

Benutzerhandbuch

Dokumentation für Cerberus Enterprise MDM

- [Einleitung](#)
- [Einrichtung](#)
 - [Android-Management-Einrichtung](#)
 - [Apple Management-Einrichtung \(APNs\)](#)
- [Übersicht zur Gerätebereitstellung](#)
- [Gerätebereitstellung - Android](#)
 - [Unterstützte Geräte](#)
 - [Registrierungstoken](#)
 - [Privat genutzte Geräte](#)
 - [Unternehmenseigene Geräte für geschäftliche und private Nutzung](#)
 - [Unternehmenseigene Geräte nur für die geschäftliche Nutzung](#)
 - [Zero-Touch](#)
 - [Authentifizierung über Google-Registrierung](#)
- [Gerätebereitstellung - Apple](#)
 - [Übersicht zur Apple-Bereitstellung](#)
 - [Apple manuelle Registrierung \(Registrierungsprofil\)](#)
 - [Apple Automated Device Enrollment \(ADE\)](#)
- [Policies-Übersicht](#)
- [Richtlinien - Android](#)
 - [Zusammenfassung](#)
 - [App-Management](#)
 - [Kiosk-Modus](#)
 - [Sicherheit](#)

- [Multimedia](#)
- [Cellular](#)
- [Netzwerk](#)
- [System](#)
- [Standort und Geofencing](#)
- [Benutzerverwaltung](#)
- [Private Nutzung](#)
- [Profilübergreifende Policies](#)
- [Statusberichterstattung](#)
- [Verschiedenes](#)
- [Richtlinien-Durchsetzungsregeln](#)
- [Richtlinien - Apple](#)
 - [Apple-Richtlinien](#)
 - [Apple-Richtlinie: Sperrcode](#)
 - [Apple-Richtlinie: Einschränkungen](#)
 - [Apple-Richtlinie: Apps & Profile](#)
- [Gerätestatus](#)
 - [Geräteübersicht](#)
 - [SIM-Verwaltung](#)
 - [Befehle](#)
 - [Standortkarte](#)
- [Dashboard-Standortkarte](#)
- [Private Apps](#)
- [Zertifikatsverwaltung](#)
- [Ereignisregeln](#)
- [Geräte](#)
 - [Geräte](#)
- [Benutzer](#)
 - [Benutzer](#)
 - [Benutzer-Editor](#)

- [Konto](#)
 - [Einstellungen](#)
- [Mandantenfähigkeit](#)
 - [Multi-Tenancy-Übersicht](#)
 - [Verwaltete Unternehmen](#)
 - [Unternehmenswechsel](#)
 - [Unterkonten](#)
- [Insights](#)

Einleitung

Cerberus Enterprise ist eine umfassende EMM-Lösung, die entwickelt wurde, um Ihnen bei der Sicherung und Verwaltung Ihrer Android- und Apple-Geräte zu helfen. Sie bietet alle wichtigen Funktionen für ein effektives Management von BYOD- und unternehmenseigenen Geräten in einem übersichtlichen und benutzerfreundlichen Dashboard, sodass Sie innerhalb von Minuten loslegen können.

Um Cerberus Enterprise effektiv zu nutzen, müssen Sie einige grundlegende Konzepte über die Funktionsweise des Systems verstehen.

Das System unterstützt die Verwaltung von sowohl Android- als auch Apple-Geräten:

Auf Android verwendet Cerberus Enterprise die offizielle [Android Management API](#), um Geräte über die [Android Device Policy](#)-App (ADP) zu verwalten. Die meisten Einstellungen werden direkt durch ADP erzwungen. Einige optionale Funktionen können zudem die Cerberus Enterprise Companion-App erfordern, welche die Möglichkeiten über ADP allein hinaus erweitert.

Auf Apple-Geräten verwaltet Cerberus Enterprise die Geräte über Apple MDM (Mobile Device Management). Die Apple-Verwaltung erfordert ein APNs-Zertifikat und kann optional mit dem Apple Business Manager integriert werden, um eine automatisierte Registrierung und App-Lizenzierung zu ermöglichen.

Jedes Gerät kann über einen oder ein (manuelle Apple-Registrierung) im System **registriert** werden. Die Registrierungsmethode ist mit einer [Richtlinie](#) verknüpft, die die auf die Geräte anzuwendenden Regeln enthält.

IT-Administratoren können die mit einem Gerät verknüpfte Richtlinie nach der Registrierung ändern. Jedes Gerät kann jedoch immer nur mit einer einzigen Richtlinie verknüpft sein.

Während des Registrierungsprozesses (Provisionierung) werden die erforderlichen Verwaltungskomponenten automatisch installiert und konfiguriert. Bei Android umfasst dies in der Regel die Android Device Policy-App (und, je nach Konfiguration, die Cerberus Enterprise Companion-App). Bei Apple-Geräten wird die Verwaltung durch MDM angewendet, sobald das Gerät registriert ist. Infolgedessen wird die entsprechende Richtlinie automatisch auf das Gerät angewendet und alle zugehörigen Regeln werden durch das Plattform-Managementsystem erzwungen.

Eine Richtlinie kann auf viele Geräte angewendet werden. In diesem Fall erhalten alle zugehörigen Geräte die Änderungen, wenn Sie die Richtlinie ändern.

Einrichtung

Android-Management- Einrichtung

Um Android-Geräte mit Cerberus Enterprise zu verwalten, müssen Sie zunächst Ihre Organisation mit Google Android Enterprise verbinden.

Der Einrichtungsprozess dauert in der Regel einige Minuten und erfordert eine **geschäftliche E-Mail-Adresse** (zum Beispiel *name@enterprise.com*) oder alternativ eine **private Google-E-Mail-Adresse**.

Was während der Einrichtung passiert

- Sie werden zu Google Android Enterprise weitergeleitet.
- Sie melden sich mit Ihrer geschäftlichen E-Mail-Adresse (oder einer privaten Google-E-Mail-Adresse) an.
- Google erstellt das Android-Management-Konto für Ihre Organisation.
- Sie werden zur Fertigstellung der Einrichtung zurück zu Cerberus Enterprise weitergeleitet.

Wichtige Informationen

Wir empfehlen die Anmeldung mit einer geschäftlichen E-Mail-Adresse statt mit einem privaten Gmail-Konto. Wenn die E-Mail-Adresse bereits mit einem Google Admin-Konto verknüpft ist, wird dieses bestehende Konto wiederverwendet und mit Cerberus Enterprise verbunden; andernfalls wird ein neues, kostenloses Google Admin-Konto erstellt. Ein Google Admin-Konto schaltet den vollen Funktionsumfang frei — zum Beispiel die Registrierung von Geräten mittels Google-Authentifizierung mit Konten, die von Ihrer Google Admin-Domain verwaltet werden.

Keine geschäftliche E-Mail-Adresse vorhanden?

Sie können sich trotzdem mit einer privaten Google-E-Mail-Adresse (zum Beispiel einem Gmail-Konto) anmelden. In diesem Fall erstellt Google ein kostenloses verwaltetes Google Play-Konto, das mit Cerberus Enterprise verknüpft wird.

Nächste Schritte

Erstellen Sie nach Abschluss der Einrichtung einen [Registrierungstoken](#) und wählen Sie die entsprechende Bereitstellungsmethode für das Gerät aus.

Apple Management- Einrichtung (APNs)

Um Apple-Geräte zu verwalten, benötigt Cerberus Enterprise das Zertifikat des Apple Push Notification service (APNs).

Verwenden Sie die mit Ihrer Organisation verknüpfte Apple-ID. Das APNs-Zertifikat ist ein Jahr gültig und muss jährlich erneuert werden, um die Verwaltung der Geräte fortsetzen zu können.

Schritt 1: Laden Sie die CSR-Datei herunter

Starten Sie im Dashboard die Apple Management-Einrichtung und laden Sie die von Cerberus Enterprise generierte, vom Anbieter signierte Zertifikatssignaturanfrage (CSR) herunter.

Schritt 2: Erstellen Sie das Push- Zertifikat im Apple-Portal

- Melden Sie sich mit Ihrer Apple-ID im Apple Push Certificates Portal an.
- Klicken Sie auf „Zertifikat erstellen“.
- Laden Sie die CSR-Datei aus Schritt 1 hoch.
- Laden Sie das erstellte Push-Zertifikat herunter.

Portal-Link: <https://identity.apple.com/>

Schritt 3: Laden Sie das Push-Zertifikat hoch

Laden Sie das von Apple heruntergeladene Push-Zertifikat wieder in Cerberus Enterprise hoch, um die Einrichtung abzuschließen.

Wenn das APNs-Zertifikat abläuft, wird die Verwaltung von Apple-Geräten unterbrochen, bis das Zertifikat erneuert wurde.

Nächste Schritte

Sobald APNs konfiguriert ist, können Sie mit der Registrierung von Apple-Geräten fortfahren. Fahren Sie fort mit [Übersicht zur Apple-Bereitstellung](#).

Übersicht zur Gerätebereitstellung

Cerberus Enterprise unterstützt die Geräteverwaltung sowohl für Android- als auch für Apple-Plattformen. Sie können jede Plattform unabhängig voneinander konfigurieren, je nachdem, welche Geräte Sie registrieren müssen.

1. Plattform-Einrichtung im Dashboard abschließen

Schließen Sie vor der Registrierung von Geräten die Plattform-Einrichtung im Cerberus Enterprise Dashboard ab. Wenn Ihr Konto noch nicht konfiguriert ist, führt Sie das Dashboard durch die erforderlichen Schritte.

Android-Einrichtung (Google Android Enterprise)

Für das vollständige Android-Einrichtungsverfahren lesen Sie [Android-Management-Einrichtung](#).

- Gehen Sie zum Registrierungsablauf im Dashboard und wählen Sie **Android Management einrichten**.
- Sie werden zu Google weitergeleitet, um sich mit einem **Geschäftskonto** anzumelden und Android Enterprise zu autorisieren.
- Nach der Autorisierung werden Sie zur Vervollständigung der Einrichtung zurück zu Cerberus Enterprise weitergeleitet.

Apple-Einrichtung (APNs-Push-Zertifikat)

Für das vollständige Apple-Einrichtungsverfahren lesen Sie [Apple-Management-Einrichtung \(APNs\)](#).

- Gehen Sie zum Registrierungsablauf im Dashboard und wählen Sie **Apple Management einrichten**.
- Laden Sie die CSR-Datei von Cerberus Enterprise herunter.
- Erstellen Sie das APNs-Zertifikat im Apple Push Certificates Portal und laden Sie das resultierende Zertifikat herunter.
- Laden Sie das heruntergeladene Zertifikat wieder in Cerberus Enterprise hoch, um die Apple-Geräteverwaltung zu aktivieren.

2. Geräte registrieren

Wählen Sie nach Abschluss der Plattform-Einrichtung die Registrierungsmethode aus, die Ihrem Geräteeigentumsmodell und dem Betriebssystem entspricht.

Android-Registrierung

Bei Android wird die Registrierung durch [Registrierungstoken](#) gesteuert. Wählen Sie die entsprechende Methode, je nachdem, ob es sich um ein privat genutztes oder ein unternehmenseigenes Gerät handelt.

- Privat genutzte Geräte (BYOD / Arbeitsprofil): [folgen Sie diesem Leitfaden](#).
- Unternehmenseigene Geräte (geschäftliche und private Nutzung / Arbeitsprofil): [folgen Sie diesem Leitfaden](#).
- Unternehmenseigene Geräte (nur geschäftliche Nutzung / vollständig verwaltet oder dediziert): [folgen Sie diesem Leitfaden](#).
- Zero-touch: [folgen Sie diesem Leitfaden](#).

Apple-Registrierung

Für Apple beginnen Sie mit dem oben beschriebenen Abschluss der APNs-Einrichtung und folgen dann den Apple-Bereitstellungsleitfäden: [Übersicht zur Apple-Bereitstellung](#).

Gerätebereitstellung - Android

Unterstützte Geräte

Im Allgemeinen ist jedes Gerät mit Android 6 oder höher und Google Play-Diensten mit Cerberus Enterprise kompatibel.

Für ein besseres Nutzererlebnis empfehlen wir die Verwendung von Geräten, die die [Android Enterprise Recommended](#)-Anforderungen erfüllen.

Einige Funktionen sind auf bestimmte Android-Versionen beschränkt oder können sich bei verschiedenen Betriebssystemversionen unterschiedlich verhalten. Weitere Informationen zu einer bestimmten Funktion finden Sie im Abschnitt [Richtlinien](#) der Dokumentation.

Cerberus Enterprise unterstützt sowohl unternehmenseigene als auch privat genutzte Geräte sowie zwei Verwaltungsmodi: Device Owner und Profile Owner.

Privat genutzte Geräte können über ein **Arbeitsprofil** verwaltet werden. Dies ermöglicht eine BYOD-Lösung, indem die geschäftlichen Daten und Apps der Mitarbeiter von den persönlichen Daten und Apps getrennt werden, was sowohl die Sicherheit als auch den Datenschutz verbessert. Diese Option eignet sich für Geräte, die sich bereits im Besitz der Mitarbeiter befinden und die Sie für die geschäftliche Nutzung in Ihrer Organisation registrieren möchten.

Unternehmenseigene Geräte können ebenfalls über ein Arbeitsprofil verwaltet werden, Sie können jedoch auch die Option **vollständig verwaltet** wählen, die eine strengere Kontrolle über das Gerät ermöglicht. Unternehmenseigene Geräte mit einem Arbeitsprofil eignen sich, wenn Sie Mitarbeitern Firmengeräte für die Arbeit zur Verfügung stellen und dennoch eine private Nutzung ermöglichen möchten. Vollständig verwaltete Geräte eignen sich besser für Geräte, die ausschließlich für die Arbeit genutzt werden müssen, oder für **dedizierte Geräte** (COSU, corporate-owned single-use), wie z. B. Kiosksysteme.

Weitere Informationen zur Gerätebereitstellung finden Sie auf der Seite [Übersicht zur Gerätebereitstellung](#).

Registrierungstoken

Cerberus Enterprise verwendet Registrierungstoken, um den Prozess der Android-Geräteregistrierung (Bereitstellung) zu starten. Das von Ihnen ausgewählte Token definiert die erste Richtlinie, die auf die registrierten Geräte angewendet wird, und beeinflusst, welche Bereitstellungsmodi zulässig sind.

Der Tab für Android-Registrierungstoken ist erst nach Abschluss der **Android-Management-Einrichtung** verfügbar.

Wo Sie Registrierungstoken finden

Öffnen Sie im Dashboard **Registrierungstoken**. Je nach Ihrer Kontokonfiguration kann die Seite mehrere Tabs anzeigen (Android-Token, Google Sign-in-Registrierung, manuelle Apple-Registrierung und Apple Automated Device Enrollment).

Wenn Ihr Android Enterprise durch eine verwaltete Google-Domain (Google Workspace) unterstützt wird, kann das Dashboard auch einen Tab **Authentifizierung über Google-Registrierung** anzeigen. Weitere Einzelheiten zur Aktivierung und Nutzung finden Sie unter **Authentifizierung über Google-Registrierung**.

Liste der Registrierungstoken (Android)

Der Tab für Android-Token zeigt eine Tabelle mit allen Token an. Durch Klicken auf eine Zeile wird die Seite mit den Token-Details geöffnet.

Spalten

- **ID**: interne Token-ID.

- **Status:** **Verfügbar**, **Benutzt** (Einmal-Token bereits verwendet) oder **Abgelaufen**.
- **Ablaufdatum:** Ablaufdatum/-zeit, oder **Nie**.
- **Richtlinie:** die dem Token zugewiesene Richtlinie (der UI-Tooltip zeigt auch die Richtlinien-ID an).
- **Private Nutzung:** Zugelassen / Nicht zulässig / Dediziertes Gerät.
- **Zugelassene Nutzungen:** Mehrfach oder nur einmalig.
- **Benutzer:** optionaler Benutzer, der den mit dem Token registrierten Geräten vorab zugewiesen wurde.

Aktionen

- Jede Zeile verfügt über eine Löschaktion (**Registrierungstoken löschen**). Das Löschen ist deaktiviert, wenn die Lizenz abgelaufen ist.
- Die Tabelle unterstützt die Auswahl mehrerer Zeilen: Sie können den Auswahlmodus aktivieren, mehrere Token auswählen und diese mit **Ausgewählte Token löschen** löschen.
- Verwenden Sie die Aktualisierungsaktion, um die Liste neu zu laden. Die Tabelle ist paginiert (10/25/50 Einträge pro Seite).

Neues Registrierungstoken erstellen

Klicken Sie im Tab für Android-Token auf **Neues Registrierungstoken**, um die Seite zur Token-Erstellung zu öffnen. Wenn Ihre Lizenz abgelaufen ist, ist die Schaltfläche zum Erstellen deaktiviert.

Token-Optionen

1. Richtlinie

Erforderlich. Die Richtlinie wird automatisch auf alle Geräte angewendet, die mit diesem Token registriert werden. Wählen Sie eine Ihrer [Android-Richtlinien](#). Wenn Sie noch keine Richtlinie haben, erstellen Sie zuerst eine.

2. Benutzer

Optional. Wenn festgelegt, werden neu registrierte Geräte automatisch diesem Benutzer zugeordnet.

3. Private Nutzung

Steuert, ob die private Nutzung auf einem mit diesem Registrierungstoken bereitgestellten Gerät zulässig ist:

- **Zugelassen:** geeignet für privat genutzte Geräte (Arbeitsprofil) sowie unternehmenseigene Geräte für die geschäftliche und private Nutzung.
- **Nicht zulässig:** geeignet für unternehmenseigene Geräte nur für die geschäftliche Nutzung (vollständig verwaltet).
- **Dediziertes Gerät:** geeignet für Kiosk-/dedizierte Geräte (das Gerät ist nicht mit einem einzelnen Benutzer verknüpft).

4. Zugelassene Nutzungen

Wählen Sie aus, ob das Token mehrfach (**Mehrfach**) oder nur einmalig (**Nur einmalig**) verwendet werden kann.

5. Ablaufdatum

Wählen Sie die Ablauf-Einheit (**Minuten, Stunden, Tage** oder **Nie**). Wenn nicht auf „Nie“ eingestellt, geben Sie den Ablaufwert ein. Der zulässige Bereich hängt von der ausgewählten Einheit ab und kann bis zu 10.000 Tage betragen.

6. Google-Authentifizierung

Steuert, ob sich der Benutzer während der Geräte-Registrierung mit einem Google-Konto authentifizieren muss:

- **Nicht festgelegt:** Die Google-Authentifizierungseinstellung auf Unternehmensebene wird verwendet, um zu bestimmen, ob sich der Benutzer während der Registrierung bei Google authentifizieren muss.
- **Optional:** Der Benutzer kann wählen, die Google-Authentifizierung während der Registrierung zu überspringen.
- **Erforderlich:** Der Benutzer muss sich mit einem Google-Konto authentifizieren, um mit der Registrierung fortzufahren.

Wenn **Erforderlich** ausgewählt ist, erscheint ein optionales Feld **Erforderliche Konto-E-Mail**. Wenn dieses gesetzt ist, muss sich der Benutzer während der Registrierung mit genau diesem Google-Konto authentifizieren.

Bereitstellungsoptionen (nur QR-Code)

Diese zusätzlichen Optionen sind in den QR-Code eingebettet und werden während der Bereitstellung vollständig verwalteter Geräte angewendet, die durch Scannen des QR-Codes registriert werden. Sie gelten nicht für Arbeitsprofile oder Geräte, die über die Registrierungs-URL

oder ein Token registriert werden.

WLAN-Konfiguration

Verwenden Sie dies, um ein Gerät während der Bereitstellung automatisch mit dem WLAN zu verbinden, damit es die Verwaltungs-App herunterladen und initialisieren kann. Verfügbare Felder umfassen **SSID**, **Versteckte SSID**, **Sicherheit** und (falls erforderlich) **Passphrase**.

Sie können auch einen HTTP-Proxy (**Proxy**) konfigurieren und, je nach Modus, **Host/Port**, **PAC URI** sowie **Proxy-Bypass-Host** festlegen.

Andere Optionen

Zusätzliche Optionen umfassen **Sprache/Region**, **Zeitzone** und **Verschlüsselung überspringen**.

Details zum Registrierungstoken

Wenn Sie ein Token öffnen, zeigt die Detailseite die Token-Konfiguration und Informationen zur Nutzung an:

- **Status**, **Ablaufdatum**, **Nutzung**, **Private Nutzung**, **Zulässige Verwendungen** und (falls gesetzt) **Google-Authentifizierung** mit der optionalen **Erforderlichen Konto-E-Mail**.
- **Token**: der ursprüngliche Wert des Registrierungstokens (kopierbar).
- **Registrierungs-URL**: eine Google Android Enterprise Registrierungs-URL (kopierbar und per E-Mail versendbar).
- **QR-Code**: wird auf der rechten Seite der Seite angezeigt und dient zur Registrierung vollständig verwalteter Geräte.

Folgen Sie für schrittweise Bereitstellungsverfahren den Android-Registrierungsleitfäden: [Privat genutzte Geräte](#)>, [Unternehmenseigene Geräte für die geschäftliche und private Nutzung](#)>, [Unternehmenseigene Geräte nur für die geschäftliche Nutzung](#)>, und [Zero-touch](#).

Privat genutzte Geräte

Von Mitarbeitern selbst genutzte Geräte können mit einem **Arbeitsprofil** eingerichtet werden. Ein Arbeitsprofil bietet einen eigenständigen Bereich für geschäftliche Apps und Daten, der von persönlichen Apps und Daten getrennt ist. Die meisten App-, Daten- und sonstigen Verwaltungsrichtlinien gelten nur für das Arbeitsprofil, während die persönlichen Apps und Daten der Mitarbeiter privat bleiben.

Um ein Arbeitsprofil auf einem privat genutzten Gerät einzurichten, verwenden Sie eine der folgenden Bereitstellungsmethoden (stellen Sie sicher, dass der [Registrierungstoken](#) auf **Private Nutzung** auf **Zugelassen** gesetzt ist):

Registrierungs-URL (Token)

Android-Version
6.0+

Sie können die Registrierungs-URL an die Endbenutzer weitergeben. Wenn ein Endbenutzer den Link auf seinem Gerät öffnet, wird er durch die Einrichtung des Arbeitsprofils geführt.

Arbeitsprofil über "*Einstellungen*" hinzufügen

Android-Version
6.0+

Um ein Arbeitsprofil auf ihrem Gerät einzurichten, kann ein Benutzer die **Einstellungen**-App des Geräts öffnen und dann die Suchleiste verwenden, um die Option **Arbeitsprofil einrichten** zu finden und darauf zu tippen.

Wenn die Suche erfolglos bleibt, kann der Standort dieser Option variieren. Hier sind einige Möglichkeiten:

- *Einstellungen -> Google-Dienste und Einstellungen -> Alle Dienste -> Arbeitsprofil einrichten.*
- *Einstellungen -> Google -> Einrichten & Wiederherstellen -> Arbeitsprofil einrichten.*

Diese Schritte starten einen Einrichtungsassistenten, der die *Android Device Policy* auf dem Gerät herunterlädt. Als Nächstes wird der Benutzer aufgefordert, einen QR-Code zu scannen oder manuell einen Registrierungstoken einzugeben, um die Einrichtung des Arbeitsprofils abzuschließen.

Android Device Policy herunterladen

Android-Version
6.0+

Um ein Arbeitsprofil auf ihrem Gerät einzurichten, kann ein Benutzer die Android Device Policy aus dem Google Play Store herunterladen. Nach der Installation der App wird der Benutzer aufgefordert, einen QR-Code zu scannen oder manuell einen Registrierungstoken einzugeben, um die Einrichtung des Arbeitsprofils abzuschließen.

Unternehmenseigene Geräte für geschäftliche und private Nutzung

Die Einrichtung eines unternehmenseigenen Geräts mit einem **Arbeitsprofil** ermöglicht die Nutzung des Geräts sowohl für geschäftliche als auch für private Zwecke. Bei unternehmenseigenen Geräten mit Arbeitsprofilen:

- Die meisten App-, Daten- und sonstigen Verwaltungsrichtlinien gelten nur für das Arbeitsprofil.
- Die persönlichen Profile der Mitarbeiter bleiben privat. Unternehmen können jedoch bestimmte geräteübergreifende Richtlinien sowie Richtlinien zur privaten Nutzung durchsetzen.
- Unternehmen können den *Blockumfang* nutzen, um Konformitätsmaßnahmen auf das gesamte Gerät oder nur auf dessen Arbeitsprofil anzuwenden.
- Die Abmeldung von Geräten und Gerätebefehle gelten für das gesamte Gerät.

Um ein unternehmenseigenes Gerät mit einem Arbeitsprofil einzurichten, verwenden Sie eine der folgenden Bereitstellungsmethoden (stellen Sie sicher, dass der [Registrierungstoken](#) auf **Private Nutzung** auf **Zugelassen** gesetzt ist):

QR-Code-Methode

Android-Version
8.0+

Auf einem neuen oder auf Werkseinstellungen zurückgesetzten Gerät tippt der Benutzer (in der Regel ein IT-Administrator) sechsmal an derselben Stelle auf den Bildschirm. Dadurch wird das Gerät angewiesen, den Benutzer zum Scannen eines QR-Codes aufzufordern.

Unternehmenseigene Geräte nur für die geschäftliche Nutzung

Vollständige Geräteverwaltung eignet sich für unternehmenseigene Geräte, die ausschließlich für geschäftliche Zwecke bestimmt sind. Unternehmen können alle Apps auf dem Gerät verwalten und das gesamte Spektrum der Richtlinien und Befehle der Android Management API erzwingen. Es ist auch möglich, ein Gerät (über eine Richtlinie) auf eine einzige App oder eine kleine Gruppe von Apps zu beschränken, um einen speziellen Zweck oder Anwendungsfall zu erfüllen. Diese Teilmenge vollständig verwalteter Geräte wird als **dedizierte Geräte** bezeichnet. Um eine vollständige Verwaltung auf einem unternehmenseigenen Gerät einzurichten, verwenden Sie eine der folgenden Bereitstellungsmethoden (stellen Sie sicher, dass der [Registrierungstoken](#) auf **Private Nutzung** auf **Nicht zulässig** gesetzt ist):

QR-Code-Methode

Android-Version
7.0+

Auf einem neuen oder auf Werkseinstellungen zurückgesetzten Gerät tippt der Benutzer (in der Regel ein IT-Administrator) sechsmal an derselben Stelle auf den Bildschirm. Dadurch wird das Gerät angewiesen, den Benutzer zum Scannen eines QR-Codes aufzufordern.

DPC-Identifikationsmethode

Android-Version
5.1+

Wenn die Android Device Policy nicht über einen QR-Code hinzugefügt werden kann, kann ein Benutzer oder IT-Administrator diese Schritte befolgen, um ein vollständig verwaltetes oder dediziertes Gerät bereitzustellen:

1. Folgen Sie dem Einrichtungsassistenten auf einem neuen oder auf Werkseinstellungen zurückgesetzten Gerät.
2. Geben Sie die WLAN-Anmeldedaten ein, um das Gerät mit dem Internet zu verbinden.

3. Wenn Sie zur Anmeldung aufgefordert werden, geben Sie **afw#setup** ein, wodurch die Android Device Policy heruntergeladen wird.
4. Scannen Sie einen QR-Code oder geben Sie manuell ein Registrierungstoken ein, um das Gerät bereitzustellen.

Zero-Touch

IT-Administratoren können unternehmenseigene Geräte über die Zero-Touch-Registrierungsmethode bereitstellen, die in [Zero-Touch-Registrierung für IT-Administratoren](#) beschrieben wird. Wenn ein Gerät zum ersten Mal eingeschaltet wird, wird es automatisch in die vom IT-Administrator definierten Einstellungen versetzt.

IT-Administratoren können Geräte, die von [autorisierten Händlern](#) erworben wurden, vorkonfigurieren und über das Cerberus Enterprise Dashboard verwalten. Um Ihr Zero-Touch-Konto zu verknüpfen, rufen Sie den Bereich **Zero-Touch** im Dashboard auf und folgen Sie dann den Anweisungen.

