

Accesso alla CLI di AMP Private Cloud tramite SSH e trasferimento di file tramite SCP

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Generare una coppia di chiavi RSA utilizzando PuTTY](#)

[Generare una coppia di chiavi RSA utilizzando Linux/Mac](#)

[Aggiunta delle chiavi pubbliche generate al portale di amministrazione AMP Private Cloud](#)

[Usare la coppia di chiavi generata per collegare il protocollo SSH all'accessorio con PuTTY](#)

[Uso della coppia di chiavi configurata per SSH nell'accessorio con Linux](#)

[Utilizzo di WinSCP per interagire con il file system di AMP Private Cloud](#)

Introduzione

Questo documento descrive la procedura per generare una coppia di chiavi SSH utilizzando PuTTY e una shell Linux, aggiungerla ad AMP e quindi accedere alla CLI. AMP Private Cloud appliance usa l'autenticazione basata su certificato per SSH nell'appliance. Di seguito viene descritta la procedura per generare rapidamente una coppia di chiavi per accedere alla CLI e interagire con il file system tramite SCP (WinSCP).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- PuTTY
- WinSCP
- Linux/Mac Shell

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

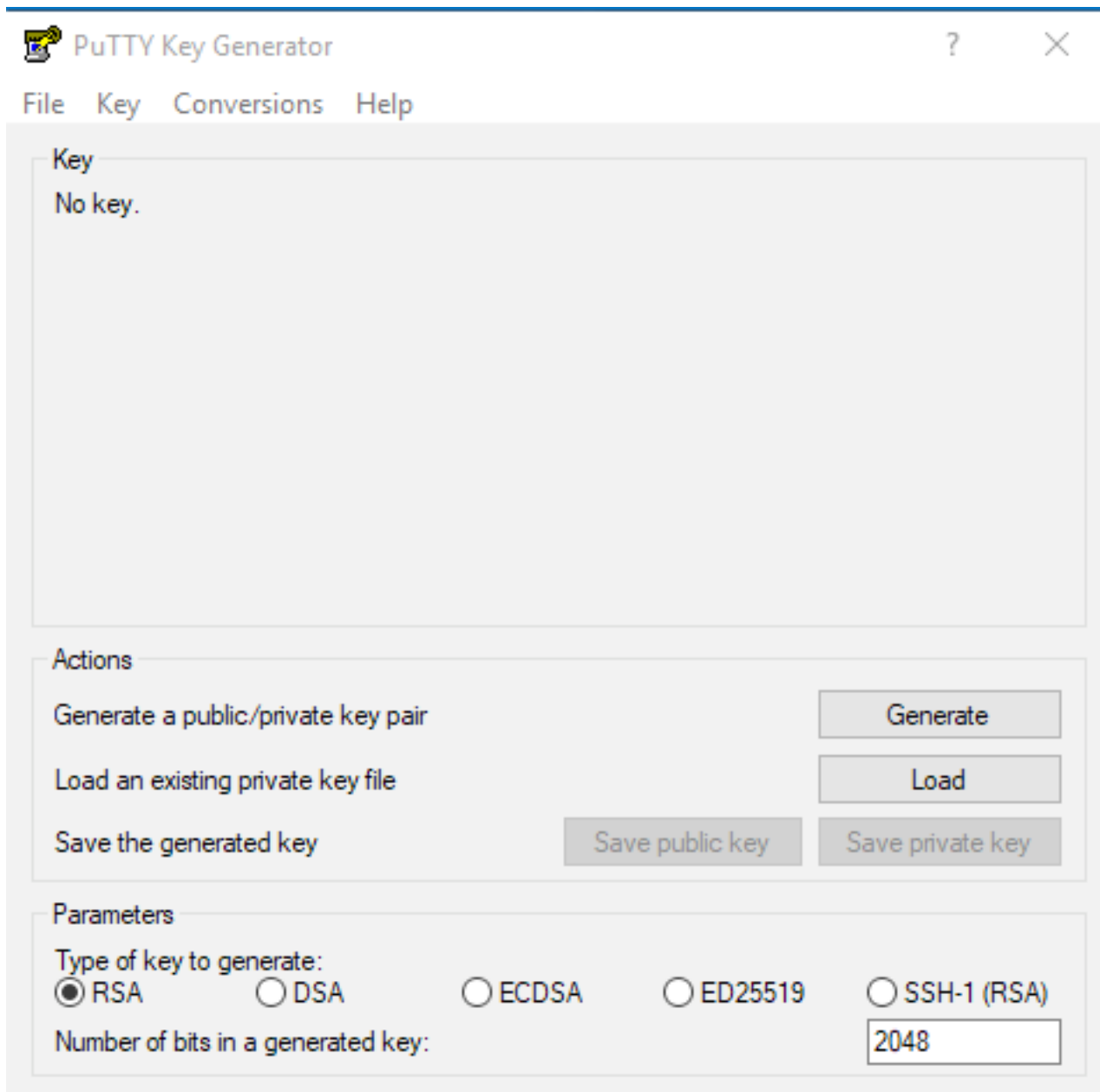
Configurazione

Il primo passo prevede la generazione di una coppia di chiavi RSA utilizzando PuTTY o la shell Linux. In seguito, la chiave pubblica deve essere aggiunta e considerata attendibile da AMP Private Cloud Appliance.

