Wachtwoordinstellingen voor updates in CBS-firmware 3.2.0.8

Doel

Het doel van dit artikel is om de wachtwoordinstellingsupdates in Cisco Business Switches Firmware 3.2.0.84 te overschrijden

Toepasselijke apparaten | Softwareversie

CBS250 | 3.2.0.84
CBS350 | 3.2.0.84

Inleiding

De firmware versie 3.2.0.84 voor Cisco Business Switches (CBS) 250 en CBS350 Series heeft verschillende optionele en verplichte wachtwoordinstellingsupdates. Een aantal van deze instellingen wordt ingeschakeld wanneer u de switch aanpast aan versie 3.2.0.84

De verplichte wachtwoordinstellingen kunnen niet worden uitgeschakeld door gebruikers in de web user interface (UI) of in de Opdracht Line Interface (CLI).

Blijf lezen om meer te weten te komen!

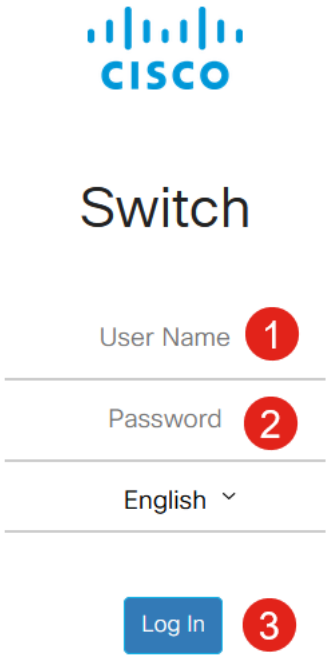
Inhoud

Menu Wachtwoord

U hebt als volgt toegang tot het gewijzigd menu Wachtwoordinstellingen:

Stap 1

Meld u aan bij de CBS switch.

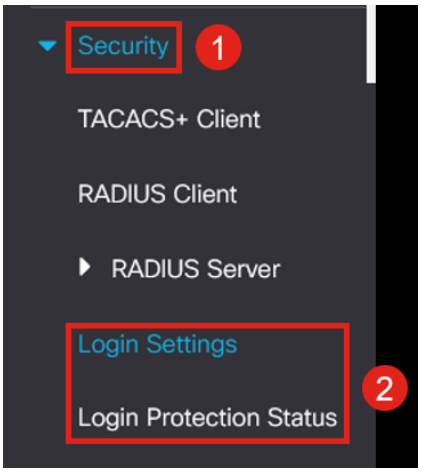


Stap 2

Kies **Geavanceerd** uit de vervolgkeuzelijst boven in de web user interface (UI) van de switch.

Stap 3

Navigeren in op **Beveiliging** en u ziet twee menuopties: *Aanmelden-instellingen* die de opties voor het menu Wachtwoord versterken en een aantal aanvullende menuopties en een nieuw menu voor *Aanmelden met* de status bevatten.

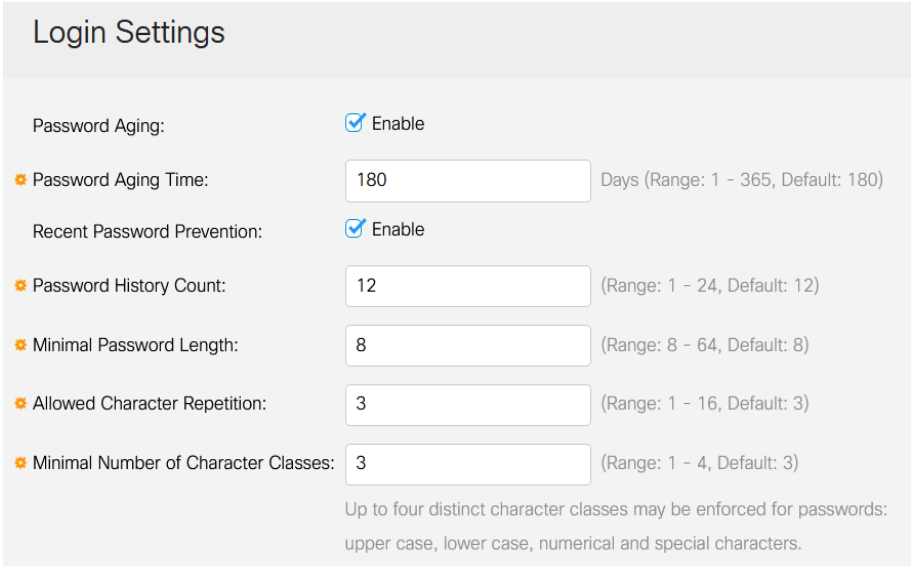


Stap 4

Klik op *Aanmelden instellingen*. Dit menu heeft twee delen - *Inloginstellingen* en *inloggen*

De *inloginstellingen* bevatten de oudere wachtwoordinstellingen en de recente wachtwoordbeveiligingsinstellingen.

