# Solicitud de acceso a la CLI de Cisco Cloud Email Security

## Contenido


Introducción

Antecedentes

Usuarios de Linux y Mac

- Prerequisites
- ¿Cómo puedo crear claves RSA privadas/públicas?
- ¿Cómo puedo abrir una solicitud de asistencia de Cisco para proporcionar mi clave pública?
- Configuración
- ¿Qué sucede si deseo conectarme a más de un dispositivo de seguridad de correo electrónico (ESA) o dispositivo de administración de seguridad (SMA)?
- ¿Cómo puedo configurar mi ESA o SMA para iniciar sesión sin solicitar una contraseña?
- ¿Cómo puede ser una vez que se hayan completado los requisitos previos?

Usuarios de Windows

- Prerequisites
- ¿Cómo puedo crear claves RSA privadas/públicas?
- ¿Cómo puedo abrir una solicitud de asistencia de Cisco para proporcionar mi clave pública?
- ¿Cómo puedo configurar mi ESA o SMA para iniciar sesión sin solicitar una contraseña?
- Configuración de PuTy
- Resolución de problemas


## Introducción

Este documento describe cómo solicitar acceso a su CLI de Cloud Email Security (CES).

## Antecedentes

Los clientes de Cisco CES tienen derecho a acceder a la CLI de su ESA y SMA a través de un proxy SSH mediante la autenticación de claves. El acceso CLI a los dispositivos alojados debe limitarse a las personas clave de la organización.

## Usuarios de Linux y Mac

Para clientes de Cisco CES:
Instrucciones para un script de shell que utiliza SSH para hacer que el acceso CLI a través del proxy CES.

### Prerequisites

Como cliente de CES, debe haber contratado a CES On-Boarding/Ops, o a Cisco TAC para que se intercambien y coloquen las claves SSH:

1. Generar claves RSA privadas/públicas.
2. Proporcione a Cisco su clave RSA pública.
3. Espere a que Cisco guarde los cambios y le notifique que sus claves se han guardado en su cuenta de cliente de CES.
4. Copie y modifique el script connect2ces.sh.

## ¿Cómo puedo crear claves RSA privadas/públicas?

Cisco recomienda utilizar 'ssh-keygen' en el terminal/CLI para Unix/Linux/OS X. Utilice el comando ssh-keygen -b 2048 -t rsa -f ~/.ssh/<NAME>.

---

Nota: Para obtener más información, visite https://www.ssh.com/academy/ssh/keygen.
Asegúrese de proteger el acceso a las claves privadas RSA en todo momento.
No envíe su clave privada a Cisco, sólo la clave pública (.pub).
Cuando envíe su clave pública a Cisco, identifique la dirección de correo electrónico/nombre/apellidos para los que está destinada la clave.

---

## ¿Cómo puedo abrir una solicitud de asistencia de Cisco para proporcionar mi clave pública?

Vaya a este enlace.

Asegúrese de identificar correctamente el SR como "Configuración SSH/CLI del cliente de Cisco CES", y así sucesivamente.

## Configuración

Para comenzar, abra la secuencia de comandos proporcionada y utilice uno de estos hosts proxy para el nombre de host.

Asegúrese de elegir el proxy correcto para su región (es decir, si es cliente de CES de EE. UU.). Para acceder a los Data Centers y dispositivos F4, utilice f4-ssh.iphmx.com. Si es cliente de EU CES y tiene un dispositivo en el DC alemán, utilice 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

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

UE (eu.iphmx.com)(alemán DC)
f17-ssh.eu.iphmx.com
f18-ssh.eu.iphmx.com

EE. UU. (iphmx.com)
f4-ssh.iphmx.com
f5-ssh.iphmx.com

## ¿Qué sucede si deseo conectarme a más de un dispositivo de seguridad de correo electrónico (ESA) o dispositivo de administración de seguridad (SMA)?

Copie y guarde una segunda copia de connect2ces.sh, como connect2ces_2.sh.

---

Nota: Debe editar 'cloud_host' para que sea el dispositivo adicional al que desea acceder. Deseará editar el 'local_port' para que sea distinto de 2222. Si no es así, recibirá un error, "ADVERTENCIA: ¡LA IDENTIFICACIÓN DE HOST REMOTO HA CAMBIADO!"

---

## ¿Cómo puedo configurar mi ESA o SMA para iniciar sesión sin solicitar una contraseña?

Lea esta guía.

## ¿Cómo puede ser una vez que se hayan completado los requisitos previos?

joe.user@my_local > ~ ./connect2ces
[-] Conectando con el servidor proxy (f4-ssh.iphmx.com)...
[-] Conexión de proxy correcta. Ahora está conectado a f4-ssh.iphmx.com.
[-] proxy que se ejecuta en PID: 31253
[-] Conectando con su dispositivo CES (esa1.rs1234-01.iphmx.com)...

Última conexión: Lun Abr 22 11:33:45 2019 desde 10.123.123.123
AsyncOS 12.1.0 para Cisco C100V build 071

Bienvenido al dispositivo virtual Cisco C100V Email Security

NOTE: Esta sesión caducará si se deja inactiva durante 140 minutos. Se perderán todos los cambios de configuración no registrados. Realice los cambios de configuración tan pronto como se realicen.

