使用ISE配置私鑰身份驗證

目錄

簡介

本文檔介紹如何建立私有安全外殼(SSH)金鑰，以便在Identity Secure Engine(ISE)上對CLI進行身份驗證。

必要條件

需求

思科建議您瞭解以下主題：

- ISE中的儲存庫。
- 證書身份驗證。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ISE 3.3補丁3
- Windows 10
- MacOS X
- SSH客戶端Putty

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

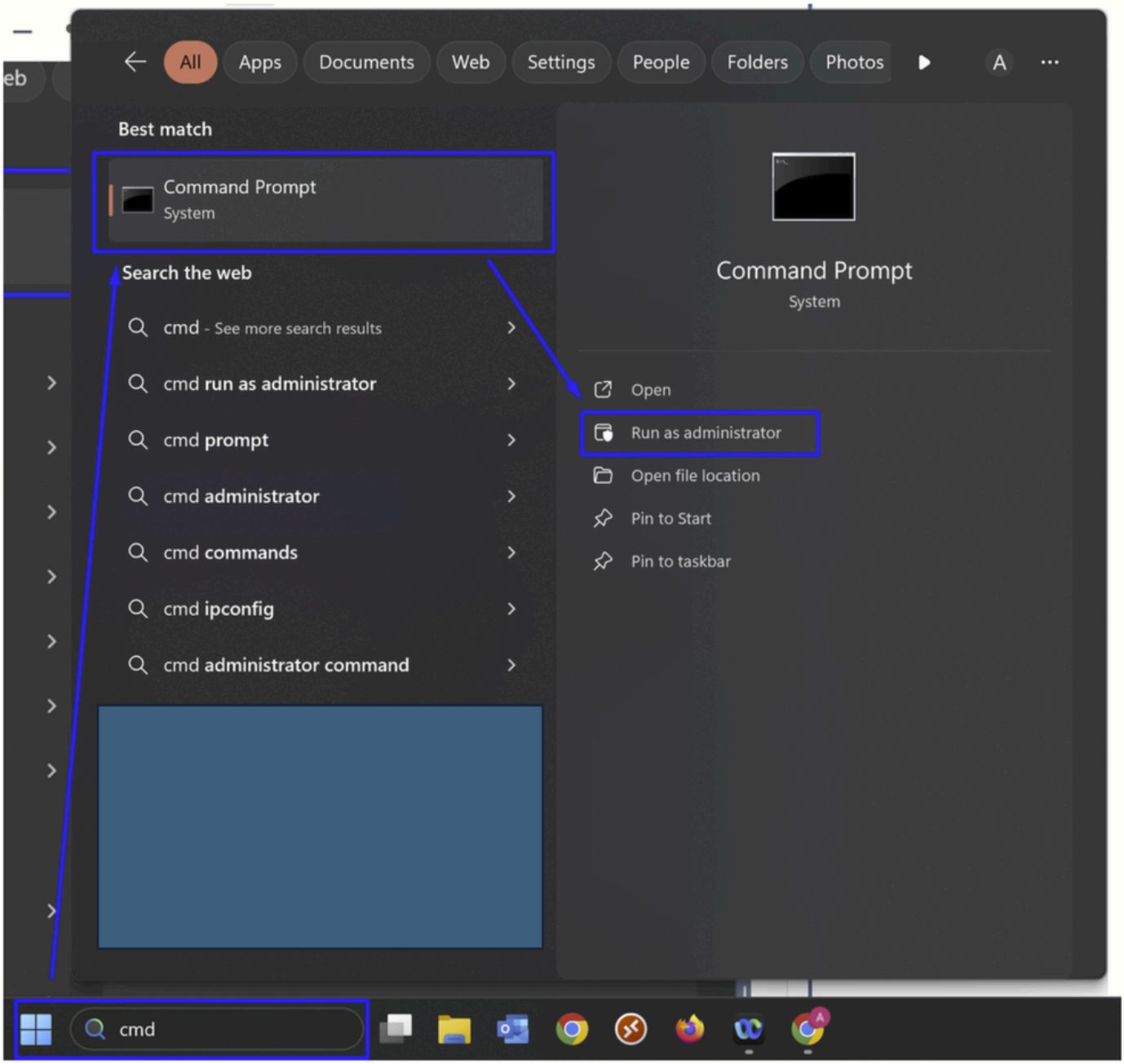
) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

