

Configurar autenticação do servidor Secure Shell (SSH) em um switch

Objetivo

Este artigo fornece instruções sobre como configurar a autenticação do servidor em um switch gerenciado, e não sobre como se conectar ao switch. Para ler um artigo sobre como se conectar a um switch via SSH + Putty, [clique aqui para ver esse artigo](#).

O Secure Shell (SSH) é um protocolo que fornece uma conexão remota segura para dispositivos de rede específicos. Essa conexão fornece uma funcionalidade semelhante a uma conexão Telnet, exceto que ela é criptografada. O SSH permite que o administrador configure o switch através da interface de linha de comando (CLI) com um programa de terceiros. O switch atua como um cliente SSH que fornece recursos SSH aos usuários na rede. O switch usa um servidor SSH para fornecer serviços SSH. Quando a autenticação do servidor SSH é desabilitada, o switch considera qualquer servidor SSH como confiável, o que diminui a segurança na rede. Se o serviço SSH estiver habilitado no switch, a segurança será aprimorada.

Dispositivos aplicáveis

- Série Sx200
- Sx300 Series
- Sx350 Series
- SG350X Series
- Sx500 Series
- Sx550X Series

Versão de software

- 1.4.5.02 - Série Sx200, Série Sx300, Série Sx500
- 2.2.0.66 - Série Sx350, Série SG350X, Série Sx550X

Configurar as definições de autenticação do servidor SSH

Habilitar serviço SSH

Quando a autenticação do servidor SSH está habilitada, o cliente SSH em execução no dispositivo autentica o servidor SSH usando o seguinte processo de autenticação:

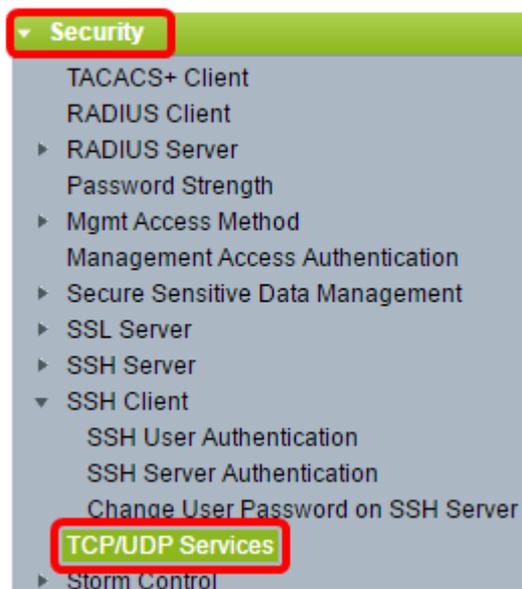
- O dispositivo calcula a impressão digital da chave pública recebida do servidor SSH.
- O dispositivo pesquisa na tabela Servidores confiáveis SSH o endereço IP e o nome de host do servidor SSH. Um dos três resultados a seguir pode ocorrer:
 1. Se for encontrada uma correspondência para o endereço e o nome do host do servidor e sua impressão digital, o servidor será autenticado.
 2. Se um endereço IP e um nome de host correspondentes forem encontrados, mas não

houver nenhuma impressão digital correspondente, a pesquisa continuará. Se nenhuma impressão digital correspondente for encontrada, a pesquisa será concluída e a autenticação falhará.

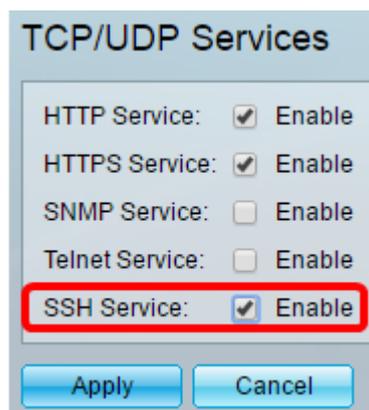
3. Se nenhum endereço IP e nome de host correspondentes forem encontrados, a pesquisa será concluída e a autenticação falhará.
 - Se a entrada para o servidor SSH não for encontrada na lista de servidores confiáveis, o processo falhará.

