System

In diesem Abschnitt können Sie systembezogene Richtlinien konfigurieren.

1. Minimale API-Version

Die minimale zulässige Android API-Version.

2. Verschlüsselungsrichtlinie

Ob die Verschlüsselung aktiviert ist.

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

3. Automatische Datums- und Uhrzeit-Synchronisierung

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

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

4. Entwickleroptionen

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

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

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

5. Modus für Common Criteria

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

Deaktiviert (Standard): Deaktiviert den Common Criteria Modus.

Aktiviert: Aktiviert den Common Criteria Modus.

6. Memory Tagging Extension (MTE)

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

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

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

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

7. Inhalts-Schutz

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

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

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

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

8. Inhaltsunterstützung

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

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

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

9. Windows deaktivieren

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

10. Netzwerk-Notausgang

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

11. Standardaktivitäten

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

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

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

11.1. Empfänger-Aktivität

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

11.2. Aktion

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

11.3. Kategorie

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

12. Erlaubte Eingabemethoden

Gibt die zulässigen Eingabemethoden an.

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

12.1. Erlaubte Eingabemethoden

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

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

13. Erlaubte Bedienhilfen

Legt die zulässigen Barrierefreiheitsdienste fest.

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

13.1. Erlaubte Barrierefreiheitsdienste

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

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

14. Systemaktualisierungsrichtlinie

Konfiguration für die Verwaltung von Systemupdates.

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

14.1. Wartungsfenster (Nur für Fenster)

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

14.2. Systemupdate-Sperrzeiten

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

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

15. Standardmäßige Anmeldeinformationsanbieter

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

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

Revision #36
Created 2025-12-09 17:58:15 UTC by Admin
Updated 2026-04-22 15:48:57 UTC by Admin