Aggiornamenti alle impostazioni delle password in CBS Firmware 3.2.0.84

Obiettivo

L'obiettivo di questo articolo è esaminare gli aggiornamenti delle impostazioni della password nel firmware degli switch aziendali Cisco 3.2.0.84

Dispositivi interessati | Versione software

CBS250 | 3.2.0.84
CBS350 | 3.2.0.84

Introduzione

La versione firmware 3.2.0.84 per gli switch Cisco Business (CBS) serie 250 e CBS350 dispone di diversi aggiornamenti opzionali e obbligatori per l'impostazione della password. Quando si aggiorna lo switch alla versione 3.2.0.84, alcune di queste impostazioni vengono abilitate

Le impostazioni obbligatorie delle password non possono essere disattivate dagli utenti nell'interfaccia utente Web o nell'interfaccia della riga di comando.

Continua a leggere per saperne di più!

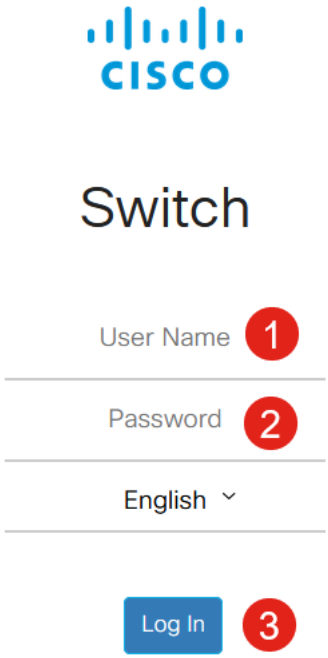
Sommario

Menu Password

Per accedere al menu delle impostazioni della password modificata:

Passaggio 1

Accedere allo switch CBS.

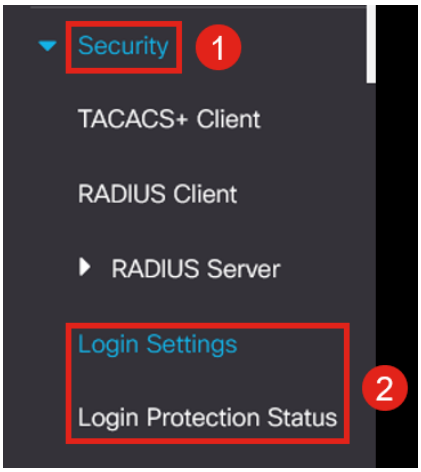


Passaggio 2

Selezionare **Advanced** (Avanzate) dall'elenco a discesa nella parte superiore dell'interfaccia utente Web dello switch.

Passaggio 3

Passare a **Sicurezza** per visualizzare due opzioni di menu: *Impostazioni di accesso*, che contiene le precedenti opzioni di menu Livello password e alcune opzioni aggiuntive, e un nuovo menu *Stato protezione accesso*.

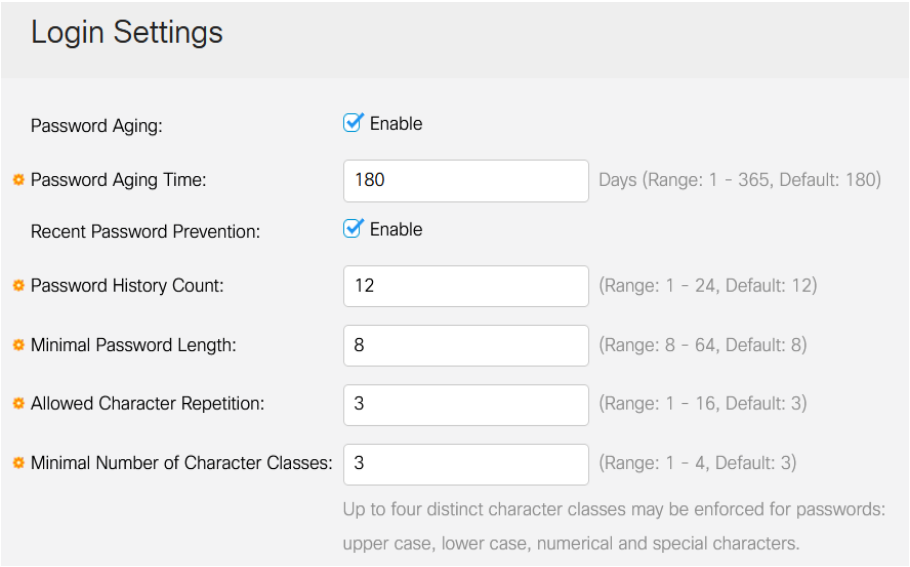


Passaggio 4

Fare clic su *Login Settings*. Questo menu è suddiviso in due sezioni: *Impostazioni di accesso* e *Blocco di accesso*

