Configuração de autenticação de host e sessão 802.1X em switches 200/220/300 Series

Objetivo

802.1X é um padrão IEEE para Controle de Acesso à Rede (PNAC - Network Access Control) baseado em Porta que fornece um método de autenticação para dispositivos conectados a portas. A página Host and Session Authentication da GUI de Administração do switch é usada para definir o tipo de autenticação usado por porta. A autenticação por porta é um recurso que permite que um administrador de rede divida as portas do switch com base no tipo desejado de autenticação. A página Hosts Autenticados exibe informações sobre os hosts que foram autenticados.

Este artigo explica como configurar a autenticação de host e de sessão por porta e como visualizar os hosts autenticados nas configurações de segurança 802.1X nos Switches Gerenciados 200/220/300 Series.

Dispositivos aplicáveis

- Série Sx200
- Série Sx220
- Sx300 Series

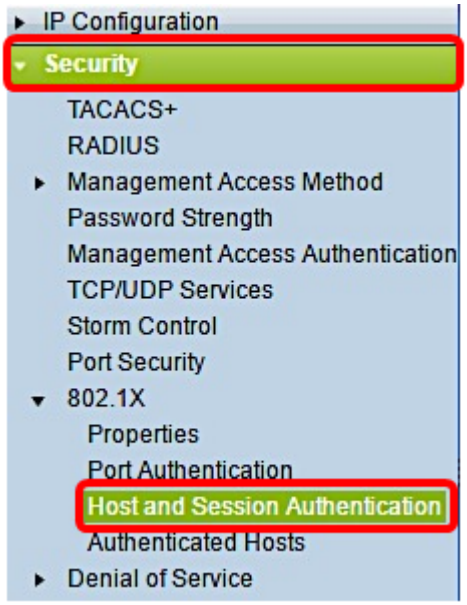
Versão de software

- 1.4.5.02 — Série Sx200, Série Sx300
- 1.1.0.14 — Série Sx220

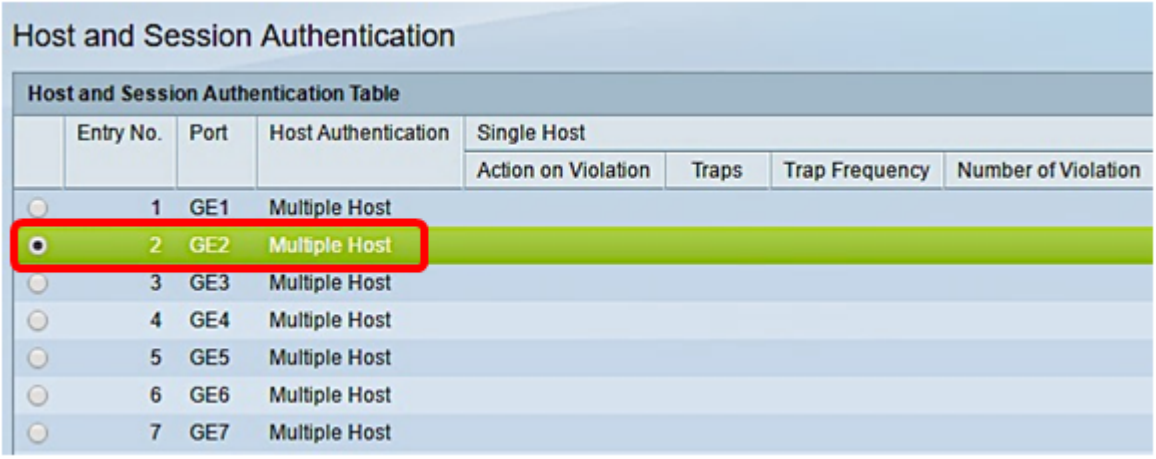
Autenticação de host e de sessão

Etapa 1. Faça login no utilitário baseado na Web e escolha **Security > 802.1X > Host and Session Authentication**.

Observação: as imagens abaixo são tiradas do switch inteligente SG220-26P.

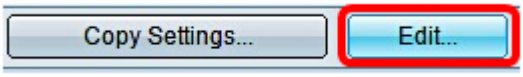


Etapa 2. Clique no botão de opção da porta que deseja editar.

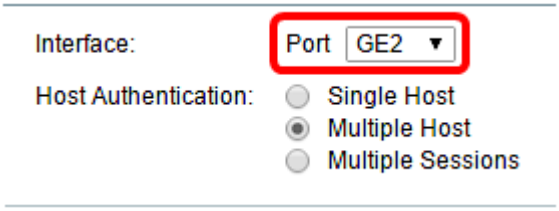


Observação: neste exemplo, a Porta GE2 é escolhida.

Etapa 3. Clique em **Editar** para editar a autenticação de host e de sessão para a porta especificada.



Etapa 4. A janela Edit Port Authentication será exibida. Na lista suspensa Interface, certifique-se de que a porta especificada seja a escolhida na Etapa 2. Caso contrário, clique na seta suspensa e escolha a porta direita.