Nota: Para suportar a configuração automática de um switch pronto para uso com a configuração padrão de fábrica, a autenticação do servidor SSH é desabilitada por padrão.

Etapa 1. Faça login no utilitário baseado na Web e escolha **Security > TCP/UDP Services**.



Etapa 2. Marque a caixa de seleção **SSH Service** para habilitar o acesso do prompt de comando dos switches através do SSH.



Etapa 3. Clique em **Apply** para ativar o serviço SSH.

Configurar as definições de autenticação do servidor SSH

Etapa 1. Faça login no utilitário baseado na Web e escolha **Security > SSH Client > SSH Server Authentication**.



Nota: Se você tiver um Sx350, SG300X ou Sx500X, mude para o modo Avançado escolhendo **Avançado** na lista suspensa Modo de exibição.

Etapa 2. Marque a caixa de seleção **Enable** SSH Server Authentication para habilitar a autenticação do servidor SSH.

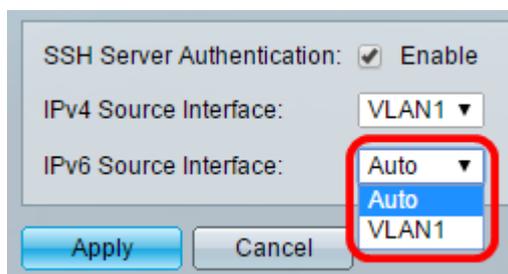


Etapa 3. (Opcional) Na lista suspensa Interface de origem IPv4, escolha a interface de origem cujo endereço IPv4 será usado como o endereço IPv4 de origem para mensagens usadas na comunicação com servidores SSH IPv4.



Nota: Se a opção Automático for escolhida, o sistema obterá o endereço IP de origem do endereço IP definido na interface de saída. Neste exemplo, VLAN1 é escolhida.

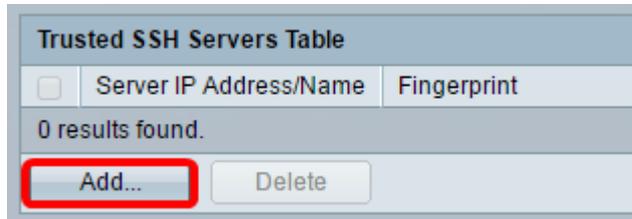
Etapa 4. (Opcional) Na lista suspensa Interface de origem IPv6, escolha a interface de origem cujo endereço IPv6 será usado como o endereço IPv6 de origem para mensagens usadas na comunicação com servidores SSH IPv6.



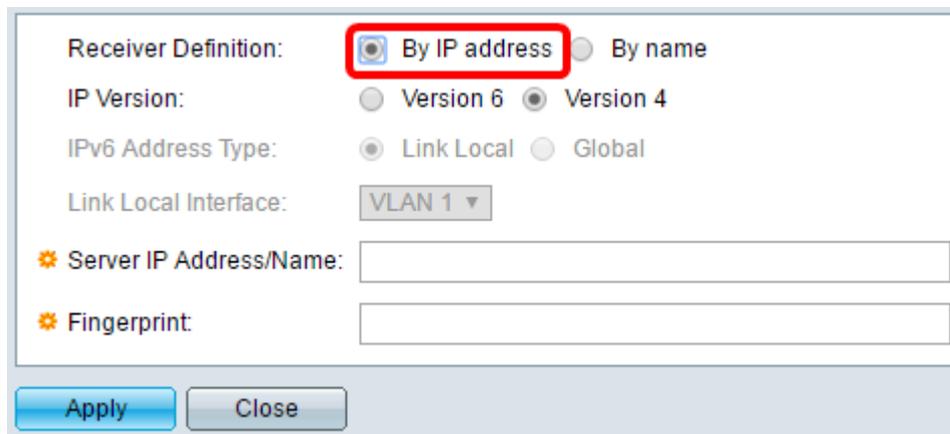
Observação: neste exemplo, a opção Automático é escolhida. O sistema usará o endereço IP origem do endereço IP definido na interface de saída.

Etapa 5. Clique em Apply.

Etapa 6. Para adicionar um servidor confiável, clique em **Add** na Tabela de Servidores SSH Confiáveis.



