Mises à jour des paramètres de mot de passe dans le micrologiciel CBS 3.2.0.84

Objectif

L'objectif de cet article est de passer en revue les mises à jour des paramètres de mot de passe dans le micrologiciel des commutateurs commerciaux Cisco 3.2.0.84

Périphériques pertinents | Version du logiciel

CBS250 |3.2.0.84
CBS350 |3.2.0.84

Introduction

La version 3.2.0.84 du micrologiciel pour les commutateurs Cisco Business Switches (CBS)250 et CBS350 comporte plusieurs mises à jour facultatives et obligatoires des paramètres de mot de passe. Un certain nombre de ces paramètres seront activés lorsque vous mettrez à jour votre commutateur vers la version 3.2.0.84

Les paramètres de mot de passe obligatoires ne peuvent pas être désactivés par les utilisateurs de l'interface utilisateur Web (UI)I ou de l'interface de ligne de commande (CLI).

Continuez à lire pour en savoir plus !

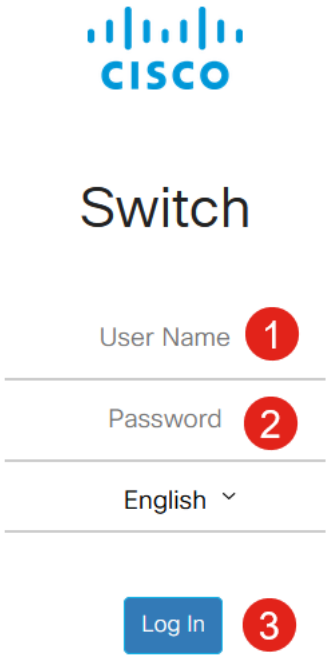
Table des matières

Menu Mot de passe

Pour accéder au menu des paramètres de mot de passe modifiés :

Étape 1

Connectez-vous à votre commutateur CBS.

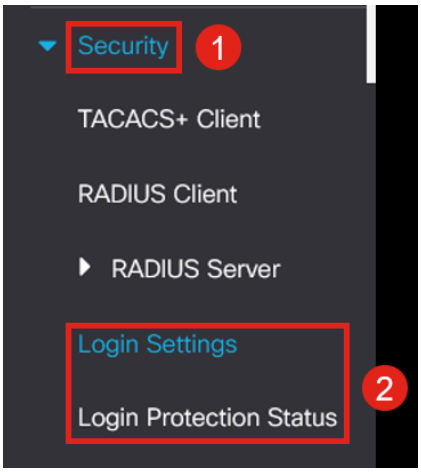


Étape 2

Choisissez **Avancé** dans la liste déroulante située en haut de l'interface utilisateur Web du commutateur.

Étape 3

Accédez à **Sécurité** et vous verrez deux options de menu : *Paramètres de connexion* qui contient l'ancienne option de menu Puissance du mot de passe et quelques options de menu supplémentaires et un nouveau menu *État de la protection de connexion*.

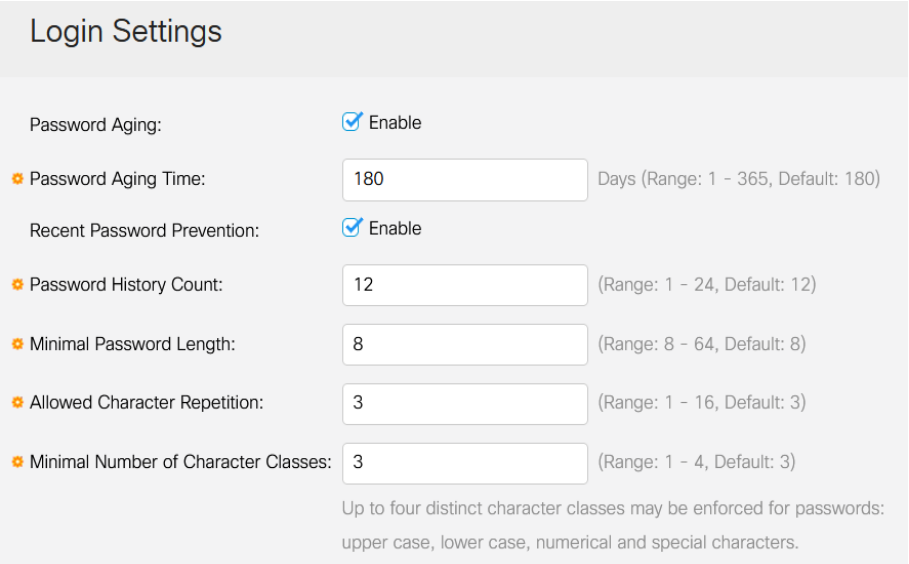


Étape 4

Cliquez sur *Paramètres de connexion*. Ce menu comporte deux sections : *Paramètres de connexion* et *Verrouillage de connexion*

Les *paramètres de connexion* incluent les anciens paramètres de résistance du mot de passe avec les paramètres de protection du mot de passe récents.

