Richtlinien - Android

- Zusammenfassung
- App-Verwaltung
- Kioskmodus
- Sicherheit
- Multimedia
- Mobilfunk
- Netzwerk
- System
- Standort und Geofences
- Benutzerverwaltung
- Private Nutzung
- Profilübergreifende Richtlinien
- Statusberichte
- Sonstiges
- Compliance-Regeln

Zusammenfassung

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

Sie können Ihre Richtlinien im Bereich **Richtlinien** des Dashboards durchsuchen und neue erstellen. Um eine Android-Richtlinie zu öffnen, klicken Sie auf die Richtlinienzeile in der Tabelle: Das System öffnet die Seite **Richtlinieneditor**.

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

> Jedes Gerät kann jeweils nur einer Richtlinie zugeordnet werden.

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

Aufbau des Richtlinieneditors

Der Richtlinieneditor ist als Reihe aufklappbarer Abschnitte organisiert. Am oberen Rand der Seite können Sie jederzeit Folgendes bearbeiten:

- **Name** (erforderlich)
- **Id** (schreibgeschützt)
- **Beschreibung** (optional)

Die folgenden Abschnitte entsprechen den Bereichen des Richtlinieneditors (zum Beispiel: App-Verwaltung, Sicherheit, Netzwerk, System, Private Nutzung, Profilübergreifende Richtlinien und mehr). Wenn Sie eine gespeicherte Richtlinie öffnen, sind die Abschnitte mit geänderten Einstellungen bereits geöffnet, die übrigen bleiben geschlossen. Verwenden Sie die Kapitelseiten dieses Handbuchs, um jeden Bereich im Detail zu verstehen.

Speichern, Löschen und zugeordnete Geräte

Verwenden Sie **Richtlinie speichern**, um Ihre Änderungen anzuwenden. Die Schaltfläche ist deaktiviert, wenn keine ausstehenden Änderungen vorhanden sind oder wenn die Lizenz abgelaufen ist.

Wenn Sie eine vorhandene Richtlinie geöffnet haben (sie hat eine Id), zeigt die Seite unten eine Aktion **Richtlinie löschen** und eine Liste **Zugeordnete Geräte** an, sodass Sie sehen können, wie viele Geräte die Richtlinie derzeit verwenden.

App-Verwaltung

In diesem Bereich können Sie Richtlinien zu App-Verfügbarkeit, Installation, Updates und Berechtigungsverwaltung festlegen.

> Managed Google Play-Konten werden automatisch erstellt, wenn Geräte bereitgestellt werden.

1. Play Store-Modus

Dieser Modus steuert, welche Apps dem Benutzer im Play Store zur Verfügung stehen, und das Verhalten auf dem Gerät, wenn Apps aus der Richtlinie entfernt werden.

> **Whitelist (Standard)**: Nur Apps, die in der Richtlinie enthalten sind, stehen zur Verfügung, und jede App, die nicht in der Richtlinie enthalten ist, wird automatisch vom Gerät deinstalliert. Der Play Store zeigt nur verfügbare Apps an.
>
> **Blacklist**: Alle Apps sind verfügbar, und jede App, die nicht auf dem Gerät sein sollte, muss in der Anwendungsrichtlinie explizit als **blockiert** markiert werden. Der Play Store zeigt alle Apps außer blockierten an.

2. Richtlinie für nicht vertrauenswürdige Apps

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

> **Nicht zulassen (Standard)**: Nicht vertrauenswürdige App-Installationen auf dem gesamten Gerät nicht zulassen.
>
> **Nur persönliches Profil**: Bei Geräten mit Arbeitsprofilen nicht vertrauenswürdige App-Installationen nur im persönlichen Profil des Geräts zulassen.
>
> **Zulassen**: Nicht vertrauenswürdige App-Installationen auf dem gesamten Gerät zulassen.

3. Google Play Protect

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

Erzwungen (Standard): Erzwingt die App-Überprüfung.

Benutzerauswahl: Ermöglicht dem Benutzer zu wählen, ob die App-Überprüfung aktiviert wird.

4. Standard-Berechtigungsrichtlinie

Die Richtlinie zum Erteilen von Laufzeitberechtigungsanfragen für Apps.

Abfragen (Standard): Den Benutzer auffordern, eine Berechtigung zu erteilen.

Erteilen: Eine Berechtigung automatisch erteilen.

Verweigern: Eine Berechtigung automatisch verweigern.

5. App-Funktionen

Steuert, ob Apps auf vollständig verwalteten Geräten oder in Arbeitsprofilen App-Funktionen bereitstellen dürfen. Erfordert Android 16 oder höher.

Zugelassen (Standard): Apps auf vollständig verwalteten Geräten oder in Arbeitsprofilen können App-Funktionen bereitstellen.

Nicht zugelassen: Apps auf vollständig verwalteten Geräten oder in Arbeitsprofilen können keine App-Funktionen bereitstellen.

6. Installation von Apps deaktiviert

Ob die Installation von Apps durch den Benutzer deaktiviert ist.

7. Deinstallation von Apps deaktiviert

Ob die Deinstallation von Anwendungen durch den Benutzer deaktiviert ist.

8. Berechtigungsrichtlinien

Explizite Erteilungen oder Verweigerungen von Berechtigungen oder Gruppen für alle Apps. Diese Werte überschreiben die Einstellung **Standard-Berechtigungsrichtlinie**.

Verwenden Sie **Berechtigungsrichtlinie hinzufügen**, um Einträge zu erstellen, und entfernen Sie sie mit der Löschaktion.

Jeder Eintrag enthält:

> **Android-Berechtigung/-gruppe**: Die Android-Berechtigung oder -gruppe (erforderlich), zum Beispiel **android.permission.READ_CALENDAR** oder **android.permission_group.CALENDAR**.
>
> **Richtlinie**: Erteilen / Verweigern / Abfragen (verwendet dieselben Richtlinienoptionen wie **Standard-Berechtigungsrichtlinie**).

9. Anwendungen

Liste der Anwendungen, die in der Richtlinie enthalten sein müssen. Das Verhalten des Listeninhalts hängt vom Wert ab, der für **Play Store-Modus** festgelegt ist.

Wenn **Play Store-Modus** auf **Whitelist** festgelegt ist, stehen nur Apps zur Verfügung, die in der Richtlinie enthalten sind, und jede App, die nicht in der Richtlinie enthalten ist, wird automatisch vom Gerät deinstalliert.

Wenn **Play Store-Modus** auf **Blacklist** festgelegt ist, sind alle Apps verfügbar, und jede App, die nicht auf dem Gerät sein sollte, muss in der Anwendungsrichtlinie explizit als **blockiert** markiert werden.

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

Um eine App hinzuzufügen, die nicht bei Google Play veröffentlicht, aber bereits auf dem Gerät vorhanden ist (zum Beispiel eine System- oder Hersteller-App), klicken Sie auf **Apps hinzufügen**, wählen Sie **Nach Paketnamen (vorinstallierte Apps)**, geben Sie den Paketnamen der App ein (z. B. **com.example.app**) und klicken Sie auf **Hinzufügen**.Die App wird mit dem Installationstyp **Erzwungen installiert** hinzugefügt. Damit die App im benutzerdefinierten Kiosk-Launcher angezeigt wird, muss der **Installationstyp** auf **Vorinstalliert** oder **Erzwungen installiert** gesetzt sein: Bei **Verfügbar** wird die App nicht angezeigt.

> Apps, die auf Managed Google Play nicht verfügbar sind, werden in der Anwendungsliste mit einem Android-Symbol markiert. Sie können nicht über Google Play installiert werden und müssen daher bereits auf dem Gerät vorhanden sein: Geräte, auf denen die App nicht vorhanden ist, können sie nicht installieren.

>

> Alle Apps, die im Play Store in Ihrem Land veröffentlicht sind, stehen standardmäßig zur Auswahl. Um Ihre eigenen privaten oder Web-Apps auszuwählen, müssen Sie sie zuerst im System hochladen. Weitere Informationen finden Sie auf der Seite **Private Apps**.

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

9.1. Installationstyp

Der für eine App auszuführende Installationstyp.

Verfügbar: Die App steht zur Installation zur Verfügung.

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

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

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

Für die Einrichtung erforderlich: Die App wird automatisch installiert und kann vom Benutzer nicht entfernt werden; sie verhindert den Abschluss der Einrichtung, bis die Installation abgeschlossen ist.

Kiosk: Die App wird automatisch im Kioskmodus installiert: Sie wird als bevorzugter Home-Intent festgelegt und für den Lock-Task-Modus auf die Whitelist gesetzt. Die Geräteeinrichtung wird erst abgeschlossen, wenn die App installiert ist. Nach der Installation können Benutzer die App nicht entfernen. Sie können diesen **Installationstyp** nur für eine App pro Richtlinie festlegen. Wenn dies in der Richtlinie vorhanden ist, wird die Statusleiste automatisch deaktiviert. Weitere Informationen finden Sie auf der speziellen Seite **Kioskmodus**.

9.2. Installationsbeschränkungen

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

> Diese Option wird nur angezeigt, wenn der **Installationstyp** auf **Vorinstalliert** oder **Erzwungen installiert** gesetzt ist.

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

Aufladen: Installieren Sie die App nur, wenn das Gerät lädt.

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

9.3. Auto-Update-Modus

Steuert den Auto-Update-Modus für die App.

