

Accesso alla CLI di Cisco Business Switch tramite SSH o Telnet

Obiettivo

È possibile accedere in remoto agli switch Cisco Business Managed Switch e configurarli tramite l'interfaccia della riga di comando (CLI). L'accesso alla CLI permette di immettere i comandi nella finestra di un terminale. Se si preferisce configurare l'uso dei comandi sullo switch dalla CLI anziché dall'utilità basata sul Web, questa è una valida alternativa. Alcune attività, ad esempio l'abilitazione della modalità Layer 3, possono essere eseguite solo dalla CLI.

Per accedere alla CLI dello switch da remoto, usare il client SSH o Telnet. I servizi Telnet e SSH devono essere attivati sullo switch prima di potervi accedere da remoto.

Nota: per istruzioni su come configurare il protocollo Transmission Control Protocol (TCP) e il protocollo User Datagram Protocol (UDP) sullo switch, fare clic [qui](#).

In questo articolo viene spiegato come accedere alla CLI dello switch in modalità SSH o Telnet sui seguenti client:

- PuTTY - Un client Telnet e SSH standard. È possibile scaricare [qui](#) un programma di installazione e installare il client sul proprio computer Windows.
- Terminale: un'applicazione preinstallata in ogni computer Mac OS X. Noto anche come shell o console.

Importante: prima di stabilire una connessione SSH o Telnet allo switch, è necessario impostare l'indirizzo IP dello switch. Per istruzioni, fare clic [qui](#).

Dispositivi interessati | Versione del software

- CBS250 ([scheda tecnica](#)) | 3.0.0
- CBS350 ([scheda tecnica](#)) | 3.0.0
- CBS350-2X ([scheda tecnica](#)) | 3.0.0
- CBS350-4X ([scheda tecnica](#)) | 3.0.0

Accesso alla CLI dello switch con SSH

Le sessioni SSH vengono chiuse una volta trascorso automaticamente il tempo di inattività configurato nello switch. Il timeout di sessione inattiva predefinito in modalità SSH è 10 minuti.

Per effettuare una connessione SSH allo switch, scegliere la piattaforma:

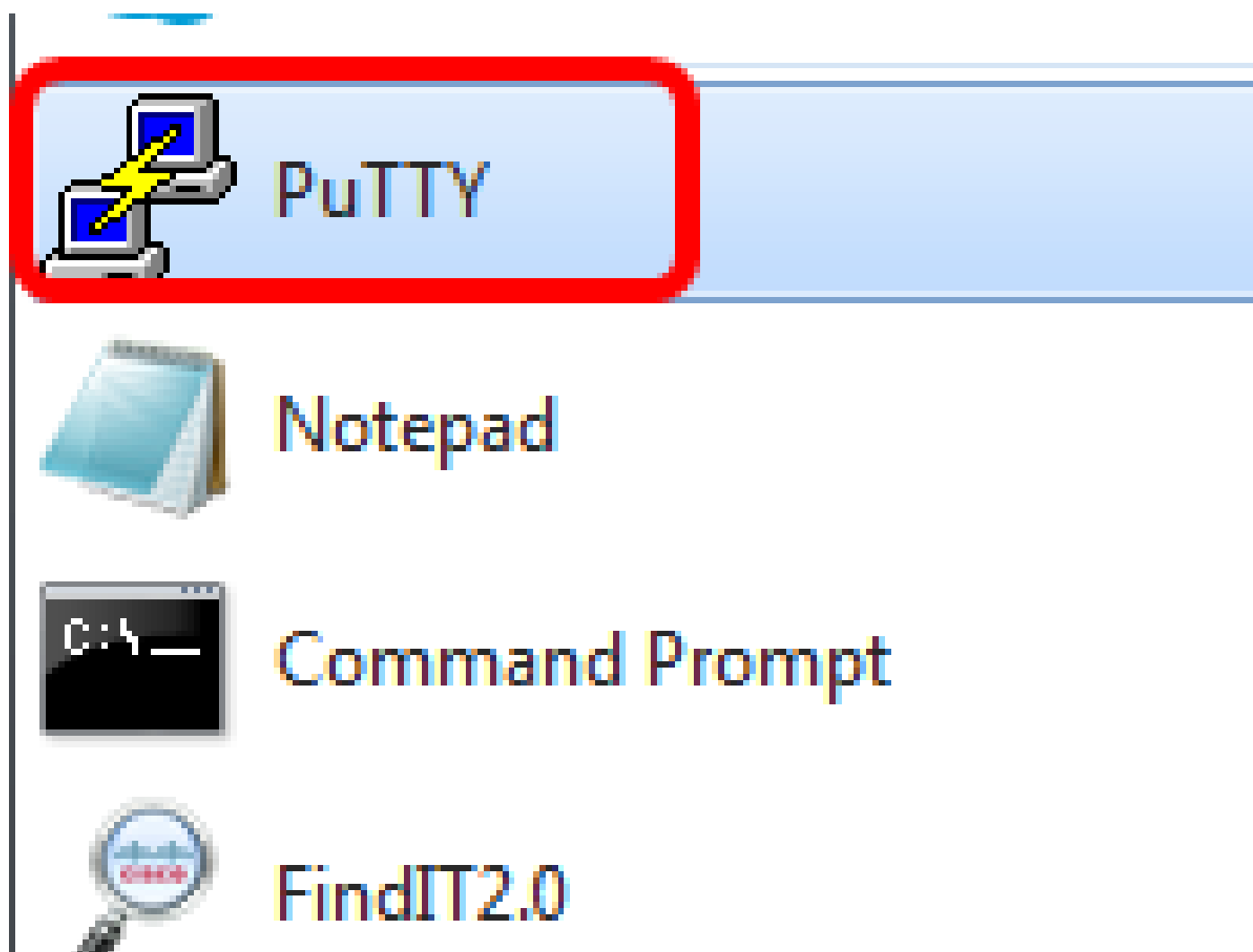
[Computer Windows con PuTTY](#)

