使用ISE配置私钥身份验证

目录

简介

本文档介绍如何创建私有安全外壳(SSH)密钥，以验证身份安全引擎(ISE)上的CLI。

先决条件

要求

Cisco 建议您了解以下主题：

- ISE中的存储库。
- 证书身份验证。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ISE 3.3补丁3
- Windows 10
- MacOS X
- SSH客户端Putty

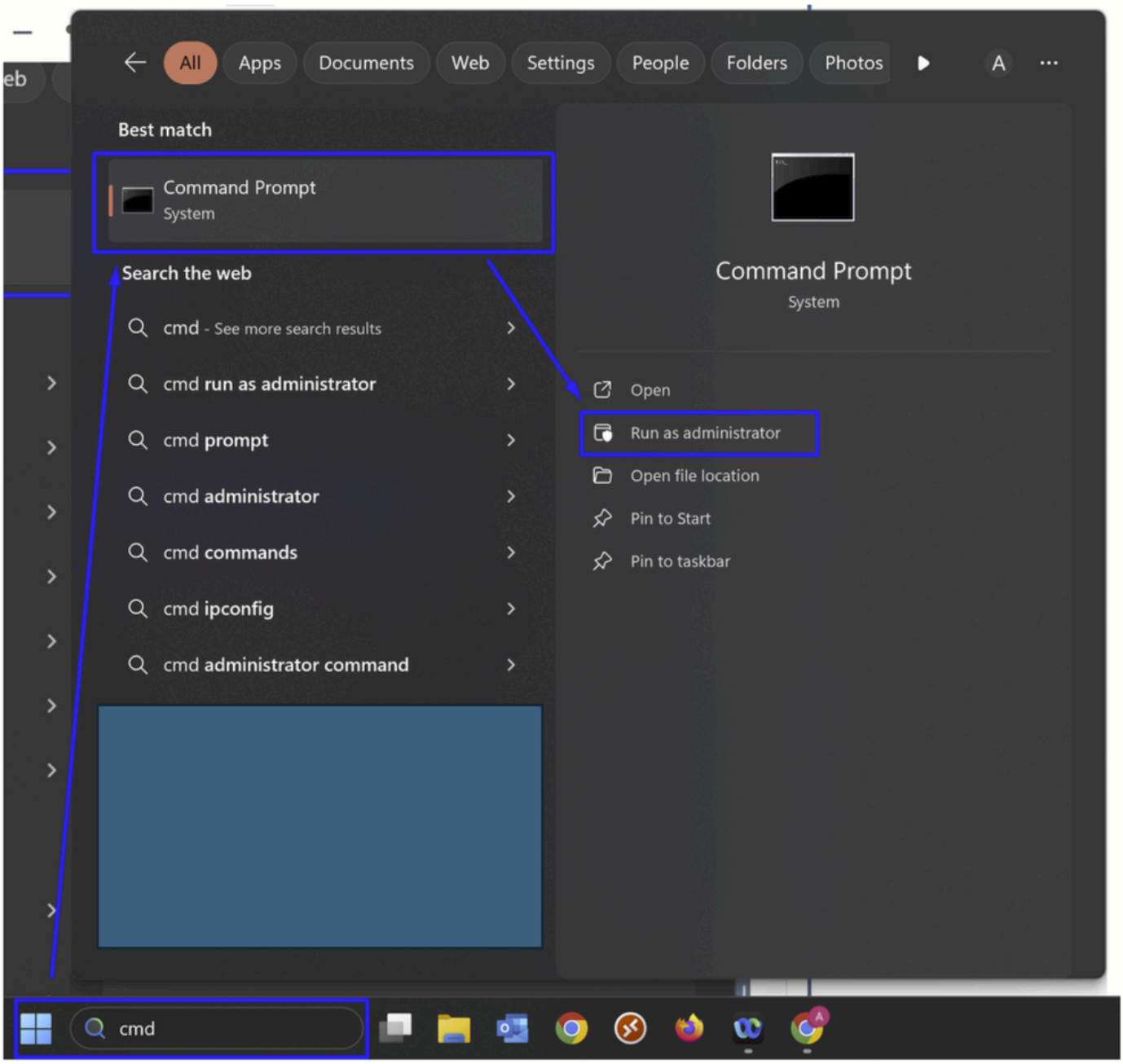
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