(Máquina esa1.rs1234-01.iphmx.com)>

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

Conexión a 127.0.0.1 cerrada.
[-] Cerrando conexión proxy...
[-] Finalizado.

connect2ces.sh

---

Nota: Asegúrese de elegir el proxy correcto para su región (es decir, si es cliente de CES de EE. UU.). Para acceder a los Data Centers y dispositivos F4, utilice f4-ssh.iphmx.com. Si es cliente de EU CES y tiene un dispositivo en el DC alemán, utilice f17-ssh.eu.iphmx.com.)

---

```
#!/bin/bash

#-- EDITAR LOS SIGUIENTES VALORES ----------------------
# Los siguientes valores ya deben establecerse con CES:
# cloud_user="username"
# cloud_host="esaX.CUSTOMER.iphmx.com" o "smaX.CUSTOMER.iphmx.com"
## [ASEGÚRESE DE QUE DISPONE DEL CONJUNTO DE DATA CENTERS CES REGIONALES ADECUADOS.]
# private_key="RUTA_LOCAL_A_SSH_PRIVATE_RSA_KEY"
# proxy_server="PROXY_SERVER" [SELECT ONLY ONE!]
#
## Para 'proxy_server', estos son proxies SSH:
##
## 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
##
## UE (c3s2.iphmx.com)
## f10-ssh.c3s2.iphmx.com
## f11-ssh.c3s2.iphmx.com
##
## UE (eu.iphmx.com)(DC alemán)
## f17-ssh.eu.iphmx.com
## f18-ssh.eu.iphmx.com
##
## EE. UU. (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="SERVIDOR_PROXY"

#-- DEJE ESTOS VALORES TAL CUAL --------------------
# 'proxy_user' no debe cambiar
# 'remote_port' permanece 22 (SSH)
# 'local_port' se puede establecer en un valor diferente, si es necesario

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

#-- NO EDITAR POR DEBAJO DE ESTA LÍNEA -----------------

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

printf "[-] Conectando con su servidor proxy ($proxy_server)...\n"
$proxycmd >/dev/null 2>&1
if nc -z 127.0.0.1 $local_port >/dev/null 2>&1; luego
printf "[-] Conexión proxy exitosa. Ahora conectado a $proxy_server.\n"
sino
printf "[-] Conexión proxy fallida. Dejando...\n"
salir
fi

# Buscar proceso ssh de proxy
proxypid=`ps -xo pid,command | grep "$cloud_host" | grep "$proxy_server" | head -n1 | sed "s/^[
\t]*//" | cut -d " " -f1`
printf "[-] proxy que se ejecuta en PID: $proxypid\n"

printf "[-] Conectando con su dispositivo CES ($cloud_host)...\n\n"
ssh -p $local_port $cloud_user@127.0.0.1

printf "[-] Cerrando conexión proxy...\n"
kill $proxypid

printf "[-] Finalizado.\n"

#-- ¿Quieres evitar tener que escribir la contraseña cada vez?
#-- Vea: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118305-
technote-esa-00.html
#-- ¿Necesita acceso a más de un ESA o SMA? Copie el mismo script y cambie el nombre a
connect2ces_2.sh o similar.
```

Documento original:https://github.com/robsherw/connect2ces.

# Usuarios de Windows

Instrucciones para utilizar PuTTY y SSH con el fin de hacer que el acceso CLI a través de proxy CES.

## Prerequisites

Como cliente de CES, debe haber contratado a CES On-Boarding/Ops, o a Cisco TAC para que intercambien y coloquen las claves SSH:

1. Generar claves RSA privadas/públicas.
2. Proporcione a Cisco su clave RSA pública.
3. Espere a que Cisco guarde y le notifique que sus claves se han guardado en su cuenta de cliente de CES.
4. Configure PuTTY como se detalla aquí en estas instrucciones.

## ¿Cómo puedo crear claves RSA privadas/públicas?

Cisco recomienda utilizar PuTTYgen (https://www.puttygen.com/) para Windows.

Para obtener más información:https://www.ssh.com/ssh/putty/windows/puttygen.

---

Nota: Asegúrese de proteger el acceso a las claves privadas RSA en todo momento.
No envíe su clave privada a Cisco, sólo la clave pública (.pub).
Cuando envíe su clave pública a Cisco, identifique la dirección de correo electrónico/nombre/apellidos para los que está destinada la clave.

---

## ¿Cómo puedo abrir una solicitud de asistencia de Cisco para proporcionar mi clave pública?

Vaya a este enlace.

Asegúrese de identificar correctamente el SR como "Configuración SSH/CLI del cliente de Cisco CES", y así sucesivamente.

## ¿Cómo puedo configurar mi ESA o SMA para iniciar sesión sin solicitar una contraseña?

Lea esta guía.

## Configuración de PuTy

Para comenzar, abra PuTTY y utilice uno de estos hosts proxy para los Nombres de Host:

Asegúrese de elegir el proxy correcto para su región (es decir, si es cliente de CES de EE. UU.). Para acceder a los Data Centers y dispositivos F4, utilice f4-ssh.iphmx.com. Si es cliente de EU CES y tiene un dispositivo en el DC alemán, utilice f17-ssh.eu.iphmx.com.)

