Atualizações de configuração de senha no firmware CBS 3.2.0.84

Objetivo

O objetivo deste artigo é revisar as atualizações de configuração de senha no Firmware 3.2.0.84 dos Cisco Business Switches

Dispositivos aplicáveis | Versão do software

CBS250 |3.2.0.84
CBS350 |3.2.0.84

Introduction

A versão 3.2.0.84 do firmware para as séries CBS (Cisco Business Switches)250 e CBS350 tem várias atualizações opcionais e obrigatórias de configuração de senha. Algumas dessas configurações serão ativadas quando você atualizar seu switch para a versão 3.2.0.84

As configurações de senha obrigatória não podem ser desabilitadas pelos usuários na interface de usuário da Web (IU)ou na Interface de Linha de Comando (CLI).

Continue lendo para saber mais!

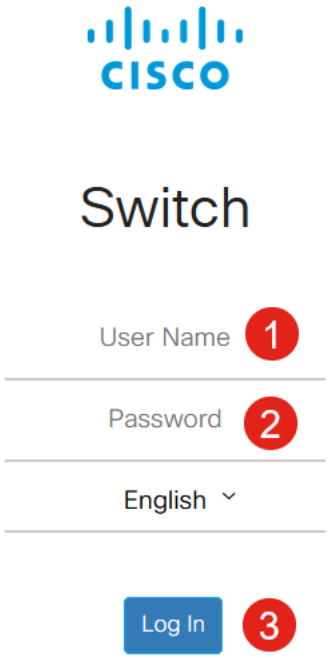
Table Of Contents

Menu Senha

Para acessar o menu de configurações de senha alterada:

Passo 1

Inicie sessão no seu switch CBS.

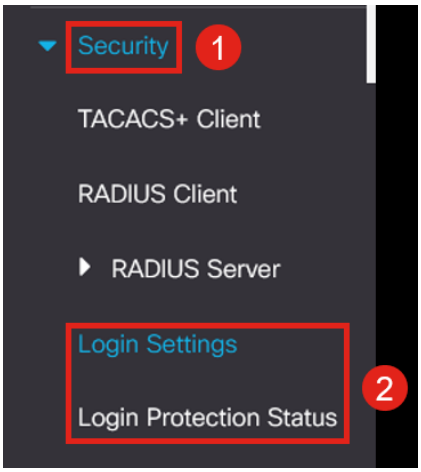


Passo 2

Escolha **Advanced** no menu suspenso na parte superior da interface do usuário da Web (UI) do switch.

Etapa 3

Navegue para **Segurança** e você verá duas opções de menu - *Configurações de login* , que contém as antigas opções de menu Força da senha e algumas opções de menu adicionais e um novo menu *Status da proteção de login*.

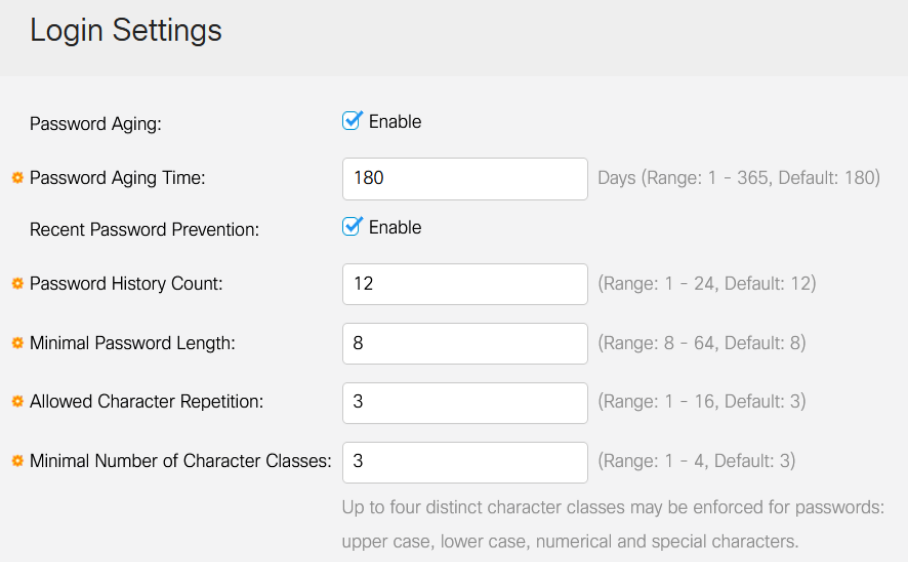


Passo 4

Clique em *Login Settings*. Este menu tem duas seções - *Configurações de login* e *Bloqueio de login*

As *Configurações de login* incluem as configurações de força de senha mais antigas com as configurações de proteção de senha recentes.