Le *impostazioni di accesso* includono le impostazioni di complessità delle password meno recenti con le impostazioni di protezione delle password più recenti.

Scadenzario password - Questa opzione è disabilitata per impostazione predefinita. Se abilitata, consente di impostare un *periodo di validità della password* in giorni.
Prevenzione delle password recenti: impedisce agli utenti di cambiare la password e di reimpostarla immediatamente sulla vecchia. Questa opzione è disattivata per impostazione predefinita.
Conteggio cronologia password: può essere impostato su un valore compreso tra 1 e 24. Per impostazione predefinita, vengono memorizzate 12 password.
Lunghezza minima password: il numero minimo di caratteri che è possibile utilizzare per la password.
Ripetizione caratteri consentita: il numero massimo di caratteri ripetibili in una riga. Ad esempio, se si imposta la password su TACRocks2222, l'operazione non riuscirà perché la password ha quattro ripetizioni 2, mentre TACRocks222 funzionerà perché ne ha solo tre.
Numero minimo di classi di caratteri - Sono disponibili quattro classi di caratteri distinte: Maiuscolo, Minuscolo, Numero e Caratteri speciali. È possibile configurare il numero di classi da utilizzare in una password.



Passaggio 5

Il menu *Blocco login* è suddiviso in due sezioni: *Ritardo risposta login* e *Imposizione periodo di attesa*, entrambe disabilitate per impostazione predefinita.

Il ritardo della *risposta di accesso* impone un ritardo compreso tra 1 e 10 secondi tra il tentativo di accesso e la risposta. Ciò può rallentare notevolmente gli attacchi al sistema da parte del dizionario automatico.

L'applicazione della *modalità non interattiva* blocca essenzialmente l'accesso allo switch per la gestione se un utente tenta di eseguire troppe operazioni di accesso con una password non corretta.

Le impostazioni includono:

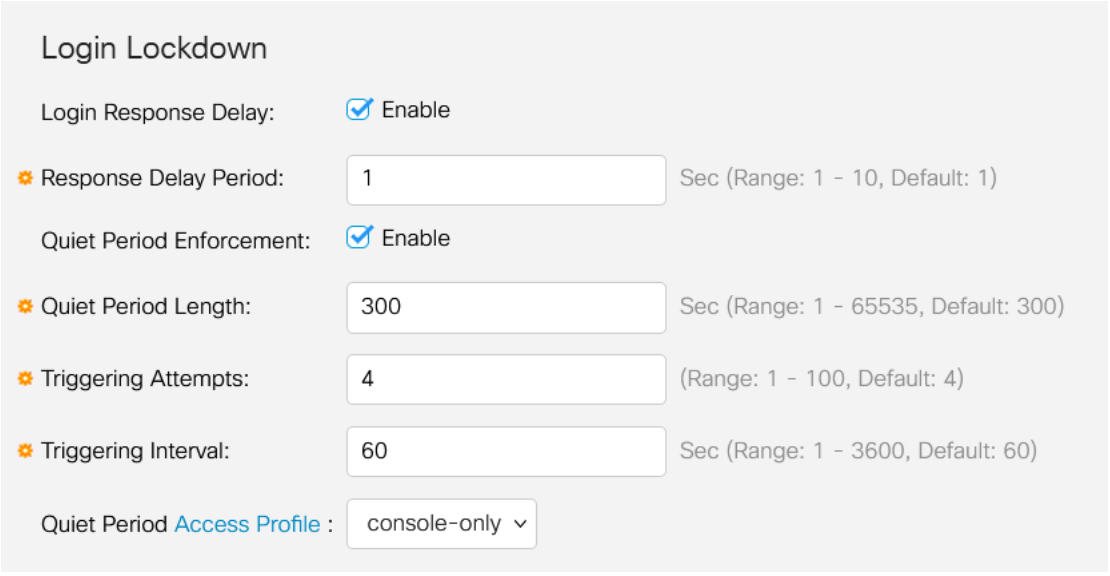
Durata periodo non interattivo: numero di secondi per cui bloccare l'accesso quando viene attivato.
Tentativi di attivazione e l'*Intervallo di attivazione* indica il numero di tentativi di accesso non riusciti (i tentativi di attivazione) nel periodo monitorato (l'intervallo di attivazione)

prima che blocchi l'accesso.