Generare una coppia di chiavi RSA utilizzando PuTTY

Passaggio 1. Verificare di aver installato completamente PuTTY.

Passaggio 2. Avviare PuTTYGen che viene installato insieme a PuTTY per generare la coppia di chiavi RSA.



Passaggio 3. Fare clic su Genera per e spostare il cursore in modo casuale per completare la generazione della coppia di chiavi.

Passaggio 4. Scegliere "Salva chiave pubblica" e "Salva chiave privata" da utilizzare nelle sezioni successive, come mostrato nell'immagine qui.



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQBan/DDbg8zkYWhaMfq0ilV1GcWLL7cfgvj8ajlpb
K3+2mXorinr4YP8S+oDsxN/b6QV899kC7z3sQevpXxC9sCiGuh+nvBWAunF
+69l2K7lDuVyqhfclH/vv5WPHJKaC47BqdWs+AuDrcCUqoDWOrHREWy
+ShZ8GII0vxxenlin5yY3IUjm8B9xmsPY/norzytm
```

Key fingerprint: ssh-rsa 2047 32:c3:07:60:8f:e4:75:e6:2d:b1:b4:1d:21:18:43:cb

Key comment: rsa-key-20190410

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair

Generate

Load an existing private key file

Load

Save the generated key

Save public key

Save private key

Parameters

Type of key to generate:

 RSA DSA ECDSA ED25519 SSH-1 (RSA)

Number of bits in a generated key:

2048

Passaggio 5. Aprire la chiave pubblica con il Blocco note in quanto il formato deve essere modificato per essere accettato nel portale di amministrazione del cloud privato di AMP.

AMP-VPC - Notepad

|---- BEGIN SSH2 PUBLIC KEY ----

Comment: "rsa-key-20190410"

