Gerätebereitstellung - Android

Unterstützte Geräte

Im Allgemeinen sind alle Geräte mit Android 6 oder höher und Google Play Services mit Cerberus Enterprise kompatibel.

Für eine bessere Benutzererfahrung empfehlen wir die Verwendung von Geräten, die die Anforderungen von Android Enterprise 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 von Unternehmen gestellte als auch privat genutzte Geräte und zwei Verwaltungsmodi: Gerätebesitzer und Profilbesitzer.

Privat genutzte Geräte können über ein **Arbeitsprofil** verwaltet werden. Dies ermöglicht eine BYOD-Lösung, indem die Arbeitsdaten und -anwendungen der Mitarbeiter von persönlichen Daten und -anwendungen getrennt gehalten werden, was sowohl die Sicherheit als auch den Datenschutz verbessert. Diese Option ist geeignet für Geräte, die bereits im Besitz von Mitarbeitern sind und die Sie für den geschäftlichen Gebrauch in Ihre Organisation einbinden möchten.

Firmenbesessene Geräte können ebenfalls über ein Arbeitsprofil verwaltet werden, aber Sie können auch die **vollständig verwaltete** Option wählen, die eine strengere Kontrolle über das Gerät ermöglicht. Firmenbesessene Geräte mit einem Arbeitsprofil sind geeignet, wenn Sie Mitarbeitern Unternehmensgeräte für die Arbeit zur Verfügung stellen, während gleichzeitig eine private Nutzung erlaubt wird. Vollständig verwaltete Geräte eignen sich besser für Geräte, die ausschließlich für geschäftliche Zwecke verwendet werden müssen, oder für **dedizierte Geräte** (COSU, corporate-owned single-use), wie z. B. Terminals.

Weitere Informationen zur Gerätebereitstellung finden Sie auf der Seite "Gerätebereitstellung" .

Enrollment-Token

Cerberus Enterprise verwendet Enrollment-Token, um den Android-Geräte-Registrierungsprozess (Provisionierung) zu starten. Das von Ihnen ausgewählte Token bestimmt die anfängliche Richtlinie, die auf registrierte Geräte angewendet wird, und beeinflusst, welche Bereitstellungsmodi zulässig sind.

> Der Tab "Android-Registrierungstoken" ist nur verfügbar, nachdem Sie die **Android Management setup** abgeschlossen haben.

Wo finde ich die Anmelde-Token?

Im Dashboard öffnen Sie **Anmelde-Token**. Je nach Konfiguration Ihres Kontos können auf der Seite mehrere Reiter angezeigt werden (Android-Token, Google-Sign-in-Anmeldung, manuelle Apple-Anmeldung und automatisierte Apple-Geräteanmeldung).

> Wenn Ihr Android Enterprise von einer verwalteten Google-Domain (Google Workspace) unterstützt wird, kann das Dashboard auch einen Reiter "**Authentifizierung mit Google-Anmeldung**" anzeigen. Für Details zur Aktivierung und Verwendung finden Sie weitere Informationen unter **Authentifizierung mit Google-Anmeldung**.

Liste der Anmelde-Token (Android)

Der Tab "Android-Token" zeigt eine Tabelle aller Token. Durch Klicken auf eine Zeile wird die Detailseite des Tokens geöffnet.

Spalten

- **ID**: interner Token-Identifikator.
- **Status**: **Verfügbar**, **Verwendet** (Einmal-Token bereits verwendet) oder **Abgelaufen**.
- **Ablaufdatum**: Ablaufdatum und -uhrzeit oder **niemals**.
- **Richtlinie**: Die dem Token zugewiesene Richtlinie (der UI-Tooltipp zeigt ebenfalls die Richtlinien-ID).
- **Private Nutzung**: Erlaubt / Nicht erlaubt / Exklusives Gerät.
- **Erlaubte Nutzung**: Mehrfach oder nur einmalig.

