Policy - Android

- Riepilogo
- Gestione app
- Modalità chiosco
- Sicurezza
- Multimedia
- Cellulare
- Rete
- Sistema
- Posizione e geofence
- Gestione utenti
- Uso personale
- Policy tra profili
- Rapporti di stato
- Varie
- Regole di conformità

Riepilogo

Le policy Android sono le entità principali del sistema: definiscono le regole applicate e fatte rispettare sui dispositivi gestiti.

Puoi sfogliare le tue policy e crearne di nuove dalla sezione **Policy** della dashboard. Per aprire una policy Android, fai clic sulla riga della policy nella tabella: il sistema apre la pagina **Editor delle policy**.

Una policy può essere associata a un token di registrazione, così verrà applicata automaticamente ai dispositivi durante il processo di provisioning. Puoi anche cambiare la policy assegnata a un dispositivo dopo il provisioning.

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

> Molte opzioni della policy si applicano solo a tipi specifici di dispositivi (completamente gestiti, dedicati, profilo di lavoro) e versioni di Android. Le impostazioni non supportate possono essere ignorate dal dispositivo o segnalate come non conformi.

Layout dell'Editor delle policy

L'Editor delle policy è organizzato in una serie di sezioni espandibili. In cima alla pagina puoi sempre modificare:

- **Nome** (obbligatorio)
- **Id** (sola lettura)
- **Descrizione** (facoltativa)

Le sezioni seguenti corrispondono ai pannelli del Policy Editor (ad esempio: Gestione app, Sicurezza, Rete, Sistema, Utilizzo personale, Policy tra profili e altro). Quando apri una policy salvata, le sezioni con impostazioni modificate sono già aperte e le altre restano chiuse. Usa le pagine dei capitoli di questo manuale per comprendere in dettaglio ogni pannello.

Salvataggio, eliminazione e dispositivi associati

Usa **Salva policy** per applicare le modifiche. Il pulsante è disattivato quando non ci sono modifiche in sospeso o quando la licenza è scaduta.

Se hai aperto una policy esistente (con un Id), la pagina mostra un'azione **Elimina policy** e un elenco **Dispositivi associati** in fondo, così puoi vedere quanti dispositivi stanno attualmente usando la policy.

Gestione app

In questa sezione puoi impostare policy relative alla disponibilità delle app, all'installazione, agli aggiornamenti e alla gestione delle autorizzazioni.

> Gli account Managed Google Play vengono creati automaticamente quando i dispositivi vengono sottoposti a provisioning.

1. Modalità Play Store

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

Whitelist (predefinita): sono disponibili solo le app presenti nella policy e qualsiasi app non presente viene automaticamente disinstallata dal dispositivo. Il Play Store mostrerà solo le app disponibili.

Blacklist: tutte le app sono disponibili e qualsiasi app che non deve essere sul dispositivo va contrassegnata esplicitamente come **bloccata** nella policy delle applicazioni. Il Play Store mostrerà tutte le app, tranne quelle bloccate.

2. Policy delle app non attendibili

La policy per le app non attendibili (app provenienti da origini sconosciute) applicata sul dispositivo. Questa opzione controlla l'impostazione di sistema Android che determina se un utente può installare app al di fuori del Play Store (sideloading).

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

Solo profilo personale: per i dispositivi con profili di lavoro, consenti l'installazione di app non attendibili solo nel profilo personale del dispositivo.

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

3. Google Play Protect

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

Applicata (predefinita): abilita forzatamente la verifica delle app.

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

4. Policy delle autorizzazioni predefinita

La policy per concedere alle app le richieste di autorizzazione a runtime.

Richiedi (predefinito): chiedi all'utente di concedere un'autorizzazione.

Concedi: concedi automaticamente un'autorizzazione.

Nega: nega automaticamente un'autorizzazione.

5. Funzioni delle app

Controlla se le app sui dispositivi completamente gestiti o nei profili di lavoro possono esporre le funzioni delle app. Richiede Android 16 o versioni successive.

Consentite (predefinito): le app sui dispositivi completamente gestiti o nei profili di lavoro possono esporre le funzioni delle app.

Non consentite: le app sui dispositivi completamente gestiti o nei profili di lavoro non possono esporre le funzioni delle app.

6. Installazione delle app disabilitata

Indica se l'installazione delle app da parte dell'utente è disabilitata.

7. Disinstallazione delle app disabilitata

Indica se la disinstallazione delle applicazioni da parte dell'utente è disabilitata.

8. Policy delle autorizzazioni

Concessioni o dinieghi espliciti di autorizzazioni o gruppi per tutte le app. Questi valori hanno la precedenza sull'impostazione **Policy delle autorizzazioni predefinita**.

Usa **Aggiungi policy delle autorizzazioni** per creare voci e rimuoverle con l'azione di eliminazione.

Ogni voce include:

> **Autorizzazione/gruppo Android**: l'autorizzazione o il gruppo Android (obbligatorio), ad esempio **android.permission.READ_CALENDAR** o **android.permission_group.CALENDAR**.
>
> **Policy**: Concedi / Nega / Richiedi (usa le stesse opzioni della **Policy delle autorizzazioni predefinita**).

9. Applicazioni

Elenco delle 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 impostata su **whitelist**, sono disponibili solo le app presenti nella policy e qualsiasi app non presente viene automaticamente disinstallata dal dispositivo.

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

Per aggiungere una nuova app, fai clic sul pulsante **Aggiungi applicazioni** (o sull'icona **Aggiungi applicazioni**), seleziona **Da Managed Google Play**, quindi scegli l'app dal Play Store e fai clic sul pulsante **Seleziona** nella scheda dell'app.

Per aggiungere un'app non pubblicata su Google Play ma già presente sul dispositivo (ad esempio un'app di sistema o del produttore), fai clic su **Aggiungi applicazioni**, seleziona **Per nome del pacchetto (app preinstallate)**, digita il nome del pacchetto dell'app (ad es. **com.example.app**) e fai clic su **Aggiungi**.L'app viene aggiunta con il tipo di installazione **Installazione forzata**. Per mostrare l'app nel launcher personalizzato kiosk, il suo **Tipo di installazione** deve essere **Preinstallata** o **Installazione forzata**: con **Disponibile** l'app non viene mostrata.

> Le app non disponibili in Managed Google Play sono contrassegnate da un'icona Android nell'elenco delle applicazioni. Non possono essere installate da Google Play, quindi devono essere già presenti sul dispositivo: i dispositivi che non hanno l'app non possono installarla.

>

> 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, raccolte visivamente in una scheda:

9.1. Tipo di installazione

Il tipo di installazione da eseguire per un'app.

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

Preinstallata: l'app viene installata automaticamente e può essere rimossa dall'utente.

Installazione forzata: l'app viene installata automaticamente e non può essere rimossa dall'utente.

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

Richiesta per la configurazione: l'app viene installata automaticamente, non può essere rimossa dall'utente e impedisce il completamento della configurazione finché l'installazione non è terminata.

Kiosk: l'app viene installata automaticamente in modalità kiosk: è impostata come intent home preferito e inserita nella whitelist per la modalità lock task. La configurazione del dispositivo non sarà completata finché l'app non è installata. Dopo l'installazione, gli utenti non potranno rimuovere l'app. Puoi impostare questo **tipo di installazione** per una sola app per policy. Quando è presente nella policy, la barra di stato viene disabilitata automaticamente. Per maggiori informazioni, leggi la pagina dedicata **Modalità kiosk**.

9.2. Vincoli di installazione

Definisce una serie di restrizioni per l'installazione dell'app. Quando sono selezionati più vincoli, devono essere soddisfatti tutti perché l'app venga installata.

> Questa opzione viene mostrata solo quando il **Tipo di installazione** è **Preinstallata** o **Installazione forzata**.

Rete senza limiti di traffico: installa l'app solo quando il dispositivo è connesso a una rete senza limiti di traffico (ad es. Wi-Fi).

In carica: installa l'app solo quando il dispositivo è in carica.

Inattivo: installa l'app solo quando il dispositivo è inattivo.

9.3. Modalità di aggiornamento automatico

Controlla la modalità di aggiornamento automatico per l'app.

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

Posticipata: l'app non viene aggiornata automaticamente per un massimo di 90 giorni da quando diventa obsoleta. Trascorsi 90 giorni da quando l'app diventa obsoleta, la versione più recente disponibile viene installata automaticamente con bassa priorità (vedi la modalità di aggiornamento automatico **Predefinita**). Dopo l'aggiornamento, l'app non viene più aggiornata automaticamente fino a 90 giorni da quando 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 riceve immediatamente la notifica di un nuovo aggiornamento non appena diventa disponibile.

9.4. Codice versione minimo

La versione minima dell'app che viene eseguita sul dispositivo. Se impostata, il dispositivo tenta di aggiornare l'app almeno a questo codice versione. Se l'app non è aggiornata, il dispositivo conterrà un **dettaglio di non conformità** con **motivo di non conformità** impostato su **APP_NOT_UPDATED**. L'app deve essere già pubblicata su Google Play con un codice versione maggiore o uguale a questo valore. Al massimo 20 app possono specificare un codice versione minimo per policy.

9.5. Ambiti delegati

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

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

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

Blocco disinstallazione: concede l'accesso al blocco della disinstallazione.

Autorizzazioni: concede l'accesso alla policy delle autorizzazioni e allo stato di concessione delle autorizzazioni.