Standard: Die App wird automatisch mit niedriger 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 verwendet, (2) das Gerät ist mit einem unbegrenzten Netzwerk verbunden, (3) das Gerät lädt. Das Gerät wird innerhalb von 24 Stunden, nachdem der Entwickler ein neues Update veröffentlicht hat, darüber benachrichtigt; danach wird die App beim nächsten Erfüllen der obigen Bedingungen aktualisiert.

Zurückgestellt: Die App wird nach dem Veralten maximal 90 Tage lang nicht automatisch aktualisiert. 90 Tage nachdem die App veraltet ist, wird die neueste verfügbare Version automatisch mit niedriger Priorität installiert (siehe **Standard** Auto-Update-Modus). Nach der Aktualisierung wird die App erst wieder automatisch aktualisiert, wenn erneut 90 Tage nach dem Veralten vergangen sind. Der Benutzer kann die App jederzeit weiterhin manuell im Play Store aktualisieren.

Hohe Priorität: Die App wird so bald wie möglich aktualisiert. Es werden keine Bedingungen angewendet. Das Gerät wird sofort über ein neues Update benachrichtigt, sobald es verfügbar ist.

9.4. Mindestversionscode

Die Mindestversion der App, die auf dem Gerät ausgeführt wird. Wenn festgelegt, versucht das Gerät, die App auf mindestens diesen Versionscode zu aktualisieren. Wenn die App nicht aktuell ist, enthält das Gerät ein **Detail zur Nichtkonformität** mit **Grund der Nichtkonformität** auf **APP_NOT_UPDATED**. Die App muss bereits bei Google Play mit einem Versionscode größer oder gleich diesem Wert veröffentlicht sein. Höchstens 20 Apps können pro Richtlinie einen Mindestversionscode angeben.

9.5. Delegierte Scopes

Die von Android Device Policy an die App delegierten Scopes. Sie können anderen Apps eine Auswahl spezieller Android-Berechtigungen erteilen:

Zertifikatinstallation: Gewährt Zugriff auf die Installation und Verwaltung von Zertifikaten.

Verwaltete Konfigurationen: Gewährt Zugriff auf die Verwaltung verwalteter Konfigurationen.

Deinstallation blockieren: Gewährt Zugriff auf das Blockieren der Deinstallation.

Berechtigungen: Gewährt Zugriff auf die Berechtigungsrichtlinie und den Status der Berechtigungserteilung.

Paketzugriff: Gewährt Zugriff auf den Paketzugriffsstatus.

System-App: Gewährt Zugriff zum Aktivieren von System-Apps.

9.6. Bevorzugtes Netzwerk

Der bevorzugte Netzwerkdienst, der für diese App verwendet werden soll. Wenn festgelegt, verwendet die App den angegebenen Enterprise-Netzwerk-Slice für ihre Verbindungen, sofern verfügbar. Dieser muss mit einem Netzwerk-Slice übereinstimmen, der im Bereich **5G-Netzwerk-Slicing-Konfiguration** des Panels **Mobilfunk** konfiguriert ist.

9.7. Standard-Berechtigungsrichtlinie

Die Standardrichtlinie für alle von der App angeforderten Berechtigungen. Wenn angegeben, überschreibt sie die richtlinienweite **Standard-Berechtigungsrichtlinie**, die für alle Apps gilt. Sie überschreibt nicht die **Berechtigungsrichtlinien**, die für alle Apps gelten.

Abfragen (Standard): Den Benutzer auffordern, eine Berechtigung zu erteilen.

Erteilen: Eine Berechtigung automatisch erteilen.

Verweigern: Eine Berechtigung automatisch verweigern.

9.8. Verbundene Arbeits- und private App

Steuert, ob die App über die Arbeits- und privaten Profile eines Geräts hinweg mit sich selbst kommunizieren kann, vorbehaltlich der Zustimmung des Benutzers (Android 11+).

Nicht zugelassen (Standard): Verhindert, dass die App profilübergreifend kommuniziert.

Zugelassen: Ermöglicht der App, nach Erhalt der Benutzerzustimmung profilübergreifend zu kommunizieren.

9.9. Ausnahme vom Always-On-VPN-Sperrmodus

Gibt an, ob der App Netzwerkzugriff erlaubt ist, wenn das VPN nicht verbunden ist und **Sperrmodus aktiviert** aktiv ist. Wird nur auf Geräten mit Android 10 oder höher unterstützt.

Erzwungen (Standard): Die App beachtet die Always-On-VPN-Sperrmoduseinstellung.

Ausgenommen: Die App ist von der Always-On-VPN-Sperrmoduseinstellung ausgenommen.

9.10. Arbeitsprofil-Widgets

Gibt an, ob die im Arbeitsprofil installierte App Widgets zum Home-Bildschirm hinzufügen darf.

Zugelassen: Die Anwendung kann Widgets zum Home-Bildschirm hinzufügen.

Nicht zugelassen: Die Anwendung kann keine Widgets zum Home-Bildschirm hinzufügen.

9.11. Benutzersteuerungseinstellungen

Gibt an, ob die Benutzersteuerung für eine bestimmte App zulässig ist. Die Benutzersteuerung umfasst Benutzeraktionen wie das Erzwingen des Beendens und das Löschen von App-Daten (Android 11+). Wenn **extensionConfig** für eine App aktiviert ist, ist die Benutzersteuerung unabhängig von dieser Einstellung nicht zulässig. Für Kiosk-Apps können Sie **Zugelassen** verwenden, um die Benutzersteuerung zu erlauben.

Nicht angegeben: Verwendet das Standardverhalten der App, um zu bestimmen, ob die Benutzersteuerung zulässig ist oder nicht.

Zugelassen: Die Benutzersteuerung ist für die App zulässig.

Nicht zugelassen: Die Benutzersteuerung ist für die App nicht zulässig.

9.12. Deaktiviert

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

9.13. Anmeldedatenanbieter zulassen

Ob die App unter Android 14 und höher als Anmeldedatenanbieter fungieren darf.

9.14. Verwaltete Konfiguration

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 die Konfiguration mit der Schaltfläche **Verwaltete Konfiguration** ändern oder sie mit der Schaltfläche **Konfiguration entfernen** löschen.

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

9.15. Berechtigungsrichtlinien

Explizite Erteilungen oder Verweigerungen von Berechtigungen für die App. Diese Werte überschreiben die **Standard-Berechtigungsrichtlinie** und die **Berechtigungsrichtlinien**, die für alle Apps gelten.

Verwenden Sie **Berechtigungsrichtlinie hinzufügen**, um eine oder mehrere Berechtigungsregeln für die App-Karte hinzuzufügen, und entfernen Sie sie mit der Löschaktion.

9.16. Track-IDs

Liste der IDs der geschlossenen Test-Tracks der App, auf die ein Gerät zugreifen kann. Wenn mehrere Track-IDs ausgewählt sind, erhalten Geräte die neueste Version aller zugänglichen Tracks. Wenn keine Track-ID ausgewählt ist, haben Geräte nur Zugriff auf den Produktions-Track der App.

> Die Option **Track-IDs** ist nur für Apps verfügbar, die mindestens eine Track-ID für Ihre Organisation haben. Weitere Informationen zum Hinzufügen Ihrer Organisation zu einem geschlossenen Test-Track für eine bestimmte App finden Sie hier.

10. Standardanwendungseinstellungen

Legen Sie Standard-Apps für unterstützte Typen fest. Wenn für mindestens einen Typ eine Standard-App festgelegt ist, können Benutzer die Standard-Apps in diesem Profil nicht ändern.

> Pro **Standardanwendungstyp** ist nur eine Standardanwendungseinstellung zulässig. Die Liste der Standardanwendungen darf keine Duplikate enthalten.

10.1. Standardanwendungstyp

Wählen Sie die zu konfigurierende App-Kategorie aus (zum Beispiel Browser, Telefon, SMS, Wallet oder Assistant). Die Verfügbarkeit hängt von der Android-Version und dem Verwaltungsmodus ab.

10.2. Standardanwendungsbereiche

Wählen Sie aus, wo die Standard-App gelten soll (Vollständig verwaltet, Arbeitsprofil oder Persönliches Profil). Es können nur Bereiche ausgewählt werden, die vom gewählten Typ unterstützt werden.

> Wenn keiner der ausgewählten Bereiche auf den Verwaltungsmodus des Geräts anwendbar ist, meldet das Gerät ein Detail zur Nichteinhaltung.

10.3. Standardanwendungen

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

>

> Wenn die Bereiche**Vollständig verwaltet** oder **Arbeitsprofil** umfassen, muss jede App auch in der Liste **Anwendungen** mit einem **Installationstyp** vorhanden sein, der nicht auf **Blockiert** gesetzt ist.

11. Auswahl des privaten Schlüssels

Ermöglicht die Anzeige einer Benutzeroberfläche auf einem Gerät, damit der Benutzer einen privaten Schlüsselalias auswählen kann, wenn keine passenden Regeln in **Regeln für die Auswahl privater Schlüssel** vorhanden sind.

> Bei Geräten unter Android P kann diese Einstellung Unternehmensschlüssel anfällig machen.