Per impostazione predefinita, se abilitata, il sistema viene bloccato dopo quattro login non riusciti in un periodo di sessanta secondi.

Il *profilo di accesso per il periodo di attesa* specifica in che modo un amministratore può accedere al dispositivo durante il blocco. Per impostazione predefinita, questa impostazione viene effettuata solo tramite la porta della console e non deve essere modificata a meno che l'utente non abbia un motivo specifico per modificarla.

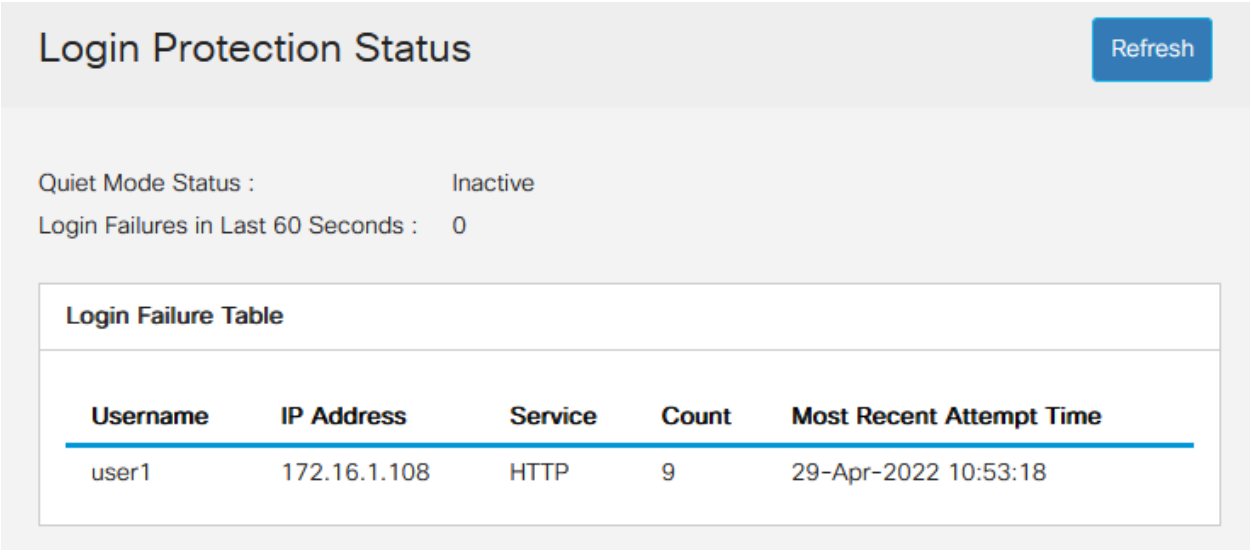
Se necessario, è possibile aggiungere altri profili di accesso in *Protezione > Metodo di accesso gestione > Profili di accesso.*



Passaggio 6

Il nuovo menu *Stato protezione accesso* è una visualizzazione informativa. Mostra gli utenti che non sono riusciti ad accedere allo switch tramite la console, il protocollo SSH o l'interfaccia utente Web.

Mostra anche quanti errori di accesso si sono verificati negli ultimi 60 secondi e se è presente un blocco che blocca le nuove connessioni SSH o Web UI.



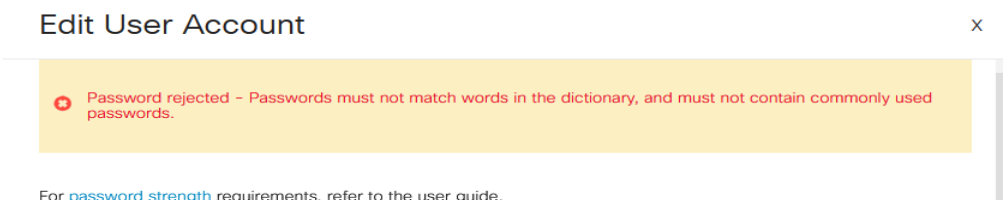
Nuove regole password obbligatorie

Queste impostazioni verranno applicate a tutti i nuovi account utente e a tutte le modifiche alle password apportate agli account utente esistenti.

