Configurando a autenticação baseada em MAC em um switch

Objetivo

O 802.1X é uma ferramenta de administração para permitir dispositivos de lista, garantindo que não haja acesso não autorizado à sua rede. Este documento mostra como configurar a autenticação baseada em MAC em um switch usando a Interface Gráfica do Usuário (GUI). Para saber como configurar a autenticação baseada em MAC usando a CLI (Command Line Interface, interface de linha de comando), clique aqui.

Note: Este guia é longo em 9 seções e 1 seção para verificar se um host foi autenticado. Pegue café, chá ou água e garanta que você tenha tempo suficiente para revisar e executar as etapas envolvidas.

Consulte o glossário para obter mais informações.

Como funciona o RADIUS?

Há três componentes principais para a autenticação 802.1X, um suplicante (cliente), um autenticador (dispositivo de rede, como um switch) e um servidor de autenticação (RADIUS). O RADIUS (Remote Authentication Dial-In User Service) é um servidor de acesso que usa o protocolo AAA (authentication, authorization, and accounting) que ajuda a gerenciar o acesso à rede. O RADIUS usa um modelo cliente-servidor no qual as informações de autenticação segura são trocadas entre o servidor RADIUS e um ou mais clientes RADIUS. Ele valida a identidade do cliente e notifica o switch se o cliente está autorizado a acessar a LAN.

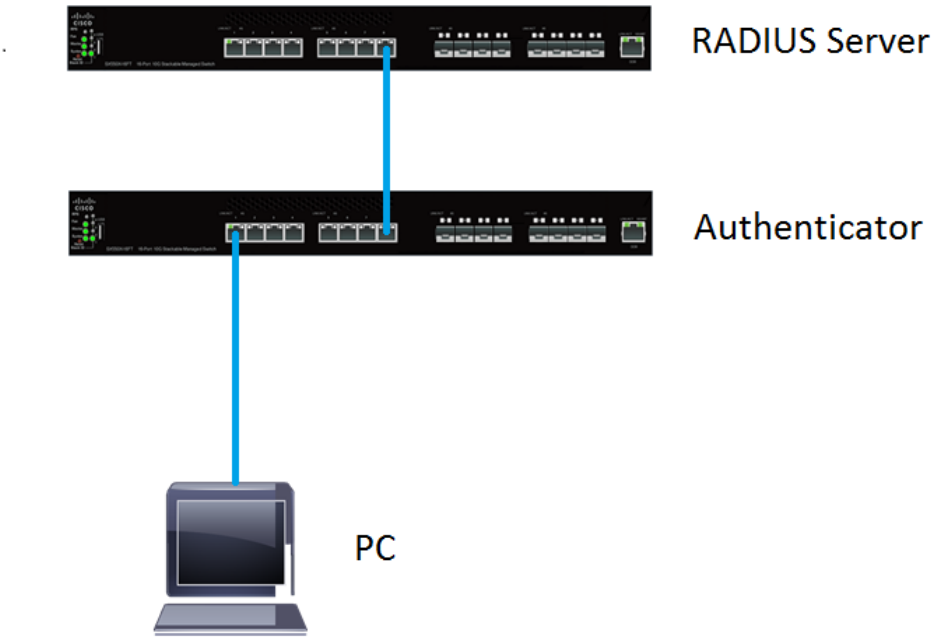
Um autenticador funciona entre o cliente e o servidor de autenticação. Primeiro, solicitará informações de identidade do cliente. Em resposta, o autenticador verificará as informações com o servidor de autenticação. Por fim, ele retransmitirá uma resposta ao cliente. Neste artigo, o autenticador seria um switch que inclui o cliente RADIUS. O switch seria capaz de encapsular e desencapsular os quadros EAP (Extensible Authentication Protocol) para interagir com o servidor de autenticação.

E a autenticação baseada em MAC?

Na autenticação baseada em MAC, quando o requerente não entende como falar com o autenticador ou não consegue, ele usa o endereço MAC do host para autenticar. Os suplicantes baseados em MAC são autenticados usando RADIUS puro (sem usar EAP). O servidor RADIUS tem um banco de dados de host dedicado que contém somente os endereços MAC permitidos. Em vez de tratar a solicitação de autenticação baseada em MAC como uma autenticação PAP (Password Authentication Protocol), os servidores reconhecem tal solicitação pelo Atributo 6 [Service-Type] = 10. Eles compararão o endereço MAC no atributo Calling-Station-Id com os endereços MAC armazenados no banco de dados do host.

A versão 2.4 acrescenta a capacidade de configurar o formato do nome de usuário enviado para suplicantes baseados em MAC e ser definido como método de autenticação EAP ou RADIUS puro. Nesta versão, você também pode configurar o formato do nome de usuário, bem como configurar uma senha específica, diferente do nome de usuário, para suplicantes baseados em MAC.

Topologia:



Note: Neste artigo, usaremos o SG550X-24 para o servidor RADIUS e o autenticador. O servidor RADIUS tem um endereço IP estático de 192.168.1.100 e o autenticador tem um endereço IP estático de 192.168.1.101.

As etapas neste documento são executadas no modo de exibição **Avançado**. Para alterar o modo para avançado, vá para o canto superior direito e selecione **Avançado** na lista suspensa *Modo de exibição*.

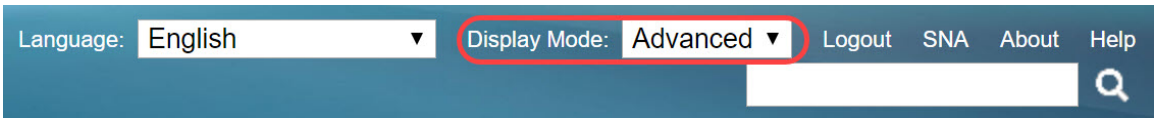


Tabela de conteúdo

Dispositivos aplicáveis

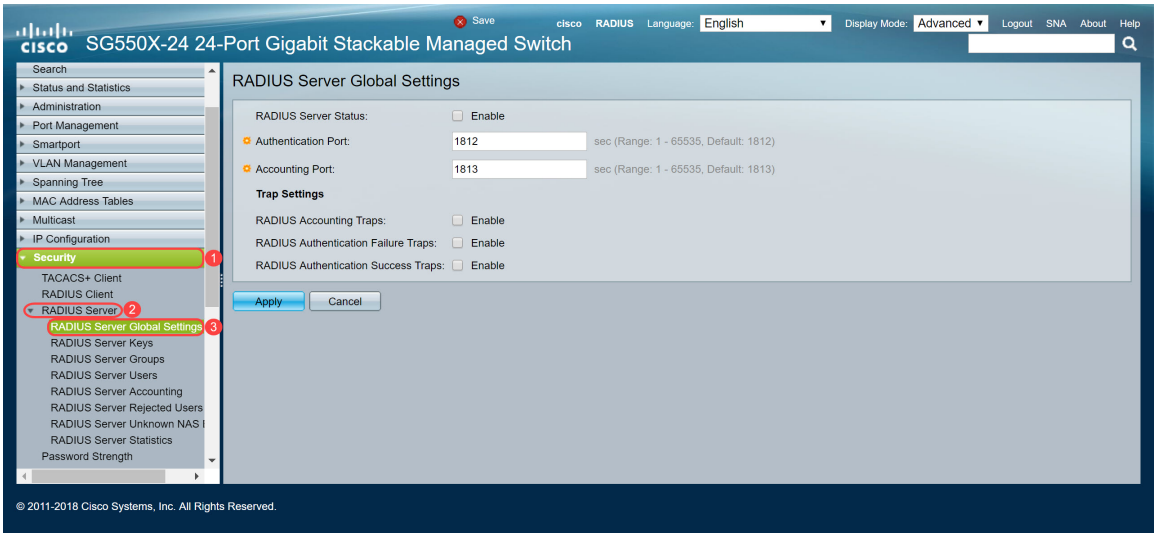
- Série Sx350X
- SG350XG Series
- Sx550X Series
- Série SG550XG

Versão de software

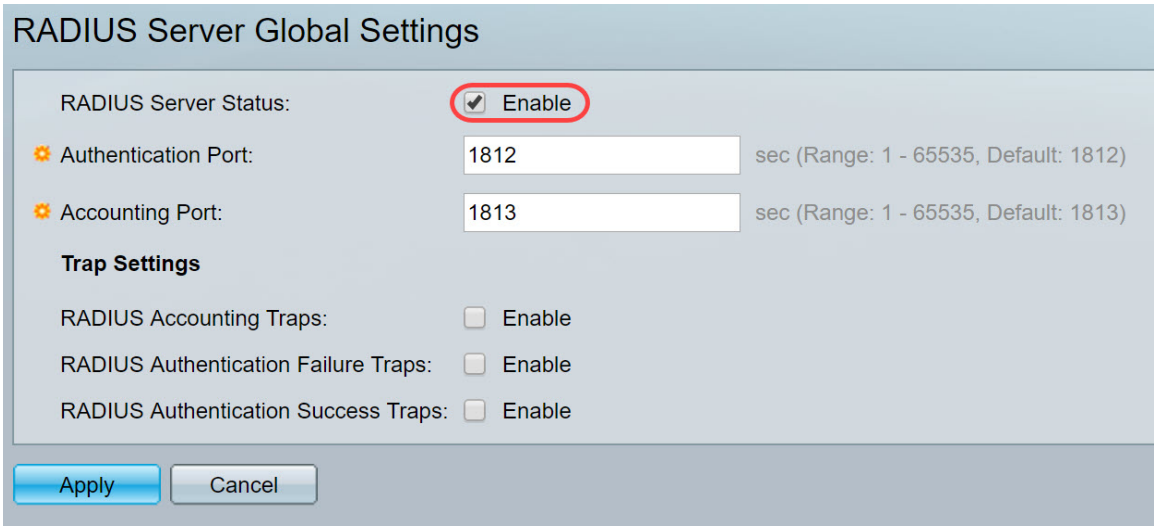
- 2.4.0.94

Configurações globais do servidor RADIUS

Etapa 1. Efetue login no utilitário baseado na Web do seu switch que será configurado como servidor RADIUS e navegue para **Segurança > Servidor RADIUS > Configurações globais do servidor RADIUS**.



Etapa 2. Para habilitar o status do recurso do servidor RADIUS, marque a caixa de seleção **Enable** no campo *RADIUS Server Status*.

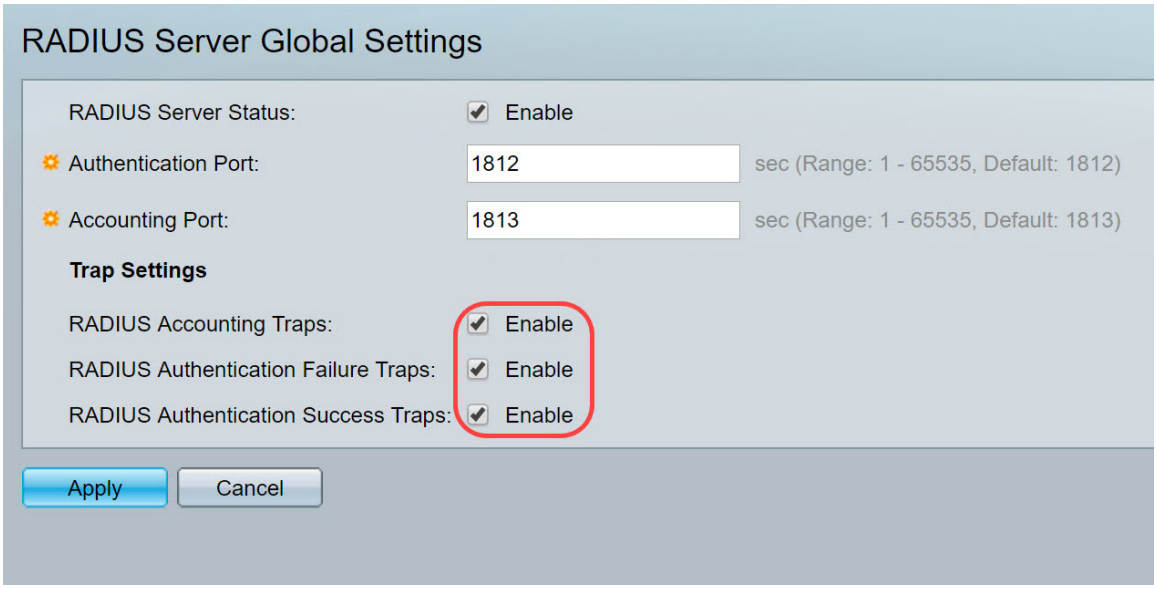


Etapa 3. Para gerar armadilhas para eventos de contabilidade RADIUS, logins que falharam ou para logins que foram bem-sucedidos, marque a caixa de seleção **Enable** desejada para gerar armadilhas. Traps são mensagens de eventos do sistema geradas via SNMP (Simple Network Management Protocol). Uma armadilha é enviada ao gerenciador SNMP do switch quando ocorre uma violação. As seguintes configurações de armadilha são:

- RADIUS Accounting Traps — Marque para gerar armadilhas para eventos de contabilidade

RADIUS.

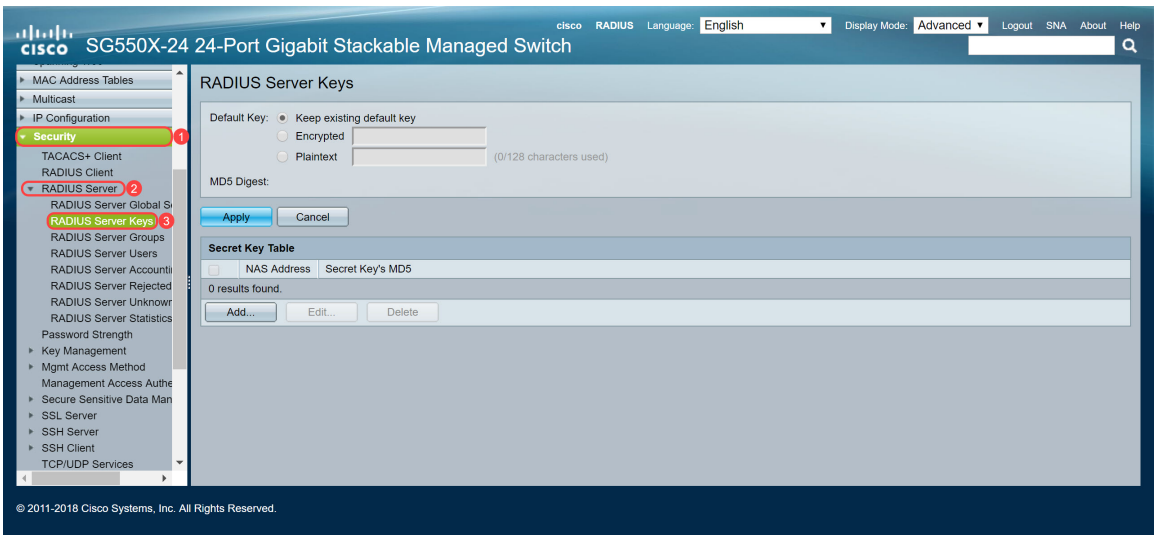
- RADIUS Authentication Failure Traps (Armadilhas de falha de autenticação RADIUS) — Marque para gerar armadilhas para logins que falharam.
- RADIUS Authentication Success Traps (Armadilhas de sucesso de autenticação RADIUS) — Marque para gerar armadilhas para logins bem-sucedidos.



