Updates für Kennworteinstellungen in der CBS-Firmware 3.2.0.84

Ziel

In diesem Artikel werden die Aktualisierungen für die Kennworteinstellungen in der Cisco Business Switches Firmware 3.2.0.84 erläutert.

Unterstützte Geräte | Software-Version

CBS 250 | 3.2.0.84
CBS 350 | 3.2.0.84

Einleitung

Die Firmware-Version 3.2.0.84 für Cisco Business Switches der Serien CBS 250 und CBS 350 enthält mehrere optionale und obligatorische Updates für die Kennworteinstellung. Eine Reihe dieser Einstellungen wird aktiviert, wenn Sie Ihren Switch auf Version 3.2.0.84 aktualisieren

Obligatorische Kennworteinstellungen können von Benutzern weder in der Webbenutzeroberfläche (UI)I noch in der Befehlszeilenschnittstelle (CLI) deaktiviert werden.

Lesen Sie weiter, um mehr zu erfahren!

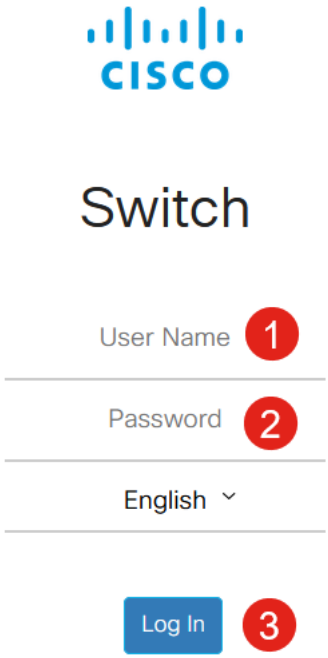
Inhalt

Kennwortmenü

So greifen Sie auf das Menü mit den geänderten Kennworteinstellungen zu:

Schritt 1

Melden Sie sich bei Ihrem CBS-Switch an.

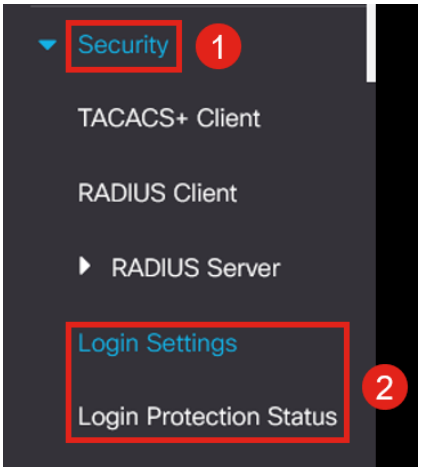


Schritt 2

Wählen Sie **Erweitert** aus dem Dropdown-Menü oben auf der Webbenutzeroberfläche des Switches aus.

Schritt 3

Navigieren Sie zu **Sicherheit**, und es werden zwei Menüoptionen angezeigt: *Anmeldungseinstellungen*, die die alten Optionen des Kennwortstärkermenüs und einige zusätzliche Menüoptionen sowie ein neues Menü *Anmeldeschutzstatus* enthalten.

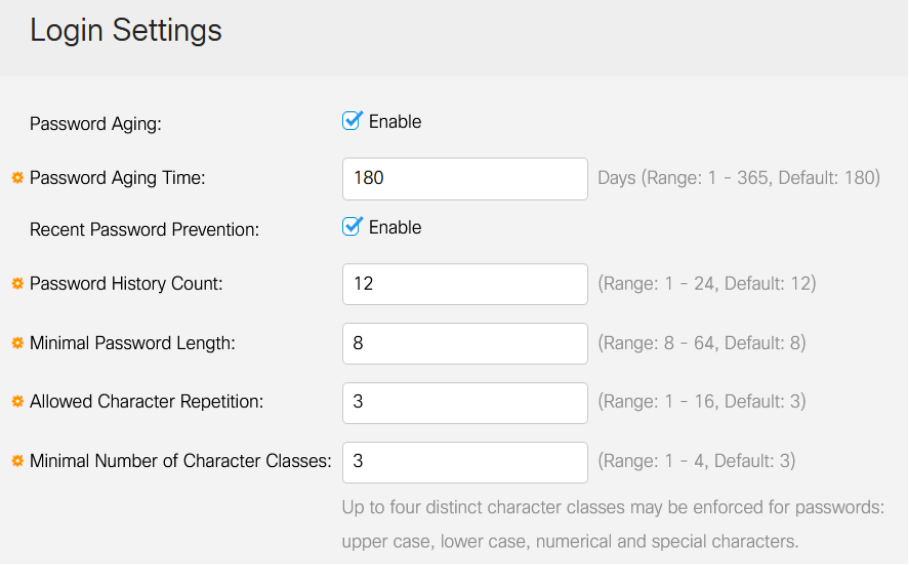


Schritt 4

Klicken Sie auf *Anmeldungseinstellungen*. Dieses Menü umfasst zwei Bereiche: *Anmeldungseinstellungen* und *Sperrung der Anmeldung.*

Die *Anmeldungseinstellungen* enthalten die älteren Einstellungen für die Kennwortstärke mit den aktuellen Einstellungen für den Kennwortschutz.

