Configuración de la autenticación de clave privada con ISE

Contenido

Introducción

Este documento describe cómo crear una clave de Secure Shell (SSH) privada para la autenticación en la CLI en Identity Secure Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Repositorio en ISE.
- Autenticación de certificados.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- parche 3 de ISE 3.3
- Windows 10
- MacOS X

- SSH Client Putty

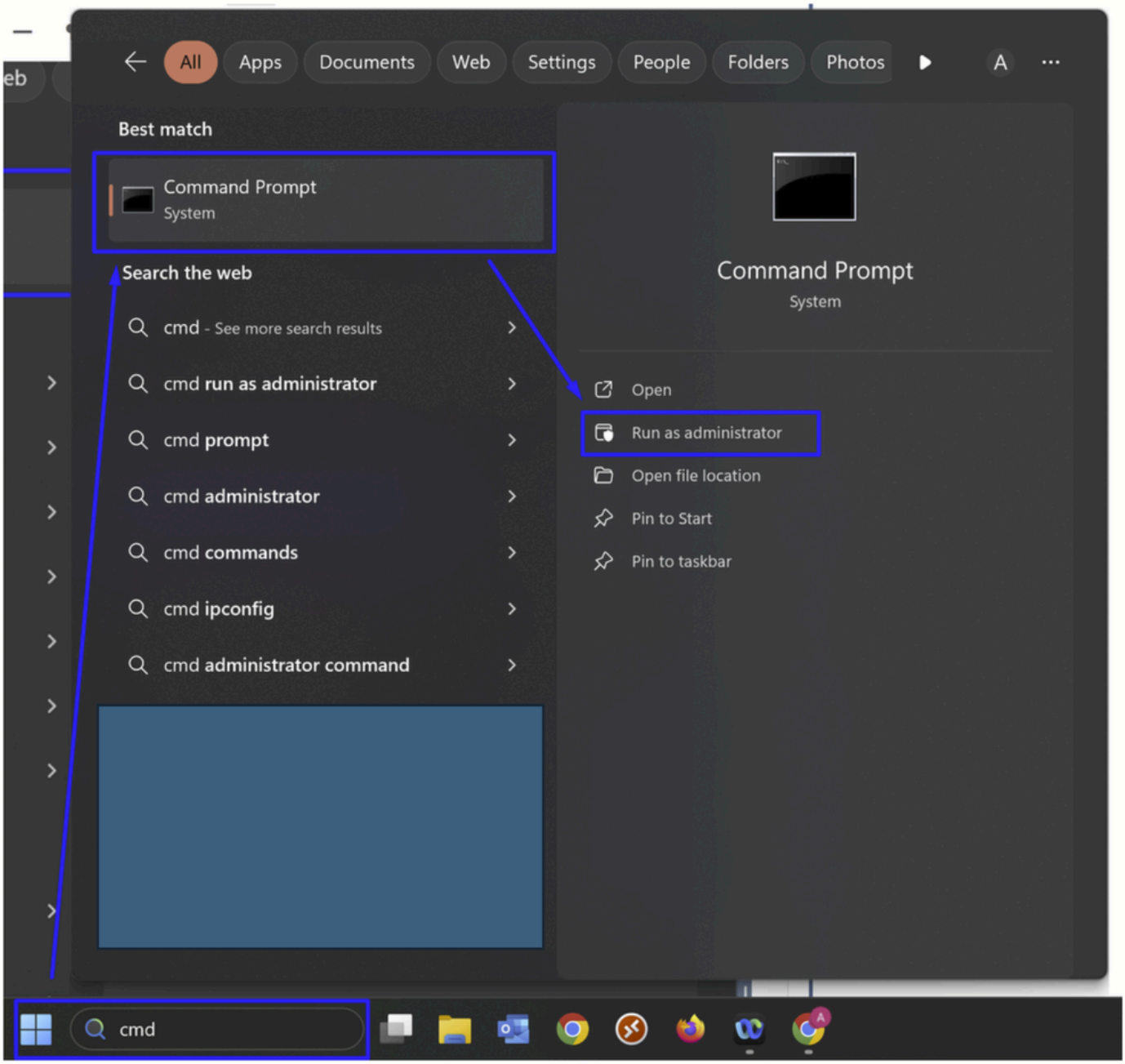
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Crear las claves privada y pública en Windows

Haga clic en el icono Buscar situado en la barra de tareas:

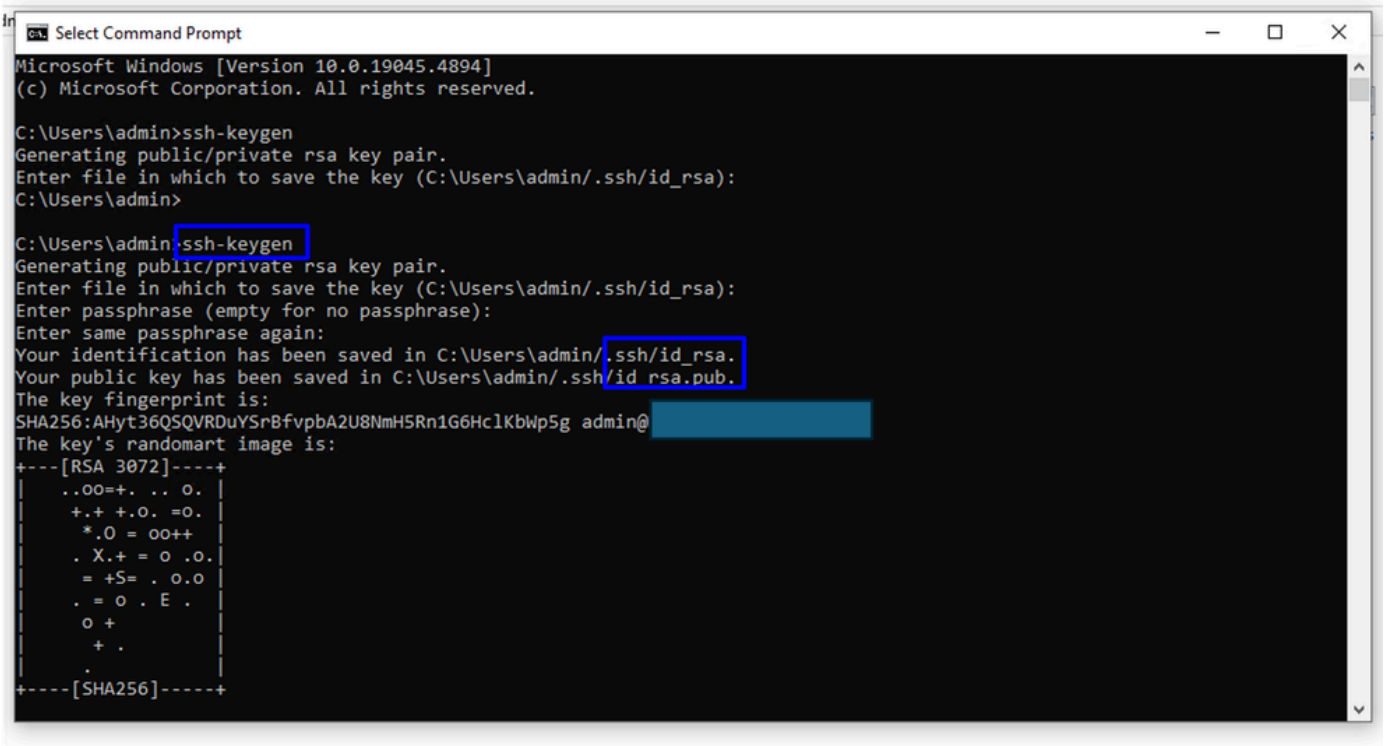
· Escriba cmd en la barra de búsqueda
· En los resultados de la búsqueda, haga clic con el botón derecho en Símbolo del sistema y seleccione Ejecutar como administrador. Esto garantiza que dispone de los permisos necesarios para ejecutar comandos



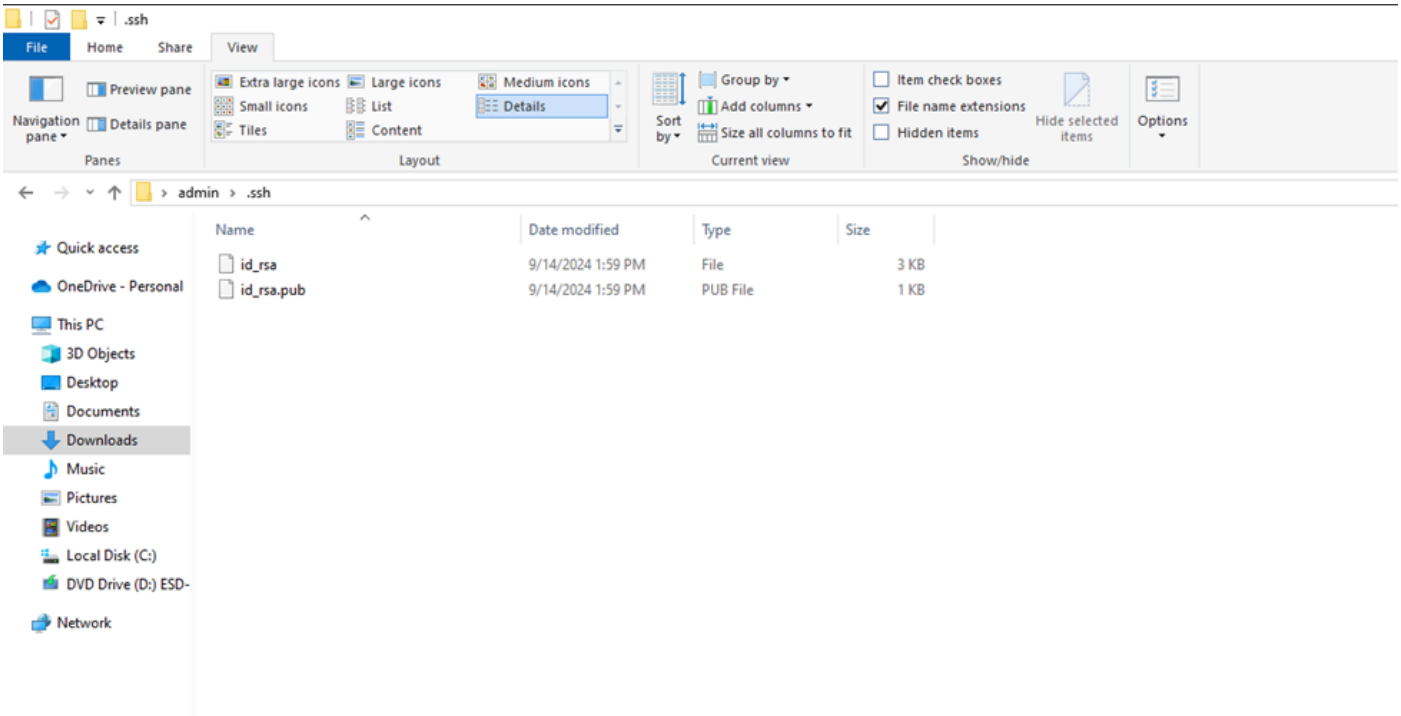
· Ejecute el siguiente comando:

```
ssh-keygen
```

- Esto le pide que introduzca la clave de cifrado dos veces. Guárdelo, ya que se trata de una contraseña para su autenticación en ISE como nueva contraseña. Después de eso, esto resulta en la creación de dos archivos, el privado (id_rsa) y el público (id_rsa.pub) claves, a continuación. Guarde los archivos en un directorio. Por ejemplo, se utilizó el predeterminado



- Comprobar dónde se almacenan los archivos



Transfiera la clave pública **(id_rsa.pub)** en la carpeta del repositorio de archivos configurada en ISE.