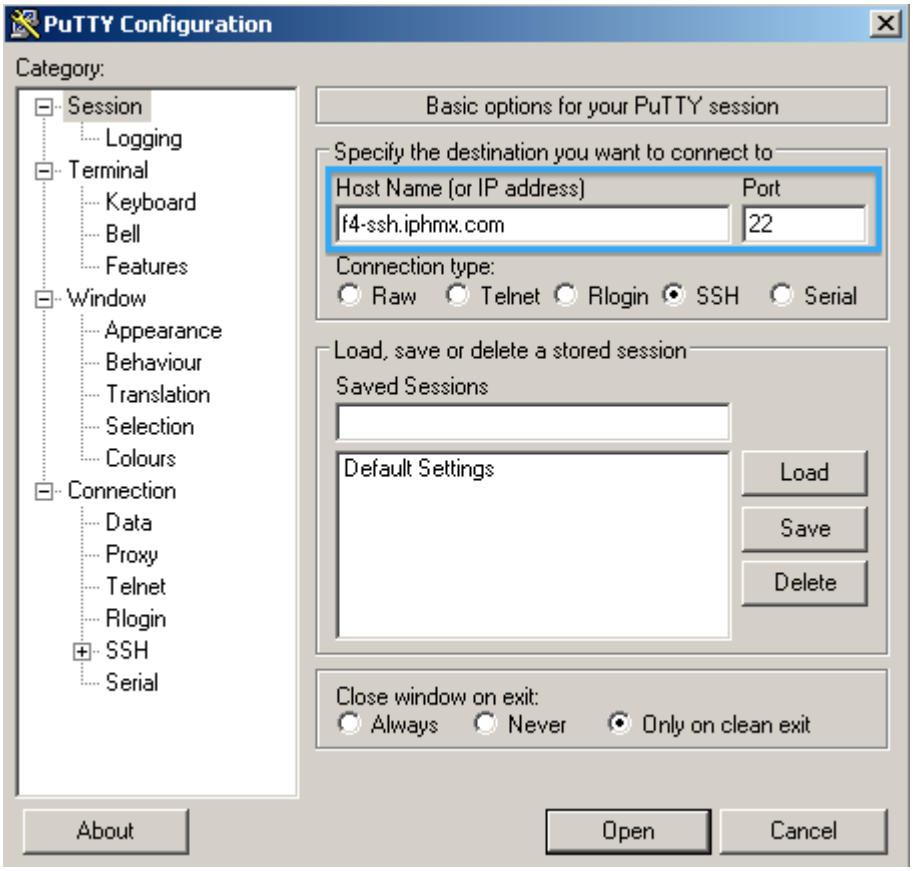
AP (ap.iphmx.com)
f15-ssh.ap.iphmx.com
f16-ssh.ap.iphmx.com

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

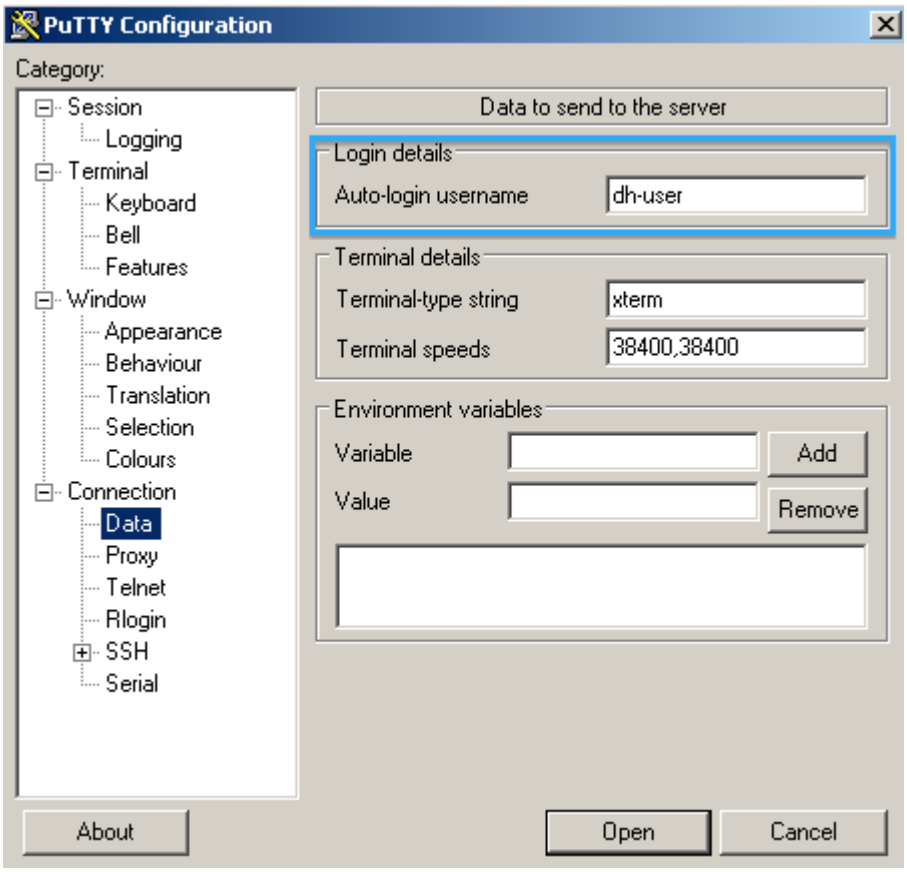
UE (c3s2.iphmx.com)
f10-ssh.c3s2.iphmx.com
f11-ssh.c3s2.iphmx.com

