datomo®
MOBILE
DEVICE MANAGEMENT

Richtlinien für Vollständig Verwaltete Geräte (COBO)

Version 14.10.2025 – Aktualisiert 16.02.2026

Übersicht

1 Konzept Vollständig Verwalteter Modus

In der Dokumentation zu „Mobilen Verwaltungskonzepten – Vollständig verwalteter Modus“ finden Sie eine generelle Beschreibung und Vorüberlegungen zu diesem Betriebsmodus.

2 Liste der Richtlinien für Vollständig Verwaltete Geräte

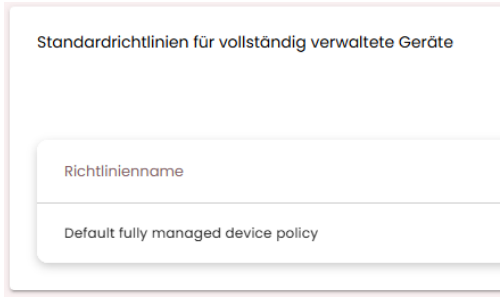
Die Richtlinien können im Tab **Richtlinien** unter **Vollständig Verwaltete Richtlinien für Geräte** verwaltet werden. Dort wird die **Liste** der Standard- und benutzerdefinierten Richtlinien angezeigt.

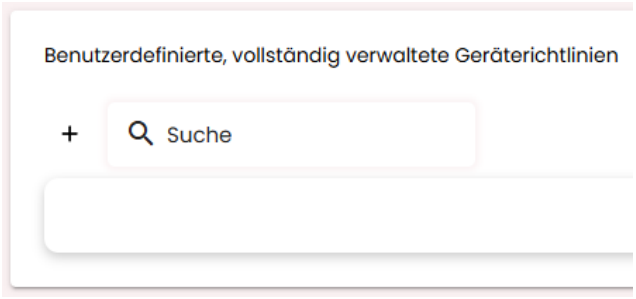
Die **Liste** bietet folgende **Optionen**:

- **Spalten anpassen**.
- **Richtliniendetails öffnen**: Durch Klicken auf die Richtlinienzeile oder die Aktion **Bearbeiten** in der Spalte **Aktionen** können Details der Richtlinie aufgerufen werden.
- **Richtlinie duplizieren**: Über die Option **Duplizieren** in der Spalte **Aktionen** kann eine Kopie der Richtlinie erstellt werden.
- **Richtlinie löschen**: Diese Option steht nicht für die Standardrichtlinie und für Richtlinien, die auf Geräten angewendet werden, zur Verfügung.

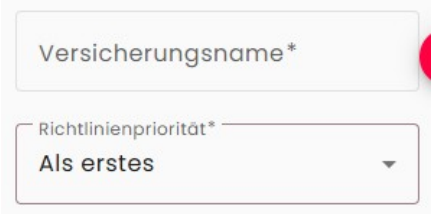
Anschließend können Sie entweder die bestehende Richtlinie **bearbeiten** oder eine **neue** erstellen.

Anschließend können Sie entweder die bestehende Richtlinie **bearbeiten** oder eine **neue** erstellen.



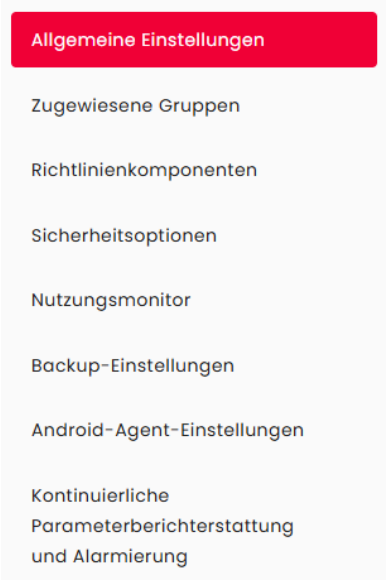


Um eine neue Richtlinie für Vollständig Verwaltete Geräte zu erstellen, tippen Sie auf das **+-Symbol** links. Beim Erstellen müssen Sie der Richtlinie einen Namen geben und die Priorität festlegen.



3 Richtliniendetails

Auf der linken Seite finden Sie die verfügbaren Optionen:



3.1 Allgemeine Einstellungen

In den allgemeinen Einstellungen finden Sie folgende **Optionen**:

- **Base Agent automatisch erneut installieren**

  Bei Veröffentlichung einer neuen Version des datomo MDM-Agenten werden die entsprechenden Operationen automatisch auf die der Richtlinie zugewiesenen Geräte übertragen.

- **Nicht kompatible Komponenten der Richtlinie automatisch entfernen**

  Wenn das Gerät die Richtlinie wechselt, werden alle zuvor installierten Komponenten (Apps und Konfigurationen), die in der aktuellen Richtlinie nicht verfügbar sind, automatisch deinstalliert.

- **Samsung Premium API aktivieren**

  Wenn diese Option aktiviert ist, erscheinen die zusätzlichen Felder **Premium-Lizenz**, **Ablaufdatum Premium-Lizenz** und **Samsung Attestation aktivieren**.
  Wenn die API aktiviert ist, sind Premium-Lizenz und Ablaufdatum erforderlich. Zusätzlich kann die Samsung-Attestation aktiviert werden, die eine erweiterte Gerätebestätigung von Samsung Knox bietet.
  Weitere Informationen zur Knox-Attestation finden Sie hier:
  https://docs.samsungknox.com/dev/knox-attestation"

- **SafetyNet Attestation (Play Integrity API)**

  Diese Option bietet eine Android-Attestation des Geräts. Wenn diese Option aktiviert ist, können Geräte mit entsperrtem Bootloader nicht registriert werden.
  Der Administrator kann das Intervall für die Geräteattestation festlegen:

  - Einmal, während der Registrierung
  - Stündlich
  - Alle 6 Stunden
  - Einmal am Tag
  - Einmal die Woche
  - Einmal im Monat

Weitere Informationen zur Play Integrity API finden Sie hier: https://developer.android.com/google/play/integrity

- **Als gelöscht markieren bei Deinstallation des Basis-Agents**

  Wenn der datomo MDM-Agent vom Gerät deinstalliert wird, kann das Geräteobjekt in der Admin-Konsole zusätzlich als gelöscht markiert werden, um die erneute Registrierung eines neuen Geräts unter demselben Eintrag zu erleichtern.

- **Remote-Zugriffsdienste aktivieren**

  Bei Aktivierung wird die datomo MDM Remote Access-Anwendung automatisch auf dem Gerät installiert. Der Administrator kann zudem die Sichtbarkeit der Einwilligung zur Initialisierung der Remote-Sitzung mit folgenden Optionen festlegen:

  - Vom Benutzer verwaltet: Der Benutzer kann entscheiden, ob die nächste Verbindung automatisch hergestellt wird oder eine Einwilligung erforderlich ist.
  - Bei jeder Verbindung erforderlich: Der Benutzer wird bei jeder Verbindung zur Einwilligung aufgefordert.
  - Automatische Verbindung: Der Benutzer wird nicht um Einwilligung gebeten.

- **Ortungsdienste aktivieren**

  Bei Aktivierung wird das datomo MDM-Standortmodul auf dem Gerät aktiviert.

  Zusätzlich kann der Administrator folgende Einstellungen vornehmen:

  - Standortintervall: Legt fest, in welchem Intervall der Standort erfasst wird (von 1 Minute bis zu 1 Monat).
  - Standortberichterstattung außerhalb der Spitzenzeiten deaktivieren: Wenn aktiviert, wird der Standort während definierter Nebenzeiten nicht erfasst.
  - Standortberichterstattung nach Agenteninstallation deaktivieren: Wenn aktiviert, wird der Standort unmittelbar nach der Aktivierung des Moduls nicht erfasst.

- **App-Monitoring-Dienst erzwingen**

  Bei Aktivierung wird eine zusätzliche Operation in die allgemeine Richtlinie aufgenommen, die als **App-Monitor-Dienst aktivieren** bezeichnet wird. Diese wird in die Warteschlange gestellt und an das Gerät gesendet, um den Benutzer aufzufordern, den datomo MDM-Zugriffsdienst zu aktivieren. Dies ist erforderlich für Funktionen, die Zugriff auf den Bildschirm des Geräts benötigen, wie z. B. die Liste erlaubter/verbotener Apps oder das Sammeln von Nutzungsdaten durch den Nutzungsmonitor.

- **Batterieoptimierung für Standort- und Nutzungsmonitor ignorieren**

  Für die Überwachung von Standort- und Nutzungsdaten (wie App-Nutzung, Datenverkehr) müssen unsere Agenten kontinuierlich im Hintergrund arbeiten. Das Android-Betriebssystem deaktiviert Apps, die nicht im Vordergrund verwendet werden, um den Batterieverbrauch zu optimieren. Unsere Apps müssen zur Liste der Apps hinzugefügt werden, die von der Batterieoptimierung ausgeschlossen sind. Diese Aktion muss vom Benutzer manuell bestätigt werden.
  Wenn diese Option aktiviert ist, erhält der Benutzer die Aufforderung, unsere Apps zur Liste der von der Batterieoptimierung ausgenommenen Apps hinzuzufügen.

- **Zusätzliche Daten zu Apps melden (App-Größe, Cache-Größe, Daten-Größe)**

  Der datomo MDM-Agent kann detailliertere Informationen zu Anwendungen abrufen, wie die App-Größe, Cache-Größe und Daten-Größe der App. Diese Option erfordert, dass der Benutzer die Nutzungszugriffsberechtigung auf dem Gerät aktiviert.

- **Gemeldete Anwendungen (Option für iOS-Geräte)**

  Diese Einstellung ermöglicht es dem Administrator zu entscheiden, ob auf iOS-Geräten alle Apps oder nur verwaltete Apps vom Gerätemonitor gemeldet werden.
  Verfügbare Optionen:

  - Alle Anwendungen melden
  - Nur verwaltete Anwendungen melden

- **Spitzenzeiten-Intervall**

  Legt fest, wie oft der Agent den Server kontaktiert. Verfügbare Optionen reichen von 5 Minuten bis einmal im Monat. Wenn deaktiviert, verbinden sich die Geräte nicht eigenständig mit dem Server. Nur durch die Admin-Konsole ausgelöste Aktionen führen zu einer Verbindung des Agents.

- **Spitzentage**

  Tage, an denen das Gerät eine Verbindung zum Server herstellt.

- **Spitzentage**

  Stunden, in denen das Gerät eine Verbindung zum Server herstellt.

- **Intervall der Gerätemonitorsitzungen**

  Intervall, in dem datomo MDM alle Gerätedaten sammelt.
  Verfügbare Optionen:

- **Anzahl der gespeicherten Gerätemonitorsitzungen**

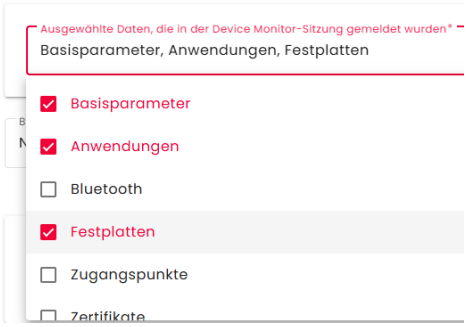
  Bestimmt die Anzahl der gespeicherten Gerätemonitorsitzungen (5-50).
  Achten Sie darauf, bei kurzen Intervallen und einer geringen Anzahl gespeicherter Sitzungen vorsichtig zu sein.

- **Anzahl der archivierten Gerätemonitorsitzungen**

  Bestimmt die Anzahl der archivierten Gerätemonitorsitzungen (0-150).
  Archivierte Gerätemonitorsitzungen sind weiterhin auf dem Server verfügbar, jedoch nicht in der Administratorkonsole einsehbar.

- **Ausgewählte Daten, die in der Device Monitor-Sitzungen gemeldet wurden (verfügbar für Android)**

  Auf Android-Geräten können alle Daten vom Gerät oder nur ein Teil davon gesammelt werden. Bei Auswahl von **Ausgewählt** kann der Administrator entscheiden, welche Daten vom Gerät erfasst werden sollen: Basisparameter, Anwendungen, Bluetooth, Festplatten, Zugangspunkte, Zertifikate, Geräteadministratoren, Gerätekonten, Software-Updates, SIM-Karten.



- **Benachrichtigung zur Geräteinaktivität**

  Diese Option bezieht sich auf das Spitzenintervall. Wenn der Agent im festgelegten Intervall keine Verbindung zum Server herstellt, kann der Administrator eine Benachrichtigung darüber erhalten. Die Inaktivitätszeit kann von 1 Tag bis zu 3 Monaten festgelegt werden.