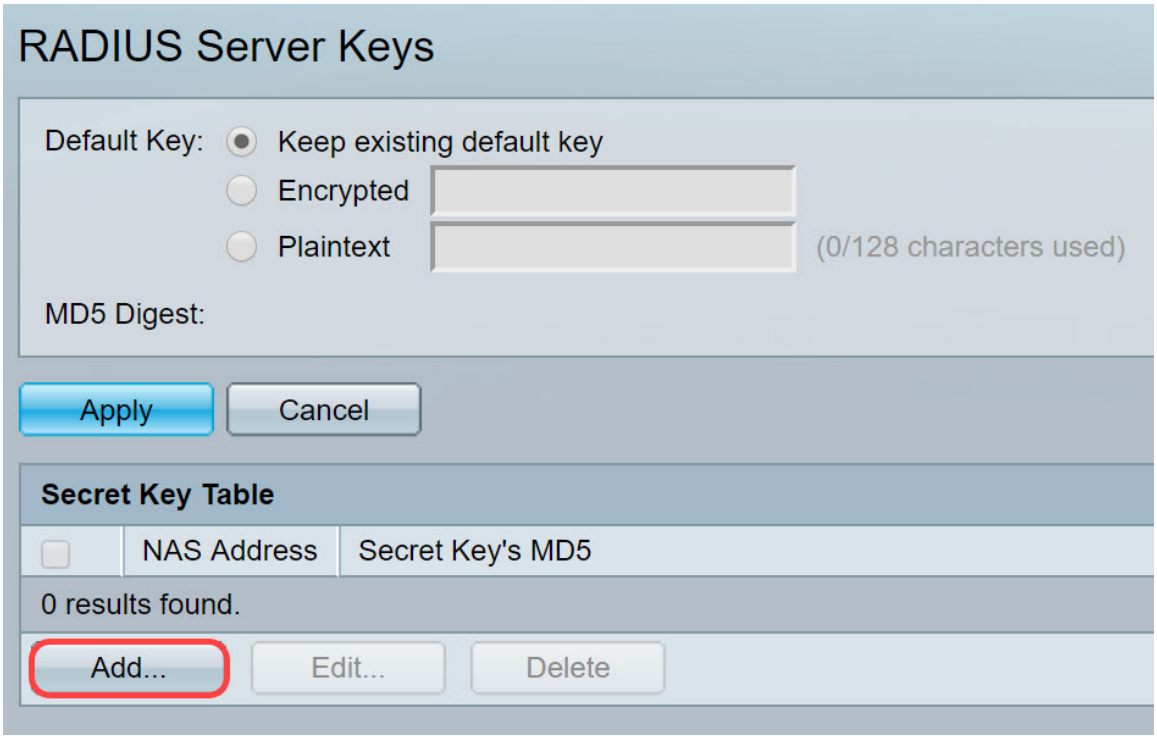
Etapa 4. Clique em **Apply** para salvar suas configurações.

Chaves de servidor RADIUS

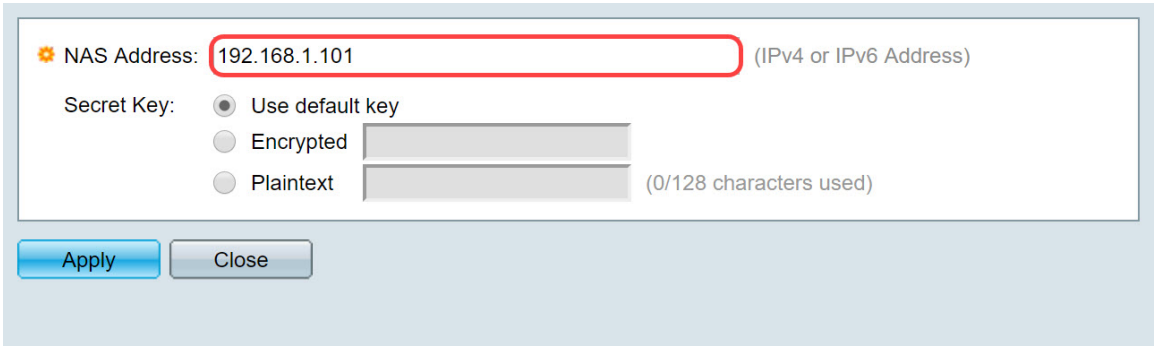
Etapa 1. Navegue até **Security > RADIUS Server > RADIUS Server Keys**. A página *Chave do servidor RADIUS* é aberta.



Etapa 2. Na seção *Tabela de chaves secretas*, clique em **Adicionar...** para adicionar uma chave secreta.



Etapa 3. A página *Adicionar chave de segredo* é aberta. No campo *Endereço NAS*, insira o endereço do switch que contém o cliente RADIUS. Neste exemplo, usaremos o endereço IP 192.168.1.101 como nosso cliente RADIUS.

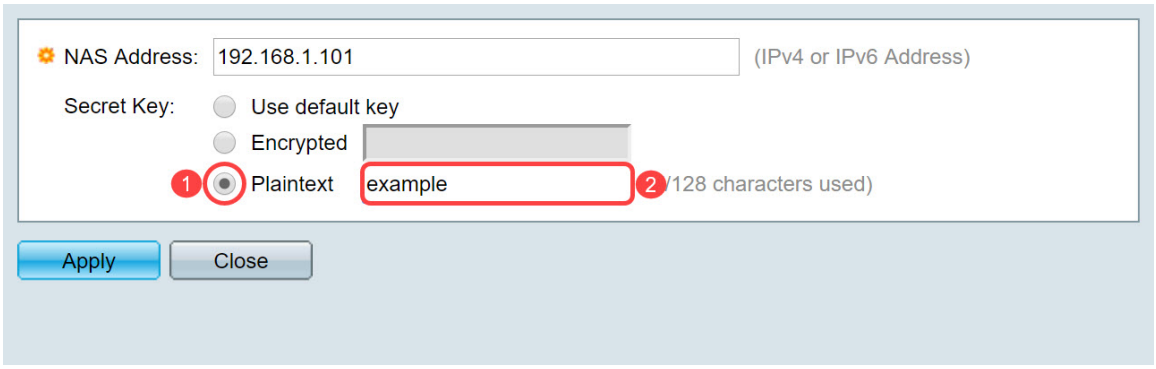


Etapa 4. Selecione um dos botões de opção usados como *chave secreta*. As seguintes opções são:

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

Neste exemplo, selecionaremos *Texto simples* e usaremos a palavra **exemplo** como nossa *chave secreta*. Depois de pressionar Aplicar, sua chave estará em um formato criptografado.

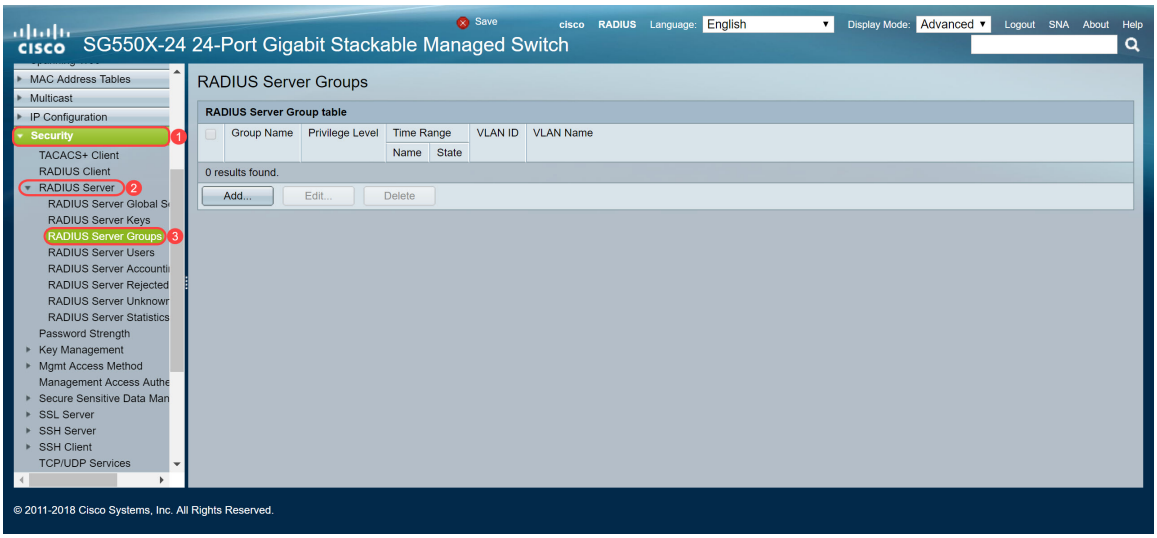
Note: Não recomendamos usar a palavra **exemplo** como chave secreta. Por favor, use uma chave mais forte. Podem ser usados até 128 caracteres. Se sua senha é muito complexa para ser lembrada, então é uma boa senha, mas ainda melhor se você puder transformá-la em uma senha memorável com caracteres especiais e números substituindo vogais — "P@55w0rds@reH@rdT0Remember". É melhor não usar nenhuma palavra que possa ser encontrada em um dicionário. É melhor escolher uma frase e trocar algumas letras por caracteres e números especiais. Consulte esta publicação do blog da Cisco para obter mais detalhes.



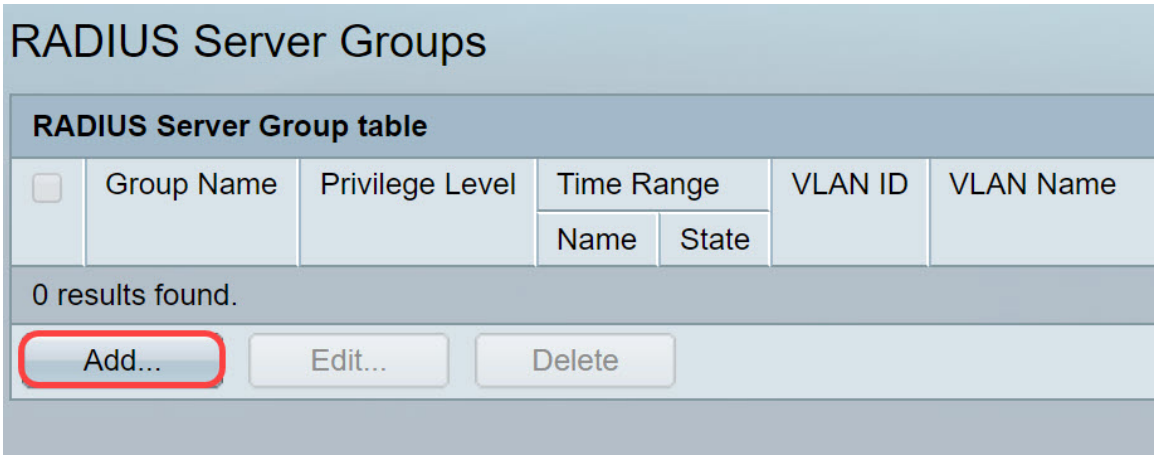
Etapa 5. Clique em **Apply** para salvar sua configuração. A chave secreta agora está criptografada com MD5. MD5 é uma função de hash criptográfico que pega um pedaço de dados e cria uma saída hexadecimal exclusiva que normalmente não é reproduzível. MD5 usa um valor hash de 128 bits.

Grupos de servidores RADIUS

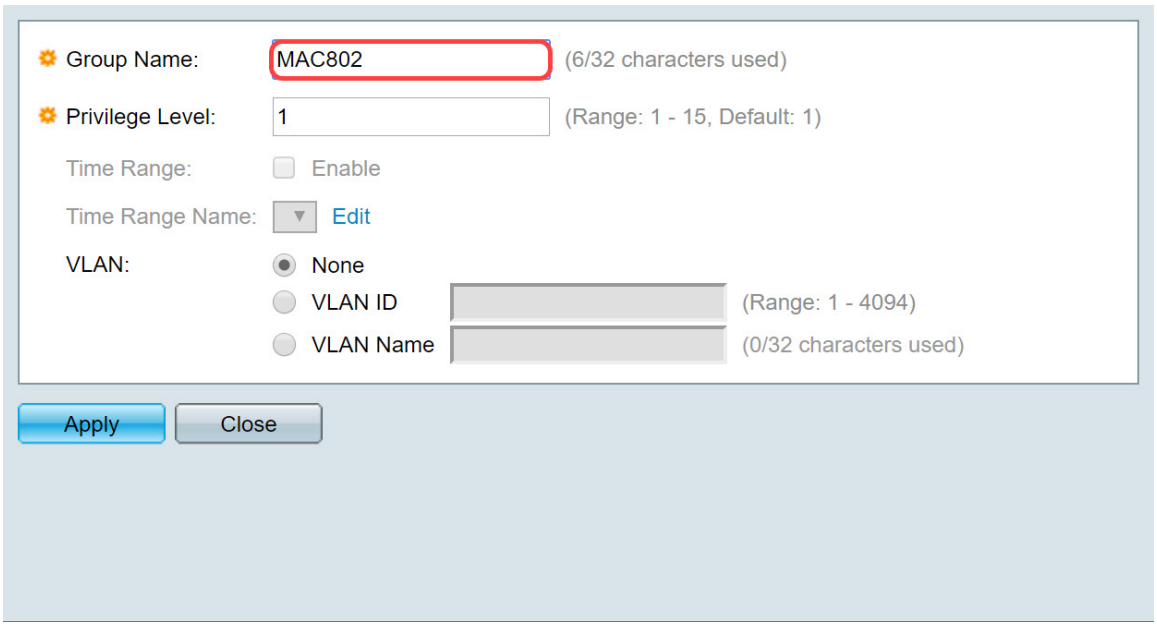
Etapa 1. Navegue até **Security > RADIUS Server > RADIUS Server Groups**.



Etapa 2. Clique em Add... para adicionar um novo grupo de servidores RADIUS.

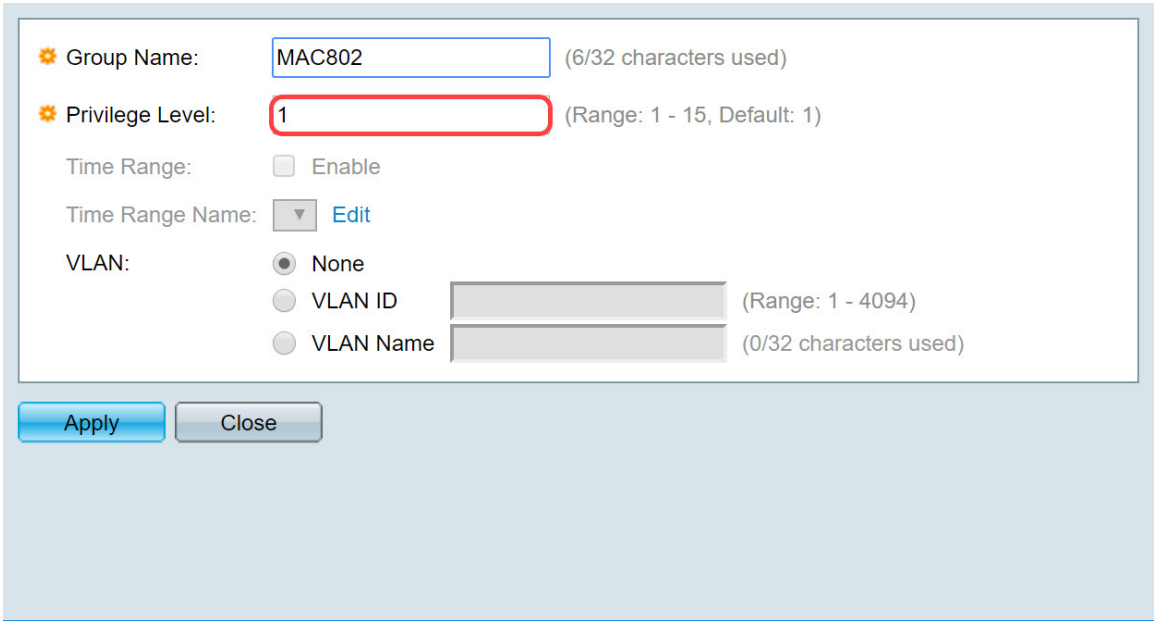


Etapa 3. A página *Adicionar grupo de servidores RADIUS* é aberta. Digite um nome para o grupo. Neste exemplo, usaremos **MAC802** como nome de grupo.



Etapa 4. Insira o nível de privilégio de acesso de gerenciamento do grupo no campo *Privilege Level*. O intervalo é de 1 a 15, 15 sendo o mais privilegiado e o valor padrão é 1. Neste exemplo, deixaremos o nível de privilégio como 1.

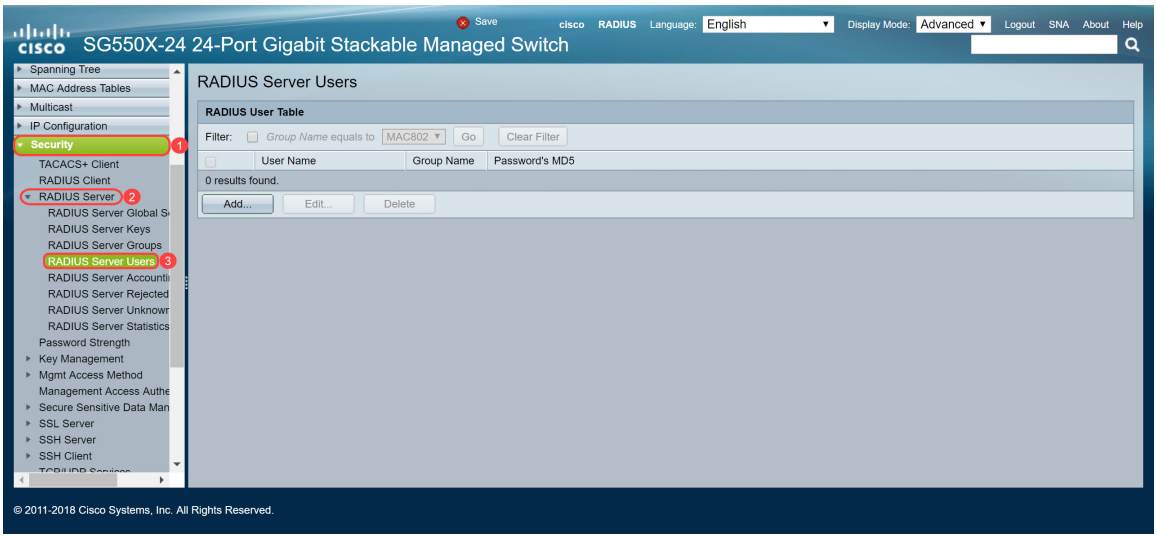
Note: Não estaremos configurando *intervalo de tempo* ou *VLAN* neste artigo.