Android-Version	Arbeitsprofil	Vollständig verwaltetes Gerät	Dediziertes Gerät
8.0+ (Pixel 7.1+)	✓	✓	✓

Authentifizierung über Google-Registrierung

Die Authentifizierung über Google-Registrierung (auch bezeichnet als **Google-Authentifizierung für die Registrierung**) ermöglicht es Benutzern, sich während der Android-Geräteregistrierung mit ihrem Google Workspace-Konto zu authentifizieren.

Diese Funktion ist nur für Android Enterprise verfügbar, das durch eine verwaltete Google-Domain (Google Workspace) unterstützt wird.

Wo Sie es finden

Öffnen Sie im Dashboard **Registrierungstoken** und wählen Sie den Tab **Authentifizierung über Google-Registrierung** aus. Der Tab wird nur angezeigt, wenn das Android Management konfiguriert ist und die Google Workspace-Integration für Ihr Unternehmen verfügbar ist.

Google-Authentifizierung aktivieren (oder deaktivieren)

Die Google-Authentifizierung wird über die **Google Admin-Konsole** aktiviert. Kehren Sie nach der Änderung der Einstellung zu Cerberus Enterprise zurück und verwenden Sie **Status aktualisieren**, um die aktuelle Konfiguration neu zu laden.

1. Melden Sie sich mit einem Administrator-Konto bei Ihrer [Google Admin-Konsole](#) an.
2. Öffnen Sie **Geräte**.
3. Navigieren Sie zu **Mobile & Endgeräte** → **Einstellungen** → **Drittanbieter-Integrationen**.
4. Suchen Sie die **Android EMM-Integration** für Cerberus Enterprise und öffnen Sie diese.
5. Klicken Sie auf **EMM-Anbieter verwalten**.

6. Schalten Sie **Authentifizierung über Google** um, um die Google-Authentifizierung für die Registrierung zu aktivieren oder zu deaktivieren.
7. Klicken Sie auf **Speichern**.
8. Kehren Sie zum Cerberus Enterprise Dashboard zurück und klicken Sie im Tab **Authentifizierung über Google-Registrierung** auf **Status aktualisieren**.

Google-Authentifizierungs-Registrierungstoken

Wenn die Google-Authentifizierung aktiviert ist, zeigt das Dashboard ein spezielles Registrierungstoken an, das für diesen Registrierungsmodus verwendet wird. Die Seite kann einen **QR-Code**, einen **Registrierungstoken**-Wert und eine **Registrierungs-URL** (kopierbar und per E-Mail versendbar) anzeigen.

Wichtige Optionen

- **Private Nutzung zulassen:** steuert, ob das Token die Registrierung von Geräten für geschäftliche und private Nutzung (Arbeitsprofil-Szenarien) oder nur für die geschäftliche Nutzung (vollständig verwaltete / dedizierte Szenarien) ermöglicht.
- **Standard-Fallback-Richtlinie:** die Richtlinie, die angewendet wird, wenn dem registrierenden Benutzer keine spezifische Standard-Richtlinie für die Google-Authentifizierung zugewiesen ist.

Richtlinien-Interaktion

Die Richtlinieneinstellung **Authentifizierung bei der Einrichtung des Geschäftskontos** (workAccountSetupConfig.authenticationType) steuert, wie sich Benutzer bei der Einrichtung des Geschäftskontos authentifizieren, aber die Einstellung **Authentifizierung über Google** in der Google Admin-Konsole und der Typ des Registrierungstokens können dennoch eine Authentifizierung erfordern.

Bei bereits registrierten Geräten gilt diese Richtlinie nur, wenn das Gerät über ein verwaltetes Google Play-Konto verwaltet wird (d. h. ohne **Authentifizierung über Google-Registrierung** registriert wurde).

Einige Aktionen (zum Beispiel das Ändern von Token-Optionen) können deaktiviert sein, wenn die Lizenz abgelaufen ist.

Ein Gerät registrieren

Während der Registrierung wird der Benutzer aufgefordert, sich mit seinem Google Workspace-Konto zu authentifizieren. Nach erfolgreicher Registrierung wird das Gerät dem authentifizierten Benutzer zugeordnet.

Arbeitsprofil (privat genutzte Geräte)

- Teilen Sie die **Registrierungs-URL** mit dem Benutzer. Wenn der Benutzer diese auf seinem Android-Gerät öffnet, wird er durch die Einrichtung des Arbeitsprofils und die Google-Authentifizierung geführt.
- Alternativ kann der Benutzer den Vorgang über die Android-Einstellungen starten und den Workflow zur Einrichtung des Arbeitsprofils wählen; anschließend kann der QR-Code gescannt oder das Registrierungstoken eingegeben werden, wenn dazu aufgefordert wird.

Unternehmenseigene Geräte

- **QR-Code-Methode:** Tippen Sie auf einem neuen oder auf Werkseinstellungen zurückgesetzten Gerät mehrmals an derselben Stelle auf den Bildschirm, bis die Aufforderung zum Scannen eines QR-Codes erscheint, und scannen Sie dann den im Dashboard angezeigten QR-Code.
- **DPC-Identifikationsmethode** (wenn das Scannen von QR-Codes nicht verfügbar ist): Folgen Sie dem Einrichtungsassistenten, verbinden Sie sich mit dem WLAN und geben Sie dann bei der Aufforderung zur Anmeldung **afw#setup** ein. Fahren Sie fort, indem Sie den QR-Code scannen oder das Registrierungstoken eingeben. Authentifizieren Sie sich bei der entsprechenden Aufforderung mit dem Google Workspace-Konto.

Für allgemeine Android-Bereitstellungsverfahren (Arbeitsprofil vs. vollständig verwaltete Geräte) lesen Sie die Standardseiten zur Android-Registrierung in diesem Handbuch.

Gerätebereitstellung - Apple

Übersicht zur Apple-Bereitstellung

Cerberus Enterprise unterstützt die Registrierung und Verwaltung von Apple-Geräten. Die Apple-Bereitstellung erfordert ein APNs-Zertifikat und kann mit verschiedenen Registrierungsmethoden durchgeführt werden.

Voraussetzung: Konfiguration von Apple Management (APNs)

Bevor Sie ein Apple-Gerät registrieren, schließen Sie die [Apple Management-Einrichtung \(APNs\)](#) ab.

Wählen Sie eine Registrierungsmethode aus

Manuelle Registrierung (Registrierungsprofil)

Diese Methode stellt eine Registrierungs-URL und eine Konfigurationsprofil-Datei (mobileconfig) bereit, die Sie auf dem Gerät installieren. Lesen Sie [Apple manuelle Registrierung](#).

Automated Device Enrollment (ADE)

Diese Methode lässt sich in den Apple Business Manager integrieren, um die Registrierung für unternehmenseigene Geräte zu automatisieren. Lesen Sie [**Apple Automated Device Enrollment \(ADE\)**](#).

Je nach Geräteflotte und Beschaffungsprozess können Sie die manuelle Registrierung und ADE parallel verwenden.

Apple manuelle Registrierung (Registrierungsprofil)

Cerberus Enterprise unterstützt die manuelle Registrierung für Apple-Geräte unter Verwendung einer Registrierungs-URL und einer Registrierungsprofil-Datei.

Die manuelle Registrierung ist verfügbar, wenn Apple Management (APNs) konfiguriert ist. Wenn Sie die APNs-Einrichtung noch nicht abgeschlossen haben, lesen Sie [**Apple Management-Einrichtung \(APNs\)**](#).

Registrierungs-URL und Profil abrufen

- Öffnen Sie den Abschnitt **Registrierung** im Dashboard und wählen Sie den Tab **Apple manuelle Registrierung (Registrierungsprofil)** aus.
- Kopieren Sie die **Registrierungs-URL** oder verwenden Sie die Aktion „Per E-Mail senden“.
- Laden Sie das **Registrierungsprofil** (mobileconfig-Datei) herunter.

So registrieren Sie ein iPhone oder iPad

iOS/iPadOS 15.0+

1. Senden Sie die Registrierungsprofil-Datei (*enroll.mobileconfig*) an das Gerät oder öffnen Sie die Registrierungs-URL in Safari auf dem Gerät.
2. Öffnen Sie auf dem Gerät *Einstellungen* → *Profil heruntergeladen* → *Installieren* und folgen Sie dann den Anweisungen.
3. Nach der Registrierung können Sie den Status unter *Einstellungen* → *Allgemein* → *VPN & Geräteverwaltung* (oder *Profile & Geräteverwaltung*) überprüfen.

Installieren Sie nur Registrierungsprofile, die Sie über Ihr Cerberus Enterprise-Dashboard erhalten haben.

Apple Automated Device Enrollment (ADE)

Automated Device Enrollment (ADE) lässt sich in den Apple Business Manager (ABM) integrieren, um unternehmenseigene Geräte automatisch zu registrieren, wenn sie zum ersten Mal eingeschaltet werden (oder nach einem Werksreset).

ADE erfordert zunächst die Konfiguration von Apple Management (APNs). Lesen Sie bei Bedarf [Apple Management-Einrichtung \(APNs\)](#).

So registrieren Sie Geräte automatisch

1. Fügen Sie Geräte Ihrem Apple Business Manager-Konto hinzu.
2. Nachdem Sie neue Geräte zu Ihrem ABM-Konto hinzugefügt haben, synchronisieren Sie diese in Cerberus Enterprise im Abschnitt **Geräte** über die Aktion **Sync von ABM**.
3. Erstellen Sie ein ADE-Profil im Dashboard unter **Registrierung** → **Apple Automated Device Enrollment (ADE)** → **Neues ADE-Profil**.
4. Weisen Sie ein ADE-Profil einem Gerät über das Feld **ADE-Profil** auf der Gerätedetailseite zu.

ADE-Profil-Einstellungen (Übersicht)

Ein ADE-Profil steuert, wie das Gerät registriert wird und wie sich der Setup-Assistent verhält. In Cerberus Enterprise umfasst ein ADE-Profil einen Namen, eine optionale erste Policy sowie einige Registrierungsoptionen.

Profilname

Ein für Menschen lesbarer Name für das Profil (zum Beispiel *Standard-ADE-Profil*).

Policy

Die Policy, die anfänglich auf registrierte Geräte angewendet wird. Sie können beim Erstellen eines neuen ADE-Profiles eine Policy zuweisen.

Registrierungsoptionen

- **MDM entfernbar:** steuert, ob die MDM-Payload vom Gerät entfernt werden kann.
- **Pairing erlauben:** steuert, ob das Koppeln erlaubt ist (von Apple in iOS 13 als veraltet markiert).
- **Setup automatisch fortsetzen:** führt den Setup-Assistenten automatisch durch seine Bildschirme.
- **Warten auf Gerätekonfiguration:** blockiert den Setup-Assistenten, bis der Server das Gerät als konfiguriert markiert.
- **Obligatorisch:** verhindert das Überspringen der Profilanwendung während des Setups.
- **Mehrbenutzer (Shared iPad):** konfiguriert das Gerät für den Shared iPad-Modus.
- **Überwacht:** fordert die Überwachung (Supervision) für das Gerät an.

Sobald einem Gerät ein ADE-Profil zugewiesen wurde, ist es bereit für die automatische Registrierung.

Policies-Übersicht

Der Abschnitt **Policies** im Dashboard (*Dashboard* → *Policies*) listet alle Policies in Ihrem Konto auf und ermöglicht es Ihnen, diese zu erstellen, zu kopieren, zu bearbeiten und zu löschen.

Policy-Liste

Policies werden in einer Tabelle angezeigt. Durch Klicken auf eine Zeile wird der entsprechende Policy-Editor geöffnet.

Spalten

- **Id**: interne Policy-Kennung.
- **MDM**: die Plattform für die Policy (Android oder Apple).
- **Name**: Name der Policy.
- **Beschreibung**: Beschreibung der Policy.
- **Devices**: Anzahl der aktuell dieser Policy zugewiesenen registrierten Geräte.

Filter und Suche

- Wenn sowohl Android Management als auch Apple Management konfiguriert sind, können Sie die Liste nach **All**, **Android** oder **Apple** filtern.
- Sie können **Search** aktivieren und nach dem Namen oder der Beschreibung einer Policy suchen.

Aktualisierung und Paginierung

- Verwenden Sie die Aktualisierungsaktion, um die Liste neu zu laden.
- Die Tabelle ist paginiert (10/25/50 Einträge pro Seite).

Eine neue Policy erstellen

Am Ende der Policies-Seite können Sie eine neue Policy erstellen. Je nachdem, welche Plattform in Ihrem Konto konfiguriert ist, werden Ihnen eine oder beide dieser Aktionen angezeigt:

- **Create new Android policy**
- **Create new Apple policy**

Wenn Ihre Lizenz abgelaufen ist, sind die Erstellung von Policies (und andere Schreibaktionen) deaktiviert.

Policies kopieren und löschen

Jede Policy-Zeile verfügt über ein Aktionsmenü, das **Copy policy** und **Delete policy** enthält.

Warnungen beim Löschen einer Policy

Beim Löschen einer Policy kann das Dashboard je nach Verwendung der Policy zusätzliche Warnungen anzeigen.

- Wenn die Policy registrierten Geräten zugewiesen ist, führt das Löschen dazu, dass die zugehörigen Geräte abgemeldet und deren Apps sowie Daten gelöscht werden.
- Wenn die Policy Enrollment-Token zugewiesen ist, können diese Token möglicherweise keine Registrierung mehr abschließen.
- Wenn die Policy als Standard für die Google-Authentifizierungsregistrierung festgelegt ist (global oder für bestimmte Benutzer), kann das Löschen dazu führen, dass Registrierungen fehlschlagen.

Mehrere Policies löschen

Die Policies-Liste unterstützt die Mehrfachauswahl von Zeilen für das Massenzlöschung. Im Mehrfachauswahlmodus können Sie mehrere Policies auswählen und diese mit einer einzigen Aktion löschen.

Das Massenzlöschung ist nur aktiviert, wenn alle ausgewählten Policies zur selben Plattform gehören (alle Android oder alle Apple).

Weiter: Policy-Einstellungen bearbeiten

Die Policies-Liste ist der Einstiegspunkt. Um die Policy-Einstellungen zu konfigurieren, nutzen Sie bitte die entsprechende Dokumentation zum Editor: [Policies → Android](#) und [Policies → Apple](#).

Policies, die auf Enrollment-Token referenziert werden, werden während der Geräte-Registrierung automatisch angewendet.

Richtlinien - Android

Zusammenfassung

Android-Richtlinien sind die Kerneinheiten des Systems: Sie definieren die Regeln, die auf verwalteten Geräten angewendet und durchgesetzt werden.

Sie können Ihre Richtlinien im Bereich **Richtlinien** des Dashboards durchsuchen und neue erstellen. Um eine Android-Richtlinie zu öffnen, klicken Sie auf die entsprechende Zeile in der Tabelle: Das System öffnet dann die Seite **Richtlinien-Editor**.

Eine Richtlinie kann mit einem [Registrierungstoken](#) verknüpft werden, sodass sie während des Bereitstellungsprozesses automatisch auf die Geräte angewendet wird. Sie können auch die einem Gerät zugewiesene Richtlinie nach der Bereitstellung ändern.

Jedes Gerät kann nur mit einer Richtlinie gleichzeitig verknüpft werden.

Viele Richtlinienoptionen gelten nur für bestimmte Gerätetypen (vollständig verwaltet, dediziert, Arbeitsprofil) und Android-Versionen. Nicht unterstützte Einstellungen können vom Gerät ignoriert oder als nicht richtlinienkonform gemeldet werden.

Layout des Richtlinien-Editors

Der Richtlinien-Editor ist als eine Reihe von erweiterbaren Abschnitten organisiert. Am oberen Seitenrand können Sie jederzeit Folgendes bearbeiten:

- **Name** (erforderlich)
- **ID** (schreibgeschützt)
- **Beschreibung** (optional)

Die folgenden Abschnitte entsprechen den Panels des Richtlinien-Editors (zum Beispiel: App-Verwaltung, Sicherheit, Netzwerk, System, Private Nutzung, profilübergreifende Richtlinien und mehr). Verwenden Sie die Kapitelseiten dieses Handbuchs, um jedes Panel im Detail zu verstehen.

Speichern, Löschen und zugehörige Geräte

Verwenden Sie **Richtlinie speichern**, um Ihre Änderungen anzuwenden. Die Schaltfläche ist deaktiviert, wenn keine ausstehenden Bearbeitungen vorliegen oder die Lizenz abgelaufen ist.

Wenn Sie eine bestehende Richtlinie geöffnet haben (sie besitzt eine ID), zeigt die Seite unten die Aktion **Richtlinie löschen** sowie eine Liste **Zugehörige Geräte** an, damit Sie sehen können, wie viele Geräte die Richtlinie aktuell verwenden.

App-Management

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

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

1. Play-Store-Modus

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

Whitelist (Standard): Nur Apps, die in der Policy enthalten sind, stehen zur Verfügung; alle Apps, die nicht in der Policy enthalten sind, werden automatisch vom Gerät deinstalliert. Der Play Store zeigt nur verfügbare Apps an.

Blacklist: Alle Apps sind verfügbar. Jede App, die nicht auf dem Gerät sein soll, muss in der Anwendungs-Policy explizit als **blockiert** markiert werden. Der Play Store zeigt alle Apps an, außer den blockierten.

2. Policy für nicht vertrauenswürdige Apps

Die Policy für nicht vertrauenswürdige Apps (Apps aus unbekannten Quellen), die auf dem Gerät erzwungen wird. Diese Option steuert die Android-Systemeinstellung, die festlegt, ob ein Benutzer Apps von außerhalb des Play Stores installieren kann (Sideloadung).

Untersagen (Standard): Installationen von nicht vertrauenswürdigen Apps auf dem gesamten Gerät untersagen.

Nur persönliches Profil: Bei Geräten mit Arbeitsprofilen werden Installationen von nicht vertrauenswürdigen Apps nur im persönlichen Profil des Geräts erlaubt.

Erlauben: Installationen von nicht vertrauenswürdigen Apps auf dem gesamten Gerät erlauben.

3. Google Play Protect

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

Erzwungen (Standard): Erzwingt die App-Verifizierung.

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

4. Standard-Berechtigungsrichtlinie

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

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

Erteilen: Eine Berechtigung automatisch erteilen.

Ablehnen: Eine Berechtigung automatisch ablehnen.

5. App-Funktionen

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

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

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

6. App-Installation deaktiviert

Ob die Installation von Apps durch den Benutzer deaktiviert ist.

7. App-Deinstallation deaktiviert

Ob die Deinstallation von Apps durch den Benutzer deaktiviert ist.

8. Berechtigungsrichtlinien

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

Verwenden Sie **Add permission policy**, um Einträge zu erstellen, und entfernen Sie diese mit der Löschaktion.

Jeder Eintrag enthält:

Android-Berechtigung/Gruppe: Die Android-Berechtigung oder Gruppe (erforderlich), zum Beispiel **android.permission.READ_CALENDAR** oder **android.permission_group.CALENDAR**.

Policy: Erteilen / Ablehnen / Abfrage (verwendet dieselben Policy-Optionen wie **Default permission policy**).

9. Anwendungen

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

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

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

Um eine neue App hinzuzufügen, klicken Sie auf die Schaltfläche **Anwendungen hinzufügen** (oder das **Anwendungen hinzufügen**-Symbol), wählen Sie **Aus verwaltetem Google Play**, 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 im Google Play Store veröffentlicht wurde, aber bereits auf dem Gerät vorhanden ist (zum Beispiel eine System- oder Hersteller-App), klicken Sie auf **Anwendungen hinzufügen**, wählen Sie **Nach Paketname (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 **Erzwungene Installation** hinzugefügt. Um die App im Kiosk-Custom-Launcher anzuzeigen, muss der **Installationstyp** auf **Vorinstalliert** oder **Erzwungene Installation** gesetzt sein: Mit **Verfügbar** wird die App nicht angezeigt.

Apps, die nicht in verwaltetem Google Play verfügbar sind, werden in der Anwendungsliste mit einem Android-Symbol markiert. Da sie nicht über Google Play installiert werden können, müssen sie bereits auf dem Gerät vorhanden sein: Geräte, die die App nicht besitzen, können sie nicht installieren.

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

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

9.1. Installationsart

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

Verfügbar: Die App steht zur Installation bereit.

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

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

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

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

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

9.2. Installationsbeschränkungen

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

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

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

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

Idle: Die App nur installieren, wenn das Gerät im Leerlauf ist.

9.3. Auto-Update-Modus

Steuert den Auto-Update-Modus für die App.

Standard: Die App wird automatisch mit niedriger Priorität aktualisiert, um die Auswirkungen auf den Benutzer zu minimieren. Die App wird aktualisiert, wenn alle folgenden Bedingungen erfüllt sind: (1) das Gerät wird nicht aktiv genutzt, (2) das Gerät ist mit einem unbegrenzten Netzwerk verbunden, (3) das Gerät wird geladen. Das Gerät wird innerhalb von 24 Stunden nach der Veröffentlichung durch den Entwickler über ein neues Update benachrichtigt, woraufhin die App beim nächsten Mal aktualisiert wird, wenn die oben genannten Bedingungen erfüllt sind.

Aufgeschoben: Die App wird für maximal 90 Tage nach dem Veralten der App nicht automatisch aktualisiert. 90 Tage nachdem die App veraltet ist, wird die neueste verfügbare Version automatisch mit niedriger Priorität installiert (siehe **Standard** Auto-Update-Modus). Nach der Aktualisierung der App erfolgt keine automatische erneute Aktualisierung, bis 90 Tage nach dem erneuten Veralten der App. Der Benutzer kann die App jederzeit manuell aus dem Play Store aktualisieren.

Hohe Priorität: Die App wird so schnell wie möglich aktualisiert. Es werden keine Einschränkungen angewendet. Das Gerät wird sofort über ein neues Update benachrichtigt, sobald es verfügbar ist.

9.4. Mindestversionscode

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

9.5. Delegierte Bereiche (Scopes)

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

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

Verwaltete Konfigurationen: Gewährt Zugriff auf die Verwaltung von verwalteten Konfigurationen.

Deinstallation blockieren: Gewährt Zugriff auf das Blockieren der Deinstallation.

Berechtigungen: Gewährt Zugriff auf die Berechtigungsrichtlinie und den Status der Berechtigungserteilung.

Paketzugriff: Gewährt Zugriff auf den Status des Paketzugriffs.

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

9.6. Bevorzugtes Netzwerk

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

9.7. Standard-Berechtigungsrichtlinie

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

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

Erteilen: Eine Berechtigung automatisch erteilen.

Ablehnen: Eine Berechtigung automatisch ablehnen.

9.8. Verbindung zwischen Arbeits- und Privatprofil-Apps

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

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

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

9.9. Ausnahme vom Always-on-VPN-Lockdown

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

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

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

9.10. Arbeitsprofil-Widgets

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

Erlaubt: Die Anwendung kann Widgets zum Startbildschirm hinzufügen.

Untersagt: Die Anwendung kann keine Widgets zum Startbildschirm hinzufügen.

9.11. Benutzereinstellungen zur Kontrolle

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

Nicht spezifiziert: Verwendet das Standardverhalten der App, um zu bestimmen, ob die Benutzerkontrolle erlaubt oder untersagt ist.

Erlaubt: Die Benutzerkontrolle ist für die App erlaubt.

Untersagt: Die Benutzerkontrolle ist für die App untersagt.

9.12. Deaktiviert

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

9.13. Anbieter für Anmeldeinformationen erlauben

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

9.14. Verwaltete Konfiguration

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

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

9.15. Berechtigungsrichtlinien

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

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

9.16. Track-IDs

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

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

10. Standard-Anwendungseinstellungen

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

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

10.1. Standard-Anwendungstyp

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

10.2. Standard-Anwendungsbereiche (Scopes)

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

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

10.3. Standard-Anwendungen

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

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

11. Private-Key-Auswahl

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

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

12. Regeln zur Auswahl des privaten Schlüssels festlegen

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

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

12.1. Privater Schlüssel-Alias

Der Alias des zu verwendenden privaten Schlüssels.

12.2. URL-Muster

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

12.3. Paketnamen

Die Paketnamen, für die diese Regel gilt. Der Hash des Signierungszertifikats für jede App wird mit dem von Play bereitgestellten Hash abgeglichen. Wenn keine Paketnamen angegeben sind, wird der Alias allen Apps zur Verfügung gestellt, die ``KeyChain.choosePrivateKeyAlias`` oder eine Überladung davon aufrufen (jedoch nicht ohne den Aufruf von ``KeyChain.choosePrivateKeyAlias``, selbst unter Android 11 und höher). Jede App mit derselben Android-UID wie ein hier spezifiziertes Paket erhält Zugriff, wenn sie ``KeyChain.choosePrivateKeyAlias`` aufruft.

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

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

Kiosk-Modus

Mit dem Kiosk-Modus können Sie die Funktionalität eines Geräts auf eine einzige App oder mehrere Apps beschränken. Die Entscheidung zwischen dem Single-App- und dem Multi-App-Kiosk-Modus hängt von Ihren Geschäftszielen ab.

Im **Single-App-Kiosk-Modus** wird ein Gerät für eine einzige Anwendung konfiguriert, sodass Endbenutzer nicht auf andere Apps auf dem Gerät zugreifen können. Sie können die App auch nicht verlassen, wodurch das Gerät zu einem dedizierten Endgerät für diese spezifische App wird. Um diesen Modus zu aktivieren, legen Sie eine App im Bereich [App-Management](#) mit dem **Installationstyp** auf **Kiosk** fest.

Im **Multi-App-Kiosk-Modus** haben Geräte Zugriff auf mehrere Anwendungen. Endbenutzer können über einen benutzerdefinierten Launcher zwischen mehreren Apps navigieren. Um diesen Modus zu aktivieren, schalten Sie die Option **Kiosk-Custom-Launcher** ein.

Wenn der Kiosk-Modus aktiviert ist, können Sie auch konfigurieren, ob Endbenutzer auf bestimmte Systemfunktionen wie die Systemeinstellungen und die Statusleiste zugreifen können.

Kiosk-Custom-Launcher

Gibt an, ob der Kiosk-Custom-Launcher aktiviert ist. Dieser ersetzt den Startbildschirm durch einen Launcher, der das Gerät auf die über die Einstellung [App-Management](#) installierten Apps beschränkt. Die Apps werden alphabetisch auf einer einzigen Seite angezeigt.

Aktionen der Ein-/Austaste

Legt das Verhalten des Geräts im Kiosk-Modus fest, wenn ein Benutzer die Ein-/Austaste gedrückt hält (Langdrücken).

Verfügbar (Standard): Das Power-Menü (z. B. Ausschalten, Neustart) wird angezeigt, wenn ein Benutzer die Ein-/Austaste eines Geräts im Kiosk-Modus gedrückt hält.

Blockiert: Das Power-Menü (z. B. Ausschalten, Neustart) wird nicht angezeigt, wenn ein Benutzer die Ein-/Austaste eines Geräts im Kiosk-Modus gedrückt hält. Hinweis: Dies kann verhindern, dass Benutzer das Gerät ausschalten.

Systemfehlermeldungen

Legt fest, ob Systemfehlermeldungen für abgestürzte oder nicht reagierende Apps im Kiosk-Modus blockiert werden. Wenn sie blockiert sind, wird das System die App zwangsweise beenden, als hätte der Benutzer die Option „App schließen“ in der Benutzeroberfläche ausgewählt.

Blockiert (Standard): Alle Systemfehlermeldungen, wie Abstürze oder „App reagiert nicht“ (ANR), werden blockiert. Wenn sie blockiert sind, beendet das System die App zwangsweise, als würde der Benutzer die App über die Benutzeroberfläche schließen.

Aktiviert: Alle Systemfehlermeldungen wie Abstürze oder „App reagiert nicht“ (ANR) werden angezeigt.

Systemnavigation

Legt fest, welche Navigationsfunktionen (z. B. Home- und Übersichtstasten) im Kiosk-Modus aktiviert sind.

Deaktiviert (Standard): Die Home- und Übersichtstasten sind nicht zugänglich.

Nur Home: Nur die Home-Taste ist aktiviert.

Aktiviert: Die Home- und Übersichtstasten sind aktiviert.

Statusleiste

Legt fest, ob Systeminformationen und Benachrichtigungen im Kiosk-Modus deaktiviert sind.

Deaktiviert (Standard): Systeminformationen und Benachrichtigungen sind im Kiosk-Modus deaktiviert.

