Requesting Cisco Cloud Email Security CLI Access

Contents

Introduction

This document describes how to request access to their Cloud Email Security (CES) CLI.

Background Information

Cisco CES customers are entitled to access the CLI of their ESA and SMA provided through an SSH Proxy using key authentication. CLI access to your hosted appliances must be limited to key individuals within your organization.

Linux and Mac Users

For Cisco CES customers:
Instructions for a shell script utilizing SSH in order to make CLI access via CES proxy.

Prerequisites

As a CES customer, you must have engaged CES On-Boarding/Ops, or Cisco TAC in order to have SSH Keys exchanged and placed:

1. Generate Private/Public RSA key(s).
2. Provide Cisco with yourPublicRSA key.
3. Wait for Cisco to save and notify you that your key(s) have been saved to your CES customer account.
4. Copy and modify the connect2ces.sh script.

How do I create Private/Public RSA keys(s)?

Cisco recommends using 'ssh-keygen' on the terminal/CLI for Unix/Linux/OS X. Use the **ssh-keygen -b 2048 -t rsa -f ~/.ssh/<NAME>** command.

Note: For more information, visit https://www.ssh.com/academy/ssh/keygen.
Ensure that you safeguard access to your RSA private keys at all times.
Do not send your private key to Cisco, only the public key (**.pub**).
When submitting your public key to Cisco, identify the email address/first name/last name that the key is for.

How do I open a Cisco Support Request to provide my public key?

Navigate to this link.

Ensure that you properly identify the SR as 'Cisco CES Customer SSH/CLI Setup', and so on.

Configuration

In order to get started, opencopy the script providedand use one of these proxy hosts for the **Host Name**.

Ensure you choose the correct proxy for your region (that is, If you are a US CES customer, in order to reach F4 data center and appliances, use the **f4-ssh.iphmx.com**. If you are an EU CES customer with an appliance in German DC, use **f17-ssh.eu.iphmx.com**.).

AP (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

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

EU (eu.iphmx.com)(German DC)
f17-ssh.eu.iphmx.com
f18-ssh.eu.iphmx.com

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

What if I want to connect to more than one Email Security Appliance (ESA) or Security Management Appliance (SMA)?

Copy and save a second copy of the **connect2ces.sh**, such as **connect2ces_2.sh**.

Note: You will want to edit the 'cloud_host' to be the additional appliance you wish to access. You will want to edit the 'local_port' to be something OTHER than 2222. If not, you will receive an error, "WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!"

How can I configure my ESA or SMA to log in without prompting for a password?

Read this guide.

What can this look like once I have the prerequisites completed?

joe.user@my_local > ~ ./connect2ces
[-] Connecting to your proxy server (f4-ssh.iphmx.com)...
[-] Proxy connection successful. Now connected to f4-ssh.iphmx.com.
[-] proxy running on PID: 31253
[-] Connecting to your CES appliance (esa1.rs1234-01.iphmx.com)...

Last login: Mon Apr 22 11:33:45 2019 from 10.123.123.123
AsyncOS 12.1.0 for Cisco C100V build 071

Welcome to the Cisco C100V Email Security Virtual Appliance

NOTE: This session will expire if left idle for 1440 minutes. Any uncommitted configuration changes will be lost. Commit the configuration changes as soon as they are made.

(Machine esa1.rs1234-01.iphmx.com)>
(Machine esa1.rs1234-01.iphmx.com)> exit

Connection to 127.0.0.1 closed.
[-] Closing proxy connection...
[-] Done.

connect2ces.sh

Note: Ensure you choose the correct proxy for your region (that is, If you are a US CES customer, in order to reach F4 data center and appliances, use the **f4-ssh.iphmx.com**. If you are an EU CES customer with an appliance in German DC, use **f17-ssh.eu.iphmx.com**.).

```
#!/bin/bash

#-- EDIT THE BELOW VALUES ----------------------
# The following values should already be established with CES:
# cloud_user="username"
```

```
# cloud_host="esaX.CUSTOMER.iphmx.com" or "smaX.CUSTOMER.iphmx.com"
## [ASSURE THAT YOU HAVE THE PROPER REGIONAL CES DATACENTER SET!]
# private_key="LOCAL_PATH_TO_SSH_PRIVATE_RSA_KEY"
# proxy_server="PROXY_SERVER" [SELECT ONLY ONE!]
#
## For 'proxy_server', these are SSH proxies:
##
## AP (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
##
## EU (c3s2.iphmx.com)
## f10-ssh.c3s2.iphmx.com
## f11-ssh.c3s2.iphmx.com
##
## EU (eu.iphmx.com)(German DC)
## f17-ssh.eu.iphmx.com
## f18-ssh.eu.iphmx.com
##
## US (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="PROXY_SERVER"

#-- LEAVE THESE VALUES AS-IS ----------
# 'proxy_user' should not change
# 'remote_port' stays 22 (SSH)
# 'local_port' can be set to different value, if needed

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

#-- DO NOT EDIT BELOW THIS LINE ----------

proxycmd="ssh -f -L $local_port:$cloud_host:$remote_port -i $private_key -N
$proxy_user@$proxy_server"

printf "[-] Connecting to your proxy server ($proxy_server)...\n"
$proxycmd >/dev/null 2>&1
if nc -z 127.0.0.1 $local_port >/dev/null 2>&1; then
printf "[-] Proxy connection successful. Now connected to $proxy_server.\n"
else
printf "[-] Proxy connection unsuccessful. Quitting...\n"
exit
fi
```

```
# Find proxy ssh process
proxypid=`ps -xo pid,command | grep "$cloud_host" | grep "$proxy_server" | head -n1 | sed "s/^[ \t]*//" | cut -d " " -f1`
printf "[-] proxy running on PID: $proxypid\n"

printf "[-] Connecting to your CES appliance ($cloud_host)...\n\n"
ssh -p $local_port $cloud_user@127.0.0.1

printf "[-] Closing proxy connection...\n"
kill $proxypid

printf "[-] Done.\n"

#-- Want to avoid having to type password each time?
#-- See: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118305-technote-esa-00.html
#-- Need access to more than one ESA or SMA? Copy the same script and rename to connect2ces_2.sh, or similar.
```

