App-Management

In diesem Abschnitt können Sie Richtlinien festlegen, die sich auf die Verfügbarkeit von Apps, deren Installation, Updates und das Berechtigungsmanagement beziehen.

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

1. Play-Store-Modus

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

> **Whitelist (Standard)**: Nur Apps, die in der Policy enthalten sind, stehen zur Verfügung; alle Apps, die nicht in der Policy enthalten sind, werden automatisch vom Gerät deinstalliert. Der Play Store zeigt nur verfügbare Apps an.
>
> **Blacklist**: Alle Apps sind verfügbar. Jede App, die nicht auf dem Gerät sein soll, muss in der Anwendungs-Policy explizit als **blockiert** markiert werden. Der Play Store zeigt alle Apps an, außer den blockierten.

2. Policy für nicht vertrauenswürdige Apps

Die Policy 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 Stores installieren kann (Sideloading).

> **Untersagen (Standard)**: Installationen von nicht vertrauenswürdigen Apps auf dem gesamten Gerät untersagen.
>
> **Nur persönliches Profil**: Bei Geräten mit Arbeitsprofilen werden Installationen von nicht vertrauenswürdigen Apps nur im persönlichen Profil des Geräts erlaubt.
>
> **Erlauben**: Installationen von nicht vertrauenswürdigen Apps auf dem gesamten Gerät erlauben.

3. Google Play Protect

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

Erzwungen (Standard): Erzwingt die App-Verifizierung.

Wahl des Benutzers: Ermöglicht dem Benutzer zu wählen, ob die App-Verifizierung aktiviert werden soll.

4. Standard-Berechtigungsrichtlinie

Die Richtlinie für die Erteilung von Laufzeit-Berechtigungsanfragen an Apps.

Abfrage (Standard): Der Benutzer wird aufgefordert, eine Berechtigung zu erteilen.

Erteilen: Eine Berechtigung automatisch erteilen.

Ablehnen: Eine Berechtigung automatisch ablehnen.

5. App-Funktionen

Steuert, ob Apps auf voll verwalteten Geräten oder in Arbeitsprofilen die Berechtigung haben, App-Funktionen bereitzustellen. Erfordert Android 16 oder höher.

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

Untersagt: Apps auf voll verwalteten Geräten oder in Arbeitsprofilen können keine App-Funktionen bereitstellen.

6. App-Installation deaktiviert

Ob die Installation von Apps durch den Benutzer deaktiviert ist.

7. App-Deinstallation deaktiviert

Ob die Deinstallation von Apps durch den Benutzer deaktiviert ist.

8. Berechtigungsrichtlinien

Explizite Berechtigungen oder Gruppen-Zuweisungen bzw. -Ablehnungen für alle Apps. Diese Werte überschreiben die Einstellung **Default permission policy**.

Verwenden Sie **Add permission policy**, um Einträge zu erstellen, und entfernen Sie diese 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**.
>
> **Policy**: Erteilen / Ablehnen / Abfrage (verwendet dieselben Policy-Optionen wie **Default permission policy**).

9. Anwendungen

Liste der Anwendungen, die in der Policy enthalten sein müssen. Das Verhalten des Listeninhalts hängt vom Wert ein, der für den **Play Store mode** festgelegt wurde.

Wenn der **Play Store mode** auf **whitelist** eingestellt ist, sind nur Apps verfügbar, die in der Policy enthalten sind; alle Apps, die nicht in der Policy enthalten sind, werden automatisch vom Gerät deinstalliert.

Wenn der **Play Store mode** auf **blacklist** eingestellt ist, sind alle Apps verfügbar. Jede App, die nicht auf dem Gerät sein soll, muss in der Anwendungs-Policy explizit als **blockiert** markiert werden.

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

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

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

9.1. Installationsart

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

Verfügbar: Die App steht zur Installation bereit.

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

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

Blockiert: Die App ist blockiert und kann nicht installiert werden. Falls die App unter einer vorherigen Policy installiert wurde, wird sie deinstalliert.

Für Setup erforderlich: Die App wird automatisch installiert, kann vom Benutzer nicht entfernt werden und verhindert den Abschluss des Setups, bis die Installation abgeschlossen ist.

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

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 werden kann.

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

Unmetered network: Die App nur installieren, wenn das Gerät mit einem unbegrenzten Netzwerk (z. B. WLAN) verbunden ist.

Laden: Die App nur installieren, wenn das Gerät geladen wird.

Idle: Die App nur installieren, 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 genutzt, (2) das Gerät ist mit einem unbegrenzten Netzwerk verbunden, (3) das Gerät wird geladen. Das Gerät wird innerhalb von 24 Stunden

nach der Veröffentlichung durch den Entwickler über ein neues Update benachrichtigt, woraufhin die App beim nächsten Mal aktualisiert wird, wenn die oben genannten Bedingungen erfüllt sind.