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

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

9.6. Rete preferenziale

Il servizio di rete preferenziale da usare per questa app. Se impostato, l'app utilizzerà la slice di rete aziendale specificata per le sue connessioni, quando disponibile. Deve corrispondere a una slice di rete configurata nella sezione **Configurazione del network slicing 5G** del pannello **Cellulare**.

9.7. Policy delle autorizzazioni predefinita

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

Richiedi (predefinito): chiedi all'utente di concedere un'autorizzazione.

Concedi: concedi automaticamente un'autorizzazione.

Nega: nega automaticamente un'autorizzazione.

9.8. App connessa tra lavoro e personale

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

Non consentito (predefinito): impedisce all'app di comunicare tra profili.

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

9.9. Esenzione dal blocco VPN Always On

Specifica se all'app è consentito l'accesso alla rete quando la VPN non è connessa e **blocco abilitato** è attivo. Supportato solo su dispositivi con Android 10 o versioni successive.

Applicata (predefinita): l'app rispetta l'impostazione di blocco della VPN always-on.

Esente: l'app è esente dall'impostazione di blocco della VPN always-on.

9.10. Widget del profilo di lavoro

Specifica se l'app installata nel profilo di lavoro può aggiungere widget alla schermata Home.

Consentito: l'applicazione può aggiungere widget alla schermata Home.

Non consentito: l'applicazione non può aggiungere widget alla schermata Home.

9.11. Impostazioni di controllo utente

Specifica se il controllo utente è consentito per una determinata app. Il controllo utente include azioni dell'utente come l'arresto forzato e la cancellazione dei dati dell'app (Android 11+). Se **extensionConfig** è abilitato per un'app, il controllo utente non è consentito indipendentemente da questa impostazione. Per le app kiosk, puoi usare **Consentito** per consentire il controllo utente.

> **Non specificato**: usa il comportamento predefinito dell'app per determinare se il controllo utente è consentito o meno.
>
> **Consentito**: il controllo utente è consentito per l'app.
>
> **Non consentito**: il controllo utente non è consentito per l'app.

9.12. Disabilitata

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

9.13. Consenti provider di credenziali

Indica se all'app è consentito agire come provider di credenziali su Android 14 e versioni successive.

9.14. Configurazione gestita

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

> L'opzione **Configurazione gestita** è disponibile solo per le app che supportano questa funzionalità.

9.15. Policy delle autorizzazioni

Concessioni o dinieghi espliciti delle autorizzazioni per l'app. Questi valori hanno la precedenza sulla **Policy delle autorizzazioni predefinita** e sulle **Policy delle autorizzazioni** che si applicano a tutte le app.

Usa **Aggiungi policy delle autorizzazioni** per aggiungere una o più regole di autorizzazione per la scheda dell'app e rimuoverle con l'azione di eliminazione.

9.16. ID delle tracce

Elenco degli ID delle tracce di test chiuso dell'app a cui un dispositivo può accedere. Se sono selezionati più ID traccia, i dispositivi ricevono la versione più recente tra tutte le tracce accessibili. Se non è selezionato alcun ID traccia, i dispositivi hanno accesso solo alla traccia di produzione

dell'app.

> L'opzione **ID delle tracce** è disponibile solo per le app che hanno almeno un ID traccia disponibile per la tua organizzazione. Per maggiori dettagli su come aggiungere la tua organizzazione a una traccia di test chiuso per un'app specifica, leggi qui.

10. Impostazioni delle applicazioni predefinite

Imposta le app predefinite per i tipi supportati. Quando è impostata un'app predefinita per almeno un tipo, agli utenti viene impedito di modificare le app predefinite in quel profilo.

> È consentita una sola impostazione di applicazione predefinita per **Tipo di applicazione predefinita**. L'elenco delle applicazioni predefinite non deve contenere duplicati.

10.1. Tipo di applicazione predefinita

Seleziona la categoria di app da configurare (ad esempio Browser, Telefono, SMS, Wallet o Assistente). La disponibilità dipende dalla versione di Android e dalla modalità di gestione.

10.2. Ambiti delle applicazioni predefinite

Seleziona dove deve essere applicata l'app predefinita (Completamente gestito, Profilo di lavoro o Profilo personale). È possibile scegliere solo gli ambiti supportati dal tipo selezionato.

> Se nessuno degli ambiti selezionati è applicabile alla modalità di gestione del dispositivo, il dispositivo segnala un dettaglio di non-conformità.

10.3. Applicazioni predefinite

Elenco delle app che possono essere impostate come predefinite per il tipo selezionato. La prima app installata e idonea viene impostata come predefinita.

> Se gli ambiti includono **Completamente gestito** o **Profilo di lavoro**, ogni app deve essere presente anche nell'elenco **Applicazioni** con **Tipo di installazione** diverso da **Bloccata**.

11. Selezione della chiave privata

Consente di mostrare sul dispositivo un'interfaccia per far scegliere all'utente un alias di chiave privata se non ci sono regole corrispondenti in **Scegli le regole della chiave privata**.

> Per i dispositivi con versioni precedenti ad Android P, impostare questa opzione può rendere vulnerabili le chiavi aziendali.

12. 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 chiama KeyChain.choosePrivateKeyAlias (o qualsiasi overload) per richiedere un alias di chiave privata per un determinato URL, oppure, per le regole non specifiche per URL (cioè se urlPattern non è impostato, o è impostato sulla stringa vuota o su .*), su Android 11 e versioni successive, direttamente, così che l'app possa chiamare KeyChain.getPrivateKey senza dover prima chiamare KeyChain.choosePrivateKeyAlias. Quando un'app chiama KeyChain.choosePrivateKeyAlias e più di una choosePrivateKeyRules corrisponde, l'ultima regola corrispondente definisce quale alias di chiave restituire.

Usa **Aggiungi regola chiave privata** per creare voci e rimuoverle con l'azione di eliminazione.

12.1. Alias della chiave privata

L'alias della chiave privata da usare.

12.2. 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.

12.3. Nomi dei pacchetti

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

Usa **Aggiungi nome del pacchetto** per aggiungere voci e rimuoverle con l'azione di eliminazione.

Per eliminare un'app, fai clic sull'icona del**cestino**, in fondo alla scheda dell'app.

Modalità chiosco

Con la modalità chiosco puoi limitare le funzionalità di un dispositivo a una singola app o a più app. La scelta tra modalità chiosco con app singola e con più app dipende dai tuoi obiettivi aziendali.

Nella **modalità chiosco con app singola**, un dispositivo viene 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 a quell'app specifica. Per abilitare questa modalità, specifica un'app nella sezione **Gestione app** con **Tipo di installazione** impostato su **Chiosco**.

Nella **modalità chiosco con più app**, i dispositivi possono accedere a più applicazioni. Gli utenti finali possono passare da un'app all'altra tramite un launcher personalizzato. Per abilitare questa modalità, attiva l'opzione **Launcher personalizzato per chiosco**.

Quando la modalità chiosco è abilitata, puoi anche configurare se gli utenti finali possono accedere a determinate funzionalità di sistema, come le impostazioni di sistema e la barra di stato.

Launcher personalizzato per chiosco

Indica se il launcher personalizzato per chiosco è abilitato. Sostituisce la schermata Home con un launcher che blocca il dispositivo sulle app installate tramite l'impostazione **Gestione app**. Le app compaiono su un'unica pagina in ordine alfabetico.

Azioni del pulsante di accensione

Imposta il comportamento di un dispositivo in modalità chiosco quando un utente tiene premuto (premere a lungo) il pulsante di accensione.

> **Disponibile (predefinito)**: Il menu di accensione (ad es. Spegni, Riavvia) viene mostrato quando un utente tiene premuto il pulsante di accensione di un dispositivo in modalità chiosco.
>
> **Bloccato**: Il menu di accensione (ad es. Spegni, Riavvia) non viene mostrato quando un utente tiene premuto il pulsante di accensione di un dispositivo in modalità chiosco. Nota: questo potrebbe impedire agli utenti di spegnere il dispositivo.

Avvisi di errore di sistema

Specifica se le finestre di errore di sistema per le app bloccate o che non rispondono vengono bloccate in modalità chiosco. Quando sono bloccate, il sistema forza l'arresto dell'app come se l'utente scegliesse l'opzione "chiudi app" nell'interfaccia.

Bloccato (predefinito): Tutte le finestre di errore di sistema, come arresti anomali e app che non risponde (ANR), vengono bloccate. Quando sono bloccate, il sistema forza l'arresto dell'app come se l'utente la chiudesse dall'interfaccia.

Attivato: Tutte le finestre di errore di sistema, come arresti anomali e app che non risponde (ANR), vengono visualizzate.

Navigazione di sistema

Specifica quali funzionalità di navigazione sono abilitate (ad es. pulsanti Home e Panoramica) in modalità chiosco.

Disattivato (predefinito): I pulsanti Home e Panoramica non sono accessibili.

Solo Home: È abilitato solo il pulsante Home.

Attivato: I pulsanti Home e Panoramica sono abilitati.

Barra di stato

Specifica se le informazioni di sistema e le notifiche sono disattivate in modalità chiosco.

Disattivato (predefinito): Le informazioni di sistema e le notifiche sono disattivate in modalità chiosco.

Solo sistema: Sulla barra di stato vengono mostrate solo le informazioni di sistema.

Attivato: Le informazioni di sistema e le notifiche vengono mostrate sulla barra di stato in modalità chiosco. Nota: perché questa policy abbia effetto, il pulsante Home del dispositivo deve essere abilitato tramite kioskCustomization.systemNavigation.