Vieillissement du mot de passe - Cette option est désactivée par défaut. Si cette option est activée, elle vous permet de définir une *durée de vieillissement du mot de passe* en jours.
Prévention des mots de passe récents - empêche les utilisateurs de modifier leur mot de passe et de le remplacer immédiatement par leur ancien mot de passe. Ceci est désactivé par défaut.
Nombre d'historiques de mot de passe - Il peut être défini sur une valeur comprise entre 1 et 24, avec 12 mots de passe mémorisés par défaut.
Longueur minimale du mot de passe : nombre minimal de caractères pouvant être utilisés pour votre mot de passe.
Répétition de caractères autorisée : nombre maximal de caractères pouvant être répétés dans une ligne. Par exemple, si vous définissez votre mot de passe sur TACRocks2222, cela échouerait, car il a quatre répétitions 2, mais TACRocks222 fonctionnerait, car il n'en a que trois.
Nombre minimal de classes de caractères - Il existe quatre classes de caractères distinctes : Majuscules, minuscules, chiffres et caractères spéciaux. Vous pouvez configurer le nombre de ces classes à utiliser dans un mot de passe.



Étape 5

Le menu *Login Lockdown* comporte deux sections : *Login Response Delay* et *Quiet Period Enforcement*, toutes deux désactivées par défaut.

Le *délai de réponse de connexion* force un délai de 1 à 10 secondes entre la tentative de connexion et la réponse. Cela peut considérablement ralentir les attaques de dictionnaires automatisés contre le système.

La *mise en application de la période de silence* verrouille essentiellement l'accès au commutateur pour la gestion si un utilisateur tente de se connecter trop souvent avec un mot de passe incorrect.

Les paramètres sont les suivants :

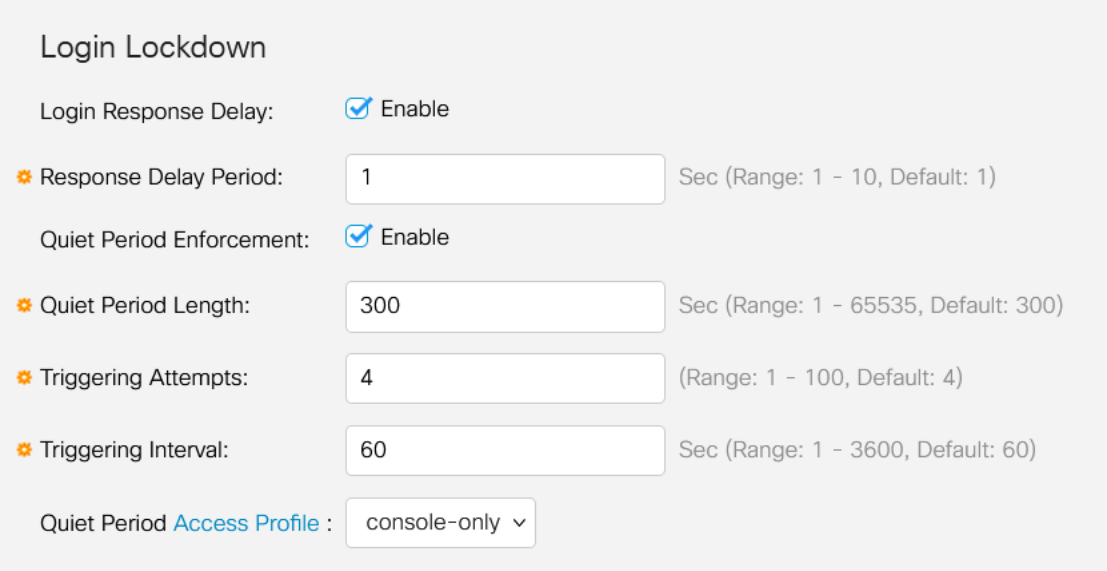
Durée de la période de silence : nombre de secondes pendant lesquelles verrouiller l'accès lorsqu'il est déclenché.
Tentatives de déclenchement et *Intervalle de déclenchement* vous indiquent le nombre

de tentatives de connexion ayant échoué (les tentatives de déclenchement) au cours de la période surveillée (l'intervalle de déclenchement) avant de verrouiller l'accès.

