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.

Revision #7
Created 2026-11-10 15:14:20 UTC by Admin
Updated 2026-11-12 09:54:05 UTC by Admin