Nur System: Nur Systeminformationen werden in der Statusleiste angezeigt.

Aktiviert: Systeminformationen und Benachrichtigungen werden in der Statusleiste im Kiosk-Modus angezeigt. Hinweis: Damit diese Richtlinie wirksam wird, muss die Home-Taste des Geräts über `kioskCustomization.systemNavigation` aktiviert sein.

Geräteeinstellungen

Legt fest, ob die Einstellungen-App im Kiosk-Modus zulässig ist.

Zulässig (Standard): Der Zugriff auf die Einstellungen-App ist im Kiosk-Modus erlaubt.

Blockiert: Der Zugriff auf die Einstellungen-App ist im Kiosk-Modus nicht erlaubt.

Sicherheit

In diesem Abschnitt können Sie sicherheitsrelevante Richtlinien konfigurieren.

Aktionen bei Sicherheitsrisiken

Wählen Sie aus, was zu tun ist, wenn ein Gerät in Statusberichten ein Sicherheitsrisiko meldet.

Unterstützte Sicherheitsrisiko-Typen:

Unbekanntes Betriebssystem: Die Play Integrity API erkennt, dass das Gerät ein unbekanntes Betriebssystem ausführt (der basicIntegrity-Check ist erfolgreich, aber `ctsProfileMatch` schlägt fehl).

Kompromittiertes Betriebssystem: Die Play Integrity API erkennt, dass das Gerät ein kompromittiertes Betriebssystem ausführt (der basicIntegrity-Check schlägt fehl).

Hardwaregestützte Bewertung fehlgeschlagen: Die Play Integrity API erkennt, dass das Gerät keine starke Garantie für die Systemintegrität bietet, falls das Label `MEETS_STRONG_INTEGRITY` nicht im Feld für Geräteintegrität angezeigt wird.

Verfügbare Aktionen:

Unternehmensdaten löschen (Standard): Gerät abmelden und Arbeitsdaten löschen (das gesamte Gerät bei vollständiger Verwaltung oder nur das Arbeitsprofil bei profilgesteuerten Geräten).

Keine Aktion: Das Gerät bleibt angemeldet und es erfolgt keine automatische Aktion.

Wenn Sie **Unternehmensdaten löschen** auswählen, können Sie auch die Löschoptionen konfigurieren:

Werkseinstellungen-Schutz beibehalten: Daten zum Werkseinstellungen-Schutz (FRP) beim Löschen des Geräts beibehalten.

Externen Speicher löschen: Zusätzlich zum Löschen des Geräts wird auch der externe Speicher (wie SD-Karten) gelöscht.

eSIMs löschen: Bei unternehmenseigenen Geräten werden beim Löschen des Geräts alle eSIMs vom Gerät entfernt. Bei im Privatbesitz befindlichen Geräten werden nur verwaltete eSIMs (eSIMs, die über den Befehl ADD_ESIM hinzugefügt wurden) auf den Geräten entfernt; privatmäßig hinzugefügte eSIMs werden nicht gelöscht.

1. Max. Zeit bis zur Sperrung

Maximale Zeit (in Sekunden) für Benutzeraktivität, bis das Gerät gesperrt wird. Ein Wert von 0 bedeutet, dass keine Einschränkung besteht.

2. Bildschirm an beim Laden

Die Modi mit angeschlossenem Akku, in denen das Gerät eingeschaltet bleibt. Wenn Sie diese Einstellung verwenden, wird empfohlen, **Max. Zeit bis zur Sperrung** zu leeren, damit sich das Gerät nicht selbst sperrt, während es eingeschaltet bleibt.

Netzteil: Die Stromquelle ist ein Netzteil.

USB-Anschluss: Die Stromquelle ist ein USB-Anschluss.

Kabelloses Ladegerät: Die Stromquelle ist kabellos.

3. Sperrbildschirm deaktiviert

Wenn dies aktiviert ist, wird der Sperrbildschirm für primäre und/oder sekundäre Displays deaktiviert. Diese Richtlinie wird nur im Modus für dedizierte Geräteverwaltung unterstützt.

4. Passwortanforderungen

Richtlinien für Passwortanforderungen.

Verwenden Sie **Passwortanforderungen konfigurieren**, um einen oder mehrere Blöcke für Passwortanforderungen hinzuzufügen. Verwenden Sie **Alle löschen**, um alle konfigurierten Passwortanforderungen zu entfernen.

Passwortanforderungen können den **Auto**-Bereich (einzelne Anforderung) oder separate **Gerät/Arbeitsprofil**-Bereiche verwenden. Komplexitätsbasierte Anforderungen müssen mit qualitätsbasierten Anforderungen für denselben Bereich gekoppelt werden.

4.1. Bereich

Der Bereich, auf den sich die Passwortanforderung bezieht.

Auto: Der Bereich ist nicht festgelegt. Die Passwortanforderungen werden auf das Arbeitsprofil für Geräte mit Arbeitsprofil und auf das gesamte Gerät für vollständig verwaltete oder dedizierte Geräte angewendet.

Gerät: Die Passwortanforderungen werden nur auf das Gerät angewendet.

Arbeitsprofil: Die Passwortanforderungen werden nur auf das Arbeitsprofil angewendet.

4.2. Länge des Passwortverlaufs

Die Länge des Passwortverlaufs. Nach dem Festlegen dieses Feldes kann der Benutzer kein neues Passwort eingeben, das mit einem Passwort aus dem Verlauf identisch ist. Ein Wert von 0 bedeutet, dass keine Einschränkung besteht.

4.3. Max. fehlgeschlagene Passworteingaben für Löschung

Anzahl der fehlerhaften Passworteingaben zur Geräteentsperrung, die eingegeben werden können, bevor das Gerät gelöscht wird. Ein Wert von 0 bedeutet, dass keine Einschränkung besteht.

4.4. Ablauf der Passwortgültigkeit (Tage)

Diese Einstellung zwingt den Benutzer dazu, sein Passwort nach der angegebenen Anzahl von Tagen regelmäßig zu aktualisieren.

4.5. Passwort-Entsperrung erforderlich

Die Zeitspanne, in der ein Gerät oder Arbeitsprofil nach einer Entsperrung mittels starker Authentifizierung (Passwort, PIN, Muster) mit anderen Authentifizierungsmethoden (z. B. Fingerabdruck, Trust-Agents, Gesichtserkennung) entsperrt werden kann. Nach Ablauf des angegebenen Zeitraums können nur noch starke Authentifizierungsmethoden zur Entsperrung des Geräts oder Arbeitsprofils verwendet werden.

Standard des Geräts: Der Zeitablauf wird auf den Standard des Geräts gesetzt.

Jeden Tag: Der Zeitablauf wird auf 24 Stunden gesetzt.

4.6. Passwortqualität

Die erforderliche Passwortqualität.

Hohe Komplexität: Definiert die hohe Passwortkomplexität als: Ab Android 12: PIN ohne sich wiederholende (4444) oder geordnete (1234, 4321, 2468) Sequenzen, Länge mindestens 8; alphabetisch, Länge mindestens 6; alphanumerisch, Länge mindestens 6.

Mittlere Komplexität: Definiert die mittlere Passwortkomplexität als: PIN ohne sich wiederholende (4444) oder geordnete (1234, 4321, 2468) Sequenzen, Länge mindestens 4; alphabetisch, Länge mindestens 4; alphanumerisch, Länge mindestens 4.

Niedrige Komplexität: Definiert die niedrige Passwortkomplexität als: Muster; PIN mit sich wiederholenden (4444) oder geordneten (1234, 4321, 2468) Sequenzen.

Keine: Es gibt keine Passwortanforderungen.

Schwach: Das Gerät muss mindestens mit einer biometrischen Erkennungstechnologie mit geringer Sicherheit gesichert sein. Dies umfasst Technologien, die die Identität einer Person erkennen können und in etwa einer 3-stelligen PIN entsprechen (Fehlererkennungsrate weniger als 1 zu 1.000).

Beliebig: Ein Passwort ist erforderlich, aber es gibt keine Einschränkungen bezüglich des Inhalts des Passworts.

Numerisch: Das Passwort muss numerische Zeichen enthalten.

Numerisch komplex: Das Passwort muss numerische Zeichen enthalten, jedoch ohne sich wiederholende (4444) oder geordnete (1234, 4321, 2468) Sequenzen.

Alphabetisch: Das Passwort muss alphabetische (oder Symbol-) Zeichen enthalten.

Alphanumerisch: Das Passwort muss sowohl numerische als auch alphabetische (oder Symbol-) Zeichen enthalten.

Komplex: Das Passwort muss die Mindestanforderungen erfüllen, die in `passwordMinimumLength`, `passwordMinimumLetters`, `passwordMinimumSymbols` usw. angegeben sind. Wenn beispielsweise `passwordMinimumSymbols` auf 2 gesetzt ist, muss das Passwort mindestens zwei Symbole enthalten.

4.7. Mindestlänge

Die minimal zulässige Passwortlänge. Ein Wert von 0 bedeutet, dass keine Einschränkung besteht.

4.8. Mindestanzahl an Buchstaben

Mindestanzahl der im Passwort erforderlichen Buchstaben.

4.9. Mindestanzahl an Kleinbuchstaben

Mindestanzahl der im Passwort erforderlichen Kleinbuchstaben.

4.10. Mindestanzahl an Großbuchstaben

Mindestanzahl der im Passwort erforderlichen Großbuchstaben.

4.11. Mindestanzahl an Nicht-Buchstaben-Zeichen

Mindestanzahl der im Passwort erforderlichen Nicht-Buchstaben-Zeichen (Ziffern oder Symbole).

4.12. Mindestanzahl an Ziffern

Mindestanzahl der im Passwort erforderlichen Ziffern.

4.13. Mindestanzahl an Symbolen

Mindestanzahl der im Passwort erforderlichen Symbole.

4.14. Einheitliche Sperre

Steuert, ob eine einheitliche Sperre für das Gerät und das Arbeitsprofil zulässig ist (auf Geräten mit Android 9 oder höher und einem Arbeitsprofil). Dies hat keine Auswirkungen auf andere Geräte.

Einheitliche Sperre zulassen: Eine gemeinsame Sperre für das Gerät und das Arbeitsprofil ist zulässig.

Getrennte Arbeitssperre erforderlich: Eine separate Sperre für das Arbeitsprofil ist erforderlich.

5. Werkseinstellung deaktiviert

Ob das Zurücksetzen auf Werkseinstellungen über die Einstellungen deaktiviert ist. Nur anwendbar auf vollständig verwaltete Geräte.

6. Werkseinstellungs-Schutz

E-Mail-Adressen von Geräteadministratoren für den Werkseinstellungs-Schutz. Wenn das Gerät einen unbefugten Werksreset erfährt, muss sich einer dieser Administratoren mit der Google-Konten-E-Mail und dem Passwort anmelden, um das Gerät zu entsperren. Wenn keine Administratoren angegeben sind, bietet das Gerät keinen Werkseinstellungs-Schutz. Nur anwendbar auf vollständig verwaltete Geräte.

Administrator-E-Mails: Verwenden Sie **Werkseinstellungs-Schutz aktivieren**, um mit der Konfiguration der Administratoren zu beginnen. Verwenden Sie dann **Administrator-E-Mail hinzufügen**, um Adressen hinzuzufügen, und die Löschaktion, um sie zu entfernen.

7. Sperrbildschirm-Funktionen

Sperrbildschirm-Funktionen (Lockscreen), die deaktiviert werden können.

7.1. Alle deaktivieren

Deaktiviert alle aktuellen und zukünftigen Anpassungen des Sperrbildschirms.

7.2. Kamera deaktivieren

Deaktiviert die Kamera auf gesicherten Sperrbildschirmen (z. B. PIN).

7.3. Benachrichtigungen deaktivieren

Deaktiviert die Anzeige aller Benachrichtigungen auf gesicherten Sperrbildschirmen.

7.4. Unzensurierte Benachrichtigungen deaktivieren

Deaktiviert unzensurierte Benachrichtigungen auf gesicherten Sperrbildschirmen.

7.5. Status von Trust-Agents ignorieren

Ignoriert den Status von Trust-Agents auf gesicherten Sperrbildschirmen.

7.6. Fingerabdruck deaktivieren

Deaktiviert den Fingerabdrucksensor auf gesicherten Sperrbildschirmen.

7.7. Texteingabe in Benachrichtigungen deaktivieren

Deaktiviert die Texteingabe in Benachrichtigungen auf gesicherten Sperrbildschirmen.

7.8. Gesichtserkennung deaktivieren

Deaktiviert die Gesichtserkennung auf gesicherten Sperrbildschirmen.

7.9. Iris-Erkennung deaktivieren

Deaktiviert die Iris-Erkennung auf gesicherten Sperrbildschirmen.

7.10. Alle biometrischen Authentifizierungen deaktivieren

Deaktiviert alle biometrischen Authentifizierungen auf gesicherten Sperrbildschirmen.

7.11. Alle Verknüpfungen deaktivieren

Deaktiviert alle Verknüpfungen auf dem gesicherten Sperrbildschirm bei Android 14 und höher.

Multimedia

In diesem Abschnitt können Sie das Verhalten von Kamera/Mikrofon, den USB-Datenzugriff, das Drucken sowie Anzeigeeinschränkungen konfigurieren.

1. Kamerazugriff

Steuert die Verwendung der Kamera und ob der Benutzer auf den Schalter für den Kamerazugriff zugreifen kann (Android 12+). Im Allgemeinen gilt das Deaktivieren der Kamera geräteweit bei vollständig verwalteten Geräten und nur innerhalb des Arbeitsprofils bei Geräten mit Arbeitsprofil.

Wahl des Benutzers (Standard): Standardverhalten des Geräts. Kameras sind verfügbar und (ab Android 12+) kann der Benutzer den Kamerazugriff umschalten.

Deaktiviert: Alle Kameras sind deaktiviert (vollständig verwaltet: geräteweit; Arbeitsprofil: nur für Apps im Arbeitsprofil). Der Schalter für den Kamerazugriff hat im verwalteten Bereich keine Auswirkung.

Erzwungen: Kameras sind verfügbar. Auf vollständig verwalteten Geräten mit Android 12+ kann der Benutzer den Kamerazugriff nicht umschalten. Auf anderen Geräten/Versionen verhält sich dies wie die Option „Wahl des Benutzers“.

2. Mikrofonzugriff

Auf vollständig verwalteten Geräten steuert dies die Verwendung des Mikrofons und ob der Benutzer auf den Schalter für den Mikrofonzugriff zugreifen kann (Android 12+). Diese Einstellung hat keine Auswirkungen auf Geräte, die nicht vollständig verwaltet sind.

Wahl des Benutzers (Standard): Standardverhalten. Das Mikrofon ist verfügbar und (ab Android 12+) kann der Benutzer den Mikrofonzugriff umschalten.

Deaktiviert: Das Mikrofon ist deaktiviert (geräteweit). Der Schalter für den Mikrofonzugriff hat keine Auswirkung.

Erzwungen: Das Mikrofon ist verfügbar. Auf Android 12+ kann der Benutzer den Mikrofonzugriff nicht umschalten. Auf Android 11 oder niedriger verhält sich dies wie die Option „Wahl des Benutzers“.

3. USB-Datenzugriff

Steuert, welche Dateien und/oder Daten über USB übertragen werden können. Wird nur auf unternehmenseigenen Geräten unterstützt.

Dateiübertragung untersagen (Standard): Dateiübertragungen sind untersagt, aber andere USB-Datenverbindungen (z. B. Maus/Tastatur) sind erlaubt.

Datenübertragung untersagen: Alle Arten von USB-Datenübertragungen sind verboten (Android 12+ mit USB HAL 1.3+). Falls nicht unterstützt, fällt das Gerät auf „Dateiübertragung untersagen“ zurück.

Datenübertragung zulassen: Alle Arten von USB-Datenübertragungen sind erlaubt.

4. Drucken

Steuert, ob das Drucken erlaubt ist (Android 9+).

Zulässig (Standard): Das Drucken ist erlaubt.

Untersagt: Das Drucken ist untersagt (Android 9+).

5. Bildschirmhelligkeitseinstellungen

Steuert den Modus der Bildschirmhelligkeit und (optional) den Helligkeitswert.

Bildschirmhelligkeitsmodus:

Wahl des Benutzers (Standard): Der Benutzer darf die Bildschirmhelligkeit konfigurieren.

Automatisch: Die Helligkeit wird automatisch geregelt und der Benutzer kann sie nicht ändern. Sie können dennoch einen Helligkeitswert festlegen, der als Teil der automatischen Anpassung verwendet wird (vollständig verwaltetes Android 9+; Arbeitsprofile auf unternehmenseigenen Android 15+).

Fest: Die Helligkeit wird auf den konfigurierten Wert gesetzt und der Benutzer kann ihn nicht ändern. Der Helligkeitswert ist erforderlich (vollständig verwaltetes Android 9+; Arbeitsprofile auf unternehmenseigenen Android 15+).

Bildschirmhelligkeit:

Wert von 1 bis 255 (1 = niedrigste, 255 = höchste Helligkeit). Ein Wert von 0 bedeutet, dass kein Helligkeitswert festgelegt ist.

6. Einstellungen zum Bildschirm-Timeout

Steuert, ob der Benutzer das Bildschirm-Timeout konfigurieren kann und (wenn erzwungen) den Timeout-Wert.

Das Feld **Bildschirm-Timeout-Modus** ermöglicht die Auswahl zwischen benutzergesteuertem und erzwungenem Verhalten.

Wahl des Benutzers (Standard): Der Benutzer darf das Bildschirm-Timeout konfigurieren.

Erzwungen: Das Bildschirm-Timeout wird auf den konfigurierten Wert gesetzt und der Benutzer kann ihn nicht ändern (vollständig verwaltetes Android 9+; Arbeitsprofile auf unternehmenseigenen Android 15+).

Bildschirm-Timeout:

Timeout-Dauer in Sekunden. Der Wert muss größer als 0 sein. Wenn er größer als **Maximale Sperrzeit** ist, kann das System den Wert begrenzen und eine Nichtkonformität melden.

7. Bildschirmaufnahme deaktiviert

Ob die Bildschirmaufnahme deaktiviert ist.

8. Lautstärkeregelung deaktiviert

Ob die Anpassung der Hauptlautstärke deaktiviert ist.

9. Einbinden physischer Medien deaktiviert

Ob das Einbinden physischer externer Medien deaktiviert ist.

Cellular

In diesem Abschnitt können Sie Richtlinien im Zusammenhang mit dem Mobilfunk konfigurieren.

1. Flugmodus

Steuert, ob der Flugmodus durch den Benutzer ein- oder ausgeschaltet werden kann.

Wahl des Benutzers (Standard): Dem Benutzer ist es erlaubt, den Flugmodus ein- oder auszuschalten.

Deaktiviert: Der Flugmodus ist deaktiviert. Dem Benutzer ist es nicht erlaubt, den Flugmodus einzuschalten. Unterstützt auf Android 9 und höher.

2. Mobilfunk 2G

Steuert, ob die Mobilfunk-2G-Einstellung durch den Benutzer ein- oder ausgeschaltet werden kann.

Wahl des Benutzers (Standard): Dem Benutzer ist es erlaubt, die Mobilfunk-2G-Unterstützung ein- oder auszuschalten.

Deaktiviert: Mobilfunk 2G ist deaktiviert. Dem Benutzer ist es nicht erlaubt, Mobilfunk 2G über die Einstellungen einzuschalten. Unterstützt auf Android 14 und höher.

3. APNs überschreiben

Steuert, ob das Überschreiben von APNs aktiviert oder deaktiviert ist. Wenn es aktiviert ist, werden nur die konfigurierten Ersatz-APNs verwendet und alle anderen APNs auf dem Gerät ignoriert.

Deaktiviert (Standard): Alle konfigurierten APN-Einstellungen werden auf dem Gerät gespeichert, sind jedoch deaktiviert und haben keine Auswirkung. Alle anderen APNs auf dem Gerät bleiben in Gebrauch.

Aktiviert: Es werden nur die Ersatz-APNs verwendet, alle anderen APNs werden ignoriert. Diese Einstellung kann nur auf voll verwalteten Geräten mit Android 10 oder höher konfiguriert werden.

4. APN-Einstellungen

Konfigurieren Sie einen oder mehrere APN-Einträge. Verwenden Sie **Add APN**, um einen Eintrag zu erstellen, und **Remove APN**, um ihn zu löschen.

Jeder APN hat erforderliche Felder:

APN-Typen: Wählen Sie einen oder mehrere Datentypen für diesen APN aus (die Verfügbarkeit hängt vom Verwaltungsmodus und der Android-Version ab).

APN-Name: Die vom Mobilfunkanbieter bereitgestellte APN-Kennung.

Anzeigename: Benutzerfreundlicher Name, der in der Benutzeroberfläche angezeigt wird.

Optionale APN-Felder:

Authentifizierungstyp, Benutzername, Passwort: Konfiguration der Anbietersauthentifizierung (falls erforderlich).

Protokoll und **Roaming-Protokoll:** Konfiguration des IP-Protokolls.

Netzwerktypen: Beschränkung der Mobilfunktechnologien, die der APN verwenden darf (z. B. LTE/5G NR).

Proxy-Adresse und **Proxy-Port:** HTTP-Proxy für den Datenverkehr (falls zutreffend).

MMS-Proxy-Adresse, MMS-Proxy-Port, MMSC (MMS Center URI): Einstellungen im Zusammenhang mit MMS.

Numerische Betreiber-ID (MCC+MNC) und **Carrier ID:** Felder zur Identifizierung des Anbieters.

Always On Einstellung: Ob die durch diesen APN aktivierte PDU-Sitzung dauerhaft (always-on) aktiv bleiben soll. Unterstützt auf Android 15 und höher.

MVNO-Typ: Identifikationstyp des mobilen virtuellen Netzbetreibers.

MTU IPv4 und **MTU IPv6:** Maximum Transmission Unit für IPv4/IPv6-Routen. Unterstützt auf Android 13 und höher.

5. Zellbroadcast-Konfiguration deaktiviert

Ob die Konfiguration von Zellbroadcast deaktiviert ist.

6. Mobilfunknetz-Konfiguration deaktiviert

Ob die Konfiguration von Mobilfunknetzen deaktiviert ist.

7. Daten-Roaming deaktiviert

Ob die Daten-Roaming-Dienste deaktiviert sind.

8. ausgehende Anrufe deaktiviert

Ob ausgehende Anrufe deaktiviert sind.

9. SMS deaktiviert

Ob das Senden und Empfangen von SMS-Nachrichten deaktiviert ist.

10. 5G Network Slicing Konfiguration

Konfigurieren Sie die Einstellungen für den bevorzugten Netzwerkdienst, um das unternehmensweite 5G-Network-Slicing zu aktivieren. Sie können bis zu 5 Unternehmens-Slices einrichten und Anwendungen spezifischen Netzwerken zuweisen, um das Traffic-Routing zu optimieren.

10.1. Standard-bevorzugtes Netzwerk

Standard-ID des bevorzugten Netzwerks für Anwendungen, die nicht in der Anwendungsliste enthalten sind, oder falls das **Preferential Network** einer App nicht festgelegt ist. Es muss eine Konfiguration für die angegebene Netzwerk-ID vorhanden sein (außer wenn **No Preferential Network** eingestellt ist).

Hinweis: Kritische Apps wie **com.google.android.apps.work.clouddpc** und **com.google.android.gms** sind von dieser Standardeinstellung ausgeschlossen.

10.2. Netzwerkdienst-Konfigurationen

Verwenden Sie **Add Network Configuration**, um eine Slice-Konfiguration zu erstellen. Sie können bis zu 5 Konfigurationen hinzufügen. Jede Konfiguration enthält:

Preferential Network ID (Auto-assigned): Die Netzwerk-ID wird automatisch zugewiesen und kann nicht geändert werden.

Fallback to Default Connection: Ob ein Fallback auf das geräteweite Standardnetzwerk erlaubt ist. Wenn dies untersagt ist, können Apps nicht auf das Internet zugreifen, falls der 5G-Slice nicht verfügbar ist.

Non-Matching Networks: Ob Apps, die dieser Konfiguration unterliegen, Netzwerke verwenden dürfen, die nicht dem bevorzugten Dienst entsprechen. Wenn dies auf **Disallowed** gesetzt ist, muss auch **Fallback to Default Connection** auf **Disallowed** stehen. Erfordert Android 14 oder höher.

Netzwerk

In diesem Abschnitt können Sie Richtlinien im Zusammenhang mit dem Netzwerk konfigurieren.

Wi-Fi-Konfigurationen können durch das System über **Wi-Fi-Konfigurationen** bereitgestellt und verwaltet werden. Je nach dem unter **Wi-Fi konfigurieren** festgelegten Wert haben Benutzer möglicherweise nur begrenzten oder gar keinen Zugriff auf das Hinzufügen/Ändern von Netzwerken.

Funkstatus des Geräts

1. Wi-Fi-Status

Steuert den aktuellen Wi-Fi-Status und ob der Benutzer diesen ändern kann.

Wahl des Benutzers (Standard): Der Benutzer darf Wi-Fi aktivieren/deaktivieren.

Aktiviert: Wi-Fi ist eingeschaltet und der Benutzer darf es nicht ausschalten (Android 13+).

Deaktiviert: Wi-Fi ist ausgeschaltet und der Benutzer darf es nicht einschalten (Android 13+).

2. Mindest-Wi-Fi-Sicherheitsstufe

Die erforderliche Mindestsicherheitsstufe für Wi-Fi-Netzwerke, mit denen sich das Gerät verbinden kann. Unterstützt ab Android 13 für vollständig verwaltete Geräte und Arbeitsprofile auf unternehmenseigenen Geräten.

Offenes Netzwerk (Standard): Das Gerät kann sich mit allen Arten von Wi-Fi-Netzwerken verbinden.

Persönliches Netzwerk: Verbietet offene Wi-Fi-Netzwerke; erfordert mindestens persönliche Sicherheit (zum Beispiel WPA2-PSK).

Unternehmensnetzwerk: Erfordert EAP-Unternehmensnetzwerke; verbietet Wi-Fi-Netzwerke unterhalb dieser Sicherheitsstufe.

192-Bit-Unternehmensnetzwerk: Erfordert 192-Bit-Unternehmensnetzwerke; strengste Option.

3. Ultra-Breitband (UWB)-Status

Steuert den Status der Ultra-Breitband-Einstellung und ob der Benutzer diese ein- oder ausschalten kann.

Wahl des Benutzers (Standard): Der Benutzer darf UWB ein- oder ausschalten.

Deaktiviert: UWB ist deaktiviert und der Benutzer darf es nicht über die Einstellungen umschalten (Android 14+).

Geräte-Konnektivitätsmanagement

4. Bluetooth-Freigabe

Steuert, ob die Bluetooth-Freigabe zulässig ist.

Zulässig: Die Bluetooth-Freigabe ist erlaubt (Standard bei vollständig verwalteten Geräten, Android 8+).

Untersagt: Die Bluetooth-Freigabe ist untersagt (Standard bei Arbeitsprofilen, Android 8+).

5. Wi-Fi konfigurieren

Steuert die Berechtigungen zur Wi-Fi-Konfiguration. Je nach gewählter Option hat der Benutzer die volle, begrenzte oder gar keine Kontrolle bei der Konfiguration von Wi-Fi-Netzwerken.

Wi-Fi konfigurieren erlauben (Standard): Der Benutzer darf Wi-Fi konfigurieren.

Hinzufügen von Wi-Fi-Konfigurationen untersagen: Das Hinzufügen neuer Wi-Fi-Konfigurationen ist untersagt. Der Benutzer kann zwischen bereits konfigurierten Netzwerken wechseln (Android 13+; vollständig verwaltete Geräte und unternehmenseigene Arbeitsprofile).

Wi-Fi-Konfiguration untersagen: Das Konfigurieren von Wi-Fi-Netzwerken ist untersagt. Bei vollständig verwalteten Geräten werden benutzerkonfigurierte Netzwerke entfernt und es bleiben nur über **Wi-Fi-Konfigurationen** konfigurierte Netzwerke beibehalten. Bei unternehmenseigenen Arbeitsprofilen sind bestehende Netzwerke nicht betroffen, aber Benutzer können keine Wi-Fi-Netzwerke hinzufügen, entfernen oder ändern.