[Computer Mac con Terminal](#)

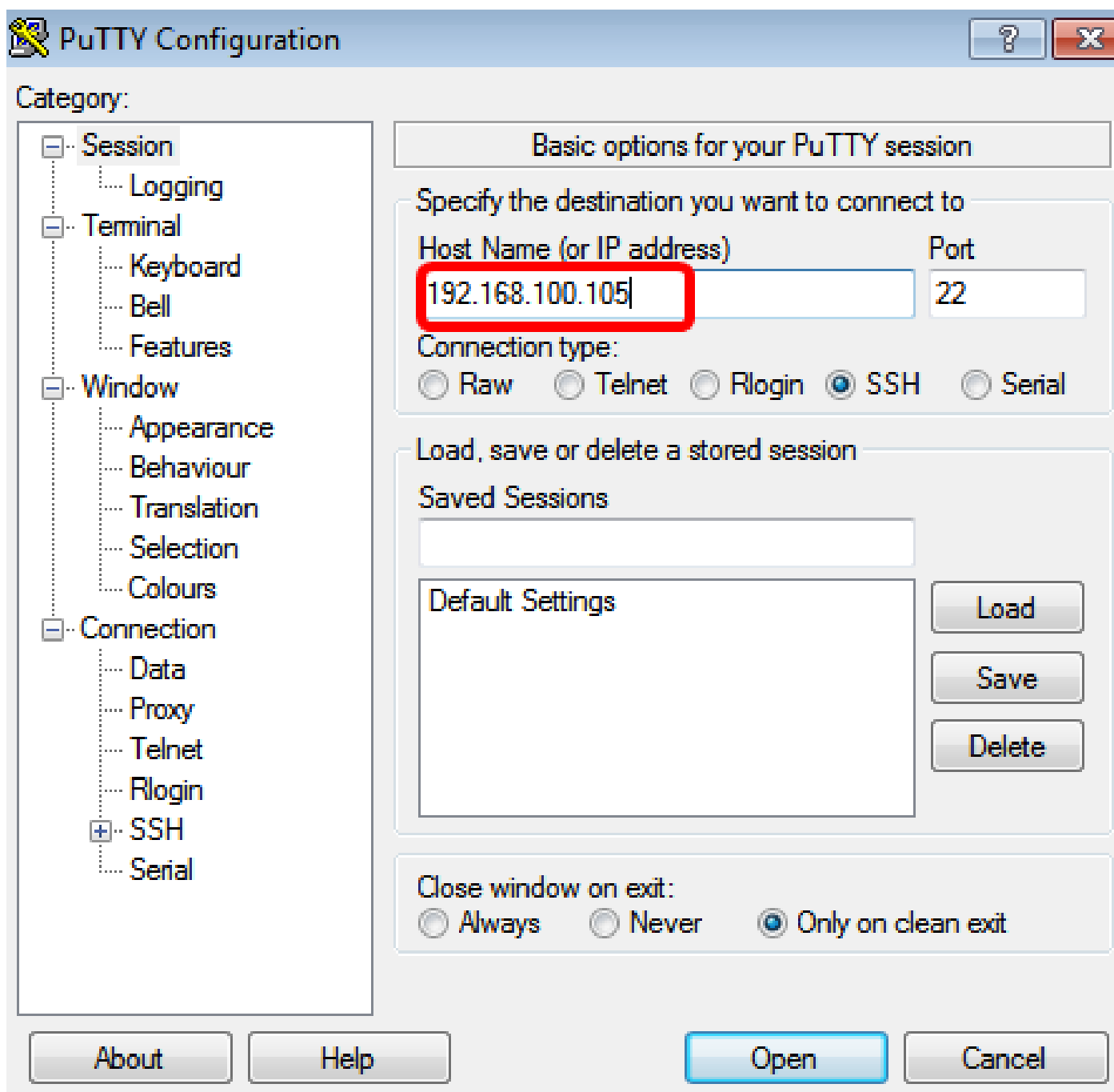
Accesso alla CLI in modalità SSH con PuTTY

Nota: le immagini possono variare in base alla versione di Windows in uso. Nell'esempio, viene usato Windows 7 Ultimate e PuTTY versione 0.63.

Passaggio 1. Avviare il client PuTTY sul computer.



Passaggio 2. Immettere il nome host o l'indirizzo IP dello switch a cui si vuole accedere da remoto nel campo Host Name (or IP address) (Nome host (o indirizzo IP)).