Original doc:https://github.com/robsherw/connect2ces.

Windows Users

Instructions for using PuTTY and utilizing SSH in order to make CLI access via CES proxy.

Prerequisites

As a CES customer, you must have engaged CES On-Boarding/Ops, or Cisco TAC to have SSH Keys exchanged and placed:

1. Generate Private/Public RSA key(s).
2. Provide Cisco with your **Public** RSA key.
3. Wait for Cisco in order to save and notify you that your key(s) have been saved to your CES customer account.
4. Setup PuTTY as detailed here in these instructions.

How do I create Private/Public RSA keys(s)?

Cisco recommends using PuTTYgen (https://www.puttygen.com/) for Windows.

For more information:https://www.ssh.com/ssh/putty/windows/puttygen.

Note: Ensure that you safeguard access to your RSA private keys at all times.
Do not send your private key to Cisco, only the public key (**.pub**).
When submitting your public key to Cisco, identify the email address/first name/last name that they key is for.

How do I open a Cisco Support Request to provide my public key?

Navigate to this link.

Ensure that you properly identify the SR as 'Cisco CES Customer SSH/CLI Setup', and so on.

How can I configure my ESA or SMA to log in without prompting for a password?

Read this guide.

PuTTy Configuration

In order to get started, open PuTTY and use one of these proxy hosts for the **Host Names**:

Ensure you choose the correct proxy for your region (that is, If you are a US CES customer, in order to reach F4 data center and appliances, use the **f4-ssh.iphmx.com**. If you are an EU CES customer with an appliance in German DC, use **f17-ssh.eu.iphmx.com**.).

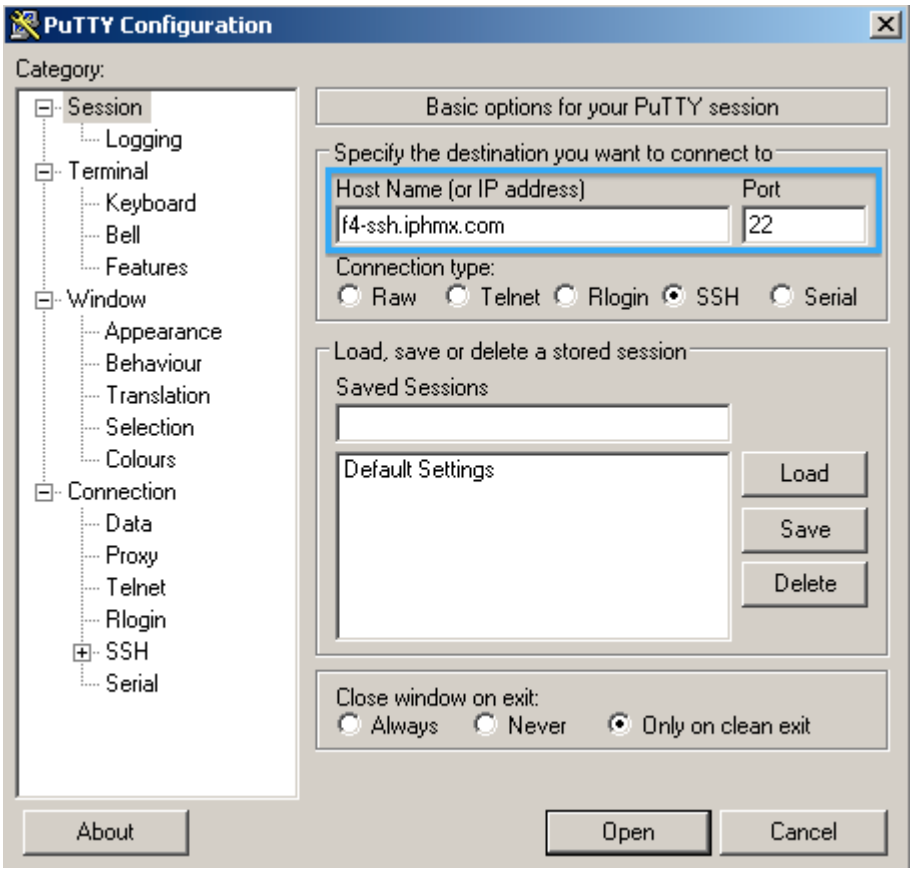
AP (ap.iphmx.com)
f15-ssh.ap.iphmx.com
f16-ssh.ap.iphmx.com