在Windows中创建私钥和公钥

单击任务栏上的“搜索”图标：

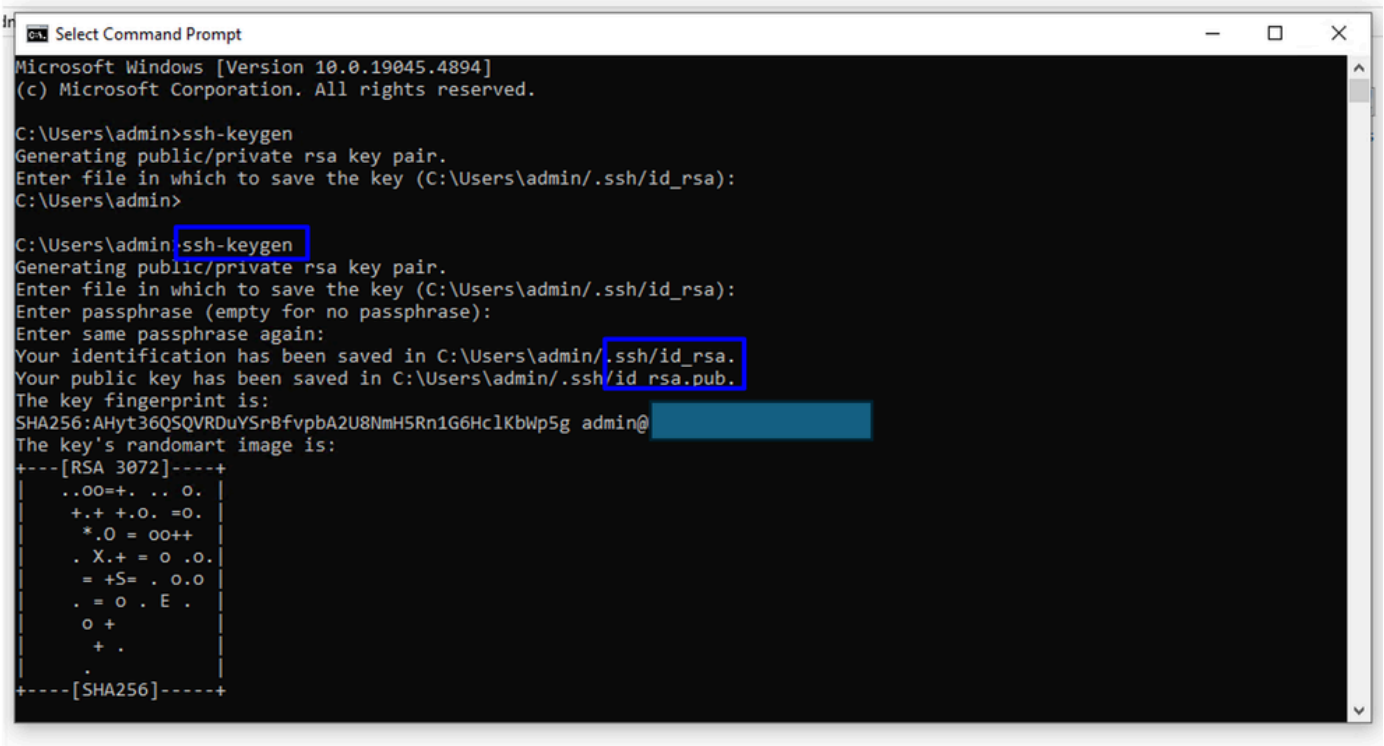
·在搜索栏中键入cmd
·在搜索结果中，右键单击Command Prompt（命令提示符）并选择Run as administrator（以管理员身份运行）。这样可以确保您具有执行命令所需的权限



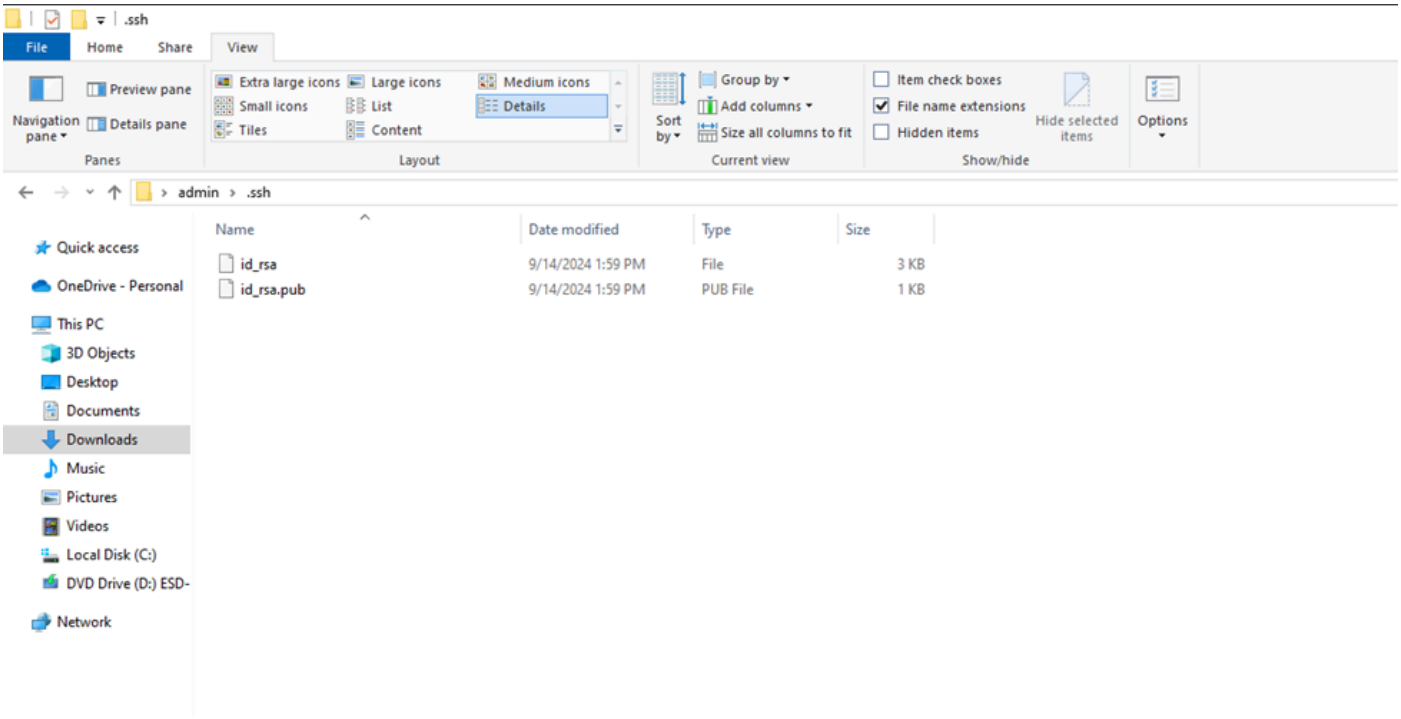
·执行下一个命令：

```
ssh-keygen
```

- 这会提示您输入加密密钥两次。请保存它，因为它是要根据ISE进行身份验证作为新密码。此后，这将导致创建两个文件，即专用(id_rsa)和公共(id_rsa.pub)密钥。将文件保存在一个目录中。例如，使用的是默认路由



