Sicherheit

In diesem Abschnitt können Sie sicherheitsbezogene Richtlinien konfigurieren.

Aktionen bei Sicherheitsrisiken

Wählen Sie, was geschehen soll, wenn ein Gerät ein SecurityRisk in Statusberichten meldet.

Unterstützte SecurityRisk-Typen:

Unbekanntes Betriebssystem: Die Play Integrity API stellt fest, dass das Gerät ein unbekanntes Betriebssystem ausführt (die basicIntegrity-Prüfung ist erfolgreich, aber ctsProfileMatch schlägt fehl).

Kompromittiertes Betriebssystem: Die Play Integrity API stellt fest, dass das Gerät ein kompromittiertes Betriebssystem ausführt (die basicIntegrity-Prüfung schlägt fehl).

Hardwaregestützte Bewertung fehlgeschlagen: Die Play Integrity API stellt fest, dass das Gerät keine starke Garantie für die Systemintegrität bietet, wenn die Bezeichnung MEETS_STRONG_INTEGRITY nicht im Feld für die Geräteintegrität angezeigt wird.

Verfügbare Aktionen:

Unternehmensdaten löschen (Standard): Registrierung aufheben und Arbeitsdaten löschen (gesamtes Gerät bei vollständig verwalteten Geräten oder nur das Arbeitsprofil bei profilverwalteten Geräten).

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

Wenn Sie **Unternehmensdaten löschen** auswählen, können Sie auch Löschoptionen konfigurieren:

Werksreset-Schutz beibehalten: Die Daten zum Werksreset-Schutz (FRP) beim Löschen des Geräts beibehalten.

Externen Speicher löschen: Beim Löschen zusätzlich den externen Speicher des Geräts (z. B. SD-Karten) löschen.

eSIMs löschen: Bei unternehmenseigenen Geräten werden beim Löschen des Geräts alle eSIMs entfernt. Bei privaten Geräten werden verwaltete eSIMs (eSIMs, die über den Befehl ADD_ESIM hinzugefügt wurden) auf den Geräten entfernt; private eSIMs werden nicht entfernt.

1. Max. Zeit bis zur Sperre

Maximale Zeit (in Sekunden) der Benutzeraktivität, bis das Gerät gesperrt wird. Ein Wert von 0 bedeutet, dass keine Einschränkung gilt.

2. Beim Laden eingeschaltet bleiben

Die Lademodi, bei denen das Gerät eingeschaltet bleibt. Wenn Sie diese Einstellung verwenden, wird empfohlen, **Max. Zeit bis zur Sperre** zu löschen, damit sich das Gerät nicht selbst sperrt, während es eingeschaltet bleibt.

AC-Ladegerät: Die Stromquelle ist ein AC-Ladegerät.

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

Drahtloses Ladegerät: Die Stromquelle ist drahtlos.

3. Tastensperre deaktiviert

Wenn true, wird die Sperrbildschirm-Funktion für primäre und/oder sekundäre Displays deaktiviert. Diese Richtlinie wird nur im Modus für dedizierte Geräteverwaltung unterstützt.

4. Passwortanforderungen

Richtlinien für Passwortanforderungen.

Verwenden Sie **Passwortanforderungen konfigurieren**, um einen oder mehrere Blöcke für Passwortanforderungen hinzuzufügen. Verwenden Sie **Alle löschen**, um alle konfigurierten Passwortanforderungen zu entfernen.

Passwortanforderungen können den Bereich **Auto** (eine einzelne Anforderung) oder separate Bereiche **Gerät**/**Arbeitsprofil** verwenden. Komplexitätsbasierte Anforderungen müssen mit qualitätsbasierten Anforderungen für denselben Bereich gekoppelt werden.

4.1. Bereich

Der Bereich, für den die Passwortanforderung gilt.

