

# Acessar uma CLI do switch SMB usando o SSH ou o Telnet

## Objetivo

Os Switches Gerenciados Cisco Small Business podem ser acessados e configurados remotamente através da Interface de Linha de Comando (CLI). O acesso à CLI permite que os comandos sejam inseridos em uma janela baseada em terminal. Se você preferir configurar usando comandos de terminal em seu switch através da CLI em vez do utilitário baseado na Web, essa seria uma alternativa mais fácil. Determinadas tarefas, como a ativação do modo de Camada 3, só podem ser executadas através da CLI.

Para acessar remotamente a CLI do seu switch, você deve usar um cliente SSH ou Telnet. Você também deve habilitar o serviço Telnet e SSH em seu switch antes de poder acessá-lo remotamente.

**Note:** Para obter instruções sobre como configurar as configurações do Transmission Control Protocol (TCP) e User Datagram Protocol (UDP) em seu switch, clique [aqui](#).

Este artigo fornece instruções sobre como acessar a CLI do seu switch por meio de SSH ou Telnet usando os seguintes clientes:

- PuTTY — Um cliente padrão Telnet e SSH. Você pode baixar um instalador [aqui](#) e instalar em seu computador Windows.
- Terminal — Um aplicativo pré-instalado em cada computador Mac OS X. Também é conhecido como shell ou console.

**Importante:** Antes de fazer uma conexão SSH ou Telnet com o switch, você deve definir o endereço IP do switch. Para obter instruções, clique [aqui](#).

## Dispositivos aplicáveis

- Sx300 Series
- Sx350 Series
- SG350X Series
- Sx500 Series
- Sx550X Series

## Versão de software

- 1.4.7.06 — Sx300, Sx500
- 2.2.8.04 — Sx350, SG350X, Sx550X

## Acesse a CLI do Switch através do SSH

As sessões SSH se desconectam automaticamente após o tempo ocioso configurado no switch ter passado. O tempo limite de sessão ociosa padrão para SSH é de 10 minutos.

Para fazer uma conexão SSH com o switch, escolha sua plataforma:

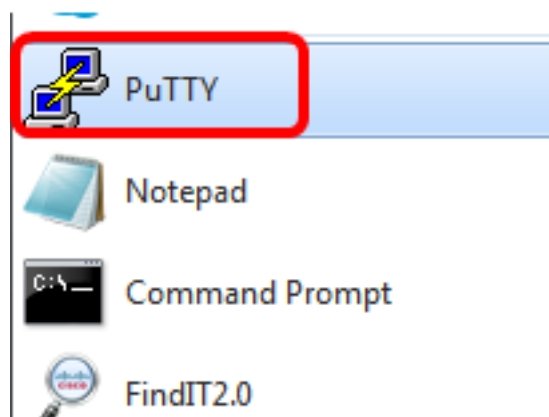
[Computador Windows com PuTTY](#)

[Computador Mac usando terminal](#)

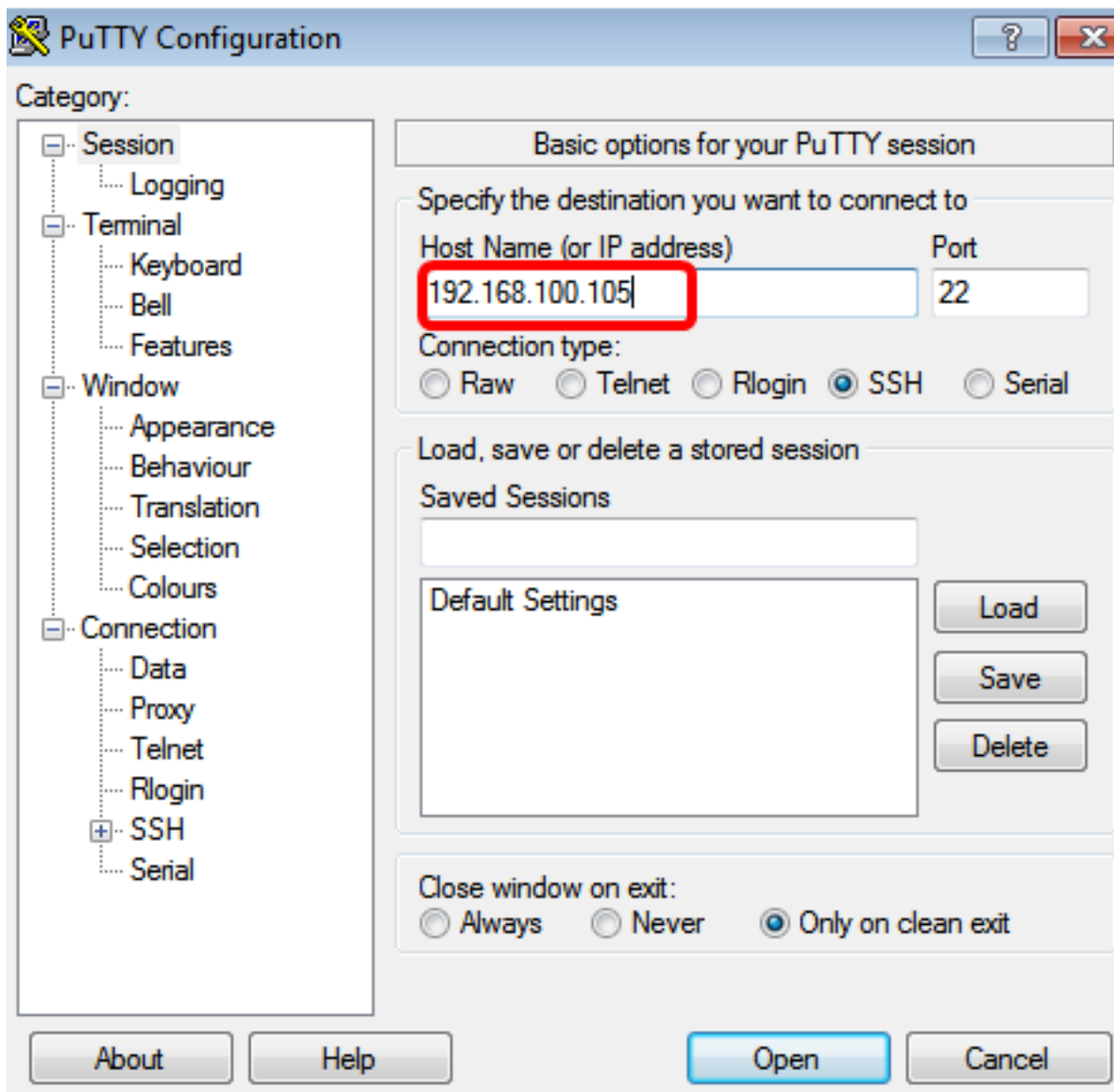
## [Acesse a CLI por meio do SSH usando PuTTY](#)

