請求Cisco Cloud Email Security CLI訪問

目錄

[簡介](#)

[背景資訊](#)

[Linux和Mac使用者](#)

- [必要條件](#)
- [如何建立私有/公有RSA金鑰？](#)
- [如何開啟思科支援要求以提供我的公鑰？](#)
- [組態](#)
- [如果要連線到多個郵件安全裝置(ESA)或安全管理裝置(SMA)，該怎麼辦？](#)
- [如何配置ESA或SMA登入而不提示輸入密碼？](#)
- [完成先決條件後，這會是什麼樣子？](#)

[Windows使用者](#)

- [必要條件](#)
- [如何建立私有/公有RSA金鑰？](#)
- [如何開啟思科支援要求以提供我的公鑰？](#)
- [如何配置ESA或SMA登入而不提示輸入密碼？](#)
- [PuTy配置](#)
- [疑難排解](#)

簡介

本文說明如何請求訪問其Cloud Email Security(CES)CLI。

背景資訊

Cisco CES客戶有權使用金鑰身份驗證通過SSH代理訪問其ESA和SMA的CLI。對託管裝置的CLI訪問必須限於組織中的關鍵人員。

Linux和Mac使用者

對於Cisco CES客戶：
有關使用SSH通過CES代理進行CLI訪問的殼指令碼的說明。

必要條件

作為CES客戶，您必須與CES On-Boarding/Ops或Cisco TAC接洽，才能交換和放置SSH金鑰：

1. 生成私有/公有RSA金鑰。
2. 向思科提供您的PublicRSA金鑰。

3. 等待Cisco儲存並通知您您的金鑰已儲存到CES客戶帳戶。
4. 複製並修改connect2ces.sh指令碼。

如何建立私有/公有RSA金鑰？

Cisco建議在用於Unix/Linux/OS X的終端/CLI上使用「ssh-keygen」。使用ssh-keygen -b 2048 -t rsa -f ~/.ssh/<NAME> 命令。

附註：有關詳細資訊，請訪問https://www.ssh.com/academy/ssh/keygen。
確保您始終可以保護對RSA私鑰的訪問。
請勿將您的私鑰傳送到Cisco，只傳送公鑰(.pub)。
將您的公鑰提交給思科時，請識別該金鑰的電子郵件地址/名字/姓氏。

如何開啟思科支援要求以提供我的公鑰？

導航到此連結。

確保正確將SR標識為「Cisco CES Customer SSH/CLI Setup」等。

組態

若要開始，請使用opencopy提供的腳本，並將其中一個代理主機用作主機名稱。

確保您為所在地區選擇正確的代理(即，如果您是美國CES客戶，為了到達F4資料中心和裝置，請使用f4-ssh.iphmx.com。如果您是歐洲CES客戶，在德國DC擁有裝置，請使用f17-ssh.eu.iphmx.com。)

美聯社(ap.iphmx.com)
f15-ssh.ap.iphmx.com
f16-ssh.ap.iphmx.com

CA(ca.iphmx.com)
f13-ssh.ca.iphmx.com
f14-ssh.ca.iphmx.com

歐盟(c3s2.iphmx.com)
f10-ssh.c3s2.iphmx.com
f11-ssh.c3s2.iphmx.com

歐盟(eu.iphmx.com)（德國DC）
f17-ssh.eu.iphmx.com
f18-ssh.eu.iphmx.com

美國(iphmx.com)
f4-ssh.iphmx.com
f5-ssh.iphmx.com

如果要連線到多個郵件安全裝置(ESA)或安全管理裝置(SMA)，該怎麼辦？

複製並儲存connect2ces.sh的第二個副本，例如connect2ces_2.sh。

附註：您將希望將「cloud_host」編輯為要訪問的附加裝置。
您將要將'local_port'編輯為2222以外的內容。否則，您將收到一個錯誤：「警告：遠端主機標識已更改！」

如何配置ESA或SMA登入而不提示輸入密碼？

閱讀本指南。

完成先決條件後，這會是什麼樣子？

joe.user@my_local > ~ ./connect2ces
[-]正在連線到您的代理伺服器(f4-ssh.iphmx.com)。..
[-]代理連線成功。現在已連線到f4-ssh.iphmx.com。
[-]在PID上運行的代理：31253
[-]正在連線到CES裝置(esa1.rs1234-01.iphmx.com)。..

上次登入時間：2019年4月22日週一11:33:45，自10.123.123.123
適用於Cisco C100V內部版本071的AsyncOS 12.1.0

歡迎使用Cisco C100V電子郵件安全虛擬裝置

附註：如果閒置1440分鐘，此會話將過期。任何未提交的配置更改都將丟失。一旦進行了配置更改，請立即提交這些更改。

(電腦esa1.rs1234-01.iphmx.com)>
(電腦esa1.rs1234-01.iphmx.com)>退出

已關閉到127.0.0.1的連線。
[-]正在關閉代理連線……
[-]完成。

connect2ces.sh

註：確保您為所在地區選擇正確的代理(即，如果您是美國CES客戶，為了到達F4資料中心和裝置，請使用f4-ssh.iphmx.com。如果您是歐洲CES客戶，在德國DC擁有裝置，請使用f17-ssh.eu.iphmx.com。)

