

# Accès à la CLI du cloud privé AMP via SSH et transfert de fichiers via SCP

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Générer une paire de clés RSA à l'aide de PuTTY](#)

[Générer une paire de clés RSA à l'aide de Linux/Mac](#)

[Ajout des clés publiques générées au portail d'administration du cloud privé AMP](#)

[Utiliser la paire de clés générée pour SSH dans l'appliance à l'aide de PuTTY](#)

[Utilisation de la paire de clés configurée pour SSH dans l'appliance à l'aide de Linux](#)

[Utilisation de WinSCP pour interagir avec le système de fichiers du cloud privé AMP](#)

## Introduction

Ce document décrit la procédure pour générer une paire de clés SSH à l'aide de PuTTY et d'un shell Linux, l'ajouter à AMP, puis accéder à l'interface de ligne de commande. L'appliance de cloud privé AMP utilise une authentification basée sur des certificats pour SSH dans l'appliance. La procédure pour générer rapidement une paire de clés, afin d'accéder à l'interface de ligne de commande et d'interagir avec le système de fichiers via SCP (WinSCP) est décrite ici.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- PuTTY
- WinSCP
- shell Linux / Mac

### Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

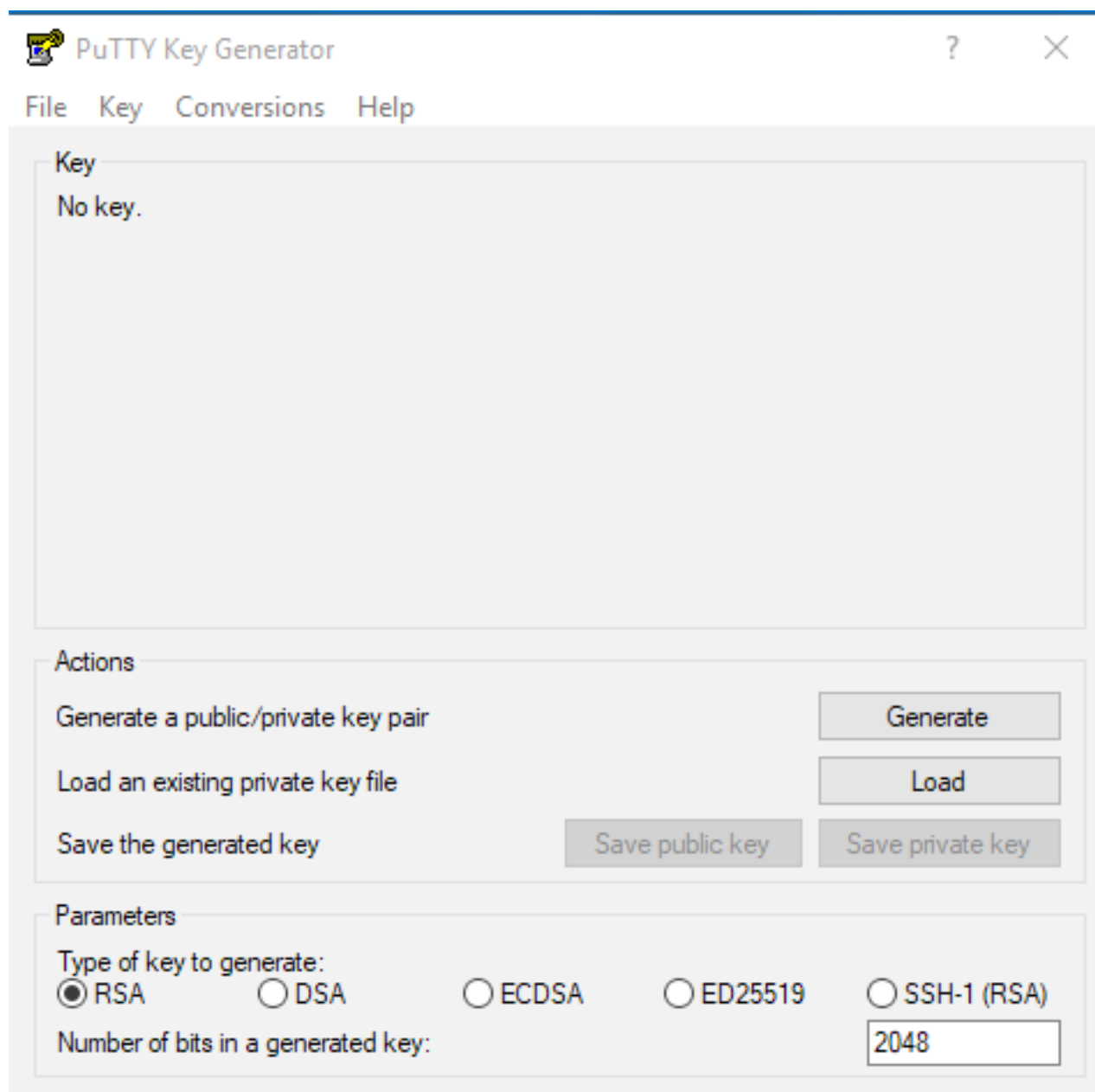
