Gerätebereitstellung - Android

- Unterstützte Geräte
- Registrierungstoken
- Persönliche Geräte
- Unternehmenseigene Geräte für berufliche und private Nutzung
- Unternehmenseigene Geräte nur für berufliche Nutzung
- Zero-touch
- Authenticate Using Google enrollment

Unterstützte Geräte

Im Allgemeinen ist jedes Gerät mit Android 6+ und Google Play Services mit Cerberus Enterprise kompatibel.

Für eine bessere Benutzererfahrung empfehlen wir Geräte, die die Anforderungen von Android Enterprise Recommended erfüllen.

> Einige Funktionen sind auf bestimmte Android-Versionen beschränkt oder können sich je nach Betriebssystemversion unterschiedlich verhalten. Weitere Informationen zu einer bestimmten Funktion finden Sie im Abschnitt Richtlinien der Dokumentation.

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

Persönliche Geräte können über ein **Arbeitsprofil** verwaltet werden. Dies ermöglicht eine BYOD-Lösung, indem die beruflichen Daten und Apps der Mitarbeiter von persönlichen Daten und Apps getrennt bleiben, was sowohl Sicherheit als auch Datenschutz verbessert. Diese Option eignet sich für Geräte, die bereits Mitarbeitern gehören und die Sie für die berufliche Nutzung in Ihrer Organisation registrieren möchten.

Unternehmenseigene Geräte können ebenfalls über ein Arbeitsprofil verwaltet werden, Sie können aber auch die Option **vollständig verwaltet** wählen, die eine strengere Kontrolle über das Gerät ermöglicht. Unternehmenseigene Geräte mit einem Arbeitsprofil eignen sich, wenn Sie Mitarbeitern Unternehmensgeräte für die Arbeit bereitstellen und gleichzeitig die private Nutzung erlauben möchten. Vollständig verwaltete Geräte eignen sich besser für Geräte, die nur für die Arbeit verwendet werden dürfen, oder für **dedizierte Geräte** (COSU, Corporate-Owned Single-Use), wie z. B. Kioske.

Weitere Informationen zur Gerätebereitstellung finden Sie auf der Seite Überblick über die Gerätebereitstellung.

Registrierungstoken

Cerberus Enterprise verwendet Registrierungstoken, um den Registrierungsprozess (die Bereitstellung) für Android-Geräte zu starten. Das ausgewählte Token definiert die anfängliche Richtlinie, die auf registrierte Geräte angewendet wird, und beeinflusst, welche Bereitstellungsmodi zulässig sind.

> Die Registerkarte für Android-Registrierungstoken ist erst nach Abschluss der **Android Management-Einrichtung** verfügbar.

Wo Sie Registrierungstoken finden

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

> Wenn Ihr Android-Unternehmen durch eine verwaltete Google-Domain (Google Workspace) unterstützt wird, kann das Dashboard zusätzlich eine Registerkarte **Authenticate Using Google Enrollment** anzeigen. Einzelheiten zum Aktivieren und Verwenden finden Sie unter **Authenticate Using Google enrollment**.

Liste der Registrierungstoken (Android)

Die Registerkarte „Android-Token“ zeigt eine Tabelle aller Token. Ein Klick auf eine Zeile öffnet die Seite mit den Token-Details.

Spalten

- **Status**: **Aktiv** (Geräte können sich mit dem Token registrieren), **Abgelaufen** (das Ablaufdatum ist überschritten) oder **Aufgebraucht** (ein Einmal-Token, das bereits

verwendet wurde).

- **Richtlinie**: die dem Token zugewiesene Richtlinie (der Tooltip zeigt die Richtlinien-ID). **Richtlinie gelöscht** bedeutet, dass die Richtlinie gelöscht wurde, nachdem das Token erstellt wurde.
- **Benutzer**: optionaler Benutzer, der Geräten vorab zugewiesen wird, die sich mit dem Token registrieren. **Benutzer gelöscht** bedeutet, dass der Benutzer gelöscht wurde, nachdem das Token erstellt wurde.
- **Registrierungen**: wie viele Geräte sich mit dem Token registriert haben, angezeigt als **n / 1** für ein Einmal-Token.
- **Persönliche Nutzung**: Zulässig / Nicht zulässig / Dediziertes Gerät.
- **Erstellt**: wann das Token erstellt wurde. Die Tabelle zeigt die neuesten Tokens zuerst.
- **Ablauf**: Ablaufdatum/-uhrzeit oder **Nie**.
- **Registrierungscode**: der Code des Tokens, den Sie auf dem Gerät eingeben, wenn Sie es ohne QR-Code registrieren.

