

# Manuale utente

- Introduzione
- 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
- Policy
  - Sommario
  - Gestione app
  - Modalità kiosk
  - Sicurezza
  - Multimedia
  - Cellulare
  - Reti
  - Sistema
  - Gestione utenti
  - Uso personale
  - Policy cross-profile
  - Rapporti di stato
  - Varie
  - Regole di applicazione delle policy
- Stato dei dispositivi

- Sommario

- Comandi

- App private

- Gestione dei certificati

# Introduzione

Cerberus Enterprise è una soluzione EMM completa, progettata per aiutarti a proteggere e gestire i tuoi dispositivi Android. Ha tutte le funzionalità giuste per una gestione efficace del BYOD e dei dispositivi di proprietà dell'azienda in una dashboard pulita e intuitiva e puoi iniziare in pochi minuti.

Per utilizzare efficacemente Cerberus Enterprise è necessario comprendere alcuni concetti chiave su come funziona il sistema.

Il sistema è basato sulle Android Management API di Google, una soluzione che consente alle aziende di gestire efficacemente i dispositivi di lavoro tramite l'app Android Device Policy (ADP), in grado di controllare i dispositivi Android registrati. La maggior parte delle funzionalità viene applicata sui dispositivi direttamente da ADP, tuttavia utilizziamo anche un'app complementare aggiuntiva, specifica per Cerberus Enterprise, che abilita alcune funzionalità aggiuntive, attualmente non supportate da ADP.

Ogni dispositivo può essere **registrato** nel sistema usando un **Enrollment token**, che può essere creato dalla dashboard. Ogni enrollment token ha una **Policy** associata, che contiene tutte le regole definite che devono essere applicate ai dispositivi.

Gli amministratori IT possono modificare la policy associata a un dispositivo dopo la registrazione, tuttavia ogni dispositivo può essere associato a una sola policy alla volta.

Durante il processo di registrazione (provisioning), l'app Android Device Policy e l'app complementare Cerberus Enterprise vengono installate automaticamente sul dispositivo. Di conseguenza, la policy corrispondente viene applicata automaticamente sul dispositivo e tutte le regole associate verranno applicate da ADP e Cerberus Enterprise.

Una policy può essere applicata a molti dispositivi. In questo caso, quando modifichi la policy, tutti i dispositivi associati riceveranno le modifiche.

# Provisioning dei dispositivi

# 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 scansionando 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 scansionare 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+)	✓	✓	✓

# Policy

# Sommario

Le policy sono le entità centrali del sistema, poiché definiscono tutte le regole che devono essere applicate e rispettate sui dispositivi.

Puoi sfogliare le tue policy e crearne di nuove dalla sezione **Policy** della dashboard. Per vedere i dettagli o modificare una policy, clicca sulla voce selezionata nella tabella.

Una policy può essere associata ad un enrollment token, in modo che venga applicata automaticamente ai dispositivi durante il processo di provisioning. È inoltre possibile modificare la policy associata ad uno specifico dispositivo specifico dopo il provisioning.

Ogni dispositivo può essere associato a una sola policy alla volta.

# Gestione app

In questa sezione puoi impostare le policy relative alla disponibilità, installazione, aggiornamento e gestione dei permessi delle app.

Gli account Managed Google Play vengono creati automaticamente quando si esegue il provisioning dei dispositivi.

## 1. Modalità Play Store

Questa modalità controlla quali app sono disponibili per l'utente nel Play Store e il comportamento sul dispositivo quando le app vengono rimosse dalla policy.

**Whitelist (impostazione predefinita):** Sono disponibili solo le app incluse nella policy e qualsiasi app non inclusa nella policy verrà automaticamente disinstallata dal dispositivo. Play Store mostrerà solo le app disponibili.

**Blacklist:** Tutte le app sono disponibili e qualsiasi app di cui si vuole impedire l'installazione sul dispositivo deve essere esplicitamente contrassegnata come **bloccata** nella policy delle applicazioni. Play Store mostrerà tutte le app, tranne quelle bloccate.

## 2. Policy per le app non attendibili

La policy per le app non attendibili (app da fonti sconosciute) applicata al dispositivo. Questa opzione controlla l'impostazione del sistema Android che consente a un utente di installare app dall'esterno del Play Store (sideloading).

**Non consentire (impostazione predefinita):** non consentire l'installazione di app non attendibili sull'intero dispositivo.

**Solo profilo personale:** per i dispositivi con profili di lavoro, consenti le installazioni di app non attendibili solo nel profilo personale del dispositivo.

**Consenti:** consente l'installazione di app non attendibili sull'intero dispositivo.



### 3. Google Play Protect

Specifica se la verifica delle app di Google Play Protect app è applicata.

**Applicato (impostazione predefinita):** Forza l'abilitazione della verifica delle app

**Scelta dell'utente:** Consenti all'utente di scegliere se abilitare la verifica delle app.

### 4. Policy di default dei permessi

La policy per fornire i permessi a runtime alle app.

**Chiedi (impostazione predefinita):** richiede all'utente di concedere i permessi.

**Concedi:** concedi automaticamente un permesso.

**Nega:** nega automaticamente un permesso.

### 5. Disabilita installazione app

Specifica se l'installazione di app da parte dell'utente è disabilitata.

### 6. Disabilita disinstallazione app

Specifica se la disinstallazione di app da parte dell'utente è disabilitata.

### 7. Policy dei permessi

Policy di concessione o diniego di specifici permessi o gruppi di permessi applicate per tutte le app. Queste policy sovrascrivono le impostazioni di **Policy di default dei permessi**.

### 8. Applicazioni

Elenco di applicazioni che devono essere incluse nella policy. Il comportamento del contenuto dell'elenco dipende dal valore impostato in **Modalità Play Store**.

Se **Modalità Play Store** è **whitelist**, sono disponibili solo le app che rientrano nella policy e qualsiasi app non presente nella policy verrà automaticamente disinstallata dal dispositivo.

Se **Modalità Play Store** è **blacklist**, tutte le app sono disponibili e qualsiasi app che non dovrebbe essere presente sul dispositivo deve essere esplicitamente contrassegnata come **bloccata** nella policy delle applicazioni.

Per aggiungere una nuova app, clicca sull'icona **+**, quindi scegli l'app dal Play Store e fai clic sul pulsante **Seleziona** nella scheda dell'app.

Tutte le app pubblicate sul Play Store nel tuo paese sono disponibili per la selezione per impostazione predefinita. Per selezionare le tue app private o web, devi prima caricarle nel sistema. Per maggiori informazioni leggi la pagina [App private](#).

Ogni app può essere configurata con le proprie impostazioni, che sono visivamente contenute in una scheda.

## 8.1. Tipo di installazione

Il tipo di installazione da eseguire per un'app.

**Disponibile:** L'app è disponibile per l'installazione.

**Preinstallata:** L'app è automaticamente installata e può essere rimossa dall'utente.

**Forza installazione:** L'app è automaticamente installata e non può essere rimossa dall'utente

**Bloccata:** L'app è bloccata e non può essere installata. Se l'app era precedentemente installata con una policy precedente, verrà disinstallata.

