Sicherheit

In diesem Abschnitt können Sie sicherheitsrelevante Richtlinien konfigurieren.

Aktionen bei Sicherheitsrisiken

Wählen Sie, was passieren soll, wenn ein Gerät in den Statusberichten ein Sicherheitsrisiko meldet.

Unterstützte Sicherheitsproblemtypen:

Unbekanntes Betriebssystem: Die Play Integrity API erkennt, dass das Gerät ein unbekanntes Betriebssystem verwendet (der grundlegende Integritätscheck ist erfolgreich, aber ctsProfileMatch schlägt fehl).

Kompromittiertes Betriebssystem: Die Play Integrity API hat erkannt, dass das Gerät ein kompromittiertes Betriebssystem verwendet (die grundlegende Integritätsprüfung ist fehlgeschlagen).

Hardware-basierte Überprüfung fehlgeschlagen: Die Play Integrity API hat festgestellt, dass das Gerät keine starke Garantie für die Systemintegrität aufweist, falls das Label "MEETS_STRONG_INTEGRITY" nicht im Bereich "Geräteintegrität" angezeigt wird.

Verfügbare Aktionen:

Firmendaten löschen (Standard): Abmelden und Arbeitsdaten löschen (gesamtes Gerät, wenn vollständig verwaltet, oder nur das Arbeitsprofil bei gerätebesessenem Profil).

Keine Aktion: Das Gerät bleibt registriert und es wird automatisch nichts unternommen.

Wenn Sie **Firmen-Daten löschen** auswählen, können Sie auch Optionen für das Löschen konfigurieren:

Werkseinstellungen-Schutz beibehalten: Behält die Factory Reset Protection (FRP)-Daten bei, wenn das Gerät gelöscht wird.

Externen Speicher löschen: Löscht zusätzlich den externen Speicher des Geräts (z. B. SD-Karten) während des Löschvorgangs.

eSIMs löschen: Bei Geräten, die dem Unternehmen gehören, werden bei einem Löschvorgang alle eSIMs vom Gerät entfernt. Bei Geräten, die sich im privaten Besitz befinden, werden nur die verwalteten eSIMs (eSIMs, die über den Befehl ADD_ESIM hinzugefügt wurden) entfernt, und es werden keine eSIMs entfernt, die sich im privaten Besitz befinden.

1. Maximale Sperrzeit

Maximale Zeit (in Sekunden) für Benutzeraktivität, bevor das Gerät gesperrt wird. Ein Wert von 0 bedeutet, dass es keine Beschränkung gibt.

2. Immer eingeschaltet lassen, wenn das Gerät geladen wird

Die Modi für das Laden des Akkus, bei denen das Gerät eingeschaltet bleibt. Wenn Sie diese Einstellung verwenden, wird empfohlen, "**Maximale Sperrzeit**" zu deaktivieren, damit sich das Gerät nicht selbst sperrt, während es eingeschaltet bleibt.

Netzteil: Die Stromquelle ist ein Netzteil.

USB-Anschluss: Die Stromquelle ist ein USB-Anschluss.

Kabelloses Ladegerät: Die Stromquelle ist drahtlos.

3. Keyguard deaktiviert

Wenn aktiviert, wird der Sperrbildschirm für den primären und/oder sekundären Bildschirm deaktiviert. Diese Richtlinie wird nur im dedizierten Geräteverwaltungsmodus unterstützt.

4. Passwortanforderungen

Passwortrichtlinien.

Verwenden Sie **Konfigurieren Sie Passwortrichtlinien**, um einen oder mehrere Passwortrichtlinien-Blöcke hinzuzufügen. Verwenden Sie **Alle löschen**, um alle konfigurierten Passwortrichtlinien zu entfernen.

Die Passwortrichtlinien können den **Auto**-Bereich (eine einzige Anforderung) oder separate **Geräte**/**Arbeitsprofil**-Bereiche verwenden. Anforderungsrichtlinien, die auf Komplexität basieren, müssen mit Anforderungsrichtlinien kombiniert werden, die auf Qualität basieren, und zwar für denselben Bereich.

4.1. Anwendungsbereich

Der Anwendungsbereich, auf den die Passwortrichtlinie Anwendung findet.

> **Automatisch**: Der Gültigkeitsbereich ist nicht definiert. Die Passwortrichtlinien gelten für das Arbeitsprofil bei Geräten mit Arbeitsprofil und für das gesamte Gerät bei vollständig verwalteten oder dedizierten Geräten.
>
> **Gerät**: Die Passwortrichtlinien gelten nur für das Gerät.
>
> **Arbeitsprofil**: Die Passwortrichtlinien gelten nur für das Arbeitsprofil.