Wachtwoord verouderen - Dit wordt normaal gesproken uitgeschakeld. Als deze functie is ingeschakeld, kunt u in enkele dagen een *wachttijd instellen*.
Recente wachtwoordpreventie - voorkomt dat gebruikers hun wachtwoord kunnen wijzigen en dat ze hun wachtwoord onmiddellijk terugwijzigen in hun oude wachtwoord. Dit wordt standaard uitgeschakeld.
Wachtwoordhistorie - het kan worden ingesteld op een waarde tussen 1 en 24, waarbij de standaard 12 wachtwoorden is onthouden.
Minimale wachtwoordlengte - het minimumaantal tekens dat voor het wachtwoord kan worden gebruikt.
Verboden herhaling van tekens - het maximale aantal tekens dat in een rij kan worden herhaald. Bijvoorbeeld, als je je wachtwoord instelt op TACRocks222 zou dit falen, omdat het vier herhaalde 2 heeft, maar TACRocks22 zou werken, omdat het er maar drie heeft.
Minimaal aantal tekenklassen - Er zijn vier afzonderlijke tekenklassen: Hogere case, lagere case, nummer en speciale tekens. U kunt instellen hoeveel van deze klassen in een wachtwoord moeten worden gebruikt.



Stap 5

Het menu *Login Lockdown heeft* twee delen: de *vertragingsduur voor inlogrespons* en de *handhaving van de Quiet Period*, die beide standaard uitgeschakeld zijn.

De *vertraging van de inlogrespons* zorgt voor een vertraging van 1 tot 10 seconden tussen de inlogpoging en de respons. Dit kan geautomatiseerde woordenboekaanvallen op het systeem drastisch vertragen.

De *Handhaving van de korte periode* sluit de toegang tot de switch voor het beheer af als een gebruiker te vaak probeert in te loggen met een incorrect wachtwoord.

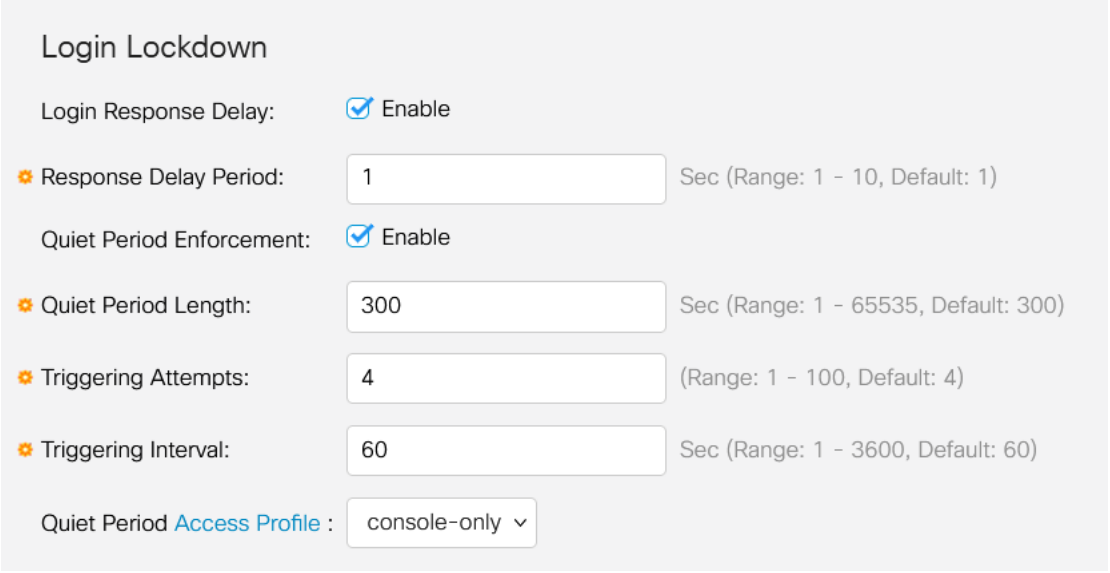
De instellingen omvatten:

Lengte stille periode - het aantal seconden om de toegang te vergrendelen wanneer deze is geactiveerd.
Trigploegen en het *kruispunt* vertellen u het aantal mislukte inlogpogingen (de triggerpogingen) in de periode die wordt gemonitord (het triggerinterval) voordat de toegang wordt afgesloten.