Nota: nell'esempio, l'indirizzo IP è 192.168.100.105.

Passaggio 3. Immettere 22 come numero di porta da usare per la sessione SSH nel campo Port (Porta).

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

Passaggio 4. Nell'area Connection type (Tipo di connessione), fare clic sul pulsante di opzione SSH per selezionare SSH come metodo di connessione allo 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

Passaggio 5. (Facoltativo) Per salvare la sessione, immettere il nome della sessione nel campo Saved Sessions (Sessioni salvate).

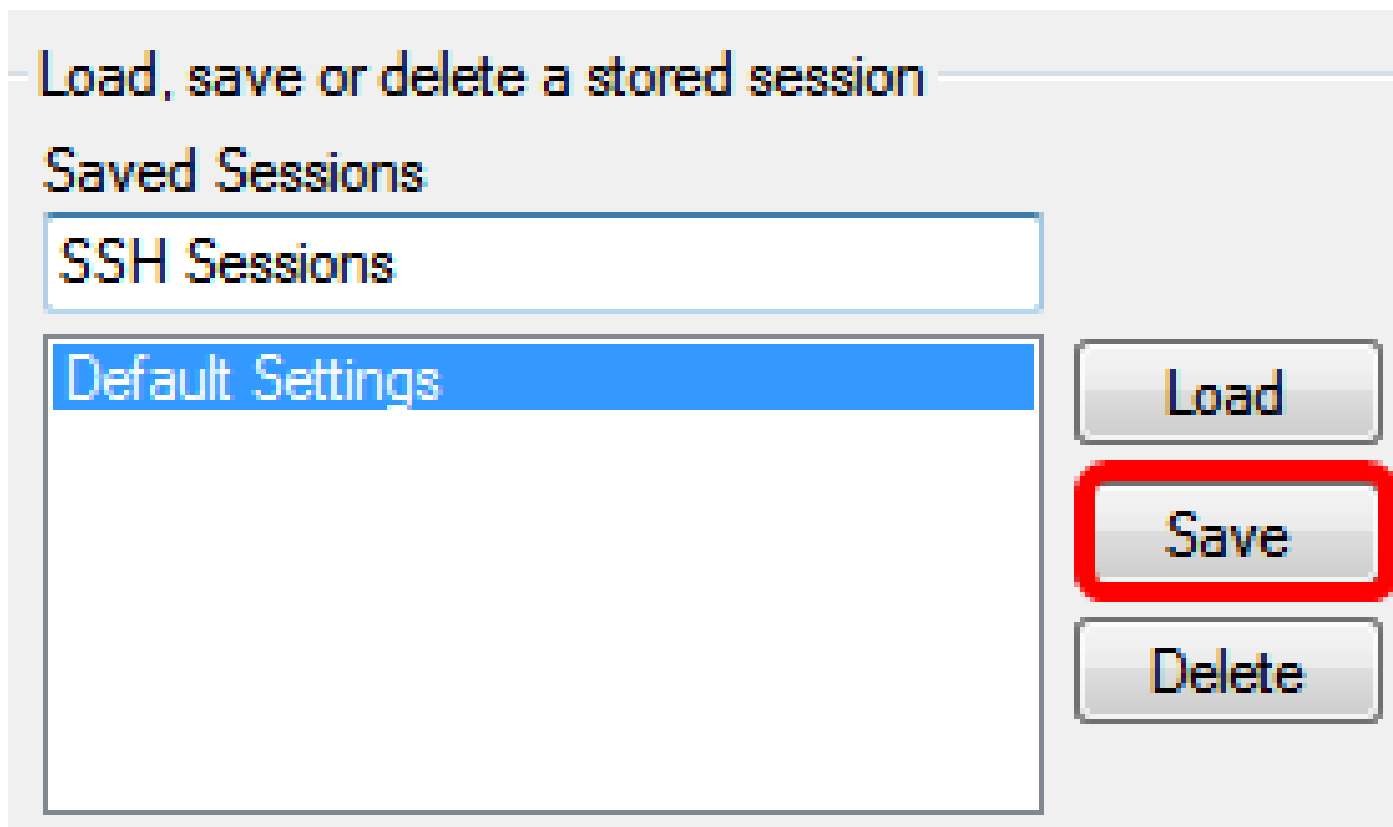
Load, save or delete a stored session

Saved Sessions

SSH Sessions

Nota: nell'esempio, vengono salvate le sessioni SSH.

Passaggio 6. (Facoltativo) Fare clic su Save (Salva) per salvare la sessione.