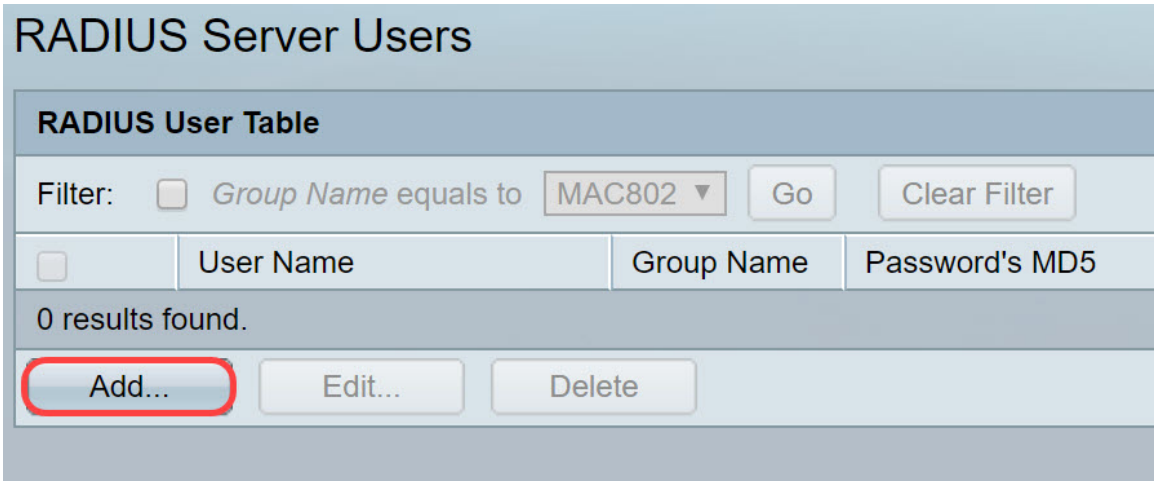
Etapa 5. Clique em **Apply** para salvar suas configurações.

Usuários de servidor RADIUS

Etapa 1. Navegue até **Security > RADIUS Server > RADIUS Server Users** para configurar usuários para RADIUS.

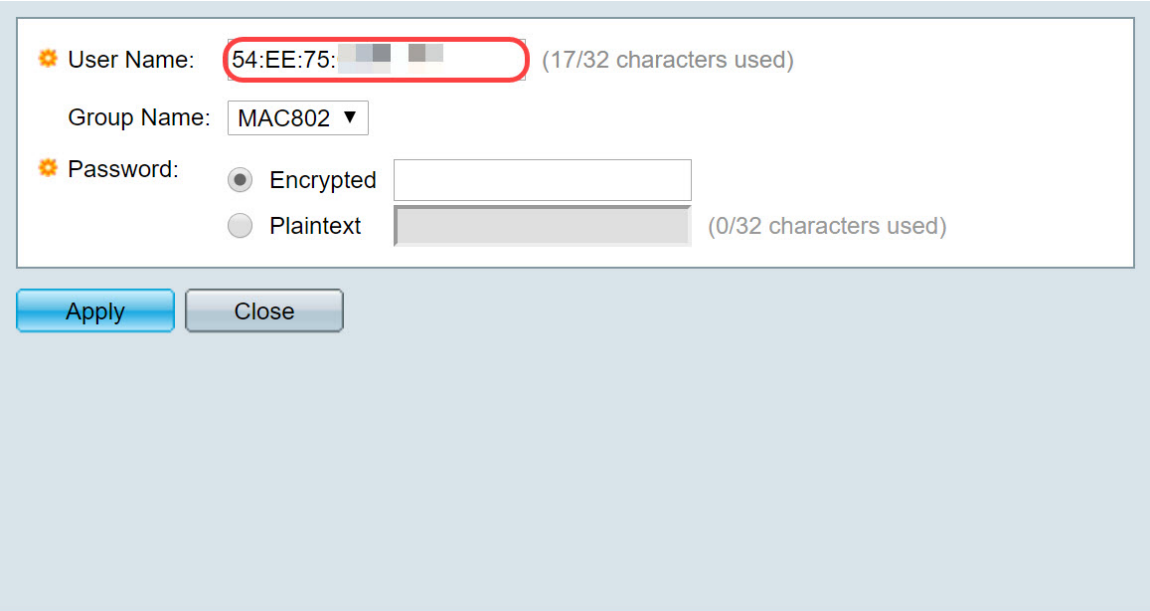


Etapa 2. Clique em Add... para adicionar um novo usuário.

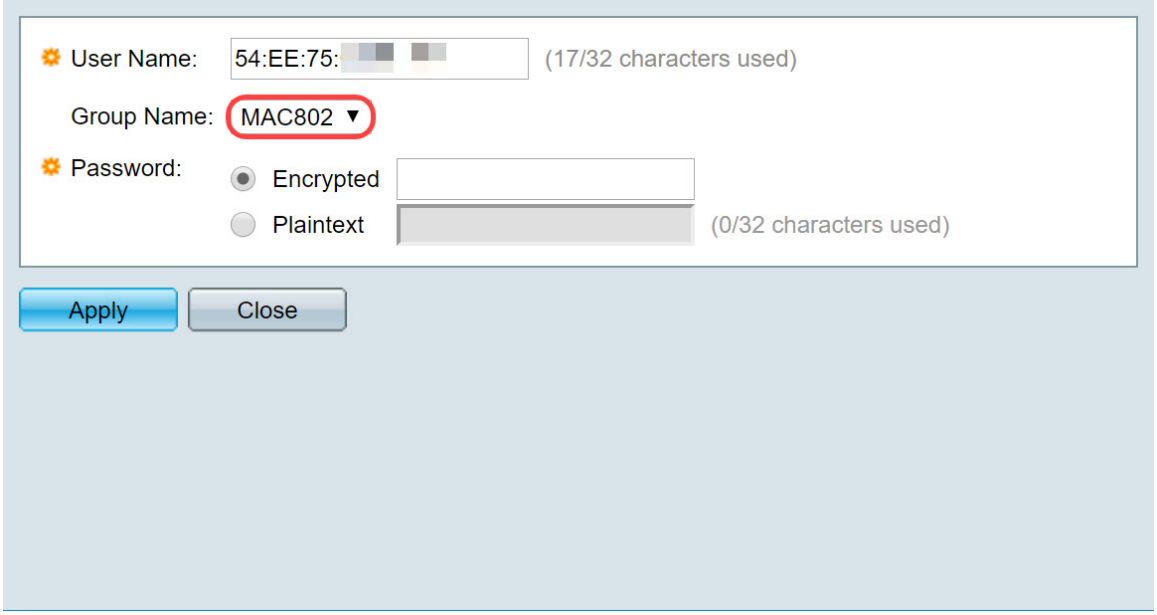


Etapa 3. A página *Adicionar usuário de servidor RADIUS* é aberta. No campo *Nome de usuário*, insira o endereço MAC de um usuário. Neste exemplo, usaremos nosso endereço MAC Ethernet em nosso computador.

Note: Uma parte do endereço MAC foi desfocada.



Etapa 4. Selecione um grupo na lista suspensa *Nome do grupo*. Conforme destacado na etapa 3 da seção Grupo de Servidores RADIUS, selecionaremos **MAC802** como nosso Nome de Grupo para este usuário.

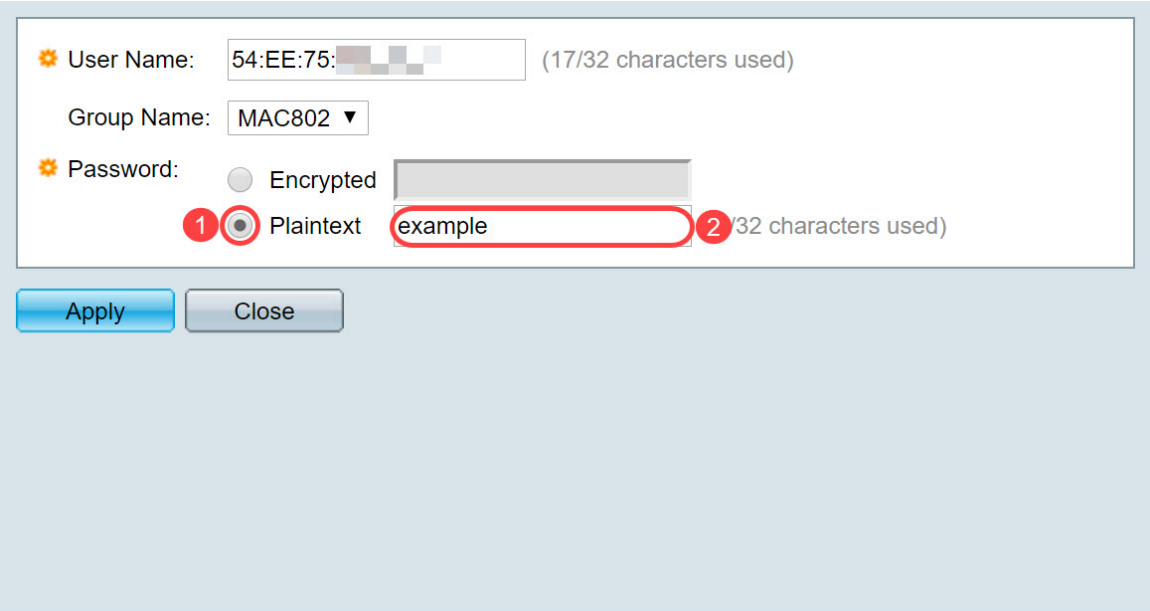


Etapa 5. Selecione um dos seguintes botões de opção:

- Criptografado — Uma chave 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.

Vamos selecionar *Texto sem formatação* como nossa senha para este usuário e digitar **por exemplo** como nossa senha em texto sem formatação.

Note: Não é recomendável usar **exemplo** como senha em texto simples. Recomendamos usar uma senha mais forte.

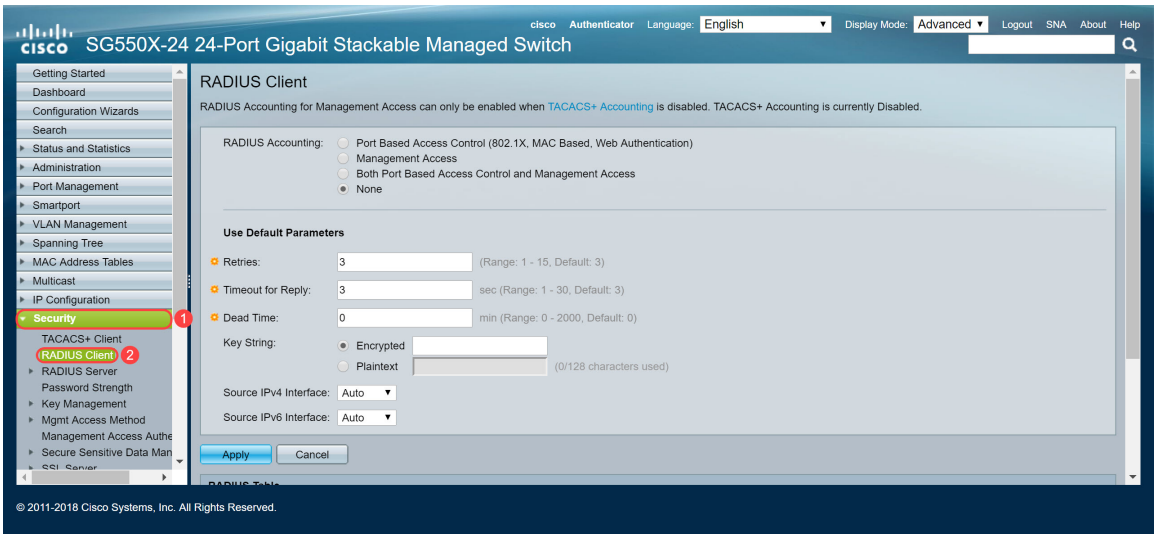


Etapa 6. Clique em **Apply** depois de concluir a configuração.

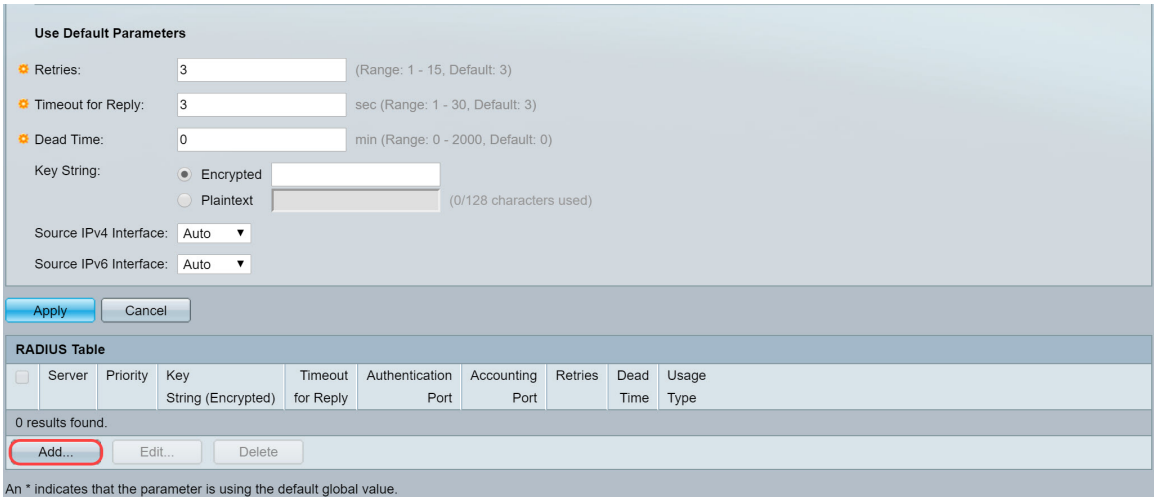
Agora você terminou de configurar o servidor RADIUS. Na próxima seção, configuraremos o segundo switch para ser um autenticador.

Cliente RADIUS

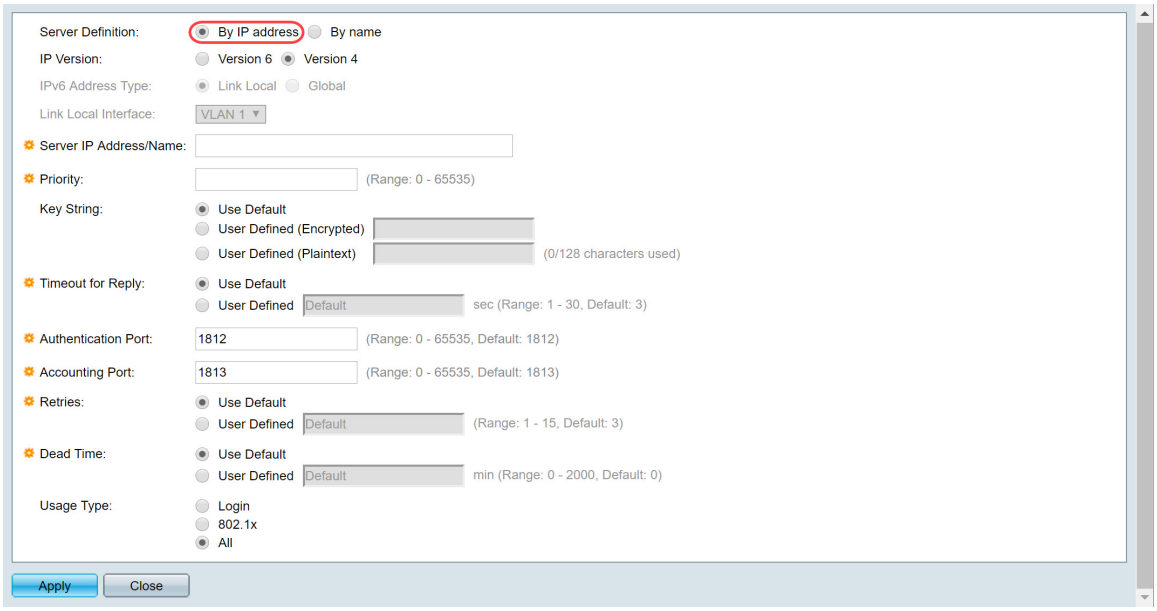
Etapa 1. Faça login no utilitário baseado na Web do seu switch que será configurado como autenticador e navegue até **Security > RADIUS Client**.



