

# Provisioning dei dispositivi

- Dispositivi supportati
- Enrollment tokens
- Dispositivi di proprietà personale
- Dispositivi di proprietà dell'azienda per uso lavorativo e personale
- Dispositivi di proprietà dell'azienda per uso esclusivo lavorativo
- Zero-touch

# Dispositivi supportati

In generale, qualsiasi dispositivo con Android 5.1+ con Google Play Services è compatibile con Cerberus Enterprise.

Per una migliore esperienza utente, suggeriamo di utilizzare dispositivi che soddisfino i requisiti di Android Enterprise Recommended.

Alcune funzionalità sono limitate a specifiche versioni di Android o possono comportarsi in modo diverso su diverse versioni del sistema operativo. Per ulteriori informazioni su una funzionalità specifica, leggi la sezione Policy della documentazione.

Cerberus Enterprise supporta dispositivi di proprietà dell'azienda e personali e due modalità di gestione, device owner e profile owner.

I **dispositivi di proprietà personale** possono essere gestiti tramite un **profilo di lavoro**, in modo che si possa implementare una soluzione BYOD mantenendo i dati e le app di lavoro dei dipendenti separati da quelli personali, per una maggiore sicurezza e privacy da ambo le parti. Questa opzione è adatta per i dispositivi già di proprietà dei dipendenti, che puoi registrare nella tua azienda per un utilizzo sicuro anche al lavoro.

I **dispositivi di proprietà dell'azienda** possono essere gestiti anche tramite un profilo di lavoro, ma hai anche l'opzione **completamente gestito**, che consente un controllo più rigoroso sul dispositivo. I dispositivi di proprietà dell'azienda con profilo di lavoro sono adatti quando si desidera fornire dispositivi aziendali ai dipendenti per l'utilizzo sul lavoro, consentendo comunque di utilizzare tali dispositivi anche per uso personale. L'opzione completamente gestita, invece, è più adatta per dispositivi che devono essere utilizzati solo al lavoro o per dispositivi dedicati (COSU o corporate-owned single-use) come i kiosk.

Per ulteriori informazioni sul provisioning dei dispositivi, leggi la sezione Provisioning dei dispositivi.

# Enrollment tokens

Cerberus Enterprise utilizza gli enrollment token per attivare il processo di provisioning.

L'enrollment token e il metodo di provisioning utilizzati stabiliscono la proprietà di un dispositivo (di proprietà personale o aziendale) e la modalità di gestione (profilo di lavoro o dispositivo completamente gestito).

Per creare un nuovo enrollment token, vai alla sezione **Enrollment tokens** nella dashboard, quindi fai clic sul pulsante **Nuovo enrollment token**.

## 1. Opzioni

Quando crei un nuovo enrollment token puoi specificare alcuni parametri che determinano alcuni aspetti del provisioning, a seconda delle tue esigenze.

### 1.1. Policy

Campo obbligatorio. Questa è la policy che verrà applicata automaticamente su tutti i dispositivi registrati utilizzando il token. Puoi selezionare una delle policy che hai creato nel tuo account. Se non hai alcuna policy nel tuo account, devi prima crearne una.

### 1.2. Utente

L'utente che verrà automaticamente associato ai dispositivi durante il provisioning.

### 1.3. Uso personale

Campo obbligatorio. Specifica se l'utilizzo personale è consentito su un dispositivo di cui è stato eseguito il provisioning con questo enrollment token.

Per **dispositivi di proprietà dell'azienda**: l'abilitazione dell'uso personale consente all'utente di configurare un profilo di lavoro sul dispositivo. La disabilitazione dell'uso personale richiede che l'utente effettui il provisioning del dispositivo come dispositivo completamente gestito.

Per **dispositivi di proprietà personale**: l'abilitazione dell'uso personale consente all'utente di configurare un profilo di lavoro sul dispositivo. La disabilitazione dell'uso personale impedirà il provisioning del dispositivo.

L'uso personale non può essere disabilitato su un dispositivo di proprietà personale.

## 1.4. Durata

Campo obbligatorio. Il periodo di validità dell'enrollment token, compreso tra 1 minuto e 30 giorni.

## 1.5. Usi consentiti

Campo obbligatorio. Specifica se l'enrollment token può essere utilizzato più volte o solo una volta.

# 2. Opzioni di provisioning

Queste opzioni aggiuntive vengono applicate durante il provisioning di dispositivi completamente gestiti registrati scansando un codice QR. Non si applicano ai profili di lavoro o ai dispositivi registrati utilizzando altri metodi di provisioning.

Se imposti una configurazione Wi-Fi, il dispositivo può connettersi automaticamente alla rete specificata senza l'interazione dell'utente durante il provisioning del dispositivo per il download dell'applicazione di gestione dei dispositivi mobili.

# Dispositivi di proprietà personale

I dispositivi di proprietà dei dipendenti possono essere configurati con un **profilo di lavoro**. Un profilo di lavoro fornisce uno spazio autonomo per le app e i dati di lavoro, separato dalle app e dai dati personali. La maggior parte delle policy di gestione delle app, dei dati e di altro tipo si applica solo al profilo di lavoro, mentre le app e i dati personali del dipendente rimangono privati. Per configurare un profilo di lavoro su un dispositivo di proprietà personale, usa uno dei seguenti metodi di provisioning (assicurati che l'enrollment token abbia **Uso personale** impostato a **Consentito**):

## Link all'enrollment token

Versione di Android
5.1+

È possibile fornire l'URL di enrollment agli utenti finali. Quando un utente finale apre il collegamento dal proprio dispositivo, verrà guidato attraverso la configurazione del profilo di lavoro.

