Policy - Android

Riepilogo

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

È possibile visualizzare le policy esistenti e crearne di nuove dalla sezione **Policy** della dashboard. Per aprire una policy Android, fare clic sulla riga della policy nella tabella: il sistema aprirà la pagina **Policy Editor**.

Una policy può essere associata a un token di registrazione, in modo che venga applicata automaticamente ai dispositivi durante il processo di configurazione. È inoltre possibile modificare la policy assegnata a un dispositivo anche dopo la configurazione.

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

> Molte opzioni di policy si applicano solo a determinati tipi di dispositivi (gestiti, dedicati, profilo di lavoro) e versioni di Android. Le impostazioni non supportate potrebbero 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. Nella parte superiore della pagina, è sempre possibile modificare:

- **Nome** (obbligatorio)
- **ID** (solo lettura)
- **Descrizione** (opzionale)

Le sezioni riportate di seguito corrispondono ai pannelli dell'editor delle policy (ad esempio: gestione delle app, sicurezza, rete, sistema, utilizzo personale, policy tra profili e altro). Utilizza le pagine di questo manuale per comprendere nel dettaglio ogni pannello.

Salva, elimina e dispositivi associati

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

Se hai aperto una policy esistente (che ha un ID), nella pagina vengono mostrate un'azione "**Elimina policy** e una lista di "**Dispositivi associati** in fondo, in modo da poter vedere quanti dispositivi stanno attualmente utilizzando la policy.

Gestione delle app

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

> Gli account Google Play gestiti vengono creati automaticamente quando i dispositivi vengono configurati.

1. Modalità Play Store

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

Elenco consentito (predefinito): Solo le app incluse nelle policy sono disponibili e qualsiasi app non presente nella policy verrà automaticamente disinstallata dal dispositivo. Il Play Store mostrerà solo le app disponibili.

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. Il Play Store mostrerà tutte le app, ad eccezione di quelle bloccate.

2. Policy sulle applicazioni non attendibili

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

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

Solo profilo personale: Per i dispositivi con profili di lavoro, consentire 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

Se la verifica delle app tramite Google Play Protect è obbligatoria.

Obbligatorio (predefinito): Abilita forzatamente la verifica delle app.

Scelta dell'utente: Consente all'utente di scegliere se abilitare o meno la verifica delle app.

4. Policy predefinita per le autorizzazioni

La policy per concedere le richieste di autorizzazioni durante l'esecuzione delle app.

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

Concedi: concedi automaticamente un'autorizzazione.

Nega: nega automaticamente un'autorizzazione.

5. Funzionalità dell'app

Controlla se le app sui dispositivi completamente gestiti o all'interno dei profili aziendali possono esporre le loro funzionalità. Richiede Android 16 o superiore.

Consentito (predefinito): Le app sui dispositivi completamente gestiti o all'interno dei profili aziendali possono esporre le loro funzionalità.

Non consentito: Le applicazioni su dispositivi completamente gestiti o all'interno dei profili aziendali non possono esporre le loro funzionalità.

6. Installazione di app disabilitata

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

7. Disinstallazione delle app disabilitata

Disattivazione della disinstallazione delle applicazioni da parte dell'utente.

8. Policy di autorizzazioni

Autorizzazioni esplicite o assegnazioni/negazioni di gruppo per tutte le app. Questi valori sovrascrivono l'impostazione della **policy delle autorizzazioni predefinita**.

Utilizza **la policy delle autorizzazioni** per creare voci e rimuoverle tramite 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**: Consenti / Nega / Richiedi (utilizza le stesse opzioni di policy di **policy predefinita per le autorizzazioni**).

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 la **modalità Play Store** è impostata su **lista consentita**, sono disponibili solo le app incluse nella policy e qualsiasi app non presente nella policy verrà automaticamente disinstallata dal dispositivo.

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

Per aggiungere una nuova app, clicca sul pulsante **Aggiungi applicazioni** (o sull'icona **Aggiungi applicazioni**), quindi scegli l'app dal Play Store e clicca 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, consulta la pagina **App private**.

Ogni app può essere configurata con le proprie impostazioni, visualizzate in modo intuitivo in una scheda:

9.1. Tipo di installazione

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 già installata in base a una policy precedente, verrà disinstallata.

Richiesto per la configurazione: L'app viene installata automaticamente e non può essere rimossa dall'utente; impedirà il completamento della configurazione fino al termine dell'installazione.

Modalità Kiosk: L'app viene installata automaticamente in modalità kiosk: viene impostata come app predefinita per l'intento "home" ed è inclusa nella lista delle app consentite per la modalità "lock task". La configurazione del dispositivo non verrà completata fino all'installazione dell'app. Dopo l'installazione, gli utenti non potranno disinstallare l'app. È possibile impostare questo **tipo di installazione** solo per una app per ogni policy. Quando questa opzione è presente nella policy, la barra di stato viene disattivata automaticamente.

Per maggiori informazioni, consultare la pagina dedicata **Modalità Kiosk**.

9.2. Vincoli di installazione

Definisce un insieme di restrizioni per l'installazione dell'app. Quando vengono selezionate più restrizioni, tutte devono essere soddisfatte affinché l'app possa essere installata.

> Questa opzione viene mostrata solo quando il **tipo di installazione** è **preinstallato** o **installato forzatamente**.

Rete non a consumo: installare l'app solo quando il dispositivo è connesso a una rete non a consumo (ad esempio, Wi-Fi).

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

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

9.3. Modalità di aggiornamento automatico

Controlla la modalità di aggiornamento automatico dell'app.

Predefinito: L'app viene aggiornata automaticamente con bassa priorità per ridurre al minimo l'impatto sull'utente. L'app viene aggiornata quando tutte le seguenti condizioni sono soddisfatte: (1) il dispositivo non è in uso attivo, (2) il dispositivo è connesso a una rete non a consumo, (3) il dispositivo è in carica. Il dispositivo viene notificato di un nuovo aggiornamento entro 24 ore dalla sua pubblicazione da parte dello sviluppatore, dopodiché l'app viene aggiornata la volta successiva in cui le condizioni sopra indicate sono soddisfatte.

Rimandata: L'aggiornamento dell'app non avviene 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 la modalità **Aggiornamento automatico** predefinita). Dopo che l'app è stata aggiornata, non viene aggiornata automaticamente di nuovo fino a 90 giorni dopo che diventa obsoleta di nuovo. L'utente può comunque aggiornare manualmente l'app dal Play Store in qualsiasi momento.

Priorità alta: L'app viene aggiornata il prima possibile. Non vengono applicate restrizioni. Il dispositivo viene immediatamente avvisato della disponibilità di un nuovo aggiornamento.

9.4. Versione minima supportata

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

9.5. Ambito delegato

Gli ambiti delegati all'app dal servizio di gestione delle policy dei dispositivi Android. È possibile concedere ad altre app una selezione di speciali autorizzazioni Android:

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

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

Blocco disinstallazione: Consente l'accesso alla funzione di blocco della disinstallazione.

Autorizzazioni: Consente l'accesso alle impostazioni delle autorizzazioni e allo stato delle concessioni di autorizzazioni.

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

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

9.6. Rete preferenziale

Servizio di rete preferenziale da utilizzare per questa app. Se impostato, l'app utilizzerà la specifica rete privata aziendale per le connessioni, quando disponibile. Questo valore deve corrispondere a una rete privata configurata nella sezione **Configurazione delle reti virtuali 5G** del pannello **Cellulare**.

9.7. Policy predefinita per le autorizzazioni

La policy predefinita per tutti i permessi richiesti dall'app. Se specificata, questa policy sovrascrive la **policy predefinita dei permessi** applicabile a tutte le app. Tuttavia, non sovrascrive le **policy**

dei permessi applicabili a tutte le app.

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

Concedi: concedi automaticamente un'autorizzazione.

Nega: nega automaticamente un'autorizzazione.

9.8. Lavoro e app personali sincronizzati

Controlla se l'app può comunicare con se stessa tra i profili lavoro e personali del dispositivo, previa autorizzazione dell'utente (Android 11+).

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

Consentito: Consente all'app di comunicare tra profili diversi previa autorizzazione dell'utente.