**Richiesta per il setup:** L'app viene installata automaticamente e non può essere rimossa dall'utente, inoltre il processo di configurazione non terminerà finché l'app non è stata installata.

**Kiosk:** l'app viene installata automaticamente in modalità kiosk: è impostata come Home Intent predefinito e messa in whitelist per la modalità *lock task*. La configurazione del dispositivo non verrà completata fino all'installazione dell'app. Dopo l'installazione, gli utenti non saranno in grado di rimuovere l'app. Puoi impostare questo **tipo di installazione** solo per una singola app per policy. Se presente nella policy, la barra di stato verrà automaticamente disabilitata. Per maggiori informazioni si prega di leggere la pagina dedicata alla [Modalità Kiosk](#).

## 8.2. Modalità di aggiornamento automatico

Controlla la modalità di aggiornamento automatico per l'app.

**Predefinita:** l'app viene aggiornata automaticamente con priorità bassa per ridurre al minimo l'impatto sull'utente. L'app viene aggiornata quando vengono soddisfatti tutti i seguenti vincoli: (1) il dispositivo non viene utilizzato attivamente, (2) il dispositivo è connesso a una rete senza limiti di dati, (3) il dispositivo è in carica. Il dispositivo viene informato di un nuovo aggiornamento entro 24 ore dalla sua pubblicazione da parte dello sviluppatore, dopodiché l'app viene aggiornata la volta successiva che vengono soddisfatti i vincoli di cui sopra.

**Posticipata:** l'app non viene aggiornata automaticamente per un massimo di 90 giorni dopo che l'app diventa obsoleta. 90 giorni dopo che l'app diventa obsoleta, l'ultima versione disponibile viene installata automaticamente con priorità bassa (vedere Modalità di aggiornamento automatico **Predefinita**). Dopo che l'app è stata aggiornata, non viene aggiornata di nuovo automaticamente fino a 90 giorni dopo che diventa nuovamente obsoleta. L'utente può comunque aggiornare manualmente l'app dal Play Store in qualsiasi momento.

**Alta priorità:** l'app viene aggiornata il prima possibile. Non vengono applicati vincoli. Il dispositivo viene avvisato immediatamente di un nuovo aggiornamento non appena diventa disponibile.

### 8.3. Version code minimo

La versione minima dell'app in esecuzione sul dispositivo. Se impostato, il dispositivo tenta di aggiornare l'app almeno a questo version code. Se l'app non è aggiornata, il dispositivo conterrà un **dettaglio di non conformità** con il **motivo della non conformità** impostato ad **APP\_NOT\_UPDATED**. L'app deve essere già pubblicata su Google Play con un codice di versione maggiore o uguale a questo valore. Per ogni policy, al massimo 20 app possono specificare un version code minimo.

### 8.4. Ambiti delegati

Gli ambiti delegati all'app da Android Device Policy. Puoi concedere ad altre app una selezione di permessi Android speciali:

**Installazione certificati:** concede l'accesso all'installazione e alla gestione dei certificati.

**Configurazioni gestite:** concede l'accesso alla gestione delle configurazioni gestite.

**Blocca disinstallazione:** concede l'accesso al blocco della disinstallazione.

**Permessi:** concede l'accesso alle policy dei permessi e allo stato di concessione dei permessi.

**Accesso ai pacchetti:** concede l'accesso allo stato di accesso ai pacchetti.

**App di sistema:** concede l'accesso per abilitare o disabilitare le app di sistema.

## 8.5. Policy di default dei permessi

La policy predefinita per tutte le autorizzazioni richieste dall'app. Se specificata, sostituisce la **Policy di default dei permessi** che si applica a tutte le app. Non sovrascrive le **Policy dei permessi** che si applicano a tutte le app.

**Chiedi (impostazione predefinita):** richiede all'utente di concedere un permesso.

**Concedi:** concedi automaticamente un permesso.

**Nega:** nega automaticamente un permesso.

## 8.6. App di lavoro e personale connesse

Controlla se l'app può comunicare con se stessa attraverso i profili di lavoro e personale di un dispositivo, previo consenso dell'utente (Android 11+).

**Non consentito (default):** impedisce all'app di comunicare tra i profili.

**Consentito:** consente all'app di comunicare tra i profili dopo aver ricevuto il consenso dell'utente.

## 8.7. Disabilitata

Indica se l'app è disabilitata. Se disabilitata, i dati dell'app vengono comunque conservati.

## 8.8. Configurazione gestita

Per configurare le impostazioni gestite dell'app, fare clic sul pulsante **Abilita configurazione gestita**. Se per l'app è già impostata una configurazione gestita, è possibile modificare la configurazione con il pulsante **Configurazione gestita**, oppure eliminarla con il pulsante **Rimuovi configurazione**.

L'opzione **Configurazione gestita** è disponibile solo per app che supportano tale funzionalità.

## 8.9. Policy dei permessi

Concessioni o rifiuti di autorizzazioni esplicite per l'app. Questi valori sostituiscono le **Policy di default dei permessi** e le **Policy dei permessi** che si applicano a tutte le app.

## 8.10. Track IDs

Elenco dei track ID dei gruppi di test chiusi dell'app a cui un dispositivo può accedere. Se vengono selezionati più track ID, i dispositivi ricevono l'ultima versione tra tutte le track accessibili. Se non viene selezionato alcun track ID, i dispositivi hanno accesso solo al track di produzione dell'app.

L'opzione **Track IDs** è disponibile solo per le app che hanno almeno un track ID disponibile per la tua organizzazione. Per maggiori informazioni su come aggiungere la tua organizzazione ad un track di testing chiuso leggi [qui](#).

## 9. Selezione della chiave privata

Consente di mostrare l'interfaccia utente sul dispositivo per consentire a un utente di scegliere un alias di chiave privata se non sono presenti regole corrispondenti in **Scegli le regole della chiave privata**.

Per i dispositivi con Android 8 e inferiore, questa opzione potrebbe rendere vulnerabili le chiavi aziendali.

## 10. Scegli le regole della chiave privata

Controlla l'accesso delle app alle chiavi private. La regola determina quale chiave privata, se presente, Android Device Policy concede all'app specificata. L'accesso viene concesso quando l'app invoca `KeyChain.choosePrivateKeyAlias` (o eventuali overload) per richiedere un alias di chiave privata per un determinato URL o per regole che non sono specifiche dell'URL (ovvero, se `urlPattern` non è impostato o è impostato su stringa vuota o `.*`) su Android 11 e versioni successive, in modo che l'app possa invocare direttamente `KeyChain.getPrivateKey`, senza dover prima invocare `KeyChain.choosePrivateKeyAlias`. Quando un'app invoca `KeyChain.choosePrivateKeyAlias` se c'è il match con più di un `choosePrivateKeyRules`, l'ultima regola matchata definisce quale key alias restituire.

### 10.1. Alias di chiave privata

L'alias della chiave privata da utilizzare.

