Provisioning dispositivi - Android

Dispositivi supportati

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

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

> Alcune funzionalità sono limitate a specifiche versioni di Android o potrebbero comportarsi in modo diverso a seconda della versione del sistema operativo. Per maggiori informazioni su una specifica funzionalità, consultare la sezione Policies della documentazione.

Cerberus Enterprise supporta sia i dispositivi aziendali che quelli personali, e offre due modalità di gestione: "device owner" e "profile owner".

I dispositivi personali possono essere gestiti tramite un **profilo aziendale**. Questo consente una soluzione BYOD, mantenendo i dati e le applicazioni aziendali dei dipendenti separati dai dati e dalle applicazioni personali, migliorando sia la sicurezza che la privacy. Questa opzione è adatta per i dispositivi già di proprietà dei dipendenti che si desidera registrare nell'organizzazione per l'uso lavorativo.

Dispositivi aziendali possono essere gestiti tramite un profilo di lavoro, ma è possibile scegliere anche l'opzione di **gestione completa**, che consente un controllo più rigoroso del dispositivo. I dispositivi aziendali con un profilo di lavoro sono adatti quando si forniscono dispositivi aziendali ai dipendenti per lavoro, pur consentendo un utilizzo personale. I dispositivi con gestione completa sono più adatti per i dispositivi che devono essere utilizzati solo per lavoro, o per i **dispositivi dedicati** (COSU, corporate-owned single-use), come le postazioni self-service.

Per maggiori informazioni sulla configurazione dei dispositivi, consultare la pagina Panoramica sulla configurazione dei dispositivi.

Token di registrazione

Cerberus Enterprise utilizza i token di registrazione per avviare il processo di registrazione (configurazione) dei dispositivi Android. Il token che scegli definisce la policy iniziale applicata ai dispositivi registrati e influenza le modalità di configurazione consentite.

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

Dove trovare i token di iscrizione

Nella dashboard, apri **Token di iscrizione**. A seconda della configurazione del tuo account, la pagina potrebbe mostrare diverse schede (token Android, iscrizione con Google, iscrizione manuale di Apple e iscrizione automatica dei dispositivi Apple).

> Se la tua azienda Android è gestita tramite un dominio Google (Google Workspace), la dashboard può anche mostrare una scheda "**Autenticazione tramite iscrizione Google**. Per maggiori dettagli su come abilitare e utilizzare questa funzionalità, consulta **Autenticazione tramite iscrizione Google**.

Elenco dei token di registrazione (Android)

La scheda "Token Android" mostra una tabella con tutti i token. Cliccando su una riga, si apre la pagina con i dettagli del token.

Colonne

- **ID**: identificativo interno del token.
- **Stato**: **Disponibile**, **Utilizzato** (token monouso già utilizzato) o **Scaduto**.
- **Scadenza**: data e ora di scadenza, oppure **Mai**.
- **Policy**: la policy assegnata al token (il tooltip nell'interfaccia utente mostra anche l'ID della policy).
- **Utilizzo personale**: consentito / non consentito / dispositivo dedicato.

- **Utilizzi consentiti**: Utilizzo multiplo o una sola volta.
- **Utente**: utente opzionale predefinito per i dispositivi registrati tramite token.

Azioni

- Ogni riga dispone di 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: è possibile attivare la modalità di selezione, selezionare più token ed eliminarli con **Elimina i token selezionati**.
- Utilizza l'azione "aggiorna" per ricaricare l'elenco. La tabella è paginata (10/25/50 elementi per pagina).

Crea un nuovo token di registrazione

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

Opzioni per i token

1. Policy

Obbligatorio. La policy viene applicata automaticamente a tutti i dispositivi registrati utilizzando questo token. Seleziona una delle tue **policy Android**. Se non hai ancora una policy, creane una prima.

2. Utente

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

3. Utilizzo personale

Controlla se l'utilizzo personale è consentito su un dispositivo configurato con questo token di iscrizione:

- **Consentito**: adatto per dispositivi di proprietà personale (con profilo di lavoro) e dispositivi aziendali utilizzati sia per lavoro che per uso personale.
- **Non consentito**: adatto per dispositivi di proprietà aziendale da utilizzare esclusivamente per lavoro (gestione completa).
- **Dispositivo dedicato**: adatto per dispositivi kiosk o dedicati (il dispositivo non è associato a un singolo utente).