#!/bin/bash

```
#--編輯以下值----------------------
#應該已經與CES建立以下值：
# cloud_user="username"
# cloud_host="esaX.CUSTOMER.iphmx.com"或"smaX.CUSTOMER.iphmx.com"
## [確保您擁有正確的區域性CES資料中心設定！]
# private_key="LOCAL_PATH_TO_SSH_PRIVATE_RSA_KEY"
# proxy_server="PROXY_SERVER" [僅選擇一個！]
#
##對於「proxy_server」，以下是SSH代理：
##
##美聯社(ap.iphmx.com)
## f15-ssh.ap.iphmx.com
## f16-ssh.ap.iphmx.com
##
## CA(ca.iphmx.com)
## f13-ssh.ca.iphmx.com
## f14-ssh.ca.iphmx.com
##
##歐盟(c3s2.iphmx.com)
## f10-ssh.c3s2.iphmx.com
## f11-ssh.c3s2.iphmx.com
##
##歐洲(eu.iphmx.com)（德國DC）
## f17-ssh.eu.iphmx.com
## f18-ssh.eu.iphmx.com
##
##美國(iphmx.com)
## f4-ssh.iphmx.com
## f5-ssh.iphmx.com

cloud_user="username"
cloud_host="esaX.CUSTOMER.iphmx.com"
private_key="LOCAL_PATH_TO_SSH_PRIVATE_RSA_KEY"
proxy_server="代理伺服器"

#--保留這些值原樣--------------------
# 'proxy_user'不應更改
# 'remote_port'保持22(SSH)
# 'local_port'可以根據需要設定為不同的值

proxy_user="dh-user"
remote_port=22
local_port=2222

#--不要在此行下編輯----------------

proxycmd="ssh -f -L $local_port:$cloud_host:$remote_port -i $private_key -N
```

```
$proxy_user@$proxy_server"

printf "[-]正在連線到代理伺服器($proxy_server)。..\n"
$proxycmd >/dev/null 2>&1
如果nc -z 127.0.0.1 $local_port >/dev/null 2>&1;然後
printf "[-]代理連線成功。現在已連線到$proxy_server。\n"
其他
printf "[-]代理連線失敗。正在退出……\n"
exit
fi

#查詢代理ssh進程
proxypid='ps -xo pid，命令 | grep "$cloud_host" | grep "$proxy_server" | head -n1 | sed "s/^[ \t]*/" | cut -d " " -f1'
printf "[-]代理在PID上運行：$proxypid\n"

printf "[-]正在連線到CES裝置($cloud_host)。..\n\n"
ssh -p $local_port $cloud_user@127.0.0.1

printf "[-]正在關閉代理連線……\n"
殺死$proxypid

printf "[-]完成。\n"

#--想避免每次都輸入密碼嗎？
#--請參閱：https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118305-technote-esa-00.html
#--需要訪問多個ESA或SMA?複製相同的指令碼並重新命名為connect2ces_2.sh或類似名稱。
```

原始文檔:https://github.com/robsherw/connect2ces。

Windows使用者

使用PuTTY和使用SSH以通過CES代理進行CLI訪問的說明。

必要條件

作為CES客戶，您必須已委託CES自註冊/運營，或思科TAC來交換和放置SSH金鑰：

1. 生成私有/公有RSA金鑰。
2. 向思科提供您的公用RSA金鑰。
3. 等待Cisco儲存並通知您您的金鑰已儲存到您的CES客戶帳戶。
4. 按照以下說明中的詳細資訊設定PuTTY。

如何建立私有/公有RSA金鑰？

思科建議對Windows使用PuTTYgen(https://www.puttygen.com/)。

有關詳細資訊，請訪問https://www.ssh.com/ssh/putty/windows/puttygen。

附註：確保您始終可以保護對RSA私鑰的訪問。
請勿將您的私鑰傳送到Cisco，只傳送公鑰(.pub)。
將您的公鑰提交給思科時，請識別其金鑰的電子郵件地址/名字/姓氏。

如何開啟思科支援要求以提供我的公鑰？

導航到此連結。

確保正確將SR標識為「Cisco CES Customer SSH/CLI Setup」等。

如何配置ESA或SMA登入而不提示輸入密碼？

閱讀本指南。

PuTy配置

若要開始，請開啟PuTTY並將以下代理主機之一用於主機名:

確保您為所在地區選擇正確的代理(即，如果您是美國CES客戶，為了到達F4資料中心和裝置，請使用f4-ssh.iphmx.com。如果您是歐洲CES客戶，在德國DC擁有裝置，請使用f17-ssh.eu.iphmx.com。)

