Richtlinien - Android

Zusammenfassung

Android-Richtlinien sind die zentralen Elemente des Systems: Sie definieren die Regeln, die auf verwalteten Geräten angewendet und durchgesetzt werden.

Sie können Ihre Richtlinien im Abschnitt **Richtlinien** des Dashboards einsehen und neue erstellen. Um eine Android-Richtlinie zu öffnen, klicken Sie auf die entsprechende Zeile in der Tabelle: das System öffnet die Seite "**Richtlinien-Editor**".

Eine Richtlinie kann mit einem Anmelde-Token verknüpft werden, sodass sie automatisch auf Geräte während des Bereitstellungsprozesses angewendet wird. Sie können auch die einem Gerät zugewiesene Richtlinie nach der Bereitstellung ändern.

> Jedes Gerät kann jeweils nur mit einer einzigen Richtlinie verknüpft werden.

> Viele Richtlinienoptionen gelten nur für bestimmte Gerätetypen (vollständig verwaltet, dediziert, Arbeitsbereich) und Android-Versionen. Nicht unterstützte Einstellungen können vom Gerät ignoriert werden oder als nicht konform gemeldet werden.

Layout des Richtlinien-Editors

Der Richtlinien-Editor ist als eine Reihe von erweitbaren Abschnitten aufgebaut. Am oberen Rand der Seite können Sie jederzeit Folgendes bearbeiten:

- **Name** (erforderlich)
- **ID** (nur lesbar)
- **Beschreibung** (optional)

Die folgenden Abschnitte entsprechen den Bedienfeldern des Richtlinien-Editors (z. B.: App-Verwaltung, Sicherheit, Netzwerk, System, Private Nutzung, Richtlinien für mehrere Profile und mehr). Verwenden Sie die Kapitel dieser Anleitung, um jedes Bedienfeld im Detail zu verstehen.

Speichern, löschen und zugeordnete Geräte

Verwenden Sie **Speichern**, um Ihre Änderungen anzuwenden. Der Button ist deaktiviert, wenn es keine ausstehenden Änderungen gibt oder wenn die Lizenz abgelaufen ist.

Wenn Sie eine bestehende Richtlinie geöffnet haben (sie hat eine ID), zeigt die Seite eine **Richtlinie löschen**-Aktion und eine **Verbundene Geräte**-Liste am unteren Rand, sodass Sie sehen können, wie viele Geräte die Richtlinie derzeit verwenden.

App-Verwaltung

In diesem Abschnitt können Sie Richtlinien für die Verfügbarkeit, Installation, Aktualisierung und das Berechtigungsmanagement von Apps festlegen.

> Verwaltete Google Play-Konten werden automatisch erstellt, wenn Geräte eingerichtet werden.

1. Play Store-Modus

Dieser Modus steuert, welche Apps dem Benutzer im Play Store angezeigt werden und wie sich das Gerät verhält, wenn Apps aus der Richtlinie entfernt werden.

Whitelist (Standard): Nur Apps, die in der Richtlinie enthalten sind, sind verfügbar, und alle Apps, die nicht in der Richtlinie enthalten sind, werden automatisch vom Gerät deinstalliert. Der Play Store zeigt nur verfügbare Apps an.

Blacklist: Alle Apps sind verfügbar, und Apps, die nicht auf dem Gerät sein sollen, müssen explizit in der App-Richtlinie als **gesperrt** gekennzeichnet werden. Der Play Store zeigt alle Apps an, außer den gesperrten.

2. Richtlinie für nicht vertrauenswürdige Apps

Die Richtlinie für nicht vertrauenswürdige Apps (Apps aus unbekannten Quellen), die auf dem Gerät durchgesetzt wird. Diese Option steuert die Android-Systemeinstellung, die bestimmt, ob ein Benutzer Apps außerhalb des Play Store installieren kann (Sideloading).

Nicht zulassen (Standard): Deaktivieren Sie die Installation von Apps aus unbekannten Quellen auf dem gesamten Gerät.

Nur für das persönliche Profil: Bei Geräten mit einem Arbeits-Profil, erlauben Sie die Installation von Apps aus unbekannten Quellen nur im persönlichen Profil des Geräts.

Erlauben: Erlaubt die Installation nicht vertrauenswürdiger Apps auf dem gesamten Gerät.

3. Google Play Protect

Ob die App-Überprüfung durch Google Play Protect erzwungen wird.

Erzwingen (Standard): Aktiviert die App-Überprüfung zwangsweise.

Benutzerwahl: Ermöglicht dem Benutzer die Auswahl, ob die App-Überprüfung aktiviert werden soll.

4. Standard-Berechtigungsrichtlinie

Die Richtlinie für die Vergabe von Berechtigungsanfragen an Apps zur Laufzeit.

Aufforderung (Standard): Fordert den Benutzer auf, eine Berechtigung zu erteilen.

Berechtigung erteilen: Eine Berechtigung automatisch erteilen.

Verweigern: Eine Berechtigung automatisch verweigern.

5. App-Funktionen

Legt fest, ob Apps auf vollständig verwalteten Geräten oder in Arbeitsbereichen Berechtigungen für den Zugriff auf App-Funktionen anfordern dürfen. Erfordert Android 16 oder höher.

Erlaubt (Standard): Apps auf vollständig verwalteten Geräten oder in Arbeitsbereichen können App-Funktionen freigeben.

Nicht erlaubt: Apps auf vollständig verwalteten Geräten oder in Arbeitsbereichen können keine App-Funktionen freigeben.

6. Installierte, deaktivierte Apps

Ob die Installation von Apps durch den Benutzer deaktiviert ist.

7. Deinstallation von Apps deaktiviert

Ist die Deinstallation von Anwendungen durch den Benutzer deaktiviert?

8. Berechtigungsrichtlinien

Explizite Berechtigungen oder Gruppenfreigaben bzw. -verweigerungen für alle Apps. Diese Werte überschreiben die Einstellung der **Standard-Berechtigungsrichtlinie**.

Verwenden Sie **die Berechtigungsrichtlinie**, um Einträge zu erstellen und diese mit der Löschfunktion zu entfernen.

Jeder Eintrag enthält:

> **Android-Berechtigung/Gruppe**: Die Android-Berechtigung oder -Gruppe (erforderlich), z. B. **android.permission.READ_CALENDAR** oder **android.permission_group.CALENDAR**.
>
> **Richtlinie**: Erlauben / Verweigern / Abfragen (verwendet dieselben Richtlinienoptionen wie die **Standardberechtigungsrichtlinie**).

9. Anwendungen

Liste der Anwendungen, die in der Richtlinie enthalten sein müssen. Das Verhalten des Inhalts der Liste hängt vom Wert ab, der für den **Google Play Store-Modus** eingestellt wurde.

Wenn der **Play Store-Modus** auf **Whitelist** eingestellt ist, sind nur Apps verfügbar, die in der Richtlinie enthalten sind, und alle Apps, die nicht in der Richtlinie enthalten sind, werden automatisch vom Gerät entfernt.

Wenn der **Play Store-Modus** auf "**Blacklist**" eingestellt ist, sind alle Apps verfügbar, und alle Apps, die nicht auf dem Gerät sein sollten, müssen explizit in der Anwendungsrichtlinie als **gesperrt** markiert werden.

Um eine neue App hinzuzufügen, klicken Sie auf die **Anwendungen hinzufügen** Schaltfläche (oder das **Anwendungen hinzufügen** Symbol), wählen Sie dann die App aus dem Play Store und klicken Sie auf die **Auswählen** Schaltfläche in der App-Karte.

> Alle Apps, die im Play Store Ihres Landes veröffentlicht sind, können standardmäßig ausgewählt werden. Um eigene private oder Web-Apps auszuwählen, müssen Sie diese zuerst in das System hochladen. Weitere Informationen finden Sie auf der **Private Apps**-Seite.

Jede App kann mit ihren eigenen Einstellungen konfiguriert werden, die visuell in einer Karte dargestellt sind:

9.1. Installationsart

Der Art der Installation, die für eine App durchgeführt werden soll.

> **Verfügbar**: Die App kann installiert werden.
>
> **Vorinstalliert**: Die App wird automatisch installiert und kann vom Benutzer entfernt werden.

Vorgeinstalliert: Die App wird automatisch installiert und kann nicht vom Benutzer entfernt werden.

Blockiert: Die App ist gesperrt und kann nicht installiert werden. Wenn die App unter einer früheren Richtlinie installiert war, wird sie deinstalliert.

Erforderlich für die Einrichtung: Die App wird automatisch installiert und kann vom Benutzer nicht entfernt werden. Sie verhindert den Abschluss der Einrichtung, bis die Installation abgeschlossen ist.

Kioskmodus: Die App wird automatisch im Kioskmodus installiert. Sie wird als bevorzugte Start-App festgelegt und für den Sperrmodus zugelassen. Die Gerätekonfiguration wird erst abgeschlossen, wenn die App installiert ist. Nach der Installation können Benutzer die App nicht deinstallieren. Sie können diesen **Installationsmodus** nur für eine App pro Richtlinie festlegen. Wenn dieser Parameter in der Richtlinie vorhanden ist, wird die Statusleiste automatisch deaktiviert. Weitere Informationen finden Sie auf der entsprechenden **Seite zum Kioskmodus**.

9.2. Installationsbeschränkungen

Definiert eine Reihe von Einschränkungen für die App-Installation. Wenn mehrere Einschränkungen ausgewählt sind, müssen alle erfüllt sein, damit die App installiert werden kann.

> Diese Option wird nur angezeigt, wenn der **Installationsmodus** auf **Vorinstalliert** oder **Erzwungene Installation** eingestellt ist.

Netzwerk ohne Datenvolumen: Installieren Sie die App nur, wenn das Gerät mit einem Netzwerk ohne Datenvolumen verbunden ist (z. B. Wi-Fi).

Laden: Installieren Sie die App nur, wenn das Gerät gerade aufgeladen wird.

Leerlauf: Installieren Sie die App nur, wenn das Gerät sich im Leerlauf befindet.

9.3. Automatischer Update-Modus

Steuert den automatischen Update-Modus für die App.

Standardmäßig: Die App wird automatisch mit geringer Priorität aktualisiert, um die Auswirkungen auf den Benutzer zu minimieren. Die App wird aktualisiert, wenn alle folgenden Bedingungen erfüllt sind: (1) das Gerät wird nicht aktiv genutzt, (2) das Gerät ist mit einem Netzwerk ohne Datenverbrauch verbunden, (3) das Gerät wird geladen. Der Benutzer wird innerhalb von 24 Stunden nach der Veröffentlichung eines neuen Updates durch den Entwickler über ein neues Update informiert, danach wird die App beim nächsten Mal aktualisiert, wenn die oben genannten Bedingungen erfüllt sind.

Verschoben: Die App wird maximal 90 Tage lang nicht automatisch aktualisiert, nachdem sie veraltet ist. 90 Tage nachdem die App veraltet ist, wird die neueste verfügbare Version automatisch mit niedriger Priorität installiert (siehe **Standard-**Auto-Update-Modus). Nach dem Update wird die App nicht erneut automatisch aktualisiert, bis sie 90 Tage nach dem erneuten Veralten aktualisiert ist. Der Benutzer kann die App jederzeit manuell aus dem Play Store aktualisieren.