### 10.2. Pattern URL

Il pattern URL da confrontare con l'URL della richiesta. Se non impostato o vuoto, corrisponde a tutti gli URL. Usa la sintassi delle espressioni regolari di `java.util.regex.Pattern`.

### 10.3. Nomi dei pacchetti

I nomi dei pacchetti a cui si applica questa regola. L'hash del certificato di firma per ogni app viene verificato rispetto all'hash fornito da Play. Se non vengono specificati nomi di pacchetto, l'alias viene fornito a tutte le app che invocano `KeyChain.choosePrivateKeyAlias` o eventuali overload (ma non senza invocare `KeyChain.choosePrivateKeyAlias`, anche su Android 11 e versioni successive). Qualsiasi app con lo stesso UID Android di un pacchetto specificato qui avrà accesso quando invoca `KeyChain.choosePrivateKeyAlias`.

Per eliminare un'app, clicca sull'icona del **cestino**, nella parte inferiore della scheda dell'app.

# Modalità kiosk

Con la modalità kiosk puoi limitare la funzionalità del dispositivo a una singola app o a più app. La scelta tra la modalità kiosk con app singola e multi-app dipende dai tuoi obiettivi aziendali.

In **modalità kiosk con app singola**, un dispositivo è configurato per una singola applicazione e non consente agli utenti finali di accedere ad altre app sul dispositivo. Inoltre non possono uscire dall'app, rendendolo un dispositivo dedicato per quella specifica app. Per abilitare questa modalità, specifica un'app nella sezione **Gestione app** con **Tipo di installazione** impostato a **Kiosk**.

In **modalità kiosk multi-app**, i dispositivi possono accedere a più applicazioni. Gli utenti finali possono navigare tra più app tramite un launcher personalizzato. Per abilitare questa modalità, attiva l'opzione **Launcher personalizzato Kiosk**.

Quando la modalità kiosk è abilitata, puoi anche configurare se gli utenti finali potranno accedere ad alcune funzionalità del sistema, come le impostazioni di sistema, la barra di stato e altro.

## Launcher personalizzato Kiosk

Se il launcher personalizzato kiosk è abilitato. Ciò sostituisce la schermata iniziale con un launcher che blocca il dispositivo alle app installate tramite l'impostazione **Gestione app**. Le app vengono visualizzate su una singola pagina in ordine alfabetico.

## Azioni del pulsante di accensione

Imposta il comportamento di un dispositivo in modalità kiosk quando un utente tiene premuto a lungo il pulsante di accensione.

**Predefinito:** non specificato, corrisponde a **Disponibile**.

**Disponibile:** il menu di accensione (ad es. Spegni, Riavvia) viene visualizzato quando un utente preme a lungo il pulsante di accensione di un dispositivo in modalità kiosk.

**Bloccato:** il menu di accensione (ad es. Spegni, Riavvia) non viene visualizzato quando un utente preme a lungo il pulsante di accensione di un dispositivo in modalità kiosk. Nota: questo potrebbe impedire agli utenti di spegnere il dispositivo.

## Avvisi di errore di sistema

Specifica se le finestre degli errori di sistema per le app che si sono arrestate in modo anomalo o che non rispondono sono bloccate in modalità kiosk. Se bloccato, il sistema forza l'arresto dell'app come se l'utente scegliesse l'opzione "termina app" nell'interfaccia utente.

**Predefinito:** non specificato, corrisponde a **Bloccato**.

**Bloccato:** Tutte le finestre degli errori di sistema, come crash e app che non rispondono (ANR) sono bloccate. Se bloccato, il sistema è bloccato. Se bloccato, il sistema forza l'arresto dell'app come se l'utente chiudesse l'app.

**Abilitato:** Tutte le finestre degli errori di sistema, come crash e app che non rispondono (ANR) sono visualizzate

## Navigazione di sistema

Specifica quali funzionalità di navigazione sono abilitate (ad es. Home, pulsante app recenti) in modalità kiosk.

**Predefinito:** non specificato, corrisponde a **Disabilitato**.

**Abilitato:** I pulsanti Home e app recenti sono abilitati.

**Disabilitato:** I pulsanti Home e app recenti non sono accessibili.

**Solo Home:** Solo il pulsante Home è abilitato.

## Barra di stato

Specifica se le informazioni di sistema e le notifiche sono disabilitate in modalità kiosk.

**Predefinito:** non specificato, corrisponde a **Disabilitato**.

**Abilitato:** informazioni di sistema e notifiche sono mostrate nella barra di stato in modalità kiosk. Nota: Affinché questa policy abbia effetto, il pulsante Home deve essere abilitato usando `kioskCustomization.systemNavigation`.

**Disabilitato:** informazioni di sistema e notifiche sono disabilitate in modalità kiosk.

**Solo sistema:** solo le informazioni di sistema sono mostrate nella barra di stato.



## Impostazioni del dispositivo

Specifica se l'app Impostazioni è consentita in modalità kiosk.

**Predefinito:** non specificato, corrisponde a **Consentito**.

**Consentito:** l'accesso all'app Impostazioni è consentito nella modalità kiosk.

**Bloccato:** l'accesso all'app Impostazioni non è consentito nella modalità kiosk.

# Sicurezza

In questa sezione è possibile configurare le policy relative alla sicurezza.

## 1. Tempo massimo per bloccare

Tempo massimo (in secondi) di inattività dell'utente fino al blocco del dispositivo. Un valore pari a 0 indica che non vi è alcuna restrizione.

## 2. Rimani acceso durante la ricarica

Le modalità di ricarica per le quali il dispositivo rimane con lo schermo acceso. Quando si utilizza questa impostazione, si consiglia di deselezionare **Tempo massimo per bloccare** in modo che il dispositivo non si blocchi da solo mentre lo schermo è acceso.

**Caricabatterie CA:** la fonte di alimentazione è un caricabatterie CA.

**Porta USB:** la fonte di alimentazione è una porta USB.

**Caricabatterie wireless:** la fonte di alimentazione è wireless.

## 3. Keyguard disabilitato

Se il keyguard (blocco schermo) è disabilitato.

## 4. Requisiti della password

Policy sui requisiti della password. È possibile impostare policy diverse per il **profilo di lavoro** o per i **dispositivi completamente gestiti** impostando il campo **Ambito**.

### 4.1. Ambito

L'ambito a cui si applica il requisito della password.

**Auto:** l'ambito non è specificato. I requisiti della password vengono applicati al profilo di lavoro per i dispositivi del profilo di lavoro e all'intero dispositivo per i dispositivi completamente gestiti o dedicati.

**Dispositivo:** i requisiti della password sono applicati soltanto al dispositivo.

**Profilo di lavoro:** i requisiti della password sono applicati soltanto al profilo di lavoro.

## 4.2. Lunghezza cronologia password

La lunghezza della cronologia delle password. Dopo aver impostato questo campo, l'utente non sarà in grado di inserire una nuova password uguale a qualsiasi password nella cronologia. Un valore pari a 0 indica che non vi è alcuna restrizione.