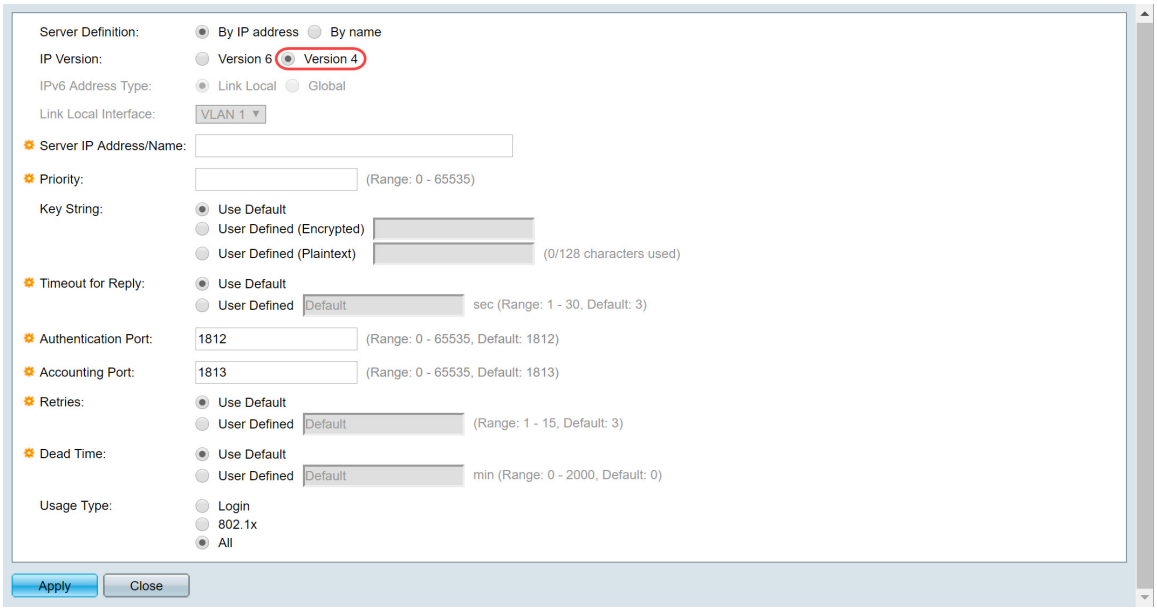
Etapa 2. Role para baixo até a seção *Tabela RADIUS* e clique em **Adicionar...** para adicionar um servidor RADIUS.



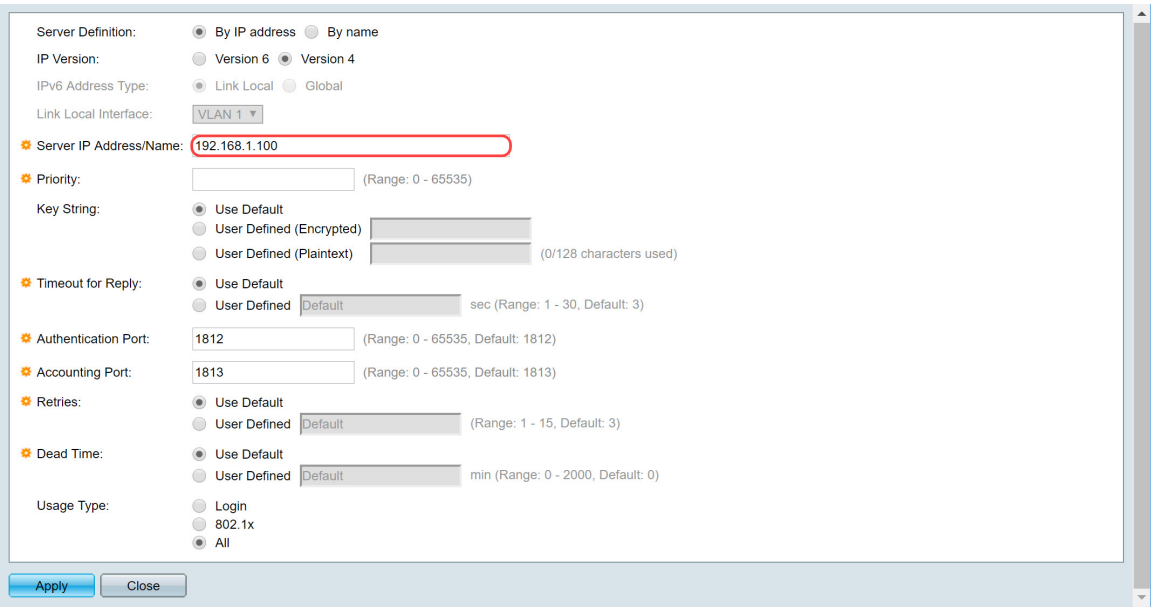
Etapa 3. (Opcional) Selecione se deseja especificar o servidor RADIUS por endereço IP ou nome no campo *Definição do servidor*. Neste exemplo, manteremos a seleção padrão de **Por endereço IP**.



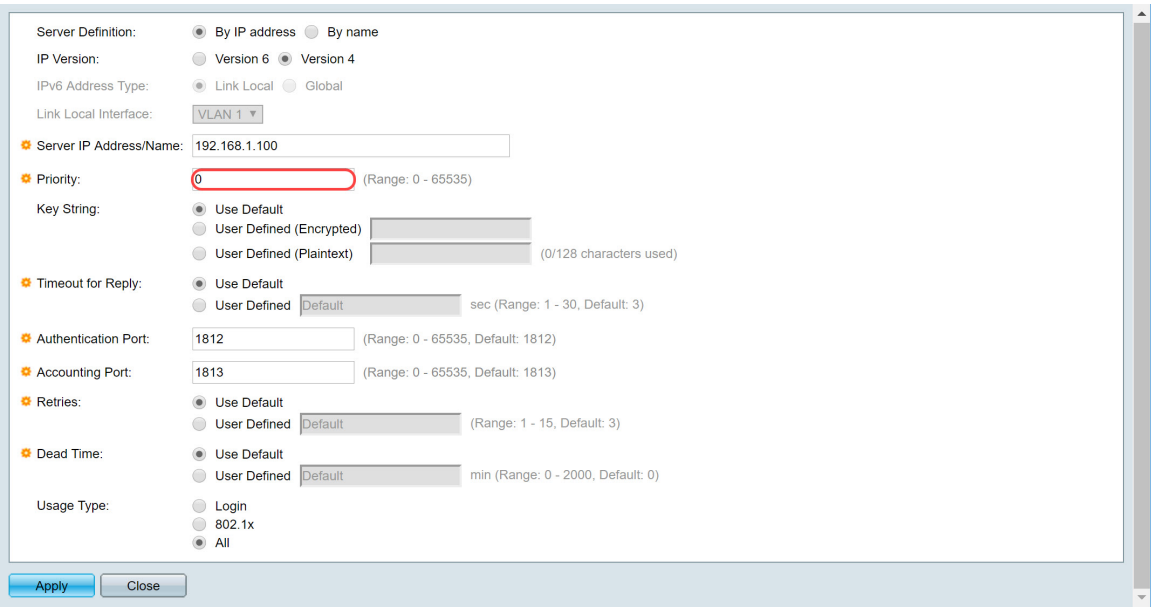
Etapa 4. (Opcional) Selecione a versão do endereço IP do servidor RADIUS no campo *IP Version* . Manteremos a seleção padrão da **versão 4** para este exemplo.



Etapa 5. Digite no servidor RADIUS por endereço IP ou nome. Digitaremos o endereço IP de **192.168.1.100** no campo *Server IP Address/Name (Endereço IP do servidor/Nome)*.

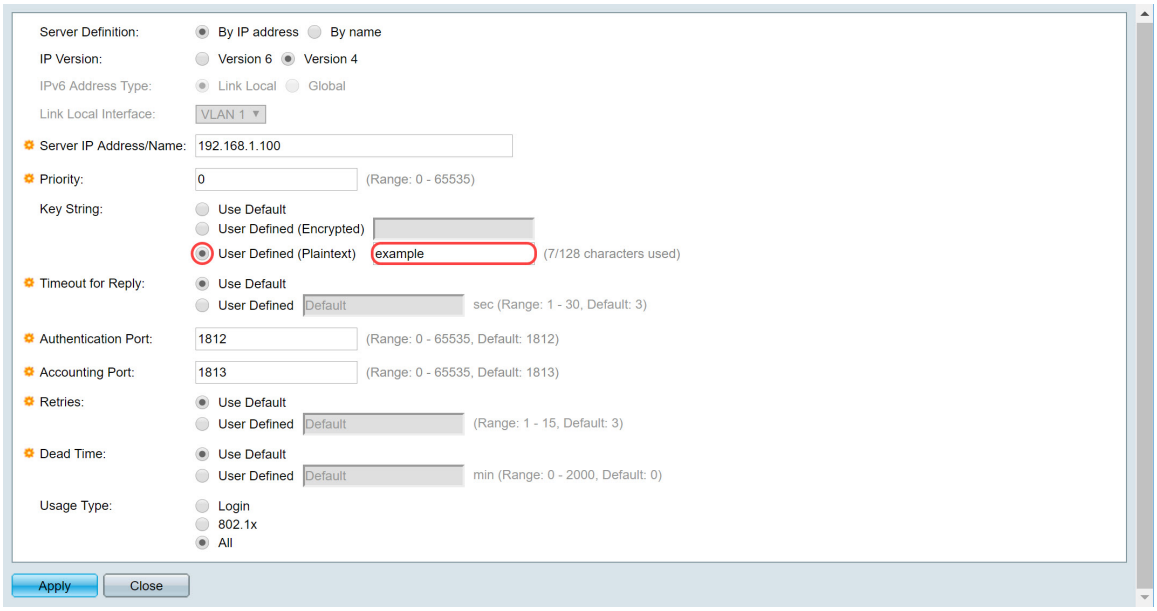


Etapa 6. Digite a prioridade do servidor. A prioridade determina a ordem em que o dispositivo tenta entrar em contato com os servidores para autenticar um usuário. O dispositivo começa com o servidor RADIUS de prioridade mais alta primeiro. Zero é a prioridade mais alta.



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 se autenticar no servidor RADIUS usando a String de chave padrão. Usaremos o **texto definido pelo usuário (texto simples)** e inseriremos o **exemplo** principal.

Note: Deixaremos o resto da configuração como padrão. Você pode configurá-los, se desejar.

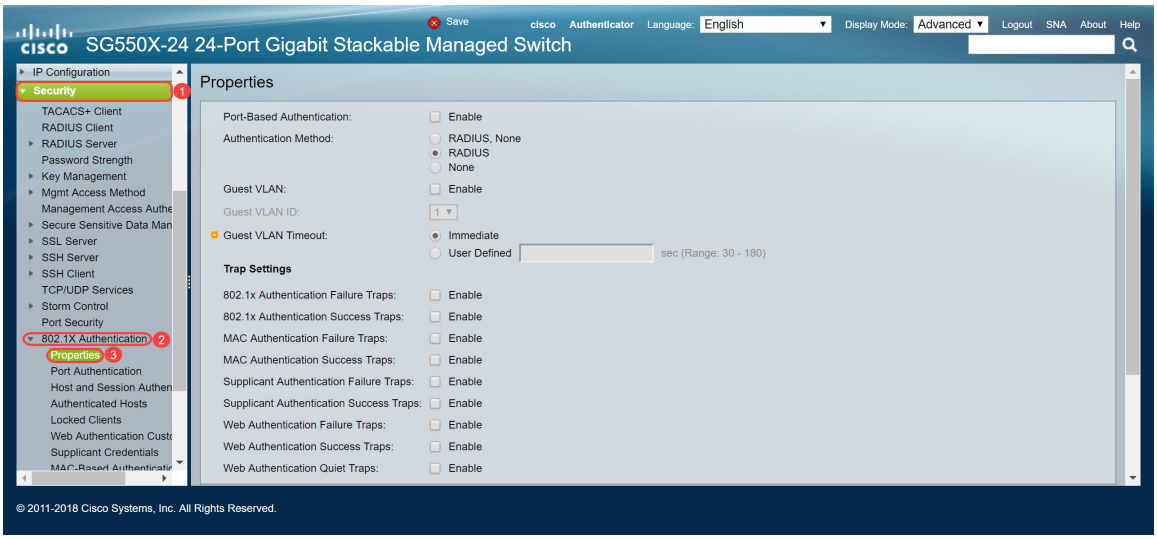


Etapa 8. Clique em **Apply** para salvar a configuração.

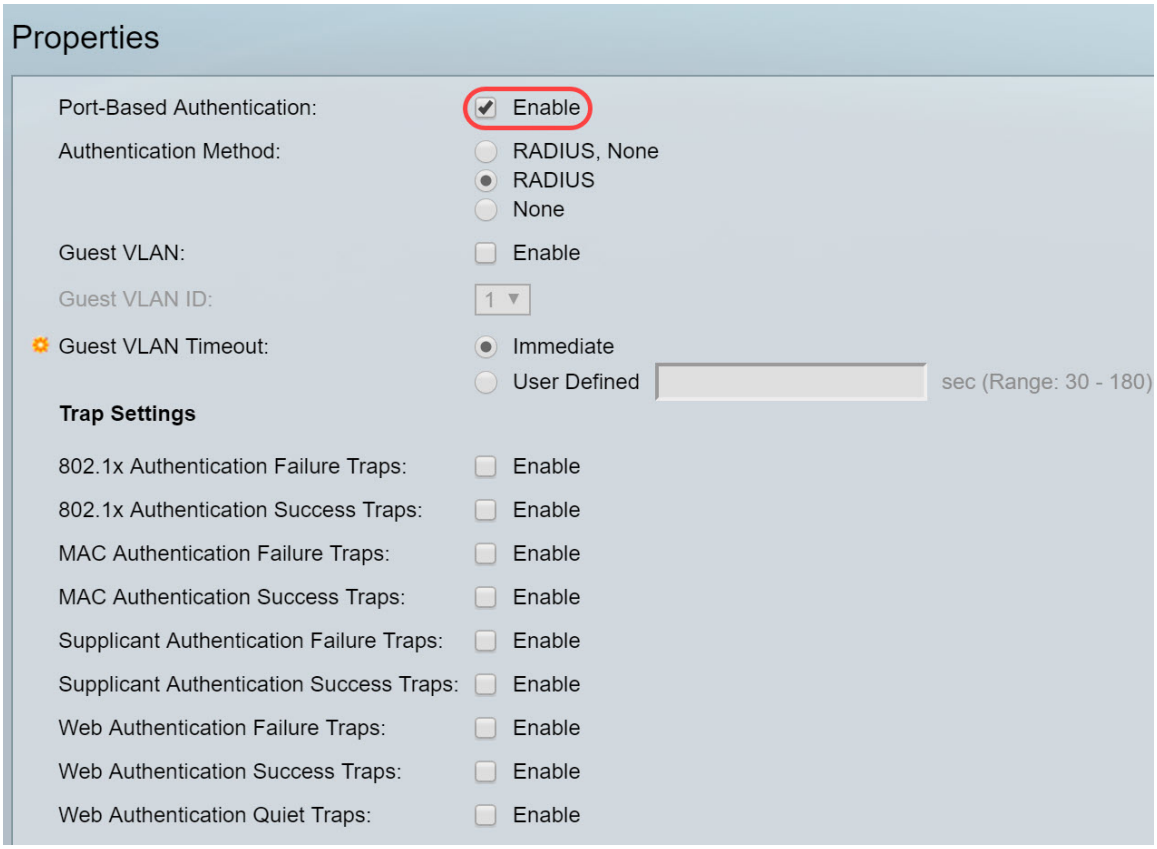
Propriedades de autenticação 802.1X

A página de propriedades é usada para habilitar globalmente a autenticação de porta/dispositivo. Para que a autenticação funcione, ela deve ser ativada global e individualmente em cada porta.