12. Regeln für die Auswahl privater Schlüssel

Steuert den Zugriff von Apps auf private Schlüssel. Die Regel bestimmt, welchen privaten Schlüssel Android Device Policy der angegebenen App gegebenenfalls gewährt. Der Zugriff wird entweder gewährt, wenn die App KeyChain.choosePrivateKeyAlias (oder Überladungen davon) aufruft, um einen privaten Schlüsselalias für eine bestimmte URL anzufordern, oder bei Regeln, die nicht URL-spezifisch sind (d. h., wenn urlPattern nicht festgelegt oder auf die leere Zeichenfolge oder .* gesetzt ist), unter Android 11 und höher direkt, sodass die App KeyChain.getPrivateKey aufrufen kann, ohne zuerst KeyChain.choosePrivateKeyAlias aufrufen zu müssen. Wenn eine App KeyChain.choosePrivateKeyAlias aufruft und mehr als eine choosePrivateKeyRules-Regel übereinstimmt, legt die letzte übereinstimmende Regel fest, welcher Schlüsselalias zurückgegeben wird.

Verwenden Sie **Private-Schlüssel-Regel hinzufügen**, um Einträge zu erstellen, und entfernen Sie sie mit der Löschaktion.

12.1. Alias des privaten Schlüssels

Der Alias des zu verwendenden privaten Schlüssels.

12.2. URL-Muster

Das URL-Muster, das mit der URL der Anfrage abgeglichen wird. Wenn nicht festgelegt oder leer, stimmt es mit allen URLs überein. Es verwendet die Syntax regulärer Ausdrücke von java.util.regex.Pattern.

12.3. Paketnamen

Die Paketnamen, für die diese Regel gilt. Der Hash des Signaturzertifikats jeder App wird mit dem von Play bereitgestellten Hash abgeglichen. Wenn keine Paketnamen angegeben sind, wird der Alias allen Apps bereitgestellt, die KeyChain.choosePrivateKeyAlias oder Überladungen davon aufrufen (jedoch nicht ohne Aufruf von KeyChain.choosePrivateKeyAlias, auch nicht unter Android 11 und höher). Jede App mit derselben Android-UID wie ein hier angegebenes Paket hat Zugriff, wenn sie KeyChain.choosePrivateKeyAlias aufruft.

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

> Um eine App zu löschen, klicken Sie auf das Symbol **Papierkorb** unten auf der Karte der App.

Kioskmodus

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

Im **Einzel-App-Kioskmodus** wird ein Gerät für eine einzelne Anwendung konfiguriert, und Endbenutzern ist der Zugriff auf andere Apps auf dem Gerät nicht gestattet. Sie können die App auch nicht beenden, wodurch das Gerät zu einem dedizierten Gerät für diese bestimmte App wird.

Um diesen Modus zu aktivieren, geben Sie eine App im Abschnitt **App-Verwaltung** an, wobei **Installationstyp** auf **Kiosk** gesetzt ist.

Im **Multi-App-Kioskmodus** dürfen Geräte auf mehrere Anwendungen zugreifen. Endbenutzer können über einen 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 außerdem konfigurieren, ob Endbenutzer auf bestimmte Systemfunktionen wie Systemeinstellungen und die Statusleiste zugreifen können.

Benutzerdefinierter Kiosk-Launcher

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

Aktionen der Power-Taste

Legt das Verhalten eines Geräts im Kioskmodus fest, wenn ein Benutzer die Power-Taste gedrückt hält (lange drückt).

> **Verfügbar (Standard)**: Das Power-Menü (z. B. Ausschalten, Neustart) wird angezeigt, wenn ein Benutzer die Power-Taste eines Geräts im Kioskmodus lange drückt.
>
> **Blockiert**: Das Power-Menü (z. B. Ausschalten, Neustart) wird nicht angezeigt, wenn ein Benutzer die Power-Taste eines Geräts im Kioskmodus lange drückt. Hinweis: Dies kann Benutzer daran hindern, das Gerät auszuschalten.

Warnungen bei Systemfehlern

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

Blockiert (Standard): Alle Systemfehlerdialoge wie Absturz und App reagiert nicht (ANR) werden blockiert. Wenn sie blockiert werden, beendet das System die App zwangsweise, als ob der Benutzer die App über die Benutzeroberfläche schließt.

Aktiviert: Alle Systemfehlerdialoge wie Absturz und App reagiert nicht (ANR) werden angezeigt.

Systemnavigation

Legt fest, welche Navigationsfunktionen (z. B. Start- und Übersicht-Schaltflächen) im Kioskmodus aktiviert sind.

Deaktiviert (Standard): Die Start- und Übersicht-Schaltflächen sind nicht zugänglich.

Nur Start: Nur die Start-Schaltfläche ist aktiviert.

Aktiviert: Die Start- und Übersicht-Schaltflächen sind aktiviert.

Statusleiste

Legt fest, ob Systeminformationen und Benachrichtigungen im Kioskmodus deaktiviert sind.

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

Nur System: In der Statusleiste werden nur Systeminformationen angezeigt.

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

Geräteeinstellungen

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

Zulässig (Standard): Der Zugriff auf die App „Einstellungen“ ist im Kioskmodus zulässig.

Blockiert: Der Zugriff auf die App „Einstellungen“ ist im Kioskmodus nicht zulässig.

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.

Multimedia

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

1. Kamerazugriff

Steuert die Nutzung der Kamera und ob der Benutzer auf den Umschalter für den Kamerazugriff zugreifen kann (Android 12+). Im Allgemeinen gilt das Deaktivieren der Kamera auf vollständig verwalteten Geräten geräteweit und auf Arbeitsprofilgeräten nur innerhalb des Arbeitsprofils.

> **Benutzerauswahl (Standard)**: Standardverhalten des Geräts. Kameras sind verfügbar und (Android 12+) kann der Benutzer den Kamerazugriff umschalten.
>
> **Deaktiviert**: Alle Kameras sind deaktiviert (vollständig verwaltet: geräteweit; Arbeitsprofil: nur für Apps im Arbeitsprofil). Der Umschalter für den Kamerazugriff hat im verwalteten Bereich keine Wirkung.
>
> **Erzwungen**: Kameras sind verfügbar. Auf vollständig verwalteten Geräten mit Android 12+ kann der Benutzer den Kamerazugriff nicht umschalten. Auf anderen Geräten/Versionen verhält sich dies wie Benutzerauswahl.

2. Mikrofonzugriff

Steuert auf vollständig verwalteten Geräten die Nutzung des Mikrofons und ob der Benutzer auf den Umschalter für den Mikrofonzugriff zugreifen kann (Android 12+). Diese Einstellung hat keine Wirkung auf Geräten, die nicht vollständig verwaltet sind.

> **Benutzerauswahl (Standard)**: Standardverhalten. Das Mikrofon ist verfügbar und (Android 12+) kann der Benutzer den Mikrofonzugriff umschalten.
>
> **Deaktiviert**: Das Mikrofon ist deaktiviert (geräteweit). Der Umschalter für den Mikrofonzugriff hat keine Wirkung.
>
> **Erzwungen**: Das Mikrofon ist verfügbar. Unter Android 12+ kann der Benutzer den Mikrofonzugriff nicht umschalten. Unter Android 11 oder älter verhält sich dies wie Benutzerauswahl.

3. USB-Datenzugriff

Steuert, welche Dateien und/oder Daten über USB übertragen werden können. Wird nur auf unternehmenseigenen Geräten unterstützt.

Dateiübertragung nicht zulassen (Standard): Dateiübertragungen sind nicht zulässig, andere USB-Datenverbindungen (z. B. Maus/Tastatur) sind jedoch zulässig.

Datenübertragung nicht zulassen: Alle Arten von USB-Datenübertragungen sind untersagt (Android 12+ mit USB HAL 1.3+). Wenn dies nicht unterstützt wird, fällt das Gerät auf „Dateiübertragung nicht zulassen“ zurück.

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

4. Drucken

Steuert, ob Drucken zulässig ist (Android 9+).

Zulässig (Standard): Drucken ist zulässig.

Nicht zulässig: Drucken ist nicht zulässig (Android 9+).

5. Bildschirmhelligkeitseinstellungen

Steuert den Bildschirmhelligkeitsmodus und (optional) den Helligkeitswert.

Bildschirmhelligkeitsmodus:

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

Automatisch: Die Helligkeit ist automatisch und der Benutzer kann sie nicht ändern. Sie können dennoch einen Helligkeitswert festlegen, der als Teil der automatischen Anpassung verwendet wird (vollständig verwaltet Android 9+; Arbeitsprofile auf unternehmenseigenen Geräten mit Android 15+).

Fest: Die Helligkeit wird auf den konfigurierten Wert gesetzt und der Benutzer kann sie nicht ändern. Der Helligkeitswert ist erforderlich (vollständig verwaltet Android 9+; Arbeitsprofile auf unternehmenseigenen Geräten mit Android 15+).

Bildschirmhelligkeit:

Wert von 1 bis 255 (1 = niedrigste, 255 = höchste). Der Wert 0 bedeutet, dass kein Helligkeitswert festgelegt ist.

6. Bildschirm-Timeout-Einstellungen

Steuert, ob der Benutzer das Bildschirm-Timeout konfigurieren kann und, wenn es erzwungen wird, den Timeout-Wert.

Das Feld **Bildschirm-Timeout-Modus** wählt zwischen benutzergesteuertem und erzwungenem Verhalten.

> **Benutzerauswahl (Standard)**: Der Benutzer darf das Bildschirm-Timeout konfigurieren.
>
> **Erzwungen**: Das Bildschirm-Timeout wird auf den konfigurierten Wert gesetzt und der Benutzer kann es nicht ändern (vollständig verwaltet Android 9+; Arbeitsprofile auf unternehmenseigenen Geräten mit Android 15+).