Impostazioni del dispositivo

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

Consentito (predefinito): L'accesso all'app Impostazioni è consentito in modalità chiosco.

Bloccato: L'accesso all'app Impostazioni non è consentito in modalità chiosco.

Sicurezza

In questa sezione puoi configurare le policy relative alla sicurezza.

Azioni per i rischi di sicurezza

Scegli cosa fare quando un dispositivo segnala un SecurityRisk nei rapporti di stato.

Tipi di SecurityRisk supportati:

Sistema operativo sconosciuto: Play Integrity API rileva che il dispositivo esegue un sistema operativo sconosciuto (il controllo basicIntegrity riesce ma ctsProfileMatch fallisce).

Sistema operativo compromesso: Play Integrity API rileva che il dispositivo esegue un sistema operativo compromesso (il controllo basicIntegrity fallisce).

Valutazione hardware non riuscita: Play Integrity API rileva che il dispositivo non offre una garanzia forte dell'integrità del sistema, se l'etichetta MEETS_STRONG_INTEGRITY non compare nel campo relativo all'integrità del dispositivo.

Azioni disponibili:

Cancella i dati aziendali (predefinito): annulla la registrazione e cancella i dati di lavoro (l'intero dispositivo se completamente gestito, o solo il profilo di lavoro per i dispositivi con profilo).

Nessuna azione: lascia il dispositivo registrato e non fare nulla automaticamente.

Quando selezioni **Cancella i dati aziendali**, puoi anche configurare le opzioni di cancellazione:

Mantieni la protezione dopo il ripristino di fabbrica: conserva i dati della protezione dopo il ripristino di fabbrica (FRP) durante la cancellazione del dispositivo.

Cancella archiviazione esterna: cancella inoltre l'archiviazione esterna del dispositivo (come le schede SD) durante l'esecuzione della cancellazione.

Cancella eSIM: per i dispositivi aziendali, rimuove tutte le eSIM dal dispositivo quando il dispositivo viene cancellato. Nei dispositivi di proprietà personale, rimuove le eSIM gestite (eSIM aggiunte tramite il comando ADD_ESIM) sul dispositivo e nessuna eSIM di proprietà personale verrà rimossa.

1. Tempo massimo prima del blocco

Tempo massimo (in secondi) di attività dell'utente prima del blocco del dispositivo. Un valore di 0 indica che non esiste alcuna restrizione.

2. Rimani attivo durante la ricarica

Le modalità di alimentazione con batteria collegata in cui il dispositivo rimane attivo. Quando usi questa impostazione, si consiglia di svuotare **Tempo massimo prima del blocco** in modo che il dispositivo non si blocchi mentre rimane attivo.

Alimentatore CA: la fonte di alimentazione è un alimentatore CA.

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

Caricatore wireless: la fonte di alimentazione è wireless.

3. Blocco schermo disattivato

Se impostato su true, disattiva la schermata di blocco per i display principale e/o secondario. Questa policy è supportata solo in modalità di gestione dispositivo dedicata.

4. Requisiti della password

Policy sui requisiti della password.

Usa **Configura i requisiti della password** per aggiungere uno o più blocchi di requisiti della password. Usa **Cancella tutto** per rimuovere tutti i requisiti della password configurati.

I requisiti della password possono usare l'ambito **Auto** (requisito singolo) o ambiti separati **Dispositivo**/**Profilo di lavoro**. I requisiti basati sulla complessità devono essere abbinati a requisiti basati sulla qualità per lo stesso 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 con profilo di lavoro e all'intero dispositivo per i dispositivi completamente gestiti o dedicati.

Dispositivo: i requisiti della password vengono applicati solo al dispositivo.

Profilo di lavoro: i requisiti della password vengono applicati solo al profilo di lavoro.

4.2. Lunghezza cronologia password

La lunghezza della cronologia delle password. Dopo aver impostato questo campo, l'utente non potrà inserire una nuova password uguale a una qualsiasi password della cronologia. Un valore di 0 indica che non esiste alcuna restrizione.

4.3. Max password non riuscite prima della cancellazione

Numero di password di sblocco del dispositivo errate che possono essere inserite prima che il dispositivo venga cancellato. Un valore di 0 indica che non esiste alcuna restrizione.

4.4. Scadenza password (giorni)

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

4.5. Richiedi sblocco con password

Il tempo dopo lo sblocco di un dispositivo o profilo di lavoro con una forma di autenticazione forte (password, PIN, sequenza) durante il quale è possibile sbloccarlo con qualsiasi altro metodo di autenticazione (ad es. impronta digitale, agenti attendibili, volto). Trascorso il periodo di tempo specificato, per sbloccare il dispositivo o il profilo di lavoro è possibile usare solo forme di autenticazione forti.

Predefinito del dispositivo: il periodo di timeout è impostato sul valore predefinito del dispositivo.

Ogni giorno: il periodo di timeout è impostato a 24 ore.

4.6. Qualità della password

La qualità della password richiesta.

Complessità elevata: definisce la fascia di complessità elevata della password come segue: su Android 12 e versioni successive: PIN senza sequenze ripetute (4444) o ordinate (1234, 4321, 2468), lunghezza minima 8; alfabetica, lunghezza minima 6; alfanumerica, lunghezza minima 6.

Complessità media: definisce la fascia di complessità media della password come segue: PIN senza sequenze ripetute (4444) o ordinate (1234, 4321, 2468), lunghezza minima 4; alfabetica, lunghezza minima 4; alfanumerica, lunghezza minima 4.

Complessità bassa: definisce la fascia di complessità bassa della password come segue: sequenza; PIN con sequenze ripetute (4444) o ordinate (1234, 4321, 2468).

Nessuna: non sono previsti requisiti della password.

Debole: il dispositivo deve essere protetto almeno con una tecnologia di riconoscimento biometrico a bassa sicurezza. Ciò include tecnologie in grado di riconoscere l'identità di un individuo approssimativamente equivalenti a un PIN di 3 cifre (rilevamento errato inferiore a 1 su 1.000).

Qualsiasi: è richiesta una password, ma non ci sono restrizioni su ciò che deve contenere.

Numerica: la password deve contenere caratteri numerici.

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

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

Alfanumerica: la password deve contenere sia caratteri numerici sia caratteri 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 della password. Un valore di 0 indica che non esiste alcuna restrizione.

4.8. Lettere minime

Numero minimo di lettere richieste nella password.

4.9. Lettere minuscole minime

Numero minimo di lettere minuscole richieste nella password.

4.10. Lettere maiuscole minime

Numero minimo di lettere maiuscole richieste nella password.

4.11. Caratteri non alfabetici minimi

Numero minimo di caratteri non alfabetici (cifre numeriche o simboli) richiesti nella password.

4.12. Cifre numeriche minime

Numero minimo di cifre numeriche richieste nella password.

4.13. Simboli minimi

Numero minimo di simboli richiesti nella password.

4.14. Blocco unificato

Controlla se è consentito un blocco unificato per il dispositivo e il profilo di lavoro, sui dispositivi con Android 9 e versioni successive e con un profilo di lavoro. Non ha alcun effetto sugli altri dispositivi.

> **Consenti blocco unificato**: è consentito un blocco comune per il dispositivo e il profilo di lavoro.
>
> **Richiedi blocco di lavoro separato**: è richiesto un blocco separato per il profilo di lavoro.

5. Ripristino di fabbrica disattivato

Indica se il ripristino di fabbrica dalle impostazioni è disattivato. Si applica solo ai dispositivi completamente gestiti.

6. Protezione dal ripristino di fabbrica

Indirizzi email degli amministratori del dispositivo per la protezione dal ripristino di fabbrica. Quando il dispositivo subisce un ripristino di fabbrica non autorizzato, richiederà a uno di questi amministratori di accedere con l'email e la password dell'account Google per sbloccare il dispositivo. Se non viene specificato alcun amministratore, il dispositivo non fornirà la protezione dal ripristino di fabbrica. Si applica solo ai dispositivi completamente gestiti.

Email degli amministratori: usa **Abilita la protezione dal ripristino di fabbrica** per iniziare a configurare gli amministratori. Poi usa **Aggiungi email amministratore** per aggiungere indirizzi e rimuoverli con l'azione di eliminazione.

7. Funzionalità del blocco schermo

Funzionalità del blocco schermo (schermata di blocco) che possono essere disattivate.

7.1. Disattiva tutto

Disattiva tutte le personalizzazioni attuali e future del blocco schermo.

7.2. Disattiva fotocamera

Disattiva la fotocamera sulle schermate di blocco protette (ad es. PIN).

7.3. Disattiva notifiche

Disattiva la visualizzazione di tutte le notifiche sulle schermate di blocco protette.

7.4. Disattiva notifiche non oscurate

Disattiva le notifiche non oscurate sulle schermate di blocco protette.

7.5. Ignora stato dell'agente attendibile

Ignora lo stato dell'agente attendibile sulle schermate di blocco protette.

7.6. Disattiva impronta digitale

Disattiva il sensore di impronte digitali sulle schermate di blocco protette.

7.7. Disattiva l'inserimento di testo nelle notifiche

Disattiva l'inserimento di testo nelle notifiche sulle schermate di blocco protette.

7.8. Disattiva autenticazione con volto

Disattiva l'autenticazione con il volto sulle schermate di blocco protette.