Cree las claves privada y pública mediante en MacOS

Haga clic en el **Finder** icono situado en el muelle
· Desplácese hasta el **Applications folder**

· Dentro de la **Applications folder**, localice y abra la carpeta Utilidades
· En la lista Utilidades, busque **Terminal**
· Haga doble clic en **Terminal** para abrirlo
· En la **Terminal** ventana, escriba "ssh-keygen -t rsa"y presione la tecla enter para ejecutarla
· Escriba la clave de encriptación dos veces y **save it**
· Ir a la ubicación de archivos
Transfiera la clave pública **(id_rsa.pub)** en la carpeta del repositorio de archivos configurada en ISE.

```
Your identification has been saved in /Users/myname/.ssh/id_rsa.
Your public key has been saved in /Users/myname/.ssh/id_rsa.pub.
The key fingerprint is:
ae:89:72:0b:85:da:5a:f4:7c:1f:c2:43:fd:c6:44:38 myname@mymac.local
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|         .       |
|        E .      |
|   .   . o       |
|  o . . S .      |
| + + o . +       |
|. + o = o +      |
| o...o * o       |
|.  oo.o .        |
+-----------------+
```

Configure el certificado para iniciar sesión en ISE

Corroborar si el archivo público se encuentra en el repositorio mediante el siguiente comando:

```
show repository
```

```
ise-primary-33/admin#
ise-primary-33/admin#show repository Sever_all
Backup-Cisco-CFG10-240222-0915.tar.gpg
cisco-secure-client-win-5.0.05040-core-vpn-webdeploy-k9.msi
cisco-secure-client-win-5.0.05040-webdeploy-k9.pkg
Ethernet1.xml
FullReport_29-Mar-2024.csv
grise04conf-CFG10-240213-2200.tar.gpg
id_rsa.pub
```

- Importe el archivo de clave pública **(id_rsa.pub)** utilizando el comando en el modo de privilegio:

```
crypto key import

        repository
```

```
ise-primary-33/admin#crypto key import public.pub repository Sever all
```

- Entre en el modo de configuración global y utilice el comando:

```
service sshd PubkeyAuthentication
```

```
ise-primary-33/admin(config)#service sshd PubkeyAuthentication
  Enabling key pair authentication automatically disables password-based
authentication.
%
% To enable key pair authentication in this Cisco ISE node,
% add at least one public key to the node. You must add
% a public key even if you want to configure private key usage in a later
step.
% If you don't already have a public key file in your system,
% add one to a repository now. Then, import the key file with the following
command:
% crypto key import <public key filename> repository <repository name>
```

Utilice el comando para comprobar que no se produce ningún error mientras se importa la clave pública. Se recomienda continuar con esto a través del puerto de la consola para evitar perder el acceso a ISE.

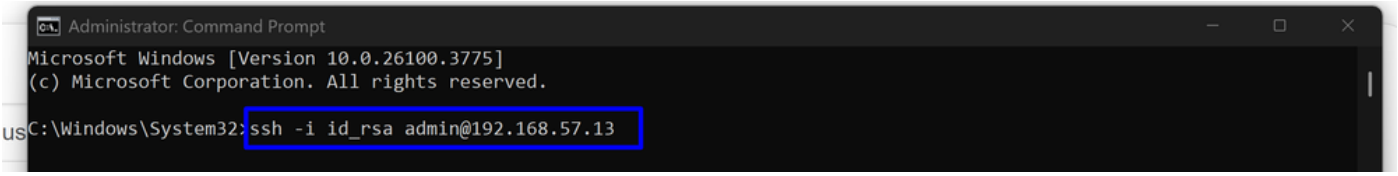
Verificación

Inicio de sesión en Windows

Intente acceder a ISE mediante **cmd** el comando:

```
ssh -i

        @
```

```
EXAMPLE:
ssh -i id_rsa admin@192.168.57.13
```



Utilice la clave de cifrado configurada en el paso Create the private and public keys in Windows para autenticarse.

Iniciar sesión en MacOS

Ingrese este comando en el terminal:

```
ssh -i

        @
```

```
EXAMPLE:
ssh -i id_rsa admin@192.168.57.13
```

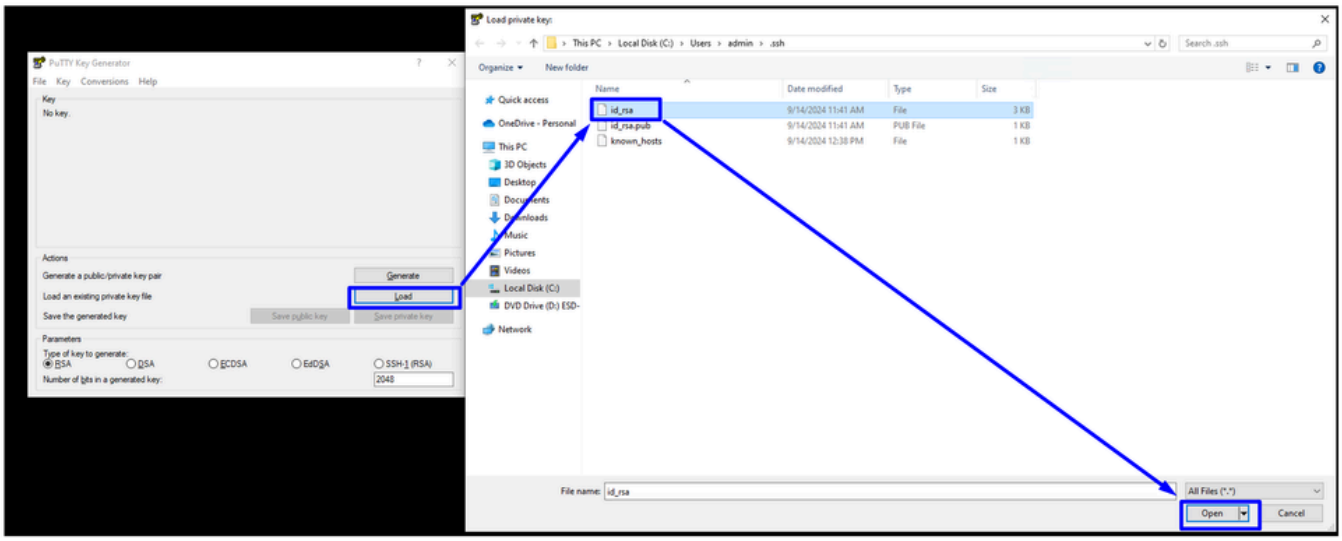
or

```
ssh -i ~/.ssh/

        @


EXAMPLE:
ssh -i ~/.ssh/id_rsa admin@192.168.57.13
```

