

Autenticação de usuário do Client Secure Shell (SSH) para os switches SG350XG e SG550XG

Objetivo

O Secure Shell (SSH) é um protocolo que fornece uma conexão remota segura a um dispositivo específico. Os switches gerenciados 350XG e 550XG Series permitem autenticar e gerenciar usuários para se conectarem ao dispositivo via SSH. A autenticação ocorre por meio de uma chave pública, de modo que o usuário pode usar essa chave para estabelecer uma conexão SSH com um dispositivo específico. As conexões SSH são úteis para solucionar problemas de uma rede remotamente, caso o administrador da rede não esteja no site da rede.

Este artigo explica como configurar a autenticação de usuário cliente nos switches gerenciados SG350XG e SG550XG Series.

Dispositivos aplicáveis

- SG350XG
- SG550XG

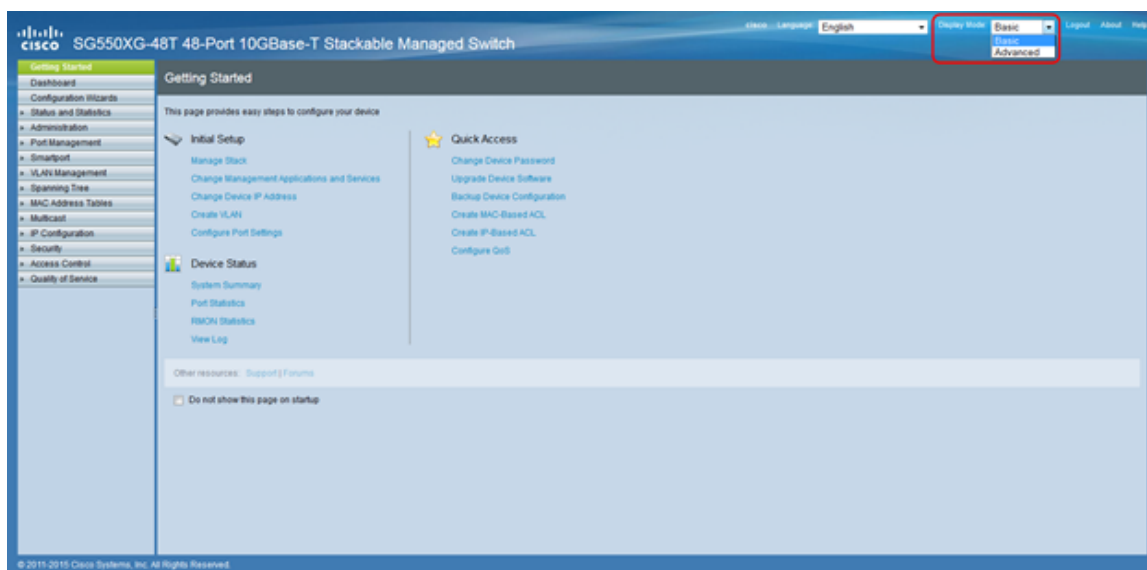
Versão de software

- v2.0.0.73

Configurar SSH Cliente Autenticação

Configuração global

Note: As capturas de tela a seguir são do monitor avançado. Para alterá-lo, clique na lista suspensa *Modo de exibição* localizada na parte superior direita do ecrã



Etapa 1. Faça login no utilitário de configuração da Web e escolha **Security > SSH Client >**

SSH User Authentication. A página *Autenticação de usuário SSH* é aberta:

| <input type="checkbox"/> | Key Type | Key Source | Fingerprint |
|--------------------------|----------|----------------|---|
| <input type="checkbox"/> | RSA | Auto Generated | 6f:bf:d8:12:60:74:ea:4c:68:a1:76:91:e5:8f:a4:d1 |
| <input type="checkbox"/> | DSA | Auto Generated | 24:31:b0:3c:5c:94:74:35:ba:d1:ce:c6:f7:16:84:48 |

Etapa 2. No *Método de autenticação de usuário SSH*, clique no botão de opção do método de autenticação global desejado.