7.9. Disattiva autenticazione con iride

Disattiva l'autenticazione con l'iride sulle schermate di blocco protette.

7.10. Disattiva tutta l'autenticazione biometrica

Disattiva tutta l'autenticazione biometrica sulle schermate di blocco protette.

7.11. Disattiva tutte le scorciatoie

Disattiva tutte le scorciatoie sulla schermata di blocco protetta su Android 14 e versioni successive.

Multimedia

In questa sezione puoi configurare il comportamento di fotocamera/microfono, l'accesso ai dati USB, la stampa e le restrizioni relative al display.

1. Accesso alla fotocamera

Controlla l'uso della fotocamera e se l'utente può accedere all'interruttore di accesso alla fotocamera (Android 12+). In generale, la disattivazione della fotocamera si applica all'intero dispositivo sui dispositivi con gestione completa e solo all'interno del profilo di lavoro sui dispositivi con profilo di lavoro.

> **Scelta utente (predefinita)**: Comportamento predefinito del dispositivo. Le fotocamere sono disponibili e (Android 12+) l'utente può attivare o disattivare l'accesso alla fotocamera.
>
> **Disattivato**: Tutte le fotocamere sono disattivate (gestione completa: su tutto il dispositivo; profilo di lavoro: solo per le app del profilo di lavoro). L'interruttore di accesso alla fotocamera non ha effetto nell'ambito gestito.
>
> **Applicato**: Le fotocamere sono disponibili. Sui dispositivi con gestione completa con Android 12+, l'utente non può attivare o disattivare l'accesso alla fotocamera. Su altri dispositivi/versioni si comporta come Scelta utente.

2. Accesso al microfono

Sui dispositivi con gestione completa, controlla l'uso del microfono e se l'utente può accedere all'interruttore di accesso al microfono (Android 12+). Questa impostazione non ha effetto sui dispositivi senza gestione completa.

> **Scelta utente (predefinita)**: Comportamento predefinito. Il microfono è disponibile e (Android 12+) l'utente può attivare o disattivare l'accesso al microfono.
>
> **Disattivato**: Il microfono è disattivato (su tutto il dispositivo). L'interruttore di accesso al microfono non ha effetto.
>
> **Applicato**: Il microfono è disponibile. Su Android 12+, l'utente non può attivare o disattivare l'accesso al microfono. Su Android 11 o versioni precedenti si comporta come Scelta utente.

3. Accesso ai dati USB

Controlla quali file e/o dati possono essere trasferiti via USB. Supportato solo sui dispositivi di proprietà dell'azienda.

Non consentire il trasferimento di file (predefinito): I trasferimenti di file non sono consentiti, ma altre connessioni dati USB (ad es. mouse/tastiera) sono consentite.

Non consentire il trasferimento di dati: Tutti i tipi di trasferimento dati USB sono vietati (Android 12+ con USB HAL 1.3+). Se non supportato, il dispositivo passa a Non consentire il trasferimento di file.

Consenti il trasferimento di dati: Tutti i tipi di trasferimento dati USB sono consentiti.

4. Stampa

Controlla se la stampa è consentita (Android 9+).

Consentito (predefinito): La stampa è consentita.

Non consentito: La stampa non è consentita (Android 9+).

5. Impostazioni della luminosità dello schermo

Controlla la modalità di luminosità dello schermo e (facoltativamente) il valore di luminosità.

Modalità di luminosità dello schermo:

Scelta utente (predefinita): All'utente è consentito configurare la luminosità dello schermo.

Automatico: La luminosità è automatica e l'utente non può modificarla. Puoi comunque impostare un valore di luminosità, usato come parte della regolazione automatica (gestione completa Android 9+; profili di lavoro su dispositivi aziendali con Android 15+).

Fissa: La luminosità viene impostata sul valore configurato e l'utente non può modificarla. Il valore di luminosità è obbligatorio (gestione completa Android 9+; profili di lavoro su dispositivi aziendali con Android 15+).

Luminosità dello schermo:

Valore da 1 a 255 (1 = minimo, 255 = massimo). Un valore pari a 0 indica che non è impostato alcun valore di luminosità.

6. Impostazioni del timeout dello schermo

Controlla se l'utente può configurare il timeout dello schermo e, quando è applicato, il valore del timeout.

Il campo **Modalità timeout schermo** consente di scegliere tra il comportamento controllato dall'utente e quello applicato.

> **Scelta utente (predefinita)**: All'utente è consentito configurare il timeout dello schermo.
>
> **Applicato**: Il timeout dello schermo viene impostato sul valore configurato e l'utente non può modificarlo (gestione completa Android 9+; profili di lavoro su dispositivi aziendali con Android 15+).

Timeout dello schermo:

> Durata del timeout in secondi. Il valore deve essere maggiore di 0. Se è maggiore del **Tempo massimo di blocco**, il sistema potrebbe limitarlo e segnalare una non conformità.

7. Acquisizione schermo disattivata

Indica se l'acquisizione dello schermo è disattivata.

8. Regolazione del volume disattivata

Indica se la regolazione del volume principale è disattivata.

9. Montaggio dei supporti fisici disattivato

Indica se il montaggio dei supporti esterni fisici è disattivato.

Cellulare

In questa sezione puoi configurare le policy relative alla rete cellulare.

1. Modalità aereo

Controlla se l'utente può attivare o disattivare la modalità aereo.

> **Scelta dell'utente (predefinita)**: all'utente è consentito attivare o disattivare la modalità aereo.
>
> **Disabilitata**: la modalità aereo è disabilitata. All'utente non è consentito attivarla. Supportato su Android 9 e versioni successive.

2. Cellulare 2G

Controlla se l'utente può attivare o disattivare l'impostazione Cellulare 2G.

> **Scelta dell'utente (predefinita)**: all'utente è consentito attivare o disattivare il cellulare 2G.
>
> **Disabilitato**: il cellulare 2G è disabilitato. All'utente non è consentito attivare il cellulare 2G dalle impostazioni. Supportato su Android 14 e versioni successive.

3. Sostituisci APNs

Controlla se gli APNs di sostituzione sono abilitati o disabilitati. Quando sono abilitati, vengono usati solo gli APNs di sostituzione configurati e tutti gli altri APNs sul dispositivo vengono ignorati.

> **Disattivato (predefinito)**: Tutte le impostazioni APN configurate vengono salvate sul dispositivo, ma sono disattivate e non hanno alcun effetto. Tutti gli altri APN sul dispositivo rimangono in uso.
>
> **Attivato**: Vengono usati solo gli APN di override, tutti gli altri APN vengono ignorati. Questa impostazione può essere configurata solo su dispositivi con gestione completa con Android 10 e versioni successive.

4. Impostazioni APN

Configura una o più voci APN. Usa **Aggiungi APN** per creare una voce e **Rimuovi APN** per eliminarla.

Ogni APN ha campi obbligatori:

Tipi di APN: Seleziona uno o più tipi di traffico per questo APN (la disponibilità dipende dalla modalità di gestione e dalla versione di Android).

Nome APN: L'identificatore APN fornito dal tuo operatore.

Nome visualizzato: Nome descrittivo mostrato nell'interfaccia.

Campi APN facoltativi:

Tipo di autenticazione, **Nome utente**, **Password**: Configura l'autenticazione dell'operatore (se richiesta).

Protocollo e **Protocollo di roaming**: Configurazione del protocollo IP.

Tipi di rete: Limita le tecnologie cellulari che l'APN può usare (ad esempio LTE/5G NR).

Indirizzo proxy e **Porta proxy**: Proxy HTTP per il traffico dati (se applicabile).

Indirizzo proxy MMS, **Porta proxy MMS**, **MMSC (URI del centro MMS)**: Impostazioni relative agli MMS.

ID numerico operatore (MCC+MNC) e **ID operatore**: Campi di identificazione dell'operatore.

Impostazione Always On: Indica se la sessione PDU attivata da questo APN deve essere sempre attiva (always-on). Supportato su Android 15 e versioni successive.

Tipo MVNO: Tipo di identificatore dell'operatore di rete mobile virtuale.

MTU IPv4 e **MTU IPv6**: Maximum Transmission Unit (unità massima di trasmissione) per le route IPv4/IPv6. Supportato su Android 13 e versioni successive.

5. Configurazione delle trasmissioni cellulari disattivata

Indica se la configurazione delle trasmissioni cellulari è disattivata.

6. Configurazione delle reti mobili disattivata

Indica se la configurazione delle reti mobili è disattivata.

7. Dati in roaming disattivati

Indica se i servizi dati in roaming sono disattivati.

8. Chiamate in uscita disattivate

Indica se le chiamate in uscita sono disattivate.

9. SMS disattivati

Indica se l'invio e la ricezione di messaggi SMS sono disattivati.

10. Configurazione del network slicing 5G

Configura le impostazioni del servizio di rete preferenziale per abilitare il network slicing 5G aziendale. Puoi impostare fino a 5 slice aziendali e assegnare le applicazioni a reti specifiche per ottimizzare l'instradamento del traffico.

10.1. Rete preferenziale predefinita

ID della rete preferenziale predefinita per le applicazioni che non sono nell'elenco delle applicazioni o se la **Rete preferenziale** di un'app non è impostata. Deve esistere una configurazione per l'ID di rete specificato (a meno che non sia impostato su **Nessuna rete preferenziale**).

Nota: le app critiche come **com.google.android.apps.work.clouddpc** e **com.google.android.gms** sono escluse da questa impostazione predefinita.