Bildschirm-Timeout:

> Timeout-Dauer in Sekunden. Der Wert muss größer als 0 sein. Wenn er größer als **Maximale Zeit bis zur Sperre** ist, kann das System ihn begrenzen und eine Nichteinhaltung melden.

7. Bildschirmaufnahme deaktiviert

Ob die Bildschirmaufnahme deaktiviert ist.

8. Lautstärkeanpassung deaktiviert

Ob die Anpassung der Hauptlautstärke deaktiviert ist.

9. Einhängen physischer Datenträger deaktiviert

Ob das Einhängen physischer externer Datenträger deaktiviert ist.

Mobilfunk

In diesem Bereich können Sie mobilfunkbezogene Richtlinien konfigurieren.

1. Flugmodus

Steuert, ob der Benutzer den Flugmodus umschalten kann.

> **Benutzerauswahl (Standard)**: Der Benutzer darf den Flugmodus ein- oder ausschalten.
>
> **Deaktiviert**: Der Flugmodus ist deaktiviert. Der Benutzer darf den Flugmodus nicht einschalten. Unterstützt ab Android 9.

2. Mobilfunk 2G

Steuert, ob der Benutzer die Mobilfunk-2G-Einstellung umschalten kann.

> **Benutzerauswahl (Standard)**: Der Benutzer darf Mobilfunk 2G ein- oder ausschalten.
>
> **Deaktiviert**: Mobilfunk 2G ist deaktiviert. Der Benutzer darf Mobilfunk 2G nicht über die Einstellungen einschalten. Unterstützt ab Android 14.

3. APNs überschreiben

Steuert, ob Override-APNs aktiviert oder deaktiviert sind. Wenn aktiviert, werden nur die konfigurierten Override-APNs verwendet und alle anderen APNs auf dem Gerät ignoriert.

> **Deaktiviert (Standard)**: Alle konfigurierten APN-Einstellungen werden auf dem Gerät gespeichert, sind jedoch deaktiviert und haben keine Wirkung. Alle anderen APNs auf dem Gerät bleiben in Verwendung.
>
> **Aktiviert**: Es werden nur die Override-APNs verwendet, alle anderen APNs 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 Pflichtfelder:

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

APN-Name: Die von Ihrem Mobilfunkanbieter bereitgestellte APN-Kennung.

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

Optionale APN-Felder:

Authentifizierungstyp, **Benutzername**, **Passwort**: Konfigurieren Sie die Anbieterauthentifizierung (falls erforderlich).

Protokoll und **Roaming-Protokoll**: IP-Protokollkonfiguration.

Netzwerktypen: Schränken Sie die Mobilfunktechnologien ein, die der APN verwenden darf (z. B. LTE/5G NR).

Proxyadresse und **Proxyport**: HTTP-Proxy für den Datenverkehr (falls zutreffend).

MMS-Proxyadresse, **MMS-Proxyport**, **MMSC (MMS-Center-URI)**: MMS-bezogene Einstellungen.

Numerische Betreiber-ID (MCC+MNC) und **Anbieter-ID**: Felder zur Anbieteridentifikation.

Always-On-Einstellung: Ob die durch diesen APN aktivierte PDU-Sitzung immer aktiv sein soll. Unterstützt ab Android 15.

MVNO-Typ: Typ der Kennung des mobilen virtuellen Netzbetreibers.

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

5. Cell-Broadcast-Konfiguration deaktiviert

Ob die Konfiguration von Cell Broadcast deaktiviert ist.

6. Konfiguration mobiler Netzwerke deaktiviert

Ob die Konfiguration mobiler Netzwerke deaktiviert ist.

7. Roaming-Daten deaktiviert

Ob Roaming-Datendienste deaktiviert sind.

8. Ausgehende Anrufe deaktiviert

Ob ausgehende Anrufe deaktiviert sind.

9. SMS deaktiviert

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

10. 5G-Network-Slicing-Konfiguration

Konfigurieren Sie die Einstellungen für bevorzugte Netzwerkdienste, um Enterprise-5G-Network-Slicing zu aktivieren. Sie können bis zu 5 Unternehmens-Slices einrichten und Anwendungen bestimmten Netzwerken zuweisen, um das Routing des Datenverkehrs zu optimieren.

10.1. Standardmäßiges bevorzugtes Netzwerk

Standardmäßige ID des bevorzugten Netzwerks für Anwendungen, die nicht in der Anwendungsliste enthalten sind, oder wenn bei einer App **Bevorzugtes Netzwerk** nicht festgelegt ist. Für die angegebene Netzwerk-ID muss eine Konfiguration vorhanden sein (sofern nicht **Kein bevorzugtes Netzwerk** festgelegt ist).

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

10.2. Netzwerkdienstkonfigurationen

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

ID des bevorzugten Netzwerks (automatisch zugewiesen): Die Netzwerk-ID wird automatisch zugewiesen und kann nicht geändert werden.

Fallback auf Standardverbindung: Ob der Fallback auf das geräteweite Standardnetzwerk zulässig ist. Wenn dies nicht zulässig ist, können Apps nicht auf das Internet zugreifen, wenn der 5G-Slice nicht verfügbar ist.

Nicht übereinstimmende Netzwerke: Ob Apps, für die diese Konfiguration gilt, andere Netzwerke als den bevorzugten Dienst verwenden dürfen. Wenn **Nicht zulässig** festgelegt ist, muss auch **Fallback auf Standardverbindung** auf **Nicht zulässig** gesetzt sein. Erfordert Android 14 oder höher.

Netzwerk

In diesem Abschnitt können Sie netzwerkbezogene Richtlinien konfigurieren.

> Wi-Fi-Konfigurationen können vom System über **WiFi-Konfigurationen** bereitgestellt und verwaltet werden. Je nach Wert, der für **Wi-Fi konfigurieren** festgelegt ist, haben Benutzer möglicherweise eingeschränkte oder keine Kontrolle über das Hinzufügen/Ändern von Netzwerken.

Funkstatus des Geräts

1. Wi-Fi-Status

Steuert den aktuellen Wi-Fi-Status und ob der Benutzer ihn ändern kann.

> **Benutzerauswahl (Standard)**: Der Benutzer darf Wi-Fi aktivieren/deaktivieren.
>
> **Aktiviert**: Wi-Fi ist eingeschaltet und der Benutzer darf es nicht ausschalten (Android 13+).
>
> **Deaktiviert**: Wi-Fi ist ausgeschaltet und der Benutzer darf es nicht einschalten (Android 13+).

2. Mindestsicherheitsstufe für Wi-Fi

Die erforderliche Mindestsicherheitsstufe von Wi-Fi-Netzwerken, mit denen das Gerät eine Verbindung herstellen kann. Unterstützt unter Android 13 und höher, für vollständig verwaltete Geräte und Arbeitsprofile auf unternehmenseigenen Geräten.

> **Offenes Netzwerk (Standard)**: Das Gerät kann eine Verbindung zu allen Arten von Wi-Fi-Netzwerken herstellen.
>
> **Persönliches Netzwerk**: Verbietet offene Wi-Fi-Netzwerke; erfordert mindestens persönliche Sicherheit (z. B. WPA2-PSK).

Unternehmensnetzwerk: Erfordert Unternehmens-EAP-Netzwerke; verbietet Wi-Fi-Netzwerke unterhalb dieser Sicherheitsstufe.

192-Bit-Unternehmensnetzwerk: Erfordert 192-Bit-Unternehmensnetzwerke; strengste Option.

3. Ultrabreitband-Status (UWB)

Steuert den Status der Ultrabreitband-Einstellung und ob der Benutzer sie ein- oder ausschalten kann.

Benutzerauswahl (Standard): Der Benutzer darf UWB ein- oder ausschalten.

Deaktiviert: UWB ist deaktiviert und der Benutzer darf es nicht über die Einstellungen umschalten (Android 14+).

Gerätekonnektivitätsverwaltung

4. Bluetooth-Freigabe

Steuert, ob die Bluetooth-Freigabe zulässig ist.

Zulässig: Die Bluetooth-Freigabe ist zulässig (Standard auf vollständig verwalteten Geräten, Android 8+).

Nicht zulässig: Die Bluetooth-Freigabe ist nicht zulässig (Standard in Arbeitsprofilen, Android 8+).

5. Wi-Fi konfigurieren

Steuert die Berechtigungen zum Konfigurieren von Wi-Fi. Je nach ausgewählter Option hat der Benutzer volle, eingeschränkte oder keine Kontrolle beim Konfigurieren von Wi-Fi-Netzwerken.

Konfigurieren von Wi-Fi zulassen (Standard): Der Benutzer darf Wi-Fi konfigurieren.

Hinzufügen von Wi-Fi-Konfigurationen nicht zulassen: Das Hinzufügen neuer Wi-Fi-Konfigurationen ist nicht zulässig. Der Benutzer kann zwischen bereits konfigurierten Netzwerken wechseln (Android 13+; vollständig verwaltete und unternehmenseigene

Arbeitsprofile).

Konfigurieren von Wi-Fi nicht zulassen: Verbietet das Konfigurieren von Wi-Fi-Netzwerken. Auf vollständig verwalteten Geräten werden benutzerkonfigurierte Netzwerke entfernt und nur über **WiFi-Konfigurationen** konfigurierte Netzwerke beibehalten. Bei unternehmenseigenen Arbeitsprofilen sind vorhandene Netzwerke nicht betroffen, aber Benutzer können keine Wi-Fi-Netzwerke hinzufügen/entfernen/ändern.

