

Acessar a CLI do switch Cisco Business usando o SSH ou o Telnet

Objetivo

Os Switches Gerenciados Empresariais da Cisco podem ser acessados e configurados remotamente através da Interface de Linha de Comando (CLI). O acesso à CLI permite que 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 por meio 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 acessá-lo remotamente.

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

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

- PuTTY - Um cliente Telnet e SSH padrão. Você pode baixar um instalador [aqui](#) e instalá-lo em seu computador com 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 | Versão de software

- CBS250 ([Folha de dados](#)) | 3.0.0
- CBS350 ([data sheet](#)) | 3.0.0
- CBS350-2X ([data sheet](#)) | 3.0.0
- CBS350-4X ([data sheet](#)) | 3.0.0

Acessar o CLI do Switch através do SSH

As sessões SSH desconectam-se 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 usando PuTTY](#)

[Computador Mac usando Terminal](#)

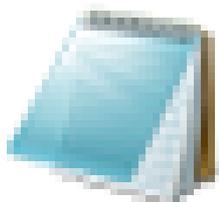
Acesse a CLI através do SSH usando PuTTY

Nota: 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.



PuTTY



Notepad

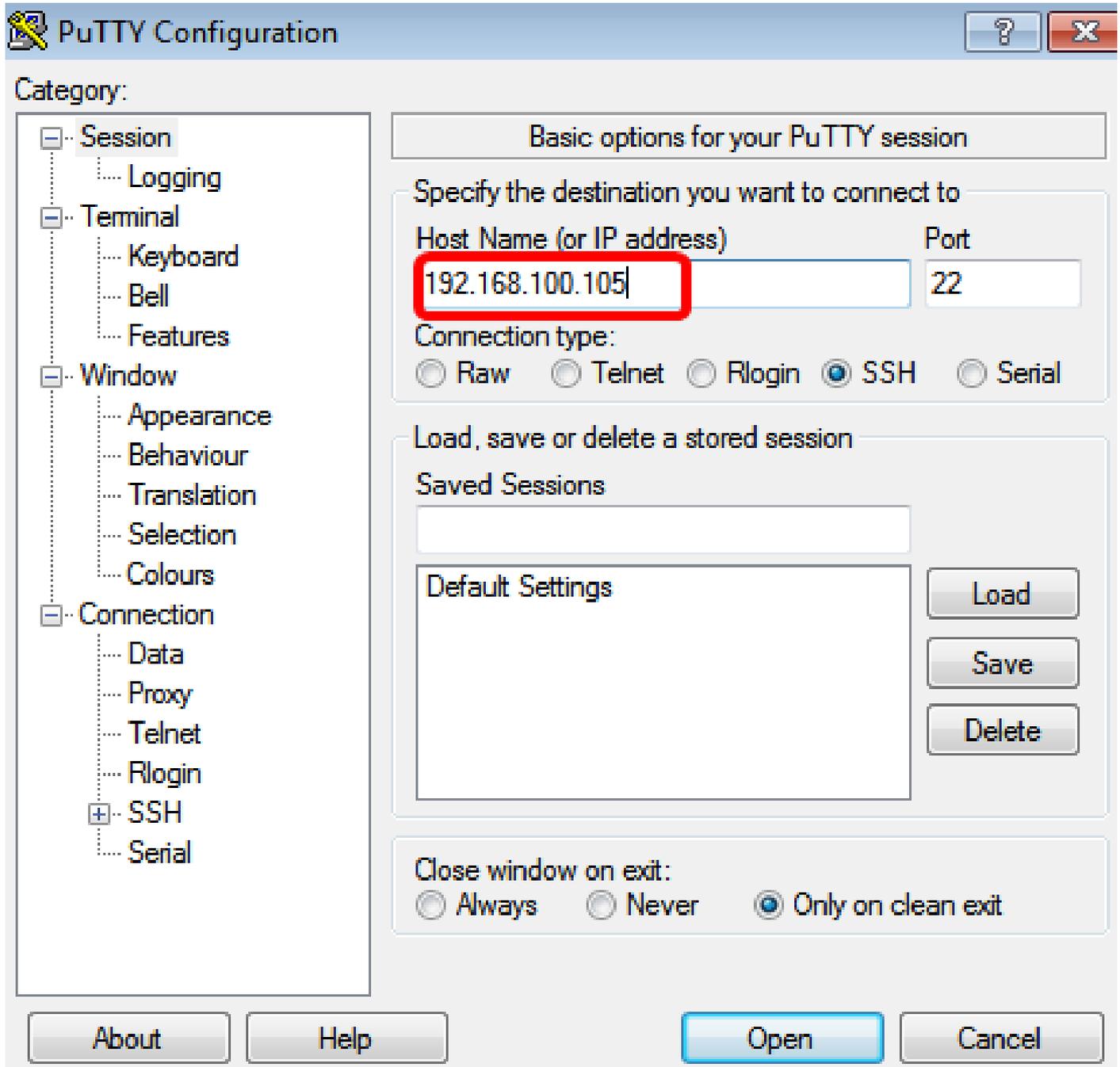


Command Prompt



FindIT2.0

Etapa 2. Insira o nome do host ou o endereço IP do switch que você deseja acessar remotamente no campo Nome do host (ou endereço IP).



Observação: neste exemplo, o endereço IP 192.168.100.105 é usado.

Etapa 3. Insira 22 como o número da porta a ser usada para a sessão SSH no campo Port.

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address)	Port
192.168.100.105	22

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

PuTTY Configuration

Category:

- Session
 - Logging
- Terminal
 - Keyboard
 - Bell
 - Features
- Window

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address)	Port
192.168.100.105	22

Connection type:

Raw Telnet Rlogin SSH Serial

Etapa 5. (Opcional) Para salvar a sessão, digite o nome da sessão no campo Sessões Salvas.

