Configurazione dell'autenticazione a chiave privata con ISE

Sommario

Introduzione

In questo documento viene descritto come creare una chiave SSH (Private Secure Shell) per l'autenticazione nella CLI con Identity Secure Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Repository in ISE.
- Autenticazione certificato.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ISE 3.3 patch 3
- Windows 10
- MacOS X

- Putty client SSH

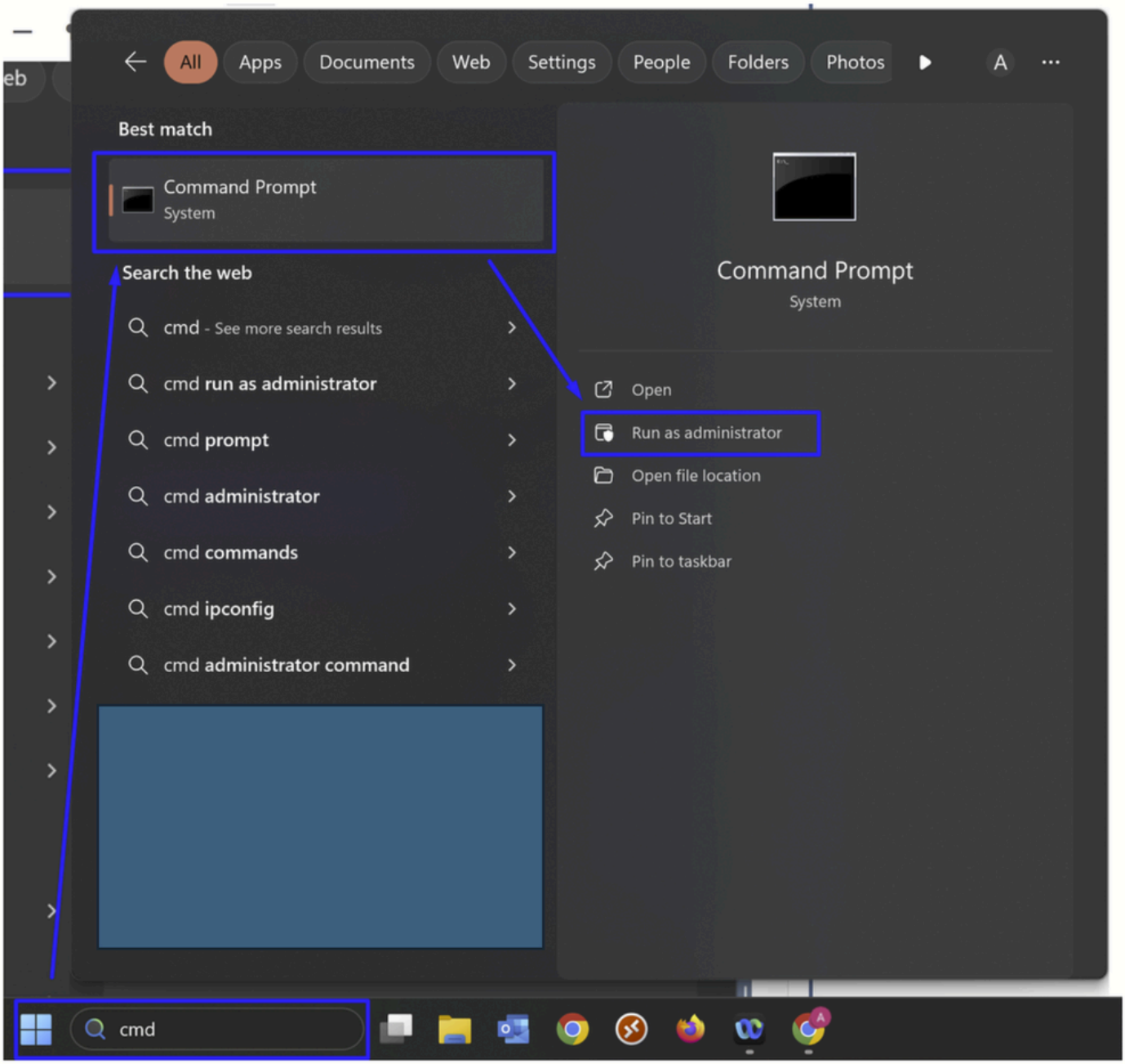
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Creare le chiavi pubbliche e private in Windows

Fare clic sull'icona Cerca nella barra delle applicazioni:

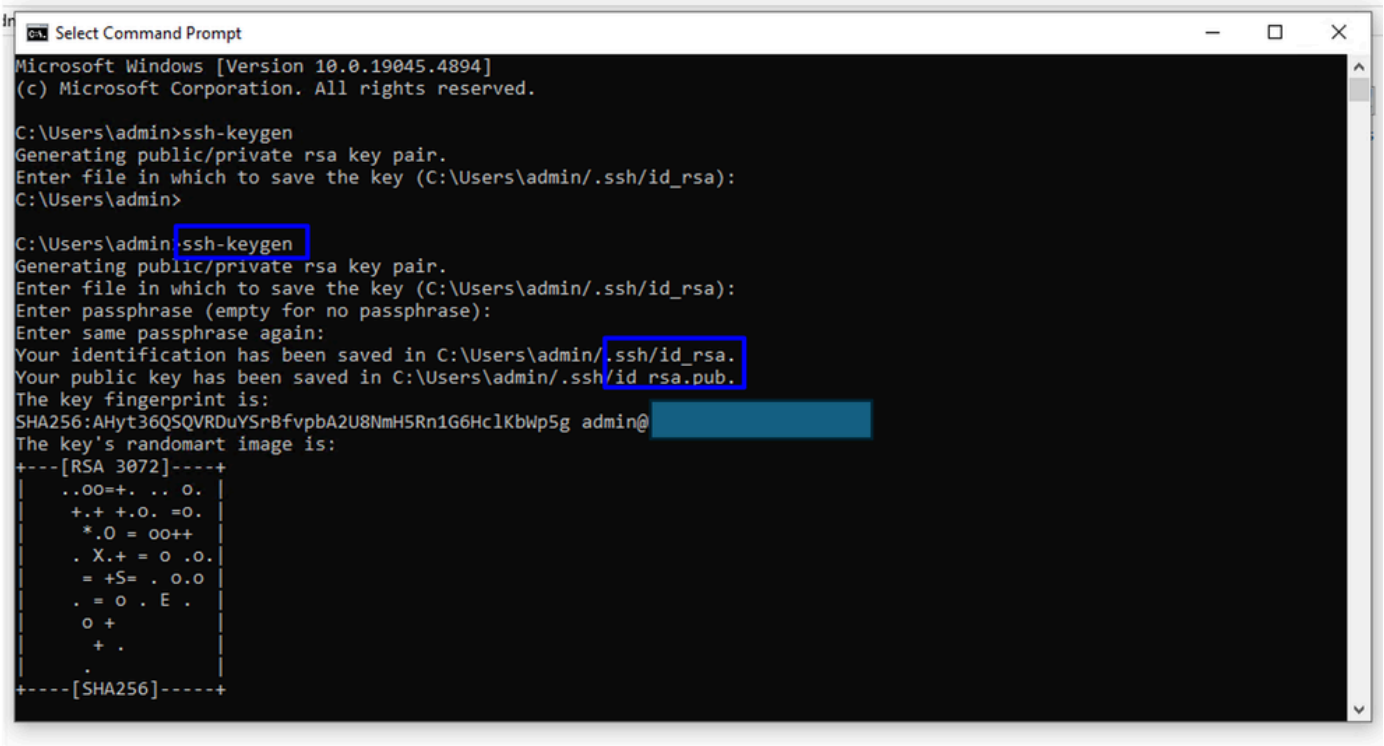
· Digitare cmd nella barra di ricerca
· Nei risultati della ricerca, fare clic con il pulsante destro del mouse sul prompt dei comandi e selezionare Esegui come amministratore. In questo modo si è certi di disporre delle autorizzazioni necessarie per eseguire i comandi



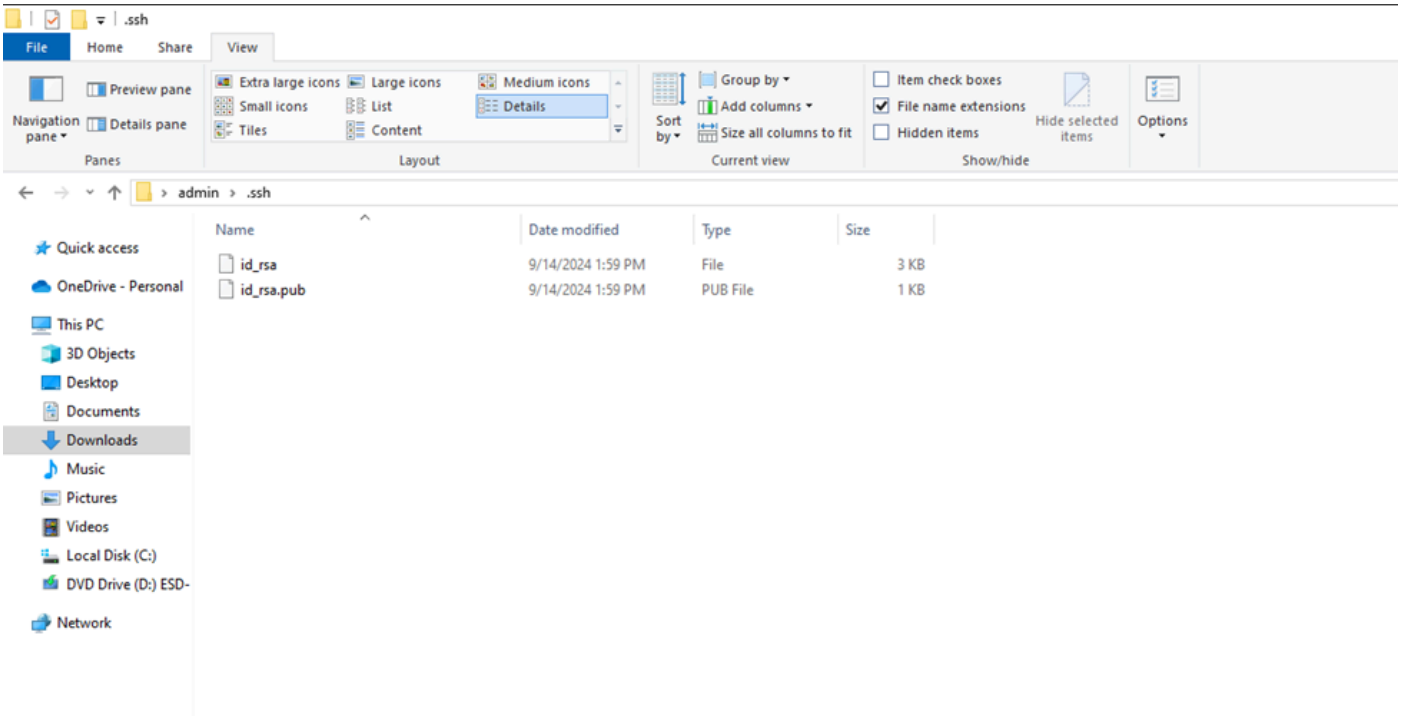
· Eseguire il comando successivo:

```
ssh-keygen
```

- Verrà richiesto di immettere la chiave di crittografia due volte. Salvarlo, perché la password deve essere autenticata con ISE come nuova password. In seguito, vengono creati due file, le chiavi private (id_rsa) e pubbliche (id_rsa.pub). Salvare i file in una directory. Ad esempio, è stato utilizzato quello predefinito



- Verificare dove sono archiviati i file



Trasferire la chiave pubblica **(id_rsa.pub)** nella cartella del repository dei file configurata con ISE.

