Sicurezza

In questa sezione, puoi configurare le policy relative alla sicurezza.

Azioni per la gestione dei rischi di sicurezza

Scegli cosa fare quando un dispositivo segnala un rischio di sicurezza nei report di stato.

Tipi di rischio di sicurezza supportati:

- **Sistema operativo sconosciuto**: L'API Play Integrity rileva che il dispositivo sta eseguendo un sistema operativo sconosciuto (il controllo basicIntegrity ha esito positivo, ma ctsProfileMatch fallisce).
- **Sistema operativo compromesso**: L'API Play Integrity rileva che il dispositivo sta utilizzando un sistema operativo compromesso (il controllo basicIntegrity non è stato superato).
- **Valutazione basata sull'hardware non riuscita**: L'API Play Integrity rileva che il dispositivo non dispone di una garanzia di integrità del sistema, se l'etichetta MEETS_STRONG_INTEGRITY non è visibile nel campo dell'integrità del dispositivo.

Azioni disponibili:

- **Cancellazione dati aziendali (impostazione predefinita)**: Deregistra e cancella i dati di lavoro (intero dispositivo se completamente gestito, oppure solo il profilo di lavoro se gestito solo per il profilo).
- **Nessuna azione**: Mantieni il dispositivo registrato e non eseguire alcuna operazione automaticamente.

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

- **Mantieni la protezione di ripristino ai dati di fabbrica**: Conserva i dati di Factory Reset Protection (FRP) durante la cancellazione del dispositivo.

Cancella la memoria esterna: Cancella anche la memoria esterna del dispositivo (come le schede SD) durante l'operazione di cancellazione.

Cancella eSIM: Per i dispositivi di proprietà dell'azienda, questa operazione rimuove tutte le eSIM dal dispositivo durante la cancellazione. Nei dispositivi di proprietà personale, questa operazione rimuove le eSIM gestite (eSIM aggiunte tramite il comando ADD_ESIM) presenti nei dispositivi, senza rimuovere le eSIM di proprietà dell'utente.

1. Tempo massimo di blocco

Tempo massimo (in secondi) di attività dell'utente prima del blocco del dispositivo. Un valore di 0 indica che non ci sono restrizioni.

2. Rimani attivo durante la ricarica

Le modalità di ricarica per le quali il dispositivo rimane attivo. Quando si utilizza questa impostazione, si consiglia di deselezionare "**Tempo massimo di 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.

Ricarica wireless: La fonte di alimentazione è wireless.

3. Blocco schermo disabilitato

Se impostato su "vero", questa opzione disabilita la schermata di blocco per i display principali e/o secondari. Questa policy è supportata solo in modalità di gestione dispositivo dedicata.

4. Requisiti della password

Policy relative ai requisiti della password.

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

I requisiti per la password possono utilizzare **l'ambito "Auto"** (un solo requisito) oppure 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 si applicano 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 si applicano solo al dispositivo.

Profilo di lavoro: I requisiti della password si applicano solo al profilo di lavoro.

4.2. Lunghezza della cronologia delle password

Lunghezza della cronologia delle password. Dopo aver impostato questo valore, l'utente non potrà inserire una nuova password identica a una password presente nella cronologia. Un valore di 0 indica che non ci sono restrizioni.

4.3. Numero massimo di tentativi di password errati prima della cancellazione del dispositivo

Numero massimo di tentativi di password errati per lo sblocco del dispositivo prima della cancellazione. Il valore 0 indica che non ci sono restrizioni.

4.4. Timeout di scadenza della password (giorni)

Questa impostazione obbliga l'utente a cambiare periodicamente la password, dopo il numero di giorni specificato.

4.5. Richiedi sblocco con password

Il tempo dopo il quale un dispositivo o un profilo di lavoro sbloccati tramite un metodo di autenticazione sicuro (password, PIN, sequenza) possono essere sbloccati con qualsiasi altro metodo (ad esempio, impronta digitale, agenti di fiducia, riconoscimento facciale). Trascorso il periodo di tempo specificato, solo i metodi di autenticazione sicuri possono essere utilizzati per sbloccare il dispositivo o il profilo di lavoro.

Impostazione predefinita del dispositivo: Il periodo di timeout è impostato sull'impostazione predefinita del dispositivo.

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

4.6. Qualità della password

Il livello di sicurezza richiesto per la password.

Complessità elevata: Definire la soglia di complessità elevata per le password come segue: Su Android 12 e versioni successive: PIN senza sequenze ripetute (4444) o ordinate (1234,

4321, 2468), lunghezza minima di 8; alfanumerico, lunghezza minima di 6.

Complessità media: Definire la soglia di complessità media per le password come segue: PIN senza sequenze ripetute (4444) o ordinate (1234, 4321, 2468), lunghezza minima di 4; alfanumerico, lunghezza minima di 4.

Bassa complessità: Definire la soglia di bassa complessità per le password come segue: schema; PIN con sequenze ripetute (4444) o ordinate (1234, 4321, 2468).