Kennwortalterung - Diese Option ist standardmäßig deaktiviert. Wenn diese Option aktiviert ist, können Sie eine *Kennwortalterzeit* in Tagen festlegen.
Kürzlich verwendeter Kennwortschutz - Verhindert, dass Benutzer ihr Kennwort ändern und sofort wieder in ihr altes Kennwort ändern. Diese Einstellung ist standardmäßig deaktiviert.
Kennwort-Verlaufszählung: Sie kann auf einen Wert zwischen 1 und 24 festgelegt werden, wobei 12 Kennwörter standardmäßig gespeichert werden.
Minimale Kennwortlänge: Die Mindestanzahl von Zeichen, die für Ihr Kennwort verwendet werden können.
Zulässige Zeichenwiederholung: Die maximale Anzahl von Zeichen, die in einer Zeile wiederholt werden können. Wenn Sie beispielsweise Ihr Kennwort auf TACRocks222 festlegen, schlägt dies fehl, weil es vier wiederholte 2 enthält, aber TACRocks22 würde funktionieren, da es nur drei enthält.
Minimale Anzahl von Zeichenklassen - Es gibt vier verschiedene Zeichenklassen: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen. Sie können festlegen, wie viele dieser Klassen in einem Kennwort verwendet werden müssen.



Schritt 5

Das Menü *"Login Lockdown*" umfasst zwei Bereiche: die *Login Response Delay* und die *Quiet Period Enforcement*, die beide standardmäßig deaktiviert sind.

Die *Login Response Delay* erzwingt eine Verzögerung von 1 bis 10 Sekunden zwischen dem Anmeldeversuch und der Antwort. Dies kann die automatischen Wörterbuchangriffe auf das System erheblich verlangsamen.

Bei der *Durchsetzung* des *Stillen* Zeitraums wird der Zugriff auf den Switch zur Verwaltung gesperrt, wenn ein Benutzer zu oft versucht, sich mit einem falschen Kennwort anzumelden.

Die Einstellungen umfassen:

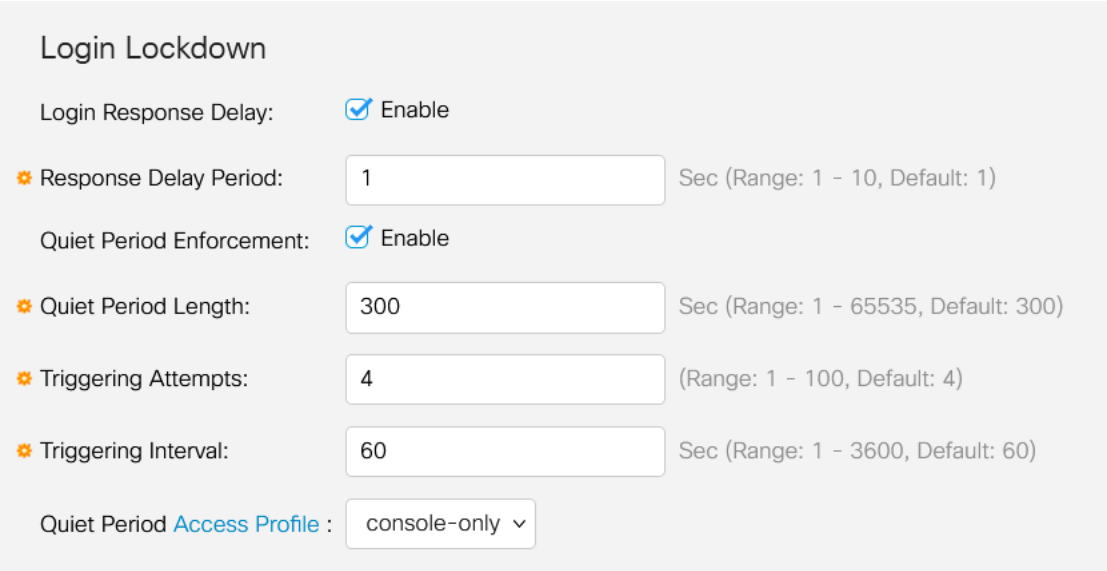
Stille Zeitdauer - Die Anzahl der Sekunden, die der Zugriff gesperrt wird, wenn er ausgelöst wird.
Triggering Attempts und das *Triggering Interval* geben Ihnen die Anzahl der fehlgeschlagenen Anmeldeversuche (die Auslöseversuche) im überwachten Zeitraum

(das Auslöseintervall) an, bevor der Zugriff gesperrt wird.

