Provisioning dispositivi - Android

- Dispositivi supportati
- Token di registrazione
- Dispositivi di proprietà personale
- Dispositivi aziendali per uso lavorativo e personale
- Dispositivi aziendali per solo uso lavorativo
- Zero-touch
- Autenticazione con Google enrollment

Dispositivi supportati

In generale, qualsiasi dispositivo con Android 6 o versione successiva e Google Play Services è compatibile con Cerberus Enterprise.

Per un'esperienza utente migliore, ti consigliamo di usare dispositivi che soddisfano i requisiti Android Enterprise Recommended.

> Alcune funzioni sono limitate a specifiche versioni di Android o possono comportarsi diversamente tra le versioni del sistema operativo. Per maggiori informazioni su una funzione specifica, vedi la sezione Policy della documentazione.

Cerberus Enterprise supporta sia i dispositivi aziendali sia quelli di proprietà personale, e due modalità di gestione: device owner e profile owner.

I dispositivi **di proprietà personale** possono essere gestiti tramite un **profilo di lavoro**. Questo consente una soluzione BYOD mantenendo separati i dati e le app di lavoro dei dipendenti dai dati e dalle app personali, migliorando sicurezza e privacy. Questa opzione è adatta ai dispositivi già di proprietà dei dipendenti che vuoi registrare nella tua organizzazione per uso lavorativo.

I dispositivi **aziendali** possono anche essere gestiti tramite un profilo di lavoro, ma puoi anche scegliere l'opzione **completamente gestito**, che consente un controllo più rigoroso sul dispositivo. I dispositivi aziendali con profilo di lavoro sono adatti quando fornisci dispositivi aziendali ai dipendenti per il lavoro, consentendo comunque l'uso personale. I dispositivi completamente gestiti sono più adatti ai dispositivi che devono essere usati solo per il lavoro o ai **dispositivi dedicati** (COSU, corporate-owned single-use), come i chioschi.

Per maggiori informazioni sul provisioning dei dispositivi, vedi la pagina Panoramica sul provisioning dei dispositivi.

Token di registrazione

Cerberus Enterprise usa i token di registrazione per avviare il processo di registrazione (provisioning) dei dispositivi Android. Il token che selezioni definisce la policy iniziale applicata ai dispositivi registrati e influenza quali modalità di provisioning sono consentite.

> La scheda dei token di registrazione Android è disponibile solo dopo aver completato la **configurazione di Android Management**.

Dove trovare i token di registrazione

Nella dashboard, apri **Token di registrazione**. A seconda della configurazione dell'account, la pagina può mostrare più schede (token Android, registrazione con accesso Google, registrazione manuale Apple e Apple Automated Device Enrollment).

> Se il tuo enterprise Android è supportato da un dominio Google gestito (Google Workspace), la dashboard può anche mostrare una scheda **Autenticazione con Google Enrollment**.
>
> Per dettagli su come abilitarla e usarla, vedi **Autenticazione con Google enrollment**.

Elenco dei token di registrazione (Android)

La scheda dei token Android mostra una tabella con tutti i token. Facendo clic su una riga si apre la pagina dei dettagli del token.

Colonne

- **Stato**: **Attivo** (i dispositivi possono registrarsi con il token), **Scaduto** (la data di scadenza è passata) o **Esaurito** (un token monouso già utilizzato).

- **Policy**: la policy assegnata al token (il tooltip mostra l'id della policy). **Policy eliminata** significa che la policy è stata eliminata dopo la creazione del token.
- **Utente**: utente facoltativo preassegnato ai dispositivi registrati con il token. **Utente eliminato** significa che l'utente è stato eliminato dopo la creazione del token.
- **Registrazioni**: quanti dispositivi si sono registrati con il token, mostrate come **n / 1** per un token monouso.
- **Uso personale**: Consentito / Non consentito / Dispositivo dedicato.
- **Creato**: quando il token è stato creato. La tabella mostra per primi i token più recenti.
- **Scadenza**: data/ora di scadenza o **Mai**.
- **Codice di registrazione**: il codice del token, quello che digiti sul dispositivo quando lo registri senza un codice QR.

Azioni

- Ogni riga ha un'azione di eliminazione (**Elimina token di registrazione**). L'eliminazione è disabilitata quando la licenza è scaduta.
- La tabella supporta la selezione di più righe: puoi abilitare la modalità di selezione, selezionare più token ed eliminarli con **Elimina token selezionati**.
- Usa l'azione di aggiornamento per ricaricare l'elenco. La tabella è paginata (10/25/50 elementi per pagina).