Wenn die Wi-Fi-Konfiguration deaktiviert ist und das Gerät beim Booten keine Verbindung herstellen kann, kann das System die **Netzwerk-Notausgang** anzeigen, um dem Benutzer eine vorübergehende Verbindung zu ermöglichen und die Richtlinie zu aktualisieren.

6. Wi-Fi-Direct-Einstellungen

Steuert die Konfiguration und Nutzung von Wi-Fi-Direct-Einstellungen. Wird auf unternehmenseigenen Geräten mit Android 13 und höher unterstützt.

Zulassen (Standard): Der Benutzer darf Wi-Fi Direct verwenden.

Untersagen: Der Benutzer darf kein Wi-Fi Direct verwenden.

7. Tethering-Einstellungen

Steuert die Tethering-Einstellungen. Je nach gewähltem Wert wird dem Benutzer die Nutzung verschiedener Formen des Tetherings teilweise oder vollständig untersagt.

Alle Tethering-Arten erlauben (Standard): Erlaubt die Konfiguration und Nutzung aller Formen des Tetherings.

Wi-Fi-Tethering untersagen: Verhindert, dass der Benutzer Wi-Fi-Tethering verwendet (unternehmenseigene Android 13+).

Alle Tethering-Arten untersagen: Verbietet alle Formen des Tetherings (vollständig verwaltete Geräte + unternehmenseigene Arbeitsprofile).

8. Wi-Fi-SSID-Richtlinie

Beschränkungen für die Wi-Fi-SSIDs, mit denen sich das Gerät verbinden kann (dies hat keinen Einfluss darauf, welche Netzwerke auf dem Gerät konfiguriert werden können). Wird auf unternehmenseigenen Geräten mit Android 13 und höher unterstützt.

SSID-Denylist (Standard): Das Gerät kann sich mit keinem Wi-Fi-Netzwerk verbinden, dessen SSID in der Liste steht, kann sich aber mit anderen Netzwerken verbinden.

SSID-Allowlist: Das Gerät kann sich nur mit den aufgeführten SSIDs verbinden. Die SSID-Liste darf nicht leer sein.

Verwenden Sie **SSID hinzufügen**, um Einträge hinzuzufügen. Je nach gewähltem Richtlinientyp wird die Liste als erlaubte oder verbotene SSIDs interpretiert.

In der Benutzeroberfläche des Richtlinien-Editors wird die SSID-Liste für Allowlisten als **Erlaubte Wi-Fi-SSIDs** und für Denylists als **Verbotene Wi-Fi-SSIDs** bezeichnet.

9. Wi-Fi-Roaming-Einstellungen

Konfigurieren Sie den Wi-Fi-Roaming-Modus pro SSID. Verwenden Sie **Wi-Fi-Roaming-Einstellung hinzufügen**, um Einträge zu erstellen.

Jeder Eintrag enthält:

SSID: Die SSID, für die die Roaming-Einstellung gilt (erforderlich).

Wi-Fi-Roaming-Modus: Standard / Deaktiviert / Aggressiv. Die Optionen „Deaktiviert“ und „Aggressiv“ erfordern Android 15+ und werden nur auf vollständig verwalteten Geräten sowie Arbeitsprofilen auf unternehmenseigenen Geräten unterstützt.

Netzwerkbeschränkungen

10. Bluetooth deaktiviert

Ob Bluetooth deaktiviert ist. Diese Einstellung wird der Option „Bluetooth-Konfiguration deaktiviert“ vorgezogen, da die Bluetooth-Konfiguration vom Benutzer umgangen werden kann.

11. Bluetooth-Kontaktsymbole-Freigabe deaktiviert

Ob die Bluetooth-Kontaktsymbole-Freigabe deaktiviert ist.

12. Bluetooth-Konfiguration deaktiviert

Ob die Konfiguration von Bluetooth deaktiviert ist.

13. Netzwerk-Reset deaktiviert

Ob das Zurücksetzen der Netzwerkeinstellungen deaktiviert ist.

14. Android Beam (ausgehend) deaktiviert

Ob die Verwendung von NFC zum Senden von Daten aus Apps deaktiviert ist.

VPN

15. Always-on-VPN-App

Geben Sie einen Paketnamen für die Always-on-VPN-App an, um sicherzustellen, dass Daten von den angegebenen verwalteten Apps immer über ein konfiguriertes VPN gesendet werden.

Hinweis: Diese Funktion erfordert den Einsatz eines VPN-Clients, der sowohl die Always-on- als auch die App-spezifische VPN-Funktion unterstützt.

16. VPN-Lockdown

Verhindert die Nutzung des Netzwerks, wenn keine VPN-Verbindung besteht.

17. VPN-Konfiguration deaktiviert

Ob die Konfiguration von VPN deaktiviert ist.

Proxy und Netzwerkdienste

18. Bevorzugter Netzwerkdienst

Steuert, ob ein bevorzugter Netzwerkdienst im Arbeitsprofil aktiviert ist. Beispielsweise kann eine Organisation mit einem Mobilfunkanbieter vereinbart haben, dass geschäftliche Daten über einen speziellen Netzwerkdienst für die Unternehmensnutzung gesendet werden (z. B. ein Enterprise-Slice in 5G-Netzen). Dies hat keine Auswirkungen auf vollständig verwaltete Geräte.

Deaktiviert: Der bevorzugte Netzwerkdienst ist im Arbeitsprofil deaktiviert.

Aktiviert: Der bevorzugte Netzwerkdienst ist im Arbeitsprofil aktiviert.

Wenn Sie Enterprise-Network-Slicing verwenden, konfigurieren Sie zusätzlich die **5G-Network-Slicing-Konfiguration** im Bereich **Mobilfunk** und weisen Apps einem Slice über die Einstellung **Bevorzugter Netzwerkdienst** zu.

19. Empfohlener globaler Proxy

Der netzwerkunabhängige globale HTTP-Proxy. Normalerweise sollten Proxys pro Netzwerk in den Wi-Fi-Konfigurationen eingerichtet werden. Ein globaler Proxy kann bei ungewöhnlichen Konfigurationen, wie etwa einer allgemeinen internen Filterung, nützlich sein. Der globale Proxy ist lediglich eine Empfehlung und einige Apps ignorieren ihn möglicherweise.

Deaktiviert

Direkt-Proxy

Proxy-Autokonfiguration (PAC)

19.1. Host

Der Host des Direkt-Proxys.

19.2. Port

Der Port des Direkt-Proxys.

19.3. PAC-URI

Die URI des zum Konfigurieren des Proxys verwendeten PAC-Skripts.

19.4. Ausgeschlossene Hosts

Bei einem Direkt-Proxy sind dies die Hosts, für die der Proxy umgangen wird. Hostnamen können Platzhalter wie ***.example.com** enthalten.

Verwenden Sie **Ausgeschlossenen Host hinzufügen**, um Einträge hinzuzufügen (nur für Direkt-Proxy verfügbar).

Wi-Fi-Konfigurationen

Definieren Sie Wi-Fi-Netzwerkkonfigurationen, die das System auf Geräten anwendet. Verwenden Sie **Wi-Fi-Konfiguration hinzufügen**, um einen Eintrag zu erstellen und diesen mit der Löschaktion wieder zu entfernen.

20. Wi-Fi-Konfigurationsfelder

Jede Konfiguration umfasst:

Konfigurationsname: Erforderlich.

SSID: Erforderlich.

Automatischer Verbindungsaufbau: Gibt an, ob das Netzwerk automatisch verbunden werden soll, wenn es in Reichweite ist.

Fast Transition: Gibt an, ob der Client versuchen soll, Fast Transition (IEEE 802.11r-2008) mit dem Netzwerk zu nutzen.

Versteckte SSID: Gibt an, ob die SSID ausgestrahlt wird.

MAC-Randomisierungsmodus: Hardware oder Automatisch (Android 13+).

20.1. Sicherheit

Wi-Fi-Sicherheitsoptionen:

WEP-PSK: WEP (Pre-Shared Key).

WPA-PSK: WPA/WPA2/WPA3-Personal (Pre-Shared Key).

WPA-EAP: WPA/WPA2/WPA3-Enterprise (Extensible Authentication Protocol).

WPA3 192-Bit-Modus: WPA-EAP-Netzwerk, das nur den WPA3 192-Bit-Modus zulässt.

20.2. Passphrase (Pre-Shared Key)

Wird angezeigt, wenn die Sicherheit auf **WEP-PSK** oder **WPA-PSK** eingestellt ist. Die Passphrase ist erforderlich.

20.3. EAP-Methode (Enterprise)

Wird angezeigt, wenn die Sicherheit auf **WPA-EAP** oder **WPA3 192-Bit-Modus** eingestellt ist. Wählen Sie eine EAP-äußere Methode:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Authentifizierung der Phase 2

Wird für Tunneling-äußere Methoden (**EAP-TTLS** und **PEAP**) angezeigt.

MSCHAPv2

PAP

20.5. EAP-Anmeldedaten von Benutzern

Wenn diese Funktion aktiviert ist, wendet das System EAP-Anmeldedaten automatisch auf Benutzerbasis auf den Geräten an. Sie können Benutzeranmeldedaten im Bereich **Benutzer** konfigurieren.

20.6. Client-Zertifikat

Für **EAP-TLS** können Sie ein Client-Zertifikat zuweisen, das für die Wi-Fi-Authentifizierung verwendet wird. Weitere Informationen finden Sie auf der Seite [Zertifikatsverwaltung](#).

Wenn bereits ein Zertifikat zugewiesen ist, können Sie **Zertifikat öffnen** verwenden, um es anzuzeigen, oder **Zertifikat ändern**, um ein anderes auszuwählen.

Alternativ können Sie einen **Alias für das Client-Zertifikatsschlüsselpaar** angeben, der auf ein im Android-Schlüsselbund gespeichertes und für die Wi-Fi-Authentifizierung zugelassenes Client-Zertifikat verweist.

Wenn sowohl das **Client-Zertifikat** als auch der **Alias für das Client-Zertifikatsschlüsselpaar** festgelegt sind, wird der Schlüsselpaar-Alias ignoriert.

20.7. Identität

Identität des Benutzers. Bei Tunneling-äußeren Protokollen (PEAP, EAP-TTLS) wird dies zur Authentifizierung innerhalb des Tunnels verwendet, während die **Anonyme Identität** für die EAP-Identität außerhalb des Tunnels verwendet wird. Bei Protokollen ohne Tunneling dient dies als EAP-Identität.

20.8. Anonyme Identität

Nur für Tunneling-Protokolle gibt dies die Identität des Benutzers an, die dem äußeren Protokoll übermittelt wird.

20.9. Passwort

Passwort des Benutzers. Wenn nicht angegeben, wird der Benutzer standardmäßig zur Eingabe aufgefordert.

20.10. Server-CA-Zertifikate

Liste der CA-Zertifikate, die zur Überprüfung der Zertifikatskette des Hosts verwendet werden sollen. Mindestens ein CA-Zertifikat muss übereinstimmen. Weitere Informationen finden Sie auf der Seite [Zertifikatsverwaltung](#).

Verwenden Sie **Server-CA-Zertifikat hinzufügen**, um Einträge hinzuzufügen, und die Löschaktion, um sie zu entfernen.

20.11. Übereinstimmung der Domänen-Suffixe

Eine Liste von Einschränkungen für den Server-Domännennamen. Die Einträge werden als Anforderungen für die Suffix-Übereinstimmung mit dem(n) DNS-Namen des alternativen Subjektnamens eines Authentifizierungsserver-Zertifikats verwendet.

System

In diesem Abschnitt können Sie systemrelevante Richtlinien konfigurieren.

1. Mindest-API-Level

Das minimal zulässige Android-API-Level.

2. Verschlüsselungsrichtlinie

Ob die Verschlüsselung aktiviert ist.

Standard: Dieser Wert wird ignoriert, d. h. es ist keine Verschlüsselung erforderlich.

Aktiviert ohne Passwort: Verschlüsselung erforderlich, aber kein Passwort für den Systemstart notwendig.

Aktiviert mit Passwort: Verschlüsselung erforderlich, wobei ein Passwort für den Systemstart notwendig ist.

3. Automatische Datum- und Zeiteinstellung

Ob die automatische Einstellung von Datum, Uhrzeit und Zeitzone auf einem unternehmenseigenen Gerät aktiviert ist.

Wahl des Benutzers (Standard): Automatische Einstellung von Datum, Uhrzeit und Zeitzone werden der Entscheidung des Benutzers überlassen.

Erzwungen: Erzwingt die automatische Einstellung von Datum, Uhrzeit und Zeitzone auf dem Gerät.

4. Entwickleroptionen

Steuert den Zugriff auf die Entwickleroptionen: Entwickleroptionen und sicherer Startmodus.

Deaktiviert (Standard): Deaktiviert alle Entwickleroptionen und verhindert den Zugriff des Benutzers darauf.

Zugelassen: Alle Entwickleroptionen sind erlaubt. Der Benutzer kann auf die Einstellungen zugreifen und diese optional konfigurieren.

5. Common-Criteria-Modus

Steuert den Common-Criteria-Modus – Sicherheitsstandards, die in den Common Criteria for Information Technology Security Evaluation (CC) definiert sind. Durch das Aktivieren des Common-Criteria-Modus werden bestimmte Sicherheitskomponenten auf einem Gerät verstärkt (z. B. AES-GCM-Verschlüsselung von Bluetooth Long Term Keys, zusätzliche Validierung für einige Netzwerkerzeugnisse und kryptografische Richtlinienintegritätsprüfungen). Der Common-Criteria-Modus wird nur auf unternehmenseigenen Geräten mit Android 11 oder höher unterstützt.

Warnung: Der Common-Criteria-Modus erzwingt ein strenges Sicherheitsmodell, das in der Regel nur für hochsensible Organisationen erforderlich ist. Die Standardnutzung des Geräts 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.

Wahl des Benutzers (Standard): Der Benutzer kann entscheiden, MTE auf dem Gerät zu aktivieren oder zu deaktivieren (sofern das Gerät dies unterstützt).

Erzwungen: MTE ist aktiviert und der Benutzer darf dies nicht ändern (Android 14+; unterstützt auf vollständig verwalteten Geräten und Arbeitsprofilen auf unternehmenseigenen Geräten).

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

7. Inhalts-Schutz

Steuert, ob der Inhaltsschutz (der nach betrügerischen Apps scannt) aktiviert ist. Dies wird ab Android 15 unterstützt.

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

Erzwungen: Der Inhaltsschutz ist aktiviert und der Benutzer kann dies nicht ändern (Android 15+).

Wahl des Benutzers: Der Inhaltsschutz wird nicht durch die Richtlinie gesteuert; der Benutzer kann wählen (Android 15+).

8. Assist-Inhalt

Steuert, ob die Weitergabe von Assist-Inhalten an eine privilegierte App wie eine Assistenten-App (z. B. Circle to Search) zulässig ist. Assist-Inhalte umfassen Screenshots und Informationen über eine App, wie z. B. den Paketnamen. Dies wird ab Android 15 unterstützt.

Zugelassen (Standard): Die Weitergabe von Assist-Inhalten an eine privilegierte App ist zulässig (Android 15+).

Nicht zulässig: Die Weitergabe von Assist-Inhalten an eine privilegierte App wird blockiert (Android 15+).

9. Fenstererstellung deaktiviert

Ob das Erstellen von Fenstern (außer App-Fenstern) deaktiviert ist. Diese Option verhindert die Anzeige der folgenden System-UIs: Toasts und Snackbars, Telefonaktivitäten (wie eingehende Anrufe) und prioritäre Telefonaktivitäten (wie laufende Anrufe), Systemwarnungen, Systemfehler und System-Overlays.

10. Netzwerk-Notausstieg

Ob der Netzwerk-Notausstieg aktiviert ist. Wenn zum Zeitpunkt des Systemstarts keine Netzwerkverbindung hergestellt werden kann, fordert der Notausstieg den Benutzer auf, sich vorübergehend mit einem Netzwerk zu verbinden, um die Geräterichtlinie zu aktualisieren. Nach der Anwendung der Richtlinie wird das temporäre Netzwerk vergessen und das Gerät setzt den Startvorgang fort. Dies verhindert, dass eine Verbindung zu einem Netzwerk unmöglich wird, falls in der letzten Richtlinie kein geeignetes Netzwerk vorhanden war und das Gerät in den App-Lock-Task-Modus startet oder der Benutzer anderweitig keinen Zugriff auf die Geräteeinstellungen hat.

11. Standardaktivitäten

Eine Liste von Standardaktivitäten zur Verarbeitung von Intents, die einem bestimmten Intent-Filter entsprechen. Beispielsweise würde diese Funktion es IT-Administratoren ermöglichen, auszuwählen, welche Browser-App Web-Links automatisch öffnet oder welche Launcher-App beim Tippen auf die Home-Taste verwendet wird.

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

11.1. Empfänger-Aktivität

Die Aktivität, die als Standard-Intent-Handler fungieren soll. Dies sollte ein Android-Komponentenname sein, z. B. `com.android.enterprise.app/.MainActivity`. Alternativ kann der Wert der Paketname einer App sein, woraufhin die Android Device Policy eine geeignete Aktivität aus dieser App zur Verarbeitung des Intents auswählt.

11.2. Aktion

Die in den Filter einzubeziehenden Intent-Aktionen. Wenn Aktionen im Filter enthalten sind, muss die Aktion eines Intents mit einem dieser Werte übereinstimmen, damit er passt. Wenn keine Aktionen enthalten sind, wird die Intent-Aktion ignoriert.

11.3. Kategorie

Die in den Filter einzubeziehenden Intent-Kategorien. Ein Intent enthält die Kategorien, die er erfordert; alle diese müssen im Filter enthalten sein, damit eine Übereinstimmung erfolgt. Mit anderen Worten: Das Hinzufügen einer Kategorie zum Filter hat keine Auswirkungen auf die Übereinstimmung, es sei denn, diese Kategorie ist im Intent spezifiziert.

12. Zulässige Eingabemethoden

Legt die zulässigen Eingabemethoden fest.

Alle erlauben: Es werden keine Einschränkungen angewendet. Alle Eingabemethoden sind zulässig.

Nur die des Systems: Nur die im System integrierten Eingabemethoden sind zulässig.

Nur die des Systems und bereitgestellten: Nur die bereitgestellten und die im System integrierten Eingabemethoden sind zulässig.

12.1. Zugelassene Eingabemethoden

Paketnamen der erlaubten Eingabemethoden. Dies gilt nur, wenn **Zulässige Eingabemethoden** auf **Nur die des Systems und bereitgestellten** gesetzt ist.

Verwenden Sie **Eingabemethode hinzufügen**, um Einträge hinzuzufügen, und die Löschaktion, um sie zu entfernen.

13. Zulässige Bedienungshilfen

Legt die zulässigen Bedienungshilfen fest.

Alle erlauben: Jede beliebige Bedienungshilfe kann verwendet werden.

Nur die des Systems: Nur die im System integrierten Bedienungshilfen können verwendet werden.

Nur die des Systems und bereitgestellten: Nur die bereitgestellten und die im System integrierten Bedienungshilfen können verwendet werden.

13.1. Zugelassene Bedienungshilfen

Zugelassene Bedienungshilfen. Dies gilt nur, wenn **Zulässige Bedienungshilfen** auf **Nur die des Systems und bereitgestellten** gesetzt ist.

Verwenden Sie **Bedienungshilfe hinzufügen**, um Einträge hinzuzufügen, und die Löschaktion, um sie zu entfernen.

14. System-Update-Richtlinie

Konfiguration zur Verwaltung von System-Updates.

Standard: Das Standard-Updateverhalten des Geräts wird befolgt, was in der Regel erfordert, dass der Benutzer System-Updates akzeptiert.

Automatisch: Automatische Installation, sobald ein Update verfügbar ist.

Fensterbasiert: Automatische Installation innerhalb eines täglichen Wartungsfensters. Dies konfiguriert auch Play-Apps so, dass sie innerhalb des Fensters aktualisiert werden. Dies wird für Kiosk-Geräte dringend empfohlen, da dies der einzige Weg ist, wie im Vordergrund fixierte Apps durch Play aktualisiert werden können.

Aufschieben: Die automatische Installation wird um maximal 30 Tage aufgeschoben.

14.1. Wartungsfenster (nur für Fensterbasiert)

Wenn die **System-Update-Richtlinie** auf **Fensterbasiert** eingestellt ist, können Sie das tägliche Wartungsfenster über die Felder **von** und **|>bis** definieren.

14.2. Sperrzeiten für System-Updates

Ein jährlich wiederkehrender Zeitraum, in dem Over-the-Air (OTA) System-Updates aufgeschoben werden, um die auf einem Gerät laufende Betriebssystemversion einzufrieren. Um ein unendliches Einfrieren des Geräts zu verhindern, muss jede Sperrperiode durch mindestens 60 Tage getrennt sein. Jede Sperrperiode darf 90 Tage nicht überschreiten.

Verwenden Sie **System-Update-Sperrperiode hinzufügen**, um Einträge zu erstellen.

15. Standard-Anmeldeinformationsanbieter

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

Nicht zulässig (Standard): Apps, für die keine credentialProviderPolicy festgelegt wurde, dürfen nicht als Anmeldeinformationsanbieter fungieren.

Nicht zulässig, außer System: Apps, für die keine credentialProviderPolicy festgelegt wurde, dürfen nicht als Anmeldeinformationsanbieter fungieren, außer den standardmäßigen Anmeldeinformationsanbietern des Herstellers (OEM).

Standort und Geofencing

Dieses Panel gruppiert die Android-Richtlinieneinstellungen, mit denen die Standortberichterstattung des Geräts, die Durchsetzung von Standorten und Geofencing-Definitionen gesteuert werden. Verwenden Sie es, wenn Cerberus Enterprise die Standorte von Geräten erfassen oder erkennen soll, wenn Geräte konfigurierte Bereiche betreten oder verlassen.

Standortberichterstattung

Standort melden

Aktiviert die Berichterstattung über die Geolokalisierung des Geräts. Die über diese Einstellung erfassten Standortdaten werden für die [Standortkarte im Dashboard](#), den Standortverlauf in der Geräteübersicht und die Geofencing-Verarbeitung verwendet.

Bei Geräten, die nicht vollständig verwaltet werden, können die Standortdaten weiterhin davon abhängen, dass die Cerberus Enterprise App über die erforderlichen Standortberechtigungen verfügt und die Standortdienste auf dem Gerät aktiviert sind.

Standortmodus

Steuert die Standorteinstellung auf unternehmenseigenen Geräten.

- **Wahl des Benutzers:** Die Standortdienste werden nicht durch die Richtlinie eingeschränkt.
- **Erzwungen:** Die Standortdienste sind auf dem Gerät aktiviert.
- **Deaktiviert:** Die Standortdienste sind auf dem Gerät deaktiviert.

Standortfreigabe deaktiviert

Deaktiviert die Standortfreigabe für Work-Apps. Auf Geräten mit Profile Owner wirkt sich dies auf das Arbeitsprofil aus. Bei vollständig verwalteten Geräten wird der Standort für das gesamte Gerät deaktiviert und überschreibt den Standortmodus des Geräts.

Automatisches Verhalten bei aktiven Geofences

Aktive Geofences erfordern die Standortberichterstattung, um zu funktionieren. Wenn mindestens ein Geofence aktiv ist, hält Cerberus Enterprise die zugehörigen Standorteinstellungen automatisch konsistent.

- **Standort melden** wird erzwungen, solange aktive Geofences existieren.
- **Standortmodus** wird auf **Erzwungen** gesetzt.
- **Standortfreigabe deaktiviert** wird erzwungen deaktiviert.

Wenn Sie versuchen, **Standort melden** zu deaktivieren, während ein oder mehrere Geofences aktiv sind, zeigt Cerberus Enterprise einen Bestätigungsdialog an. Wenn Sie fortfahren, werden alle aktiven Geofences in der Richtlinie deaktiviert.

Geofence-Liste

Eine Richtlinie kann bis zu **10 Geofences** enthalten. Geofence-Namen müssen innerhalb der Richtlinie eindeutig sein.

Verwenden Sie **Geofence hinzufügen**, um einen neuen Eintrag zu erstellen. Jeder Geofence enthält diese Hauptfelder:

- **Name**: erforderlich und eindeutig.
- **Breitengrad** und **Längengrad**: das Zentrum des Bereichs.
- **Radius (m)**: erforderlich, von **100** bis **10000** Meter.
- **Beschreibung**: optionale Notizen für Administratoren.
- **Betreten melden** und **Verlassen melden**: wählen Sie aus, welche Übergangereignisse generiert werden sollen.
- **Aktiv**: aktiviert oder deaktiviert den Geofence, ohne ihn zu löschen.

Mindestens eine der Optionen **Betreten melden** oder **Verlassen melden** muss für jeden Geofence aktiviert bleiben.

Kartenbearbeitungswerkzeuge

Jede Geofence-Karte enthält eine Kartenvorschau des Bereichs. Sie können die Geometrie direkt über die Karte oder über die numerischen Felder bearbeiten.

- Klicken Sie auf die Karte, um das Zentrum des Geofences zu verschieben, wenn die Bereichsbearbeitung entsperrt ist.
- Verwenden Sie die Schaltfläche **Aktueller Standort**, um die Karte auf Ihrer aktuellen Browserposition zu zentrieren.
- Verwenden Sie die Schaltfläche **Karte neu zentrieren**, um die bevorzugte Ansicht für diesen Geofence wiederherzustellen.
- Verwenden Sie die Sperrschaltfläche, um versehentliche Änderungen an der Geofence-Geometrie zu verhindern.

Wo Geofence-Daten angezeigt werden

Geofence-Übergänge können auf der Android-[Geräteübersicht](#)-Seite im **Geofence**-Tab des Standort-Panels eingesehen werden. Dieser Tab zeigt Übergänge auf einer dedizierten Karte zusammen mit Filterwerkzeugen und der Übergangsliste an.

Benutzerverwaltung

Benutzer hinzufügen deaktiviert

Ob das Hinzufügen neuer Benutzer und Profile deaktiviert ist. Bei Geräten, bei denen der managementMode auf **DEVICE_OWNER** eingestellt ist, wird dieses Feld ignoriert und der Benutzer darf niemals Benutzer hinzufügen oder entfernen.

Kontenbearbeitung deaktiviert

Ob das Hinzufügen oder Entfernen von Konten deaktiviert ist.

Konfiguration von Benutzeranmeldedaten deaktiviert

Ob die Konfiguration von Benutzeranmeldedaten deaktiviert ist.

Benutzerentfernung deaktiviert

Ob das Entfernen anderer Benutzer deaktiviert ist.

Festlegen des Benutzer-Icons deaktiviert

Ob das Ändern des Benutzer-Icons deaktiviert ist.

Festlegen des Hintergrundbilds deaktiviert

Ob das Ändern des Hintergrundbilds deaktiviert ist.

Authentifizierung bei der Einrichtung des Geschäftskontos

Steuert, wie sich Benutzer bei der Einrichtung des Geschäftskontos authentifizieren. Diese Option ist nur für Android-Unternehmen verfügbar, die durch eine verwaltete Google-Domain (Google Workspace) unterstützt werden.

Während der Geräteeinrichtung/Registrierung beeinflusst diese Richtlinie, ob eine Anmeldung mit einem Geschäftskonto erforderlich ist, aber die Einstellung **Authentifizierung über Google** in der Google Admin Konsole und der Registrierungstyp können weiterhin eine Authentifizierung erfordern.

Bei bereits registrierten Geräten gilt diese Richtlinie nur, wenn das Gerät über ein verwaltetes Google Play-Konto verwaltet wird (d. h. registriert ohne **Registrierung über Authentifizierung mit Google**).

Weitere Einzelheiten und Fehlerbehebung finden Sie unter [Registrierung über Authentifizierung mit Google](#).

Blockierte Kontotypen

Kontotypen, die nicht vom Benutzer verwaltet werden können. Diese Option verhindert, dass Gerätebenutzer nicht genehmigte Konten hinzufügen.

Verwenden Sie **Blockierten Kontotyp hinzufügen**, um einen oder mehrere Kontotypen hinzuzufügen.

Jeder Eintrag hat ein Pflichtfeld **Kontotyp**. Geben Sie eine Zeichenfolge wie **com.google** ein. Entfernen Sie einen Eintrag über die Löschaktion.