Wenn diese Funktion aktiviert ist, wird das System standardmäßig nach vier fehlgeschlagenen Anmeldungen in 60 Sekunden gesperrt.

Das *Quiet Period Access Profile* legt fest, wie ein Administrator während des Sperrvorgangs auf das Gerät zugreifen kann. Standardmäßig erfolgt dies nur über den Konsolen-Port und sollte nicht geändert werden, es sei denn, der Benutzer hat einen bestimmten Grund, diesen zu ändern.

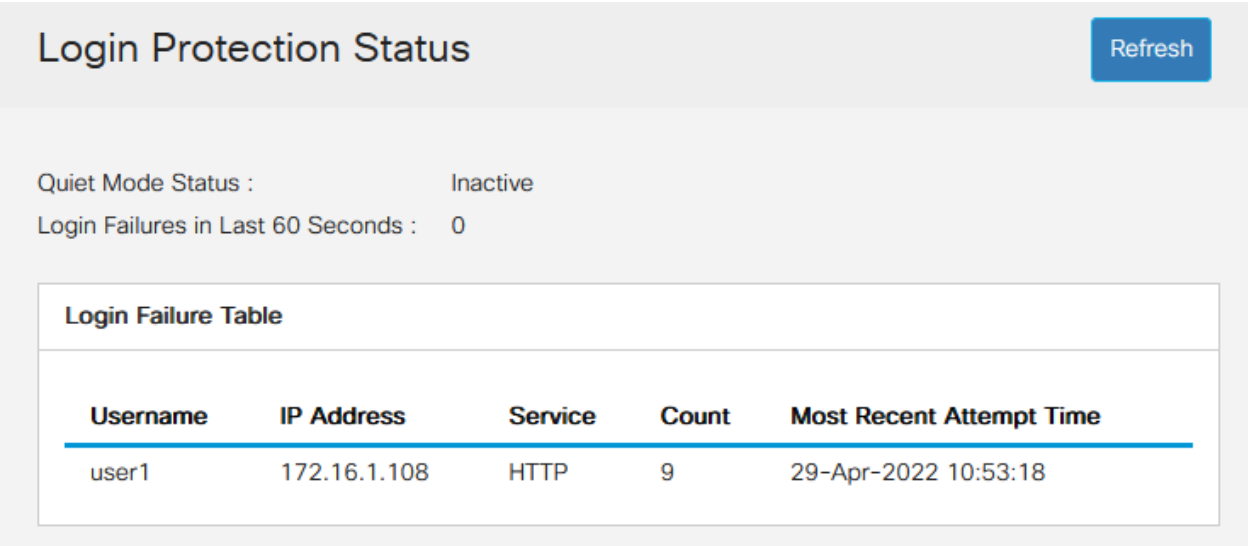
Weitere Zugriffsprofile können bei Bedarf unter *Sicherheit > Mgmt-Zugriffsmethode > Zugriffsprofile* hinzugefügt werden.



Schritt 6

Das neue Menü *Anmeldeschutzstatus* dient zur Informationsanzeige. Es zeigt an, welche Benutzer sich nicht über die Konsole, SSH oder die Webbenutzeroberfläche beim Switch angemeldet haben.

Es zeigt auch, wie viele Anmeldefehler in den letzten 60 Sekunden aufgetreten sind und ob es ein Sperren gibt, das neue SSH- oder Web-UI-Verbindungen blockiert.



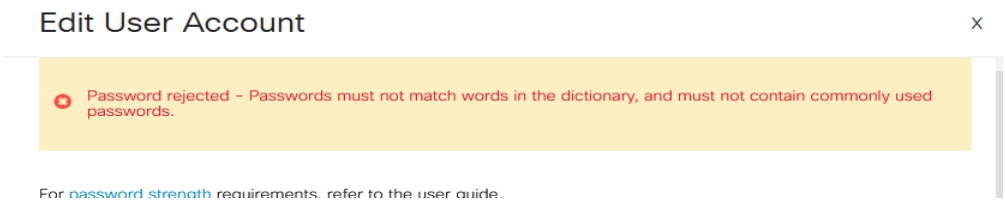
Neue Regeln für obligatorisches Kennwort

Diese gelten für alle neuen Benutzerkonten und alle Kennwortänderungen, die an vorhandenen Benutzerkonten vorgenommen wurden.