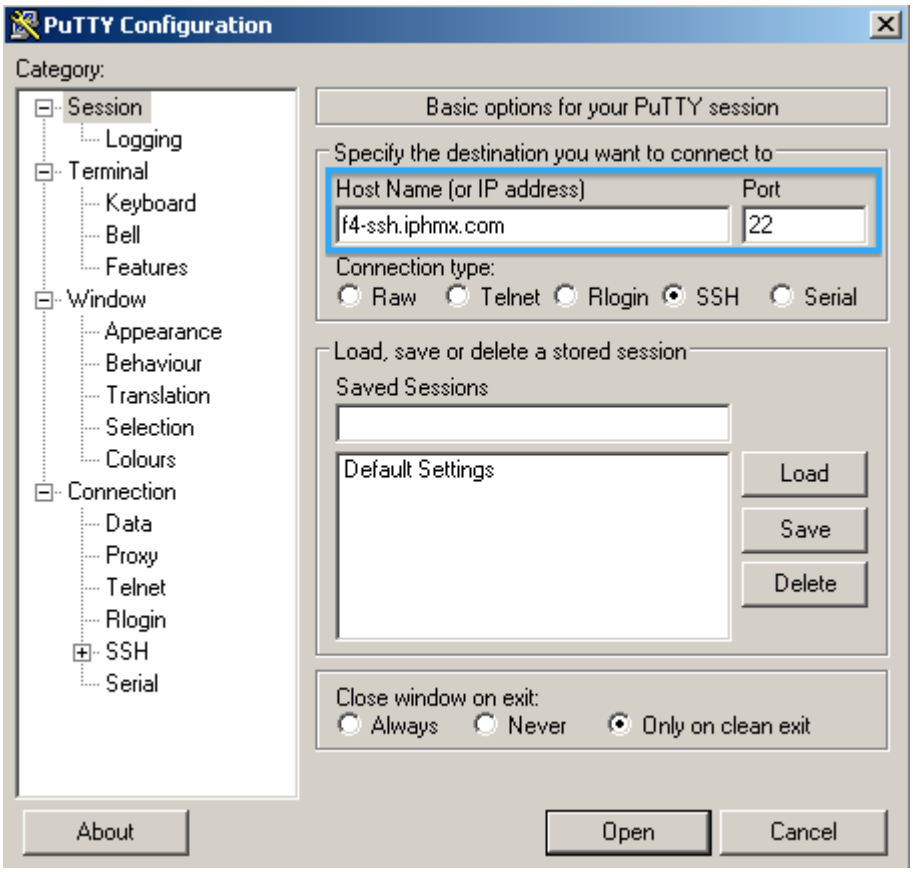
美聯社(ap.iphmx.com)
f15-ssh.ap.iphmx.com
f16-ssh.ap.iphmx.com

CA(ca.iphmx.com)
f13-ssh.ca.iphmx.com
f14-ssh.ca.iphmx.com

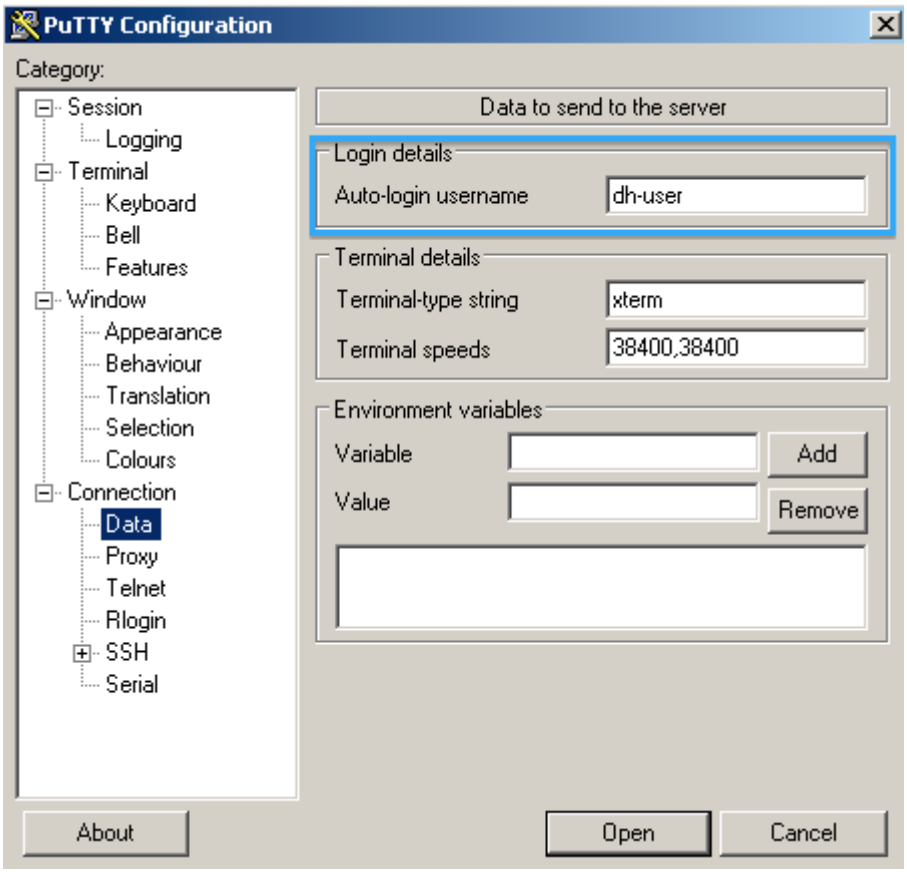
歐盟(c3s2.iphmx.com)
f10-ssh.c3s2.iphmx.com
f11-ssh.c3s2.iphmx.com