UE (eu.iphmx.com)(alemán DC)
f17-ssh.eu.iphmx.com
f18-ssh.eu.iphmx.com

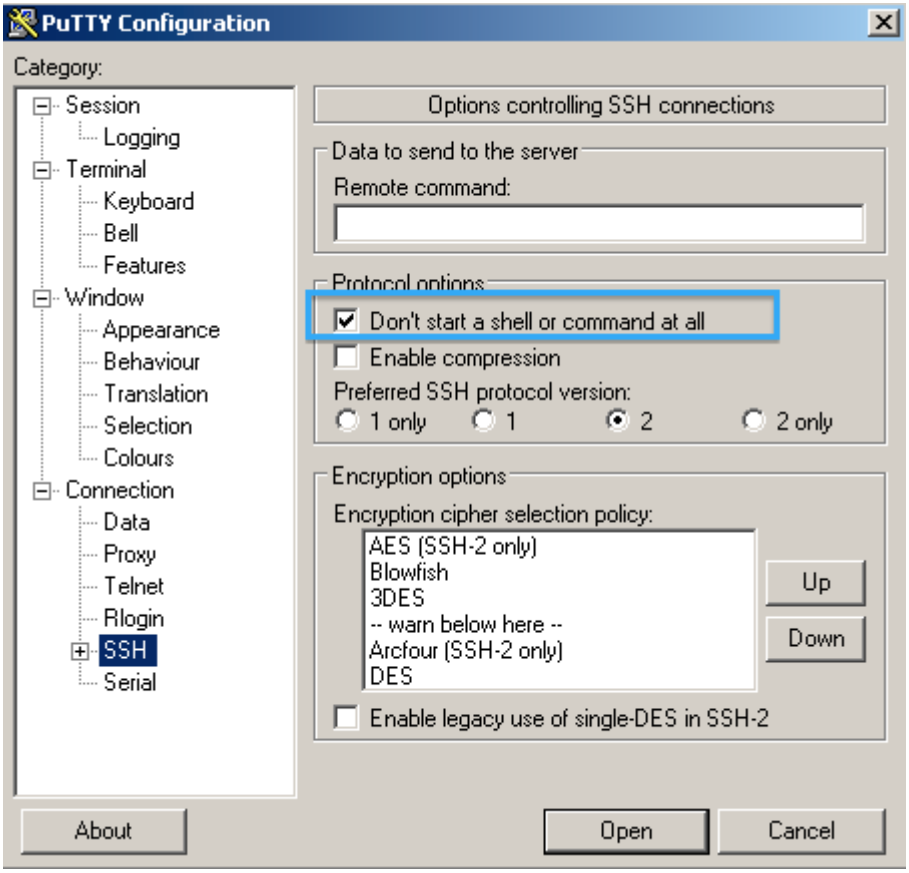
EE. UU. (iphmx.com)
f4-ssh.iphmx.com
f5-ssh.iphmx.com



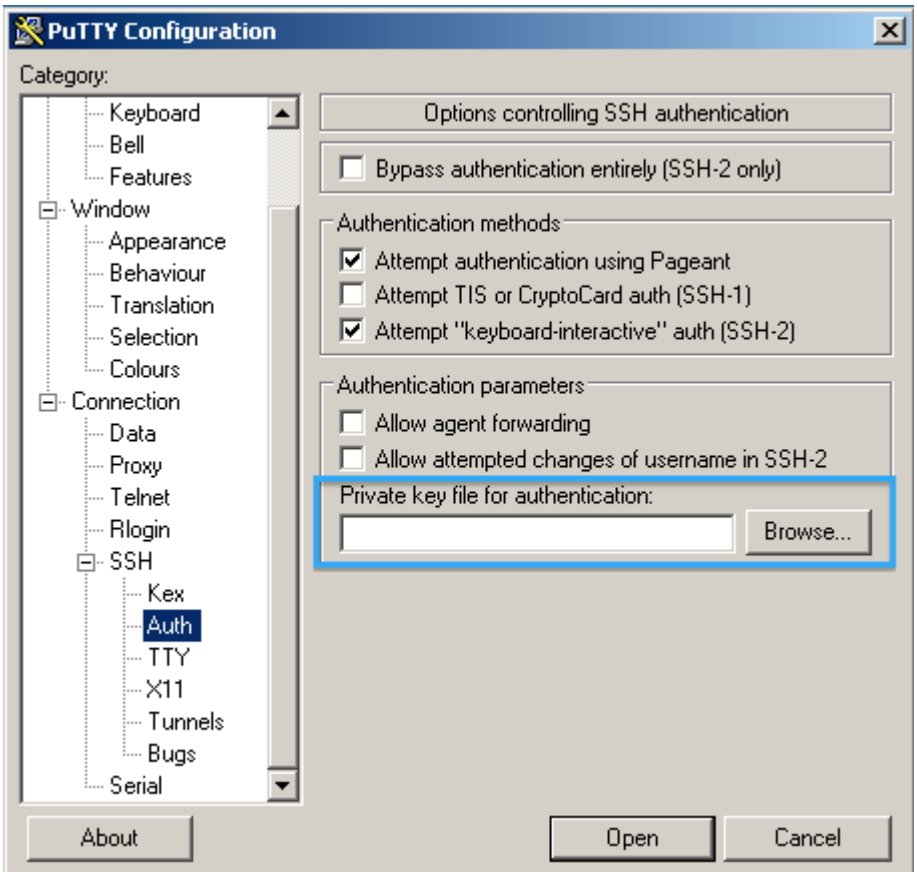

ClickData y para los detalles de inicio de sesión, utilice el nombre de usuario de inicio de sesión automático e ingrese dh-user.