9.9. Eccezione alla modalità VPN Always On che impedisce il blocco del dispositivo

Specifica se l'app può utilizzare la rete quando la VPN non è connessa e la modalità **blocco** è attiva. Supportato solo sui dispositivi con Android 10 e versioni successive.

Applicata (predefinito): L'app rispetta l'impostazione di blocco VPN sempre attiva.

Escluso: L'app non è soggetta all'impostazione di blocco VPN sempre attiva.

9.10. Widget per il profilo di lavoro

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

Consentito: L'applicazione può aggiungere widget alla schermata principale.

Non consentito: L'applicazione non può aggiungere widget alla schermata principale.

9.11. Impostazioni di controllo utente

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

Non specificato: Utilizza il comportamento predefinito dell'app per determinare se il controllo da parte dell'utente è consentito o meno.

Consentito: L'app consente il controllo da parte dell'utente.

Non consentito: Il controllo da parte dell'utente non è consentito per questa app.

9.12. Disabilitato

L'app è disabilitata. Quando disabilitata, i dati dell'app vengono comunque conservati.

9.13. Consenti al provider di credenziali

Se l'app può agire come provider di credenziali su Android 14 e versioni successive.

9.14. Configurazione gestita

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

> **La configurazione gestita** è disponibile solo per le app che supportano questa funzionalità.

9.15. Policy di autorizzazioni

Definizione esplicita delle autorizzazioni concesse o negate per l'app. Questi valori sovrascrivono la **policy predefinita delle autorizzazioni** e le **policy delle autorizzazioni** applicabili a tutte le app.

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

9.16. Traccia gli ID

Elenco degli ID di tracciamento per la versione di test dell'app a cui un dispositivo può accedere. Se vengono selezionati più ID di tracciamento, i dispositivi ricevono l'ultima versione tra tutte le versioni disponibili. Se non viene selezionato alcun ID di tracciamento, i dispositivi hanno accesso solo alla versione di produzione dell'app.

> **L'opzione "ID di tracciamento"** è disponibile solo per le app che hanno almeno un ID di tracciamento disponibile per la tua organizzazione. Per maggiori dettagli su come aggiungere la tua organizzazione a un programma di test chiuso per un'app specifica, consulta qui.

10. Impostazioni predefinite dell'applicazione

Imposta le app predefinite per i tipi supportati. Quando un'app predefinita è impostata per almeno un tipo, gli utenti non possono modificare le app predefinite in quel profilo.

>

> È consentita una sola impostazione di app predefinita per ogni**tipo di app predefinita**. L'elenco delle app predefinite non deve contenere duplicati.

10.1. Tipo di applicazione predefinito

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

10.2. Ambito predefinito delle applicazioni

Seleziona dove applicare l'app predefinita (Gestione completa, Profilo lavoro o Profilo personale). Solo gli ambiti supportati dal tipo selezionato possono essere scelti.

> 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 **Gestione completa** o **Profilo di lavoro**, ogni app deve essere presente anche nell'elenco delle **Applicazioni** con il tipo di **installazione** non impostato su **Bloccato**.

11. Selezione della chiave privata

Consente di visualizzare un'interfaccia utente su un dispositivo per consentire all'utente di scegliere un alias di chiave privata se non sono presenti regole corrispondenti in **Regole di selezione della chiave privata**.

> Per i dispositivi con Android precedenti alla versione P, impostare questa opzione potrebbe rendere le chiavi aziendali vulnerabili.

12. Scegli le regole per la chiave privata

Controlla l'accesso delle app alle chiavi private. La regola determina quale chiave privata, se presente, la policy del dispositivo Android 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 che non sono specifiche per un URL

(cioè, se urlPattern non è impostato o è impostato su una stringa vuota o ".*") su Android 11 e versioni successive, direttamente, in modo che l'app possa chiamare KeyChain.getPrivateKey senza dover prima chiamare KeyChain.choosePrivateKeyAlias. Quando un'app chiama KeyChain.choosePrivateKeyAlias e più di una regola choosePrivateKeyRules corrisponde, l'ultima regola corrispondente definisce quale alias di chiave restituire.

Utilizza **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 utilizzare.

12.2. Modello dell'URL

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

12.3. Nomi dei pacchetti

Ai 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 vengono specificati nomi di pacchetti, l'alias viene fornito a tutte le app che chiamano KeyChain.choosePrivateKeyAlias o qualsiasi metodo sovraccarico (ma solo se viene chiamata 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.

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

> Per eliminare un'app, fai clic sull'icona del **cestino** che si trova nella parte inferiore della scheda dell'app.

Modalità chiosco

Con la modalità chiosco, è possibile limitare le funzionalità di un dispositivo a una singola app o a più app. La scelta tra la modalità chiosco con una singola app e quella con più app dipende dagli obiettivi della tua azienda.

In **modalità chiosco con una singola app**, un dispositivo è configurato per eseguire una sola applicazione e non consente agli utenti finali di accedere ad altre app sul dispositivo. Inoltre, non possono uscire dall'app, trasformando il dispositivo in uno dedicato a quella specifica applicazione.

Per abilitare questa modalità, specifica un'app nella sezione **Gestione delle app** e imposta il parametro **Tipo di installazione** su **Chiosco**.

In **modalità chiosco multi-app**, ai dispositivi è consentito l'accesso a più applicazioni. Gli utenti finali possono navigare tra diverse app tramite un launcher personalizzato. Per abilitare questa modalità, attiva l'opzione **launcher personalizzato per chiosco**.

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

Avvio personalizzato per la modalità kiosk

Indica se l'avvio personalizzato per la modalità kiosk è abilitato. Questo sostituisce la schermata iniziale con un avvio che blocca il dispositivo alle app installate tramite l'impostazione "**Gestione delle app**". Le app vengono visualizzate in una singola pagina in ordine alfabetico.

Azioni del pulsante di accensione

Definisce il comportamento del dispositivo in modalità kiosk quando un utente preme e tiene premuto (pressione prolungata) il pulsante di accensione.

> **Disponibile (predefinito)**: Il menu di alimentazione (ad esempio, Spegnimento, Riavvio) viene visualizzato quando un utente preme e tiene premuto (pressione prolungata) il pulsante di accensione di un dispositivo in modalità kiosk.
>
> **Bloccato**: Il menu di alimentazione (ad esempio, Spegnimento, Riavvio) non viene visualizzato quando un utente preme e tiene premuto 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 di dialogo per errori di sistema delle app che si bloccano o non rispondono sono disabilitate in modalità kiosk. Se disabilitate, il sistema interromperà forzatamente l'app, come se l'utente avesse scelto l'opzione "chiudi app" nell'interfaccia utente.

Bloccato (predefinito): Tutte le finestre di dialogo per errori di sistema, come i crash e le applicazioni che non rispondono (ANR), sono bloccate. Quando sono bloccate, il sistema interrompe forzatamente l'app, come se l'utente la chiudesse dall'interfaccia utente.

Attivato: Tutte le finestre di dialogo relative agli errori di sistema, come i crash e le applicazioni che non rispondono (ANR), vengono visualizzate.

Navigazione del sistema

Specifica quali funzionalità di navigazione sono abilitate (ad esempio, i pulsanti Home e Panoramica) in modalità kiosk.

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

Solo Home: È attivo solo il pulsante Home.

Attivato: I pulsanti Home e panoramica sono attivi.

Barra di stato

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

Disabilitato (predefinito): Le informazioni di sistema e le notifiche sono disabilitate in modalità kiosk.

Solo informazioni di sistema: Vengono visualizzate solo le informazioni di sistema nella barra di stato.

Attivato: In modalità kiosk, nella barra di stato vengono visualizzate le informazioni di sistema e le notifiche. Nota: affinché questa impostazione 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 kiosk.

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

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

Sicurezza

In questa sezione, puoi configurare le policy relative alla sicurezza.

Azioni per la gestione dei rischi di sicurezza

Scegli cosa fare quando un dispositivo segnala un rischio di sicurezza nei report di stato.