> **Auto**: Der Bereich ist nicht angegeben. Die Passwortanforderungen werden bei Arbeitsprofilgeräten auf das Arbeitsprofil und bei vollständig verwalteten oder dedizierten Geräten auf das gesamte Gerät angewendet.
>
> **Gerät**: Die Passwortanforderungen werden nur auf das Gerät angewendet.
>
> **Arbeitsprofil**: Die Passwortanforderungen werden nur auf das Arbeitsprofil angewendet.

4.2. Länge des Passwortverlaufs

Die Länge des Passwortverlaufs. Nach dem Festlegen dieses Felds kann der Benutzer kein neues Passwort eingeben, das mit einem der Passwörter im Verlauf übereinstimmt. Ein Wert von 0 bedeutet, dass keine Einschränkung gilt.

4.3. Max. fehlgeschlagene Passwörter bis zum Löschen

Anzahl der falschen Geräteentsperrungspasswörter, die eingegeben werden können, bevor das Gerät gelöscht wird. Ein Wert von 0 bedeutet, dass keine Einschränkung gilt.

4.4. Ablaufzeit für Passwörter (Tage)

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

4.5. Passwortentsperrung erforderlich

Die Zeitspanne, nachdem ein Gerät oder Arbeitsprofil mit einer starken Authentifizierungsform (Passwort, PIN, Muster) entsperrt wurde, in der es mit jeder anderen Authentifizierungsmethode (z. B. Fingerabdruck, Vertrauensagenten, Gesicht) entsperrt werden kann. Nach Ablauf der angegebenen Zeitspanne können nur starke Authentifizierungsformen zum Entsperren des Geräts oder Arbeitsprofils verwendet werden.

> **Gerätestandard**: Die Zeitüberschreitung ist auf den Gerätestandard festgelegt.
>
> **Jeden Tag**: Die Zeitüberschreitung ist auf 24 Stunden festgelegt.

4.6. Passwortqualität

Die erforderliche Passwortqualität.

Komplexität hoch: Definieren Sie die hohe Passwortkomplexitätsstufe wie folgt: Unter Android 12 und höher: PIN ohne wiederholte (4444) oder geordnete (1234, 4321, 2468) Sequenzen, Länge mindestens 8; alphabetisch, Länge mindestens 6; alphanumerisch, Länge mindestens 6.

Komplexität mittel: Definieren Sie die mittlere Passwortkomplexitätsstufe wie folgt: PIN ohne wiederholte (4444) oder geordnete (1234, 4321, 2468) Sequenzen, Länge mindestens 4; alphabetisch, Länge mindestens 4; alphanumerisch, Länge mindestens 4.

Komplexität niedrig: Definieren Sie die niedrige Passwortkomplexitätsstufe wie folgt: Muster; PIN mit wiederholten (4444) oder geordneten (1234, 4321, 2468) Sequenzen.

Keine: Es gelten keine Passwortanforderungen.

Schwach: Das Gerät muss mindestens mit einer biometrischen Erkennungstechnologie mit geringer Sicherheit gesichert sein. Dies umfasst Technologien, die die Identität einer Person erkennen können und in etwa einer 3-stelligen PIN entsprechen (Falscherkennung weniger als 1 zu 1.000).

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

Numerisch: Das Passwort muss numerische Zeichen enthalten.

Numerisch komplex: Das Passwort muss numerische Zeichen ohne wiederholte (4444) oder geordnete (1234, 4321, 2468) Sequenzen enthalten.

Alphabetisch: Das Passwort muss alphabetische (oder Symbol-)Zeichen enthalten.

Alphanumerisch: Das Passwort muss sowohl numerische als auch alphabetische (oder Symbol-)Zeichen enthalten.

Komplex: Das Passwort muss die Mindestanforderungen erfüllen, die in passwordMinimumLength, passwordMinimumLetters, passwordMinimumSymbols usw. angegeben sind. Wenn passwordMinimumSymbols beispielsweise 2 ist, muss das Passwort mindestens zwei Symbole enthalten.

4.7. Mindestlänge

Die zulässige Mindestlänge des Passworts. Ein Wert von 0 bedeutet, dass keine Einschränkung gilt.