Private Nutzung

Wenn Sie [ein unternehmenseigenes Gerät für die geschäftliche und private Nutzung bereitstellen](#), können Sie bestimmte Regeln festlegen, um die Nutzung des Geräts für private Zwecke außerhalb des Arbeitsprofils einzuschränken.

Dieser Abschnitt gilt nur für unternehmenseigene Geräte mit Arbeitsprofil. Er hat keine Auswirkungen auf vollständig verwaltete oder im Privatbesitz befindliche Geräte.

1. Kamera deaktiviert

Ob die Kamera deaktiviert ist.

2. Bildschirmaufnahme deaktiviert

Ob die Bildschirmaufnahme deaktiviert ist.

3. Max. Tage mit deaktiviertem Arbeitsprofil

Steuert, wie lange das Arbeitsprofil deaktiviert bleiben kann.

4. Bluetooth-Freigabe

Steuert, ob die Bluetooth-Freigabe im persönlichen Profil eines unternehmenseigenen Geräts mit Arbeitsprofil zulässig ist.

5. Privater Bereich

Steuert, ob ein privater Bereich auf dem Gerät zulässig ist.

6. Play-Store-Modus

Dieser Modus steuert, welche Apps dem Benutzer im Play Store des persönlichen Profils erlaubt oder blockiert werden.

Blacklist (Standard): Alle Apps sind verfügbar; jede App, die nicht auf dem Gerät sein darf, muss im Bereich **Anwendungen** explizit als **Blockiert** markiert werden.

Whitelist: Nur Apps, die im Bereich **Anwendungen** explizit angegeben sind und bei denen der **Installationstyp** auf **Verfügbar** gesetzt ist, dürfen im persönlichen Profil installiert werden.

7. Anwendungen

Liste der Anwendungen, die im persönlichen Profil erlaubt oder blockiert werden müssen. Das Verhalten des Listeninhalts hängt vom Wert des **Play-Store-Modus** ab.

Um eine neue App aus dem Play Store hinzuzufügen, klicken Sie auf das **+**-Symbol.

7.1. Installationstyp

Arten von Installationsverhalten, die eine Anwendung im persönlichen Profil haben kann.

Blockiert: Die App ist blockiert und kann nicht im persönlichen Profil installiert werden.

Verfügbar: Die App steht zur Installation im persönlichen Profil zur Verfügung.

8. Blockierte Kontotypen

Kontotypen, die nicht vom Benutzer verwaltet werden können. Diese Option verhindert, dass Gerätebenutzer nicht genehmigte Konten in ihrem persönlichen Profil hinzufügen.

Profilübergreifende Policies

Gilt nur für Geräte mit persönlichen und Arbeitsprofilen.

Profilübergreifendes Kopieren/Einfügen

Ob Text, der aus einem Profil (privat oder Arbeit) kopiert wurde, in das andere Profil eingefügt werden kann.

Untersagt (Standard): Verhindert, dass Benutzer Text, der aus dem Arbeitsprofil kopiert wurde, in das persönliche Profil einfügen können. Text, der aus dem persönlichen Profil kopiert wurde, kann in das Arbeitsprofil eingefügt werden.

Erlaubt: In einem beliebigen Profil kopierter Text kann in das andere Profil eingefügt werden.

Profilübergreifender Datenaustausch

Ob Daten aus einem Profil (privat oder Arbeit) mit Apps im anderen Profil geteilt werden können. Dies steuert speziell den einfachen Datenaustausch über Intents. Die Verwaltung anderer profilübergreifender Kommunikationskanäle, wie z. B. die Kontaktsuche, Kopieren/Einfügen oder die Verbindung zwischen Arbeits- und Privat-Apps, wird separat konfiguriert.

Untersagt: Verhindert den Datenaustausch sowohl vom persönlichen Profil zum Arbeitsprofil als auch vom Arbeitsprofil zum persönlichen Profil.

Arbeit zu Privat untersagt (Standard): Verhindert, dass Benutzer Daten vom Arbeitsprofil an Apps im persönlichen Profil weitergeben. Private Daten können mit Arbeits-Apps geteilt werden.

Erlaubt: Daten aus jedem der beiden Profile können mit dem anderen Profil geteilt werden.

Standard-Arbeitsprofil-Widgets

Standardverhalten für Arbeitsprofil-Widgets. Wenn eine bestimmte App keine Widget-Richtlinie definiert, wird das hier festgelegte Standardverhalten angewendet.

Profilübergreifende App-Funktionen

Steuert, ob Apps im persönlichen Profil die App-Funktionen von Apps im Arbeitsprofil aufrufen können. Dies erfordert Android 16 oder höher.

Diese Einstellung hängt von der Option **App functions** auf Policy-Ebene (im Abschnitt App-Management) ab. Wenn die Option App-Funktionen auf **Disallowed** gesetzt ist, wird die API die auf **Allowed** gesetzten profilübergreifenden App-Funktionen ablehnen.

Arbeitskontakte im persönlichen Profil

Ob Kontakte, die im Arbeitsprofil gespeichert sind, in den Kontaktsuchen und bei eingehenden Anrufen des persönlichen Profils angezeigt werden können.

Erlaubt (Standard): Ermöglicht es, dass Kontakte aus dem Arbeitsprofil im persönlichen Profil angezeigt werden.

Untersagt: Verhindert, dass Apps im persönlichen Profil auf Kontakte aus dem Arbeitsprofil zugreifen oder diese suchen können.

Untersagt, außer für System-Apps: Verhindert, dass die meisten persönlichen Apps auf Kontakte aus dem Arbeitsprofil zugreifen können; ausgenommen hiervon sind die vom OEM vorinstallierten Standard-Apps für Telefon, Nachrichten und Kontakte (Android 14+).

Wenn die Funktion „Work-Kontakte im persönlichen Profil“ konfiguriert ist, können Sie optional eine Liste von **ausgenommenen Paketnamen** festlegen. Je nach gewähltem Modus fungieren diese Ausnahmen als Allowlist oder Blocklist für persönliche Apps.

Statusberichterstattung

In diesem Abschnitt können Sie konfigurieren, welche Daten vom Gerät abgerufen werden sollen. Die Statusdaten können auf der Dashboard-Seite [Gerätestatus](#) eingesehen werden.

Anwendungsberichte

Ob App-Berichte aktiviert sind. (Informationen, die über eine installierte App gemeldet werden.)

Diese Option ist systembedingt erforderlich (für die Integration von Begleit-Apps) und ist immer aktiviert; sie kann nicht deaktiviert werden.

Entfernte Apps einbeziehen

Ob entfernte Apps in die Anwendungsberichte einbezogen werden.

Geräteeinstellungen

Ob die Berichterstattung über Geräteeinstellungen aktiviert ist. (Informationen über sicherheitsrelevante Geräteeinstellungen auf dem Gerät.)

Software-Info

Ob die Berichterstattung über Software-Infos aktiviert ist. (Informationen über die Software des Geräts.)

Speicherinfo

Ob die Berichterstattung über den Speicher aktiviert ist. (Ein Ereignis im Zusammenhang mit Speicher- und Speicherkapazitätsmessungen.)

Netzwerkinfo

Ob die Berichterstattung über Netzwerk-Infos aktiviert ist. (Netzwerkinfo des Geräts.)

Anzeige-Info

Ob die Berichterstattung über Displays aktiviert ist. Berichtsdaten sind für im Privatbesitz befindliche Geräte mit Arbeitsprofilen nicht verfügbar. (Anzeigeinformationen des Geräts.)

Energieverwaltungsereignisse

Ob die Berichterstattung über Energieverwaltungsereignisse aktiviert ist. Berichtsdaten sind für im Privatbesitz befindliche Geräte mit Arbeitsprofilen nicht verfügbar.

Hardwarestatus

Ob die Berichterstattung über den Hardwarestatus aktiviert ist. Berichtsdaten sind für im Privatbesitz befindliche Geräte mit Arbeitsprofilen nicht verfügbar.

Systemeigenschaften

Ob die Berichterstattung über Systemeigenschaften aktiviert ist.

Common-Criteria-Modus

Ob die Berichterstattung über den Common-Criteria-Modus aktiviert ist.

Verschiedenes

1. Easter-Egg-Spiel deaktiviert

Gibt an, ob das Easter-Egg-Spiel in den Einstellungen deaktiviert ist.

2. Erste Nutzungshinweise überspringen

Kennzeichnung zum Überspringen von Hinweisen bei der ersten Nutzung. Ein Enterprise-Administrator kann die Systemempfehlung aktivieren, dass Apps beim ersten Start ihre Benutzer-Tutorials und andere Einführungshinweise überspringen.

3. Kurze Support-Nachricht

Eine Nachricht, die dem Benutzer im Einstellungsbildschirm angezeigt wird, wenn Funktionen durch den Administrator deaktiviert wurden. Wenn die Nachricht länger als 200 Zeichen ist, kann sie gekürzt werden.

4. Lange Support-Nachricht

Eine Nachricht, die dem Benutzer im Einstellungsbildschirm des Geräteadministrators angezeigt wird.

5. Informationen zum Sperrbildschirm des Besitzers

Die Informationen zum Gerätebesitzer, die auf dem Sperrbildschirm angezeigt werden sollen.

6. Einrichtungsaktionen

Aktionen, die während des Einrichtungsprozesses durchgeführt werden. Während der Registrierung können Sie von dem Benutzer verlangen, eine oder mehrere Apps zu öffnen, die für die

Geräteeinrichtung erforderlich sind.

Verwenden Sie **Einrichtungsaktion hinzufügen**, um Einträge zu erstellen und diese mit der Löschaktion wieder zu entfernen.

6.1. App starten

Paketname der zu startenden App

6.2. Titel

Bietet eine für den Benutzer sichtbare Nachricht, um zu erklären, warum das Starten der App erforderlich ist.

6.3. Beschreibung

Bietet eine für den Benutzer sichtbare Nachricht, um dem Benutzer zu erklären, warum das Starten der App erforderlich ist.

7. Sichtbarkeit des Unternehmens-Anzeigenamens

Steuert, ob der Anzeigename des Unternehmens auf dem Gerät sichtbar ist (zum Beispiel als Nachricht auf dem Sperrbildschirm bei unternehmenseigenen Geräten).

Sichtbar (Standard): Der Anzeigename des Unternehmens ist auf dem Gerät sichtbar (unterstützt für Arbeitsprofile ab Android 7+ und vollständig verwaltete Geräte ab Android 8+).

Ausgeblendet: Der Anzeigename des Unternehmens wird auf dem Gerät ausgeblendet.

Richtlinien- Durchsetzungsregeln

Wenn ein Gerät oder Arbeitsprofil gegen eine der unten aufgeführten Richtlinieneinstellungen verstößt, blockiert die Android Device Policy standardmäßig sofort die Nutzung des Geräts oder Arbeitsprofils:

- **Passwortanforderungen**
- **Verschlüsselungsrichtlinie**
- **Sperrbildschirm deaktiviert**
- **Zulässige Eingabemethoden**
- **Zulässige Bedienungshilfen**

Wenn das Gerät oder Arbeitsprofil nach 10 Tagen weiterhin nicht richtlinienkonform ist, führt die Android Device Policy einen Werksreset des Geräts durch oder löscht das Arbeitsprofil.

In diesem Abschnitt können Sie die standardmäßigen Durchsetzungsregeln für die Richtlinienkonformität überschreiben oder neue hinzufügen.

Regeln

Liste der Regeln, die das Verhalten definieren, wenn eine bestimmte Richtlinie nicht auf ein Gerät angewendet werden kann.

Verwenden Sie **Regel hinzufügen**, um eine neue Regel zu erstellen. Jede Regelkarte kann über die Löschaktion entfernt werden.

Name der Einstellung

Die übergeordnete Richtlinie, die durchgesetzt werden soll. Zum Beispiel **Anwendungen** oder **Passwortanforderungen**.

Erforderlich. Der Wert muss mit einem unterstützten übergeordneten Richtliniennamen übereinstimmen; andernfalls wird das Feld als ungültig markiert.

Blockieren nach Anzahl der Tage

Anzahl der Tage, die die Richtlinie nicht konform ist, bevor das Gerät oder Arbeitsprofil blockiert wird. Um den Zugriff sofort zu blockieren, setzen Sie den Wert auf 0. **Blockieren nach Anzahl der**

Tage muss kleiner sein als **Löschen nach Anzahl der Tage**. Nur anwendbar auf unternehmenseigene Geräte.

Zulässiger Bereich: 0–300.

Blockumfang

Gibt den Umfang der Blockierungsaktion an. Nur anwendbar auf unternehmenseigene Geräte.

Standard (neue Regel): **Arbeitsprofil**.

Arbeitsprofil: Die Blockierungsaktion wird nur auf Apps im Arbeitsprofil angewendet. Apps im persönlichen Profil sind nicht betroffen.

Gesamtes Gerät: Die Blockierungsaktion wird auf das gesamte Gerät angewendet, einschließlich der Apps im persönlichen Profil.

Löschen nach Anzahl der Tage

Anzahl der Tage, die die Richtlinie nicht konform ist, bevor das Gerät oder Arbeitsprofil gelöscht wird.

Löschen nach Anzahl der Tage muss größer sein als **Blockieren nach Anzahl der Tage**. Nur anwendbar auf unternehmenseigene Geräte.

Erforderlich. Standard (neue Regel): **1**.

Zulässiger Bereich: 1–300.

Werkseinstellungs-Schutz beibehalten

Ob die Daten zum Werkseinstellungs-Schutz auf dem Gerät erhalten bleiben. Diese Einstellung gilt nicht für Arbeitsprofile.

Standard (neue Regel): aktiviert.

Richtlinien - Apple

Apple-Richtlinien

Apple-Richtlinien definieren Verwaltungseinstellungen, die Cerberus Enterprise über MDM auf Apple-Geräte anwendet. Diese Einstellungen werden im Dashboard im Apple-Richtlinien-Editor konfiguriert.

Bevor Sie beginnen

Die Geräteverwaltung für Apple erfordert die Konfiguration von Apple Management (APNs). Lesen Sie bei Bedarf die Seite [Apple Management setup \(APNs\)](#).

Apple Policy Editor öffnen

Öffnen Sie im Dashboard **Policies** und klicken Sie auf **Create new Apple policy**. Um eine bestehende Apple Policy zu bearbeiten, klicken Sie auf die entsprechende Zeile in der Policies-Tabelle.

Editor-Layout

Der Apple Policy Editor ist als eine Reihe von erweiterbaren Abschnitten organisiert. Am oberen Seitenrand können Sie jederzeit Folgendes bearbeiten:

- **Name** (erforderlich)
- **Id** (schreibgeschützt)
- **Beschreibung** (optional)

Policy-Abschnitte

Die folgenden Abschnitte entsprechen den derzeit im Apple Policy Editor verfügbaren Panels:

- **App-Management:** Konfiguration von appbezogenen Einschränkungen und verwalteten Apps.

- **Passcode-Einstellungen:** Konfiguration von Passcode-Anforderungen und zugehörigen Regeln.
- **Security:** Steuerung von Funktionen wie Auto Unlock und biometrischem Entsperren.
- **iCloud:** Bestimmte iCloud-Dienste erlauben oder untersagen (Backup, Schlüsselbund-Synchronisierung, Private Relay usw.).
- **Multimedia:** Kamera und zugehörige Funktionen erlauben oder untersagen.
- **Cellular:** Steuerung von Mobilfunk-Einstellungen (App-Mobilfunkdaten, eSIM, Tarifänderungen).
- **Networking:** Steuerung von AirDrop/AirPrint/AirPlay und anderen Konnektivitätseinstellungen.
- **Accounts:** Einschränkung der Kontomodifikation und (optional) Konfiguration von Google- und Mail-Konten.

Viele Optionen im Apple Policy Editor enthalten einen Tooltip, der Anforderungen und unterstützte OS-Versionen dokumentiert.

Speichern, Löschen und zugehörige Geräte

Verwenden Sie **Save policy**, um Ihre Änderungen zu übernehmen. Die Schaltfläche ist deaktiviert, wenn keine ausstehenden Bearbeitungen vorliegen oder die Lizenz abgelaufen ist.

Beim Bearbeiten einer bestehenden Policy wird auf der Seite auch die Aktion **Delete policy** angezeigt. Der Editor kann am Ende eine Liste **Associated devices** anzeigen, damit Sie sehen können, wie viele Geräte die Policy derzeit verwenden.

Nächste Seiten

- **Passcode:** Konfiguration von Passcode-Anforderungen und zugehörigen Sicherheitsoptionen.
- **Restrictions:** Definition erlaubter Funktionen und Einschränkungen auf OS-Ebene.
- **Apps & Profile:** Konfiguration installierter Apps und Konfigurationsprofile.

Apple-Richtlinie: Sperrcode

Der Bereich **Sperrcode-Einstellungen** steuert die Anforderungen an den Gerätesperrcode und zugehörige Sicherheitsregeln (zum Beispiel Mindestlänge und Komplexität).

Optionen

Im Apple-Richtlinien-Editor werden Sperrcode-Optionen mithilfe einer Kombination aus Schaltern und numerischen Feldern konfiguriert. Viele Felder enthalten Tooltips, die unterstützte OS-Versionen und Anforderungen an die Aufsicht (Supervision) angeben.

Sperrcode-Schalter

- **ChangeAtNextAuth:** Erzwingt eine Passwortrücksetzung bei der nächsten Authentifizierung des Benutzers.
- **RequireAlphanumericPasscode:** Erfordert mindestens einen Buchstaben und eine Zahl.
- **RequireComplexPasscode:** Erfordert einen „komplexen“ Sperrcode (keine sich wiederholenden oder aufeinanderfolgenden Muster und mindestens ein nicht-alphanumerisches Zeichen).
- **RequirePasscode:** Erfordert einen Sperrcode ohne zusätzliche Anforderungen an Länge oder Qualität. Hinweis: Das Einstellen anderer Sperrcode-Optionen setzt implizit einen Sperrcode voraus.

Numerische Felder

- **FailedAttemptsResetInMinutes:** Minuten, bevor der Zähler für fehlgeschlagene Versuche zurückgesetzt wird (erfordert MaximumFailedAttempts).
- **MaximumFailedAttempts:** erlaubte fehlgeschlagene Versuche, bevor das Gerät gelöscht/gesperrt wird (Bereich: 2–11).
- **MaximumGracePeriodInMinutes:** wie lange das Gerät ohne Eingabe des Sperrcodes entsperrt bleiben kann (0 = keine).
- **MaximumInactivityInMinutes:** Inaktivitätszeit, bevor das Gerät gesperrt wird (Bereich: 0–15).
- **MaximumPasscodeAgeInDays:** maximales Alter des Sperrcodes vor einer erzwungenen Änderung (Bereich: 0–730).
- **MinimumComplexCharacters:** Mindestanzahl an „komplexen“ Zeichen (Bereich: 0–4).

- **MinimumLength:** Mindestlänge des Sperrcodes (Bereich: 0–16).
- **PasscodeReuseLimit:** Länge des Sperrcode-Verlaufs, um die Wiederverwendung alter Sperrcodes zu verhindern (Bereich: 1–50).

Apple-Richtlinie: Einschränkungen

Die Abschnitte „Einschränkungen“ steuern, welche Betriebssystem-Funktionen auf verwalteten Apple-Geräten erlaubt sind. Im Apple-Richtlinien-Editor werden diese Optionen als gruppierte Panels mit mehreren Schaltern angezeigt.

Viele Einschränkungen werden nur auf bestimmten OS-Versionen unterstützt und können eine Aufsicht (Supervision) der Geräte erfordern. Verwenden Sie die Tooltips im Dashboard für verbindliche Anforderungen.

Sicherheit

- **Automatisches Entsperren erlauben**
- **Fingerabdruck zum Entsperren erlauben**
- **Ändern von Fingerabdruck/Touch ID erlauben**

iCloud

- **iCloud-Adressbuch erlauben**
- **iCloud-Backup erlauben**
- **iCloud-Lesezeichen erlauben**
- **iCloud-Kalender erlauben**
- **iCloud Schreibtisch und Dokumente erlauben**
- **iCloud-Dokumentensynchronisierung erlauben**
- **iCloud Freeform erlauben**
- **iCloud-Schlüsselbund-Synchronisierung erlauben**
- **iCloud Mail erlauben**
- **iCloud-Notizen erlauben**
- **iCloud-Fotobibliothek erlauben**
- **iCloud Private Relay erlauben**
- **iCloud-Erinnerungen erlauben**

Multimedia

- **Kamera erlauben**
- **Ändern der Freigabeoptionen erlauben**
- **Zugriff auf USB-Laufwerke über die Dateien-App erlauben**

Mobilfunk

- **Ändern der mobilen Daten pro App erlauben**
- **Ändern des Mobilfunktarifs erlauben**
- **Ändern der eSIM-Einstellungen erlauben**
- **Ausgehende eSIM-Transfers erlauben**

Netzwerk

- **AirDrop erlauben**
- **Eingehende AirPlay-Anfragen erlauben**
- **AirPrint erlauben**
- **Speichern von AirPrint-Anmeldedaten erlauben**
- **AirPrint iBeacon-Entdeckung erlauben**
- **Ändern der Bluetooth-Einstellungen erlauben**
- **Ändern der Bluetooth-Freigabe erlauben**
- **Zugriff auf Netzlaufwerke über die Dateien-App erlauben**
- **Ändern der Internetfreigabe erlauben**

Konten (Einschränkung)

Das Panel „Konten“ enthält sowohl eine Einschränkung als auch (optional) die Kontokonfiguration. Der Schalter für die Einschränkung steuert, ob der Benutzer Systemkonten ändern kann.

- **Ändern von Konten erlauben**

Apple-Richtlinie: Apps & Profile

Dieser Abschnitt dokumentiert, wie verwaltete Anwendungen und Account-Payloads für Apple-Geräte konfiguriert werden.

App-Verwaltung

Das **App-Verwaltung**-Panel enthält sowohl allgemeine appbezogene Einschränkungen als auch eine Liste der verwalteten Apps.

Allgemeine App-Einschränkungen

- **App Clips erlauben**
- **App-Installation erlauben**
- **App-Entfernung erlauben**
- **Automatische App-Downloads erlauben**
- **Ausblenden von Apps erlauben**
- **Sperren von Apps erlauben**
- **In-App-Käufe erlauben**

Verwaltete Apps

Verwenden Sie **Anwendung hinzufügen**, um eine App zur Richtlinie hinzuzufügen. Jede verwaltete App wird als Karte angezeigt. Sie können die Karte erweitern, um ihre Einstellungen zu bearbeiten, oder die App über die Löschaktion entfernen.

- **App Store ID:** die App Store-Kennung der verwalteten App.
- **Bundle ID:** die App-Bundle-Kennung.
- **Installationsverhalten:** steuert, ob die App installiert bleiben muss oder vom Benutzer installiert/entfernt werden kann.
- **Zuweisung:** Typ der Lizenzzuweisung.
- **VPP-Lizenz:** VPP-Lizenztyp, der für die Installation über den App Store verwendet wird.

Konten

Das **Konten**-Panel ermöglicht es Ihnen, Konten zu konfigurieren, die auf verwaltete Geräte angewendet werden. Es enthält außerdem einen Schalter für Einschränkungen zur Kontomodifikation.

Einschränkung

- **Kontomodifikation erlauben:** Wenn deaktiviert, können Benutzer Konten wie Apple-Konten und Internetkonten nicht ändern.

Konten hinzufügen

Verwenden Sie **Google-Konto hinzufügen** oder **Mail-Konto hinzufügen**, um Konten-Payloads zur Richtlinie hinzuzufügen. Jedes Konto wird als Karte mit seinen Konfigurationsfeldern angezeigt.

Kontodaten von Benutzern

Sowohl Google- als auch Mail-Kontokarten bieten einen Schalter für **Kontodaten von Benutzern**. Wenn dieser aktiviert ist, wendet das System die Kontodaten auf Benutzerbasis an. Wenn er deaktiviert ist, geben Sie die Kontenidentität in der Richtlinie ein.

Google-Kontofelder

- **Sichtbarer Name:** der dem Benutzer für das Konto angezeigte Name.
- **Google-E-Mail-Adresse:** die E-Mail-Adresse des Benutzers.
- **Vollständiger Name:** der vollständige Name des Benutzers.

Mail-Kontofelder

Mail-Konten enthalten Identitätsfelder sowie die Konfiguration für ein- und ausgehende Server. Hostnamen sind erforderlich.

- **Sichtbarer Name:** der dem Benutzer für das Mail-Konto angezeigte Name.
- **E-Mail-Adresse:** die E-Mail-Adresse des Benutzers.
- **Vollständiger Name:** der vollständige Name des Benutzers.

Posteingangsserver

- **Servertyp:** Mail-Protokoll (zum Beispiel IMAP oder POP).
- **Authentifizierungsmethode:** Authentifizierungsmethode für den Server.
- **IMAP-Pfadpräfix:** wird nur angezeigt, wenn der Servertyp IMAP ist.
- **Hostname:** erforderlich.
- **Port:** Server-Port (1-65535).

Ausgangsserver

- **Authentifizierungsmethode**
- **Hostname:** erforderlich.
- **Port:** Server-Port (1-65535).

S/MIME-Optionen

Für Mail-Konten können Sie auch das S/MIME-Verschlüsselungs- und Signaturverhalten konfigurieren.

Verschlüsselung

- **S/MIME-Verschlüsselung**
- **Identität durch Benutzer überschreibbar**
- **Schalter für Nachrichten-Verschlüsselung aktiviert**
- **Durch Benutzer überschreibbar**

Signierung

- **S/MIME-Signierung**
- **Identität durch Benutzer überschreibbar**
- **Durch Benutzer überschreibbar**

Die Optionen für Konten und Einschränkungen enthalten Tooltips im Dashboard, die Voraussetzungen und unterstützte OS-Versionen dokumentieren.

Gerätestatus

Geräteübersicht

Öffnen Sie ein Gerät über **Dashboard** → **Geräte**, indem Sie auf die Gerätezeile klicken. Der Seitentitel zeigt das Geräte-**Modell** (sofern verfügbar) und die interne **ID** an.

Historische Daten vs. aktuelle Registrierung

Wenn ein Gerät über mehrere Registrierungen verfügt, kann Cerberus Enterprise einen schreibgeschützten historischen Datensatz anzeigen. In diesem Fall zeigt die Seite ein **Historische Daten**-Banner und eine Schaltfläche zur Rückkehr zu den aktuellen Registrierungsdaten an.

Obere Felder

Der obere Bereich fasst die Geräteidentität, die Zuweisung und den Verwaltungsstatus zusammen. Einige Felder sind plattformspezifisch und erscheinen nur bei Android- oder Apple-Geräten.

- **ID** und **Modell**: schreibgeschützte Identifikatoren.
- **Benutzer**: zeigt den aktuell zugewiesenen Benutzer an (falls vorhanden). Über das Benutzermenü können Sie den **Benutzer öffnen** oder den **Benutzer ändern**, oder einen Benutzer zuweisen, wenn noch keiner festgelegt ist.
- **Verwaltungsmodus** und **Eigentum**: werden in der Benutzeroberfläche mit Tooltips angezeigt.
- **Status**: aktueller Gerätestatus (mit Symbol und Tooltip-Details).
- **ADE-Profil** (nur Apple): zeigt das zugewiesene Automated Device Enrollment-Profil an (falls vorhanden) und ermöglicht es Ihnen, dieses zu öffnen oder zu ändern.
- **Policy**: zeigt die zugewiesene Policy an und ermöglicht es Ihnen, diese zu öffnen oder zu ändern, oder eine zuzuweisen, wenn noch keine festgelegt ist.
- **Status der Policy-Konformität** (wenn eine Policy zugewiesen ist): gibt an, ob das Gerät konform ist.
- **Policy-Version** (wenn eine Policy zugewiesen ist): gibt an, ob auf dem Gerät die neueste Policy-Version angewendet wurde.
- **Registriert am** und **Letzter Statusbericht**: Zeitstempel für die Registrierung und den letzten gemeldeten Status.
- **Abgemeldet am**: wird angezeigt, wenn das Gerät abgemeldet wurde.

Einige Daten und Panels sind nur verfügbar, wenn die entsprechende Kategorie in der Geräte-Policy aktiviert ist. Weitere Informationen finden Sie auf den Seiten [Statusmeldung](#) und [Standort und Geofence](#).