Tipi di rischio di sicurezza supportati:

- **Sistema operativo sconosciuto**: L'API Play Integrity rileva che il dispositivo sta eseguendo un sistema operativo sconosciuto (il controllo basicIntegrity ha esito positivo, ma ctsProfileMatch fallisce).
- **Sistema operativo compromesso**: L'API Play Integrity rileva che il dispositivo sta utilizzando un sistema operativo compromesso (il controllo basicIntegrity non è stato superato).
- **Valutazione basata sull'hardware non riuscita**: L'API Play Integrity rileva che il dispositivo non dispone di una garanzia di integrità del sistema, se l'etichetta MEETS_STRONG_INTEGRITY non è visibile nel campo dell'integrità del dispositivo.

Azioni disponibili:

- **Cancellazione dati aziendali (impostazione predefinita)**: Deregistra e cancella i dati di lavoro (intero dispositivo se completamente gestito, oppure solo il profilo di lavoro se gestito solo per il profilo).
- **Nessuna azione**: Mantieni il dispositivo registrato e non eseguire alcuna operazione automaticamente.

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

- **Mantieni la protezione di ripristino ai dati di fabbrica**: Conserva i dati di Factory Reset Protection (FRP) durante la cancellazione del dispositivo.

Cancella la memoria esterna: Cancella anche la memoria esterna del dispositivo (come le schede SD) durante l'operazione di cancellazione.

Cancella eSIM: Per i dispositivi di proprietà dell'azienda, questa operazione rimuove tutte le eSIM dal dispositivo durante la cancellazione. Nei dispositivi di proprietà personale, questa operazione rimuove le eSIM gestite (eSIM aggiunte tramite il comando ADD_ESIM) presenti nei dispositivi, senza rimuovere le eSIM di proprietà dell'utente.

1. Tempo massimo di blocco

Tempo massimo (in secondi) di attività dell'utente prima del blocco del dispositivo. Un valore di 0 indica che non ci sono restrizioni.

2. Rimani attivo durante la ricarica

Le modalità di ricarica per le quali il dispositivo rimane attivo. Quando si utilizza questa impostazione, si consiglia di deselezionare "**Tempo massimo di 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.

Ricarica wireless: La fonte di alimentazione è wireless.

3. Blocco schermo disabilitato

Se impostato su "vero", questa opzione disabilita la schermata di blocco per i display principali e/o secondari. Questa policy è supportata solo in modalità di gestione dispositivo dedicata.

4. Requisiti della password

Policy relative ai requisiti della password.

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

I requisiti per la password possono utilizzare **l'ambito "Auto"** (un solo requisito) oppure 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 si applicano 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 si applicano solo al dispositivo.

Profilo di lavoro: I requisiti della password si applicano solo al profilo di lavoro.

4.2. Lunghezza della cronologia delle password

Lunghezza della cronologia delle password. Dopo aver impostato questo valore, l'utente non potrà inserire una nuova password identica a una password presente nella cronologia. Un valore di 0 indica che non ci sono restrizioni.

4.3. Numero massimo di tentativi di password errati prima della cancellazione del dispositivo

Numero massimo di tentativi di password errati per lo sblocco del dispositivo prima della cancellazione. Il valore 0 indica che non ci sono restrizioni.

4.4. Timeout di scadenza della password (giorni)

Questa impostazione obbliga l'utente a cambiare periodicamente la password, dopo il numero di giorni specificato.

4.5. Richiedi sblocco con password

Il tempo dopo il quale un dispositivo o un profilo di lavoro sbloccati tramite un metodo di autenticazione sicuro (password, PIN, sequenza) possono essere sbloccati con qualsiasi altro metodo (ad esempio, impronta digitale, agenti di fiducia, riconoscimento facciale). Trascorso il periodo di tempo specificato, solo i metodi di autenticazione sicuri possono essere utilizzati per sbloccare il dispositivo o il profilo di lavoro.

Impostazione predefinita del dispositivo: Il periodo di timeout è impostato sull'impostazione predefinita del dispositivo.

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

4.6. Qualità della password

Il livello di sicurezza richiesto per la password.

Complessità elevata: Definire la soglia di complessità elevata per le password come segue: Su Android 12 e versioni successive: PIN senza sequenze ripetute (4444) o ordinate (1234,

4321, 2468), lunghezza minima di 8; alfanumerico, lunghezza minima di 6.

Complessità media: Definire la soglia di complessità media per le password come segue: PIN senza sequenze ripetute (4444) o ordinate (1234, 4321, 2468), lunghezza minima di 4; alfanumerico, lunghezza minima di 4.

Bassa complessità: Definire la soglia di bassa complessità per le password come segue: schema; PIN con sequenze ripetute (4444) o ordinate (1234, 4321, 2468).

Nessuna: Non sono presenti requisiti per le password.

Debole: Il dispositivo deve essere protetto con una tecnologia di riconoscimento biometrico a bassa sicurezza, almeno. Questo include tecnologie in grado di riconoscere l'identità di un individuo che siano grosso modo equivalenti a un codice PIN di 3 cifre (la probabilità di un falso riconoscimento è inferiore a 1 su 1.000).

Qualsiasi: è richiesta una password, ma non ci sono restrizioni sul suo contenuto.

Numerico: La password deve contenere caratteri numerici.

Numerico complesso: La password deve contenere caratteri numerici, senza sequenze ripetute (come 4444) o ordinate (come 1234, 4321, 2468).

Alfanumerico: La password deve contenere caratteri alfanumerici (o simboli).

Alfanumerico: La password deve contenere sia numeri che caratteri alfabetici (o simboli).

Complessità: 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. Numero minimo di lettere

Numero minimo di caratteri richiesti per la password.

4.9. Numero minimo di lettere minuscole

Numero minimo di lettere minuscole richieste nella password.

4.10. Numero minimo di lettere maiuscole

Numero minimo di lettere maiuscole richieste nella password.

4.11. Numero minimo di caratteri non alfabetici richiesti

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

4.12. Numero minimo di cifre numeriche

Numero minimo di cifre numeriche richieste nella password.

4.13. Numero minimo di simboli

Numero minimo di simboli richiesti nella password.

4.14. Blocco unificato

Controlla se il blocco unificato è consentito per il dispositivo e il profilo aziendale, sui dispositivi con Android 9 e versioni successive che dispongono di un profilo aziendale. Questa impostazione non ha effetto su altri dispositivi.

> **Consenti blocco unificato**: È consentito un blocco comune per il dispositivo e il profilo aziendale.
>
> **Richiedi blocco del lavoro separato**: È richiesto un blocco separato per il profilo aziendale.

5. Ripristino ai dati di fabbrica disabilitato

Se la reimpostazione ai dati di fabbrica dalle impostazioni è disabilitata. Si applica solo ai dispositivi completamente gestiti.

6. Protezione dalla reimpostazione ai dati di fabbrica

Indirizzi email degli amministratori del dispositivo per la protezione dalla reimpostazione ai dati di fabbrica. In caso di reimpostazione ai dati di fabbrica non autorizzata, sarà necessario che uno di questi amministratori effettui l'accesso con l'indirizzo email e la password dell'account Google per sbloccare il dispositivo. Se non vengono specificati amministratori, il dispositivo non fornirà protezione dalla reimpostazione ai dati di fabbrica. Si applica solo ai dispositivi completamente gestiti.

Indirizzi email degli amministratori: utilizzare **Abilita protezione dalla reimpostazione ai dati di fabbrica** per iniziare a configurare gli amministratori. Quindi, utilizzare **Aggiungi indirizzo email dell'amministratore** per aggiungere gli indirizzi e rimuoverli con l'azione di eliminazione.

7. Funzionalità di Keyguard

Funzionalità di Keyguard (schermata di blocco) che possono essere disabilitate.

7.1. Disabilita tutto

Disabilita tutte le personalizzazioni attuali e future della schermata di blocco.

7.2. Disabilita la fotocamera

Disabilita la fotocamera nelle schermate di blocco sicure (ad esempio, con PIN).

7.3. Disabilita le notifiche

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

7.4. Disabilita le notifiche non oscurate

Disabilita le notifiche non oscurate nelle schermate di blocco protette.

7.5. Ignora lo stato dell'agente di fiducia

Ignora lo stato dell'agente di fiducia nelle schermate di blocco sicure.

7.6. Disabilita l'impronta digitale

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

7.7. Disabilita l'inserimento di testo nelle notifiche

Disabilita l'inserimento di testo nelle notifiche quando si utilizza la schermata di blocco sicura.

