Configurar o servidor RADIUS (Remote Authentication Dial-In User Service) em um switch

Objetivo

O Remote Authentication Dial-In User Service (RADIUS) é um protocolo de rede que fornece gerenciamento centralizado de Autenticação, Autorização e Contabilidade (AAA ou Triple A) para usuários que se conectam e usam um serviço de rede. Um servidor RADIUS regula o acesso à rede verificando a identidade dos usuários através das credenciais de login inseridas. Por exemplo, uma rede Wi-Fi pública é instalada em um campus universitário. Apenas os alunos que têm a senha podem acessar essas redes. O servidor RADIUS verifica as senhas inseridas pelos usuários e permite ou nega o acesso conforme apropriado.

A configuração de um servidor RADIUS é útil para melhorar a segurança, pois ele autentica antes de autorizar um cliente ou usuário a obter acesso à rede. O servidor RADIUS responde a problemas do cliente relacionados à disponibilidade, retransmissão e timeouts do servidor. O servidor RADIUS também lida com solicitações de conexão de usuários, autentica o usuário e envia as informações de configuração necessárias ao cliente para fornecer serviços ao usuário.

O servidor RADIUS é um servidor que centraliza o controle de uma rede feita de dispositivos habilitados para RADIUS. Os servidores RADIUS baseiam suas decisões de encaminhamento em endereços 802.1X ou Media Access Control (MAC).

Este artigo explica como configurar as configurações de RADIUS nos switches Sx350, SG350X e Sx550X Series.

Dispositivos aplicáveis

- Sx350 Series
- SG350X Series
- Sx550X Series

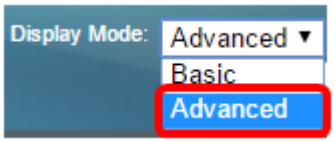
Versão de software

- 2.2.5.68

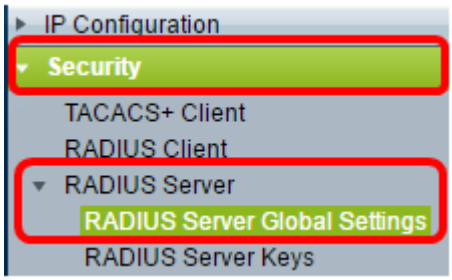
Configurar o servidor RADIUS

Definir configurações globais do servidor RADIUS

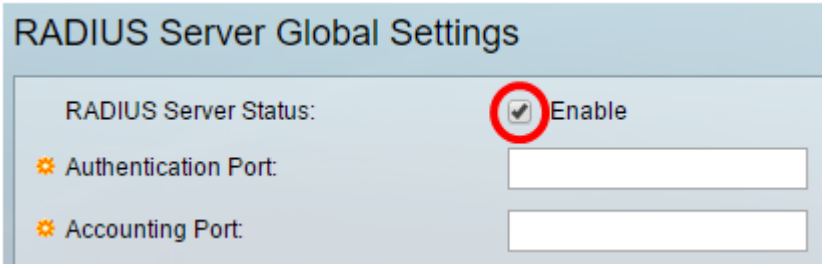
Etapa 1. Efetue login no utilitário baseado na Web do switch e escolha **Avançado** na lista suspensa Modo de exibição.



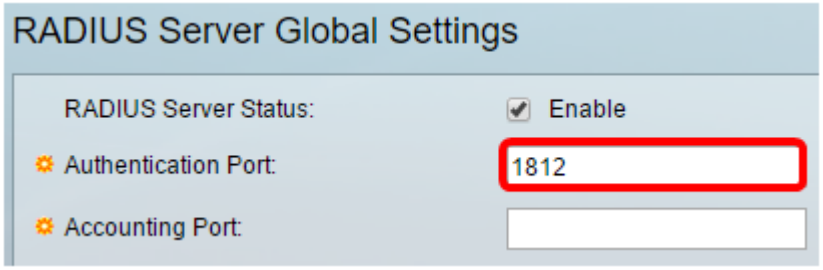
Etapa 2. Escolha **Security > RADIUS Server > RADIUS Server Global Settings**.