Als het systeem ingeschakeld is, wordt het standaard vergrendeld na vier mislukte logins in een periode van zestig seconden.

Het *Quiet Period Access Profile* specificeert hoe een beheerder het apparaat tijdens de afsluiting kan benaderen. Standaard wordt dit alleen via de console-poort gebruikt en deze mag niet worden gewijzigd zonder dat de gebruiker een specifieke reden heeft om de poort te wijzigen.

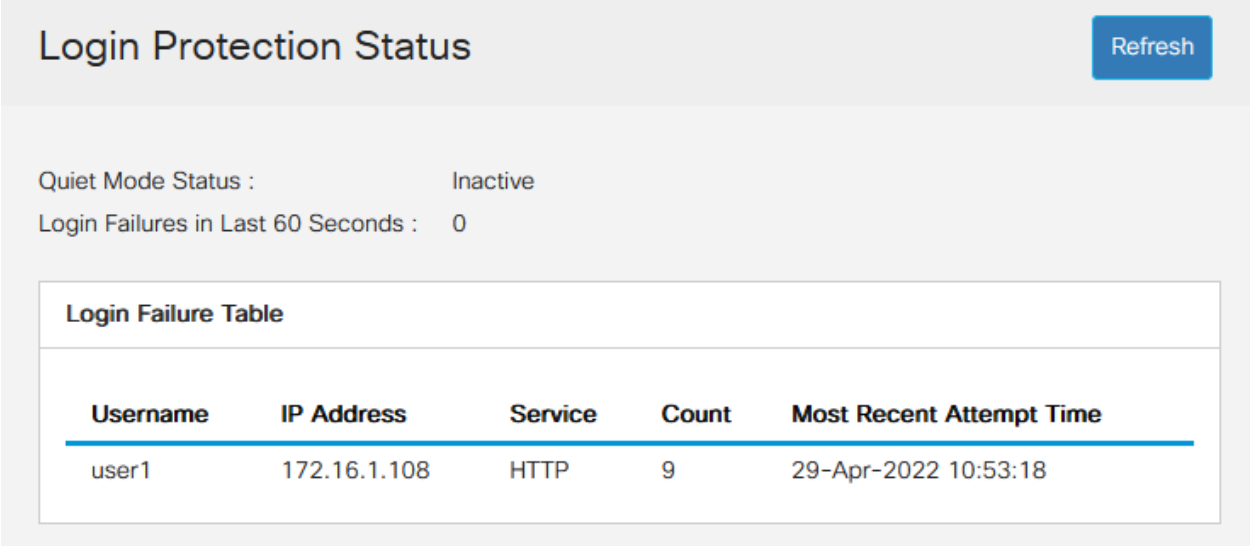
Aanvullende toegangsprofielen kunnen indien nodig worden toegevoegd onder *Security > MGMT Access Methode > Access Profiles.*



Stap 6

Het nieuwe menu *Login Protection* is een informatiedisplay. Het toont wat gebruikers in de switch door de console, SSH, of het Web UI niet hebben kunnen inloggen.

Het laat ook zien hoeveel inlogfouten in de laatste 60 seconden zijn gebeurd, en als er een sluitingssluiting is die nieuwe SSH- of Web UI-verbindingen blokkeert.



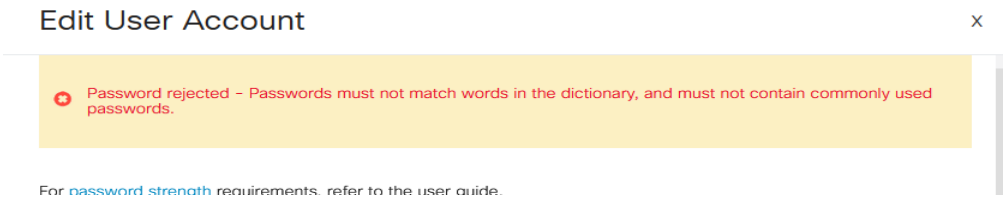
Nieuwe verplichte wachtwoordregels

Deze zijn van toepassing op alle nieuwe gebruikersrekeningen en alle wachtwoordwijzigingen die in bestaande gebruikersrekeningen worden aangebracht.