7.8. Disabilita l'autenticazione tramite riconoscimento facciale

Disabilita l'autenticazione tramite riconoscimento facciale nelle schermate di blocco protette.

7.9. Disabilita l'autenticazione tramite iride

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

7.10. Disabilita tutte le autenticazioni biometriche

Disabilita tutte le autenticazioni biometriche sulle schermate di blocco sicure.

7.11. Disabilita tutte le scorciatoie

Disabilita tutte le scorciatoie nella schermata di blocco sicura su Android 14 e versioni successive.

Multimedia

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

1. Accesso alla fotocamera

Controlla l'utilizzo della fotocamera e se l'utente può attivare o disattivare l'accesso alla fotocamera (solo su Android 12+). In generale, disabilitare la fotocamera si applica a tutti i dispositivi gestiti, e solo all'interno del profilo di lavoro sui dispositivi con profilo di lavoro.

> **Scelta dell'utente (predefinito)**: Comportamento predefinito del dispositivo. Le fotocamere sono disponibili e (su Android 12+) l'utente può attivare o disattivare l'accesso alla fotocamera.
>
> **Disabilitato**: Tutte le fotocamere sono disabilitate (gestione completa: a livello di dispositivo; profilo di lavoro: solo per le app del profilo di lavoro). L'interruttore di accesso alla fotocamera non ha effetto nell'ambito gestito.
>
> **Applicata**: Le fotocamere sono disponibili. Sui dispositivi completamente gestiti con Android 12 o versioni successive, l'utente non può abilitare o disabilitare l'accesso alla fotocamera. Su altri dispositivi/versioni, il comportamento è simile alla scelta dell'utente.

2. Accesso al microfono

Su dispositivi completamente gestiti, controlla l'utilizzo del microfono e se l'utente può accedere all'interruttore per abilitare o disabilitare l'accesso al microfono (Android 12+). Questa impostazione non ha effetto sui dispositivi non completamente gestiti.

> **Scelta dell'utente (predefinita)**: Comportamento predefinito. Il microfono è disponibile e (in Android 12+) l'utente può attivare o disattivare l'accesso al microfono.
>
> **Disattivato**: Il microfono è disattivato a livello di dispositivo. L'interruttore di accesso al microfono non ha alcun effetto.
>
> **Applicata**: Il microfono è disponibile. Su Android 12 e versioni successive, l'utente non può attivare o disattivare l'accesso al microfono. Su Android 11 o versioni precedenti, il comportamento è simile alla scelta dell'utente.

3. Accesso ai dati tramite USB

Controlla quali file e/o dati possono essere trasferiti tramite USB. Supportato solo sui dispositivi di proprietà aziendale.

Disabilita il trasferimento di file (predefinito): Il trasferimento di file è disabilitato, ma altre connessioni USB (ad esempio mouse/tastiera) sono consentite.

Non consentire il trasferimento dati: Tutti i tipi di trasferimento dati tramite USB sono bloccati (Android 12+ con USB HAL 1.3+). Se non supportato, il dispositivo ricade sull'opzione "Non consentire il trasferimento file".

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

4. Stampa

Consente o meno la stampa (Android 9+).

Consentito (predefinito): La stampa è consentita.

Non consentito: La stampa non è consentita (Android 9 e versioni successive).

5. Impostazioni della luminosità dello schermo

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

Modalità luminosità dello schermo:

Scelta dell'utente (predefinito): L'utente può configurare la luminosità dello schermo.

Automatico: La luminosità è regolata automaticamente e l'utente non può modificarla. È comunque possibile impostare un valore di luminosità, che viene utilizzato come parte della regolazione automatica (Android 9+ con gestione completa; profili aziendali su dispositivi Android 15+).

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

Luminosità dello schermo:

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

6. Impostazioni del timeout dello schermo

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

Il campo **Modalità timeout dello schermo** consente di scegliere tra un comportamento controllato dall'utente e uno imposto.

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

Timeout dello schermo: Obbligatorio: il timeout dello schermo è impostato sul valore configurato e l'utente non può modificarlo (Android 9+ con gestione completa; profili di lavoro su dispositivi Android aziendali 15+)

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

7. Acquisizione schermo disabilitata

Se l'acquisizione schermo è disabilitata.

Regolazione del volume disabilitata

La possibilità di regolare il volume principale è disabilitata.

9. Montaggio di supporti fisici disabilitato

Montaggio di supporti esterni fisici: disabilitato.

Cellulare

In questa sezione, puoi configurare le impostazioni relative alla connettività cellulare.

1. Modalità aereo

Consente o meno all'utente di attivare o disattivare la modalità aereo.

Scelta dell'utente (predefinito): L'utente può attivare o disattivare la modalità aereo.

Disabilitato: La modalità aereo è disattivata. L'utente non può attivare o disattivare la modalità aereo. Supportato su Android 9 e versioni successive.

2. Cellulare 2G

Consente di definire se l'utente può attivare o disattivare l'impostazione della rete cellulare 2G.

Scelta utente (predefinito): L'utente può attivare o disattivare la rete cellulare 2G.

Disabilitato: La rete cellulare 2G è disabilitata. L'utente non può attivare o disattivare la rete cellulare 2G tramite le impostazioni. Supportato su Android 14 e versioni successive.

3. Sovrascrivi le configurazioni APN

Controlla se le configurazioni APN personalizzate sono attive o disattive. Quando attive, vengono utilizzate solo le configurazioni APN personalizzate e tutte le altre configurazioni APN sul dispositivo vengono ignorate.

Disabilitato (predefinito): Tutte le impostazioni APN configurate vengono salvate sul dispositivo, ma sono disabilitate e non hanno effetto. Tutte le altre impostazioni APN sul dispositivo rimangono attive.

Abilitato: Vengono utilizzati solo gli APN sovrascritti, mentre tutti gli altri APN vengono ignorati. Questa impostazione può essere configurata solo sui dispositivi gestiti 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 profilo 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'identificativo APN fornito dal tuo operatore.

Nome visualizzato: Nome amichevole mostrato nell'interfaccia utente.

Campi APN facoltativi:

Tipo di autenticazione, **Nome utente**, **Password**: Configura l'autenticazione del gestore (se necessario).

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

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

Indirizzo del proxy e **porta del proxy**: proxy HTTP per il traffico dati (se applicabile).

Indirizzo del proxy MMS, **Porta del proxy MMS**, **MMSC (URI del server MMS)**: impostazioni relative a MMS.

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

Impostazione "Sempre attivo": indica se la sessione PDU attivata da questa APN deve essere sempre attiva. Supportata su Android 15 e versioni successive.

Tipo MVNO: Identificatore del tipo di operatore di rete mobile virtuale.

MTU IPv4 e **MTU IPv6**: Unità Massima di Trasmissione per le route IPv4/IPv6. Supportato su Android 13 e versioni successive.

5. Configurazione della trasmissione cellulare disabilitata

Che la configurazione della trasmissione cellulare sia disabilitata.

6. Configurazione delle reti mobili disabilitata

La configurazione delle reti mobili è disabilitata.

7. Dati in roaming disabilitati

Servizi di roaming disabilitati.

8. Chiamate in uscita disabilitate

Se le chiamate in uscita sono disabilitate.

9. SMS disabilitati

L'invio e la ricezione di SMS sono disabilitati.

10. Configurazione dello slicing della rete 5G

Configura le impostazioni del servizio di rete preferenziale per abilitare lo slicing della rete 5G aziendale. Puoi configurare fino a 5 slice aziendali e assegnare applicazioni a reti specifiche per un instradamento del traffico ottimizzato.

10.1. Rete preferenziale predefinita

ID della rete preferenziale predefinita per le applicazioni che non sono presenti nell'elenco delle applicazioni, oppure se la **Rete preferenziale** dell'app non è configurata. Deve avere una configurazione per l'ID di rete specificato (a meno che non sia impostato su **Nessuna rete preferenziale**).

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

10.2. Configurazione dei servizi di rete

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

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

Passaggio alla connessione predefinita: Indica se è consentito passare alla connessione di rete predefinita del dispositivo. Se non consentito, le app non possono accedere a Internet se la rete 5G non è disponibile.