Par défaut, s'il est activé, il verrouillera le système après quatre échecs de connexion en soixante secondes.

Le *profil d'accès aux périodes de silence* spécifie comment un administrateur peut accéder au périphérique pendant le verrouillage. Par défaut, il s'agit uniquement du port de console et ne doit pas être modifié, sauf si l'utilisateur a une raison spécifique de le modifier.

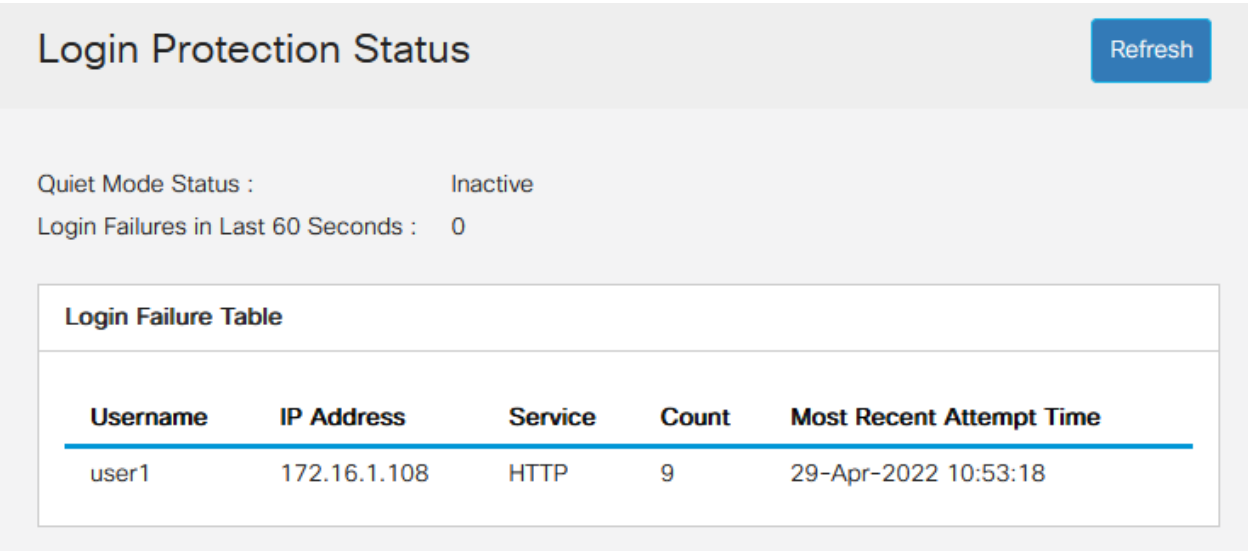
Des profils d'accès supplémentaires peuvent être ajoutés si nécessaire sous *Sécurité > Méthode d'accès de gestion > Profils d'accès.*



Étape 6

Le nouveau menu *Login Protection Status* est un affichage d'informations. Elle indique les utilisateurs qui n'ont pas pu se connecter au commutateur via la console, SSH ou l'interface utilisateur Web.

Il indique également le nombre d'échecs de connexion survenus au cours des 60 dernières secondes et, s'il y a un blocage des nouvelles connexions SSH ou Web de l'interface utilisateur.



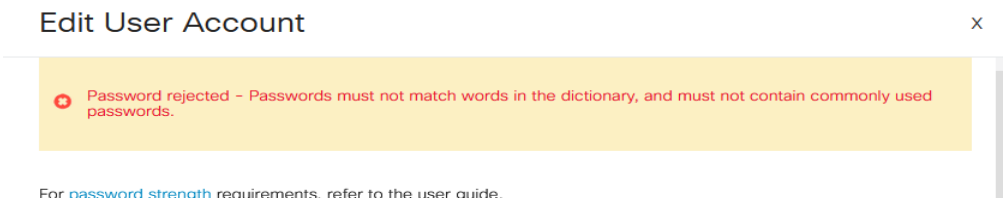
Nouvelles règles de mot de passe obligatoire

Celles-ci s'appliqueront à tous les nouveaux comptes d'utilisateurs et à toute modification de mot de passe apportée aux comptes d'utilisateurs existants.