> Wenn das Konfigurieren von Wi-Fi deaktiviert ist und das Gerät beim Start keine Verbindung herstellen kann, kann das System den **Netzwerk-Notzugang** anzeigen, damit der Benutzer vorübergehend eine Verbindung herstellen und die Richtlinie aktualisieren kann.

6. Wi-Fi-Direct-Einstellungen

Steuert das Konfigurieren und Verwenden von Wi-Fi-Direct-Einstellungen. Unterstützt auf unternehmenseigenen Geräten mit Android 13 und höher.

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

Nicht zulassen: Der Benutzer darf Wi-Fi Direct nicht verwenden.

7. Tethering-Einstellungen

Steuert die Tethering-Einstellungen. Je nach festgelegtem Wert ist dem Benutzer die Nutzung verschiedener Tethering-Formen teilweise oder vollständig untersagt.

Gesamtes Tethering zulassen (Standard): Ermöglicht die Konfiguration und Nutzung aller Tethering-Formen.

Wi-Fi-Tethering nicht zulassen: Untersagt dem Benutzer die Nutzung von Wi-Fi-Tethering (unternehmenseigen, Android 13+).

Gesamtes Tethering nicht zulassen: Untersagt alle Tethering-Formen (vollständig verwaltete und unternehmenseigene Arbeitsprofile).

8. Wi-Fi-SSID-Richtlinie

Einschränkungen, mit welchen Wi-Fi-SSIDs das Gerät eine Verbindung herstellen kann (dies wirkt sich nicht darauf aus, welche Netzwerke auf dem Gerät konfiguriert werden können). Unterstützt auf unternehmenseigenen Geräten mit Android 13 und höher.

SSID-Sperrliste (Standard): Das Gerät kann keine Verbindung zu Wi-Fi-Netzwerken herstellen, deren SSID aufgeführt ist, aber zu anderen Netzwerken.

SSID-Zulassungsliste: Das Gerät kann nur eine Verbindung zu den aufgeführten SSIDs herstellen. Die SSID-Liste darf nicht leer sein.

Verwenden Sie **SSID hinzufügen**, um Einträge hinzuzufügen. Je nach ausgewähltem Richtlinientyp wird die Liste als zulässige oder abgelehnte SSIDs interpretiert.

In der Benutzeroberfläche des Richtlinieneditors wird die SSID-Liste bei Zulassungslisten als **Zulässige Wi-Fi-SSIDs** und bei Sperrlisten als **Abgelehnte Wi-Fi-SSIDs** bezeichnet.

9. Wi-Fi-Roaming-Einstellungen

Konfigurieren Sie den Wi-Fi-Roaming-Modus pro SSID. Verwenden Sie **Wi-Fi-Roaming-Einstellung hinzufügen**, um Einträge zu erstellen.

Jeder Eintrag enthält:

SSID: Die SSID, für die die Roaming-Einstellung gilt (erforderlich).

Wi-Fi-Roaming-Modus: Standard / Deaktiviert / Aggressiv. Deaktiviert und Aggressiv erfordern Android 15+ und werden nur auf vollständig verwalteten Geräten und Arbeitsprofilen auf unternehmenseigenen Geräten unterstützt.

Netzwerkeinschränkungen

10. Bluetooth deaktiviert

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

11. Bluetooth-Kontaktfreigabe deaktiviert

Ob die Bluetooth-Kontaktfreigabe deaktiviert ist.

12. Bluetooth-Konfiguration deaktiviert

Ob das Konfigurieren von Bluetooth deaktiviert ist.

13. Netzwerk-Reset deaktiviert

Ob das Zurücksetzen der Netzwerkeinstellungen deaktiviert ist.

14. Ausgehender Beam deaktiviert

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

VPN

15. Always-On-VPN-App

Geben Sie einen Paketnamen für Always-On-VPN an, um sicherzustellen, dass Daten bestimmter verwalteter Apps immer über ein konfiguriertes VPN geleitet werden.

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

16. VPN-Lockdown

Untersagt die Netzwerknutzung, wenn das VPN nicht verbunden ist.

17. VPN-Konfiguration deaktiviert

Ob das Konfigurieren von VPN deaktiviert ist.

Proxy- und Netzwerkdienste

18. Bevorzugter Netzwerkdienst

Steuert, ob der bevorzugte Netzwerkdienst im Arbeitsprofil aktiviert ist. Beispielsweise kann eine Organisation eine Vereinbarung mit einem Mobilfunkanbieter haben, dass Arbeitsdaten über einen für die Unternehmensnutzung reservierten Netzwerkdienst des Anbieters gesendet werden (z. B. ein Unternehmens-Slice in 5G-Netzwerken). Dies hat keine Auswirkung auf vollständig verwaltete Geräte.

Deaktiviert: Der bevorzugte Netzwerkdienst ist im Arbeitsprofil deaktiviert.

Aktiviert: Der bevorzugte Netzwerkdienst ist im Arbeitsprofil aktiviert.

> Wenn Sie Enterprise-Network-Slicing verwenden, konfigurieren Sie außerdem **5G-Network-Slicing-Konfiguration** im Richtlinien-Panel **Mobilfunk** und weisen Sie Apps über ihre Einstellung **Bevorzugtes Netzwerk** einem Slice zu.

19. Empfohlener globaler Proxy

Der netzwerkunabhängige globale HTTP-Proxy. In der Regel sollten Proxys pro Netzwerk in WiFi-Konfigurationen konfiguriert werden. Ein globaler Proxy kann für ungewöhnliche Konfigurationen wie eine allgemeine interne Filterung nützlich sein. Der globale Proxy ist lediglich eine Empfehlung und einige Apps ignorieren ihn möglicherweise.

Deaktiviert

Direkter Proxy

Proxy-Autokonfiguration (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, mit dem der Proxy konfiguriert wird.

19.4. Ausgeschlossene Hosts

Bei einem direkten Proxy die Hosts, für die der Proxy umgangen wird. Hostnamen können Platzhalter wie ***.example.com** enthalten.

Verwenden Sie **Ausgeschlossenen Host hinzufügen**, um Einträge hinzuzufügen (nur für direkten Proxy verfügbar).

Wi-Fi-Konfigurationen

Definieren Sie Wi-Fi-Netzwerkkonfigurationen, die das System auf Geräten anwendet. Verwenden Sie **Wi-Fi-Konfiguration hinzufügen**, um einen Eintrag zu erstellen, und entfernen Sie ihn über die Löschaktion.

20. Felder der Wi-Fi-Konfiguration

Jede Konfiguration umfasst:

Konfigurationsname: Erforderlich.

SSID: Erforderlich.

Automatisch verbinden: Ob automatisch eine Verbindung zum Netzwerk hergestellt werden soll, wenn es in Reichweite ist.

Fast Transition: Ob der Client versuchen soll, Fast Transition (IEEE 802.11r-2008) mit dem Netzwerk zu verwenden.

Versteckte SSID: Ob die SSID gesendet wird.

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

20.1. Sicherheit

Wi-Fi-Sicherheitsoptionen:

WEP-PSK: WEP (Pre-Shared Key).

WPA-PSK: WPA/WPA2/WPA3-Personal (Pre-Shared Key).

WPA-EAP: WPA/WPA2/WPA3-Enterprise (Extensible Authentication Protocol).

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

20.2. Passphrase (Pre-Shared Key)

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

20.3. EAP-Methode (Enterprise)

Wird angezeigt, wenn Sicherheit auf **WPA-EAP** oder **WPA3-192-Bit-Modus** gesetzt ist. Wählen Sie eine äußere EAP-Methode:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Phase-2-Authentifizierung

Wird für tunnelnde äußere Methoden (**EAP-TTLS** und **PEAP**) angezeigt.

MSCHAPv2

PAP

20.5. EAP-Anmeldeinformationen von Benutzern

Wenn aktiviert, wendet das System EAP-Anmeldeinformationen automatisch pro Benutzer auf Geräten an. Sie können Benutzeranmeldeinformationen im Bereich **Benutzer** konfigurieren.

20.6. Clientzertifikat

Für **EAP-TLS** können Sie ein Clientzertifikat für die Wi-Fi-Authentifizierung zuweisen. Weitere Informationen finden Sie auf der Seite **Zertifikatsverwaltung**.

Wenn bereits ein Zertifikat zugewiesen ist, können Sie über **Zertifikat öffnen** es anzeigen oder über **Zertifikat ändern** ein anderes auswählen.

Alternativ können Sie einen **Alias für das Clientzertifikat-Schlüsselpaar** angeben, der auf ein im Android-Schlüsselspeicher gespeichertes Clientzertifikat verweist, das für die Wi-Fi-Authentifizierung zugelassen ist.

> Wenn sowohl**Clientzertifikat** als auch **Alias für das Clientzertifikat-Schlüsselpaar** festgelegt sind, wird der Schlüsselpaar-Alias ignoriert.

20.7. Identität

Identität des Benutzers. Bei tunnelnden äußeren Protokollen (PEAP, EAP-TTLS) wird sie zur Authentifizierung innerhalb des Tunnels verwendet, und die **anonyme Identität** wird für die EAP-Identität außerhalb des Tunnels verwendet. Bei nicht tunnelnden äußeren Protokollen wird sie für die EAP-Identität verwendet.

20.8. Anonyme Identität

Nur für tunnelnde Protokolle: Gibt die Identität des Benutzers an, die dem äußeren Protokoll präsentiert wird.