Creare le chiavi pubbliche e private tramite in MacOS

Fare clic sull' **Finder** icona situata nel dock
· Passare alla **Applications folder**

· All'interno della cartella **Applications folder**, individuare e aprire la cartella Utilities
· Nell'elenco Utilità, individuare **Terminal**
· Fare doppio clic su **Terminal** per aprirlo
· Nella **Terminal** finestra, digitare "ssh-keygen -t rsa" e premere il tasto Invio per eseguirlo
· Scrivere la chiave di crittografia due volte e **save it**
· Vai alla posizione dei file
Trasferire la chiave pubblica **(id_rsa.pub)** nella cartella del repository dei file configurata con 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 .        |
+-----------------+
```

Configurazione del certificato per l'accesso ad ISE

Verificare se il file pubblico si trova nel repository utilizzando il comando seguente:

```
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
```

- Importare il file di chiave pubblica **(id_rsa.pub)** utilizzando il comando in modalità di esecuzione privilegiata:

```
crypto key import

        repository
```

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

- Accedere alla modalità di configurazione globale e utilizzare il 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>
```

Utilizzare il comando per verificare che non vengano restituiti errori durante l'importazione della chiave pubblica. Si consiglia di procedere con questa operazione tramite la porta console per evitare di perdere l'accesso all'ISE.

Verifica

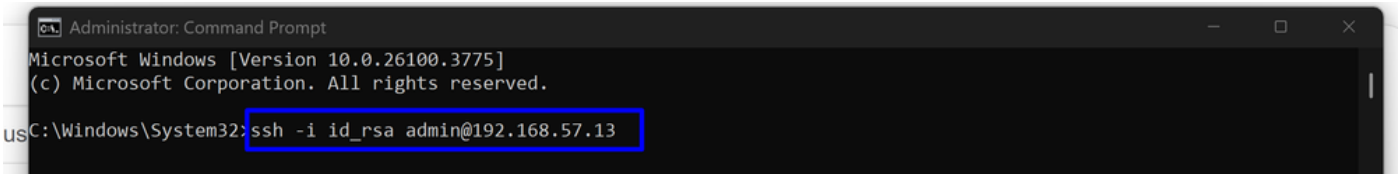
Accesso a Windows

Provare ad accedere all'ISE tramite **cmd** il comando:

```
ssh -i

        @


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



Utilizzare la chiave di crittografia configurata nel passaggio Creare le chiavi pubblica e privata in Windows per l'autenticazione.

Accesso a MacOS

Immettere questo comando nel terminale:

```
ssh -i

        @
```

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

o

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

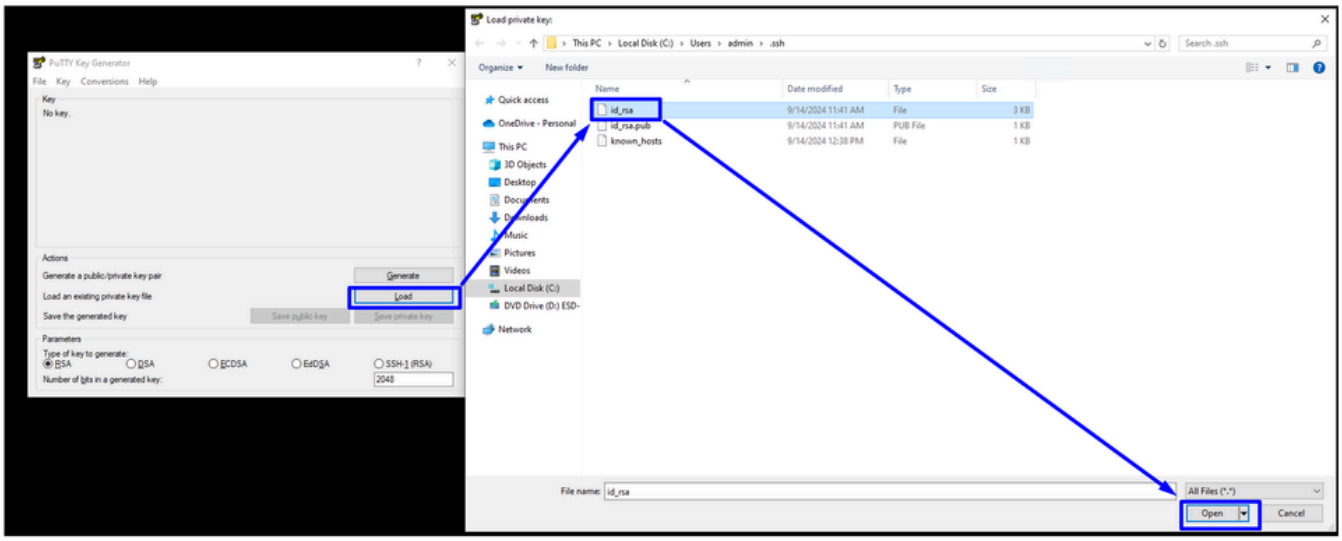
```
        @
```

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

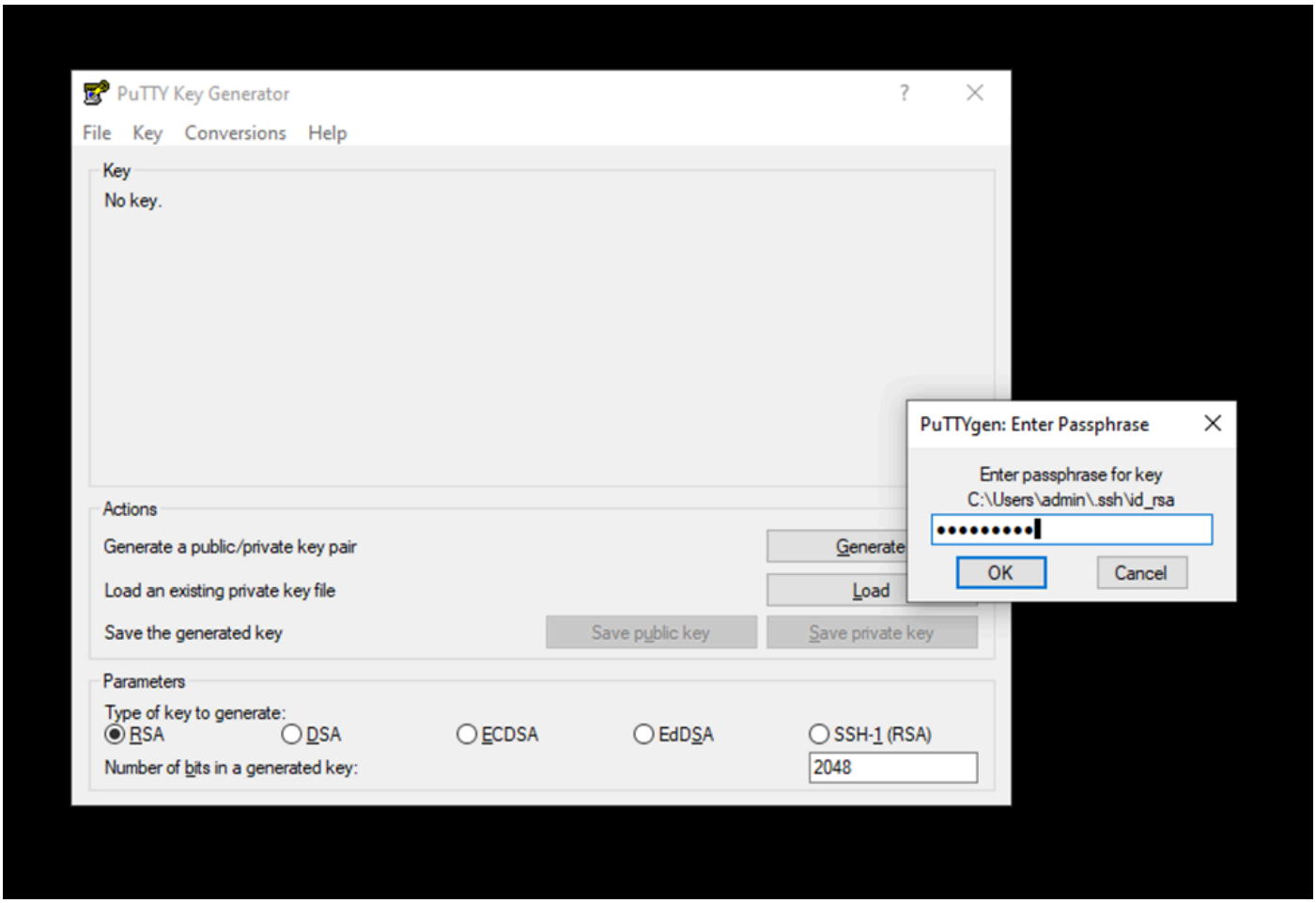
Utilizzare la chiave di crittografia configurata nel passaggio Creare le chiavi pubbliche e private tramite in MacOS per eseguire l'autenticazione.

Login Putty