在Windows中建立私鑰和公鑰

按一下工作列上的「搜尋」圖示：

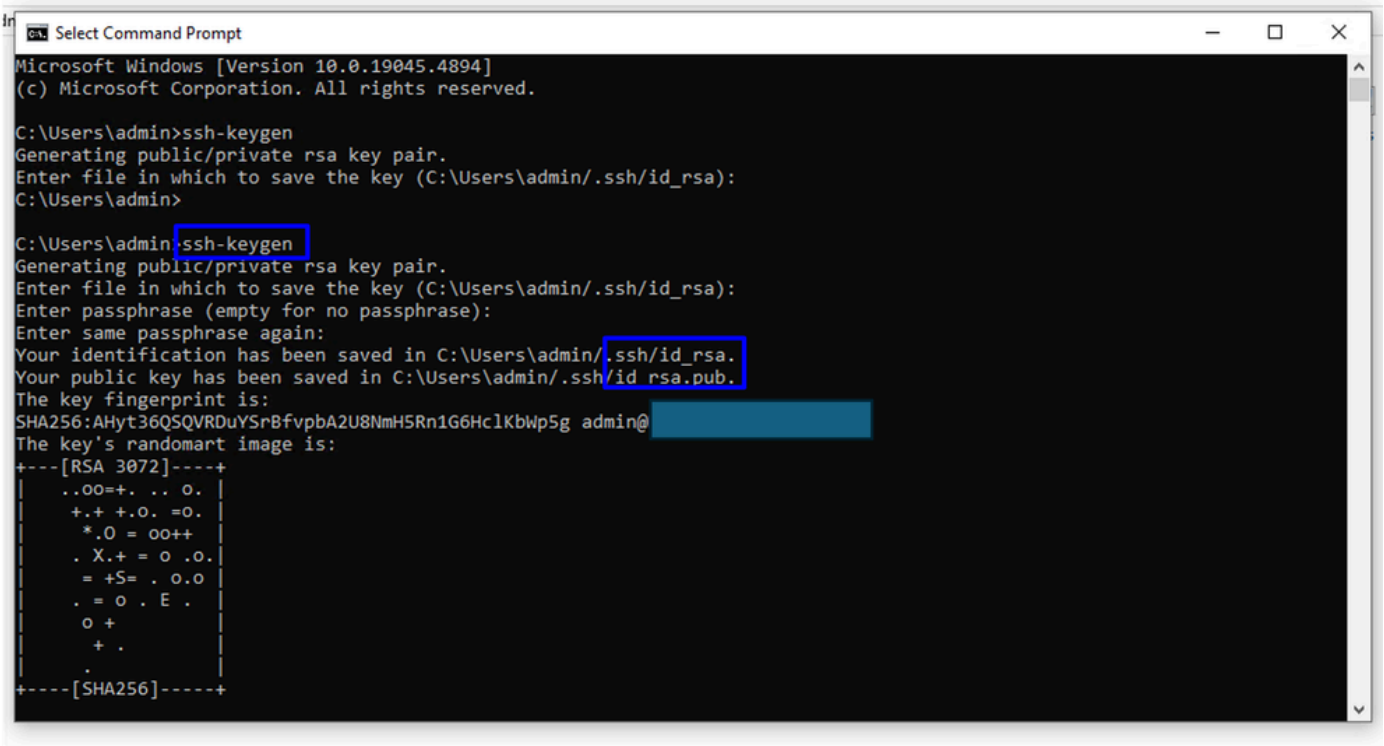
·在搜尋欄中鍵入cmd
·在搜尋結果中，按一下右鍵命令提示符，然後選擇以管理員身份運行。這可確保您擁有執行命令所需的許可權



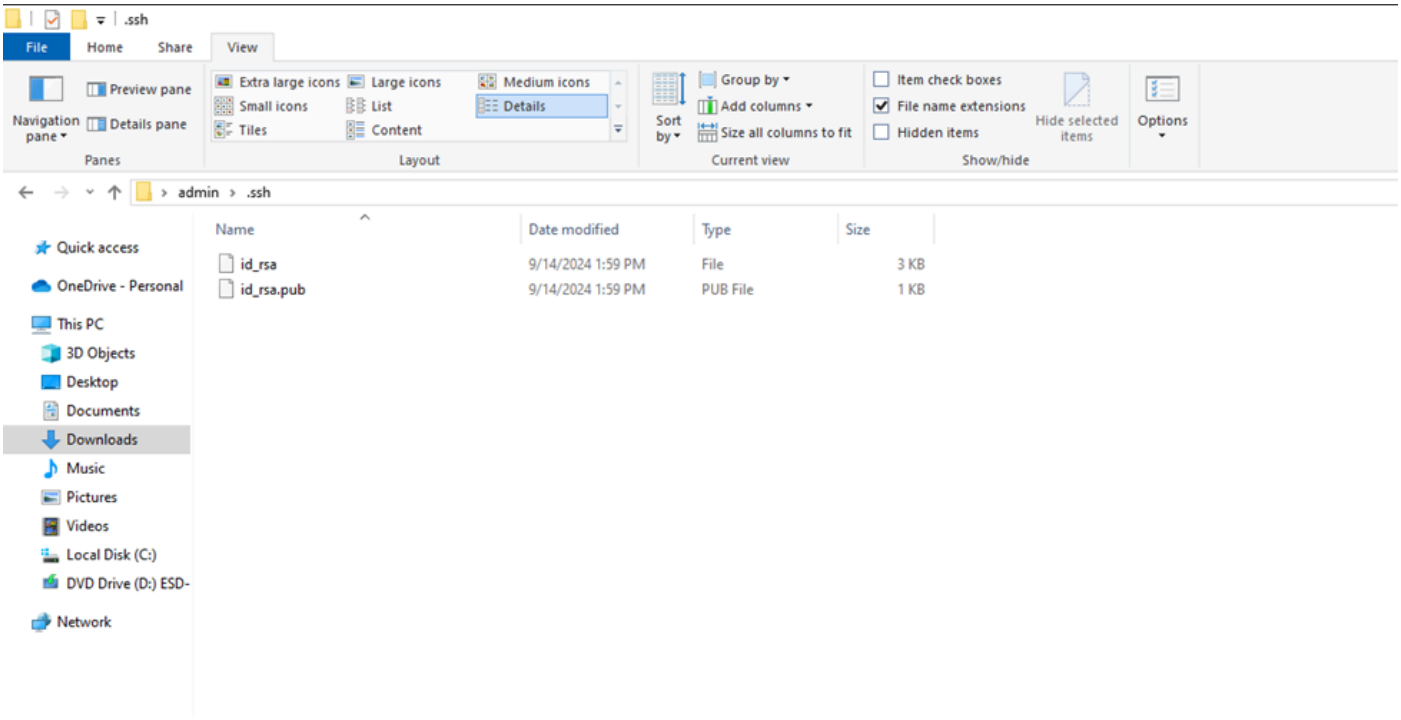
·執行下一個命令：

ssh-keygen

- 這將提示您輸入加密金鑰兩次。請儲存該密碼，因為此密碼用於根據ISE進行身份驗證，作為新密碼。在此之後，將建立兩個檔案，分別是私有(id_rsa)和公共(id_rsa.pub)金鑰。將檔案儲存在一個目錄中。例如，使用的是預設的