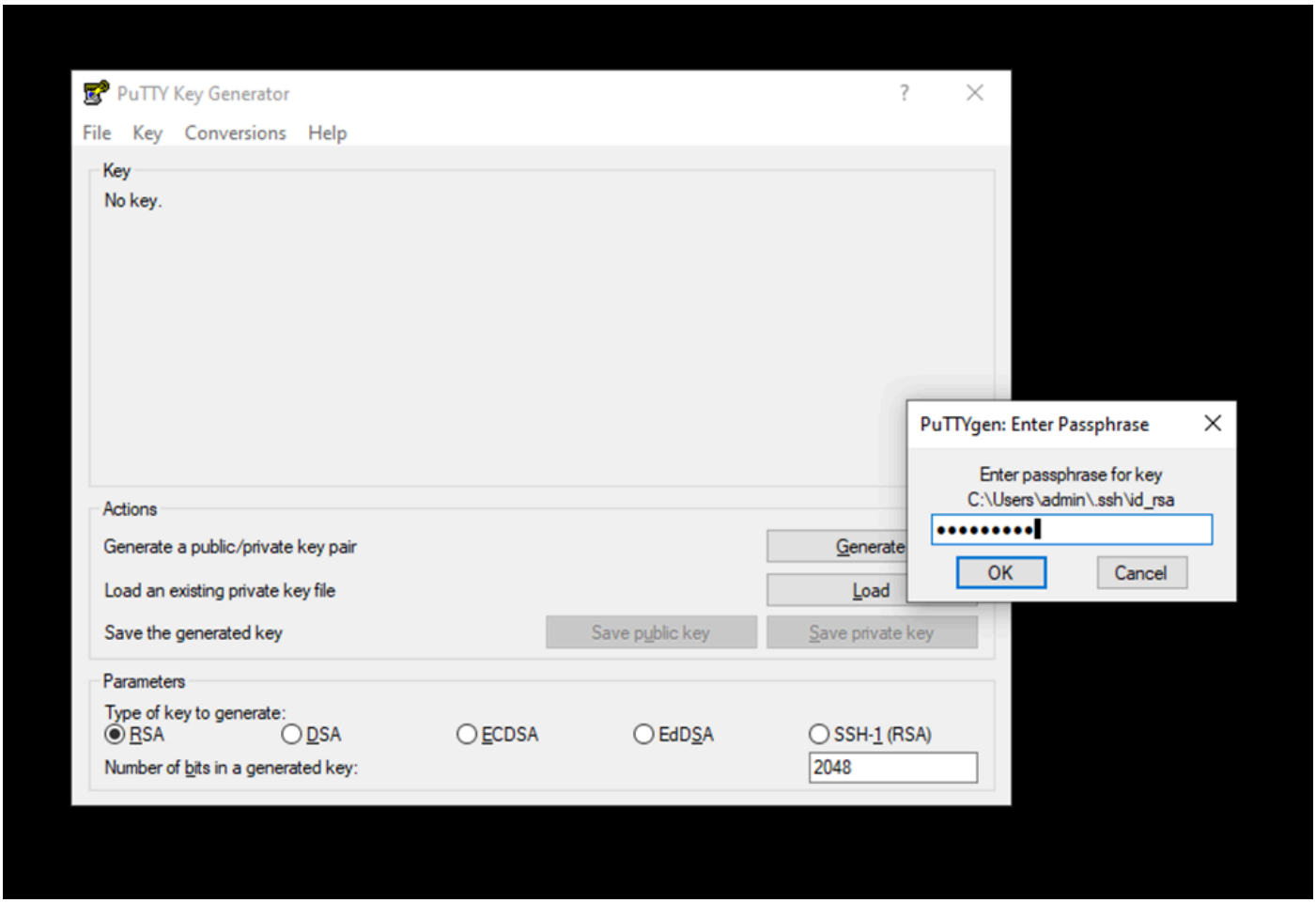
Utilice la clave de cifrado configurada en el paso Create the private and public keys via in MacOS para autenticarse.

Entrar en Putty

Abra PuTTy key generator (busque por PuttyGen en la barra de búsqueda inicial), haga clic en Cargar, seleccione todos los archivos y abra la clave privada generada desde cmd (Windows) o terminal (MacOS):