## 4.3. Numero massimo di password errate per il wipe

Numero di password di sblocco del dispositivo errate che possono essere immesse prima che un dispositivo venga formattato alle impostazioni di fabbrica. Un valore pari a 0 indica che non vi è alcuna restrizione.

## 4.4. Scadenza password

Questa impostazione obbliga l'utente ad aggiornare periodicamente la propria password, dopo il numero di giorni specificato.

## 4.5. Richiedi sblocco con password

Il periodo di tempo durante il quale un dispositivo o un profilo di lavoro che è stato sbloccato utilizzando una forma di autenticazione forte (password, PIN, sequenza) può essere sbloccato utilizzando qualsiasi altro metodo di autenticazione (ad es. impronta digitale, trust agent, volto). Allo scadere del periodo di tempo specificato, è possibile utilizzare solo forme di autenticazione forti per sbloccare il dispositivo o il profilo di lavoro.

**Valore predefinito del dispositivo:** Il periodo di tempo è impostato al valore predefinito del dispositivo.

**Ogni giorno:** Il periodo di tempo è impostato a 24 ore.

## 4.6. Qualità della password

La qualità della password richiesta.

**Nessuna:** Non ci sono requisiti per la password.

**Debole:** il dispositivo deve essere protetto con una tecnologia di riconoscimento biometrico a bassa sicurezza, come minimo. Ciò include tecnologie in grado di riconoscere l'identità di un individuo che sono approssimativamente equivalenti a un PIN di 3 cifre (il falso rilevamento è

inferiore a 1 su 1.000).

**Qualsiasi:** è richiesta una password, ma non ci sono restrizioni sul contenuto di essa.

**Numerica:** la password deve contenere caratteri numerici.

**Numerica complessa:** la password deve contenere caratteri numerici senza ripetizioni (4444) o sequenze di caratteri ordinate (1234, 4321, 2468).

**Alfabetica:** la password deve contenere caratteri alfabetici (o simboli).

**Alfanumerica:** la password deve contenere sia caratteri numerici che alfabetici (o simboli).

**Complessa:** la password deve soddisfare i requisiti minimi specificati in `passwordMinimumLength`, `passwordMinimumLetters`, `passwordMinimumSymbols`, ecc. Ad esempio, se `passwordMinimumSymbols` è 2, la password deve contenere almeno due simboli.

## 4.7. Lunghezza minima

La lunghezza minima consentita per la password. Un valore di 0 indica che non ci sono restrizioni.

## 4.8. Lettere minime

Il minimo numero di lettere richiesto nella password.

## 4.9. Lettere minuscole minime

Il minimo numero di lettere minuscole richiesto nella password.

## 4.10. Lettere maiuscole minime

Il minimo numero di lettere maiuscole richiesto nella password.

## 4.11. Caratteri non alfabetici minimi

Il minimo numero di caratteri non alfabetici (numeri o simboli) richiesto nella password.

## 4.12. Cifre numeriche minime

Il minimo numero di cifre numeriche richiesto nella password.

## 4.13. Simboli minimi

Il minimo numero di simboli richiesto nella password.

## 5. Ripristino delle impostazioni di fabbrica disabilitato

Se il ripristino delle impostazioni di fabbrica è disabilitato. Si applica solo ai dispositivi completamente gestiti.

## 6. Protezione ripristino impostazioni di fabbrica

Indirizzi e-mail degli amministratori del dispositivo per la protezione del ripristino delle impostazioni di fabbrica. Quando il dispositivo subisce un ripristino delle impostazioni di fabbrica non autorizzato, sarà necessario che uno di questi amministratori acceda con l'e-mail e la password dell'account Google per sbloccare il dispositivo. Se non viene specificato alcun amministratore, il dispositivo non fornirà la protezione per il ripristino dei dati di fabbrica. Si applica solo ai dispositivi completamente gestiti.

## 7. Funzioni di blocco schermo

Funzionalità del keyguard (blocco schermo) che possono essere disabilite.

### 7.1. Disabilita tutto

Disabilita tutte le attuali e future personalizzazioni del keyguard.

### 7.2. Disabilita la fotocamera

Disabilita la fotocamera sulle schermate di blocco sicure (e.g. PIN).

### 7.3. Disabilita le notifiche

Disabilita la visualizzazione di tutte le notifiche sulle schermate di blocco sicure.

### 7.4. Disabilita le notifiche non modificate

Disabilita le notifiche non modificate sulle schermate di blocco sicure.

### 7.5. Ignora lo stato del trust agent

Ignora lo stato del trust agent sulle schermate di blocco sicure.

### 7.6. Disabilita l'impronta digitale

Disabilita il sensore di impronte digitali sulle schermate di blocco sicure.

## 7.7. Disabilita l'inserimento del testo nelle notifiche

Disabilita l'inserimento di testo nelle notifiche sulle schermate di blocco sicure.

## 7.8. Disabilita autenticazione con il volto

Disabilita l'autenticazione tramite il volto sulle schermate di blocco sicure.

## 7.9. Disabilita autenticazione con l'iride

Disabilita l'autenticazione tramite l'iride sulle schermate di blocco sicure.

## 7.10. Disabilita tutte le autenticazioni biometriche

Disabilita tutti i tipi di autenticazione biometrica sulle schermate di blocco sicure.

# Multimedia

## Fotocamera disattivata

Se tutte le fotocamere del dispositivo sono disabilitate.

## Acquisizione dello schermo disattivata

Se l'acquisizione dello schermo è disabilitata.

## Regola il volume disattivato

Se la regolazione del volume principale è disabilitata.

## Montare il supporto fisico disabilitato

Se è disabilitata la possibilità per l'utente di montare il supporto fisico esterno.

## Riattiva microfono disattivato

Se il microfono è disattivato e la regolazione del volume del microfono è disabilitata.

## Trasferimento file USB disattivato

Se il trasferimento di file tramite USB è disabilitato.

# Cellulare

## Configurazione Cell Broadcast disattivata

Se la configurazione di Cell Broadcast è disabilitata.

## Configurazione reti mobili disabilitata

Se la configurazione delle reti mobili è disabilitata.

## Dati in roaming disattivati

Se i servizi dati in roaming sono disabilitati.

## Chiamate in uscita disattivate

Se le chiamate in uscita sono disabilitate.

## SMS disabilitati

Se l'invio e la ricezione di messaggi SMS è disabilitato.



# Reti

Gli amministratori IT possono eseguire il provisioning silenzioso delle configurazioni Wi-Fi aziendali sui dispositivi gestiti. Le configurazioni Wi-Fi possono anche essere bloccate, per impedire agli utenti di creare configurazioni o modificare configurazioni aziendali.

## 1. Bluetooth disattivato

Se il Bluetooth è disabilitato. Preferisci questa impostazione a `bluetoothConfigDisabled` perché `bluetoothConfigDisabled` può essere ignorato dall'utente.

## 2. Condivisione dei contatti Bluetooth disabilitata

Se la condivisione dei contatti Bluetooth è disabilitata.

## 3. Configurazione Bluetooth disabilitata

Se la configurazione del Bluetooth è disabilitata.