Crea un nuovo token di registrazione

Nella scheda dei token Android, fai clic su **Nuovo token di registrazione** per aprire la pagina di creazione del token. Se la licenza è scaduta, il pulsante di creazione è disabilitato.

Opzioni del token

1. Policy

Obbligatorio. La policy applicata automaticamente a tutti i dispositivi registrati con questo token.

Seleziona una delle tue **policy Android**. Se non hai ancora nessuna policy, creane prima una.

2. Utente

Facoltativo. Se impostato, i dispositivi appena registrati vengono associati automaticamente a questo utente.

3. Uso personale

Controlla se l'uso personale è consentito su un dispositivo di cui è stato eseguito il provisioning con questo token di registrazione:

- **Consentito**: adatto ai dispositivi di proprietà personale (profilo di lavoro) e ai dispositivi aziendali per uso lavorativo e personale.
- **Non consentito**: adatto ai dispositivi aziendali per solo uso lavorativo (completamente gestiti).
- **Dispositivo dedicato**: adatto ai dispositivi kiosk/dedicati (il dispositivo non è associato a un singolo utente).

4. Utilizzi consentiti

Seleziona se il token può essere usato più volte (**Multiplo**) o una sola volta (**Una sola volta**).

5. Scadenza

Seleziona l'unità di scadenza (**Minuti**, **Ore**, **Giorni** o **Mai**). Se non è impostata su Mai, inserisci il valore di scadenza. L'intervallo consentito dipende dall'unità selezionata e può arrivare fino a 10.000 giorni.

6. Autenticazione Google

Controlla se l'utente deve autenticarsi con un account Google durante la registrazione del dispositivo:

- **Non specificato**: viene usata l'impostazione di autenticazione Google a livello di enterprise per determinare se l'utente deve autenticarsi con Google durante la registrazione.
- **Facoltativo**: l'utente può scegliere di saltare l'autenticazione Google durante la registrazione.
- **Obbligatorio**: l'utente deve autenticarsi con un account Google per procedere con la registrazione.

Quando è selezionato **Obbligatorio**, appare un campo facoltativo **Email dell'account richiesto**. Se impostato, l'utente deve autenticarsi con quello specifico account Google durante la registrazione.

Opzioni di provisioning (solo codice QR)

Queste opzioni aggiuntive sono incorporate nel codice QR e vengono applicate durante il provisioning dei dispositivi completamente gestiti registrati tramite scansione del codice QR. Non si applicano ai profili di lavoro né ai dispositivi registrati usando l'URL di registrazione o il token.

Configurazione Wi-Fi

Usalo per consentire a un dispositivo di connettersi automaticamente al Wi-Fi durante il provisioning, così può scaricare e inizializzare l'app di gestione. I campi disponibili includono **SSID**, **SSID nascosto**, **Sicurezza** e (se necessario) **Passphrase**.

Puoi anche configurare un proxy HTTP (**Proxy**) e, a seconda della modalità, impostare **Host**/**Porta**, **URI PAC** e **Host di esclusione proxy**.

Altre opzioni

Le opzioni aggiuntive includono **Locale**, **Fuso orario** e **Salta crittografia**.

Dettagli del token di registrazione

Quando apri un token, la pagina dei dettagli mostra la configurazione e le informazioni sull'utilizzo del token:

- **Stato**, **Scadenza**, **Utilizzo**, **Uso personale**, **Utilizzi consentiti** e (se impostata) **Autenticazione Google** con l'**email dell'account richiesto** facoltativa.
- **Token**: il valore grezzo del token di registrazione (copiabile).
- **URL di registrazione**: un URL di registrazione di Google Android Enterprise (copiabile e inviabile via email).
- **Codice QR**: mostrato sul lato destro della pagina, usato per registrare dispositivi completamente gestiti.

> Per procedure di provisioning dettagliate, segui le guide alla registrazione Android: **Dispositivi di proprietà personale**, **Dispositivi aziendali per uso lavorativo e personale**, **Dispositivi aziendali per solo uso lavorativo** e **Zero-touch**.

Dispositivi di proprietà personale

I dispositivi di proprietà dei dipendenti possono essere configurati con un **profilo di lavoro**. Un profilo di lavoro offre 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 di app, dati e altro si applica solo al profilo di lavoro, mentre le app e i dati personali dei dipendenti restano privati.
Per configurare un profilo di lavoro su un dispositivo di proprietà personale, usa uno dei seguenti metodi di provisioning (assicurati che il token di registrazione abbia ***Uso personale*** impostato su **Consentito**):

Link del token di registrazione

Versione Android
6.0+

Puoi fornire l'URL di registrazione agli utenti finali. Quando un utente finale apre il link dal proprio dispositivo, viene guidato nella configurazione del profilo di lavoro.