Vencimento da senha - Desativado por padrão. Se habilitado, permite definir um *Tempo de Vencimento da Senha* em Dias.
Prevenção de Senha Recente - impede que os usuários alterem suas senhas e as alterem imediatamente para a senha antiga. Essa opção está desativada por padrão.
Contagem do histórico de senhas - Pode ser definido para um valor entre 1 e 24, com o padrão sendo 12 senhas lembradas.
Tamanho mínimo da senha - o número mínimo de caracteres que podem ser usados para sua senha.
Repetição de caracteres permitida - o número máximo de caracteres que podem ser repetidos em uma linha. Por exemplo, se você definir sua senha para TACRocks222, isso falhará, porque ela tem quatro repetidos 2, mas TACRocks22 funcionará, porque ela tem apenas três.
Número mínimo de classes de caracteres - Há quatro classes de caracteres distintas: Maiúscula, minúscula, número e caracteres especiais. Você pode configurar quantas dessas classes precisam ser usadas em uma senha.



Etapa 5

O menu *Bloqueio de login* tem duas seções - o *Atraso da resposta de login* e a *Aplicação do período silencioso*, ambas desativadas por padrão.

O *Atraso de resposta de logon* força um atraso de 1 a 10 segundos entre a tentativa de logon e a resposta. Isso pode retardar drasticamente os ataques automatizados de dicionário contra o sistema.

O *Quiet Period Enforcement* basicamente bloqueia o acesso ao switch para gerenciamento se um usuário tentar fazer login muitas vezes com uma senha incorreta.

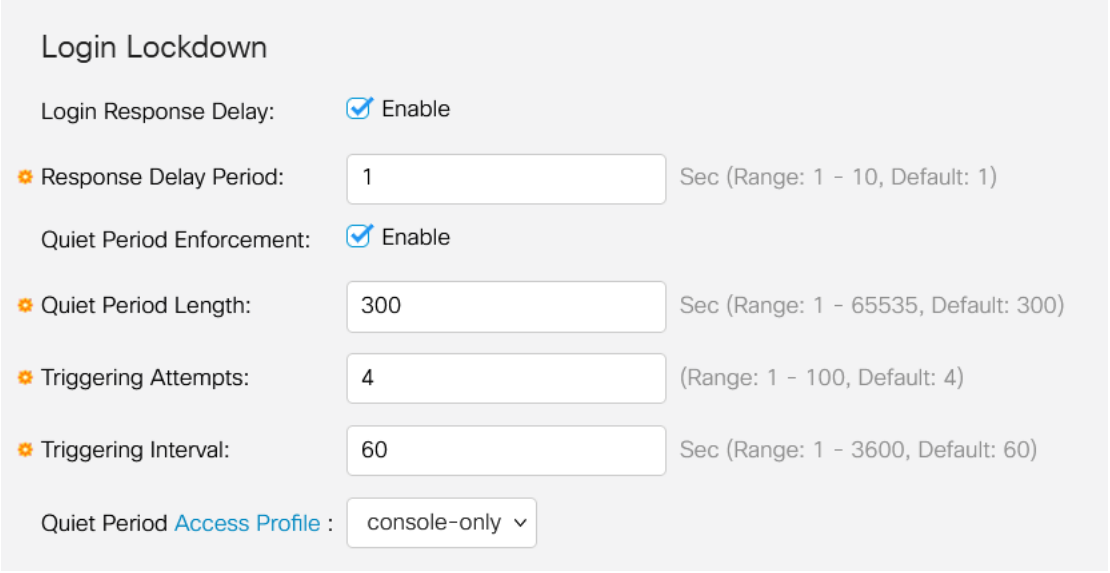
As configurações incluem:

Quiet Period Length - o número de segundos para bloquear o acesso quando ele é disparado.
Triggering Attempts e o *Triggering Interval* informam o número de tentativas de login com falha (as tentativas de disparo) no período que está sendo monitorado (o intervalo de disparo) antes de bloquear o acesso.