**Note:** As imagens podem variar de acordo com a versão do sistema operacional Windows que você está usando. Neste exemplo, o Windows 7 Ultimate é usado e a versão PuTTY é 0,63.

Etapa 1. Inicie o cliente PuTTY em seu computador.

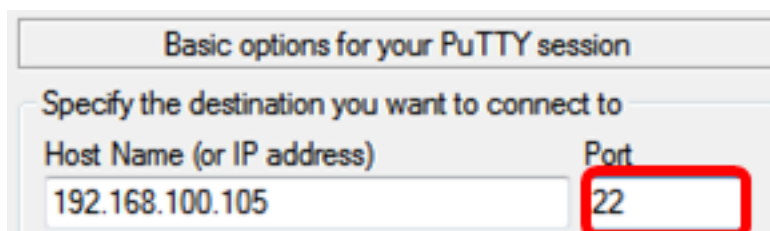


Etapa 2. Insira o nome do host ou o endereço IP do switch que deseja acessar remotamente no campo *Host Name (ou IP address)*.

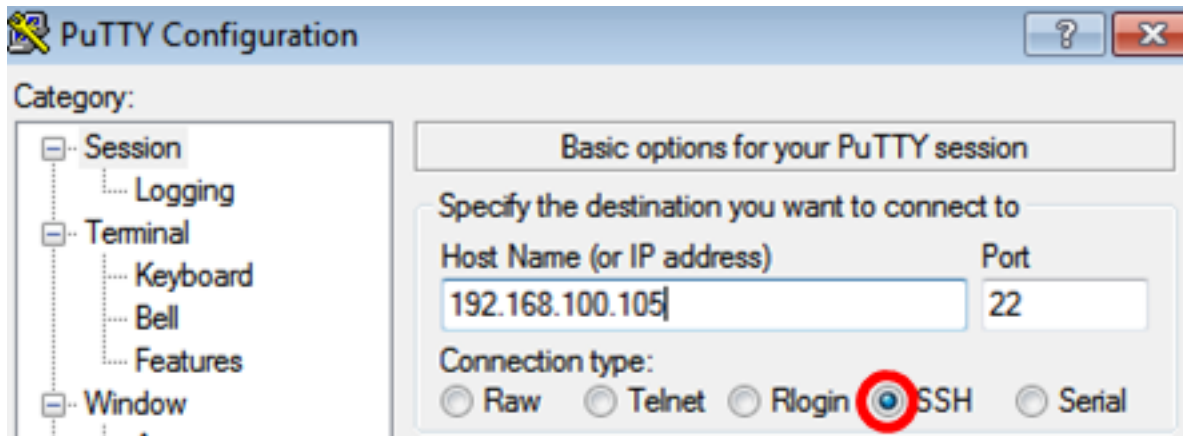


**Note:** Neste exemplo, o endereço IP 192.168.100.105 é usado.

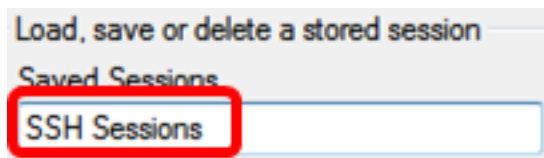
Etapa 3. Digite **22** como o número da porta a ser usada para a sessão SSH no campo *Porta*.



Etapa 4. Na área Tipo de conexão, clique no botão de opção **SSH** para escolher SSH como seu método de conexão com o switch.