Reti non corrispondenti: Indica se le applicazioni soggette a questa configurazione possono utilizzare reti diverse da quella preferenziale. Se impostato su **Non consentito**, anche l'opzione **Passaggio 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 Wi-Fi**. A seconda del valore impostato in **Configura Wi-Fi**, gli utenti potrebbero avere un controllo limitato o nullo sull'aggiunta/modifica delle reti.

Stato della radio del dispositivo

Stato di Wi-Fi

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

> **Scelta dell'utente (predefinito)**: all'utente è consentito abilitare o disabilitare il Wi-Fi.
>
> **Attivato**: il Wi-Fi è attivo e l'utente non può disabilitarlo (Android 13 e versioni successive).
>
> **Disattivato**: il Wi-Fi è disattivato e l'utente non può riattivarlo (Android 13 e versioni successive).

2. Livello minimo di sicurezza Wi-Fi

Il livello minimo di sicurezza Wi-Fi richiesto per le reti a cui il dispositivo può connettersi. Supportato su Android 13 e versioni successive, per dispositivi gestiti completamente e profili di lavoro su dispositivi aziendali.

> **Rete aperta (predefinito)**: Il dispositivo può connettersi a tutti i tipi di reti Wi-Fi.
>
> **Rete personale**: Impedisce la connessione a reti Wi-Fi aperte; richiede almeno una sicurezza di livello 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; è l'opzione più restrittiva.

3. Stato della tecnologia Ultra Wideband (UWB)

Controlla lo stato dell'impostazione Ultra Wideband e se l'utente può attivare o disattivare questa funzionalità.

Scelta dell'utente (predefinita): L'utente può attivare o disattivare l'Ultra Wideband.

Disattivato: UWB è disattivato e l'utente non può attivarlo o disattivarlo tramite le impostazioni (Android 14 e versioni successive).

Gestione della connettività dei dispositivi

4. Condivisione via Bluetooth

Controlla se la condivisione via Bluetooth è consentita.

Consentito: La condivisione via Bluetooth è consentita (impostazione predefinita per i dispositivi completamente gestiti, Android 8+).

Non consentito: La condivisione via Bluetooth non è consentita (impostazione predefinita per i profili aziendali, Android 8+).

5. Configurare 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): L'utente può 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 all'altra tra quelle già configurate (Android 13+; profili di lavoro aziendali e dispositivi di proprietà dell'azienda).

Non consentire la configurazione di reti Wi-Fi: Impedisce la configurazione di nuove reti Wi-Fi. Per i dispositivi gestiti centralmente, questa opzione rimuove le reti configurate dall'utente e mantiene solo le reti configurate tramite **configurazioni Wi-Fi**. Per i profili di lavoro aziendali, le reti esistenti non vengono modificate, ma gli utenti non possono aggiungere, rimuovere o modificare le reti Wi-Fi.

> Quando la configurazione Wi-Fi è disabilitata e il dispositivo non riesce a connettersiall'avvio, il sistema può mostrare la **funzione di bypass della rete** per consentire all'utente di connettersi temporaneamente e aggiornare le policy.

6. Impostazioni Wi?Fi Direct

Controlli per la configurazione e l'utilizzo delle impostazioni Wi-Fi Direct. Supportato su dispositivi aziendali con Android 13 e versioni successive.

Consenti (predefinito): L'utente può utilizzare Wi-Fi Direct.

Non consentire: L'utente non può utilizzare Wi-Fi Direct.

7. Impostazioni di tethering

Controlla le impostazioni di tethering. In base al valore impostato, l'utente può essere parzialmente o completamente impedito di utilizzare diverse forme di tethering.

Consenti tutte le modalità di tethering (predefinito): Consente la configurazione e l'utilizzo di tutte le forme di tethering.

Non consentire il tethering Wi-Fi: Impedisce all'utente di utilizzare il tethering Wi-Fi (solo dispositivi Android 13+ di proprietà aziendale).

Disabilita tutte le funzionalità di tethering: Impedisce l'utilizzo di qualsiasi tipo di tethering (dispositivi completamente gestiti e profili di lavoro aziendali).

8. Policy relativa all'SSID Wi-Fi

Restrizioni sulle reti Wi-Fi a cui il dispositivo può connettersi (questo non influisce sulle reti che possono essere configurate sul dispositivo). Supportato su dispositivi aziendali con Android 13 e versioni successive.

Elenco delle reti Wi-Fi non consentite (predefinito): Il dispositivo non può connettersi a nessuna rete Wi-Fi il cui nome (SSID) è presente nell'elenco, ma può connettersi ad altre reti.

Elenco delle reti Wi-Fi consentite: Il dispositivo può connettersi solo alle reti con SSID presenti nell'elenco. L'elenco degli SSID non deve essere vuoto.

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

Nell'interfaccia utente 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 per il 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'identificativo SSID a cui si applica l'impostazione di roaming (obbligatorio).
>
> **Modalità roaming Wi-Fi**: Predefinita / Disabilitata / Aggressiva. Le opzioni Disabilitata e Aggressiva richiedono Android 15 o superiore e sono supportate solo su dispositivi completamente gestiti e profili di lavoro su dispositivi aziendali.

Restrizioni di rete

Bluetooth disabilitato

Bluetooth disabilitato. Preferire questa impostazione rispetto a "Configurazione Bluetooth disabilitata" perché quest'ultima può essere modificata dall'utente.

11. Condivisione contatti Bluetooth disabilitata

Se la condivisione contatti tramite Bluetooth è disabilitata.

12. Configurazione Bluetooth disabilitata

La configurazione di Bluetooth è disabilitata.

13. Ripristino di rete disabilitato

Se il ripristino delle impostazioni di rete è disabilitato.

14. Trasmissione in uscita disabilitata

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

VPN

App VPN sempre attiva

Specifica un nome pacchetto VPN sempre attiva per garantire che i dati delle app gestite indicate vengano sempre trasmessi tramite una VPN configurata.

> Nota: questa funzionalità richiede la distribuzione di un client VPN che supporti sia la funzionalità VPN sempre attiva che le funzionalità VPN specifiche per app.

16. Blocco VPN

Impedisce la connessione alla rete quando la VPN non è attiva.

17. Configurazione VPN disabilitata

La configurazione VPN è disabilitata.

Servizi proxy e di rete

18. Servizio di rete preferenziale

Abilita o disabilita il servizio di rete preferenziale sul profilo di lavoro. Ad esempio, un'organizzazione potrebbe avere un accordo con un operatore che prevede l'utilizzo di una rete dedicata ai servizi aziendali (ad esempio, una rete aziendale su reti 5G) per il traffico dati aziendale. Questa impostazione non ha effetto sui dispositivi completamente gestiti.

Disabilitato: Il servizio di rete preferenziale è disabilitato nel profilo di lavoro.

Attivato: Il servizio di rete preferenziale è attivo nel profilo di lavoro.

>

> Se utilizzi il network slicing aziendale, configura anche**Configurazione del Network Slicing 5G** nella sezione **Cellulare** e assegna le applicazioni a una slice utilizzando la loro impostazione **Rete Preferenziale**.

19. Proxy globale consigliata

Il proxy HTTP globale indipendente dalla rete. In genere, i proxy dovrebbero essere configurati per ogni rete nelle impostazioni Wi-Fi. Un proxy globale può essere utile per configurazioni particolari, come la filtrazione interna generale. Il proxy globale è solo un suggerimento e alcune app potrebbero ignorarlo.

Disabilitato

Proxy diretto

Proxy di configurazione automatica (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 utilizzato per configurare il proxy.

19.4. Host esclusi

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

Utilizza **Aggiungi host esclusi** per aggiungere voci (disponibile solo per proxy diretto).

Configurazioni Wi-Fi

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

20. Campi di configurazione Wi-Fi

Ogni configurazione include:

Nome della configurazione: Obbligatorio.

SSID: Obbligatorio.

Connessione automatica: Indica se la rete deve connettersi automaticamente quando è disponibile.

Transizione rapida: Indica se il dispositivo deve tentare di utilizzare la transizione rapida (IEEE 802.11r-2008) con la rete.