Aprire PuTTy key generator (ricerca per PuttyGen nella barra di ricerca iniziale), fare clic su Carica, selezionare tutti i file e aprire la chiave privata generata da cmd (Windows) o terminale (MacOS):

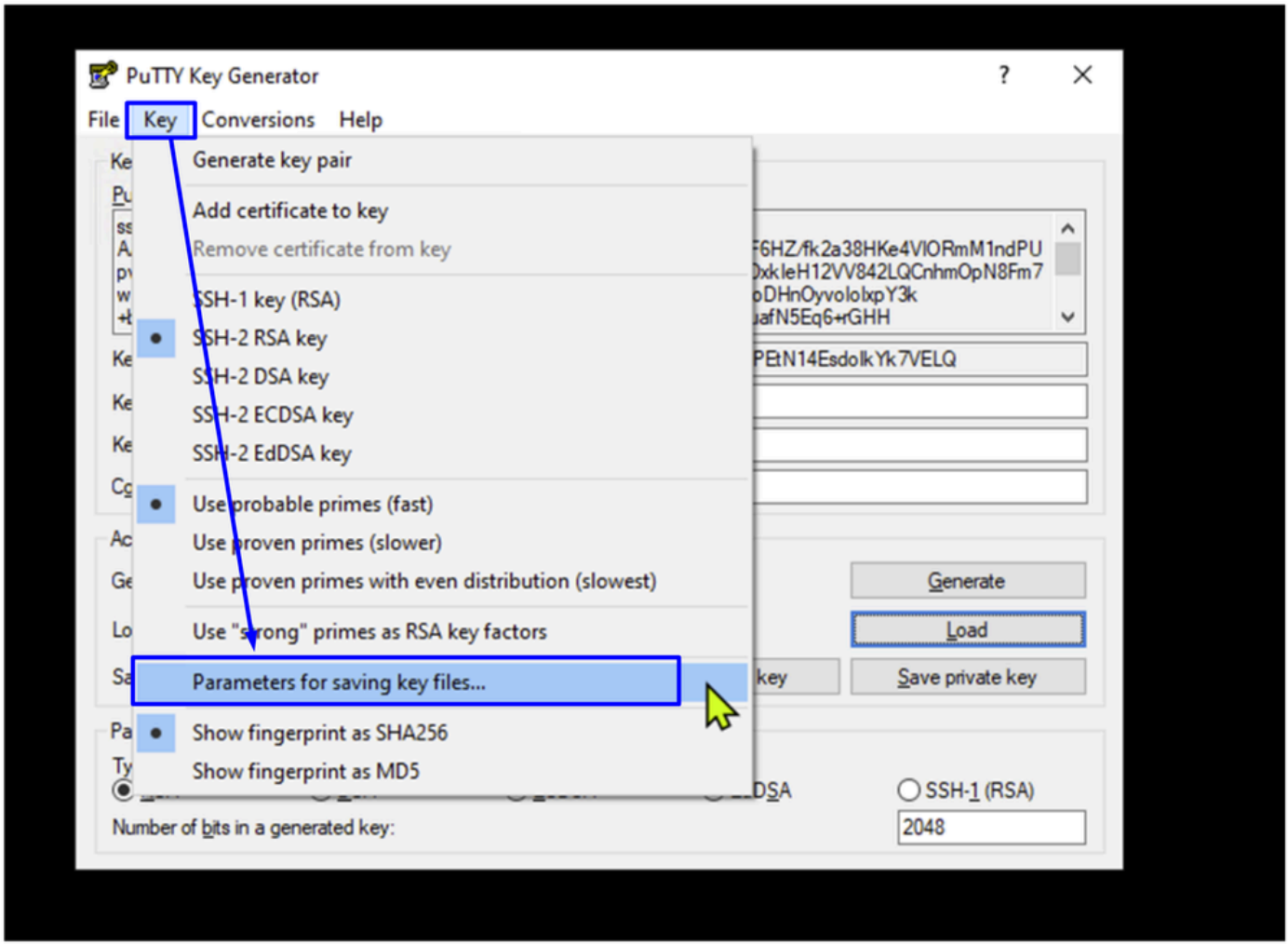


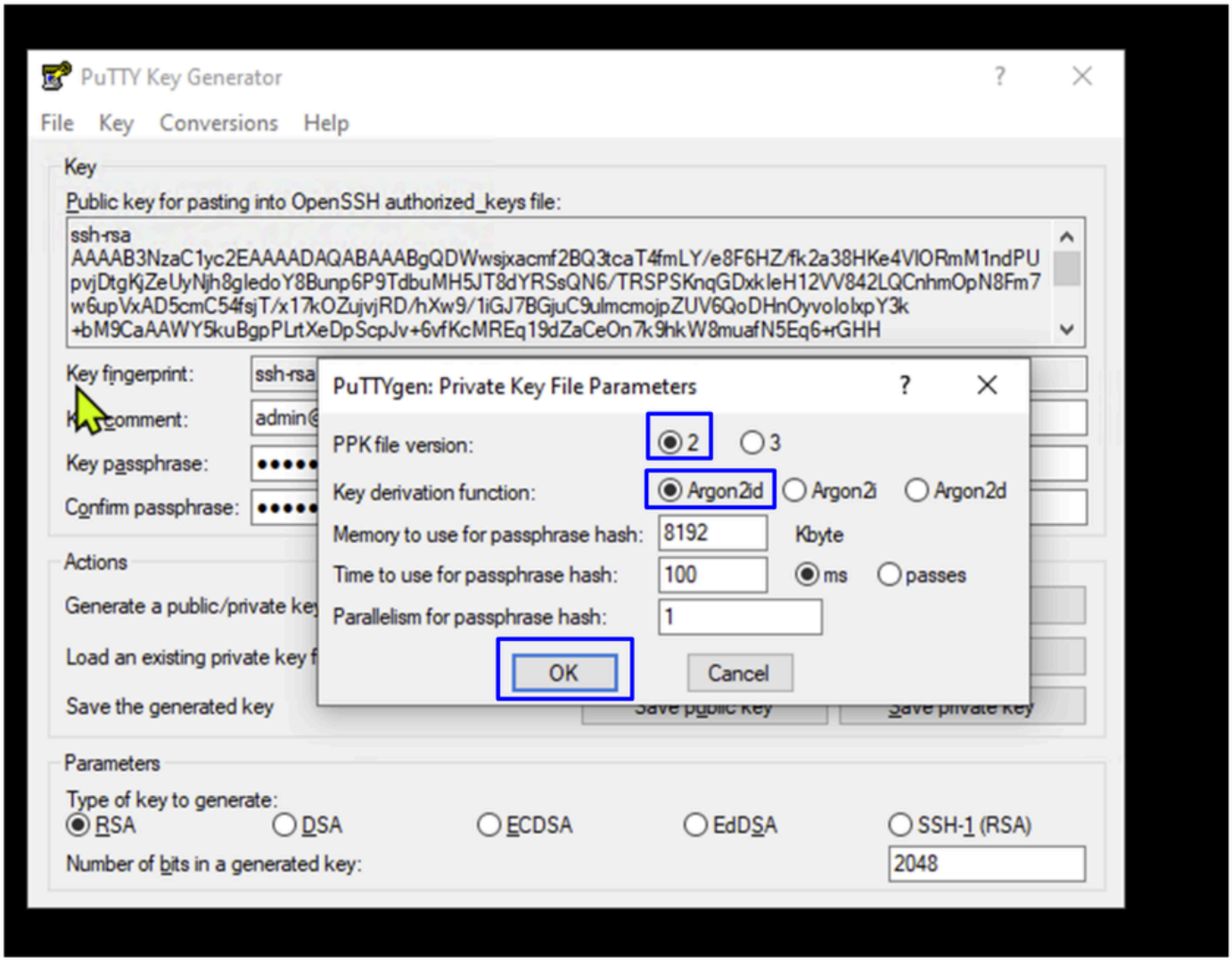
- Scrivere la chiave di crittografia utilizzata in precedenza nel comando o nel terminale



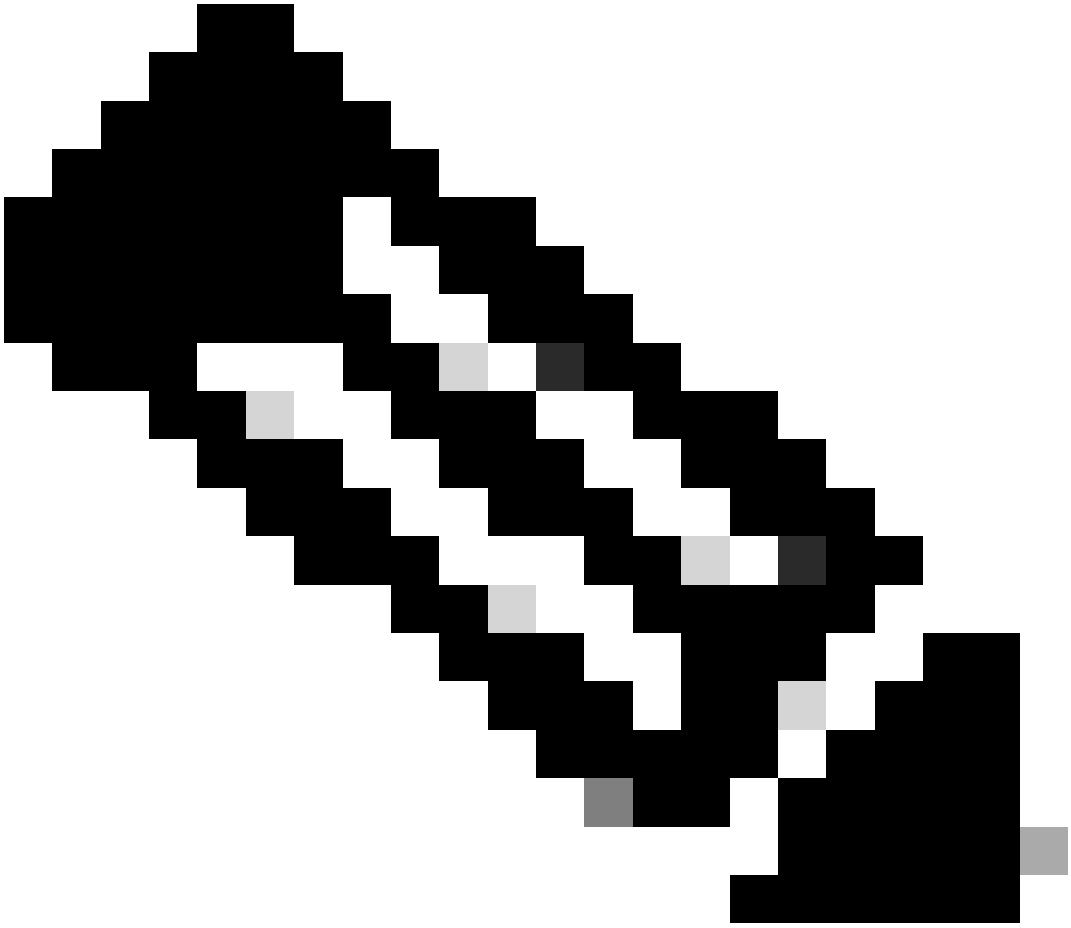
Convertire questo file in una versione Putty compatibile eseguendo i passaggi seguenti:

- Fare clic su Chiave > Parametri per il salvataggio dei file di chiave