Panels

Der Geräte-Editor ist in erweiterbare Abschnitte unterteilt. Je nach Plattform und Status sehen Sie möglicherweise einen oder mehrere der folgenden Panels:

- **Standortkarte:** ein Tab-Panel mit **Standort**verlauf für das aktuelle Gerät und bei Android-Geräten einem **Geofence**-Tab für Geofence-Übergänge, sofern Geofence-Daten verfügbar sind.
- **SIM-Verwaltung** (nur Android): Geräte-EID, installierte SIMs und eSIMs sowie der Verlauf der eSIM-Befehle. Weitere Informationen finden Sie auf der speziellen Seite [SIM-Verwaltung](#).
- **Befehle:** Befehle an das Gerät senden und die Befehlshistorie anzeigen (plattformspezifisch).
- **Sicherheitsstatus** (nur Android): Status, Play Integrity-Urteil und Sicherheitsrisiken.
- **App-Berichte** (nur Android): installierte Apps und Feedback-/Fehlerberichte.
- **Verwaltete Anwendungen** (nur Apple): Status verwalteter Apps und Installationsdetails.
- **Details zur Nichtkonformität:** wird angezeigt, wenn ein Gerät nicht konform ist; listet die Policy-Einstellungen auf, die nicht der Konformität entsprechen.
- **Statusberichte:** zusätzliche vom Gerät gemeldete Daten, die als Baumstruktur aus Kategorien und Werten angezeigt werden.
- **Registrierungshistorie:** frühere Registrierungen für dasselbe physische Gerät, angezeigt als Liste.

Standort-Panel-Tabs

Das **Standortkarte**-Panel verwendet nun Tabs, damit der Standortverlauf und die Geofence-Übergänge getrennt bleiben.

- **Standort:** zeigt Verlaufsfiler, eine Suche nach Datumsbereichen, Standort-Marker, den Genauigkeitskreis und Live-Tracking-Steuerungen für das aktuelle Gerät an.
- **Geofence** (nur Android): zeigt die Geofence-Übergangshistorie auf einer speziellen Karte mit Zeitraumfiltern, einem optionalen Schalter für archivierte Geofences und einer Seitenliste der Übergänge an.

Informationen zum vollständigen Verhalten dieser Tabs finden Sie unter [Standortkarte](#).

Aktionen

Am Ende der Seite können Sie Daten aktualisieren und je nach Plattform, Gerätestatus und Lizenzstatus Aktionen durchführen.

- **Daten aktualisieren:** den Datensatz des Geräts neu laden.
- **Gerät deaktivieren / Gerät aktivieren** (nur Android): in unterstützten Zuständen verfügbar.
- **Gerät abmelden:** entfernt die Verwaltung vom Gerät. Das genaue Verhalten hängt von der Plattform und dem Eigentum ab (beispielsweise kann Android ein Arbeitsprofil löschen oder einen Werksreset durchführen).
- **Gerät löschen:** verfügbar, wenn das Gerät bereits abgemeldet wurde und sein Datensatz entfernt werden kann.

SIM-Verwaltung

Bei Android-Geräten bietet der Geräte-Editor ein **SIM-Verwaltung**-Panel, um die auf dem Gerät installierten SIMs und eSIM-Profile zu verwalten, eSIM-Profile hinzuzufügen oder zu entfernen und den Verlauf der an das Gerät gesendeten eSIM-Befehle anzuzeigen. Dieses Panel ist nur für Android-Geräte verfügbar.

SIM-Informationen werden von vollständig verwalteten Geräten gemeldet, wenn die Meldung von **Netzwerk-Infos** in der Geräte-Richtlinie aktiviert ist (diese Option ist in Cerberus Enterprise immer aktiviert). Weitere Informationen finden Sie auf der Seite [Statusmeldung](#).

Geräte-EID

Die EID (eUICC-Identifikator) identifiziert die eSIM-Hardware des Geräts. Mobilfunkanbieter nutzen sie, um eSIM-Profile an das Gerät zu binden; daher ist das Abrufen der EID in der Regel der erste Schritt eines eSIM-Bereitstellungsprozesses.

- **Unternehmenseigene Geräte** (Android 13 und höher): Die EID wird automatisch zusammen mit dem Gerätestatus gemeldet, eine Benutzerinteraktion ist nicht erforderlich.
- **Privat genutzte Geräte** (Android 13 und höher): Verwenden Sie die Schaltfläche **EID anfordern**. Der Benutzer erhält auf dem Gerät eine Benachrichtigung mit der Bitte, die EID zu teilen, und kann die Anfrage entweder genehmigen oder ablehnen. Die EID wird nur angezeigt, wenn der Benutzer zustimmt. Solange die Anfrage aussteht, bleibt die Schaltfläche deaktiviert.

Beim Senden einer EID-Anfrage wird zuerst ein Bestätigungsdialog angezeigt, da der Benutzer eine Benachrichtigung auf dem Gerät erhält.

Installierte SIMs

Die Tabelle **Installierte SIMs** listet die aktuell für das Gerät bekannten SIMs auf, einschließlich physischer SIMs und eSIM-Profile. Auf privat genutzten Geräten werden eSIM-Profile, die mit dem Befehl **eSIM hinzufügen** installiert wurden, auch dann angezeigt, wenn das Gerät keine SIM-

Informationen meldet.

- **Anbieter:** der mit der SIM verknüpfte Mobilfunkanbieter (sofern gemeldet).
- **Telefonnummer:** die mit der SIM verknüpfte Telefonnummer (sofern gemeldet).
- **ICCID:** die Integrated Circuit Card Identifier der SIM.
- **Aktivierungsstatus:** ob die eSIM aktiviert ist oder nicht. Wird nur für eSIMs auf Android 15 und höher gemeldet.
- **Konfigurationsmodus:** ob die eSIM durch einen Administrator oder durch den Benutzer konfiguriert wurde. Wird nur für eSIMs auf Android 15 und höher gemeldet.
- **SIM-Typ:** zeigt an, ob das Gerät den Eintrag als eSIM meldet.

eSIMs mit einem laufenden oder bereits ausgeführten (nicht fehlgeschlagenen) Entfernungskommando zeigen einen vorübergehenden Aktivierungsstatus **Wird entfernt** an. Der Eintrag verschwindet aus der Liste, sobald das Gerät die aktualisierte SIM-Liste meldet. Solange eine Entfernung läuft, ist die Schaltfläche zum Entfernen nicht verfügbar, um zu verhindern, dass derselbe Befehl doppelt gesendet wird.

eSIM entfernen

Verwenden Sie die Schaltfläche zum Entfernen neben einer installierten eSIM, um deren Profil vom Gerät zu löschen. Ein Bestätigungsdialog fordert Sie auf, die ICCID der zu entfernenden eSIM zu bestätigen, bevor der Befehl gesendet wird. Das Entfernen einer eSIM wird ab Android 15 unterstützt.

eSIM hinzufügen

Der Bereich **eSIM hinzufügen** installiert ein neues eSIM-Profil auf dem Gerät (unterstützt ab Android 15). Dies erfordert:

- **Gültigkeit:** wie lange der Befehl gültig ist, wenn er nicht sofort ausgeführt werden kann.
- **Aktivierungscode:** der vom Mobilfunkanbieter bereitgestellte Aktivierungscode für das eSIM-Profil. Sie können den vollständigen Code oder nur die SM-DP+-Adresse eingeben, damit das Gerät ein Profil findet, das der Anbieter bereits mit seiner EID verknüpft hat.
- **Aktivierungsstatus:** ob das eSIM-Profil nach dem Download automatisch aktiviert werden soll oder deaktiviert bleiben soll, damit der Benutzer es manuell aktivieren kann.

Befehlshistorie

Unterhalb des Bereichs „eSIM hinzufügen“ zeigt das Panel den Verlauf der an das Gerät gesendeten eSIM-Befehle: **eSIM hinzufügen**, **eSIM entfernen** und **EID anfordern**. Die Tabelle ist sortierbar und unterstützt die Paginierung. Einige Zeilen können erweitert werden, um die Befehlsparameter (z. B. den Aktivierungscode oder die ICCID) und den Ausführungsstatus anzuzeigen, einschließlich der eSIM-Fehlerdetails, falls ein Vorgang auf dem Gerät fehlschlägt.

- **Erstellungsdatum**
- **Befehl**
- **Gültigkeit**
- **Status**
- **Fehler:** zeigt den eSIM-Fehlerstatus an (zum Beispiel *Benutzer hat abgelehnt*, *Ungültiger Aktivierungscode* oder *ICCID nicht gefunden*), wenn die Befehlsausführung dies meldet.
- **Ausführungsdatum**

eSIMs löschen bei Löschen und Abmelden

Wenn Sie das Gerät über das Befehlsfeld löschen, steuert die Option **eSIMs löschen**, ob eSIM-Profile zusammen mit dem Löschvorgang entfernt werden. Bei privat genutzten Geräten mit einem Arbeitsprofil ist diese Option standardmäßig aktiviert (verwaltete eSIMs werden gelöscht, privat genutzte eSIMs sind nicht betroffen). Dieselbe Option steht auch im Bestätigungsdialog **Gerät abmelden** zur Verfügung.

Befehle

Der Geräte-Editor bietet ein **Befehle**-Panel, um Remote-Befehle an ein verwaltetes Gerät zu senden. Die verfügbaren Befehle hängen von der Plattform (Android oder Apple) und dem Gerätestatus ab.

Wenn das Gerät derzeit nicht online ist, wird der Befehl zugestellt und ausgeführt, sobald sich das Gerät mit dem Internet verbindet. Für Android-Befehle können Sie den Parameter **Gültigkeit** festlegen, um zu bestimmen, wie lange ein nicht zugestellter Befehl gültig bleibt.

Android (AMAPI)-Befehle

Für Android-Geräte enthält das Befehlsfeld ein Feld **Gültigkeit** (Wert + Einheit) und einen **Befehl**-Auswähler. Einige Befehle erfordern zusätzliche Parameter, die dynamisch erscheinen, wenn Sie den Befehl auswählen.

Gemeinsame Parameter

- **Gültigkeit:** wie lange der Befehl gültig ist, wenn er nicht sofort ausgeführt werden kann.
- **Befehl:** wählen Sie die Aktion aus, die an das Gerät gesendet werden soll.

Befehle mit zusätzlichen Feldern

- **Passwort zurücksetzen:** erfordert **Neues Passwort** und **Neues Passwort bestätigen**. Zu den optionalen Schaltern gehören **Jetzt sperren**, **Eingabe erforderlich** sowie **Bei Neustart nicht nach Anmeldedaten fragen**.
- **App-Daten löschen:** erfordert den Ziel-**Paketnamen**.
- **Verlustmodus starten:** erfordert eine **Verlustmeldung** und unterstützt optionale Kontaktfelder (Straße, Organisation, Telefonnummer, E-Mail).
- **Löschen:** unterstützt eine **Nachricht zum Löschgrund** (wird Benutzern auf Privatgeräten angezeigt) sowie optionale Lösch-Flags, einschließlich **eSIMs löschen**.

Die eSIM-Befehle (**eSIM hinzufügen**, **eSIM entfernen**, **EID anfordern**) sind im speziellen Bereich **SIM-Verwaltung** verfügbar.

Befehlshistorie

Unterhalb der Steuerelemente zum Senden zeigt das Dashboard eine Befehlshistorie-Tabelle an. Die Tabelle ist sortierbar und unterstützt Paginierung. Einige Zeilen können erweitert werden, um zusätzliche Parameter oder Ausführungsdetails anzuzeigen.

Android-Historien-Spalten

- **Erstellungsdatum**
- **Befehl**
- **Gültigkeit**
- **Status**
- **Fehler**
- **Ausführungsdatum**

Apple (MDM)-Befehle

Für Apple-Geräte bietet das Befehls-Panel einen **Befehlsauswahl**. Einige Befehle erfordern zusätzliche Eingaben. Wie bei Android wird unten eine Befehlshistorie-Tabelle angezeigt.

Befehle mit zusätzlichen Feldern

- **InstallApplication**: erfordert die Anwendungs-**Bundle ID**.
- **SendNotification**: erfordert eine **Benachrichtigungsnachricht** (maximale Länge 200 Zeichen).

Apple-Historien-Spalten

- **Erstellungsdatum**
- **Befehl**
- **Status**
- **Statuszeitpunkt**

Aktualisieren

Verwenden Sie die Aktion „Aktualisieren“ im Befehls-Panel, um die Befehlshistorie neu zu laden.

Standortkarte

Diese Seite dokumentiert die gerätespezifischen Standort-Tools, die in der [Geräteübersicht](#) verfügbar sind. Das Panel enthält einen **Standort**-Tab für den Positionsverlauf und bei Android-Geräten einen **Geofence**-Tab für Geofence-Übergänge.

Voraussetzungen

Geräte-Standortdaten werden nur angezeigt, wenn die Standortmeldung in der Geräte-Policy aktiviert ist. Um dies zu aktivieren, öffnen Sie die Policy und schalten Sie **Standort und Geofence** → **Standort melden** ein. Weitere Details finden Sie unter [Standort und Geofence](#).

Bei Geräten, die nicht vollständig verwaltet werden, können die Standortdaten weiterhin davon abhängen, dass die Cerberus Enterprise App über die erforderlichen Standortberechtigungen verfügt und die Standortdienste auf dem Gerät aktiviert sind.

Informationen zur globalen Multi-Device-Karte, die im Dashboard verfügbar ist, finden Sie unter [Dashboard Standortkarte](#).

Ladevorgang und kein Datensatz vorhanden

- Während die Standortdaten geladen werden, zeigt das Panel ein Lade-Overlay auf der Karte an.
- Wenn für das Gerät keine Standortdaten verfügbar sind, zeigt das Panel die Meldung **Keine Standortdaten verfügbar** zusammen mit einem Hinweis zur Aktivierung der Standortmeldung in der zugewiesenen Policy an.
- Wenn ein Datumsfilter aktiv ist und keine Proben übereinstimmen, zeigt das Panel **Keine Daten im ausgewählten Datumsbereich verfügbar** an.

Standort-Tab

Öffnen Sie den **Standort**-Tab, um den Verlauf für ein einzelnes Gerät zu prüfen. Zu den verfügbaren Filtern gehören der letzte bekannte Standort, kürzliche Verlaufszeiträume, ein benutzerdefinierter Datumsbereich und Live-Tracking.

- **Letzter**: zeigt den zuletzt bekannten Standort an.
- **Heute, Letzte 7 Tage** und **Letzte 30 Tage**: zeigen aufgezeichnete Standorte für den ausgewählten Zeitraum an.
- **Suche**: ermöglicht die Auswahl eines benutzerdefinierten Datumsbereichs.
- **Live**: startet oder stoppt das Live-Tracking für das aktuelle Gerät.

Markendetails

Wenn Sie auf einen Standort-Marker klicken, öffnet sich ein Informationsfenster mit:

- Der Zeitstempel des Standortdatensatzes.
- Die gemeldete **Genauigkeit** (in Metern).
- Die gemeldete **Geschwindigkeit**, sofern das Gerät diese bereitstellt.
- Der gemeldete **Kurs** oder die Peilung, sofern das Gerät diese bereitstellt.

Genauigkeitskreis

Wenn das Informationsfenster geöffnet ist, wird ein Genauigkeitskreis um den Marker angezeigt. Der Radius des Kreises entspricht der gemeldeten Genauigkeit (in Metern). Durch Schließen des Informationsfensters wird der Kreis ausgeblendet.

Live-Tracking

In der Geräteverlaufsansicht startet die Auswahl des **Live**-Filters eine Echtzeit-Tracking-Anfrage für dieses spezifische Gerät. Cerberus Enterprise bittet vor dem Starten der Anfrage um Bestätigung.

- Live-Tracking läuft bis zu **15 Minuten**.
- Das Gerät zeigt eine Benachrichtigung an, während das Live-Tracking aktiv ist.
- Während das Live-Tracking aktiv ist, aktualisiert sich das Panel kontinuierlich mit dem neuesten Standort und die Live-Anzeige bleibt sichtbar.

- Durch erneutes Auswählen des Live-Filters können Sie das Live-Tracking vor Ablauf des Timeouts beenden.

Geofence-Tab

Bei Android-Geräten zeigt der zweite Tab Geofence-Übergänge an, die aus den in der zugewiesenen Policy definierten Geofences generiert wurden. Dieser Tab ist verfügbar, wenn Geofence-Daten für das Gerät vorhanden sind.

- Die Karte zeigt die aktuellen Geofence-Bereiche zusammen mit den aufgezeichneten Übergangspunkten an.
- Die Übergangsliste auf der rechten Seite ermöglicht es Ihnen, **Eintritts-** und **Austritts** ereignisse einzusehen.
- Die verfügbaren Filter sind **Heute**, **Letzte 7 Tage**, **Letzte 30 Tage** sowie eine benutzerdefinierte Suche nach einem Datumsbereich.
- **Archivierte einbeziehen** zeigt auch Übergänge an, die mit alten Geofence-Definitionen zusammenhängen, welche in der aktuellen Policy nicht mehr vorhanden sind.

Geofence-Übergangsdetails

Durch Auswahl eines Übergangs werden dessen Details auf der Karte geöffnet und der entsprechende Listeneintrag hervorgehoben. Wenn verfügbar, zeigt Cerberus Enterprise für diesen Übergang auch die Gerätekoordinaten und die gemeldete Genauigkeit an.

Dashboard-Standortkarte

Die Dashboard-Standortkarte bietet eine globale Übersicht über die zuletzt bekannte Position von Geräten, die Standortdaten melden. Öffnen Sie sie im **Dashboard**, um mehrere Geräte auf derselben Google Maps anzuzeigen.

Voraussetzungen

Ein Gerät wird nur dann auf dieser Karte angezeigt, wenn die Standortmeldung in der zugewiesenen Richtlinie aktiviert ist. Um dies zu aktivieren, öffnen Sie die Richtlinie und schalten Sie **Standort und Geofencing** → **Standort melden** ein. Weitere Details finden Sie unter

[Standort und Geofencing](#).

Bei Geräten, die nicht vollständig verwaltet werden, können die Standortdaten weiterhin davon abhängen, dass die Cerberus Enterprise App über die erforderlichen Standortberechtigungen verfügt und die Standortdienste auf dem Gerät aktiviert sind.

Informationen zum gerätespezifischen Verlauf und zu Geofencing-Übergängen, die im Geräte-Editor verfügbar sind, finden Sie unter [Standortkarte](#).

Ladevorgang und kein Datenzustand

- Während die Standortdaten geladen werden, zeigt die Karte eine Ladeanimation an.
- Wenn derzeit keine Geräte über verfügbare Standortdaten verfügen, zeigt die Seite die Meldung **Keine Standortdaten verfügbar** an.

Marker und Cluster

Jedes Gerät mit verfügbaren Standortdaten wird als Marker angezeigt. Wenn viele Geräte nah beieinander liegen, werden die Marker automatisch zu Clustern zusammengefasst, um die

Lesbarkeit der Karte zu gewährleisten.

Geräte, die sich derzeit im Live-Tracking befinden, werden mit einem animierten Marker hervorgehoben, damit sie auf der Karte leichter zu finden sind.

Kartensteuerung

Wenn die Karte Gerätepositionen enthält, zeigt Cerberus Enterprise Aktionsschaltflächen in der oberen rechten Ecke der Karte an.

- **Aktueller Standort:** verwendet Ihren Browser-Standort, um die Karte an Ihre aktuelle Position zu bewegen und den gemeldeten Genauigkeitsbereich anzupassen.
- **Karte zentrieren:** passt die Karte wieder an die aktuell angezeigten Geräte-Marker an.
- **Tracked** Live-Tracking-Statusanzeige: erscheint, wenn ein oder mehrere Geräte im Live-Tracking sind, und zeigt an, wie viele aktuell aktiv sind.
- **Alle Live-Trackings stoppen:** Die Symbolschaltfläche innerhalb der Live-Tracking-Statusanzeige stoppt nach einer Bestätigung das Live-Tracking für alle aktuell verfolgten Geräte.

Marker-Details

Durch Klicken auf einen Marker wird ein Informationsfenster mit Folgendem geöffnet:

- Das Geräte**Modell** und die interne **ID**.
- Zeitstempel des zuletzt gemeldeten Standorts.
- Die gemeldete **Genauigkeit** in Metern.
- Die gemeldete **Geschwindigkeit**, sofern verfügbar.
- Der gemeldete **Kurs** oder die Peilung, sofern verfügbar.

Die Geräte-ID im Informationsfenster ist ein Link, der die entsprechende [Geräteübersicht](#) öffnet.

Aktionen im Informationsfenster

Jedes Informationsfenster enthält außerdem Aktionsschaltflächen für das ausgewählte Gerät.

- **Geräte-Link:** Der Gerätenamen und die ID am oberen Rand des Informationsfensters öffnen die entsprechende Geräteübersichtsseite.
- **Hineinzoomen:** zentriert die Karte auf das ausgewählte Gerät und passt den gemeldeten Genauigkeitskreis enger um dieses an.

- **Live:** startet das Live-Tracking für dieses Gerät. Wenn das Live-Tracking bereits aktiv ist, stoppt dieselbe Schaltfläche es nach einer Bestätigung.
- **Live-Tracking aktiv:** Wenn vorhanden, zeigt diese Statuszeile an, dass das ausgewählte Gerät bereits in Echtzeit verfolgt wird.

Genauigkeitskreis

Wenn ein Marker ausgewählt wird, zeigt die Karte einen Genauigkeitskreis um den Standort an. Der Radius des Kreises entspricht der gemeldeten Genauigkeit.

Live-Tracking-Verhalten

Das Starten des Live-Trackings aus einem Informationsfenster heraus sendet eine Echtzeit-Tracking-Anfrage an das jeweilige Gerät. Cerberus Enterprise aktualisiert die Karte dann automatisch, solange die Sitzung aktiv ist.

- Jede Live-Tracking-Sitzung läuft bis zu **15 Minuten**.
- Das Gerät zeigt eine Benachrichtigung an, solange das Live-Tracking aktiv ist.
- Das Live-Tracking kann entweder über das Informationsfenster des ausgewählten Geräts oder über die globale Schaltfläche **Alle Live-Trackings stoppen** auf der Karte gestoppt werden.

Private Apps

In diesem Bereich des Dashboards können Sie Ihre eigenen privaten Android-Apps hochladen oder Web-Apps erstellen, um diese auf Ihren Geräten zu verteilen.

Die einzigen Details, die Sie angeben müssen, sind der Titel und die APK einer App. Private Apps werden automatisch für Ihre Organisation genehmigt und sind in der Regel innerhalb von 10 Minuten bereit zur Verteilung. Sie können insgesamt bis zu 15 private Apps pro Tag hochladen. Beachten Sie, dass Web-Apps ebenfalls auf dieses Limit angerechnet werden.

Wenn Sie zum ersten Mal eine private App veröffentlichen, müssen Sie eine E-Mail-Adresse angeben, um Benachrichtigungen der Play Console über Ihre Apps und Ihr Google Play Entwicklerkonto zu erhalten. Zudem erstellt Managed Play automatisch ein Play-Entwicklerkonto im Namen Ihrer Organisation. Für dieses Konto müssen Sie keine Registrierungsgebühr bezahlen.

Über den iFrame veröffentlichte private Apps:

- Sie unterliegen nicht denselben Prüfungen wie andere Apps. Infolgedessen können sie nicht in öffentliche Apps umgewandelt werden.
- Sie sind nicht übertragbar. Sie können das Eigentum an einer App nicht auf ein anderes Play-Entwicklerkonto übertragen.

Weitere Einzelheiten finden Sie in der [Managed Google Play Hilfe](#)

Zertifikatsverwaltung

Das Dashboard enthält einen Bereich **Zertifikate** zum Importieren, Anzeigen und Löschen von Zertifikaten. Durch Klicken auf eine Zertifikatszeile wird der Zertifikats-Editor geöffnet.

Zertifikatsliste

Zertifikate werden in einer sortierbaren, paginierten Tabelle angezeigt. Die Liste umfasst sowohl Client-Zertifikate als auch Zertifizierungsstellen (CA).

Filter

Am oberen Seitenrand können Sie Filter über die Chip-Liste aktivieren. Einige Filter schließen sich gegenseitig aus.

- **Alle:** zeigt alle Zertifikate an.
- **Client:** zeigt nur Client-Zertifikate an.
- **Zertifizierungsstelle (CA):** zeigt nur CA-Zertifikate an.
- **Suche:** zeigt ein Textfeld (Label **Name oder Dateiname**) an, um nach dem Zertifikatsnamen oder dem importierten Dateinamen zu suchen.
- **Ohne Benutzer:** zeigt Client-Zertifikate an, die keinem Benutzer zugeordnet sind.

Tabellenspalten

- **Name**
- **Typ**
- **Ablaufdatum**
- **Benutzer** (wird für Client-Zertifikate angezeigt)
- **Importierter Dateiname**
- **Importdatum**

Aktionen

- **Zertifikat öffnen:** Klicken Sie auf eine Zeile, um den Zertifikats-Editor zu öffnen.
- **Zertifikat löschen:** nur verfügbar, wenn das Zertifikat nicht mit Benutzern/Richtlinien verknüpft ist und nicht von Geräten verwendet wird. Die Aktion kann auch deaktiviert

sein, wenn die Lizenz abgelaufen ist.

- **Mehrzeilenauswahl:** Sie können die Mehrzeilenauswahl aktivieren, um mehrere Zertifikate gleichzeitig zu löschen. Es können nur löschbare Zertifikate ausgewählt werden.
- **Aktualisieren:** die Zertifikatsliste neu laden.

Zertifikate importieren

Um Zertifikate zu importieren, klicken Sie auf **Zertifikat importieren** und wählen Sie eine oder mehrere Dateien aus. Unterstützte Formate werden im Tooltip der Import-Schaltfläche angezeigt.

Clients

Unterstütztes Format: Base64-kodiertes PKCS#12 (.p12 / .pfx).

Client-Zertifikate identifizieren einen Benutzer oder ein Gerät im Unternehmensnetzwerk. Client-Zertifikate können mit einem bestimmten Benutzer verknüpft werden.

Jedes Client-Zertifikat kann optional einem bestimmten Benutzer zugewiesen werden: Dies ermöglicht die Bereitstellung derselben Wi-Fi-EAP-Konfiguration auf vielen Geräten. Sie können dies im Abschnitt [Netzwerkkonfiguration](#) der Richtlinie über die Option **EAP-Anmeldedaten von Benutzern** tun.

Alternativ können Sie ein Zertifikat einem Benutzer von der Seite **Benutzer** aus zuweisen.

Zertifizierungsstellen (CA)

Unterstützte Formate: Base64-kodiertes X.509 (.crt / .pem / .cer / .der).

CA-Zertifikate identifizieren eine Zertifizierungsstelle und zeigen dem Gerät an, dass allen von dieser CA ausgestellten Zertifikaten vertraut werden soll. Das Dashboard validiert, ob ein importiertes X.509-Zertifikat eine CA ist.

Zertifikats-Editor

Wenn Sie ein Zertifikat öffnen, zeigt der Editor dessen Hauptfelder und eine schreibgeschützte **Zertifikat-Informationen**-Anzeige an.

Hauptfelder

- **Name** (erforderlich)
- **ID** (schreibgeschützt)
- **Typ** (schreibgeschützt)
- **Ablaufdatum** (schreibgeschützt)
- **Importdatum** (schreibgeschützt)
- **Importierter Dateiname** (schreibgeschützt)

Benutzerzuordnung (Client-Zertifikate)

Für **Client**-Zertifikate zeigt der Editor ein **Benutzer**-Feld an. Wenn ein Benutzer zugewiesen ist, ermöglicht ein Menü die Optionen **Benutzer öffnen**, **Benutzer ändern** oder **Benutzerverknüpfung aufheben**. Wenn kein Benutzer zugewiesen ist, können Sie über die Benutzer-Aktionsschaltfläche einen zuweisen.

Zertifikat löschen

Die Aktion Löschen ist deaktiviert, wenn das Zertifikat derzeit mit einem Benutzer verknüpft oder in Richtlinien verwendet wird. Sie kann auch deaktiviert sein, wenn die Lizenz abgelaufen ist.