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

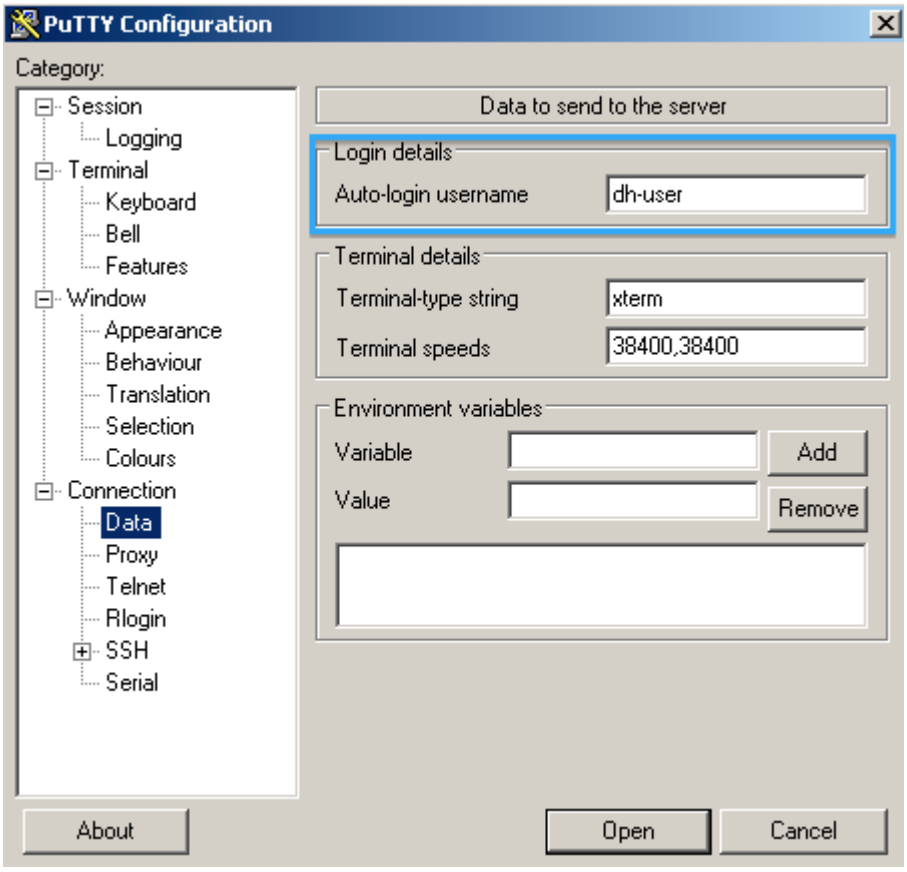
EU (c3s2.iphmx.com)
f10-ssh.c3s2.iphmx.com
f11-ssh.c3s2.iphmx.com