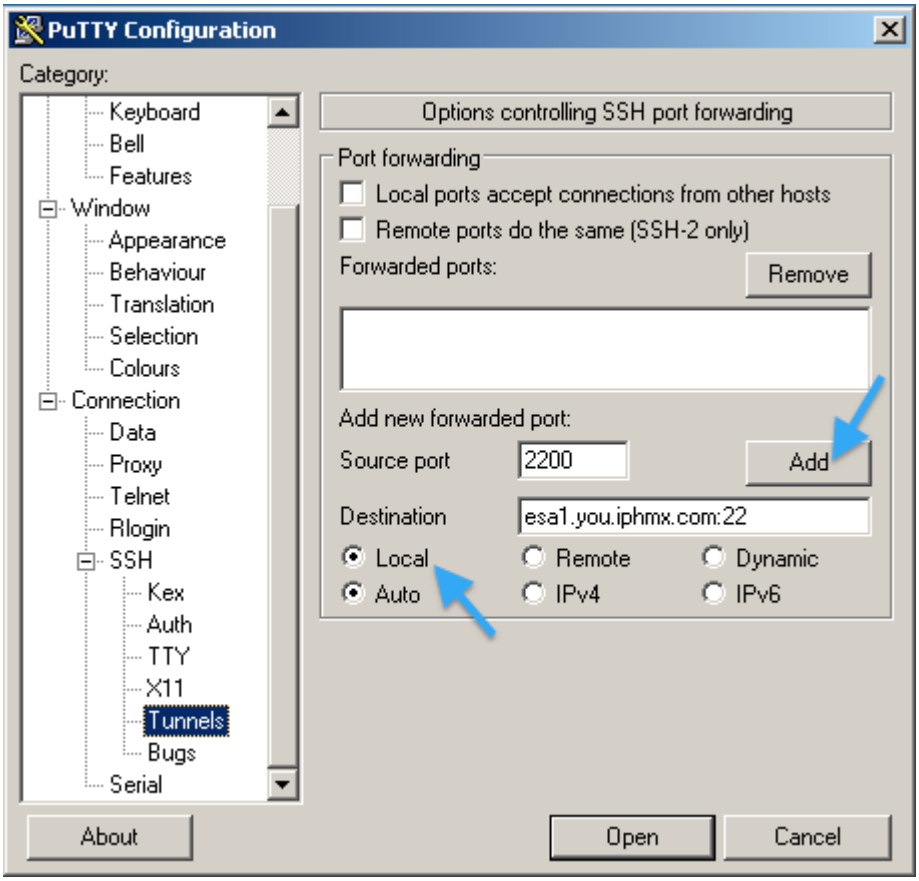

Elija SSH y marque No inicie un shell o comando en absoluto.



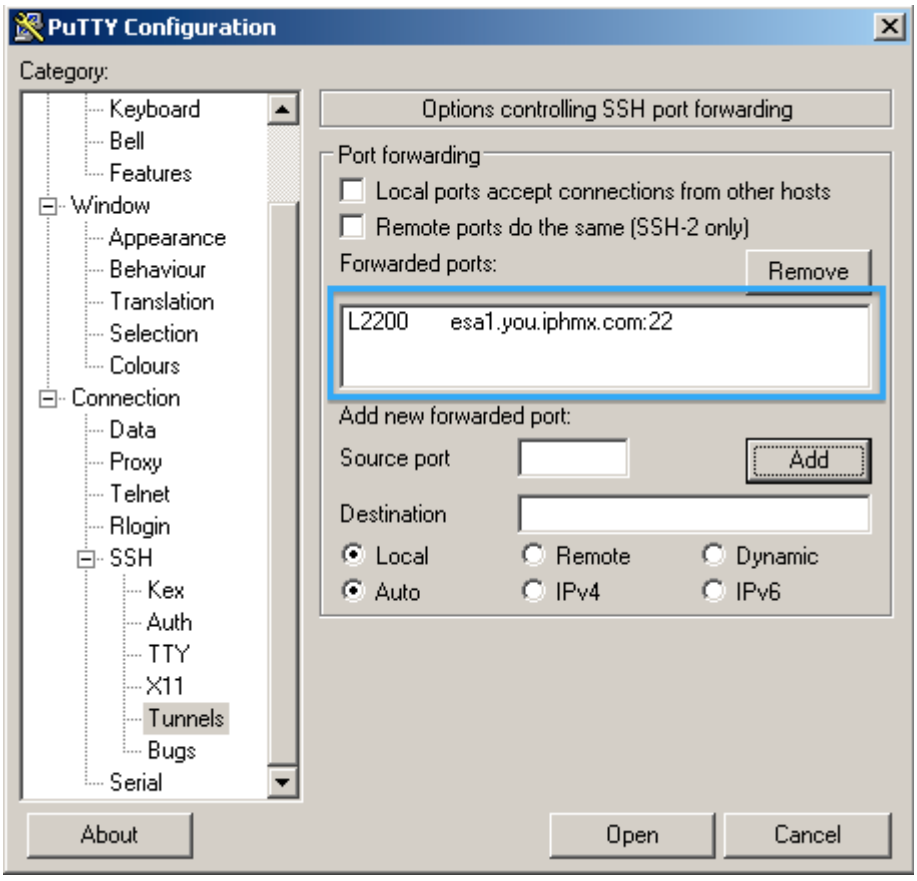

Haga clic en Authand for Private key file for authentication, explore y elija su clave privada.