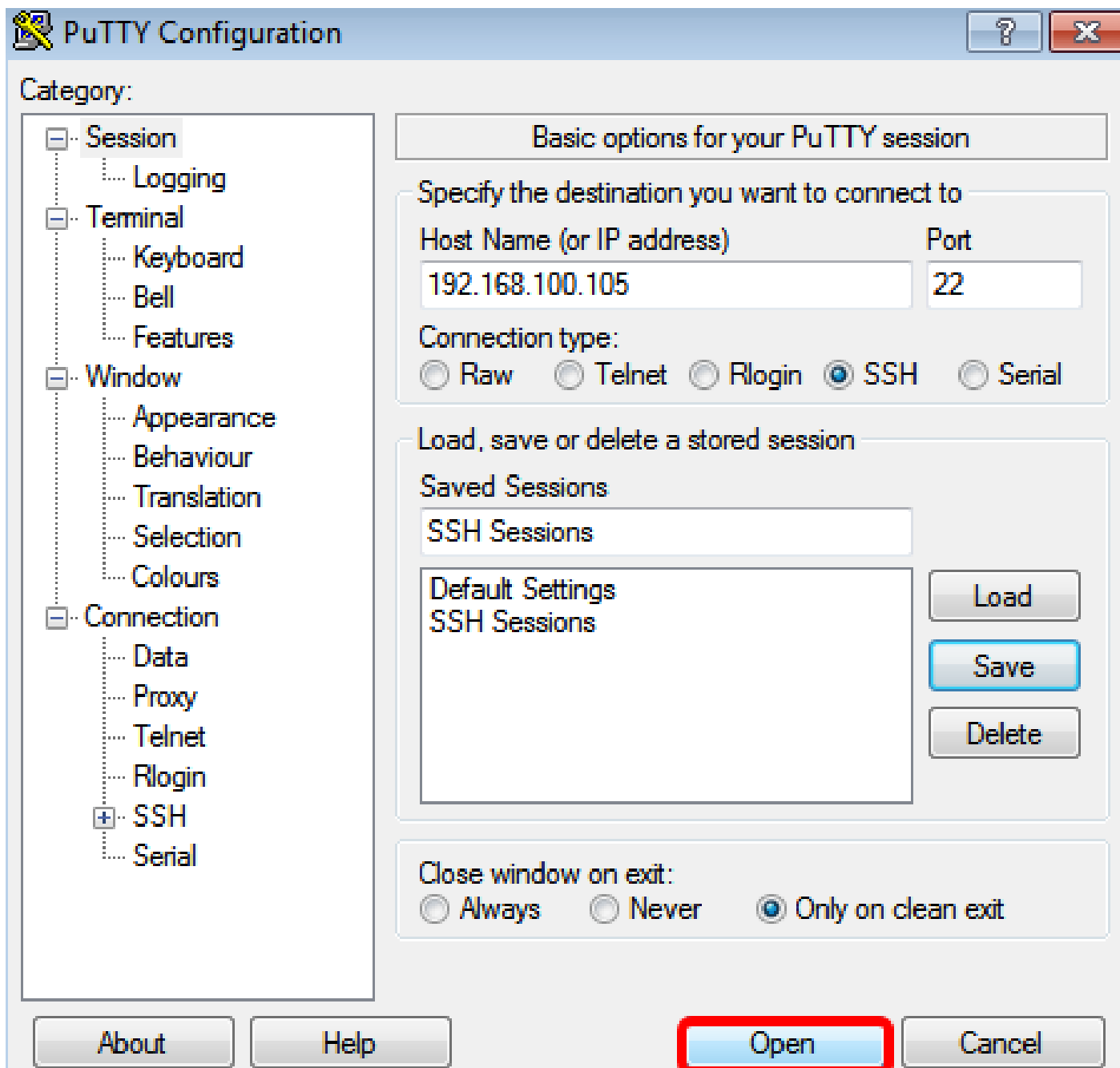


Passaggio 7. (Facoltativo) Nell'area Close window on exit (Chiudi la finestra all'uscita), fare clic sul pulsante di opzione per scegliere il comportamento della finestra SSH quando si chiude la sessione.



Nota: nell'esempio, è stata selezionata l'opzione Only on clean exit (Solo in caso di clean exit).

Passaggio 8. Fare clic su Open (Apri) per avviare la sessione.



Passaggio 9. Se è la prima volta che si utilizza SSH per connettersi allo switch, si potrebbe ricevere un avviso di violazione della sicurezza. Scopo dell'avviso è informare l'utente che il computer a cui sta tentando di connettersi potrebbe non essere lo switch. Dopo aver verificato di aver immesso l'indirizzo IP corretto nel campo Host Name (Nome host) al passaggio 4, fare clic su Yes (Sì) per aggiornare la chiave Rivest Shamir Adleman 2 (RSA2) e includere il nuovo 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.

Passaggio 10. Immettere il nome utente e la password dello switch nei campi login as (Accedi come), User Name (Nome utente) e Password.

```
192.168.100.105 - PuTTY
login as: cisco

User Name:cisco
Password:*****

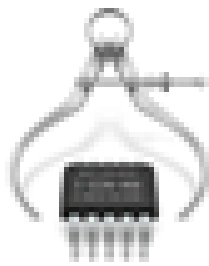
SG350X#
```

La procedura per accedere alla CLI dello switch da remoto in modalità SSH con PuTTY è ora conclusa.

Accesso alla CLI in modalità SSH con Terminal

Nota: le immagini possono variare in base al sistema operativo in uso sul computer Mac. Nell'esempio, viene utilizzato macOS Sierra e Terminal versione 2.7.1.

Passaggio 1. Andare a Applications > Utilities (Applicazioni > Utilità), quindi lanciare l'applicazione Terminal.app.



