Gestione app

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

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

1. Modalità Play Store

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

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

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

2. Policy per le app non attendibili

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

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

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

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

3. Google Play Protect

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

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

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

4. Policy di default dei permessi

La policy per fornire i permessi a runtime alle app.

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

Concedi: concedi automaticamente un permesso.

Nega: nega automaticamente un permesso.

5. Disabilita installazione app

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

6. Disabilita disinstallazione app

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

7. Policy dei permessi

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

8. Applicazioni

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

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

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

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

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

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

8.1. Tipo di installazione

Il tipo di installazione da eseguire per un'app.

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

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

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

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

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

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

8.2. Modalità di aggiornamento automatico

Controlla la modalità di aggiornamento automatico per l'app.

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

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

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

8.3. Version code minimo

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

8.4. Ambiti delegati

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

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

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

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

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

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

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

8.5. Policy di default dei permessi

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

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

Concedi: concedi automaticamente un permesso.

Nega: nega automaticamente un permesso.

8.6. App di lavoro e personale connesse

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

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

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

8.7. Disabilitata

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

8.8. Configurazione gestita

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

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

8.9. Policy dei permessi

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

8.10. Track IDs

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

>

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

9. Selezione della chiave privata

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

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

10. Scegli le regole della chiave privata

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

10.1. Alias di chiave privata

L'alias della chiave privata da utilizzare.

10.2. Pattern URL

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

10.3. Nomi dei pacchetti

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

Qualsiasi app con lo stesso UID Android di un pacchetto specificato qui avrà accesso quando invoca KeyChain.choosePrivateKeyAlias.

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

Revision #5
Created 5 March 2023 15:57:36 by Admin
Updated 30 March 2023 11:01:01 by Admin