

# Accessing the CLI of AMP Private Cloud via SSH and Transferring Files via SCP

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Generate an RSA key pair using PuTTY](#)

[Generate an RSA key pair using Linux/Mac](#)

[Adding the generated public keys to the AMP Private Cloud Administration Portal](#)

[Use the generated key pair to SSH into the appliance using PuTTY](#)

[Using the configured key pair to SSH into the appliance using Linux](#)

[Using WinSCP to interact with the file system of AMP Private Cloud](#)

## Introduction

This document describes the procedure to generate an SSH key pair using PuTTY and using a Linux shell, add it to AMP, and then access the CLI. AMP Private Cloud appliance uses certificate-based authentication to SSH into the appliance. The procedure to generate a key pair quickly, in order to access the CLI and to interact with the file system via SCP (WinSCP) is detailed here.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- PuTTY
- WinSCP
- Linux / Mac shell

### Components Used

This document is not restricted to specific software and hardware versions.

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. If your network is live, ensure that you understand the potential impact of any command.

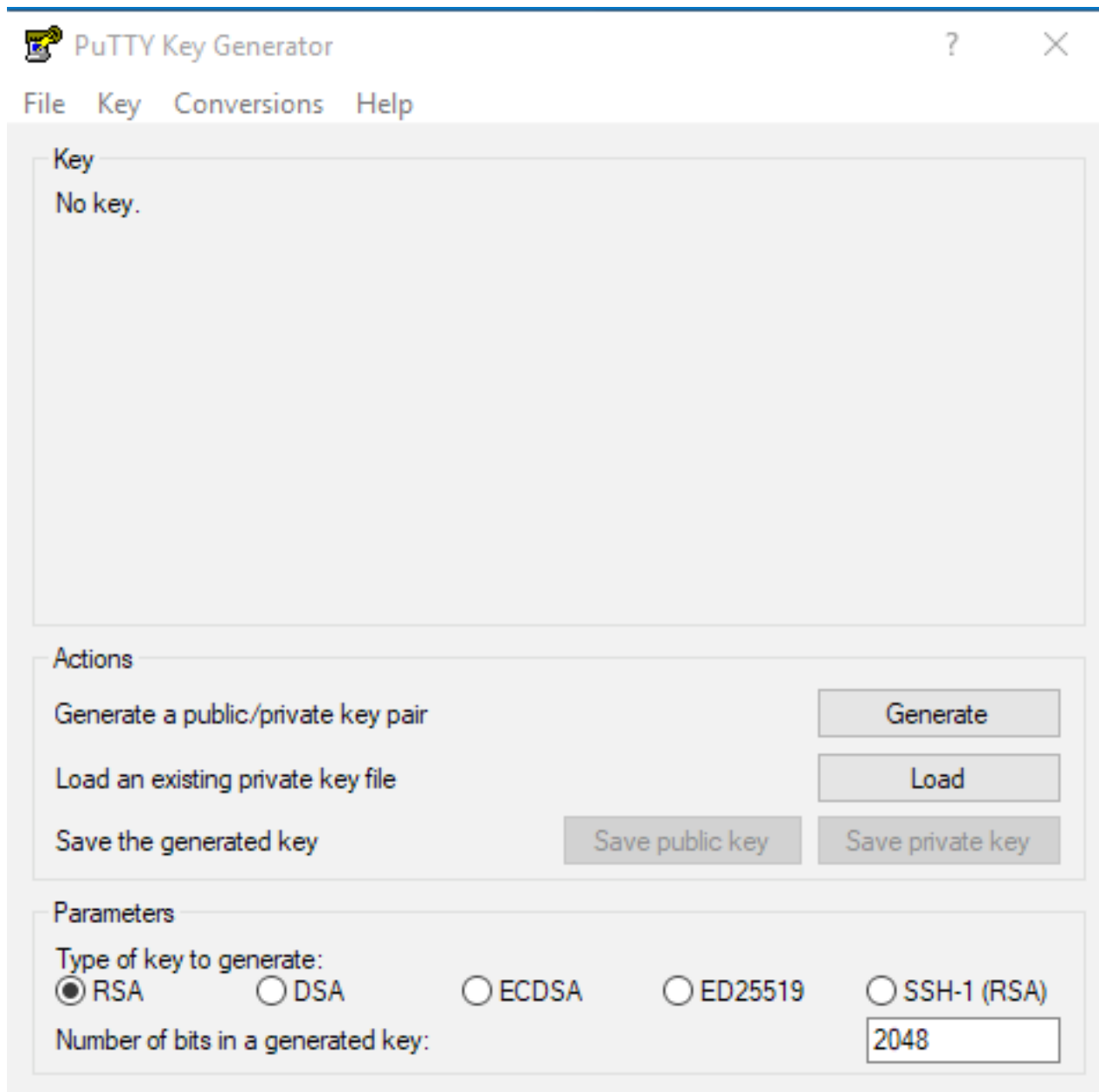
## Configure

The first step involves generating an RSA key pair either using PuTTY or Linux shell. After this, the public key needs to be added and trusted by the AMP Private Cloud Appliance.

## Generate an RSA key pair using PuTTY

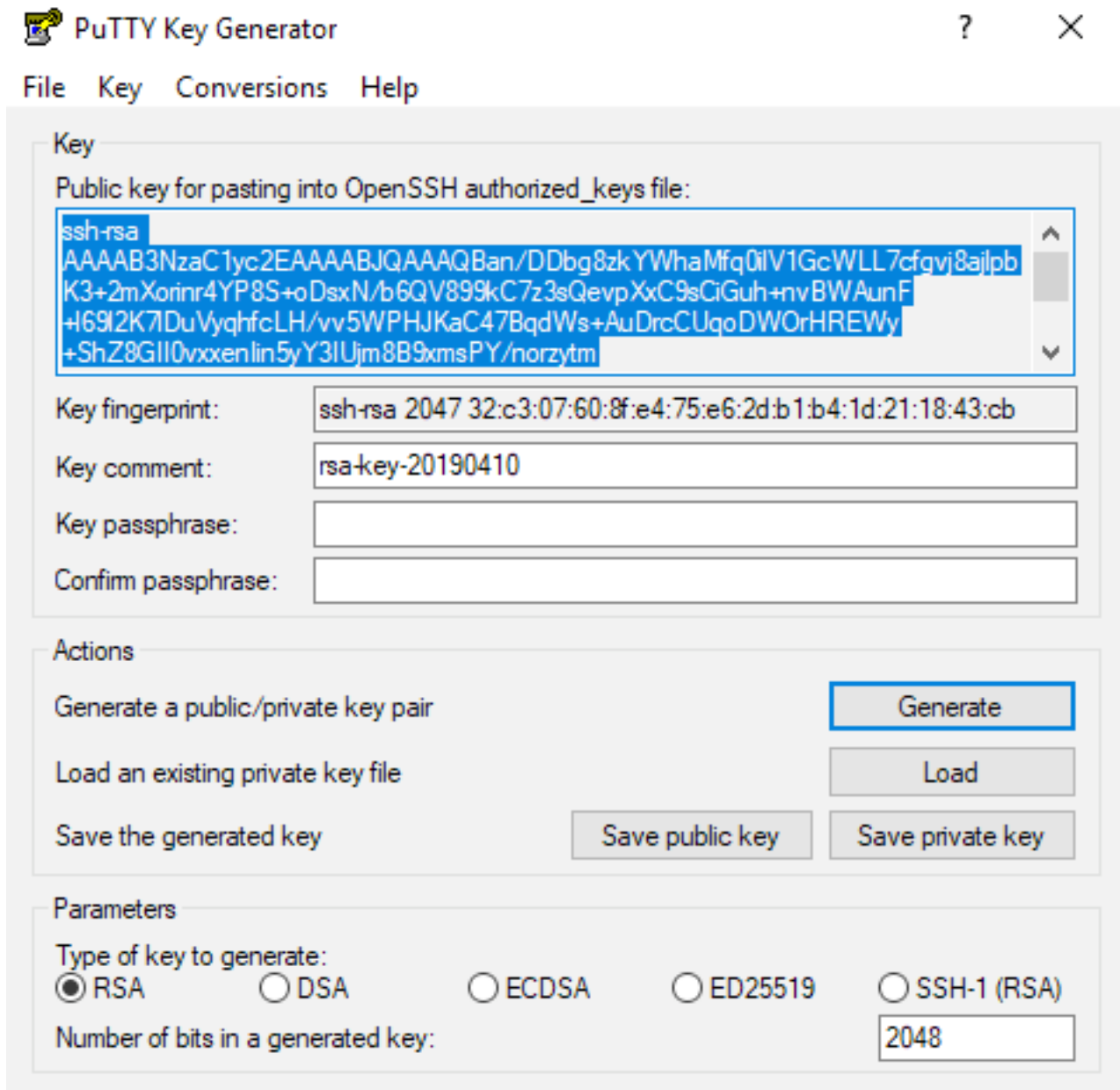
Step 1. Ensure that you have installed PuTTY completely.