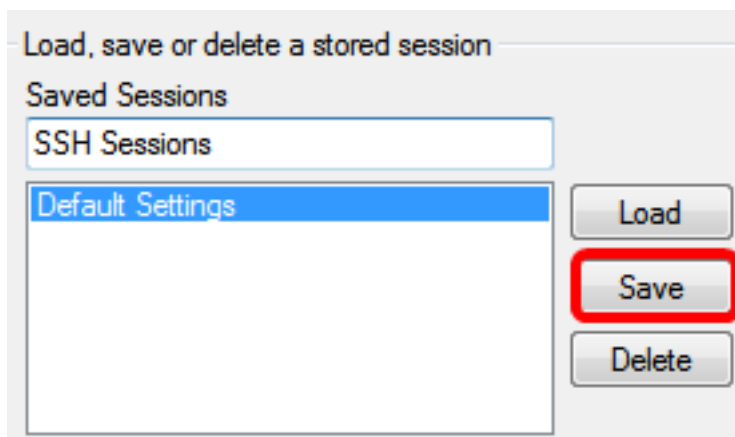


Etapa 5. (Opcional) Para salvar a sessão, insira o nome da sessão no campo *Sessões salvas*.

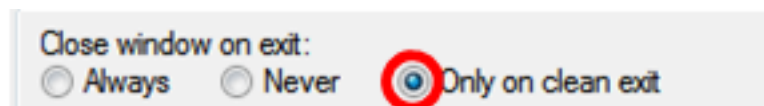


**Note:** Neste exemplo, são usadas sessões SSH.

Etapa 6. (Opcional) Clique em **Salvar** para salvar a sessão.

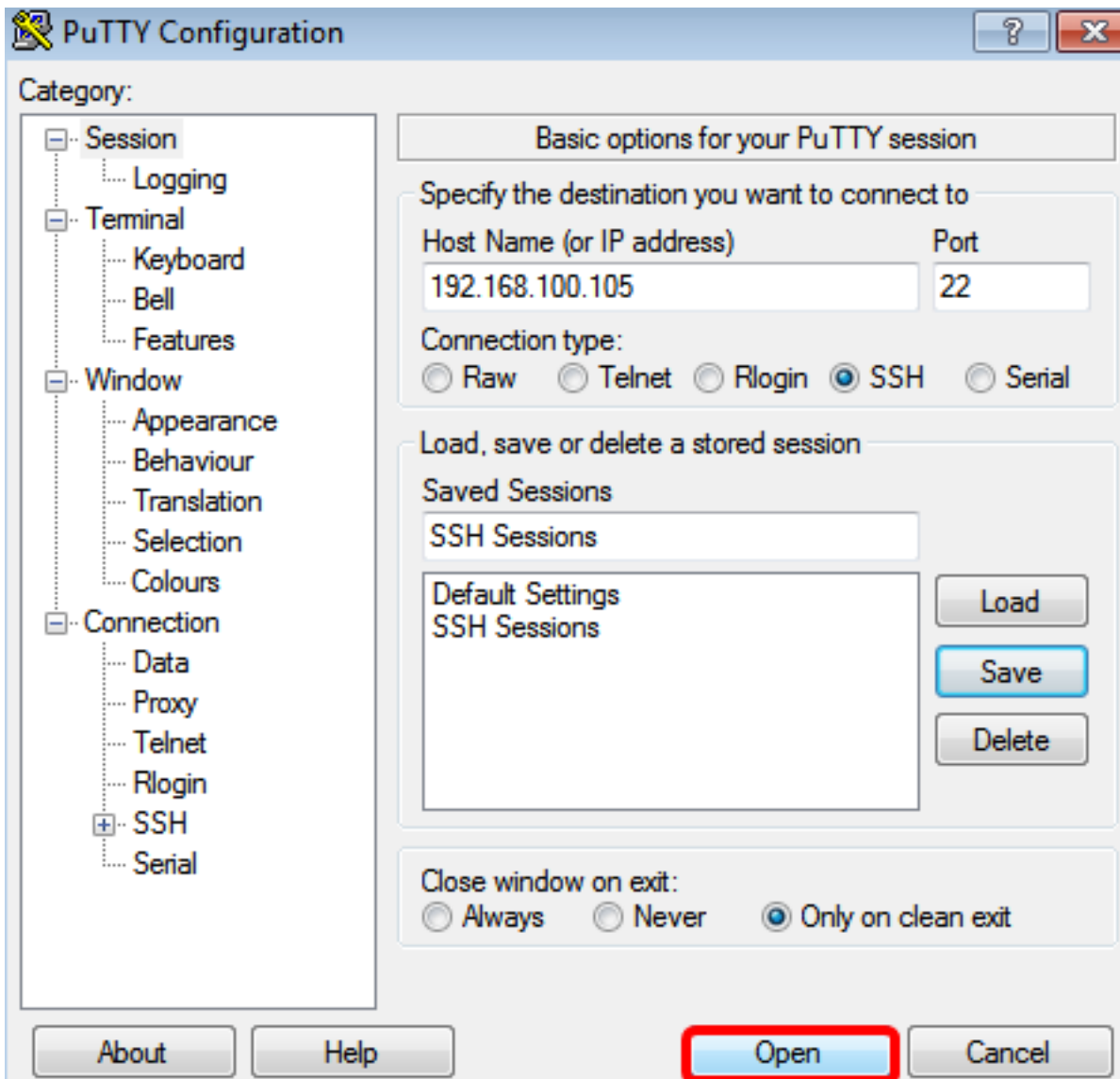


Passo 7. (Opcional) Na janela Fechar na área de saída, clique no botão de opção para escolher o comportamento da janela SSH ao sair.