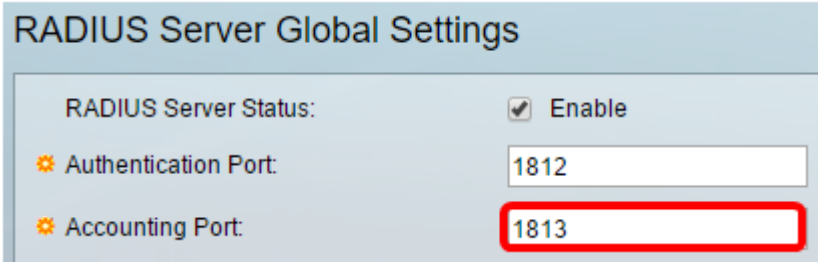
Etapa 3. Marque a caixa de seleção **Enable (Habilitar)** para RADIUS Server Status (Status do servidor RADIUS).



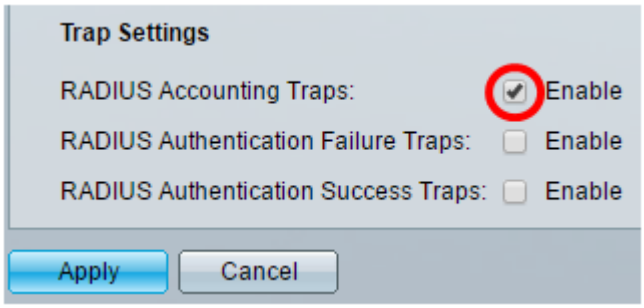
Etapa 4. Insira o número da porta UDP (User Datagram Protocol) da porta do servidor RADIUS para solicitações de autenticação. O intervalo vai de 1 a 65535 e o padrão é 1812.



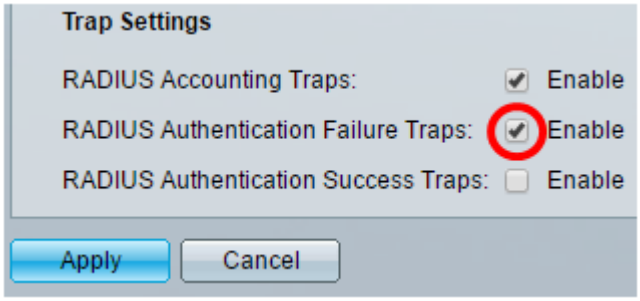
Etapa 5. Insira o número da porta UDP da porta do servidor RADIUS para solicitações de contabilização. O intervalo vai de 1 a 65535 e o padrão é 1813.



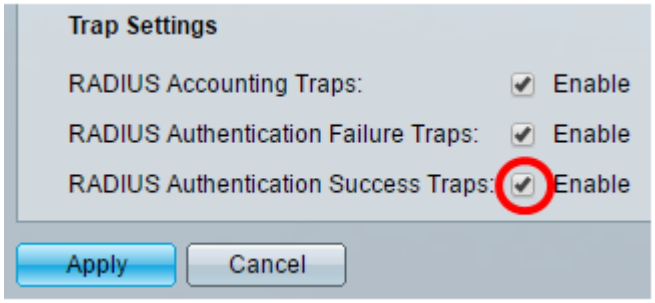
Etapa 6. (Opcional) Para gerar armadilhas para eventos de contabilidade RADIUS, marque a caixa de seleção **Enable** para RADIUS Accounting Traps em Trap Settings (Configurações de interceptação).



Passo 7. (Opcional) Para gerar armadilhas para logins que falharam, marque a caixa de seleção **Habilitar** para armadilhas de falha de autenticação RADIUS.



Etapa 8. (Opcional) Para gerar armadilhas para logins bem-sucedidos, marque a caixa de seleção **Enable** para RADIUS Authentication Success Traps.



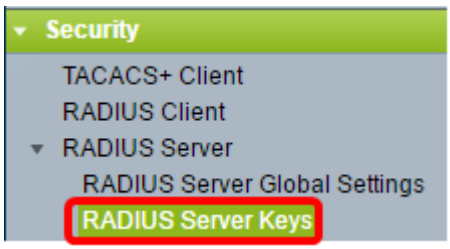
Etapa 9. Clique em Apply.