歐盟(eu.iphmx.com)（德國DC）
f17-ssh.eu.iphmx.com
f18-ssh.eu.iphmx.com

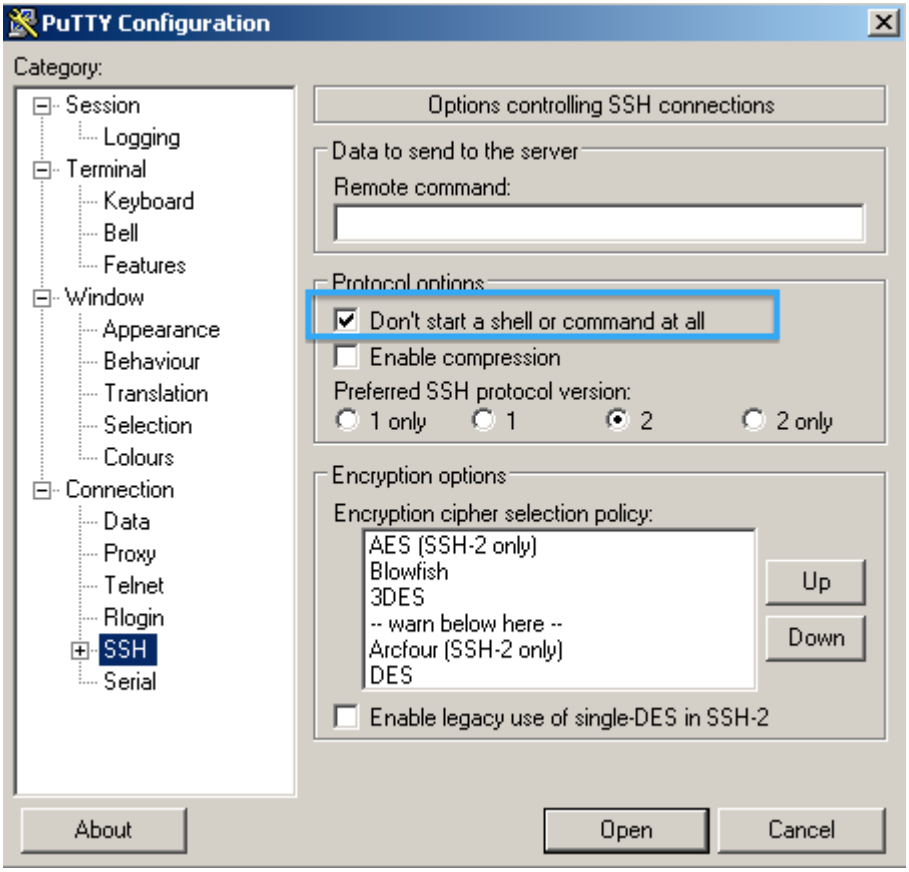
美國(iphmx.com)
f4-ssh.iphmx.com
f5-ssh.iphmx.com