**Note:** Neste exemplo, somente em saída limpa é escolhida.

Etapa 8. Clique em **Abrir** para iniciar a sessão.



Etapa 9. Se esta for sua primeira vez usando SSH para se conectar ao switch, você poderá receber um aviso de violação de segurança. Este aviso informa que é possível que você esteja se conectando a outro computador fingindo ser o switch. Depois de garantir que você inseriu o endereço IP correto no campo Host Name na Etapa 4, clique em **Yes** para atualizar a chave Rivest Shamir Adleman 2 (RSA2) para incluir o novo switch.

## PuTTY Security Alert



The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.

The server's rsa2 key fingerprint is:

ssh-rsa 1024 6f:7d:af:33:11:8c:b1:8b:15:3f:b1:ed:45:b9:46:63

If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.

If you want to carry on connecting just once, without adding the key to the cache, hit No.

If you do not trust this host, hit Cancel to abandon the connection.

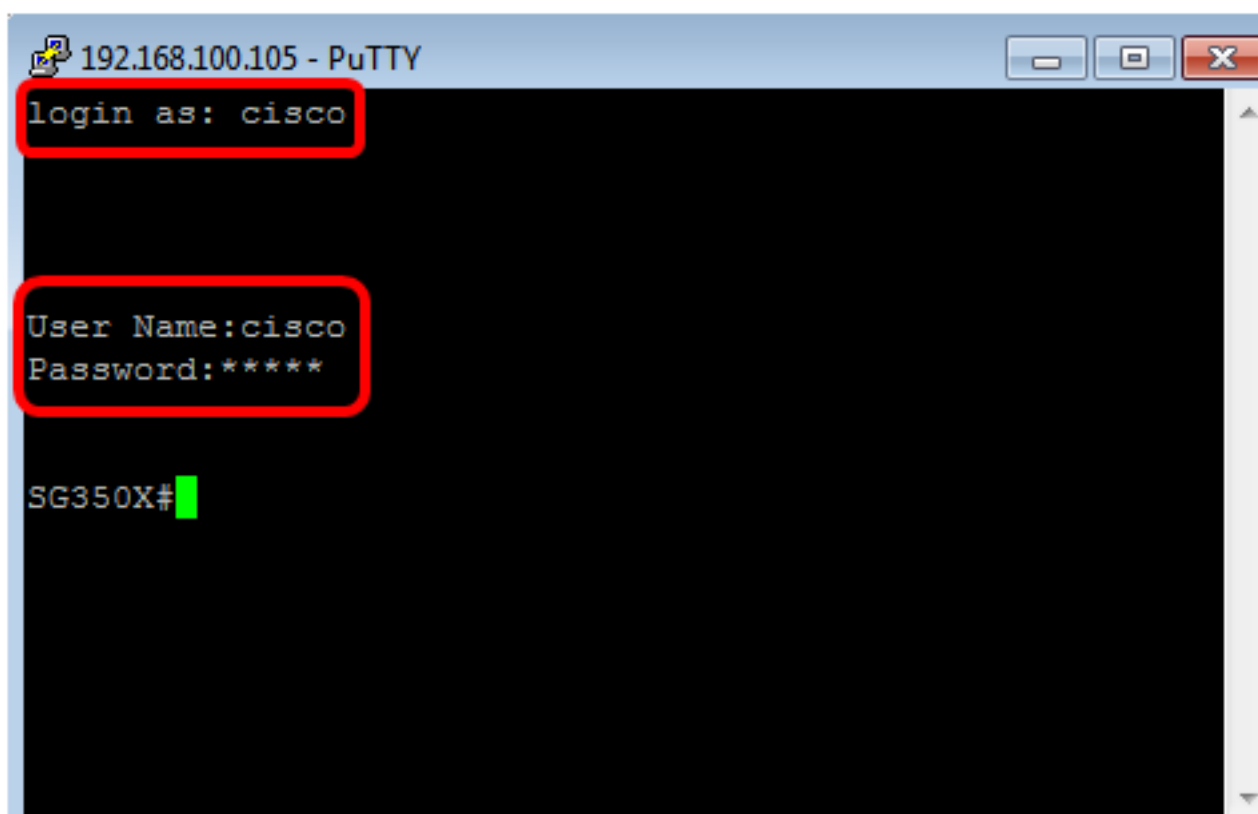
Yes

No

Cancel

Help

Etapa 10. Insira o nome de usuário e a senha do switch nos campos *login como*, *Nome de usuário* e *Senha*.



Agora você deve ter acessado remotamente com êxito a CLI do seu switch por meio do SSH usando PuTTY.