- **Bei Überschreiten der Inaktivität löschen (wipe)**

  Zusätzlich zur Benachrichtigung kann der Administrator festlegen, dass das Gerät gelöscht wird, wenn die Inaktivität überschritten wird.

- **Bei Überschreiten der Inaktivität des Gerät als gewiped markieren**

  Zusätzlich zur Benachrichtigung kann der Administrator festlegen, dass das Gerät als gelöscht markiert wird, wenn die Inaktivität überschritten wird. Dies entfernt die alten Gerätedaten aus der Administratorkonsole, sodass das Gerät auf demselben Eintrag erneut registriert werden kann.

- **Bestätigungsmodus für Base Agent**

  Diese Option legt fest, wie Operationen, die an das Gerät gesendet werden, behandelt werden:

  - **Silent Modus** - Operationen werden ohne Benutzerinteraktion ausgeführt.
  - **Information Modus** - Der Benutzer wird über anstehende Operationen in den Benachrichtigungen informiert.
  - **Confirmation Modus** - Der Benutzer muss die Ausführung von Aktionen auf dem Gerät genehmigen.

- **Base Agent Administratorkennwort**

  Passwort zum Entsperren blockierter Apps (Richtlinienoption).

- **Synchronisierungsintervall**

  Mit dieser Option wird die automatische Zeitsynchronisierung vom NTP-Server in einem festgelegten Intervall (von 1 Stunde bis 1 Woche) aktiviert.

  Wenn das Intervall aktiviert ist, sind der Name und der Port des NTP-Servers erforderlich.

- **Benachrichtigung wenn der Status der Richtlinie sich auf dem Gerät ändert**

  Bei Aktivierung wird der Administrator über das Alarm-System eine Meldung über die Änderung des Richtlinienstatus erhalten.

- **Gerätelimit pro Benutzer**

  Mit dieser Option kann die Anzahl der Geräte begrenzt werden, die während der Benutzerregistrierung erstellt werden. Der Wert muss numerisch sein, von 1 bis 999999.

- **Zeitraum der Agentenbetriebsprotokolle (iOS / macOS)**

  Zeitraum, in dem die Operationsprotokolle auf Apple-Geräten gespeichert werden. Wählbar zwischen einem Tag und drei Monaten.

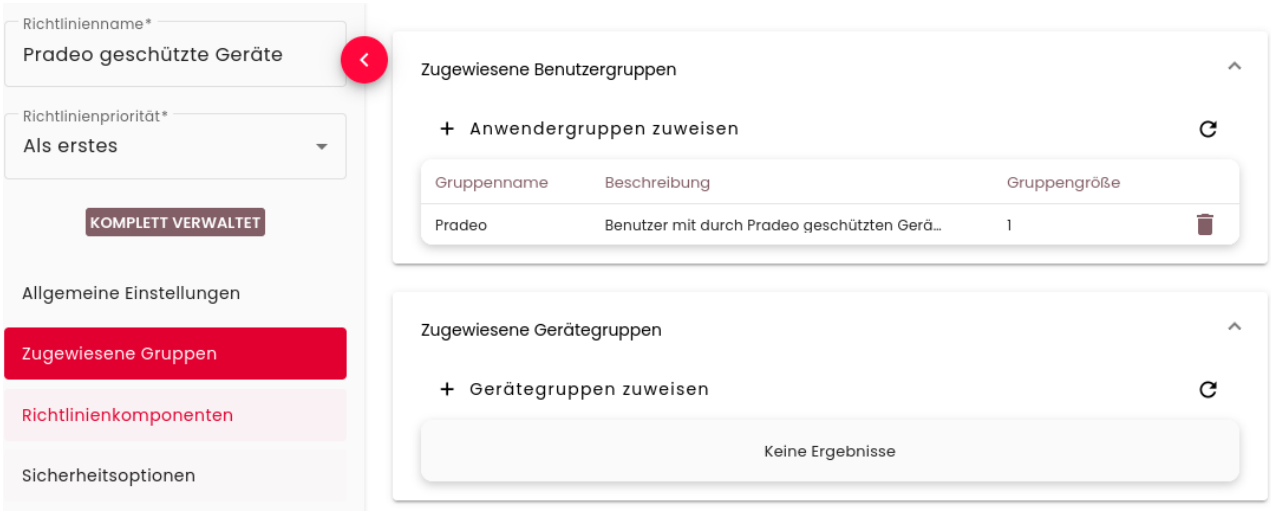
- **Standard-Telefonanwendung (Android)**

  Es kann ein benutzerdefinierter Paketname als Standard-Telefonanwendung auf dem Gerät festgelegt werden. Gilt nur für Apps, die Telefonfunktionen bieten. Die Option ist ab Android 14+ verfügbar.

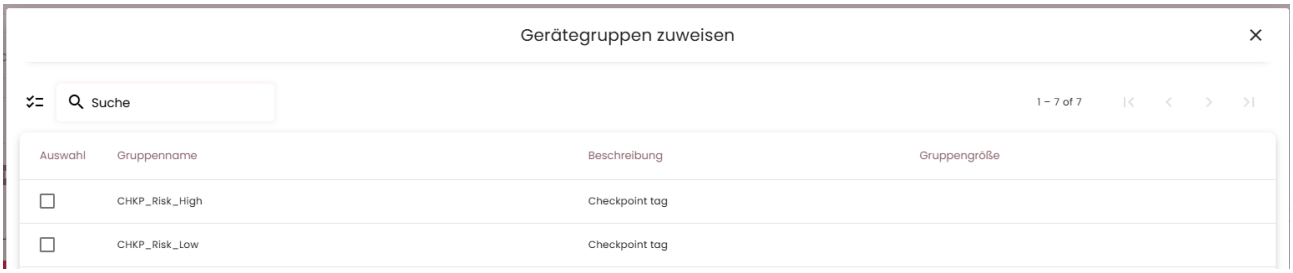
3.2 Zugewiesene Gruppen

Benutzer-, Geräte- und Smart-Gruppen können der Richtlinie zugewiesen werden - **außer der Standardrichtlinie**. Diese Richtlinie kann keiner Gruppe zugeordnet werden, dementsprechend fehlt dieser Eintrag in den Richtlinieneinstellungen.

Der Administrator kann mehrere Gruppen gleichzeitig auswählen, indem er die **Schaltfläche + Anwendergruppen-/Gerätegruppen zuweisen** verwendet.



Beim Auswählen von Gruppen wird die Gruppengröße angezeigt, mit der Möglichkeit, die Liste der zugewiesenen Benutzer oder Geräte anzuzeigen.
Smart-Gruppen sind in der Geräteliste mit dem zusätzlichen Tag [SMART] verfügbar.

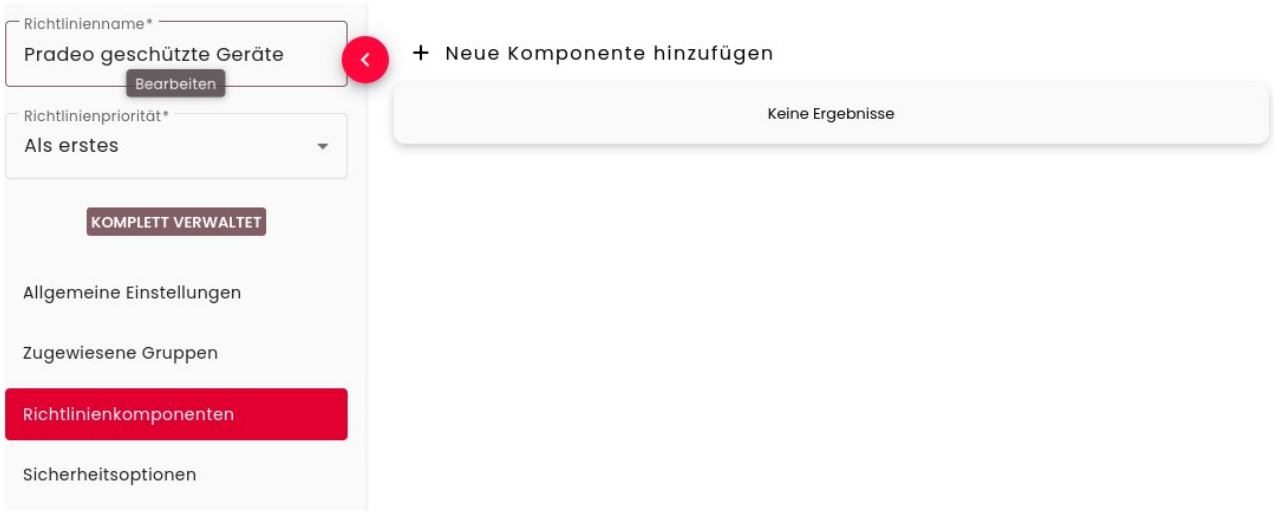


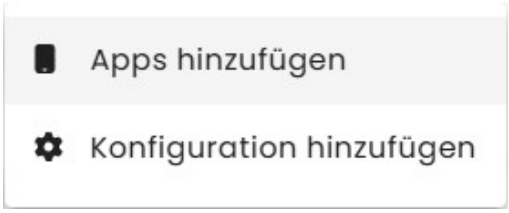
Jede Zuweisung / Trennung einer Gruppe von der Richtlinie kann die Richtlinie auf den Geräten ändern.

***HINWEIS**: Geräte erhalten die höchste Richtlinie aus der Liste, basierend auf der Gruppenzuweisung (Benutzer- oder Gerätegruppe).*

3.3 Richtlinienkomponenten

Hier können Sie Komponenten zu Ihrer Richtlinie hinzufügen. Sie können zwischen Anwendungen oder Konfigurationen wählen.





Die Liste der Anwendungen und Konfigurationen zeigt nur Elemente an, bei denen die Optionen **Automatische Installation** und **Automatische Aktualisierung** deaktiviert sind.

Beim Hinzufügen einer Anwendung sehen wir Details zur Anwendung, wie: Symbol, Name, Version, Anwendungsgruppen, zugewiesene Plattformen. Zusätzlich sehen wir, ob die Anwendung im verwalteten Google Play Store aktiviert ist und ob die Anwendung eine verwaltete Konfiguration hat.

Beim Hinzufügen einer Konfiguration sehen wir die Konfigurationsdetails, wie: Name, Konfigurationstyp, Erstellerdaten, zugewiesene Plattformen. Außerdem gibt es Informationen zur Verfügbarkeit des Unternehmensstores.

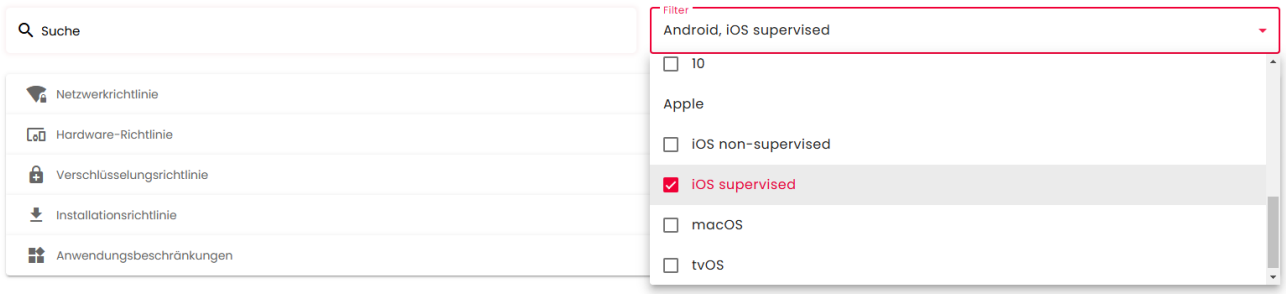
Den der Richtlinie zugewiesene Komponenten werden in der Reihenfolge von oben nach unten ausgeführt. Die Reihenfolge kann durch Verschieben der Elemente in der Liste geändert werden (ziehen Sie das erste Symbol auf der linken Seite).

Nach dem Hinzufügen von Komponenten zur Liste gibt es folgende Optionen:

- **Anzahl der Wiederholversuche** (nur für Apps):
  - Installation obligatorisch - Bei einem Fehlschlag wird der Versuch in der nächsten Peak-Zeit wiederholt.
  - Einmaliger Installationsversuch – Nach dem ersten Fehlschlag schlägt die Operation fehl und wird nicht automatisch wiederholt.
  - Mehrere Installationsversuche – Der Administrator kann angeben, wie oft die Installation automatisch wiederholt wird.
- **Fehler ignorieren** - Wenn aktiviert, wird das nächste Richtlinien-Element ausgeführt, auch wenn das vorherige fehlgeschlagen ist.
- **Unabhängig** - Wenn aktiviert, wird die Ausführung nicht auf das Ende des vorherigen Komponenten warten (Fehler, Erfolg oder Abbruch).
- **Android Verwaltete Konfiguration** - Diese Option ist für Android-Anwendungen mit verwalteten Konfigurationen verfügbar. Wenn aktiviert, kann der Administrator die verwaltete Konfiguration der Anwendung festlegen, sodass für verschiedene Geräte (die verschiedenen Richtlinien zugewiesen sind) unterschiedliche Konfigurationseinstellungen für die Anwendung gelten. Die Liste der Konfigurationsparameter hängt von der Anwendung selbst ab.