10.2. Configurazioni dei servizi di rete

Usa **Aggiungi configurazione di rete** per creare una configurazione di slice. Puoi aggiungere fino a 5 configurazioni. Ogni configurazione ha:

ID rete preferenziale (assegnato automaticamente): L'ID di rete viene assegnato automaticamente e non può essere modificato.

Fallback alla connessione predefinita: Indica se è consentito il fallback alla rete predefinita del dispositivo. Se non consentito, le app non possono accedere a internet se lo slice 5G non è disponibile.

Reti non corrispondenti: Indica se le app soggette a questa configurazione possono usare reti diverse dal servizio preferenziale. Se impostato su **Non consentito**, anche **Fallback alla connessione predefinita** deve essere **Non consentito**. Richiede Android 14 e versioni successive.

Rete

In questa sezione puoi configurare le policy relative alla rete.

> Le configurazioni Wi-Fi possono essere fornite e gestite dal sistema tramite **Configurazioni WiFi**. A seconda del valore impostato su **Configura Wi-Fi**, gli utenti possono avere un controllo limitato o nullo sull'aggiunta/modifica delle reti.

Stato radio del dispositivo

1. Stato Wi-Fi

Controlla lo stato attuale del Wi-Fi e se l'utente può modificarne lo stato.

Scelta utente (predefinita): All'utente è consentito abilitare/disabilitare il Wi-Fi.

Attivato: Il Wi-Fi è attivo e all'utente non è consentito disattivarlo (Android 13+).

Disattivato: Il Wi-Fi è disattivato e all'utente non è consentito attivarlo (Android 13+).

2. Livello di sicurezza Wi-Fi minimo

Il livello di sicurezza minimo richiesto delle reti Wi-Fi a cui il dispositivo può connettersi. Supportato su Android 13 e versioni successive, per i dispositivi con gestione completa e i profili di lavoro sui dispositivi di proprietà dell'azienda.

Rete aperta (predefinita): Il dispositivo può connettersi a tutti i tipi di reti Wi-Fi.

Rete personale: Non consente le reti Wi-Fi aperte; richiede almeno la sicurezza personale (ad esempio WPA2-PSK).

Rete aziendale: Richiede reti EAP aziendali; non consente reti Wi-Fi con un livello di sicurezza inferiore.

Rete aziendale a 192 bit: Richiede reti aziendali a 192 bit; opzione più restrittiva.

3. Stato ultra wideband (UWB)

Controlla lo stato dell'impostazione ultra wideband e se l'utente può attivarla o disattivarla.

Scelta utente (predefinita): All'utente è consentito attivare o disattivare UWB.

Disattivato: UWB è disattivato e all'utente non è consentito attivarlo o disattivarlo tramite le impostazioni (Android 14+).

Gestione della connettività del dispositivo

4. Condivisione Bluetooth

Controlla se la condivisione Bluetooth è consentita.

Consentito: La condivisione Bluetooth è consentita (predefinito sui dispositivi con gestione completa, Android 8+).

Non consentito: La condivisione Bluetooth non è consentita (predefinito sui profili di lavoro, Android 8+).

5. Configura Wi-Fi

Controlla i privilegi di configurazione del Wi-Fi. A seconda dell'opzione selezionata, l'utente ha il controllo completo, limitato o nullo sulla configurazione delle reti Wi-Fi.

Consenti la configurazione del Wi-Fi (predefinito): All'utente è consentito configurare il Wi-Fi.

Non consentire l'aggiunta di configurazioni Wi-Fi: L'aggiunta di nuove configurazioni Wi-Fi non è consentita. L'utente può passare da una rete già configurata all'altra (Android 13+; gestione completa e profili di lavoro su dispositivi aziendali).

Non consentire la configurazione del Wi-Fi: Non consente di configurare le reti Wi-Fi. Per i dispositivi con gestione completa, rimuove le reti configurate dall'utente e mantiene solo le

reti configurate tramite **Configurazioni WiFi**. Per i profili di lavoro sui dispositivi aziendali, le reti esistenti non sono interessate, ma gli utenti non possono aggiungere/rimuovere/modificare le reti Wi-Fi.

> Quando la configurazione del Wi-Fi è disattivata e il dispositivo non riesce a connettersi all'avvio, il sistema può mostrare la **procedura di emergenza per la rete** per consentire all'utente di connettersi temporaneamente e aggiornare la policy.

6. Impostazioni Wi-Fi Direct

Controlla la configurazione e l'uso delle impostazioni Wi-Fi Direct. Supportato sui dispositivi di proprietà dell'azienda con Android 13 e versioni successive.

Consenti (predefinito): All'utente è consentito usare Wi-Fi Direct.

Non consentire: All'utente non è consentito usare Wi-Fi Direct.

7. Impostazioni di tethering

Controlla le impostazioni di tethering. In base al valore impostato, all'utente è parzialmente o completamente vietato usare diverse forme di tethering.

Consenti tutto il tethering (predefinito): Consente la configurazione e l'uso di tutte le forme di tethering.

Non consentire il tethering Wi-Fi: Vieta all'utente di usare il tethering Wi-Fi (dispositivi aziendali Android 13+).

Non consentire alcun tethering: Vieta tutte le forme di tethering (gestione completa + profili di lavoro su dispositivi aziendali).

8. Policy SSID Wi-Fi

Restrizioni sugli SSID Wi-Fi a cui il dispositivo può connettersi (questo non influisce sulle reti che possono essere configurate sul dispositivo). Supportato sui dispositivi di proprietà dell'azienda con Android 13 e versioni successive.

Lista di blocco SSID (predefinita): Il dispositivo non può connettersi a nessuna rete Wi-Fi il cui SSID è elencato, ma può connettersi ad altre reti.

Lista di consentiti SSID: Il dispositivo può connettersi solo agli SSID elencati. L'elenco degli SSID non deve essere vuoto.

Usa **Aggiungi SSID** per aggiungere voci. A seconda del tipo di policy selezionato, l'elenco viene interpretato come SSID consentiti o non consentiti.

Nell'interfaccia dell'editor delle policy, l'elenco degli SSID è etichettato come **SSID Wi-Fi consentiti** per le liste di consentiti e **SSID Wi-Fi non consentiti** per le liste di blocco.

9. Impostazioni di roaming Wi-Fi

Configura la modalità di roaming Wi-Fi per SSID. Usa **Aggiungi impostazione di roaming Wi-Fi** per creare voci.

Ogni voce include:

SSID: L'SSID a cui si applica l'impostazione di roaming (obbligatorio).

Modalità di roaming Wi-Fi: Predefinita / Disattivata / Aggressiva. Disattivata e Aggressiva richiedono Android 15+ e sono supportate solo sui dispositivi con gestione completa e sui profili di lavoro dei dispositivi aziendali.

Restrizioni di rete

10. Bluetooth disattivato

Indica se il Bluetooth è disattivato. Preferisci questa impostazione a Configurazione Bluetooth disattivata, perché la configurazione Bluetooth disattivata può essere aggirata dall'utente.

11. Condivisione contatti Bluetooth disattivata

Indica se la condivisione dei contatti Bluetooth è disattivata.

12. Configurazione Bluetooth disattivata

Indica se la configurazione del Bluetooth è disattivata.

13. Ripristino rete disattivato

Indica se il ripristino delle impostazioni di rete è disattivato.

14. Beam in uscita disattivato

Indica se l'uso di NFC per inviare dati dalle app tramite beam è disattivato.

VPN

15. App VPN Always On

Specifica un nome pacchetto VPN Always On per assicurarti 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 sia la funzionalità Always On sia quella VPN per app.

16. Blocco VPN

Impedisce la connessione di rete quando la VPN non è connessa.

17. Configurazione VPN disattivata

Indica se la configurazione della VPN è disattivata.

Proxy e servizi di rete

18. Servizio di rete preferenziale

Controlla se il servizio di rete preferenziale è abilitato sul profilo di lavoro. Ad esempio, un'organizzazione può avere un accordo con un operatore affinché i dati di lavoro vengano inviati tramite un servizio di rete dell'operatore dedicato all'uso aziendale (ad esempio, uno slice aziendale sulle reti 5G). Questo non ha effetto sui dispositivi con gestione completa.

Disattivato: Il servizio di rete preferenziale è disattivato sul profilo di lavoro.

Attivato: Il servizio di rete preferenziale è abilitato sul profilo di lavoro.

> Se usi il network slicing aziendale, configura anche **Configurazione del network slicing 5G** nel pannello della policy **Cellulare** e assegna le app a uno slice tramite la loro impostazione **Rete preferenziale**.

19. Proxy globale consigliato

Il proxy HTTP globale indipendente dalla rete. In genere, i proxy dovrebbero essere configurati per rete nelle configurazioni WiFi. Un proxy globale può essere utile per configurazioni particolari come il filtraggio interno generale. Il proxy globale è solo un consiglio e alcune app potrebbero ignorarlo.

Disattivato

Proxy diretto

Configurazione automatica del proxy (PAC)

19.1. Host

L'host del proxy diretto.

19.2. Porta

La porta del proxy diretto.

19.3. URI PAC

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

19.4. Host esclusi

Per un proxy diretto, gli host per cui il proxy viene ignorato. I nomi host possono contenere caratteri jolly come ***.example.com**.

Usa **Aggiungi host escluso** per aggiungere voci (disponibile solo per il proxy diretto).