SSID nascosto: Indica se il nome della rete (SSID) verrà trasmesso.

Modalità di randomizzazione MAC: Hardware o Automatica (Android 13 e versioni successive).

20.1. Sicurezza

Opzioni di sicurezza Wi-Fi:

WEP-PSK: WEP (chiave precondivisa).

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

WPA-EAP: WPA/WPA2/WPA3-Enterprise (Protocollo di autenticazione estendibile).

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

20.2. Password (Chiave precondivisa)

Mostrato quando la sicurezza è **WEP-PSK** o **WPA-PSK**. La password è richiesta.

20.3. Metodo EAP (Enterprise)

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

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Autenticazione, fase 2

Mostrato per il tunneling dei metodi esterni (**EAP-TTLS** e **PEAP**).

MSCHAPv2

PAP

20.5. Credenziali EAP fornite dagli utenti

Quando abilitata, il sistema applica automaticamente le credenziali EAP ai dispositivi, configurandole su base individuale per ogni utente. È possibile configurare le credenziali degli utenti nella sezione **Utenti**.

20.6. Certificato client

Per **EAP-TLS**, è possibile assegnare un certificato client utilizzato per l'autenticazione Wi-Fi. Per maggiori informazioni, consulta la pagina **Gestione dei certificati**.

Se un certificato è già assegnato, è possibile utilizzare **Apri certificato** per visualizzarlo oppure **Cambia certificato** per selezionarne uno diverso.

In alternativa, è possibile specificare **l'alias della coppia di chiavi del certificato client**, che fa riferimento a un certificato client memorizzato nel keychain di Android ed è consentito per l'autenticazione Wi-Fi.

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

20.7. Identità

Identità dell'utente. Per i protocolli di tunneling esterni (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 che non utilizzano il tunneling, questo viene utilizzato per l'identità EAP.

20.8. Identità anonima

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

20.9. Password

Password dell'utente. Se non specificata, verrà richiesto l'inserimento da parte dell'utente.

20.10. Certificati CA del server

Elenco dei certificati CA da utilizzare per verificare la catena di certificati dell'host. Almeno un certificato CA deve corrispondere. Per maggiori informazioni, consultare la pagina **Gestione dei certificati**.

Utilizza **Aggiungi certificato CA del server** per aggiungere elementi e rimuoverli utilizzando l'azione di eliminazione.

20.11. Il suffisso del dominio corrisponde

Un elenco di vincoli per il nome di dominio del server. Le voci vengono utilizzate come requisiti di corrispondenza del suffisso rispetto al nome DNS del nome alternativo del soggetto di un certificato del server di autenticazione.

Sistema

In questa sezione, è possibile configurare le policy relative al sistema.

1. Livello API minimo

Il livello minimo dell'API Android consentito.

2. Policy di crittografia

Se la crittografia è abilitata.

> **Predefinito**: Questo valore viene ignorato, ovvero non è richiesta alcuna crittografia.
>
> **Attivato senza password**: La crittografia è richiesta, ma non è necessaria alcuna password per l'avvio.
>
> **Attivato con password**: La crittografia è richiesta e la password è necessaria per l'avvio.

3. Data e ora impostate automaticamente

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

> **Scelta dell'utente (predefinito)**: La data, l'ora e il fuso orario vengono impostati in base alla scelta dell'utente.
>
> **Applicata**: Imposta automaticamente la data, l'ora e il fuso orario sul dispositivo.

4. Impostazioni per sviluppatori

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

> **Disattivata (predefinito)**: Disabilita tutte le impostazioni per sviluppatori e impedisce all'utente di accedervi.

Consentito: Consente tutte le impostazioni per sviluppatori. L'utente può accedere e, opzionalmente, configurare le impostazioni.

5. Modalità Common Criteria

Controlli: Modalità Criteri Comuni – standard di sicurezza definiti nei Criteri Comuni per la Valutazione della Sicurezza dell'Informazione (CC). L'attivazione della Modalità Criteri Comuni aumenta 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 dell'integrità delle policy crittografiche). La Modalità Criteri Comuni è supportata solo sui dispositivi di proprietà dell'azienda con Android 11 o versioni successive. Attenzione: la Modalità Criteri Comuni impone un modello di sicurezza rigoroso, generalmente richiesto solo per organizzazioni con esigenze di sicurezza elevate. L'utilizzo normale del dispositivo potrebbe risentirne; attivala solo se necessario.

Disabilitata (predefinito): Disabilita la Modalità Criteri Comuni.

Attivata: Abilita la Modalità Criteri Comuni.

6. Estensione per il Tagging della Memoria (MTE)

Controlla l'estensione per il Tagging della Memoria (MTE) sul dispositivo.

Scelta dell'utente (predefinita): L'utente può scegliere di abilitare o disabilitare MTE sul dispositivo (se supportato dal dispositivo).

Forzata: MTE è abilitata e l'utente non può modificarla (Android 14 e versioni successive; supportata sui dispositivi completamente gestiti e sui profili di lavoro sui dispositivi di proprietà aziendale).

Disabilitata: MTE è disabilitata e l'utente non può modificarla (Android 14 e versioni successive; supportata solo sui dispositivi completamente gestiti).

7. Protezione dei contenuti

Controlla se la protezione dei contenuti (che verifica la presenza di app potenzialmente dannose) è abilitata. Questa funzionalità è supportata su Android 15 e versioni successive.

Disabilitato (predefinito): La protezione dei contenuti è disabilitata e l'utente non può modificarla.

Applicata: La protezione dei contenuti è abilitata e l'utente non può modificarla (Android 15 e versioni successive).

Scelta dell'utente: La protezione dei contenuti non è gestita dalla policy; l'utente può scegliere (Android 15 e versioni successive).

8. Assistenza contenuti

Controlla se l'invio di AssistContent a un'app privilegiata, come un'app di assistenza (ad esempio, Circle to Search), è consentito. AssistContent include screenshot e informazioni su un'app, come il nome del pacchetto. Questa funzionalità è supportata su Android 15 e versioni successive.

Consentito (predefinito): È consentito inviare contenuti di supporto a un'app privilegiata (Android 15 e versioni successive).

Non consentito: L'invio di contenuti di supporto a un'applicazione privilegiata è bloccato (Android 15 e versioni successive).

9. Crea finestre disabilitate

Se la creazione di finestre aggiuntive, separate dalle finestre dell'app, è disabilitata. Questa opzione impedisce la visualizzazione delle seguenti interfacce utente del sistema: notifiche e barre di avviso, attività del telefono (come chiamate in arrivo) e attività telefoniche prioritarie (come chiamate in corso), avvisi di sistema, errori di sistema e sovrapposizioni di sistema.

10. Porta di emergenza per la rete

Se la funzione "porta di emergenza per la rete" è attiva. Se non è possibile stabilire una connessione di rete all'avvio, la porta di emergenza chiede all'utente di connettersi temporaneamente a una rete per aggiornare le impostazioni del dispositivo. Dopo l'applicazione delle impostazioni, la connessione temporanea viene dimenticata e il dispositivo continua l'avvio. Questo impedisce di non poter connettersi a una rete se non è disponibile una rete adatta nelle impostazioni correnti e il dispositivo si avvia in una modalità specifica, oppure se l'utente non riesce ad accedere alle impostazioni del dispositivo.

11. Attività predefinite

Un elenco di attività predefinite per la gestione delle richieste che corrispondono a un determinato filtro. Ad esempio, questa funzionalità consentirebbe agli amministratori IT di scegliere quale app browser si apre automaticamente per i link web, o quale app di avvio viene utilizzata quando si

tocca il pulsante Home.

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

11.1. Attività del dispositivo ricevente

L'attività che deve essere l'handler predefinito. Questo deve essere il nome di un componente Android, ad esempio 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.

11.2. Azione

Le azioni da includere nel filtro. Se nel filtro sono incluse delle azioni, l'azione di un'intent deve corrispondere a uno di quei valori per essere considerata valida. Se non sono incluse azioni, l'azione dell'intent viene ignorata.

11.3. Categoria

Le categorie di intent da utilizzare nel filtro. Un intent include le categorie richieste, e tutte queste categorie devono essere incluse nel filtro affinché corrisponda. In altre parole, aggiungere una categoria al filtro non ha alcun effetto sulla corrispondenza, a meno che tale categoria non sia specificata nell'intent.