- **Benutzer**: Optionaler Benutzer, der Geräten zugewiesen werden kann, die mit einem Token registriert wurden.

Aktionen

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

Erstellen Sie einen neuen Registrierungstoken

Im Tab "Android-Token" klicken Sie auf **Neuen Registrierungstoken erstellen**, um die Seite zur Token-Erstellung zu öffnen. Wenn Ihre Lizenz abgelaufen ist, ist die Schaltfläche "Erstellen" deaktiviert.

Token-Optionen

1. Richtlinie

Erforderlich. Die Richtlinie wird automatisch auf alle Geräte angewendet, die mit diesem Token registriert wurden. Wählen Sie eine Ihrer **Android-Richtlinien**. Wenn Sie noch keine Richtlinie haben, erstellen Sie zuerst eine.

2. Benutzer

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

3. Persönliche Nutzung

Legt fest, ob die persönliche Nutzung auf einem Gerät erlaubt ist, das mit diesem Anmelde-Token konfiguriert wurde:

- **Erlaubt**: Geeignet für privat genutzte Geräte (Arbeitsprofil) und firmeneigene Geräte für geschäftliche und private Nutzung.
- **Nicht erlaubt**: Geeignet für firmeneigene Geräte, die ausschließlich für geschäftliche Zwecke verwendet werden (vollständig verwaltet).

- **Dediziertes Gerät**: Geeignet für Kiosk- oder spezielle Geräte (das Gerät ist nicht mit einem einzelnen Benutzer verknüpft).

4. Erlaubte Nutzungsmöglichkeiten

Wählen Sie, ob das Token mehrfach (**mehrmals**) oder nur einmal (**nur einmal**) verwendet werden darf.

5. Ablaufdatum

Wählen Sie die Einheit für das Ablaufdatum (**Minuten**, **Stunden**, **Tage** oder **Nie**). Wenn kein Wert für "Nie" ausgewählt wurde, geben Sie den Ablaufwert ein. Der zulässige Bereich hängt von der ausgewählten Einheit ab und kann bis zu 10.000 Tage betragen.

Optionen für die Gerätebereitstellung (nur QR-Code)

Diese zusätzlichen Optionen sind im QR-Code enthalten und werden während der Bereitstellung von vollständig verwalteten Geräten angewendet, die durch Scannen des QR-Codes registriert wurden. Sie gelten nicht für Arbeitsprofile oder Geräte, die mit der Registrierungs-URL oder dem Token registriert wurden.

Wi-Fi-Konfiguration

Verwenden Sie dies, um ein Gerät automatisch mit einem Wi-Fi-Netzwerk während der Einrichtung zu verbinden, sodass es die Verwaltungs-App herunterladen und initialisieren kann. Verfügbare Felder sind **SSID**, **Versteckter SSID**, **Sicherheit** und (falls erforderlich) **Passphrase**.

Sie können auch einen HTTP-Proxy (**Proxy**) konfigurieren und, abhängig vom Modus, **Host**/**Port**, **PAC-URI** und **Host für die Proxy-Umgehung** festlegen.

Andere Optionen

Weitere Optionen umfassen **die Ländereinstellung**, **die Zeitzone** und **die Option, die Verschlüsselung zu überspringen**.

Details zum Anmelde-Token

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

- **Status**, **Ablaufdatum**, **Verwendung**, **Persönliche Nutzung**, und **Erlaubte Nutzungen**.
- **Token**: Der Rohwert des Anmelde-Tokens (kopiermöglich).

- **Anmelde-URL**: Eine Google Android Enterprise Anmelde-URL (zum Kopieren und Versenden per E-Mail).
- **QR-Code**: Wird auf der rechten Seite der Seite angezeigt und dient zur Registrierung von Geräten mit vollständiger Verwaltung.

> Für detaillierte Anleitungen zur Gerätekonfiguration, folgen Sie den Android-Einrichtungsrichtlinien: **Privatgeräte**, **Firmenbesitzene Geräte für Arbeit und Privat**, **Firmenbesitzene Geräte nur für den beruflichen Gebrauch**, und **Zero-Touch**.