4.8. Mindestanzahl Buchstaben

Mindestanzahl der im Passwort erforderlichen Buchstaben.

4.9. Mindestanzahl Kleinbuchstaben

Mindestanzahl der im Passwort erforderlichen Kleinbuchstaben.

4.10. Mindestanzahl Großbuchstaben

Mindestanzahl der im Passwort erforderlichen Großbuchstaben.

4.11. Mindestanzahl Nicht-Buchstaben-Zeichen

Mindestanzahl der im Passwort erforderlichen Nicht-Buchstaben-Zeichen (Ziffern oder Symbole).

4.12. Mindestanzahl Ziffern

Mindestanzahl der im Passwort erforderlichen Ziffern.

4.13. Mindestanzahl Symbole

Mindestanzahl der im Passwort erforderlichen Symbole.

4.14. Einheitliche Sperre

Steuert, ob eine einheitliche Sperre für das Gerät und das Arbeitsprofil auf Geräten mit Android 9 und höher mit Arbeitsprofil zulässig ist. Dies hat keine Auswirkung auf andere Geräte.

> **Einheitliche Sperre zulassen**: Eine gemeinsame Sperre für das Gerät und das Arbeitsprofil ist zulässig.
>
> **Separate Arbeitssperre erforderlich**: Eine separate Sperre für das Arbeitsprofil ist erforderlich.

5. Werksreset deaktiviert

Ob das Zurücksetzen auf die Werkseinstellungen über die Einstellungen deaktiviert ist. Gilt nur für vollständig verwaltete Geräte.

6. Werksreset-Schutz

E-Mail-Adressen der Geräteadministratoren für den Werksreset-Schutz. Wenn das Gerät einen nicht autorisierten Werksreset erfährt, muss sich 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 Werksreset-Schutz. Gilt nur für vollständig verwaltete Geräte.

Administrator-E-Mail-Adressen: Verwenden Sie **Werksreset-Schutz aktivieren**, um mit der Konfiguration von Administratoren zu beginnen. Verwenden Sie dann **Administrator-E-Mail hinzufügen**, um Adressen hinzuzufügen, und entfernen Sie sie über die Löschaktion.

7. Tastensperrfunktionen

Tastensperrfunktionen (Sperrbildschirm), die deaktiviert werden können.

7.1. Alle deaktivieren

Alle aktuellen und zukünftigen Anpassungen der Tastensperre deaktivieren.

7.2. Kamera deaktivieren

Die Kamera auf sicheren Sperrbildschirmen (z. B. PIN) deaktivieren.

7.3. Benachrichtigungen deaktivieren

Das Anzeigen aller Benachrichtigungen auf sicheren Sperrbildschirmen deaktivieren.

7.4. Unredigierte Benachrichtigungen deaktivieren

Unredigierte Benachrichtigungen auf sicheren Sperrbildschirmen deaktivieren.

7.5. Status des Vertrauensagenten ignorieren

Den Status des Vertrauensagenten auf sicheren Sperrbildschirmen ignorieren.

7.6. Fingerabdruck deaktivieren

Den Fingerabdrucksensor auf sicheren Sperrbildschirmen deaktivieren.

7.7. Texteingabe in Benachrichtigungen deaktivieren

Die Texteingabe in Benachrichtigungen auf sicheren Sperrbildschirmen deaktivieren.

7.8. Gesichtserkennung deaktivieren

Die Gesichtserkennung auf sicheren Sperrbildschirmen deaktivieren.

7.9. Iriserkennung deaktivieren

Die Iriserkennung auf sicheren Sperrbildschirmen deaktivieren.

7.10. Alle biometrischen Authentifizierungen deaktivieren

Alle biometrischen Authentifizierungen auf sicheren Sperrbildschirmen deaktivieren.

7.11. Alle Verknüpfungen deaktivieren

Alle Verknüpfungen auf sicheren Sperrbildschirmen unter Android 14 und höher deaktivieren.

Revision #58
Created 2025-12-09 17:58:14 UTC by Admin
Updated 2026-11-12 09:54:00 UTC by Admin