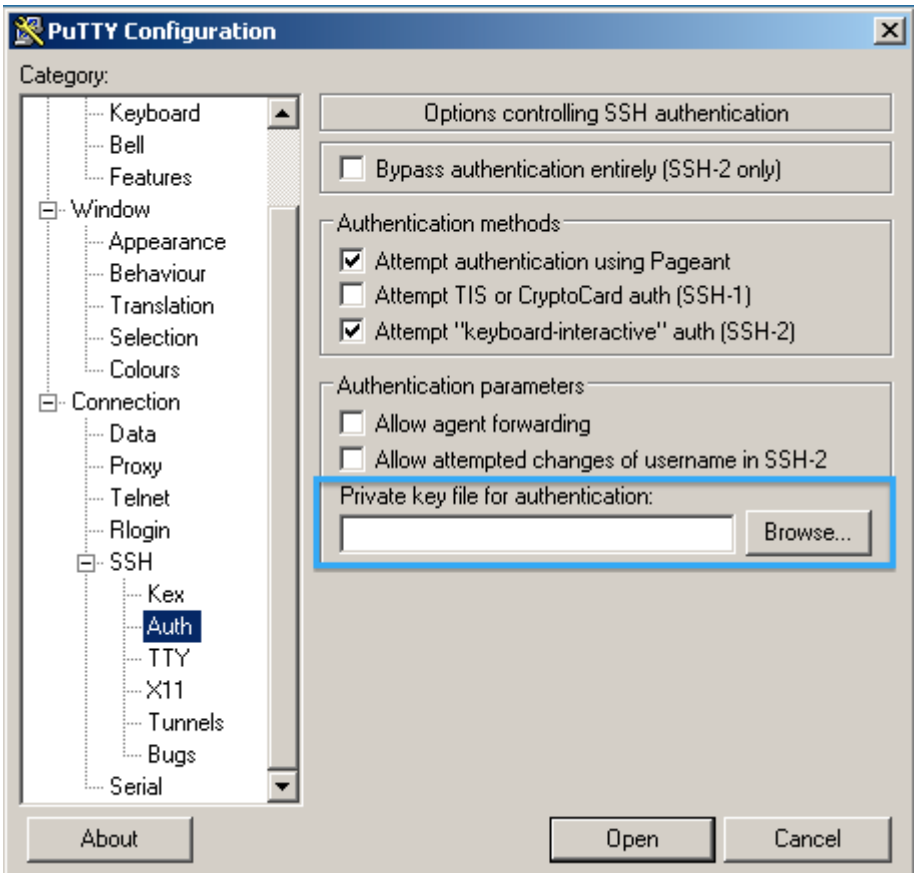
按一下資料獲取登入詳細資訊，使用自動登入使用者名稱並輸入dh-user。



選擇SSH並選中Don't start a shell or command all。

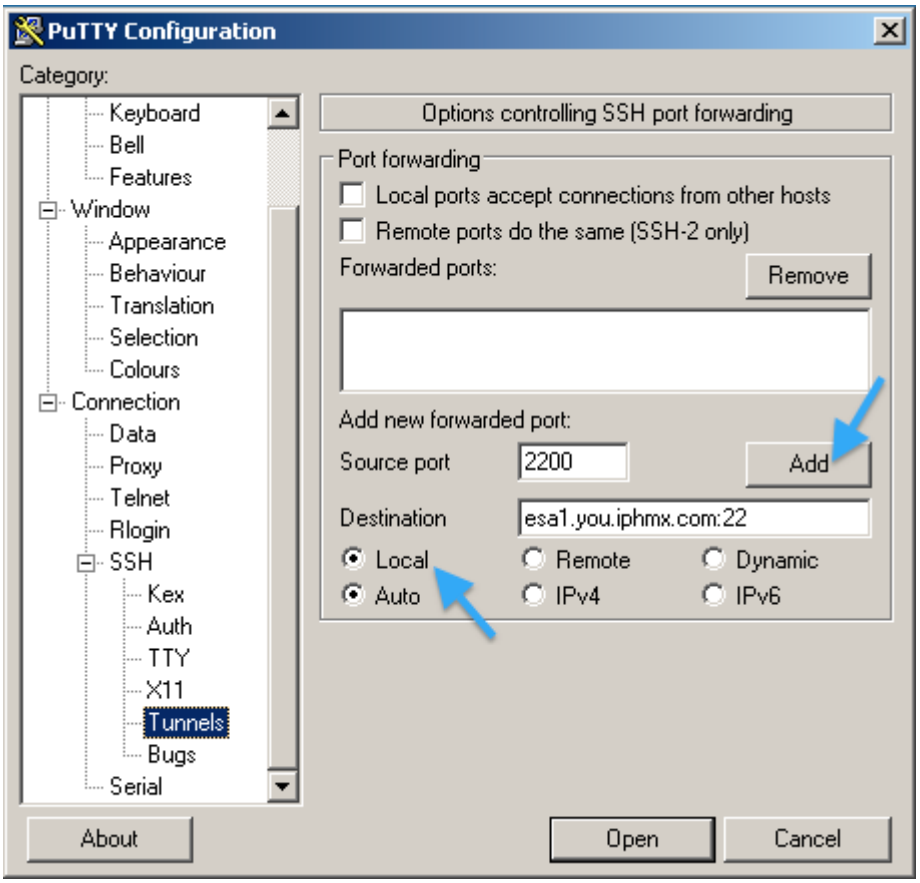


按一下Authand for Private key file for authentication，瀏覽並選擇您的私鑰。