- 验证文件的存储位置



传输在ISE上(id_rsa.pub)配置的文件存储库文件夹中的公钥。

在MacOS中通过创建私钥和公钥

单击位于Finder坞站中的图标
·导航至 Applications folder
·在中，找到Applications folder并打开“实用程序”文件夹
·在实用程序列表中，查找 Terminal
·双击打Terminal开它
·在窗Terminal口中键入“ssh-keygen -t rsa”，然后按Enter键执行该命令
·写加密密钥两次，然后 save it
·转到文件位置
传输在ISE上(id_rsa.pub)配置的文件存储库文件夹中的公钥。

```
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 .       |
+-----------------+
```

配置证书以登录ISE

使用下一命令验证公用文件是否位于存储库下：

```
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
```

- 在特权模式下(id_rsa.pub)使用命令导入公钥文件：

```
crypto key import

        repository
```

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

- 进入全局配置模式并使用命令：

```
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>
```

请使用命令来验证您在导入公钥时不会收到任何错误。建议通过控制台端口继续此步骤，以避免失去对ISE的访问。

验证

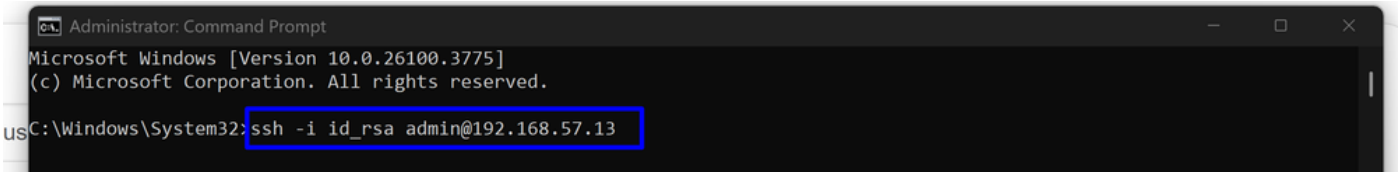
登录Windows

使用命令尝试通过cmd访问ISE:

```
ssh -i

        @


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



使用步骤在Windows中创建私有密钥和公钥中配置的加密密钥进行身份验证。

登录MacOS

在终端中输入以下命令：