```
AAAAB3NzaC1yc2EAAAABJQAAAQBan/DDbg8zkYWhaMfq0ilV1GcWLL7cfgvj8ajl
pbK3+2mXorinr4YP8S+oDsxN/b6QV899kC7z3sQevpXxC9sCiGuh+nvBWAunF+16
9l2K7lDuVyqhfclH/vv5WPHJKaC47BqdWs+AuDrcCUqoDWOrHREWy+ShZ8GII0vx
xenIin5yY3IUjm8B9xmsPY/norzytm+Wh6h0HdQtfgYBAj6TxGbcdK5VcLFaxbMB
CR8cEMx2yW6lUb2DSUwL78eDkFRhf1VWey07HbQ5zm/KPkijNXFCrk9BAmVXvPW4
w5FZSKKYQJgns1pjggcmpPbR879ib1xz7neUG+ktj16T4G3p
```

---- END SSH2 PUBLIC KEY ----

Passaggio 6. Rimuovere le prime due righe che iniziano con "—BEGIN" e l'ultima riga che inizia con "—END"

Passaggio 7. Rimuovere tutte le interruzioni di riga per rendere continuo il contenuto della chiave pubblica.

Passaggio 8. Inserire la parola "ssh-rsa" all'inizio del file. Salvare il file.

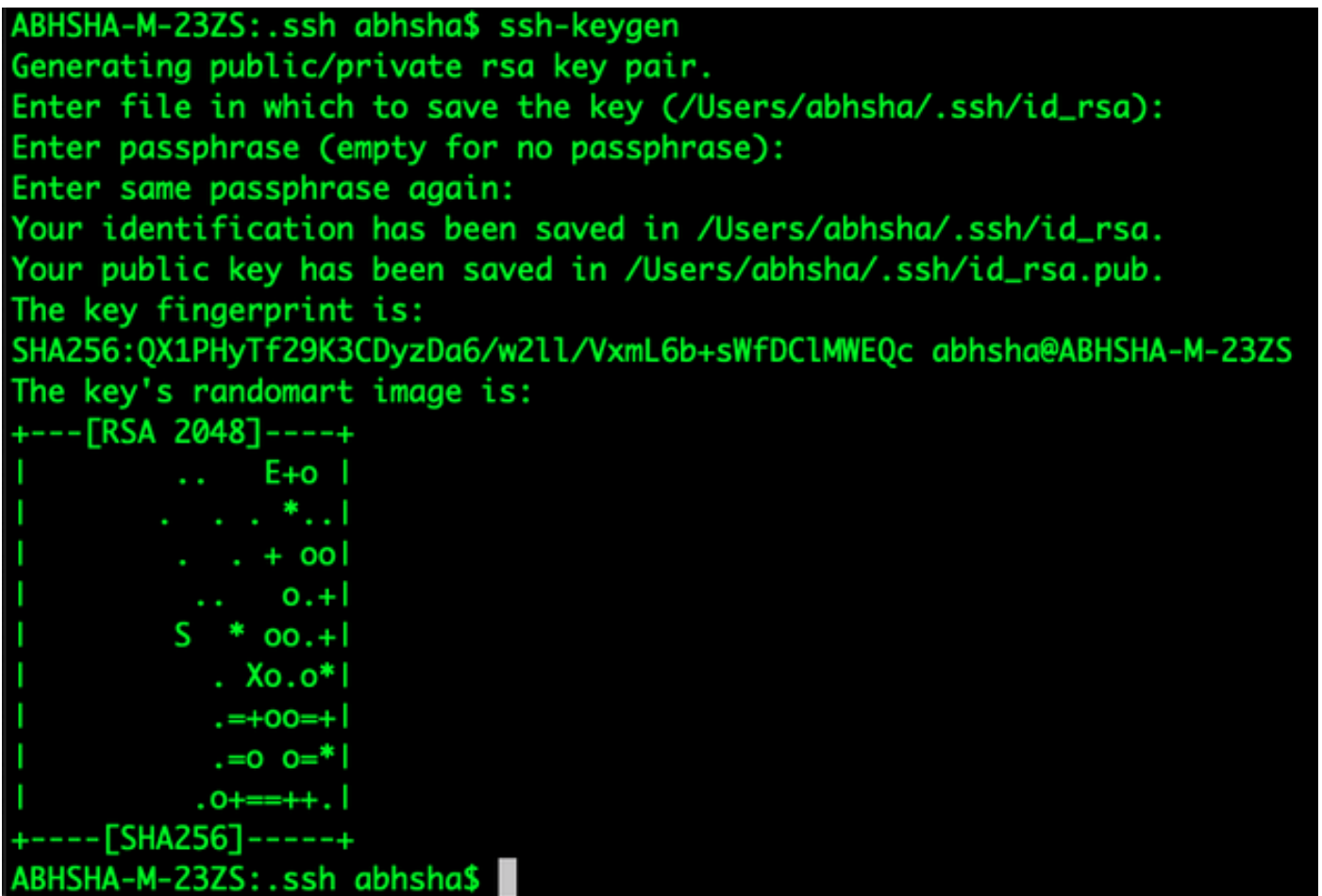