Etapa 10. Um  ícone indica que a configuração foi salva com êxito. Para salvar permanentemente a configuração, vá para a página Operações de arquivo ou clique no 

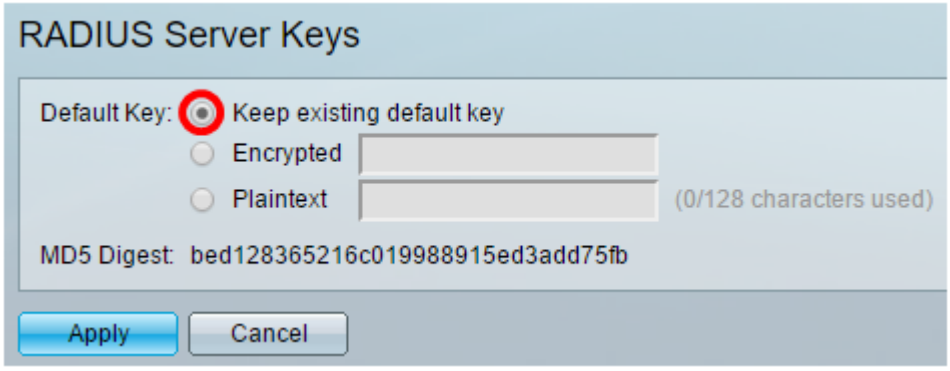
ícone na parte superior da página. Caso contrário, clique em **Fechar**.

Configurar chaves de servidor RADIUS

Etapa 1. Escolha **RADIUS Server Keys** em RADIUS Server.



Etapa 2. (Opcional) Insira a chave RADIUS padrão, se necessário. Os valores inseridos na chave padrão são aplicados a todos os servidores configurados (na página Adicionar servidor RADIUS) para usar a chave padrão.



Default Key — (Chave padrão) Escolha a string de chave padrão que deseja usar para autenticação e criptografia entre o dispositivo e o cliente RADIUS. As opções são:

- Manter chave padrão existente — Para servidores especificados, o dispositivo tenta autenticar o cliente RADIUS usando a String de Chave padrão existente.
- Criptografado — Para criptografar as comunicações usando o algoritmo Message Digest 5 (MD5), insira a chave na forma criptografada.
- Texto sem formatação — Digite a sequência de caracteres no modo de texto sem formatação.

MD5 Digest — Exibe o resumo MD5 da senha digitada pelo usuário.

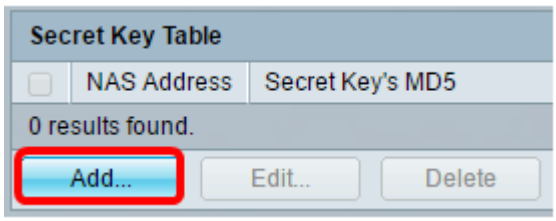
Note: Neste exemplo, a opção Manter chave padrão existente em Chave padrão é selecionada.

Etapa 3. Clique em Apply.

Etapa 4. Um  ícone indica que a configuração foi salva com êxito. Para salvar permanentemente a configuração, vá para a página Operações de arquivo ou clique no 

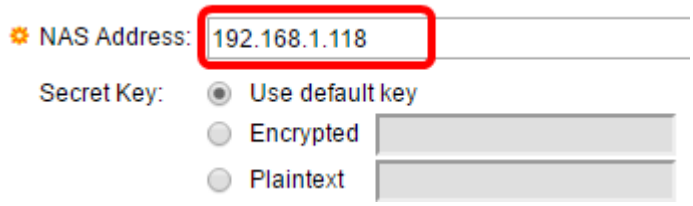
ícone na parte superior da página.

Etapa 5. (Opcional) Na área Tabela de chaves secretas, clique no botão **Adicionar** para adicionar uma chave secreta.



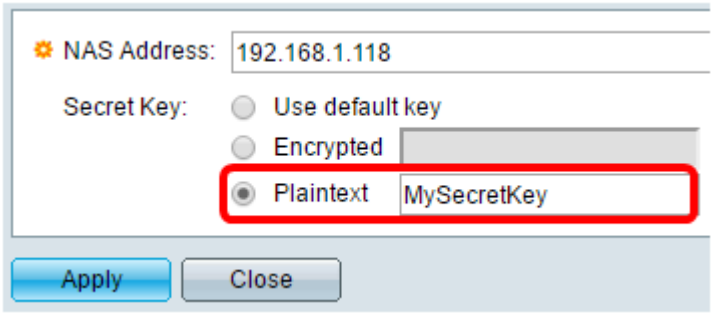
Etapa 6. Insira o endereço IP do NAS ou o switch que contém o cliente RADIUS no campo *NAS Address*.