System Information.app



Terminal.app



VoiceOver Utility.app

Passaggio 2. Immettere il comando ssh e l'indirizzo IP per accedere alla CLI dello 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: nell'esempio, viene usato 192.168.100.105.

Passaggio 3. Quando viene visualizzato un messaggio che chiede se si vuole proseguire con la connessione, immettere Yes (Si).

```
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
```

Passaggio 4. Immettere il nome utente e la password dello switch nei campi User Name (Nome utente) e Password.

La procedura per accedere alla CLI dello switch da remoto in modalità SSH con Terminal è ora conclusa.

Accesso alla CLI dello switch in modalità Telnet

Le sessioni Telnet vengono chiuse una volta trascorso automaticamente il tempo di inattività configurato nello switch. Il timeout di sessione inattiva predefinito in modalità Telnet è 10 minuti.

Per effettuare una connessione Telnet allo switch, scegliere la piattaforma:

[Computer Windows con PuTTY](#)

[Computer Mac con Terminal](#)

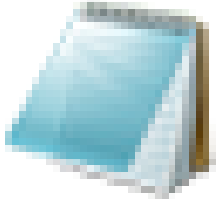
Accesso alla CLI in modalità Telnet con PuTTY

Nota: le immagini possono variare in base alla versione di Windows in uso. Nell'esempio, viene usato Windows 7 Ultimate e PuTTY versione 0.63.

Passaggio 1. Avviare il client PuTTY sul computer.



PuTTY



Notepad

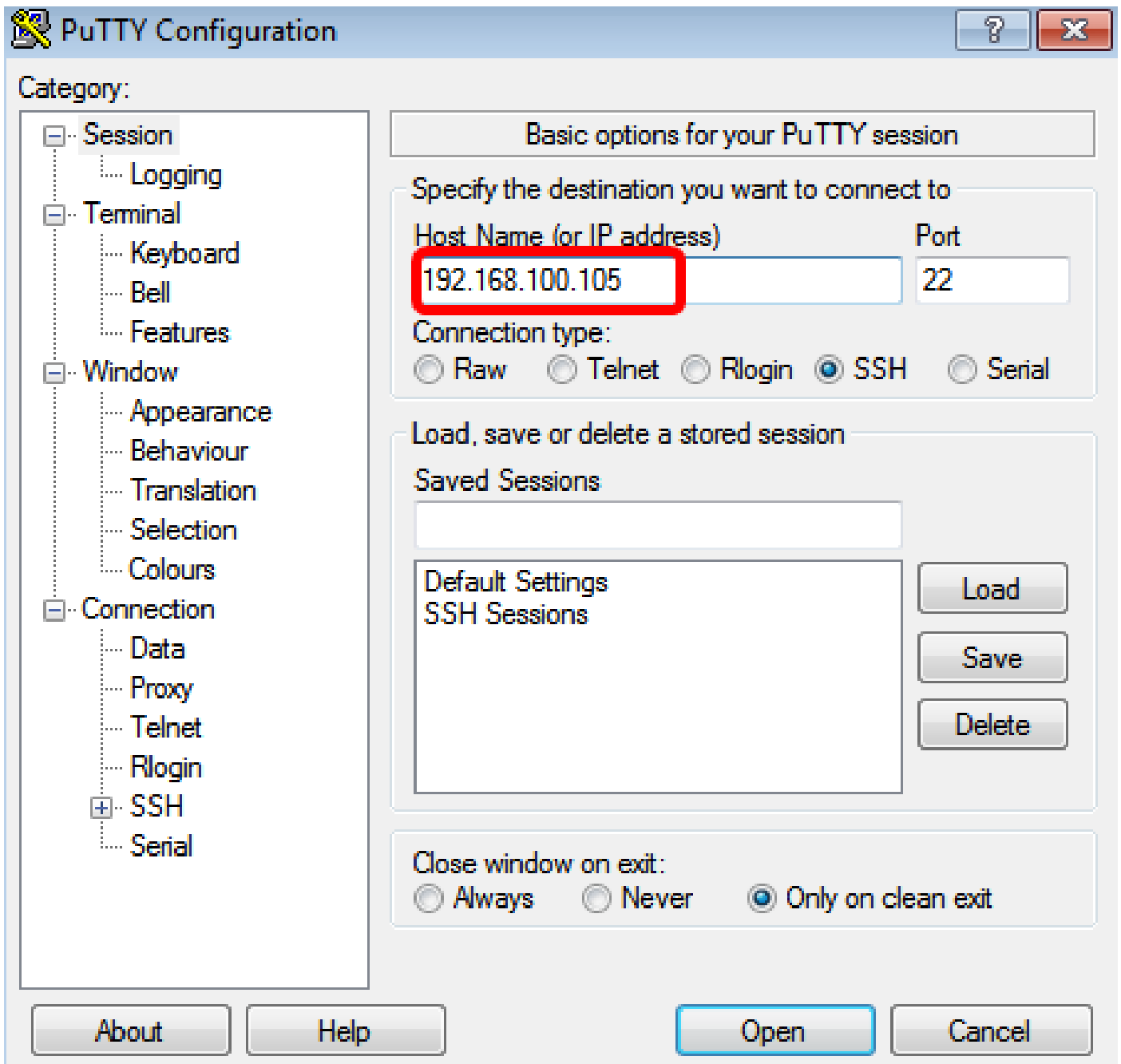


Command Prompt



FindIT2.0

Passaggio 2. Immettere il nome host o l'indirizzo IP dello switch a cui si vuole accedere da remoto nel campo Host Name (or IP address) (Nome host (o indirizzo IP)).