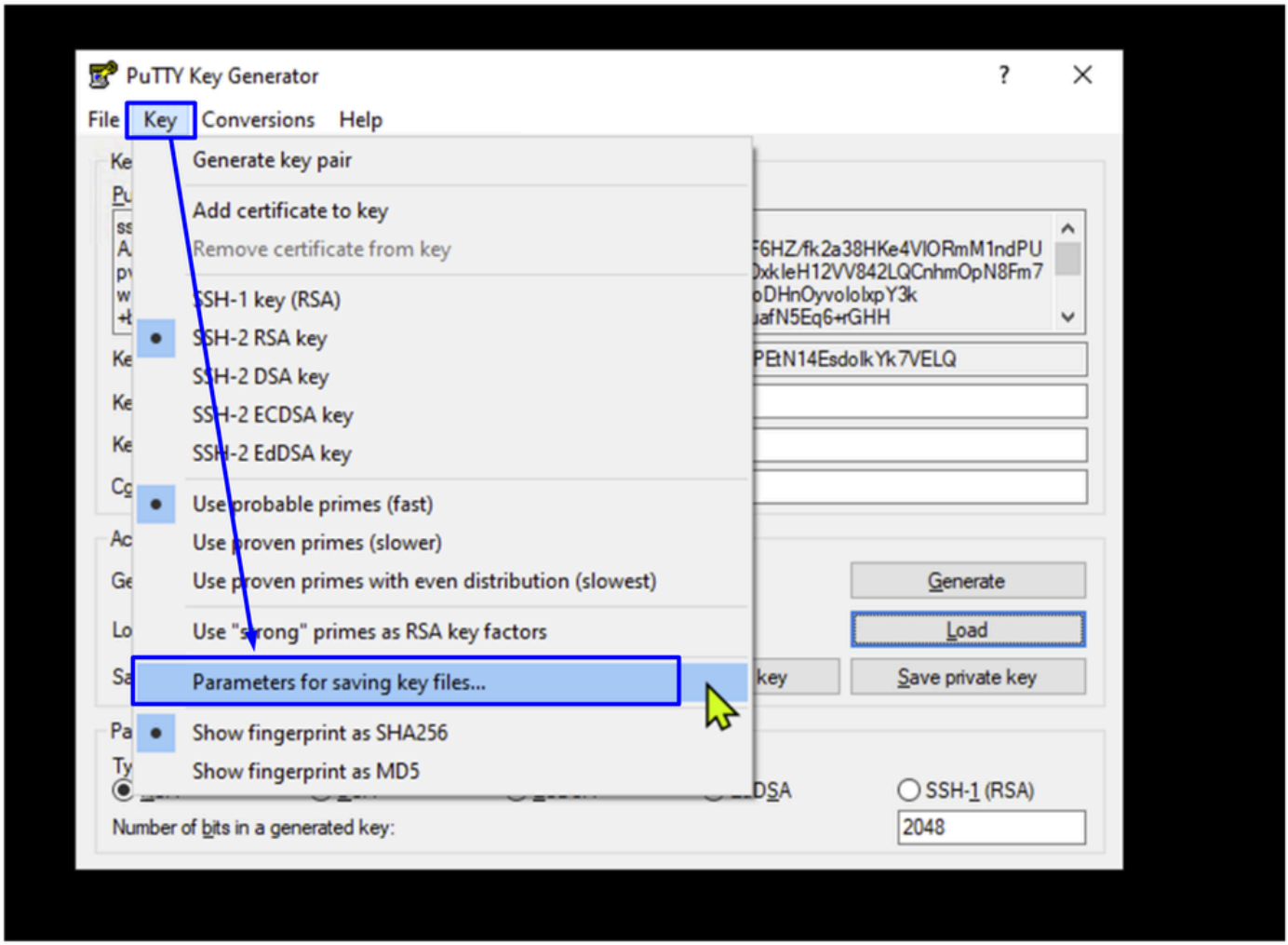


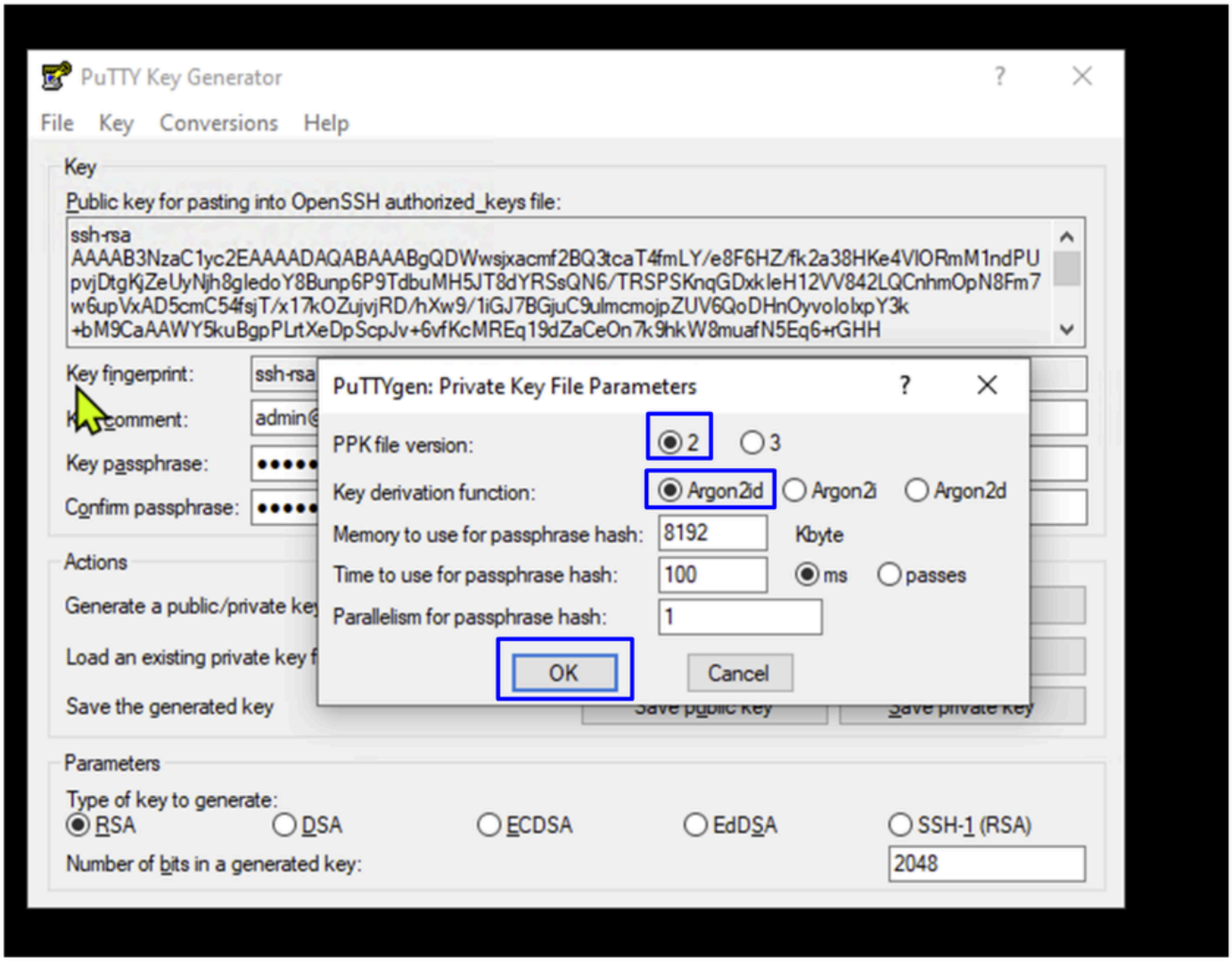
- Escriba la clave de cifrado utilizada anteriormente en el cmd o terminal