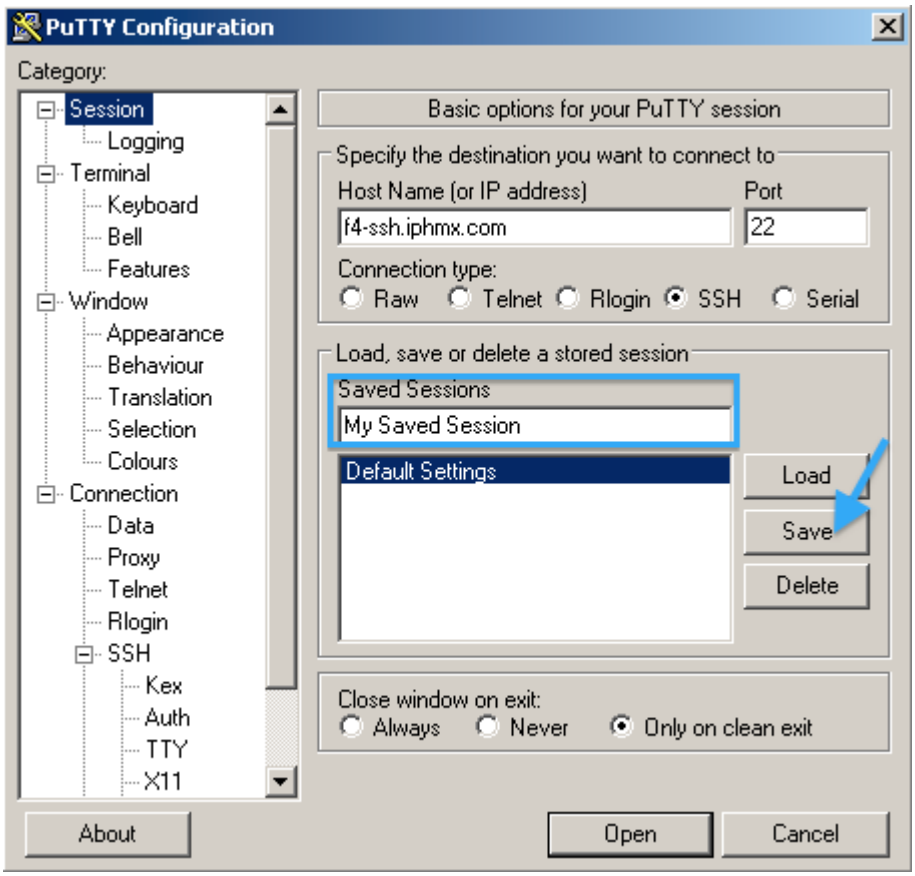

Haga clic en Túneles.
Ingrese en un puerto de origen; este es cualquier puerto arbitrario de su elección (ejemplo utiliza 2200).
Ingrese en unDestino; se trata de su ESA o SMA + 22 (especificando la conexión SSH).



Después de hacer clic en Add, debe tener este aspecto.