Por padrão, se estiver habilitado, ele bloqueará o sistema após quatro logons com falha em um período de sessenta segundos.

O *Quiet Period Access Profile* especifica como um administrador pode acessar o dispositivo durante o bloqueio. Por padrão, isso ocorre apenas através da porta de console e não deve ser alterado, a menos que o usuário tenha um motivo específico para alterá-lo.

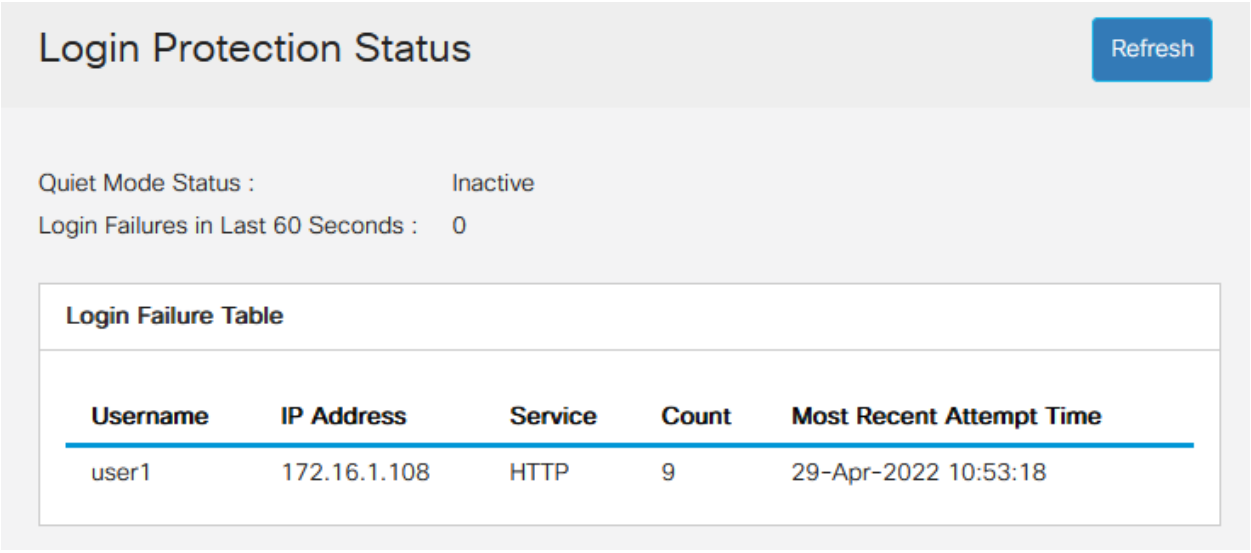
Perfis de acesso adicionais podem ser adicionados, se necessário, em *Segurança > Método de acesso de gerenciamento > Perfis de acesso.*



Etapa 6

O novo menu *Login Protection Status* é uma exibição informativa. Ele mostra quais usuários falharam ao fazer login no switch através do console, do SSH ou da interface de usuário da Web.

Ele também mostra quantas falhas de login ocorreram nos últimos 60 segundos e se há um bloqueio bloqueando novas conexões SSH ou Web UI.



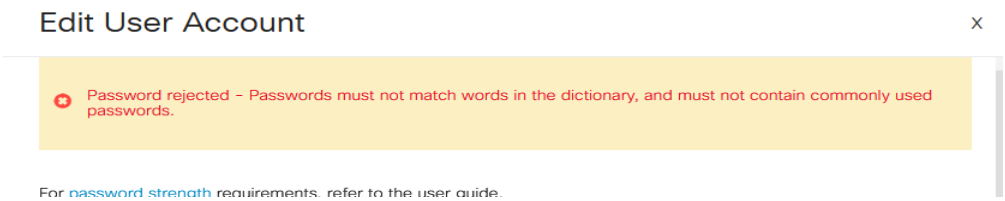
Novas regras de senha obrigatória

Isso se aplicará a todas as novas contas de usuário e quaisquer alterações de senha feitas nas contas de usuário existentes.