EU (eu.iphmx.com)(German DC)
f17-ssh.eu.iphmx.com
f18-ssh.eu.iphmx.com

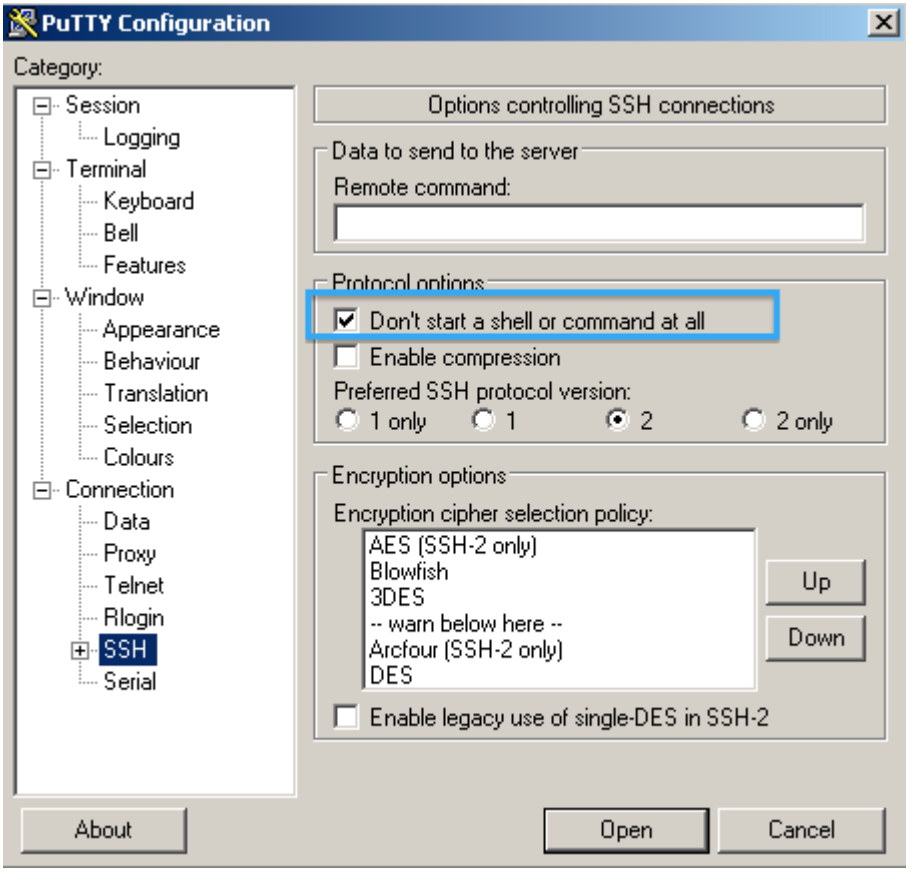
US (iphmx.com)
f4-ssh.iphmx.com
f5-ssh.iphmx.com



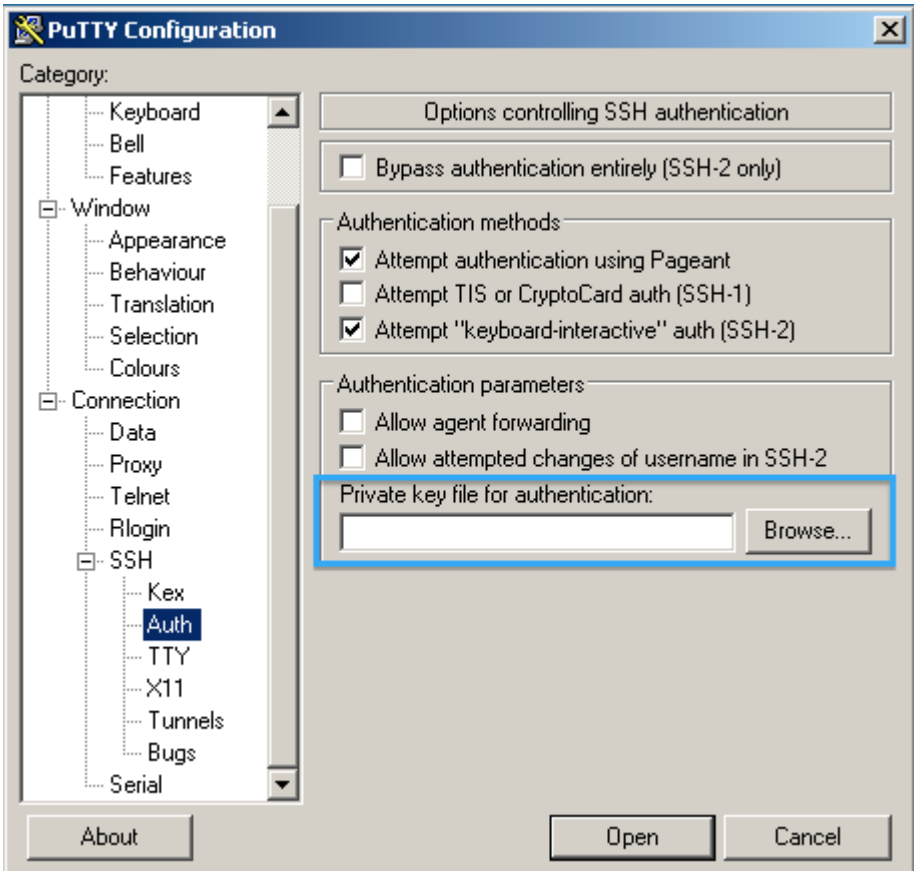
Click**Data**and for login details, use auto-login username and enter **dh-user**.



Choose **SSH** and check **Don't start a shell or command at all**.