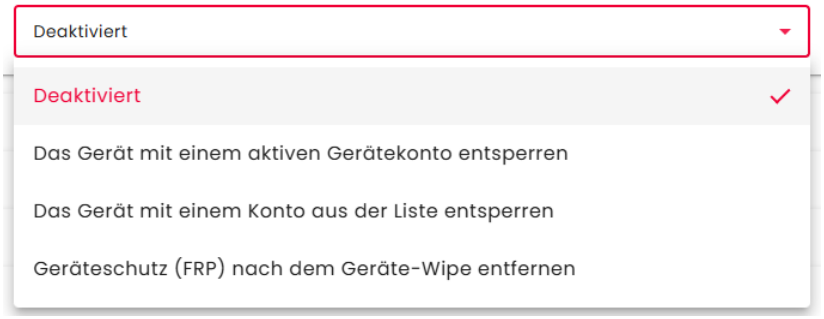
3.4 Sicherheitsoptionen

Die List der Sicherheitsoptionen kann nach Plattformen gefiltert werden, um Optionen gezielt für die gewünschte(n) Plattform(en) auszuwählen.



3.4.1 Löschrichtlinie

- Daten-Wipe bei einem Wechsel der SIM-Karte (Android)
- Wipe ausführen, wenn keine SIM-Karte erkannt wird (Android)
  (Daten-Wipe bei einem Wechsel der SIM-Karte muss aktiviert sein)
- Speicherkarte wipen (Android)
  (Daten-Wipe bei einem Wechsel der SIM-Karte muss aktiviert sein)
- Unternehmens-Wipe bei Jailbreak-Detektion (iOS)
- Wipe bei Root-Detektion (Android)
- Aktivierungssperre erlauben (iOS)
- Zurücksetzen auf Werkseinstellungen sperren (Android / iOS)
- Geräteschutz (FRP) (Android)

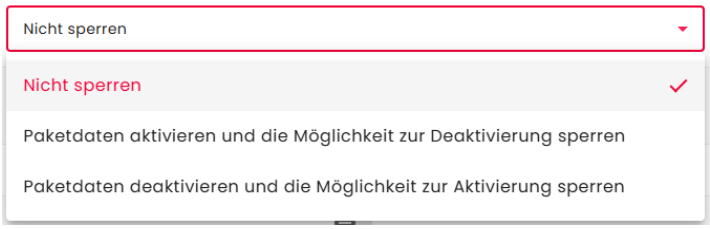


Weitere Details zu den Optionen der Löschrichtlinie finden Sie in der separaten Dokumentation zu dem Thema.

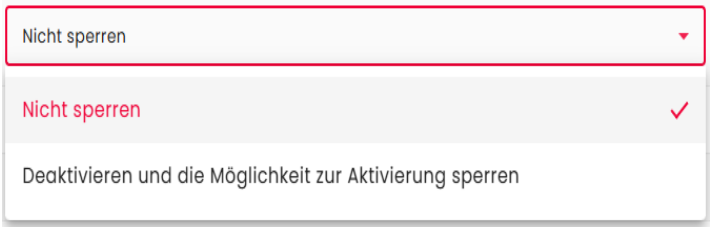
3.4.2 Netzwerkrichtlinie

- WLAN sperren (Android / iOS)
  - Manuelle WLAN-Konfiguration sperren (Android / iOS / Windows)
  - Automatische Verbindung zu WLAN-Hotspots sperren (Android / iOS supervised / Windows)
  - Anzeige von WLAN-Hotspots sperren (Windows)
  - Hotspot-Änderungen deaktivieren (iOS supervised)
- WLAN im Schlafmodus aktiviert halten (Android)
- Verhindern Sie, dass WLAN ausgeschaltet wird (Android / iOS supervised)
  Verhindert, dass WLAN in den Einstellungen oder im Kontrollzentrum deaktiviert wird. Erwägen Sie, den Flugmodus in den Hardwareeinschränkungen zu blockieren, da dies dazu führen kann, dass diese Einstellungen umgangen werden. Es verhindert nicht die Auswahl des zu verwendenden Wi-Fi-Netzwerks
- Bluetooth sperren (Android / iOS supervised)
  Wenn Bluetooth gesperrt ist, können auf Samsung-Geräten folgende Optionen freigeschaltet werden:
  - Erweitertes Audio-Verteilungsprofil (A2DP) aktivieren
  - Audio/Video Fernbedienungsprofil (AVRCP) aktivieren
  - Handsfree-Profil (HFP) aktivieren
  - Headsetprofil (HSP) aktivieren
  - Adressbuchprofil (PBAP) aktivieren
  - Serial Port Profil (SPP) aktivieren
  - Dateiaustausch über Bluetooth aktivieren

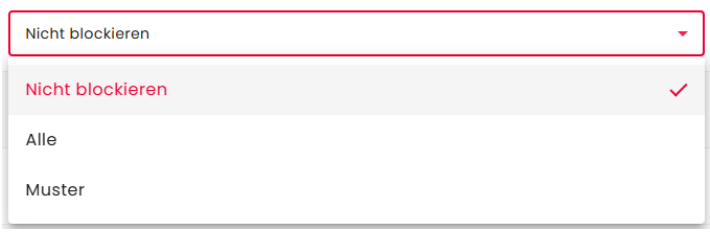
- Mobildaten sperren (nur Samsung-Geräte)



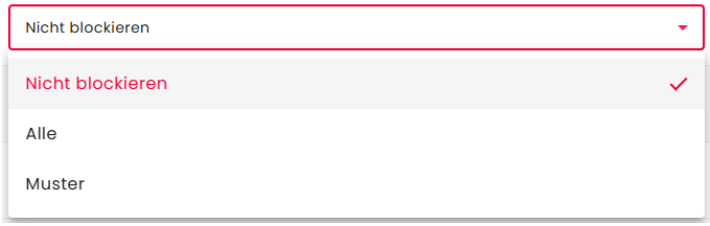
- Mobile Daten beim Roaming sperren (Android / Windows)



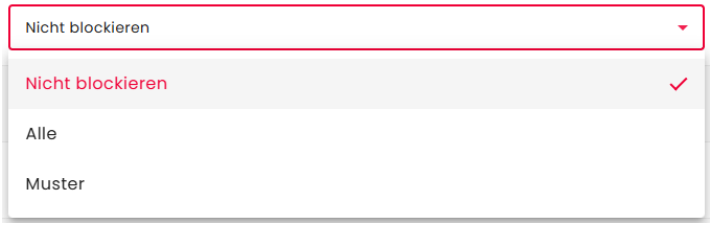
- WLAN-Tethering sperren (Android / Windows)
- USB Tethering sperren (Android)
- VPN über mobile Daten sperren (Windows)
- Geräteinformationen an Microsoft senden sperren (Windows)
- VPN über mobile Daten beim Roaming sperren (Windows)
- Erstellen von VPN Konfigurationen sperren (iOS supervised)
- Eingehende MMS sperren (Android)
- Zurücksetzen der Netzwerkeinstellungen deaktivieren (Android)
- VPN-Einstellungen deaktivieren (Android)
- Änderung des Mobilfunktarifs deaktivieren (iOS supervised)
- Ändern von eSIMS Einstellungen deaktivieren (iOS supervised)
- Private DNS Einstellungen blockieren (Android)
- Ausgehende Anrufe blockieren (Android)



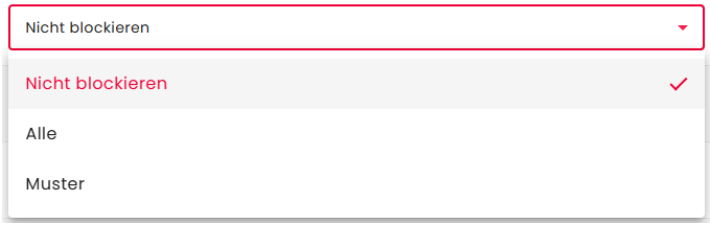
- Eingehende Anrufe blockieren (Android)



- Eingehende SMS Nachrichten blockieren (Android)



- Eingehende SMS Nachrichten blockieren (Android)



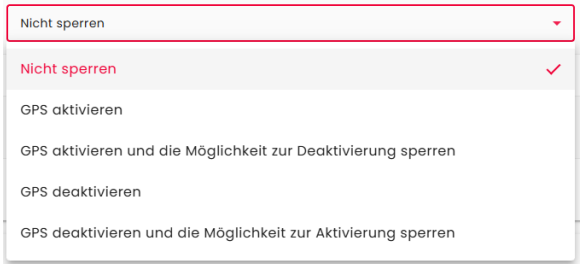
- Änderungen der verwalteten Netzwerkseinstellungen deaktivieren (Android)
- Liste der verwalteten WLAN-Konfigurationen überwachen (Android)
- Globalen Hintergrundabruf beim Roaming blockieren (iOS supervised)
- Sprachanrufe blockieren, wenn das Gerät mit einem Passcode gesperrt ist (iOS supervised)
- Änderung der Mobilfunkdaten durch Apps deaktivieren (iOS supervised)
- Host-Kopplung deaktivieren (iOS supervised)
- Bluetooth-Konfiguration blockieren (Android)
- Konfiguration für mobile Netzwerke blockieren (Android)
- Cell-Broadcast-Konfiguration blockieren (Android)
  (Es blockiert die Konfiguration der Wireless Emergency Alerts (WEA) und AMBER-Warnungen)

- SMS-Nachrichten deaktivieren (Android)
- RCS-Nachrichten blockieren (Samsung, iOS)
- 2G-Mobilfunk verbieten (Android)
- Ultrabreitband (UWB) verbieten (Android)
- 2G-Mobilfunk verbieten (Android)
- Ultrabreitband (UWB) verbieten (Android)
- Mobilfunknetz blockieren (Samsung)
- Änderungen an den Einstellungen für Remote-Management-Teilen sperren (macOS)
- Änderungen der Einstellungen zum Datei-teilen sperren (macOS)
- Änderungen der Einstellungen zum Internet-teilen sperren (macOS)
- Medienfreigabeeinstellungen ändern sperren (macOS)
- Änderungen der Einstellungen für die Freigabe von Remote-Apple-Events sperren (macOS)
- Satellietenverbindungen sperren (iOS)
- Änderungen der Einstellungen für Bluetooth-Teilen sperren (macOS)
- Änderungen der Einstellungen zum Drucker-teilen sperren (macOS)

Weitere Details zu den Netzwerk-Richtlinienoptionen finden Sie in der separaten Dokumentation zu dem Thema.

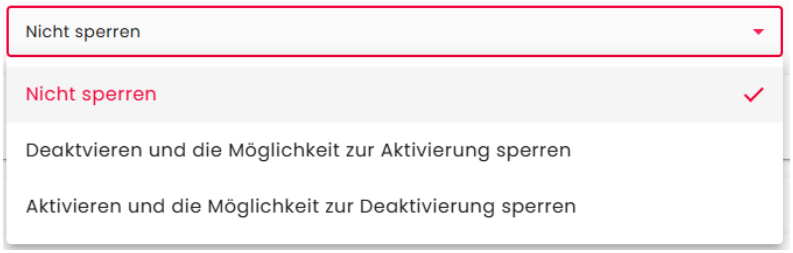
3.4.3 Standortrichtlinie

- GPS sperren (nur Samsung-Geräte)



- Nur den GPS-Modus aktivieren (Android)

- Ortungsdienste sperren (Windows)



- Android Standortsperre (Android)

Weitere Details zu den Standortrichtlinien finden Sie in der separaten Dokumentation zu dem Thema..