20.9. Passwort

Passwort des Benutzers. Wenn nicht angegeben, wird standardmäßig der Benutzer zur Eingabe aufgefordert.

20.10. Server-CA-Zertifikate

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

Verwenden Sie **Server-CA-Zertifikat hinzufügen**, um Einträge hinzuzufügen, und entfernen Sie sie über die Löschaktion.

20.11. Übereinstimmungen von Domänensuffixen

Eine Liste von Einschränkungen für den Serverdomänennamen. Die Einträge werden als Suffix-Übereinstimmungsanforderungen gegen die DNS-Namen des alternativen Antragstellernamens eines Authentifizierungsserverzertifikats verwendet.

System

In diesem Abschnitt können Sie systembezogene Richtlinien konfigurieren.

1. Mindest-API-Level

Das zulässige Mindest-API-Level für Android.

2. Verschlüsselungsrichtlinie

Ob die Verschlüsselung aktiviert ist.

> **Standard**: Dieser Wert wird ignoriert, d. h. keine Verschlüsselung erforderlich.
>
> **Aktiviert ohne Passwort**: Verschlüsselung erforderlich, aber kein Passwort zum Starten erforderlich.
>
> **Aktiviert mit Passwort**: Verschlüsselung erforderlich und Passwort zum Starten erforderlich.

3. Automatisches Datum und Uhrzeit

Ob automatisches Datum, Uhrzeit und Zeitzone auf einem unternehmenseigenen Gerät aktiviert sind.

> **Benutzerauswahl (Standard)**: Automatisches Datum, Uhrzeit und Zeitzone bleiben der Wahl des Benutzers überlassen.
>
> **Erzwungen**: Automatisches Datum, Uhrzeit und Zeitzone auf dem Gerät erzwingen.

4. Entwicklereinstellungen

Steuert den Zugriff auf Entwicklereinstellungen: Entwickleroptionen und abgesicherter Modus.

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

Erlaubt: Erlaubt alle Entwicklereinstellungen. Der Benutzer kann auf die Einstellungen zugreifen und sie optional konfigurieren.

5. Common-Criteria-Modus

Steuert den Common-Criteria-Modus – Sicherheitsstandards, die in den Common Criteria for Information Technology Security Evaluation (CC) definiert sind. Das Aktivieren des Common-Criteria-Modus erhöht bestimmte Sicherheitskomponenten auf einem Gerät (zum Beispiel: AES-GCM-Verschlüsselung von Bluetooth-Langzeitschlüsseln, zusätzliche Validierung für einige Netzwerkzertifikate und kryptografische Integritätsprüfungen von Richtlinien). Der Common-Criteria-Modus wird nur auf unternehmenseigenen Geräten mit Android 11 oder höher unterstützt. Warnung: Der Common-Criteria-Modus erzwingt ein strenges Sicherheitsmodell, das normalerweise nur für hochsensible Organisationen erforderlich ist. Die normale Gerätenutzung kann beeinträchtigt werden; aktivieren Sie ihn nur, wenn er 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.

Benutzerauswahl (Standard): Der Benutzer kann wählen, ob MTE auf dem Gerät aktiviert oder deaktiviert wird (falls das Gerät dies unterstützt).

Erzwungen: MTE ist aktiviert und der Benutzer darf dies nicht ändern (Android 14+; unterstützt auf vollständig verwalteten Geräten und Arbeitsprofilen auf unternehmenseigenen Geräten).

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

7. Inhaltsschutz

Steuert, ob der Inhaltsschutz (der nach irreführenden Apps sucht) aktiviert ist. Dies wird ab Android 15 unterstützt.

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

Erzwungen: Der Inhaltsschutz ist aktiviert und der Benutzer kann dies nicht ändern (Android 15+).

Benutzerauswahl: Der Inhaltsschutz wird nicht durch die Richtlinie gesteuert; der Benutzer kann wählen (Android 15+).

8. Assist-Inhalte

Steuert, ob AssistContent an eine privilegierte App wie eine Assistenten-App gesendet werden darf (zum Beispiel Circle to Search). AssistContent umfasst Screenshots und Informationen zu einer App, etwa 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 wird blockiert (Android 15+).

9. Erstellen von Fenstern deaktiviert

Ob das Erstellen von Fenstern neben App-Fenstern deaktiviert ist. Diese Option verhindert die Anzeige der folgenden Systemoberflächen: Toasts und Snackbars, Telefonaktivitäten (z. B. eingehende Anrufe) und priorisierte Telefonaktivitäten (z. B. laufende Anrufe), Systemwarnungen, Systemfehler und Systemoverlays.

10. Netzwerk-Notausgang

Ob der Netzwerk-Notausgang aktiviert ist. Wenn beim Start keine Netzwerkverbindung hergestellt werden kann, fordert der Notausgang den Benutzer auf, vorübergehend eine Verbindung zu einem Netzwerk herzustellen, um die Geräterichtlinie zu aktualisieren. Nach dem Anwenden der Richtlinie wird das temporäre Netzwerk vergessen und das Gerät setzt den Startvorgang fort. Dies verhindert, dass keine Verbindung zu einem Netzwerk hergestellt werden kann, wenn die letzte Richtlinie kein geeignetes Netzwerk enthält und das Gerät im Lock-Task-Modus in eine App startet 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 auswählen, welche Browser-App Weblinks automatisch öffnet oder welche Launcher-App beim Tippen auf die Home-Taste verwendet wird.

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

11.1. Empfängeraktivität

Die Aktivität, die als standardmäßiger Intent-Handler dienen soll. Dies sollte ein Android-Komponentenname sein, z. B. com.android.enterprise.app/.MainActivity. Alternativ kann der Wert der Paketname einer App sein; in diesem Fall wählt Android Device Policy eine geeignete Aktivität aus der App aus, um den Intent zu verarbeiten.

11.2. Aktion

Die Intent-Aktionen, die im Filter abgeglichen werden sollen. Wenn Aktionen im Filter enthalten sind, muss die Aktion eines Intents einer dieser Werte sein, damit er übereinstimmt. Wenn keine Aktionen enthalten sind, wird die Intent-Aktion ignoriert.

11.3. Kategorie

Die Intent-Kategorien, die im Filter abgeglichen werden sollen. Ein Intent enthält die Kategorien, die er benötigt; alle diese Kategorien müssen im Filter enthalten sein, damit eine Übereinstimmung erzielt wird. Mit anderen Worten: Das Hinzufügen einer Kategorie zum Filter hat keine Auswirkungen auf den Abgleich, es sei denn, diese Kategorie ist im Intent angegeben.

12. Zulässige Eingabemethoden

Gibt die zulässigen Eingabemethoden an.

> **Alle erlaubt**: Keine Einschränkung angewendet. Alle Eingabemethoden sind erlaubt.
>
> **Nur Systemeigene**: Nur die integrierten Eingabemethoden des Systems sind erlaubt.
>
> **Nur Systemeigene und bereitgestellte**: Nur die bereitgestellten und die integrierten Eingabemethoden des Systems sind erlaubt.

12.1. Erlaubte Eingabemethoden

Paketnamen von Eingabemethoden, die erlaubt sind. Gilt nur, wenn **Zulässige Eingabemethoden** auf **Nur Systemeigene und bereitgestellte** festgelegt ist.

Verwenden Sie **Eingabemethode hinzufügen**, um Einträge hinzuzufügen, und entfernen Sie sie mit der Löschaktion.

13. Zulässige Bedienungshilfen

Gibt die zulässigen Bedienungshilfen an.

> **Alle erlaubt**: Jede Bedienungshilfe kann verwendet werden.
>
> **Nur Systemeigene**: Nur die integrierten Bedienungshilfen des Systems können verwendet werden.
>
> **Nur Systemeigene und bereitgestellte**: Nur die bereitgestellten und die integrierten Bedienungshilfen des Systems können verwendet werden.

13.1. Erlaubte Bedienungshilfen

Erlaubte Bedienungshilfen. Gilt nur, wenn **Zulässige Bedienungshilfen** auf **Nur Systemeigene und bereitgestellte** festgelegt ist.

Verwenden Sie **Bedienungshilfe hinzufügen**, um Einträge hinzuzufügen, und entfernen Sie sie mit der Löschaktion.

14. Systemupdate-Richtlinie

Konfiguration für die Verwaltung von Systemupdates.

> **Standard**: Folgt dem Standard-Updateverhalten für das Gerät, bei dem der Benutzer Systemupdates in der Regel akzeptieren muss.
>
> **Automatisch**: Automatisch installieren, sobald ein Update verfügbar ist.
>
> **Zeitfenster**: Automatisch innerhalb eines täglichen Wartungsfensters installieren. Dadurch werden auch Play-Apps so konfiguriert, dass sie innerhalb des Zeitfensters aktualisiert werden. Dies wird für Kiosk-Geräte dringend empfohlen, da dies die einzige Möglichkeit ist, Apps, die dauerhaft im Vordergrund angeheftet sind, über Play zu aktualisieren.
>
> **Aufschieben**: Automatische Installation um bis zu maximal 30 Tage aufschieben.

14.1. Wartungsfenster (nur Zeitfenster)

Wenn **Systemupdate-Richtlinie** auf **Zeitfenster** festgelegt ist, können Sie das tägliche Wartungsfenster über die Felder **von** und **bis** definieren.