Ereignisregeln

Ereignisregeln ermöglichen es Ihnen, Reaktionen auf unterstützte Geräteereignisse zu automatisieren. Öffnen Sie **Dashboard** → **Ereignisregeln**, um Regeln zu erstellen, die Ereignisse wie Registrierung, Abmeldung, Nichtkonformität und Android-Geofencing überwachen und dann automatisch eine oder mehrere Aktionen auslösen.

Was eine Ereignisregel bewirken kann

Jede Regel kombiniert ein **Subjekt**, ein **Ereignis** und eine oder zwei **Aktionen**. Unterstützte Subjekte sind **Alle Geräte**, **Bestimmtes Gerät** und **Richtlinie**.

- **Ereignisse:** Gerät registriert, Gerät abgemeldet, Gerät wird nicht konform, Geofence betreten, Geofence verlassen.
- **Geräteaktionen:** Gerät deaktivieren, Gerät aktivieren, Gerät sperren.
- **E-Mail-Aktion:** eine Benachrichtigungs-E-Mail an Administratoren und, wenn aktiviert, an delegierte Manager senden.

Eine Regel kann entweder nur eine E-Mail-Aktion, nur eine Geräteaktion oder eine Kombination aus einer Geräteaktion und einer E-Mail-Aktion enthalten. Wenn beide Aktionen konfiguriert sind, führt Cerberus Enterprise zuerst die Geräteaktion und danach die E-Mail-Aktion aus.

Plattform- und Kompatibilitätsregeln

Die verfügbaren Ereignisse und Aktionen hängen vom ausgewählten Subjekt sowie von der für dieses Subjekt geltenden Plattform ab.

- **Android** unterstützt Ereignisse für Registrierung, Abmeldung, Nichtkonformität und Geofencing.
- **Apple** unterstützt Ereignisse für Registrierung, Abmeldung und Nichtkonformität.

- **Gerät deaktivieren** und **Gerät aktivieren** sind nur für Android verfügbar.
- **Gerät sperren** und **E-Mail senden** sind sowohl für Android als auch für Apple verfügbar, sofern das ausgewählte Ereignis sie unterstützt.
- **Gerät abgemeldet** unterstützt nur E-Mail-Aktionen.

Regelliste

Die Liste der Ereignisregeln ist die Hauptverwaltungsseite für diese Funktion. Sie enthält eine durchsuchbare Tabelle mit Regelname, Subjekt, Ereignis, Aktionen, Plattform, Aktivierungsstatus und Aktualisierungszeit.

- Verwenden Sie die Filter-Chips, um zwischen allen Regeln, aktivierten Regeln, deaktivierten Regeln und der Textsuche zu wechseln.
- Verwenden Sie die Schaltfläche **Aktualisieren**, um die aktuelle Tabellenansicht neu zu laden.
- Verwenden Sie den Aktivierungsschalter in jeder Zeile, um eine Regel vorübergehend zu aktivieren oder zu deaktivieren.
- Verwenden Sie den Modus zur Mehrfachauswahl von Zeilen, um mehrere Regeln gleichzeitig zu löschen.
- Verwenden Sie **Ereignisregel erstellen**, um den Editor für eine neue Regel zu öffnen.

Regel-Editor

Der Editor ist in die Abschnitte **Allgemein**, **Geltungsbereich**, **Trigger** und **Aktionen** unterteilt. Am unteren Seitenrand sorgt eine fixierte Aktionsleiste dafür, dass die Hauptschaltflächen beim Scrollen sichtbar bleiben.

Allgemein

- **Name**: erforderlich, bis zu 150 Zeichen.
- **Beschreibung**: optional, bis zu 2000 Zeichen.
- **Regel aktiviert**: speichert die Regel im Status „aktiviert“ oder „deaktiviert“.

Geltungsbereich

Der Geltungsbereich definiert, auf welche Geräte die Regel angewendet werden kann. Der Editor zeigt außerdem die aufgelöste Plattform und, falls verfügbar, den effektiven Richtlinienkontext an.

- **Alle Geräte:** Die Regel kann auf alle unterstützten Geräte im Unternehmen angewendet werden.
- **Bestimmtes Gerät:** Wählen Sie ein verwaltetes Gerät aus dem Auswahldialog aus.
- **Richtlinie:** Wählen Sie eine Richtlinienvorlage aus dem Auswahldialog aus.

Trigger

Der Bereich „Trigger“ filtert die verfügbaren Ereignisse automatisch basierend auf dem ausgewählten Geltungsbereich und der Plattform.

Geofencing-Trigger

Regeln für das Betreten und Verlassen eines Geofence werden nur für Android unterstützt und erfordern einen gültigen Android-Richtlinienkontext. Informationen zur Standortübermittlung und zu Geofence-Definitionen finden Sie unter [Standort und Geofence](#).

- Wenn das Subjekt **Alle Geräte** ist, gilt die Regel immer für **Jeden Geofence**.
- Wenn das Subjekt ein Gerät oder eine Richtlinie ist, können Sie entweder **Jeden Geofence** oder einen **Bestimmten Geofence** wählen.
- Die Liste der spezifischen Geofences wird aus dem effektiven Richtlinienkontext des ausgewählten Geräts oder der ausgewählten Richtlinie geladen.

Aktionen

Im Bereich „Aktionen“ können Sie eine optionale Geräteaktion und eine optionale E-Mail-Benachrichtigung auswählen. Die Benutzeroberfläche blendet nicht unterstützte Kombinationen automatisch aus.

- Wenn für das ausgewählte Ereignis und den gewählten Geltungsbereich keine Geräteaktion verfügbar ist, können Sie dennoch eine reine E-Mail-Regel speichern.
- Wenn E-Mail für das ausgewählte Ereignis und die Plattform deaktiviert ist, steht der Schalter für E-Mail-Benachrichtigungen nicht zur Verfügung.
- Eine Regel ohne jegliche Aktion ist ungültig und kann nicht gespeichert werden.

E-Mail-Empfänger

E-Mail-Aktionen schließen immer Unternehmensbenutzer mit der Rolle **ADMIN** ein. Wenn das Unternehmen über Multi-Tenancy verwaltet wird, können Sie die Empfänger erweitern, um MT-Manager einzubeziehen.

- **Nur Hauptmanager:** schließt Unternehmensadministratoren und die Hauptkontakte der MT-Manager ein.
- **Hauptmanager und Unterkonten-Manager:** schließt auch die zugewiesenen Unterkonten-Manager ein.
- Die Vorschau-Liste zeigt die tatsächlichen E-Mail-Adressen an, die verwendet werden, wenn die Regel ausgeführt wird.
- Nur delegierte Manager mit zugewiesenem Zugriff auf das Unternehmen werden in die endgültige Empfängerliste aufgenommen.

Ausführungsverhalten

Ereignisregeln werden sofort ausgeführt, wenn Cerberus Enterprise ein unterstütztes Ereignis von den Backend-Integrationen erhält. Deaktivierte Regeln werden automatisch übersprungen.

Erfolgreiche und fehlgeschlagene Ausführungen werden im Systemprotokoll mit für Menschen lesbaren Nachrichten aufgezeichnet.

Geräte

Geräte

Der Bereich **Geräte** im Dashboard (*Dashboard* → *Geräte*) listet alle in Ihrem Konto registrierten Geräte auf. Auf dieser Seite können Sie die Liste filtern, einen Gerätedatensatz öffnen und Geräteaktionen wie Deaktivieren oder Abmelden durchführen.

Filter

Am oberen Seitenrand können Sie über die Chip-Liste einen oder mehrere Filter aktivieren. Die ausgewählten Chips stellen die aktuell aktiven Filter dar.

Verfügbare Filter

- **Alle:** zeigt alle Geräte an.
- **Android:** zeigt nur Android-Geräte an.
- **Apple:** zeigt nur Apple-Geräte an.
- **Unternehmenseigene:** zeigt nur unternehmenseigene Geräte an.
- **Privat genutzte:** zeigt nur privat genutzte Geräte an.
- **Profile owner:** zeigt nur Geräte mit Android-Arbeitsprofil an.
- **Device owner:** zeigt nur vollständig verwaltete Android-Geräte an.
- **Aktiv:** zeigt Geräte im aktiven Status an.
- **Konform:** zeigt Geräte an, die richtlinienkonform sind.
- **Nicht konform:** zeigt Geräte an, die nicht richtlinienkonform sind.
- **Sicher:** zeigt Geräte mit einem sicheren Status an.
- **Nicht sicher:** zeigt Geräte mit einem unsicheren Status an.
- **Richtlinie nicht aktualisiert:** zeigt Geräte mit ausstehenden Richtlinienänderungen an.
- **Status nicht aktualisiert:** zeigt Geräte an, die in den letzten 72 Stunden keinen Status gemeldet haben.
- **App-Fehler:** zeigt Geräte an, deren Apps Fehlermeldungen gesendet haben.
- **Suche:** aktiviert ein Textsuchfeld.

Suche

Wenn Sie den Filter **Suche** aktivieren, erscheint ein Textfeld mit der Bezeichnung **ID, Modell oder Benutzer**. Die Liste wird automatisch aktualisiert, sobald Sie mit dem Tippen aufhören.

Gerätetabelle

Geräte werden in einer sortierbaren, paginierten Tabelle angezeigt. Durch Klicken auf eine Zeile wird der Geräte-Editor geöffnet.

Spalten

- **ID:** interne Gerätekennung.
- **MDM:** Plattform (Android oder Apple).
- **Modell:** Gerätemodell.
- **Besitzverhältnis:** unternehmenseigen oder privat genutzt (mit Details im Tooltip).
- **Verwaltungsmodus:** Verwaltungsmodus (mit Details im Tooltip).
- **Richtlinie:** aktuell zugewiesene Richtlinie.
- **Benutzer:** zugeordneter Benutzer (Name, E-Mail oder ID, je nach Verfügbarkeit).
- **Letzter Statusbericht:** Zeitstempel des aktuellsten Statusberichts (sofern verfügbar).
- **Status:** Gerätestatus (mit Details im Tooltip).
- **Konformität:** Anzeige des Konformitätsstatus.
- **Sicherheit:** Sicherheitsstatus (mit Details im Tooltip).
- **App-Fehler:** Anzeige von App-Fehlermeldungen.

Aktualisierung und Paginierung

- Verwenden Sie die Aktualisierungsaktion, um die Liste neu zu laden.
- Die Tabelle ist paginiert (10/25/50 Einträge pro Seite).

Geräteaktionen

Jede Gerätereihe kann je nach Plattform und Gerätestatus Aktionen bereitstellen. Einige Aktionen sind deaktiviert, wenn Ihre Lizenz abgelaufen oder gekündigt wurde.

Gerätespezifische Aktionen

- **Gerät deaktivieren / Gerät aktivieren:** verfügbar für Android-Geräte in unterstützten Zuständen.
- **Gerät abmelden:** entfernt die Verwaltung. Bei Android kann dies das Löschen des Arbeitsprofils oder einen Werksreset bewirken (abhängig vom Besitzverhältnis); bei Apple werden die Richtlinieneinstellungen entfernt.

- **Gerät löschen:** verfügbar für Geräte, die bereits abgemeldet wurden (entfernt den Datensatz aus dem System).

Mehrfachauswahl von Zeilen

Sie können die Mehrfachauswahl von Zeilen über die Aktionsleiste unter der Tabelle aktivieren. Wenn diese aktiviert ist, können Sie mehrere Zeilen auswählen und Massenaktionen (Deaktivieren, Aktivieren, Abmelden oder Löschen) durchführen, abhängig davon, welche Geräte ausgewählt wurden.

Apple Business Manager-Synchronisierung

Wenn die Apple-Verwaltung konfiguriert ist und ein Token für die automatische Geräteregistrierung vorliegt, zeigt die Seite möglicherweise die Aktion **Von ABM synchronisieren** an, um Geräte aus dem Apple Business Manager zu importieren.

Gerät registrieren

Verwenden Sie **Gerät registrieren**, um den Bereich für Registrierungstoken zu öffnen und mit der Registrierung eines neuen Geräts zu beginnen.

Benutzer

Benutzer

Der Bereich **Benutzer** des Dashboards (*Dashboard* → *Benutzer*) listet alle in Ihrem Konto konfigurierten Benutzer auf. Auf dieser Seite können Sie nach Benutzern suchen, den Benutzer-Editor öffnen, neue Benutzer erstellen und Benutzer löschen, die derzeit nicht mit Geräten verknüpft sind.

Suche

Am oberen Seitenrand befindet sich ein Suchfeld mit der Bezeichnung **Suche** und dem Platzhalter **Name, Benutzername oder E-Mail**. Die Liste aktualisiert sich automatisch, sobald Sie mit der Eingabe aufhören.

Benutzertabelle

Benutzer werden in einer sortierbaren, paginierten Tabelle angezeigt. Durch Klicken auf eine Zeile wird der Benutzer-Editor geöffnet.

Spalten

- **ID**: interner Benutzeridentifikator.
- **Vorname**: Vorname des Benutzers.
- **Nachname**: Nachname des Benutzers.
- **Benutzername**: Benutzername (oft ein Verzeichnis-Benutzername).
- **E-Mail**: E-Mail-Adresse des Benutzers.
- **Geräte**: Anzahl der aktuell mit dem Benutzer verknüpften Geräte.
- **Wi-Fi-Zertifikat**: Anzeige, ob dem Benutzer ein Wi-Fi-Zertifikat zugewiesen ist.

Aktualisierung und Paginierung

- Die Aktion Aktualisieren lädt die Liste neu.
- Die Tabelle ist paginiert (10/25/50 Einträge pro Seite).

Benutzeraktionen

Neuen Benutzer erstellen

Verwenden Sie **Neuen Benutzer erstellen**, um den Dialog zur Benutzererstellung zu öffnen. Diese Aktion ist deaktiviert, wenn Ihre Lizenz abgelaufen ist.

Synchronisierung mit Google Workspace

Wenn die Verzeichnis-Synchronisierung mit Google Workspace für Ihr Konto verfügbar ist, zeigt die Seite **Synchronisierung mit Google Workspace** an. Wenn Sie eine Synchronisierung starten, wird während der Ausführung des Vorgangs ein Fortschrittsanzeiger angezeigt.

Benutzer löschen

Sie können einen Benutzer nur löschen, wenn dieser mit keinem Gerät verknüpft ist (die Spalte **Geräte** muss 0 sein). Die Löschaktion ist deaktiviert, wenn Ihre Lizenz abgelaufen oder beendet wurde.

Mehrzeilenauswahl und Massenlöschung

In der Aktionsleiste unter der Tabelle können Sie die Mehrzeilenauswahl aktivieren. In diesem Modus können Sie mehrere Benutzer auswählen und diese gesammelt löschen.

- **Berechtigung:** Nur Benutzer mit **Geräte** = 0 können zur Löschung ausgewählt werden.
- **Alle auswählen:** Das Kontrollkästchen **Alle** wählt alle berechtigten Zeilen auf der aktuellen Seite aus.
- **Massenlöschung:** **Ausgewählte Benutzer löschen** ist deaktiviert, wenn keine Zeilen ausgewählt sind oder wenn Ihre Lizenz abgelaufen bzw. beendet wurde.

Wi-Fi-Zertifikate und EAP

Die Spalte **Wi-Fi-Zertifikat** zeigt an, ob einem Benutzer derzeit ein Zertifikat zugewiesen ist. Benutzerzertifikate werden in der Regel für Wi-Fi-EAP-Konfigurationen (z. B. EAP-TLS) verwendet. Informationen zur Zuweisung und Verwaltung von Zertifikaten finden Sie unter

[Zertifikatsverwaltung](#).

Benutzer-Editor

Der Benutzer-Editor ist über *Dashboard* → *Benutzer* durch Klicken auf eine Benutzerzeile verfügbar. Er ermöglicht es Ihnen, Benutzerdetails zu bearbeiten, benutzerbezogene Wi-Fi-EAP-Anmeldedaten zu konfigurieren und die mit dem Benutzer verknüpften Geräte anzuzeigen.

Benutzerdetails

Der obere Bereich enthält die Hauptfelder des Benutzers. Einige Felder sind Pflichtfelder; der Editor zeigt Validierungsfehler an, wenn diese fehlen oder ungültig sind.

- **ID:** schreibgeschützter Identifikator.
- **Vorname:** Pflichtfeld.
- **Nachname:** Pflichtfeld.
- **Benutzername:** Pflichtfeld.
- **E-Mail:** Pflichtfeld und muss eine gültige E-Mail-Adresse sein.
- **Telefonnummer:** optional.
- **Google-Konto:** optional; falls angegeben, muss eine gültige E-Mail-Adresse sein.

Standardrichtlinie für die Google-Authentifizierung

In Google Workspace-Umgebungen mit aktivierter Google-Authentifizierung kann der Editor **Standardrichtlinie für die Google-Authentifizierung** anzeigen. Dies ist die Richtlinie, die auf Geräte angewendet wird, die von diesem Benutzer mittels Google-Authentifizierung registriert wurden.

- **Richtlinie ändern:** öffnet den Dialog zur Richtlinienauswahl.
- **Richtlinie öffnen:** öffnet die ausgewählte Richtlinie im Richtlinien-Editor (sofern eine Richtlinie festgelegt ist).
- Nachdem Sie eine neue Standardrichtlinie ausgewählt haben, müssen Sie den Benutzer speichern, um die Änderung anzuwenden. Der Editor zeigt eine Benachrichtigung an, die Sie an das Speichern erinnert.

Wi-Fi-EAP-Anmeldedaten

Der Bereich **Wi-Fi-EAP-Anmeldedaten** wird verwendet, um benutzerbezogene Anmeldedaten zu konfigurieren, die automatisch auf den Geräten des Benutzers installiert werden, wenn die zugewiesene Richtlinie eine Wi-Fi-EAP-Konfiguration enthält, die diese erfordert. Die Wi-Fi-EAP-Konfiguration ist Teil der Android-Richtlinie [Netzwerkkonfiguration](#).

Client-Zertifikat

Sie können einem Benutzer optional ein Client-Zertifikat zuweisen. Wenn ein Zertifikat zugewiesen wurde, wird es im Feld **Client-Zertifikat** angezeigt und ein Menü bietet Aktionen an. Wenn kein Zertifikat zugewiesen ist, zeigt das Feld **Kein Zertifikat zugewiesen** an, und Sie können eines zuweisen.

- **Zertifikat zuweisen:** öffnet den Dialog zur Zertifikatsauswahl.
- **Zertifikat öffnen:** öffnet den Zertifikats-Editor.
- **Zertifikat ändern:** wählt ein anderes Client-Zertifikat aus.
- **Zertifikat trennen:** entfernt das Zertifikat vom Benutzer. Das System entfernt das Zertifikat auch von allen mit diesem Benutzer verknüpften Geräten.

Informationen zum Import und zur Verwaltung von Zertifikaten finden Sie unter [Zertifikatsverwaltung](#).

Identität, anonyme Identität und Passwort

- **Identität:** Identität des Benutzers. Bei Tunneling-Outer-Protokollen (PEAP, EAP-TTLS) wird diese innerhalb des Tunnels verwendet.
- **Anonyme Identität:** wird bei Tunneling-Outer-Protokollen als die außerhalb des Tunnels präsentierte Identität verwendet. Wenn nichts angegeben wird, ist der Standardwert eine leere Zeichenfolge.
- **Passwort:** das Benutzerpasswort für EAP-Methoden, die dies erfordern. Wenn nichts angegeben wird, kann das Gerät den Benutzer zur Eingabe auffordern. Eine Anzeigen/Verbergen-Aktion schaltet die Sichtbarkeit des Passworts um.

Verknüpfte Geräte

Der Bereich **Verknüpfte Geräte** zeigt die Liste der Geräte an, die aktuell mit dem Benutzer verknüpft sind. Wenn der Benutzer ein oder mehrere verknüpfte Geräte hat, kann der Benutzer

nicht gelöscht werden.

Speichern und Löschen

- **Benutzer speichern:** wird nur aktiviert, wenn das Formular gültig ist, noch Änderungen ausstehen und die Lizenz aktiv ist. Während des Speicherns wird ein Fortschrittsanzeiger angezeigt.
- **Benutzer löschen:** deaktiviert, wenn der Benutzer mit Geräten verknüpft ist oder die Lizenz abgelaufen/beendet wurde. Wenn das Löschen zulässig ist, wird ein Bestätigungsdialog angezeigt. Falls der Benutzer Registrierungstoken zugewiesen ist, warnt der Dialog, dass Geräte, die mit diesen Token registriert wurden, keinem Benutzer mehr zugeordnet sind.

Warnung vor nicht gespeicherten Änderungen

Wenn Sie nicht gespeicherte Änderungen haben und versuchen, die Seite zu verlassen, fragt das Dashboard, ob Sie die Änderungen verwerfen möchten.

Konto

Einstellungen

Die **Einstellungen**-Seite (*Dashboard* → *Einstellungen*) fasst Konto- und Lizenzinformationen zusammen und bietet Aktionen zur Verwaltung der Abrechnung, des Plattform-Setups (Android Management und Apple Management) sowie optionaler Verzeichnis-/Token-Integrationen.

Lizenz-Banner (ablaufend / abgelaufen)

Wenn Ihre Lizenz **bald abläuft**, **abgelaufen ist** oder **beendet wurde**, wird ein auffälliges Banner am oberen Seitenrand angezeigt. Je nach Abonnementstatus bietet es entweder die Aktion **Abrechnung verwalten** (Stripe-Kundenportal) oder die Aktion **Lizenz kaufen**.

Wenn die Lizenz abgelaufen ist, wird das Konto auf das bloße Abmelden von Geräten beschränkt. Nach Ablauf der Nachfrist kann das Konto gekündigt werden und Geräte können automatisch abgemeldet werden.

Zugriff des Enterprise Managers

Die Karte **Zugriff des Enterprise Managers** wird nur für Unternehmen angezeigt, die von einem Multi-Tenancy-Konto verwaltet werden (zum Beispiel von einem Managed Service Provider). Sie zeigt, welche Managerkonten auf Ihr Unternehmen zugreifen können, und ermöglicht es, deren Zugriff zu steuern.

Die Karte zeigt:

- Der **Eigentümer** des Unternehmens. Der Eigentümer hat immer Zugriff, und sein Zugriff kann nicht entzogen werden.
- Jedes Managerkonto des Multi-Tenancy-Kontos, gekennzeichnet als **Hauptmanager** oder **Unterkonto**, mit Name, Benutzername und Zugriffsstatus (**Erteilt**, **Entzogen** oder **Nicht erteilt**).

Zugriff erteilen und entziehen

Verwenden Sie **Erteilen**, um einem Managerkonto den Zugriff auf Ihr Unternehmen und dessen Verwaltung zu erlauben, und **Entziehen**, um diesen Zugriff zu entfernen. Jede Aktion muss bestätigt werden. Ein Manager, dem der Zugriff entzogen wurde, kann nicht mehr im Unternehmen arbeiten, auch wenn er gerade darin tätig ist.

- Als Unternehmensadministrator können Sie jedem aufgeführten Managerkonto Zugriff erteilen oder entziehen.
- Der Hauptmanager kann seinen eigenen Unterkonten Zugriff erteilen oder entziehen, aber nur solange ihm selbst Zugriff erteilt ist. Er kann sich nicht selbst Zugriff erteilen und seinen eigenen Zugriff nicht entziehen.

Wenn Sie dem **Hauptmanager** den Zugriff entziehen, wird auch allen seinen Unterkonten der Zugriff entzogen. In diesem Fall listet der Bestätigungsdialog die Unterkonten auf, die den Zugriff verlieren.

Kontoinformationen

Die Karte **Kontoinformationen** zeigt schreibgeschützte Felder:

- **Benutzername**
- **Unternehmensname**
- **Unternehmens-ID**

Passwort ändern

Wenn Sie nicht mit Google, Apple oder Microsoft angemeldet sind, zeigt die Karte auch die Aktion **Passwort ändern** an. Dadurch wird ein Dialog geöffnet, um mit dem Passwortänderungsprozess fortzufahren.

Sie können Ihr Passwort auch jederzeit über das Benutzermenü in der oberen Symbolleiste mit **Passwort ändern** ändern. Das ist nützlich für Multi-Tenancy-Konten, die ihr Passwort ändern können, ohne ein Unternehmen zu öffnen.

Wenn ein Administrator Ihr Konto erstellt oder Ihr Passwort zurückgesetzt hat, melden Sie sich mit einem temporären Passwort an und müssen ein neues Passwort wählen, bevor Sie fortfahren können.

Lizenzinformationen

Die Karte **Lizenzinformationen** zeigt den aktuellen Lizenzstatus und Ihr Gerätelimit an. Sie bietet außerdem Aktionen zur Kontaktaufnahme mit dem Vertrieb sowie zur Verwaltung der Abrechnung oder zum Kauf einer Lizenz.

- **Lizenzstatus:** wird als **Aktiv** oder **Abgelaufen** angezeigt (mit einem Icon-Badge und Tooltip).
- **Kostenlose Testversion:** wird angezeigt, wenn sich das Konto derzeit im Testmodus befindet.
- **Lizenzierte Geräte:** maximale Anzahl der durch die Lizenz erlaubten Geräte. Der Link *Benötigen Sie mehr Geräte?* öffnet eine Nachricht, um den Support zu kontaktieren.
- **Nächste geplante Verlängerung:** wird für aktive Abonnements angezeigt, die sich automatisch verlängern. Andernfalls zeigt die Karte das **Ablaufdatum** an.

Android Management

Die Karte **Android Management** zeigt den Android Management-Status für Ihr Unternehmen an. Wenn Android Management noch nicht konfiguriert ist, bietet die Karte die Aktion **Android Management einrichten**, die den Einrichtungsprozess öffnet.

Konfiguriert (Status)

Wenn Android Management konfiguriert ist, kann die Karte Folgendes anzeigen:

- **Management-ID**
- **Bindungstyp:** gibt an, ob das Unternehmen ein **verwaltetes Google Play-Konto** oder eine **verwaltete Google-Domain** verwendet.
- **Mit Google Workspace synchronisiert** (Badge wird angezeigt, wenn die Verzeichnissynchronisierung aktiv ist)
- **Mit Google Workspace synchronisieren** (wird angezeigt, wenn die Verzeichnissynchronisierung nicht konfiguriert ist; öffnet das Anleitungs-Panel am unteren Seitenrand)

Android Enterprise-Bindung

Android Management kann entweder mit einem **verwalteten Google Play-Konto** oder einer **verwalteten Google-Domain** verknüpft werden. Das Feld **Bindungstyp** zeigt an, welche Option derzeit mit Ihrem Unternehmen verknüpft ist.

Ein **verwaltetes Google Play-Konto** ist ein leichtgewichtiges Android Enterprise-Konto. Es eignet sich zur Verwaltung von Android-Geräten und Apps über Cerberus Enterprise, ist jedoch getrennt von einer Google Workspace- oder Cloud Identity-Organisation. Es bietet nicht die zentrale Google-Administrationserfahrung, die mit einer verwalteten Google-Domain verfügbar ist.

Eine **verwaltete Google-Domain** verknüpft Android Enterprise mit der Google-Identität Ihrer Organisation. IT-Administratoren können Google-Produkte wie Google Workspace, Cloud Identity und Gemini über die Google Admin-Konsole verwalten und gleichzeitig weiterhin Android-Apps und Richtlinien in Cerberus Enterprise verwalten. Dies bietet einen effizienteren, integrierten Ansatz für das Android-Management und ermöglicht Registrierungs- sowie Benutzerverwaltungs-Workflows auf Basis von Google Workspace.

Wenn das Unternehmen ein verwaltetes Google Play-Konto verwendet, bietet die Karte Einstellungen die Optionen **Upgrade auf verwaltete Google-Domain** und eine Informationsaktion an. Das Upgrade öffnet den geführten Prozess von Google, um das bestehende Android Enterprise in eine verwaltete Domain zu überführen.

Während des Upgrades kann Google automatisch ein bestehendes Google Admin-Konto verknüpfen, das mit Ihrer geschäftlichen E-Mail-Adresse verbunden ist, oder ein neues kostenloses Google Admin-Konto erstellen. Verwenden Sie eine geschäftliche E-Mail-Adresse wie *name@enterprise.com*, um die geführte Einrichtung von Google fortzusetzen.