- Aktualisierungsrichtlinie
  - Hinweise zu Software-Updates verzögern (iOS supervised / macOS)
    (Aktiviert die Optionen: Software-Updates verzögern um und Verzögern Sie kleinere Software-Updates um)
  - Sichtbarkeit der nicht-OS-Software-Updates für Benutzer verzögern (macOS)
    (Aktiviert die Optionen: Software-Updates verzögern um und Verzögern Sie die Nicht-Betriebssystem-Softwareaktualisierung um)
  - Software-Updates verzögern um (iOS supervised / macOS)
    (Mögliche Optionen: Deaktiviert, 1-90 Tage)
  - Verzögern Sie kleinere Software-Updates um (macOS)
    (Mögliche Optionen: Deaktiviert, 1-90 Tage)
  - Verzögern Sie die Nicht-Betriebssystem-Softwareaktualisierung um (macOS)
    (Mögliche Optionen: Deaktiviert, 1-90 Tage)
  - Erzwingen Sie verzögerte größere Software-Updates (macOS)
    (Aktiviert die Option: Verzögern Sie ein großes Software-Update um)
    - Verzögern Sie ein großes Software-Update um (macOS)
      (Mögliche Optionen: Deaktiviert, 1-90 Tage)
  - Systemversion verwalten (Samsung E-FOTA)
  - OTA Update sperren (Android)

    OTA Update sperren mit folgenden Optionen:

- Keine Richtlinie - es wird keine OTA-Richtlinie angewendet
- Automatisch - Updates werden automatisch installiert
- Zeitplan - Administrator kann ein Zeitfenster (Tage und Uhrzeit) festlegen, in dem das Update installiert wird
- Aufgeschoben - Systemupdates werden um 30 Tage verschoben

- Zebra OTA-Updates aktivieren (nur Zebra-Geräte)
- Automatische Software-Updates deaktivieren (nur Samsung-Geräte)
- Automatische Suche nach Updates deaktivieren (nur Samsung-Geräte)
  HINWEIS: Verfügbar auf Samsung-Geräten mit Premium-Lizenz

Weitere Details zu der Aktualisierungsrichtlinie finden Sie in der separaten Dokumentation zu dem Thema.

3.4.4 Hardware-Richtlinie

- Kamera sperren (Android, iOS supervised, macOS)
- Manuelle Abmeldung deaktivieren (Samsung, macOS)
- Manuelle Entfernung des Arbeitsprofils deaktivieren (Android)
- USB Media Player sperren (nur Samsung-Geräte)
- Ermöglichen Sie, dass Geräte von einem nicht gekoppelten Gerät in die Wiederherstellung gestartet werden (OS supervised)
- Entwicklermodus sperren (Android)
- Taskmanager sperren (nur Samsung-Geräte)
- NFC sperren (Samsung, Andorid, Windows)
- Ausgehende NFC Beam Verbindungen sperren (Android)
- SD-Karte sperren (Android, Windows)
- Kopieren & Einfügen sperren (Windows)
- Screenshots sperren (Samsung, iOS, macOS, Windows)

- Fernüberwachung des Bildschirms durch die Classroom-App deaktivieren (iOS, macOS)
  *(Wird bei **S**creenshots sperren automatisch aktiviert)*

- Verhindern Sie, dass Siri benutzergenerierte Inhalte aus dem Web abfragt (OS supervised)
- automatische Tastaturkorrektur deaktivieren (OS supervised)
- USB Dateimanager sperren (Android, Windows)
- Multiwindow-Modus sperren (nur Samsung-Geräte)
- Safe Mode sperren (Android)
- Flugmodus sperren (Android)
- USB Zubehör im gesperrten Zustand erlauben (OS supervised)
- Pop-Up für die Einrichtung von in der Nähe befindlicher, neuer Geräte deaktivieren (OS supervised)
- AirPrint deaktivieren (OS supervised)
  - Speichern von AirPrint Zugangsdaten in der iCloud deaktivieren (OS supervised)
  - Vertrauenswürdige Zertifikate für TLS Druckkommunikation erforderlich (OS supervised)
  - Erkennen von AirPrint Druckern mit iBeacon deaktivieren (OS supervised)
- eingehende AirPlay-Anfragen deaktivieren (tvOS)
- Automatische MacOS Entsperrung deaktivieren (OS supervised, macOS)
- iCloud Desktop- und Dokumentendienste sperren (macOS)
- Touch-ID daran hindern, ein Gerät zu entsperren (iOS non-supervised, iOS suervised, macOS)
- Biometrische Änderung deaktivieren (OS supervised)
- Erzwungenes Biometrie-Timeout (macOS)
  (Mögliche Optionen: 1 Tag - 2 Wochen)

- Inhaltsspeicherung sperren (macOS)
  HINWEIS: Option ist veraltet
- Nachschlagen deaktivieren (OS supervised, macOS)
- Tastaturkürzel deaktivieren (OS supervised)
- QuickPath-Tastatur deaktivieren (OS supervised)
- Rechtschreibprüfung der Tastatur deaktivieren (OS supervised)
- Schlafmodus des Geräts sperren (tvOS)
- Benutzer daran hindern, die Zugangsdaten im verwalteten Schlüsselspeicher zu konfigurieren (Android)
- Siri deaktivieren (OS supervised)
- Siri bei gesperrtem Gerät deaktivieren (iOS supervised)
- Verbindungen zu Siri-Servern zum Diktieren deaktivieren (iOS supervised)
- Verbindungen zu Siri-Servern für Übersetzungszwecke deaktivieren (iOS supervised)
- Automatische Übertragungs von Diagnoseberichten an Apple deaktivieren (iOS supervised, macOS)
- Control Center nicht auf dem Sperrbildschirm anzeigen (iOS supervised)
- Fotostream blockieren (iOS supervised)
  HINWEIS: Wird von Apple nicht mehr unterstützt
- Möglichkeit, nicht vertrauenswürdige TLS-Verbindungen herzustellen, blockieren (iOS supervised)
- Deaktiviert Backups von Enterprise Books (iOS supervised)
- Aktualisierung der Zertifikatsvertrauensdatenbank nicht zulassen (iOS supervised)
- Deaktiviert eine Synchronisation von Metadaten von Enterprise Books (iOS supervised)
- Änderung der Benachrichtigungseinstellungen deaktivieren (iOS supervised)
- Deaktiviert die Benachrichtigungshistorie auf dem Sperrbildschirm (iOS supervised)
- Deaktiviert die heutige Benachrichtigungshistorie auf dem Sperrbildschirm (iOS supervised)

- Geräte, die von diesem Gerät eine AirPlay-Anfrage erhalten, müssen einen Pairing-Pass verwenden
- Geräte, die von diesem Gerät eine AirPlay-Anfrage erhalten, müssen einen Pairing-Pass verwenden (iOS supervised)
- Verschlüsseltes Backup erzwingen (iOS supervised)
- Pairing von Uhren deaktivieren (iOS supervised)
- Handgelenkerkennung erzwingen (iOS supervised)
- Passcode-Änderung deaktivieren (iOS supervised, macOS)
- Änderung des Gerätenamens blockieren (iOS supervised, macOS)
- Änderung der Diagnoseübermittlung deaktivieren (iOS supervised)
- Diktat deaktivieren (iOS supervised, macOS)
- Bildschirmzeit deaktivieren (iOS supervised)
- Änderung des Hintergrundbilds deaktivieren (Android, iOS supervised, macOS)
- Live Voicemail deaktivieren (iOS supervised)
- Obszönitätsfilter des Assistenten erzwingen (iOS supervised, macOS)
- Deaktivieren der automatischen Dimmung bei iPad-Geräten mit OLED-Displays (iOS supervised)
- iPhone-Spiegelung verbieten (iOS supervised, macOS)
- Schreibtools deaktivieren (iOS supervised, macOS)
- Alle Tastenkürzel deaktivieren (Android)

Weitere Details zu der Hardware-Richtlinie finden Sie in der separaten Dokumentation zu dem Thema.

3.4.5 Verschlüsselungsrichtlinie

- Interne Speicherverschlüsselung (Android, iOS)
- Sicheren Start deaktivieren (Android)

- Modus Gemeinsame Kriterien aktivieren (Android)

Weitere Details zu der Verschlüsselungsrichtlinie finden Sie in der separaten Dokumentation zu dem Thema.

3.4.6 Installationsrichtlinie

- Anwendungs-Installer sperren (Android, iOS supervised, Windows)
  (Aktiviert die Option: Unbekannte Quellen sperren und Anwendungsverwaltung deaktivieren automatisch)
  - Benachrichtigung,wenn die Anwendungsinstallion gesperrt ist (Android)
  - USB Debugging erlauben (Android)
  - Unbekannte Quellen sperren (Android)
  - Anwendungsverwaltung deaktivieren (Android)
  - Kontoerstellungen unter Verwendung von Google Play deaktivieren (Android)
- USB-Debugging auf Geräten mit Windows 10 Mobile erlauben (Windows)
- Unbekannte Quellen auf Geräten mit Windows 10 Mobile sperren (Windows)
- Manuelle Installation von ROOT-Zertifikaten sperren (Windows)
- App Store deaktivieren (iOS supervised)
  (Benutzer können weiterhin Host-Apps (iTunes, Configurator) verwenden, um ihre Apps zu installieren oder zu aktualisieren.)
- Benutzer die interaktive Installation von Konfigurationsprofilen und Zertifikaten verbieten (iOS supervised)

Weitere Details zu den Installationsrichtlinien finden Sie in der separaten Dokumentation zu dem Thema.

3.4.7 Anwendungsbeschränkungen

- Sprachaufzeichnungsanwendung sperren (nur Samsung-Geräte, Windows)
- Google Play Protect nicht erzwingen (Android)

- Einstellungen sperren (Android)
  (Aktiviert die Option: Uhrzeiteinstellungen sperren)
  - Uhrzeiteinstellungen sperren (nur Samsung-Geräte)
- Automatisches Einstellen von Datum und Uhrzeit erzwingen (Android, iOS supervised, tvOS)
- Browser sperren (Android, iOS supervised, Windows)
- Kontoänderungen deaktivieren (Android)
- Erstellen von Mailkonten sperren (Android, Windows)
- Benutzerverwaltung deaktivieren (nur Samsung-Geräte)
  (Verfügbar für Geräte, die die Verwaltung zusätzlicher Benutzerkonten unterstützen)
- Samsung Galaxy Store deaktivieren (nur Samsung-Geräte)
- Deinstallation von Systemanwendungen deaktivieren (iOS supervised)
- AirDrop deaktivieren (iOS supervised)
- Teilen von verwalteten Dokumenten über AirDrop sperren (iOS)
- AirDrop Funktion Kennwort teilen deaktivieren (iOS supervised, macOS)
- Teilen von Daten aus nicht verwalteten Anwendungen sperren (iOS)
- Teilen von Daten aus verwalteten Apps sperren (iOS)
  (Aktiviert die Optionen Nicht verwalteten Apps das Lesen von Kontakten von verwalteten Kontakt-Konten erlauben und Verwalteten Apps das Schreiben von Kontakten auf nicht verwaltete Kontakt-Konten erlauben.)
  - Nicht verwalteten Apps das Lesen von Kontakten von verwalteten Kontakt-Konten erlauben (iOS)
  - Verwalteten Apps das Schreiben von Kontakten auf nicht verwaltete Kontakt-Konten erlauben (iOS)
- AutoFill-Funktion von Kennwörtern in Apps deaktivieren (iOS supervised, macOS)
- Aktivieren Sie die Einschränkungen Freigabe von Daten aus nicht verwalteten/verwalteten Apps nicht zulassen für die Kopier- und Einfügefunktion (iOS)

- Keine Anfrage von Kennwörten von in der Nähe befindlicher Geräte erlauben (iOS supervised, macOS, tvOS)
- Vor dem automatischen Ausfüllen von Kennwörtern oder Kreditkarteninformationen ist eine Authentifizierung mit Face-/Touch-ID erforderlich (iOS supervised)
- private iCloud-Relay deaktivieren (iOS supervised, macOS)
- iCloud Fotobibliothek deaktivieren (iOS, macOS)
- Apple Music deaktivieren (iOS supervised, macOS)
- iCloud Backups deaktivieren (iOS supervised)
- iCloud Dokumentensynchronisierung deaktivieren (iOS supervised, macOS)
- iCloud Keychain-Synchronisierung deaktivieren (iOS supervised, macOS)
- iCloud Lesezeichen-Synchronisierung deaktivieren (macOS)
- iCloud Mail deaktivieren (macOS)
- iCloud Kalender deaktivieren (macOS)
- iCloud Erinnerungen deaktivieren (macOS)
- iCloud Adressbuch deaktivieren (macOS)
- iCloud Notizen deaktivieren (macOS)
- iTunes deaktivieren (iOS supervised)
- iTunes Anwendung zum Teilen von Dateien deaktivieren (macOS)
- Zwingen Sie den Benutzer, bei jeder Transaktion sein iTunes-Passwort einzugebe (von Apple nicht mehr unterstützt) (iOS)
- Spotlight Internet-Suche deaktivieren (iOS supervised, macOS)
- Koppeln von Apple TV mit der Remote App oder Control Center Widget deaktivieren (tvOS)
- Maximal erlaubte Altersfreigabe für Filme (iOS, tvOS)
  (Mögliche Optionen: Deaktiviert, Keine, Alle, NC-17, R, PG-13, PG, G)
- Maximal erlaubte Altersfreigabe für TV-Sendungen (iOS, tvOS)
  (Mögliche Optionen: Deaktiviert, Keine, Alle, TV-MA, TV-14, TV-PG, TV-G, TV-Y7, TV-Y)