- 驗證檔案儲存位置



在ISE上配置(id_rsa.pub)的檔案儲存庫資料夾中傳輸公鑰。

在MacOS中通過建立私鑰和公鑰

按一下位於Finder塢站中的圖示
·導航至 Applications folder
·在中Applications folder找到並開啟Utilities資料夾
·在實用程式清單中，查詢 Terminal
·按兩下以打Terminal開它
·在視窗Terminal中鍵入「ssh-keygen -t rsa」，然後按enter鍵執行此命令
·寫加密金鑰兩次，然後 save it
·轉到檔案位置
在ISE上配置(id_rsa.pub)的檔案儲存庫資料夾中傳輸公鑰。

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

配置證書以登入ISE

使用下一個命令驗證公用檔案是否位於儲存庫下：

```
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
```

- 在許可權模式下使**(id_rsa.pub)**用命令匯入公鑰檔案：

```
crypto key import

        repository
```

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

- 進入全域性配置模式並使用命令：

```
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>
```

請使用命令驗證您在匯入公鑰時是否沒有任何錯誤。建議通過控制檯埠繼續操作，以避免失去對ISE的訪問。

驗證

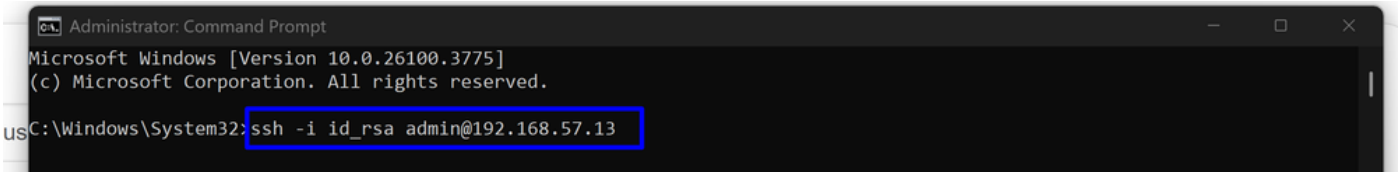
登入Windows

使用命令嘗試通過cmd訪問ISE:

```
ssh -i

        @


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



使用步驟在Windows中建立私鑰和公鑰中配置的加密金鑰進行身份驗證。

登入MacOS

在終端機中輸入以下命令：