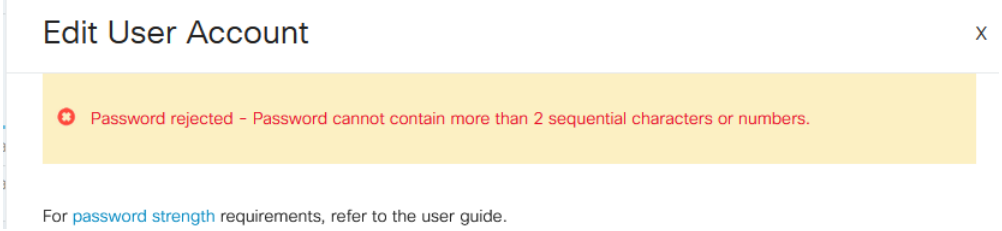
Novas regras **NÃO PODEM** ser desativadas.
Ele verificará se a senha não é de uma lista de senhas comuns conhecidas. Essa lista de senhas comuns foi compilada escolhendo as 10.000 senhas mais usadas de uma lista das 10.000.000 senhas mais comuns. Esta lista pode ser encontrada no link **github**.
Nenhuma variação das senhas comuns usando maiúsculas/minúsculas ou usando as seguintes substituições de caracteres:
"$" para "s", "@" para "a", "0" para "o", "1" para "l", "!" para "i", "3" para "e"
Ele bloqueará senhas que incluam mais de dois caracteres sequenciais seguidos (novamente procurando substituições comuns e maiúsculas/minúsculas). Por exemplo, se uma senha contiver *abc*, ela será bloqueada porque tem três letras sequenciais. Assim como *@bc*, já que existe a substituição comum do símbolo @ por um símbolo. Da mesma forma, o *cba* será bloqueado porque é sequencial na ordem inversa. Outros exemplos incluem "efg123!$", "abcd765%", "kji!$378", "qr$58!230".
A nova senha não deve conter o nome de usuário. Por exemplo, no "Admin548" para admin de usuário.
A nova senha não deve conter o nome do fabricante. Por exemplo, no C!sc0IsCool.
A nova senha não deve conter o nome do produto. Por exemplo, no CBSCo0l$witch

Mensagens de erro

Se tentar usar uma senha que esteja no dicionário ou contenha senhas comumente usadas, você verá a seguinte mensagem de erro.



Se você usar uma senha que contenha caracteres sequenciais, receberá novamente a seguinte mensagem de erro.

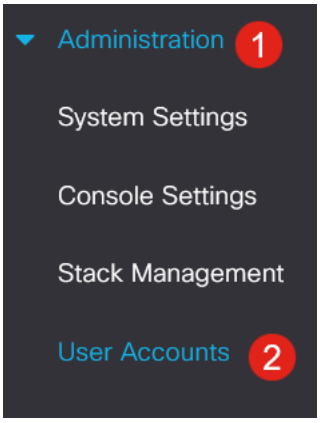


Gerador de Senha

Para ajudá-lo a criar senhas válidas durante a criação de novos usuários ou a edição de usuários existentes, um gerador aleatório de senhas foi criado na interface de usuário da Web do switch.

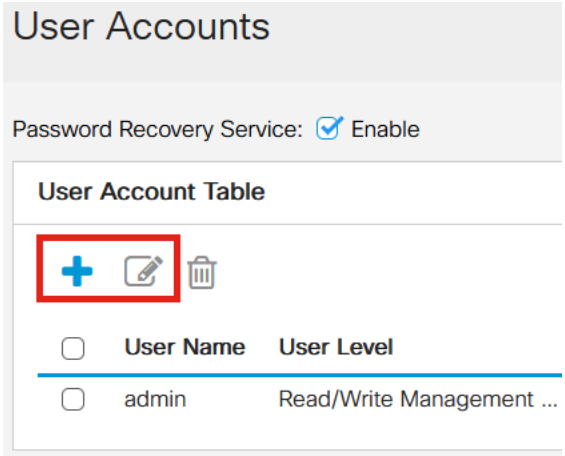
Passo 1

Vá para **Administração > Contas de usuário**.