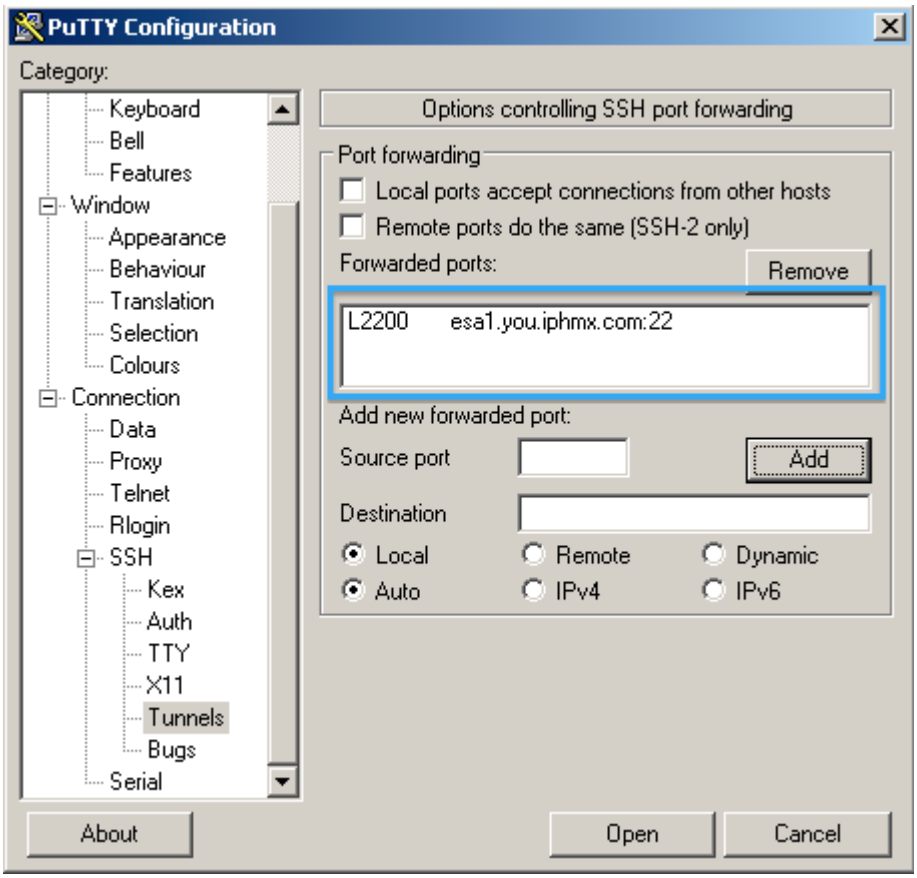


按一下「Tunnels」。
輸入來源連線埠;這是您選擇的任意埠（示例使用2200）。

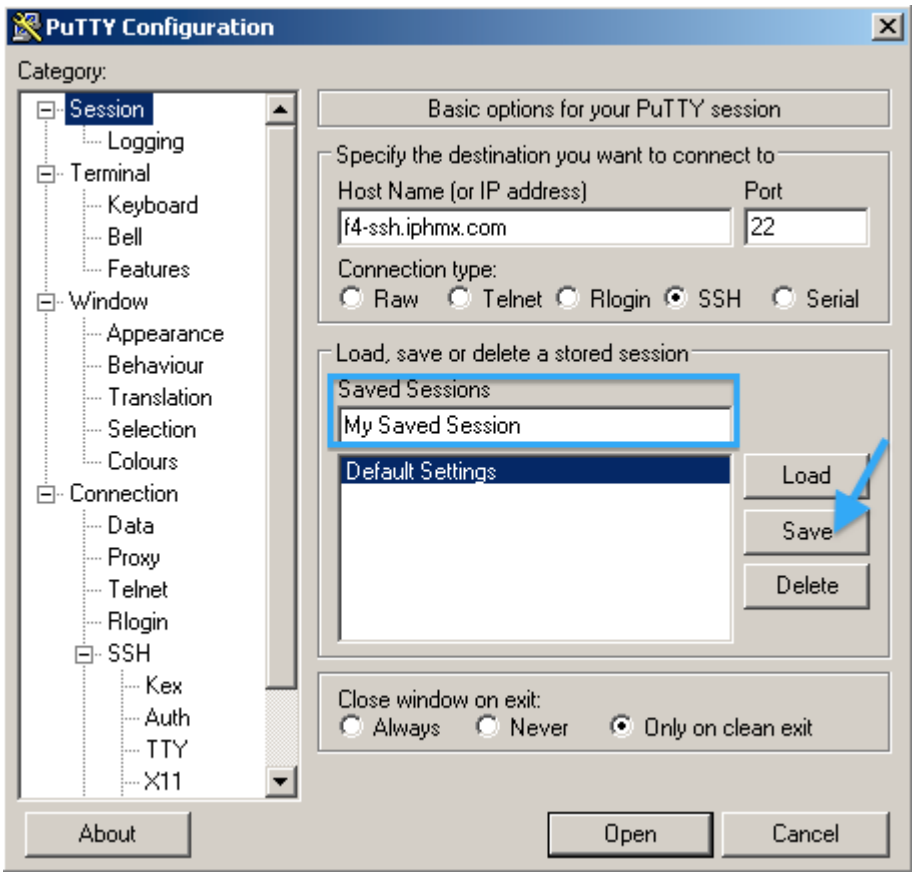
輸入aDestination;這是您的ESA或SMA + 22（指定SSH連線）。