Note: Na imagem abaixo, 192.168.1.118 é usado como um exemplo do endereço IP.



Passo 7. Escolha sua chave secreta preferida.

Note: Na imagem abaixo, Texto sem formatação é escolhido como exemplo.



As opções são:

- Usar chave padrão — Para servidores especificados, o dispositivo tenta autenticar o cliente RADIUS usando a String de Chave padrão existente.
- Criptografado — Para criptografar comunicações usando MD5, insira a chave na forma criptografada.
- Texto sem formatação — Digite a sequência de caracteres no modo de texto sem formatação. Você pode digitar até 128 caracteres.

Etapa 8. Clique em Apply.

Etapa 9. Um  ícone indica que a configuração foi salva com êxito. Para salvar permanentemente a configuração, vá para a página Operações de arquivo ou clique no 

ícone na parte superior da página. Caso contrário, clique em **Fechar**.

Configurar grupos de servidores RADIUS

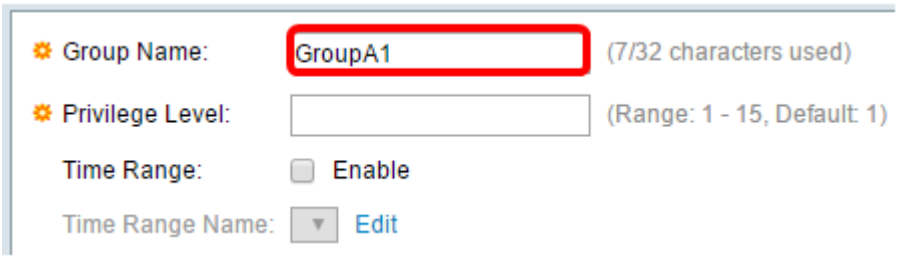
Os grupos de servidores RADIUS são um grupo de usuários que usarão o dispositivo como seu servidor RADIUS. Para configurar um grupo, siga as instruções abaixo:

Etapa 1. Escolha **RADIUS Server Groups** em RADIUS Server.

Etapa 2. Clique no botão **Add** na tabela RADIUS Server Group.

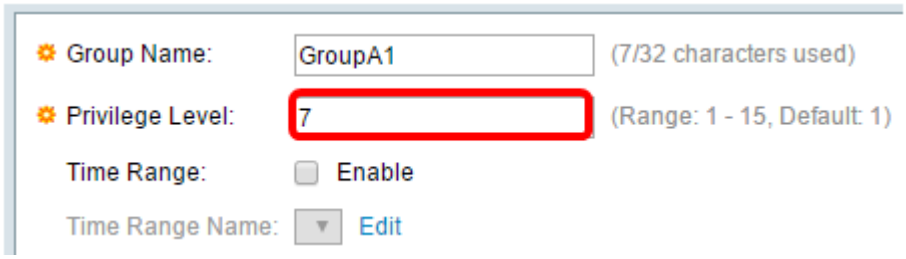
Etapa 3. Na janela pop-up, insira um nome para o grupo no campo *Nome do grupo*. Você pode digitar até 32 caracteres.

Note: Na imagem abaixo, GroupA1 é usado como exemplo.



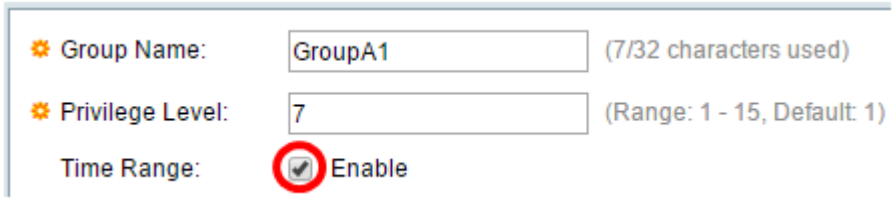
Etapa 4. Insira o nível de privilégio que deseja atribuir ao grupo. O nível de privilégio determina o nível de acesso que você atribuirá a cada grupo criado. Você pode definir os níveis de 1 a 15. O valor padrão é 1.

Note: Neste exemplo, 7 é usado.



