Configurar a autenticação de porta 802.1x em um switch

Objetivo

O IEEE 802.1x é um padrão que facilita o controle de acesso entre um cliente e um servidor. Antes que os serviços possam ser fornecidos a um cliente por uma LAN (Local Area Network, rede local) ou switch, o cliente conectado à porta do switch deve ser autenticado pelo servidor de autenticação que executa o RADIUS (Remote Authentication Dial-In User Service, serviço de usuário de discagem de autenticação remota).

A autenticação 802.1x restringe a conexão de clientes não autorizados a uma LAN por meio de portas acessíveis para publicidade. A autenticação 802.1x é um modelo cliente-servidor. Neste modelo, os dispositivos de rede têm as seguintes funções específicas:

Cliente ou requerente — Um cliente ou requerente é um dispositivo de rede que solicita acesso à LAN. O cliente está conectado a um autenticador.

Autenticador — Um autenticador é um dispositivo de rede que fornece serviços de rede e ao qual as portas suplicantes estão conectadas. Os seguintes métodos de autenticação são suportados:

Baseado em 802.1x — Suportado em todos os modos de autenticação. Na autenticação baseada em 802.1x, o autenticador extrai as mensagens EAP (Extensible Authentication Protocol) das mensagens 802.1x ou dos pacotes EAP sobre LAN (EAPoL) e as passa para o servidor de autenticação, usando o protocolo RADIUS.

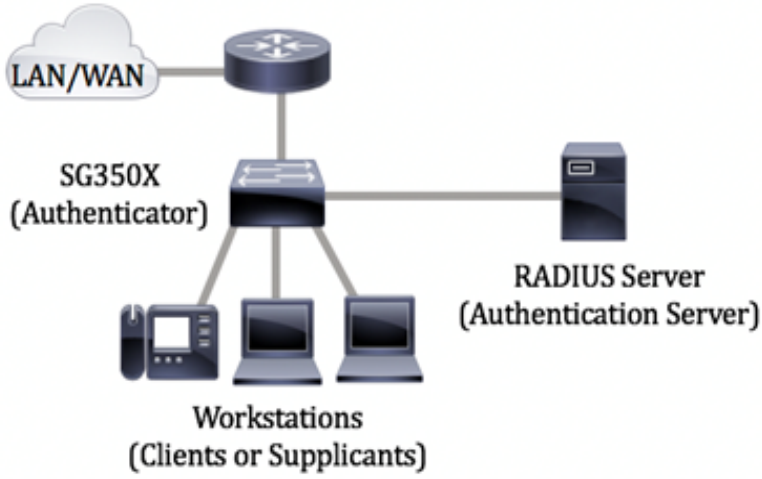
Baseado em MAC — Suportado em todos os modos de autenticação. Com base no Media Access Control (MAC), o próprio autenticador executa a parte do cliente EAP do software em nome dos clientes que buscam acesso à rede.

Baseado na Web — Suportado somente em modos de sessões múltiplas. Com a autenticação baseada na Web, o próprio autenticador executa a parte do cliente EAP do software em nome dos clientes que procuram acesso à rede.

Servidor de autenticação — Um servidor de autenticação executa a autenticação real do cliente. O servidor de autenticação do dispositivo é um servidor de autenticação RADIUS com extensões EAP.

Note: Um dispositivo de rede pode ser um cliente ou um suplicante, um autenticador ou ambos por porta.

A imagem abaixo exibe uma rede que configurou os dispositivos de acordo com as funções específicas. Neste exemplo, um switch SG350X é usado.



Diretrizes para a configuração do 802.1x:

Crie uma rede de acesso virtual (VLAN). Para criar VLANs usando o utilitário baseado na Web do switch, clique aqui. Para obter instruções baseadas na CLI, clique aqui.

Defina as configurações de porta para VLAN no switch. Para configurar usando o utilitário baseado na Web, clique aqui. Para usar a CLI, clique aqui.

Configure as propriedades 802.1x no switch. 802.1x deve ser globalmente ativado no switch para habilitar a autenticação baseada em porta 802.1x. Para obter instruções, clique aqui.

(Opcional) Configure o intervalo de tempo no switch. Para saber como configurar as definições de intervalo de tempo no comutador, clique aqui.

Configurar a autenticação de porta 802.1x. Este artigo fornece instruções sobre como configurar as configurações de autenticação de porta 802.1x em seu switch.

Para saber como configurar a autenticação baseada em mac em um switch, clique aqui.

Dispositivos aplicáveis

Sx300 Series

Sx350 Series

SG350X Series

Sx500 Series

Sx550X Series

Versão de software

1.4.7.06 — Sx300, Sx500

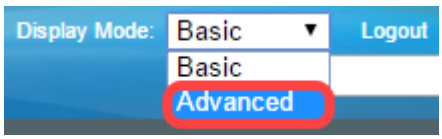
2.2.8.04 — Sx350, SG350X, Sx550X

Definir as configurações de autenticação de porta 802.1x em um switch

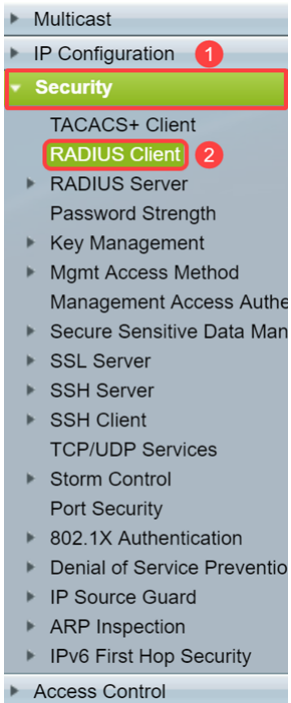
Definir configurações do cliente RADIUS

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

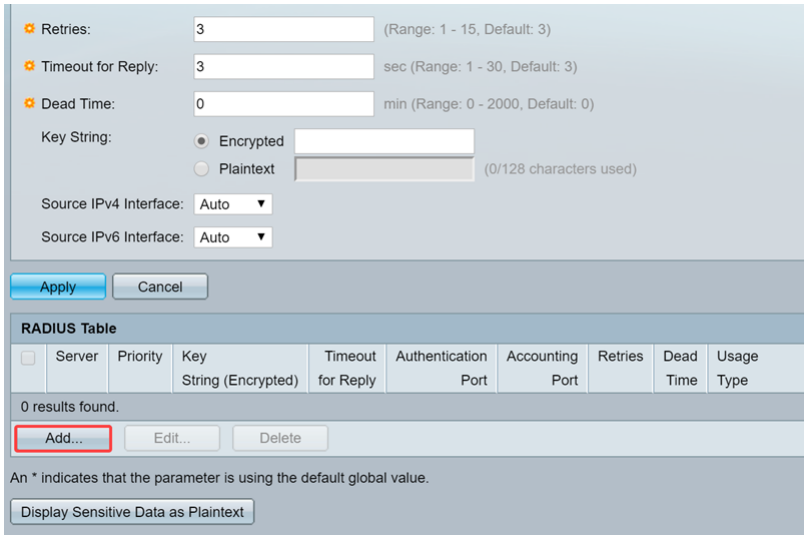
Note: As opções de menu disponíveis podem variar dependendo do modelo do dispositivo. Neste exemplo, o SG550X-24 é usado.



Etapa 2. Navegue até **Security > RADIUS Client**.