## 4. Configurazione tethering disabilitata

Se la configurazione del tethering e degli hotspot portatili è disabilitata.

## 5. Configurazione Wi-Fi disabilitata

Se la configurazione degli access point Wi-Fi è disabilitata.

## 6. Ripristino della rete disabilitato

Se il reset delle impostazioni di rete è disabilitato.

## 7. Raggio in uscita disabilitato

Se l'utilizzo di NFC per trasmettere dati dalle app è disabilitato.

## 8. App VPN sempre attiva

Specificare una VPN sempre attiva per garantire che i dati delle app gestite specificate passino sempre attraverso una VPN configurata.

Nota: questa funzionalità richiede la distribuzione di un client VPN che supporti le funzionalità Always On e VPN per-app.

## 9. Blocco VPN

Non consente il collegamento in rete quando la VPN non è connessa.

## 10. Configurazione VPN disabilitata

Se la configurazione della VPN è disabilitata.

## 11. Servizio di rete preferenziale

Controlla se il servizio di rete preferenziale è abilitato nel profilo di lavoro. Ad esempio, un'organizzazione può stipulare un accordo con un operatore per l'invio di tutti i dati di lavoro dai dispositivi dei propri dipendenti tramite un servizio di rete dedicato all'uso aziendale. Un esempio di servizio di rete preferenziale supportato è l'Enterprise Network Slicing sulle reti 5G. Questa opzione non ha alcun effetto sui dispositivi completamente gestiti.

**Disabilitato:** il servizio di rete preferenziale è disabilitato sul profilo di lavoro.

**Abilitato:** il servizio di rete preferenziale è abilitato sul profilo di lavoro.

## 12. Proxy globale consigliato

Il proxy HTTP globale indipendente dalla rete. In genere i proxy devono essere configurati per rete in openNetworkConfiguration. Tuttavia, per configurazioni insolite come il filtraggio interno

generale può essere utile un proxy HTTP globale. Se il proxy non è accessibile, l'accesso alla rete potrebbe interrompersi. Il proxy globale è solo una raccomandazione e alcune app potrebbero ignorarlo.

**Disabilitato**

**Proxy diretto**

**Autoconfigurazione proxy (PAC)**

## 12.1 Host

L'host del proxy diretto.

## 12.2 Porta

La porta del proxy diretto.

## 12.3. URI PAC

L'URI dello script PAC usato per configurare il proxy.

## 12.4. Host esclusi

Per un proxy diretto, gli host per cui il proxy viene bypassato. I nomi di host possono contenere wildcard come ad esempio \*.example.com.

# 13. Configurazioni Wi-Fi

Configurazione di rete per il dispositivo.

## 13.1. Nome configurazione

## 13.2. SSID

## 13.3. Connessione automatica

Indica se la rete deve essere connessa automaticamente quando è visibile.

## 13.4. Transizione veloce

Indica se il client dovrebbe usare Fast Transition (IEEE 802.11r-2008) con la rete.

## 13.5. SSID nascosto

Indica se l'SSID sarà trasmesso.

## 13.6. Sicurezza

**WEP (chiave precondivisa)**

**WPA/WPA2/WPA3-Personal (chiave precondivisa)**

**WPA/WPA2/WPA3-Enterprise (Extensible Authentication Protocol)**

## 13.7. Frase d'accesso

Password, per le opzioni di sicurezza **chiave precondivisa**.

## 13.8. Metodo EAP

Metodo di Extensible Authentication Protocol

**EAP-TLS**

**EAP-TTLS**

**PEAP**

**EAP-SIM**

**EAP-AKA**

## 13.9. Autenticazione di fase 2

**MSCHAPv2**

**PAP**

## 13.10. Credenziali EAP dagli utenti

Se abilitato, il sistema applicherà automaticamente le credenziali EAP sui dispositivi in base all'utente. È possibile configurare le credenziali dell'utente nella sezione **Utenti**.

## 13.11. Certificato Client

Certificato da utilizzare per l'autenticazione dei dispositivi con questa rete Wi-Fi. Per maggiori informazioni leggi la sezione **Gestione dei certificati**.

## 13.12. Identità

Identità dell'utente. Per i protocolli esterni di tunneling (PEAP, EAP-TTLS), questo viene utilizzato per l'autenticazione all'interno del tunnel e l'**identità anonima** viene utilizzata per l'identità EAP all'esterno del tunnel. Per i protocolli esterni senza tunneling, viene utilizzato per l'identità EAP. Questo valore è soggetto alle espansioni di stringa.

### 13.13. Identità anonima

Solo per i protocolli di tunneling, indica l'identità dell'utente presentato al protocollo esterno. Questo valore è soggetto alle espansioni di stringa. Se non specificato, utilizzare una stringa vuota.

### 13.14. Password

Password dell'utente. Se non specificato, per impostazione predefinita viene richiesto all'utente.

### 13.15. Certificati CA del server

Elenco dei certificati CA da utilizzare per verificare la catena di certificati dell'host. Almeno uno dei certificati CA deve corrispondere. Se non impostato, il client non verifica che il certificato del server sia firmato da una CA specifica. Potrebbe comunque essere applicata una verifica utilizzando i certificati CA del sistema. Per maggiori informazioni leggi la sezione **Gestione dei certificati**.

# Sistema

## 1. Livello API minimo

Il livello API Android minimo consentito.

## 2. Policy di crittografia

Se la crittografia è abilitata.

**Predefinito:** questo valore viene ignorato, ovvero non è richiesta alcuna crittografia.

**Abilitato senza password:** crittografia richiesta ma nessuna password richiesta per l'avvio.

**Abilitato con password:** crittografia richiesta con password richiesta per l'avvio.

## 3. Data e ora automatiche

Se la data, l'ora e il fuso orario automatici sono abilitati su un dispositivo di proprietà dell'azienda.

**Predefinito:** non specificato. L'impostazione predefinita è **Scelta dell'utente**.

**Scelta dell'utente:** la data, l'ora e il fuso orario automatici sono lasciati alla scelta dell'utente.

**Applicato:** applica la data, l'ora e il fuso orario automatici sul dispositivo.

## 4. Modalità posizione

Il grado di rilevamento della posizione abilitato. L'utente può modificare il valore a meno che l'utente non sia altrimenti bloccato dall'accesso alle impostazioni del dispositivo. Si applica solo ai dispositivi di proprietà dell'azienda.

**Predefinito:** l'impostazione predefinita è **Scelta dell'utente**.

**Scelta dell'utente:** l'impostazione della posizione non è limitata sul dispositivo. Nessun comportamento specifico è impostato o imposto.

**Applicato:** abilita l'impostazione della posizione sul dispositivo.

**Disabilitato:** disabilita l'impostazione della posizione sul dispositivo.

## 5. Impostazioni sviluppatore

Controlla l'accesso alle impostazioni dello sviluppatore: opzioni sviluppatore e avvio sicuro.