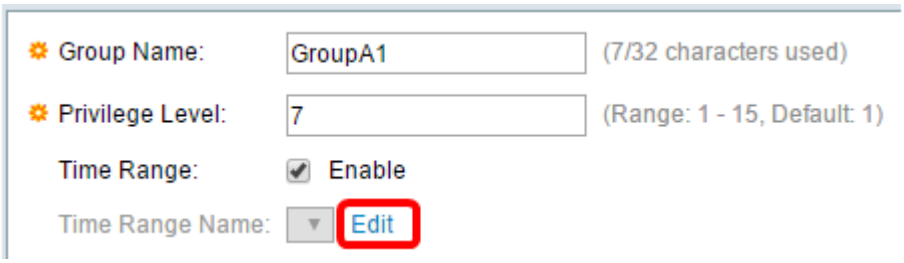
- 1 (Read-Only CLI Access) — Os usuários do grupo não podem acessar a GUI e só podem acessar comandos CLI que não alteram a configuração do dispositivo.
- 7 (Read/Limited Write CLI Access) — Os usuários do grupo não podem acessar a GUI e só podem acessar alguns comandos CLI que alteram a configuração do dispositivo. Consulte o guia de referência da CLI para obter mais informações.
- 15 (Read/Write Management Access) — Os usuários do grupo podem acessar a GUI e podem configurar o dispositivo.

Etapa 5. (Opcional) Se quiser aplicar um intervalo de tempo para esse grupo, marque a caixa de seleção **Habilitar** para o Intervalo de tempo. Caso contrário, vá para o passo 15.

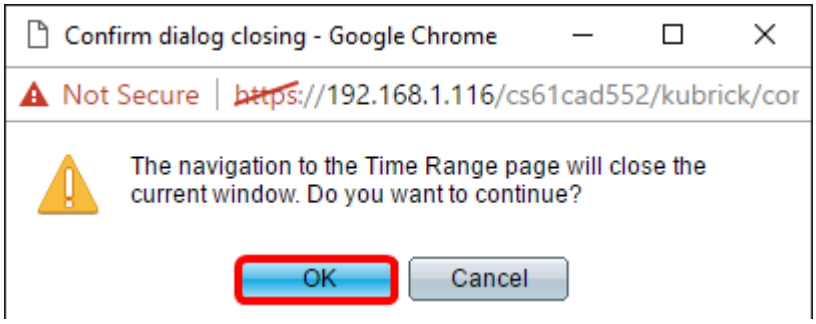


Etapa 6. Clique no link **Editar** ao lado de Nome do intervalo de tempo para definir as

configurações de Hora.

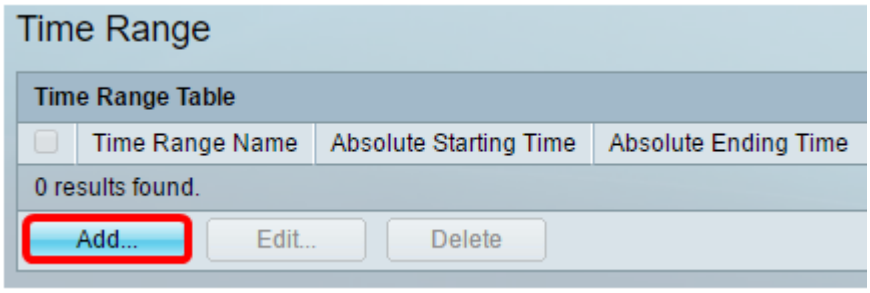


Passo 7. Uma janela pop-up será exibida informando que a janela atual será fechada para que você possa continuar com as configurações de Intervalo de tempo. Click **OK**.



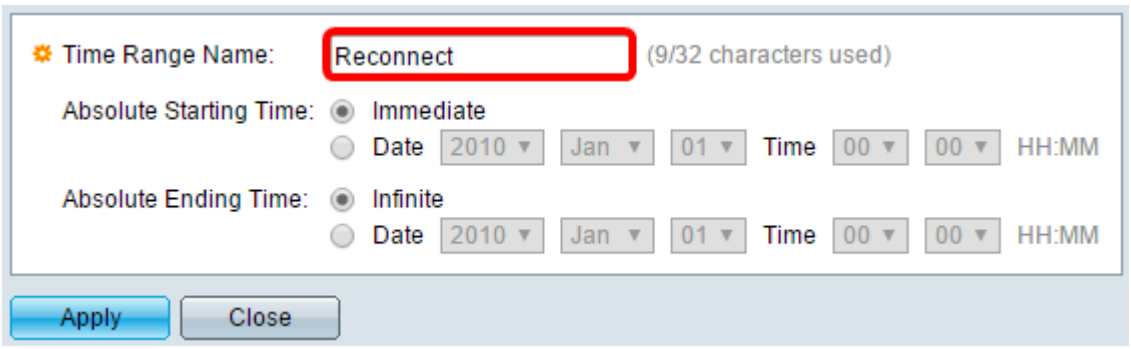
Em seguida, você será direcionado à página Intervalo de tempo.