Aggiungi profilo di lavoro da "*Impostazioni*"

Versione Android
6.0+

Per configurare un profilo di lavoro sul proprio dispositivo, un utente può aprire l'app ***Impostazioni*** del dispositivo, poi usare la barra di ricerca per trovare e toccare l'opzione ***Configura il profilo di lavoro***.

Se la ricerca non dà risultati, la posizione di questa opzione può variare. Ecco alcune possibilità:

- *Impostazioni -> Servizi e preferenze Google -> Tutti i servizi -> Configura il profilo di lavoro*.
- *Impostazioni -> Google -> Configura e ripristina -> Configura il profilo di lavoro*.

Questi passaggi avviano una procedura guidata di configurazione che scarica *Android Device Policy* sul dispositivo. Poi all'utente viene chiesto di scansionare un codice QR o inserire manualmente un token di registrazione per completare la configurazione del profilo di lavoro.

Scarica Android Device Policy

Versione Android
6.0+

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

iPhone e iPad personali

Gli iPhone e gli iPad personali (e i Mac) si registrano con **User Enrollment** di Apple: l'utente accede con il proprio Managed Apple Account nelle impostazioni del dispositivo e vengono gestite solo le app, gli account e i dati di lavoro. Su iPhone e iPad le app dell'App Store della policy e l'app **Cerberus Enterprise** vengono installate con una licenza utente di quell'account. La posizione dei dispositivi personali viene raccolta solo se la loro policy attiva **Posizione e geofence sui dispositivi personali** e l'utente lo consente. Leggi **Registrazione con account Apple**.

Dispositivi aziendali per uso lavorativo e personale

Configurare un dispositivo aziendale con un **profilo di lavoro** consente di usarlo sia per il lavoro sia per uso personale. Sui dispositivi aziendali con profilo di lavoro:

- La maggior parte delle policy di gestione di app, dati e altro si applica solo al profilo di lavoro.
- I profili personali dei dipendenti restano privati. Tuttavia, le aziende possono applicare determinate policy a livello di dispositivo e policy sull'uso personale.
- Le aziende possono usare *Ambito di blocco* per applicare azioni di conformità all'intero dispositivo o solo al suo profilo di lavoro.
- L'annullamento della registrazione e i comandi del dispositivo si applicano all'intero dispositivo.

Per configurare un dispositivo aziendale con un profilo di lavoro, usa uno dei seguenti metodi di provisioning (assicurati che il token di registrazione abbia **Uso personale** impostato su **Consentito**):

Metodo con codice QR

Versione Android
8.0+

Su un dispositivo nuovo o ripristinato alle impostazioni di fabbrica, l'utente (in genere un amministratore IT) tocca lo schermo sei volte nello stesso punto. Questo fa sì che il dispositivo chieda all'utente di scansionare un codice QR.

Dispositivi aziendali per solo uso lavorativo

La **gestione completa del dispositivo** è adatta ai dispositivi aziendali destinati esclusivamente al lavoro. Le aziende possono gestire tutte le app sul dispositivo e applicare l'intera gamma di policy e comandi dell'Android Management API.
È anche possibile bloccare un dispositivo (tramite policy) su una singola app o su un piccolo insieme di app per uno scopo o un caso d'uso dedicato. Questo sottoinsieme di dispositivi completamente gestiti è chiamato **dispositivi dedicati**.
Per configurare la gestione completa su un dispositivo aziendale, usa uno dei seguenti metodi di provisioning (assicurati che il token di registrazione abbia **Uso personale** impostato su **Non consentito**):

Metodo con codice QR

Versione Android
7.0+

Su un dispositivo nuovo o ripristinato alle impostazioni di fabbrica, l'utente (in genere un amministratore IT) tocca lo schermo sei volte nello stesso punto. Questo fa sì che il dispositivo chieda all'utente di scansionare un codice QR.

Metodo con identificatore DPC

Versione 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. Segui la procedura guidata di configurazione su un dispositivo nuovo o ripristinato alle impostazioni di fabbrica.
2. Inserisci i dati di accesso Wi-Fi per collegare il dispositivo a internet.
3. Quando ti viene chiesto di accedere, inserisci **afw#setup**, che scarica Android Device Policy.
4. Scansiona un codice QR o inserisci manualmente un token di registrazione per eseguire il provisioning del dispositivo.