按一下Add後，必須如下所示。

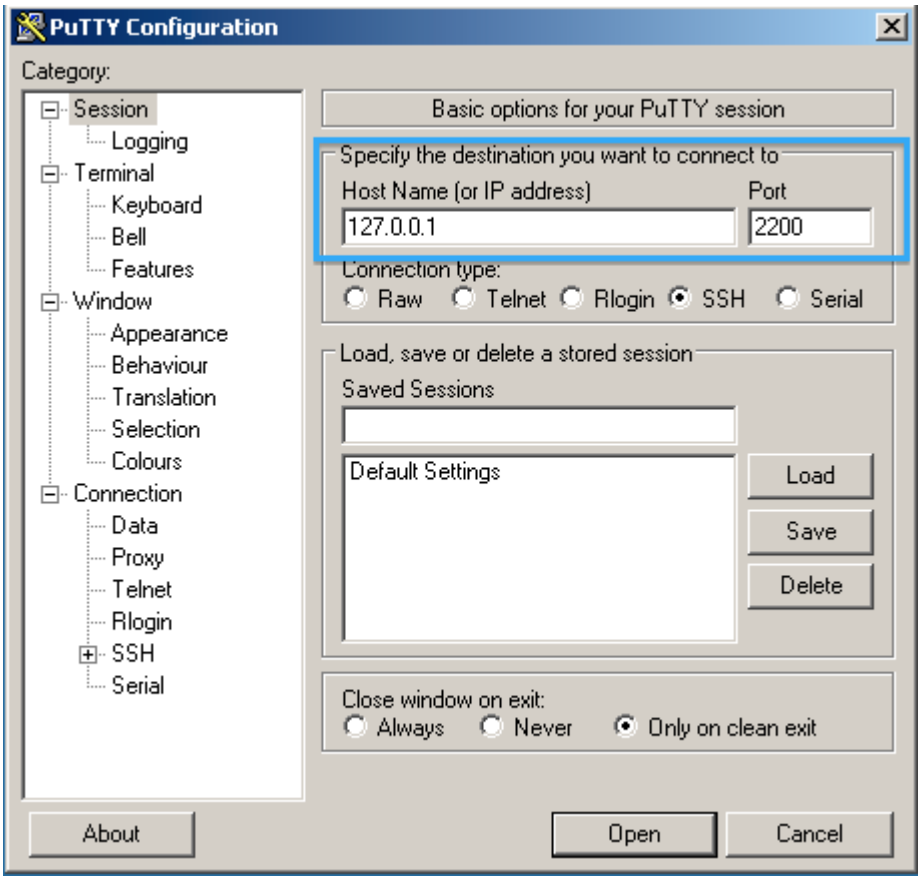


若要儲存會話以供將來使用，請按一下Session。
輸入「儲存的會話」的名稱，然後按一下儲存。



此時，可以按一下Open並啟動代理會話。
不會出現任何登入或命令提示符。現在，您需要開啟與ESA或SMA的第二個PuTTY會話。

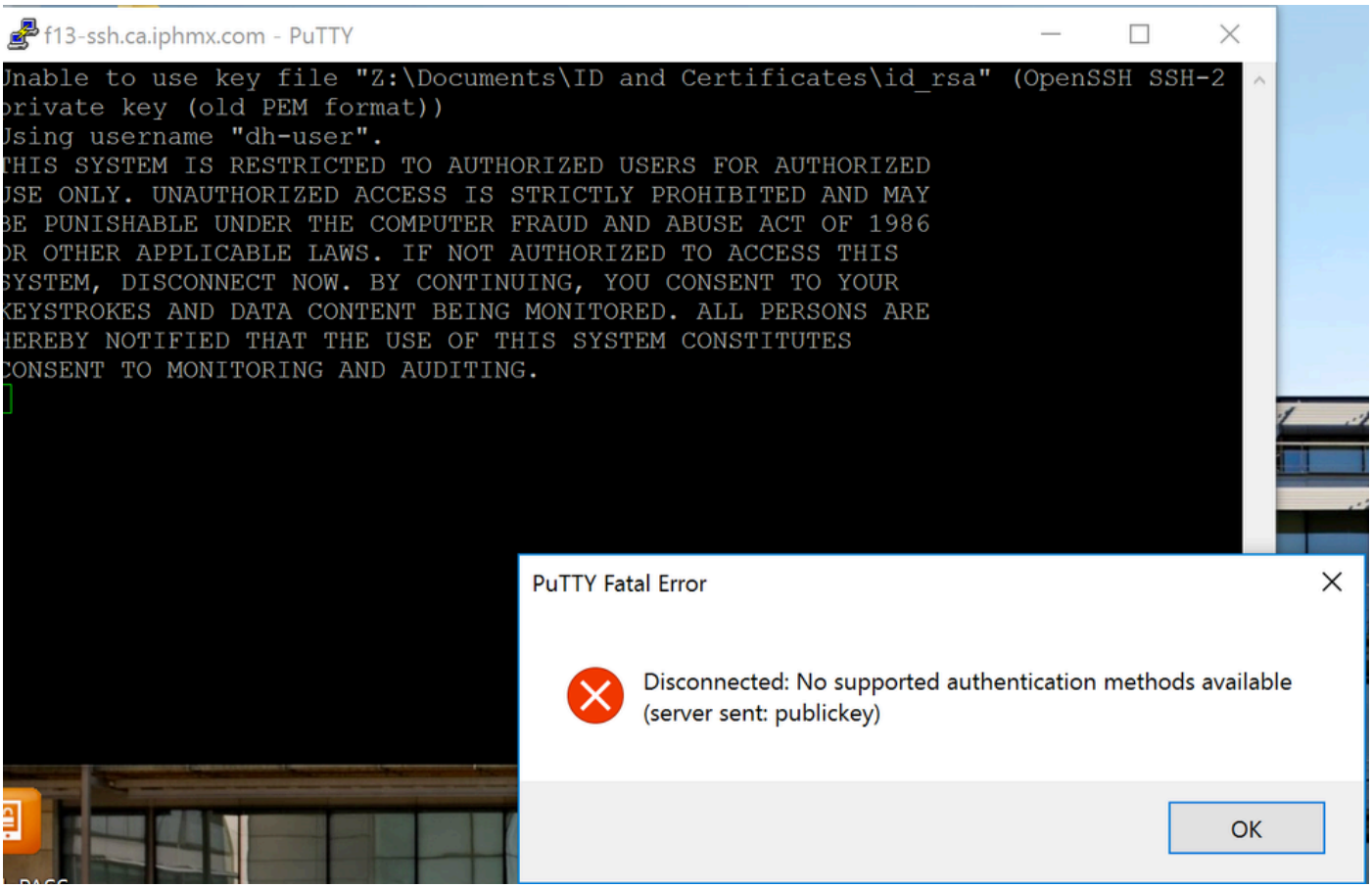
使用主機名127.0.0.1並在前面所示的隧道配置中使用源埠號。
在本示例中，使用2200。
按一下Open以連線到裝置。



