

Configurar autenticação de usuário do Secure Shell (SSH) em um switch

Objetivo

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.

No modo CLI via SSH, o administrador pode executar configurações mais avançadas em uma conexão segura. As conexões SSH são úteis na solução de problemas de uma rede remotamente, nos casos em que o administrador da rede não está fisicamente presente no local da rede. O switch permite que o administrador autentique e gerencie usuários para se conectar à rede via SSH. A autenticação ocorre por meio de uma chave pública que o usuário pode usar para estabelecer uma conexão SSH com uma rede específica.

O recurso de cliente SSH é um aplicativo executado sobre o protocolo SSH para fornecer autenticação e criptografia de dispositivo. Ele permite que um dispositivo faça uma conexão segura e criptografada para outro dispositivo que executa o servidor SSH. Com autenticação e criptografia, o cliente SSH permite uma comunicação segura em uma conexão Telnet não segura.

Este artigo fornece instruções sobre como configurar a autenticação de usuário cliente em um switch gerenciado.

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

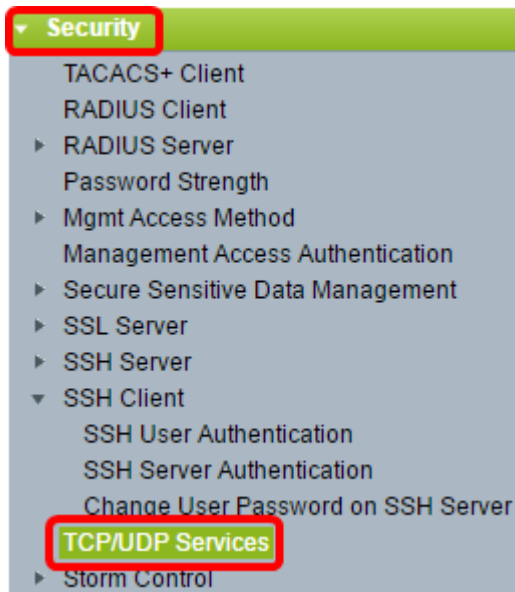
Configurar as definições de autenticação de usuário do cliente SSH

Habilitar serviço SSH

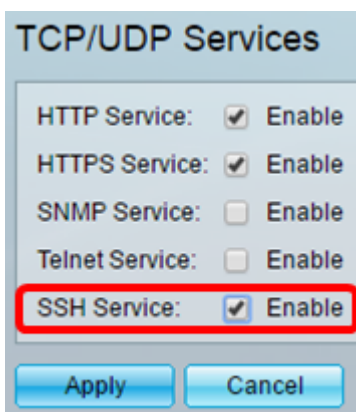
Nota: Para suportar a configuração automática de um dispositivo pronto para uso (dispositivo com configuração padrão de fábrica), a autenticação do servidor SSH é

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 de usuário SSH

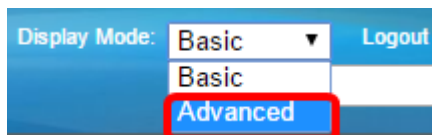
Use esta página para escolher um método de autenticação de usuário SSH. Você pode definir um nome de usuário e uma senha no dispositivo se o método de senha for escolhido. Você também pode gerar uma chave Ron Rivest, Adi Shamir e Leonard Adleman (RSA) ou Digital Signature Algorithm (DSA) se o método de chave pública ou privada estiver selecionado.

Os pares de chaves padrão RSA e DSA são gerados para o dispositivo quando ele é inicializado. Uma dessas chaves é usada para criptografar os dados que estão sendo baixados do servidor SSH. A chave RSA é usada por padrão. Se o usuário excluir uma ou ambas as chaves, elas serão geradas novamente.

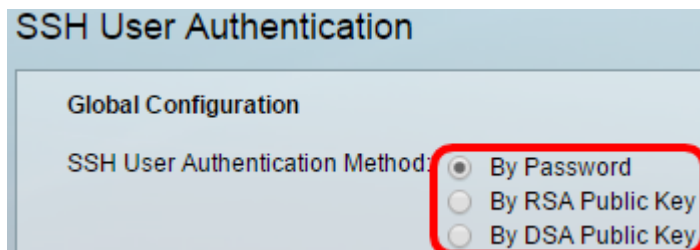
Etapa 1. Faça login no utilitário baseado na Web e escolha **Security > SSH Client > SSH User Authentication**.



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



Etapa 2. Em Global Configuration, clique no Método de autenticação de usuário SSH desejado.