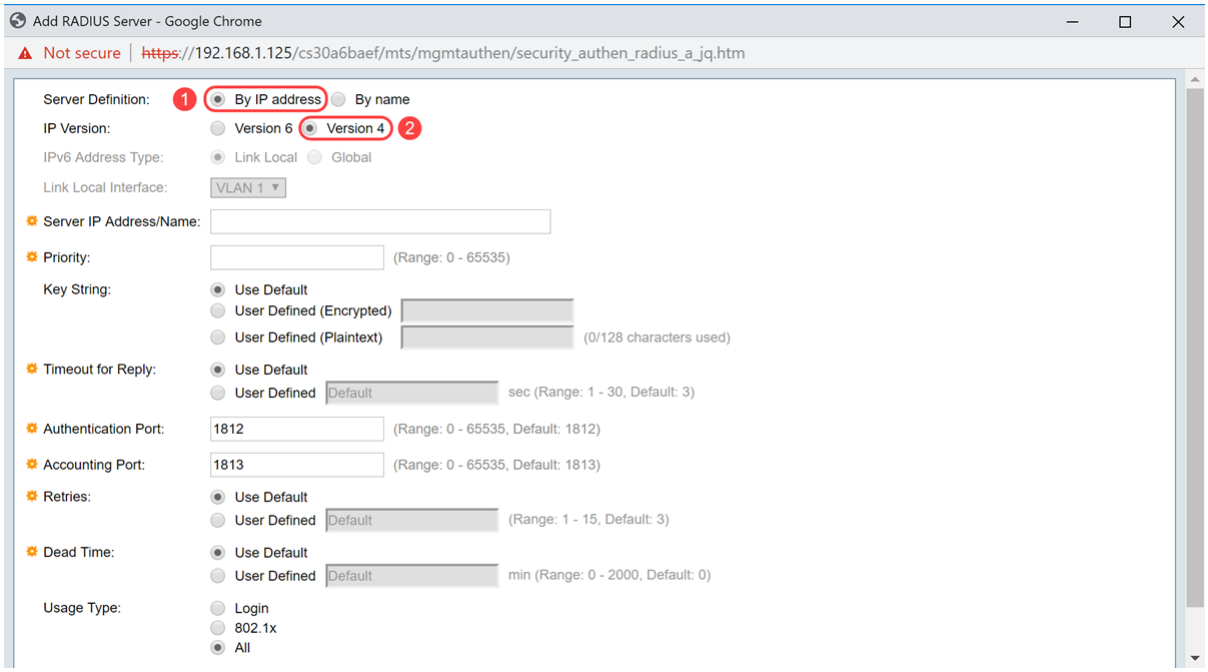


Etapa 3. Role para baixo até a seção *Tabela RADIUS* e clique em **Adicionar...** para adicionar um servidor RADIUS.



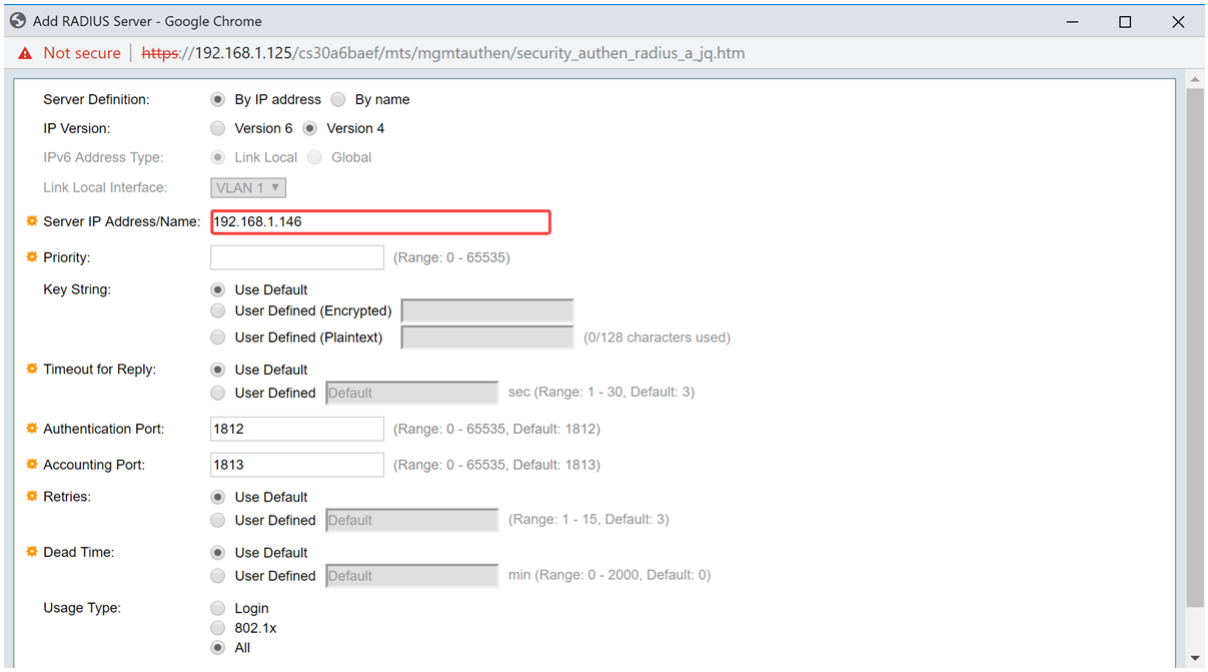
Etapa 4. Selecione se deseja especificar o servidor RADIUS por endereço IP ou nome no campo *Server Definition*. Selecione a versão do endereço IP do servidor RADIUS no campo *IP Version*.

Note: Usaremos **By IP address** e **Version 4** neste exemplo.

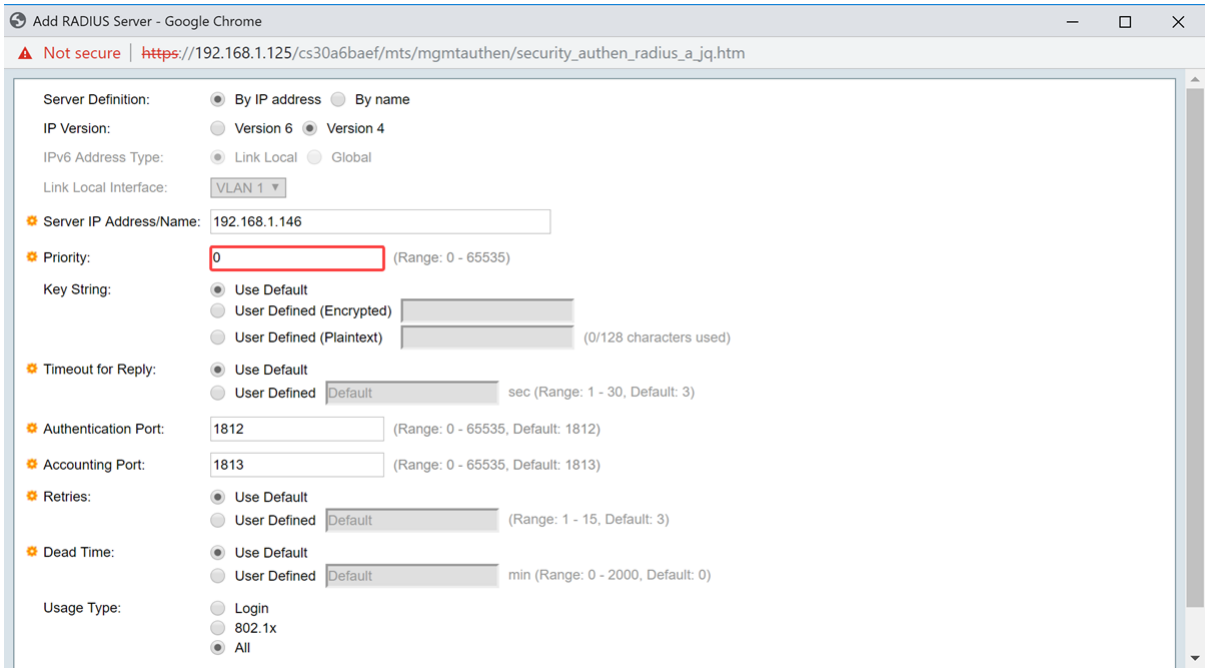


Etapa 5. Digite no servidor RADIUS por endereço IP ou nome.

Note: Digitaremos o endereço IP de **192.168.1.146** no campo *Server IP Address/Name (Endereço IP do servidor/Nome)*.