Geräte, die von Privatpersonen genutzt werden

Geräte, die von Mitarbeitern genutzt werden, können mit einem **Arbeitsprofil** konfiguriert werden. Ein Arbeitsprofil bietet eine separate Umgebung für Arbeitsanwendungen und -daten, getrennt von persönlichen Anwendungen und Daten. Die meisten Richtlinien für Anwendungen, Daten und andere Verwaltungsfunktionen gelten nur für das Arbeitsprofil, während die persönlichen Anwendungen und Daten der Mitarbeiter privat bleiben.
Um ein Arbeitsprofil auf einem persönlich genutzten Gerät einzurichten, verwenden Sie eine der folgenden Bereitstellungsmethoden (stellen Sie sicher, dass das Einschreibungs-Token auf ***Privatnutzung*** gesetzt ist auf **Erlaubt**):

Link zum Registrierungstoken

Android-Version
6.0+

Sie können die Enrollment-URL den Endbenutzern zur Verfügung stellen. Wenn ein Endbenutzer den Link auf ihrem Gerät öffnet, wird er durch die Einrichtung des Arbeitsbereichs geführt.

Fügen Sie ein Arbeitsprofil von *"Einstellungen"*

Android-Version
6.0+

Um ein Arbeitsbereichsprofil auf ihrem Gerät einzurichten, kann ein Benutzer:

1. Gehen Sie zu *Einstellungen > Google > Einrichten & Wiederherstellen*.
2. Tippen Sie auf "*Ihr Arbeitsprofil einrichten*".

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

Laden Sie die Android-Geräteeinstellungen herunter

Android-Version
6.0+

Um ein Arbeitskonto auf ihrem Gerät einzurichten, kann ein Benutzer die App „Android-Geräteeinstellungen“ aus dem Google Play Store herunterladen. Nach der Installation der App wird der Benutzer aufgefordert, einen QR-Code zu scannen oder einen Aktivierungscode manuell einzugeben, um die Einrichtung des Arbeitskontos abzuschließen.

Geräte, die dem Unternehmen gehören und sowohl für die Arbeit als auch für den persönlichen Gebrauch bestimmt sind

Die Einrichtung eines vom Unternehmen bereitgestellten Geräts mit einem **Arbeitsprofil** ermöglicht die Nutzung des Geräts sowohl für geschäftliche als auch für private Zwecke. Bei Geräten, die vom Unternehmen bereitgestellt werden und über ein Arbeitsprofil verfügen:

- Die meisten Richtlinien für Apps, Daten und andere Einstellungen gelten nur für das Arbeitsprofil.
- Die persönlichen Profile der Mitarbeiter bleiben privat. Unternehmen können jedoch bestimmte geräteweite Richtlinien und Nutzungsrichtlinien für private Zwecke durchsetzen.
- Unternehmen können die *Block-Funktion* verwenden, um Compliance-Aktionen für ein gesamtes Gerät oder nur für dessen Arbeitsbereich durchzusetzen.
- Die Geräteabmeldung und die Gerätebefehle gelten für das gesamte Gerät.

Um ein unternehmenseigenes Gerät mit einem Arbeitsbereich einzurichten, verwenden Sie eine der folgenden Bereitstellungsmethoden (stellen Sie sicher, dass das Anmeldetoken die Option **Persönliche Nutzung** auf **Erlaubt** eingestellt hat):

Methode mit QR-Code

Android-Version
8.0+

Bei einem neuen oder auf Werkseinstellungen zurückgesetzten Gerät tippt der Benutzer (in der Regel ein IT-Administrator) sechs Mal an derselben Stelle auf den Bildschirm. Dadurch wird das Gerät dazu veranlasst, den Benutzer aufzufordern, einen QR-Code zu scannen.