Etapa 8. Clique no botão **Adicionar** em Tabela de intervalo de tempo.

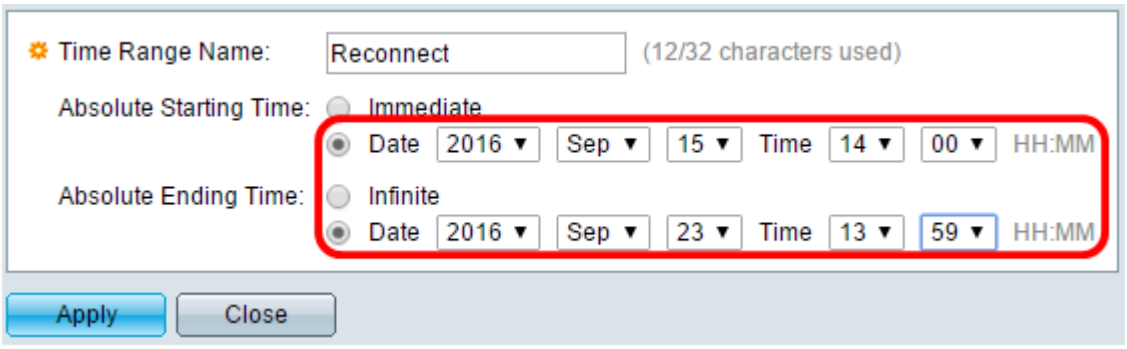


Etapa 9. Insira um nome para o Intervalo de tempo no campo *Nome do intervalo de tempo*.

Note: Na imagem abaixo, Reconnect é usado como exemplo.



Etapa 10. Escolha sua hora de início e término absoluta preferida clicando no botão de opção.



- Hora de início absoluta — Para definir a hora de início, escolha uma das seguintes opções:
- Imediato — Escolha esta opção se quiser que o intervalo de tempo comece imediatamente.
- Data, Hora — Escolha esta opção se quiser especificar a data e a hora em que o Intervalo de Tempo começa.
- Hora de término absoluta — Para definir a hora de início, escolha uma das seguintes opções:
- Infinito — Escolha isso se quiser que o intervalo de tempo nunca termine.
- Data, Hora — Escolha esta opção se quiser especificar a data e a hora em que o Intervalo de Tempo termina.

Note: Neste exemplo, Data e hora são escolhidas.

Etapa 11. Clique em Apply.

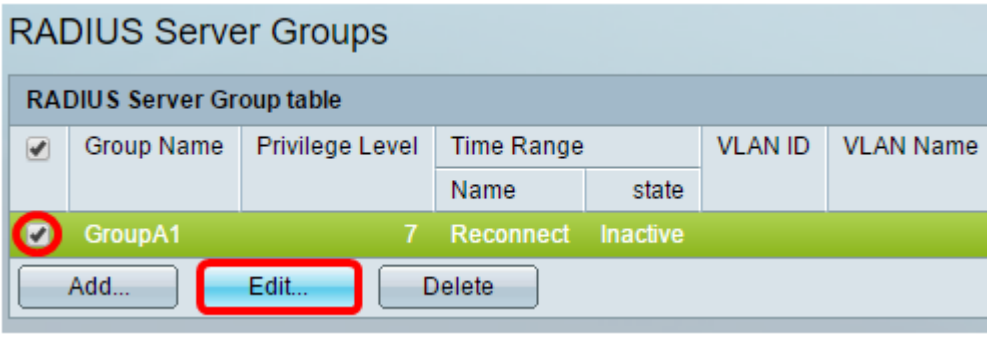
Etapa 12. Um  ícone indica que a configuração foi salva com êxito. Para salvar permanentemente a configuração, vá para a página Operações de arquivo ou clique no 

ícone na parte superior da página. Caso contrário, clique em **Fechar**.