As opções disponíveis são as seguintes:

- Por senha - Esta opção permite configurar uma senha para autenticação do usuário. Digite uma senha ou mantenha o padrão, "anonymous".
- Por chave pública RSA - Essa opção permite que você use uma chave pública RSA para autenticação de usuário. RSA é usado para criptografia e assinatura. Se isso estiver selecionado, crie uma chave pública e privada RSA no bloco de tabela de chave de usuário SSH.
- Por chave pública DSA - Esta opção permite que você use uma chave pública DSA para autenticação do usuário. O DSA é usado somente para assinatura. Se isso estiver selecionado, crie uma chave pública/privada DSA no bloco Tabela de chaves de usuário SSH.

Etapa 3. Localize a área *Credenciais*. No campo *Nome de usuário*, digite o nome de usuário.

SSH User Authentication

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: anonymous)

Etapa 4. Se **By Password (Por senha)** tiver sido selecionado na [Etapa 2](#), clique no botão de opção do método de senha desejado no campo *Password (Senha)*. A senha padrão é "anonymous".

SSH User Authentication

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: anonymous)

As opções disponíveis são descritas da seguinte maneira:

- Encriptado - Introduza uma senha encriptada.
- Texto sem formatação - Insira uma senha como texto simples.

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

SSH User Authentication

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: anonymous)

Etapa 6. (Opcional) Para restaurar o nome de usuário e a senha padrão, clique em **Restaurar credenciais padrão**. A senha padrão é "anonymous".

SSH User Authentication

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: anonymous)

Apply Cancel **Restore Default Credentials** Display Sensitive Data as Plaintext

Passo 7. (Opcional) Para exibir os dados confidenciais como texto não criptografado ou como texto criptografado, clique em **Exibir dados confidenciais como texto não criptografado/criptografado**.

SSH User Authentication

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: anonymous)

Apply Cancel Restore Default Credentials **Display Sensitive Data as Plaintext**

Note: O nome do botão mudará dependendo da configuração atual. O botão sempre alterna a exibição dos dados.

Tabela de chave de usuário SSH

Esta seção explica como gerenciar a tabela de usuários SSH.

Etapa 1. Navegue até a *Tabela de chaves de usuário SSH*. Na lista exibida, marque as caixas de seleção à esquerda da chave que deseja gerenciar .

| SSH User Key Table | | | |
|-------------------------------------|----------|--------------|---|
| <input type="checkbox"/> | Key Type | Key Source | Fingerprint |
| <input checked="" type="checkbox"/> | RSA | User Defined | 8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a |
| <input type="checkbox"/> | DSA | User Defined | 6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c |

Generate Edit... Delete Details

Etapa 2. (Opcional) Clique em **Gerar** para gerar uma nova chave. A nova chave substitui a chave selecionada. Uma janela de confirmação aparecerá. Clique em OK para continuar.

| SSH User Key Table | | | |
|-------------------------------------|----------|--------------|---|
| <input type="checkbox"/> | Key Type | Key Source | Fingerprint |
| <input checked="" type="checkbox"/> | RSA | User Defined | 8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a |
| <input type="checkbox"/> | DSA | User Defined | 6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c |

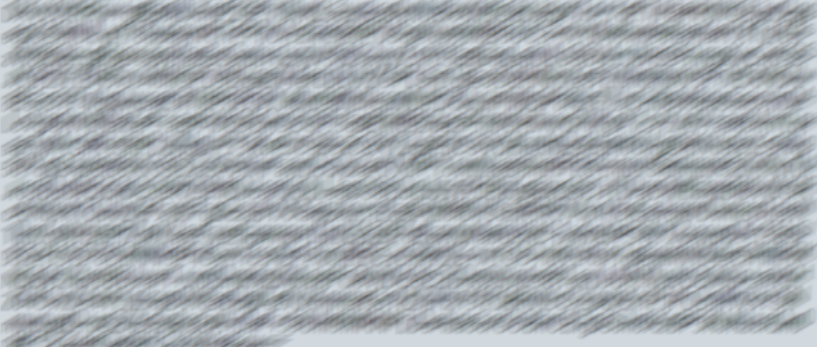
Etapa 3. (Opcional) Clique em **Excluir** para excluir a chave selecionada. Uma janela de confirmação aparecerá. Clique em OK para continuar.