Hohe Priorität: Die App wird so schnell wie möglich aktualisiert. Es werden keine Einschränkungen angewendet. Das Gerät wird sofort über eine neue Aktualisierung informiert, sobald diese verfügbar ist.

9.4. Minimale Versionsnummer

Die minimale Version der App, die auf dem Gerät ausgeführt wird. Wenn ein Wert festgelegt ist, versucht das Gerät, die App auf mindestens diese Versionsnummer zu aktualisieren. Wenn die App nicht auf dem neuesten Stand ist, enthält das Gerät einen **Nicht-Konformitäts-Hinweis** mit **Nicht-Konformitäts-Grund**, der auf **APP_NOT_UPDATED** gesetzt ist. Die App muss bereits im Google Play Store mit einer Versionsnummer veröffentlicht sein, die größer oder gleich diesem Wert ist. Maximal 20 Apps dürfen pro Richtlinie eine minimale Versionsnummer angeben.

9.5. Delegierte Berechtigungen

Die Berechtigungen, die der App von der Android-Geräterichtlinie zugewiesen wurden. Sie können anderen Apps eine Auswahl an speziellen Android-Berechtigungen gewähren:

Zertifikatsinstallation: Ermöglicht den Zugriff auf die Installation und Verwaltung von Zertifikaten.

Verwaltete Konfigurationen: Ermöglicht den Zugriff auf die Verwaltung von verwalteten Konfigurationen.

Deinstallation blockieren: Ermöglicht den Zugriff auf die Funktion zum Blockieren der Deinstallation.

Berechtigungen: Ermöglicht den Zugriff auf die Berechtigungsrichtlinie und den Status der Berechtigungsvergabe.

Paketberechtigungen: Ermöglicht den Zugriff auf den Status der Paketberechtigungen.

System-App: Ermöglicht den Zugriff zum Aktivieren von System-Apps.

9.6. Bevorzugtes Netzwerk

Der bevorzugte Netzwerkdienst, der für diese App verwendet werden soll. Wenn dieser Wert festgelegt ist, verwendet die App bei Verfügbarkeit den angegebenen Unternehmens-Netzwerkslice für ihre Verbindungen. Dieser muss mit einem in der **5G-Netzwerkslice-Konfiguration** des **Mobilfunk-**Bereichs konfigurierten Netzwerkslice übereinstimmen.

9.7. Standard-Berechtigungsrichtlinie

Die Standardrichtlinie gilt für alle Berechtigungen, die von der App angefordert werden. Falls angegeben, überschreibt dies die auf Richtlinienebene definierte **Standardberechtigungsrichtlinie**, die für alle Apps gilt. Sie überschreibt jedoch nicht die **Berechtigungsrichtlinien**, die für alle Apps gelten.

Aufforderung (Standard): Fordert den Benutzer auf, eine Berechtigung zu erteilen.

Berechtigung erteilen: Eine Berechtigung automatisch erteilen.

Verweigern: Eine Berechtigung automatisch verweigern.

9.8. Verbundene Arbeits- und persönliche Anwendungen

Steuert, ob die App über die Work- und Personalprofile eines Geräts hinweg kommunizieren darf, vorbehaltlich der Zustimmung des Benutzers (Android 11+).

Nicht erlaubt (Standard): Verhindert die Kommunikation der App zwischen verschiedenen Profilen.

Erlaubt: Ermöglicht der App die Kommunikation zwischen verschiedenen Profilen, nachdem die Benutzererlaubnis erteilt wurde.

9.9. Ausnahme für die Always-On-VPN-Sperre

Gibt an, ob die App Netzwerkverbindungen nutzen darf, wenn kein VPN verbunden ist und die **Sperre aktiviert** ist. Nur auf Geräten mit Android 10 und höher unterstützt.

Erzwungen (Standard): Die App respektiert die Einstellung für das Always-On-VPN, die aktiviert wurde.

Ausgenommen: Die App unterliegt nicht der Einstellung für das Always-On-VPN.

9.10. Arbeitsbereich-Widgets

Gibt an, ob die im Arbeitsbereich installierte App erlaubt ist, Widgets zum Home-Bildschirm hinzuzufügen.

Erlaubt: Die Anwendung darf Widgets zum Home-Bildschirm hinzufügen.

Nicht erlaubt: Die Anwendung darf keine Widgets zum Home-Bildschirm hinzufügen.

9.11. Benutzereinstellungen für die Steuerung

Gibt an, ob die Benutzersteuerung für eine bestimmte App zulässig ist. Die Benutzersteuerung umfasst Benutzeraktionen wie das erzwungene Beenden und Löschen von App-Daten (Android 11+). Wenn für eine App **extensionConfig** aktiviert ist, ist die Benutzersteuerung unabhängig von

dieser Einstellung nicht zulässig. Bei Kiosk-Apps können Sie mit **Erlaubt** die Benutzersteuerung aktivieren.

> **Nicht spezifiziert**: Verwendet das Standardverhalten der App, um zu bestimmen, ob die Benutzersteuerung erlaubt oder verboten ist.
>
> **Erlaubt**: Die App erlaubt die Benutzersteuerung.
>
> **Nicht erlaubt**: Die App erlaubt keine Benutzersteuerung.

9.12. Deaktiviert

Ob die App deaktiviert ist. Wenn die App deaktiviert ist, bleiben die App-Daten erhalten.

9.13. Credential-Anbieter erlauben

Ob die App als Anmeldeinformationsanbieter auf Android 14 und höher verwendet werden darf.

9.14. Konfigurationsverwaltung

Um die verwalteten Einstellungen der App zu konfigurieren, klicken Sie auf die Schaltfläche " **Verwaltete Konfiguration aktivieren**. Wenn für die App bereits eine verwaltete Konfiguration festgelegt ist, können Sie diese mit der Schaltfläche "**Verwaltete Konfiguration** ändern oder mit der Schaltfläche "**Konfiguration entfernen** löschen.

> **Die Option "Verwaltete Konfiguration"** ist nur für Apps verfügbar, die diese Funktionalität unterstützen.

9.15. Berechtigungsrichtlinien

Explizite Berechtigungen, die für die App gewährt oder verweigert werden. Diese Werte überschreiben die **Standardberechtigungsrichtlinie** und die **Berechtigungsrichtlinien**, die für alle Apps gelten.

Verwenden Sie **die Richtlinie zur Berechtigungsverwaltung**, um eine oder mehrere Berechtigungsregeln für die App-Karte hinzuzufügen, und entfernen Sie diese mit der Löschfunktion.

9.16. Verfolgen Sie IDs

Liste der Test-IDs für die geschlossene Testphase der App, auf die ein Gerät zugreifen kann. Wenn mehrere Test-IDs ausgewählt sind, erhalten die Geräte die neueste Version unter allen verfügbaren Testversionen. Wenn keine Test-IDs ausgewählt sind, haben die Geräte nur Zugriff auf die Produktionsversion der App.

>

> **Die Option "Track-IDs"** ist nur für Apps verfügbar, die mindestens eine Track-ID für Ihr Unternehmen bereitstellen. Weitere Informationen zum Hinzufügen Ihres Unternehmens zu einem geschlossenen Testprogramm für eine bestimmte App finden Sie hier.

10. Standardmäßige Anwendungseinstellungen

Standard-Apps für unterstützte Typen festlegen. Wenn für mindestens einen Typ eine Standard-App festgelegt ist, können Benutzer in diesem Profil keine Standard-Apps ändern.

> Es ist nur eine Standard-App-Einstellung pro **Standard-App-Typ** erlaubt. Die Liste der Standard-Anwendungen darf keine Duplikate enthalten.

10.1. Standard-App-Typ

Wählen Sie die App-Kategorie aus, die Sie konfigurieren möchten (z. B. Browser, Wählprogramm, SMS, Wallet oder Assistent). Die Verfügbarkeit hängt von der Android-Version und dem Verwaltungsmodus ab.

10.2. Standardmäßige Anwendungsbereiche

Wählen Sie aus, wo die Standard-App angewendet werden soll (vollständig verwaltet, Arbeitsbereich oder privater Bereich). Nur die für den ausgewählten Typ unterstützten Bereiche können ausgewählt werden.

> Wenn keiner der ausgewählten Bereiche für den Verwaltungsmodus des Geräts relevant ist, meldet das Gerät einen Nicht-Konformitäts-Hinweis.

10.3. Voreinstellungen für Anwendungen

Liste der Apps, die als Standard für den ausgewählten Typ festgelegt werden können. Die zuerst installierte und geeignete App wird als Standard festgelegt.

> Wenn die Berechtigungen "**Vollständig verwaltet**" oder "**Arbeitsprofil**" umfassen, muss jede App auch in der Liste der "**Anwendungen**" vorhanden sein, wobei der "**Installationsmodus**" nicht auf "**Blockiert**" eingestellt sein darf.

11. Auswahl des privaten Schlüssels

Ermöglicht die Anzeige einer Benutzeroberfläche auf einem Gerät, damit der Benutzer einen privaten Schlüssel-Alias auswählen kann, falls keine passenden Regeln in **Regeln für die Auswahl**

des privaten Schlüssels vorhanden sind.

> Für Geräte mit Android-Versionen vor P kann das Aktivieren dieser Einstellung dazu führen, dass Unternehmensschlüssel anfällig werden.

12. Wählen Sie Regeln für private Schlüssel

Steuert den Zugriff von Apps auf private Schlüssel. Die Regel bestimmt, welcher private Schlüssel, falls vorhanden, von Android Device Policy für die angegebene App gewährt wird. Der Zugriff wird entweder gewährt, wenn die App KeyChain.choosePrivateKeyAlias (oder eine der Varianten) aufruft, um einen privaten Schlüssel-Alias für eine bestimmte URL anzufordern, oder für Regeln, die nicht URL-spezifisch sind (d.h. wenn urlPattern nicht gesetzt ist oder leer ist oder .* lautet), direkt, sodass die App KeyChain.getPrivateKey aufrufen kann, ohne vorher KeyChain.choosePrivateKeyAlias aufrufen zu müssen. Wenn eine App KeyChain.choosePrivateKeyAlias aufruft und mehr als eine choosePrivateKeyRules übereinstimmt, bestimmt die letzte übereinstimmende Regel, welcher Schlüssel-Alias zurückgegeben wird.

Verwenden Sie **Regel für privaten Schlüssel hinzufügen**, um Dateneinträge zu erstellen und diese mit der Löschfunktion zu entfernen.

12.1. Alias für den privaten Schlüssel

Der Alias des privaten Schlüssels, der verwendet werden soll.

12.2. Muster für die URL

Das URL-Muster, das mit der URL der Anfrage verglichen wird. Wenn es nicht gesetzt oder leer ist, werden alle URLs abgeglichen. Dabei wird die reguläre Ausdrucks-Syntax von java.util.regex.Pattern verwendet.