Você será direcionado para a página principal.

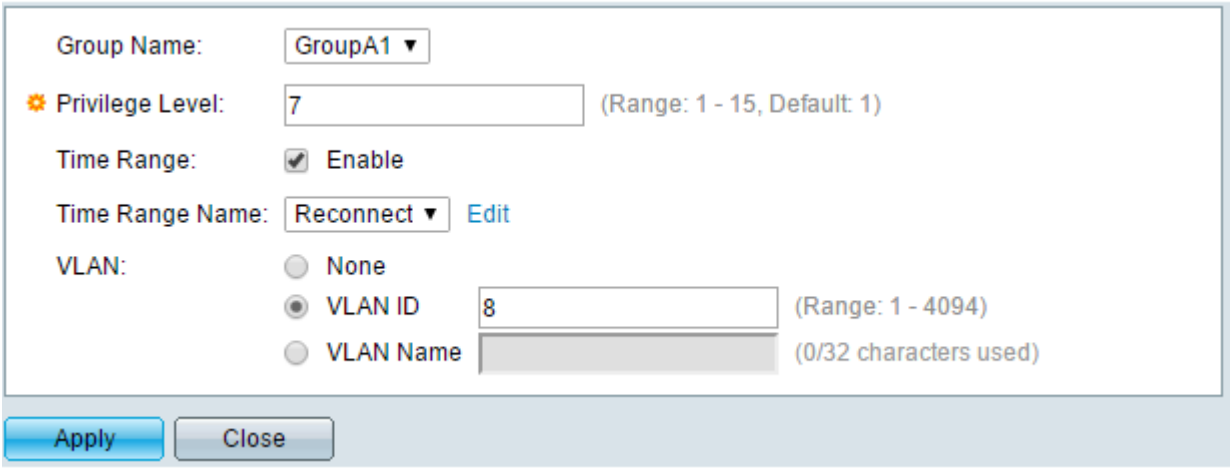
Etapa 13. Clique em **RADIUS Server Groups** novamente em RADIUS Server.

Etapa 14. O grupo recém-criado agora aparecerá na tabela RADIUS Server Group. Marque a caixa ao lado do nome do grupo e clique em **Editar**.



Etapa 15. (Opcional) Escolha a VLAN para o grupo. As opções são:

- Nenhum — Nenhuma VLAN especificada.
- VLAN ID — Especifique um ID de VLAN.
- Nome da VLAN — Especifique um nome de VLAN.



Note: Neste exemplo, a VLAN ID 8 é usada.

Etapa 16. Clique em Apply.

Etapa 17. Um  ícone indica que a configuração foi salva com êxito. Para salvar permanentemente a configuração, vá para a página Operações de arquivo ou clique no 

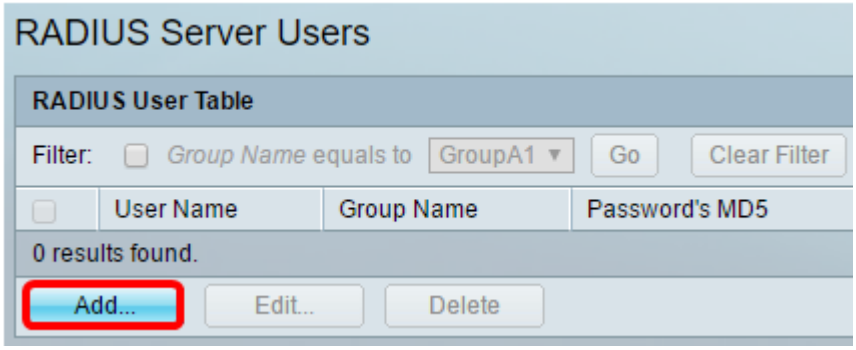
ícone na parte superior da página. Caso contrário, clique em **Fechar**.