```
AMP-VPC - Notepad
File Edit Format View Help
ssh-rsa AAAAB3NzaC1yc2EAAAQBAn/DObg8zkYwHaMfq011V1GcLL7c fgvj8aj1pbK3+2mXon1nr4YP8S+oDsxl/b6QV899kc7z3sQevpXxC9sC1Guh+nv8WAunF+16912K71DuVyqhfcLH/vv5hPHJKaC47BqdWs
+AuDrcCUgoDw0rHREHy+ShZ8GII0vxxenIIn5yY3IUj=889xmsPY/norzyt
m+Wh6h0HdQtfgyBAj6TxGbcdK5VcLFaxbHBCR8cEMx2yw61Ub2DSUwL78eDkFRhf1VWey07HbQ5zm/KPk1jIXFCrk9BAmXvPW4w5FZSKKYQJgns1pjggcmpPbR8791b1xz7neUG+ktj16T4G3p
```

Generare una coppia di chiavi RSA utilizzando Linux/Mac

Passaggio 1. Dalla CLI di Linux/Mac, immettere il comando "ssh-keygen"

Passaggio 2. Inserire i parametri obbligatori e in questo modo viene generata la coppia di chiavi RSA nella cartella "~/.ssh"



```
ABHSHA-M-23ZS:~/.ssh abhsha$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/abhsha/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/abhsha/.ssh/id_rsa.
Your public key has been saved in /Users/abhsha/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:QX1PhyTf29K3CDyzDa6/w21l/VxmL6b+sWfDC1MWEQc abhsha@ABHSHA-M-23ZS
The key's randomart image is:
+----[RSA 2048]-----+
|          ..  E+o |
|         . . . *..|
|        . . + oo|
|       ..  o.+|
|      S * oo.+|
|     . Xo.o*|
|    .+=+oo=+|
|   . =o o=*|
|  .o+==++.|
+-----[SHA256]-----+
ABHSHA-M-23ZS:~/.ssh abhsha$
```

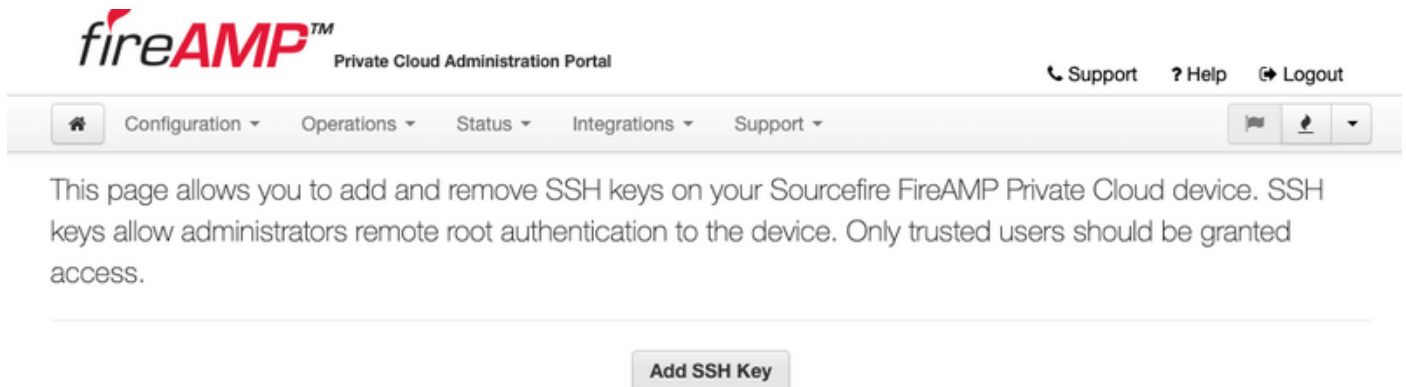
Passaggio 3. Se si apre il contenuto di id_rsa.pub che è la chiave pubblica, è possibile vedere che è già nel formato richiesto.