| SSH User Key Table | | | |
|-------------------------------------|----------|--------------|---|
| <input type="checkbox"/> | Key Type | Key Source | Fingerprint |
| <input checked="" type="checkbox"/> | RSA | User Defined | 8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a |
| <input type="checkbox"/> | DSA | User Defined | 6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c |

Etapa 4. (Opcional) Clique em **Detalhes** para exibir os detalhes da chave selecionada.

| SSH User Key Table | | | |
|-------------------------------------|----------|--------------|---|
| <input type="checkbox"/> | Key Type | Key Source | Fingerprint |
| <input checked="" type="checkbox"/> | RSA | User Defined | 8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a |
| <input type="checkbox"/> | DSA | User Defined | 6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c |

A página Detalhes da chave de usuário SSH é exibida. Clique em **Back** para retornar à Tabela de chaves de usuário SSH.

| SSH User Key Details | |
|--------------------------|---|
| SSH Server Key Type: | RSA |
| Public Key: | <pre> ---- BEGIN SSH2 PUBLIC KEY ---- Comment: RSA Public Key AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxb XRqFXeMQ2LNyUTCK8hcu0zV5SipsQ8AFRZmpnaVkEgSunFK5YYJ2AckP9NyMikihWfRWm UXT6SBOK/BJk7GPXhcs0JE6lI3uPCyiC50vzGRBGhWSH/oGBxMqkavDGpcToaDyKQ== ---- END SSH2 PUBLIC KEY ---- </pre> |
| Private Key (Encrypted): | <pre> ---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ---- Comment: RSA Private Key </pre>  <pre> ---- END SSH2 PRIVATE KEY ---- </pre> |

Etapa 5. Clique em **Editar** para editar a chave escolhida.

| SSH User Key Table | | | |
|-------------------------------------|----------|--------------|---|
| <input type="checkbox"/> | Key Type | Key Source | Fingerprint |
| <input checked="" type="checkbox"/> | RSA | User Defined | 8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a |
| <input type="checkbox"/> | DSA | User Defined | 6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c |

A janela *Editar configurações de autenticação do cliente SSH* é aberta:

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

Key Type:

Public Key:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;
---- END SSH2 PUBLIC KEY ----
```

Private Key: Encrypted

Plaintext

Etapa 6. Selecione o tipo de chave desejado na lista suspensa *Tipo de chave*.

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

Key Type:

Public Key:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;
---- END SSH2 PUBLIC KEY ----
```