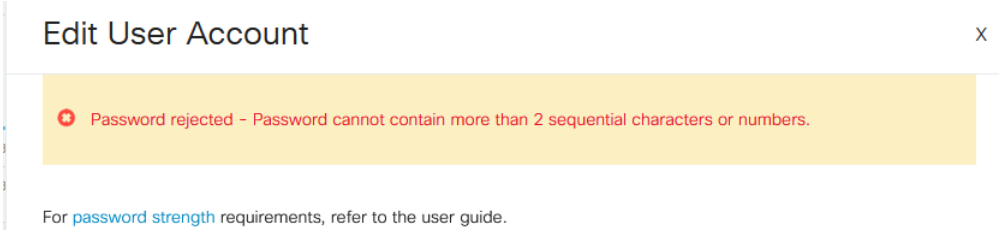
Nieuwe regels **KUNNEN NIET** worden uitgeschakeld.
Het zal controleren of het wachtwoord niet voorkomt in een lijst met bekende gemeenschappelijke wachtwoorden. Deze gemeenschappelijke wachtwoordlijst werd samengesteld door de 10.000 meest gebruikte wachtwoorden te kiezen uit een lijst met de 10.000.000 meest voorkomende wachtwoorden. Deze lijst is te vinden op de link github.
Geen wijzigingen van de gemeenschappelijke wachtwoorden in een bovenste/onderste geval of met behulp van de volgende tekensubstituties:
"$" voor "s", "@" voor "a", "0" voor "o", "1" voor "l", "!" voor "i", "3" voor "e"
Het zal wachtwoorden blokkeren die meer dan twee sequentiële tekens in een rij bevatten (opnieuw op zoek naar gemeenschappelijke substituties en case). Als een wachtwoord bijvoorbeeld *abc* bevat, wordt het geblokkeerd omdat het drie opeenvolgende letters heeft. Dat zou *@bc ook doen* omdat het @-symbool veel wordt vervangen door een ander. Op dezelfde manier zal *cba* worden geblokkeerd, omdat het in omgekeerde volgorde sequentieel is. Andere voorbeelden zijn "efg123!$", "abcd765%", "kji!$378", "qr$58!230".
Een nieuw wachtwoord mag de gebruikersnaam niet bevatten. Bijvoorbeeld, geen "Admin548" voor gebruikersbeheer.
Een nieuw wachtwoord mag de naam van de fabrikant niet bevatten. Bijvoorbeeld, geen C!sc0isCool.
Een nieuw wachtwoord mag de productnaam niet bevatten. Bijvoorbeeld, geen CBSCo0l$switch

Foutmeldingen

Als u een wachtwoord probeert te gebruiken dat in het woordenboek voorkomt of algemeen gebruikte wachtwoorden bevat, ziet u de volgende foutmelding.



Als u een wachtwoord gebruikt dat opeenvolgende tekens bevat, krijgt u opnieuw de volgende foutmelding.



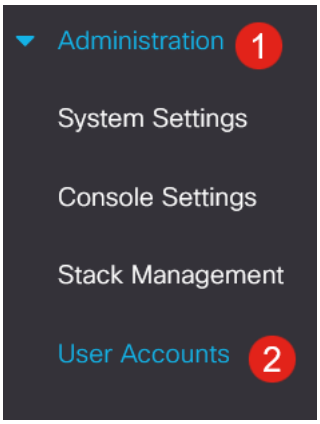
Wachtwoordgenerator

Om u te helpen met geldige wachtwoorden te komen wanneer u nieuwe gebruikers

maakt of bestaande gebruiker bewerkt, is een willekeurige wachtwoordgenerator ingebouwd in de web UI van de switch.

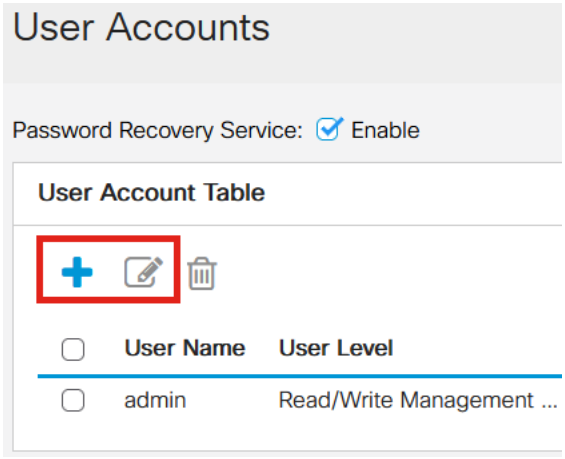
Stap 1

Ga naar **Administratie > Gebruikersrekeningen**.