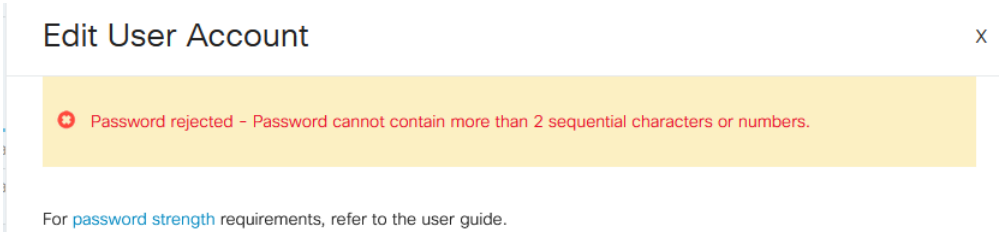
Neue Regeln **können NICHT** deaktiviert werden.
Sie wird überprüfen, ob das Kennwort nicht aus einer Liste bekannter allgemeiner Passwörter stammt. Diese allgemeine Kennwortliste wurde erstellt, indem die 10.000 am häufigsten verwendeten Passwörter aus einer Liste der 10.000.000 gängigsten Passwörter ausgewählt wurden. Diese Liste finden Sie unter dem github-Link.
Es gibt keine Variationen häufiger Passwörter, die Groß-/Kleinschreibung verwenden oder die folgenden Zeichen ersetzen:
"$" für "s", "@" für "a", "0" für "o", "1" für "l", "!" bei "i", "3" bei "e"
Kennwörter, die mehr als zwei aufeinander folgende Zeichen enthalten, werden blockiert (erneut auf der Suche nach gängigen Ersatzzeichen und Groß-/Kleinschreibung). Wenn beispielsweise ein Kennwort *abc* enthält, wird es blockiert, da es drei aufeinander folgende Buchstaben enthält. So würde *@bc*, da es die übliche Ersetzung des @-Symbols für a gibt. Ebenso wird *cba* blockiert, da es in umgekehrter Reihenfolge sequenziell ist. Weitere Beispiele sind "efg123!$", "abcd765%", "kji!$378", "qr$58!230".
Das neue Kennwort darf den Benutzernamen nicht enthalten. Beispiel: Kein "Admin548" für Benutzeradministrator.
Das neue Kennwort darf den Herstellernamen nicht enthalten. Zum Beispiel kein C!sc0lsCool.
Das neue Kennwort darf den Produktnamen nicht enthalten. Zum Beispiel kein CBSCo0l$witch

Fehlermeldungen

Wenn Sie versuchen, ein Kennwort zu verwenden, das entweder im Wörterbuch enthalten ist oder häufig verwendete Kennwörter enthält, wird die folgende Fehlermeldung angezeigt.



Wenn Sie ein Kennwort mit sequenziellen Zeichen verwenden, wird erneut die folgende Fehlermeldung angezeigt.

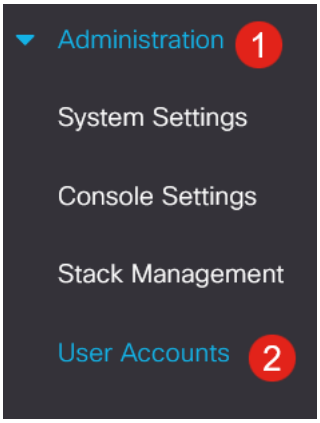


Kennwortgenerator

Um Ihnen bei der Erstellung von gültigen Kennwörtern zu helfen, wenn Sie entweder neue Benutzer erstellen oder vorhandene Benutzer bearbeiten, wurde ein Zufallskennwortergenerator in die Webbenutzeroberfläche des Switches integriert.

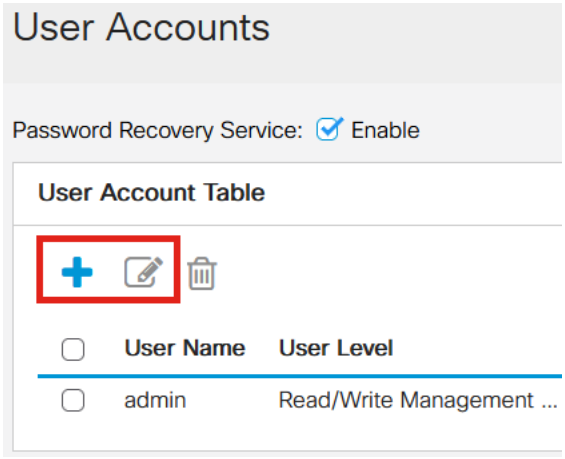
Schritt 1

Gehen Sie zu **Administration > User Accounts**.