Nessuna: Non sono presenti requisiti per le password.

Debole: Il dispositivo deve essere protetto con una tecnologia di riconoscimento biometrico a bassa sicurezza, almeno. Questo include tecnologie in grado di riconoscere l'identità di un individuo che siano grosso modo equivalenti a un codice PIN di 3 cifre (la probabilità di un falso riconoscimento è inferiore a 1 su 1.000).

Qualsiasi: è richiesta una password, ma non ci sono restrizioni sul suo contenuto.

Numerico: La password deve contenere caratteri numerici.

Numerico complesso: La password deve contenere caratteri numerici, senza sequenze ripetute (come 4444) o ordinate (come 1234, 4321, 2468).

Alfanumerico: La password deve contenere caratteri alfanumerici (o simboli).

Alfanumerico: La password deve contenere sia numeri che caratteri alfabetici (o simboli).

Complessità: 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 per la password. Un valore di 0 indica che non ci sono restrizioni.

4.8. Numero minimo di lettere

Numero minimo di caratteri richiesti per la password.

4.9. Numero minimo di lettere minuscole

Numero minimo di lettere minuscole richieste nella password.

4.10. Numero minimo di lettere maiuscole

Numero minimo di lettere maiuscole richieste nella password.

4.11. Numero minimo di caratteri non alfabetici richiesti

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

4.12. Numero minimo di cifre numeriche

Numero minimo di cifre numeriche richieste nella password.

4.13. Numero minimo di simboli

Numero minimo di simboli richiesti nella password.

4.14. Blocco unificato

Controlla se il blocco unificato è consentito per il dispositivo e il profilo aziendale, sui dispositivi con Android 9 e versioni successive che dispongono di un profilo aziendale. Questa impostazione non ha effetto su altri dispositivi.

> **Consenti blocco unificato**: È consentito un blocco comune per il dispositivo e il profilo aziendale.
>
> **Richiedi blocco del lavoro separato**: È richiesto un blocco separato per il profilo aziendale.

5. Ripristino ai dati di fabbrica disabilitato

Se la reimpostazione ai dati di fabbrica dalle impostazioni è disabilitata. Si applica solo ai dispositivi completamente gestiti.

6. Protezione dalla reimpostazione ai dati di fabbrica

Indirizzi email degli amministratori del dispositivo per la protezione dalla reimpostazione ai dati di fabbrica. In caso di reimpostazione ai dati di fabbrica non autorizzata, sarà necessario che uno di questi amministratori effettui l'accesso con l'indirizzo email e la password dell'account Google per sbloccare il dispositivo. Se non vengono specificati amministratori, il dispositivo non fornirà protezione dalla reimpostazione ai dati di fabbrica. Si applica solo ai dispositivi completamente gestiti.

Indirizzi email degli amministratori: utilizzare **Abilita protezione dalla reimpostazione ai dati di fabbrica** per iniziare a configurare gli amministratori. Quindi, utilizzare **Aggiungi indirizzo email dell'amministratore** per aggiungere gli indirizzi e rimuoverli con l'azione di eliminazione.

7. Funzionalità di Keyguard

Funzionalità di Keyguard (schermata di blocco) che possono essere disabilitate.

7.1. Disabilita tutto

Disabilita tutte le personalizzazioni attuali e future della schermata di blocco.

7.2. Disabilita la fotocamera

Disabilita la fotocamera nelle schermate di blocco sicure (ad esempio, con PIN).

7.3. Disabilita le notifiche

Disabilita la visualizzazione di tutte le notifiche sulle schermate di blocco sicure.

7.4. Disabilita le notifiche non oscurate

Disabilita le notifiche non oscurate nelle schermate di blocco protette.

7.5. Ignora lo stato dell'agente di fiducia

Ignora lo stato dell'agente di fiducia nelle schermate di blocco sicure.

7.6. Disabilita l'impronta digitale

Disabilita il sensore di impronte digitali nelle schermate di blocco sicure.

7.7. Disabilita l'inserimento di testo nelle notifiche

Disabilita l'inserimento di testo nelle notifiche quando si utilizza la schermata di blocco sicura.

7.8. Disabilita l'autenticazione tramite riconoscimento facciale

Disabilita l'autenticazione tramite riconoscimento facciale nelle schermate di blocco protette.

7.9. Disabilita l'autenticazione tramite iride

Disabilita l'autenticazione tramite iride nelle schermate di blocco sicure.

7.10. Disabilita tutte le autenticazioni biometriche

Disabilita tutte le autenticazioni biometriche sulle schermate di blocco sicure.

7.11. Disabilita tutte le scorciatoie

Disabilita tutte le scorciatoie nella schermata di blocco sicura su Android 14 e versioni successive.

Revision #41
Created 2023-03-05 15:57:36 UTC by Admin
Updated 2026-04-22 15:47:15 UTC by Admin