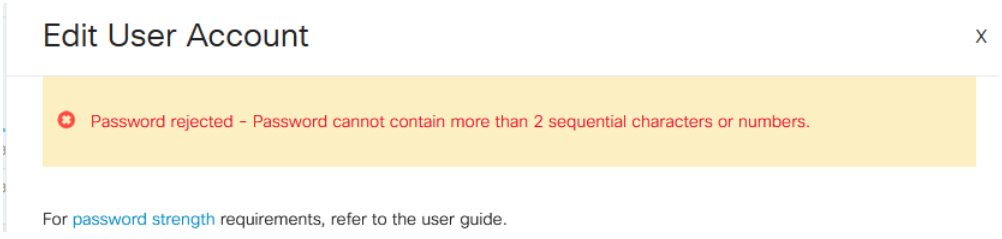
Les nouvelles règles **NE PEUVENT PAS** être désactivées.
Il vérifie que le mot de passe ne figure pas dans une liste de mots de passe courants connus. Cette liste commune de mots de passe a été compilée en sélectionnant les 10 000 mots de passe les plus utilisés dans une liste des 10 000 000 mots de passe les plus courants. Cette liste se trouve sur le lien **github**.
Aucune variation des mots de passe courants utilisant la majuscule ou la minuscule ou utilisant les substitutions de caractères suivantes :
"$" pour « s », "@" pour « a », « 0 » pour « o », « 1 » pour « l », " ! » pour « i », « 3 » pour « e “"
Il bloquera les mots de passe qui incluent plus de deux caractères séquentiels dans une ligne (à la recherche de substitutions et de majuscules courantes). Par exemple, si un mot de passe contient *abc*, il sera bloqué car il comporte trois lettres séquentielles. Il en va de même pour *@bc* puisqu'il y a la substitution courante du symbole @ pour un. De même, *cba* sera bloqué car il est séquentiel dans l'ordre inverse. D'autres exemples incluent “ efg123 !$ ”, “ abcd765% ”, “ kji !$378 ”, « qr$58 ! 230 ».
Le nouveau mot de passe ne doit pas contenir le nom d'utilisateur. Par exemple, aucun ” Admin548 “ pour l'utilisateur admin.
Le nouveau mot de passe ne doit pas contenir le nom du fabricant. Par exemple, no C!sc0IsCool.
Le nouveau mot de passe ne doit pas contenir le nom du produit. Par exemple, no CBSCo0l$witch

Messages d'erreur

Si vous essayez d'utiliser un mot de passe qui se trouve dans le dictionnaire ou contient des mots de passe couramment utilisés, le message d'erreur suivant s'affiche.



Si vous utilisez un mot de passe contenant des caractères séquentiels, vous obtiendrez à nouveau le message d'erreur suivant.

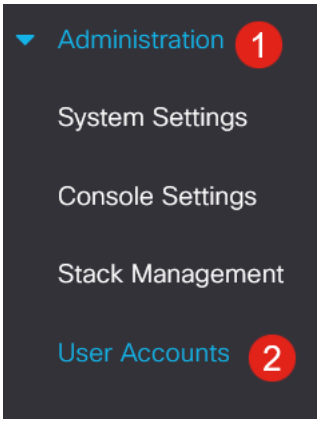


Générateur de mots de passe

Pour vous aider à trouver des mots de passe valides lors de la création de nouveaux utilisateurs ou de la modification d'un utilisateur existant, un générateur de mots de passe aléatoire a été intégré à l'interface utilisateur Web du commutateur.

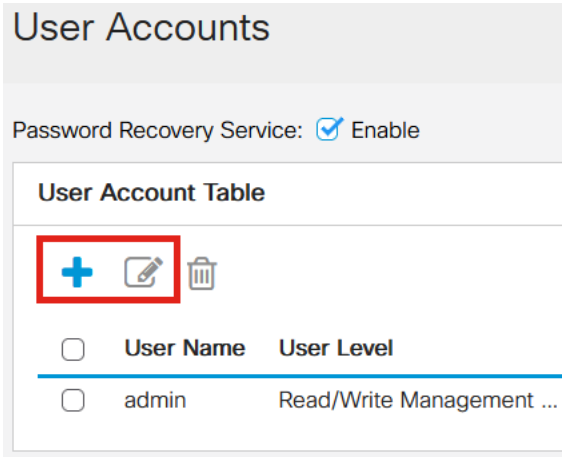
Étape 1

Accédez à **Administration > User Accounts**.