Geräte, die dem Unternehmen gehören und ausschließlich für geschäftliche Zwecke bestimmt sind

Die vollständige Geräteverwaltung ist für geräte geeignet, die dem Unternehmen gehören und ausschließlich für geschäftliche Zwecke bestimmt sind. Unternehmen können alle Apps auf dem Gerät verwalten und die gesamte Bandbreite 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 Auswahl von Apps zu beschränken, um einen bestimmten Zweck oder eine bestimmte Anwendung zu erfüllen. Diese Teilmenge der vollständig verwalteten Geräte wird als **dedizierte Geräte** bezeichnet.
Um eine vollständige Verwaltung auf einem vom Unternehmen bereitgestellten Gerät einzurichten, verwenden Sie eine der folgenden Bereitstellungsmethoden (stellen Sie sicher, dass der Anmeldetoken die Option **Privatnutzung** auf **nicht erlaubt** gesetzt hat):

Methode mit QR-Code

Android-Version
7.0+

Bei einem neuen oder auf Werkseinstellungen zurückgesetzten Gerät tippt der Benutzer (in der Regel ein IT-Administrator) sechs Mal an derselben Stelle auf den Bildschirm. Dadurch wird das Gerät dazu veranlasst, den Benutzer aufzufordern, einen QR-Code zu scannen.

Methode zur Identifizierung des Geräteverwaltungsprofils

Android-Version
5.1+

Wenn das Android-Geräteverwaltungsprofil nicht über einen QR-Code hinzugefügt werden kann, kann ein Benutzer oder ein IT-Administrator diese Schritte ausführen, um ein vollständig verwaltetes oder ein dediziertes Gerät einzurichten:

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

3. Wenn Sie aufgefordert werden, sich anzumelden, geben Sie **afw#setup** ein, wodurch die Android-Gerätedirigierungsrichtlinie heruntergeladen wird.
4. Scannen Sie einen QR-Code oder geben Sie einen Enrollment-Token manuell ein, um das Gerät zu registrieren.

Null-Konfiguration

IT-Administratoren können firmeneigene Geräte mit der Methode der "Zero-Touch"-Registrierung bereitstellen, die in "Zero-Touch"-Registrierung für IT-Administratoren beschrieben ist. Beim ersten Einschalten des Geräts wird dieses automatisch in die vom IT-Administrator definierten Einstellungen versetzt.

IT-Administratoren können Geräte, die von autorisierten Händlern erworben wurden, vorkonfigurieren und mit dem Cerberus Enterprise Dashboard verwalten. Um Ihr Zero-Touch-Konto zu verknüpfen, gehen Sie zum **Zero-Touch**-Bereich im Dashboard und befolgen Sie dann die Anweisungen.

Android-Version	Arbeitsbereich	Vollständig verwaltetes Gerät	Exklusiv zugewiesenes Gerät
8.0+ (Pixel 7.1+)	✓	✓	✓

Authentifizieren Sie mit der Google-Anmeldung

Authentifizieren Sie mit der Google-Anmeldung (auch bekannt als **Google-Authentifizierung für die Anmeldung**), die es Benutzern ermöglicht, sich mit ihrem Google Workspace-Konto während der Android-Geräteanmeldung zu authentifizieren.

> Diese Funktion ist nur für Android-Geräte verfügbar, die in einer verwalteten Google-Domäne (Google Workspace) registriert sind.

Wo finde ich das?

Im Dashboard öffnen Sie **Enrollment-Token** und wählen Sie den Reiter **Authentifizierung mit Google Enrollment**. Der Reiter wird nur angezeigt, wenn Android Management konfiguriert ist und die Google Workspace-Integration für Ihr Unternehmen verfügbar ist.

Aktivieren (oder deaktivieren) Sie die Google-Authentifizierung

Die Google-Authentifizierung ist über die **Google Admin-Konsole** aktiviert. Nachdem Sie die Einstellung geändert haben, kehren Sie zu Cerberus Enterprise zurück und verwenden Sie **Status aktualisieren**, um die aktuelle Konfiguration neu zu laden.