## Configuration

La première étape consiste à générer une paire de clés RSA à l'aide de PuTTY ou du shell Linux. Après cela, la clé publique doit être ajoutée et approuvée par l'appliance de cloud privé AMP.

## Générer une paire de clés RSA à l'aide de PuTTY

Étape 1. Vérifiez que vous avez installé PuTTY.

Étape 2. Lancez PuTTYGen qui est installé avec PuTTY pour générer la paire de clés RSA.



Étape 3. Cliquez sur Generate (Générer) pour déplacer le curseur de manière aléatoire afin de terminer la génération de la paire de clés.

Étape 4. Choisissez « Enregistrer la clé publique » et « Enregistrer la clé privée » qui sera utilisé dans les sections suivantes, comme l'illustre l'image ici.



## 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

Étape 5. Ouvrez la clé publique avec le Bloc-notes, car le format doit être modifié pour être accepté dans AMP Private Cloud Administration Portal.



|----- 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 -----

Étape 6. Supprimez les 2 premières lignes commençant par "—BEGIN » et la dernière ligne commençant par "— END »

Étape 7. Supprimez tous les sauts de ligne pour faire du contenu de la clé publique une seule ligne continue.

Étape 8. Entrez le mot « ssh-rsa » au début du fichier. Enregistrez le fichier.