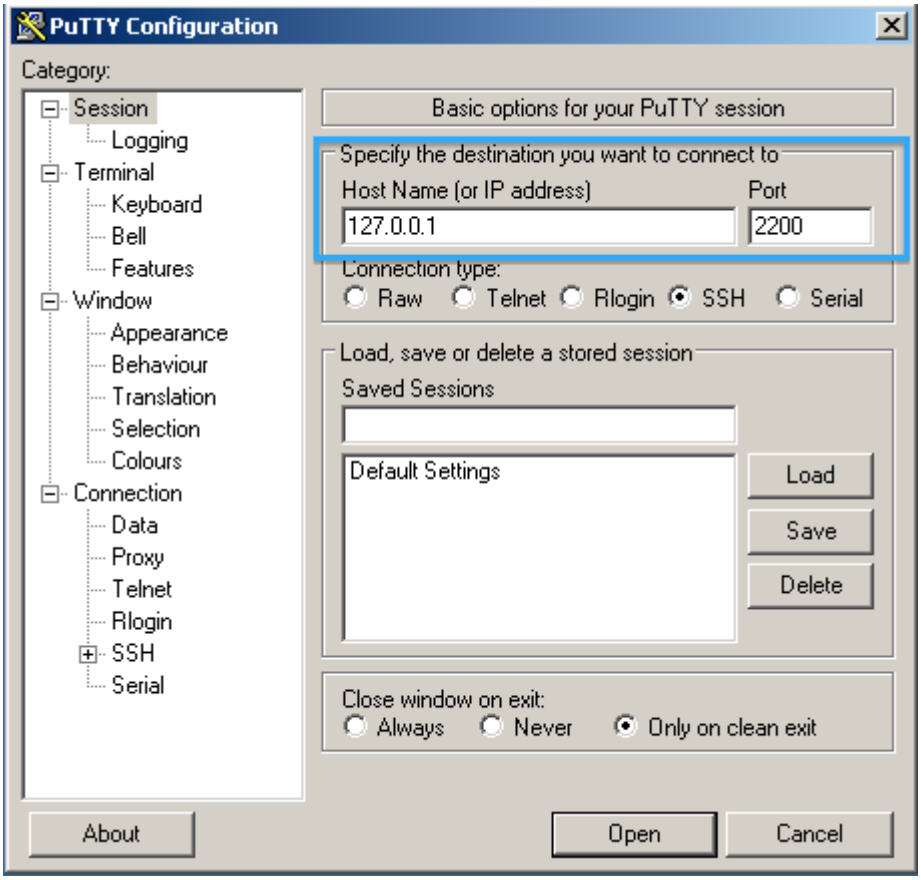



Para guardar la sesión para un uso futuro, haga clic en Session.
Introduzca un nombre para la sesión guardada y haga clic en Guardar.



En este momento, puede hacer clic en Abrir e iniciar la sesión de proxy.
No habrá ningún inicio de sesión ni símbolo del sistema. Ahora tendrá que abrir una segunda sesión de PuTTY a su ESA o SMA.

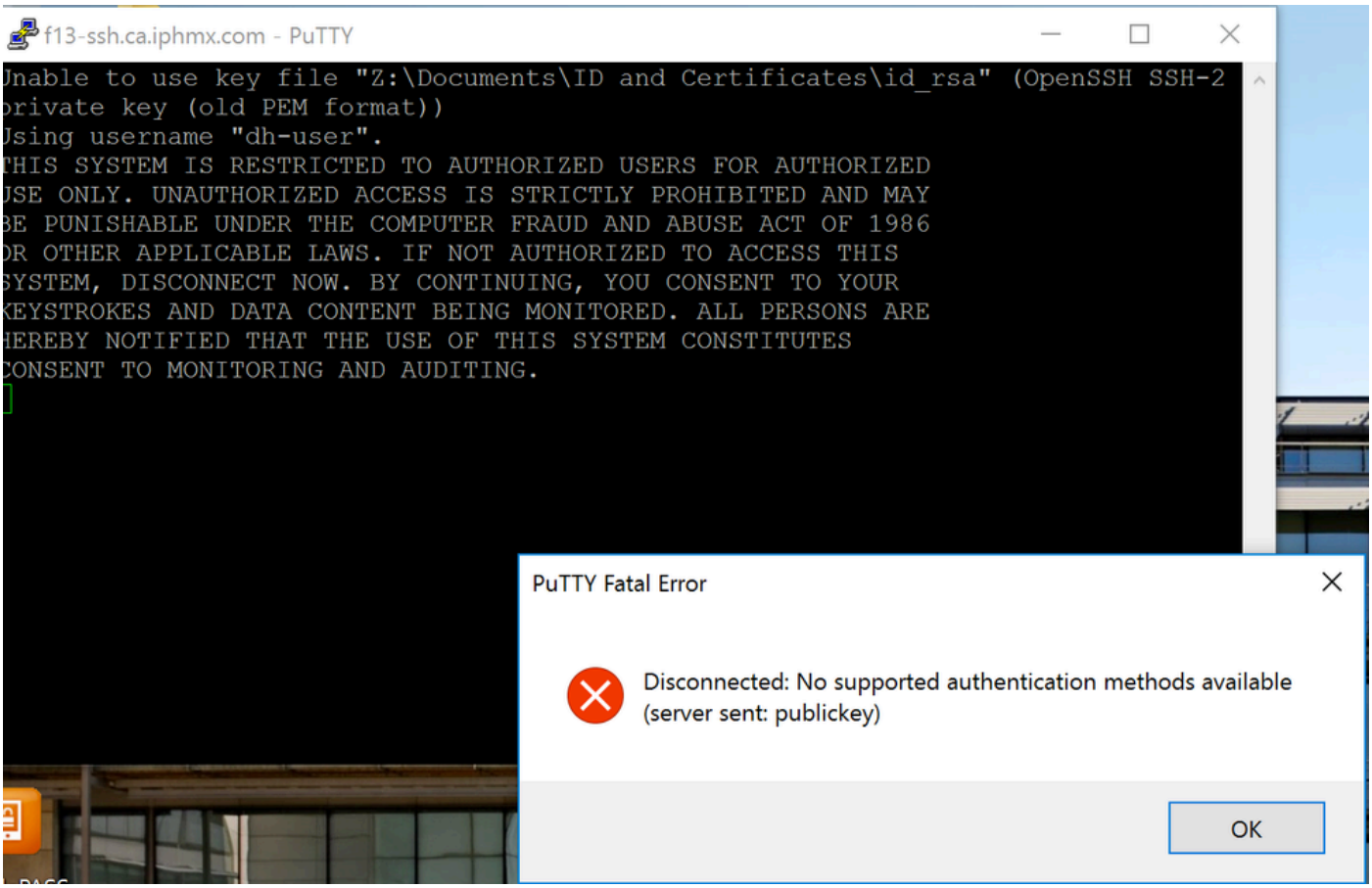
Utilice el nombre de host 127.0.0.1 y el número de puerto de origen en la configuración de túnel que se muestra anteriormente.
Para este ejemplo se utiliza 2200.
Haga clic en Abrir para conectarse a su dispositivo.