Passo 7. Na área Definição do receptor, clique em um dos métodos disponíveis para definir o servidor SSH:

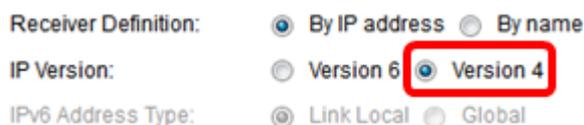


As opções são:

- Por endereço IP — Esta opção permite que você defina o servidor SSH com um endereço IP.
- Por nome — Essa opção permite definir o servidor SSH com um nome de domínio totalmente qualificado.

Observação: neste exemplo, By IP address (Por endereço IP) é escolhido. Se Por nome for escolhido, vá para a [Etapa 11](#).

Etapa 8. (Opcional) Se você escolheu Por endereço IP na Etapa 6, clique na versão IP do servidor SSH no campo Versão IP.



As opções disponíveis são:

- Versão 6 — Essa opção permite inserir um endereço IPv6.
- Versão 4 — Essa opção permite inserir um endereço IPv4.

Nota: Neste exemplo, a Versão 4 é escolhida. O botão de opção IPv6 estará disponível apenas se um endereço IPv6 estiver configurado no switch.

Etapa 9. (Opcional) Se você escolheu Versão 6 como a versão do endereço IP na Etapa 7, clique no tipo do endereço IPv6 em Tipo de endereço IPv6.

IP Version: Version 6 Version 4
IPv6 Address Type: Link Local Global
Link Local Interface:

As opções disponíveis são:

- Link Local — O endereço IPv6 identifica exclusivamente os hosts em um único link de rede. Um endereço de link local tem um prefixo FE80, não é roteável e pode ser usado para comunicação apenas na rede local. Apenas um endereço de link local é suportado. Se existir um endereço de link local na interface, essa entrada substituirá o endereço na configuração. Essa opção é escolhida por padrão.
- Global — O endereço IPv6 é um unicast global visível e acessível em outras redes.

Etapa 10. (Opcional) Se você escolher Link Local como o tipo de endereço IPv6 na Etapa 9, escolha a interface apropriada na lista suspensa Link Local Interface.

Etapa 11. No campo *Server IP Address/Name*, insira o endereço IP ou o nome de domínio do servidor SSH.

* Server IP Address/Name:
* Fingerprint:

Observação: neste exemplo, um endereço IP é inserido.

Etapa 12. No campo *Fingerprint*, insira a impressão digital do servidor SSH. Uma impressão digital é uma chave criptografada usada para autenticação. Nesse caso, a impressão digital é usada para autenticar a validade do servidor SSH. Se houver uma correspondência entre o endereço IP/Nome do servidor e a impressão digital, o servidor SSH será autenticado.

Receiver Definition: By IP address By name
IP Version: Version 6 Version 4
IPv6 Address Type: Link Local Global
Link Local Interface:
* Server IP Address/Name:
* Fingerprint:

Etapa 13. Clique em **Apply** para salvar sua configuração.

Etapa 14. (Opcional) Para excluir um servidor SSH, marque a caixa de seleção do servidor que deseja excluir e clique em **Excluir**.

Trusted SSH Servers Table		
<input checked="" type="checkbox"/>	Server IP Address/Name	Fingerprint
<input checked="" type="checkbox"/>	192.168.1.1	76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8

Etapa 15. (Opcional) Clique no botão **Save** na parte superior da página para salvar as alterações no arquivo de configuração de inicialização.

Save cisco

Port Gigabit PoE Stackable Managed Switch

SSH Server Authentication

SSH Server Authentication: Enable

IPv4 Source Interface: ▼

IPv6 Source Interface: ▼

Trusted SSH Servers Table		
<input type="checkbox"/>	Server IP Address/Name	Fingerprint
<input type="checkbox"/>	192.168.1.1	76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8

Agora você deve ter definido as configurações de autenticação do servidor SSH em seu switch gerenciado.

Exibir um vídeo relacionado a este artigo...

[Clique aqui para ver outras palestras técnicas da Cisco](#)

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.