1. Melden Sie sich mit einem Administrator-Konto in Ihrer **Google Admin-Konsole** an.
2. Öffnen Sie **Geräte**.
3. Gehen Sie zu **Mobile Geräte und Endpunkte → Einstellungen → Integrationen von Drittanbietern**.
4. Finden Sie die **Android EMM-Integration** für Cerberus Enterprise und öffnen Sie diese.
5. Klicken Sie auf **Verwalten von EMM-Anbietern**.
6. Aktivieren Sie **Authentifizierung mit Google**, um die Google-Authentifizierung für die Anmeldung zu aktivieren oder zu deaktivieren.
7. Klicken Sie auf **Speichern**.
8. Gehen Sie zurück zum Cerberus Enterprise-Dashboard und klicken Sie auf **Status aktualisieren** im Reiter **Authentifizierung mit Google-Registrierung**.

Google-Authentifizierungs-Registrierungstoken

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

Wichtige Optionen

- **Persönliche Nutzung zulassen**: Steuert, ob das Token Geräte sowohl für geschäftliche als auch für private Zwecke (Work-Profile-Szenarien) oder nur für geschäftliche Zwecke (vollständig verwaltete/dedizierte Szenarien) registrieren kann.
- **Fallback-Standardrichtlinie**: Die Richtlinie, die angewendet wird, wenn dem Benutzer, der das Gerät registriert, keine spezifische Google-Authentifizierungs-Standardrichtlinie zugewiesen ist.

Richtlinien-Interaktion

Die Richtlinieneinstellung **Authentifizierung bei der Einrichtung des Arbeitskontos** (workAccountSetupConfig.authenticationType) steuert, wie Benutzer während der Einrichtung des Arbeitskontos authentifiziert werden, aber die Einstellung in der Google Admin-Konsole **Authentifizierung mit Google** und der Typ des Anmelde-Tokens können dennoch eine Authentifizierung erfordern.

Für Geräte, die bereits registriert sind, gilt diese Richtlinie nur, wenn das Gerät mit einem verwalteten Google Play-Konto verwaltet wird (d. h. die Registrierung erfolgte ohne **Authentifizierung mit Google**).

> Einige Aktionen (z. B. 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 einer erfolgreichen Registrierung wird das Gerät mit dem authentifizierten Benutzer verknüpft.

Arbeitsprofil (persönlich genutzte Geräte)

- Teilen Sie die **Anmelde-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 die Einrichtung über die Android-Einstellungen starten und den Assistenten zur Konfiguration des Arbeitsprofils auswählen. Anschließend wird er aufgefordert, den QR-Code zu scannen oder den Anmelde-Token einzugeben.

Geräte, die dem Unternehmen gehören

- **Methode mit QR-Code**: Bei einem neuen oder auf Werkseinstellungen zurückgesetzten Gerät mehrmals an derselben Stelle auf den Bildschirm tippen, bis der QR-Code-Aufforderung angezeigt wird, und dann den im Dashboard angezeigten QR-Code scannen.
- **Methode zur Geräteidentifizierung** (wenn das Scannen von QR-Codes nicht möglich ist): Folgen Sie dem Einrichtungsassistenten, verbinden Sie sich mit einem Wi-Fi-Netzwerk und geben Sie dann, wenn Sie zur Anmeldung aufgefordert werden, **afw#setup** ein und fahren Sie mit dem Scannen des QR-Codes oder der Eingabe des Registrierungstokens fort. Authentifizieren Sie sich anschließend mit dem Google Workspace-Konto, wenn Sie dazu aufgefordert werden.

Für allgemeine Android-Einrichtungsprozesse (Arbeitsprofil vs. vollständig verwaltetes Gerät) finden Sie weitere Informationen in den Standard-Android-Registrierungsseiten dieses Handbuchs.