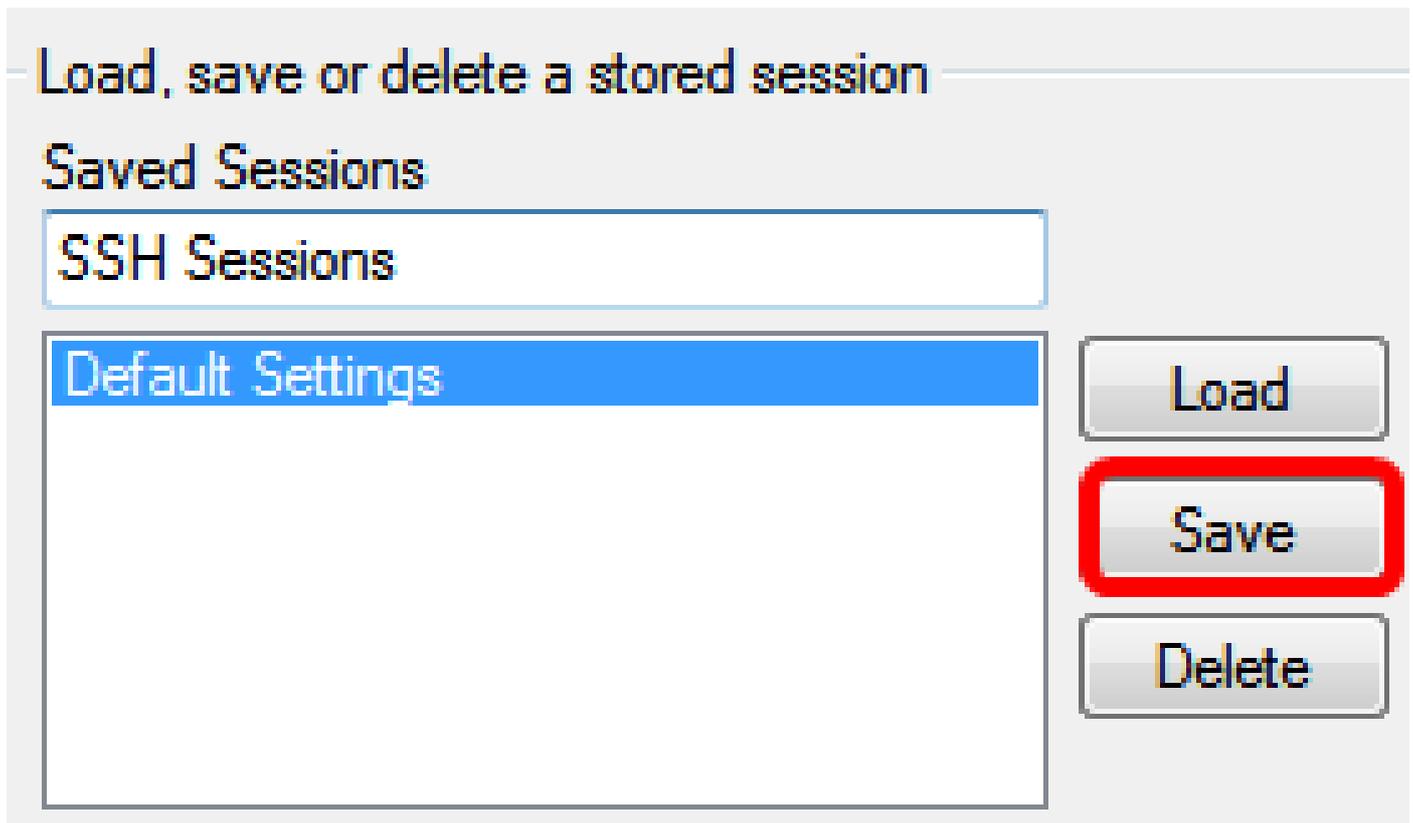
Load, save or delete a stored session

Saved Sessions

SSH Sessions

Observação: neste exemplo, as sessões SSH são usadas.