Aktionen

- Jede Zeile hat eine Löschaktion (**Registrierungstoken löschen**). Das Löschen ist deaktiviert, wenn die Lizenz abgelaufen ist.
- Die Tabelle unterstützt die Mehrfachauswahl: Sie können den Auswahlmodus aktivieren, mehrere Token auswählen und sie 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 auf der Registerkarte „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, die automatisch auf alle Geräte angewendet wird, die mit diesem Token registriert werden. Wählen Sie eine Ihrer **Android-Richtlinien** aus. Wenn Sie noch keine Richtlinie haben, erstellen Sie zuerst eine.

2. Benutzer

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

3. Persönliche Nutzung

Legt fest, ob die persönliche Nutzung auf einem Gerät zulässig ist, das mit diesem Registrierungstoken bereitgestellt wird:

- **Zulässig**: geeignet für persönliche Geräte (Arbeitsprofil) und unternehmenseigene Geräte für berufliche und private Nutzung.
- **Nicht zulässig**: geeignet für unternehmenseigene Geräte nur für berufliche Nutzung (vollständig verwaltet).
- **Dediziertes Gerät**: geeignet für Kiosk-/dedizierte Geräte (das Gerät ist keinem einzelnen Benutzer zugeordnet).

4. Zulässige Verwendungen

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

5. Ablauf

Wählen Sie die Ablaufeinheit (**Minuten**, **Stunden**, **Tage** oder **Nie**). Wenn nicht auf Nie gesetzt, 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

Legt fest, ob der Benutzer sich während der Geräteregistrierung mit einem Google-Konto authentifizieren muss:

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

Wenn **Erforderlich** ausgewählt ist, wird ein optionales Feld **E-Mail-Adresse des erforderlichen Kontos** angezeigt. Wenn festgelegt, muss sich der Benutzer während der Registrierung mit genau diesem Google-Konto authentifizieren.

Bereitstellungsoptionen (nur QR-Code)

Diese zusätzlichen Optionen werden in den QR-Code eingebettet und 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 das Token registriert werden.

Wi-Fi-Konfiguration

Verwenden Sie diese Option, damit ein Gerät während der Bereitstellung automatisch eine Verbindung zu Wi-Fi herstellt, sodass es die Verwaltungs-App herunterladen und initialisieren kann. Verfügbare Felder sind **SSID**, **Ausgeblendete SSID**, **Sicherheit** und (bei Bedarf) **Passphrase**.

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

Weitere Optionen

Weitere Optionen sind **Gebietsschema**, **Zeitzone** und **Verschlüsselung überspringen**.

Details zum Registrierungstoken

Wenn Sie ein Token öffnen, zeigt die Detailseite die Token-Konfiguration und Nutzungsinformationen an:

- **Status**, **Ablauf**, **Nutzung**, **Persönliche Nutzung**, **Zulässige Verwendungen** und (falls festgelegt) **Google-Authentifizierung** mit der optionalen **E-Mail-Adresse des erforderlichen Kontos**.
- **Token**: der Rohwert des Registrierungstokens (kopierbar).
- **Registrierungs-URL**: eine Registrierungs-URL für Google Android Enterprise (kopierbar und per E-Mail sendbar).
- **QR-Code**: wird auf der rechten Seite der Seite angezeigt und dient zur Registrierung vollständig verwalteter Geräte.

> Schritt-für-Schritt-Anleitungen zur Bereitstellung finden Sie in den Android-Registrierungsleitfäden: **Persönliche Geräte**, **Unternehmenseigene Geräte für berufliche und private Nutzung**, **Unternehmenseigene Geräte nur für berufliche Nutzung** und **Zero-touch**.

Persönliche Geräte

Geräte von Mitarbeitern können mit einem **Arbeitsprofil** eingerichtet werden. Ein Arbeitsprofil bietet einen eigenständigen Bereich für berufliche Apps und Daten, getrennt von persönlichen Apps und Daten. Die meisten App-, Daten- und anderen Verwaltungsrichtlinien gelten nur für das Arbeitsprofil, während die persönlichen Apps und Daten der Mitarbeiter privat bleiben.
Um ein Arbeitsprofil auf einem persönlichen Gerät einzurichten, verwenden Sie eine der folgenden Bereitstellungsmethoden (stellen Sie sicher, dass beim Registrierungstoken ***Persönliche Nutzung*** auf **Zulässig** gesetzt ist):

Link zum Registrierungstoken

Android-Version
6.0+

Sie können den Endbenutzern die Registrierungs-URL bereitstellen. Wenn ein Endbenutzer den Link von seinem Gerät aus öffnet, wird er durch die Einrichtung des Arbeitsprofils geführt.

