

# Configurar a força da senha e as configurações de complexidade no switch

## Objetivo

Na primeira vez que você fizer login no utilitário baseado na Web do seu switch, será necessário usar o nome de usuário e a senha padrão, que são: cisco/cisco. Em seguida, é necessário inserir e configurar uma nova senha para a conta da cisco. A complexidade da senha é habilitada por padrão. Se a senha escolhida não for complexa o suficiente, você será avisado para criar outra senha.

Como as senhas são usadas para autenticar os usuários que acessam o dispositivo, senhas simples são possíveis perigos à segurança. Portanto, os requisitos de complexidade de senha são aplicados por padrão e podem ser configurados conforme necessário.

Este artigo fornece instruções sobre como definir regras de complexidade de senha nas contas de usuário em seu switch.

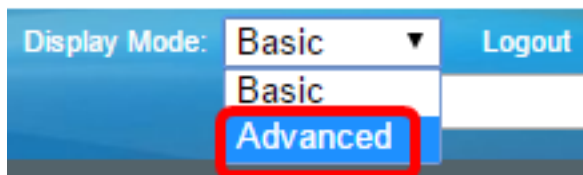
## Dispositivos aplicáveis | Versão do software

- Sx250 | 2.2.5.68 ([Baixe o mais recente](#))
- Sx300 Series | 1.4.7.05 ([Baixe o mais recente](#))
- Sx350 Series | 2.2.5.68 ([Baixe o mais recente](#))
- SG350X Series | 2.2.5.68 ([Baixe o mais recente](#))
- Sx550X Series | 2.2.5.68 ([Baixe o mais recente](#))

## Configurar a força da senha e as configurações de complexidade no switch

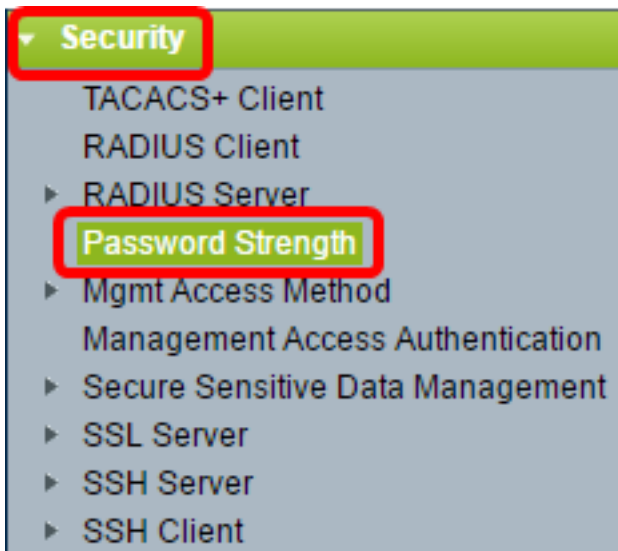
Etapa 1. Efetue login no utilitário baseado na Web do seu switch e escolha **Avançado** na lista suspensa Modo de exibição.

**Note:** Neste exemplo, foi usado o switch SG350X-48MP.

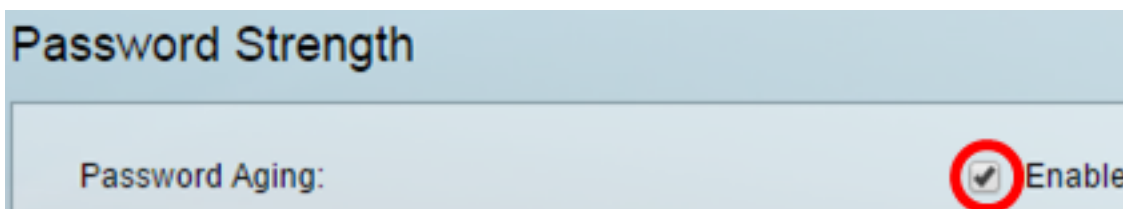


**Note:** Se você tiver um switch Sx300 Series, vá para a [Etapa 2](#).

[Etapa 2](#). Escolha **Security > Password Strength**.



Etapa 3. (Opcional) Desmarque a caixa de seleção **Habilitar** vencimento de senha para desabilitar o recurso de envelhecimento de senha. Se esta opção estiver ativada, o usuário será solicitado a alterar a senha quando o tempo de envelhecimento da senha especificado expirar. Este recurso é ativado por padrão.