12. Metodi di input consentiti

Specifica i metodi di input consentiti.

> **Metodi consentiti:** Nessuna restrizione applicata. Tutti i metodi di input sono consentiti.
>
> **Solo metodi di input integrati nel sistema**: Sono consentiti solo i metodi di input integrati nel sistema.
>
> **Solo quelli forniti e integrati nel sistema**: Sono consentiti solo i metodi di input forniti e quelli integrati nel 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**.

Utilizza **"Aggiungi metodo di input"** per aggiungere elementi e rimuoverli tramite l'azione di eliminazione.

13. Servizi di accessibilità consentiti

Specifica i servizi di accessibilità consentiti.

Servizi consentiti: tutti: è possibile utilizzare qualsiasi servizio di accessibilità.

Servizi di accessibilità integrati: È possibile utilizzare solo i servizi di accessibilità integrati nel sistema.

Solo servizi forniti e integrati: È possibile utilizzare solo i servizi di accessibilità forniti e quelli integrati nel sistema.

13.1. Servizi di accessibilità consentiti

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

Utilizza il servizio di accessibilità **Aggiungi** per aggiungere elementi e rimuoverli con l'azione di eliminazione.

14. Policy di aggiornamento del sistema

Configurazione per la gestione degli aggiornamenti del sistema.

Predefinito: Segui il comportamento predefinito per gli aggiornamenti del dispositivo, che in genere richiede all'utente di accettare gli aggiornamenti del sistema.

Installazione automatica: Installa automaticamente non appena è disponibile un aggiornamento.

Installazione in finestra temporale: Installa automaticamente all'interno di una finestra di manutenzione giornaliera. Questo configura anche le app di Play per essere aggiornate all'interno della finestra temporale. Si consiglia vivamente per i dispositivi kiosk, poiché è l'unico modo in cui le app fissate in primo piano possono essere aggiornate tramite Play.

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

14.1. Finestra di manutenzione (Solo finestra)

Quando "**Policy di aggiornamento del sistema**" è impostata su "**Modalità grafica**", puoi definire la finestra di manutenzione giornaliera utilizzando i campi "**da**" e "**a**".

14.2. Periodi di blocco aggiornamento sistema

Un periodo annuale in cui gli aggiornamenti del sistema via etere (OTA) vengono sospesi per bloccare la versione del sistema operativo in esecuzione su un dispositivo. Per evitare che il dispositivo rimanga bloccato indefinitamente, ogni periodo di blocco deve essere separato da almeno 60 giorni. Ogni periodo di blocco non deve superare i 90 giorni.

Utilizzare **Definisci periodo di blocco aggiornamenti di sistema** per creare voci.

15. Fornitori di credenziali predefiniti

Controlla quali app possono funzionare come fornitori di credenziali su Android 14 e versioni successive.

> **Non consentite (impostazione predefinita)**: Le app a cui non è stata specificata la policy "credentialProviderPolicy" non possono funzionare come fornitori di credenziali.
>
> **Non consentito, ad eccezione del sistema**: Le app a cui non è stata specificata la policy "credentialProviderPolicy" non possono funzionare come fornitori di credenziali, ad eccezione dei fornitori di credenziali predefiniti del produttore.

Posizione e geofence

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

Segnalazione della posizione

Segnala posizione

Abilita la segnalazione della geolocalizzazione del dispositivo. I dati di localizzazione raccolti tramite questa impostazione sono utilizzati dalla **mappa posizione del dashboard**, la cronologia delle posizioni nella panoramica del dispositivo e l'elaborazione dei geofence.

> Su dispositivi non completamente gestiti, i dati di posizione possono comunque dipendere dalle autorizzazioni di posizione richieste per l'app Cerberus Enterprise e dall'abilitazione dei servizi di localizzazione sul dispositivo.

Modalità di localizzazione

Gestisce l'impostazione della posizione sui dispositivi aziendali

- **Scelta dell'utente**: i servizi di localizzazione non sono limitati dalla policy.
- **Impostati**: i servizi di localizzazione sono abilitati sul dispositivo.
- **Disabilitato**: i servizi di localizzazione sono disabilitati sul dispositivo.

Condivisione della posizione disabilitata

Disattiva la condivisione della posizione per le app aziendali. Sui dispositivi di proprietà del profilo, ciò influisce sul profilo di lavoro. Sui dispositivi completamente gestiti, disabilita la posizione per l'intero dispositivo e sovrascrive la modalità di localizzazione del dispositivo.

Comportamento automatico con geofences attive

Le geofences attive richiedono la segnalazione della posizione per funzionare. Quando almeno una geofence è attiva, Cerberus Enterprise mantiene automaticamente costanti le impostazioni di localizzazione correlate.

- **La segnalazione della posizione** è forzata durante l'attivazione delle geofences.
- **Modalità posizione** è forzata a **Forzata**.
- **Condivisione della posizione disabilitata** è forzata.

Se tenti di disabilitare **Report location** mentre una o più recinzioni geolocate sono attive, Cerberus Enterprise mostra una finestra di dialogo di conferma. Se continui, tutte le recinzioni geolocate attive nella policy vengono disattivate.

Elenco geofence

Una policy può contenere fino a **10 geofences**. I nomi delle geofences 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 **100** a **10000** metri.
- **Descrizione**: note facoltative per gli amministratori.
- **Report ingresso** e **Report uscita**: seleziona quali eventi di transizione devono essere generati.
- **Attivo**: abilita o disabilita la recinzione geografica senza eliminarla.

> Almeno uno tra **Report entra** e **Report esci** deve rimanere abilitato per ogni recinzione geografica.

Strumenti di modifica mappa

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

- Clicca sulla mappa per spostare il centro della geofence quando la modifica dell'area è sbloccata.
- Usa il pulsante **Posizione attuale** per centrare la mappa sulla tua posizione del browser.
- Usa il pulsante **Ricentra mappa** per ripristinare la vista preferita per quella geofence.
- Usa il pulsante di blocco per evitare modifiche accidentali alla geometria della geofence.

Dove compaiono i dati della geofence

Le transizioni delle geofence possono essere visualizzate nella pagina Android **Panoramica dispositivo**, all’interno della scheda **Geofence** del pannello delle posizioni. Tale scheda mostra le transizioni su una mappa dedicata, insieme a strumenti di filtro e alla lista delle transizioni.

Gestione degli utenti

Aggiungi utente disabilitato

Specifica se la possibilità di aggiungere nuovi utenti e profili è disabilitata. Per i dispositivi in cui managementMode è **DEVICE_OWNER**, questo campo viene ignorato e l'utente non può aggiungere o rimuovere utenti.

Modifica degli account disabilitati

Possibilità di abilitare o disabilitare l'aggiunta o la rimozione di account.

Configurazione delle 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 utente come disabilitata

Se la possibilità di cambiare l'icona utente è disabilitata.

Imposta sfondo disabilitato

Impossibile modificare lo sfondo.

Configurazione dell'autenticazione per l'account di lavoro

Controlla come gli utenti eseguono l'autenticazione durante la configurazione dell'account di lavoro. Questa opzione è disponibile solo per le aziende Android con un dominio Google gestito (Google Workspace).

Durante la configurazione/registrazione del dispositivo, questa policy determina se è necessario effettuare l'accesso con un account aziendale, ma l'impostazione **Autenticazione tramite Google** nella console di amministrazione di Google e il tipo di token di registrazione possono comunque richiedere l'autenticazione.

Per i dispositivi già registrati, questa policy si applica solo se il dispositivo è gestito tramite un account Google Play aziendale (ovvero, registrato senza **autenticazione tramite Google**).

Per maggiori dettagli e per la risoluzione dei problemi, consultare **Autenticazione tramite Google**.

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.

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

Ogni elemento ha un campo "**Tipo di account**" (obbligatorio). Inserire una stringa come, ad esempio, **com.google**. Eliminare un elemento utilizzando l'azione "cancella".

Utilizzo personale

Quando configuri un dispositivo aziendale per uso lavorativo e personale, è possibile specificare alcune regole per limitare il modo in cui l'utente può utilizzare il dispositivo per uso personale, al di fuori del profilo aziendale.