```
ssh -i

        @


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

或

```
ssh -i ~/.ssh/
```

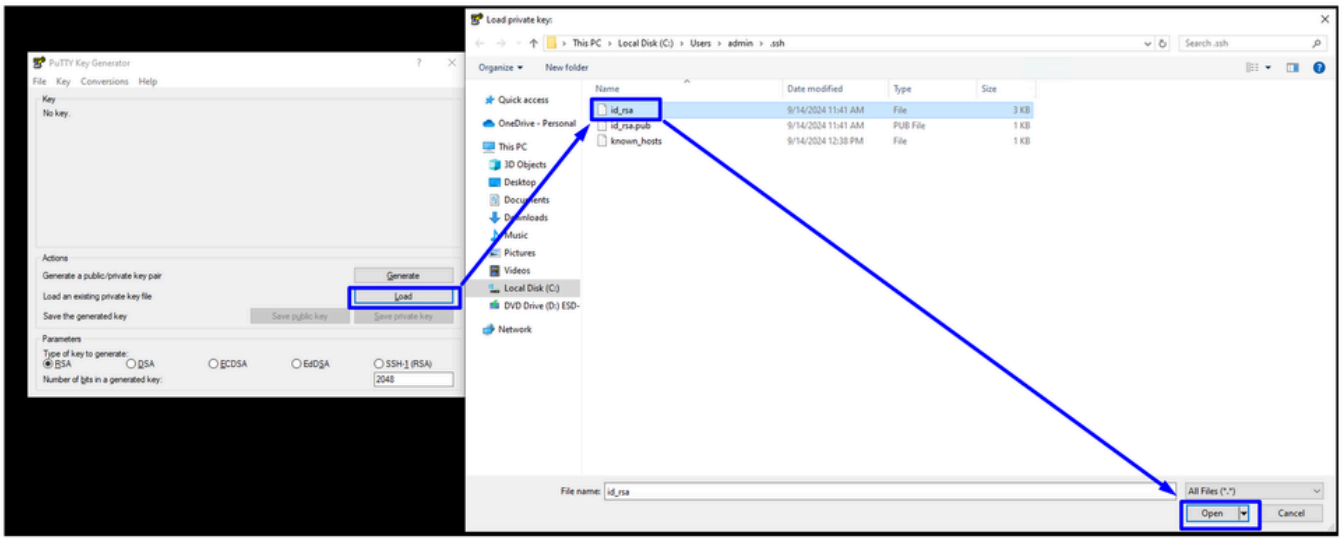
```
        @
```

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

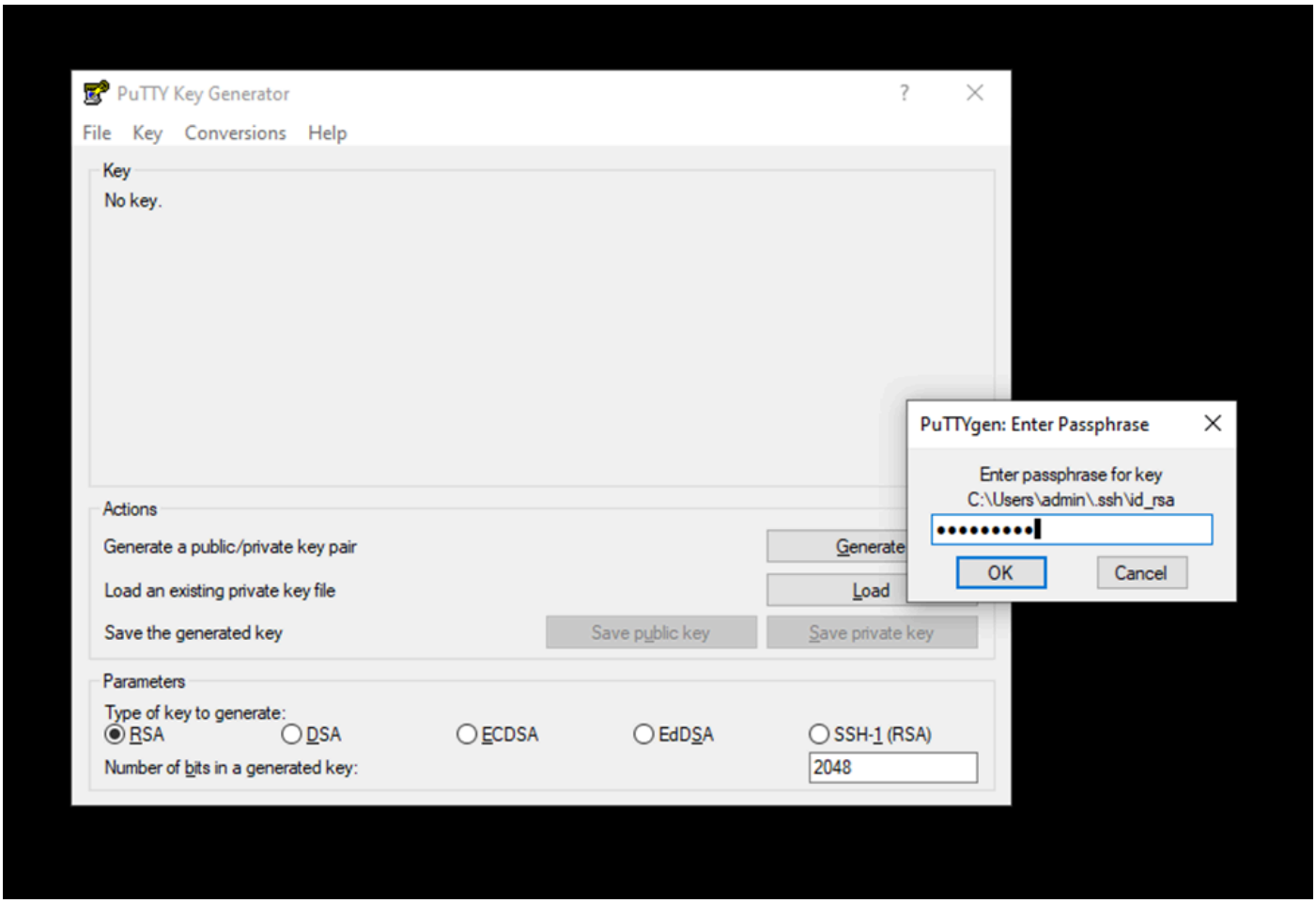
使用步骤在MacOS中创建私有密钥和公钥中配置的加密密钥进行身份验证。

登录Putty

打PuTTy key generator开（在开始搜索栏中按PuttyGen搜索），点击Load，选择所有文件，并打开从cmd(Windows)或terminal(MacOS)生成的私钥：