Apple Device Management

Die Karte **Apple Device Management** zeigt den Status des Apple Device Managements (MDM) für Ihr Unternehmen an. Wenn das Apple Management noch nicht konfiguriert ist, bietet die Karte die Aktion **Apple Management einrichten**, die den Einrichtungsprozess öffnet.

Konfiguriert (Status)

Wenn das Apple Management konfiguriert ist, kann die Karte Folgendes anzeigen:

- **Apple-ID**
- **Ablaufdatum des Apple Push Zertifikats:** zeigt das Ablaufdatum und ein Icon-Badge an. Wenn das Zertifikat bald abläuft oder bereits abgelaufen ist, ist das Badge anklickbar und öffnet die Anweisungen zur Verlängerung.
- **Ablaufdatum des ABM-Tokens:** zeigt das Ablaufdatum des Apple Business Manager Tokens an (mit einem anklickbaren Badge, wenn eine Aktion erforderlich ist).
- **VPP-Token:** zeigt den Organisationsnamen und das Ablaufdatum für den Apple Volume Purchase Program Token an (mit einem anklickbaren Badge, wenn eine Aktion erforderlich ist).

- **Apple Business Manager Portal:** Link, der angezeigt wird, wenn ein ABM-Token vorhanden ist.
- **Mit Apple Business Manager synchronisieren** und **Mit Apple Volume Purchase Program synchronisieren:** wird angezeigt, wenn Token fehlen.

Das Apple Management erfordert die Einrichtung des APNs-Zertifikats. Falls erforderlich, siehe [Apple Management Einrichtung \(APNs\)](#).

Einstellungen & Datenschutz

Die Karte **Einstellungen & Datenschutz** enthält einen Schalter für Marketing-Präferenzen sowie Links zu den Nutzungsbedingungen und der Datenschutzerklärung. Verwenden Sie **Einstellungen speichern**, um Änderungen zu übernehmen (während des Speicherns wird ein Fortschrittsanzeiger angezeigt).

Feedback senden

Wenn Abonnements für das Konto aktiviert sind, kann die Seite eine **Feedback senden**-Karte mit Links zu: **Feature-Anfrage stellen** und externen Bewertungsplattformen anzeigen.

Inline-Einrichtungs- und Verlängerungsanweisungen

Am Ende der Seite kann das Dashboard je nach aktuellem Status erweiterbare Anleitungs-Panels anzeigen (zum Beispiel, wenn ein Zertifikat oder Token fehlt oder bald abläuft).

Apple Push Zertifikat (APNs) erneuern

Wenn das APNs-Zertifikat bald abläuft oder bereits abgelaufen ist, zeigt die Seite ein Panel mit Schritten zum Herunterladen einer CSR, zur Erneuerung des Zertifikats im Apple-Portal und zum Hochladen des neuen Zertifikats in Cerberus Enterprise an.

Mit Apple Business Manager (ABM) synchronisieren

Wenn der ABM-Token fehlt, abgelaufen ist oder bald abläuft, zeigt die Seite ein Panel mit Schritten zum Herunterladen eines Tokens aus dem Apple Business Manager und zum Hochladen in Cerberus Enterprise an.

Mit dem Apple Volume Purchase Program (VPP) synchronisieren

Wenn der VPP-Token fehlt, abgelaufen ist oder bald abläuft, zeigt die Seite ein Panel mit Schritten zum Herunterladen eines Content-Tokens aus dem Apple Business Manager und zum Hochladen in Cerberus Enterprise an.

Mit Google Workspace synchronisieren

Wenn die Google Workspace Verzeichnissynchronisierung nicht konfiguriert ist, zeigt die Seite ein Panel an, das die Integration erklärt und eine Autorisierungsschaltfläche bereitstellt. Es listet außerdem den erforderlichen Google OAuth-Scope auf:

<https://www.googleapis.com/auth/admin.directory.user.readonly>.

Für die erste Android-Einrichtung siehe **[Android Management Einrichtung](#)**.

Mandantenfähigkeit

Multi-Tenancy-Übersicht

Der Bereich **Multi-Tenancy** steht MSP- und Enterprise-Manager-Konten zur Verfügung, die mehrere Kundenunternehmen über einen einzigen Login verwalten. Dieses Kapitel erläutert das Enterprise-Scope-Modell, das Wechseln zwischen Unternehmen, die Verwaltung von Unternehmen sowie Unterkonten.

Um ein Multi-Tenancy-Konto anzufordern, kontaktieren Sie bitte enterprise@cerberusapp.com.

Kernkonzepte

- **Haupt-Multi-Tenancy-Konto:** das primäre Manager-Konto, das auf den globalen Multi-Tenancy-Arbeitsbereich zugreifen kann.
- **Unterkonto:** ein vom Hauptkonto erstelltes, delegiertes Manager-Konto mit auswählbaren Unternehmenszuweisungen.
- **Ausgewählter Unternehmenskontext:** das aktive Unternehmen, das derzeit im Dashboard für die täglichen Abläufe geöffnet ist.
- **Delegierung:** eine vom Unternehmenseigentümer erteilte Berechtigung, die es einem Manager-Konto ermöglicht, das Unternehmen zu betreten und zu verwalten.

Navigationsmodell

Wenn kein Unternehmenskontext ausgewählt ist, zeigt die Seitennavigation Multi-Tenancy-Bereiche wie **Enterprises** und, für Hauptkonten, **Sub-accounts** an. Nach dem Betreten eines Unternehmens wechselt das Dashboard zur standardmäßigen Einzelunternehmen-Navigation (Home, Benutzer, Geräte, Registrierung, Richtlinien und mehr).

Eigentum und Delegierung

Jedes verwaltete Unternehmen hat einen Eigentümer. Der Eigentümer kann jederzeit auf dieses Unternehmen zugreifen. Manager-Konten, die nicht der Eigentümer sind, können nur dann auf ein Unternehmen zugreifen, wenn eine Delegierung erteilt wurde.

- Wenn ein Unternehmen einen eigenen Administrator hat, ist dieser Administrator der Eigentümer und entscheidet, welche Managerkonten auf das Unternehmen zugreifen können.
- Wenn ein Unternehmen keinen eigenen Administrator hat, ist das Haupt-Multi-Tenancy-Konto der Eigentümer.
- Bei Unternehmen, deren Eigentümer ein Administrator des Kunden ist, kann das Hauptkonto seinen eigenen Unterkonten Zugriff erteilen oder entziehen, solange ihm selbst Zugriff erteilt ist, sich selbst jedoch keinen Zugriff erteilen.
- Wenn der Unternehmensadministrator dem Hauptkonto den Zugriff entzieht, wird auch seinen Unterkonten der Zugriff entzogen.
- Wenn Sie ein Unternehmen aus den Zuweisungen eines Unterkontos entfernen, wird auch dessen Zugriff auf das Unternehmen entfernt. Wenn Sie es später erneut zuweisen, muss der Zugriff erneut erteilt werden.

Unternehmensadministratoren verwalten den Zugriff über die Karte **Zugriff des Enterprise Managers** auf der Seite **Einstellungen**.

Eigentümer- und Delegierungsstatus werden direkt auf den Unternehmenskarten angezeigt, um den Zugriffsumfang vor dem Betreten eines Unternehmens explizit zu machen.

Lizenz- und Abrechnungsaktionen

Multi-Tenancy-Ansichten zeigen den Lizenzstatus, die Gerätelimitierung und Abrechnungsaktionen des Unternehmens an. Je nach Abonnementstatus des Unternehmens und Ihren Berechtigungen kann die Karte **Abrechnung verwalten** oder **Lizenz kaufen** anzeigen.

Für von einem Multi-Tenancy-Konto erstellte Unternehmen wird die Lizenzierung durch die Multi-Tenancy-Benutzer verwaltet. Das Hauptkonto kann die Lizenzierung jederzeit verwalten, während Unterkonten die Lizenzierung nur dann verwalten können, wenn das Hauptkonto die Berechtigung **Lizenz verwalten kann** für dieses Unterkonto aktiviert hat.

Seiten in diesem Kapitel

- [Verwaltete Unternehmen](#): Suche, Filter, Kartendetails und Unternehmenserstellung.
- [Unternehmenswechsel](#): Verhalten des oberen Wechselfelds und Übergänge im Umfang.
- [Unterkonten](#): delegierte Administratoren, Zuweisungen und Verwaltung von Anmeldedaten.

Verwaltete Unternehmen

Die **Enterprises**-Seite (*Dashboard* → *Enterprises*) ist die Schaltzentrale für den verwalteten Unternehmenszugriff. Sie listet alle Unternehmen auf, die für Ihr Multi-Tenancy-Konto sichtbar sind, und ermöglicht es Ihnen, diese zu filtern, Eigentum/Delegierung zu prüfen, in einen Unternehmenskontext zu wechseln und neue verwaltete Unternehmen zu erstellen (nur Hauptkonten).

Suche und Filter

- **Unternehmen suchen:** Filtert nach Unternehmensname oder Unternehmens-ID.
- **Delegierung:** **Alle**, **Delegiert** oder **Nicht delegiert**.
- **Lizenzstatus:** **Alle**, **Gültig**, **Läuft bald ab**, **Abgelaufen** oder **Beendet**.

Unternehmenskarten

Jede Unternehmenskarte zeigt wichtige Verwaltungsmetadaten an:

- **Lizenzstatus** mit Icon-Badge und kontextuellem Tooltip.
- **Lizenzierte Geräte** (Gerätelimit des Unternehmens).
- **Nächste geplante Verlängerung** oder **Ablaufdatum**, je nach Abonnementstatus.
- **Delegierungsstatus** (**Eigentümer**, **Erteilt** oder **Nicht erteilt**).
- **Anzeigename des Eigentümers** und Benutzername.

Zuletzt ausgewählte Unternehmen

Unternehmen, auf die Sie kürzlich zugegriffen haben, sind in einem Bereich **Zuletzt ausgewählt** angeheftet, um das wiederholte Wechseln des Kontextes zu beschleunigen.

Unternehmensaktionen

- **Unternehmen betreten:** Öffnet den ausgewählten Unternehmenskontext, sofern der Zugriff durch Delegierung/Eigentum erlaubt ist.

- **Abrechnung verwalten:** Öffnet die Abrechnungsverwaltung des Unternehmens, sofern verfügbar und zulässig.
- **Lizenz kaufen:** Öffnet den Kaufprozess für das Unternehmen, wenn keine aktive Abrechnung vorliegt.

Wer kann Lizenzen verwalten?

Für von einem Multi-Tenancy-Konto erstellte Unternehmen wird die Lizenzverwaltung durch die Multi-Tenancy-Benutzer gesteuert. Das Hauptkonto kann jederzeit die Abrechnungs- und Lizenzaktionen für diese Unternehmen verwalten.

Unterkonten können Abrechnungs- und Lizenzaktionen nur verwalten, wenn das Hauptkonto die Berechtigung **Lizenz verwalten kann** auf der [Unterkonten](#)-Seite erteilt.

Verwaltetes Unternehmen erstellen

Haupt-Multi-Tenancy-Konten können **Verwaltetes Unternehmen erstellen** aus dem Aktionsbereich am unteren Rand erweitern.

- **Unternehmensname** ist erforderlich.
- **Unternehmensspezifischen Admin-Benutzer erstellen** steuert den Eigentumsmodus.
- Wenn aktiviert, sind **Admin-Benutzername** (E-Mail-Format) und **Admin-Name** erforderlich.
- Vor der Erstellung fasst ein Bestätigungsdialog den Vorgang zusammen und warnt gegebenenfalls davor, dass temporäre Anmeldedaten per E-Mail an den neuen Admin-Benutzer gesendet werden.

Der neue Administrator muss bei der ersten Anmeldung mit dem temporären Passwort ein neues Passwort wählen.

Eigentumsmodus

- **Unternehmensspezifischer Admin aktiviert:** Der neue Admin-Benutzer ist Eigentümer des Unternehmens und kann die Verwaltung an Ihr Multi-Tenancy-Konto delegieren.
- **Unternehmensspezifischer Admin deaktiviert:** Das Unternehmen gehört direkt Ihrem Multi-Tenancy-Konto.

Unternehmenskontingent

Wenn das Konto das konfigurierte Unternehmenskontingent erreicht, wird die Erstellung blockiert und das Formular zeigt eine Support-Kontaktmeldung mit der aktuellen und der maximalen Anzahl an Unternehmen an.

Wenn das Unternehmenskontingent erreicht ist, können Sie keine weiteren verwalteten Unternehmen erstellen, bis Ihr Limit erhöht wird.

Unternehmenswechsel

Der Unternehmens-Switcher in der oberen Symbolleiste ermöglicht es Multi-Tenancy-Benutzern, zwischen delegierten Unternehmen zu wechseln, ohne sich abmelden zu müssen. Er steht zur Verfügung, wenn mindestens ein Unternehmenskontext ausgewählt werden kann.

Verhalten des Switchers

- Der Trigger zeigt den aktuellen Unternehmensnamen (oder die Unternehmens-ID, falls kein Name verfügbar ist) an.
- Das Menü listet die delegierten/zugreifbaren Unternehmen auf und kennzeichnet das aktuell ausgewählte Unternehmen.
- Während des Wechsels werden die Switcher-Aktionen vorübergehend deaktiviert, um gleichzeitige Änderungen am Geltungsbereich zu verhindern.

Unternehmen verlassen

Das Switcher-Menü enthält die Option **Unternehmen verlassen**, die den aktuellen Unternehmenskontext löscht und Sie zum globalen Multi-Tenancy-Arbeitsbereich zurückführt.

Regeln zum Kontext-Reset

Der Wechsel des Unternehmens oder das Verlassen des Unternehmens setzt den Dashboard-Geltungsbereich zurück. Unternehmensspezifische Seiten und Daten werden für den neu ausgewählten Kontext aktualisiert, und die Sichtbarkeit des Menüs passt sich an, ob ein Unternehmen aktuell ausgewählt ist.

Das ausgewählte Unternehmen gilt für alle geöffneten Browser-Tabs. Wenn Sie in einem Tab das Unternehmen wechseln oder verlassen, laden die anderen Tabs das Dashboard bei der nächsten Aktion neu, sodass sie nie mit einem anderen als dem angezeigten Unternehmen arbeiten.

Verwenden Sie den Switcher für schnelle betriebliche Kontextwechsel, aber überprüfen Sie den ausgewählten Unternehmensnamen, bevor Sie sensible Aktionen wie

Richtlinienaktualisierungen oder Gerätebefehle ausführen.

Unterkonten

Die **Unterkonten**-Seite (*Dashboard* → *Unterkonten*) steht Haupt-Multi-Tenancy-Konten zur Verfügung. Sie ermöglicht es Ihnen, delegierte Manager-Benutzer zu erstellen, verwaltete Unternehmen zuzuweisen, Abrechtsberechtigungen zu steuern und die Anmeldedaten der Unterkonten zu verwalten.

Unterkontenliste

Jede Unterkontenkarte zeigt Identitäts- und Verwaltungssteuerungen an:

- **Name** und **Benutzername/E-Mail**.
- **Verwaltete Unternehmen** Multi-Select-Zuweisung.
- **Schalter für die Berechtigung „Lizenz verwalten kann“**.
- **Passwort zurücksetzen** und **Löschen**-Aktionen.

Zuweisung verwalteter Unternehmen

Unternehmenszuweisungen werden über das Multi-Select-Feld **Verwaltete Unternehmen** bearbeitet. Wenn Sie den Selektor nach Änderungen schließen, fragt das Dashboard vor dem Speichern der Aktualisierungen um Bestätigung.

Durch die Zuweisung wird ein Unternehmen für das Unterkonto verfügbar, das Unterkonto kann es jedoch erst öffnen, nachdem der Zugriff erteilt wurde. Wenn Sie ein Unternehmen aus den Zuweisungen entfernen, wird auch der Zugriff des Unterkontos darauf entfernt.

Berechtigung zur Lizenzverwaltung

Der Schalter **Lizenz verwalten kann** steuert, ob ein Unterkonto auf Abrechnungs-/Lizenzverwaltungsaktionen des Unternehmens zugreifen kann.

Für von dem Multi-Tenancy-Konto erstellte Unternehmen hat das Hauptkonto stets die Rechte zur Lizenzverwaltung. Unterkonten erhalten die Rechte zur Lizenzverwaltung nur dann, wenn dieser Schalter vom Hauptkonto aktiviert wurde.

Passwort zurücksetzen

Passwort zurücksetzen generiert ein neues temporäres Passwort und sendet es nach der Bestätigung per E-Mail an das Unterkonto.

Bei der Anmeldung mit einem temporären Passwort, ob nach einem Zurücksetzen oder bei einem neu erstellten Unterkonto, muss der Benutzer ein neues Passwort wählen, bevor er fortfahren kann.

Unterkonto löschen

Das Löschen eines Unterkontos erfordert eine Bestätigung und entfernt dauerhaft den delegierten Zugriff für dieses Konto.

Unterkonto erstellen

Verwenden Sie das Aktionspanel am unteren Rand **Unterkonto erstellen**, um einen neuen delegierten Manager hinzuzufügen.

- **E-Mail:** erforderlich und wird als E-Mail-Format validiert.
- **Name:** erforderlicher Anzeigename.
- **Lizenz verwalten kann:** optionale initiale Abrechnungsberechtigung.
- Vor der Erstellung warnt ein Bestätigungsdialo g davor, dass eine E-Mail mit einem temporären Passwort an die angegebene Adresse gesendet wird.

Insights

Hier sind einige Artikel, die vertiefen, wie MDM Ihrem Unternehmen helfen kann:

Was ist der Kiosk-Modus? Ein Leitfaden zur Sperrung von Android- und Apple-Geräten für Unternehmen

Der Kiosk-Modus verwandelt Standard-Smartphones und Tablets in spezialisierte Business-Tools. Cerberus Enterprise hilft Unternehmen dabei, Geräte auf eine einzige App oder einen kleinen, genehmigten Satz von Apps zu beschränken – ideal für Anwendungsfälle wie POS-Systeme im Einzelhandel, Check-in-Terminals für Gäste oder die Flottenavigation. Gleichzeitig wird es einfacher, diese spezialisierten Geräte in großem Maßstab zu sichern, zu unterstützen und zu verwalten.

So wählen Sie die richtige MDM- Lösung: Eine 7-Punkte-Checkliste für kleine Unternehmen

Die Entscheidung für ein MDM spät im Kaufprozess zu treffen, fällt leichter, wenn der Vergleich praxisnah bleibt. Diese Checkliste hilft kleinen Unternehmen dabei, Anbieter anhand der sieben Kriterien zu bewerten, die bei realen Implementierungen meist am wichtigsten sind: Sicherheit, Android- und Apple-Unterstützung, Benutzerfreundlichkeit für schlanke Teams, Skalierbarkeit, Datenschutzgrenzen, Gesamtbetriebskosten (TCO) und die tägliche Supportfähigkeit.

Ein sicheres und fokussiertes digitales Klassenzimmer schaffen:

Ein Leitfaden zu MDM für K-12-

Schulen

Von der Schule verwaltete Geräte funktionieren am besten, wenn sie sich auf das Lernen konzentrieren können. Cerberus Enterprise hilft K-12-Organisationen dabei, die Geräte der Schüler durch verwaltete Apps, Kiosk-ähnliche Einschränkungen, standardisierte Setups für gemeinsam genutzte oder ausgeliehene Geräte sowie Remote-Wiederherstellungsaktionen, die Verluste, Abweichungen und Unterrichtsstörungen reduzieren, fokussiert zu halten.

Ausstattung Ihrer

Außendiensttechniker: Wie MDM

die Effizienz und Sicherheit vor Ort

steigert

Außendiensttechniker sind bei der Arbeit vor Ort auf mobile Geräte angewiesen, um Zeitpläne, Servicehinweise, technische Referenzen, die Kundenhistorie und Arbeitsaktualisierungen abzurufen. Cerberus Enterprise hilft dabei, diese Geräte einsatzbereit zu halten – durch verwaltete Apps, standardisierte Gerätemodelle, Remote-Support-Befehle und standortbezogene Sichtbarkeit, die die Einsatzkoordination verbessern kann, während gleichzeitig die Sicherheit im Außendienst gestärkt wird.

Jenseits der Karte: Wie MDM für ein intelligenteres

Flottenmanagement und Fahrersicherheit sorgt

Flottenbetriebe sind für Navigation, Disposition, Messaging, Protokollierung und die Ausführung von Einsätzen vor Ort auf mobile Geräte angewiesen. Cerberus Enterprise hilft dabei, diese Geräte durch verwaltete Apps, Kiosk- und dedizierte Gerätekontrollen, sichere Kommunikationsrichtlinien, Remote-Fehlerbehebung und standortbezogene Überwachung auf genehmigte Arbeitsabläufe zu fokussieren, was Ausfallzeiten reduzieren und sicherere Fahrbetriebe unterstützen kann.

Wie Geofences, Live-Tracking und Standortkarten den

Unternehmensbetrieb verbessern

Standortbezogene Funktionen in Cerberus Enterprise helfen Unternehmen dabei, von einer einfachen Geräteübersicht zu einer praxisnahen operativen Kontrolle überzugehen. Regelmäßige Standortberichte, Live-Tracking, Geofence-Übergänge und interaktive Karten können Logistik,

Außendienst, das Gesundheitswesen, den Einzelhandel, das Baugewerbe und andere verteilte Teams unterstützen, die einen besseren Einblick benötigen, wo gearbeitet wird und wann Geräte wichtige Bereiche betreten oder verlassen.

Wie Multi-Tenancy MSPs dabei hilft, MDM-Dienste zu skalieren und neue Einnahmequellen zu erschließen

Multi-Tenancy ermöglicht es MSPs, Wiederverkäufern und Organisationen mit mehreren Unternehmen, mehrere Betriebe über ein einziges Cerberus Enterprise-Konto zu verwalten und dabei jede Umgebung getrennt zu halten. Dieses Modell reduziert den operativen Aufwand, verbessert die Skalierbarkeit der Dienste und unterstützt den delegierten Zugriff durch Unterkonten sowie eine explizite, kundengesteuerte Administration. Zudem schafft es stärkere Geschäftsmöglichkeiten für Anbieter, die Softwarelizenzierung mit Onboarding, Support, Compliance und Managed Mobility Services kombinieren möchten.

Steigerung der betrieblichen Effizienz durch MDM-Lösungen

Mobile Device Management zentralisiert die Kontrolle über Unternehmensgeräte und vereinfacht so die Registrierung, Konfiguration und Wartung. Automatisierte Bereitstellung und Massenoperationen reduzieren den manuellen IT-Aufwand und gewährleisten konsistente Richtlinien auf allen Geräten. Sicherheitsfunktionen wie Verschlüsselung, Konformitätsüberwachung und das Löschen aus der Ferne schützen Unternehmensdaten. Insgesamt verbessert MDM die Produktivität, während es gleichzeitig die Supportkosten und die betriebliche Komplexität reduziert.

Erweiterte Sicherheit im Android

Enterprise Management

Android Enterprise nutzt ein Arbeitsprofil, um geschäftliche Apps und Daten von persönlichen Inhalten auf demselben Gerät zu isolieren. Diese Containerisierung schafft getrennte, verschlüsselte Umgebungen, die unabhängig von den IT-Administratoren verwaltet werden. Sicherheitsrichtlinien können die Weitergabe von Unternehmensdaten steuern, ohne persönliche Apps zu beeinträchtigen. Die Architektur schützt Geschäftsdaten selbst dann, wenn persönliche Anwendungen kompromittiert werden.

Apple iPhone MDM und

automatisierte Registrierung

Apples MDM-Framework ermöglicht die zentralisierte Verwaltung von iPhones in Unternehmensumgebungen. In Kombination mit dem Apple Business Manager können sich Geräte bei der ersten Aktivierung automatisch registrieren und konfigurieren. Administratoren können Unternehmens-Apps lautlos bereitstellen und konfigurieren, Sicherheitseinstellungen erzwingen und die Konformität überwachen. Diese Automatisierung gewährleistet eine konsistente Gerätekonfiguration und reduziert Konfigurationsfehler.

Mobile Device Management

verstehen

Mobile Device Management bietet eine zentralisierte Plattform zur Überwachung, Sicherung und Steuerung von mobilen Geräten, die auf Unternehmenssysteme zugreifen. Zu den Kernfunktionen gehören das Durchsetzen von Sicherheitsrichtlinien, die Verwaltung von Anwendungen sowie das Remote-Sperren oder Löschen verlorener Geräte. MDM hilft dabei, Unternehmensdaten zu schützen und gleichzeitig die Gerätekonformität aufrechtzuerhalten. Es ermöglicht Organisationen

jeder Größe, eine wachsende mobile Belegschaft sicher zu verwalten.

Bereitstellungsmodelle für Unternehmensgeräte

Organisationen können verschiedene Besitzmodelle für Geräte wie BYOD, CYOD, COPE, COBO und COSU übernehmen. Jedes Modell balanciert Kosten, Flexibilität für den Nutzer und Sicherheitskontrolle auf unterschiedliche Weise. BYOD priorisiert den Komfort der Nutzer, während COBO und COSU die unternehmensweite Kontrolle und Sicherheit maximieren. Die Wahl des richtigen Modells hängt von regulatorischen Anforderungen, den Bedürfnissen der Belegschaft und der IT-Managementkapazität ab.

MDM vs. EMM vs. UEM

MDM konzentriert sich auf die Verwaltung und Sicherung mobiler Geräte durch das Durchsetzen von Richtlinien, Konfigurationskontrolle und Fernverwaltung. EMM erweitert diesen Umfang um die Verwaltung von Anwendungen und Inhalten, während UEM versucht, alle Endpunkte einschließlich Laptops und Desktops zu verwalten. Für viele KMU führen vollständige EMM- oder UEM-Suites zu unnötiger Komplexität. In der Praxis decken robuste MDM-Funktionen oft die meisten Anforderungen des mobilen Managements ab.

MDM auf privaten Telefonen und der Datenschutz der Mitarbeiter

Moderne MDM-Systeme nutzen Containerisierung, um geschäftliche und private Daten auf im Besitz der Mitarbeiter befindlichen Geräten zu trennen. Arbeitgeber können nur die Arbeitsumgebung verwalten und überwachen, einschließlich Unternehmens-Apps und Informationen zur Gerätekonformität. Private Daten wie Fotos, Nachrichten und der Browserverlauf bleiben für das Unternehmen unzugänglich. Diese technische Trennung ermöglicht sichere BYOD-Programme bei gleichzeitigem Schutz der Privatsphäre der Mitarbeiter.

MDM-ROI und geschäftlicher

Mehrwert

MDM sollte als strategische Investition und nicht nur als einfacher Sicherheitsaufwand bewertet werden. Es generiert finanzielle Erträge durch verringerten Geräteverlust, niedrigere IT-Supportkosten und verbesserte betriebliche Effizienz. Automatisiertes Management steigert zudem die Produktivität der Mitarbeiter und reduziert Ausfallzeiten. Darüber hinaus verringert eine stärkere Sicherheit das Risiko und die finanziellen Auswirkungen von Datenschutzverletzungen.

HIPAA-konformes

Gerätemanagement

Organisationen im Gesundheitswesen müssen elektronische Patientendaten gemäß den HIPAA-Sicherheitsanforderungen schützen. MDM hilft bei der Durchsetzung von Verschlüsselung, Authentifizierungskontrollen, sicherer Datenübertragung und detaillierten Audit-Protokollen. Es ermöglicht zudem das Löschen aus der Ferne sowie die zentralisierte Durchsetzung von Richtlinien für Geräte, die auf medizinische Systeme zugreifen. Diese Kontrollen reduzieren Compliance-Risiken und ermöglichen gleichzeitig mobile Arbeitsabläufe im Gesundheitswesen.

MDM für den Einzelhandel: Betrieb und Sicherheit

Einzelhandelsunternehmen sind für Kassensysteme (POS), Bestandsmanagement und In-Store-Abläufe auf mobile Geräte angewiesen. MDM stellt sicher, dass diese Geräte sicher, aktuell und konform mit Standards wie PCI-DSS bleiben. Eine zentralisierte Verwaltung reduziert Ausfallzeiten und vereinfacht die Bereitstellung von Geräten an mehreren Standorten. Das Ergebnis sind eine verbesserte betriebliche Effizienz und ein verringertes Risiko für sicherheitsrelevante Vorfälle im Zahlungsverkehr.