز من المصنع أو سيحذف ملف العمل.

في هذا القسم، يمكنك تجاوز قواعد تطبيق الامتثال الافتراضية أو إضافة قواعد جديدة.

## القواعد

قائمة القواعد التي تحدد السلوك عندما يتعذر تطبيق سياسة معينة على جهاز.

استخدم **إضافة قاعدة** لإنشاء قاعدة جديدة. يمكن إزالة كل بطاقة قاعدة باستخدام إجراء الحذف.

### اسم الإعداد

السياسة العليا المراد تطبيقها. على سبيل المثال، **التطبيقات** أو **متطلبات كلمة المرور**.

**مطلوب.** يجب أن تطابق القيمة اسم سياسة علني مدعومًا؛ وإلا فسيتم وضع علامة غير صالح على الحقل.

### الحظر بعد عدد الأيام

عدد الأيام التي تكون فيها السياسة غير ممتثلة قبل حظر الجهاز أو ملف تعريف العمل. لحظر الوصول فورًا، عيّن القيمة 0. يجب أن يكون **الحظر بعد عدد الأيام** أقل من **المحو بعد عدد الأيام** . لا ينطبق إلا على الأجهزة المملوكة للشركة.

النطاق المسموح به: 0–300.

### نطاق الحظر

يحدد نطاق إجراء الحظر. لا ينطبق إلا على الأجهزة المملوكة للشركة.

الافتراضي (قاعدة جديدة): **ملف تعريف العمل**.

**ملف تعريف العمل**: يُطبّق إجراء الحظر على التطبيقات في ملف تعريف العمل فقط. لا تتأثر التطبيقات في ملف التعريف الشخصي.

**الجهاز بأكمله**: يُطبّق إجراء الحظر على الجهاز بأكمله، بما في ذلك التطبيقات في ملف التعريف الشخصي.

## المحو بعد عدد الأيام

عدد الأيام التي تكون فيها السياسة غير ممتثلة قبل محو الجهاز أو ملف تعريف العمل. **المحو بعد عدد الأيام** يجب أن يكون أكبر من **الحظر بعد عدد الأيام**. ينطبق الإعداد على الأجهزة المملوكة للشركة.

**مطلوب.** الافتراضي (قاعدة جديدة): **1**.

النطاق المسموح به: 1–300.

## الحفاظ على حماية إعادة ضبط المصنع

ما إذا كانت بيانات حماية إعادة ضبط المصنع محفوظة على الجهاز. ينطبق هذا الإعداد على ملفات تعريف العمل.

الافتراضي (قاعدة جديدة): ممكّن.