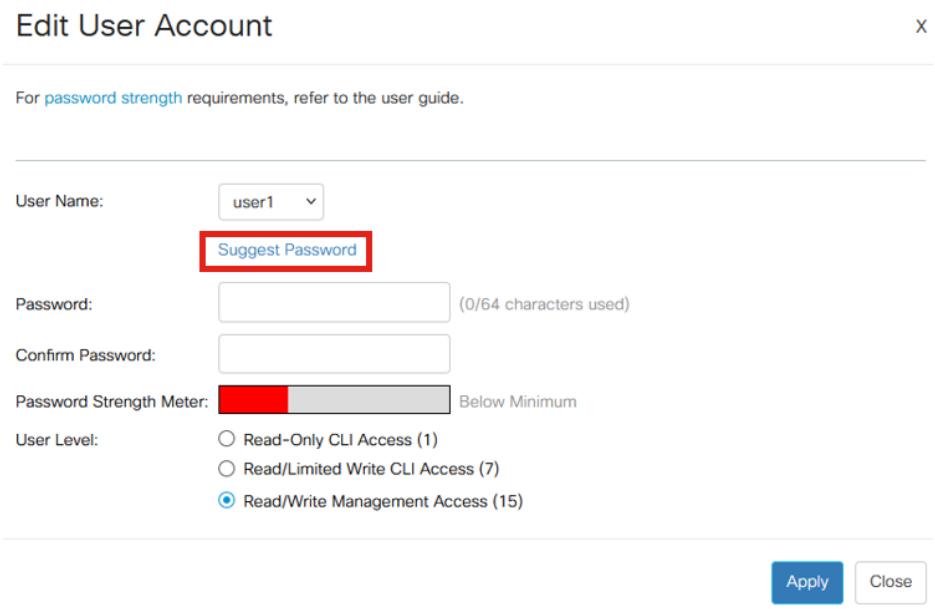
Schritt 2

Sie können ein Benutzerkonto *hinzufügen* oder *bearbeiten*.



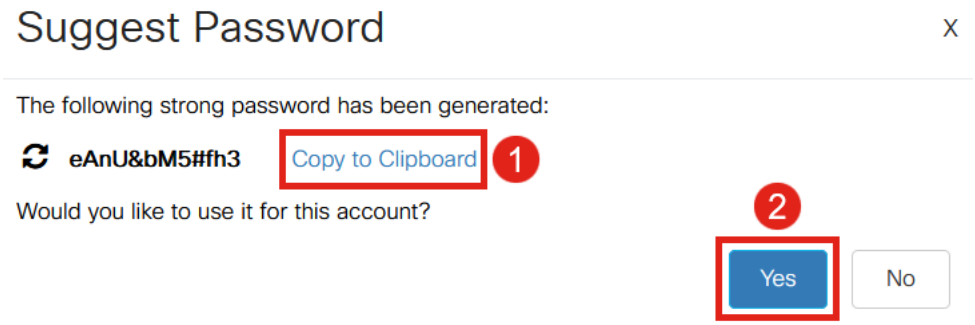
Schritt 3

Klicken Sie auf den Link **Kennwort vorschlagen**.



Schritt 4

Es öffnet sich eine Seite mit dem Passwortvorschlag, und Sie können dieses neue Passwort in die Zwischenablage kopieren. Um das Kennwort für das Konto zu verwenden, klicken Sie einfach auf **Ja**.



Es ist SEHR wichtig, dass Sie dieses Kennwort in die Zwischenablage kopieren, bevor Sie Ja sagen, es für das Konto zu verwenden. Wenn Sie dieses Kennwort nicht speichern, bevor Sie mit "Ja" sagen, können Sie das Kennwort nicht ermitteln, und es ist unwahrscheinlich, dass Sie sich daran erinnern. Speichern Sie das kopierte Kennwort in einem Dokument an einem sicheren Ort.

Dieser Prozess generiert ein gültiges Kennwort, aber es ist möglich, dass das von ihm generierte Kennwort kein "sicheres" Kennwort sein kann, das der Kennwortstärkeregelung entspricht. Wenn das Kennwort "schwach" lautet, können Sie ein anderes empfohlenes Kennwort ausprobieren oder Zeichen am Ende der Zeichenfolge hinzufügen.

Schlussfolgerung

Sie kennen jetzt alle Aktualisierungen für die Kennworteinstellungen in der Cisco Business Switches Firmware 3.2.0.84.