- Maximal erlaubte Altersfreigabe für Anwendungen (iOS, tvOS)
  (Mögliche Optionen: Deaktiviert, Keine, Alle, 17+, 12+, 9+, 4+)
- Finde mein Gerät in der Find My-App deaktivieren (iOS supervised)
- Finde meine Freunde in der Find My-App deaktivieren (iOS supervised)
- Änderungen an Meine Freunde suchen deaktivieren. (iOS supervised)
- Handoff deaktivieren (iOS, macOS)
- Ortungsdienste für Suchfunktion sperren (Windows)
- Speichern als Funktion in MS Office sperren (Windows)
- Teilen über Funktion in MS Office sperren (Windows)
- Kontoänderungen auf Apple Geräten deaktivieren (iOS supervised)
- Verwendung von TLS 1.0/1.1 in Safari erlauben (iOS, macOS)
- Einen Benutzer am Hinzufügen von App-Clips hindern (iOS supervised)
  (Dadurch werden alle vorhandenen App-Clips auf dem Gerät entfernt)
- Personalisierte Apple-Werbung einschränken (iOS)
- Deinstallation der Anwendung deaktivieren (iOS, tvOS)
  (Diese Option verhindert die Deinstallation der verwalteten Apps)
- Aktivieren Sie die Möglichkeit, die Sicherung vom Google-Konto wiederherzustellen (Android)
- Vertrauenswürdigkeit von Unternehmens-Apps deaktivieren (iOS)
- In-App-Käufe deaktivieren (iOS)
- Passbook Benachrichtigungen auf dem Sperrbildschirm blockieren (iOS)
- Erzwingen Sie eine eingeschränkte Anzeigenverfolgung (iOS)
- automatische Ausfüllen in Safari deaktivieren (iOS supervised, macOS)
- JavaScript in Safari deaktivieren (iOS)
- Popups in Safari blockieren (iOS)
- Safari-Betrugswarnung aktivieren (iOS)

- Von Safari akzeptierte Cookies (iOS)
  (Mögliche Optionen: Nie, Von besuchten Websites, Stets)
- Game Center deaktivieren (iOS supervised, macOS)
- Hinzufügen von Freunden zum Game Center deaktivieren (iOS supervised, macOS)
- Multiplayer-Spiele blockieren (iOS supervised, macOS)
- Entfernen von Apps deaktivieren (iOS supervised)
- Verhindern Sie das automatische Herunterladen von Apps, die auf einem anderen Gerät gekauft wurden (iOS supervised)
- Entfernen Sie die Registerkarte **Book Store** aus der Bücher-App (iOS supervised, macOS)
- Download der Apple Books-Medien deaktivieren, die als Erotik gekennzeichnet sind (iOS, macOS, tvOS)
- iMessage-App deaktivieren (iOS supervised)
- Blenden Sie explizite Musik- oder Videoinhalte aus, die Sie im iTunes Store gekauft haben (iOS supervised, macOS, tvOS)
- Verbindung zu Netzlaufwerken in der Dateien-App deaktivieren (iOS supervised)
- Verbindung zu allen angeschlossenen USB-Geräten in der Dateien-App deaktivieren (iOS supervised)
- News-App deaktivieren (iOS supervised)
- Podcasts deaktivieren (iOS supervised, macOS)
- Apple Music Radio deaktivieren (iOS supervised)
- freigegebenen Fotostream deaktivieren (iOS)
- FaceTime-App ausblenden (iOS supervised)
- Automatische Klassen beitritt in Classroom erzwingen (iOS supervised, macOS)
  (Erfordert die Classroom-App.)
- Erfordert Genehmigung zum Verlassen von Klassen in Classroom (iOS supervised, macOS)
  (Erfordert die Classroom-App.)

- Erzwingen Sie eine unaufgeforderte App- und Gerätesperre in Classroom (iOS supervised, macOS)
  (Erfordert die Classroom-App.)
- Erzwingen Sie die unaufgeforderte Bildschirmbeobachtung im Klassenzimmer (iOS supervised, macOS)
  (Erfordert die Classroom-App.)
- Inhaltserfassung auf dem Gerät deaktivieren (Android)
- Inhaltsvorschläge auf dem Gerät deaktivieren (Android)
- Konfiguration der Standard-Applikationen nicht zulassen (Android)
- Verhindern der Installation von Anwendungen aus alternativen Anwendungsquellen (iOS supervised)
- Verteilung von Webanwendungen verbieten (iOS)
- Erstellung neuer Genmoji verbieten (iOS)
- Image Playground verbieten (iOS, macOS)
- Image Wand verbieten (iOS)
- Verhindern, dass das System Text in der Handschrift des Benutzers generiert (iOS)
- Apple Intelligence-Berichte deaktivieren (iOS, macOS)
- Verstecken von Anwendungen deaktivieren (iOS)
- Sperren von Anwendungen deaktivieren (iOS)
- Änderung Standard Browser sperren (iOS)
- Änderung Standard Telefonanwendung sperren (iOS)
- Änderung Standard Nachrichtenanwendung sperren (iOS)
- Externe Intelligence-Integrationen für Siri sperren (iOS)
- Anonymen-Modus für externe Intelligence-Anbieter erzwingen (iOS supervised, macOS)
- IPhone-Widgets auf dem Mac sperren (iOS)
- Mail Privatsphärenschutz deaktivieren (iOS supervised)

- Smarte Mail-Antworten deaktivieren (iOS, macOS)
- Manuelle Mail-Zusammenfassungen sperren (iOS, macOS)
- Notizen-Transkribierung sperren (iOS, macOS)
- Notizen-Transkribierung-Zusammenfassungen sperren (iOS, macOS)
- Safari Inhalt-Zusammenfassungen sperren (iOS, macOS)
- Visuelle Intelligence-Zusammenfassungen sperren (iOS)
- Leeren des Safari-Verlaufs sperren (iOS, macOS)
- Safari Privates Surfen sperren (iOS, macOS)
- Anwendung Freeform und iCloud-Synchronisation sperren (macOS)

Weitere Details zu den Anwendungsbeschränkungen finden Sie in der separaten Dokumentation zu dem Thema.

3.4.8 Apprichtlinien

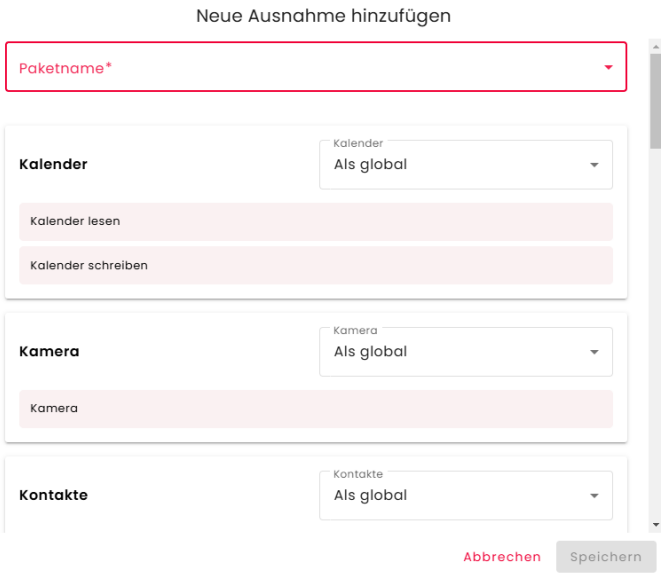
- Anwendungsrichtlinie für Android Geräte (Android) Verfügbare Optionen:
  - Nicht nach einem Kennwort fragen
  - nach Sperrcode fragen - Der Benutzer wird aufgefordert, den Sperrcode einzugeben, um alle Anwendungen zu öffnen.
  - Nach Administratorkennwort fragen - Der Benutzer wird aufgefordert, das Administratorpasswort einzugeben, um alle Anwendungen zu öffnen.
- Wenn Ausnahmen von der globalen Richtlinie erforderlich sind, können wir eine anwendungsspezifische Richtlinie definieren. Verfügbare Optionen:
  - Anwendungspaketname - Paketname der Anwendung
  - Deinstallationsperren - Wenn aktiviert, wird die Deinstallation des angegebenen Paketnamens blockiert.
  - Stop erzwingen sperren - Wenn aktiviert, wird die Möglichkeit, den angegebenen Paketnamen auf dem Gerät zu stoppen, blockiert.

- Löschen der Daten sperren - Wenn aktiviert, wird die Möglichkeit, die Daten des angegebenen Paketnamens auf dem Gerät zu löschen, blockiert.

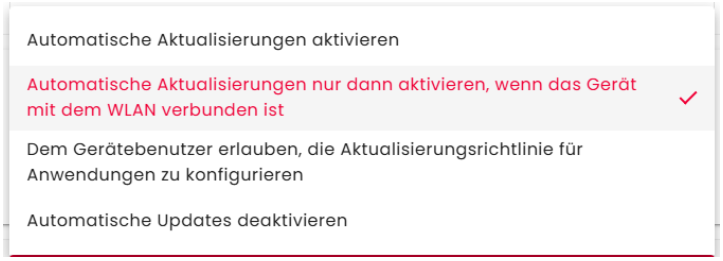
- Kennwortrichtlinie - Es können Ausnahmen von der globalen Richtlinie für den angegebenen Paketnamen festgelegt werden.

- Zeitüberschreitung des Anwendungskennworts (Android)
  Timeout für die Android-Anwendungsrichtlinie, wenn der Zugriff auf die Anwendung durch ein Passwort (Sperrcode oder Administratorkennwort) geschützt ist.
  (Mögliche Werte: 1 Minute bis 15 Minuten.)
- Benachrichtigung, wenn eine Anwendung durch ein Kennwort gesperrt wurde (Android)
  Benutzerdefinierter Text, der angezeigt wird, wenn der Zugriff auf eine Anwendung durch ein Passwort (Sperrcode oder Administratorpasswort) geschützt ist.
- Ablehnungsliste für Android-Anwendungen (Android)
  Liste der Paketnamen, die auf der Blockliste stehen. Der Zugriff auf diese Paketnamen wird blockiert.
- Benachrichtigung, wenn Anwendung auf der Blacklist steht (Android)
  Benutzerdefinierter Text, der angezeigt wird, wenn versucht wird, eine Anwendung zu öffnen, die sich auf der Blockliste befindet.
- Apple Anwendungsrichtlinie (iOS supervised)
  Globale Anwendungsrichtlinie für Apple-Geräte.
  Mögliche Werte:
  - Anwendungen aus der Liste blockieren
  - Anwendungen aus der Liste erlauben

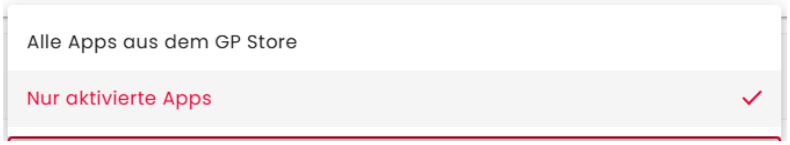
- Apple-Anwendungsliste (iOS supervised)
  Liste der Apple-Paketnamen, die in der Apple-Anwendungsrichtlinie enthalten sein sollen (Zulassungs- oder Sperrliste).
- Device-Owner-Anwendungsrichtlinie (Android)
- Globale Device-Owner-Anwendungsberechtigungsrichtlinie (Android)
- Ausnahmen für Anwendungsberechtigungen
  Der Administrator kann Ausnahmen von der globalen Berechtigungsrichtlinie hinzufügen. Für jede Anwendung können Ausnahmen für folgende Berechtigungskategorien festgelegt werden:
  - Kalender
  - Kamera
  - Kontakte
  - Standort
  - Mikrofon
  - Telefon
  - Sensoren
  - SMS
  - Speicher



- Richtlinieneinstellungen der automatisch aktualisierten verwalteten Anwendung Google Play (Android)



- Verfügbarkeit der Apps im MGP-Store (Android)



Weitere Details zu den Apprichtlinien finden Sie in der separaten Dokumentation zu dem Thema.