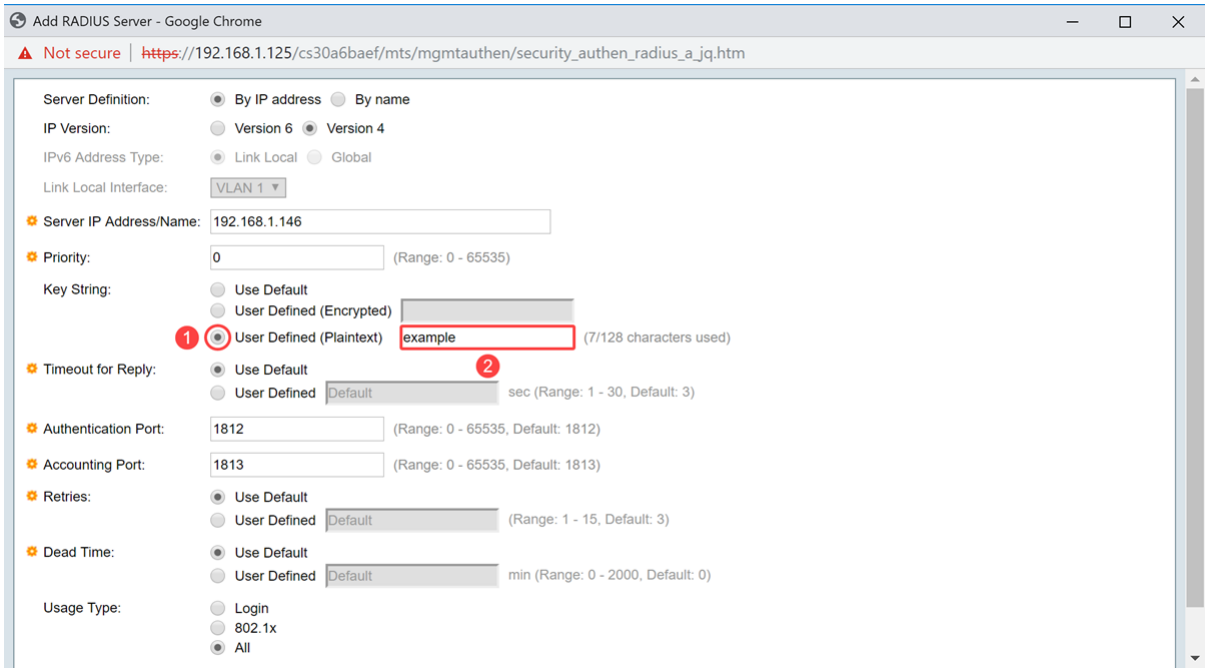
Etapa 6. Digite a prioridade do servidor. A prioridade determina a ordem em que o dispositivo tenta entrar em contato com os servidores para autenticar um usuário. O dispositivo começa com o servidor RADIUS de prioridade mais alta primeiro. 0 é a prioridade mais alta.



Passo 7. Digite a sequência de chaves usada para autenticar e criptografar a comunicação entre o dispositivo e o servidor RADIUS. Essa chave deve corresponder à chave configurada no servidor RADIUS. Ele pode ser inserido no formato **Criptografado** ou **Texto simples**. Se **Usar padrão** estiver selecionado, o dispositivo tentará autenticar no servidor RADIUS usando a string de chave padrão.

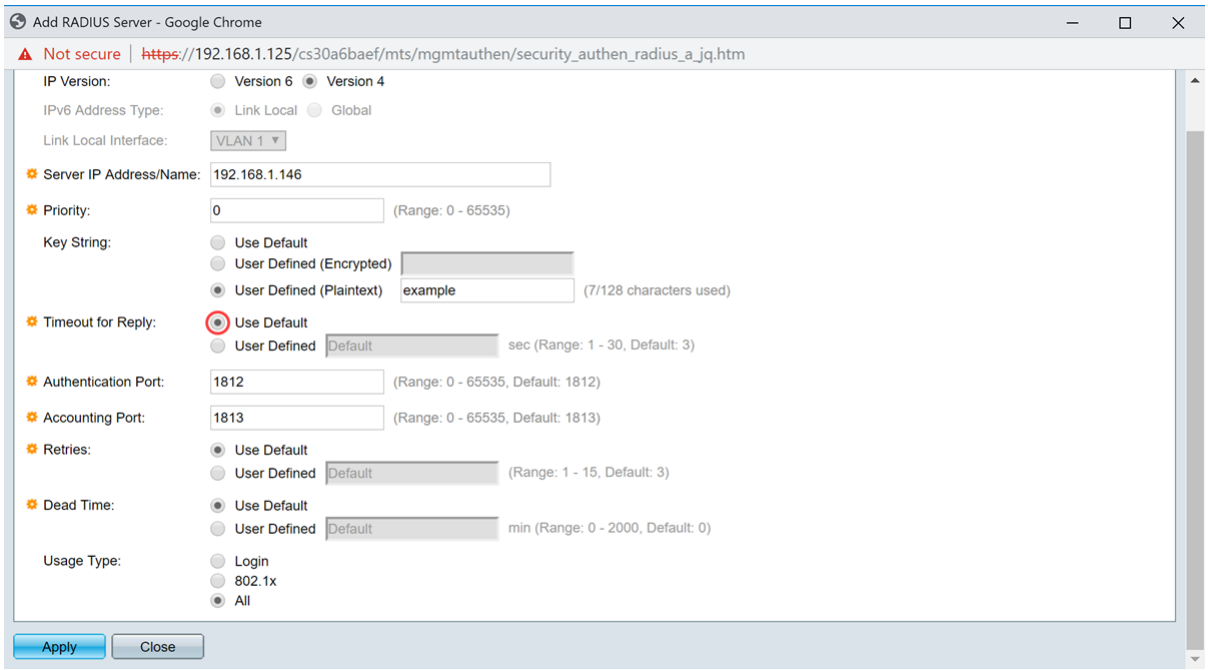
Note: Usaremos o **texto definido pelo usuário (texto simples)** e inseriremos o **exemplo** principal.

Para saber como configurar as definições do servidor RADIUS no comutador, clique aqui.



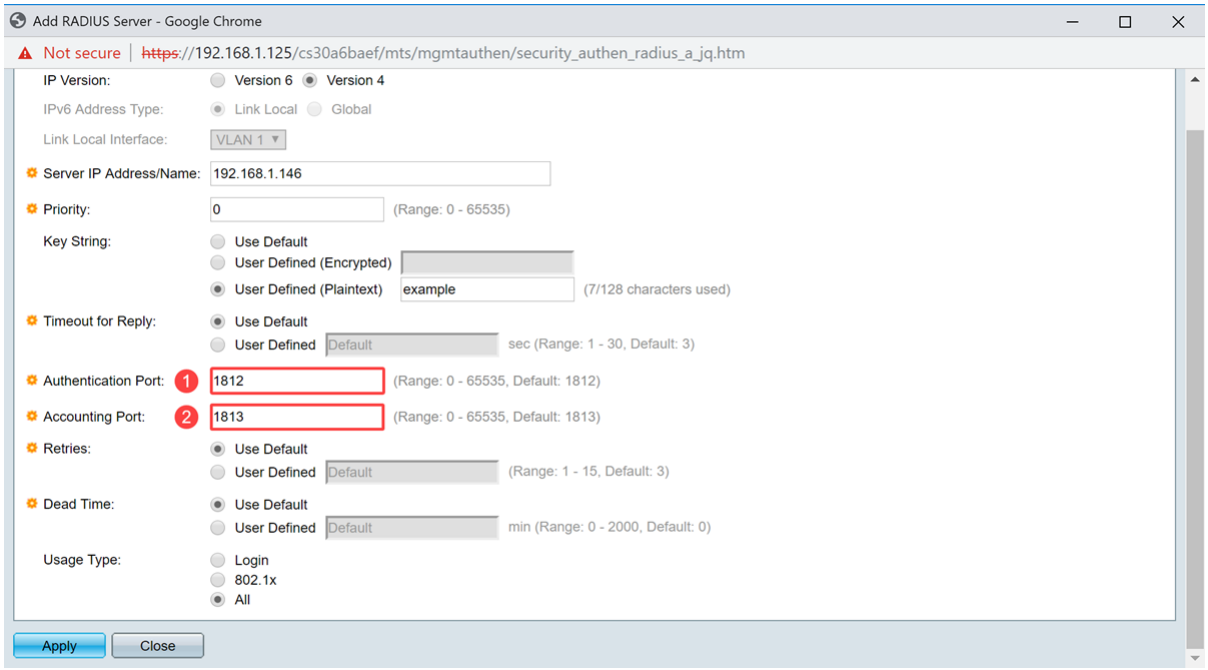
Etapa 8. No campo *Timeout for Reply*, selecione **Use Default** ou **User Defined**. Se **Definido pelo Usuário** tiver sido selecionado, digite o número de segundos que o dispositivo espera por uma resposta do servidor RADIUS antes de tentar novamente a consulta ou alternando para o próximo servidor se o número máximo de novas tentativas for feito. Se **Usar padrão** estiver selecionado, o dispositivo usará o valor de tempo limite padrão.