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

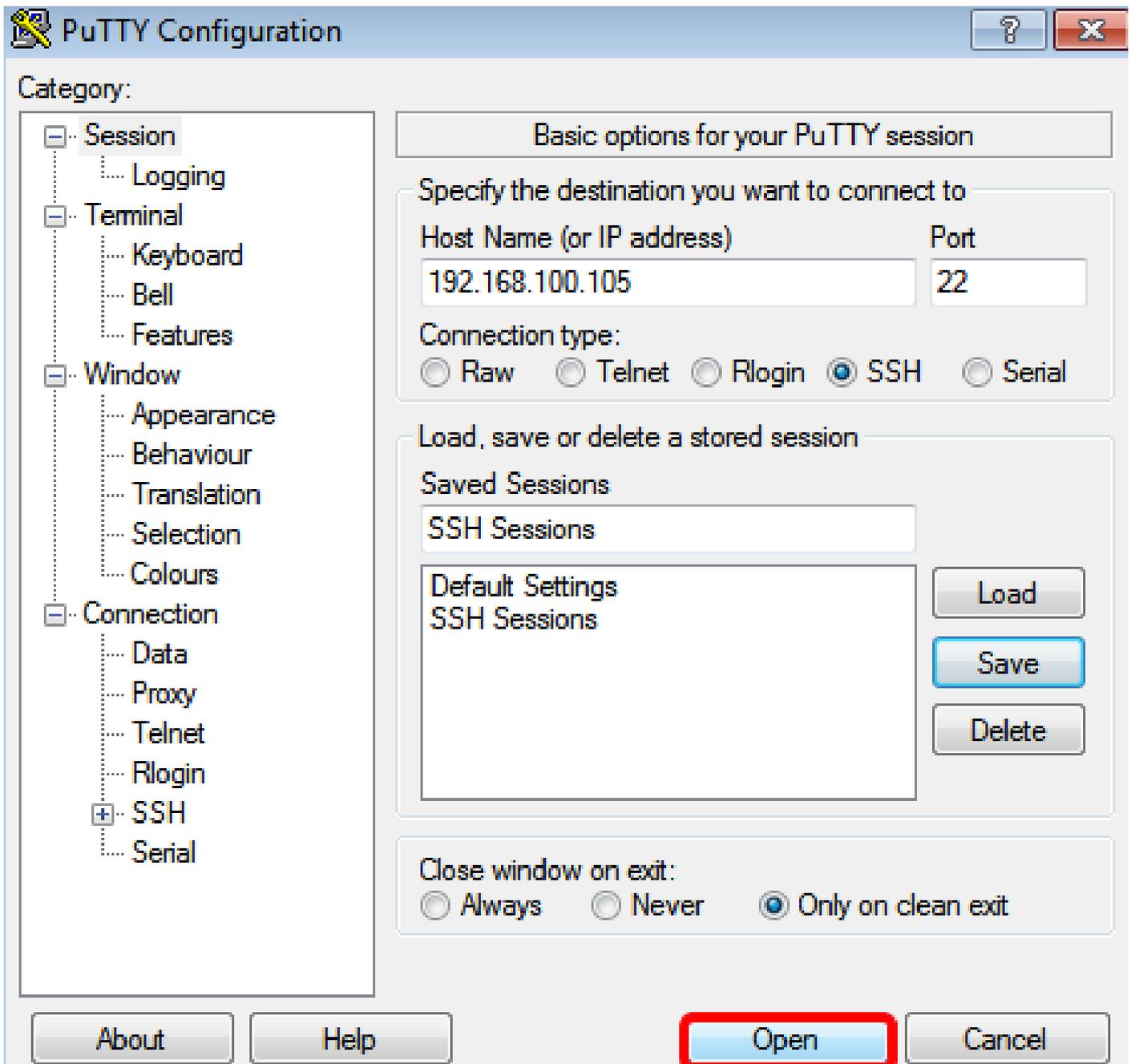


Etapa 7. (Opcional) Na área Fechar janela ao sair, clique no botão de opção para escolher o comportamento da janela SSH ao sair.



Observação: neste exemplo, a opção Somente na saída limpa é escolhida.

Etapa 8. Clique em Abrir para iniciar a sessão.



Etapa 9. Se esta for a primeira vez que você usa SSH para se conectar ao switch, você poderá receber um Aviso de violação de segurança. Este aviso avisa 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 (Nome do host) na Etapa 4, clique em Yes para atualizar a chave RSA2 (Rivest Shamir Adleman 2) para incluir o novo switch.



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.

Etapa 10. Insira o nome de usuário e a senha do switch nos campos login as, User Name e Password.

```
192.168.100.105 - PuTTY
login as: cisco

User Name:cisco
Password:*****

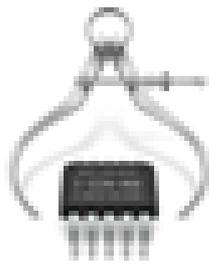
SG350X#
```

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

Acessar o CLI através do SSH usando o Terminal

Nota: 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 Terminal é 2.7.1.

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



System
Information.app



Terminal.app



VoiceOver
Utility.app

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

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

```
Cisco — ssh 192.168.100.105 — 81x24
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)?
```

Nota: Neste exemplo, 192.168.100.105.

Etapa 3. Quando aparecer a mensagem perguntando se você deseja continuar a conexão, digite Yes.

```
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
```

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

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

Acessar a CLI do Switch através de Telnet

As sessões Telnet desconectam-se 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 usando PuTTY](#)

[Computador Mac usando Terminal](#)

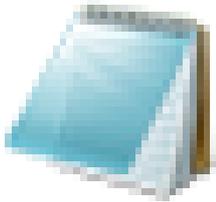
Acessar a CLI através de Telnet usando PuTTY

Nota: 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.