12.3. Paketnamen

Die Paketnamen, auf die diese Regel angewendet wird. Der Hash des Signaturzertifikats für jede App wird mit dem von Play bereitgestellten Hash abgeglichen. Wenn keine Paketnamen angegeben sind, wird der Alias allen Apps zur Verfügung gestellt, die KeyChain.choosePrivateKeyAlias oder eine seiner Varianten aufrufen (aber nicht ohne den Aufruf von KeyChain.choosePrivateKeyAlias, auch auf Android 11 und höher). Jede App mit der gleichen Android-UID wie ein hier angegebenes Paket hat Zugriff, wenn sie KeyChain.choosePrivateKeyAlias aufruft.

Verwenden Sie **Paketnamen hinzufügen**, um Einträge hinzuzufügen und sie mit der Löschfunktion zu entfernen.

Um eine App zu löschen, klicken Sie auf das**Papierkorb-**Symbol, das sich am unteren Rand der App-Karte befindet.

Kioskmodus

Mit dem Kioskmodus können Sie die Funktionalität eines Geräts auf eine einzelne App oder mehrere Apps beschränken. Die Wahl zwischen einem Kioskmodus für eine einzelne App und einem für mehrere Apps hängt von Ihren Geschäftszielen ab.

Im **Kioskmodus für eine einzelne App** wird ein Gerät für eine einzelne Anwendung konfiguriert und verhindert, dass Endbenutzer auf andere Apps auf dem Gerät zugreifen. Sie können auch nicht aus der App heraus, wodurch das Gerät ausschließlich für diese bestimmte App bestimmt ist. Um diesen Modus zu aktivieren, geben Sie eine App im Abschnitt **App-Verwaltung** an und setzen Sie den **Installationsmodus** auf **Kiosk**.

Im **Mehr-App-Kioskmodus** können Geräte auf mehrere Anwendungen zugreifen. Endbenutzer können mit einem benutzerdefinierten Launcher zwischen mehreren Apps wechseln. Um diesen Modus zu aktivieren, aktivieren Sie die Option "**Benutzerdefinierter Kiosk-Launcher**".

Wenn der Kioskmodus aktiviert ist, können Sie auch konfigurieren, ob Endbenutzer auf bestimmte Systemfunktionen zugreifen können, wie z. B. Systemeinstellungen und die Statusleiste.

Benutzerdefinierter Kiosk-Launcher

Gibt an, ob der angepasste Kiosk-Launcher aktiviert ist. Dieser ersetzt den Startbildschirm durch einen Launcher, der das Gerät auf die über die **App-Verwaltung**-Einstellungen installierten Apps beschränkt. Die Apps werden auf einer einzigen Seite in alphabetischer Reihenfolge angezeigt.

Aktionen für den Power-Button

Legt das Verhalten eines Geräts im Kioskmodus fest, wenn ein Benutzer den Power-Button gedrückt hält.

> **Verfügbar (Standard)**: Das Power-Menü (z. B. Ausschalten, Neustarten) wird angezeigt, wenn ein Benutzer im Kioskmodus den Power-Button eines Geräts gedrückt hält.
>
> **Blockiert**: Das Power-Menü (z. B. Ausschalten, Neustarten) wird nicht angezeigt, wenn ein Benutzer im Kioskmodus die Power-Taste eines Geräts gedrückt hält. Hinweis: Dies kann verhindern, dass Benutzer das Gerät ausschalten.

Systemfehlerwarnungen

Legt fest, ob Systemfehlerdialoge für abgestürzte oder nicht reagierende Apps im Kioskmodus unterdrückt werden. Wenn die Anzeige unterdrückt wird, beendet das System die App, als ob der Benutzer die Option "App schließen" in der Benutzeroberfläche wählt.

Blockiert (Standard): Alle Systemfehlerdialoge, z. B. bei Abstürzen oder wenn eine App nicht reagiert (ANR), werden unterdrückt. Wenn die Anzeige unterdrückt ist, beendet das System die App, als ob der Benutzer die App über die Benutzeroberfläche schließen würde.

Aktiviert: Alle Systemfehlerdialoge, wie z. B. bei Abstürzen oder wenn eine App nicht reagiert (ANR), werden angezeigt.

Systemnavigation

Legt fest, welche Navigationsfunktionen (z. B. Home- und Übersichts-Buttons) im Kioskmodus aktiviert sind.

Deaktiviert (Standard): Die Schaltflächen "Home" und "Übersicht" sind nicht zugänglich.

Nur Startseite: Nur die Schaltfläche "Startseite" ist aktiviert.

Aktiviert: Die Schaltflächen "Startseite" und "Übersicht" sind aktiviert.

Statusleiste

Gibt an, ob Systeminformationen und Benachrichtigungen im Kioskmodus deaktiviert werden sollen.

Deaktiviert (Standard): Systeminformationen und Benachrichtigungen sind im Kioskmodus deaktiviert.

Nur System: Nur Systeminformationen werden in der Statusleiste angezeigt.

Aktiviert: Im Kioskmodus werden Systeminformationen und Benachrichtigungen in der Statusleiste angezeigt. Hinweis: Damit diese Richtlinie wirksam wird, muss die Home-Taste des Geräts über kioskCustomization.systemNavigation aktiviert sein.

Geräteeinstellungen

Legt fest, ob die Einstellungen-App im Kioskmodus zulässig ist.

Zulässig (Standard): Der Zugriff auf die Einstellungen-App ist im Kioskmodus erlaubt.

Blockiert: Der Zugriff auf die Einstellungen-App ist im Kioskmodus nicht erlaubt.

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.

Multimedia

In diesem Abschnitt können Sie das Verhalten von Kamera/Mikrofon, den USB-Datenzugriff, das Drucken sowie bildschirmspezifische Einschränkungen konfigurieren.

1. Zugriff auf die Kamera

Steuert die Nutzung der Kamera und ob der Benutzer den Kameraschalter aktivieren/deaktivieren kann (Android 12+). Im Allgemeinen gilt: Die Deaktivierung der Kamera wirkt sich bei vollständig verwalteten Geräten geräteweit aus und nur innerhalb des Arbeitsbereichs bei Geräten mit Arbeitsbereich.

> **Benutzerwahl (Standard)**: Standardverhalten des Geräts. Kameras sind verfügbar und (ab Android 12) kann der Benutzer den Zugriff auf die Kamera aktivieren/deaktivieren.
>
> **Deaktiviert**: Alle Kameras sind deaktiviert (bei vollständiger Verwaltung: geräuzweit; bei Arbeitsprofil: nur für Apps im Arbeitsprofil). Der Kameraschalter hat im verwalteten Bereich keine Wirkung.
>
> **Erzwungen**: Kameras sind verfügbar. Bei vollständig verwalteten Geräten mit Android 12 oder höher kann der Benutzer den Zugriff auf die Kamera nicht selbst aktivieren oder deaktivieren. Bei anderen Geräten/Versionen verhält sich dies wie bei der Benutzereinstellung.

2. Zugriff auf das Mikrofon

Bei vollständig verwalteten Geräten steuert diese Einstellung die Nutzung des Mikrofons und ob der Benutzer den Mikrofontast (Android 12+) aktivieren oder deaktivieren kann. Diese Einstellung hat keine Auswirkungen auf Geräte, die nicht vollständig verwaltet werden.

> **Benutzerwahl (Standard)**: Standardverhalten. Das Mikrofon ist verfügbar und (ab Android 12) kann der Benutzer den Mikrofonzugriff aktivieren oder deaktivieren.
>
> **Deaktiviert**: Das Mikrofon ist deaktiviert (für das gesamte Gerät). Der Umschalter für den Mikrofonzugriff hat keine Auswirkung.
>
> **Erzwungen**: Das Mikrofon ist verfügbar. Unter Android 12+ kann der Benutzer den Mikrofonzugriff nicht selbst aktivieren oder deaktivieren. Unter Android 11 oder älter verhält sich dies wie bei einer Benutzerwahl.

3. Zugriff auf USB-Daten

Steuert, welche Dateien und/oder Daten über USB übertragen werden können. Nur auf firmeneigenen Geräten unterstützt.

Dateitransfer deaktivieren (Standard): Der Dateitransfer ist deaktiviert, aber andere USB-Datenverbindungen (z. B. Maus/Tastatur) sind weiterhin möglich.

Datenübertragung verbieten: Alle Arten von USB-Datenübertragungen sind verboten (Android 12+ mit USB HAL 1.3+). Wenn nicht unterstützt, wechselt das Gerät in den Modus "Dateiübertragung verbieten".

Datenübertragung zulassen: Alle Arten von USB-Datenübertragungen sind erlaubt.

4. Drucken

Legt fest, ob das Drucken erlaubt ist (Android 9+).

Erlaubt (Standard): Das Drucken ist erlaubt.

Nicht erlaubt: Das Drucken ist nicht erlaubt (Android 9+).

5. Einstellungen für die Bildschirmhelligkeit

Steuert den Bildschirmhelligkeitsmodus und (optional) den Helligkeitswert.

Bildschirmhelligkeitsmodus:

Benutzereinstellung (Standard): Der Benutzer darf die Bildschirmhelligkeit konfigurieren.

Automatisch: Die Helligkeit wird automatisch eingestellt, und der Benutzer kann diese Einstellung nicht ändern. Sie können dennoch einen Helligkeitswert festlegen, der bei der automatischen Anpassung verwendet wird (vollständig verwaltete Android-Geräte ab Version 9; Arbeitsprofile auf firmeneigenen Android-Geräten ab Version 15).

Behoben: Die Helligkeit wird auf den konfigurierten Wert eingestellt, und der Benutzer kann diese Einstellung nicht ändern. Ein Helligkeitswert ist erforderlich (vollständig verwaltete Android-Geräte ab Version 9; Arbeitsprofile auf firmeneigenen Android-Geräten ab Version 15).

Bildschirmhelligkeit:

Wert von 1 bis 255 (1 = niedrigste, 255 = höchste Helligkeit). Ein Wert von 0 bedeutet, dass keine Helligkeit eingestellt ist.

6. Einstellungen für die Bildschirm-Timeout-Funktion

Steuert, ob der Benutzer die Bildschirm-Timeout-Funktion konfigurieren kann, und, falls erzwungen, den Timeout-Wert.

Das Feld **Bildschirmsperr-Modus** ermöglicht die Auswahl zwischen benutzerdefinierter und erzwungener Einstellung.

Benutzerdefinierte Einstellung (Standard): Der Benutzer kann die Bildschirm-Timeout-Funktion selbst konfigurieren.

Erzwungen: Die Bildschirm-Timeout-Funktion wird auf den konfigurierten Wert gesetzt und der Benutzer kann diese Einstellung nicht ändern (vollständig verwaltetes Android 9+; Arbeitsprofile auf firmeneigenen Android-Geräten ab Version 15).

Bildschirm-Timeout: Erzwingt den konfigurierten Wert, den der Benutzer nicht ändern kann (vollständig verwaltetes Android 9+; Arbeitsprofile auf firmeneigenen Android-Geräten ab Version 15)

Zeitspanne bis zum Timeout in Sekunden. Der Wert muss größer als 0 sein. Wenn er größer ist als **Maximale Sperrzeit**, kann das System ihn möglicherweise begrenzen und eine Nichtkonformität melden.