Configurazioni Wi-Fi

Definisci le configurazioni di rete Wi-Fi che il sistema applicherà sui dispositivi. Usa **Aggiungi configurazione Wi-Fi** per creare una voce e rimuoverla con l'azione di eliminazione.

20. Campi della configurazione Wi-Fi

Ogni configurazione include:

Nome configurazione: obbligatorio.

SSID: obbligatorio.

Connessione automatica: indica se connettersi automaticamente alla rete quando è nel raggio d'azione.

Transizione rapida: indica se il client deve tentare di usare la transizione rapida (IEEE 802.11r-2008) con la rete.

SSID nascosto: indica se l'SSID verrà trasmesso.

Modalità di randomizzazione MAC: Hardware o Automatica (Android 13+).

20.1. Sicurezza

Opzioni di sicurezza Wi-Fi:

WEP-PSK: WEP (chiave precondivisa).

WPA-PSK: WPA/WPA2/WPA3-Personal (chiave precondivisa).

WPA-EAP: WPA/WPA2/WPA3-Enterprise (Extensible Authentication Protocol).

Modalità WPA3 a 192 bit: rete WPA-EAP che consente solo la modalità WPA3 a 192 bit.

20.2. Passphrase (chiave precondivisa)

Visualizzato quando la sicurezza è **WEP-PSK** o **WPA-PSK**. La passphrase è obbligatoria.

20.3. Metodo EAP (Enterprise)

Visualizzato quando la sicurezza è **WPA-EAP** o **Modalità WPA3 a 192 bit**. Seleziona un metodo EAP esterno:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Autenticazione fase 2

Visualizzato per i metodi esterni con tunneling (**EAP-TTLS** e **PEAP**).

MSCHAPv2

PAP

20.5. Credenziali EAP dagli utenti

Se attivato, il sistema applica automaticamente le credenziali EAP sui dispositivi per singolo utente. Puoi configurare le credenziali degli utenti nella sezione **Utenti**.

20.6. Certificato client

Per **EAP-TLS**, puoi assegnare un certificato client usato per l'autenticazione Wi-Fi. Per ulteriori informazioni leggi la pagina **Gestione dei certificati**.

Se è già assegnato un certificato, puoi usare **Apri certificato** per visualizzarlo o **Cambia certificato** per selezionarne uno diverso.

In alternativa, puoi specificare **Alias coppia di chiavi del certificato client**, che fa riferimento a un certificato client archiviato nel keychain di Android e consentito per l'autenticazione Wi-Fi.

> Se sono impostati sia **Certificato client** sia **Alias coppia di chiavi del certificato client**, l'alias della coppia di chiavi viene ignorato.

20.7. Identità

Identità dell'utente. Per i protocolli esterni con tunneling (PEAP, EAP-TTLS), viene usata per l'autenticazione all'interno del tunnel, mentre **Identità anonima** viene usata per l'identità EAP

all'esterno del tunnel. Per i protocolli esterni senza tunneling, viene usata per l'identità EAP.

20.8. Identità anonima

Solo per i protocolli con tunneling, indica l'identità dell'utente presentata al protocollo esterno.

20.9. Password

Password dell'utente. Se non specificata, per impostazione predefinita viene richiesta all'utente.

20.10. Certificati CA del server

Elenco dei certificati CA da usare per verificare la catena di certificati dell'host. Almeno un certificato CA deve corrispondere. Per ulteriori informazioni leggi la pagina **Gestione dei certificati**.

Usa **Aggiungi certificato CA del server** per aggiungere voci e rimuoverle con l'azione di eliminazione.

20.11. Corrispondenze dei suffissi di dominio

Un elenco di vincoli per il nome di dominio del server. Le voci vengono usate come requisiti di corrispondenza dei suffissi rispetto ai nomi DNS del nome alternativo del soggetto di un certificato del server di autenticazione.

Sistema

In questa sezione puoi configurare le policy relative al sistema.

1. Livello API minimo

Il livello API Android minimo consentito.

2. Policy di crittografia

Indica se la crittografia è attivata.

> **Predefinito**: questo valore viene ignorato, ovvero non è richiesta alcuna crittografia.
>
> **Attivata senza password**: crittografia richiesta ma nessuna password necessaria per l'avvio.
>
> **Attivata con password**: crittografia richiesta con password necessaria per l'avvio.

3. Data e ora automatiche

Indica se data, ora e fuso orario automatici sono attivati su un dispositivo aziendale.

> **Scelta dell'utente (predefinito)**: data, ora e fuso orario automatici sono lasciati alla scelta dell'utente.
>
> **Applicati**: applica data, ora e fuso orario automatici sul dispositivo.

4. Impostazioni sviluppatore

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

> **Disattivato (predefinito)**: disattiva tutte le impostazioni sviluppatore e impedisce all'utente di accedervi.

Consentito: consente tutte le impostazioni sviluppatore. L'utente può accedervi e configurarle facoltativamente.

5. Modalità Common Criteria

Controlla la modalità Common Criteria—standard di sicurezza definiti nel Common Criteria for Information Technology Security Evaluation (CC). L'attivazione della modalità Common Criteria incrementa alcuni componenti di sicurezza su un dispositivo (ad esempio: crittografia AES-GCM delle chiavi a lungo termine Bluetooth, convalida aggiuntiva per alcuni certificati di rete e controlli di integrità delle policy crittografiche). La modalità Common Criteria è supportata solo su dispositivi aziendali con Android 11 o versioni successive. Avviso: la modalità Common Criteria applica un modello di sicurezza rigoroso, in genere richiesto solo da organizzazioni altamente sensibili. L'uso standard del dispositivo potrebbe esserne influenzato; attivala solo se necessario.

Disattivato (predefinito): disattiva la modalità Common Criteria.

Attivato: attiva la modalità Common Criteria.

6. Memory Tagging Extension (MTE)

Controlla Memory Tagging Extension (MTE) sul dispositivo.

Scelta dell'utente (predefinito): l'utente può scegliere di attivare o disattivare MTE sul dispositivo (se supportato dal dispositivo).

Applicato: MTE è attivato e l'utente non può modificarlo (Android 14+; supportato su dispositivi completamente gestiti e profili di lavoro su dispositivi aziendali).

Disattivato: MTE è disattivato e l'utente non può modificarlo (Android 14+; supportato solo su dispositivi completamente gestiti).

7. Protezione dei contenuti

Controlla se la protezione dei contenuti (che analizza le app ingannevoli) è attivata. È supportata su Android 15 e versioni successive.

Disattivato (predefinito): la protezione dei contenuti è disattivata e l'utente non può modificarlo.

Applicato: la protezione dei contenuti è attivata e l'utente non può modificarlo (Android 15+).

Scelta dell'utente: la protezione dei contenuti non è controllata dalla policy; l'utente può scegliere (Android 15+).

8. Contenuti Assist

Controlla se AssistContent può essere inviato a un'app con privilegi, ad esempio un'app assistente (come Circle to Search). AssistContent include screenshot e informazioni su un'app, come il nome del pacchetto. È supportato su Android 15 e versioni successive.

Consentito (predefinito): il contenuto Assist può essere inviato a un'app con privilegi (Android 15+).

Non consentito: il contenuto Assist è bloccato e non può essere inviato a un'app con privilegi (Android 15+).

9. Creazione finestre disattivata

Indica se la creazione di finestre diverse da quelle delle app è disattivata. Questa opzione impedisce la visualizzazione delle seguenti interfacce 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.

10. Connessione di rete di emergenza

Indica se la connessione di rete di emergenza è attivata. Se all'avvio non è possibile stabilire una connessione di rete, la connessione di emergenza chiede all'utente di connettersi temporaneamente a una rete per aggiornare la policy del dispositivo. Dopo l'applicazione della policy, la rete temporanea viene dimenticata e il dispositivo continua l'avvio. Ciò evita di restare senza connessione di rete se l'ultima policy non contiene una rete adatta e il dispositivo si avvia in un'app in modalità lock task, o se l'utente non può in altro modo raggiungere le impostazioni del dispositivo.

11. Attività predefinite

Un elenco di attività predefinite per gestire gli intent che corrispondono a un determinato filtro di intent. Ad esempio, questa funzionalità consente agli amministratori IT di scegliere quale app browser apre automaticamente i link web o quale app launcher viene usata quando si tocca il pulsante Home.

Usa **Aggiungi attività predefinita** per creare voci. All'interno di una voce, usa **Aggiungi azione** e **Aggiungi categoria** per creare il filtro di intent.

11.1. Attività ricevente

L'attività che deve essere il gestore predefinito degli intent. Deve 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, il che fa sì che Android Device Policy scelga un'attività appropriata dall'app per gestire l'intent.

11.2. Azione

Le azioni degli intent da confrontare nel filtro. Se il filtro include delle azioni, l'azione di un intent deve essere uno di quei valori perché corrisponda. Se non sono incluse azioni, l'azione dell'intent viene ignorata.

11.3. Categoria

Le categorie degli intent da confrontare nel filtro. Un intent include le categorie che richiede; tutte devono essere incluse nel filtro perché la corrispondenza avvenga. In altre parole, aggiungere una categoria al filtro non influisce sulla corrispondenza, a meno che quella categoria non sia specificata nell'intent.

12. Metodi di input consentiti

Specifica i metodi di input consentiti.

> **Tutti consentiti**: nessuna restrizione applicata. Tutti i metodi di input sono consentiti.
>
> **Solo quelli di sistema**: sono consentiti solo i metodi di input preinstallati del sistema.
>
> **Solo quelli di sistema e forniti**: sono consentiti solo i metodi di input forniti e quelli preinstallati del sistema.