Configurar usuários do servidor RADIUS

Para adicionar usuários ao grupo criado anteriormente:

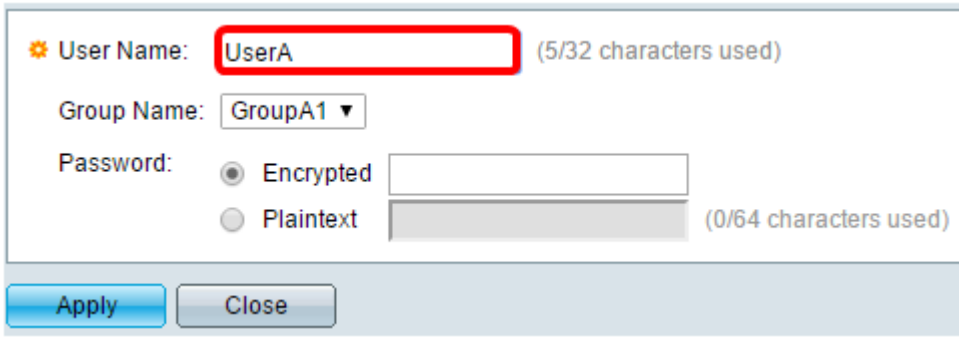
Etapa 1. Clique em **RADIUS Server Users** em RADIUS Server.

Etapa 2. Clique no botão **Add (Adicionar)** em RADIUS User Table (Tabela de usuários RADIUS).

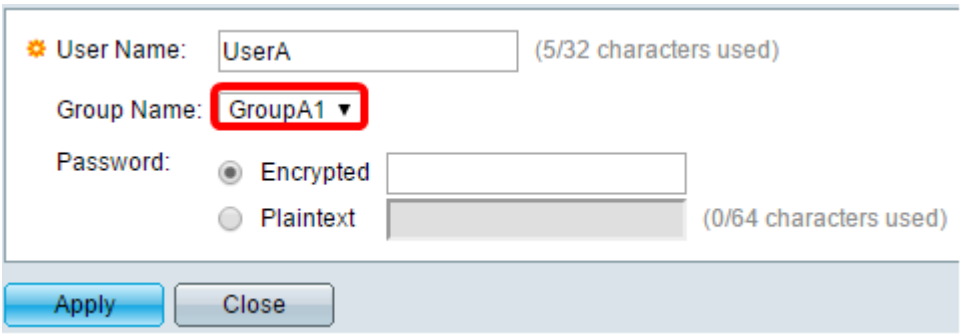


Etapa 3. Digite o nome do usuário no campo *Nome de usuário*.

Note: Neste exemplo, UserA é usado.

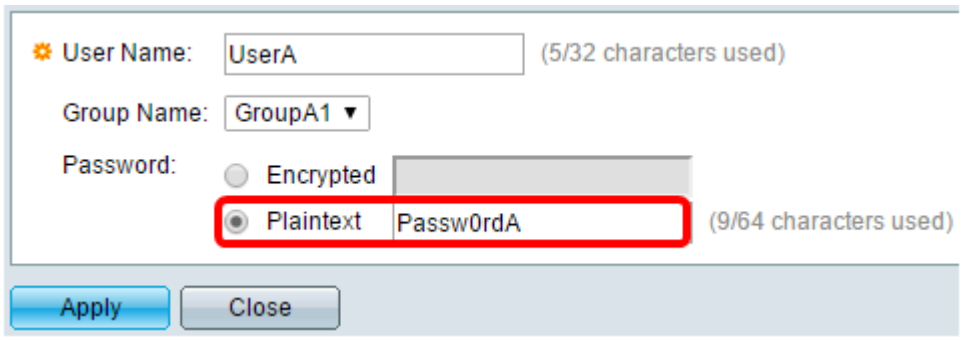


Etapa 4. Escolha o grupo ao qual o usuário pertence na lista suspensa Nome do grupo.



Etapa 5. Clique em um botão de opção na área Senha.

Etapa 6. Digite sua senha preferida.



- Criptografado — Uma sequência de chaves é usada para criptografar comunicações usando MD5. Para usar criptografia, insira a chave no formato criptografado.
- Texto sem formatação — Se você não tiver uma string de chave criptografada (de outro dispositivo), digite a string de chave no modo texto sem formatação. A string de chave

criptografada é gerada e exibida.

Note: Neste exemplo, Texto simples é escolhido.

Etapa 6. Clique em Apply.

Passo 7. Um  ícone indica que a configuração foi salva com êxito. Para salvar permanentemente a configuração, vá para a página Operações de arquivo ou clique no 

ícone na parte superior da página. Caso contrário, clique em **Fechar**.

Agora você deve ter configurado com êxito as configurações do servidor RADIUS no switch.