PuTTY



Notepad

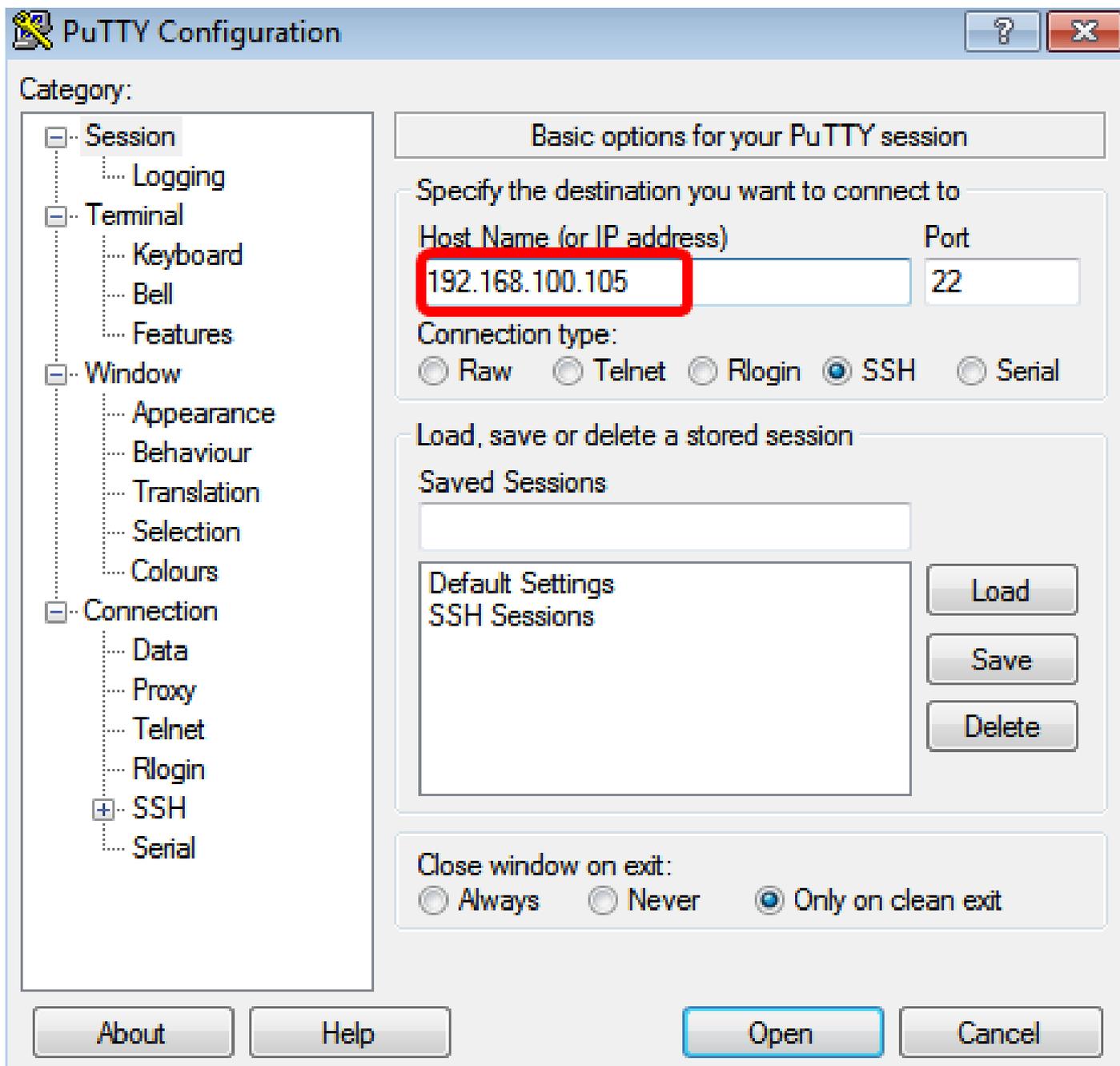


Command Prompt



FindIT2.0

Etapa 2. Insira o nome do host ou o endereço IP do switch que você deseja acessar remotamente no campo Nome do host (ou endereço IP).



Nota: 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.

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address)

192.168.100.105

Port

23

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)

192.168.100.105

Port

23

Connection type:

Raw Telnet Rlogin SSH Serial

Etapa 5. (Opcional) Para salvar a sessão, digite o nome da sessão no campo Sessões Salvas.