7. Bildschirmaufnahme deaktiviert

Ob die Bildschirmaufnahme deaktiviert ist.

Lautstärkeanpassung deaktiviert

Ob die Einstellung der Hauptlautstärke deaktiviert ist.

9. Das Mounten von physischen Medien ist deaktiviert

Ob das Mounten von physischen externen Medien deaktiviert ist.

Mobilfunk

In diesem Abschnitt können Sie zelluläreinstellungen konfigurieren.

1. Flugmodus

Steuert, ob der Benutzer den Flugmodus aktivieren und deaktivieren kann.

> **Benutzereinstellung (Standard)**: Der Benutzer darf den Flugmodus aktivieren oder deaktivieren.
>
> **Deaktiviert**: Der Flugmodus ist deaktiviert. Der Benutzer darf den Flugmodus nicht aktivieren. Unterstützt auf Android 9 und höher.

2. Mobilfunk 2G

Legt fest, ob der Benutzer die Einstellung für Mobilfunk 2G aktivieren oder deaktivieren kann.

> **Benutzereinstellung (Standard)**: Der Benutzer darf die Einstellung für Mobilfunk 2G aktivieren oder deaktivieren.
>
> **Deaktiviert**: Mobilfunk 2G ist deaktiviert. Der Benutzer darf Mobilfunk 2G über die Einstellungen nicht aktivieren. Unterstützt auf Android 14 und höher.

3. APN-Einstellungen überschreiben

Steuert, ob das Überschreiben der APN-Einstellungen aktiviert oder deaktiviert ist. Wenn aktiviert, werden nur die konfigurierten APN-Überschreibungen verwendet und alle anderen APNs auf dem Gerät werden ignoriert.

> **Deaktiviert (Standard)**: Alle konfigurierten APN-Einstellungen werden auf dem Gerät gespeichert, sind aber deaktiviert und haben keine Wirkung. Alle anderen APNs auf dem Gerät bleiben aktiv.
>
> **Aktiviert**: Nur die überschreibenden APN-Einstellungen werden verwendet, alle anderen APN-Einstellungen werden ignoriert. Diese Einstellung kann nur auf vollständig verwalteten Geräten mit Android 10 und höher konfiguriert werden.

4. APN-Einstellungen

Konfigurieren Sie einen oder mehrere APN-Einträge. Verwenden Sie **APN hinzufügen**, um einen Eintrag zu erstellen, und **APN entfernen**, um ihn zu löschen.

Jeder APN hat erforderliche Felder:

APN-Typen: Wählen Sie einen oder mehrere Datentypen für diesen APN aus (die Verfügbarkeit hängt vom Verwaltungsmodus und der Android-Version ab).

APN-Name: Die vom Netzbetreiber bereitgestellte APN-Kennung.

Anzeigename: Freundlicher Name, der in der Benutzeroberfläche angezeigt wird.

Optionale APN-Felder:

Authentifizierungstyp, **Benutzername**, **Passwort**: Konfigurieren Sie die Anmeldemethode des Anbieters (falls erforderlich).

Protokoll und **Roaming-Protokoll**: Konfiguration des IP-Protokolls.

Netzwerktypen: Beschränken Sie die verwendeten Mobilfunktechnologien (z. B. LTE/5G NR).

Proxy-Adresse und **Proxy-Port**: HTTP-Proxy für Datenverkehr (falls zutreffend).

MMS-Proxy-Adresse, **MMS-Proxy-Port**, **MMSC (URI des MMS-Zentrums)**: Einstellungen für MMS.

Numerische Operator-ID (MCC+MNC) und **Träger-ID**: Felder zur Identifizierung des Mobilfunkanbieters.

Immer aktiv: Gibt an, ob die durch dieses APN aktivierte PDN-Verbindung immer aktiv sein soll. Unterstützt ab Android 15.

MVNO-Typ: Kennzeichnet den Typ des virtuellen Mobilfunknetzbetreibers.

MTU IPv4 und **MTU IPv6**: Maximale Übertragungseinheit für IPv4-/IPv6-Verbindungen. Unterstützt ab Android 13.

5. Cell-Broadcast-Konfiguration deaktiviert

Ob die Konfiguration für Cell Broadcast deaktiviert ist.

6. Mobile Netzwerkkonfiguration deaktiviert

Ob die Konfiguration für mobile Netzwerke deaktiviert ist.

7. Roaming-Daten deaktiviert

Ob Roaming-Daten aktiviert sind.

8. Ausgehende Anrufe deaktiviert

Ob ausgehende Anrufe deaktiviert sind.

9. SMS-Funktion deaktiviert

Ob das Senden und Empfangen von SMS-Nachrichten deaktiviert ist.

10. Konfiguration der 5G-Netz-Slicing-Funktion

Konfigurieren Sie die Einstellungen für bevorzugte Netzwerkdienste, um Enterprise-5G-Netz-Slicing zu aktivieren. Sie können bis zu 5 Enterprise-Slices einrichten und Anwendungen bestimmten Netzwerken zuweisen, um die Datenübertragung zu optimieren.

10.1. Standardmäßige bevorzugte Netzwerkeinstellungen

Standardmäßige bevorzugte Netzwerk-ID für Anwendungen, die nicht in der Anwendungsliste enthalten sind, oder wenn eine Anwendung keine **bevorzugte Netzwerk**einstellung hat. Es muss eine Konfiguration für die angegebene Netzwerk-ID vorhanden sein (es sei denn, sie ist auf **keine bevorzugte Netzwerk** eingestellt).

Hinweis: Kritische Anwendungen wie **com.google.android.apps.work.clouddpc** und **com.google.android.gms** sind von dieser Standardeinstellung ausgenommen.

10.2. Konfigurationen für Netzwerkdienste

Verwenden Sie **Netzwerkkonfiguration hinzufügen**, um eine Slice-Konfiguration zu erstellen. Sie können bis zu 5 Konfigurationen hinzufügen. Jede Konfiguration hat:

> **Bevorzugte Netzwerk-ID (automatisch zugewiesen)**: Die Netzwerk-ID wird automatisch zugewiesen und kann nicht geändert werden.

Fallback auf die Standardverbindung: Legt fest, ob auf die standardmäßige Netzwerkverbindung des Geräts zurückgegriffen werden darf. Wenn dies nicht zulässig ist, können Apps nicht auf das Internet zugreifen, wenn das 5G-Netzwerk nicht verfügbar ist.

Nicht übereinstimmende Netzwerke: Legt fest, ob Apps, die dieser Konfiguration unterliegen, Netzwerke verwenden dürfen, die nicht der bevorzugten Verbindung entsprechen. Wenn dies auf **Deaktiviert** eingestellt ist, muss auch **Fallback auf die Standardverbindung** ebenfalls auf **Deaktiviert** eingestellt sein. Erfordert Android 14 oder höher.

Netzwerkfunktionen

In diesem Abschnitt können Sie netzwerkbezogene Richtlinien konfigurieren.

> Wi-Fi-Einstellungen können vom System bereitgestellt und verwaltet werden, über die **Wi-Fi-Einstellungen**. Je nach Wert, der bei **Wi-Fi-Konfiguration** eingestellt ist, haben Benutzer möglicherweise eingeschränkte oder keine Kontrolle über das Hinzufügen/Ändern von Netzwerken.

Zustand des drahtlosen Geräts

1. Wi-Fi-Status

Steuert den aktuellen Wi-Fi-Status und ermöglicht dem Benutzer, diesen zu ändern.

Benutzerwahl (Standard): Der Benutzer darf Wi-Fi aktivieren/deaktivieren.

Aktiviert: Wi-Fi ist eingeschaltet und der Benutzer darf es nicht deaktivieren (Android 13+).

Deaktiviert: Wi-Fi ist ausgeschaltet, und der Benutzer darf es nicht aktivieren (Android 13+).

2. Mindest-Sicherheitsstufe für Wi-Fi

Die minimale erforderliche Sicherheitsstufe für Wi-Fi-Netzwerke, mit denen sich das Gerät verbinden kann. Unterstützt ab Android 13 für vollständig verwaltete Geräte und Arbeitsprofile auf firmeneigenen Geräten.

Offenes Netzwerk (Standard): Das Gerät kann mit allen Arten von Wi-Fi-Netzwerken verbunden werden.

Persönliches Netzwerk: Verhindert die Nutzung offener Wi-Fi-Netzwerke; erfordert mindestens eine persönliche Sicherheitsfunktion (z. B. WPA2-PSK).

Unternehmensnetzwerk: Erfordert Unternehmens-EAP-Netzwerke; verbietet Wi-Fi-Netzwerke mit einem niedrigeren Sicherheitsniveau.

Unternehmensnetzwerk mit 192 Bit: Erfordert Unternehmensnetzwerke mit 192 Bit; die strengste Option.

3. Status von Ultra-Weitband (UWB)

Steuert den Status der Ultra-Weitband-Einstellung und ob der Benutzer sie aktivieren oder deaktivieren kann.

> **Benutzerwahl (Standard)**: Der Benutzer kann Ultra-Weitband aktivieren oder deaktivieren.
>
> **Deaktiviert**: UWB ist deaktiviert und der Benutzer kann diese Einstellung über die Einstellungen nicht ändern (Android 14+).

Gerätekonnektivitätsverwaltung

4. Bluetooth-Freigabe

Steuert, ob das Teilen über Bluetooth erlaubt ist.

> **Erlaubt**: Bluetooth-Freigabe ist erlaubt (standardmäßig bei vollständig verwalteten Geräten, Android 8+).
>
> **Nicht erlaubt**: Bluetooth-Freigabe ist nicht erlaubt (standardmäßig für verwaltete Profile, Android 8+).

5. Wi-Fi konfigurieren

Steuert die Berechtigungen zur Konfiguration von Wi-Fi. Je nach gewählter Option hat der Benutzer volle, eingeschränkte oder keine Kontrolle über die Konfiguration von Wi-Fi-Netzwerken.

> **Wi-Fi-Konfiguration zulassen (Standard)**: Der Benutzer darf Wi-Fi-Netzwerke konfigurieren.
>
> **Wi-Fi-Konfiguration verbieten**: Das Hinzufügen neuer Wi-Fi-Konfigurationen ist nicht zulässig. Der Benutzer kann zwischen bereits konfigurierten Netzwerken wechseln (Android 13+; vollständig verwaltete und firmeneigenen Arbeitsumgebungen).
>
> **Das Konfigurieren von Wi-Fi verbieten**: Verhindert das Konfigurieren von Wi-Fi-Netzwerken. Bei vollständig verwalteten Geräten werden benutzerkonfigurierte Netzwerke entfernt und nur Netzwerke beibehalten, die über **Wi-Fi-Konfigurationen** konfiguriert wurden. Bei firmeneigenen Arbeitsumgebungen bleiben bestehende Netzwerke unverändert, aber Benutzer können keine Wi-Fi-Netzwerke hinzufügen, entfernen oder ändern.