當系統提示時，使用您的裝置使用者名稱和密碼，與使用UI訪問時相同。

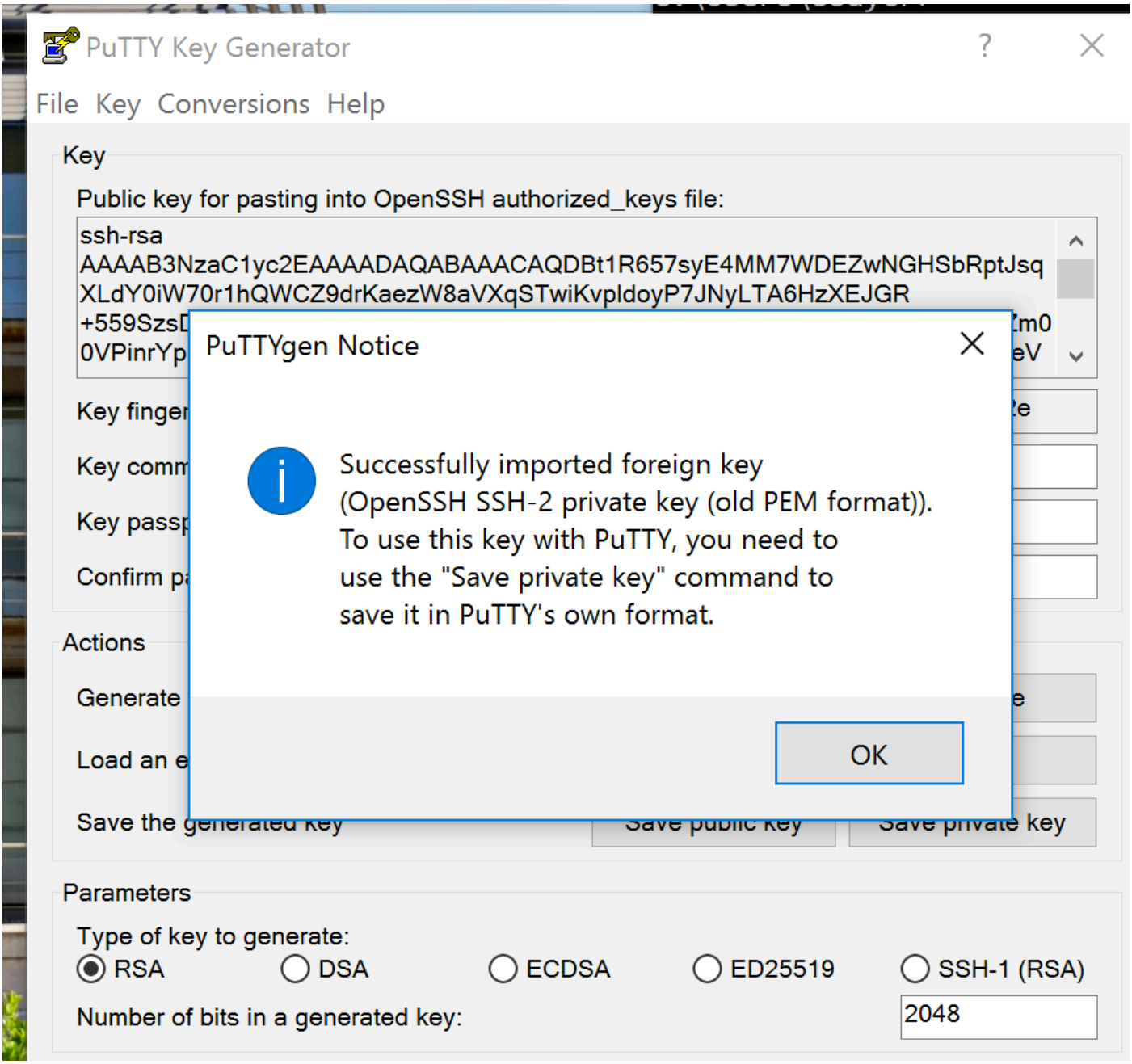
疑難排解

如果您的SSH金鑰對是使用OpenSSH（非PuTTy）生成的，則您將無法連線，並會出現「舊PEM格式」錯誤。



可以使用PuTTY金鑰生成器轉換私鑰。

- 開啟PuTy金鑰生成器。
- 按一下Loadin瀏覽和載入現有私鑰。
- 您需要按一下下拉選單並選擇所有檔案(.)，以便找到私鑰。
- 找到您的私鑰後，按一下Opening。
- Puttygen將提供類似此圖中的通知。



- 按一下儲存私鑰。
- 在PuTTY會話中，使用此轉換的私鑰並儲存會話。
- 嘗試使用轉換的私鑰重新連線。

確認您能夠通過命令列訪問裝置。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。