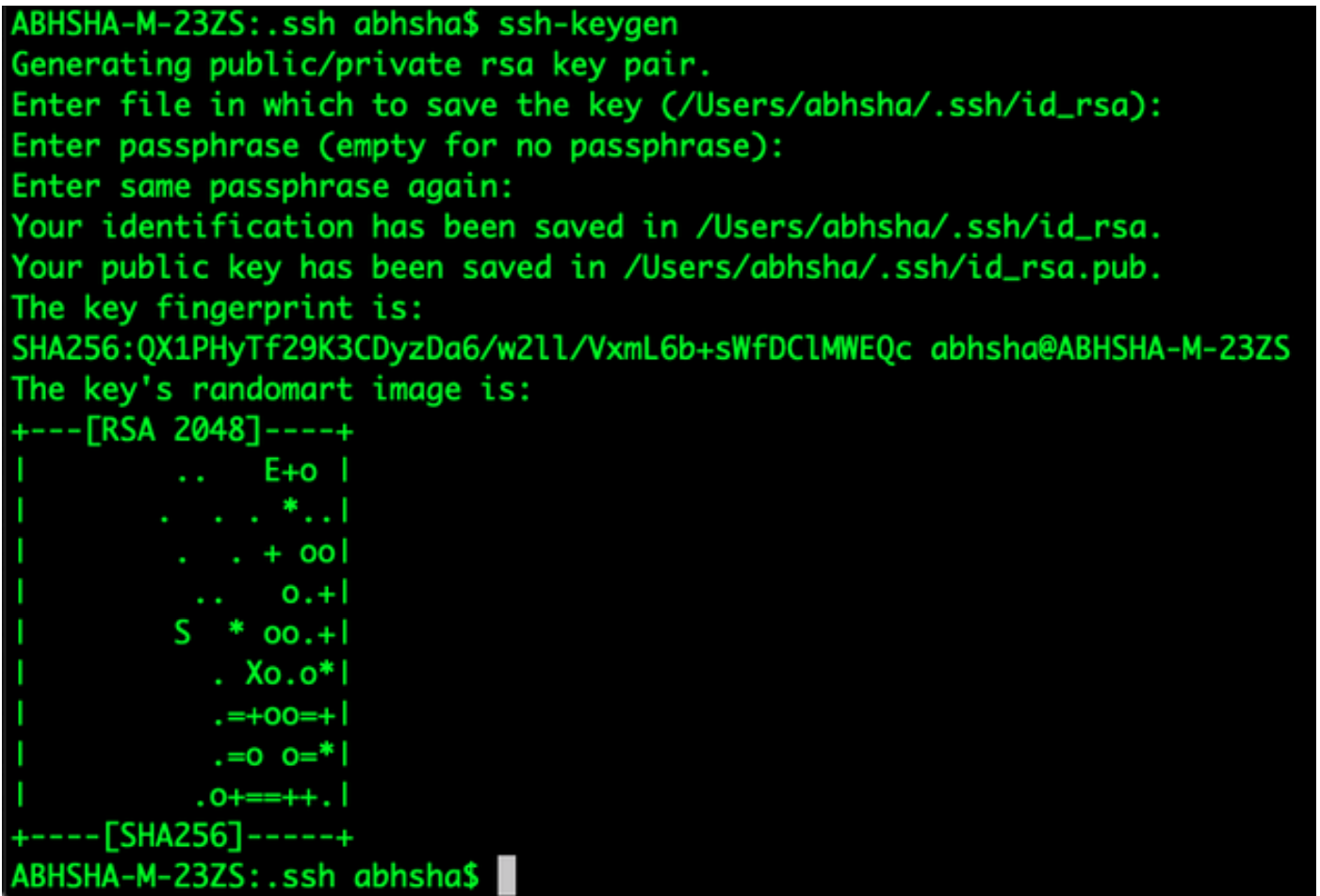


```
AMP-VPC - Notepad
File Edit Format View Help
ssh-rsa AAAAB3NzaC1yc2EAAAQBan/DObg8zkYwHaMfq011V1GcLL7c fgvj8aj1pbK3+2mXon1nr4YP85+oDsxdI/b6QV899kC7z3sQevpXxC9sC1Guh+nv8WAunF+16912K71DuVyqhfLH/vv5hPHJKaC47BqdWs
+AuDrcUqoDw0rHREHy+ShZ8GII0vxxenIIn5yY3IUjm889xmsPY/norzyt
m+Wh6h0HdQtfgyBAj6TxGbcdK5VcLFaxbMBCR8cEMx2yw61Ub2DSUwL78eDkFRhf1VWey07HbQ5zm/KPk1jIXFCrk9BAmXvPW4w5FZSKKYQJgns1pjggcmpPbR8791b1xz7neUG+ktj16T4G3p
```

## Générer une paire de clés RSA à l'aide de Linux/Mac

Étape 1. Sur l'interface de ligne de commande Linux/Mac, entrez la commande « ssh-keygen »