>

> Wenn die Wi-Fi-Konfiguration deaktiviert ist und das Gerät beim Start keine Verbindung herstellen kann, kann das System die **Notfallverbindung** anzeigen, damit der Benutzer sich vorübergehend verbinden und die Richtlinie aktualisieren kann.

6. Einstellungen für Wi-Fi Direct

Steuerelemente zum Konfigurieren und Verwenden von Wi-Fi Direct-Einstellungen. Unterstützt auf firmeneigenen Geräten mit Android 13 und höher.

Erlauben (Standard): Der Benutzer darf Wi-Fi Direct verwenden.

Deaktivieren: Der Benutzer darf Wi-Fi Direct nicht verwenden.

7. Einstellungen für den mobilen Hotspot

Steuert die Einstellungen für die mobile Hotspot-Funktion. Je nach gewählter Einstellung kann die Nutzung verschiedener Formen der mobilen Hotspot-Funktion teilweise oder vollständig eingeschränkt werden.

Alle Verbindungsarten zulassen (Standard): Ermöglicht die Konfiguration und Nutzung aller Verbindungsarten.

Wi-Fi-Tethering deaktivieren: Verhindert, dass der Benutzer Wi-Fi als Hotspot nutzt (bei Android-Geräten ab Version 13 im Besitz des Unternehmens).

Alle Verbindungsfreigabe-Optionen deaktivieren: Verhindert alle Arten von Verbindungsfreigabe (vollständig verwaltet + firmeneigene Arbeitsumgebungen).

8. Wi-Fi SSID-Richtlinie

Einschränkungen, zu welchen Wi-Fi SSIDs sich das Gerät verbinden kann (diese Einstellung beeinflusst nicht, welche Netzwerke auf dem Gerät konfiguriert werden können). Unterstützt auf firmeneigenen Geräten mit Android 13 oder höher.

SSID-Sperrliste (Standard): Das Gerät kann sich nicht mit Wi-Fi-Netzwerken verbinden, deren SSID in dieser Liste aufgeführt ist, kann aber mit anderen Netzwerken verbunden werden.

SSID-Zulassungsliste: Das Gerät kann sich nur mit den in dieser Liste aufgeführten Wi-Fi-Netzwerken verbinden. Die SSID-Liste darf nicht leer sein.

Verwenden Sie **"SSID hinzufügen"**, um Einträge hinzuzufügen. Je nach ausgewähltem Richtlinientyp wird die Liste als Liste der zulässigen oder der verbotenen SSIDs interpretiert.

Im Policy Editor-Interface wird die SSID-Liste als **Zulässige Wi-Fi-SSIDs** für Erlaubnislisten und als **Verbotene Wi-Fi-SSIDs** für Sperrlisten bezeichnet.

9. Wi-Fi-Roaming-Einstellungen

Konfigurieren Sie den Wi-Fi-Roaming-Modus pro SSID. Verwenden Sie **Hinzufügen der Wi-Fi-Roaming-Einstellungen**, um Einträge zu erstellen.

Jeder Eintrag enthält:

> **SSID**: Der SSID, für den die Roaming-Einstellungen gelten (erforderlich).
>
> **Wi-Fi-Roaming-Modus**: Standard / Deaktiviert / Aggressiv. Die Optionen "Deaktiviert" und "Aggressiv" erfordern Android 15 oder höher und werden nur auf vollständig verwalteten Geräten und Unternehmensprofilen auf firmeneigenen Geräten unterstützt.

Netzwerkbeschränkungen

Bluetooth deaktiviert

Ob Bluetooth deaktiviert ist. Bevorzugen Sie diese Einstellung gegenüber „Bluetooth-Konfiguration deaktiviert“, da „Bluetooth-Konfiguration deaktiviert“ vom Benutzer umgangen werden kann.

11. Bluetooth-Kontaktfreigabe deaktiviert

Ob die Bluetooth-Kontaktfreigabe deaktiviert ist.

12. Bluetooth-Konfiguration deaktiviert

Ob die Bluetooth-Konfiguration deaktiviert ist.

13. Netzwerk-Reset deaktiviert

Ob das Zurücksetzen der Netzwerkeinstellungen deaktiviert ist.

14. Ausgehendes Beam deaktiviert

Ob die Verwendung von NFC zum Übertragen von Daten von Apps deaktiviert ist.

VPN

15. Immer verbunden VPN-App

Geben Sie einen Paketnamen für das "Always On VPN" an, um sicherzustellen, dass Daten von den konfigurierten verwalteten Apps immer über ein VPN übertragen werden.

> Hinweis: Diese Funktion erfordert die Installation eines VPN-Clients, der sowohl die "Always On"- als auch die VPN-Funktionen pro App unterstützt.

16. VPN-Sperre

Verhindert Netzwerkzugriff, wenn keine VPN-Verbindung besteht.

17. VPN-Konfiguration deaktiviert

Ob die VPN-Konfiguration deaktiviert ist.

Proxy- und Netzwerkdienste

18. Bevorzugter Netzwerkdienst

Aktiviert den bevorzugten Netzwerkdienst für das Arbeitskonto. Beispielsweise kann ein Unternehmen eine Vereinbarung mit einem Mobilfunkanbieter haben, die besagt, dass Arbeitsdaten über einen speziellen Mobilfunkdienst für Unternehmen übertragen werden (z. B. einen dedizierten Kanal in 5G-Netzwerken). Dies hat keine Auswirkungen auf vollständig verwaltete Geräte.

Deaktiviert: Der bevorzugte Netzwerkdienst ist im Arbeitsbereich deaktiviert.

Aktiviert: Der bevorzugte Netzwerkdienst ist im Arbeitsbereich aktiviert.

> Wenn Sie Network Slicing im Unternehmensbereich verwenden, konfigurieren Sie außerdem **5G-Netzwerk-Slicing-Konfiguration** im Bereich **Mobilfunk** der Richtlinie und weisen Sie Apps mithilfe ihrer **Bevorzugte Netzwerk**-Einstellung einem Slice zu.

19. Empfohlener globaler Proxy

Der netzwerkunabhängige globale HTTP-Proxy. Proxies sollten in der Regel pro Netzwerk in den WLAN-Einstellungen konfiguriert werden. Ein globaler Proxy kann für ungewöhnliche Konfigurationen, z. B. allgemeine interne Filterung, nützlich sein. Der globale Proxy ist nur eine Empfehlung, und einige Apps können ihn ignorieren.

Deaktiviert

Direkter Proxy

Automatische Proxy-Konfiguration (PAC)

19.1. Host

Der Host des direkten Proxys.

19.2. Port

Der Port des direkten Proxys.

19.3. PAC-URI

Die URI des PAC-Skripts, das zur Konfiguration des Proxys verwendet wird.

19.4. Ausgeschlossene Hosts

Für einen direkten Proxy sind dies die Hosts, für die der Proxy umgangen wird. Hostnamen dürfen Platzhalter enthalten, z. B. ***.example.com**.

Verwenden Sie **Hinzufügen ausgeschlossener Hosts**, um Einträge hinzuzufügen (nur für direkten Proxy verfügbar).

WLAN-Konfigurationen

Definieren Sie WLAN-Netzwerkkonfigurationen, die das System auf Geräten anwendet. Verwenden Sie **Hinzufügen einer WLAN-Konfiguration**, um einen Eintrag zu erstellen, und entfernen Sie ihn mit der Löschfunktion.

20. Felder für die Wi-Fi-Konfiguration

Jede Konfiguration beinhaltet:

Konfigurationsname: Erforderlich.

SSID: Erforderlich.

Automatische Verbindung: Legt fest, ob automatisch eine Verbindung zu dem Netzwerk hergestellt werden soll, wenn es in Reichweite ist.

Schneller Übergang: Gibt an, ob der Client versuchen soll, den schnellen Übergang (IEEE 802.11r-2008) für das Netzwerk zu verwenden.

Verstecktes SSID: Gibt an, ob das SSID übertragen wird.

MAC-Adress-Randomisierung: Hardware oder Automatisch (Android 13+).

20.1. Sicherheit

Wi-Fi-Sicherheitsoptionen:

WEP-PSK: WEP (vorgegebener Schlüssel).

WPA-PSK: WPA/WPA2/WPA3-Personal (Vorgegebener Schlüssel).

WPA-EAP: WPA/WPA2/WPA3-Enterprise (Erweitertes Authentifizierungsprotokoll).

WPA3-Modus mit 192-Bit-Verschlüsselung: Ein WPA-EAP-Netzwerk, das nur den WPA3-Modus mit 192-Bit-Verschlüsselung zulässt.

20.2. Passphrase (vorgegebener Schlüssel)

Wird angezeigt, wenn die Sicherheit auf **WEP-PSK** oder **WPA-PSK** eingestellt ist. Die Passphrase ist erforderlich.

20.3. EAP-Methode (Enterprise)

Wird angezeigt, wenn die Sicherheit auf **WPA-EAP** oder **WPA3 192-Bit-Modus** eingestellt ist. Wählen Sie eine EAP-Außenmethode:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Authentifizierung in Phase 2

Wird für das Tunneling von äußeren Methoden (**EAP-TTLS** und **PEAP**) angezeigt.

MSCHAPv2

PAP

20.5. EAP-Anmeldedaten von Benutzern

Wenn aktiviert, wendet das System automatisch EAP-Anmeldedaten auf Geräten pro Benutzer an. Sie können Benutzeranmeldedaten im Abschnitt **Benutzer** konfigurieren.

20.6. Client-Zertifikat

Für **EAP-TLS** können Sie ein Client-Zertifikat zuweisen, das für die Wi-Fi-Authentifizierung verwendet wird. Weitere Informationen finden Sie auf der Seite **Zertifikatsverwaltung**.

Wenn ein Zertifikat bereits zugewiesen ist, können Sie mit "**Zertifikat öffnen**" dieses anzeigen oder mit "**Zertifikat ändern**" ein anderes auswählen.

Alternativ können Sie einen **Client-Zertifikats-Schlüsselpaar-Alias** angeben, der auf ein im Android-Schlüsselbund gespeichertes Client-Zertifikat verweist und für die Wi-Fi-Authentifizierung verwendet wird.

> Wenn sowohl das **Client-Zertifikat** als auch der **Alias für das Client-Zertifikats-Schlüsselpaar** angegeben sind, wird der Alias für das Schlüsselpaar ignoriert.

20.7. Identität

Identität des Benutzers. Für Tunneling von äußeren Protokollen (PEAP, EAP-TTLS) wird dies zur Authentifizierung innerhalb des Tunnels verwendet, und **die anonyme Identität** wird für die EAP-Identität außerhalb des Tunnels verwendet. Für nicht-tunnelnde äußere Protokolle wird dies für die EAP-Identität verwendet.

20.8. Anonyme Identität

Nur für Tunneling-Protokolle: Dies gibt die Identität des Benutzers an, der dem äußeren Protokoll präsentiert wird.

20.9. Passwort

Passwort des Benutzers. Wenn nicht angegeben, wird der Benutzer aufgefordert, ein Passwort einzugeben.

