# Sistema

In questa sezione puoi configurare le policy relative al sistema.

## 1. Livello API minimo

Il livello API Android minimo consentito.

## 2. Policy di crittografia

Indica se la crittografia è attivata.

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

## 3. Data e ora automatiche

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

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

## 4. Impostazioni sviluppatore

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

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

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

## 5. Modalità Common Criteria

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

**Disattivato (predefinito)**: disattiva la modalità Common Criteria.

**Attivato**: attiva la modalità Common Criteria.

## 6. Memory Tagging Extension (MTE)

Controlla Memory Tagging Extension (MTE) sul dispositivo.

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

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

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

## 7. Protezione dei contenuti

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

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

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

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

## 8. Contenuti Assist

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

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

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

## 9. Creazione finestre disattivata

Indica se la creazione di finestre diverse da quelle delle app è disattivata. Questa opzione impedisce la visualizzazione delle seguenti interfacce di sistema: toast e snackbar, attività telefoniche (come le chiamate in arrivo) e attività telefoniche prioritarie (come le chiamate in corso), avvisi di sistema, errori di sistema e overlay di sistema.

## 10. Connessione di rete di emergenza

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

## 11. Attività predefinite

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

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

### 11.1. Attività ricevente

L'attività che deve essere il gestore predefinito degli intent. Deve essere il nome di un componente Android, ad es. com.android.enterprise.app/.MainActivity. In alternativa, il valore può essere il nome del pacchetto di un'app, il che fa sì che Android Device Policy scelga un'attività appropriata dall'app per gestire l'intent.

### 11.2. Azione

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

### 11.3. Categoria

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

## 12. Metodi di input consentiti

Specifica i metodi di input consentiti.

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

### 12.1. Metodi di input consentiti

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

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

## 13. Servizi di accessibilità consentiti

Specifica i servizi di accessibilità consentiti.

**Tutti consentiti**: è possibile usare qualsiasi servizio di accessibilità.

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

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

## 13.1. Servizi di accessibilità consentiti

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

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

# 14. Policy di aggiornamento del sistema

Configurazione per la gestione degli aggiornamenti del sistema.

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

**Automatico**: installa automaticamente non appena un aggiornamento è disponibile.

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

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

## 14.1. Finestra di manutenzione (solo A intervalli)

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

## 14.2. Periodi di blocco degli aggiornamenti del sistema

Un periodo di tempo che si ripete ogni anno in cui gli aggiornamenti di sistema over-the-air (OTA) vengono posticipati per bloccare la versione del sistema operativo in esecuzione su un dispositivo. Per evitare di bloccare il dispositivo a tempo indefinito, ogni periodo di blocco deve essere separato da almeno 60 giorni. Ogni periodo di blocco non deve superare i 90 giorni.

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

## 15. Provider di credenziali predefiniti

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

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

---

Revision #65
Created 2023-03-05 15:57:36 UTC by Admin
Updated 2026-11-12 09:52:42 UTC by Admin