Load, save or delete a stored session

Saved Sessions

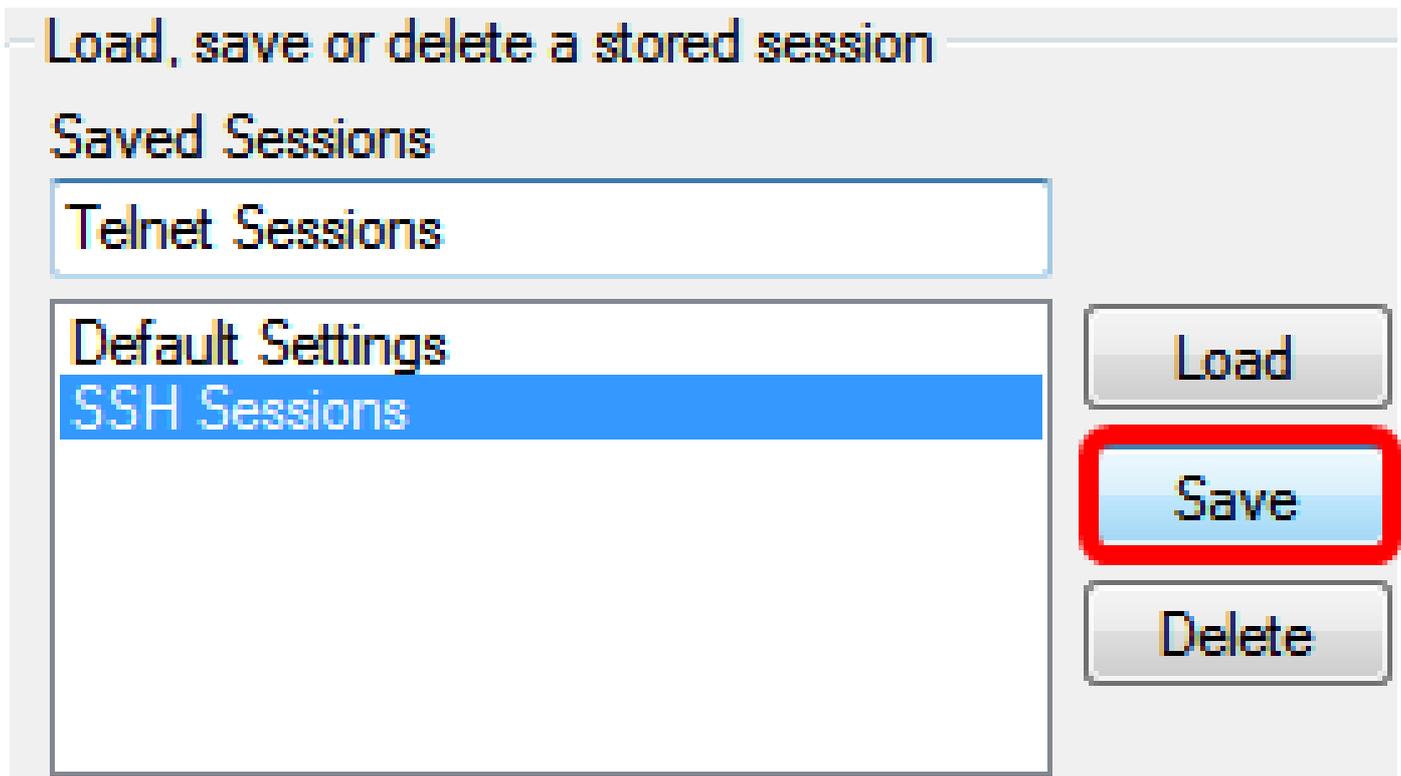
Telnet Sessions

Default Settings

SSH Sessions

Observação: neste exemplo, são usadas sessões Telnet.