Nota: nell'esempio, viene usato 192.168.100.105.

Passaggio 3. Immettere 23 nel campo Port (Porta) come numero di porta da usare nella sessione Telnet.

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

Passaggio 4. Nell'area Connection type (Tipo di connessione), fare clic sul pulsante di opzione Telnet per selezionare Telnet come metodo di connessione allo 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

Passaggio 5. (Facoltativo) Per salvare la sessione, immettere il nome della sessione nel campo Saved Sessions (Sessioni salvate).

Load, save or delete a stored session

Saved Sessions

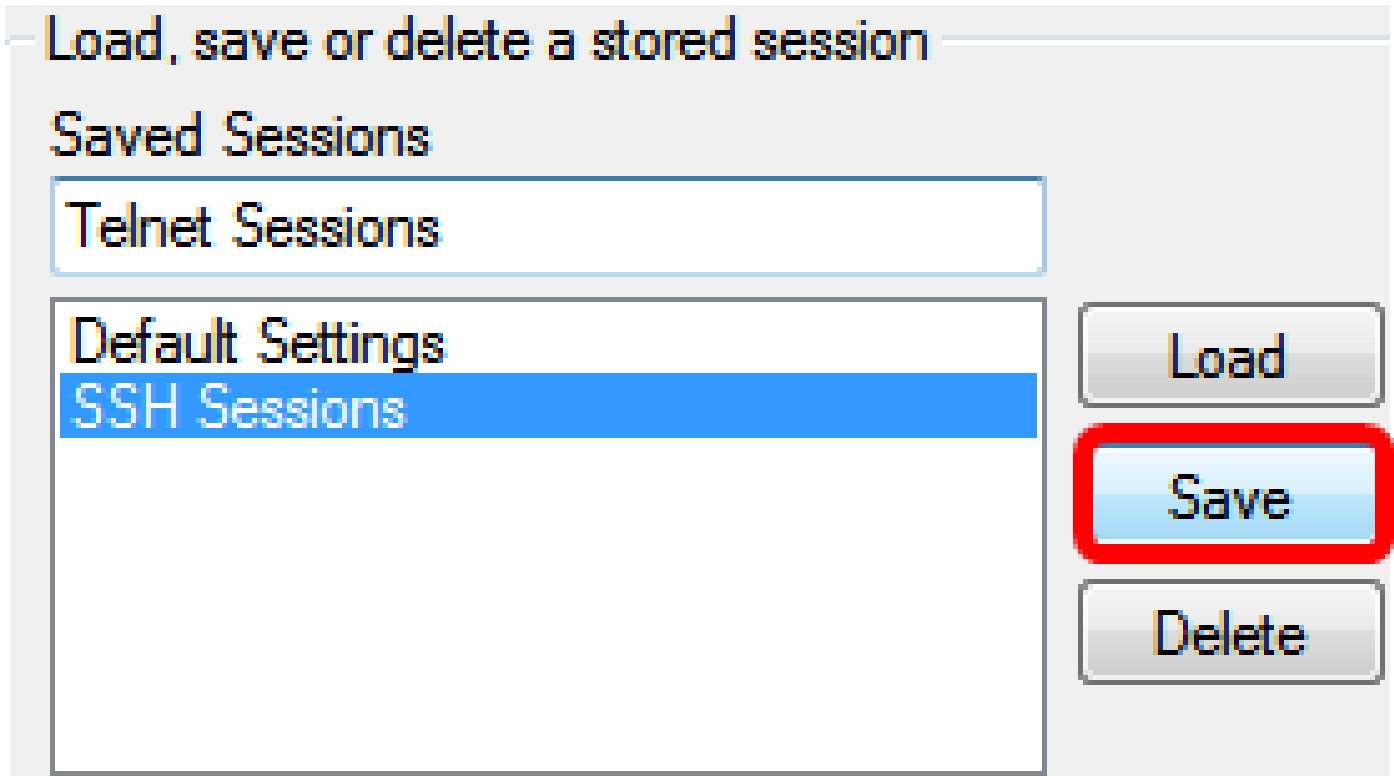
Telnet Sessions

Default Settings

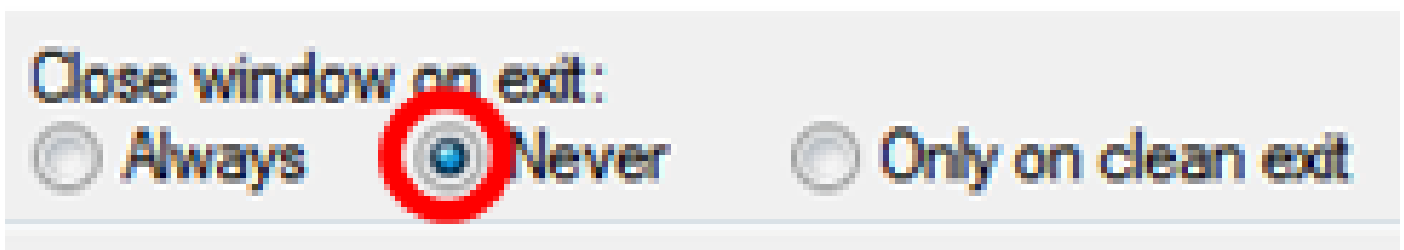
SSH Sessions

Nota: nell'esempio, vengono salvate le sessioni Telnet.