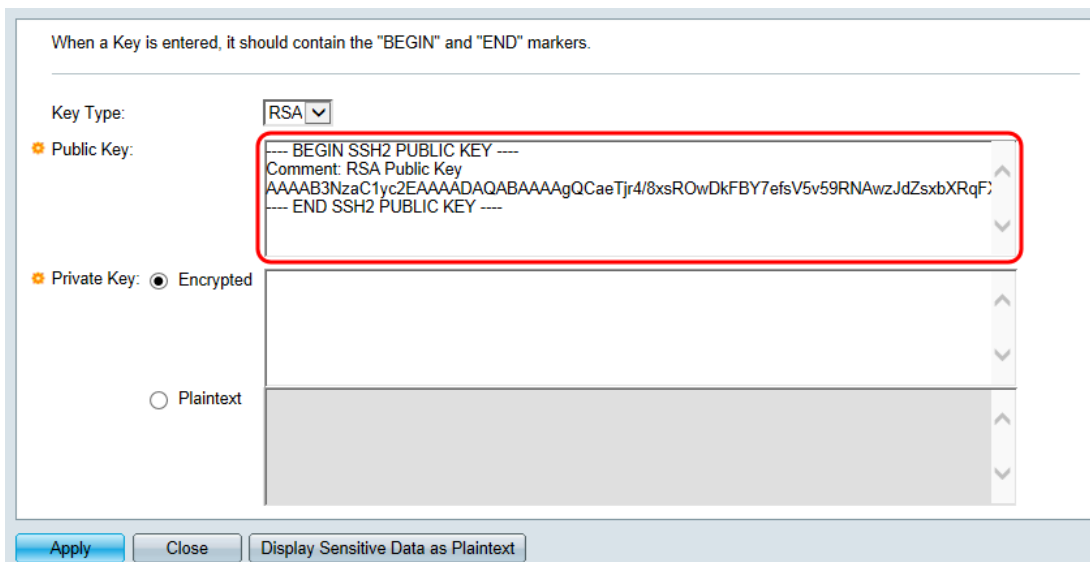
Private Key: Encrypted

Plaintext

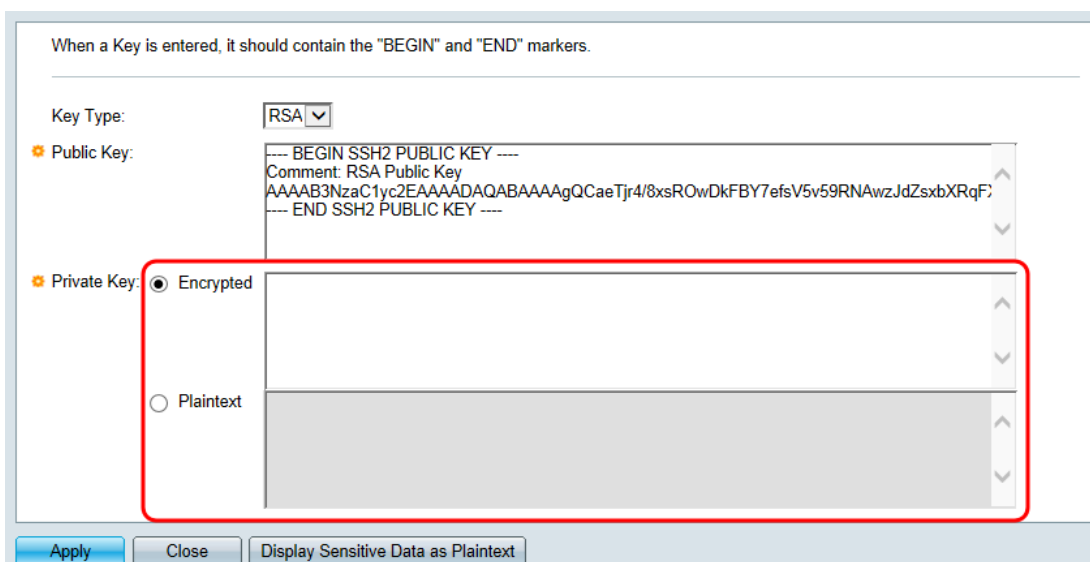
As opções disponíveis são as seguintes:

- RSA - RSA é usado para criptografia e assinatura.
- DSA - O DSA é usado somente para assinatura.

Passo 7. No campo *Chave pública*, você pode editar a chave pública atual.



Etapa 8. No campo *Chave privada*, você pode editar a chave privada atual. Clique no botão Botão de opção **criptografado** para ver a chave privada atual como criptografada. Caso contrário, clique no botão de opção **Texto sem formatação** para ver a chave privada atual como texto sem formatação.



Etapa 9. Clique em **Aplicar** para salvar suas alterações.

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF'  
-----END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

Apply

Close

Display Sensitive Data as Plaintext