Etapa 1. Navegue até **Security > 802.1X Authentication > Properties**.

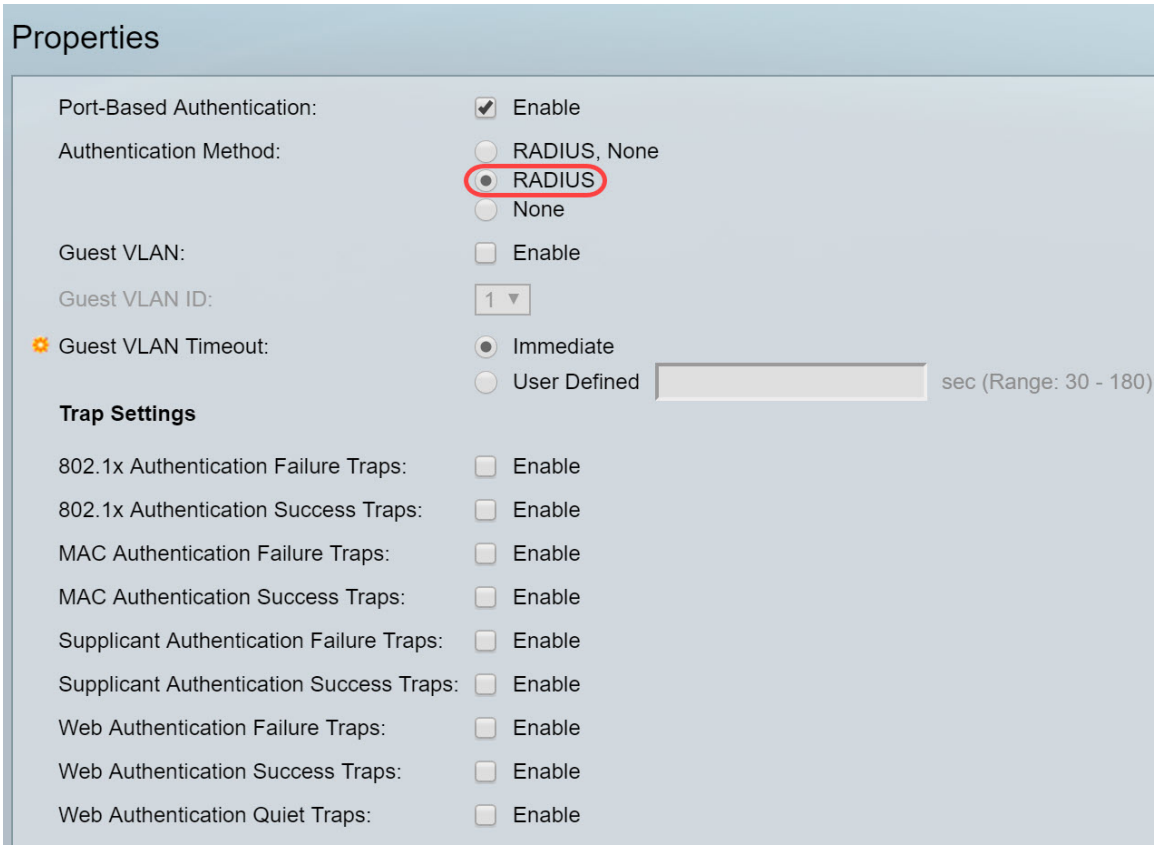


Etapa 2. Marque a caixa de seleção **Habilitar** para habilitar a autenticação baseada em porta.

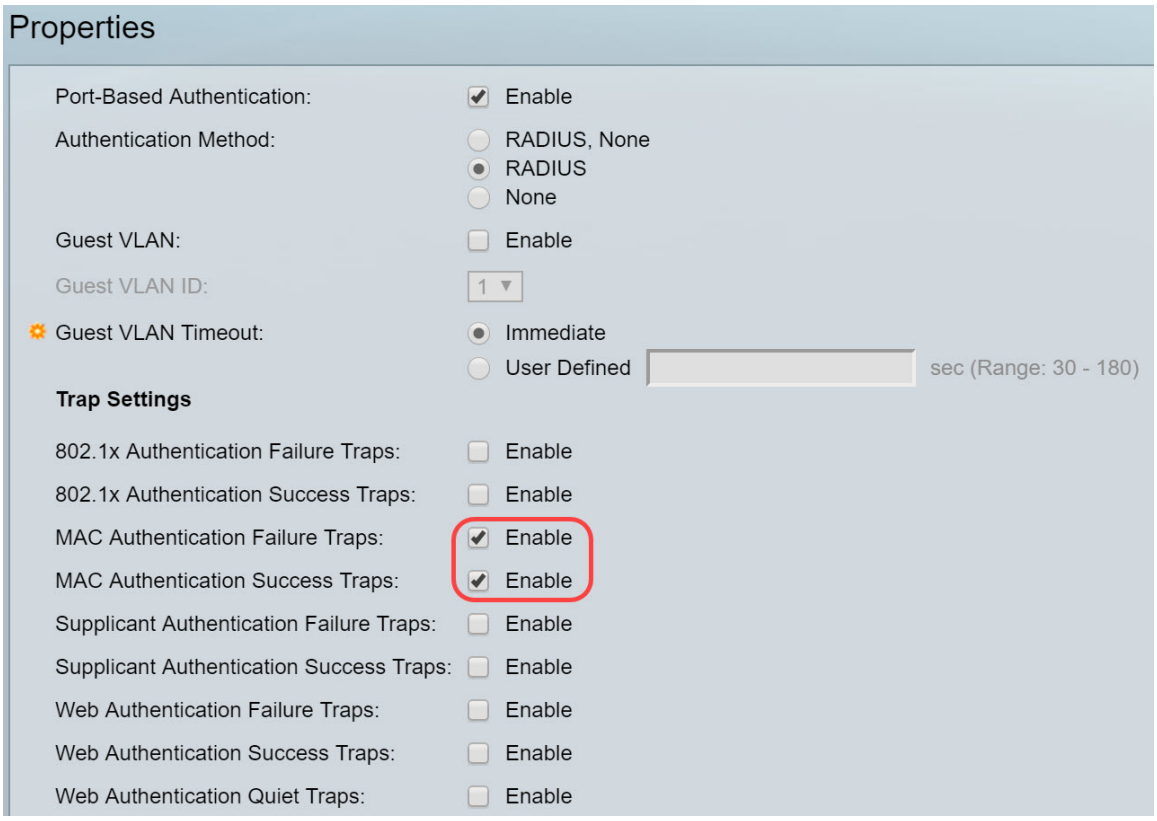


Etapa 3. Selecione os métodos de autenticação do usuário. Escolheremos o RADIUS como nosso método de autenticação. As seguintes opções são:

- RADIUS, None — Execute a autenticação de porta primeiro usando o servidor RADIUS. Se nenhuma resposta for recebida do RADIUS (por exemplo, se o servidor estiver inoperante), nenhuma autenticação será executada e a sessão será permitida. Se o servidor estiver disponível, mas as credenciais do usuário estiverem incorretas, o acesso será negado e a sessão encerrada.
- RADIUS — Autentique o usuário no servidor RADIUS. Se nenhuma autenticação for executada, a sessão não será permitida.
- Nenhum — Não autentique o usuário. Permita a sessão.



Etapa 4. (Opcional) Marque a caixa de seleção **Enable** para *MAC Authentication Failure Traps* e *MAC Authentication Success Traps*. Isso gerará uma armadilha se a autenticação MAC falhar ou for bem-sucedida. Neste exemplo, habilitaremos as armadilhas de *falha de autenticação MAC* e as *armadilhas de êxito de autenticação MAC*.

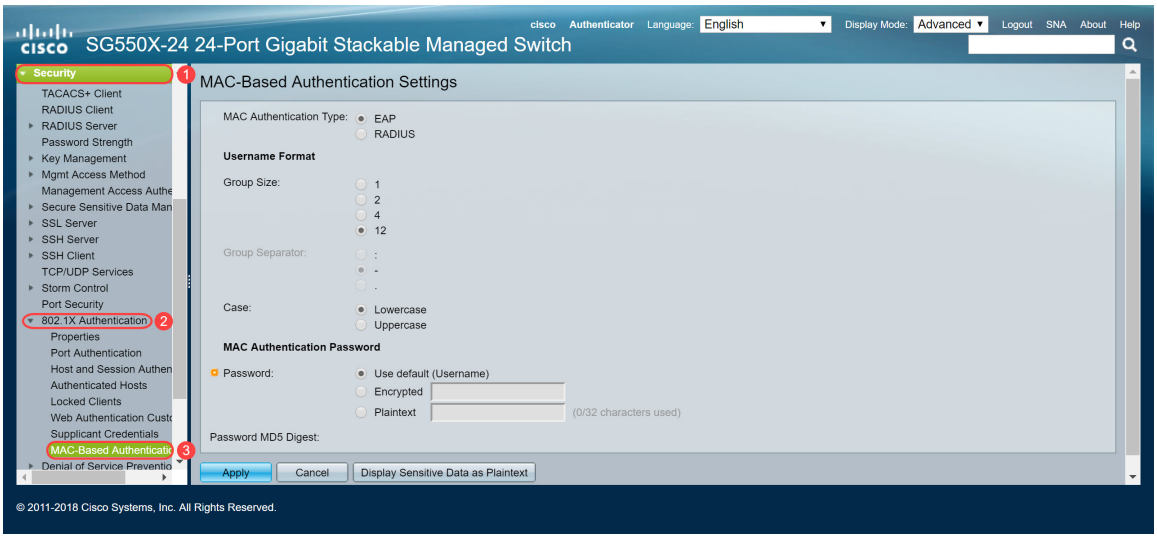


Etapa 5. Clique em Apply.

Autenticação 802.1X Configurações de Autenticação Baseada em MAC

Esta página permite que você configure várias configurações aplicáveis à autenticação baseada em MAC.

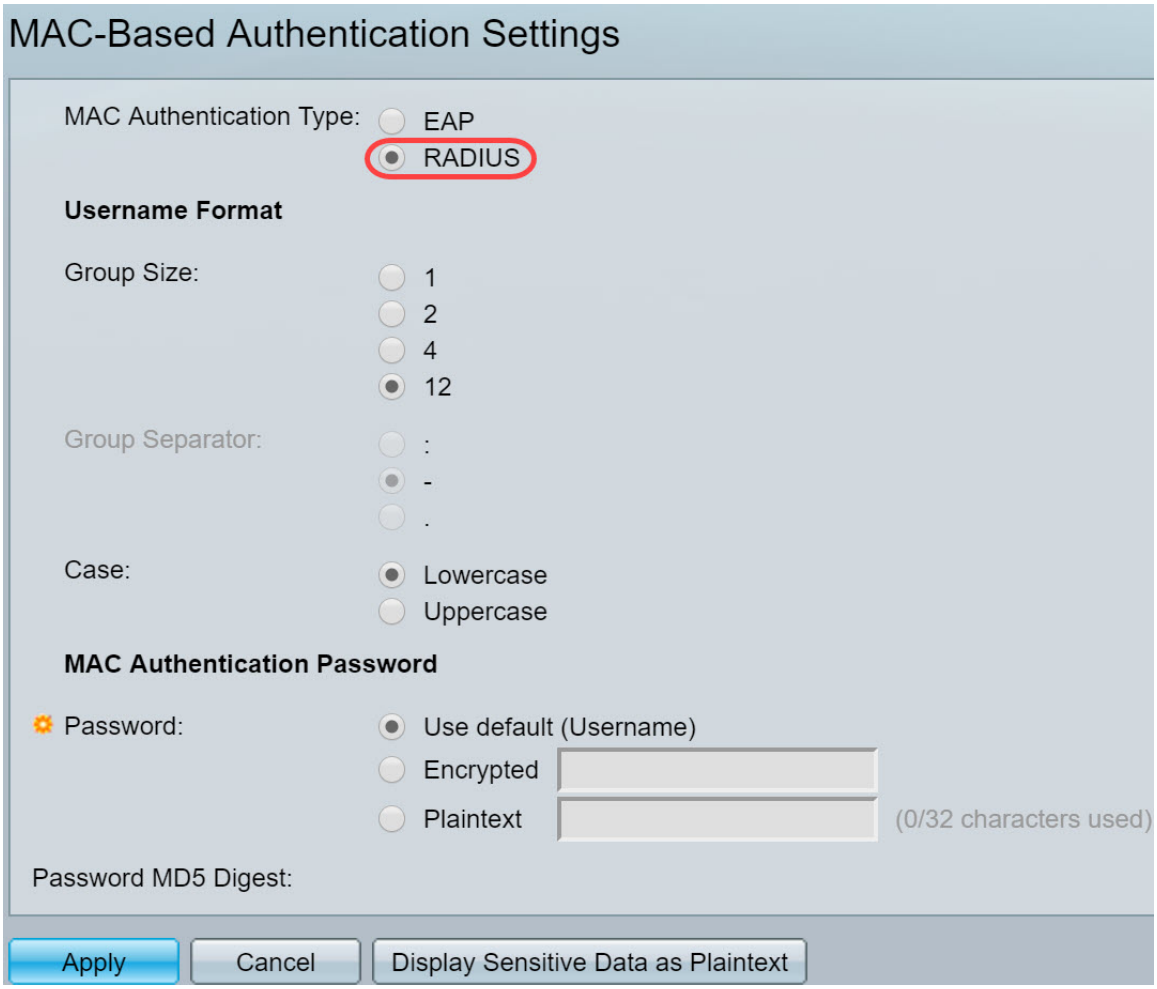
Etapa 1. Navegue até **Security > 802.1X Authentication > MAC-Based Authentication Settings**.



Etapa 2. No *MAC Authentication Type*, selecione uma das seguintes opções:

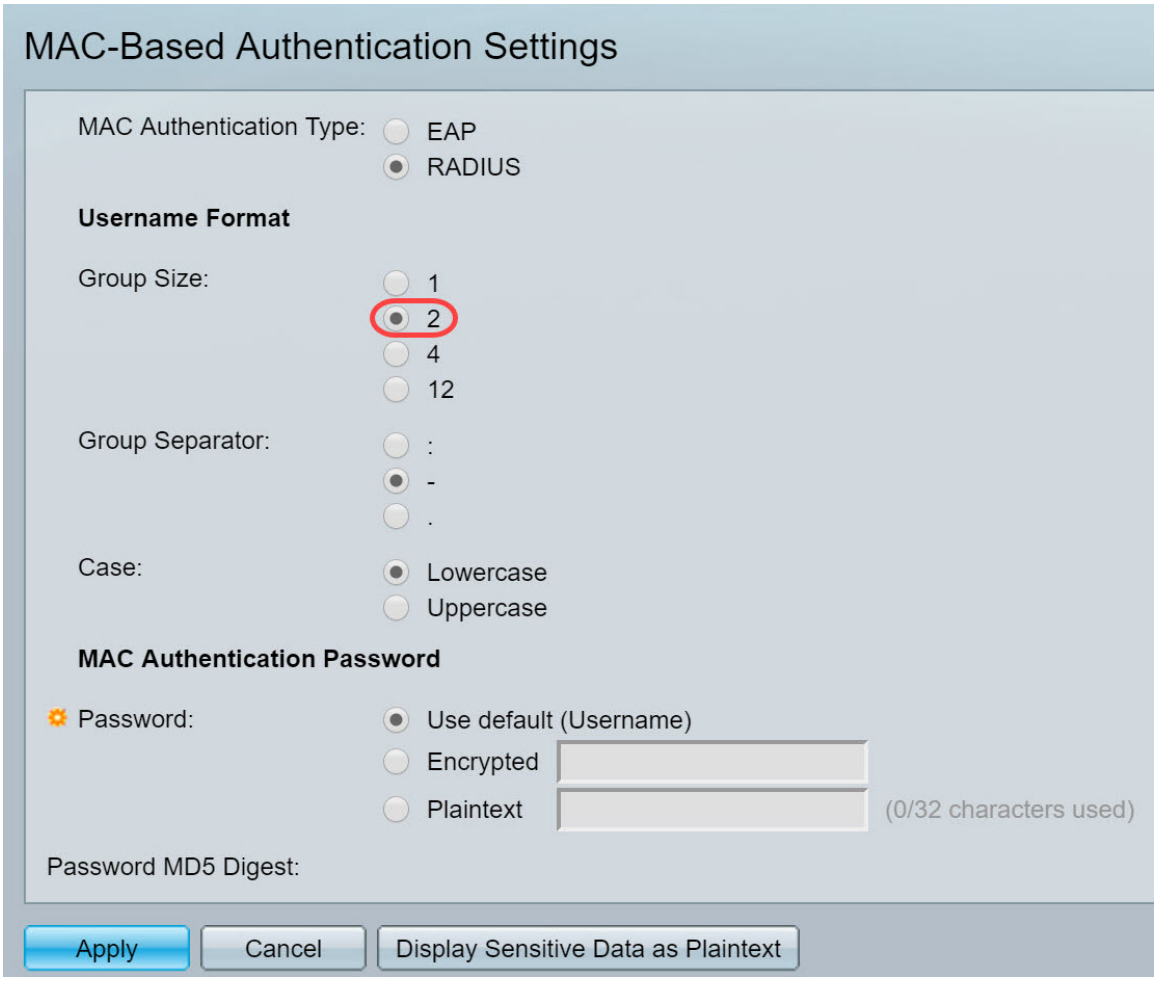
- EAP — Use RADIUS com encapsulamento EAP para o tráfego entre o switch (cliente RADIUS) e o servidor RADIUS, que autentica um suplicante baseado em MAC.
- RADIUS — use RADIUS sem encapsulamento EAP para o tráfego entre o switch (cliente RADIUS) e o servidor RADIUS, que autentica um suplicante baseado em MAC.