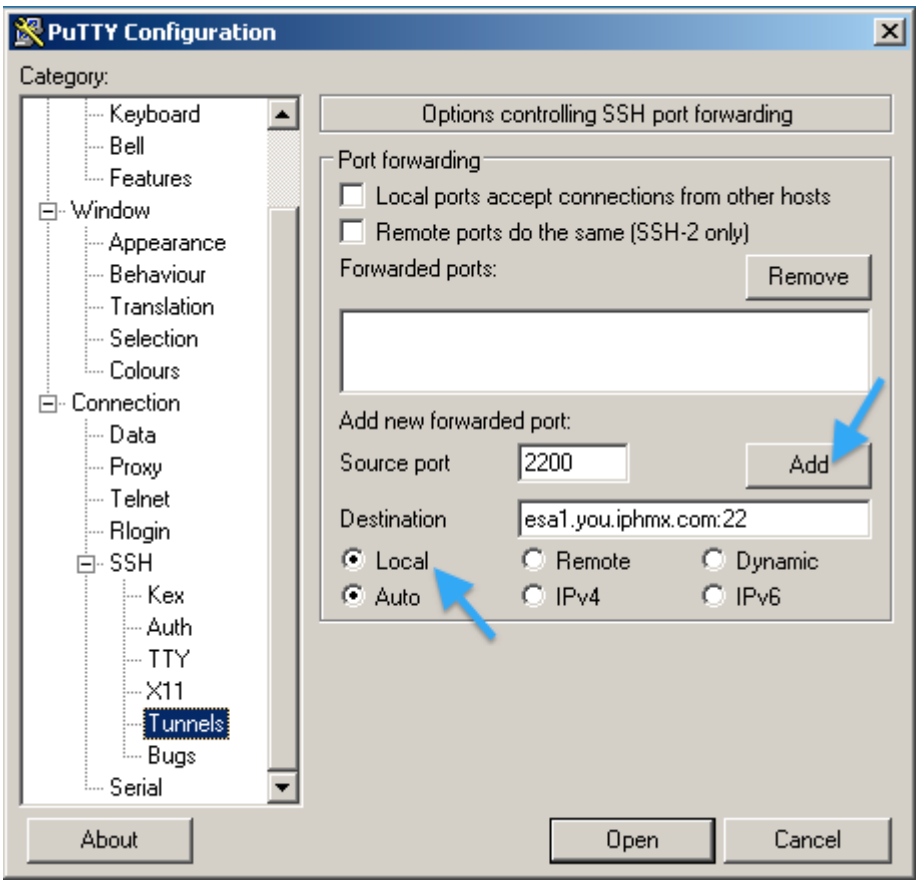


Click **Auth**and for **Private key file for authentication**, browse and choose your private key.

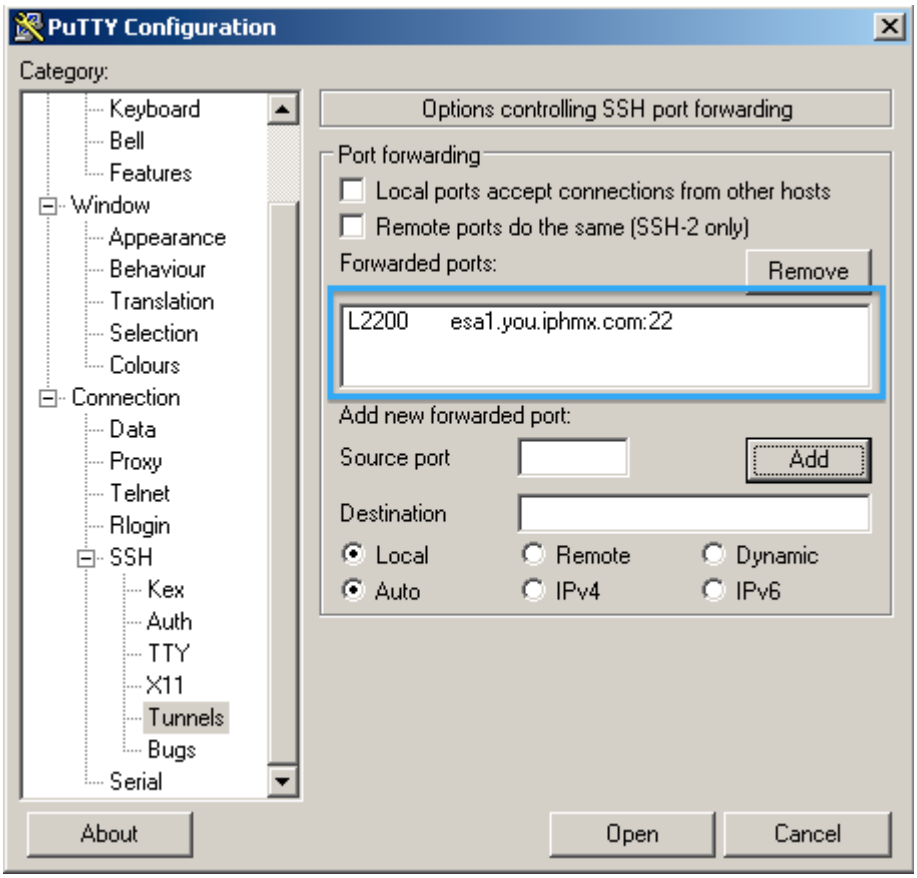


Click **Tunnels**.
Enter in a **Source port**; this is any arbitrary port of your choice (example uses 2200).