## Aggiunta profilo di lavoro da "*Impostazioni*"

Versione di Android
5.1+

Per configurare un profilo di lavoro sul suo dispositivo, l'utente può:

1. Andare su *Impostazioni* > *Google* > *Configura e ripristina*.
2. Toccare "*Configura il tuo profilo di lavoro*".

Questi passaggi avviano una configurazione guidata che scarica *Android Device Policy* sul dispositivo. Successivamente, all'utente verrà richiesto di eseguire la scansione di un codice QR o di inserire manualmente un enrollment token per completare la configurazione del profilo di lavoro.

## Download di Android Device Policy

Versione di Android
5.1+

Per configurare un profilo di lavoro sul proprio dispositivo, l'utente può scaricare Android Device Policy dal Google Play Store. Dopo l'installazione dell'app, all'utente verrà richiesto di scansionare un codice QR o di inserire manualmente un enrollment token per completare la configurazione del profilo di lavoro.

# Dispositivi di proprietà dell'azienda per uso lavorativo e personale

La configurazione di un dispositivo di proprietà dell'azienda con un **profilo di lavoro** attiva il dispositivo sia per il lavoro che per l'uso personale. Sui dispositivi di proprietà dell'azienda con profili di lavoro:

- La maggior parte delle policy di gestione di app, dati e di altro tipo si applicano esclusivamente al profilo di lavoro.
- Il profilo personale del dipendente rimane privato. Tuttavia, le aziende possono applicare determinate policy a livello di dispositivo e policy di utilizzo personale.
- Le aziende possono utilizzare *Blocca ambito* per imporre azioni di compliance al dispositivo o solo sul profilo di lavoro.
- Il disenrollment del dispositivo e i comandi del dispositivo si applicano a livello di dispositivo.

Per configurare un dispositivo di proprietà dell'azienda con un profilo di lavoro, usa uno dei seguenti metodi di provisioning (assicurati che l'enrollment token abbia **Uso personale** impostato a **Consentito**):

## Metodo del QR code

Versione di Android
8.0+

Su un dispositivo nuovo o ripristinato ai dati di fabbrica, l'utente (in genere un amministratore IT) tocca lo schermo sei volte nello stesso punto. Ciò attiva sul dispositivo la richiesta all'utente di scansione un codice QR.

# Dispositivi di proprietà dell'azienda per uso esclusivo lavorativo

La **Gestione completa del dispositivo** è adatta per i dispositivi di proprietà dell'azienda destinati esclusivamente a scopi di lavoro. Le aziende possono gestire tutte le app sul dispositivo e applicare l'intera gamma di policy e comandi delle API di Android Management.

È anche possibile bloccare un dispositivo (tramite policy) a una singola app o a un piccolo insieme di app per uno scopo specifico o un caso d'uso. Questo sottoinsieme di dispositivi completamente gestiti è denominato **dispositivi dedicati**.

Per configurare la gestione completa su un dispositivo di proprietà dell'azienda, utilizza uno dei seguenti metodi di provisioning (assicurati che l'enrollment token abbia **Uso personale** impostato a **Non consentito**):

## Metodo del QR code

Versione di Android
7.0+

Su un dispositivo nuovo o ripristinato ai dati di fabbrica, l'utente (in genere un amministratore IT) tocca lo schermo sei volte nello stesso punto. Ciò attiva sul dispositivo la richiesta all'utente di scansionare un codice QR.

## Metodo dell'identificativo DPC

Versione di Android
5.1+

Se Android Device Policy non può essere aggiunto tramite codice QR, un utente o un amministratore IT può seguire questi passaggi per eseguire il provisioning di un dispositivo completamente gestito o dedicato:

1. Seguire la configurazione guidata su un dispositivo nuovo o ripristinato alle impostazioni di fabbrica
2. Immettere i dettagli di accesso Wi-Fi per connettere il dispositivo a Internet
3. Quando viene chiesto di accedere ad un account Google, inserire **afw#setup**, che farà partire il download di Android Device Policy

4. Eseguire la scansione di un codice QR o inserire manualmente un enrollment token per eseguire il provisioning del dispositivo.

# Zero-touch

Gli amministratori IT possono eseguire il provisioning dei dispositivi di proprietà dell'azienda utilizzando il metodo di enrollment zero-touch, descritto in [Registrazione zero-touch per gli amministratori IT](#). Quando un dispositivo viene acceso per la prima volta, il dispositivo viene automaticamente configurato con le impostazioni definite dall'amministratore IT.

Gli amministratori IT possono preconfigurare i dispositivi acquistati da [rivenditori autorizzati](#) e gestirli utilizzando la dashboard di Cerberus Enterprise. Per collegare il tuo account Zero-touch, vai alla sezione **Zero-touch** nella dashboard, quindi segui le istruzioni.

Versione di Android	Profilo di lavoro	Dispositivo completamente gestito	Dispositivo dedicato
8.0+ (Pixel 7.1+)	✓	✓	✓