Neste exemplo, vamos escolher RADIUS como o tipo de autenticação MAC.

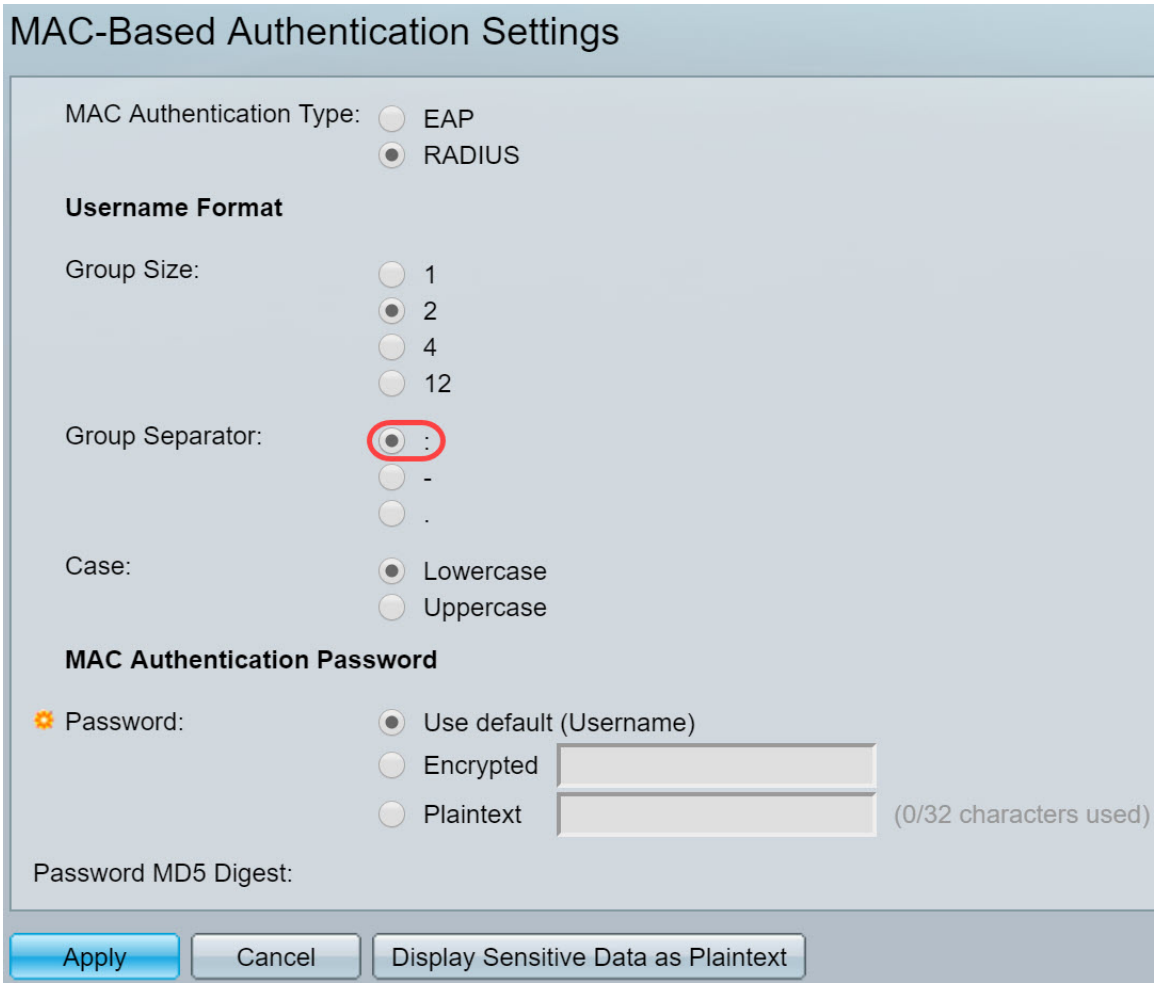


Etapa 3. No *Formato do Nome de Usuário*, selecione o número de caracteres ASCII entre delimitadores do endereço MAC enviado como nome de usuário. Neste caso, escolheremos 2 como o tamanho do nosso grupo.

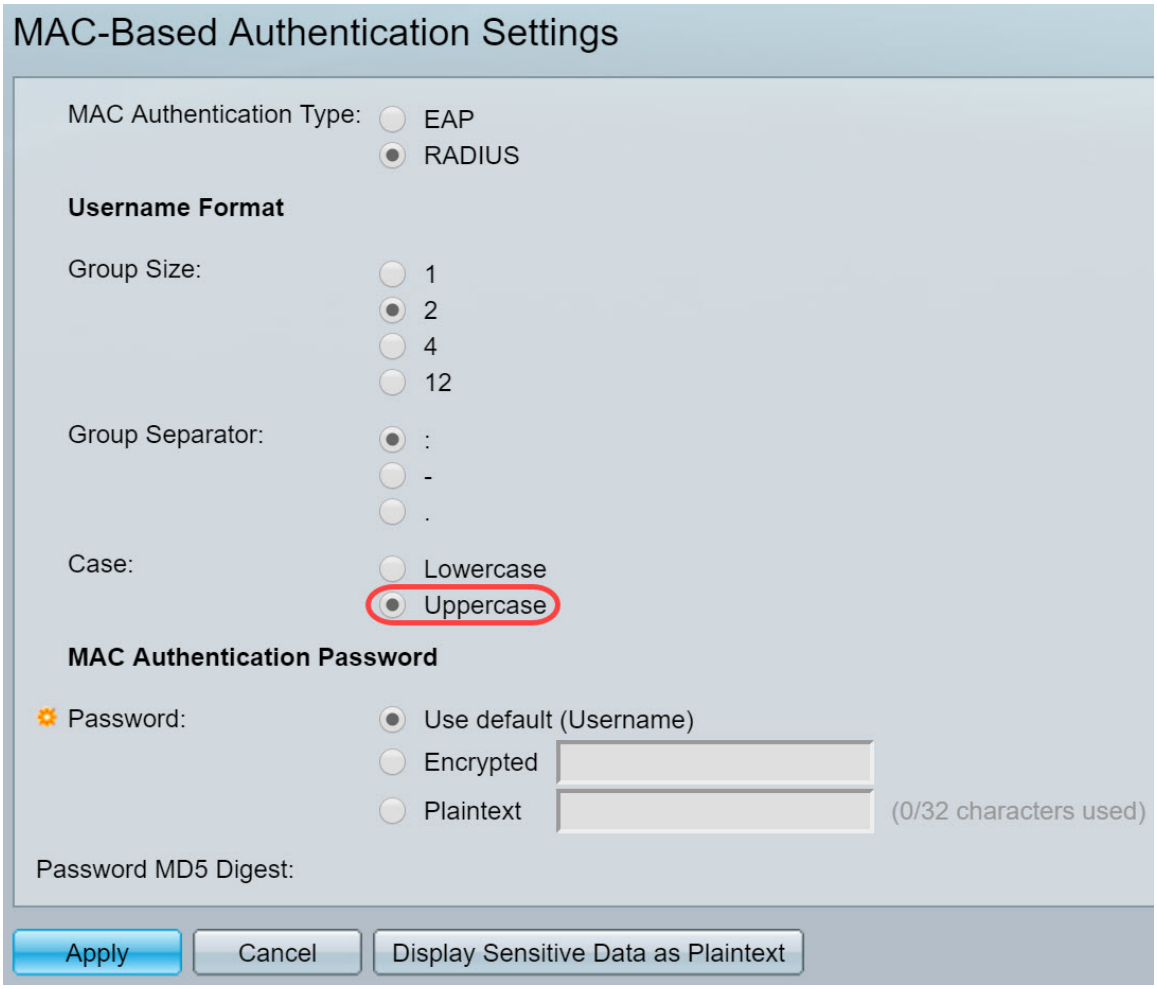
Note: Certifique-se de que o formato do nome de usuário é o mesmo que o modo como você insere o endereço MAC na seção *Usuários do servidor Radius*.



Etapa 4. Selecione o caractere usado como delimitador entre os grupos definidos de caracteres no endereço MAC. Neste exemplo, selecionaremos **:** como nosso separador de grupo.

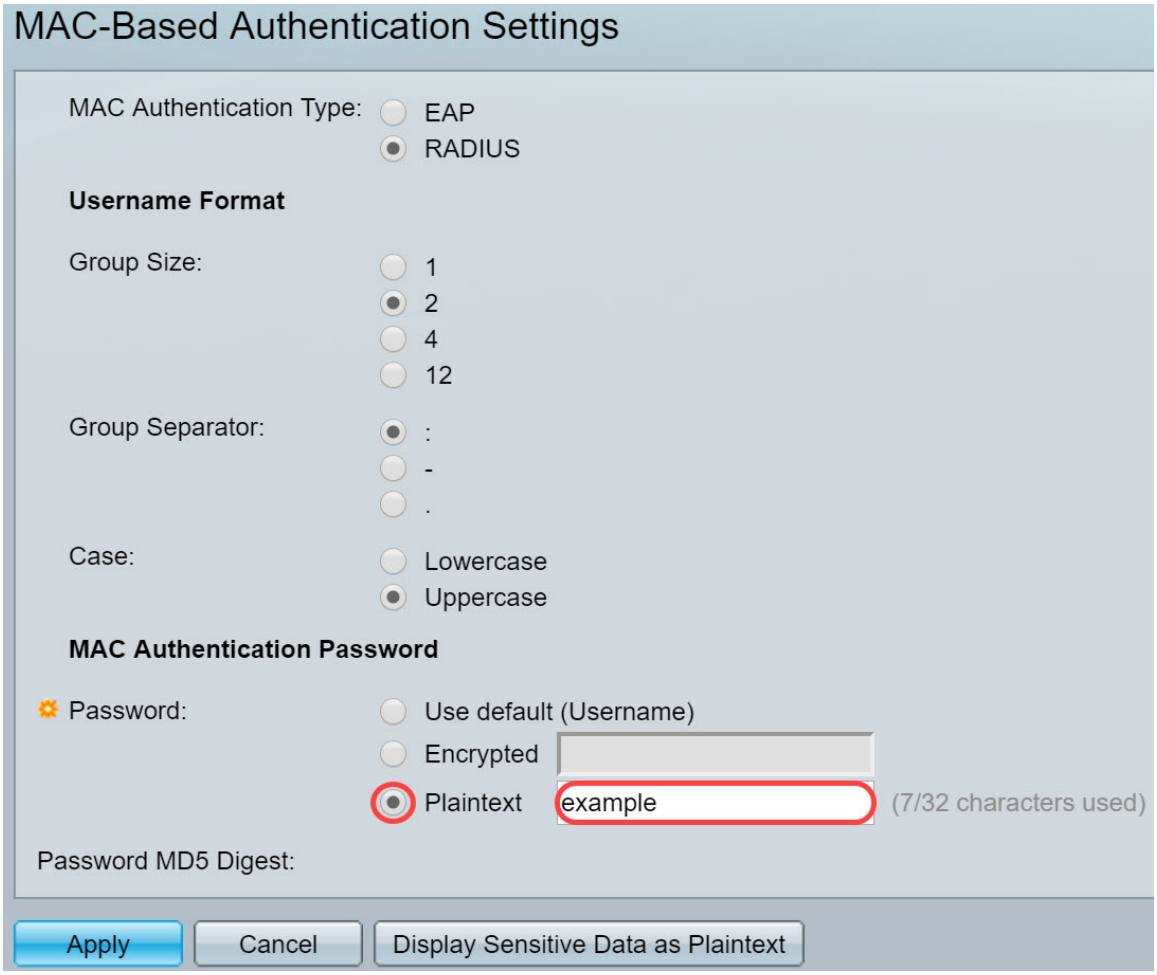


Etapa 5. No campo *Case*, selecione **Lowercase** ou **Uppercase** para enviar o nome de usuário em letras minúsculas ou maiúsculas.



Etapa 6. A senha define como o switch será usado para autenticação através do servidor RADIUS. Selecione uma das seguintes opções:

- Usar padrão (Nome de usuário) — Selecione esta opção para usar o nome de usuário definido como a senha.
- Criptografado — Defina uma senha no formato criptografado.
- Texto sem formatação — Defina uma senha no formato de texto sem formatação.



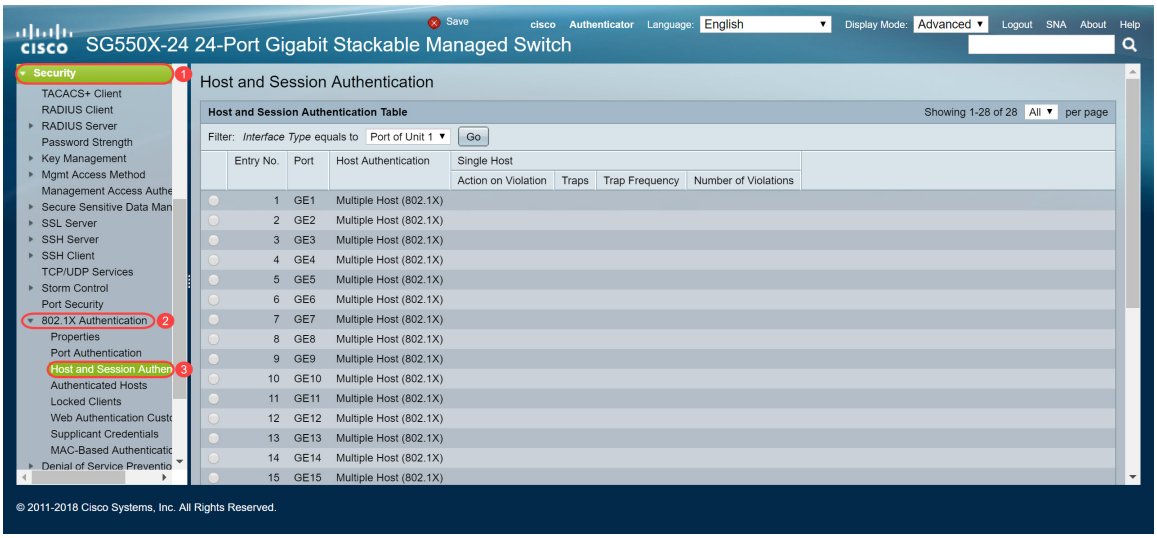
Nota: *Resumo do algoritmo 5 (MD5) de resumo de mensagem de senha* exibe a senha do sumário MD5. MD5 é uma função de hash criptográfico que pega um pedaço de dados e cria uma saída hexadecimal exclusiva que normalmente não é reproduzível. MD5 usa um valor hash de 128 bits.

Passo 7. Clique em **Apply** e as configurações serão salvas no arquivo Running Configuration.