**Predefinito:** non specificato. L'impostazione predefinita è **Disabilitato**.

**Disabilitato:** disabilita tutte le impostazioni sviluppatore e impedisce all'utente di accedervi.

**Consentito:** consente tutte le impostazioni dello sviluppatore. L'utente può accedere e, facoltativamente, configurare le impostazioni.

## 6. Common Criteria Mode

Controlla il Common Criteria Mode: standard di sicurezza definiti nei Common Criteria for Information Technology Security Evaluation (CC). L'abilitazione del Common Criteria Mode aumenta alcuni componenti di sicurezza su un dispositivo, inclusa la crittografia AES-GCM delle chiavi Bluetooth a lungo termine e gli archivi delle configurazioni Wi-Fi. Avviso: la modalità Common Criteria applica un modello di sicurezza rigoroso, in genere richiesto solo per i prodotti IT utilizzati nei sistemi di sicurezza nazionale e in altre organizzazioni altamente sensibili. L'utilizzo standard del dispositivo potrebbe risentirne. Abilitare solo se necessario.

**Predefinito:** non specificato. L'impostazione predefinita è **Disabilitato**.

**Disabilitato:** impostazione predefinita. Disabilita il Common Criteria Mode.

**Abilitato:** abilita il Common Criteria Mode.

## 7. Condividi la posizione disabilitato

Se la condivisione della posizione è disabilitata per le app di lavoro. Sui dispositivi di proprietà personale, disabilita la posizione per il profilo di lavoro. Sui dispositivi completamente gestiti, disattiva la posizione sull'intero dispositivo (ignorando anche l'impostazione "Modalità posizione").

## 8. Crea finestre disabilitato

Se la creazione di finestre oltre alle finestre delle app è disabilitata. Questa opzione impedisce la visualizzazione delle seguenti interfacce utente di sistema: toast e snackbar, attività telefoniche (come le chiamate in arrivo) e attività telefoniche prioritarie (come le chiamate in corso), avvisi di sistema, errori di sistema e overlay di sistema.

## 9. Network escape hatch

Se il network escape hatch è abilitato. Se non è possibile stabilire una connessione di rete al momento dell'avvio, l'escape hatch richiede all'utente di connettersi temporaneamente a una rete per aggiornare le policy del dispositivo. Dopo aver applicato la policy, la rete temporanea verrà dimenticata e il dispositivo continuerà ad avviarsi. Ciò previene l'impossibilità di connettersi a una rete se non è presente una rete adatta nell'ultima policy e il dispositivo si avvia con un'app in modalità lock task, o per qualsiasi altro motivo l'utente non può accedere alle impostazioni del dispositivo.

## 10. Attività predefinite

Un elenco di attività predefinite per la gestione degli Intent che corrispondono a un particolare IntentFilter. Ad esempio, questa funzione consentirebbe agli amministratori IT di scegliere quale app del browser apre automaticamente i collegamenti Web o quale launcher viene utilizzato quando si tocca il pulsante Home.

### 10.1. Attività del ricevitore

L'attività che dovrebbe essere il gestore dell'Intent predefinito. Dovrebbe essere il nome di un componente Android, ad es. `com.android.enterprise.app/.MainActivity`. In alternativa, il valore può essere il nome del pacchetto di un'app, che fa sì che Android Device Policy scelga un'attività appropriata dall'app per gestire l'Intent.

### 10.2. Azione

Le azioni dell'Intent da matchare nel filtro. Se nel filtro sono incluse azioni, l'azione di un Intent deve essere uno di quei valori affinché corrisponda. Se non sono incluse azioni, l'azione dell'Intent viene ignorata.

### 10.3. Categoria

Le categorie di Intent da matchare nel filtro. Un Intent include le categorie che richiede, che devono essere tutte incluse nel filtro per avere un match. In altre parole, l'aggiunta di una categoria al filtro non ha alcun impatto sul match a meno che tale categoria non sia specificata



nell'Intent.

## 11. Metodi di input permessi

Specifica i metodi di input permessi.

**Tutto consentito:** nessuna restrizione applicata. Tutti i metodi di input sono permessi.

**Solo di sistema:** sono consentiti solo i metodi di input integrati del sistema.

**Solo di sistema e forniti:** sono consentiti solo i metodi di input integrati del sistema e quelli indicati.

### 11.1. Metodi di input consentiti

Package name dei metodi di input che sono consentiti. Si applica solo quando **Metodi di input permessi** è impostato a **Solo di sistema e forniti**.

## 12. Servizi di accessibilità permessi

Specifica i servizi di accessibilità permessi.

**Tutto consentito:** qualsiasi servizio di accessibilità può essere usato.

**Solo di sistema:** sono consentiti solo i servizi di accessibilità integrati del sistema.

**Solo di sistema e forniti:** sono consentiti solo i servizi di accessibilità integrati del sistema e quelli indicati.

### 12.1. Servizi di accessibilità consentiti

Servizi di accessibilità che possono essere usati. Si applica solo quando **Servizi di accessibilità permessi** è impostato a **Solo di sistema e forniti**.

## 13. Policy di aggiornamento sistema

Configurazione per la gestione degli aggiornamenti di sistema.

**Predefinito:** seguire il comportamento di aggiornamento predefinito per il dispositivo, che in genere richiede che l'utente accetti gli aggiornamenti di sistema.

**Automatico:** installa automaticamente non appena è disponibile un aggiornamento.

**Finestra:** installazione automatica all'interno di una finestra di manutenzione giornaliera. Ciò configura anche le app Play da aggiornare all'interno della finestra. Questa opzione è fortemente consigliata per i dispositivi kiosk perché questo è l'unico modo in cui le app permanentemente bloccate in primo piano possono essere aggiornate da Play.

**Posticipa:** posticipa l'installazione automatica fino a un massimo di 30 giorni.

## 14. Periodi di blocco dell'aggiornamento del sistema

Un periodo di tempo che si ripete ogni anno in cui gli aggiornamenti di sistema over-the-air (OTA) vengono posticipati per bloccare la versione del sistema operativo in esecuzione su un dispositivo. Per evitare il congelamento del dispositivo a tempo indeterminato, ogni periodo di blocco deve essere separato da almeno 60 giorni.

# Gestione utenti

## Aggiungi utente disabilitato

Se l'aggiunta di nuovi utenti e profili è disabilitata.

## Modifica account disabilitato

Se l'aggiunta o la rimozione di account è disabilitata.

## Configurazione credenziali utente disabilitata

Se la configurazione delle credenziali utente è disabilitata.

## Rimuovi utente disabilitato

Se la rimozione di altri utenti è disabilitata.

## Imposta l'icona dell'utente disabilitato

Se la modifica dell'icona dell'utente è disabilitata.

## Imposta sfondo disattivato

Se la modifica dello sfondo è disabilitata.

## Tipi di account bloccati

Tipi di account che non possono essere gestiti dall'utente. Questa opzione impedisce agli utenti del dispositivo di aggiungere account non approvati.



# Uso personale

Quando esegui il provisioning di un dispositivo di proprietà dell'azienda per lavoro e uso personale, puoi specificare alcune regole per limitare il modo in cui l'utente può utilizzare il dispositivo per uso personale, al di fuori del profilo di lavoro.

