# 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.

---

Revision #58
Created 2025-12-17 09:32:29 UTC by Admin
Updated 2026-11-12 09:53:13 UTC by Admin