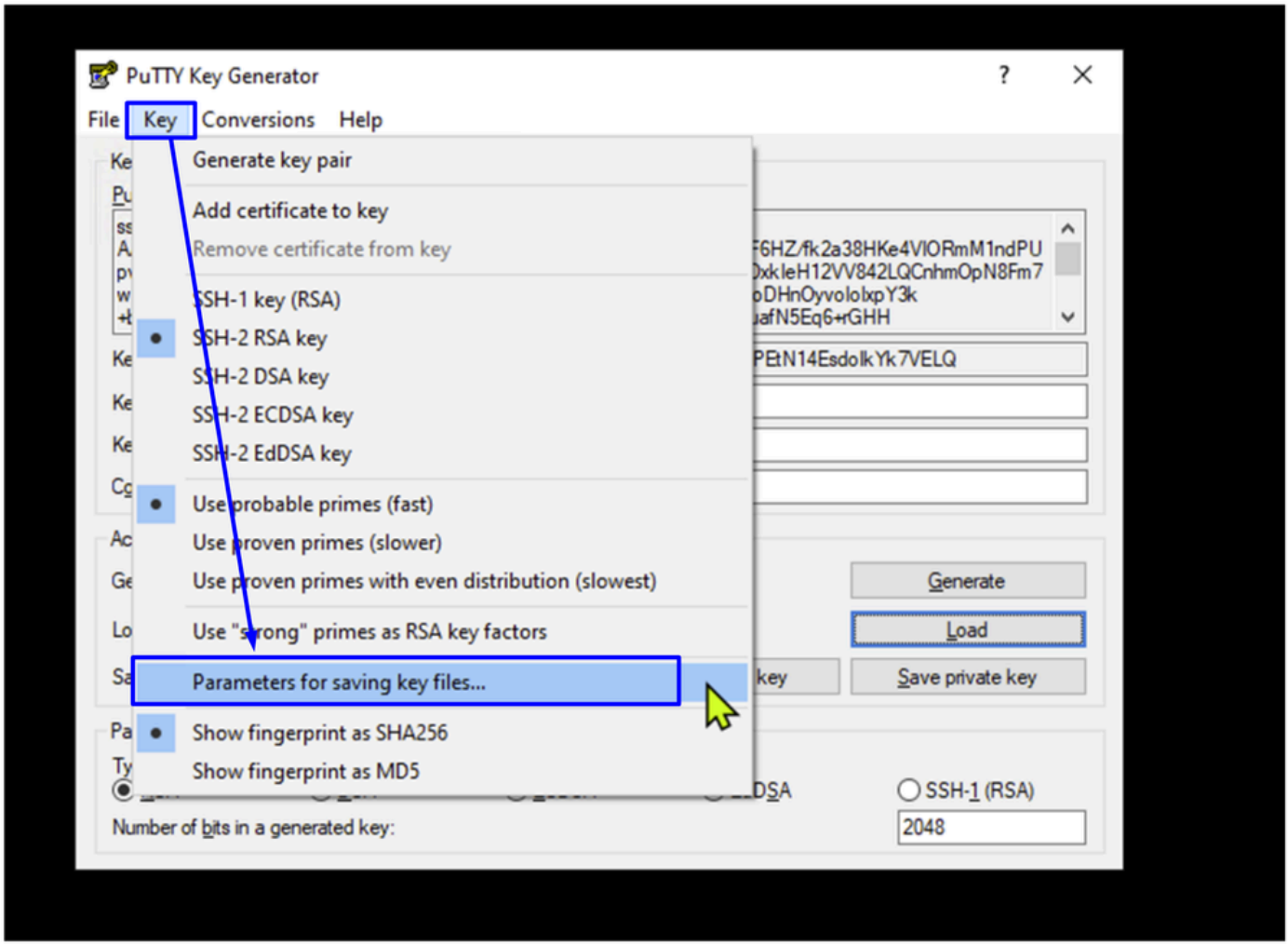


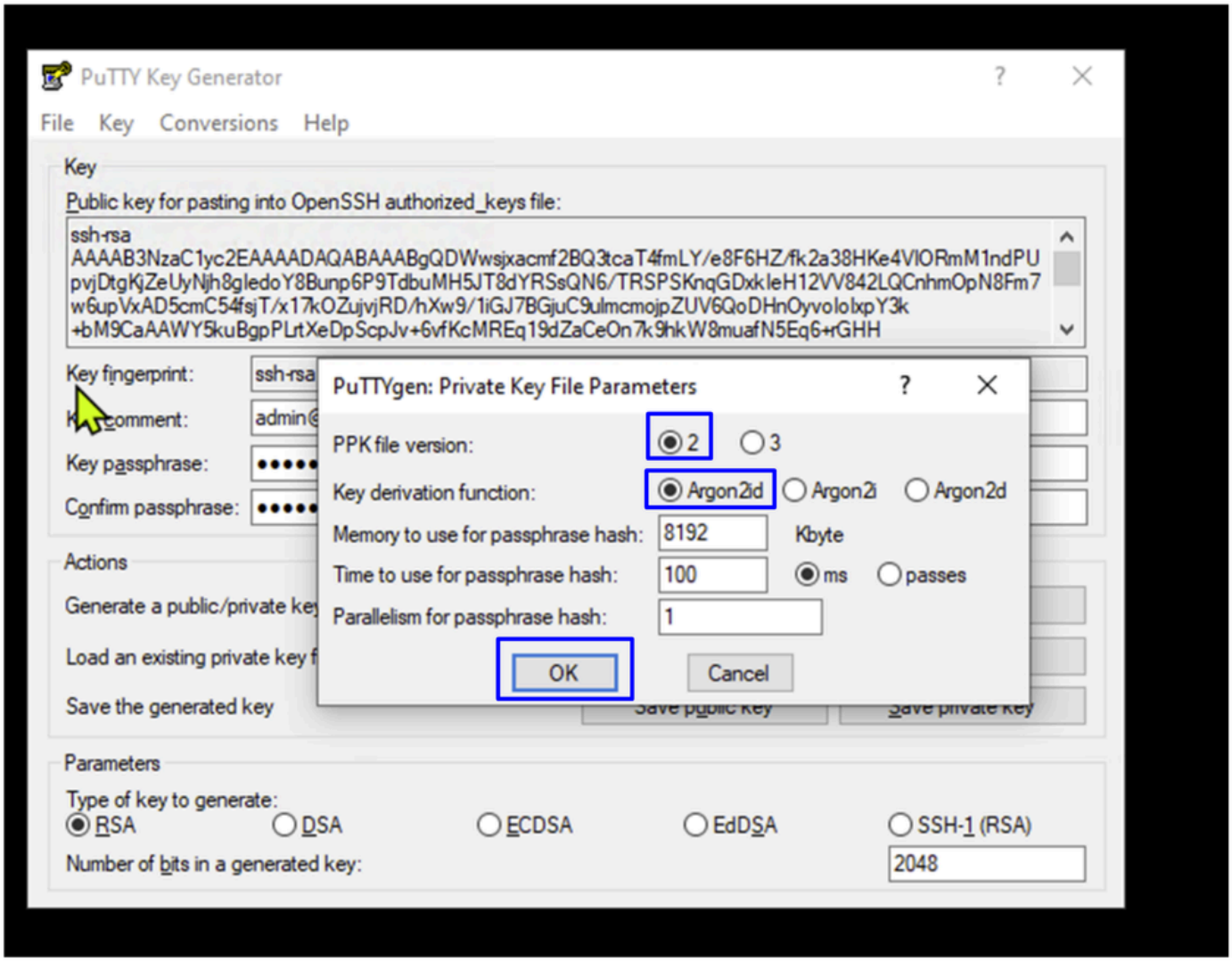
- 写下以前在cmd或terminal中使用的加密密钥



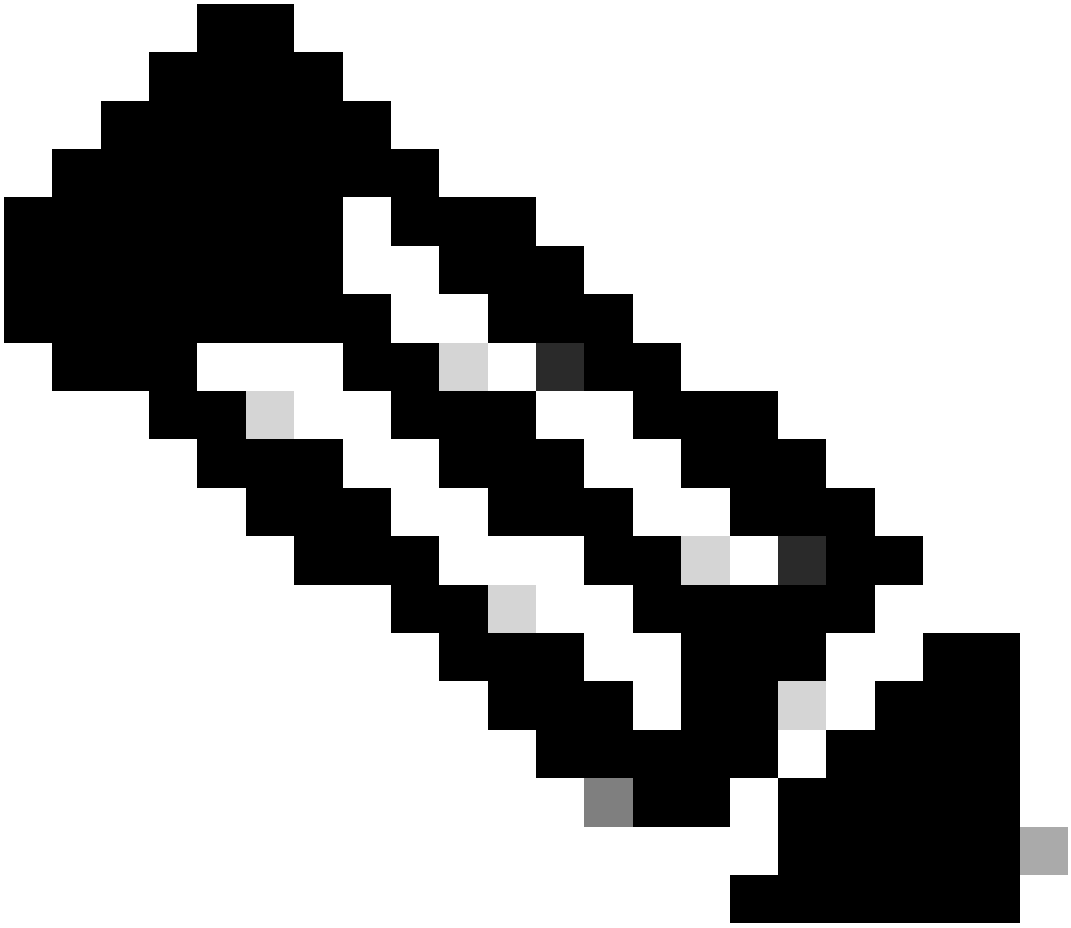
通过执行以下步骤将此文件转换为兼容的Putty版本：

- 点击Key > Parameters以保存密钥文件


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