20.10. Server-CA-Zertifikate

Liste der CA-Zertifikate, die zur Überprüfung der Zertifikatskette des Hosts verwendet werden. Mindestens ein CA-Zertifikat muss übereinstimmen. Weitere Informationen finden Sie auf der **Zertifikatsverwaltung**-Seite.

Verwenden Sie **das Hinzufügen des Server-CA-Zertifikats**, um Einträge hinzuzufügen und sie mit der Löschfunktion zu entfernen.

20.11. Das Domänenpräfix stimmt überein

Eine Liste von Einschränkungen für den Server-Domänennamen. Die Einträge werden als Suffix-Übereinstimmungsanforderungen für den/die DNS-Namen des alternativen Betreffnamens eines Authentifizierungsserver-Zertifikats verwendet.

System

In diesem Abschnitt können Sie systembezogene Richtlinien konfigurieren.

1. Minimale API-Version

Die minimale zulässige Android API-Version.

2. Verschlüsselungsrichtlinie

Ob die Verschlüsselung aktiviert ist.

> **Standardwert**: Dieser Wert wird ignoriert, d. h. keine Verschlüsselung erforderlich.
>
> **Aktiviert ohne Passwort**: Verschlüsselung erforderlich, aber kein Passwort erforderlich, um das Gerät zu starten.
>
> **Aktiviert mit Passwort**: Verschlüsselung erforderlich, ein Passwort ist zum Starten des Geräts notwendig.

3. Automatische Datums- und Uhrzeit-Synchronisierung

Ist die automatische Datums-, Zeit- und Zeitzonensynchronisierung für Geräte, die dem Unternehmen gehören, aktiviert?

> **Benutzerwahl (Standard)**: Ob die automatische Datums-, Zeit- und Zeitzonensynchronisierung aktiviert ist, wird vom Benutzer festgelegt.
>
> **Erzwungen**: Erzwingen Sie die automatische Datums-, Zeit- und Zeitzonensynchronisierung auf dem Gerät.

4. Entwickleroptionen

Steuert den Zugriff auf die Entwicklereinstellungen: Entwickleroptionen und sicherer Start.

> **Deaktiviert (Standard)**: Deaktiviert alle Entwicklereinstellungen und verhindert, dass der Benutzer darauf zugreifen kann.

Erlaubt: Ermöglicht alle Entwicklereinstellungen. Der Benutzer kann auf diese zugreifen und sie optional konfigurieren.

5. Modus für Common Criteria

Steuerelemente für den Common Criteria Modus – Sicherheitsstandards, die im Common Criteria for Information Technology Security Evaluation (CC) definiert sind. Durch das Aktivieren des Common Criteria Modus werden bestimmte Sicherheitskomponenten auf einem Gerät erhöht (z. B. AES-GCM-Verschlüsselung von Bluetooth Long Term Keys, zusätzliche Validierung für einige Netzwerkzertifikate und kryptografische Richtlinieneintegritätsprüfungen). Der Common Criteria Modus wird nur auf firmeneigenen Geräten mit Android 11 oder höher unterstützt. Warnung: Der Common Criteria Modus erzwingt ein striktes Sicherheitsmodell, das in der Regel nur für hochsensible Organisationen erforderlich ist. Die normale Gerätefunktionalität kann beeinträchtigt werden; aktivieren Sie ihn nur, wenn dies erforderlich ist.

Deaktiviert (Standard): Deaktiviert den Common Criteria Modus.

Aktiviert: Aktiviert den Common Criteria Modus.

6. Memory Tagging Extension (MTE)

Steuert die Memory Tagging Extension (MTE) auf dem Gerät.

Benutzereinstellung (Standard): Der Benutzer kann MTE auf dem Gerät aktivieren oder deaktivieren (sofern vom Gerät unterstützt).

Erzwungen: MTE ist aktiviert und der Benutzer darf diese Einstellung nicht ändern (Android 14+; unterstützt auf vollständig verwalteten Geräten und in Arbeitsbereichen auf geräteeigenen Geräten).

Deaktiviert: MTE ist deaktiviert und der Benutzer darf diese Einstellung nicht ändern (Android 14+; unterstützt nur auf vollständig verwalteten Geräten).

7. Inhalts-Schutz

Aktiviert den Inhalts-Schutz (der nach betrügerischen Apps sucht). Dies wird ab Android 15 unterstützt.

Deaktiviert (Standard): Der Inhalts-Schutz ist deaktiviert und der Benutzer kann dies nicht ändern.

Erzwungen: Der Inhalts-Schutz ist aktiviert und kann vom Benutzer nicht geändert werden (Android 15+).

Benutzerwahl: Der Inhalts-Schutz wird nicht durch die Richtlinie gesteuert; der Benutzer kann dies selbst bestimmen (Android 15+).

8. Inhaltsunterstützung

Steuert, ob AssistContent an privilegierte Apps wie Assistenten-Apps (z. B. Circle to Search) gesendet werden darf. AssistContent enthält Screenshots und Informationen über eine App, z. B. den Paketnamen. Dies wird ab Android 15 unterstützt.

Erlaubt (Standard): Assist-Inhalte dürfen an eine privilegierte App gesendet werden (Android 15+).

Nicht erlaubt: Das Senden von Assist-Inhalten an eine privilegierte App ist blockiert (Android 15+).

9. Windows deaktivieren

Ob das Erstellen von Fenstern zusätzlich zu den Anwendungsfenstern deaktiviert ist. Diese Option verhindert die Anzeige der folgenden System-Benutzeroberflächen: Benachrichtigungen und Snackbars, Telefonaktivitäten (z. B. eingehende Anrufe) und Prioritäts-Telefonaktivitäten (z. B. laufende Anrufe), Systemwarnungen, Systemfehler und System-Overlays.

10. Netzwerk-Notausgang

Ob die Netzwerk-Notausgangsfunktion aktiviert ist. Wenn beim Starten des Geräts keine Netzwerkverbindung hergestellt werden kann, fordert die Notausgangsfunktion den Benutzer auf, sich vorübergehend mit einem Netzwerk zu verbinden, um die Gerätekonfiguration zu aktualisieren. Nach dem Anwenden der Konfiguration wird die temporäre Netzwerkverbindung vergessen, und das Gerät startet den Startvorgang fort. Dies verhindert, dass das Gerät keine Netzwerkverbindung herstellen kann, wenn im letzten Konfigurationsprofil kein geeignetes Netzwerk vorhanden ist, oder wenn sich das Gerät in einem App-Lock-Task-Modus befindet oder der Benutzer anderweitig nicht auf die Geräteeinstellungen zugreifen kann.

11. Standardaktivitäten

Eine Liste von Standardaktivitäten zur Verarbeitung von Intents, die einem bestimmten Intent-Filter entsprechen. Beispielsweise können IT-Administratoren mit dieser Funktion festlegen, welche

Browser-App automatisch Web-Links öffnet oder welche Launcher-App beim Tippen auf die Home-Taste verwendet wird.

Verwenden Sie **Standardaktivität hinzufügen**, um Einträge zu erstellen. Innerhalb eines Eintrags verwenden Sie **Aktion hinzufügen** und **Kategorie hinzufügen**, um den Intent-Filter zu erstellen.

11.1. Empfänger-Aktivität

Die Aktivität, die als Standard-Intent-Handler verwendet werden soll. Dies sollte ein Name einer Android-Komponente sein, z. B. com.android.enterprise.app/.MainActivity. Alternativ kann der Wert auch der Paketname einer App sein, wodurch Android Device Policy eine geeignete Aktivität aus der App zur Verarbeitung des Intents auswählt.

11.2. Aktion

Die Aktionen, die im Filter übereinstimmen müssen. Wenn Aktionen im Filter enthalten sind, muss die Aktion einer Absicht einer dieser Werte entsprechen, um übereinzustimmen. Wenn keine Aktionen enthalten sind, wird die Aktion der Absicht ignoriert.

11.3. Kategorie

Die Kriterienkategorien, die im Filter übereinstimmen müssen. Eine Kriterienkategorie enthält die Kategorien, die sie benötigt, und alle diese Kategorien müssen im Filter enthalten sein, damit eine Übereinstimmung erzielt wird. Mit anderen Worten: Das Hinzufügen einer Kategorie zum Filter hat keinen Einfluss auf die Übereinstimmung, es sei denn, diese Kategorie ist in der Kriterienkategorie selbst angegeben.

12. Erlaubte Eingabemethoden

Gibt die zulässigen Eingabemethoden an.

> **Alle zulässigen**: Es werden keine Einschränkungen angewendet. Alle Eingabemethoden sind erlaubt.
>
> **Nur System**: Nur die vom System integrierten Eingabemethoden sind zulässig.
>
> **Nur vom System und bereitgestellte**: Nur die vom System integrierten und bereitgestellten Eingabemethoden sind zulässig.

12.1. Erlaubte Eingabemethoden

Ermöglichte Paketnamen für Eingabemethoden. Gilt nur, wenn **Erlaubte Eingabemethoden** auf **Nur System- und angegebene** eingestellt ist.

Verwenden Sie **die Option zum Hinzufügen einer Eingabemethode**, um Einträge hinzuzufügen und entfernen Sie sie mit der Löschfunktion.

13. Erlaubte Bedienhilfen

Legt die zulässigen Barrierefreiheitsdienste fest.

> **Alle zulässigen**: Jeder Barrierefreiheitsdienst kann verwendet werden.
>
> **Nur System-**: Nur die vom System integrierten Barrierefreiheitsdienste können verwendet werden.
>
> **Nur System- und angegebene**: Nur die angegebenen und die in das System integrierten Bedienhilfen können verwendet werden.

13.1. Erlaubte Barrierefreiheitsdienste

Erlaubte Barrierefreiheitsdienste. Gilt nur, wenn **Erlaubte Barrierefreiheitsdienste** auf **Nur System- und angebotene** eingestellt ist.

Verwenden Sie den **Barrierefreiheitsdienst zum Hinzufügen** und entfernen Sie Einträge mit der Löschfunktion.

14. Systemaktualisierungsrichtlinie

Konfiguration für die Verwaltung von Systemupdates.

> **Standard**: Das Gerät verhält sich beim Update standardmäßig so, dass der Benutzer Systemupdates akzeptieren muss.
>
> **Automatisch**: Installiert die Updates automatisch, sobald eine neue Version verfügbar ist.
>
> **Im Zeitfenster**: Installiert Updates automatisch innerhalb eines definierten Wartungszeitfensters. Dies konfiguriert auch Play-Apps so, dass sie innerhalb dieses Zeitfensters aktualisiert werden. Dies wird dringend für Geräte im Kiosk-Modus empfohlen, da dies die einzige Möglichkeit ist, Apps, die dauerhaft im Vordergrund fixiert sind, mit Play zu aktualisieren.
>
> **Verschieben**: Automatischer Update-Vorgang kann um maximal 30 Tage verschoben werden.