Étape 2. Entrez les paramètres requis et cela génère la paire de clés RSA au niveau du dossier "~/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+sWfDClMWEQc 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$
```

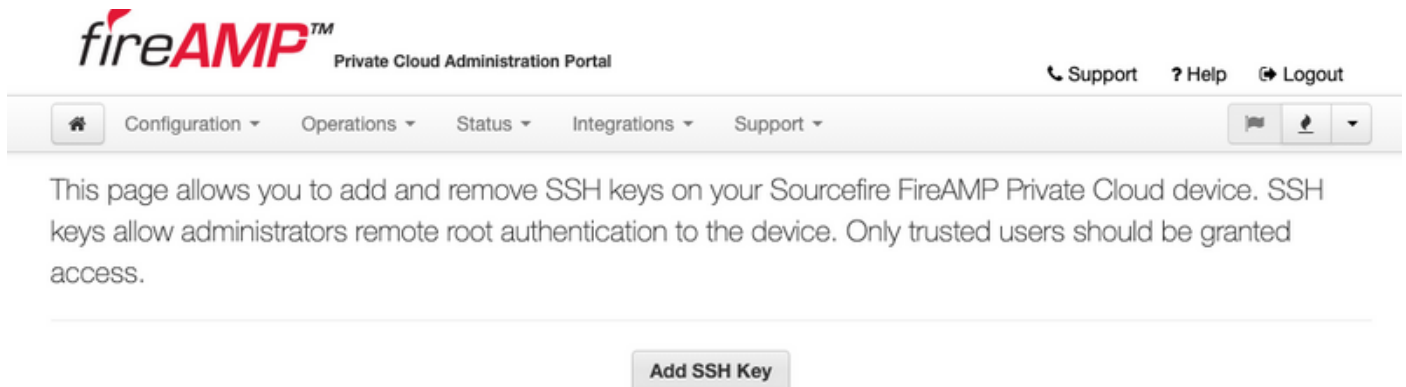
Étape 3. Si vous ouvrez le contenu de id\_rsa.pub qui est la clé publique, vous pouvez voir qu'il est déjà dans le format requis.

```
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$
```

## Ajout des clés publiques générées au portail d'administration du cloud privé AMP

Étape 1. Accédez au portail d'administration du cloud privé AMP > Configuration > SSH