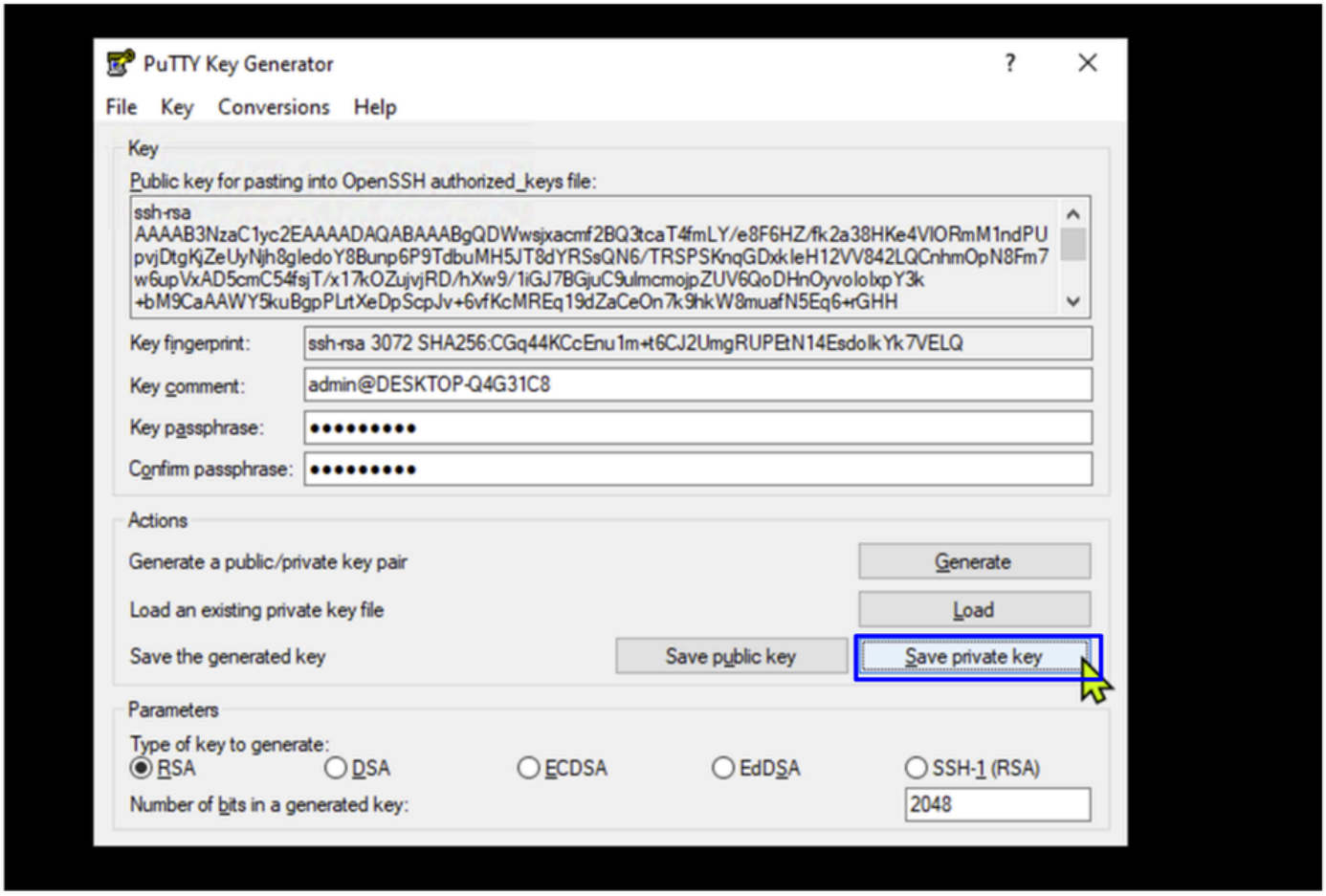


- PPK file version :选择2
- **Key derivation function**:选择Argon2id



注意：对于其余参数，请使用默认值。

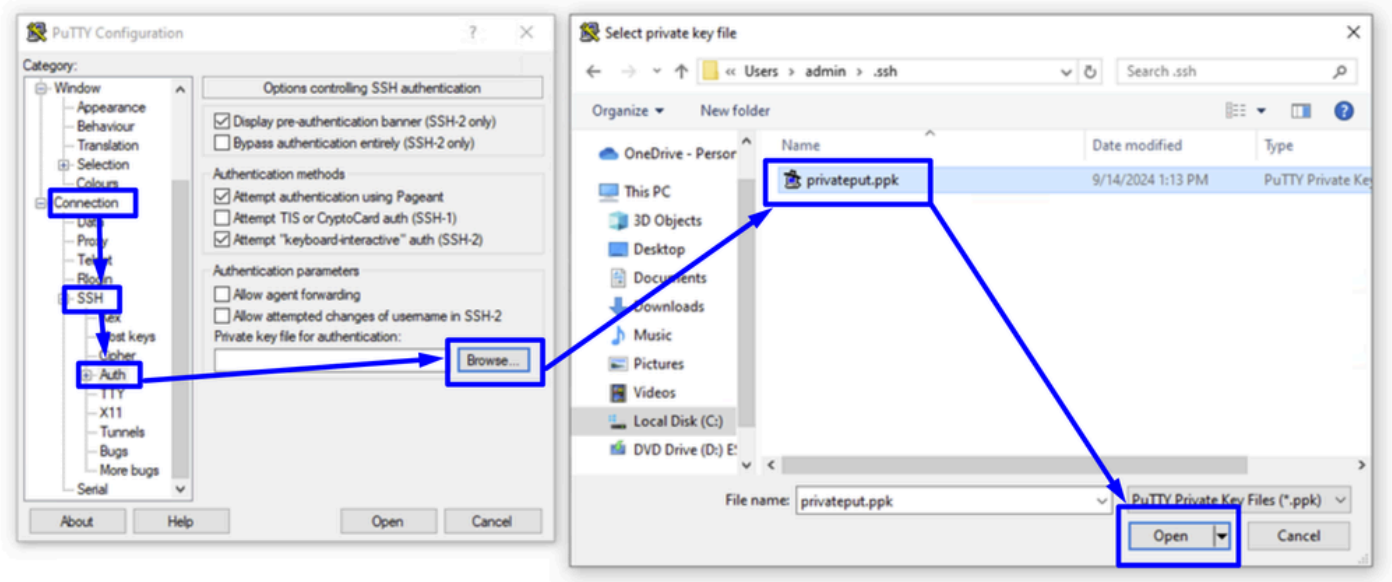
- 点击 Ok



- 点击 Save private Key

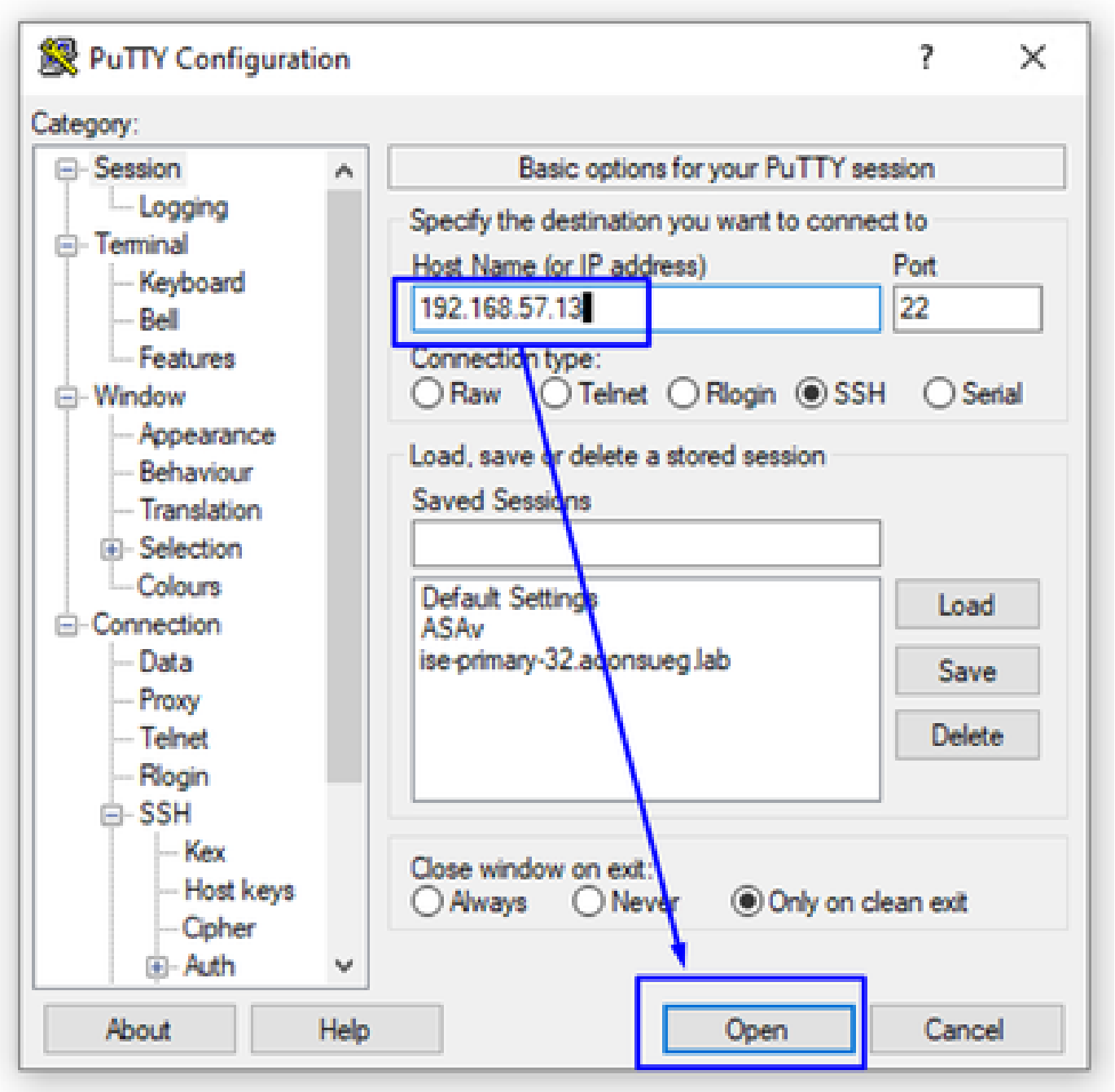
在计算机上保存密钥后，通过参考以下示例，即可使用该密钥：