```
ssh -i

        @


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

或

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

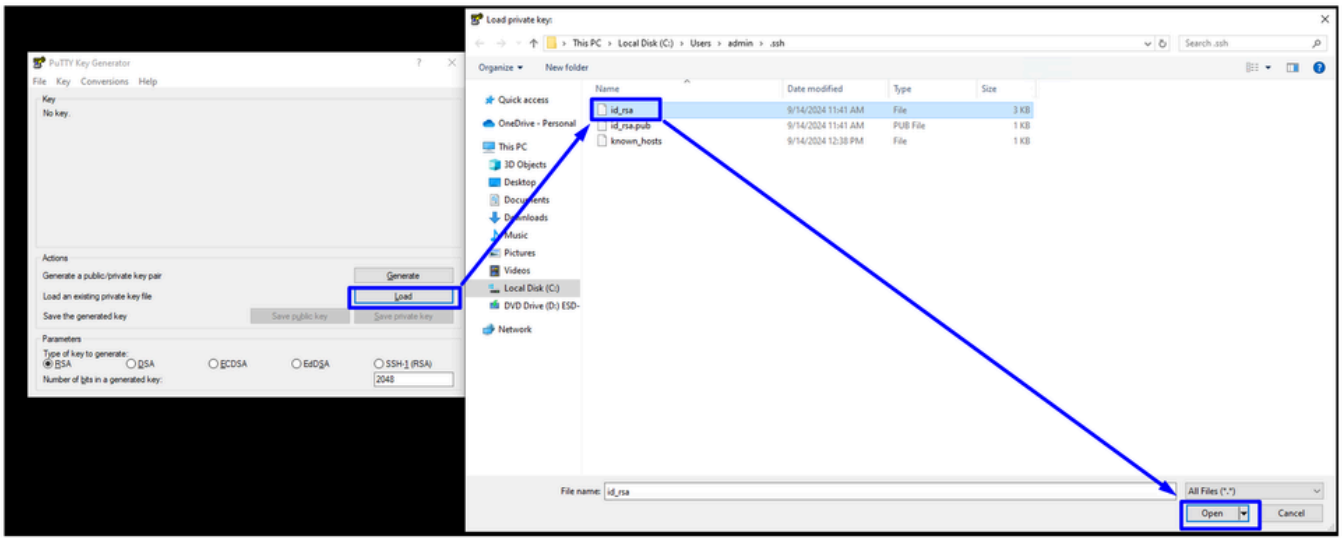
```
        @
```

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

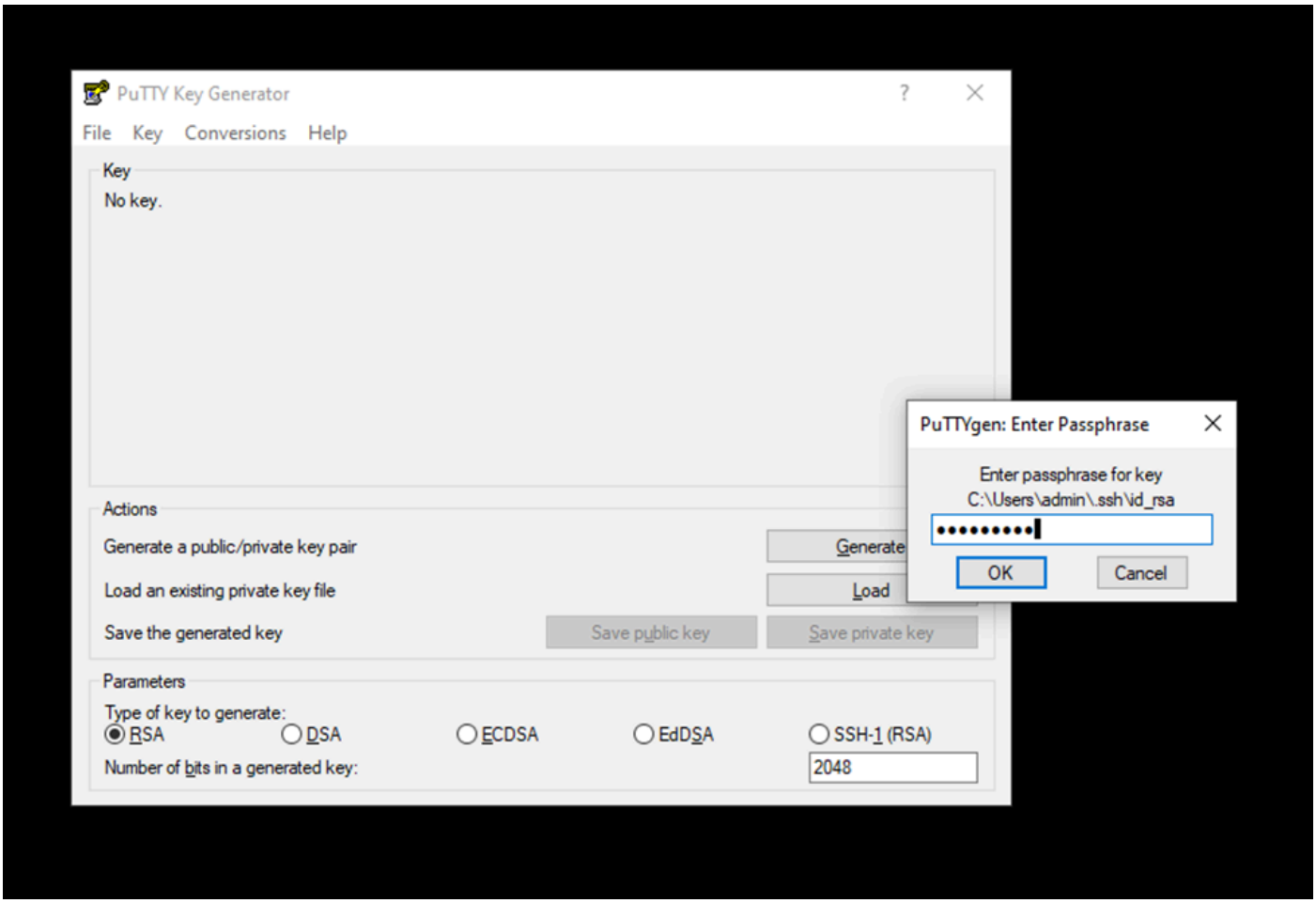
使用步驟在MacOS中通過建立私有金鑰和公鑰中配置的加密金鑰進行身份驗證。

登入Putty

打PuTTy key generator開（在開始搜尋欄中按PuttyGen搜尋），按一下「載入」，選擇所有檔案，然後開啟從cmd(Windows)或terminal(MacOS)生成的私鑰：