3.4.9 Samsung KSP

- Samsung Knox Service Plugin aktivieren - nur für Samsung-Geräte
  Wenn aktiviert, wird das Samsung Knox Service Plugin automatisch installiert, und die verwaltete Konfiguration kann festgelegt werden.

  Weitere Details zu den Konfigurationsoptionen des Samsung Knox Service Plugin finden Sie in der separaten Dokumentation zu dem Thema.

3.4.10 Zebra OEMConfig

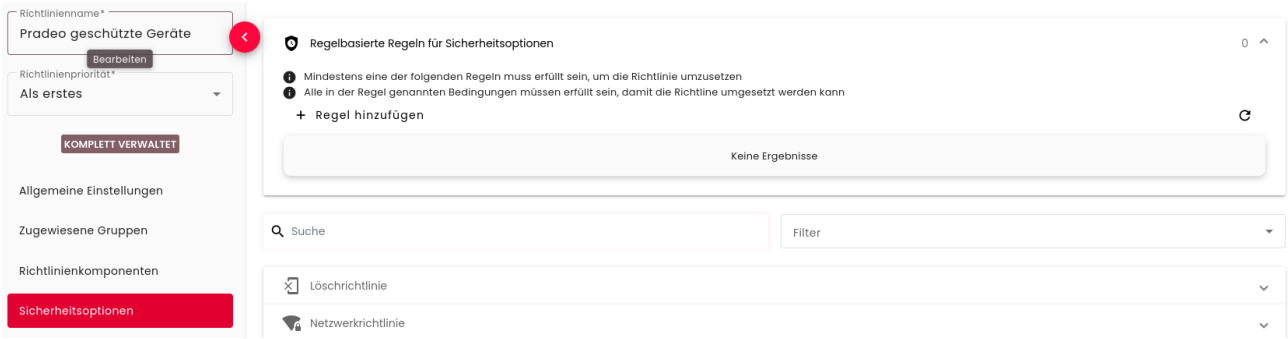
- Zebra OEMConfig aktivieren - nur für Zebra-Geräte ab Android 11
  Wenn aktiviert, wird Zebra OEMConfig Applikation automatisch installiert, und die verwaltete Konfiguration kann festgelegt werden.

  Weitere Details zu den Konfigurationsoptionen von Zebra OEMConfig finden Sie in der separaten Dokumentation zu dem Thema.

3.5 Regelbasierte Regeln für Sicherheitsoptionen

In Richtlinien für Vollständig Verwaltete Geräte kann der Administrator regelbasierte Sicherheitsoptionen basierend auf Standort, Zeitperiode oder Geschwindigkeit definieren.
Um ein regelbasiertes Verhalten zu implementieren, muss der Administrator zunächst Regeln hinzufügen, auf deren Grundlage die regelbasierten Sicherheitsoptionen auf dem Gerät angewendet werden.

Auf der Registerkarte Sicherheitsoptionen gibt es ein Feld Regelbasierte Sicherheitsoptionen mit der Schaltfläche Regel hinzufügen.



Es ist möglich, mehrere Regeln in einer regelbasierten Richtlinie hinzuzufügen. Jede Regel kann Bedingungen aus drei Typen enthalten:

3.5.1 Zeitbedingung -

Einschränkungen werden angewendet während:

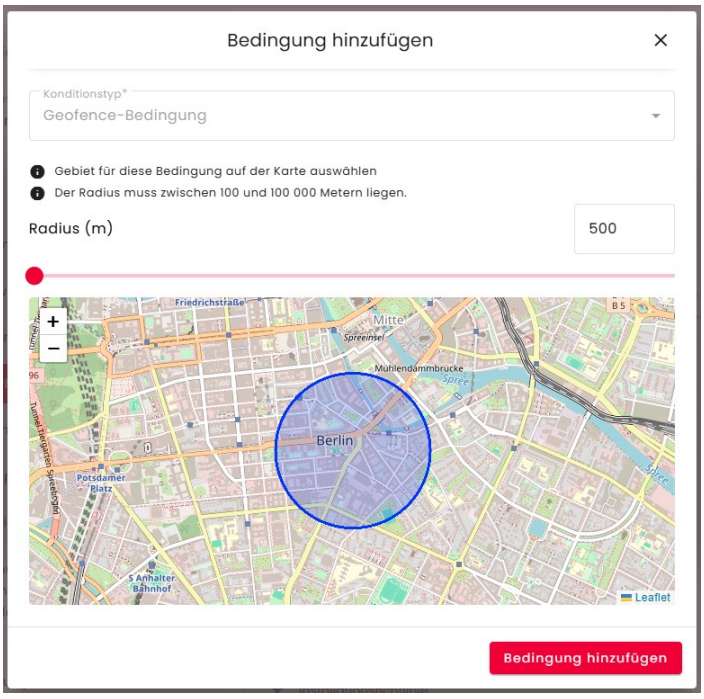
- Hauptzeit
- Nebenzeit

3.5.2 Bedingung Geschwindigkeit

Einschränkungen werden angewendet, wenn das Gerät mit einer Geschwindigkeit über dem Limit (50–200 km/h) bewegt wird.

3.5.3 Geofence-Bedingung

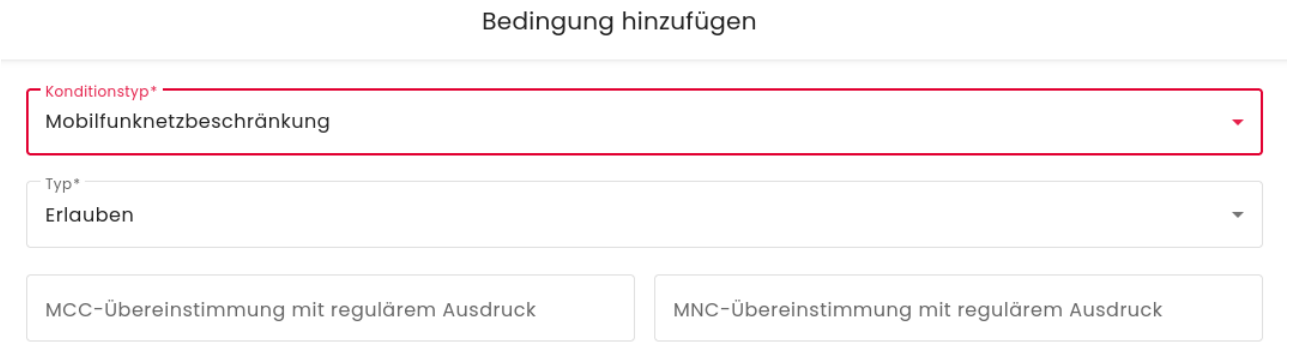
Einschränkungen werden angewendet, wenn der Gerätestandort aus dem definierten Bereich gemeldet wird.



3.5.4 Mobilfunknetz-Einschränkung

Definiert, ob regelbasierte Einschränkungen gelten, abhängig vom verbundenen Mobilfunknetz. Sie umfasst drei Felder:

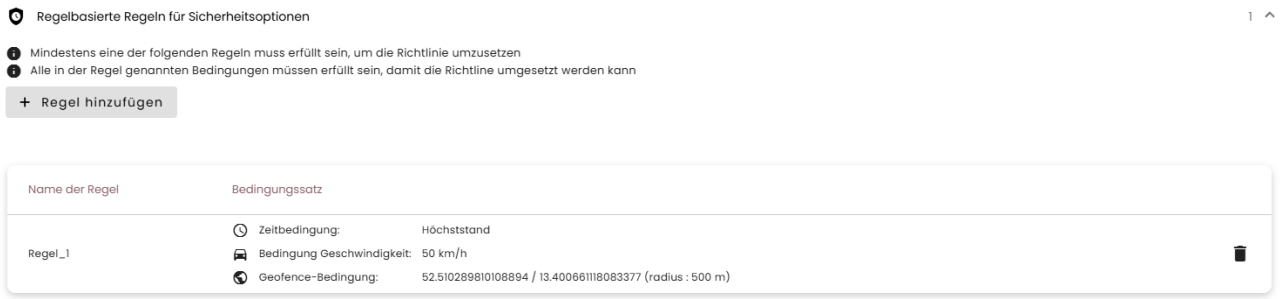
- Typ, wo Sie erlauben oder verweigern auswählen, um das Regelverhalten festzulegen,
- MCC (Mobile Country Code), wo Sie einen regulären Ausdruck eingeben, um den Mobilfunkländercode zu vergleichen,
- und MNC (Mobile Network Code), wo Sie einen regulären Ausdruck eingeben, um den Mobilfunknetzcode zu vergleichen.



Mindestens eine der definierten Regeln muss erfüllt sein, um die Einschränkungsrichtlinie anzuwenden.

Alle Bedingungen innerhalb der Regel müssen erfüllt sein, um die Einschränkungsrichtlinie anzuwenden.

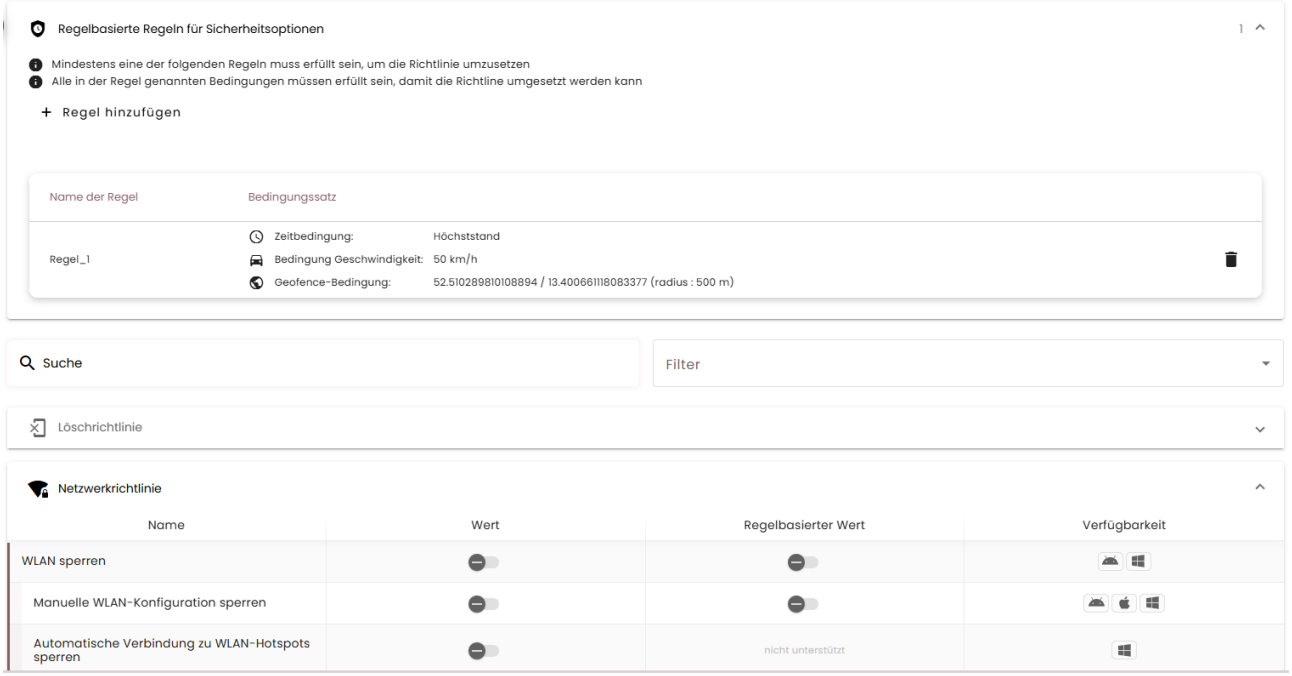
Nach dem Hinzufügen von Regeln sieht die Liste wie folgt aus:



Basierend auf dem obigen Beispiel (siehe Bild) muss mindestens eine der Regeln (mit den Namen „Regel_1“) erfüllt sein, um die Einschränkungsrichtlinie anzuwenden.

Das bedeutet, dass das Gerät entweder den ersten Standort im Geräte-Peak oder den zweiten Standort jederzeit betreten muss.

Regelbasierte Sicherheitsoptionen können in der Standardliste der Sicherheitsoptionen (zusätzliche Spalte neben der Standard-Einstellung) festgelegt werden.



