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.

Revision #42
Created 2023-03-05 15:57:36 UTC by Admin
Updated 2026-04-22 15:47:12 UTC by Admin