Zero-touch

Gli amministratori IT possono eseguire il provisioning di dispositivi aziendali usando il metodo di registrazione zero-touch, descritto in Registrazione zero-touch per gli amministratori IT. Quando un dispositivo viene acceso per la prima volta, viene automaticamente impostato sulle configurazioni definite dall'amministratore IT.

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

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

Autenticazione con Google enrollment

L'autenticazione con Google enrollment (detta anche **Autenticazione Google per la registrazione**) consente agli utenti di autenticarsi con il proprio account Google Workspace durante la registrazione dei dispositivi Android.

> Questa funzione è disponibile solo per gli enterprise Android supportati da un dominio Google gestito (Google Workspace).

Dove trovarla

Nella dashboard, apri **Token di registrazione** e seleziona la scheda **Autenticazione con Google Enrollment**. La scheda viene mostrata solo quando Android Management è configurato e l'integrazione con Google Workspace è disponibile per il tuo enterprise.

Abilita (o disabilita) l'autenticazione Google

L'autenticazione Google viene abilitata dalla **Google Admin console**. Dopo aver modificato l'impostazione, torna a Cerberus Enterprise e usa **Aggiorna stato** per ricaricare la configurazione corrente.

1. Accedi alla tua **Google Admin console** con un account amministratore.
2. Apri **Dispositivi**.
3. Vai a **Mobile e endpoint** → **Impostazioni** → **Integrazioni di terze parti**.
4. Trova l'**integrazione Android EMM** per Cerberus Enterprise e aprila.
5. Fai clic su **Gestisci provider EMM**.
6. Attiva o disattiva **Autentica usando Google** per abilitare o disabilitare l'autenticazione Google durante la registrazione.
7. Fai clic su **Salva**.

8. Torna alla dashboard di Cerberus Enterprise e fai clic su **Aggiorna stato** nella scheda **Autenticazione con Google Enrollment**.

Token di registrazione per l'autenticazione Google

Quando l'autenticazione Google è abilitata, la dashboard mostra un token di registrazione dedicato usato per questa modalità di registrazione. La pagina può mostrare un **codice QR**, un valore **Token di registrazione** e un **URL di registrazione** (copiabile e inviabile via email).

Opzioni principali

- **Consenti uso personale**: controlla se il token può registrare dispositivi per uso lavorativo e personale (scenari con profilo di lavoro) o per solo uso lavorativo (scenari completamente gestiti/dedicati).
- **Policy predefinita di fallback**: la policy applicata quando l'utente che esegue la registrazione non ha assegnata una policy predefinita specifica per l'autenticazione Google.

Interazione con le policy

L'impostazione della policy **Autenticazione per la configurazione dell'account di lavoro** (workAccountSetupConfig.authenticationType) controlla come gli utenti si autenticano durante la configurazione dell'account di lavoro, ma l'impostazione della Google Admin Console **Autentica usando Google** e il tipo di token di registrazione possono comunque richiedere l'autenticazione.

Per i dispositivi già registrati, questa policy si applica solo se il dispositivo è gestito da un account Managed Google Play (ovvero registrato senza **Autenticazione con Google Enrollment**).

> Alcune azioni (ad esempio la modifica delle opzioni del token) possono essere disabilitate quando la licenza è scaduta.

Registra un dispositivo

Durante la registrazione, all'utente viene chiesto di autenticarsi con il proprio account Google Workspace. Dopo una registrazione riuscita, il dispositivo viene associato all'utente autenticato.

Profilo di lavoro (dispositivi di proprietà personale)

- Condividi l'**URL di registrazione** con l'utente. Quando l'utente lo apre sul proprio dispositivo Android, viene guidato nella configurazione del profilo di lavoro e nell'autenticazione Google.
- In alternativa, l'utente può partire dalle Impostazioni di Android e scegliere il flusso di configurazione del profilo di lavoro, poi scansionare il codice QR o inserire il token di registrazione quando richiesto.

Dispositivi aziendali

- **Metodo con codice QR**: su un dispositivo nuovo o ripristinato alle impostazioni di fabbrica, tocca lo schermo più volte nello stesso punto finché non appare la richiesta del codice QR, poi scansiona il codice QR mostrato nella dashboard.
- **Metodo con identificatore DPC** (quando la scansione del codice QR non è disponibile): segui la procedura guidata di configurazione, connettiti al Wi-Fi, poi quando ti viene chiesto di accedere inserisci **afw#setup** e procedi scansionando il codice QR o inserendo il token di registrazione. Quando richiesto, autenticati con l'account Google Workspace.

Per le procedure generali di provisioning Android (profilo di lavoro vs completamente gestito), vedi le pagine standard sulla registrazione Android in questo manuale.