### [Acesse a CLI por meio do SSH usando o Terminal](#)

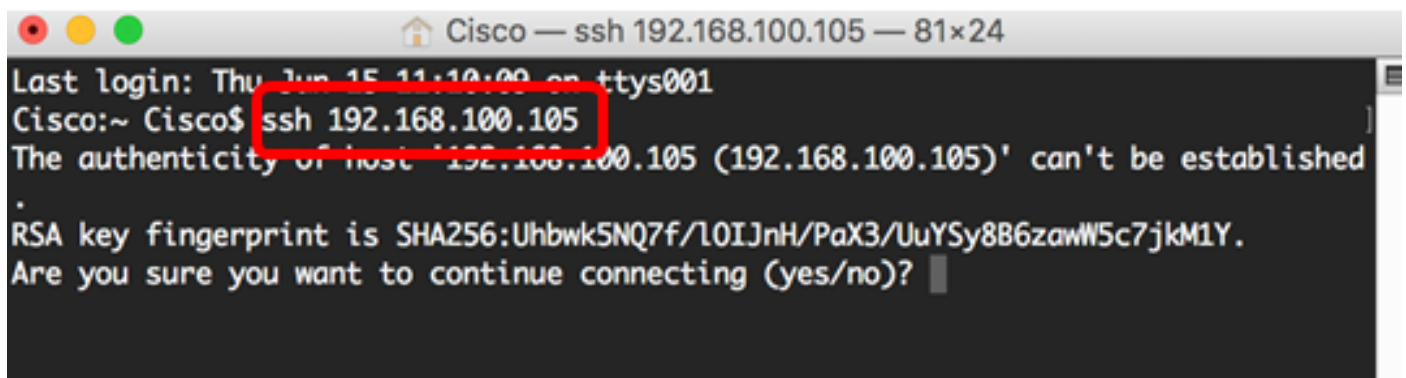
**Note:** As imagens podem variar de acordo com a versão do sistema operacional do computador Mac que você está usando. Neste exemplo, o macOS Sierra é usado e a versão do Terminal é 2.7.1.

Etapa 1. Vá para **Applications > Utilities** e inicie o aplicativo **Terminal.app**.



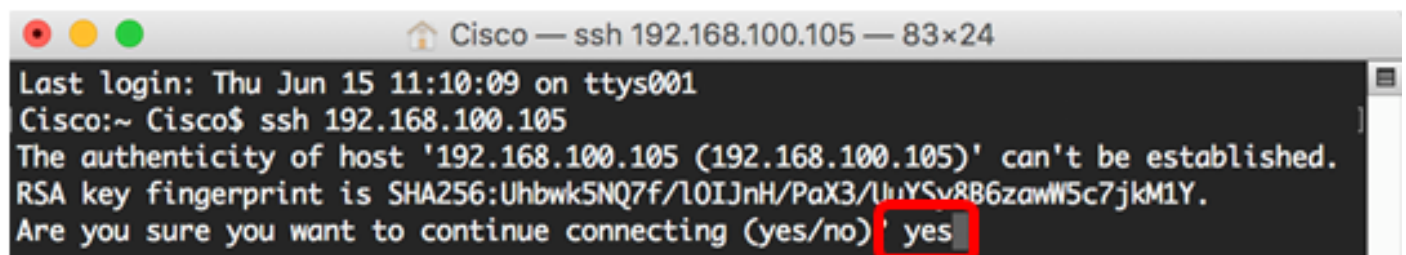
Etapa 2. Insira o comando **ssh** e, em seguida, o endereço IP para acessar a CLI do switch.

```
Cisco: ~Cisco$ ssh [ip-address]
```



**Note:** Neste exemplo, 192.168.100.105.

Etapa 3. Depois de aparecer a mensagem perguntando se você deseja continuar a conexão, digite **Yes**.



Etapa 4. Insira o nome de usuário e a senha do switch nos campos *Nome de usuário* e *Senha*.



```
Cisco — ssh 192.168.100.105 — 83x24
Last login: Thu Jun 15 11:10:09 on ttys001
Cisco:~ Cisco$ ssh 192.168.100.105
The authenticity of host '192.168.100.105 (192.168.100.105)' can't be established.
RSA key fingerprint is SHA256:Uhbwk5NQ7f/10IJnH/PaX3/UuYSy8B6zawW5c7jkM1Y.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.100.105' (RSA) to the list of known hosts.

User Name:cisco
Password:*****

SG350X#
```

Agora você deve ter acessado remotamente com êxito a CLI do seu switch por meio do SSH usando o Terminal.

## Acesse a CLI do Switch por meio do Telnet

As sessões Telnet se desconectam automaticamente após o tempo ocioso configurado no switch ter passado. O tempo limite de sessão ociosa padrão para Telnet é de 10 minutos.

Para fazer uma conexão Telnet com o switch, escolha sua plataforma:

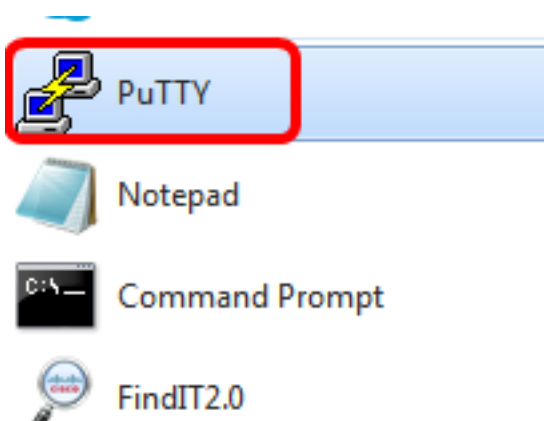
[Computador Windows com PuTTY](#)