Etapa 4. Insira o número de dias que podem decorrer antes que o usuário seja solicitado a alterar a senha. O valor padrão é 180 e o intervalo é de 1 a 356 dias. Neste exemplo, 90 é usado.

**Note:** Se você desabilitou esse recurso na Etapa 3, vá para a [Etapa 5](#).



**Note:** O envelhecimento de senha também se aplica a comprimento zero ou nenhuma senha.

[Etapa 5](#). (Opcional) Marque a caixa de seleção **Password Complexity Settings** para ativar regras de complexidade para senhas. Se esse recurso foi ativado, as novas senhas devem estar de acordo com as seguintes configurações padrão:

- Ter um tamanho mínimo de oito caracteres.
- Contém caracteres de pelo menos três classes de caracteres (letras maiúsculas, letras minúsculas, números e caracteres especiais disponíveis em um teclado padrão).
- Ser diferentes da senha atual.
- Não conter um caractere repetido mais de três vezes consecutivas.
- Não repetir ou inverter o nome do usuário ou qualquer variante alcançada alternando entre letras maiúsculas e minúsculas.
- Não repetir ou inverter o nome do fabricante ou qualquer variante alcançada alternando entre letras maiúsculas e minúsculas.



**Note:** Se você não quiser habilitar as Configurações de complexidade de senha, vá para a [Etapa](#)

## 10.

Etapa 6. (Opcional) Insira o número mínimo de caracteres necessários para as senhas no campo *Tamanho mínimo da senha*. O valor padrão é 8 e o intervalo é de 0 a 64 caracteres.

**Note:** Um comprimento zero ou nenhuma senha é permitida e ainda pode ter a senha envelhecida atribuída a ela.

Password Complexity Settings:  Enable

---

Minimal Password Length:

**Note:** Neste exemplo, 12 é usado.

Passo 7. Digite o número de vezes que um caractere pode ser repetido no campo *Repetição de Caracteres Permitida*. O valor padrão é 3, e o intervalo é de 0 a 16 instâncias.

Allowed Character Repetition:

**Note:** Neste exemplo, 2 é usado.

Etapa 8. Digite o número de classes de caracteres que devem estar presentes em uma senha. Até quatro classes de caracteres distintas podem ser aplicadas para senhas. O valor padrão é 3 e o intervalo é de 0 a 4 classes de caracteres.

As aulas são:

- 1 — Caso mais baixo
- 2 — Caso superior
- 3 — Dígitos ou Números
- 4 — Símbolos ou caracteres especiais

Minimal Number of Character Classes:

**Note:** Neste exemplo, 4 é usado.

Etapa 9. (Opcional) Marque a caixa de seleção **Habilitar** a nova senha deve ser diferente da atual para exigir uma senha exclusiva após a alteração da senha.

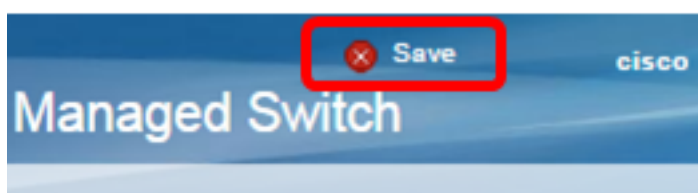
The New Password Must Be Different Than the Current One:  Enable

[Etapa 10.](#) Clique em Apply.

## Password Strength

Password Aging:	<input checked="" type="checkbox"/> Enable
✱ Password Aging Time:	<input type="text" value="90"/>
Password Complexity Settings:	<input checked="" type="checkbox"/> Enable
✱ Minimal Password Length:	<input type="text" value="12"/>
✱ Allowed Character Repetition:	<input type="text" value="2"/>
✱ Minimal Number of Character Classes:	<input type="text" value="4"/>
	Up to four distinct character classes: upper case, lower case, number, and special character.
The New Password Must Be Different Than the Current One:	<input checked="" type="checkbox"/> Enable

Etapa 11. (Opcional) Clique em **Salvar** para salvar as configurações no arquivo de configuração de inicialização.



Agora você deve ter configurado com êxito as configurações de intensidade e complexidade da senha do switch.

Para obter mais informações, incluindo links para todos os artigos relacionados à sua série de switches, consulte a página de produto apropriada:

- [Página de produto dos switches 250 Series](#)
- [Página de produto dos switches 300 Series](#)
- [Página de produto dos switches 350 Series](#)
- [Página de produto dos switches 350X Series](#)
- [Página de produto dos switches 550 Series](#)
- [Página de produto dos switches 550X Series](#)