Questa sezione si applica solo ai dispositivi di proprietà dell'azienda con profilo di lavoro. Non avranno alcun effetto sui dispositivi completamente gestiti o di proprietà personale.

## 1. Fotocamera disattivata

Se la fotocamera è disabilitata.

## 2. Cattura schermo disattivata

Se la cattura dello schermo (screenshot / screen recording) è disabilitata.

## 3. Numero massimo di giorni senza lavoro

Controlla per quanto tempo il profilo di lavoro può rimanere disattivato.

## 4. Modalità Play Store

Questa modalità controlla quali app sono consentite o bloccate per l'utente nel Play Store del profilo personale.

**Blocklist (impostazione predefinita):** Tutte le app sono disponibili e qualsiasi app che non dovrebbe essere presente sul dispositivo deve essere esplicitamente contrassegnata come **Bloccato** nella sezione **Applicazioni**.

**Lista consentita:** Solo le app esplicitamente specificate nella sezione **Applicazioni** con **Tipo di installazione** impostato a **Disponibile** possono essere installate nel profilo

personale.

## 5. Applicazioni

Elenco delle applicazioni che devono essere consentite o bloccate sul profilo personale. Il comportamento del contenuto della lista dipende dal valore impostato nella **Modalità Play Store**.

Per aggiungere una nuova app dal Play Store, clicca sull'icona +.

### 5.1. Tipo di installazione

Tipi di modalità di installazione che può avere un'applicazione del profilo personale.

**Bloccato:** l'app è bloccata e non può essere installata nel profilo personale.

**Disponibile:** l'app è disponibile per l'installazione nel profilo personale.

## 6. Tipi di account bloccati

Tipi di account che non possono essere gestiti dall'utente. Questa opzione impedisce agli utenti del dispositivo di aggiungere account non approvati sul proprio profilo personale.

# Policy cross-profile

Si applica solo ai dispositivi con profili personali e di lavoro.

## Mostra i contatti di lavoro nel profilo personale

Se i contatti archiviati nel profilo di lavoro possono essere visualizzati nelle ricerche dei contatti del profilo personale e nelle chiamate in arrivo.

**Consentito (impostazione predefinita):** consente ai contatti del profilo di lavoro di essere visualizzati nelle ricerche dei contatti del profilo personale e nelle chiamate in arrivo.

**Non consentito:** impedisce la visualizzazione dei contatti del profilo di lavoro nelle ricerche dei contatti del profilo personale e nelle chiamate in arrivo.

## Copia/incolla cross-profilo

Se il testo copiato da un profilo (personale o di lavoro) può essere incollato nell'altro profilo.

**Non consentito (impostazione predefinita):** impedisce agli utenti di incollare nel profilo personale il testo copiato dal profilo di lavoro. Il testo copiato dal profilo personale può essere incollato nel profilo di lavoro e il testo copiato dal profilo di lavoro può essere incollato nel profilo di lavoro.

**Consentito:** il testo copiato in uno dei profili può essere incollato nell'altro profilo.

## Condivisione dei dati cross-profilo

Se i dati di un profilo (personale o di lavoro) possono essere condivisi con le app nell'altro profilo. Controlla in modo specifico la semplice condivisione dei dati tramite intent. Gestione di altri canali di comunicazione cross-profilo, come ricerca contatti, copia/incolla, o le app di lavoro e personali connesse, sono configurate separatamente.

**Non consentito:** impedisce la condivisione dei dati dal profilo personale al profilo di lavoro e dal profilo di lavoro al profilo personale.

**Da lavoro a personale non consentito (impostazione predefinita):** impedisce agli utenti di condividere i dati dal profilo di lavoro alle app nel profilo personale. I dati personali

possono essere condivisi con le app di lavoro.

**Consentito:** i dati di entrambi i profili possono essere condivisi con l'altro profilo.



# Rapporti di stato

In questa sezione è possibile configurare quali dati devono essere recuperati dal dispositivo. I dati sullo stato sono consultabili dalla pagina **Stato dei dispositivi** della dashboard.

## Geolocalizzazione

Se il reporting della geolocalizzazione è abilitato.

## Rapporti applicativi

Se i rapporti sulle app sono abilitati. (Informazioni riportate su un'app installata)

Questa opzione è richiesta dal sistema e non può essere disabilitata.

## Includi le app rimosse

Se le app rimosse sono incluse nei rapporti sulle applicazioni.

## Impostazioni del dispositivo

Se la segnalazione delle impostazioni del dispositivo è abilitata. (Informazioni sulle impostazioni del dispositivo relative alla sicurezza sul dispositivo.)

## Informazioni software

Se la segnalazione delle informazioni sul software è abilitata. (Informazioni sul software del dispositivo.)

## Informazioni sulla memoria

Se la segnalazione della memoria è abilitata. (Un evento correlato alle misurazioni della memoria e dello storage.)

## Informazioni sulla rete

Se la segnalazione delle informazioni di rete è abilitata. (Informazioni sulla rete del dispositivo.)

## Informazioni sul display

Se i rapporti sui display sono abilitati. I dati dei rapporti non sono disponibili per i dispositivi di proprietà personale con profili di lavoro. (Informazioni sul display del dispositivo.)

## Eventi di gestione dell'alimentazione

Se la segnalazione degli eventi di gestione dell'alimentazione è abilitata. I dati dei rapporti non sono disponibili per i dispositivi di proprietà personale con profili di lavoro.

## Stato dell'hardware

Se la segnalazione dello stato dell'hardware è abilitata. I dati dei rapporti non sono disponibili per i dispositivi di proprietà personale con profili di lavoro.

## Proprietà di sistema

Se la segnalazione delle proprietà di sistema è abilitata.

## Common Criteria Mode

Se il reporting Common Criteria Mode è abilitato.

# Varie

## 1. Gioco easter egg disabilitato

Se il gioco Easter egg nelle Impostazioni è disabilitato.

## 2. Salta i suggerimenti per il primo utilizzo

Contrassegna per saltare i suggerimenti al primo utilizzo. L'amministratore aziendale può abilitare la raccomandazione di sistema affinché le app saltino l'esercitazione per l'utente e altri suggerimenti introduttivi al primo avvio.

## 3. Messaggio di supporto breve

Un messaggio visualizzato all'utente nella schermata delle impostazioni ogni volta che la funzionalità è stata disabilitata dall'amministratore. Se il messaggio è più lungo di 200 caratteri potrebbe essere troncato.

## 4. Messaggio di supporto lungo

Un messaggio visualizzato all'utente nella schermata delle impostazioni dell'amministratore del dispositivo.

## 5. Informazioni sulla schermata di blocco del proprietario

Le informazioni sul proprietario del dispositivo da mostrare nella schermata di blocco.

## 6. Azioni di setup

Azioni da intraprendere durante il processo di configurazione. Durante l'enrollment, puoi richiedere all'utente di aprire una o più app necessarie per la configurazione del dispositivo.