3.6 Mobiler Bedrohungsschutz

Mobile Threat Defense (MTD) von Pradeo ist eine Sicherheitslösung, die speziell entwickelt wurde, um mobile Geräte vor verschiedenen Cyberbedrohungen wie Malware, Phishing-Angriffen, unsicheren Netzwerkverbindungen und riskanten Geräteeinstellungen – etwa Jailbreaking oder Rooting – zu schützen. MTD überwacht kontinuierlich das Geräteverhalten, die App-Aktivitäten sowie den Netzwerkverkehr, um solche Bedrohungen in Echtzeit zu erkennen und zu blockieren, sodass sensible Daten auf mobilen Geräten sicher bleiben.

Die Integration von MTD in datomo MDM ermöglicht eine zentralisierte Sicherheitsverwaltung und -durchsetzung. Diese Lösung bietet Administratoren eine vereinfachte Möglichkeit, Bedrohungen zu überwachen sowie Antworten wie Behebungsmaßnahmen automatisiert durchzuführen, die sich auf die Nutzererfahrung auswirken. Nutzer profitieren von nahtlosem Hintergrundschutz ohne zusätzliche Interaktionen.

Diese Option ist zusätzlich kostenpflichtig. Für weitere Informationen wenden Sie sich bitte an unseren Support.

Weitere Details zum Molbien Bedrohungsschutz finden Sie in der separaten Dokumentation zu dem Thema.

3.7 Nutzungsmonitor

Diese Anwendung überwacht und meldet die Benutzeraktivität an den Essentials MDM-Server, einschließlich eingehender und ausgehender Sprachanrufe, genutzter Paketdaten (WiFi, GPRS) und bietet Einblicke in eingehende und ausgehende SMS- und MMS-Nachrichten.

- Aktivieren des Nutzungsmonitor-Dienstes
  Wenn diese Option aktiviert ist, wird der Android-Nutzungsmonitor-Agent automatisch mit den folgenden Optionen installiert:
  - Gerätedaten nach einen Neustart berichten
    Wenn aktiviert, sammelt und sendet der Nutzungsmonitor Daten nach einem Neustart des Geräts.
  - Melden Sie den Datenverkehr über WLAN
    Intervall für die WLAN-Datenmeldung. Mögliche Optionen:
    - Nicht melden
    - Alle 15 Minuten
    - Alle 30 Minuten
    - Stündlich
    - alle 6 Stunden
    - Täglich
    - Alle 3 Tage
    - jede Woche
    - alle 2 Wochen
    - Jeden Monat
    - Alle 3 Monate

- Melden Sie den Datenverkehr über GPRS
  Intervall für die GPRS-Datenmeldung. Mögliche Optionen:
  - Nicht melden
  - Alle 15 Minuten
  - Alle 30 Minuten
  - Stündlich
  - alle 6 Stunden
  - Täglich
  - Alle 3 Tage
  - jede Woche
  - alle 2 Wochen
  - Jeden Monat
  - Alle 3 Monate

Zusätzlich kann der Nutzungsmonitor erweiterte Daten melden, wie:

- Gerätestatus berichten
  Wenn aktiviert, werden Daten gemeldet, wenn das Gerät ein- oder ausgeschaltet wird.
- Zeit zum Sperren/Entsperren des Bildschirms berichten
  Wenn aktiviert, wird die Zeit gemeldet, zu der der Bildschirm gesperrt/entsperrt wurde.
- Anwendungsnutzung berichten
  Wenn aktiviert, wird die Zeit gemeldet, zu der Anwendungen im Vordergrund genutzt wurden.
  - Erweiterte Parameter melden
    Intervall für die Meldung erweiterter Parameter. Mögliche Optionen:
    - Nicht melden
    - Alle 15 Minuten
    - Alle 30 Minuten

- Stündlich
- alle 6 Stunden
- Täglich
- Alle 3 Tage
- jede Woche
- alle 2 Wochen
- Jeden Monat
- Alle 3 Monate

3.8 Backup-Einstellungen

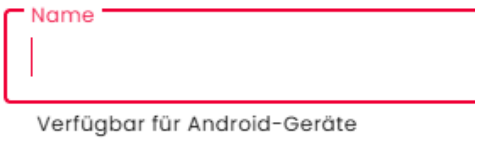
- Einstellungen für die Backup-Synchronisierung (nur Backup der Kontakte unterstützt)
  Der Administrator kann das Synchronisierungsintervall festlegen.
  - Sicherungsintervall
    Mögliche Optionen:
    - Deaktiviert
    - Einmal am Tag
    - Einmal die Woche
    - Einmal im Monat
  - Mit Aktionen wie Kontakte sichern und Kontakte wiederherstellen kann der Administrator Kontakte von einem Gerät auf ein anderes übertragen (auch zwischen Android- und Apple-Geräten).
- Synchronisierung von Geschäftskontakten
  Zusätzlich zur Kontaktsynchronisierung ist es möglich, Geschäftskontakte auf das Gerät zu synchronisieren, basierend auf Benutzergruppen in der MDM-Lösung. Die Datenquelle kann einfach aus integrierten IDPs wie Active Directory eingerichtet werden. Verfügbare Optionen:
  - Grundlegender Synchronisierungstyp
    Diese Option bestimmt das Standardverhalten der Synchronisierung:
    - Keine der Kontakte - standardmäßig werden keine Kontakte synchronisiert

        - Nur Kontakte von Benutzergruppen - alle Kontakte, die in den Benutzergruppen verfügbar sind, deren Mitglied der Benutzer des Geräts ist
        - Kontakte aller Gruppen - alle Kontakte aus allen Gruppen werden synchronisiert
    - Kontaktsynchronisation der zusätzlichen Gruppen
      Zusätzlich zum Standardverhalten ermöglicht diese Option das Hinzufügen von Benutzern aus den zusätzlichen Benutzergruppen im System.
    - Synchronisierungsintervall für Geschäftskontakte
      Mögliche Optionen:
        - Deaktiviert
        - Einmal am Tag
        - Einmal die Woche
        - Einmal im Monat
    - Standard-Mobiltelefonnummer für Geschäftskontakte
      Bei der Synchronisierung von Geschäftskontakten können wir auswählen, welche Telefonnummer des Nutzers als Standardmarkiert wird. Mögliche Optionen:
        - Handy-Nummer
        - Büro-Telefon

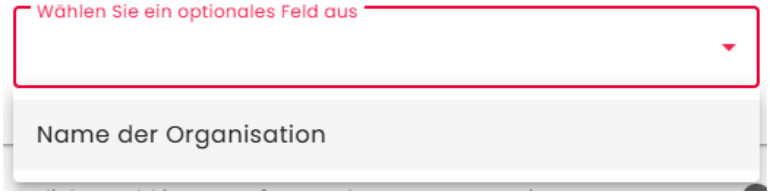
3.9 Android-Agent-Einstellungen

Hier können Sie eine Reihe von Werten festlegen, die im Agenten angezeigt werden.

- Auf dem Gerät angezeigter Organisationsname
  Mit dieser Option können Sie den Namen der Organisation konfigurieren, der auf dem Sperrbildschirm des Geräts angezeigt wird.



- Optionales Feld auswählen



Zusätzlich können wir als Teil des Organisationsnamens ein Feld aus dem datomo MDM-System angeben. Die Auswahl zeigt das ursprüngliche Organisationsnamenfeld sowie alle benutzerdefinierten Felder der Organisation. Um diesen Wert zum Organisationsnamenfeld anzuzeigen, das auf den Geräten angezeigt wird, müssen wir den _ _VALUE_ _ Token in das Textfeld oben (Organisationsnamenfeld) einfügen.

- **Z**usätzliches Feld im Hauptfenster des Agenten anzeigen
  (Verfügbar für Android- und macOS-Geräte)
  Diese Option zeigt den ausgewählten Feldwert im Hauptbereich unseres Android Base Agent und macOS Agent an.
  - Wert der zweiten Zeile der Überschrift datomo Base Agent

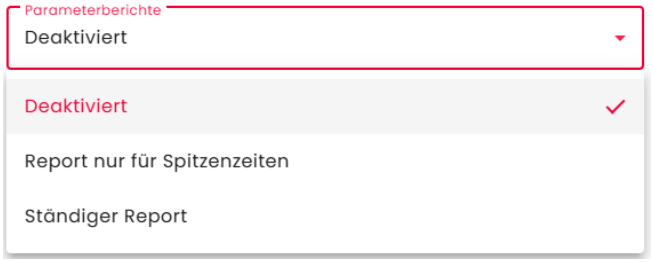
Als Feld kann der ursprüngliche Organisationsname oder ein beliebiges benutzerdefiniertes Organisationsfeld ausgewählt werden.

  - Gerätedetailfelder im Agenten (Android, macOS)
    Liste der Gerätefelder, die im Android Base Agent und macOS Agent angezeigt werden. Verfügbare Felder sind:
    - Gerätefelder
    - Benutzerdefinierte Gerätefelder
    - Benutzerfelder
    - Benutzerdefinierte Benutzerfelder
    - SIM-Kartenfelder
    - Benutzerdefinierte SIM-Kartenfelder

3.10 Kontinuierliche Parameterberichterstattung und Alarmierung

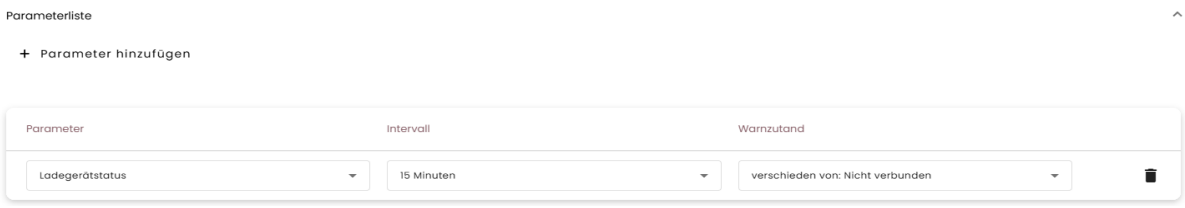
Dies ermöglicht es dem System, mehrere Parameter vom Gerät zu melden, wie z. B. Ladezustand, Batteriestand, freier RAM-Speicher, Batteriespannung, Batterietemperatur, Batteriezustand und niedriger Batteriestand. Zusätzlich gibt es die Option, ausgewählte Werte aus bestimmten Dateien des Geräts zu melden.

- Parameterberichte
  Zunächst müssen wir auswählen, ob die Parameter dauerhaft (zu jeder Zeit) oder nur während des Peak-Zeitraums gemeldet werden sollen.



  Wenn diese Option ausgewählt wird, können definierte Parameter und Werte aus Anwendungsdateien ausgewählt werden.

- Parameterliste
  Mit dieser Option können wir Parameter wie Ladezustand, Signalstärke, Batteriestand, freien RAM-Speicher, Batteriestrom, Batterietemperatur, Batteriezustand, niedrigen Batteriestand und Verfügbarkeit des Remote-Access-Ports hinzufügen. Für jeden Parameter kann das Meldungsintervall festgelegt werden (von 1 Minute bis 1 Stunde) sowie verschiedene Alarmbedingungen. Wenn eine Bedingung erfüllt ist, wird eine Benachrichtigung erzeugt und im Benachrichtigungsbereich angezeigt.