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

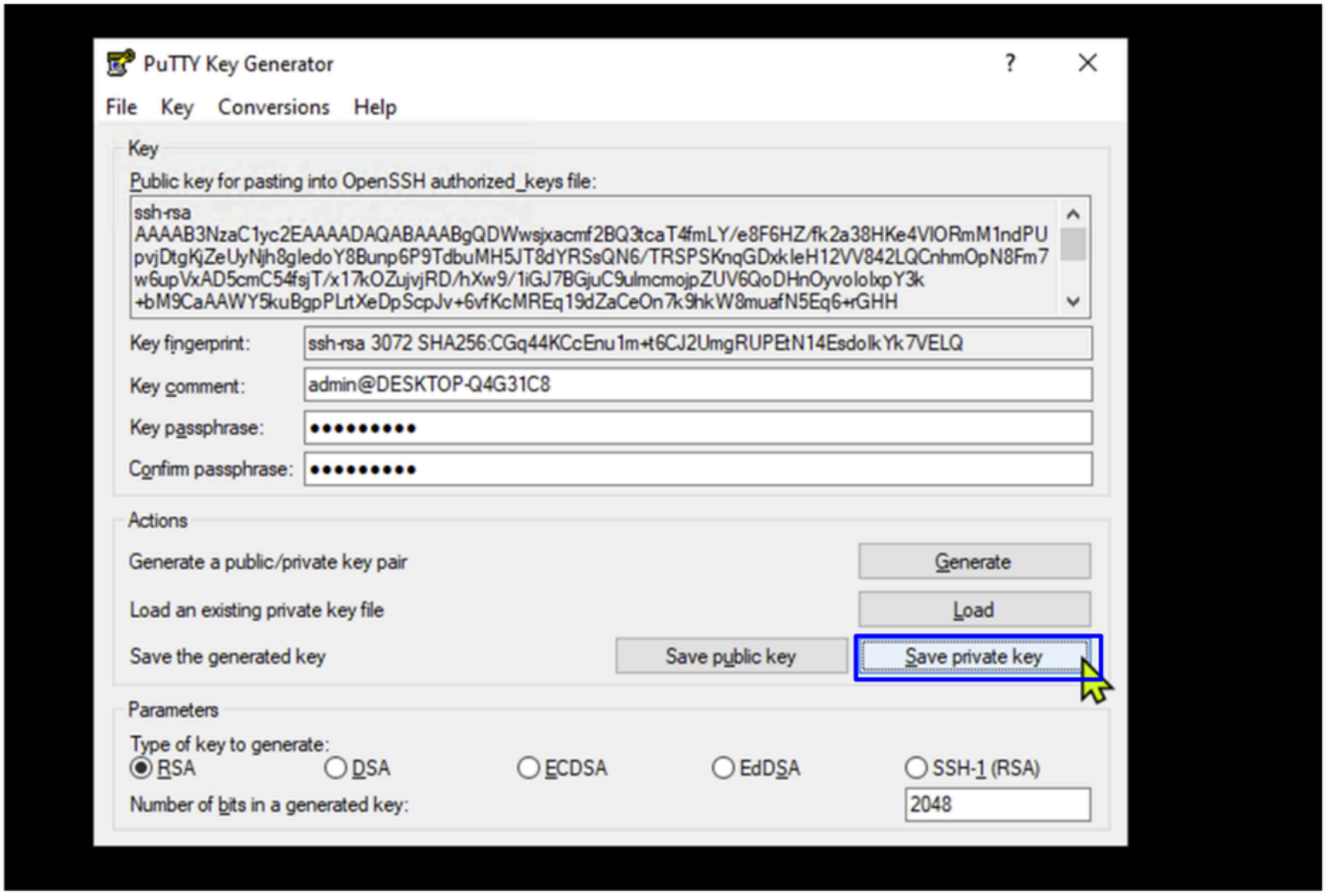


- PPK file version : Scegliere 2
- **Key derivation function**: Scegliere Argon2id



Nota: Per gli altri parametri, utilizzate i valori di default.

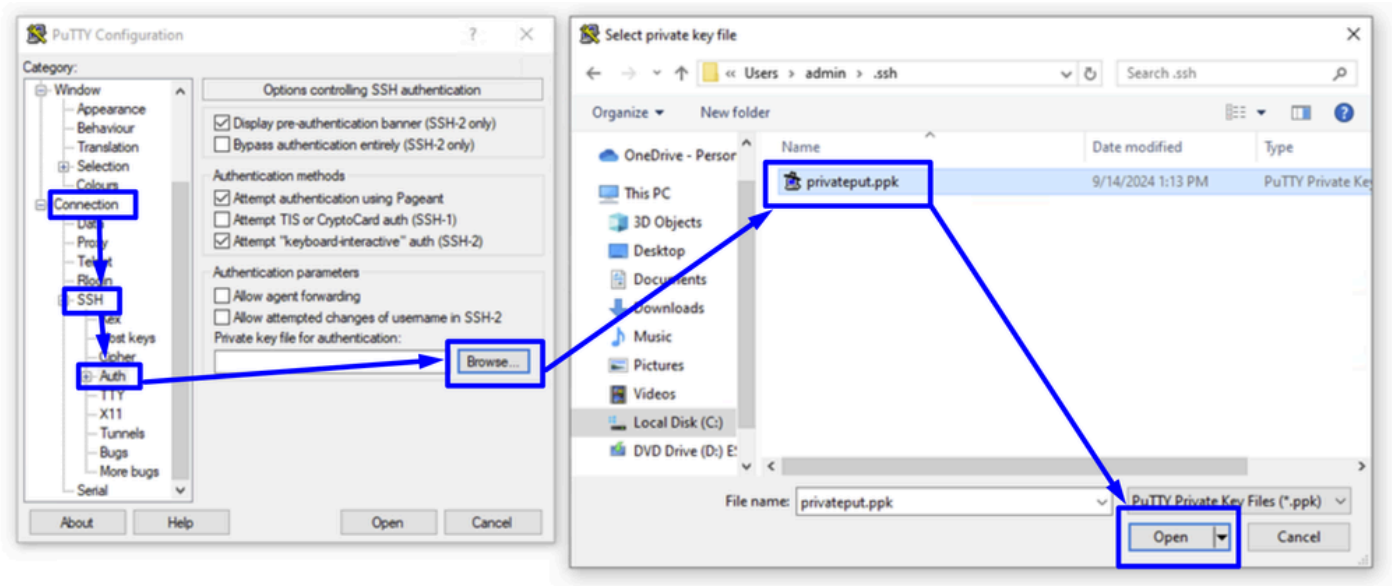
- Fare clic su Ok



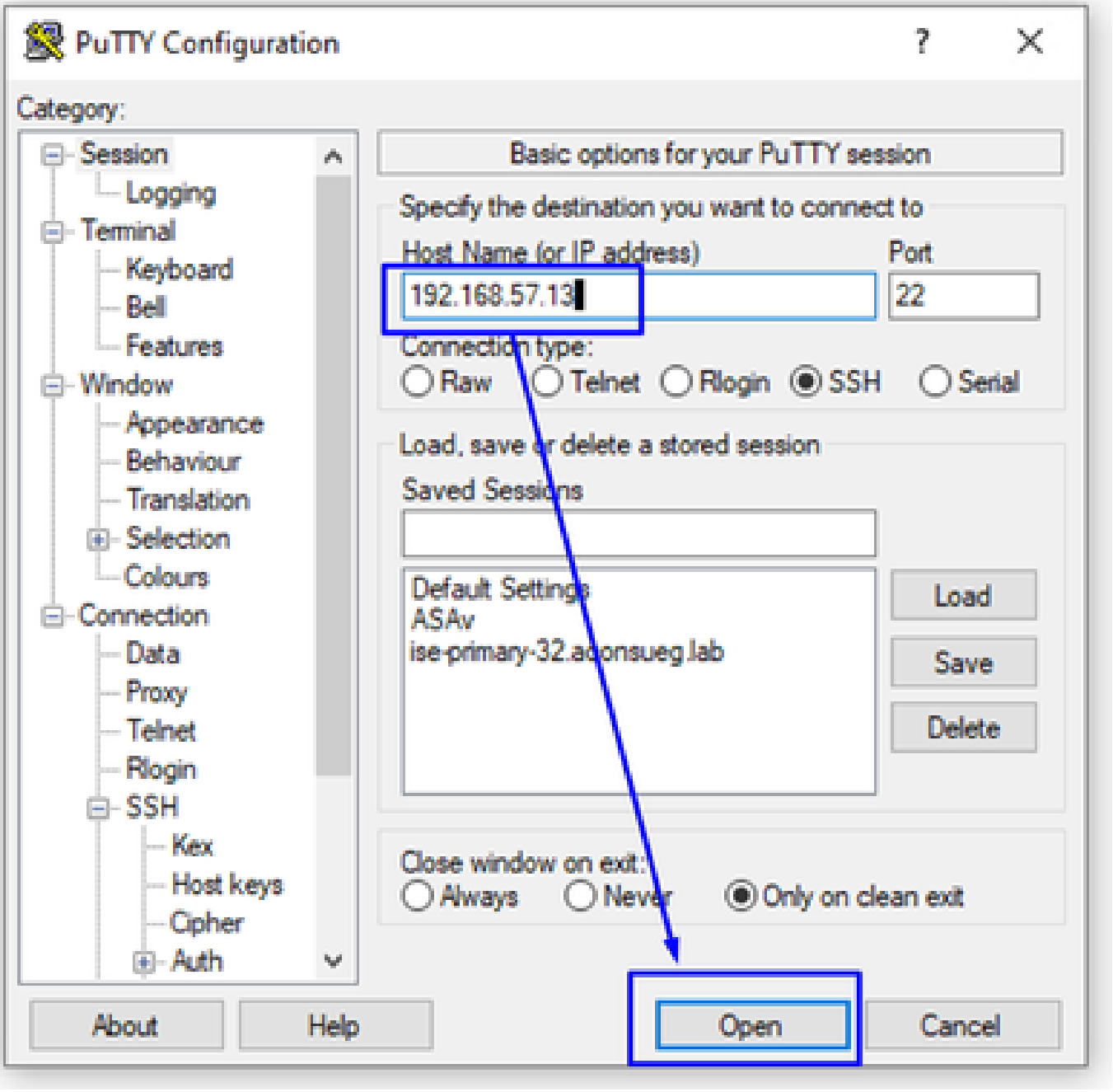
- Fare clic su Save private Key

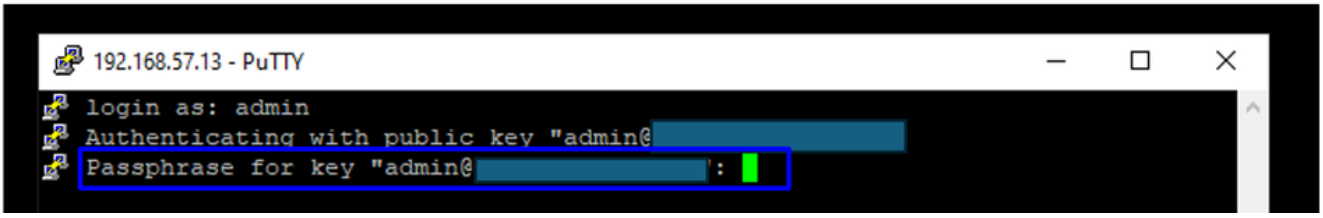
Dopo aver salvato la chiave nel computer, è possibile utilizzarla facendo riferimento agli esempi seguenti:

- Apri Putty
- Fare clic su **Connection > SSH > Auth > Browse**
- Selezionare la chiave privata e fare clic su Open



- Torna alla sessione, imposta l'indirizzo IP o il nome host (FQDN) dell'ISE
- Fare clic su Apri





Utilizzare la chiave di crittografia configurata nel passaggio Creare le chiavi pubblica e privata tramite in MacOS o Creare le chiavi pubblica e privata in Windows per l'autenticazione.

Risoluzione dei problemi

Estrai messaggi di errore dal sito endpoint aggiungendo nella connessione ssh il contrassegno -v

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

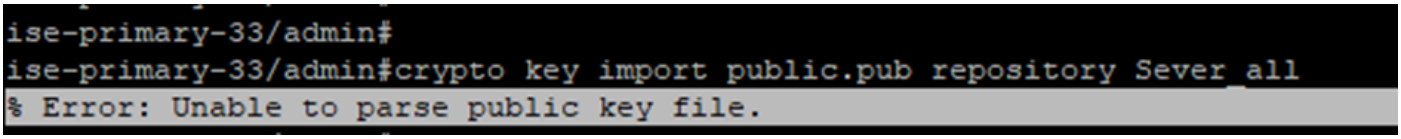
```
Example for MacOS:
ssh -v -i id_rsa admin@192.168.57.13
```

o

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

Errore di importazione della chiave pubblica

Errore %: Impossibile analizzare il file della chiave pubblica.



In caso di problemi durante l'importazione di più chiavi pubbliche, contatta il supporto Cisco.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).