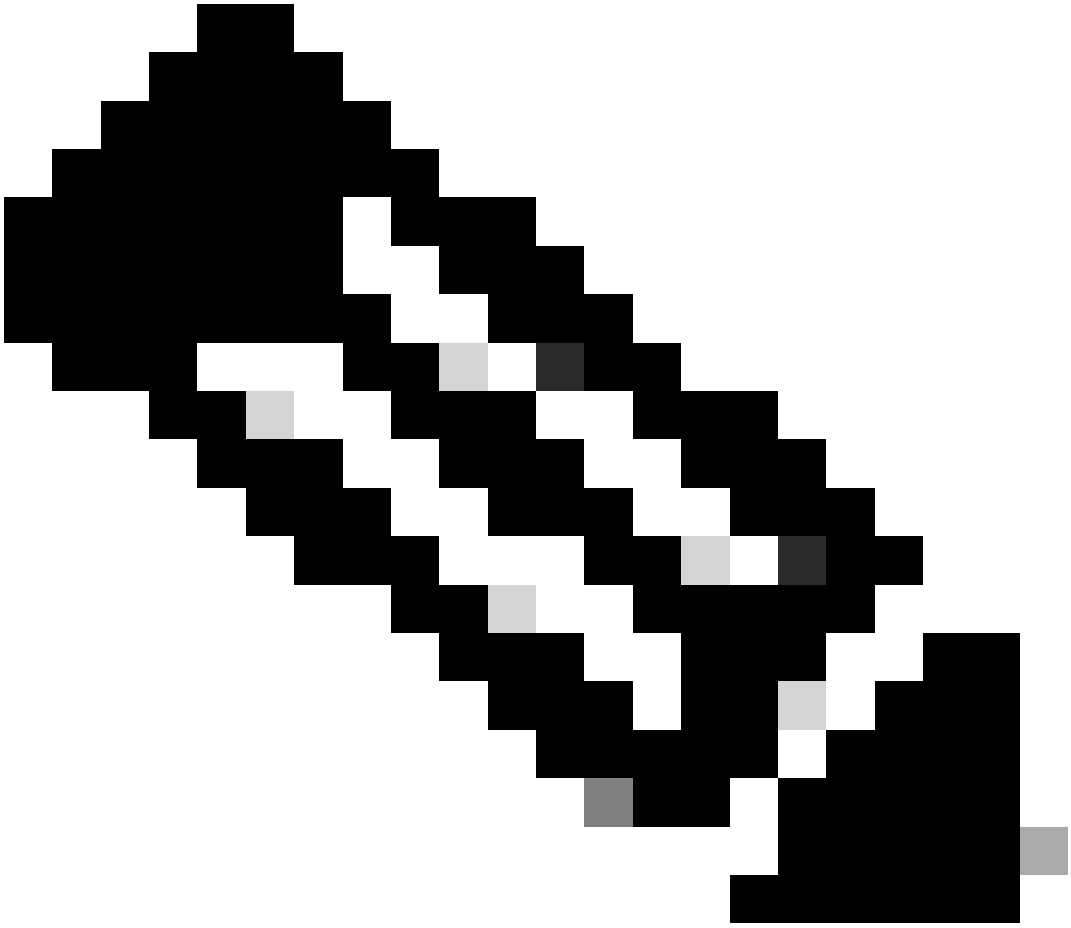
Convierta este archivo a una versión compatible con Putty ejecutando los siguientes pasos:

- Haga clic en Key > Parameters para guardar archivos de claves


PuTTY Key Generator
File
Key
Conversions
Help
Generate key pair
Add certificate to key
Remove certificate from key
SSH-1 key (RSA)
SSH-2 RSA key
SSH-2 DSA key
SSH-2 ECDSA key
SSH-2 EdDSA key
Use probable primes (fast)
Use proven primes (slower)
Use proven primes with even distribution (slowest)
Use "strong" primes as RSA key factors
Parameters for saving key files...
Show fingerprint as SHA256
Show fingerprint as MD5
Generate
Load
Save private key
SSH-1 (RSA)
Number of bits in a generated key:
2048

