Sistema

1. Livello API minimo

Il livello API Android minimo consentito.

2. Policy di crittografia

Se la crittografia è abilitata.

Predefinito: questo valore viene ignorato, ovvero non è richiesta alcuna crittografia.

Abilitato senza password: crittografia richiesta ma nessuna password richiesta per l'avvio.

Abilitato con password: crittografia richiesta con password richiesta per l'avvio.

3. Data e ora automatiche

Se la data, l'ora e il fuso orario automatici sono abilitati su un dispositivo di proprietà dell'azienda.

Predefinito: non specificato. L'impostazione predefinita è **Scelta dell'utente**.

Scelta dell'utente: la data, l'ora e il fuso orario automatici sono lasciati alla scelta dell'utente.

Applicato: applica la data, l'ora e il fuso orario automatici sul dispositivo.

4. Modalità posizione

Il grado di rilevamento della posizione abilitato. L'utente può modificare il valore a meno che l'utente non sia altrimenti bloccato dall'accesso alle impostazioni del dispositivo. Si applica solo ai dispositivi di proprietà dell'azienda.

Predefinito: l'impostazione predefinita è **Scelta dell'utente**.

Scelta dell'utente: l'impostazione della posizione non è limitata sul dispositivo. Nessun comportamento specifico è impostato o imposto.

Applicato: abilita l'impostazione della posizione sul dispositivo.

Disabilitato: disabilita l'impostazione della posizione sul dispositivo.

5. Impostazioni sviluppatore

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

Predefinito: non specificato. L'impostazione predefinita è **Disabilitato**.

Disabilitato: disabilita tutte le impostazioni sviluppatore e impedisce all'utente di accedervi.

Consentito: consente tutte le impostazioni dello sviluppatore. L'utente può accedere e, facoltativamente, configurare le impostazioni.

6. Common Criteria Mode

Controlla il Common Criteria Mode: standard di sicurezza definiti nei Common Criteria for Information Technology Security Evaluation (CC). L'abilitazione del Common Criteria Mode aumenta alcuni componenti di sicurezza su un dispositivo, inclusa la crittografia AES-GCM delle chiavi Bluetooth a lungo termine e gli archivi delle configurazioni Wi-Fi. Avviso: la modalità Common Criteria applica un modello di sicurezza rigoroso, in genere richiesto solo per i prodotti IT utilizzati nei sistemi di sicurezza nazionale e in altre organizzazioni altamente sensibili. L'utilizzo standard del dispositivo potrebbe risentirne. Abilitare solo se necessario.

Predefinito: non specificato. L'impostazione predefinita è **Disabilitato**.

Disabilitato: impostazione predefinita. Disabilita il Common Criteria Mode.

Abilitato: abilita il Common Criteria Mode.

7. Condividi la posizione disabilitato

Se la condivisione della posizione è disabilitata per le app di lavoro. Sui dispositivi di proprietà personale, disabilita la posizione per il profilo di lavoro. Sui dispositivi completamente gestiti, disattiva la posizione sull'intero dispositivo (ignorando anche l'impostazione "Modalità posizione").

8. Crea finestre disabilitato

Se la creazione di finestre oltre alle finestre delle app è disabilitata. Questa opzione impedisce la visualizzazione delle seguenti interfacce utente 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.

9. Network escape hatch

Se il network escape hatch è abilitato. Se non è possibile stabilire una connessione di rete al momento dell'avvio, l'escape hatch richiede all'utente di connettersi temporaneamente a una rete per aggiornare le policy del dispositivo. Dopo aver applicato la policy, la rete temporanea verrà dimenticata e il dispositivo continuerà ad avviarsi. Ciò previene l'impossibilità di connettersi a una rete se non è presente una rete adatta nell'ultima policy e il dispositivo si avvia con un'app in modalità lock task, o per qualsiasi altro motivo l'utente non può accedere alle impostazioni del dispositivo.

10. Attività predefinite

Un elenco di attività predefinite per la gestione degli Intent che corrispondono a un particolare IntentFilter. Ad esempio, questa funzione consentirebbe agli amministratori IT di scegliere quale app del browser apre automaticamente i collegamenti Web o quale launcher viene utilizzato quando si tocca il pulsante Home.

10.1. Attività del ricevitore

L'attività che dovrebbe essere il gestore dell'Intent predefinito. Dovrebbe 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, che fa sì che Android Device Policy scelga un'attività appropriata dall'app per gestire l'Intent.

10.2. Azione

Le azioni dell'Intent da matchare nel filtro. Se nel filtro sono incluse azioni, l'azione di un Intent deve essere uno di quei valori affinché corrisponda. Se non sono incluse azioni, l'azione dell'Intent viene ignorata.

10.3. Categoria

Le categorie di Intent da matchare nel filtro. Un Intent include le categorie che richiede, che devono essere tutte incluse nel filtro per avere un match. In altre parole, l'aggiunta di una categoria al filtro non ha alcun impatto sul match a meno che tale categoria non sia specificata

nell'Intent.

11. Metodi di input permessi

Specifica i metodi di input permessi.

> **Tutto consentito**: nessuna restrizione applicata. Tutti i metodi di input sono permessi.
>
> **Solo di sistema**: sono consentiti solo i metodi di input integrati del sistema.
>
> **Solo di sistema e forniti**: sono consentiti solo i metodi di input integrati del sistema e quelli indicati.

11.1. Metodi di input consentiti

Package name dei metodi di input che sono consentiti. Si applica solo quando **Metodi di input permessi** è impostato a **Solo di sistema e forniti**.

12. Servizi di accessibilità permessi

Specifica i servizi di accessibilità permessi.

> **Tutto consentito**: qualsiasi servizio di accessibilità può essere usato.
>
> **Solo di sistema**: sono consentiti solo i servizi di accessibilità integrati del sistema.
>
> **Solo di sistema e forniti**: sono consentiti solo i servizi di accessibilità integrati del sistema e quelli indicati.

12.1. Servizi di accessibilità consentiti

Servizi di accessibilità che possono essere usati. Si applica solo quando **Servizi di accessibilità permessi** è impostato a **Solo di sistema e forniti**.

13. Policy di aggiornamento sistema

Configurazione per la gestione degli aggiornamenti di sistema.

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

Automatico: installa automaticamente non appena è disponibile un aggiornamento.

Finestra: installazione automatica all'interno di una finestra di manutenzione giornaliera. Ciò configura anche le app Play da aggiornare all'interno della finestra. Questa opzione è fortemente consigliata per i dispositivi kiosk perché questo è l'unico modo in cui le app permanentemente bloccate in primo piano possono essere aggiornate da Play.

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

14. Periodi di blocco dell'aggiornamento 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 il congelamento del dispositivo a tempo indeterminato, ogni periodo di blocco deve essere separato da almeno 60 giorni.

Revision #5
Created 5 March 2023 15:57:36 by Admin
Updated 19 April 2023 07:54:45 by Admin