Passaggio 6. (Facoltativo) Fare clic su Save (Salva) per salvare la sessione.

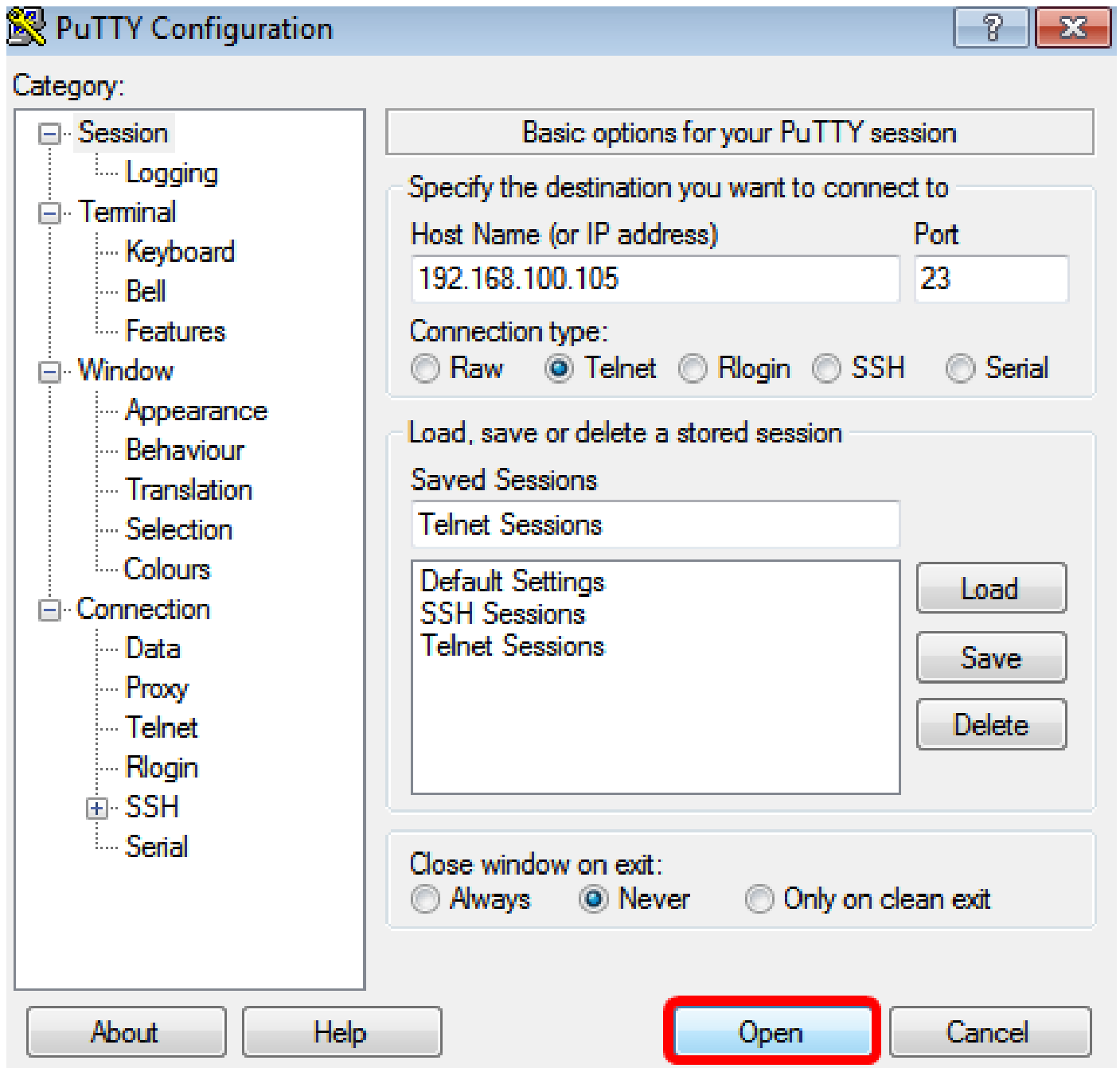


Passaggio 7. (Facoltativo) Nell'area Close window on exit (Chiudi la finestra all'uscita), fare clic sul pulsante di opzione per scegliere il comportamento della finestra Telnet quando si chiude la sessione.