14.2. Sperrzeiträume für Systemupdates

Ein jährlich wiederkehrender Zeitraum, in dem Over-the-Air-(OTA-)Systemupdates verschoben werden, um die auf einem Gerät ausgeführte Betriebssystemversion einzufrieren. Um ein unbegrenztes Einfrieren des Geräts zu verhindern, müssen die einzelnen Sperrzeiträume durch mindestens 60 Tage getrennt sein. Ein Sperrzeitraum darf 90 Tage nicht überschreiten.

Verwenden Sie **Sperrzeitraum für Systemupdate hinzufügen**, um Einträge zu erstellen.

15. Standard-Anmeldeinformationsanbieter

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

> **Nicht erlaubt (Standard)**: Apps mit nicht angegebener credentialProviderPolicy dürfen nicht als Anmeldeinformationsanbieter fungieren.
>
> **Nicht erlaubt außer System**: Apps mit nicht angegebener credentialProviderPolicy dürfen nicht als Anmeldeinformationsanbieter fungieren, mit Ausnahme der Standard-Anmeldeinformationsanbieter des OEM.

Standort und Geofences

Dieses Panel fasst die Android-Richtlinieneinstellungen zusammen, die die Standortmeldung, die Standortdurchsetzung und Geofence-Definitionen für Geräte steuern. Verwenden Sie es, wenn Cerberus Enterprise Gerätestandorte erfassen oder erkennen soll, wenn Geräte in konfigurierte Bereiche eintreten oder sie verlassen.

Standortmeldung

Standort melden

Aktiviert die Geolokalisierungsmeldung für Geräte. Die über diese Einstellung erfassten Standortdaten werden von der **Standortkarte im Dashboard**, dem Standortverlauf der Geräteübersicht und der Geofence-Verarbeitung verwendet.

> Standortverlauf und Geofence-Ereignisse werden **90 Tage** lang aufbewahrt, ältere Daten werden jede Nacht automatisch gelöscht. Der letzte Standort jedes registrierten Geräts bleibt immer erhalten, sodass das Gerät auf den Karten bleibt.

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

> Auf persönlichen Apple-Geräten (User Enrollment) sind Standort und Geofences standardmäßig deaktiviert: Sie sind nur verfügbar, wenn in der Apple-Richtlinie **Standort und Geofences auf persönlichen Geräten** aktiviert ist, und nur, wenn der Benutzer den Standort für die App Cerberus Enterprise zulässt.

Standortmodus

Steuert die Gerätestandort-Einstellung auf unternehmenseigenen Geräten.

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

- **Deaktiviert**: Standortdienste sind auf dem Gerät deaktiviert.

Standortfreigabe deaktiviert

Deaktiviert die Standortfreigabe für Arbeits-Apps. Auf Geräten mit Profilinhaber betrifft dies das Arbeitsprofil. Auf vollständig verwalteten Geräten wird der Standort für das gesamte Gerät deaktiviert und der Gerätestandortmodus überschrieben.

Automatisches Verhalten bei aktiven Geofences

Aktive Geofences erfordern eine funktionierende Standortmeldung. Wenn mindestens ein Geofence aktiv ist, hält Cerberus Enterprise die zugehörigen Standorteinstellungen automatisch konsistent.

- **Standort melden** wird zwangsweise aktiviert, solange aktive Geofences vorhanden sind.
- **Standortmodus** wird zwangsweise auf **Erzwungen** gesetzt.
- **Standortfreigabe deaktiviert** wird zwangsweise deaktiviert.

Wenn Sie versuchen, **Standort melden** zu deaktivieren, während ein 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. Jeder Geofence enthält diese Hauptfelder:

- **Name**: erforderlich und eindeutig.
- **Breitengrad** und **Längengrad**: der Mittelpunkt des Bereichs.
- **Radius (m)**: erforderlich, von **200** bis **10000** Metern.
- **Beschreibung**: optionale Notizen für Administratoren.
- **Eintritt melden** und **Austritt melden**: Wählen Sie aus, welche Übergangsereignisse generiert werden sollen.
- **Aktiv**: aktiviert oder deaktiviert den Geofence, ohne ihn zu löschen.

> Mindestens eines von**Eintritt melden** oder **Austritt melden** muss für jeden Geofence aktiviert bleiben.

> Der Mindestradius betrug zuvor 100 Meter. Bestehende Geofences mit weniger als 200 Metern funktionieren weiterhin und bleiben beim Speichern der Richtlinie unverändert, auch wenn Sie sie verschieben oder umbenennen. Wenn Sie ihren Radius ändern, muss er mindestens 200 Meter betragen.

Kartenbearbeitungswerkzeuge

Jede Geofence-Karte enthält eine Kartenvorschau des Bereichs. Sie können die Geometrie über die Karte oder über die numerischen Felder bearbeiten.

- Klicken Sie auf die Karte, um den Geofence-Mittelpunkt zu verschieben, wenn die Bereichsbearbeitung entsperrt ist.
- Verwenden Sie die Schaltfläche **Aktueller Standort**, um die Karte auf Ihre aktuelle Browserposition zu zentrieren.
- Verwenden Sie die Schaltfläche **Karte neu zentrieren**, um den bevorzugten Ansichtsbereich für diesen Geofence wiederherzustellen.
- Verwenden Sie die Sperrschaltfläche, um versehentliche Änderungen an der Geofence-Geometrie zu verhindern.

Wo Geofence-Daten angezeigt werden

Geofence-Übergänge können auf der Seite **Geräteübersicht** unter Android im Tab **Geofence** des Standort-Panels überprüft werden. Dieser Tab zeigt Übergänge auf einer eigenen Karte zusammen mit Filterwerkzeugen und der Übergangsliste.

Benutzerverwaltung

Hinzufügen von Benutzern deaktiviert

Ob das Hinzufügen neuer Benutzer und Profile deaktiviert ist. Bei Geräten, deren managementMode **DEVICE_OWNER** ist, wird dieses Feld ignoriert und der Benutzer darf niemals Benutzer hinzufügen oder entfernen.

Ändern von Konten deaktiviert

Ob das Hinzufügen oder Entfernen von Konten deaktiviert ist.

Konfiguration von Benutzeranmeldeinformationen deaktiviert

Ob die Konfiguration von Benutzeranmeldeinformationen deaktiviert ist.

Entfernen von Benutzern deaktiviert

Ob das Entfernen anderer Benutzer deaktiviert ist.

Festlegen des Benutzersymbols deaktiviert

Ob das Ändern des Benutzersymbols deaktiviert ist.

Festlegen des Hintergrundbilds deaktiviert

Ob das Ändern des Hintergrundbilds deaktiviert ist.

Authentifizierung bei der Einrichtung des Arbeitskontos

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

Während der Geräteeinrichtung/Registrierung beeinflusst diese Richtlinie, ob eine Anmeldung mit einem Arbeitskonto erforderlich ist, aber die Einstellung **Authenticate Using Google** in der Google Admin Console und der Typ des Registrierungstokens können weiterhin eine Authentifizierung erfordern.

Für bereits registrierte Geräte gilt diese Richtlinie nur, wenn das Gerät von einem verwalteten Google Play-Konto verwaltet wird (d. h. registriert ohne **Authenticate Using Google Enrollment**).

Weitere Informationen und Hilfe zur Fehlerbehebung finden Sie unter **Authenticate Using Google enrollment**.

Blockierte Kontotypen

Kontotypen, die vom Benutzer nicht verwaltet werden können. Diese Option verhindert, dass Gerätebenutzer nicht genehmigte Konten hinzufügen.

Verwenden Sie **Blockierten Kontotyp hinzufügen**, um einen oder mehrere Kontotypen hinzuzufügen.

Jeder Eintrag hat ein Feld **Kontotyp** (erforderlich). Geben Sie eine Zeichenfolge wie **com.google** ein. Entfernen Sie einen Eintrag mit der Löschaktion.

Private Nutzung

Wenn Sie ein unternehmenseigenes Gerät für Arbeit und private Nutzung bereitstellen, können Sie Regeln festlegen, um einzuschränken, wie der Benutzer das Gerät außerhalb des Arbeitsprofils privat nutzen kann.

> Dieser Abschnitt gilt nur für unternehmenseigene Geräte mit Arbeitsprofil. Er hat keine Auswirkungen auf vollständig verwaltete oder private Geräte.

1. Kamera deaktiviert

Ob die Kamera deaktiviert ist.

2. Bildschirmaufnahme deaktiviert

Ob die Bildschirmaufnahme deaktiviert ist.

3. Max. Tage mit ausgeschalteter Arbeit

Legt fest, wie lange das Arbeitsprofil deaktiviert bleiben kann.

4. Bluetooth-Freigabe

Legt fest, ob die Bluetooth-Freigabe im persönlichen Profil eines unternehmenseigenen Geräts mit Arbeitsprofil zulässig ist.

5. Privater Bereich

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

6. Play-Store-Modus

Dieser Modus steuert, welche Apps dem Benutzer im Play Store des persönlichen Profils erlaubt oder blockiert werden.

> **Blocklist (Standard)**: Alle Apps sind verfügbar, und jede App, die nicht auf dem Gerät sein sollte, muss im Bereich **Anwendungen** ausdrücklich als **Blockiert** markiert werden.
>
> **Allowlist**: Nur Apps, die im Bereich **Anwendungen** ausdrücklich mit dem auf **Verfügbar** gesetzten **Installationstyp** angegeben sind, dürfen im persönlichen Profil installiert werden.

7. Anwendungen

Liste der Anwendungen, die im persönlichen Profil erlaubt oder blockiert werden müssen. Das Verhalten des Listeninhalts hängt vom Wert ab, der für **Play-Store-Modus** festgelegt ist.