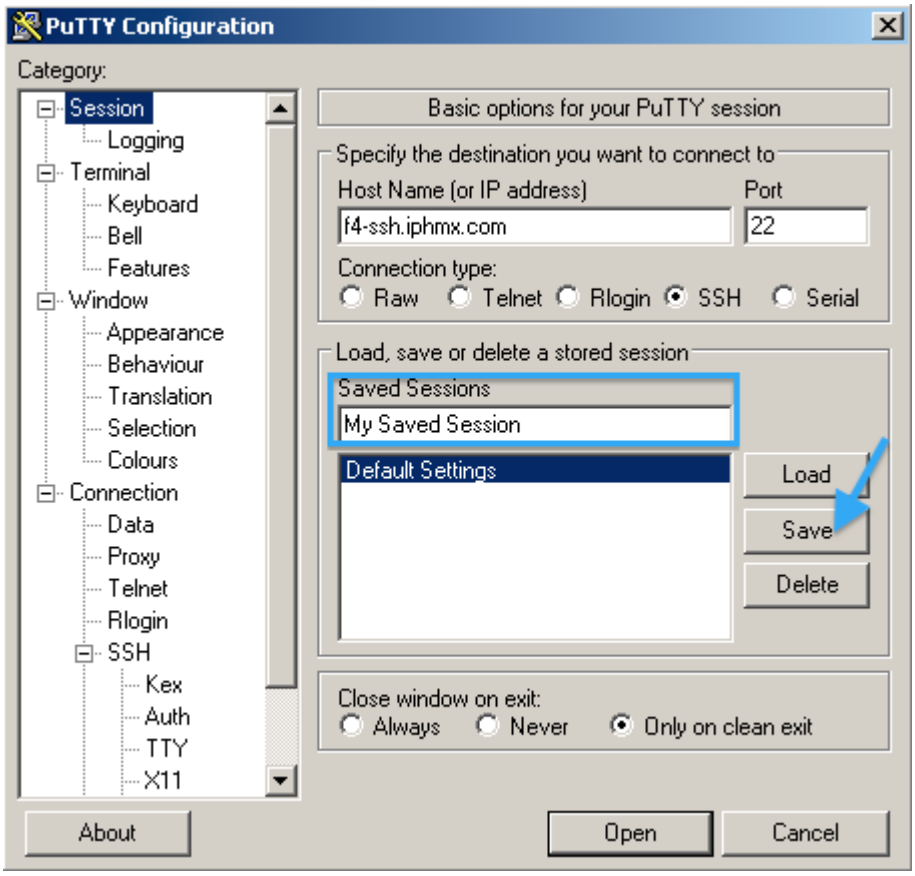
Enter in a**Destination**; this is your ESA or SMA + 22 (specifying SSH connection).



After you click **Add** it must look like this.

