o host do 802.1X e a configuração da autenticação de sessão no 200/220/300 Series comutam

Objetivo

o 802.1X é um padrão de IEEE para o controle de acesso de rede com base na porta (PNAC) que fornece um método de autenticação aos dispositivos que são conectados às portas. A página do host e da autenticação de sessão na administração GUI de seu interruptor é usada para definir que tipo do autenticação é usado em uma base por porto. A autenticação da porta per. é uma característica que permita que um administrador de rede divida as portas de switch baseadas no tipo desejado de autenticação. A página autenticada dos anfitriões indica a informação sobre os anfitriões que foram autenticados.

Este artigo explica como configurar o host e a autenticação de sessão em uma base por porto e como ver os anfitriões autenticados em configurações de segurança do 802.1X no Switches controlado 200/220/300 Series.

Dispositivos aplicáveis

- Sx200 Series
- Sx220 Series
- Sx300 Series

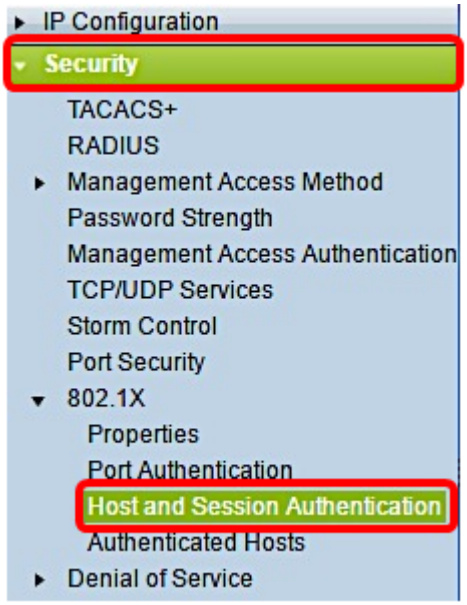
Versão de software

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

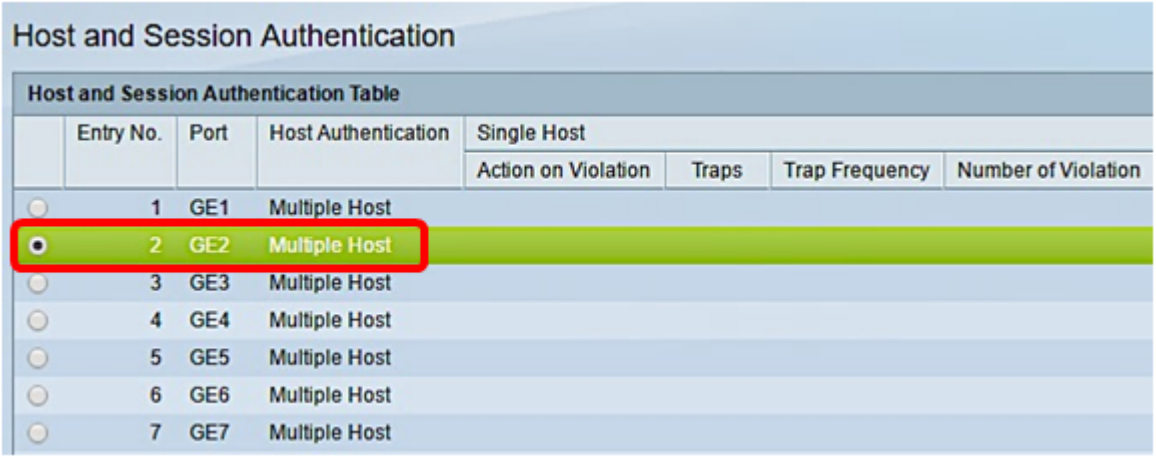
Host e autenticação de sessão

Etapa 1. Entre à utilidade com base na Web e escolha a **Segurança > o 802.1X > o host e a autenticação de sessão**.

Nota: As imagens abaixo são tomadas do interruptor SG220-26P Smart.

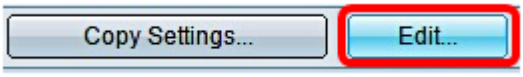


Etapa 2. Clique o botão de rádio da porta que você quer editar.

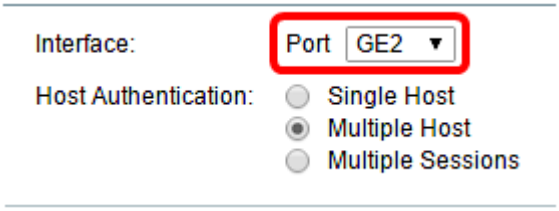


Nota: Neste exemplo, a porta GE2 é escolhida.

Etapa 3. O clique **edita** para editar o host e a autenticação de sessão para a porta especificada.



Etapa 4. A janela de autenticação da porta da edição estalará então acima. Da lista de drop-down da relação, certifique-se que a porta especificada é essa que você escolheu em etapa 2. Se não, clique a seta da gota-para baixo e escolha a porta direita.