```
ABHSHA-M-23ZS: .ssh abhsha$
ABHSHA-M-23ZS: .ssh abhsha$ ls
id_rsa          id_rsa.pub      known_hosts
ABHSHA-M-23ZS: .ssh abhsha$
ABHSHA-M-23ZS: .ssh abhsha$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQD12Brou9ABf5tLpZKZpF/nPxTnvs9I6cKC+tycnzC6iR1BT/zmqJ
5SVCSmdhnbwOD9cbWzQ7RYgI46SFLa3JeFU11jFzSmAWqI94AHAjFHVp3W5idcZeq9xxsvSm9Z/NPD+roDEGLnRY+y
VMT2wrHGEyxNyWZ0ZL04Vetmfqof1nx8ixIq+5SwXRdJGFsBNWF0hh8v5rhbxk1ByTVcqGYL3P4JCfMth4tCQDyPd/
CWAIA/263oVDwS4eWEL7haZS+zsqGytOvrNpHnMeoHbc23LKwiFv1xQFy7WFDmxIAGiELVRAKqsv//onbHz/zG/K2J
JUL/grTai5amOFq7f2njp abhsha@ABHSHA-M-23ZS
ABHSHA-M-23ZS: .ssh abhsha$
```

Aggiunta delle chiavi pubbliche generate al portale di amministrazione AMP Private Cloud

Passaggio 1. Passare al portale di amministrazione di AMP Private Cloud > Configurazione > SSH

Passaggio 2. Fare clic su "Add SSH Key" (Aggiungi chiave SSH)



The screenshot shows the FireAMP Private Cloud Administration Portal. The page title is "fireAMP™ Private Cloud Administration Portal". The navigation menu includes "Configuration", "Operations", "Status", "Integrations", and "Support". The main content area