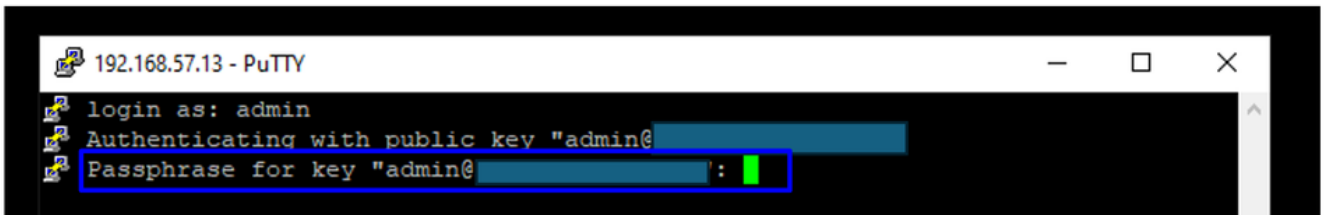
- 开放性腻子
- 点击**Connection > SSH > Auth > Browse**
- 选择您的私钥并单击 Open



- 返回会话，设置ISE的IP地址或主机名(FQDN)

- 单击“打开”





使用[在MacOS中创建私有密钥和公钥]或[在Windows中创建私有密钥和公钥]步骤中配置的加密密钥进行身份验证。

故障排除

从终端站点签出错误消息，在SSH连接中添加标志-v

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

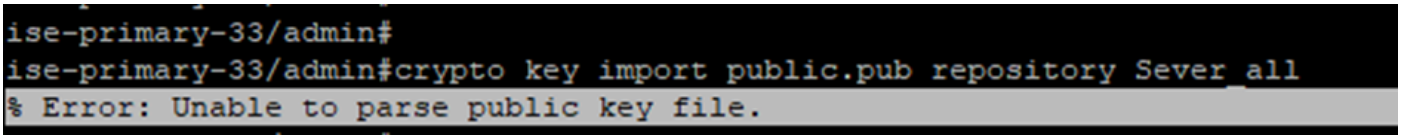
```
Example for MacOS:
ssh -v -i id_rsa admin@192.168.57.13
```

或

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

导入公钥时出错

%ERROR:无法分析公钥文件。



如果您在导入多个公钥时遇到任何不便，请联系思科支持。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。