14.1. Wartungsfenster (Nur für Fenster)

Wenn "**Richtlinie für Systemupdates**" auf "**Grafische Oberfläche**" eingestellt ist, können Sie das tägliche Wartungsfenster mit den Feldern "**von**" und "**bis**" festlegen.

14.2. Systemupdate-Sperrzeiten

Ein jährlich wiederkehrender Zeitraum, in dem Over-the-Air (OTA)-Systemupdates verschoben werden, um die auf einem Gerät laufende Betriebssystemversion zu fixieren. Um ein dauerhaftes Einfrieren des Geräts zu vermeiden, muss jeder Fixierungszeitraum durch mindestens 60 Tage getrennt sein. Jeder Fixierungszeitraum darf nicht länger als 90 Tage dauern.

Verwenden Sie **"System-Update-Sperrzeit festlegen"**, um Einträge zu erstellen.

15. Standardmäßige Anmeldeinformationsanbieter

Steuert, welche Apps unter Android 14 und höher als Anmeldeinformationsanbieter fungieren dürfen.

> **Nicht erlaubt (Standard)**: Apps, bei denen die credentialProviderPolicy nicht angegeben ist, dürfen nicht als Anmeldeinformationsanbieter fungieren.
>
> **Nicht zulässig, außer für Systemanwendungen**: Apps, bei denen die `credentialProviderPolicy` nicht angegeben ist, dürfen nicht als Anmeldeinformationsanbieter fungieren, außer für die standardmäßigen Anmeldeinformationsanbieter des Geräteherstellers.

Standort und Geofence

Dieses Panel gruppiert die Android-Richtlinien-Einstellungen, die die Standortmeldungen, die Standortdurchsetzung und die Geofence-Definitionen steuern. Verwenden Sie es, wenn Sie möchten, dass Cerberus Enterprise Standortdaten erfasst oder erkennt, wenn Geräte konfigurierte Bereiche betreten oder verlassen.

Standortmeldungen

Standort melden

Aktiviert die Standortbestimmungsberichterstattung für Geräte. Standortdaten, die über diese Einstellung erfasst werden, werden von der **Standortkarte im Dashboard**, der Geräteübersicht-Standorthistorie und der Geofencing-Verarbeitung verwendet.

> Bei Geräten, die nicht vollständig verwaltet werden, können Standortdaten weiterhin davon abhängen, dass die Cerberus Enterprise-App die erforderlichen Standortberechtigungen besitzt und die Standortdienste auf dem Gerät aktiviert sind.

Standortmodus

Steuert die Standortfunktion für dienstlich gestellte Geräte.

- **Benutzerwahl**: Standortdienste werden nicht durch die Richtlinie eingeschränkt.
- **Erzwungen**: Standortdienste sind auf dem Gerät aktiviert.
- **Deaktiviert**: Standortdienste sind auf dem Gerät deaktiviert.

Standortfreigabe deaktiviert

Deaktiviert die Standortfreigabe für Arbeits-Apps. Bei geräteeigenen Profilen wirkt sich dies auf das Arbeitsprofil aus. Bei vollständig verwalteten Geräten wird die Standortfunktion für das gesamte Gerät deaktiviert und der Geräte-Standortmodus außer Kraft gesetzt.

Automatisches Verhalten bei aktiven Geozäunen

Aktive Geozäune benötigen Standortmeldungen, um zu funktionieren. Wenn mindestens ein Geozäun aktiv ist, hält Cerberus Enterprise die zugehörigen Standorteinstellungen automatisch konsistent.

- **Die Standortmeldung** wird erzwungen, während aktive Geozäune vorhanden sind.
- **Standortmodus** wird auf **Erzwungen** gesetzt.
- **Die Ortungsfreigabe deaktiviert** wird erzwungen.

Wenn Sie versuchen, **Standort melden** zu deaktivieren, während eine oder mehrere Geofences aktiv sind, zeigt Cerberus Enterprise einen Bestätigungsdialog an. Wenn Sie fortfahren, werden alle aktiven Geofences in der Richtlinie deaktiviert.

Geofence-Liste

Eine Richtlinie kann bis zu **10 Geofences** enthalten. Geofence-Namen müssen innerhalb der Richtlinie eindeutig sein.

Verwenden Sie **Geofence hinzufügen**, um einen neuen Eintrag zu erstellen. Jedes Geofence enthält diese Hauptfelder:

- **Name**: erforderlich und eindeutig.
- **Latitude** und **Longitude**: der Mittelpunkt des Bereichs.
- **Radius (m)**: erforderlich, von **100** bis **10000** Meter.
- **Beschreibung**: optionale Notizen für Administratoren.
- **Berichteingabe** und **Berichteausgang**: wählen Sie aus, welche Übergangsereignisse generiert werden sollen.
- **Aktiv**: aktiviert oder deaktiviert den geografischen Zaun, ohne ihn zu löschen.

> Mindestens eines von **Report enter** oder **Report exit** muss für jeden geografischen Zaun aktiviert bleiben.

Kartenbearbeitungswerkzeuge

Jede Geofence-Karte enthält eine Kartenansicht des Bereichs. Sie können die Geometrie direkt aus der Karte oder aus den numerischen Feldern bearbeiten.

- Klicken Sie auf die Karte, um den Geofence-Mittelpunkt zu verschieben, wenn die Bearbeitung des Bereichs freigeschaltet ist.
- Verwenden Sie die **Aktuelle Position** Schaltfläche, um die Karte auf Ihre aktuelle Browserposition zu zentrieren.

- Verwenden Sie die **Recenter map** Schaltfläche, um die bevorzugte Ansicht für dieses Geofence wiederherzustellen.
- Verwenden Sie die Schloss-Schaltfläche, um unbeabsichtigte Änderungen an der Geofence-Geometrie zu verhindern.

Wo Geofencedaten angezeigt werden

Geofence-Übergänge können im Android **Geräteübersicht** Seite, im **Geofence** Reiter des Standort-Panels gefunden werden. Dieser Reiter zeigt Übergänge auf einer speziellen Karte zusammen mit Filtertools und der Übergangsliste.

Benutzerverwaltung

Benutzer hinzufügen (deaktiviert)

Gibt an, ob das Hinzufügen neuer Benutzer und Profile deaktiviert ist. Bei Geräten, bei denen managementMode auf **DEVICE_OWNER** eingestellt ist, wird dieses Feld ignoriert, und der Benutzer darf keine Benutzer hinzufügen oder entfernen.

Kontenänderungen deaktiviert

Ob das Hinzufügen oder Entfernen von Konten deaktiviert ist.

Benutzeranmeldedaten-Konfiguration deaktiviert

Ob die Konfiguration der Benutzeranmeldedaten deaktiviert ist.

Benutzer deaktivieren entfernen

Ob das Entfernen anderer Benutzer deaktiviert ist.

Benutzer-Symbol festlegen deaktiviert

Ob das Ändern des Benutzer-Symbols deaktiviert ist.

Hintergrundbild festlegen deaktiviert

Ob das Ändern des Hintergrundbilds deaktiviert ist.

Authentifizierung für die Einrichtung des Arbeitskontos

Steuert, wie Benutzer bei der Einrichtung eines Arbeitskontos authentifiziert werden. Diese Option ist nur für Android-Unternehmensstrukturen verfügbar, die von einer verwalteten Google-Domain (Google Workspace) unterstützt werden.

Während der Gerätekonfiguration/Registrierung beeinflusst diese Richtlinie, ob eine Anmeldung für ein Arbeitskonto erforderlich ist, aber die Einstellung "**Authentifizierung mit Google**" in der Google Admin-Konsole sowie der Typ des Registrierungstokens können weiterhin eine Authentifizierung erfordern.

Für Geräte, die bereits registriert sind, gilt diese Richtlinie nur, wenn das Gerät über ein verwaltetes Google Play-Konto verwaltet wird (d. h. wenn es ohne **Authentifizierung mit Google** registriert wurde).

Für weitere Details und zur Fehlerbehebung, siehe **Authentifizierung mit Google**.

Blockierte Kontotypen

Kontotypen, die der Benutzer nicht verwalten kann. Diese Option verhindert, dass Benutzer Geräte nicht genehmigte Konten hinzufügen.

Verwenden Sie **Kontoart für Sperrung hinzufügen**, um eine oder mehrere Kontoarten hinzuzufügen.

Jeder Eintrag hat ein **Kontotypfeld** (erforderlich). Geben Sie eine Zeichenkette wie z. B. **com.google** ein. Entfernen Sie einen Eintrag mit der Löschfunktion.

Privatnutzung

Beim Bereitstellen eines dienstlich genutzten Geräts für Arbeit und Privat, können Sie bestimmte Regeln festlegen, um die Nutzung des Geräts durch den Benutzer außerhalb des Arbeitsbereichs einzuschränken.

> Dieser Abschnitt gilt nur für dienstlich genutzte Geräte mit Arbeitsprofil. Er hat keine Auswirkungen auf vollständig verwaltete oder privat genutzte Geräte.

1. Kamera deaktiviert

Ist die Kamera deaktiviert?

2. Bildschirmaufnahme deaktiviert

Ob die Bildschirmaufnahme deaktiviert ist.

3. Maximale Anzahl an Tagen mit Freizeitausgleich

Steuert, wie lange das Arbeits-Profil deaktiviert bleiben kann.

4. Bluetooth-Freigabe

Steuert, ob Bluetooth-Freigabe im persönlichen Profil eines geräteverwalteten Geräts mit einem Arbeitsbereich erlaubt ist.

5. Privater Bereich

Legt fest, ob auf dem Gerät ein privater Bereich erlaubt ist.

6. Play Store-Modus

Dieser Modus steuert, welche Apps für den Benutzer im Play Store des persönlichen Profils erlaubt oder blockiert sind.

> **Blacklist (Standard)**: Alle Apps sind verfügbar, und alle Apps, die nicht auf dem Gerät sein sollten, müssen explizit im Abschnitt **Anwendungen** als **Blockiert** markiert werden.
>
> **Allowlist**: Nur Anwendungen, die explizit im Abschnitt **Anwendungen** angegeben sind und bei denen der **Installationsmodus** auf **Verfügbar** eingestellt ist, dürfen im persönlichen Profil installiert werden.

7. Anwendungen

Liste der Anwendungen, die im persönlichen Profil erlaubt oder gesperrt werden müssen. Das Verhalten der Liste hängt vom Wert ab, der für **Installationsmodus** eingestellt ist.

Um eine neue App aus dem Play Store hinzuzufügen, klicken Sie auf das **+**-Symbol.

7.1. Installationsart

Arten von Installationsverhalten, die eine persönliche Profil-Anwendung haben kann.

> **Blockiert**: Die App ist gesperrt und kann nicht im persönlichen Profil installiert werden.
>
> **Verfügbar**: Die App kann im persönlichen Profil installiert werden.

8. Blockierte Kontotypen

Kontotypen, die der Benutzer nicht verwalten kann. Diese Option verhindert, dass Gerätebenutzer nicht genehmigte Konten in ihrem persönlichen Profil hinzufügen.

Richtlinien für mehrere Profile

Gilt nur für Geräte mit persönlichem und geschäftlichem Profil.

