Regole di conformità

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

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

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

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

Regole

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

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

Nome impostazione

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

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

Blocca dopo giorni

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

Intervallo consentito: 0–300.

Ambito del blocco

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

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

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

Cancella dati dopo giorni

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

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

Intervallo consentito: 1–300.

Mantieni la protezione dopo il ripristino di fabbrica

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

Predefinito (nuova regola): attivato.

Revision #7
Created 2026-11-10 15:12:57 UTC by Admin
Updated 2026-11-12 09:52:44 UTC by Admin