has a heading "SSH Key" and a sub-heading "This page allows you to add and remove SSH keys on your Sourcefire FireAMP Private Cloud device. SSH keys allow administrators remote root authentication to the device. Only trusted users should be granted access." Below the text is a button labeled "Add SSH Key".

Passaggio 3. Aggiungere il contenuto della chiave pubblica e salvarlo.

SSH Key

Name

Enabled

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQD12Brou9ABf5tLpZKZpF/nPxTnvs9I6cKC+tycnzC6iR1BT/zmqJ5SVCSmdhnbwOD9cbWzQ7RYgI46SFLa3JeF
U11jFzSmAWqI94AHAjFHVp3W5idcZeq9xxsvSm9Z/NPD+roDEGLnRY+yVMT2wrHGEyxNyWZ0ZL04Vetmfqof1nx8ixIq+5SwXRdJGFsBNWF0hh8v5rhbx
k1ByTVcqGYL3P4JCfMth4tCQDyPd/CWAIA/263oVDwS4eWEL7haZS+zsqGytOvrNpHnMeoHbc23LKwiFv1xQFy7WFDmxIAGiELVRAKqsv//onbHz/zG/K2
JUL/grTai5amOFq7f2njp abhsha@ABHSHA-M-23ZS
```

Passaggio 4. Dopo aver salvato l'accessorio, verificare che si stia "riconfigurando" l'accessorio.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

Configuration Changed

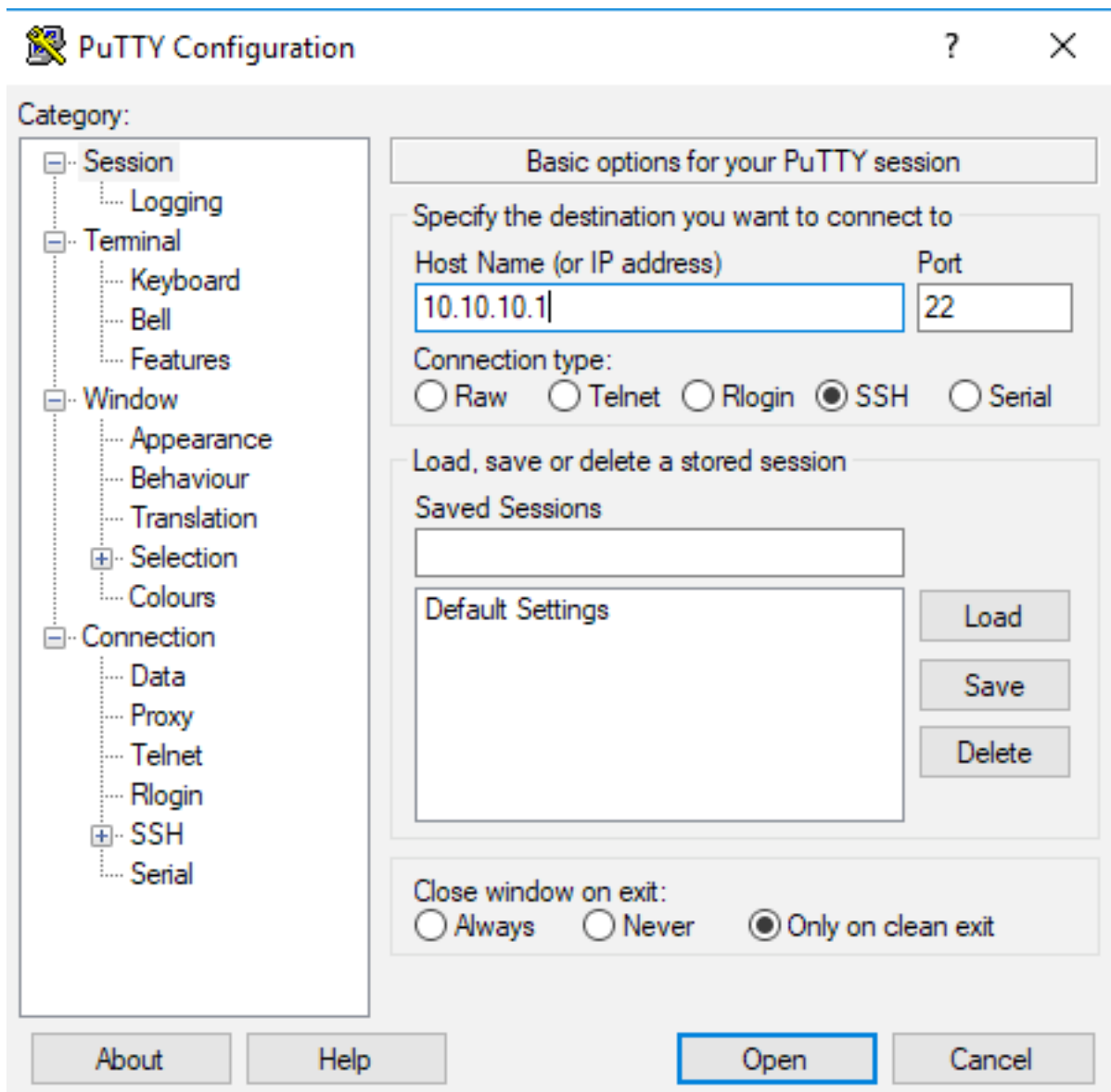
Configuration changes do not take effect until reconfiguration is performed.