## 6.1. Avvia app

Package name dell'app da avviare

## 6.2. Titolo

Titolo del messaggio rivolto all'utente per spiegare perché è necessario avviare l'app.

## 6.3. Descrizione

Testo del messaggio rivolto all'utente per spiegare perché è necessario avviare l'app.

# Regole di applicazione delle policy

Se un dispositivo o un profilo di lavoro non è conforme a una delle impostazioni delle policy elencate di seguito, Android Device Policy blocca immediatamente l'utilizzo del dispositivo o del profilo di lavoro per impostazione predefinita:

- **Requisiti della password**
- **Policy di crittografia**
- **Keyguard disabilitato**
- **Metodi di input permessi**
- **Servizi di accessibilità permessi**

Se il dispositivo o il profilo di lavoro rimane non conforme dopo 10 giorni, Android Device Policy ripristinerà i dati di fabbrica del dispositivo o eliminerà il profilo di lavoro.

In questa sezione è possibile ignorare le regole di applicazione della compliance predefinite o aggiungerne di nuove.

## Regole

Elenco di regole che definiscono il comportamento quando una determinata policy non può essere applicata al dispositivo.

### Nome dell'impostazione

Il criterio di primo livello da applicare. Ad esempio, **Applicazioni** o **Requisiti della password**.

### Blocco dopo giorni

Numero di giorni in cui c'è non conformità alla policy prima che il dispositivo o profilo di lavoro venga bloccato. Per bloccare l'accesso immediatamente, impostare a 0. **Blocco dopo giorni** deve essere inferiore a **Cancella dopo giorni**.

### Ambito di blocco

Specifica l'ambito dell'azione di blocco. Applicabile solo a dispositivi di proprietà dell'azienda.

**Profilo di lavoro:** l'azione di blocco è applicata solo alle app nel profilo di lavoro. Le app nel profilo personale non sono interessate.

**Intero dispositivo:** l'azione di blocco è applicata all'intero dispositivo, incluse le app nel profilo personale.

## Cancella dopo giorni

Numero di giorni in cui c'è non conformità alla policy prima che il dispositivo o profilo di lavoro venga cancellato.

**Cancella dopo giorni** deve essere maggiore di **Blocco dopo giorni**.

## Mantieni la protezione del ripristino delle impostazioni di fabbrica

Se la configurazione della protezione del ripristino delle informazioni di fabbrica viene mantenuta sul dispositivo. Questa impostazione non si applica ai profili di lavoro.

# Stato dei dispositivi

# Sommario

Puoi vedere la lista dei tuoi dispositivi dalla sezione **Dispositivi** della dashboard. Per vedere i dettagli o modificare un dispositivo, clicca sull'elemento corrispondente nella tabella.

Nella pagina del dispositivo puoi vedere lo stato corrente e i dati recuperati dal dispositivo.

Alcuni dati sono recuperati solo se la categoria corrispondente è abilitata nella policy del dispositivo. Per maggiori informazioni leggi la pagina [Rapporti di stato](#)



# Comandi

Da questa sezione puoi inviare specifici comandi ad un dispositivo gestito. Nella tabella presente, puoi verificare tutti i comandi inviati in precedenza e se sono stati eseguiti con successo.

Se un dispositivo non è attualmente online, il comando verrà consegnato ed eseguito appena il dispositivo si riconnette a internet. Puoi impostare il parametro **Durata** per scegliere per quanto tempo deve restare valido un comando che non è consegnato immediatamente.

## Blocca

Blocca il dispositivo, come se fosse scaduto il timeout di spegnimento schermo.

## Riavvia

Riavvia il dispositivo. Supportato solo da API level 24+.

## Reimposta password

Reimposta la password dell'utente. Devi specificare la nuova password in **Nuova password** e **Conferma nuova password**. Inoltre ci sono queste opzioni aggiuntive:

- **Blocca adesso**: blocca il dispositivo dopo il reset della password (come con il comando **Blocca**).
- **Richiedi inserimento**: non permette ad altri amministratori di cambiare la password nuovamente finché l'utente non l'ha inserita.
- **Non chiedere le credenziali all'avvio**: non chiedere le credenziali utente all'avvio del dispositivo (e.g. per dispositivi kiosk).

## Rinunciare alla proprietà

Con questo comando gli amministratori IT possono cedere la proprietà dei dispositivi di proprietà dell'azienda al dipendente. Il profilo di lavoro del dispositivo verrà cancellato e tutte le policy del dispositivo verranno ripristinate allo stato di fabbrica, lasciando intatti i dati personali. In tal modo, l'IT perde la proprietà del dispositivo e in futuro non dovrebbe aspettarsi che il dispositivo venga registrato nuovamente.

# App private

Da questa sezione della dashboard puoi caricare le tue app private Android o creare web app da distribuire sui tuoi dispositivi.

Gli unici dettagli che devi fornire sono il titolo e l'APK di un'app. Le app private vengono approvate automaticamente per la tua organizzazione e in genere sono pronte per la distribuzione entro 10 minuti. Puoi caricare un totale di 15 app private al giorno. Tieni presente che anche le web app vengono conteggiate in questo totale.

La prima volta che pubblichi un'app privata, dovrai fornire un indirizzo email per ricevere notifiche da Play Console relative alle tue app e all'account sviluppatore Google Play. Inoltre, la versione gestita di Google Play crea automaticamente un account Play Developer per conto della tua organizzazione. Non è necessario pagare una quota di registrazione per questo account.

Le app private pubblicate tramite l'iframe:

- Non sono soggette agli stessi controlli delle altre app. Di conseguenza, non possono essere convertite in app pubbliche.
- Non sono trasferibili. Non puoi trasferire la proprietà di un'app a un altro account sviluppatore di Google Play.

Per maggiori dettagli visita la [Guida di Managed Google Play](#)

# Gestione dei certificati

Puoi controllare l'elenco dei certificati dalla sezione **Certificati** sulla dashboard. Per vedere i dettagli o modificare un certificato, clicca sulla voce selezionata nella tabella.

Per importare nuovi certificati, clicca sul pulsante **Importa certificato**. Ci sono due tipi di certificati che possono essere importati:

## Client

Formato supportato: PKCS#12 codificato in base-64

Si tratta di certificati che identificano un utente o un dispositivo sulla rete aziendale.

Ogni certificato client può essere facoltativamente assegnato a un utente specifico: questo consente l'implementazione della stessa configurazione WiFi EAP su molti dispositivi, utilizzando l'opzione **Credenziali EAP dagli utenti** nella sezione di configurazione della rete della policy. Per assegnare un utente, apri il certificato dalla tabella (fai clic sulla voce nella tabella), quindi fai clic sull'icona nel campo **Utente**.

In alternativa, puoi assegnare un certificato ad un utente dalla pagina **Utente**.

## Autorità di certificazione (CA)

Formato supportato: X.509 codificato in base-64

Si tratta di certificati che identificano una Certificate Authority. Indica al dispositivo che tutti i certificati emessi dalla CA devono essere considerati attendibili.