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

7.1. Installationstyp

Mögliche Installationsverhalten einer Anwendung im persönlichen Profil.

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

8. Blockierte Kontotypen

Kontotypen, die vom Benutzer nicht verwaltet werden können. Diese Option verhindert, dass Gerätebenutzer nicht genehmigte Konten in ihrem persönlichen Profil hinzufügen.

Profilübergreifende Richtlinien

Gilt nur für Geräte mit privaten und Arbeitsprofilen.

Profilübergreifendes Kopieren/Einfügen

Ob aus einem Profil (privat oder Arbeit) kopierter Text in das andere Profil eingefügt werden kann.

> **Nicht zulässig (Standard)**: Verhindert, dass Benutzer in das private Profil Text einfügen, der aus dem Arbeitsprofil kopiert wurde. Aus dem privaten Profil kopierter Text kann in das Arbeitsprofil eingefügt werden.
>
> **Zulässig**: In einem der beiden Profile kopierter Text kann in das jeweils andere Profil eingefügt werden.

Profilübergreifende Datenfreigabe

Ob Daten aus einem Profil (privat oder Arbeit) für Apps im anderen Profil freigegeben werden können. Steuert insbesondere die einfache Datenfreigabe über Intents. Die Verwaltung anderer profilübergreifender Kommunikationskanäle wie Kontaktsuche, Kopieren/Einfügen, oder verbundene Arbeits- & private Apps wird separat konfiguriert.

> **Nicht zulässig**: Verhindert, dass Daten sowohl vom privaten Profil an das Arbeitsprofil als auch vom Arbeitsprofil an das private Profil freigegeben werden.
>
> **Arbeit an privat nicht zulässig (Standard)**: Verhindert, dass Benutzer Daten aus dem Arbeitsprofil für Apps im privaten Profil freigeben. Private Daten können für Arbeits-Apps freigegeben werden.
>
> **Zulässig**: Daten aus einem der beiden Profile können für das jeweils andere Profil freigegeben werden.

Standard für Widgets im Arbeitsprofil

Standardverhalten für Widgets im Arbeitsprofil. Wenn für eine bestimmte App keine Widget-Richtlinie definiert ist, gilt der hier festgelegte Standard.

Profilübergreifende App-Funktionen

Steuert, ob Apps im privaten Profil App-Funktionen von Apps im Arbeitsprofil aufrufen können. Dies erfordert Android 16 oder höher.

> Diese Einstellung hängt von der Option **App-Funktionen** auf Richtlinienebene ab (im Abschnitt App-Verwaltung). Wenn App-Funktionen auf **Nicht zulässig** gesetzt sind, lehnt die API profilübergreifende App-Funktionen mit der Einstellung **Zulässig** ab.

Arbeitskontakte im privaten Profil

Ob im Arbeitsprofil gespeicherte Kontakte in Kontaktsuchen und bei eingehenden Anrufen im privaten Profil angezeigt werden können.

Zulässig (Standard): Ermöglicht, dass Arbeitsprofilkontakte im privaten Profil angezeigt werden.

Nicht zulässig: Verhindert, dass private Apps auf Arbeitsprofilkontakte zugreifen und Arbeitskontakte nachschlagen.

Nicht zulässig außer System: Verhindert, dass die meisten privaten Apps auf Arbeitsprofilkontakte zugreifen, mit Ausnahme der Standard-Apps des OEM für Telefon, Nachrichten und Kontakte (Android 14+).

Wenn Arbeitskontakte im privaten Profil konfiguriert ist, können Sie optional eine Liste mit Einträgen für **Ausgenommene Paketnamen** definieren. Je nach ausgewähltem Modus wirken diese Ausnahmen als Zulassungs- oder Sperrliste für private Apps.

Statusberichte

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

Die Statusdaten können auf der Dashboard-Seite **Gerätestatus** angezeigt werden.

Anwendungsberichte

Ob App-Berichte aktiviert sind. (Informationen, die über eine installierte App gemeldet werden.)

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

Entfernte Apps einschließen

Ob entfernte Apps in Anwendungsberichte einbezogen werden.

Geräteeinstellungen

Ob die Berichterstellung für Geräteeinstellungen aktiviert ist. (Informationen zu sicherheitsrelevanten Geräteeinstellungen auf dem Gerät.)

Softwareinformationen

Ob die Berichterstellung für Softwareinformationen aktiviert ist. (Informationen zur Gerätesoftware.)

Speicherinformationen

Ob die Speicherberichterstellung aktiviert ist. (Ein Ereignis zu Speicher- und Speicherplatzmessungen.)

Netzwerkinformationen

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

Displayinformationen

Ob die Displayberichterstellung aktiviert ist. Berichtsdaten sind für private Geräte mit Arbeitsprofil nicht verfügbar. (Displayinformationen des Geräts.)

Ereignisse zur Energieverwaltung

Ob die Berichterstellung für Ereignisse zur Energieverwaltung aktiviert ist. Berichtsdaten sind für private Geräte mit Arbeitsprofil nicht verfügbar.

Hardwarestatus

Ob die Berichterstellung für den Hardwarestatus aktiviert ist. Berichtsdaten sind für private Geräte mit Arbeitsprofil nicht verfügbar.

Systemeigenschaften

Ob die Berichterstellung für Systemeigenschaften aktiviert ist.

Common-Criteria-Modus

Ob die Berichterstellung für den Common-Criteria-Modus aktiviert ist.

Sonstiges

1. Easter-Egg-Spiel deaktiviert

Ob das Easter-Egg-Spiel in den Einstellungen deaktiviert ist.

2. Hinweise zur ersten Verwendung überspringen

Flag zum Überspringen von Hinweisen bei der ersten Verwendung. Der Unternehmensadministrator kann die Systemempfehlung aktivieren, dass Apps ihre Benutzereinführung und andere einführende Hinweise beim ersten Start überspringen.

3. Kurze Supportnachricht

Eine Nachricht, die dem Benutzer im Einstellungsbildschirm angezeigt wird, wo immer Funktionalität durch den Administrator deaktiviert wurde. Wenn die Nachricht länger als 200 Zeichen ist, wird sie möglicherweise abgeschnitten.

4. Lange Supportnachricht

Eine Nachricht, die dem Benutzer im Einstellungsbildschirm für Geräteadministratoren angezeigt wird.

5. Info des Eigentümers auf dem Sperrbildschirm

Die Informationen zum Geräteeigentümer, die auf dem Sperrbildschirm angezeigt werden sollen.

6. Einrichtungsaktionen

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

Verwenden Sie **Einrichtungsaktion hinzufügen**, um Einträge zu erstellen, und entfernen Sie sie mit der Löschaktion.

6.1. App starten

Paketname der zu startenden App

6.2. Titel

Stellt eine benutzergerichtete Nachricht bereit, um dem Benutzer zu erklären, warum die App gestartet werden muss.

6.3. Beschreibung

Stellt eine benutzergerichtete Nachricht bereit, um dem Benutzer zu erklären, warum die App gestartet werden muss.

7. Sichtbarkeit des Anzeigenamens des Unternehmens

Steuert, ob der Anzeigename des Unternehmens auf dem Gerät sichtbar ist (z. B. als Sperrbildschirmnachricht auf unternehmenseigenen Geräten).

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

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

Compliance-Regeln

Wenn ein Gerät oder Arbeitsprofil die unten aufgeführten Richtlinieneinstellungen nicht erfüllt, blockiert Android Device Policy standardmäßig sofort die Nutzung des Geräts oder Arbeitsprofils:

- **Passwortanforderungen**
- **Verschlüsselungsrichtlinie**
- **Tastensperre deaktiviert**
- **Zulässige Eingabemethoden**
- **Zulässige Bedienungshilfen**

Wenn das Gerät oder Arbeitsprofil nach 10 Tagen weiterhin nicht konform ist, setzt Android Device Policy das Gerät auf die Werkseinstellungen zurück oder löscht das Arbeitsprofil.

In diesem Abschnitt können Sie die standardmäßigen Regeln zur Compliance-Durchsetzung überschreiben 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 über die Löschaktion entfernt werden.

Name der Einstellung

Die auf oberster Ebene durchzusetzende Richtlinie. Zum Beispiel **Anwendungen** oder **Passwortanforderungen**.

Erforderlich. Der Wert muss mit einem unterstützten Richtliniennamen auf oberster Ebene übereinstimmen; andernfalls wird das Feld als ungültig markiert.

Blockieren nach Tagen

Anzahl der Tage, in denen die Richtlinie nicht compliant ist, bevor das Gerät oder Arbeitsprofil blockiert wird. Um den Zugriff sofort zu blockieren, legen Sie 0 fest. **Blockieren nach Tagen** muss kleiner als **Löschen nach Tagen** sein. Gilt nur für Geräte im Unternehmenseigentum.

Zulässiger Bereich: 0–300.

Blockierungsbereich

Gibt den Bereich der Blockierungsaktion an. Gilt nur für Geräte im Unternehmenseigentum.

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

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

Löschen nach Tagen

Anzahl der Tage, in denen die Richtlinie nicht compliant ist, bevor das Gerät oder Arbeitsprofil gelöscht wird.
Löschen nach Tagen muss größer als **Blockieren nach Tagen** sein. Gilt nur für Geräte im Unternehmenseigentum.

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

Zulässiger Bereich: 1–300.

Werksreset-Schutz beibehalten

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

Standard (neue Regel): aktiviert.