12.1. Metodi di input consentiti

Nomi dei pacchetti dei metodi di input consentiti. Si applica solo quando **Metodi di input consentiti** è impostato su **Solo quelli di sistema e forniti**.

Usa **Aggiungi metodo di input** per aggiungere voci e rimuoverle con l'azione di eliminazione.

13. Servizi di accessibilità consentiti

Specifica i servizi di accessibilità consentiti.

Tutti consentiti: è possibile usare qualsiasi servizio di accessibilità.

Solo quelli di sistema: è possibile usare solo i servizi di accessibilità preinstallati del sistema.

Solo quelli di sistema e forniti: è possibile usare solo i servizi di accessibilità forniti e quelli preinstallati del sistema.

13.1. Servizi di accessibilità consentiti

Servizi di accessibilità consentiti. Si applica solo quando **Servizi di accessibilità consentiti** è impostato su **Solo quelli di sistema e forniti**.

Usa **Aggiungi servizio di accessibilità** per aggiungere voci e rimuoverle con l'azione di eliminazione.

14. Policy di aggiornamento del sistema

Configurazione per la gestione degli aggiornamenti del sistema.

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

Automatico: installa automaticamente non appena un aggiornamento è disponibile.

A intervalli: installa automaticamente entro una finestra di manutenzione giornaliera. Questo configura anche le app Play per l'aggiornamento entro la finestra. È fortemente consigliato per i dispositivi kiosk, perché è l'unico modo in cui Play può aggiornare le app fissate in modo persistente in primo piano.

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

14.1. Finestra di manutenzione (solo A intervalli)

Quando **Policy di aggiornamento del sistema** è impostato su **A intervalli**, puoi definire la finestra di manutenzione giornaliera usando i campi **da** e **a**.

14.2. Periodi di blocco degli aggiornamenti 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 di bloccare il dispositivo a tempo indefinito, ogni periodo di blocco deve essere separato da almeno 60 giorni. Ogni periodo di blocco non deve superare i 90 giorni.

Usa **Aggiungi periodo di blocco degli aggiornamenti del sistema** per creare voci.

15. Provider di credenziali predefiniti

Controlla quali app possono agire come provider di credenziali su Android 14 e versioni successive.

> **Non consentito (predefinito)**: le app con credentialProviderPolicy non specificato non possono agire come provider di credenziali.
>
> **Non consentito tranne per il sistema**: le app con credentialProviderPolicy non specificato non possono agire come provider di credenziali, fatta eccezione per i provider di credenziali predefiniti dell'OEM.

Posizione e geofence

Questo pannello raggruppa le impostazioni della policy Android che controllano la segnalazione della posizione del dispositivo, l'applicazione forzata della posizione e la definizione dei geofence. Usalo quando vuoi che Cerberus Enterprise raccolga la posizione dei dispositivi o rilevi quando i dispositivi entrano o escono dalle aree configurate.

Segnalazione della posizione

Segnala posizione

Abilita la segnalazione della posizione geografica del dispositivo. I dati sulla posizione raccolti tramite questa impostazione vengono usati dalla **mappa delle posizioni della dashboard**, dalla cronologia delle posizioni nella panoramica del dispositivo e dall'elaborazione dei geofence.

> La cronologia posizioni e gli eventi geofence vengono conservati per **90 giorni** e i dati più vecchi vengono eliminati automaticamente ogni notte. L'ultima posizione di ogni dispositivo registrato viene sempre conservata, così il dispositivo resta sulle mappe.

> Sui dispositivi non completamente gestiti, i dati sulla posizione possono comunque dipendere dall'app Cerberus Enterprise che dispone delle autorizzazioni di posizione richieste e dall'attivazione dei servizi di localizzazione sul dispositivo.

> Sui dispositivi Apple personali (User Enrollment), la posizione e i geofence sono disattivati per impostazione predefinita: sono disponibili solo quando la policy Apple ha **Posizione e geofence sui dispositivi personali** attivo e solo se l'utente consente la posizione per l'app Cerberus Enterprise.

Modalità posizione

Controlla l'impostazione della posizione del dispositivo sui dispositivi di proprietà dell'azienda.

- **Scelta utente**: i servizi di localizzazione non sono limitati dalla policy.
- **Applicato**: i servizi di localizzazione sono abilitati sul dispositivo.

- **Disattivato**: i servizi di localizzazione sono disattivati sul dispositivo.

Condivisione posizione disattivata

Disattiva la condivisione della posizione per le app di lavoro. Sui dispositivi con profilo proprietario, questo influisce sul profilo di lavoro. Sui dispositivi con gestione completa, disattiva la posizione per l'intero dispositivo e sostituisce la modalità posizione del dispositivo.

Comportamento automatico con geofence attivi

I geofence attivi richiedono che la segnalazione della posizione funzioni. Quando almeno un geofence è attivo, Cerberus Enterprise mantiene automaticamente coerenti le impostazioni della posizione correlate.

- **Segnala posizione** viene attivato forzatamente finché esistono geofence attivi.
- **Modalità posizione** viene impostata forzatamente su **Applicato**.
- **Condivisione posizione disattivata** viene disattivata forzatamente.

Se provi a disattivare **Segnala posizione** mentre uno o più geofence sono attivi, Cerberus Enterprise mostra una finestra di conferma. Se continui, tutti i geofence attivi nella policy vengono disattivati.

Elenco dei geofence

Una policy può contenere fino a **10 geofence**. I nomi dei geofence devono essere univoci all'interno della policy.

Usa **Aggiungi geofence** per creare una nuova voce. Ogni geofence contiene questi campi principali:

- **Nome**: obbligatorio e univoco.
- **Latitudine** e **Longitudine**: il centro dell'area.
- **Raggio (m)**: obbligatorio, da **200** a **10000** metri.
- **Descrizione**: note facoltative per gli amministratori.
- **Segnala ingresso** e **Segnala uscita**: scegli quali eventi di transizione devono essere generati.
- **Attivo**: abilita o disattiva il geofence senza eliminarlo.

> Almeno una tra**Segnala ingresso** e **Segnala uscita** deve rimanere abilitata per ogni geofence.

> In precedenza il raggio minimo era 100 metri. I geofence esistenti con raggio inferiore a 200 metri continuano a funzionare e vengono mantenuti così come sono quando salvi la policy, anche se li sposti o li rinomini. Se ne modifichi il raggio, deve essere di almeno 200 metri.

Strumenti di modifica della mappa

Ogni scheda geofence include un'anteprima della mappa dell'area. Puoi modificare la geometria dalla mappa o dai campi numerici.

- Fai clic sulla mappa per spostare il centro del geofence quando la modifica dell'area è sbloccata.
- Usa il pulsante **Posizione attuale** per centrare la mappa sulla posizione attuale del browser.
- Usa il pulsante **Ricentra mappa** per ripristinare l'area di visualizzazione preferita per quel geofence.
- Usa il pulsante di blocco per evitare modifiche accidentali alla geometria del geofence.

Dove compaiono i dati dei geofence

Le transizioni dei geofence possono essere esaminate nella pagina **Panoramica dispositivo** di Android, nella scheda **Geofence** del pannello della posizione. Quella scheda mostra le transizioni su una mappa dedicata insieme agli strumenti di filtro e all'elenco delle transizioni.

Gestione utenti

Aggiunta utenti disattivata

Indica se l'aggiunta di nuovi utenti e profili è disattivata. Per i dispositivi in cui managementMode è **DEVICE_OWNER**, questo campo viene ignorato e l'utente non può mai aggiungere o rimuovere utenti.

Modifica account disattivata

Indica se l'aggiunta o la rimozione di account è disattivata.

Configurazione credenziali utente disattivata

Indica se la configurazione delle credenziali utente è disattivata.

Rimozione utenti disattivata

Indica se la rimozione di altri utenti è disattivata.

Impostazione icona utente disattivata

Indica se la modifica dell'icona utente è disattivata.

Impostazione sfondo disattivata

Indica se la modifica dello sfondo è disattivata.

Autenticazione durante la configurazione dell'account di lavoro

Controlla come gli utenti si autenticano durante la configurazione dell'account di lavoro. Questa opzione è disponibile solo per le aziende Android supportate da un dominio Google gestito (Google Workspace).

Durante la configurazione/registrazione del dispositivo, questa policy influenza se è richiesto l'accesso a un account di lavoro, ma l'impostazione **Autenticati con Google** della Google Admin Console 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 **Autenticati con Google Enrollment**).

Per maggiori dettagli e per la risoluzione dei problemi, consulta **Autenticati con Google Enrollment**.

Tipi di account bloccati

Tipi di account che l'utente non può gestire. Questa opzione impedisce agli utenti del dispositivo di aggiungere account non approvati.

Usa **Aggiungi tipo di account bloccato** per aggiungere uno o più tipi di account.

Ogni voce ha un campo **Tipo di account** (obbligatorio). Inserisci una stringa come **com.google**. Rimuovi una voce usando l'azione di eliminazione.

Uso personale

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

> Questa sezione si applica solo ai dispositivi aziendali con profilo di lavoro. Non ha alcun effetto sui dispositivi completamente gestiti o di proprietà personale.

1. Fotocamera disattivata

Indica se la fotocamera è disattivata.

2. Cattura schermo disattivata

Indica se la cattura schermo è disattivata.