 **Reconfigure Now**

Reconfiguration

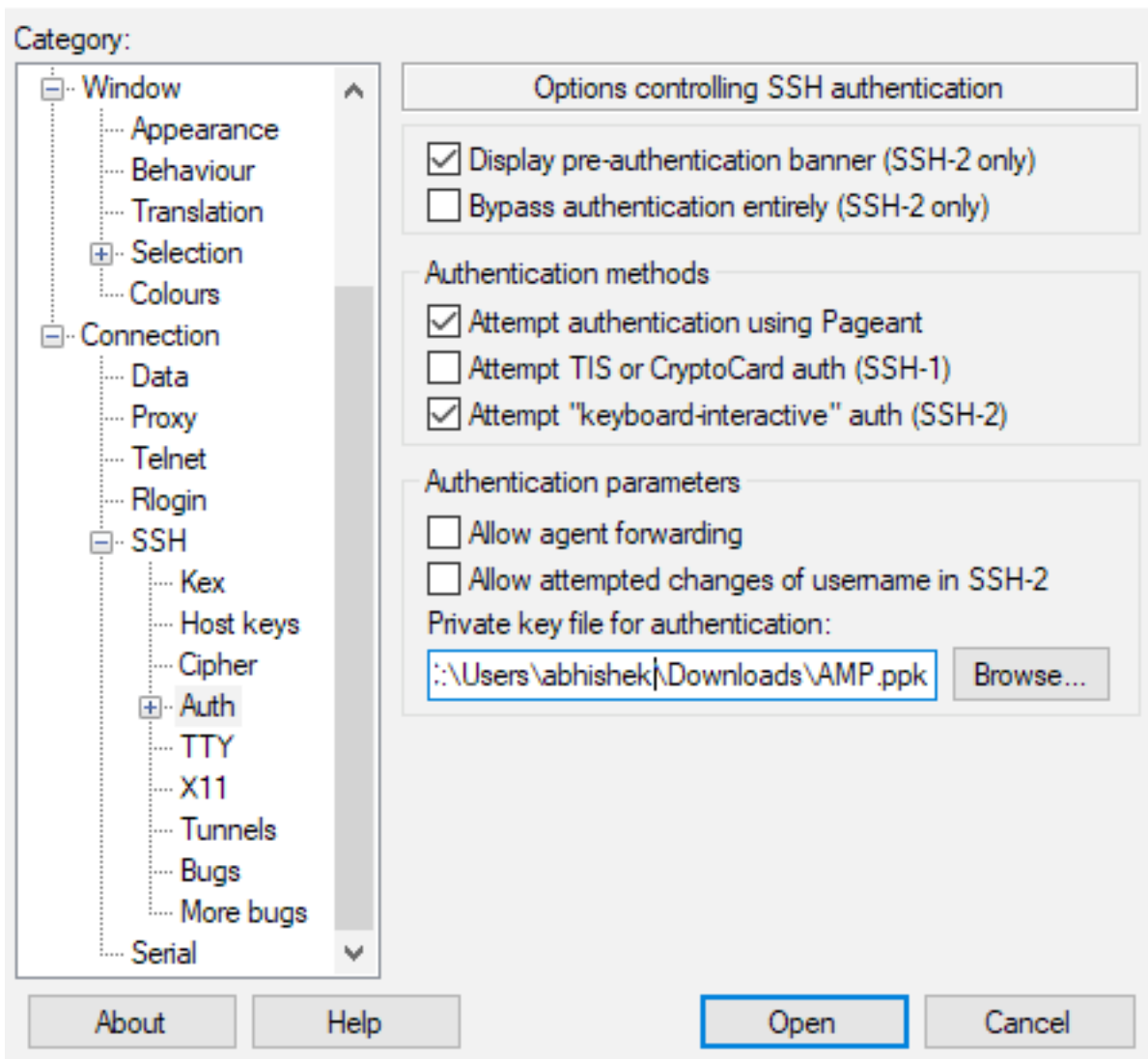
Usare la coppia di chiavi generata per collegare il protocollo SSH all'accessorio con PuTTY