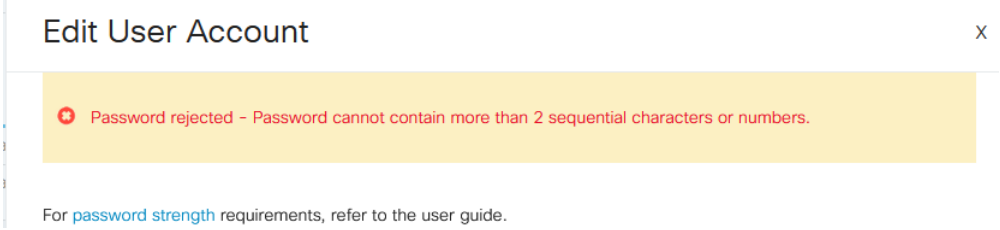
IMPOSSIBILE disabilitare nuove regole.
Verificherà che la password non provenga da un elenco di password comuni note. Questo elenco comune di password è stato compilato scegliendo le 10.000 password più utilizzate da un elenco delle 10.000.000 di password più comuni. L'elenco è disponibile sul collegamento **github**.
Nessuna variazione delle password comuni utilizzando maiuscole/minuscole o le seguenti sostituzioni di caratteri:
"$" per "s", "@" per "a", "0" per "o", "1" per "l", "!" per "i", "3" per "e"
Le password che includono più di due caratteri sequenziali in una riga verranno bloccate (anche in questo caso, verranno cercate le sostituzioni e le maiuscole più comuni). Ad esempio, se una password contiene *abc*, verrà bloccata in quanto contiene tre lettere sequenziali. Lo stesso vale per *@bc*, visto che in genere il simbolo @ viene sostituito con un simbolo. Analogamente, *cba* verrà bloccato in quanto sequenziale in ordine inverso. Altri esempi sono "efg123!$", "abcd765%", "kji!$378", "qr$58!230".
La nuova password non deve contenere il nome utente. Ad esempio, no "Admin548" per user admin.
La nuova password non deve contenere il nome del produttore. Ad esempio, no C!sc0IsCool.
La nuova password non deve contenere il nome del prodotto. Ad esempio, no CBSCo0l$switch

Messaggi di errore

Se si tenta di utilizzare una password presente nel dizionario o che contiene password di uso comune, verrà visualizzato il seguente messaggio di errore.



Se si utilizza una password che contiene caratteri sequenziali, verrà visualizzato nuovamente il seguente messaggio di errore.

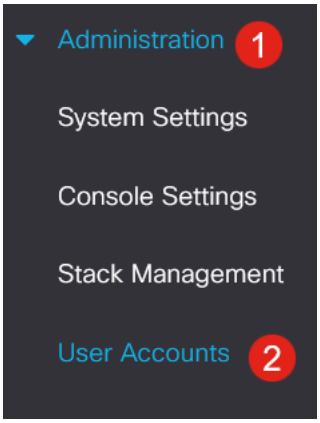


Generatore password

Per facilitare la creazione di password valide durante la creazione di nuovi utenti o la modifica di utenti esistenti, è stato incorporato un generatore di password casuale nell'interfaccia utente Web dello switch.

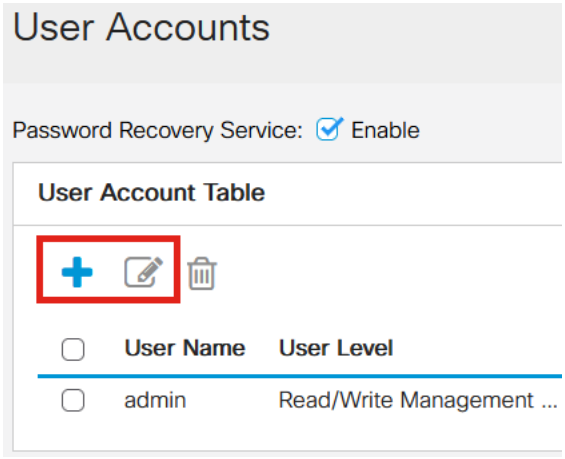
Passaggio 1

Selezionare **Amministrazione > Account utente**.