Note: Neste exemplo, **Usar padrão** foi selecionado.



Etapa 9. Insira o número da porta UDP da porta do servidor RADIUS para solicitação de autenticação no campo *Authentication Port (Porta de autenticação)*. Insira o número da porta UDP da porta do servidor RADIUS para solicitações de contabilização no campo *Porta de Contabilidade*.

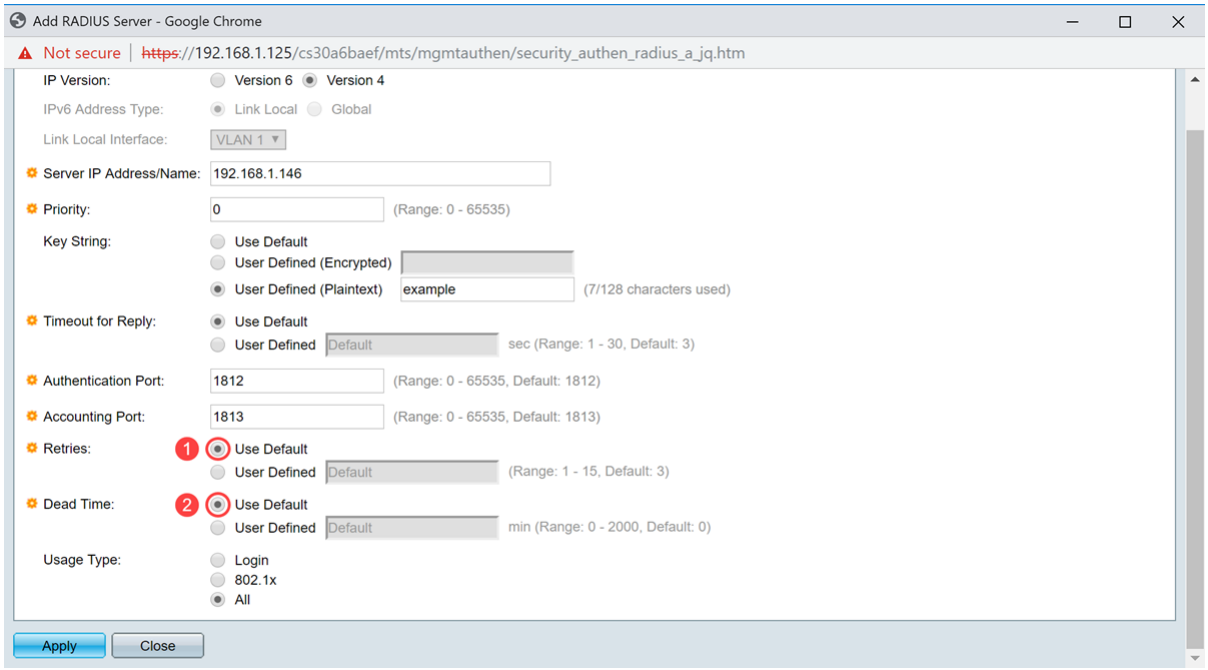
Note: Neste exemplo, usaremos o valor padrão para a porta de autenticação e a porta de contabilização.



Etapa 10. Se **Definido pelo usuário** estiver selecionado no campo *Tentativas*, insira o número de solicitações enviadas ao servidor RADIUS antes que uma falha seja considerada como ocorrida. Se **Usar padrão** tiver sido selecionado, o dispositivo usará o valor padrão para o número de novas tentativas.

Se **Definido pelo Usuário** estiver selecionado para *Tempo de Dead*, insira o número de minutos que devem passar antes que um servidor RADIUS não responsivo seja ignorado para solicitações de serviço. Se **Usar padrão** foi selecionado, o dispositivo usa o valor padrão para o tempo de inatividade. Se você inseriu 0 minutos, não há tempo de inatividade.

Note: Neste exemplo, selecionaremos **Usar padrão** para ambos os campos.



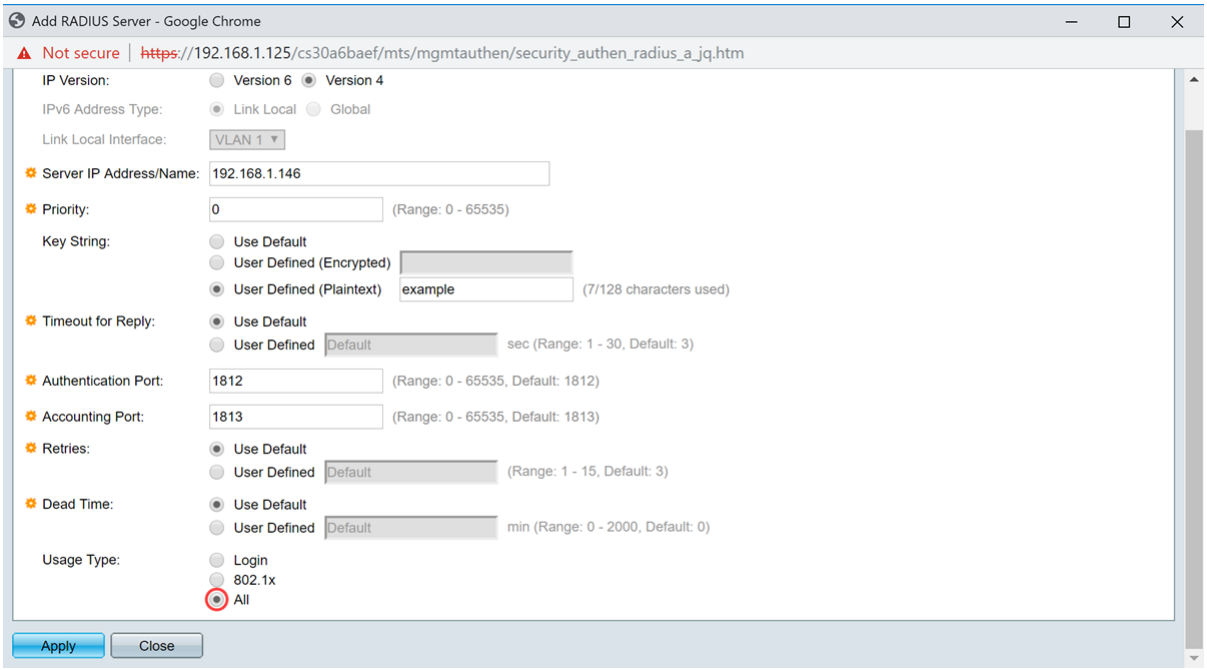
Etapa 11. No campo *Tipo de uso*, insira o tipo de autenticação do servidor RADIUS. As opções são:

Login - O servidor RADIUS é usado para autenticar usuários que pedem para administrar o