Passaggio 1. Aprire PuTTY e immettere l'indirizzo IP del portale AMP Private Cloud Administration.



Passaggio 2. Nel riquadro sinistro, selezionare Connection > SSH e fare clic su Auth.

Passaggio 3. Selezionare la chiave privata generata da PuTTYGen. Questo è un file PPK.



Passaggio 4. Fare clic su Open (Apri) e, quando viene richiesto un nome utente, immettere "root" (radice) per accedere alla CLI di AMP Private Cloud.

Uso della coppia di chiavi configurata per SSH nell'accessorio con Linux

Passaggio 1. Se le coppie di chiavi pubblica e privata sono archiviate correttamente nel percorso `~/.ssh`, è necessario essere in grado di eseguire il protocollo SSH sull'appliance AMP Private Cloud usando semplicemente il comando `ssh` senza richiedere alcuna password.

```
ssh root@<INDIRIZZO-IP-AMP>
```

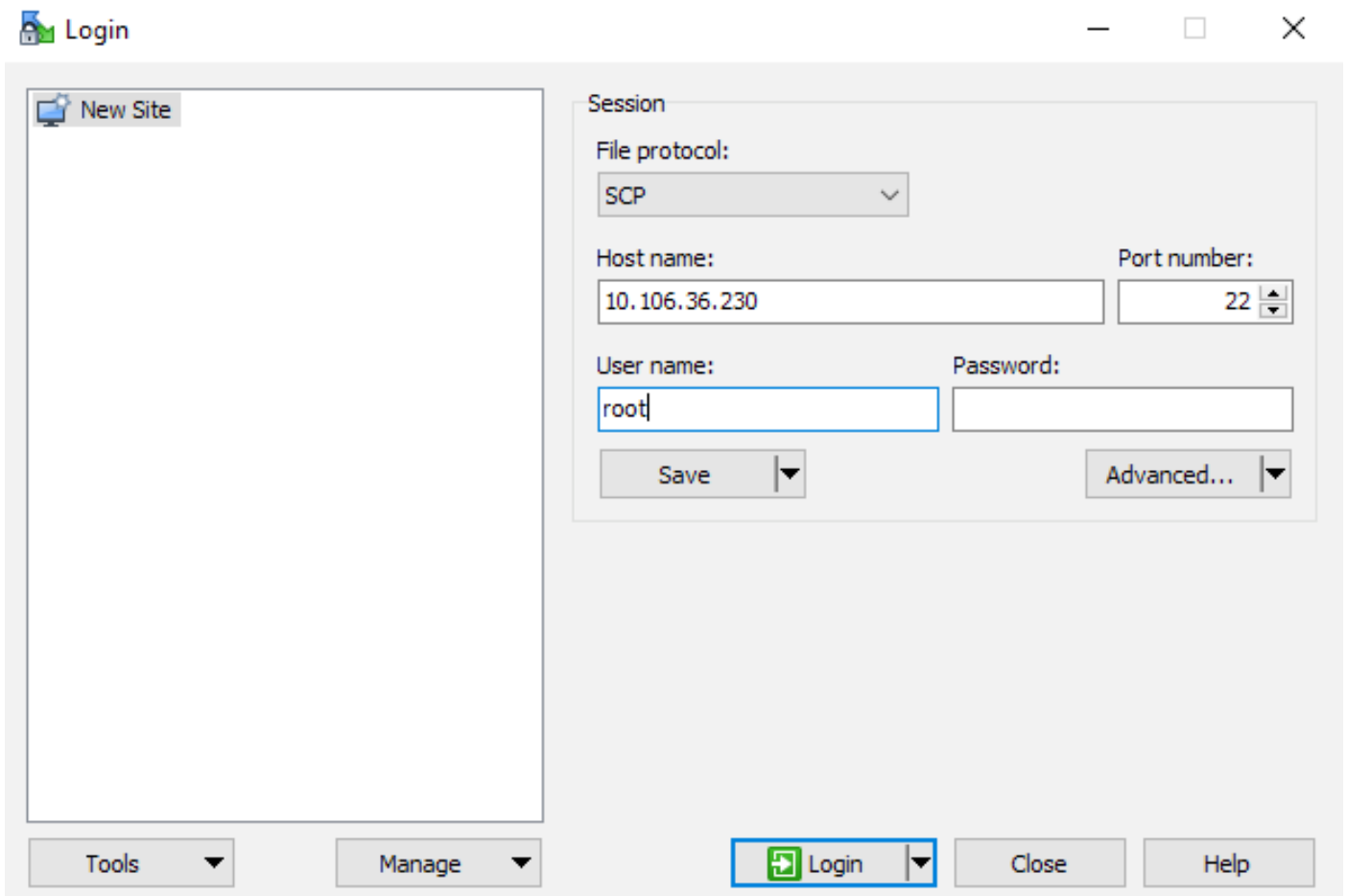


```
[abhishek@supecomputer .ssh]$ ssh root@10.106.36.230
The authenticity of host '10.106.36.230 (10.106.36.230)' can't be established.
RSA key fingerprint is SHA256:mvHHLqnMJhPBBBpPankbdXV7pJxBha5NE1h1GdBs1fg.
RSA key fingerprint is MD5:27:78:7c:39:de:b9:b7:d8:45:87:8e:09:96:33:b6:db.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.106.36.230' (RSA) to the list of known hosts.
Last login: Fri Mar 29 03:30:46 2019 from 173.39.68.177
[root@fireamp ~]#
[root@fireamp ~]#
```

Utilizzo di WinSCP per interagire con il file system di AMP Private Cloud

Passaggio 1. Installare WinSCP nel computer e avviarlo.

Passaggio 2. Immettere l'indirizzo IP del portale AMP Private Cloud Administration e selezionare File Protocol come SCP. Immettere il nome utente come root e lasciare il campo password.



Passaggio 3. Selezionare Avanzate > Avanzate > SSH > Autenticazione

Passaggio 4. Selezionare il file PPK generato come chiave privata da PuTTYgen.

Advanced Site Settings



Environment

- Directories
- Recycle bin
- Encryption
- SFTP
- SCP/Shell

Connection

- Proxy
- Tunnel

SSH

- Key exchange
- Authentication**
- Bugs

Note

Bypass authentication entirely

Authentication options

- Attempt authentication using Pageant
- Attempt 'keyboard-interactive' authentication
 - Respond with password to the first prompt
- Attempt TIS or CryptoCard authentication (SSH-1)

Authentication parameters

- Allow agent forwarding

Private key file:

...

Display Public Key Tools ▾

GSSAPI

- Attempt GSSAPI authentication
 - Allow GSSAPI credential delegation

Color ▾ OK Cancel Help

Passaggio 5. Fare clic su OK e quindi su Accesso. Una volta accettata la richiesta, dovrebbe essere possibile accedere.