Sicurezza

In questa sezione puoi configurare le policy relative alla sicurezza.

Azioni per i rischi di sicurezza

Scegli cosa fare quando un dispositivo segnala un SecurityRisk nei rapporti di stato.

Tipi di SecurityRisk supportati:

Sistema operativo sconosciuto: Play Integrity API rileva che il dispositivo esegue un sistema operativo sconosciuto (il controllo basicIntegrity riesce ma ctsProfileMatch fallisce).

Sistema operativo compromesso: Play Integrity API rileva che il dispositivo esegue un sistema operativo compromesso (il controllo basicIntegrity fallisce).

Valutazione hardware non riuscita: Play Integrity API rileva che il dispositivo non offre una garanzia forte dell'integrità del sistema, se l'etichetta MEETS_STRONG_INTEGRITY non compare nel campo relativo all'integrità del dispositivo.

Azioni disponibili:

Cancella i dati aziendali (predefinito): annulla la registrazione e cancella i dati di lavoro (l'intero dispositivo se completamente gestito, o solo il profilo di lavoro per i dispositivi con profilo).

Nessuna azione: lascia il dispositivo registrato e non fare nulla automaticamente.

Quando selezioni **Cancella i dati aziendali**, puoi anche configurare le opzioni di cancellazione:

Mantieni la protezione dopo il ripristino di fabbrica: conserva i dati della protezione dopo il ripristino di fabbrica (FRP) durante la cancellazione del dispositivo.

Cancella archiviazione esterna: cancella inoltre l'archiviazione esterna del dispositivo (come le schede SD) durante l'esecuzione della cancellazione.

Cancella eSIM: per i dispositivi aziendali, rimuove tutte le eSIM dal dispositivo quando il dispositivo viene cancellato. Nei dispositivi di proprietà personale, rimuove le eSIM gestite (eSIM aggiunte tramite il comando ADD_ESIM) sul dispositivo e nessuna eSIM di proprietà personale verrà rimossa.

1. Tempo massimo prima del blocco

Tempo massimo (in secondi) di attività dell'utente prima del blocco del dispositivo. Un valore di 0 indica che non esiste alcuna restrizione.

2. Rimani attivo durante la ricarica

Le modalità di alimentazione con batteria collegata in cui il dispositivo rimane attivo. Quando usi questa impostazione, si consiglia di svuotare **Tempo massimo prima del blocco** in modo che il dispositivo non si blocchi mentre rimane attivo.

Alimentatore CA: la fonte di alimentazione è un alimentatore CA.

Porta USB: la fonte di alimentazione è una porta USB.

Caricatore wireless: la fonte di alimentazione è wireless.

3. Blocco schermo disattivato

Se impostato su true, disattiva la schermata di blocco per i display principale e/o secondario. Questa policy è supportata solo in modalità di gestione dispositivo dedicata.

4. Requisiti della password

Policy sui requisiti della password.

Usa **Configura i requisiti della password** per aggiungere uno o più blocchi di requisiti della password. Usa **Cancella tutto** per rimuovere tutti i requisiti della password configurati.

I requisiti della password possono usare l'ambito **Auto** (requisito singolo) o ambiti separati **Dispositivo**/**Profilo di lavoro**. I requisiti basati sulla complessità devono essere abbinati a requisiti basati sulla qualità per lo stesso ambito.

4.1. Ambito

L'ambito a cui si applica il requisito della password.

Auto: l'ambito non è specificato. I requisiti della password vengono applicati al profilo di lavoro per i dispositivi con profilo di lavoro e all'intero dispositivo per i dispositivi completamente gestiti o dedicati.

Dispositivo: i requisiti della password vengono applicati solo al dispositivo.

Profilo di lavoro: i requisiti della password vengono applicati solo al profilo di lavoro.

4.2. Lunghezza cronologia password

La lunghezza della cronologia delle password. Dopo aver impostato questo campo, l'utente non potrà inserire una nuova password uguale a una qualsiasi password della cronologia. Un valore di 0 indica che non esiste alcuna restrizione.

4.3. Max password non riuscite prima della cancellazione

Numero di password di sblocco del dispositivo errate che possono essere inserite prima che il dispositivo venga cancellato. Un valore di 0 indica che non esiste alcuna restrizione.

4.4. Scadenza password (giorni)

Questa impostazione obbliga l'utente ad aggiornare periodicamente la password dopo il numero di giorni specificato.

4.5. Richiedi sblocco con password

Il tempo dopo lo sblocco di un dispositivo o profilo di lavoro con una forma di autenticazione forte (password, PIN, sequenza) durante il quale è possibile sbloccarlo con qualsiasi altro metodo di autenticazione (ad es. impronta digitale, agenti attendibili, volto). Trascorso il periodo di tempo specificato, per sbloccare il dispositivo o il profilo di lavoro è possibile usare solo forme di autenticazione forti.

Predefinito del dispositivo: il periodo di timeout è impostato sul valore predefinito del dispositivo.

Ogni giorno: il periodo di timeout è impostato a 24 ore.

4.6. Qualità della password

La qualità della password richiesta.

Complessità elevata: definisce la fascia di complessità elevata della password come segue: su Android 12 e versioni successive: PIN senza sequenze ripetute (4444) o ordinate (1234, 4321, 2468), lunghezza minima 8; alfabetica, lunghezza minima 6; alfanumerica, lunghezza minima 6.