Arbeitsprofil aus *„Einstellungen“* hinzufügen

Android-Version
6.0+

Um ein Arbeitsprofil auf ihrem Gerät einzurichten, kann ein Benutzer die App ***Einstellungen*** öffnen und dann über die Suchleiste die Option ***Arbeitsprofil einrichten*** suchen und antippen.

Wenn die Suche erfolglos bleibt, kann der Speicherort 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 *Android Device Policy* auf dem Gerät herunterlädt. Anschließend wird der Benutzer aufgefordert, einen QR-Code zu scannen oder manuell ein 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 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 ein Registrierungstoken einzugeben, um die Einrichtung des Arbeitsprofils abzuschließen.

Persönliche iPhones und iPads

Private iPhones und iPads (und Macs) registrieren sich mit Apples **Benutzerregistrierung**: Der Benutzer meldet sich mit seinem Managed Apple Account in den Geräteeinstellungen an, und nur die Arbeits-Apps, Konten und Daten werden verwaltet. Auf iPhones und iPads werden die App Store-Apps der Richtlinie und die **Cerberus Enterprise**-App mit einer Benutzerlizenz dieses Kontos installiert. Der Standort privater Geräte wird nur erfasst, wenn ihre Richtlinie **Standort und Geofences auf privaten Geräten** aktiviert und der Benutzer es zulässt. Lesen Sie **Apple-kontogesteuerte Registrierung**.

Unternehmenseigene Geräte für berufliche und private Nutzung

Das Einrichten eines unternehmenseigenen Geräts mit einem **Arbeitsprofil** ermöglicht die Nutzung des Geräts sowohl beruflich als auch privat. Auf unternehmenseigenen Geräten mit Arbeitsprofilen:

- Die meisten App-, Daten- und anderen Verwaltungsrichtlinien gelten nur für das Arbeitsprofil.
- Die persönlichen Profile der Mitarbeiter bleiben privat. Unternehmen können jedoch bestimmte geräteweite Richtlinien und Richtlinien zur privaten Nutzung durchsetzen.
- Unternehmen können *Block scope* verwenden, um Compliance-Aktionen für ein gesamtes Gerät oder nur für dessen Arbeitsprofil durchzusetzen.
- Das Aufheben der Geräteregistrierung und Gerätebefehle gelten für ein gesamtes Gerät.

Um ein unternehmenseigenes Gerät mit einem Arbeitsprofil einzurichten, verwenden Sie eine der folgenden Bereitstellungsmethoden (stellen Sie sicher, dass beim Registrierungstoken **Persönliche Nutzung** auf **Zulässig** gesetzt ist):

QR-Code-Methode

Android-Version
8.0+

Auf einem neuen oder auf die Werkseinstellungen zurückgesetzten Gerät tippt der Benutzer (in der Regel ein IT-Administrator) sechsmal an dieselbe Stelle auf dem Bildschirm. Dadurch fordert das Gerät den Benutzer auf, einen QR-Code zu scannen.

Unternehmenseigene Geräte nur für berufliche Nutzung

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

QR-Code-Methode

Android-Version
7.0+

Auf einem neuen oder auf die Werkseinstellungen zurückgesetzten Gerät tippt der Benutzer (in der Regel ein IT-Administrator) sechsmal an dieselbe Stelle auf dem Bildschirm. Dadurch fordert das Gerät den Benutzer auf, einen QR-Code zu scannen.

Methode mit DPC-Kennung

Android-Version
5.1+

Wenn Android Device Policy nicht per 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 die Werkseinstellungen zurückgesetzten Gerät.
2. Geben Sie die Wi-Fi-Anmeldedaten ein, um das Gerät mit dem Internet zu verbinden.
3. Wenn Sie zur Anmeldung aufgefordert werden, geben Sie **afw#setup** ein, wodurch 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 mit der Zero-touch-Registrierungsmethode bereitstellen, die unter Zero-touch-Registrierung für IT-Administratoren beschrieben wird. Wenn ein Gerät zum ersten Mal eingeschaltet wird, wird es automatisch gezwungen, die vom IT-Administrator definierten Einstellungen zu übernehmen.