Autenticação de host e sessão 802.1X

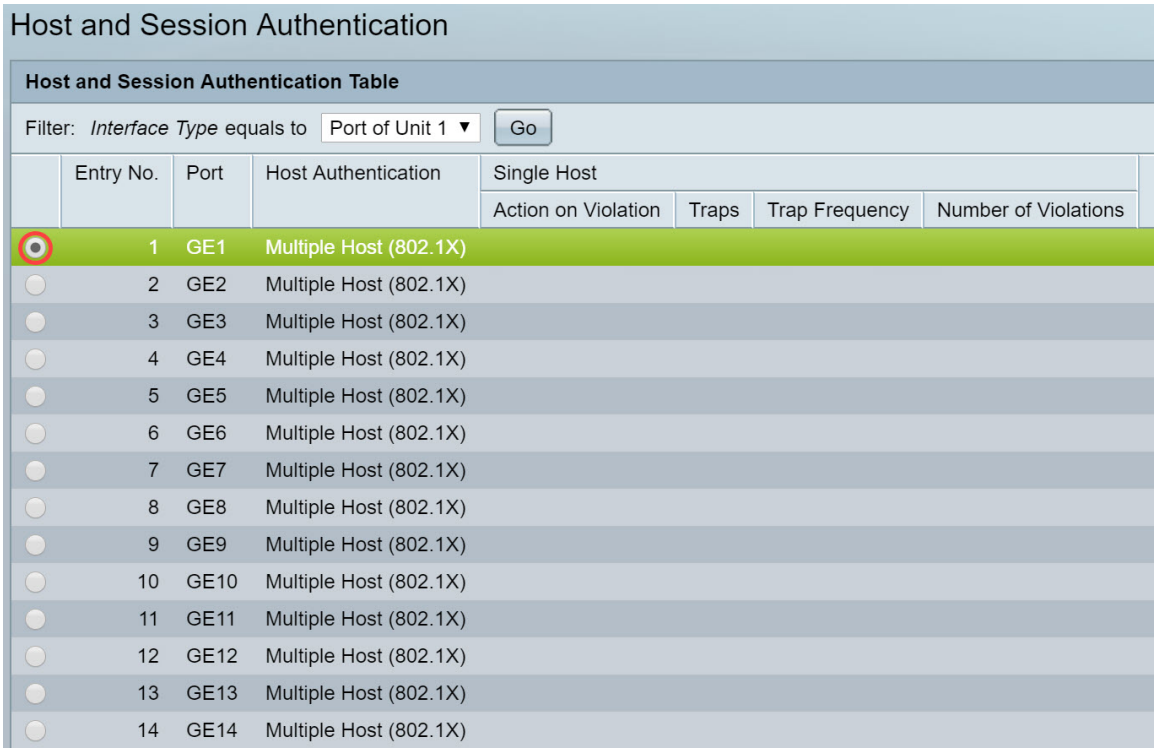
A página *Autenticação de Host e Sessão* permite definir o modo no qual o 802.1X opera na porta e a ação a ser executada se uma violação tiver sido detectada.

Etapa 1. Navegue até **Security > 802.1X Authentication > Host and Session Authentication**.

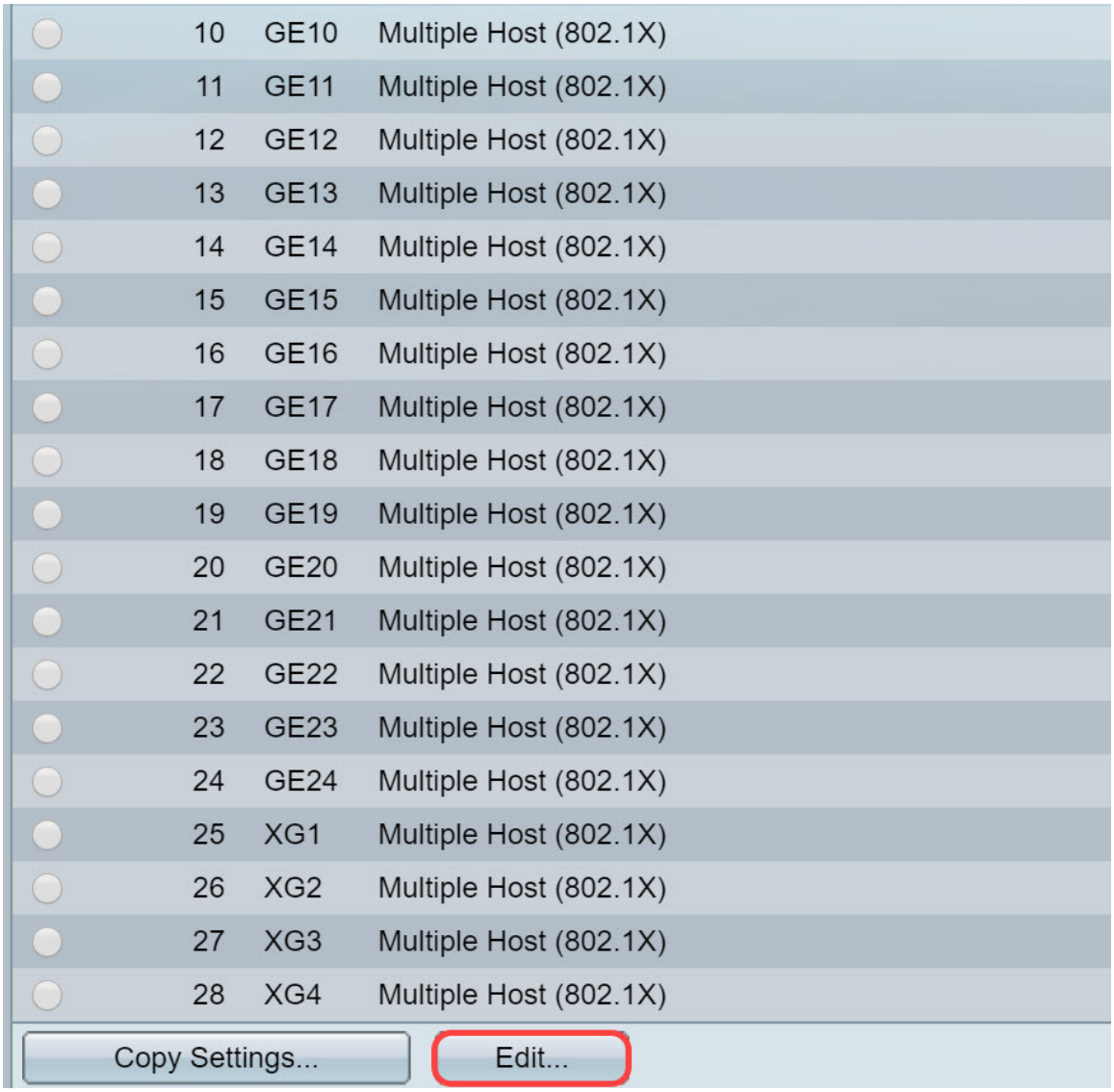


Etapa 2. Selecione a porta que deseja configurar a autenticação do host. Neste exemplo,

estaremos configurando GE1 à medida que ele é conectado a um host final.

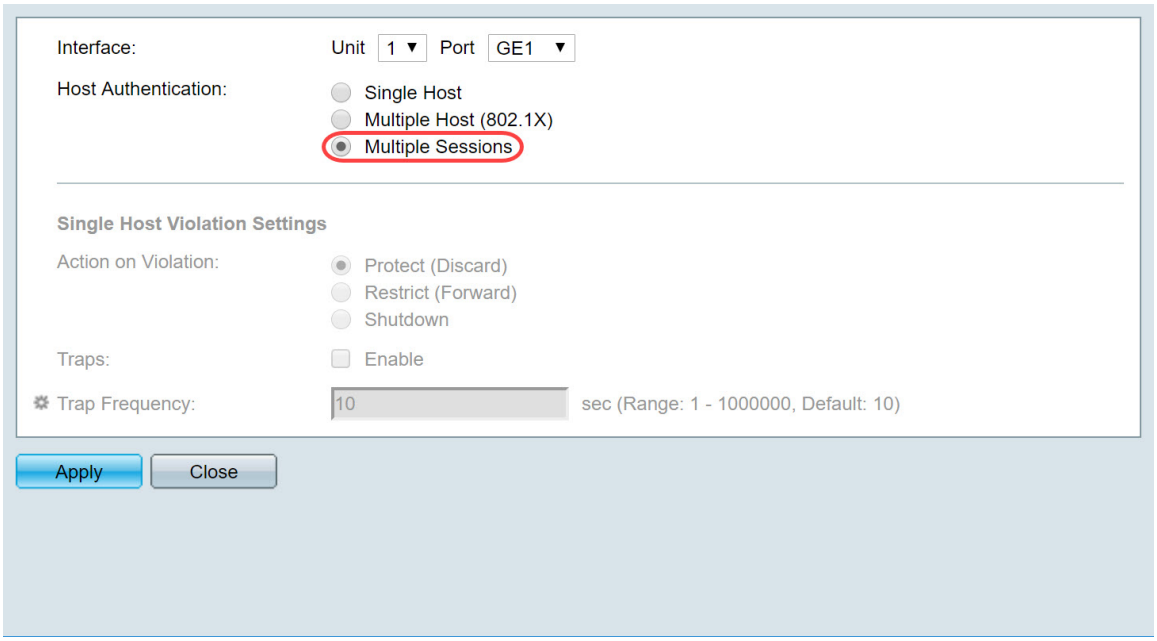


Etapa 3. Clique em **Editar...** para configurar a porta.



Etapa 4. No campo *Autenticação de host*, selecione uma das seguintes opções:

1. Modo de host único
   - Uma porta é autorizada se houver um cliente autorizado. Apenas um host pode ser autorizado em uma porta.
   - Quando uma porta não é autorizada e a VLAN de convidado está ativada, o tráfego não marcado é remapeado para a VLAN de convidado. O tráfego marcado é descartado, a menos que pertença à VLAN do convidado ou a uma VLAN não autenticada. Se uma VLAN de convidado não estiver habilitada na porta, somente o tráfego marcado pertencente às VLANs não autenticadas será interligado.
   - Quando uma porta é autorizada, o tráfego não marcado e marcado do host autorizado é interligado com base na configuração da porta de associação de VLAN estática. O tráfego de outros hosts é descartado.
   - Um usuário pode especificar que o tráfego não marcado do host autorizado será remapeado para uma VLAN atribuída por um servidor RADIUS durante o processo de autenticação. O tráfego marcado é descartado, a menos que pertença à VLAN atribuída ao RADIUS ou às VLANs não autenticadas. A atribuição de VLAN Radius em uma porta está definida na Página *de Autenticação de Porta*.
2. Modo multihost
   - Uma porta é autorizada se houver pelo menos um cliente autorizado.
   - Quando uma porta não é autorizada e uma VLAN de convidado é ativada, o tráfego não marcado é remapeado para a VLAN de convidado. O tráfego marcado é descartado, a menos que pertença à VLAN do convidado ou a uma VLAN não autenticada. Se a VLAN de convidado não estiver habilitada em uma porta, somente o tráfego marcado pertencente a VLANs não autenticadas será interligado.
   - Quando uma porta é autorizada, o tráfego não marcado e marcado de todos os hosts conectados à porta é ligado em ponte, com base na configuração da porta de associação da VLAN estática.
   - Você pode especificar que o tráfego não marcado da porta autorizada será remapeado para uma VLAN atribuída por um servidor RADIUS durante o processo de autenticação. O tráfego marcado é descartado, a menos que pertença à VLAN atribuída ao RADIUS ou às VLANs não autenticadas. A atribuição de VLAN Radius em uma porta é definida na página *Autenticação de porta*.
3. Modo multissessões
   - Diferentemente dos modos de host único e de host múltiplo, uma porta no modo de multisessão não tem um status de autenticação. Esse status é atribuído a cada cliente conectado à porta.
   - O tráfego marcado pertencente a uma VLAN não autenticada é sempre interligado, independentemente de o host ser autorizado ou não.
   - O tráfego marcado e não marcado de hosts não autorizados que não pertencem a uma VLAN não autenticada é remapeado para a VLAN de convidado se estiver definido e ativado na VLAN ou é descartado se a VLAN de convidado não estiver habilitada na porta.
   - Você pode especificar que o tráfego não marcado da porta autorizada será remapeado para uma VLAN atribuída por um servidor RADIUS durante o processo de autenticação. O tráfego marcado é descartado, a menos que pertença à VLAN atribuída ao RADIUS ou às VLANs não autenticadas. A atribuição de VLAN Radius em uma porta é definida na página *Autenticação de porta*.



Etapa 5. Clique em **Apply** para salvar sua configuração.

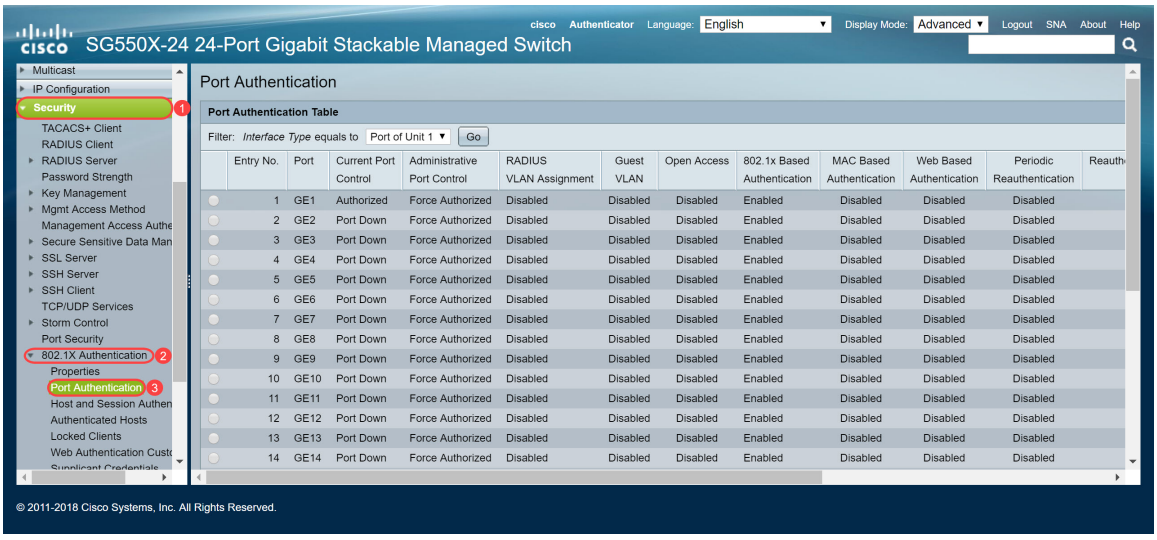
Note: Usar *as configurações de cópia...* para aplicar a mesma configuração de GE1 a várias portas. Deixe a porta conectada ao servidor RADIUS como *Host Múltiplo (802.1X)*.

Autenticação de porta de autenticação 802.1X

A página *Port Authentication* permite a configuração de parâmetros para cada porta. Como algumas das alterações de configuração só são possíveis enquanto a porta está no estado Force Authorized (Forçar autorização), como a autenticação do host, recomenda-se que você altere o controle de porta para Force Authorized (Forçar autorização) antes de fazer alterações. Quando a configuração estiver concluída, retorne o controle de porta ao seu estado anterior.

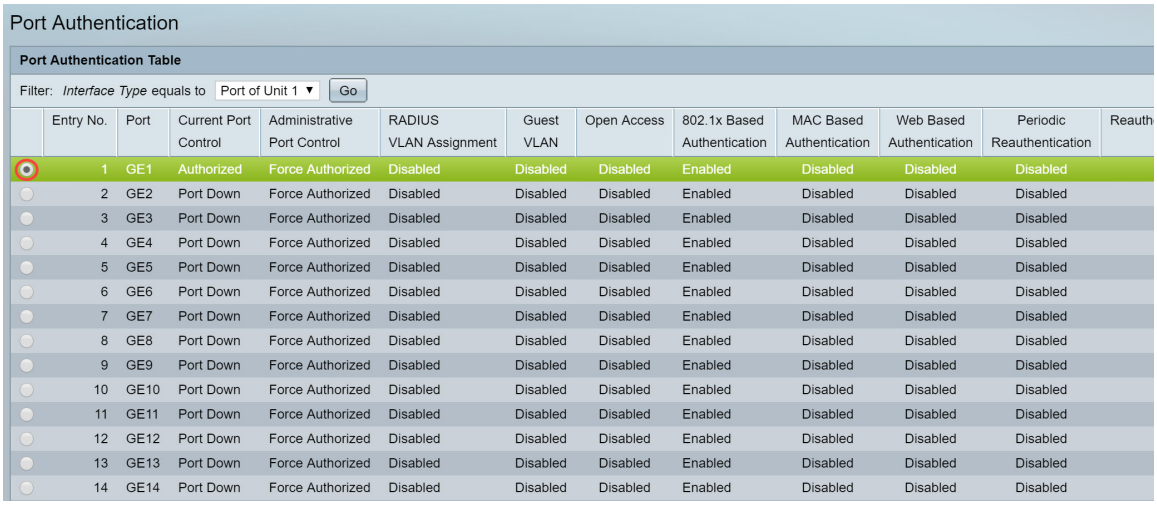
Note: Só definiremos as configurações necessárias para a autenticação baseada em MAC. O resto da configuração será deixado como padrão.