Complessità media: definisce la fascia di complessità media della password come segue: PIN senza sequenze ripetute (4444) o ordinate (1234, 4321, 2468), lunghezza minima 4; alfabetica, lunghezza minima 4; alfanumerica, lunghezza minima 4.

Complessità bassa: definisce la fascia di complessità bassa della password come segue: sequenza; PIN con sequenze ripetute (4444) o ordinate (1234, 4321, 2468).

Nessuna: non sono previsti requisiti della password.

Debole: il dispositivo deve essere protetto almeno con una tecnologia di riconoscimento biometrico a bassa sicurezza. Ciò include tecnologie in grado di riconoscere l'identità di un individuo approssimativamente equivalenti a un PIN di 3 cifre (rilevamento errato inferiore a 1 su 1.000).

Qualsiasi: è richiesta una password, ma non ci sono restrizioni su ciò che deve contenere.

Numerica: la password deve contenere caratteri numerici.

Numerica complessa: la password deve contenere caratteri numerici senza sequenze ripetute (4444) o ordinate (1234, 4321, 2468).

Alfabetica: la password deve contenere caratteri alfabetici (o simboli).

Alfanumerica: la password deve contenere sia caratteri numerici sia caratteri alfabetici (o simboli).

Complessa: la password deve soddisfare i requisiti minimi specificati in passwordMinimumLength, passwordMinimumLetters, passwordMinimumSymbols ecc. Ad esempio, se passwordMinimumSymbols è 2, la password deve contenere almeno due simboli.

4.7. Lunghezza minima

La lunghezza minima consentita della password. Un valore di 0 indica che non esiste alcuna restrizione.

4.8. Lettere minime

Numero minimo di lettere richieste nella password.

4.9. Lettere minuscole minime

Numero minimo di lettere minuscole richieste nella password.

4.10. Lettere maiuscole minime

Numero minimo di lettere maiuscole richieste nella password.

4.11. Caratteri non alfabetici minimi

Numero minimo di caratteri non alfabetici (cifre numeriche o simboli) richiesti nella password.

4.12. Cifre numeriche minime

Numero minimo di cifre numeriche richieste nella password.

4.13. Simboli minimi

Numero minimo di simboli richiesti nella password.

4.14. Blocco unificato

Controlla se è consentito un blocco unificato per il dispositivo e il profilo di lavoro, sui dispositivi con Android 9 e versioni successive e con un profilo di lavoro. Non ha alcun effetto sugli altri dispositivi.

> **Consenti blocco unificato**: è consentito un blocco comune per il dispositivo e il profilo di lavoro.
>
> **Richiedi blocco di lavoro separato**: è richiesto un blocco separato per il profilo di lavoro.

5. Ripristino di fabbrica disattivato

Indica se il ripristino di fabbrica dalle impostazioni è disattivato. Si applica solo ai dispositivi completamente gestiti.

6. Protezione dal ripristino di fabbrica

Indirizzi email degli amministratori del dispositivo per la protezione dal ripristino di fabbrica. Quando il dispositivo subisce un ripristino di fabbrica non autorizzato, richiederà a uno di questi amministratori di accedere con l'email e la password dell'account Google per sbloccare il dispositivo. Se non viene specificato alcun amministratore, il dispositivo non fornirà la protezione dal ripristino di fabbrica. Si applica solo ai dispositivi completamente gestiti.

Email degli amministratori: usa **Abilita la protezione dal ripristino di fabbrica** per iniziare a configurare gli amministratori. Poi usa **Aggiungi email amministratore** per aggiungere indirizzi e rimuoverli con l'azione di eliminazione.

7. Funzionalità del blocco schermo

Funzionalità del blocco schermo (schermata di blocco) che possono essere disattivate.

7.1. Disattiva tutto

Disattiva tutte le personalizzazioni attuali e future del blocco schermo.

7.2. Disattiva fotocamera

Disattiva la fotocamera sulle schermate di blocco protette (ad es. PIN).

7.3. Disattiva notifiche

Disattiva la visualizzazione di tutte le notifiche sulle schermate di blocco protette.

7.4. Disattiva notifiche non oscurate

Disattiva le notifiche non oscurate sulle schermate di blocco protette.

7.5. Ignora stato dell'agente attendibile

Ignora lo stato dell'agente attendibile sulle schermate di blocco protette.

7.6. Disattiva impronta digitale

Disattiva il sensore di impronte digitali sulle schermate di blocco protette.

7.7. Disattiva l'inserimento di testo nelle notifiche

Disattiva l'inserimento di testo nelle notifiche sulle schermate di blocco protette.

7.8. Disattiva autenticazione con volto

Disattiva l'autenticazione con il volto sulle schermate di blocco protette.

7.9. Disattiva autenticazione con iride

Disattiva l'autenticazione con l'iride sulle schermate di blocco protette.

7.10. Disattiva tutta l'autenticazione biometrica

Disattiva tutta l'autenticazione biometrica sulle schermate di blocco protette.

7.11. Disattiva tutte le scorciatoie

Disattiva tutte le scorciatoie sulla schermata di blocco protetta su Android 14 e versioni successive.

Revision #64
Created 2023-03-05 15:57:36 UTC by Admin
Updated 2026-11-12 09:52:44 UTC by Admin