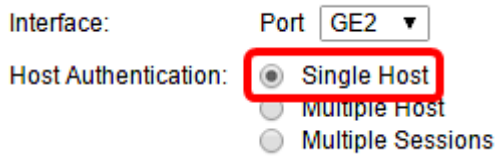
Nota: Se você está usando o 200 ou 300 Series, o indicador do host da edição e da autenticação de sessão aparece.

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

campo da *autenticação do host*. As opções são:

- Host único — O interruptor concede somente um único acesso host autorizado à porta.
- Host múltiplo (802.1X) — Os host múltiplos podem aceder à porta única. Este é o modo padrão. O interruptor exige somente o primeiro host ser autorizado, depois disso todos clientes restantes que são conectados à porta têm o acesso à rede. Se a autenticação falhar, primeiro host e todos os clientes anexados estão negados o acesso à rede.
- Sessões múltiplas — O host múltiplo pode aceder à porta única, porém cada host deve ser autenticado.

Nota: Neste exemplo, o host único é escolhido.

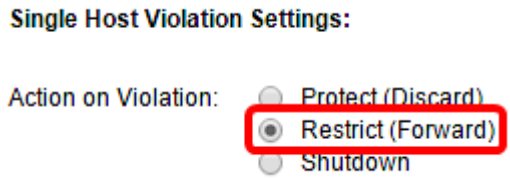


Nota: Se você escolheu o host múltiplo ou as sessões múltiplas, salte para pisar 9.

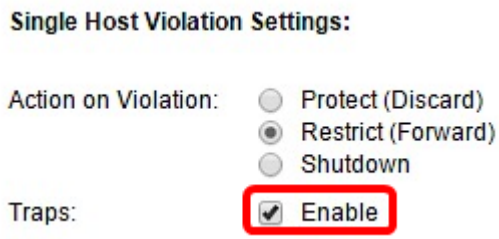
Etapa 6. Na área dos ajustes da violação do host único, clique o botão de rádio que corresponde à ação desejada na violação. Uma violação ocorre se os pacotes chegam de um host que tenha um MAC address que não combine o MAC address do suplicante original. Quando isto ocorre, a ação determina o que acontece aos pacotes que chegam dos anfitriões que não são considerados o suplicante original. As opções são:

- Proteja (descarte) — Deixa cair os pacotes. Esta é a ação padrão.
- Restrinja (dianteiro) — Dá o acesso e para a frente os pacotes.
- Parada programada — Obstrui os pacotes e fecham a porta. As sobras da porta para baixo até reactivated ou até que o interruptor estiver recarregado.

Nota: Neste exemplo, restrinja (dianteiro) é escolhido.



A verificação (opcional) de etapa 7. **permite no** campo das *armadilhas* de permitir armadilhas. As armadilhas são mensagens geradas do Simple Network Management Protocol (SNMP) usadas para relatar eventos do sistema. Uma armadilha está enviada ao SNMP Manager do interruptor quando uma violação ocorre.



Etapa 8. Incorpore o tempo desejado reservado aos segundos entre armadilhas enviadas no *campo de frequência da armadilha*. Isto define como as armadilhas são enviadas

frequentemente.

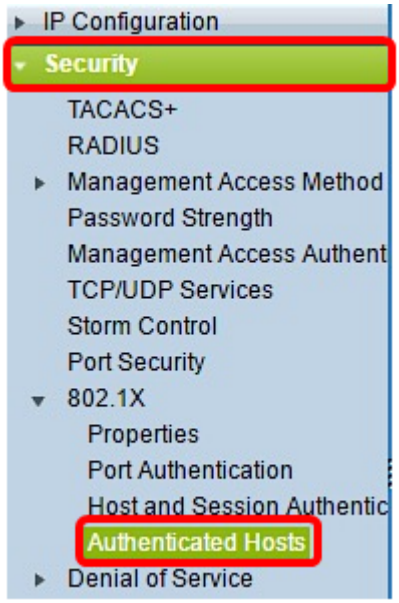
Nota: Neste exemplo, 30 segundos são usados.

Etapa 9. O clique **aplica-se**.

Você deve agora ter configurado o host e a autenticação de sessão em seu interruptor.

Vendo anfitriões autenticados

Etapa 1. Entre à utilidade com base na Web e escolha a **Segurança > o 802.1X > host autenticado**.



A tabela autenticada dos anfitriões indica a informação seguinte para anfitriões autenticados.

- Nome de usuário — Especifica o nome do suplicante que foi autenticado na porta.
- Porta — Especifica o número de porta a que o suplicante é conectado.

- Tempo de sessão — Especifica o tempo onde inteiro o suplicante foi conectado à porta. O formato é DD: HH: MILÍMETRO: SS (dia: Hora: Minuto: Em segundo).
- Método de autenticação — Especifica o método usado para autenticar. Os valores possíveis são:
- Nenhum — Especifica que o suplicante não esteve autenticado.
- Raio — Especifica que o suplicante esteve autenticado pelo servidor Radius.
- MAC address — Especifica o MAC address do suplicante.
- ID de VLAN — Especifica que VLAN o host pertence. A coluna do ID de VLAN está somente disponível no 220 Series esperto mais o Switches.