IT-Administratoren können Geräte vorkonfigurieren, die bei autorisierten Wiederverkäufern gekauft wurden, und sie über das Cerberus Enterprise Dashboard verwalten. Um Ihr Zero-touch-Konto zu verknüpfen, wechseln Sie im Dashboard zum Bereich **Zero-touch** und folgen Sie den Anweisungen.

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

Authenticate Using Google enrollment

Authenticate Using Google enrollment (auch als **Google Authentication for Enrollment** bezeichnet) ermöglicht Benutzern, sich während der Android-Geräteregistrierung mit ihrem Google Workspace-Konto zu authentifizieren.

> Diese Funktion ist nur für Android-Unternehmen verfügbar, die durch eine verwaltete Google-Domain (Google Workspace) unterstützt werden.

Wo Sie die Funktion finden

Öffnen Sie im Dashboard **Registrierungstoken** und wählen Sie die Registerkarte **Authenticate Using Google Enrollment** aus. Die Registerkarte wird nur angezeigt, wenn Android Management konfiguriert ist und die Google Workspace-Integration für Ihr Unternehmen verfügbar ist.

Google-Authentifizierung aktivieren (oder deaktivieren)

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

1. Melden Sie sich mit einem Administratorkonto bei der **Google Admin Console** an.
2. Öffnen Sie **Geräte**.
3. Wechseln Sie zu **Mobilgeräte & Endpunkte → Einstellungen → Integrationen von Drittanbietern**.
4. Suchen Sie die **Android EMM-Integration** für Cerberus Enterprise und öffnen Sie sie.
5. Klicken Sie auf **EMM-Anbieter verwalten**.
6. Schalten Sie **Authenticate Using 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 auf **Status aktualisieren** auf der Registerkarte **Authenticate Using Google Enrollment**.

Registrierungstoken für die Google-Authentifizierung

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

Wichtige Optionen

- **Persönliche Nutzung zulassen**: legt fest, ob das Token Geräte für berufliche und private Nutzung (Arbeitsprofilszenarien) oder nur für berufliche Nutzung (vollständig verwaltete/dedizierte Szenarien) registrieren kann.
- **Fallback-Standardrichtlinie**: die Richtlinie, die angewendet wird, wenn dem registrierenden Benutzer keine spezifische Standardrichtlinie für die Google-Authentifizierung zugewiesen ist.

Zusammenspiel mit Richtlinien

Die Richtlinieneinstellung **Authentifizierung bei der Einrichtung des Arbeitskontos** (workAccountSetupConfig.authenticationType) legt fest, wie sich Benutzer bei der Einrichtung des Arbeitskontos authentifizieren, aber die Einstellung **Authenticate Using Google** in der Google Admin Console und der Typ des Registrierungstokens können weiterhin eine Authentifizierung erfordern.

Bei bereits registrierten Geräten gilt diese Richtlinie nur, wenn das Gerät von einem verwalteten Google Play-Konto verwaltet wird (d. h. ohne **Authenticate Using Google Enrollment** registriert wurde).

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

Gerät registrieren

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

Arbeitsprofil (persönliche Geräte)

- Teilen Sie die **Registrierungs-URL** mit dem Benutzer. Wenn der Benutzer sie auf seinem Android-Gerät öffnet, wird er durch die Einrichtung des Arbeitsprofils und die Google-Authentifizierung geführt.
- Alternativ kann der Benutzer in den Android-Einstellungen beginnen und den Einrichtungsablauf für das Arbeitsprofil wählen und dann den QR-Code scannen oder das Registrierungstoken eingeben, wenn er dazu aufgefordert wird.

Unternehmenseigene Geräte

- **QR-Code-Methode**: Tippen Sie auf einem neuen oder auf die Werkseinstellungen zurückgesetzten Gerät mehrmals an dieselbe Stelle, bis die QR-Code-Aufforderung erscheint, und scannen Sie dann den im Dashboard angezeigten QR-Code.
- **Methode mit DPC-Kennung** (wenn das Scannen von QR-Codes nicht verfügbar ist): Folgen Sie dem Einrichtungsassistenten, stellen Sie eine Verbindung zu Wi-Fi her, und geben Sie dann, wenn Sie zur Anmeldung aufgefordert werden, **afw#setup** ein, und fahren Sie fort, indem Sie den QR-Code scannen oder das Registrierungstoken eingeben. Wenn Sie dazu aufgefordert werden, authentifizieren Sie sich mit dem Google Workspace-Konto.

Allgemeine Android-Bereitstellungsverfahren (Arbeitsprofil vs. vollständig verwaltet) finden Sie auf den Standardseiten zur Android-Registrierung in diesem Handbuch.