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

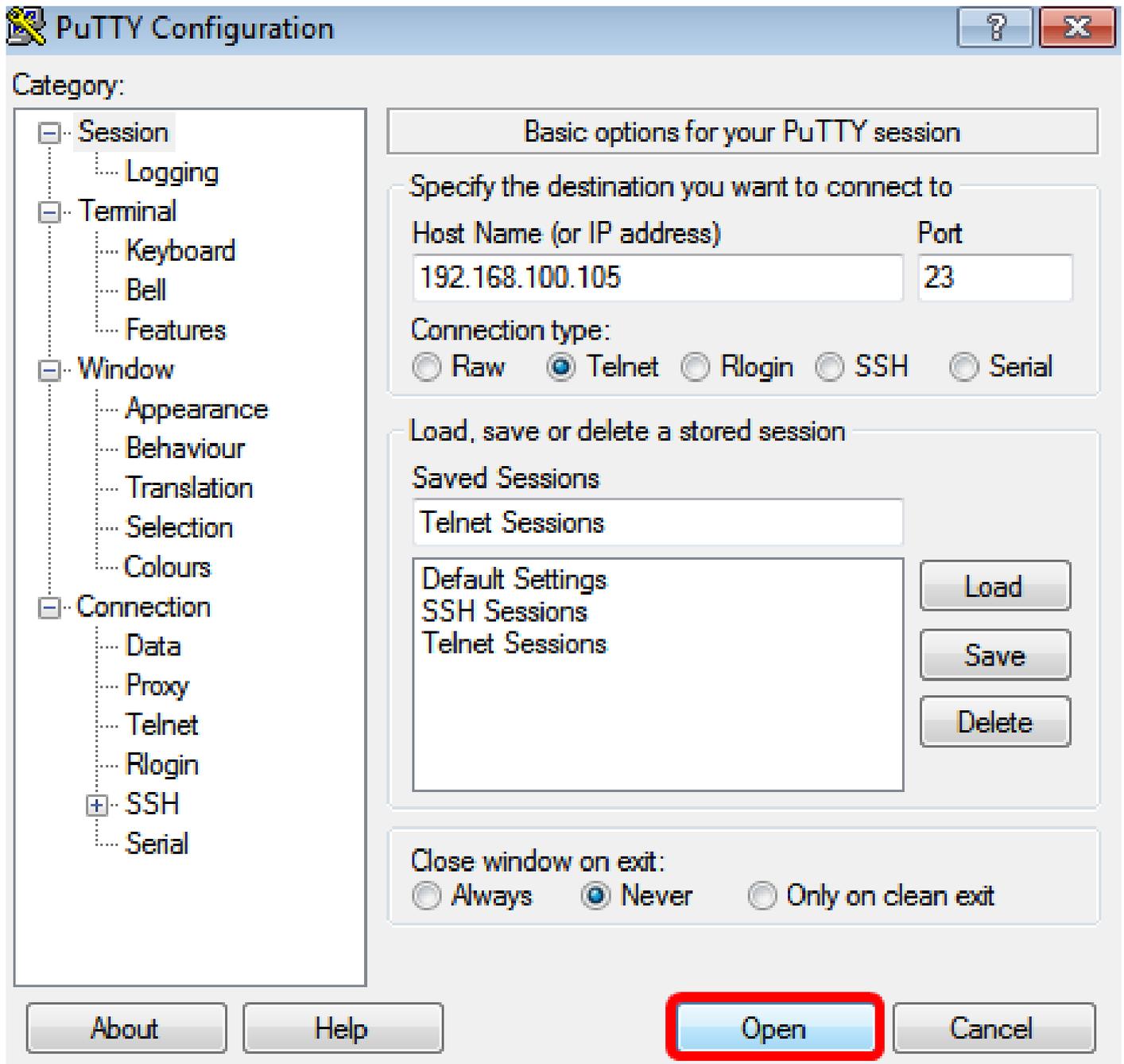


Passo 7. (Opcional) Na área Fechar janela ao sair, clique no botão de opção para escolher o comportamento da janela SSH ao sair.