[Computador Mac usando terminal](#)

### [Acesse o CLI por Telnet usando PuTTY](#)

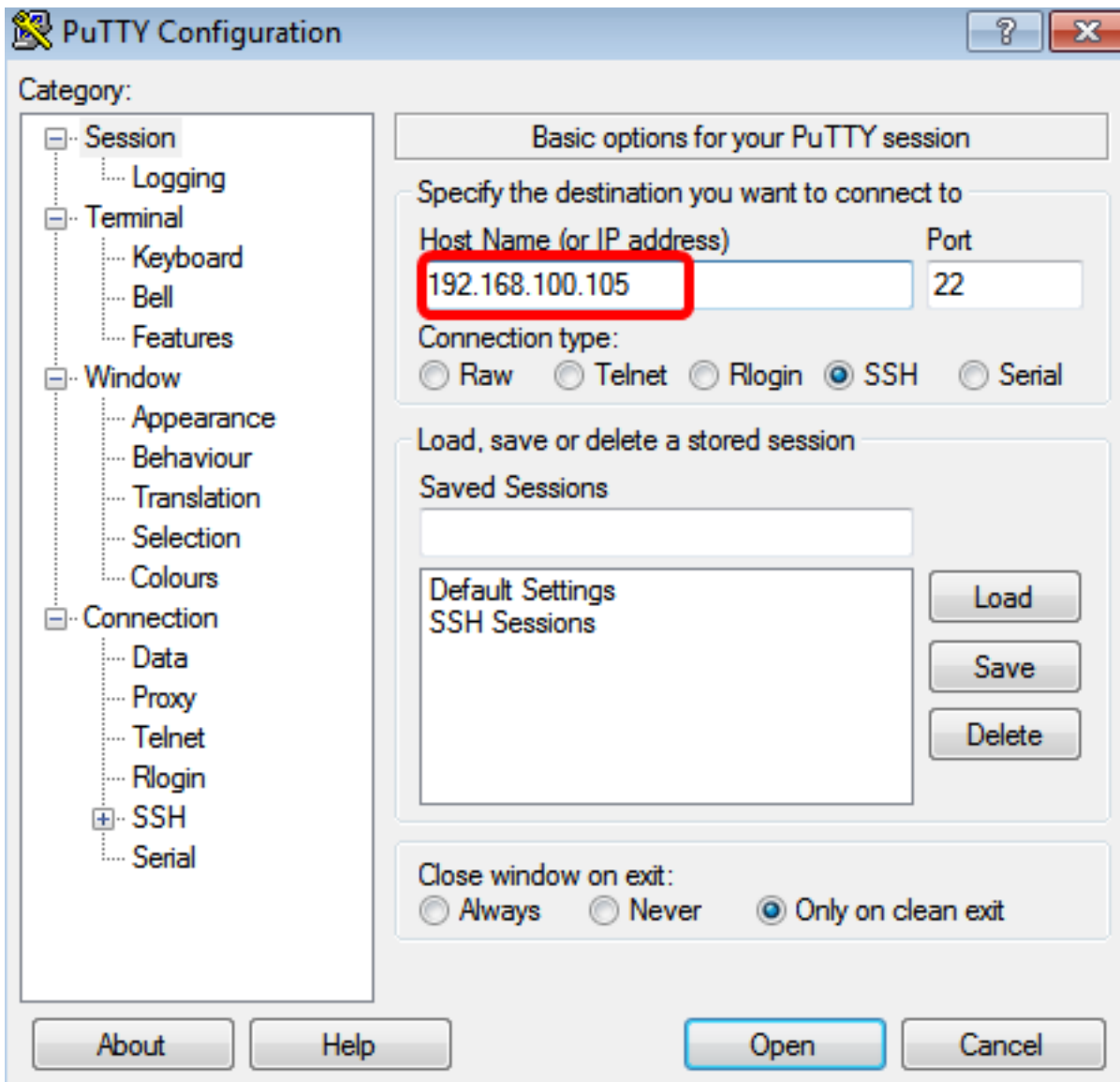
**Note:** As imagens podem variar de acordo com a versão do sistema operacional Windows que você está usando. Neste exemplo, o Windows 7 Ultimate é usado e a versão PuTTY é 0,63.

Etapa 1. Inicie o cliente PuTTY em seu computador.



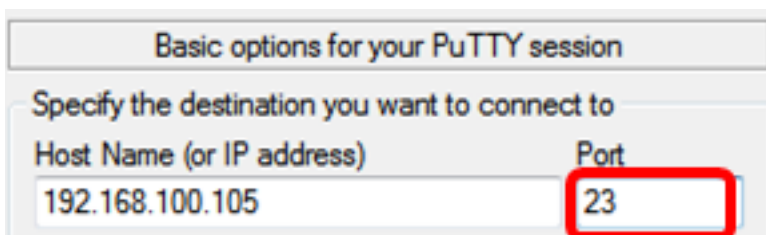
Etapa 2. Insira o nome do host ou o endereço IP do switch que deseja acessar remotamente no campo *Host Name (ou IP address)*.





**Note:** Neste exemplo, 192.168.100.105 é usado.

Etapa 3. Digite **23** como o número da porta a ser usada para a sessão Telnet no campo Porta.