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

1. Fotocamera disattivata

Se la fotocamera è disattivata.

2. Acquisizione schermo disabilitata

Se l'acquisizione schermo è disabilitata.

3. Giorni massimi di permesso

Controlla per quanto tempo il profilo lavoro può rimanere disattivato.

4. Condivisione via Bluetooth

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

5. Spazio privato

Controlla se è consentito l'utilizzo di spazi privati sul dispositivo.

6. Modalità Play Store

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

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

Elenco consentito: Solo le applicazioni specificate esplicitamente nella sezione **Applicazioni** e con **Tipo di installazione** impostato su **Disponibile** possono essere installate nel profilo personale.

7. Applicazioni

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

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

7.1. Tipo di installazione

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

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

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

8. 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 al proprio profilo personale.

Policy applicabili a più profili

Si applica solo ai dispositivi con profili personali e aziendali.

Copia e incolla tra profili diversi

Che il testo copiato da un profilo (personale o aziendale) possa essere incollato nell'altro profilo.

> **Non consentito (predefinito)**: Impedisce agli utenti di incollare nel profilo personale testo copiato dal profilo aziendale. Il testo copiato dal profilo personale può essere incollato nel profilo aziendale.
>
> **Consentito**: Il testo copiato in uno dei due profili può essere incollato nell'altro profilo.

Condivisione dei dati tra profili

Definisce se i dati di un profilo (personale o aziendale) possono essere condivisi con le app nell'altro profilo. Controlla specificamente la condivisione di dati tramite intent. La gestione di altri canali di comunicazione tra profili, come la ricerca di contatti, copia/incolla,
o app aziendali e personali connesse, viene configurata separatamente.

> **Non consentito**: Impedisce la condivisione di dati sia dal profilo personale al profilo aziendale, sia dal profilo aziendale al profilo personale.
>
> **Non consentito (impostazione predefinita)**: Impedisce agli utenti di condividere dati dal profilo aziendale con le applicazioni nel profilo personale. I dati personali possono essere condivisi con le applicazioni aziendali.
>
> **Consentito**: Consente agli utenti di condividere i dati da un profilo con l'altro.

Widget predefiniti per il profilo di lavoro

Comportamento predefinito per i widget del profilo di lavoro. Se un'app specifica non definisce una policy per i widget, viene applicata quella impostata qui.

Funzionalità delle app che operano tra profili diversi

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

>

> Questa impostazione dipende dall'opzione a livello di policy**Funzionalità delle app** (nella sezione Gestione app). Se Funzionalità delle app è impostata su **Non consentite**, l'API rifiuterà le funzionalità tra profili impostate su **Consentite**.

Contatti di lavoro nel profilo personale

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

Consentito (predefinito): Consente la visualizzazione dei contatti del profilo di lavoro nel profilo personale.

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

Non consentito, eccetto per il sistema: Impedisce alla maggior parte delle app personali di accedere ai contatti del profilo di lavoro, ad eccezione delle app predefinite Dialer, Messaggi e Contatti del produttore (OEM) (Android 14 e versioni successive).

Quando i contatti di lavoro nel profilo personale sono configurati, è possibile definire opzionalmente un elenco di voci di **nome del pacchetto escluso**. A seconda della modalità selezionata, queste esclusioni funzionano come una whitelist o una blacklist per le app personali.

Reportistica sullo stato

In questa sezione, è possibile configurare quali dati devono essere recuperati dal dispositivo. I dati relativi allo stato possono essere visualizzati nella pagina del **stato del dispositivo**.

Report applicazioni

Se i report delle applicazioni sono abilitati. (Informazioni riportate su un'applicazione installata.)

> Questa opzione è obbligatoria per il sistema (per l'integrazione con l'app companion) ed è sempre abilitata; non può essere disabilitata.

Includi le app rimosse

Se le app rimosse sono incluse nei report delle applicazioni.

Impostazioni del dispositivo

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

Informazioni sul software

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

Informazioni sulla memoria

Se la segnalazione dell'utilizzo della memoria è abilitata. (Un evento relativo alla misurazione della memoria e dello spazio di archiviazione.)

Informazioni sulla rete

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

Mostra informazioni

Abilita o meno la visualizzazione dei report. I dati dei report non sono disponibili per i dispositivi di proprietà privata con profili di lavoro. (Informazioni di visualizzazione del dispositivo.)

Eventi di gestione dell'alimentazione

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

Stato dell'hardware

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

Proprietà del sistema

Se la segnalazione delle proprietà del sistema è abilitata.

Modalità Common Criteria

Se la modalità Common Criteria è attiva.

Varie

1. Gioco a sorpresa disabilitato

Se il gioco a sorpresa nelle Impostazioni è disabilitato.

2. Salta i suggerimenti per il primo utilizzo

Flag per saltare i suggerimenti al primo utilizzo. L'amministratore Enterprise può abilitare la raccomandazione del sistema per le app, in modo che queste non mostrino il tutorial per l'utente e altri suggerimenti introduttivi al primo avvio.

3. Breve messaggio di supporto

Un messaggio visualizzato all'utente nella schermata delle impostazioni quando una funzionalità è stata disattivata dall'amministratore. Se il messaggio è più lungo di 200 caratteri, potrebbe essere troncato.

4. Messaggio di supporto dettagliato

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

5. Informazioni sullo schermo di blocco del proprietario

Le informazioni sul proprietario del dispositivo da visualizzare sullo schermo di blocco.

6. Azioni di configurazione

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

Utilizza **Aggiungi azione di configurazione** per creare elementi e rimuoverli con l'azione di eliminazione.

6.1. Avvia l'app

Nome del pacchetto dell'app da avviare

6.2. Titolo

Fornisce un messaggio all'utente, per spiegare perché l'app deve essere avviata.

6.3. Descrizione

Fornisce un messaggio all'utente, per spiegare perché l'app deve essere avviata.

7. Visibilità del nome visualizzato per dispositivi aziendali

Controlla se il nome visualizzato dell'azienda è visibile sul dispositivo (ad esempio, come messaggio sullo schermo di blocco dei dispositivi aziendali).

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

Nascosto: Il nome dell'azienda non è visibile sul dispositivo.

Regole di applicazione delle policy

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

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

Se il dispositivo o il profilo di lavoro non risultano conformi dopo 10 giorni, la policy Android reimposterà il dispositivo alle impostazioni di fabbrica o eliminerà il profilo di lavoro.

In questa sezione, è possibile sovrascrivere le regole di applicazione della conformità predefinite oppure aggiungerne di nuove.

Regole

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

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

Nome impostazione

La policy di livello superiore da applicare. Ad esempio, **Applicazioni** o **Requisiti password**.

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

Blocca dopo X giorni

Numero di giorni in cui la policy non è conforme prima che il dispositivo o il profilo di lavoro vengano bloccati. Per bloccare l'accesso immediatamente, impostare su 0. **Blocca dopo X giorni** deve essere inferiore a **Cancellazione dopo X giorni**. Applicabile solo ai dispositivi di proprietà dell'azienda.

Intervallo consentito: da 0 a 300.

Ambito di blocco

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

Impostazione predefinita (nuova regola): **Profilo lavoro**.

> **Profilo lavoro**: L'azione di blocco viene applicata solo alle app presenti nel profilo lavoro. Le app nel profilo personale non sono interessate.
>
> **Dispositivo intero**: L'azione di blocco viene applicata all'intero dispositivo, comprese le app presenti nel profilo personale.

Cancellazione dopo giorni

Numero di giorni in cui la policy non è conforme prima che il dispositivo o il profilo di lavoro vengano resettati.
Cancellazione dopo giorni deve essere maggiore di **Blocco dopo giorni**. Applicabile solo ai dispositivi di proprietà dell'azienda.

Obbligatorio. Valore predefinito (nuova regola): **1**.

Intervallo consentito: da 1 a 300.

Mantieni la protezione di ripristino ai dati di fabbrica

Se i dati di protezione del ripristino alle impostazioni di fabbrica sono mantenuti sul dispositivo. Questa impostazione non si applica ai profili di lavoro.

Predefinito (nuova regola): abilitato.