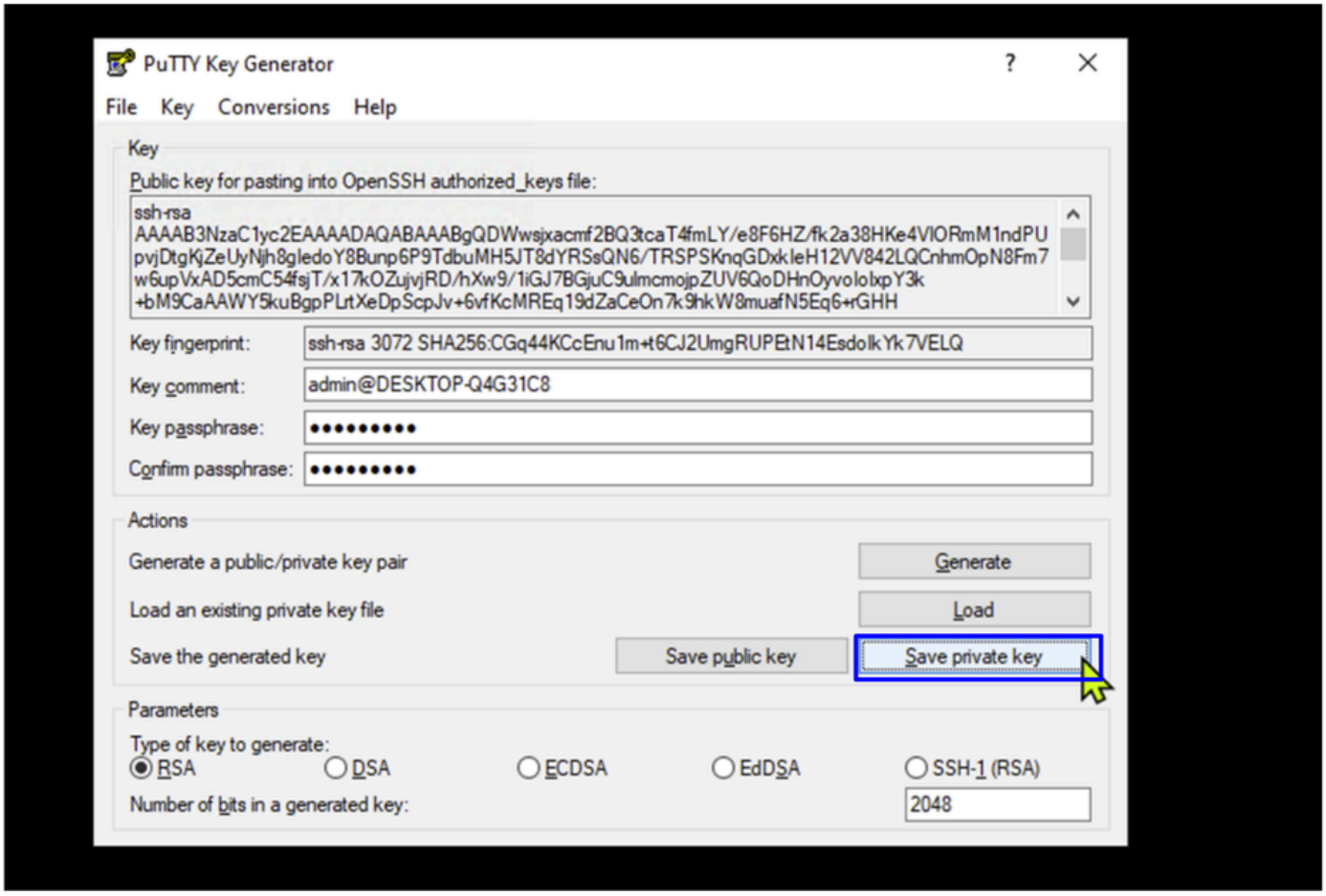


- PPK file version : Elija 2
- **Key derivation function**: Elija Argon2id



Nota: Para el resto de los parámetros, utilice los valores predeterminados.