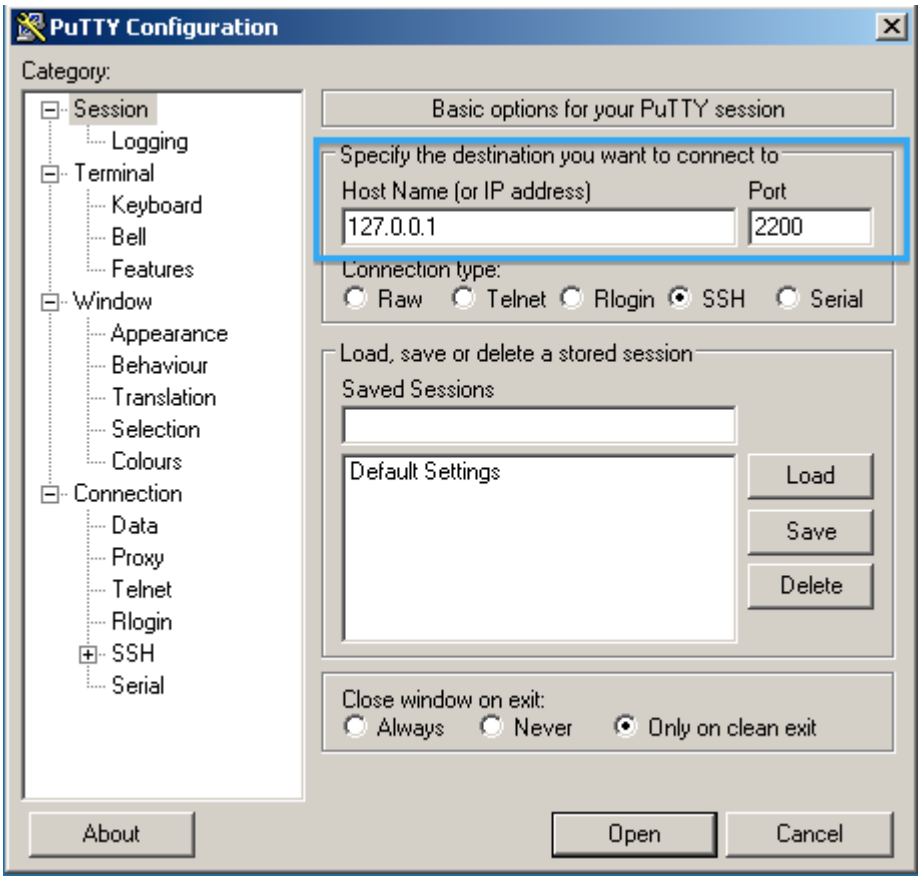


In order to save the session for future use, click **Session**.
Enter a name for your 'Saved Session', and click **Save**.



At this time you can click **Open** and initiate the proxy session.
There will not be any login or command prompt. You will now need to open a second PuTTY session to your ESA or SMA.

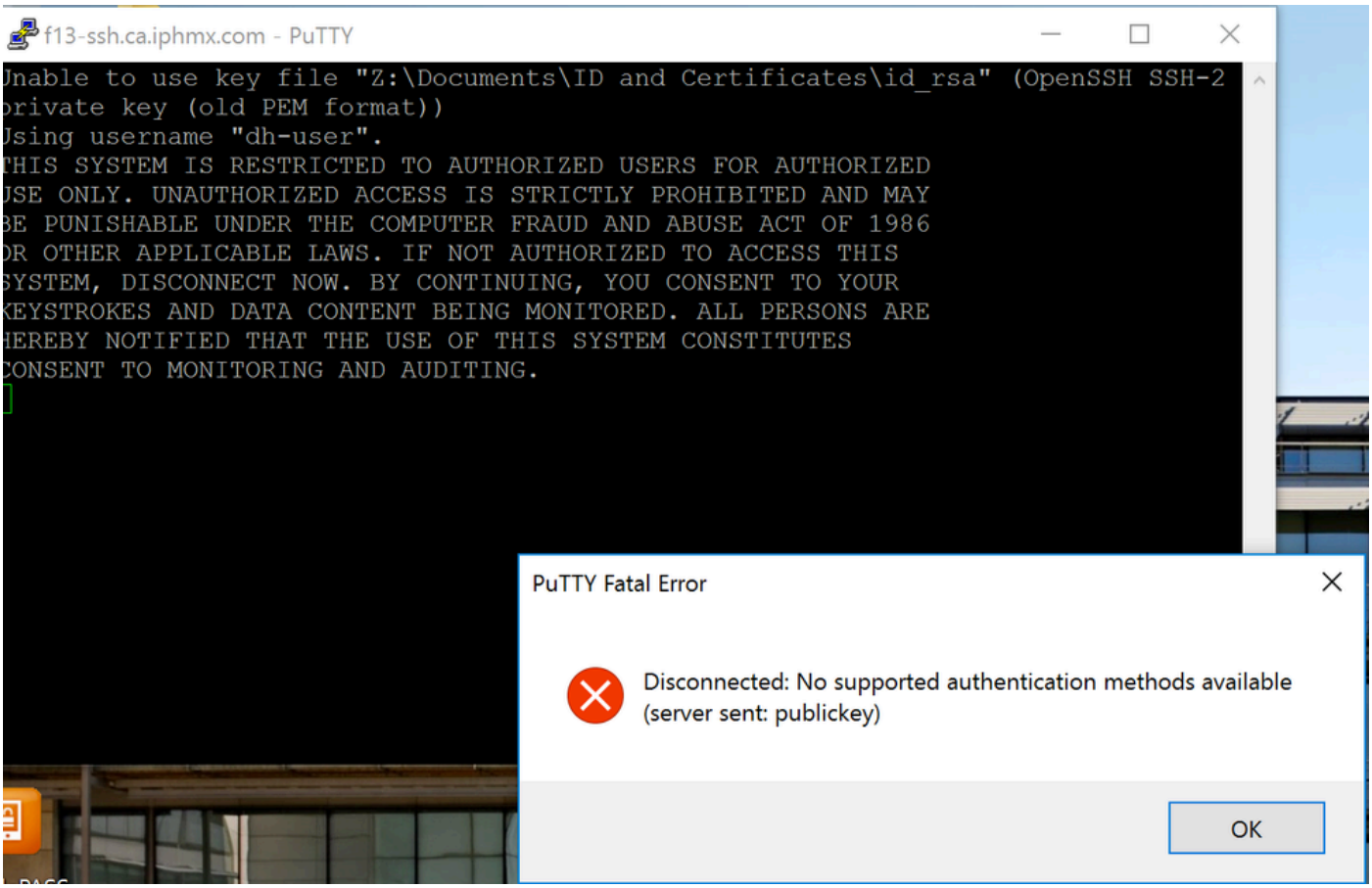
Use the hostname 127.0.0.1 and use the source port number in the tunnel configuration shown earlier. For this example, 2200 is used.
Click**Open**in order to connect to your appliance.