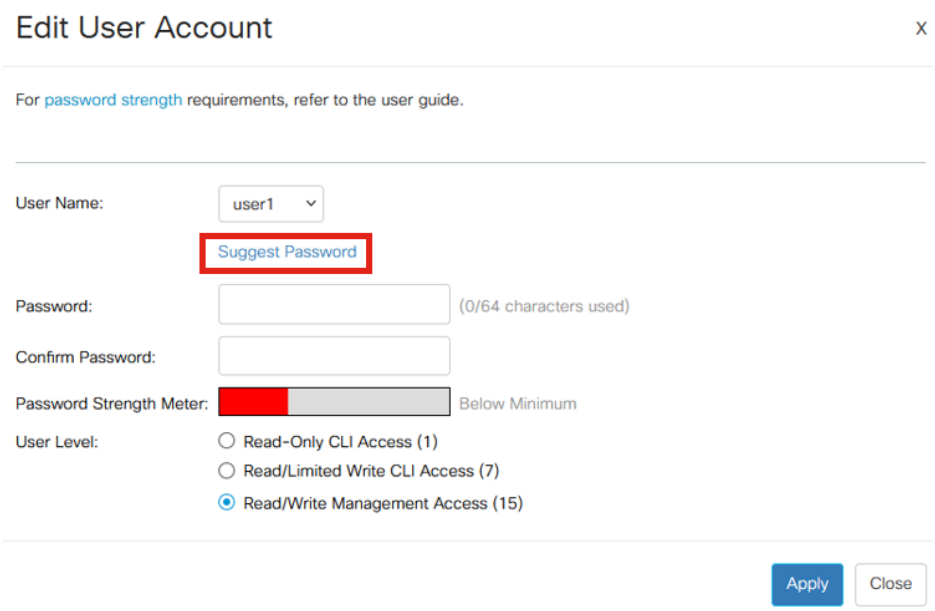
Passaggio 2

Aggiungere o *modificare* un account utente.



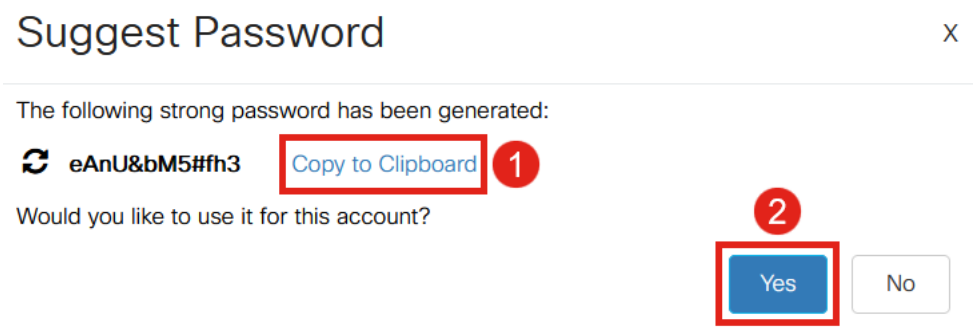
Passaggio 3

Fare clic sul collegamento **Suggerisci password**.



Passaggio 4

Verrà aperta una pagina con il suggerimento della password ed è possibile copiare la nuova password negli Appunti. Per utilizzare la password dell'account, fare clic su **Sì**.



ÈMOLTO importante copiare questa password negli Appunti prima di dire Sì per utilizzarla per l'account. Se non si salva la password prima di confermare il messaggio, non sarà possibile individuare la password ed è improbabile che la si ricordi. Salvare la password copiata in un documento in una posizione sicura.

Questo processo genererà una password valida, ma è possibile che la password generata non sia una password complessa in base al misuratore di complessità della password. Se la password è "Debole", provare con un'altra password suggerita o aggiungere caratteri alla fine della stringa.

Conclusioni

A questo punto è possibile ottenere tutte le informazioni sugli aggiornamenti delle impostazioni delle password in Cisco Business Switch Firmware 3.2.0.84