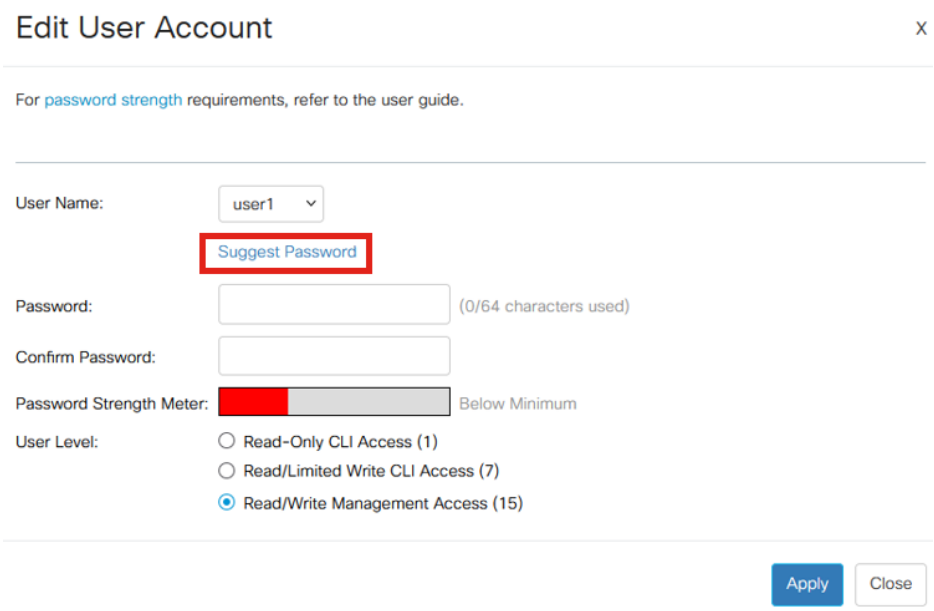
Stap 2

Voeg een gebruikersaccount toe of *Bewerk* een gebruikersaccount.



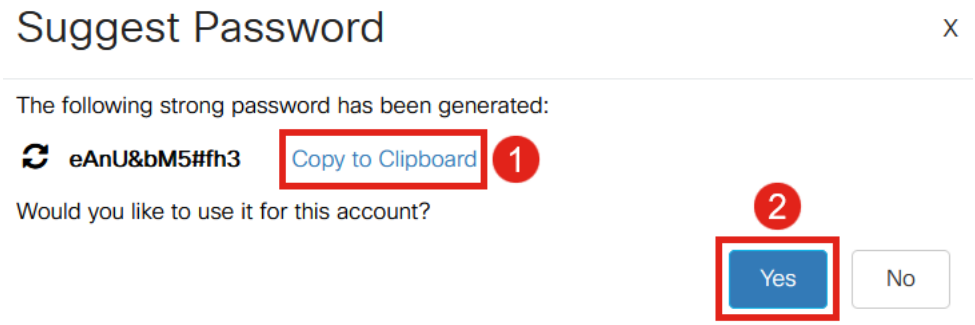
Stap 3

Klik op de link **Wachtwoord suggereren**.



Stap 4

Er wordt een pagina geopend met de wachtwoordsuggestie en u kunt het nieuwe wachtwoord naar het klembord kopiëren. Als u het wachtwoord voor de account wilt gebruiken, klikt u op **Ja**.



Het is zeer belangrijk dat u dit wachtwoord naar het klembord kopieert voordat u ja zegt om het voor de account te gebruiken. Als u dit wachtwoord niet opslaat voordat u ja zegt, kunt u niet te weten komen wat het wachtwoord is, en het is onwaarschijnlijk dat u het zich herinnert. Sla het gekopieerde wachtwoord in een document op een veilige locatie op.

Dit proces zal een geldig wachtwoord genereren, maar het is mogelijk dat het wachtwoord dat het genereert geen "sterk" wachtwoord zal zijn volgens de wachtwoordsterktemeter. Als het wachtwoord zegt "Zwak", kunt u een ander voorgesteld wachtwoord proberen of tekens toevoegen aan het einde van de string.

Conclusie

U weet nu alles over de wachtwoordinstellingsupdates in Cisco Business Switches Firmware 3.2.0.84