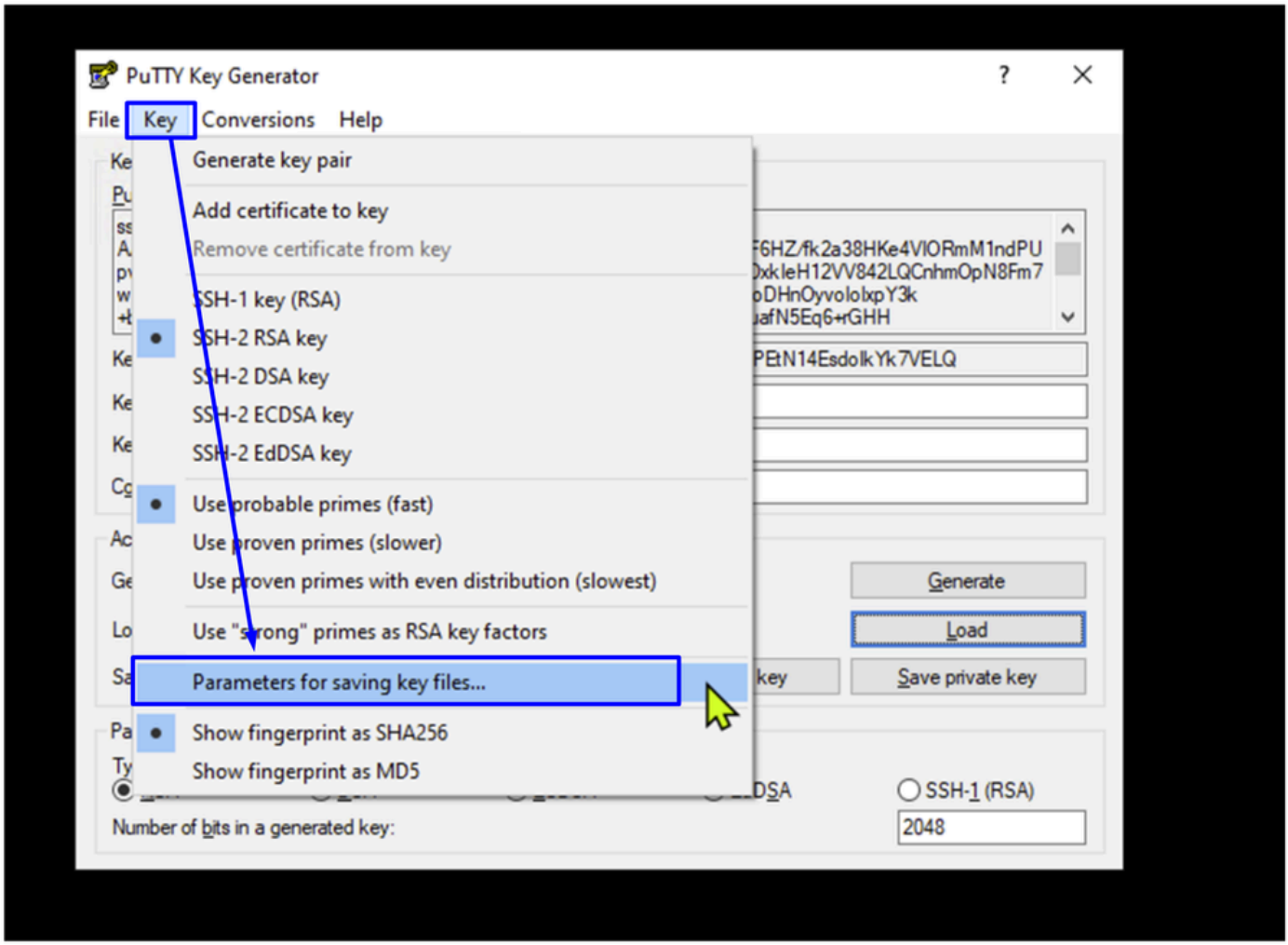


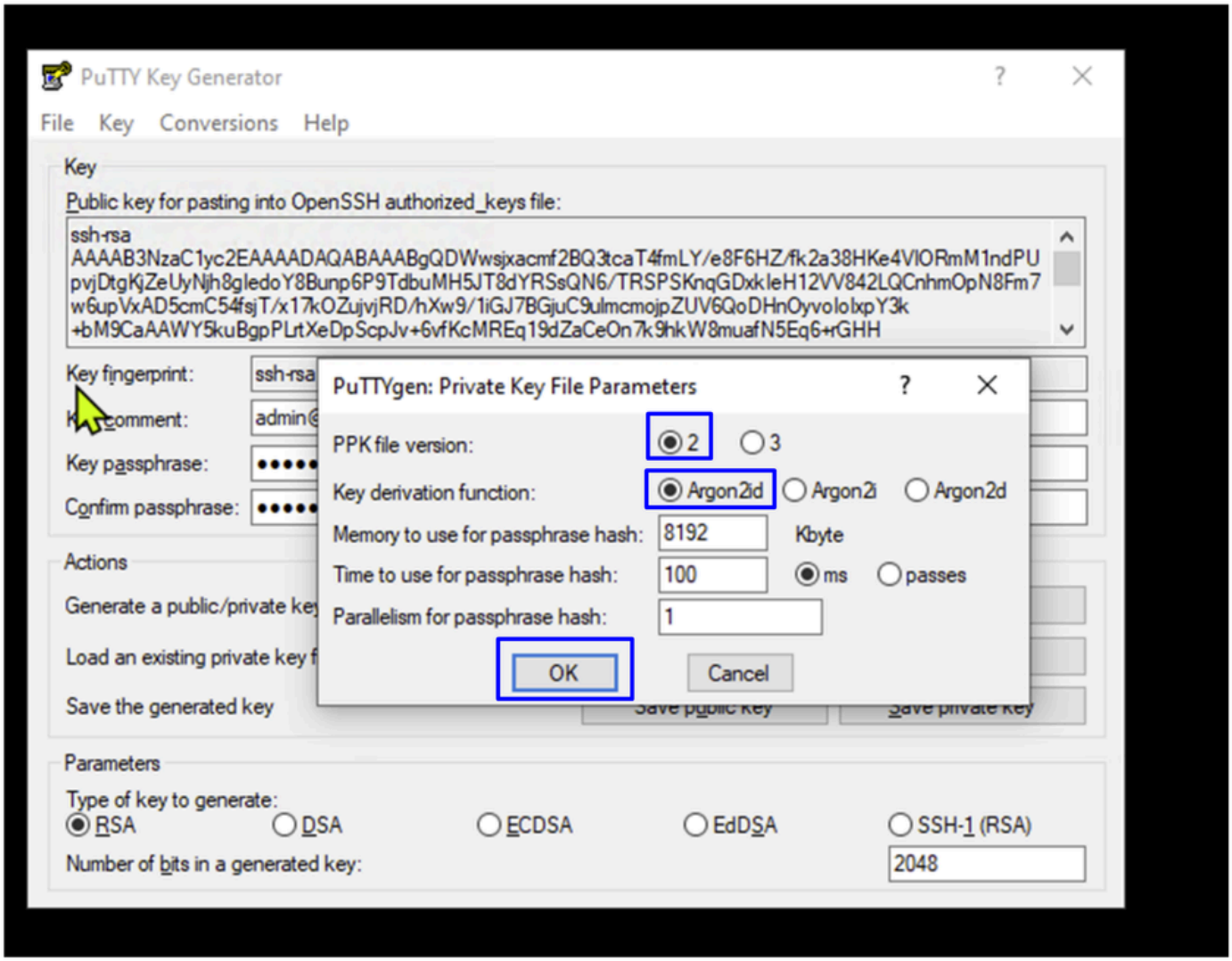
- 寫入以前在cmd或terminal中使用的加密金鑰



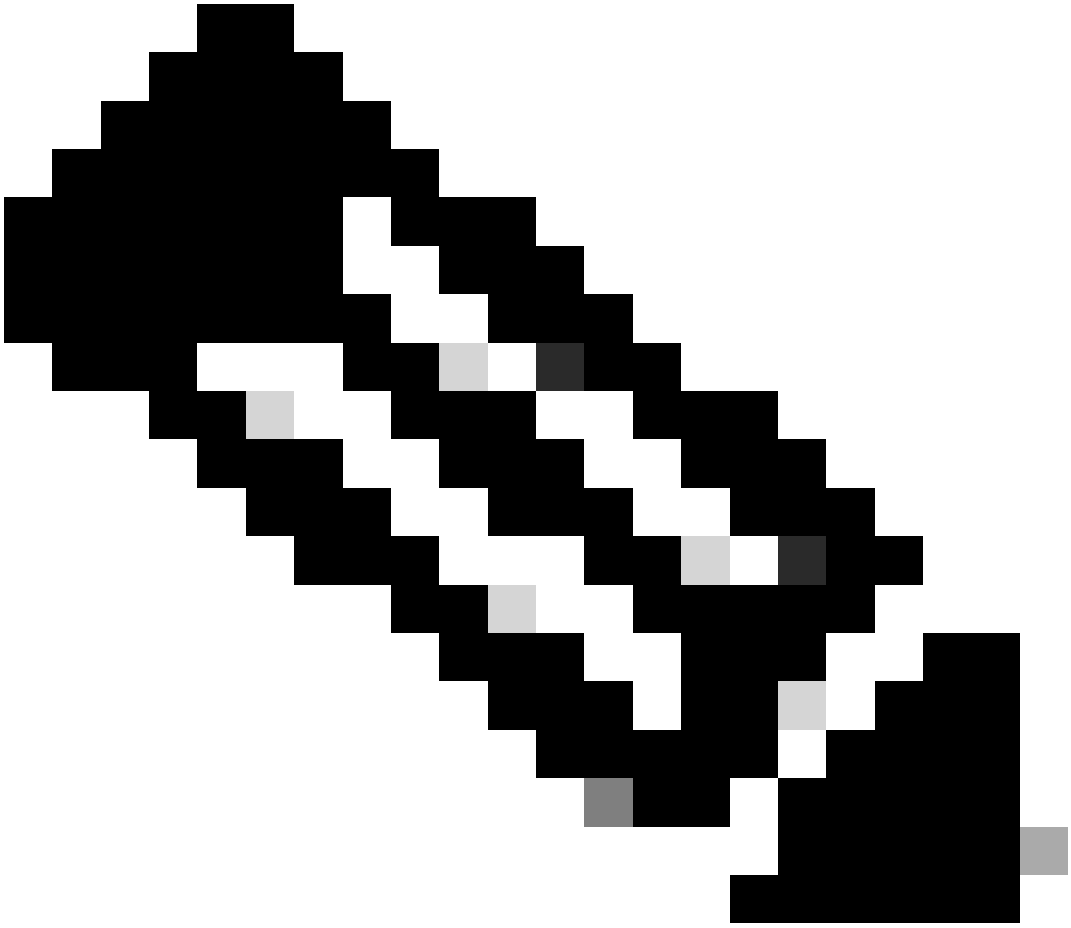
通過執行以下步驟，將此檔案轉換為相容的Putty版本：

- 按一下用於儲存金鑰檔案的金鑰>引數


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