Aufgeschoben: Die App wird für maximal 90 Tage nach dem Veralten der App 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 der App erfolgt keine automatische erneute Aktualisierung, bis 90 Tage nach dem erneuten Veralten der App. 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 ein neues Update benachrichtigt, sobald es verfügbar ist.

9.4. Mindestversionscode

Die Mindestversion der App, die auf dem Gerät ausgeführt wird. Wenn dieser Wert festgelegt ist, versucht das Gerät, die App auf mindestens diesen Versionscode zu aktualisieren. Wenn die App nicht auf dem neuesten Stand ist, zeigt das Gerät ein **Non compliance detail** mit dem **Non compliance reasonAPP_NOT_UPDATED** an. Die App muss bereits in Google Play mit einem Versionscode veröffentlicht worden sein, der größer als oder gleich diesem Wert ist. Pro Policy können maximal 20 Apps einen Mindestversionscode spezifizieren.

9.5. Delegierte Bereiche (Scopes)

Die von der Android Device Policy an die App delegierten Bereiche (Scopes). Sie können anderen Apps eine Auswahl an speziellen Android-Berechtigungen gewähren:

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

Verwaltete Konfigurationen: Gewährt Zugriff auf die Verwaltung von verwalteten 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 Status des Paketzugriffs.

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

9.6. Bevorzugtes Netzwerk

Der bevorzugte Netzwerkdienst, der für diese App verwendet werden soll. Wenn dieser festgelegt ist, nutzt die App bei Verfügbarkeit den angegebenen Enterprise-Network-Slice für ihre Verbindungen. Dies muss mit einem Network Slice übereinstimmen, der im Abschnitt **5G Network Slicing Configuration** des **Cellular**-Panels konfiguriert wurde.

9.7. Standard-Berechtigungsrichtlinie

Die Standardrichtlinie für alle von der App angeforderten Berechtigungen. Wenn diese angegeben wird, überschreibt sie die auf Policy-Ebene geltende **Default permission policy**, die für alle Apps gilt. Sie überschreibt jedoch nicht die **Permission policies**, die für alle Apps gelten.

Abfrage (Standard): Der Benutzer wird aufgefordert, eine Berechtigung zu erteilen.

Erteilen: Eine Berechtigung automatisch erteilen.

Ablehnen: Eine Berechtigung automatisch ablehnen.

9.8. Verbindung zwischen Arbeits- und Privatprofil-Apps

Steuert, ob die App unter Vorbehalt der Zustimmung des Benutzers (Android 11+) zwischen dem Arbeits- und dem Privatprofil des Geräts kommunizieren kann.

Untersagt (Standard): Verhindert die profilübergreifende Kommunikation der App.

Erlaubt: Ermöglicht der App die profilübergreifende Kommunikation nach Erhalt der Zustimmung des Benutzers.

9.9. Ausnahme vom Always-on-VPN-Lockdown

Legt fest, ob der App die Netzwerkverbindung erlaubt ist, wenn das VPN nicht verbunden ist und **lockdown enabled** aktiv ist. Nur auf Geräten mit Android 10 oder höher unterstützt.

Erzwungen (Standard): Die App respektiert die Always-on-VPN-Lockdown-Einstellung.

Ausgenommen: Die App ist von der Always-on-VPN-Lockdown-Einstellung ausgenommen.

9.10. Arbeitsprofil-Widgets

Legt fest, ob die im Arbeitsprofil installierte App berechtigt ist, Widgets zum Startbildschirm hinzuzufügen.

Erlaubt: Die Anwendung kann Widgets zum Startbildschirm hinzufügen.

Untersagt: Die Anwendung kann keine Widgets zum Startbildschirm hinzufügen.

9.11. Benutzereinstellungen zur Kontrolle

Legt fest, ob die Benutzerkontrolle für eine bestimmte App zulässig ist. Die Benutzerkontrolle umfasst Aktionen wie das Beenden des Anwendungsprozesses (Force-Stop) und das Löschen von Anwendungsdaten (Android 11+). Wenn **extensionConfig** für eine App aktiviert ist, ist die Benutzerkontrolle unabhängig von dieser Einstellung untersagt. Bei Kiosk-Apps können Sie **Allowed** verwenden, um die Benutzerkontrolle zu erlauben.

> **Nicht spezifiziert**: Verwendet das Standardverhalten der App, um zu bestimmen, ob die Benutzerkontrolle erlaubt oder untersagt ist.
>
> **Erlaubt**: Die Benutzerkontrolle ist für die App erlaubt.
>
> **Untersagt**: Die Benutzerkontrolle ist für die App untersagt.

9.12. Deaktiviert

Ob die App deaktiviert ist. Wenn sie deaktiviert ist, bleiben die Anwendungsdaten erhalten.

9.13. Anbieter für Anmeldedaten erlauben

Ob die App auf Android 14 und höher als Anbieter für Anmeldedaten fungieren darf.