Nota: Quando um dispositivo (cliente SSH) tenta estabelecer uma sessão SSH para o servidor SSH, o servidor SSH usa um dos seguintes métodos para autenticação do cliente:

- Por senha — Esta opção permite que você configure uma senha para autenticação do usuário. Essa é a configuração padrão e a senha padrão é anônima. Se essa opção for escolhida, certifique-se de que as credenciais de nome de usuário e senha tenham sido estabelecidas no servidor SSH.
- Por chave pública RSA — Esta opção permite usar a chave pública RSA para autenticação de usuários. Uma chave RSA é uma chave criptografada baseada na fatoração de inteiros grandes. Essa chave é o tipo mais comum de chave usada para a autenticação de usuário SSH.
- Por chave pública DSA — Esta opção permite usar uma chave pública DSA para autenticação do usuário. Uma chave DSA é uma chave criptografada baseada no algoritmo discreto ElGamal. Essa chave não é comumente usada para autenticação de usuário SSH, pois leva mais tempo no processo de autenticação.

Observação: neste exemplo, Por senha é escolhido.

Etapa 3. Na área Credenciais, insira o nome do usuário no campo *Nome de usuário*.

Credentials

Username: ciscosbuser1 (0/70 characters used)

Password: Encrypted AUy3Nne84DHjTuVuzd1A
 Plaintext (Default Password)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

Observação: neste exemplo, ciscosbuser1 é usado.

Etapa 4. (Opcional) Se você escolher Por senha na Etapa 2, clique no método e insira a senha no campo *Criptografado* ou *Texto simples*.

Password: Encrypted AUy3Nne84DHjTuVuzd1A
 Plaintext Ci\$C0\$B\$wi+ch

As opções são:

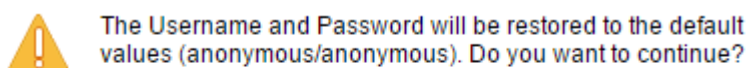
- Criptografada — Esta opção permite que você insira uma versão criptografada da senha.
- Texto sem formatação — Esta opção permite que você insira uma senha de texto sem formatação.

Observação: neste exemplo, Texto sem formatação é escolhido e uma senha de texto sem formatação é inserida.

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

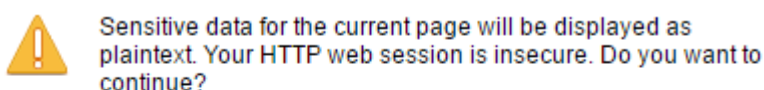
Etapa 6. (Opcional) Clique em **Restaurar credenciais padrão** para restaurar o nome de usuário e a senha padrão e clique em **OK** para continuar.

Nota: O nome de usuário e a senha serão restaurados para os valores padrão: anônimo/anônimo.



OK Cancel

Etapa 7. (Opcional) Clique em **Exibir Dados Confidenciais como Texto sem Formatação** para mostrar os dados confidenciais da página em formato de texto sem formatação e clique em **OK** para continuar.



Don't show me this again

OK Cancel

Configurar tabela de chave de usuário SSH

Etapa 8. Marque a caixa de seleção da chave que deseja gerenciar.

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb

Generate Edit... Delete Details

Observação: neste exemplo, RSA é escolhido.

Etapa 9. (Opcional) Clique em **Gerar** para gerar uma nova chave. A nova chave substituirá a chave marcada e, em seguida, clique em **OK** para continuar.



Generating a new key will overwrite the existing key. Do you want to continue?



Etapa 10. (Opcional) Clique em **Editar** para editar uma chave atual.

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb

Generate Edit... Delete Details

Etapa 11. (Opcional) Escolha um tipo de chave na lista suspensa Tipo de chave.

Key Type: 

Public Key: 

Comment:

Observação: neste exemplo, RSA é escolhido.

Etapa 12. (Opcional) Insira a nova chave pública no campo *Public Key*.

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type: RSA

Public Key:

```

--- BEGIN SSH2 PUBLIC KEY ---
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAQDAQDAb0QFu8yktUlebpLhpETIs79pWy+k0F8g4x
ovw+0T55Bq2pys5O7FwoxKTLIXFVW5CFdRw26QS2w0oLnH0TecsC13qzhFuOEVBPhKC
akyEuy6x8fFsKwdLIld8iUVIbyXk4psIDQD2u0U7AHVRH4ITcXpinexS0MQ==
--- END SSH2 PUBLIC KEY ---

```

Private Key: Encrypted


Plaintext

Apply Close Display Sensitive Data as Plaintext

Etapa 13. (Opcional) Insira a nova chave privada no campo *Private Key*.