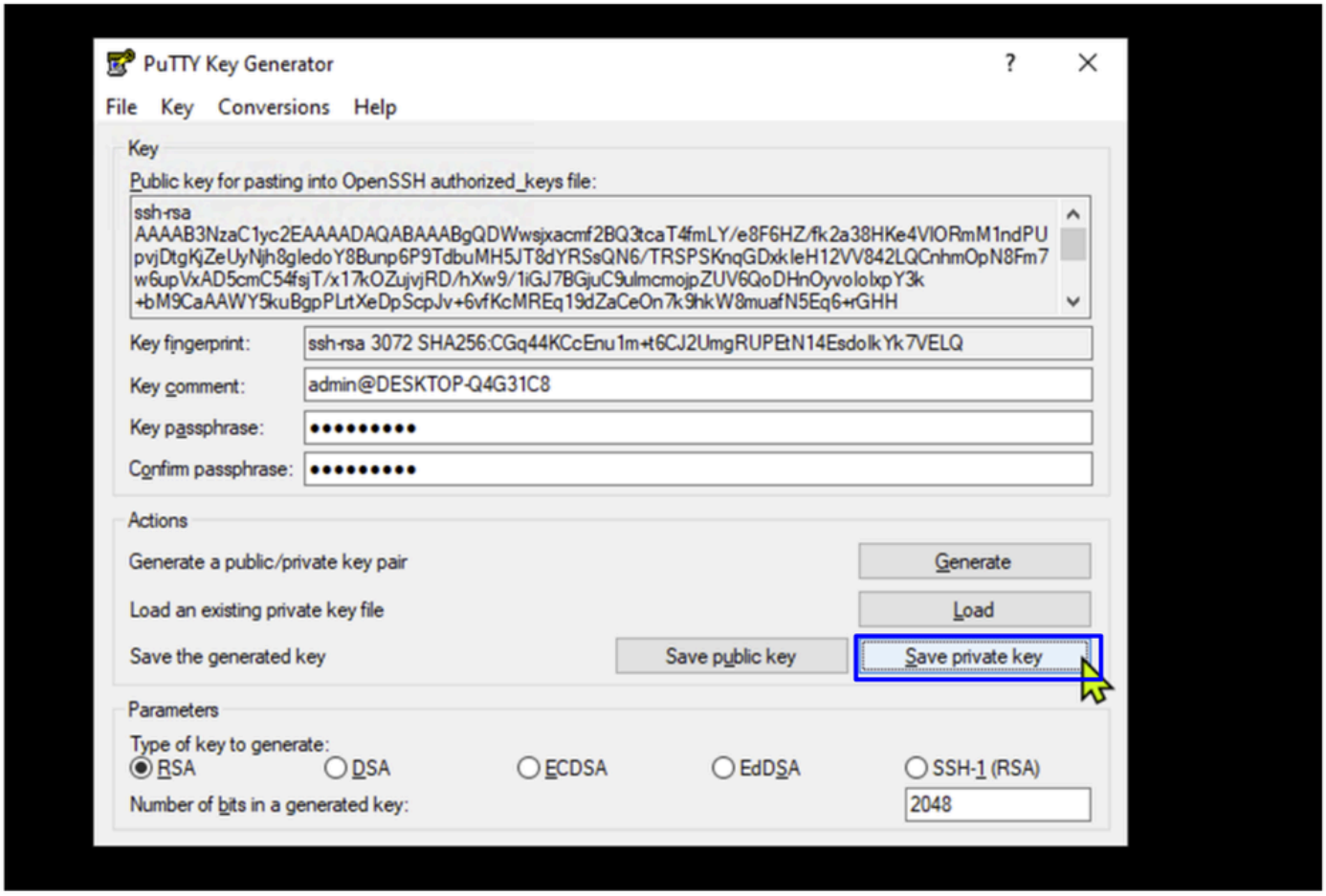


- PPK file version :選擇2
- **Key derivation function**:選擇Argon2id



附註：對於其餘引數，使用預設值。

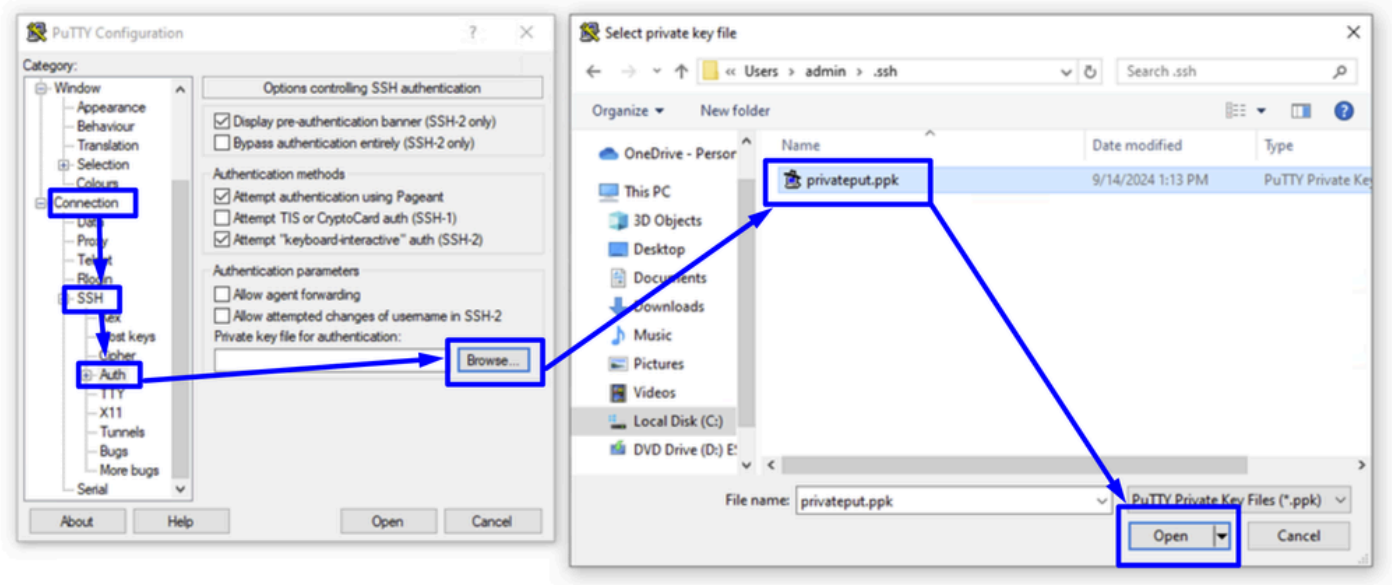
- 按一下 Ok



- 按一下 Save private Key

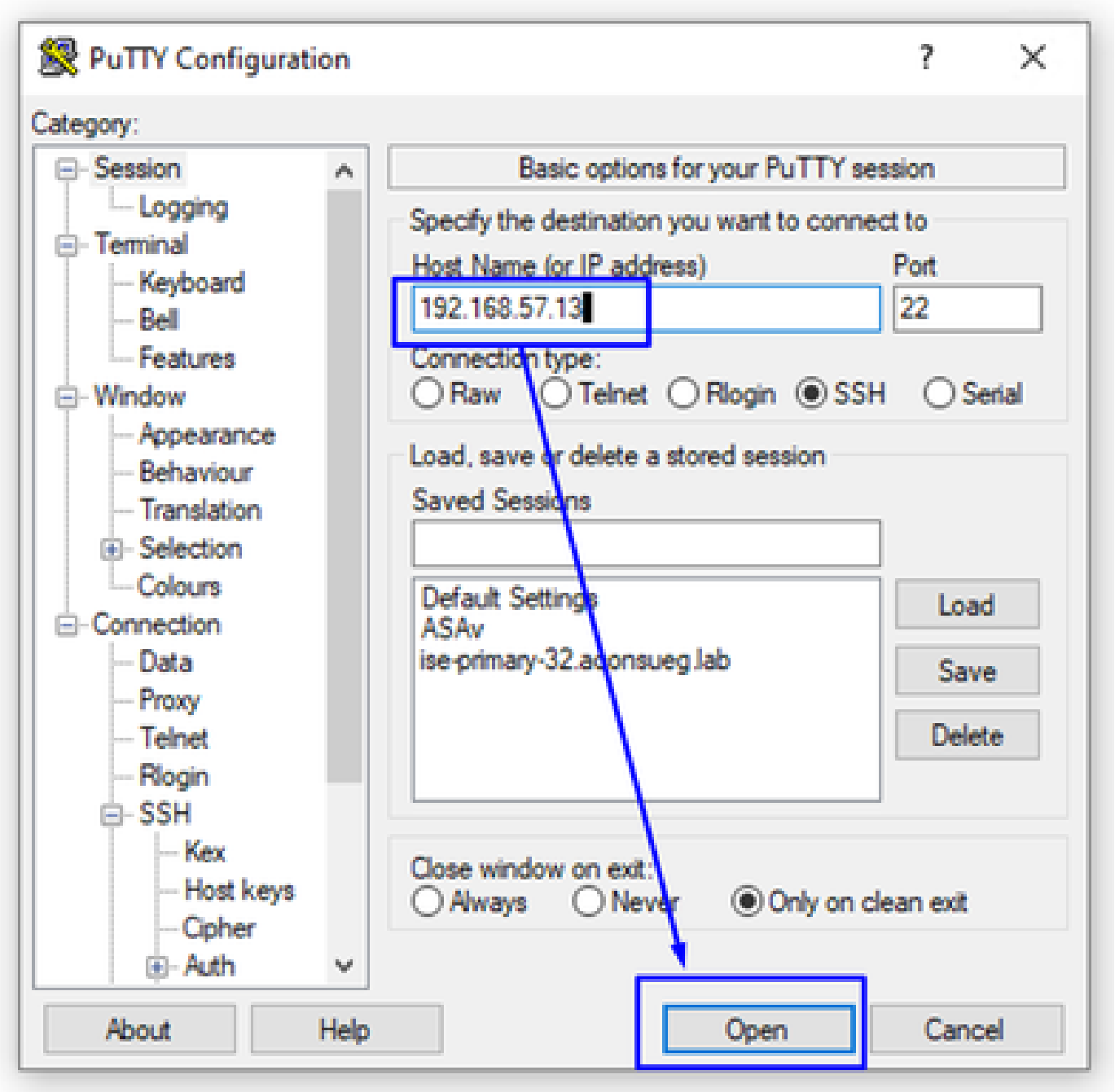
在電腦上儲存金鑰後，通過參考以下示例，即可使用該金鑰：