Kopieren und Einfügen zwischen Profilen

Ob Text, der aus einem Profil (privat oder geschäftlich) kopiert wurde, in das andere Profil eingefügt werden kann.

> **Nicht erlaubt (Standard)**: Verhindert, dass Benutzer Text, der aus dem Arbeits-Profil kopiert wurde, in das persönliche Profil einfügen. Text, der aus dem persönlichen Profil kopiert wurde, kann in das Arbeits-Profil eingefügt werden.
>
> **Erlaubt**: Text, der in einem der Profile kopiert wurde, kann in das andere Profil eingefügt werden.

Datenaustausch zwischen Profilen

Legt fest, ob Daten von einem Profil (privat oder geschäftlich) mit Apps im anderen Profil geteilt werden können. Steuert insbesondere den einfachen Datenaustausch über Intents. Die Verwaltung anderer Kommunikationskanäle zwischen Profilen, wie z. B. Kontaktsuche, Kopieren/Einfügen oder verbundene geschäftliche und private Apps, wird separat konfiguriert.

> **Nicht zulässig**: Verhindert den Datenaustausch sowohl vom privaten Profil zum geschäftlichen Profil als auch vom geschäftlichen Profil zum privaten Profil.
>
> **Datenübertragung vom Unternehmensprofil zum privaten Profil nicht zulässig (Standard)**: Verhindert, dass Benutzer Daten vom Unternehmensprofil an Apps im privaten Profil weitergeben. Persönliche Daten können mit Unternehmens-Apps geteilt werden.
>
> **Erlaubt**: Daten können von jedem Profil mit dem anderen Profil geteilt werden.

Standardmäßig werden Widgets für das Arbeitsbereichsprofil angezeigt

Standardverhalten für Widgets im Arbeitsbereich. Wenn eine bestimmte App keine Widget-Richtlinie definiert, wird die hier festgelegte Standardeinstellung verwendet.

Funktionen von Apps, die mehrere Profile nutzen

Steuert, ob Apps im persönlichen Profil Funktionen von Apps im Arbeitsbereich aufrufen können. Dies erfordert Android 16 oder höher.

> Diese Einstellung hängt von der auf Richtlinien-Ebene festgelegten Option **App-Funktionen** ab (im Bereich App-Verwaltung). Wenn "App-Funktionen" auf **Nicht zulässig** eingestellt ist, lehnt die API App-Funktionen zwischen Profilen ab, die auf **Zulässig** eingestellt sind.

Kontakte aus dem Arbeitsbereich im persönlichen Profil

Ob Kontakte, die im Arbeitsbereich gespeichert sind, in den Kontaktsuchen und eingehenden Anrufen des persönlichen Profils angezeigt werden können.

Erlaubt (Standard): Ermöglicht die Anzeige von Kontakten des Arbeitsbereichs im persönlichen Profil.

Deaktiviert: Verhindert, dass persönliche Apps auf Kontakte des Arbeitsbereichs zugreifen und diese suchen können.

Nicht erlaubt, außer für System-Anwendungen: Verhindert, dass die meisten privaten Apps auf Kontakte des Arbeitsbereichsprofils zugreifen, außer für die Standard-Telefon-, Nachrichten- und Kontakte-Apps des Geräteherstellers (Android 14+).

Wenn die Kontakte für den Arbeitsbereich im persönlichen Profil konfiguriert sind, können Sie optional eine Liste von **ausgenommenen Paketnamen** definieren. Je nach ausgewähltem Modus verhalten sich diese Ausnahmen wie eine Zulassungs- oder Sperrliste für persönliche Apps.

Statusberichte

In diesem Abschnitt können Sie konfigurieren, welche Daten vom Gerät abgerufen werden sollen.

Die Statusdaten können im **Gerätestatus**-Dashboard angezeigt werden.

Anwendungsberichte

Sind Anwendungsberichte aktiviert? (Informationen über installierte Anwendungen werden angezeigt.)

> Diese Option ist vom System erforderlich (für die Integration mit der Begleit-App) und ist immer aktiviert; sie kann nicht deaktiviert werden.

Entfernte Apps einschließen

Ob entfernte Apps in den App-Berichten enthalten sind.

Geräteeinstellungen

Ob die Berichterstellung für Geräte-Einstellungen aktiviert ist. (Informationen zu sicherheitsrelevanten Geräte-Einstellungen auf dem Gerät.)

Software-Informationen

Ob die Berichterstattung über Software-Informationen aktiviert ist. (Informationen zur Software des Geräts.)

Speicherinformationen

Ist die Speicherberichterstattung aktiviert? (Ein Ereignis im Zusammenhang mit Speicher- und Speichermessungen.)

Netzwerkinformationen

Ob die Berichterstellung von Netzwerkinformationen aktiviert ist. (Netzwerkinformationen des Geräts.)

Information anzeigen

Ob die Anzeige von Berichten aktiviert ist. Berichtsdaten sind für persönlich genutzte Geräte mit Arbeitsumgebungen nicht verfügbar. (Anzeigeinformationen des Geräts.)

Energieverwaltungsereignisse

Ob die Berichterstellung von Energieverwaltungsereignissen aktiviert ist. Daten sind für privat genutzte Geräte mit Arbeits-Profilen nicht verfügbar.

Gerätestatus

Ob die Statusberichte für die Hardware aktiviert sind. Daten für Geräte, die sich im privaten Besitz befinden und nur ein Arbeitsbereich haben, sind nicht verfügbar.

Systemeigenschaften

Ob die Berichterstellung von Systemeigenschaften aktiviert ist.

Modus für Common Criteria

Ob die Berichterstellung im Common Criteria Modus aktiviert ist.

Sonstiges

1. Osterei-Spiel deaktiviert

Ob das Osterei-Spiel in den Einstellungen deaktiviert ist.

2. Erste Bedienungshinweise überspringen

Flag, um Hinweise beim ersten Gebrauch zu überspringen. Enterprise-Administratoren können die Systemempfehlung aktivieren, damit Apps ihr Benutzer-Tutorial und andere Einführungshinweise beim ersten Start überspringen.

3. Kurze Support-Nachricht

Eine Nachricht, die dem Benutzer im Einstellungsbereich angezeigt wird, wenn eine Funktion vom Administrator deaktiviert wurde. Wenn die Nachricht länger als 200 Zeichen ist, kann sie abgeschnitten werden.

4. Längere Supportmeldung

Eine Nachricht, die dem Benutzer im Bereich "Geräteadministratoren-Einstellungen" angezeigt wird.

5. Informationen zur Sperre durch den Gerätebesitzer

Informationen zum Gerätebesitzer, die auf dem Sperrbildschirm angezeigt werden.

6. Einrichtungsschritte

Aktionen, die während des Einrichtungsprozesses ausgeführt werden. Während der Registrierung können Sie den Benutzer auffordern, eine oder mehrere Apps zu öffnen, die für die Gerätekonfiguration erforderlich sind.

Verwenden Sie die Option **Aktion zum Hinzufügen einrichten**, um Einträge zu erstellen, und entfernen Sie sie mit der Löschaktion.

6.1. App starten

Paketname der zu startenden App

6.2. Titel

Zeigt eine Nachricht für den Benutzer an, um zu erklären, warum die App gestartet werden muss.

6.3. Beschreibung

Zeigt eine Nachricht für den Benutzer an, um zu erklären, warum die App gestartet werden muss.

7. Sichtbarkeit des Anzeigenamens für Unternehmen

Steuert, ob der Anzeigename des Unternehmens auf dem Gerät sichtbar ist (z. B. als Nachricht auf dem Sperrbildschirm bei geräteverwalteten Geräten).

Sichtbar (Standard): Der Anzeigename des Unternehmens ist auf dem Gerät sichtbar (wird auf Work Profiles unter Android 7+ und auf vollständig verwalteten Geräten unter Android 8+ unterstützt).

Versteckt: Der Anzeigename des Unternehmens ist auf dem Gerät ausgeblendet.

Regeln zur Durchsetzung von Richtlinien

Wenn ein Gerät oder ein Arbeitsbereich nicht mit einer der unten aufgeführten Richtlinien übereinstimmt, blockiert Android Device Policy standardmäßig die Nutzung des Geräts oder des Arbeitsbereichs

- **Passwortanforderungen**
- **Verschlüsselungsrichtlinie**
- **Keyguard deaktiviert**
- **Erlaubte Eingabemethoden**
- **Erlaubte Bedienhilfen**

Wenn das Gerät oder das Arbeitskonto auch nach 10 Tagen nicht mehr den Richtlinien entspricht, setzt die Android-Geräterichtlinie das Gerät auf die Werkseinstellungen zurück oder löscht das Arbeitskonto.

In diesem Abschnitt können Sie die Standard-Richtlinien für die Durchsetzung der Compliance außer Kraft setzen oder neue hinzufügen.

Regeln

Liste der Regeln, die das Verhalten definieren, wenn eine bestimmte Richtlinie nicht auf ein Gerät angewendet werden kann.

Verwenden Sie **Regel hinzufügen**, um eine neue Regel zu erstellen. Jede Regelkarte kann mit der Löschfunktion entfernt werden.

Name der Einstellung

Die Top-Level-Richtlinie, die durchgesetzt werden soll. Zum Beispiel **Anwendungen** oder **Passwortrichtlinien**.

Erforderlich. Der Wert muss mit einem unterstützten, übergeordneten Richtliniennamen übereinstimmen; andernfalls wird das Feld als ungültig markiert.

Sperren nach Tagen

Anzahl der Tage, nach denen ein Gerät oder ein Arbeitsbereich gesperrt wird, wenn die Richtlinie nicht eingehalten wird. Um den Zugriff sofort zu sperren, setzen Sie den Wert auf 0. "**Sperren nach Tagen**" muss kleiner sein als "**Löschen nach Tagen**". Gilt nur für Geräte, die dem Unternehmen gehören.

Erlaubter Bereich: 0–300.

Block-Scope

Definiert den Gültigkeitsbereich einer Blockaktion. Nur für firmeneigene Geräte anwendbar.

Standard (neue Regel): **Arbeitsprofil**.

> **Arbeitsprofil**: Die Blockierungsaktion wird nur auf Apps im Arbeitsprofil angewendet. Apps im privaten Profil sind nicht betroffen.
>
> **Gesamtes Gerät**: Die Blockieraktion wird für das gesamte Gerät angewendet, einschließlich der Apps im persönlichen Profil.

Daten löschen nach Tagen

Anzahl der Tage, an denen ein Gerät oder ein Arbeitsbereich nicht den Richtlinien entspricht, bevor es gelöscht wird.
Anzahl der Tage bis zum Löschen muss größer sein als **Anzahl der Tage bis zur Sperrung**. Nur für von der Firma gestellte Geräte gültig.

Erforderlich. Standardwert (neue Regel): **1**.

Erlaubter Bereich: 1–300.

Werksseitigen Schutz beibehalten

Ob die Daten zum Werksreset-Schutz auf dem Gerät gespeichert bleiben. Diese Einstellung gilt nicht für Arbeitsprofile.

Standard (neue Regel): aktiviert.