

# Sicurezza

In questa sezione è possibile configurare le policy relative alla sicurezza.

## 1. Tempo massimo per bloccare

Tempo massimo (in secondi) di inattività dell'utente fino al blocco del dispositivo. Un valore pari a 0 indica che non vi è alcuna restrizione.

## 2. Rimani acceso durante la ricarica

Le modalità di ricarica per le quali il dispositivo rimane con lo schermo acceso. Quando si utilizza questa impostazione, si consiglia di deselezionare **Tempo massimo per bloccare** in modo che il dispositivo non si blocchi da solo mentre lo schermo è acceso.

**Caricabatterie CA:** la fonte di alimentazione è un caricabatterie CA.

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

**Caricabatterie wireless:** la fonte di alimentazione è wireless.

## 3. Keyguard disabilitato

Se il keyguard (blocco schermo) è disabilitato.

## 4. Requisiti della password

Policy sui requisiti della password. È possibile impostare policy diverse per il **profilo di lavoro** o per i **dispositivi completamente gestiti** impostando il campo **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 del profilo di lavoro e all'intero dispositivo per i dispositivi completamente gestiti o dedicati.

**Dispositivo:** i requisiti della password sono applicati soltanto al dispositivo.

**Profilo di lavoro:** i requisiti della password sono applicati soltanto al profilo di lavoro.

## 4.2. Lunghezza cronologia password

La lunghezza della cronologia delle password. Dopo aver impostato questo campo, l'utente non sarà in grado di inserire una nuova password uguale a qualsiasi password nella cronologia. Un valore pari a 0 indica che non vi è alcuna restrizione.

## 4.3. Numero massimo di password errate per il wipe

Numero di password di sblocco del dispositivo errate che possono essere immesse prima che un dispositivo venga formattato alle impostazioni di fabbrica. Un valore pari a 0 indica che non vi è alcuna restrizione.

## 4.4. Scadenza password

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

## 4.5. Richiedi sblocco con password

Il periodo di tempo durante il quale un dispositivo o un profilo di lavoro che è stato sbloccato utilizzando una forma di autenticazione forte (password, PIN, sequenza) può essere sbloccato utilizzando qualsiasi altro metodo di autenticazione (ad es. impronta digitale, trust agent, volto). Allo scadere del periodo di tempo specificato, è possibile utilizzare solo forme di autenticazione forti per sbloccare il dispositivo o il profilo di lavoro.

**Valore predefinito del dispositivo:** Il periodo di tempo è impostato al valore predefinito del dispositivo.

**Ogni giorno:** Il periodo di tempo è impostato a 24 ore.

## 4.6. Qualità della password

La qualità della password richiesta.

**Nessuna:** Non ci sono requisiti per la password.

**Debole:** il dispositivo deve essere protetto con una tecnologia di riconoscimento biometrico a bassa sicurezza, come minimo. Ciò include tecnologie in grado di riconoscere l'identità di un individuo che sono approssimativamente equivalenti a un PIN di 3 cifre (il falso rilevamento è

inferiore a 1 su 1.000).

**Qualsiasi:** è richiesta una password, ma non ci sono restrizioni sul contenuto di essa.

**Numerica:** la password deve contenere caratteri numerici.

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

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

**Alfanumerica:** la password deve contenere sia caratteri numerici che 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 per la password. Un valore di 0 indica che non ci sono restrizioni.

## 4.8. Lettere minime

Il minimo numero di lettere richiesto nella password.

## 4.9. Lettere minuscole minime

Il minimo numero di lettere minuscole richiesto nella password.

## 4.10. Lettere maiuscole minime

Il minimo numero di lettere maiuscole richiesto nella password.

## 4.11. Caratteri non alfabetici minimi

Il minimo numero di caratteri non alfabetici (numeri o simboli) richiesto nella password.

## 4.12. Cifre numeriche minime

Il minimo numero di cifre numeriche richiesto nella password.

## 4.13. Simboli minimi

Il minimo numero di simboli richiesto nella password.

## 5. Ripristino delle impostazioni di fabbrica disabilitato

Se il ripristino delle impostazioni di fabbrica è disabilitato. Si applica solo ai dispositivi completamente gestiti.

## 6. Protezione ripristino impostazioni di fabbrica

Indirizzi e-mail degli amministratori del dispositivo per la protezione del ripristino delle impostazioni di fabbrica. Quando il dispositivo subisce un ripristino delle impostazioni di fabbrica non autorizzato, sarà necessario che uno di questi amministratori acceda con l'e-mail e la password dell'account Google per sbloccare il dispositivo. Se non viene specificato alcun amministratore, il dispositivo non fornirà la protezione per il ripristino dei dati di fabbrica. Si applica solo ai dispositivi completamente gestiti.

## 7. Funzioni di blocco schermo

Funzionalità del keyguard (blocco schermo) che possono essere disabilitate.

### 7.1. Disabilita tutto

Disabilita tutte le attuali e future personalizzazioni del keyguard.

### 7.2. Disabilita la fotocamera

Disabilita la fotocamera sulle schermate di blocco sicure (e.g. PIN).

### 7.3. Disabilita le notifiche

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

### 7.4. Disabilita le notifiche non modificate

Disabilita le notifiche non modificate sulle schermate di blocco sicure.

### 7.5. Ignora lo stato del trust agent

Ignora lo stato del trust agent sulle schermate di blocco sicure.

### 7.6. Disabilita l'impronta digitale

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

## 7.7. Disabilita l'inserimento del testo nelle notifiche

Disabilita l'inserimento di testo nelle notifiche sulle schermate di blocco sicure.

## 7.8. Disabilita autenticazione con il volto

Disabilita l'autenticazione tramite il volto sulle schermate di blocco sicure.

## 7.9. Disabilita autenticazione con l'iride

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

## 7.10. Disabilita tutte le autenticazioni biometriche

Disabilita tutti i tipi di autenticazione biometrica sulle schermate di blocco sicure.

---

Revision #4

Created 5 March 2023 15:57:36 by Admin

Updated 17 April 2023 15:25:45 by Admin