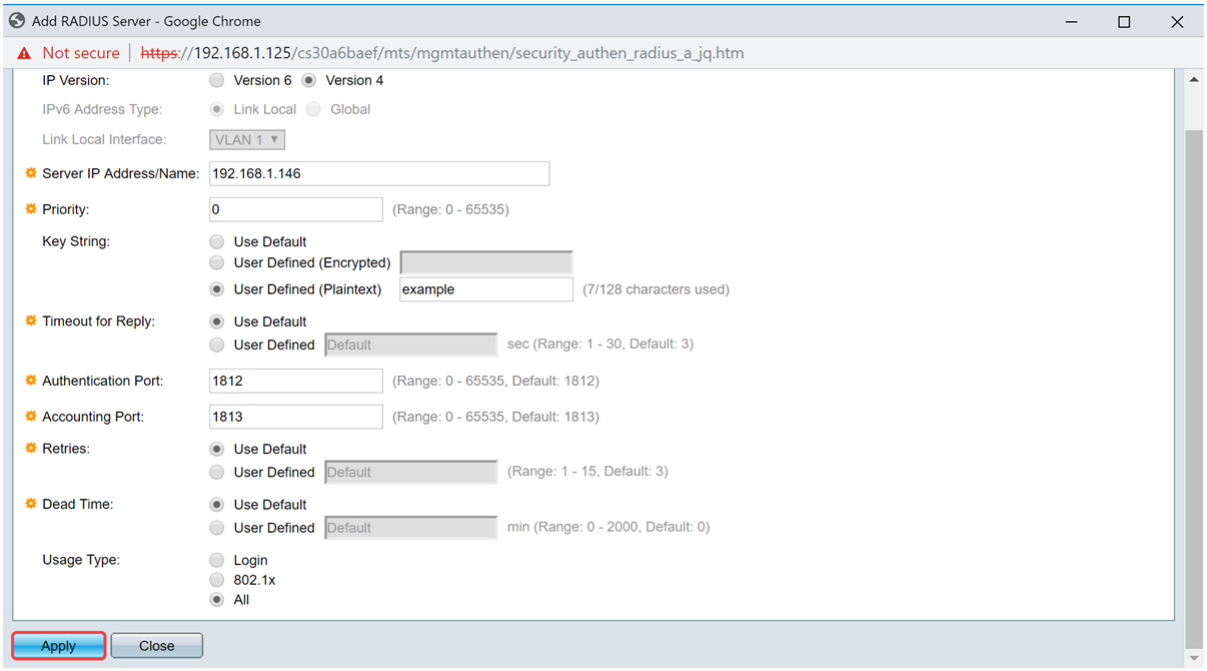
dispositivo.

802.1x - O servidor RADIUS é usado para autenticação 802.1x.

Todos - O servidor RADIUS é usado para autenticar o usuário que solicita a administração do dispositivo e a autenticação 802.1x.



Etapa 12. Clique em Apply.

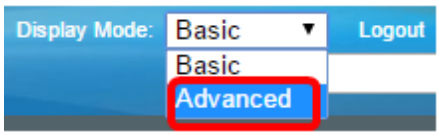


Definir as configurações de autenticação de porta 802.1x

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

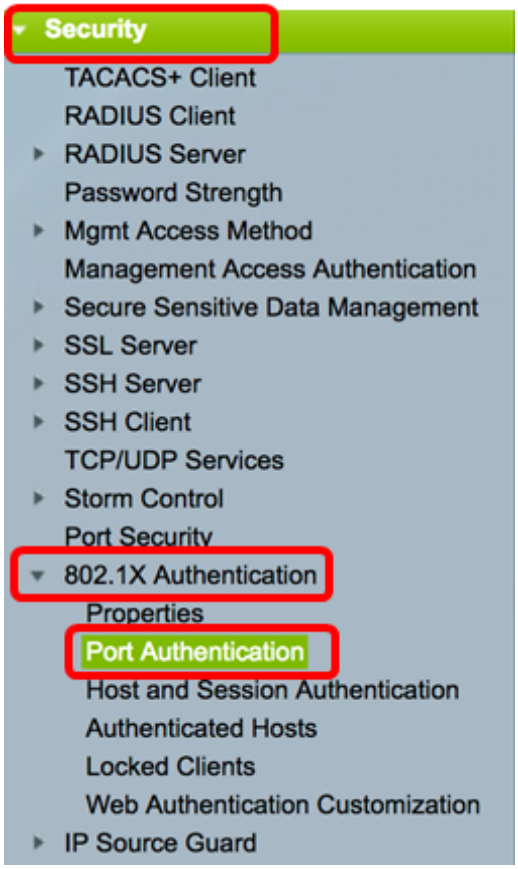
Note: As opções de menu disponíveis podem variar dependendo do modelo do dispositivo.

Neste exemplo, o SG350X-48MP é usado.



Note: Se você tiver um switch Sx300 ou Sx500 Series, vá para a Etapa 2.

Etapa 2. Escolha **Security > 802.1X Authentication > Port Authentication**.

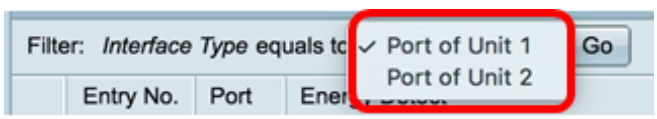


Etapa 3. Escolha uma interface na lista suspensa *Tipo de interface*.

Porta — Na lista suspensa *Tipo de interface*, escolha **Porta** se apenas uma única porta precisar ser escolhida.

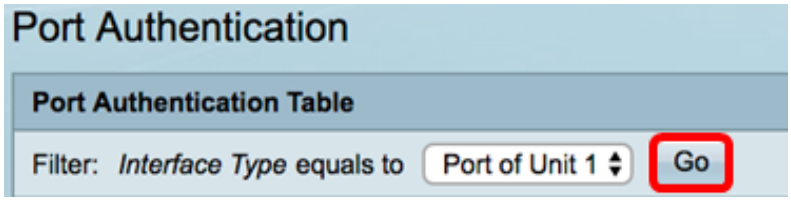
LAG — Na lista suspensa *Tipo de interface*, escolha o LAG a ser configurado. Isso afeta o grupo de portas definido na configuração do LAG.

Note: Neste exemplo, Port of Unit 1 (Porta da unidade 1) é escolhido.

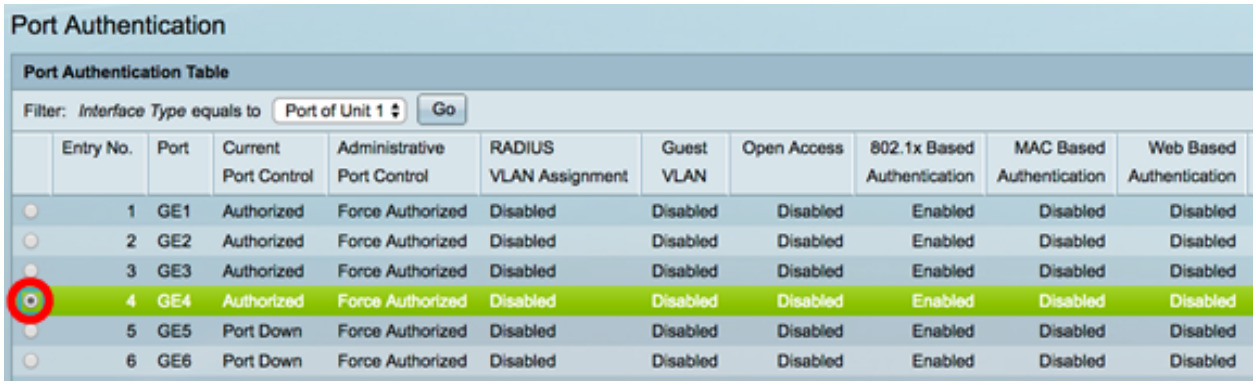


Note: Se você tiver um switch não empilhável, como um switch Sx300 Series, vá para a Etapa 5.

Etapa 4. Clique em **Ir** para exibir uma lista de portas ou LAGs na interface.



Etapa 5. Clique na porta que deseja configurar.



Note: Neste exemplo, GE4 é escolhido.

Etapa 6. Role para baixo na página e clique em **Editar**.

Passo 7. (Opcional) Se quiser editar outra interface, escolha nas listas suspensas Unidade e Porta.

Note: Neste exemplo, a porta GE4 da unidade 1 é escolhida.

Etapa 8. Clique no botão de opção que corresponde ao controle de porta desejado na área Administrative Port Control. As opções são:

Forçar não autorizado — Nega o acesso à interface movendo a porta para o estado não autorizado. A porta descartará o tráfego.

Auto — A porta se move entre um estado autorizado ou não autorizado com base na autenticação do requerente.

Force Authorized (Forçar autorização) - Autoriza a porta sem autenticação. A porta encaminhará o tráfego.

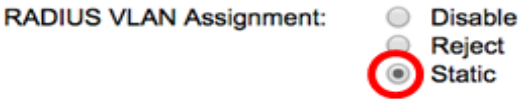
Note: Neste exemplo, Automático é escolhido.

Etapa 9. Clique no botão de opção RADIUS VLAN Assignment (Atribuição de VLAN RADIUS) para configurar a atribuição de VLAN dinâmica na porta selecionada. As opções são:

Desabilitar — Recurso não habilitado.

Rejeitar — Se o servidor RADIUS autorizou o requerente, mas não forneceu uma VLAN suplicante, o requerente será rejeitado.