3. Giorni massimi con lavoro disattivato

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

4. Condivisione Bluetooth

Controlla se la condivisione Bluetooth è consentita nel profilo personale di un dispositivo aziendale con profilo di lavoro.

5. Spazio privato

Controlla se è consentito uno spazio privato sul dispositivo.

6. Modalità Play Store

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

Blocklist (predefinita): tutte le app sono disponibili e qualsiasi app che non deve essere sul dispositivo va contrassegnata esplicitamente come **Bloccata** nella sezione **Applicazioni**.

Allowlist: solo le app specificate esplicitamente nella sezione **Applicazioni** con **Tipo di installazione** impostato su **Disponibile** possono essere installate nel profilo personale.

7. Applicazioni

Elenco delle applicazioni che devono essere consentite o bloccate nel profilo personale. Il comportamento del contenuto dell'elenco dipende dal valore impostato in **Modalità Play Store**.

Per aggiungere una nuova app dal Play Store, fai clic sull'icona **+**.

7.1. Tipo di installazione

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

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

Disponibile: l'app può essere installata nel profilo personale.

8. 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 nel proprio profilo personale.

Policy tra profili

Si applica solo ai dispositivi con profilo personale e di lavoro.

Copia/incolla tra profili

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

> **Non consentito (predefinito)**: 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.
>
> **Consentito**: Il testo copiato in uno dei due profili può essere incollato nell'altro profilo.

Condivisione dei dati tra profili

Indica se i dati di un profilo (personale o di lavoro) possono essere condivisi con le app dell'altro profilo. Controlla in particolare la condivisione semplice dei dati tramite intent. La gestione degli altri canali di comunicazione tra profili, come la ricerca dei contatti, il copia/incolla,
o le app di lavoro e personali collegate, viene configurata separatamente.

> **Non consentito**: Impedisce la condivisione dei dati sia dal profilo personale al profilo di lavoro sia dal profilo di lavoro al profilo personale.
>
> **Da lavoro a personale non consentito (predefinito)**: Impedisce agli utenti di condividere dati dal profilo di lavoro alle app del profilo personale. I dati personali possono essere condivisi con le app di lavoro.
>
> **Consentito**: I dati di uno dei due profili possono essere condivisi con l'altro profilo.

Widget del profilo di lavoro predefiniti

Comportamento predefinito dei widget del profilo di lavoro. Se un'app specifica non definisce una policy per i widget, segue il valore predefinito impostato qui.

Funzioni delle app tra profili

Controlla se le app del profilo personale possono richiamare le funzioni delle app del profilo di lavoro. Richiede Android 16 o versioni successive.

> Questa impostazione dipende dall'opzione **Funzioni delle app** a livello di policy (nella sezione Gestione app). Se Funzioni delle app è impostato su **Non consentito**, l'API rifiuterà Funzioni delle app tra profili impostato su **Consentito**.

Contatti di lavoro nel profilo personale

Indica se i contatti memorizzati nel profilo di lavoro possono essere mostrati nelle ricerche dei contatti e nelle chiamate in arrivo del profilo personale.

Consentito (predefinito): Consente ai contatti del profilo di lavoro di comparire nel profilo personale.

Non consentito: Impedisce alle app personali di accedere ai contatti del profilo di lavoro e di cercare i contatti di lavoro.

Non consentito tranne per il sistema: Impedisce alla maggior parte delle app personali di accedere ai contatti del profilo di lavoro, tranne che per le app Dialer, Messaggi e Contatti predefinite dell'OEM (Android 14+).

Quando Contatti di lavoro nel profilo personale è configurato, puoi facoltativamente definire un elenco di voci **Nome pacchetto esente**. A seconda della modalità selezionata, queste esenzioni funzionano come allowlist o blocklist per le app personali.

Rapporti di stato

In questa sezione puoi configurare quali dati devono essere recuperati dal dispositivo. I dati di stato possono essere visualizzati nella pagina della dashboard **Stato dispositivo**.

Rapporti delle applicazioni

Indica se i rapporti delle app sono attivati. (Informazioni segnalate su un'app installata.)

> Questa opzione è richiesta dal sistema (per l'integrazione con l'app companion) ed è sempre attivata; non può essere disattivata.

Includi app rimosse

Indica se le app rimosse sono incluse nei rapporti delle applicazioni.

Impostazioni del dispositivo

Indica se il reporting delle impostazioni del dispositivo è attivato. (Informazioni sulle impostazioni di sicurezza del dispositivo.)

Informazioni software

Indica se il reporting delle informazioni software è attivato. (Informazioni sul software del dispositivo.)

Informazioni sulla memoria

Indica se il reporting della memoria è attivato. (Un evento relativo alle misurazioni di memoria e archiviazione.)

Informazioni di rete

Indica se il reporting delle informazioni di rete è attivato. (Informazioni di rete del dispositivo.)

Informazioni sul display

Indica se il reporting dei display è attivato. 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

Indica se il reporting degli eventi di gestione dell'alimentazione è attivato. I dati dei rapporti non sono disponibili per i dispositivi di proprietà personale con profili di lavoro.

Stato dell'hardware

Indica se il reporting dello stato dell'hardware è attivato. I dati dei rapporti non sono disponibili per i dispositivi di proprietà personale con profili di lavoro.

Proprietà di sistema

Indica se il reporting delle proprietà di sistema è attivato.

Modalità Common Criteria

Indica se il reporting della modalità Common Criteria è attivato.

Varie

1. Gioco easter egg disattivato

Indica se il gioco easter egg nelle Impostazioni è disattivato.

2. Salta i suggerimenti al primo utilizzo

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

3. Messaggio di supporto breve

Un messaggio mostrato all'utente nella schermata delle impostazioni ovunque l'amministratore abbia disattivato una funzionalità. Se il messaggio supera i 200 caratteri, potrebbe essere troncato.

4. Messaggio di supporto lungo

Un messaggio mostrato all'utente nella schermata delle impostazioni degli amministratori del dispositivo.

5. Informazioni del proprietario nella schermata di blocco

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

6. Azioni di configurazione

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

Usa **Aggiungi azione di configurazione** per creare voci e rimuoverle con l'azione di eliminazione.

6.1. Avvia app

Nome del pacchetto dell'app da avviare

6.2. Titolo

Fornisce un messaggio per l'utente per spiegargli perché l'app deve essere avviata.

6.3. Descrizione

Fornisce un messaggio per l'utente per spiegargli perché l'app deve essere avviata.

7. Visibilità del nome visualizzato dell'azienda

Controlla se il nome visualizzato dell'azienda è visibile sul dispositivo (ad esempio come messaggio nella schermata di blocco sui dispositivi di proprietà dell'azienda).

Visibile (predefinito): Il nome visualizzato dell'azienda è visibile sul dispositivo (supportato sui profili di lavoro con Android 7+ e sui dispositivi con gestione completa con Android 8+).

Nascosto: Il nome visualizzato dell'azienda è nascosto sul dispositivo.

Regole di conformità

Se un dispositivo o un profilo di lavoro non rispetta una delle impostazioni della policy elencate di seguito, Android Device Policy blocca immediatamente l'uso del dispositivo o del profilo di lavoro per impostazione predefinita:

- **Requisiti della password**
- **Policy di crittografia**
- **Blocco schermo disattivato**
- **Metodi di input consentiti**
- **Servizi di accessibilità consentiti**

Se il dispositivo o il profilo di lavoro rimane non conforme dopo 10 giorni, Android Device Policy eseguirà un ripristino alle impostazioni di fabbrica del dispositivo o eliminerà il profilo di lavoro.

In questa sezione puoi sostituire le regole di applicazione della conformità predefinite o aggiungerne di nuove.

Regole

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

Usa **Aggiungi regola** per creare una nuova regola. Ogni scheda regola può essere rimossa con l'azione di eliminazione.

Nome impostazione

La policy di primo livello da applicare. Ad esempio **Applicazioni** o **Requisiti della password**.

Obbligatorio. Il valore deve corrispondere a un nome di policy di primo livello supportato; in caso contrario il campo viene contrassegnato come non valido.

Blocca dopo giorni

Numero di giorni di non conformità della policy prima che il dispositivo o il profilo di lavoro venga bloccato. Per bloccare l'accesso immediatamente, imposta 0. **Blocca dopo giorni** deve essere inferiore a **Cancella dati dopo giorni**. Si applica solo ai dispositivi aziendali.

Intervallo consentito: 0–300.

Ambito del blocco

Specifica l'ambito dell'azione di blocco. Si applica solo ai dispositivi aziendali.

Predefinito (nuova regola): **Profilo di lavoro**.

> **Profilo di lavoro**: l'azione di blocco viene applicata solo alle app nel profilo di lavoro. Le app nel profilo personale non sono interessate.
>
> **Intero dispositivo**: l'azione di blocco viene applicata all'intero dispositivo, incluse le app nel profilo personale.

Cancella dati dopo giorni

Numero di giorni di non conformità della policy prima che il dispositivo o il profilo di lavoro venga cancellato.
Cancella dati dopo giorni deve essere maggiore di **Blocca dopo giorni**. Si applica solo ai dispositivi aziendali.

Obbligatorio. Predefinito (nuova regola): **1**.

Intervallo consentito: 1–300.

Mantieni la protezione dopo il ripristino di fabbrica

Indica se i dati di protezione dopo il ripristino di fabbrica vengono conservati sul dispositivo. Questa impostazione non si applica ai profili di lavoro.

Predefinito (nuova regola): attivato.