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.

Revision #44
Created 2023-03-05 15:57:36 UTC by Admin
Updated 2026-06-11 16:17:37 UTC by Admin