Estático — Se o servidor RADIUS autorizou o requerente, mas não forneceu uma VLAN suplicante, o requerente é aceito.



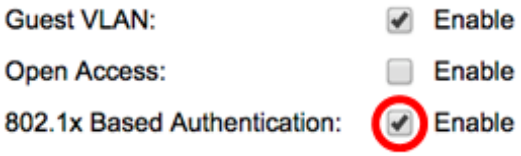
Note: Neste exemplo, Estático é escolhido.

Etapa 10. Marque a caixa de seleção **Enable** na VLAN Guest para ativar a VLAN Guest para portas não autorizadas. A VLAN de convidado faz com que a porta não autorizada ingresse automaticamente na VLAN escolhida na área ID da VLAN de convidado das propriedades 802.1.

Etapa 11. (Opcional) Marque a caixa de seleção **Habilitar** acesso aberto para habilitar o acesso aberto. O Open Access ajuda a compreender os problemas de configuração dos hosts que se conectam à rede, monitora situações ruins e permite que esses problemas sejam corrigidos.

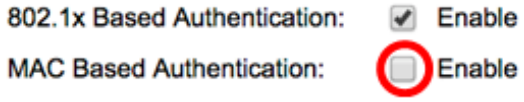
Note: Quando o Open Access é ativado em uma interface, o switch trata todas as falhas recebidas de um servidor RADIUS como sucessos e permite acesso à rede para estações conectadas a interfaces, independentemente dos resultados da autenticação. Neste exemplo, o acesso aberto está desabilitado.

Etapa 12. Marque a caixa de seleção **Enable** 802.1x Based Authentication para habilitar a autenticação 802.1X na porta.



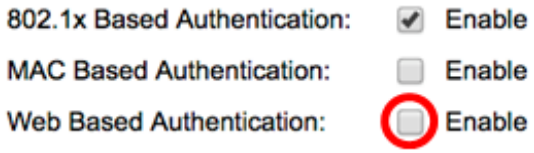
Etapa 13. Marque a caixa de seleção **Enable** MAC Based Authentication para habilitar a autenticação de porta com base no endereço MAC suplicante. Apenas oito autenticações baseadas em MAC podem ser usadas na porta.

Note: Para que a autenticação MAC seja bem-sucedida, o nome de usuário e a senha suplicante do servidor RADIUS devem ser o endereço MAC suplicante. O endereço MAC deve estar em letras minúsculas e ser inserido sem o . ou - separadores (como 0020aa00bcc).



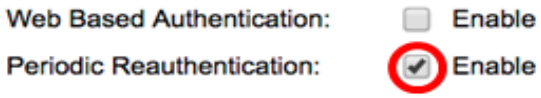
Note: Neste exemplo, a autenticação baseada em MAC está desabilitada.

Etapa 14. Marque a caixa de seleção **Enable** Web Based Authentication para habilitar a autenticação baseada na Web no switch. Neste exemplo, a autenticação baseada na Web está desabilitada.



Note: Neste exemplo, a autenticação baseada na Web está desabilitada.

Etapa 15. (Opcional) Marque a caixa de seleção **Habilitar** Autenticação Periódica para forçar a porta a se autenticar novamente após um determinado tempo. Esse tempo é definido no campo *Período de reautenticação*.

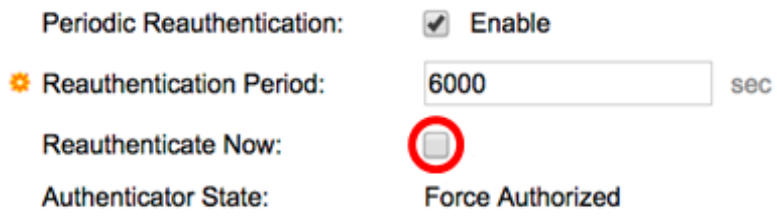


Note: Neste exemplo, a reautenticação de período está habilitada.

Etapa 16. (Opcional) Insira um valor no campo *Período de reautenticação*. Esse valor representa a quantidade de segundos antes da interface autenticar novamente a porta. O valor padrão é 3600 segundos e o intervalo é de 300 a 4294967295 segundos.

Note: Neste exemplo, 6000 segundos são configurados.

Etapa 17. (Opcional) Marque a caixa de seleção **Enable Reauthenticate Now (Ativar reautenticação agora) para forçar uma reautenticação imediata da porta.** Neste exemplo, a reautenticação imediata está desabilitada.

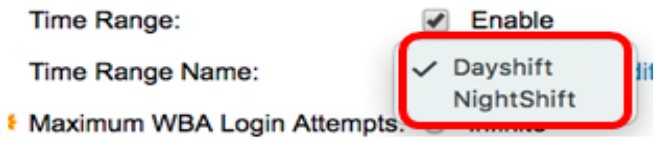


A área Estado do autenticador exibe o estado de autorização da porta.

Etapa 18. (Opcional) Marque a caixa de seleção **Habilitar** intervalo de tempo para habilitar um limite no tempo em que a porta está autorizada.

Note: Neste exemplo, o intervalo de tempo está ativado. Se preferir ignorar este recurso, vá para a Etapa 20.

Etapa 19. (Opcional) Na lista suspensa Nome do intervalo de tempo, escolha um intervalo de tempo a ser usado.



Note: Neste exemplo, Dayshift é escolhido.

Etapa 20. Na área Maximum WBA Login Attempts (Máximo de tentativas de login da WBA), clique em Infinite for no limit (Infinito para sem limite) ou em User Defined (Definido pelo usuário) para definir um limite. Se Definido pelo usuário for escolhido, insira o número máximo de tentativas de login permitidas para autenticação baseada na Web.

Note: Neste exemplo, Infinite é escolhido.

Etapa 21. Na área Maximum WBA Silence Period (Período de silêncio máximo da WBA), clique em Infinite for no limit (Infinito para sem limite) ou em User Defined (Definido pelo usuário) para definir um limite. Se Definido pelo usuário for escolhido, insira o comprimento máximo do período silencioso para a autenticação baseada na Web permitida na interface.

Note: Neste exemplo, Infinite é escolhido.

Etapa 22. Na área Máximo de hosts, clique em Infinito para sem limite ou Definido pelo usuário para definir um limite. Se Definido pelo usuário for escolhido, insira o número máximo de hosts autorizados permitidos na interface.

Note: Defina esse valor como 1 para simular o modo de host único para autenticação baseada na Web no modo multisessões. Neste exemplo, Infinite é escolhido.

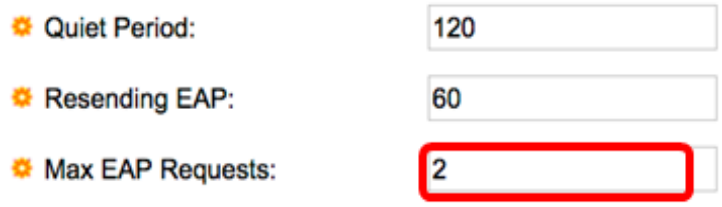
Etapa 23. No campo *Quiet Period*, insira o tempo em que o switch permanece no estado silencioso após uma falha de troca de autenticação. Quando o switch está em estado silencioso, isso significa que o switch não está ouvindo novas solicitações de autenticação do cliente. O valor padrão é 60 segundos e o intervalo é de um a 65535 segundos.

Note: Neste exemplo, o período de silêncio é definido como 120 segundos.

Etapa 24. No campo *Reenviando EAP*, insira a hora em que o switch espera por uma mensagem de resposta do requerente antes de reenviar uma solicitação. O valor padrão é 30 segundos e o intervalo é de um a 65535 segundos.

Note: Neste exemplo, reenviar EAP é definido como 60 segundos.

Etapa 25. No campo *Máximo de solicitações EAP*, insira o número máximo de solicitações EAP que podem ser enviadas. O EAP é um método de autenticação usado no 802.1X que fornece troca de informações de autenticação entre o switch e o cliente. Nesse caso, as solicitações EAP são enviadas ao cliente para autenticação. O cliente deve responder e corresponder às informações de autenticação. Se o cliente não responder, outra solicitação EAP é definida com base no valor EAP de reenvio e o processo de autenticação é reiniciado. O valor padrão é 2 e o intervalo é de 1 a 10.