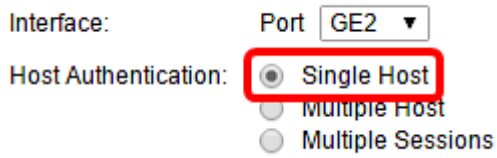
Observação: Se você estiver usando a Série 200 ou 300, a janela Editar Host e Autenticação de Sessão será exibida.

Etapa 5. Clique no botão de opção que corresponde ao modo de autenticação desejado no

campo *Host Authentication*. As opções são:

- Host único — O switch concede acesso à porta apenas a um único host autorizado.
- Vários hosts (802.1X) — Vários hosts podem obter acesso a uma única porta. Este é o modo padrão. O switch exige que apenas o primeiro host seja autorizado, e depois disso todos os outros clientes conectados à porta têm acesso à rede. Se a autenticação falhar, o acesso à rede será negado ao primeiro host e a todos os clientes conectados.
- Várias Sessões — Vários hosts podem obter acesso a uma única porta, no entanto cada host deve ser autenticado.

Observação: neste exemplo, Host único é escolhido.

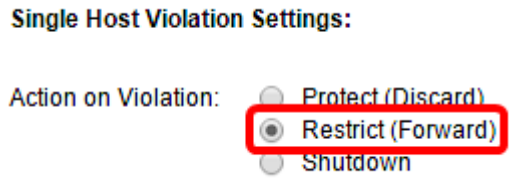


Observação: se você escolher Vários Hosts ou Várias Sessões, vá para a Etapa 9.

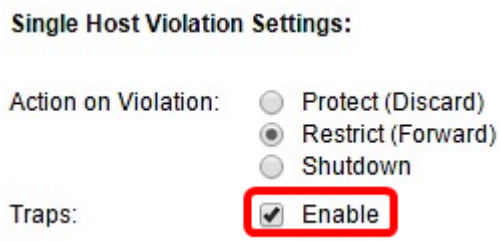
Etapa 6. Na área Configurações de violação de host, clique no botão de opção que corresponde à Ação desejada sobre violação. Uma violação ocorre se os pacotes chegarem de um host que tenha um endereço MAC que não corresponda ao endereço MAC do solicitante original. Quando isso ocorre, a ação determina o que acontece com os pacotes que chegam de hosts que não são considerados o suplicante original. As opções são:

- Proteger (Descartar) — Descarta os pacotes. Esta é a ação padrão.
- Restringir (Encaminhar) — Concede acesso e encaminha os pacotes.
- Desligar - Bloqueia os pacotes e desliga a porta. A porta permanece inativa até que seja reativada ou até que o switch seja reinicializado.

Observação: neste exemplo, Restringir (Encaminhar) é escolhido.



Etapa 7. (Opcional) Marque **Enable** no campo *Traps* para ativar armadilhas. Traps são mensagens geradas do Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol) usadas para relatar eventos do sistema. Uma interceptação (trapping) é enviada ao gerenciador SNMP do switch quando ocorre uma violação.



Etapa 8. Insira o tempo permitido desejado em segundos entre interceptações enviadas no campo *Frequência de interceptação*. Isso define a frequência com que as interceptações

são enviadas.

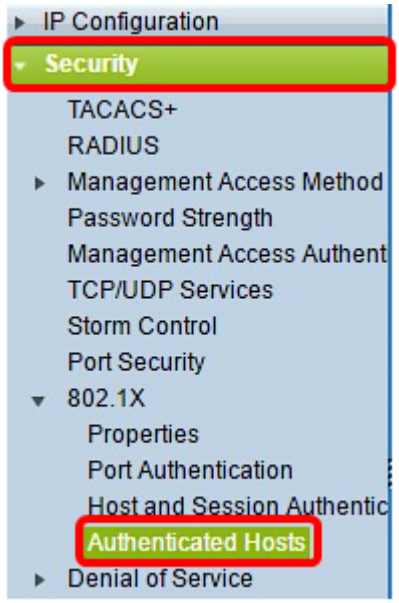
Observação: neste exemplo, são usados 30 segundos.

Etapa 9. Clique em Apply.

Agora você deve ter configurado o Host e a Autenticação de Sessão em seu switch.

Exibindo Hosts Autenticados

Etapa 1. Faça login no utilitário baseado na Web e escolha **Security > 802.1X > Authenticated Host**.



A Tabela de Hosts Autenticados exibe as seguintes informações para hosts autenticados.

- Nome de usuário — Especifica o nome do solicitante que foi autenticado na porta.
- Porta — Especifica o número da porta à qual o solicitante está conectado.
- Tempo da Sessão — Especifica o tempo inteiro em que o solicitante esteve conectado à

porta. O formato é DD:HH:MM:SS (Dia:Hora:Minuto:Segundo).

- Método de autenticação — Especifica o método usado para autenticar. Os valores possíveis são:
- Nenhum — Especifica que o requerente não foi autenticado.
- Radius — Especifica que o requerente foi autenticado pelo servidor RADIUS.
- Endereço MAC — Especifica o endereço MAC do requerente.
- ID da VLAN — Especifica a qual VLAN o host pertence. A coluna VLAN ID está disponível apenas nos Switches Smart Plus da série 220.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.