Liste der Alarmierungsbedingungen:

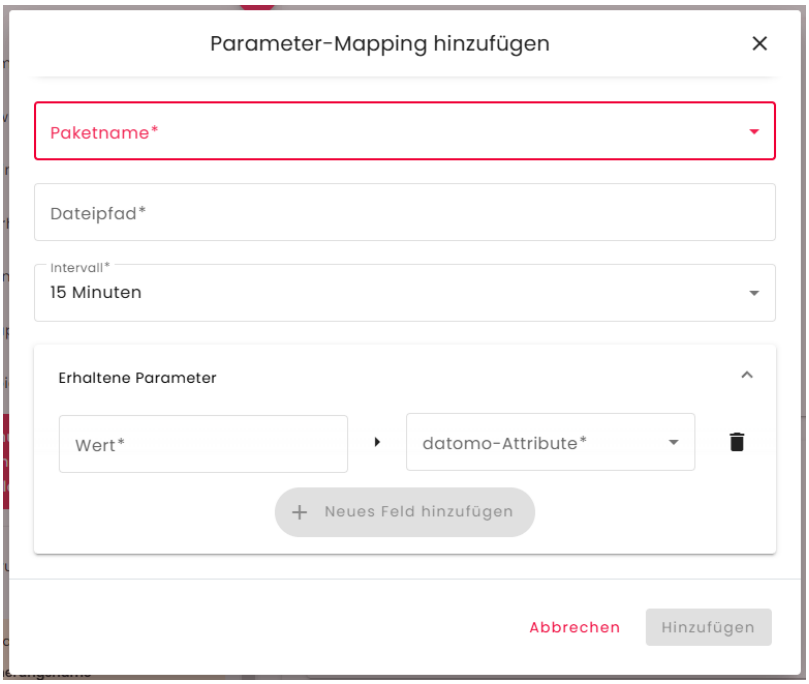
- Ladegerätstatus
  - verschieden von: Nicht verbunden
  - verschieden von: In Verbindung gebracht
  - verschieden von: unbekannter Status
- Signalstärke
  - niedriger als - 45dBM
  - niedriger als - 80dBM
  - niedriger als - 91dBM
  - niedriger als – 100dBM
- Batterie Level
  - niedriger als 10%
  - niedriger als 15%
  - niedriger als 20%
  - niedriger als 30%
  - niedriger als 40%
  - niedriger als 50%
- Arbeitsspeicher frei
  - niedriger als 10%
  - niedriger als 20%
  - niedriger als 30%
  - niedriger als 40%
  - niedriger als 50%

- Batteriespannung
  - höher als 2V
  - höher als 3V
  - höher als 4V
  - höher als 5V
  - höher als 6V
  - höher als 7V
  - höher als 8V
  - höher als 9V
  - höher als 10V
- Batterietemperatur
  - höher als 20°C
  - höher als 30°C
  - höher als 40°C
  - höher als 50°C
  - höher als 60°C
  - höher als 70°C
  - höher als 80°C
  - höher als 90°C
  - höher als 100°C
- Batteriezustand
  - verschieden von: Unbekannt
  - verschieden von: Gut
  - verschieden von: Überhitzen

        - verschieden von: Tot
        - verschieden von: Überspannung
        - verschieden von: Nicht näher bezeichneter Fehler
        - verschieden von: Kalt
    - Niedriger Batteriestand
        - gleich: Nicht gemeldet
        - gleich: Gemeldet
    - Verfügbarkeit des Ports für den Fernzugriff
        - gleich: Standard-Port für den Fernzugriff ist nicht verfügbar

    HINWEIS: Nicht alle Parameter werden von allen Android-Herstellern angezeigt.

- Parameter aus der Anwendungsdatei
  Eine Funktion zum Auslesen von Werten aus einer angegebenen Datei und deren Anzeige auf dem Reiter Gerätedetails.
  Der Administrator kann Folgendes angeben:
    - Paketname - Paketname der Anwendung, die die Daten speichert
    - Dateipfad - Pfad zur Datei, aus der die Werte abgerufen werden (unterstützte Dateiformate: json, xml, ini)
    - Intervall - Intervall der Wert-Synchronisation
    - Erhaltene Parameter:
        - Wert - Name des Parameters, der aus der Datei abgerufen wird.
        - datomo-Attribute - Benutzerdefiniertes Gerät- oder Benutzerfeld, in dem der Wert gespeichert wird.



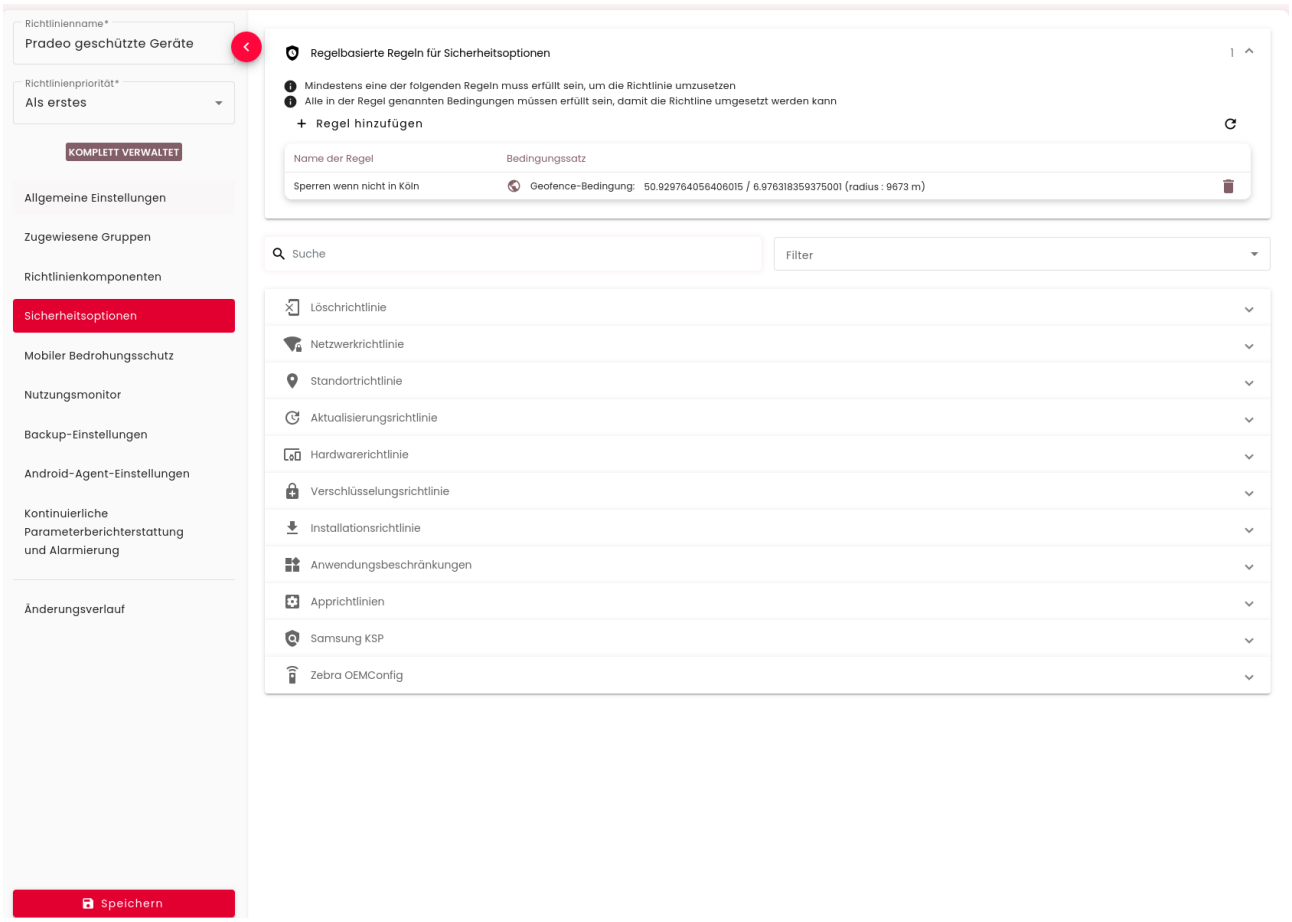
Wenn das datomo benutzerdefinierte Feld zugewiesen wird und einen Wert aus der Datei enthält, ist es nicht möglich, den Wert dieses Feldes manuell in der Admin-Konsole zu ändern.

3.11 Änderungsverlauf

Diese Seite zeigt eine Liste der Änderungen innerhalb der Richtlinie. Alle Änderungen sind in Revisionen gruppiert. Der Administrator kann einsehen, wer, wann und was in der Richtlinie geändert hat.

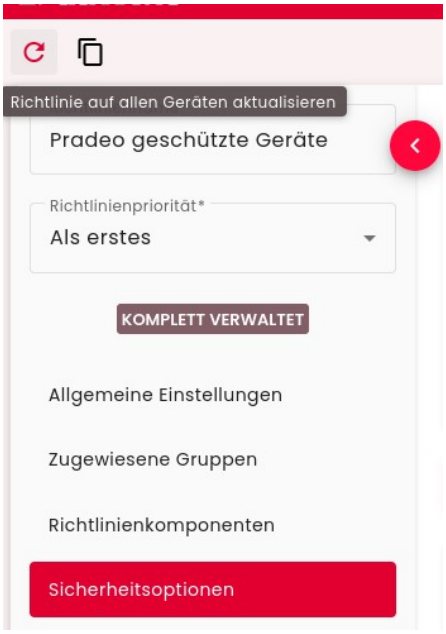
4 Speichern der Richtliniendetails

Sobald eine Änderung auf der Seite mit den **Richtlinien-Details** vorgenommen wird, erscheint die Schaltfläche **"Speichern"** im linken unteren Bereich des Bildschirms.

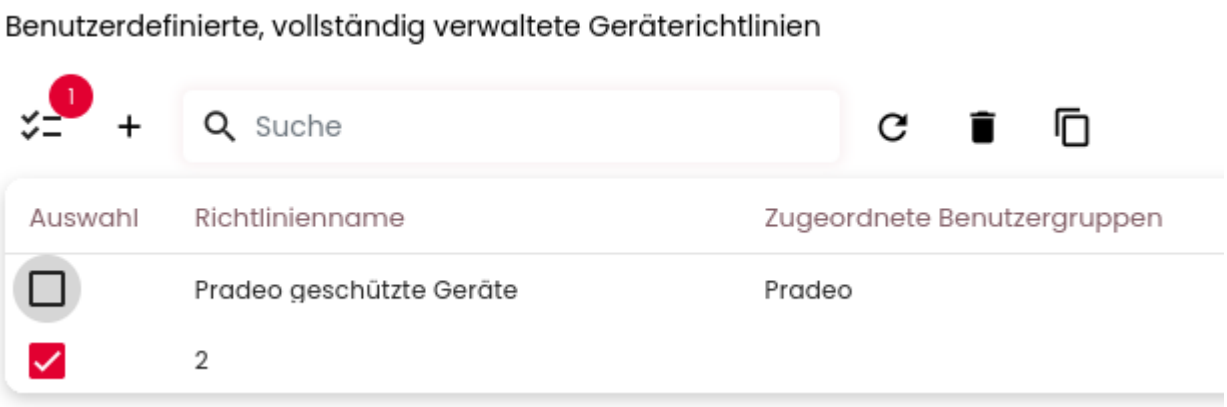


5 Richtlinien auf allen Geräten aktualisieren

Die Richtlinie kann auf den zugewiesenen Geräten entweder über die Registerkarte "Geräte" oder von der Seite mit den Richtlinien-Details neu geladen werden. Die Option steht im linken oberen Bereich des Bildschirms zur Verfügung.

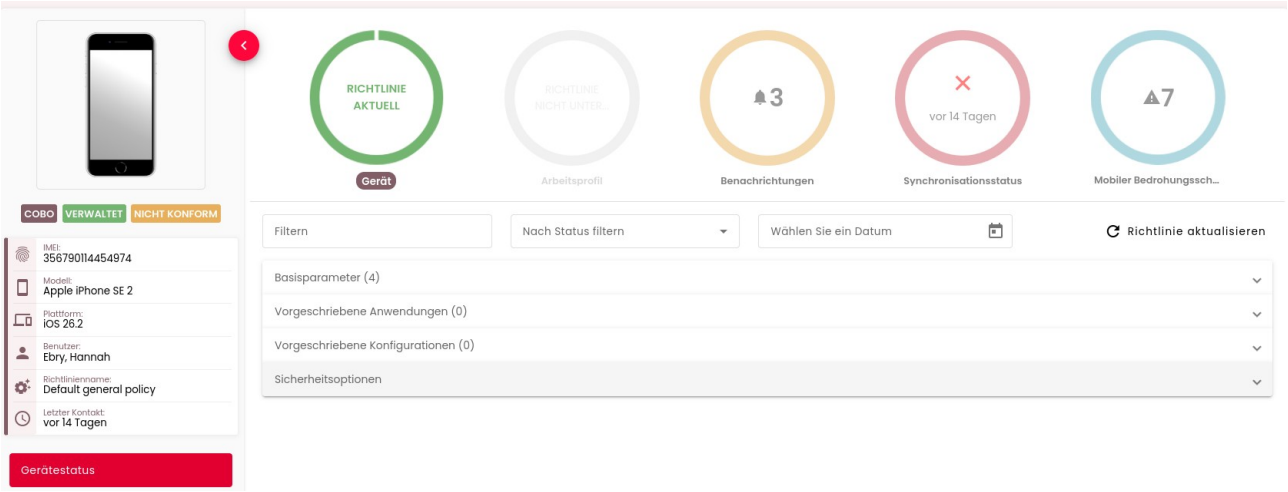


Zusätzlich lassen sich Richtlinien auch aus der Übersichtsllste der Richtlinien mithilfe der nach Auswahl einer oder mehrerer Richtlinien aktualisieren.



6 Richtlinienstatus auf dem Gerät

Der Richtlinienstatus für ein bestimmtes Gerät kann im Bereich Gerätedetails > Tab Gerätestatus überprüft werden. Hier sind die angewendeten Einschränkungen, obligatorischen Anwendungen und Konfigurationen sichtbar.



Über diesen Tab kann die Richtlinie auf dem Gerät auch aktualisiert werden.