Etapa 1. Navegue até **Security > 802.1X Authentication > Port Authentication**.

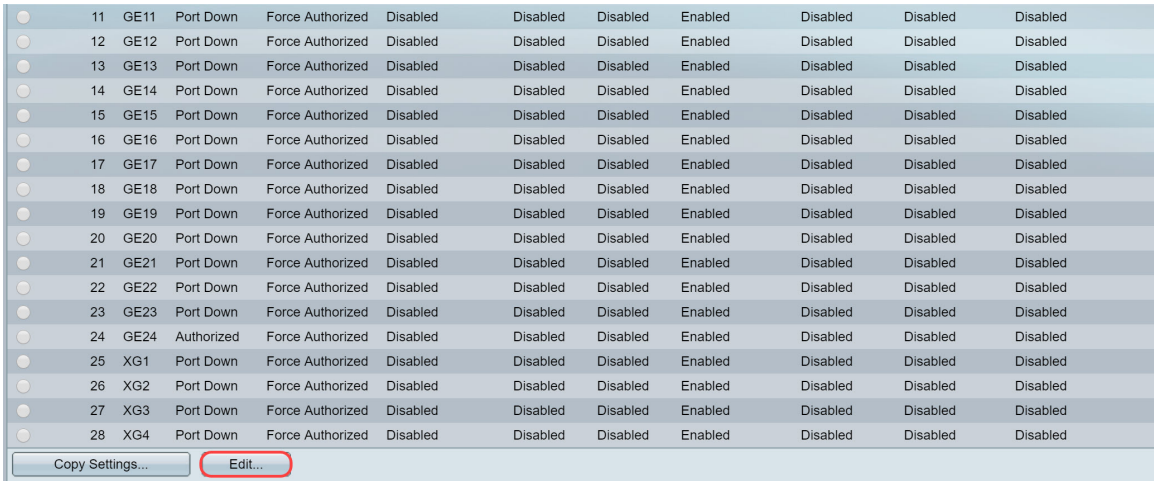


Etapa 2. Selecione a porta que deseja configurar a autorização de porta.

Note: Não configure a porta à qual o switch está conectado. O switch é um dispositivo confiável, portanto, deixe essa porta como *Autorizada Forçada*.



Etapa 3. Em seguida, role para baixo e clique em **Editar...** para configurar a porta.

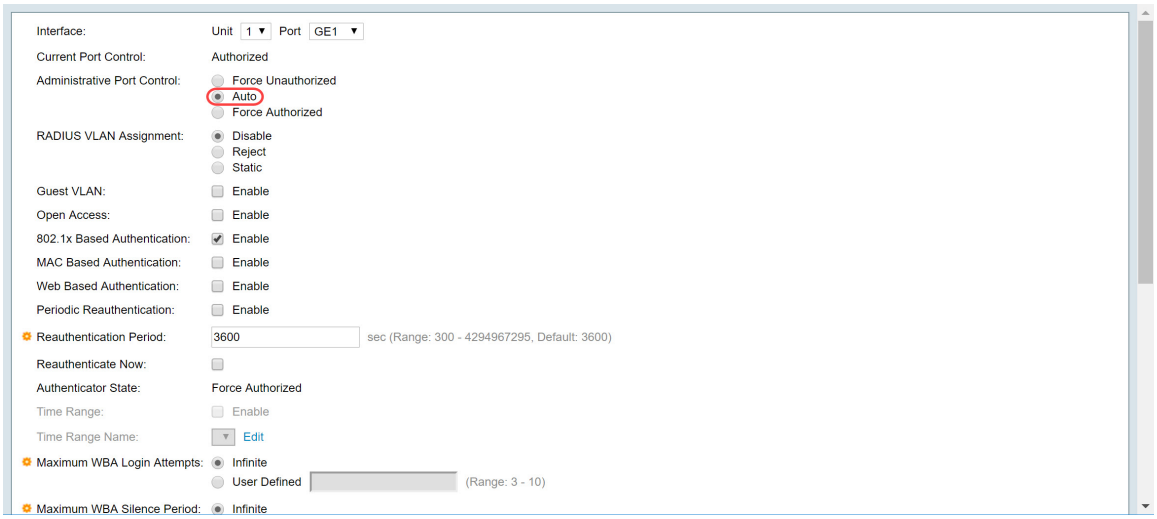


Na página *Editar autenticação de porta*, o campo *Controle de porta atual* exibe o estado de autorização de porta atual. Se o estado for *Autorizado*, a porta será autenticada ou o *Controle Administrativo de Porta* será *Forçado*. Por outro lado, se o estado for *Não autorizado*, a porta não será autenticada ou o *Controle Administrativo de Porta* será *Forçado Não Autorizado*. Se o suplicante estiver ativado em uma interface, o controle de porta atual será Suplicante.

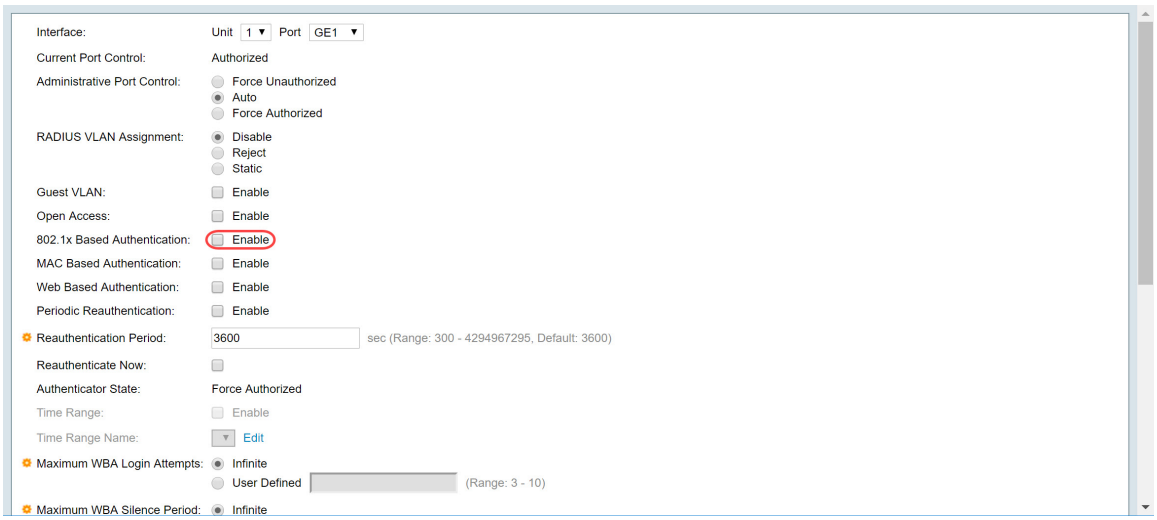
Etapa 4. Selecione o estado de autorização da porta administrativa. Configure a porta como **Auto** . As opções disponíveis são:

- Forçado não autorizado — Nega o acesso à interface movendo a interface para o estado não autorizado. O dispositivo não fornece serviços de autenticação ao cliente através da interface.
- Auto (Automático): permite autenticação e autorização baseadas em portas no dispositivo. A interface se move entre um estado autorizado ou não autorizado com base na troca de autenticação entre o dispositivo e o cliente.
- Autorizado Forçado — Autoriza a interface sem autenticação.

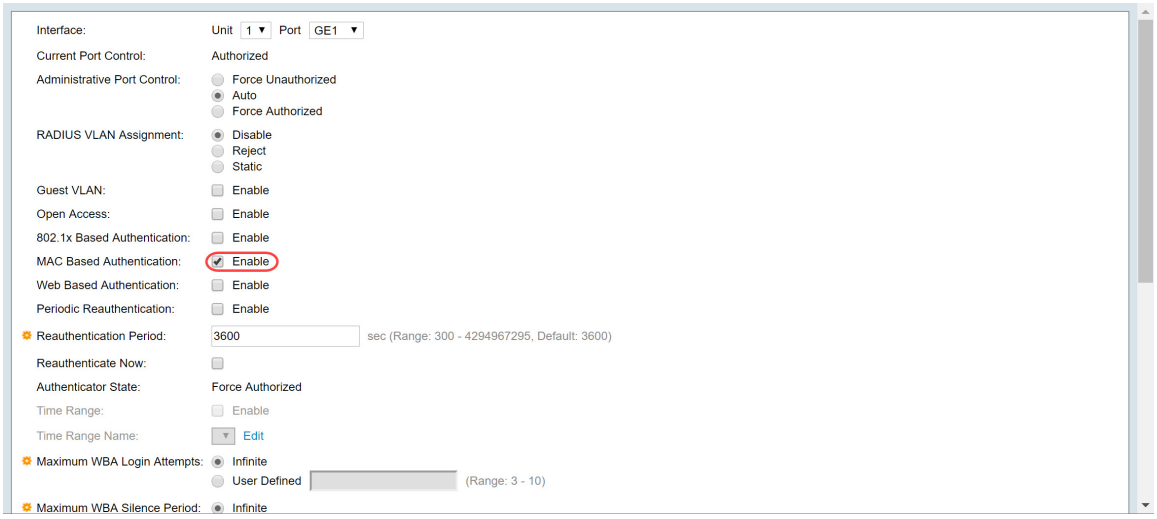
Nota: *Autorizado Forçado* é o valor padrão.



Etapa 5. No campo *802.1X Based Authentication*, desmarque a caixa de seleção **Enable**, pois não usaremos 802.1X como nossa autenticação. O valor padrão da *Autenticação Baseada em 802.1x* está ativado.



Etapa 6. Marque a caixa de seleção **Enable** for *MAC Based Authentication* as we want to enable port authentication based on the supplicant MAC address. Apenas 8 autenticações baseadas em MAC podem ser usadas na porta.



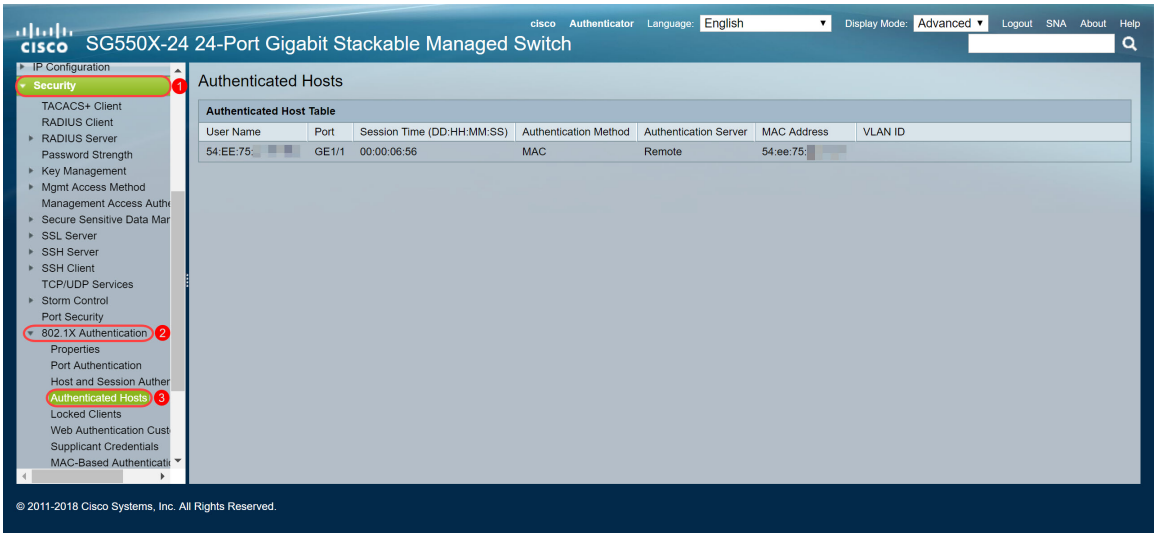
Passo 7. Clique em **Aplicar** para salvar suas alterações.

Para salvar sua configuração, pressione o botão **Save (Salvar)** na parte superior da tela.

Conclusão

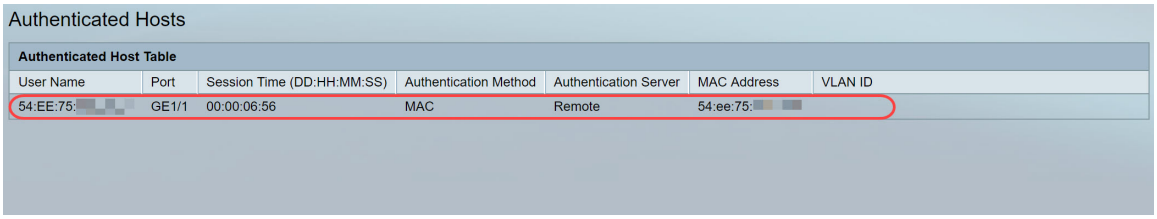
Agora, você configurou com êxito a autenticação baseada em MAC em seu switch. Para verificar se a autenticação baseada em MAC está funcionando, siga as etapas abaixo.

Etapa 1. Navegue até **Security > 802.1X Authentication > Authenticated Hosts** para exibir detalhes sobre usuários autenticados.

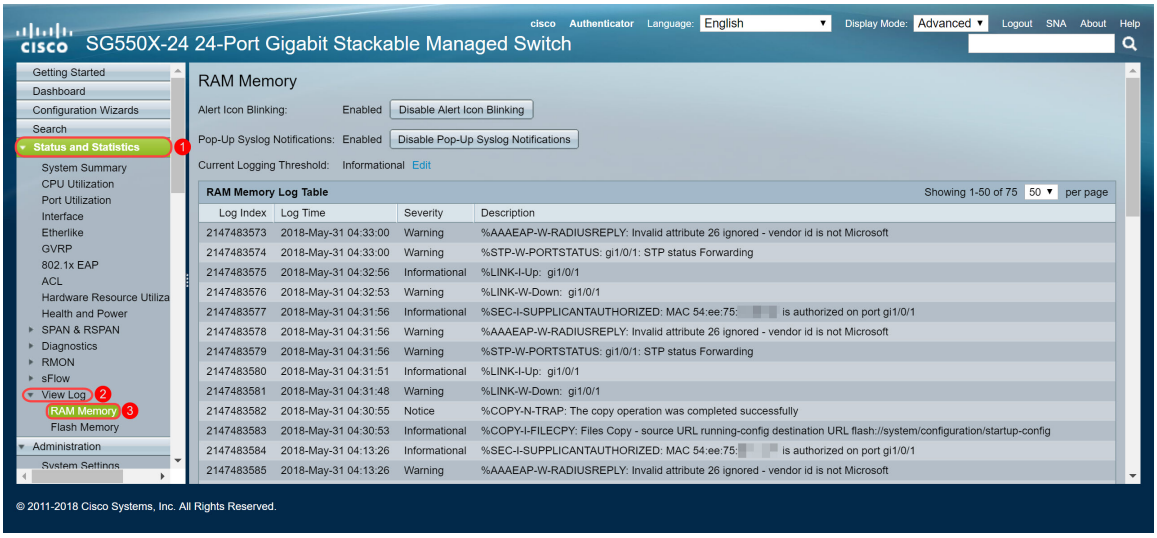


Etapa 2. Neste exemplo, você pode ver que nosso endereço MAC Ethernet foi autenticado na *Tabela de Host Autenticado*. Os campos a seguir definem como:

- Nome de usuário — Nomes de requerente autenticados em cada porta.
- Porta — Número da porta.
- Hora da sessão (DD:HH:MM:SS) — Tempo durante o qual o requerente foi autenticado e o acesso autorizado na porta.
- Método de autenticação — Método pelo qual a última sessão foi autenticada.
- Servidor autenticado — servidor RADIUS.
- Endereço MAC — Exibe o endereço MAC do suplicante.
- VLAN ID — VLAN da porta.



Etapa 3. (Opcional) Navegue até **Status e Statistics > View Log > RAM Memory**. A página *Memória RAM* exibirá todas as mensagens salvas na RAM (cache) em ordem cronológica. As entradas são armazenadas no registro da RAM de acordo com a configuração na página *Configurações de log*.



Etapa 4. Na *tabela de registro de memória RAM*, você deve ver uma mensagem de registro informacional que indica que seu endereço MAC está sendo autorizado na porta gi1/0/1.

Note: Parte do endereço MAC está desfocada.

2147483584 2018-May-31 04:13:26 Informational %SEC-I-SUPPLICANTAUTHORIZED: MAC 54:ee:75: is authorized on port gi1/0/1

Exibir a versão de vídeo deste artigo...

[Clique aqui para ver outras palestras técnicas da Cisco]