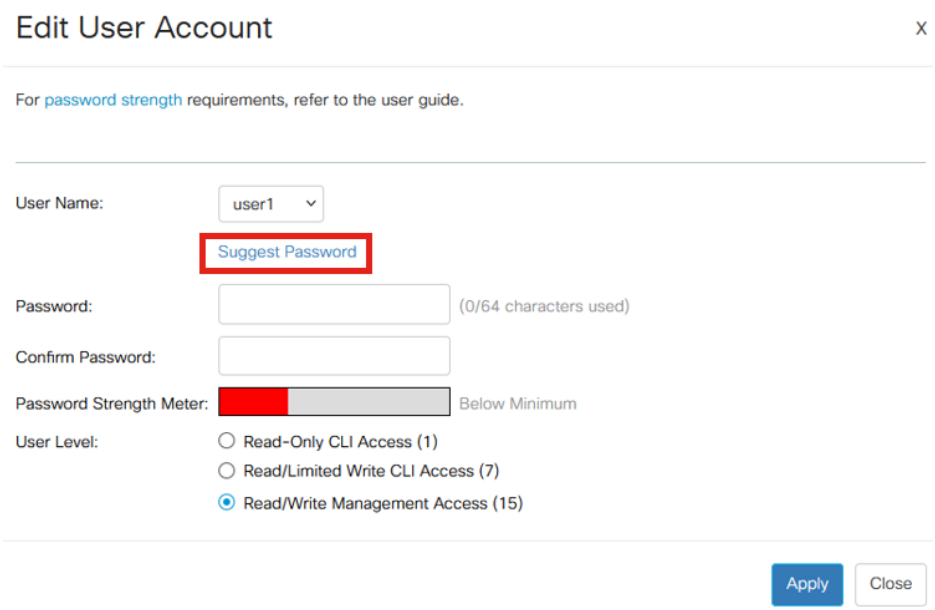
Passo 2

Adicione ou *edite* uma conta de usuário.



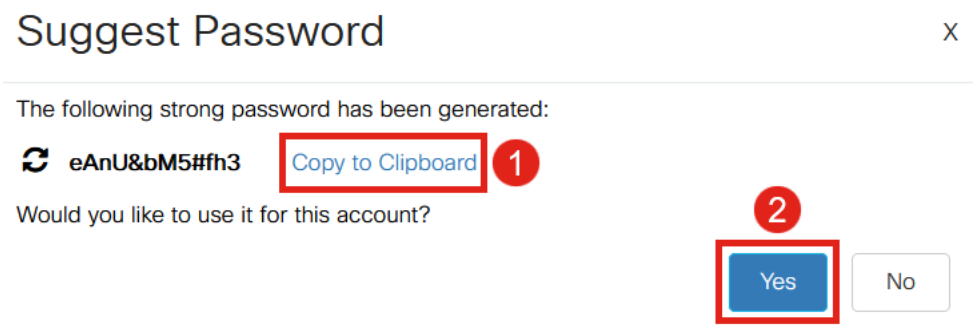
Etapa 3

Clique no link **Sugerir senha**.



Passo 4

Será aberta uma página com a sugestão de senha, e você poderá copiar esta nova senha para a área de transferência. Para usar a senha da conta, basta clicar em **Sim**.



ÉMUITO importante que você copie essa senha para a área de transferência antes de dizer Sim para usá-la para a conta. Se você não salvar essa senha antes de dizer sim, não poderá descobrir qual é a senha e é improvável que se lembre dela. Salve a senha copiada em um documento em um local seguro.

Esse processo irá gerar uma senha válida, mas é possível que a senha que ele gera não seja uma senha "forte" de acordo com o medidor de força da senha. Se ele informar que a senha é "Fraca", você poderá tentar outra senha sugerida ou adicionar caracteres ao final da string.

Conclusão

Agora você sabe tudo sobre as atualizações de configuração de senha no Cisco Business Switches Firmware 3.2.0.84