4.2. Länge des Passwort-Verlaufs

Die Länge der Passwort-Historie. Nach dem Festlegen dieses Wertes kann der Benutzer kein neues Passwort eingeben, das mit einem Passwort in der Historie übereinstimmt. Ein Wert von 0 bedeutet, dass es keine Einschränkung gibt.

4.3. Maximale Anzahl fehlgeschlagener Passworteingaben, bevor ein Löschvorgang ausgelöst wird

Anzahl der zulässigen falschen Passwörter zum Entsperren des Geräts, bevor eine Löschung erfolgt. Ein Wert von 0 bedeutet, dass es keine Einschränkung gibt.

4.4. Passwort-Ablaufzeit (Tage)

Diese Einstellung zwingt den Benutzer, sein Passwort regelmäßig zu ändern, und zwar nach der angegebenen Anzahl von Tagen.

4.5. Passwort zum Entsperren erforderlich

Die Zeit, die vergeht, bevor ein Gerät oder ein Arbeitsbereich nach der Entsperrung mit einer starken Authentifizierungsmethode (Passwort, PIN, Muster) mit einer anderen Authentifizierungsmethode (z. B. Fingerabdruck, Vertrauensagenten, Gesichtserkennung) entsperrt werden kann, beträgt. Nach Ablauf dieser Zeit können nur starke Authentifizierungsmethoden verwendet werden, um das Gerät oder den Arbeitsbereich zu entsperren.

> **Geräteeinstellung**: Der Timeout-Wert ist auf die Geräteeinstellung festgelegt.
>
> **Jeden Tag**: Die Timeout-Dauer ist auf 24 Stunden eingestellt.

4.6. Qualität des Passworts

Die erforderliche Passwortqualität.

Hohe Komplexität: Definieren Sie den Bereich für hohe Passwortkomplexität wie folgt: Bei Android 12 und höher: PIN ohne sich wiederholende (4444) oder geordnete (1234, 4321, 2468) Sequenzen, mindestens 8 Zeichen; alphabetisch, mindestens 6 Zeichen; alphanumerisch, mindestens 6 Zeichen.

Mittlere Komplexität: Definieren Sie den Bereich für mittlere Passwortkomplexität wie folgt: PIN ohne sich wiederholende (4444) oder geordnete (1234, 4321, 2468) Sequenzen, mindestens 4 Zeichen; alphabetisch, mindestens 4 Zeichen; alphanumerisch, mindestens 4 Zeichen.

Geringe Komplexität: Definieren Sie den Bereich für geringe Passwortkomplexität wie folgt: Muster; PIN mit wiederholenden (4444) oder geordneten (1234, 4321, 2468) Sequenzen.

Keine: Es gibt keine Passwortanforderungen.

Schwache: Das Gerät muss mit einer biometrischen Technologie mit geringem Sicherheitsniveau gesichert sein, mindestens aber. Dies umfasst Technologien, die die Identität einer Person erkennen können und in etwa der Sicherheit eines 3-stelligen PINs entsprechen (die Fehlerrate beträgt weniger als 1 von 1.000).

Beliebig: Ein Passwort ist erforderlich, aber es gibt keine Einschränkungen hinsichtlich des Passwortinhalts.

Zahlen: Das Passwort muss numerische Zeichen enthalten.

Zahlenfolge: Das Passwort muss numerische Zeichen enthalten, wobei sich keine Ziffern wiederholen dürfen (z.B. 4444) und keine aufsteigenden oder absteigenden Reihenfolgen enthalten sein dürfen (z.B. 1234, 4321, 2468).

Alphabetische Zeichen: Das Passwort muss alphabetische (oder Sonderzeichen) enthalten.

Alphanumerisch: Das Passwort muss sowohl numerische als auch alphabetische (oder Sonderzeichen) enthalten.

Komplex: Das Passwort muss die in den Einstellungen `passwordMinimumLength`, `passwordMinimumLetters`, `passwordMinimumSymbols` usw. definierten Mindestanforderungen erfüllen. Beispielsweise muss das Passwort, wenn `passwordMinimumSymbols` den Wert 2 hat, mindestens zwei Sonderzeichen enthalten.

4.7. Mindestlänge

Die Mindestlänge für Passwörter. Ein Wert von 0 bedeutet, dass es keine Beschränkung gibt.

4.8. Mindestanzahl an Buchstaben

Mindestanzahl an Buchstaben für das Passwort.