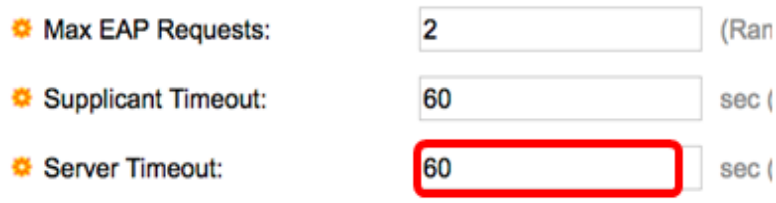
Note: Neste exemplo, o valor padrão 2 é usado.

Etapa 26. No campo *Timeout do requerente*, insira o tempo antes das solicitações EAP serem enviadas ao requerente. O valor padrão é 30 segundos e o intervalo é de um a 65535 segundos.

Note: Neste exemplo, o tempo limite do suplicante é definido como 60 segundos.

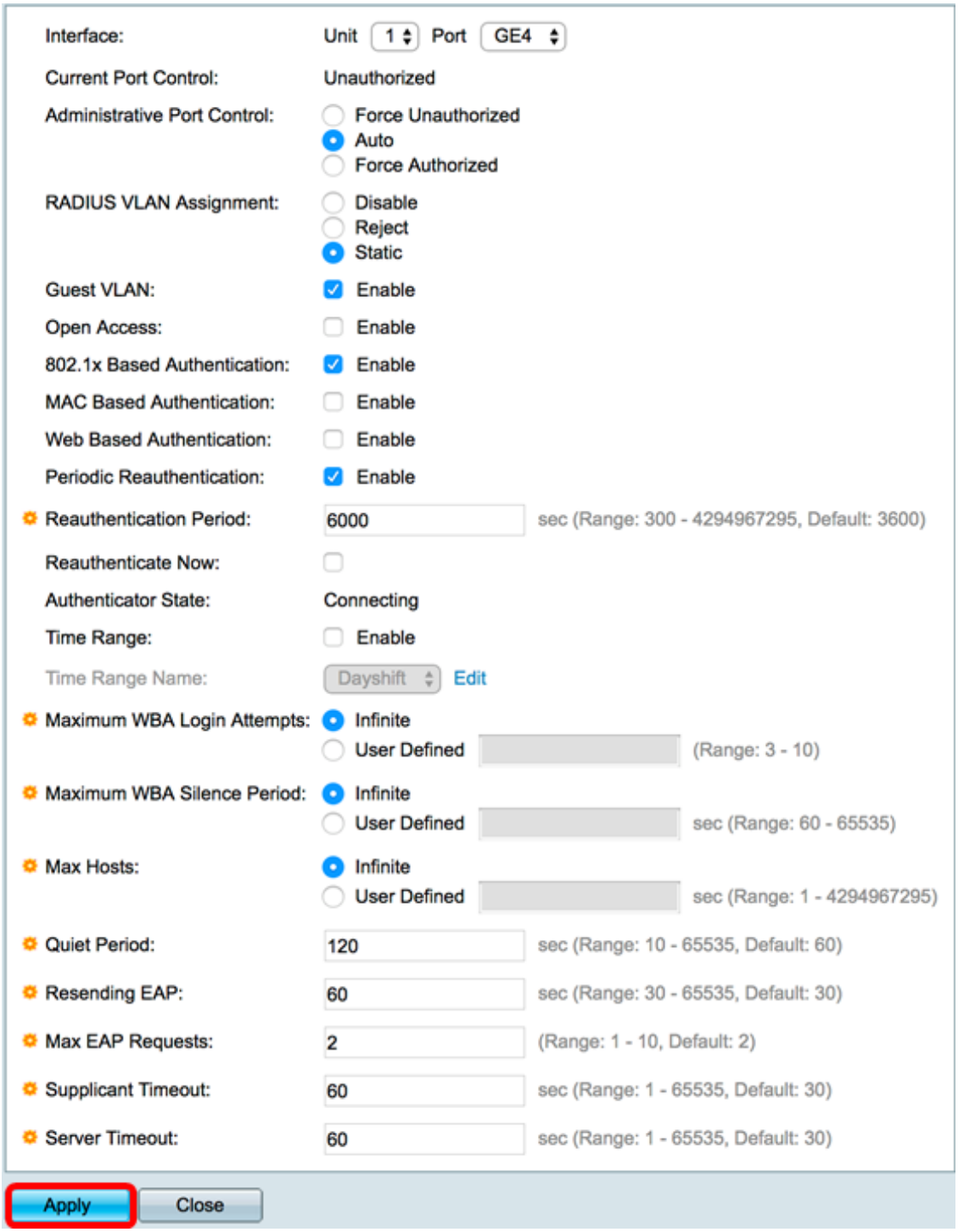
Etapa 27. No campo *Server Timeout*, insira o tempo decorrido antes que o switch envie uma

solicitação novamente para o servidor RADIUS. O valor padrão é 30 segundos e o intervalo é de um a 65535 segundos.

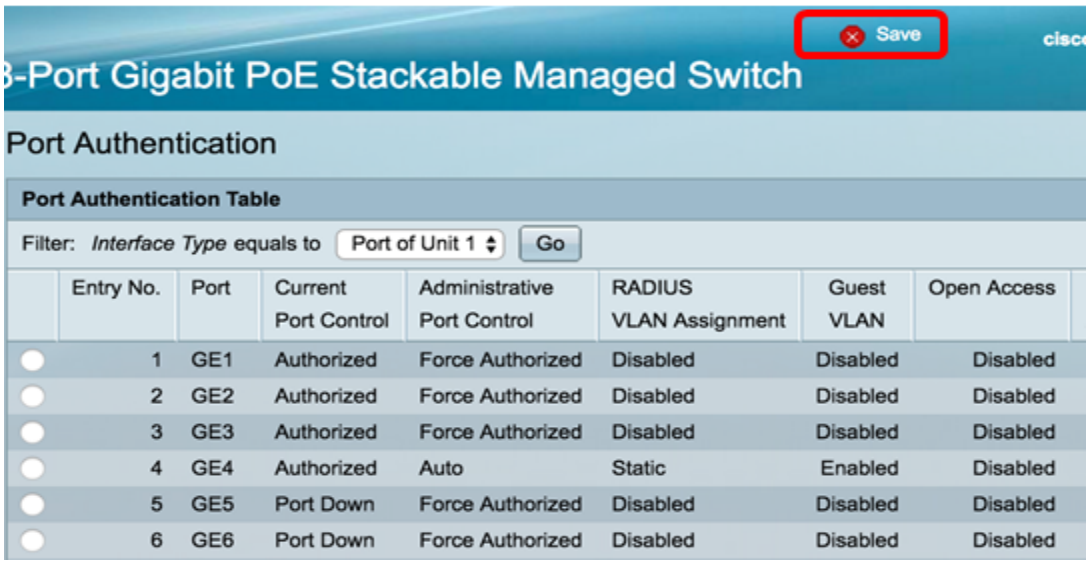


Note: Neste exemplo, o tempo limite do servidor é definido como 60 segundos.

Etapa 28. Clique em **Aplicar** e, em seguida, clique em **Fechar**.



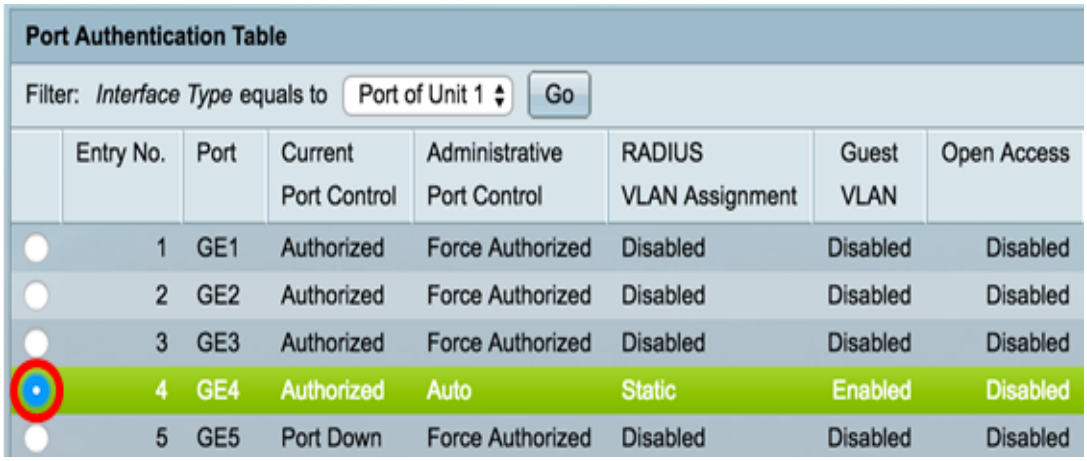
Etapa 29. (Opcional) Clique em **Salvar** para salvar as configurações no arquivo de configuração de inicialização.



