App-Verwaltung

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

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

1. Play Store-Modus

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

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

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

2. Richtlinie für nicht vertrauenswürdige Apps

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

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

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

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

3. Google Play Protect

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

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

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

4. Standard-Berechtigungsrichtlinie

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

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

Berechtigung erteilen: Eine Berechtigung automatisch erteilen.

Verweigern: Eine Berechtigung automatisch verweigern.

5. App-Funktionen

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

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

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

6. Installierte, deaktivierte Apps

Ob die Installation von Apps durch den Benutzer deaktiviert ist.

7. Deinstallation von Apps deaktiviert

Ist die Deinstallation von Anwendungen durch den Benutzer deaktiviert?

8. Berechtigungsrichtlinien

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

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

Jeder Eintrag enthält:

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

9. Anwendungen

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

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

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

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

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

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

9.1. Installationsart

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

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

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

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

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

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

9.2. Installationsbeschränkungen

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

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

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

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

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

9.3. Automatischer Update-Modus

Steuert den automatischen Update-Modus für die App.

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

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

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

9.4. Minimale Versionsnummer

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

9.5. Delegierte Berechtigungen

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

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

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

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

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

Paketberechtigungen: Ermöglicht den Zugriff auf den Status der Paketberechtigungen.

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

9.6. Bevorzugtes Netzwerk

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

9.7. Standard-Berechtigungsrichtlinie

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

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

Berechtigung erteilen: Eine Berechtigung automatisch erteilen.

Verweigern: Eine Berechtigung automatisch verweigern.

9.8. Verbundene Arbeits- und persönliche Anwendungen

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

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

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

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

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

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

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

9.10. Arbeitsbereich-Widgets

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

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

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

9.11. Benutzereinstellungen für die Steuerung

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

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

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

9.12. Deaktiviert

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

9.13. Credential-Anbieter erlauben

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

9.14. Konfigurationsverwaltung

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

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

9.15. Berechtigungsrichtlinien

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

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

9.16. Verfolgen Sie IDs

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

>

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

10. Standardmäßige Anwendungseinstellungen

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

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

10.1. Standard-App-Typ

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

10.2. Standardmäßige Anwendungsbereiche

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

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

10.3. Voreinstellungen für Anwendungen

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

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

11. Auswahl des privaten Schlüssels

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

des privaten Schlüssels vorhanden sind.

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

12. Wählen Sie Regeln für private Schlüssel

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

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

12.1. Alias für den privaten Schlüssel

Der Alias des privaten Schlüssels, der verwendet werden soll.

12.2. Muster für die URL

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

12.3. Paketnamen

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

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

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

Revision #36
Created 2025-12-09 17:58:20 UTC by Admin
Updated 2026-04-22 15:48:55 UTC by Admin