Etapa 4. Na área Tipo de conexão, clique no botão de opção **Telnet** para escolher Telnet como seu método de conexão com o switch.

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address)	Port
192.168.100.105	23

Connection type:

Raw  Telnet  Rlogin  SSH  Serial

Etapa 5. (Opcional) Para salvar a sessão, insira o nome da sessão no campo *Sessões salvas*.

Load, save or delete a stored session

Saved Sessions

Telnet Sessions

Default Settings

SSH Sessions

**Note:** Neste exemplo, são usadas sessões Telnet.

Etapa 6. (Opcional) Clique em **Salvar** para salvar a sessão.

Load, save or delete a stored session

Saved Sessions

Telnet Sessions

Default Settings

SSH Sessions

Load

Save

Delete

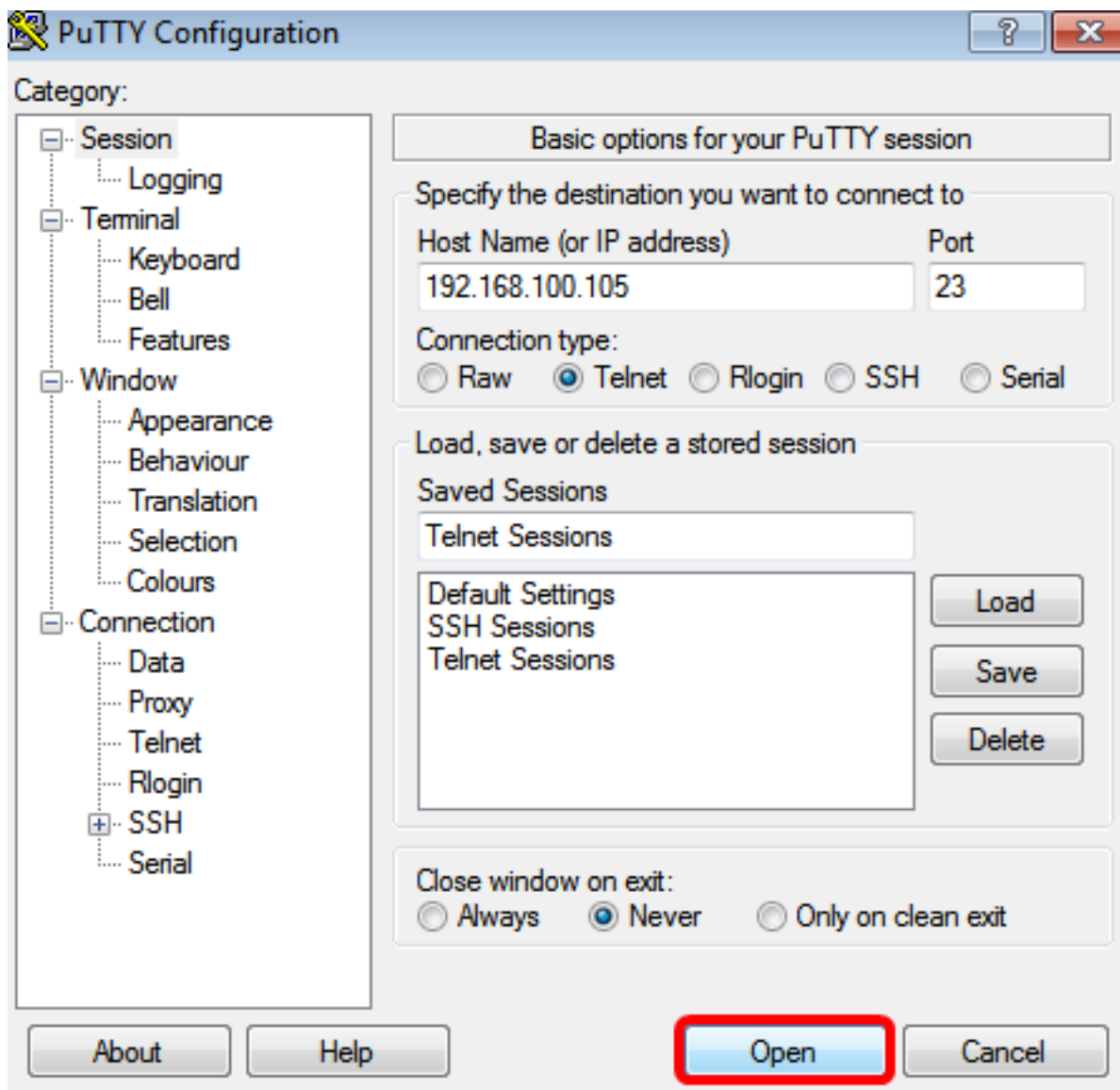
Passo 7. Opcional) Na janela Fechar na área de saída, clique no botão de opção para escolher o comportamento da janela SSH ao sair.