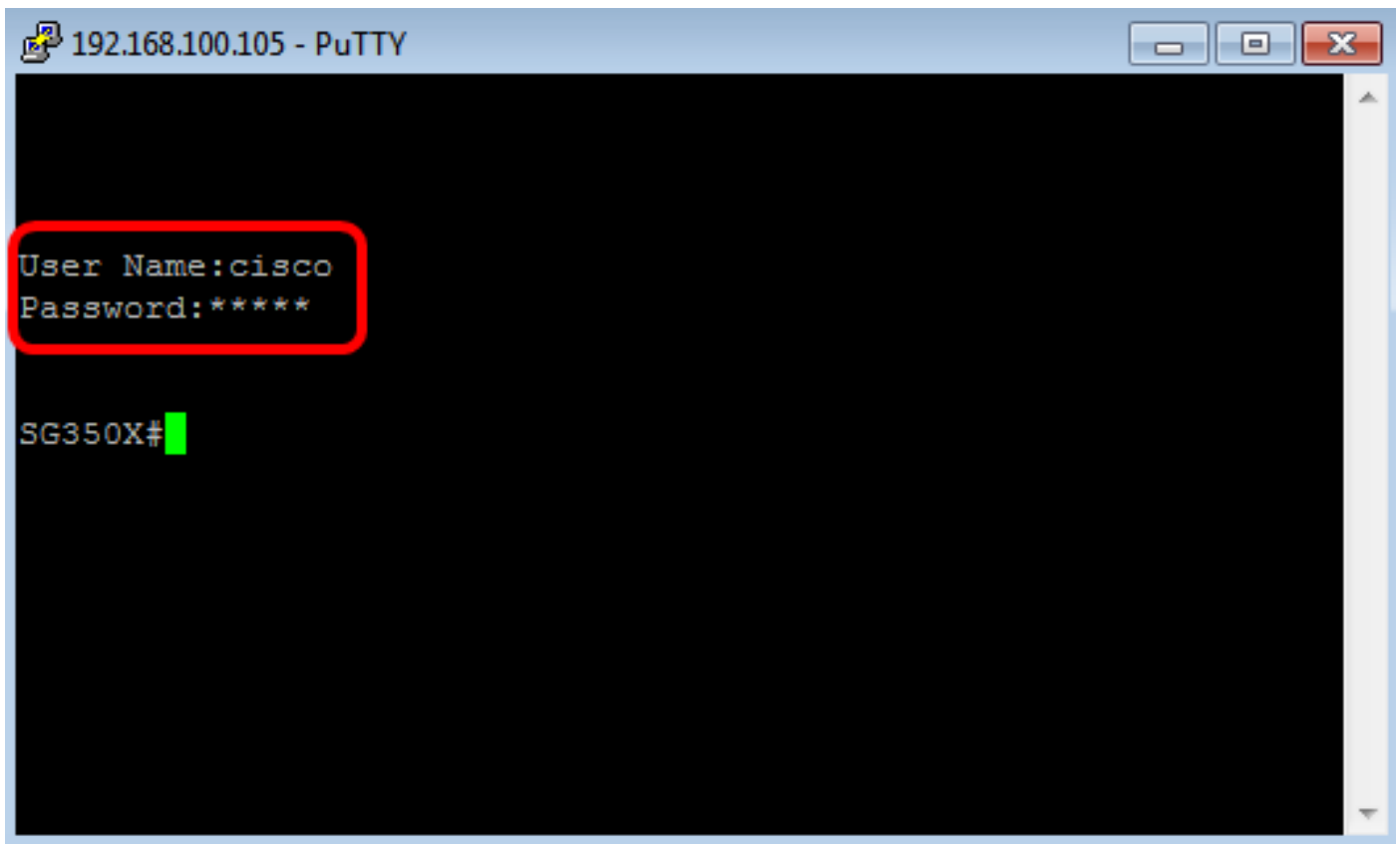


Nota: nell'esempio, è stata selezionata l'opzione Never (Mai).

Passaggio 8. Fare clic su Open (Apri) per avviare la sessione.



Passaggio 9. Immettere il nome utente e la password dello switch nei campi login as (Accedi come), User Name (Nome utente) e Password.



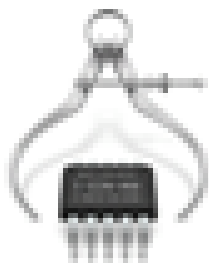
```
192.168.100.105 - PuTTY
User Name:cisco
Password:*****
SG350X#
```

La procedura per accedere alla CLI dello switch da remoto in modalità Telnet con PuTTY è ora conclusa.

Accesso alla CLI in modalità Telnet con Terminal

Nota: le immagini possono variare in base al sistema operativo in uso sul computer Mac. Nell'esempio, viene utilizzato macOS Sierra e Terminal versione 2.7.1.

Passaggio 1. Andare a Applications > Utilities (Applicazioni > Utilità), quindi lanciare l'applicazione Terminal.app.



System
Information.app



VoiceOver
Utility.app

Passaggio 2. Immettere il comando telnet e l'indirizzo IP per accedere alla CLI dello 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: nell'esempio, viene usato 192.168.100.105.

Passaggio 3. Immettere il nome utente e la password dello switch nei campi User Name (Nome utente) e Password.

La procedura per accedere alla CLI dello switch da remoto in modalità Telnet con Terminal è ora conclusa.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).