Cuando se le solicite, utilice el nombre de usuario y la contraseña del dispositivo, tal y como lo hará con el acceso a la interfaz de usuario.

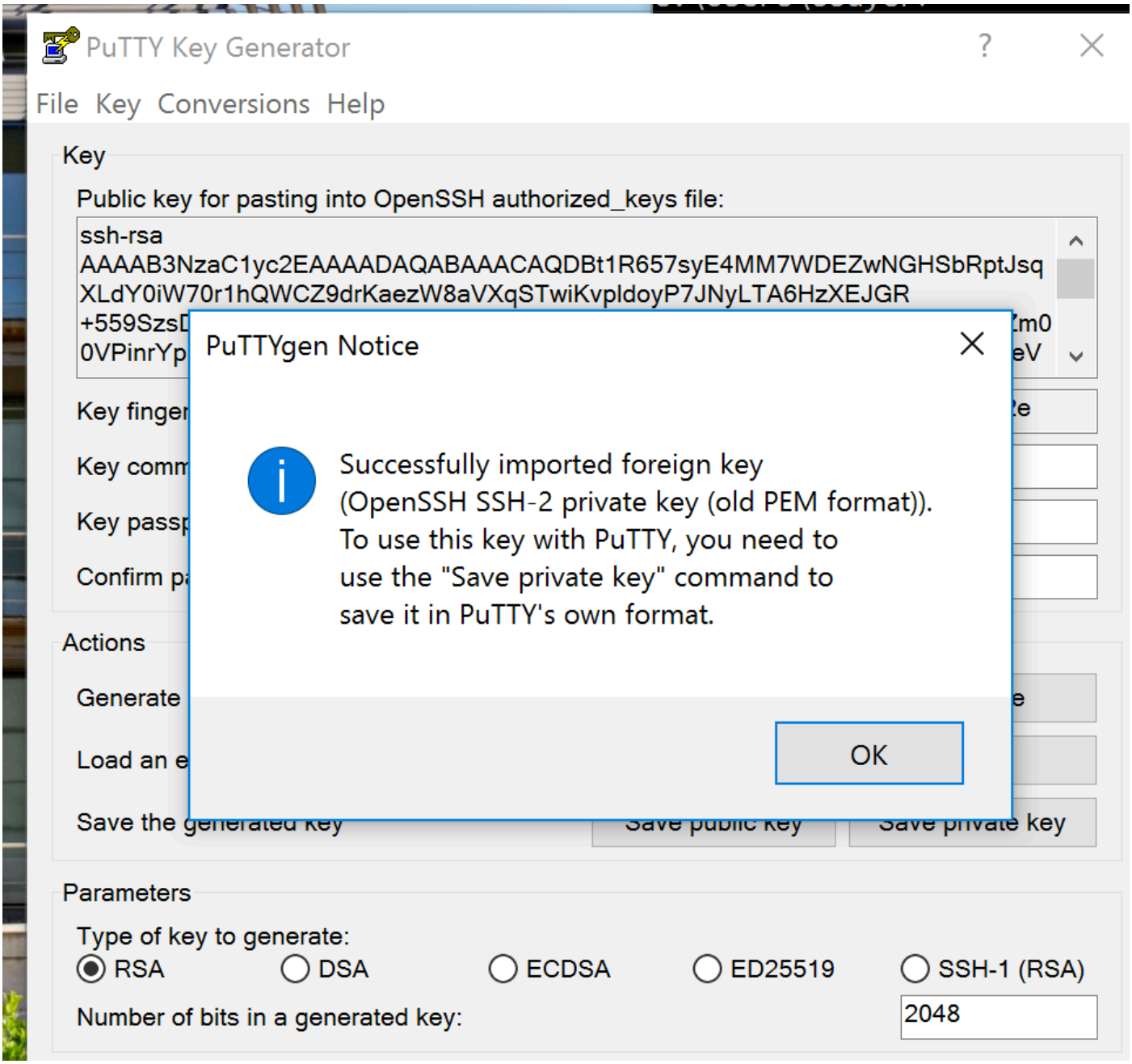
## Resolución de problemas

Si su par de claves SSH se generó utilizando OpenSSH (no PuTTy), no podrá conectarse y se le mostrará un error de "formato PEM antiguo".




La clave privada se puede convertir mediante el generador de claves PuTTY.

- Abra el generador de claves PuTy.
- Haga clic en Load para examinar y cargar su clave privada existente.
- Deberá hacer clic en la lista desplegable y elegirTodos los archivos (.)para poder localizar la clave privada.
- Haga clic enAbrir una vez que haya localizado la clave privada.
- Puttygen proporcionará un aviso como en esta imagen.




- Haga clic en Guardar clave privada.
- Desde la sesión PuTTY, utilice esta clave privada convertida y guarde la sesión.
- Intente volver a conectarse con la clave privada convertida.

Confirme que puede acceder a sus dispositivos a través de la línea de comandos.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).