Close window on exit:

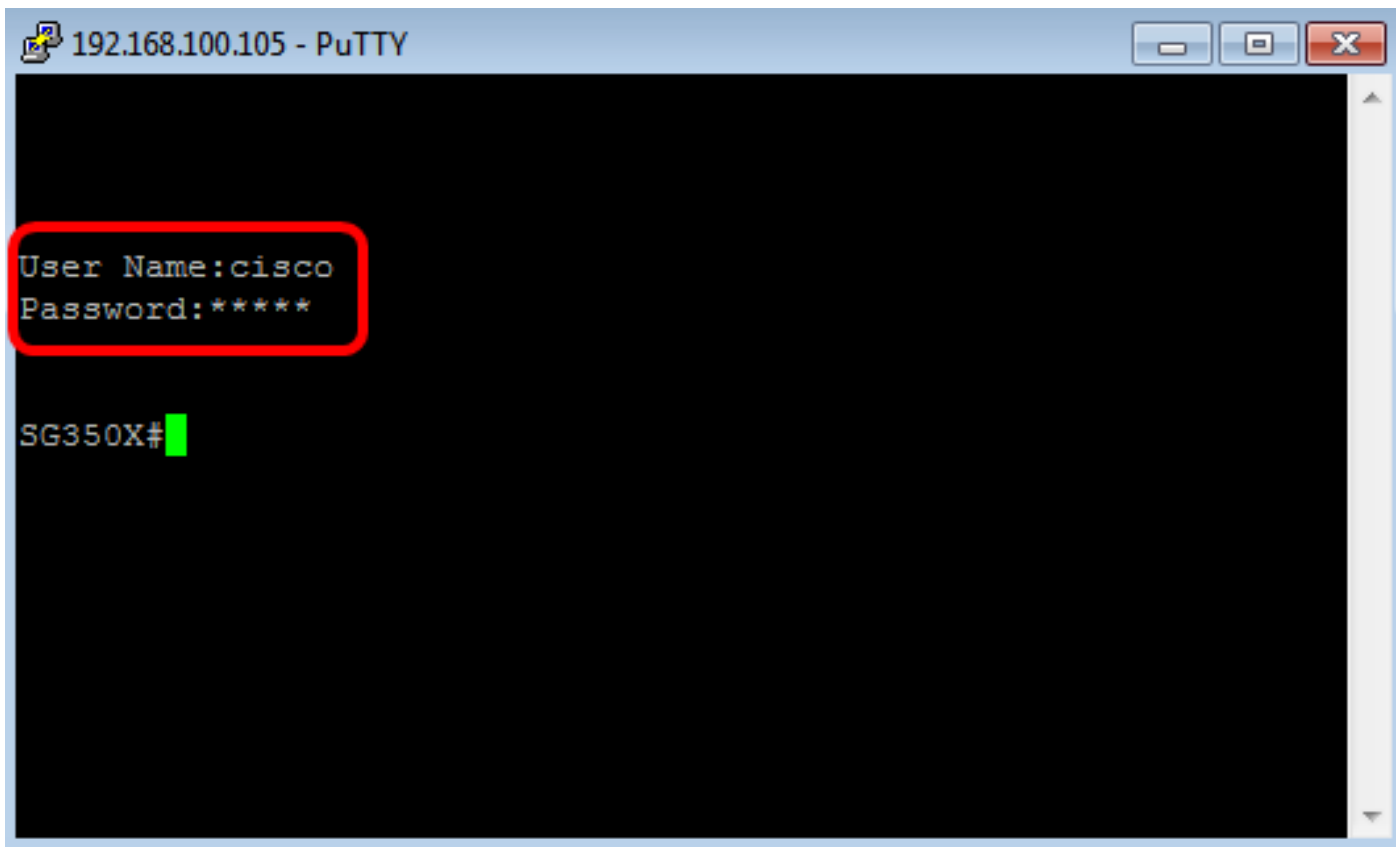
Always  Never  Only on clean exit

**Note:** Neste exemplo, Nunca é escolhido.

Etapa 8. Clique em **Abrir** para iniciar a sessão.



Etapa 9. Insira o nome de usuário e a senha do switch nos campos login como, *Nome de usuário* e *Senha*.



Agora você deve ter acessado remotamente com êxito a CLI do seu switch por meio do Telnet usando PuTTY.

### [Acesse a CLI por meio do Telnet usando o Terminal](#)

**Note:** As imagens podem variar de acordo com a versão do sistema operacional do computador Mac que você está usando. Neste exemplo, o macOS Sierra é usado e a versão do Terminal é 2.7.1.

Etapa 1. Vá para **Applications > Utilities** e inicie o aplicativo **Terminal.app**.



Etapa 2. Insira o comando **telnet** e, em seguida, o endereço IP para acessar a CLI do switch.

```
Cisco: ~Cisco$ telnet [ip-address]
```

```
Cisco — telnet 192.168.100.105 — 66x21
Last login: Fri Jun 16 08:15:06 on console
Cisco:~ Cisco$ telnet 192.168.100.105
Trying 192.168.100.105...
Connected to 192.168.100.105.
Escape character is '^]'.

User Name: █
```

**Note:** Neste exemplo, 192.168.100.105.

Etapa 3. Insira o nome de usuário e a senha do switch nos campos *Nome de usuário* e *Senha*.

```
Last login: Fri Jun 16 08:15:06 on console
Cisco:~ Cisco$ telnet 192.168.100.105
Trying 192.168.100.105...
Connected to 192.168.100.105.
Escape character is '^]'.

User Name:cisco
Password:*****

SG350X# █
```

Agora você deve ter acessado remotamente com êxito a CLI do seu switch por meio do Telnet usando o Terminal.