Étape 2. Cliquez sur Ajouter une clé SSH.



Étape 3. Ajoutez le contenu de la clé publique et enregistrez-le.

### 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
```

Étape 4. Une fois que vous avez sauvegardé ce fichier, assurez-vous de reconfigurer l'appliance.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

### Configuration Changed

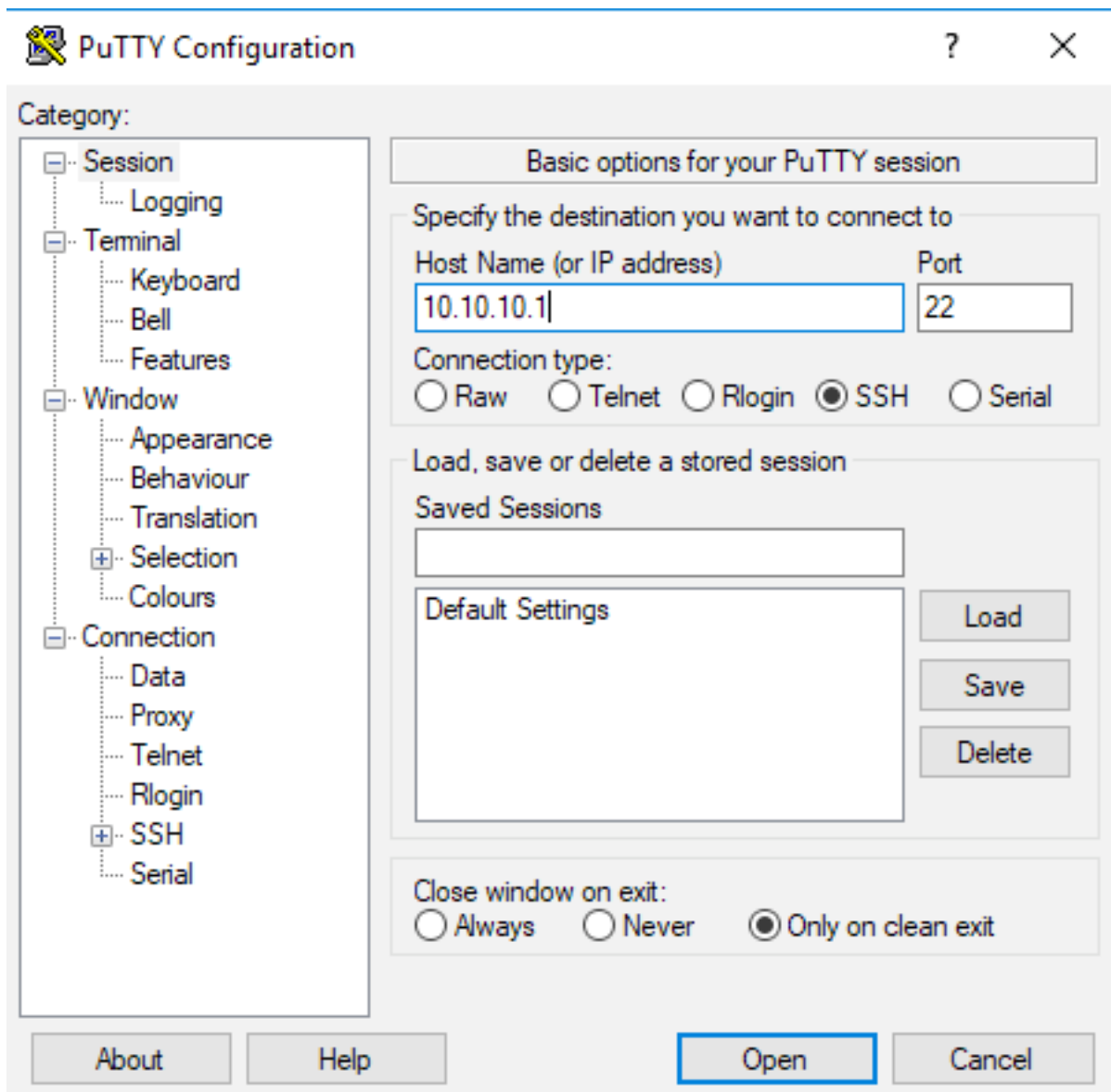
Configuration changes do not take effect until reconfiguration is performed.