4.9. Mindestanzahl an Kleinbuchstaben

Mindestanzahl an Kleinbuchstaben, die im Passwort erforderlich sind.

4.10. Mindestanzahl an Großbuchstaben

Mindestanzahl an Großbuchstaben, die im Passwort erforderlich sind.

4.11. Mindestanzahl an nicht-alphabetischen Zeichen

Mindestanzahl an nicht-alphabetischen Zeichen (Ziffern oder Symbolen), die im Passwort erforderlich sind.

4.12. Mindestanzahl an Ziffern

Mindestanzahl an Ziffern, die im Passwort enthalten sein müssen.

4.13. Mindestanzahl an Symbolen

Mindestanzahl an Symbolen, die im Passwort erforderlich sind.

4.14. Einheitliche Sperre

Legt fest, ob für das Gerät und das Arbeitskonto eine einheitliche Sperre zulässig ist, bei Geräten mit Android 9 oder höher und einem Arbeitskonto. Dies hat keine Auswirkung auf andere Geräte.

> **Einheitliche Sperre erlauben**: Eine gemeinsame Sperre für das Gerät und das Arbeitskonto ist zulässig.
>
> **Separate Work-Profil-Sperre erforderlich**: Für das Arbeitskonto ist eine separate Sperre erforderlich.

5. Zurücksetzen auf Werkseinstellungen deaktiviert

Ob das Zurücksetzen auf Werkseinstellungen in den Einstellungen deaktiviert ist. Gilt nur für vollständig verwaltete Geräte.

6. Schutz vor dem Zurücksetzen auf Werkseinstellungen

E-Mail-Adressen der Geräteadministratoren für den Schutz vor dem Zurücksetzen auf Werkseinstellungen. Wenn das Gerät ein nicht autorisiertes Zurücksetzen auf Werkseinstellungen durchführt, muss einer dieser Administratoren mit der E-Mail-Adresse und dem Passwort des Google-Kontos anmelden, um das Gerät zu entsperren. Wenn keine Administratoren angegeben sind, bietet das Gerät keinen Schutz vor dem Zurücksetzen auf Werkseinstellungen. Nur für vollständig verwaltete Geräte.

E-Mail-Adressen der Geräteadministratoren: Verwenden Sie **Factory Reset Protection aktivieren**, um mit der Konfiguration der Administratoren zu beginnen. Verwenden Sie dann **E-Mail-Adresse eines Administrators hinzufügen**, um Adressen hinzuzufügen, und entfernen Sie sie mit der Löschfunktion.

7. Keyguard-Funktionen

Keyguard-Funktionen (Bildschirmsperre), die deaktiviert werden können.

7.1. Alle deaktivieren

Alle aktuellen und zukünftigen Anpassungen des Bildschirmsperrbildschirms deaktivieren.

7.2. Kamera deaktivieren

Kamera auf gesicherten Sperrbildschirmen (z. B. PIN) deaktivieren.

7.3. Benachrichtigungen deaktivieren

Benachrichtigungen nicht auf gesicherten Sperrbildschirmen anzeigen.

7.4. Nicht bearbeitete Benachrichtigungen deaktivieren

Nicht bearbeitete Benachrichtigungen auf gesicherten Sperrbildschirmen deaktivieren.

7.5. Zustand des Vertrauens-Agenten ignorieren

Zustand des Vertrauens-Agenten auf gesicherten Sperrbildschirmen ignorieren.

7.6. Fingerabdrucksensor deaktivieren

Fingerabdrucksensor für gesicherte Sperrbildschirme deaktivieren.

7.7. Texteingabe in Benachrichtigungen deaktivieren

Texteingabe in Benachrichtigungen auf gesicherten Sperrbildschirmen deaktivieren.

7.8. Gesichtserkennung deaktivieren

Gesichtserkennung für gesicherte Sperrbildschirme deaktivieren.

7.9. Iris-Authentifizierung deaktivieren

Iris-Authentifizierung für gesicherte Sperrbildschirme deaktivieren.

7.10. Gesamte biometrische Authentifizierung deaktivieren

Gesamte biometrische Authentifizierung für gesicherte Sperrbildschirme deaktivieren.

7.11. Alle Verknüpfungen deaktivieren

Alle Verknüpfungen auf dem gesicherten Sperrbildschirm bei Android 14 und höher deaktivieren.

Revision #36
Created 2025-12-09 17:58:14 UTC by Admin
Updated 2026-04-22 15:48:44 UTC by Admin