When prompted use your appliance username and password, the same as you will with UI access.

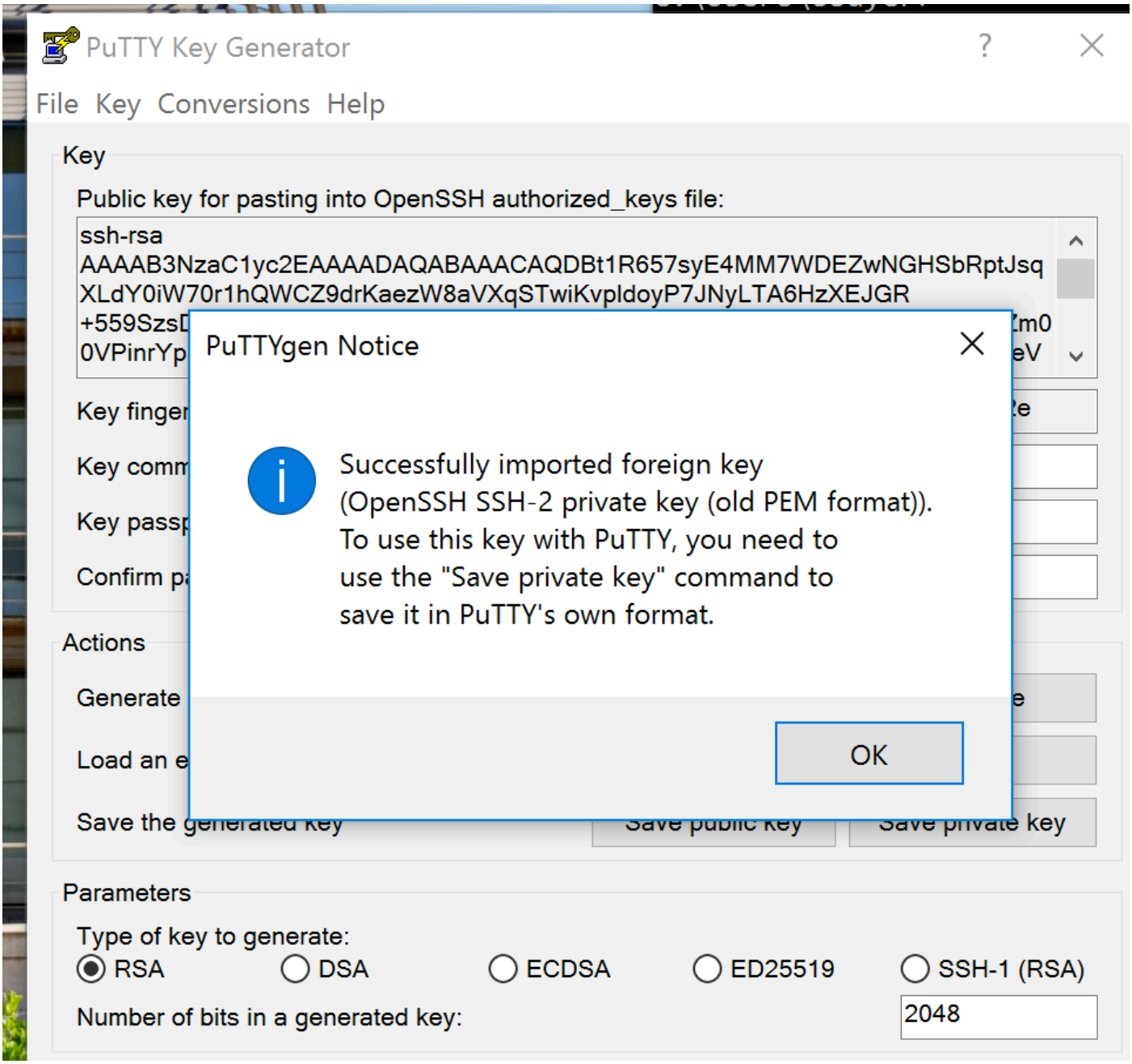
Troubleshooting

If your SSH key pair was generated using OpenSSH (non-PuTTy), you are unable to connect and will be presented with an "old PEM format" error.



The private key can be converted using[PuTTY Key Generator](#).

- Open PuTTy Key Generator.
- Click**Load**in order to browse and load your existing private key.
- You will need to click the drop-down and choose**All Files (.)**so you can locate the private key.
- Click**Open**once you have located your private key.
- Puttygen will provide a notice like in this image.



- Click**Save private key**.
- From your PuTTY session, use this converted private key and save the session.
- Attempt re-connecting with the converted private key.

Confirm that you are able to access your appliances via the command line.