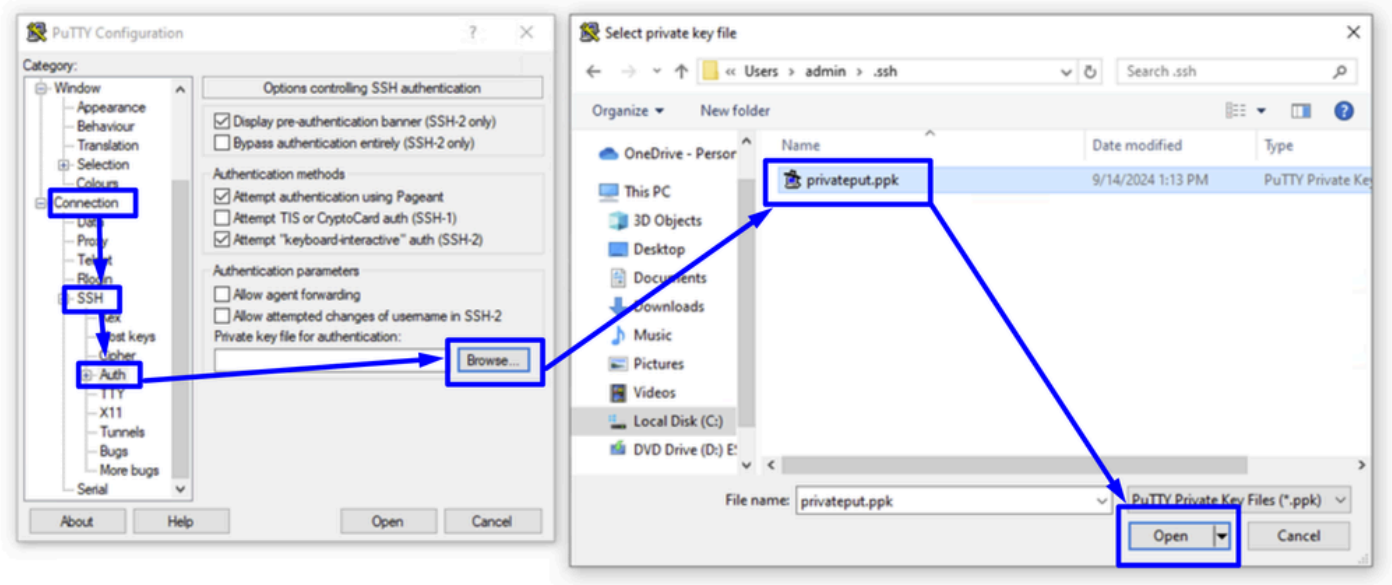
- Haga clic en Ok



- Haga clic en Save private Key

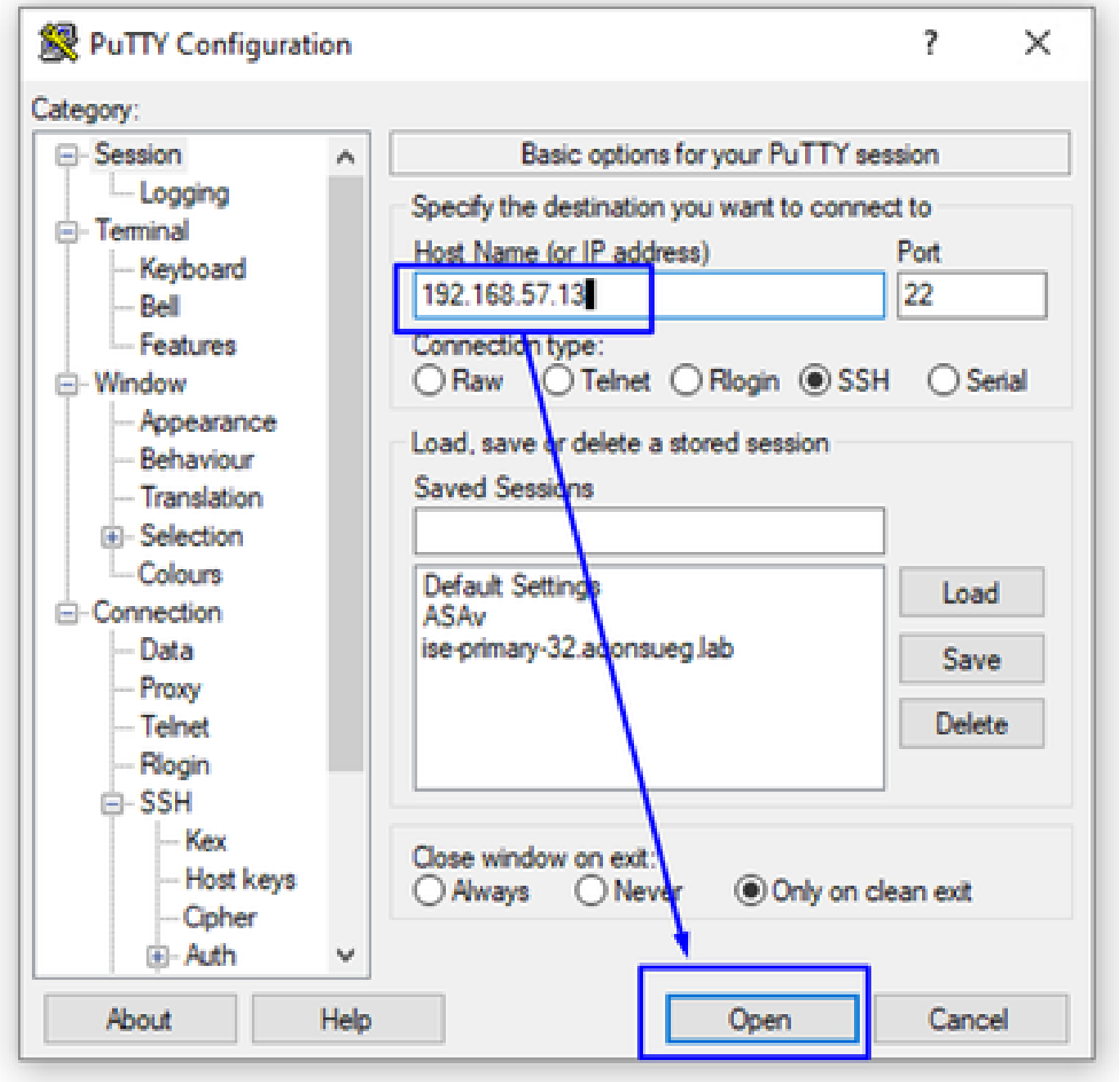
Una vez guardada la clave en el equipo, podrá utilizarla en los siguientes ejemplos:

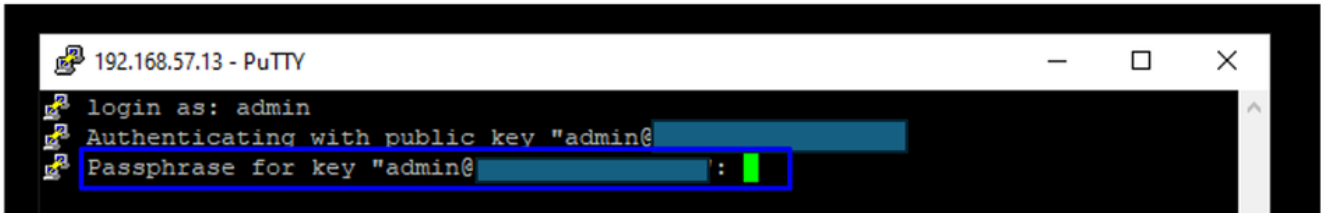
- Masilla abierta
- Haga clic en **Connection > SSH > Auth > Browse**
- Seleccione su clave privada y haga clic en Open



- Vuelva a la sesión y establezca la dirección IP o el nombre de host (FQDN) de ISE

- Haga clic en Abrir





Utilice la clave de cifrado configurada en el paso Create the private and public keys via in MacOS o Create the private and public keys in Windows para autenticarse.

Troubleshoot

Desproteja los mensajes de error del sitio del extremo agregando en la conexión ssh el indicador -v

```
Example for Windows:
ssh -v -i id_rsa admin@192.168.57.13
```

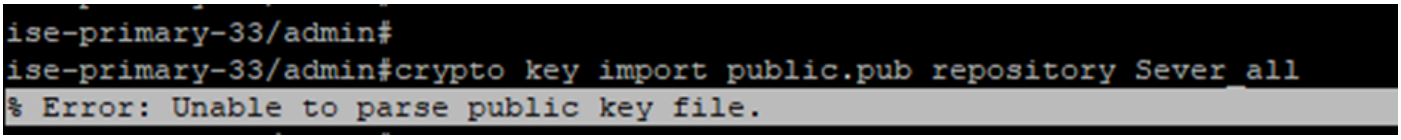
```
Example for MacOS:
ssh -v -i id_rsa admin@192.168.57.13
```

or

```
ssh -v -i ~/.ssh/id_rsa admin@192.168.57.13
```

Error al importar la clave pública

%ERROR: No se puede analizar el archivo de clave pública.



Si tiene algún inconveniente al importar más de una clave pública, póngase en contacto con el servicio de asistencia de Cisco.

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).