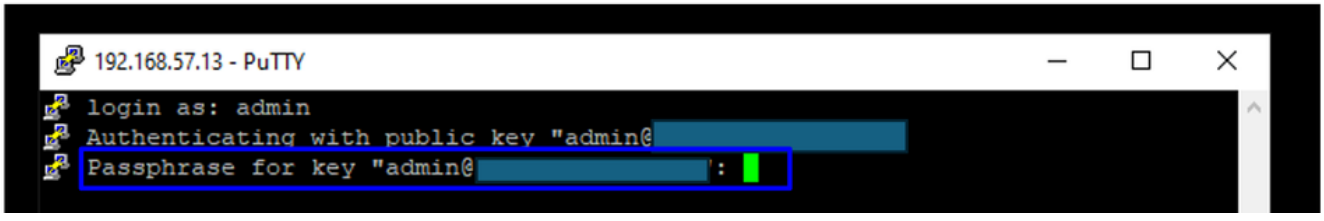
- 開放性膩子
- 按一**Connection** 下**> SSH > Auth > Browse**
- 選擇您的私鑰並按一下 Open



- 返回會話，設定ISE的IP地址或主機名(FQDN)

- 按一下「開啟」





使用步驟在MacOS中通過建立私鑰和公鑰或在Windows中建立私鑰和公鑰中配置的加密金鑰進行身份驗證。

疑難排解

檢查來自終端站點的錯誤消息，在ssh連線中新增標誌-v

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

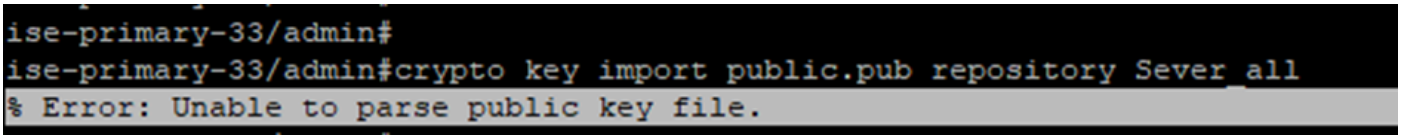
```
Example for MacOS:
ssh -v -i id_rsa admin@192.168.57.13
```

或

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

匯入公鑰時出錯

%錯誤：無法分析公鑰檔案。



如果您匯入多個公鑰時遇到任何不便，請聯絡思科支援人員。

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）。