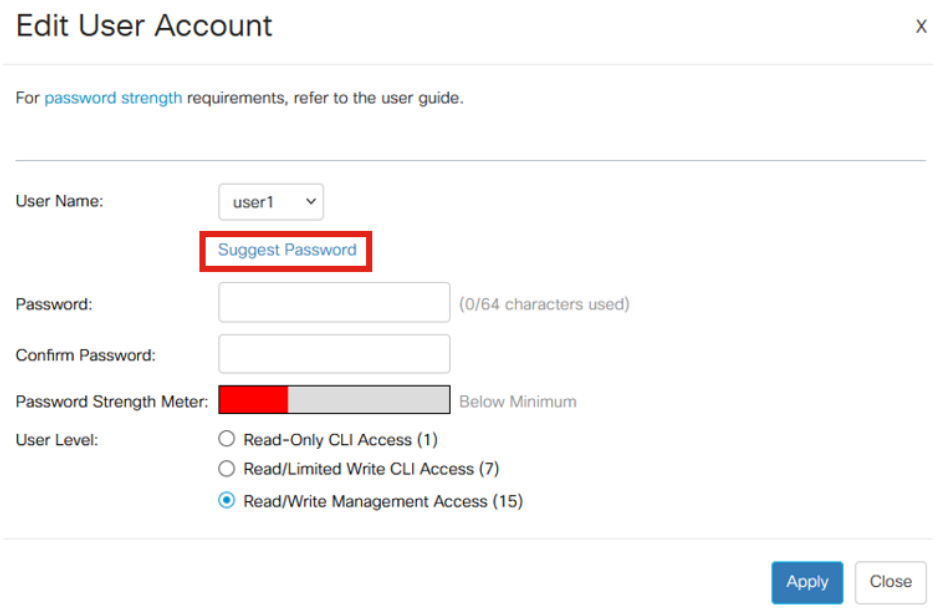
Étape 2

Ajouter ou *modifier* un compte d'utilisateur.



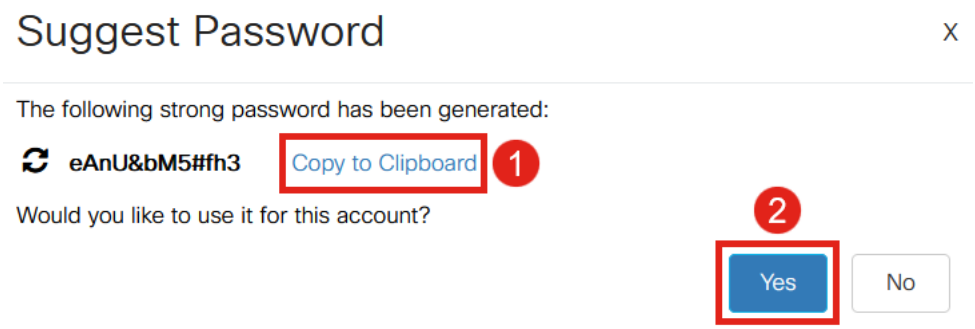
Étape 3

Cliquez sur le lien **Suggérer le mot de passe**.



Étape 4

Une page s'ouvre avec la suggestion de mot de passe, et vous pouvez copier ce nouveau mot de passe dans le presse-papiers. Pour utiliser le mot de passe du compte, cliquez simplement sur **Oui**.



Il est TRÈS important que vous copiez ce mot de passe dans le presse-papiers avant de dire Oui pour l'utiliser pour le compte. Si vous n'enregistrez pas ce mot de passe avant de dire oui, vous ne pourrez pas savoir quel est le mot de passe et il est peu probable que vous vous en souviendrez. Enregistrez le mot de passe copié dans un document dans un emplacement sécurisé.

Ce processus générera un mot de passe valide, mais il est possible que le mot de passe qu'il génère ne soit pas un mot de passe “ Strong ” selon le compteur de puissance du mot de passe. Si le mot de passe est 'Faible', vous pouvez essayer un autre mot de passe suggéré ou ajouter des caractères à la fin de la chaîne.

Conclusion

Vous savez maintenant tout sur les mises à jour des paramètres de mot de passe dans le micrologiciel Cisco Business Switches 3.2.0.84