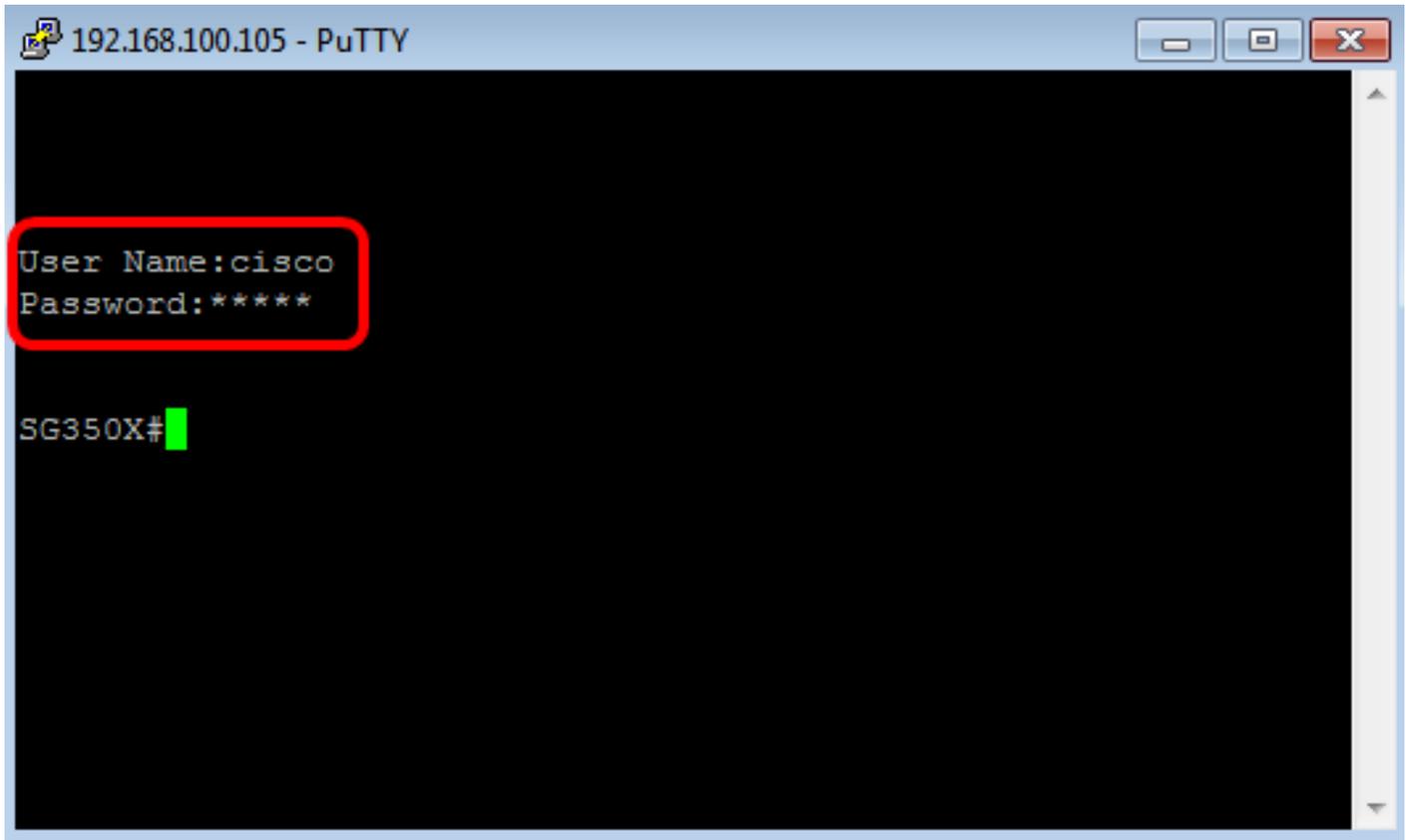


Nota: Neste exemplo, Nunca é escolhido.

Etapa 8. Clique em Abrir para iniciar a sessão.



Etapa 9. Insira o nome de usuário e a senha do switch nos campos login as, User Name e Password.



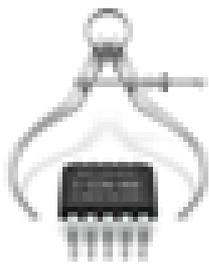
```
192.168.100.105 - PuTTY
User Name:cisco
Password:*****
SG350X#
```

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

Acessar o CLI através de Telnet usando Terminal

Nota: 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 Terminal é 2.7.1.

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



System
Information.app



VoiceOver
Utility.app

Etapa 2. Insira o comando telnet e 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: █
```

Nota: 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.

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

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.