4. Utilizzi consentiti

Seleziona se il token può essere utilizzato più volte (**Più volte**) o solo una volta (**Una sola volta**).

5. Scadenza

Seleziona l'unità di tempo per la scadenza (**Minuti**, **Ore**, **Giorni**, oppure **Mai**). Se non impostato su "Mai", inserisci il valore di scadenza. L'intervallo consentito dipende dall'unità selezionata e può arrivare fino a 10.000 giorni.

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 la scansione del codice QR. Non si applicano ai profili di lavoro o ai dispositivi registrati tramite l'URL o il token di registrazione.

Configurazione Wi-Fi

Utilizza questa opzione per consentire a un dispositivo di connettersi automaticamente a Wi-Fi durante la configurazione, in modo che possa scaricare e inizializzare l'app di gestione. I campi disponibili includono **SSID**, **SSID nascosto**, **Sicurezza** e, se necessario, **Frase di sicurezza**.

È possibile configurare anche un proxy HTTP (**Proxy**) e, a seconda della modalità, impostare **Host**/**Port**, **PAC URI** e **host di bypass del proxy**.

Altre opzioni

Altre opzioni includono **Lingua**, **Fuso orario** e **Salta la 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**, **Utilizzo personale**, e **Utilizzi consentiti**.
- **Token**: il valore del token di registrazione (copiabile).
- **URL di registrazione**: un URL di registrazione di Google Android Enterprise (copiabile e inviabile tramite email).
- **Codice QR**: visualizzato sul lato destro della pagina, utilizzato per registrare i dispositivi gestiti.

> Per le procedure di configurazione dettagliate, consultare le guide di registrazione per Android: **Dispositivi di proprietà privata**, **Dispositivi aziendali per lavoro e uso personale**, **Dispositivi aziendali per uso lavorativo**, e **Registrazione automatica**.

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 separato per le app e i dati aziendali, distinto dalle app e dai dati personali. La maggior parte delle policy di gestione, dei dati e di altre funzionalità si applicano solo al profilo di lavoro, mentre le app e i dati personali dei dipendenti rimangono privati.
Per configurare un profilo di lavoro su un dispositivo di proprietà personale, utilizzare uno dei seguenti metodi di provisioning (assicurarsi che il token di iscrizione abbia ***Utilizzo 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, verrà guidato attraverso la configurazione del profilo aziendale.

Aggiungi il profilo aziendale da "*Impostazioni*"

Versione Android
6.0+

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

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

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

Questi passaggi avviano una procedura guidata che scarica *Android Device Policy* sul dispositivo. Successivamente, l'utente verrà invitato a scansionare un codice QR o a inserire manualmente un token di registrazione per completare la configurazione del profilo aziendale.

Scarica Android Device Policy

Versione Android
6.0+

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 chiesto di scansionare un codice QR o di inserire manualmente un token di registrazione per completare la configurazione del profilo aziendale.

Dispositivi aziendali per l'uso lavorativo e personale

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

- La maggior parte delle policy relative ad applicazioni, dati e altre impostazioni si applica solo al profilo di lavoro.
- I profili personali dei dipendenti rimangono privati. Tuttavia, le aziende possono applicare determinate policy a livello di dispositivo e policy sull'utilizzo personale.
- Le aziende possono utilizzare il *perimetro di blocco* per applicare azioni di conformità a un intero dispositivo o solo al suo profilo di lavoro.
- La disattivazione del dispositivo e i comandi applicati al dispositivo si estendono all'intero dispositivo.

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

Metodo con codice QR

Versione Android
8.0+

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

Dispositivi aziendali da utilizzare esclusivamente per lavoro

La gestione completa del dispositivo è adatta ai dispositivi aziendali destinati esclusivamente all'uso lavorativo. 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 configurare un dispositivo (tramite policy) in modo che possa eseguire una sola applicazione o un piccolo insieme di applicazioni, per scopi o utilizzi specifici. Questo sottoinsieme di dispositivi completamente gestiti è definito come **dispositivi dedicati**.
Per configurare la gestione completa su un dispositivo di proprietà aziendale, utilizzare uno dei seguenti metodi di provisioning (assicurarsi che il token di registrazione abbia **l'utilizzo 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 (solitamente un amministratore IT) tocca lo schermo sei volte nello stesso punto. Questo attiva il dispositivo, che chiede all'utente di scansionare un codice QR.