9.14. Verwaltete Konfiguration

Um die verwalteten Einstellungen der App zu konfigurieren, klicken Sie auf die Schaltfläche **Enable managed configuration**. Wenn bereits eine verwaltete Konfiguration für die App festgelegt wurde, können Sie die Konfiguration mit der Schaltfläche **Managed configuration** ändern oder sie mit der Schaltfläche **Remove configuration** löschen.

> Die Option **Managed configuration** steht nur für Apps zur Verfügung, die diese Funktionalität unterstützen.

9.15. Berechtigungsrichtlinien

Explizite Berechtigungserteilungen oder -ablehnungen für die App. Diese Werte überschreiben die **Default permission policy** sowie die **Permission policies**, die für alle Apps gelten.

Verwenden Sie **Add permission policy**, um eine oder mehrere Berechtigungsregeln für die App-Karte hinzuzufügen, und entfernen Sie diese mit der Löschaktion.

9.16. Track-IDs

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

>

Die Option**Track IDs** steht nur für Apps zur Verfügung, die mindestens eine Track-ID für Ihre Organisation bereitstellen. Weitere Einzelheiten dazu, wie Sie Ihre Organisation einem geschlossenen Test-Track für eine bestimmte App hinzufügen, finden Sie hier.

10. Standard-Anwendungseinstellungen

Legen Sie Standard-Apps für unterstützte Typen fest. Wenn eine Standard-App für mindestens einen Typ festgelegt wurde, wird den Benutzern das Ändern der Standard-Apps in diesem Profil verhindert.

Pro **Default application type** ist nur eine Standard-Anwendungseinstellung zulässig. Die Liste der Standard-Anwendungen darf keine Duplikate enthalten.

10.1. Standard-Anwendungstyp

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

10.2. Standard-Anwendungsbereiche (Scopes)

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

Wenn keiner der ausgewählten Bereiche für den Verwaltungsmodus des Geräts anwendbar ist, meldet das Gerät ein Detail zur Nichteinhaltung (Non-compliance detail).

10.3. Standard-Anwendungen

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

Wenn die Bereiche **Fully managed** oder **Work profile** beinhalten, muss jede App auch in der Liste **Applications** vorhanden sein, wobei die **Install type** nicht auf **Blocked** gesetzt sein darf.

11. Private-Key-Auswahl

Ermöglicht die Anzeige einer Benutzeroberfläche auf einem Gerät, damit ein Benutzer einen privaten Schlüssel-Alias auswählen kann, falls keine passenden Regeln in **Choose private key rules** vorhanden sind.

> Bei Geräten mit einer Android-Version unter Android P kann das Festlegen dieser Option Enterprise-Schlüssel anfällig machen.

12. Regeln zur Auswahl des privaten Schlüssels festlegen

Steuert den Zugriff von Apps auf private Schlüssel. Die Regel bestimmt, welcher private Schlüssel (falls vorhanden) der Android Device Policy der angegebenen App gewährt wird. Der Zugriff wird entweder gewährt, wenn die App `KeyChain.choosePrivateKeyAlias` (oder eine Überladung davon) aufruft, um einen privaten Schlüssel-Alias für eine bestimmte URL anzufragen, oder bei Regeln, die nicht URL-spezifisch sind (das heißt, wenn `urlPattern` nicht gesetzt ist oder auf einen leeren String bzw. `.*` gesetzt wurde) ab Android 11 und höher direkt, sodass die App `KeyChain.getPrivateKey` aufrufen kann, ohne zuvor `KeyChain.choosePrivateKeyAlias` aufrufen zu müssen. Wenn eine App `KeyChain.choosePrivateKeyAlias` aufruft und mehr als eine `choosePrivateKeyRules` zutrifft, definiert die letzte passende Regel, welcher Schlüssel-Alias zurückgegeben wird.

Verwenden Sie **Add private key rule**, um Einträge zu erstellen, und entfernen Sie diese mit der Löschaktion.

12.1. Privater Schlüssel-Alias

Der Alias des zu verwendenden privaten Schlüssels.

12.2. URL-Muster

Das URL-Muster, das mit der URL der Anfrage abgeglichen wird. Wenn es nicht festgelegt oder leer ist, werden alle URLs abgeglichen. Dies verwendet die reguläre Ausdruckssyntax von java.util.regex.Pattern.

12.3. Paketnamen

Die Paketnamen, für die diese Regel gilt. Der Hash des Signierungszertifikats 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 Überladung davon aufrufen (jedoch nicht ohne den Aufruf von `KeyChain.choosePrivateKeyAlias`, selbst unter Android 11 und höher). Jede App mit derselben Android-UID wie ein hier spezifiziertes Paket erhält Zugriff, wenn sie `KeyChain.choosePrivateKeyAlias` aufruft.

Verwenden Sie **Add package name**, um Einträge hinzuzufügen, und entfernen Sie diese mit der Löschaktion.

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

Revision #10
Created 2026-06-24 08:06:36 UTC by Admin
Updated 2026-07-07 10:53:46 UTC by Admin