 **Reconfigure Now**

Reconfiguration

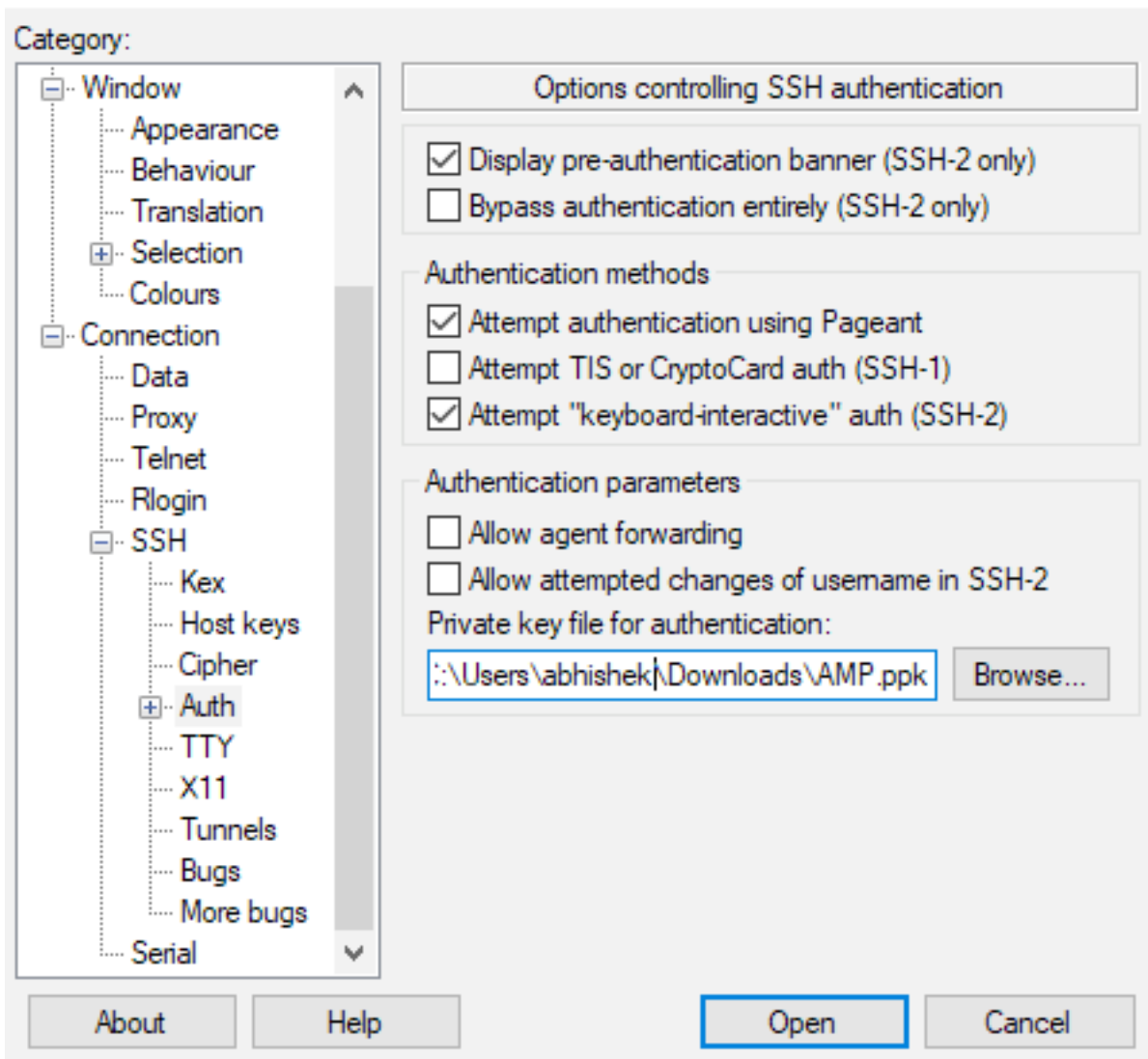
## Utiliser la paire de clés générée pour SSH dans l'apppliance à l'aide de PuTTY