Nota: Você pode editar a chave privada e clicar em Criptografada para ver a chave privada atual como um texto criptografado ou Texto sem formatação para ver a chave privada atual em texto sem formatação.

Etapa 14. (Opcional) Clique em **Exibir Dados Confidenciais como Texto sem Formatação** para mostrar os dados criptografados da página em formato de texto sem formatação e clique em **OK** para continuar.

 Sensitive data for the current page will be displayed as plaintext. Your HTTP web session is insecure. Do you want to continue?

Don't show me this again

OK Cancel

Etapa 15. Clique em **Aplicar** para salvar suas alterações e clique em **Fechar**.

Etapa 16. (Opcional) Clique em **Excluir** para excluir a chave marcada.

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb

Generate Edit... Delete Details

Etapa 17. (Opcional) Depois que aparecer uma mensagem de confirmação, como mostrado abaixo, clique em **OK** para excluir a chave.



The selected user defined key will be deleted and replaced by an auto generated key. Do you want to continue?

OK

Cancel

Etapa 18. (Opcional) Clique em **Detalhes** para ver os detalhes da chave marcada.

SSH User Key Details

SSH Server Key Type: RSA

Public Key: --- BEGIN SSH2 PUBLIC KEY ---
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAQgQDAb0QFu6yktUlebpLhpETIs79pV
Rovv+0T55Bq2pys5O7FwoxKTLIXFVW5CFdRw26QS2w0oLnH0TecsCI3qzH
7LYhakyEuy6x6fFsKwdLlId8iUVlbyXk4psIDQD2u0U7AHVRH4ITcXpinexS0M
--- END SSH2 PUBLIC KEY ---

Private Key (Encrypted): --- BEGIN SSH2 ENCRYPTED PRIVATE KEY ---
Comment: RSA Private Key
UM5POag2XRmC4XxM1VhmxNkAdj+ml75ZsprMYh/PkuAVm40EHk41YQDg
+zh87iJBUpwHPId1ivhgjBJuF9sFtKTIU3DKUg1IOrKcM90JapMOyDpD7M+4
gBd08SbtMQWZdFy7hj6rSTCO0YPKpVhkylBwye44QdjCaCGojE/FIKuMHBz
dkVPHkwi2ExfbENqD60yc7pFex+oaah/ugmYgjBmOnNbrViXCrHiUSAKUWz
RUDaVM7V2u67+yw+/yNJ+XvRYkhsQZRON8cOi4ilHV1MImJoRGrdiuR/CjE
X3zOhmB8o6iyCa32MPlhy08yfPN4YgrHh0cpxeWcY1ZRIG0vZ4lxUJ423xYL
rdclnoll4EWSk+sj1vzrGidXHCRzQkkMqLp+E5zl9npJc0t6+64tKqAD3CVaHk
VwR5JXrle2vHdik2af2AO3JZsobtTO0dMSA5zPdN4CCERPLAEaACTCQOkE
MqHATSyFcG+h0X2MitxV5XsWUaJe/dH/BNeljYrzKRF6y9V37PFBizSLAtE2
62u0QPBRglLu6lL4j4jCtN54PauVkr48mw3JgsWszKXgHmSx/ok7Tu4gPcn-
UI37c0vNZwDadMZ/1ZKLEkBOJtJIJevDsWslvclKZAvoSmLu2B20hUM2uor1
5GngylqcT5vYLMGpDL2k2PzUgFuLvbAOFzIri1c1czqyjy+JCbP/cl7TAOeGA7
LtCY8DrAo8y5O15CcgUIZJddWLRqunDGpygscAaor050vG3/5A1C8YRMh2F
86OuHWS+0HHqnJnmgrOICj/O/DISeRnHkr8juT1sBuwpFDd+wT0L/KzRN1L
4OwOYCjkdgm7GgOI2eOnY9YvyD/RyjcMm11JFA1RwPCSQWhyPrZgcCQS
0FLgLKZNZ1XNJkdqDBmb6CfyvXeGP76EH+EQ==
--- END SSH2 PRIVATE KEY ---

Back Display Sensitive Data as Plaintext

Etapa 19. (Opcional) Clique no botão **Save** na parte superior da página para salvar as alterações no arquivo de configuração de inicialização.

Port Gigabit PoE Stackable Managed Switch

Save

cisco Language: E

SSH User Authentication

✓ Success. To permanently save the configuration, go to the [File Operations](#) page or c

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

✱ Username: (0/70 characters used)

✱ Password: Encrypted
 Plaintext (Default Password)

SSH User Key Table

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb

Agora você deve ter definido as configurações de autenticação de usuário do cliente no switch gerenciado.

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.