Metodo di identificazione del profilo dispositivo

Versione Android
5.1+

Se non è possibile aggiungere la policy per il dispositivo Android tramite codice QR, un utente o un amministratore IT può seguire questi passaggi per configurare un dispositivo completamente gestito o dedicato:

1. Segui la procedura guidata su un dispositivo nuovo o riportato alle impostazioni di fabbrica.
2. Inserisci le credenziali Wi-Fi per connettere il dispositivo a Internet.
3. Quando ti viene richiesto di accedere, inserisci **afw#setup**, che scarica la policy del dispositivo Android.
4. Scansiona un codice QR oppure inserisci manualmente un token di registrazione per configurare il dispositivo.

Configurazione automatica

Gli amministratori IT possono configurare i dispositivi aziendali utilizzando il metodo di registrazione automatica, descritto in Registrazione automatica per amministratori IT. Quando un dispositivo viene acceso per la prima volta, viene automaticamente configurato con le impostazioni definite dall'amministratore IT.

Gli amministratori IT possono preconfigurare i dispositivi acquistati da rivenditori autorizzati e gestirli tramite il pannello di controllo di Cerberus Enterprise. Per collegare il tuo account Zero-touch, vai nella sezione **Zero-touch** del pannello di controllo e segui le istruzioni.

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

Autenticazione tramite registrazione con Google

Autenticazione tramite registrazione con Google (nota anche come **Autenticazione Google per la registrazione**) consente agli utenti di autenticarsi con il proprio account Google Workspace durante la registrazione del dispositivo Android.

> Questa funzionalità è disponibile solo per le aziende Android che utilizzano un dominio Google gestito (Google Workspace).

Dove trovarlo

Nella dashboard, apri **I token di registrazione** e seleziona la scheda **Autenticazione tramite Google Enrollment**. La scheda viene visualizzata solo quando Android Management è configurato e l'integrazione con Google Workspace è disponibile per la tua azienda.

Abilita (o disabilita) l'autenticazione tramite Google

L'autenticazione Google è abilitata dalla **console di amministrazione di Google**. Dopo aver modificato l'impostazione, torna a Cerberus Enterprise e utilizza **Aggiorna stato** per ricaricare la configurazione corrente.

1. Accedi al tuo **pannello di amministrazione di Google** utilizzando un account amministratore.
2. Apri **Dispositivi**.
3. Vai su **Dispositivi mobili e endpoint** → **Impostazioni** → **Integrazioni di terze parti**.
4. Trova l'**integrazione Android EMM**> per Cerberus Enterprise e aprila.
5. Fai clic su **Gestisci i provider EMM**.
6. Attiva o disattiva **l'autenticazione tramite Google** per abilitare o disabilitare l'autenticazione Google per la registrazione.
7. Fai clic su **Salva**.
8. Ritorna alla dashboard di Cerberus Enterprise e fai clic su **Aggiorna stato** nella scheda **Autenticazione tramite Google Enrollment**.

Token di registrazione tramite autenticazione Google

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

Opzioni principali

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

Interazione con le policy

L'impostazione della policy **Configurazione dell'autenticazione dell'account di lavoro** (workAccountSetupConfig.authenticationType) controlla come gli utenti si autenticano durante la configurazione dell'account di lavoro, ma l'impostazione della console di amministrazione di Google **Autenticazione tramite 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 tramite un account Google Play aziendale (ovvero, registrato senza **Autenticazione tramite Google**).

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

Registra un dispositivo

Durante la registrazione, l'utente viene invitato a autenticarsi con il proprio account Google Workspace. Dopo una registrazione andata a buon fine, 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 la apre sul proprio dispositivo Android, viene guidato attraverso la configurazione del profilo di lavoro e l'autenticazione di Google.
- In alternativa, l'utente può iniziare dalle impostazioni di Android e scegliere la procedura di configurazione del profilo di lavoro, quindi scansionare il codice QR o inserire il token di registrazione quando richiesto.

Dispositivi aziendali

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

Per le procedure generali di configurazione di Android (profilo di lavoro rispetto a dispositivo completamente gestito), consultare le pagine standard di registrazione di Android presenti in questo manuale.