Agora você deve ter configurado com êxito as configurações de autenticação de porta 802.1x em seu switch.

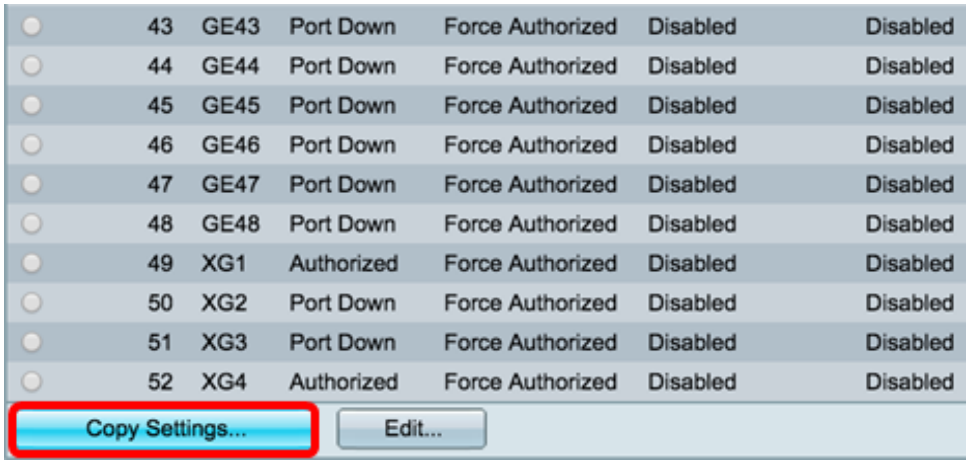
Aplicar configurações de interface a várias interfaces

Etapa 1. Clique no botão de opção da interface que você deseja aplicar a configuração de autenticação a várias interfaces.



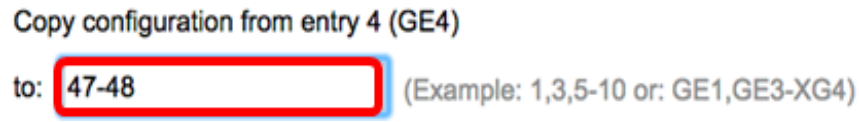
Note: Neste exemplo, GE4 é escolhido.

Etapa 2. Role para baixo e clique em **Copiar configurações**.



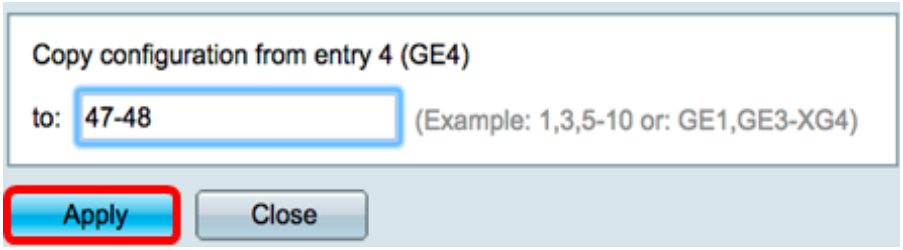
Etapa 3. No campo *to*, insira o intervalo de interfaces que você deseja aplicar à

configuração da interface escolhida. Você pode usar os números de interface ou o nome das interfaces como entrada. Você pode inserir cada interface separada por uma vírgula (como 1, 3, 5 ou GE1, GE3, GE5) ou pode inserir um intervalo de interfaces (como 1-5 ou GE1-GE5).

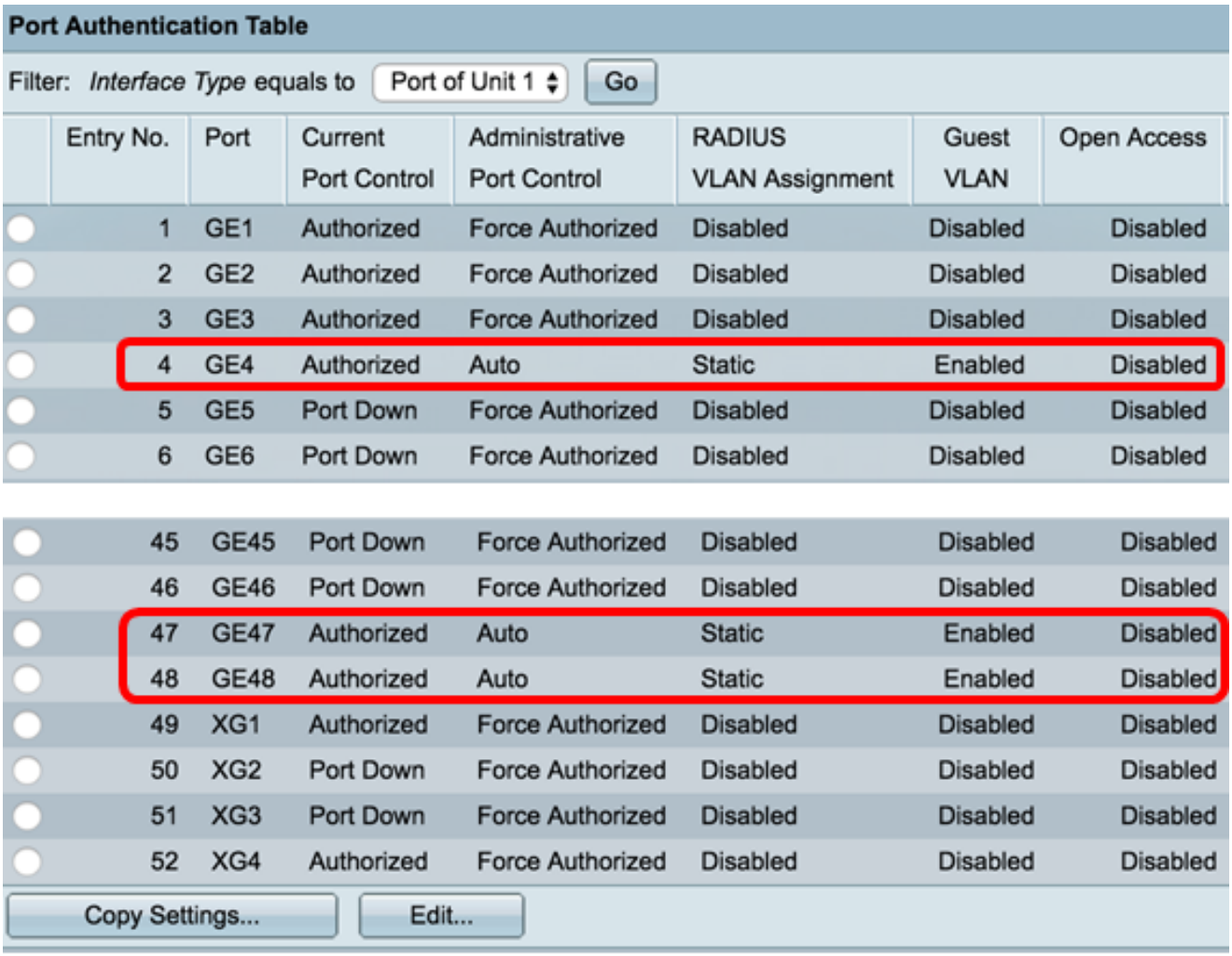


Note: Neste exemplo, as configurações serão aplicadas às portas 47 a 48.

Etapa 4. Clique em **Aplicar** e, em seguida, clique em **Fechar**.



A imagem abaixo representa as alterações após a configuração.



Agora você deve ter copiado com êxito as configurações de autenticação 802.1x de uma porta e aplicado a outra porta ou portas no switch.