Étape 1. Ouvrez PuTTY et saisissez l'adresse IP du portail d'administration de cloud privé AMP.



Étape 2. Dans le volet gauche, sélectionnez **Connection > SSH** et cliquez sur **Auth**.

Étape 3. Sélectionnez la clé privée générée par PuTTYGen. Il s'agit d'un fichier PPK.



Étape 4. Cliquez sur Ouvrir et, lorsqu'il vous demande un nom d'utilisateur, saisissez « root » et vous devez atterrir à l'interface de ligne de commande du cloud privé AMP.

## Utilisation de la paire de clés configurée pour SSH dans l'appliance à l'aide de Linux

Étape 1. Si les paires de clés privées et publiques sont stockées correctement sur le chemin `~/.ssh`, vous devez être en mesure d'effectuer une SSH sur l'appliance de cloud privé AMP en exécutant simplement la commande `ssh` sans vous demander de mot de passe.

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

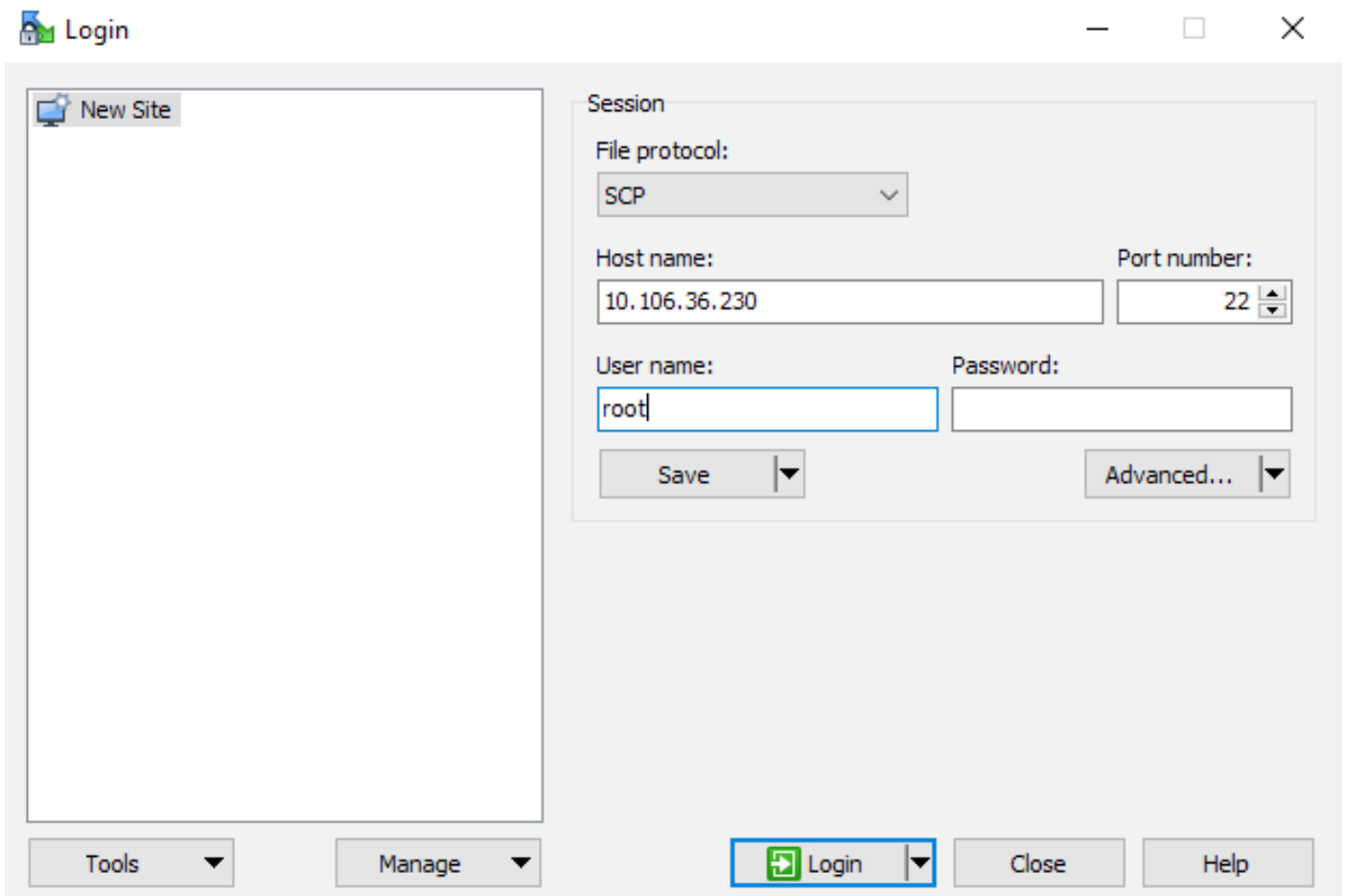


```
[abhishek@supecomputer .ssh]$ ssh root@10.106.36.230
The authenticity of host '10.106.36.230 (10.106.36.230)' can't be established.
RSA key fingerprint is SHA256:mvHHLqnMJhPBBBpPankbdXV7pJxBha5NE1h1GdBs1fg.
RSA key fingerprint is MD5:27:78:7c:39:de:b9:b7:d8:45:87:8e:09:96:33:b6:db.
Are you sure you 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 ~]#
```

## Utilisation de WinSCP pour interagir avec le système de fichiers du cloud privé AMP

Étape 1. Installez WinSCP sur votre machine et lancez-la.

Étape 2. Saisissez l'adresse IP du portail d'administration du cloud privé AMP et sélectionnez le protocole de fichier SCP. Saisissez le nom d'utilisateur en tant que root et laissez le champ password.



Étape 3. Sélectionnez Advanced > Advanced > SSH > Authentication

Étape 4. Sélectionnez le fichier PPK qui a été généré en tant que clé privée par 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

Étape 5. Cliquez sur OK, puis sur Connexion. Vous devriez pouvoir vous connecter correctement après avoir accepté l'invite.