Step 2. Launch PuTTYGen which is installed along with PuTTY to generate the RSA key pair.

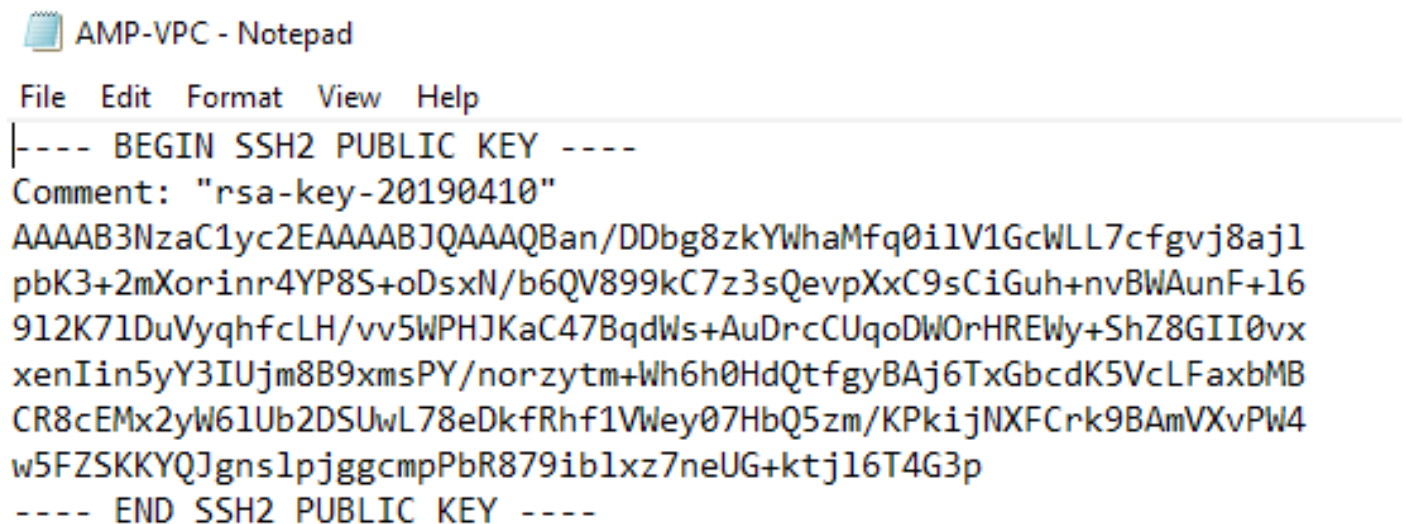


Step 3. Click Generate to and move the cursor randomly to complete the key pair generation.

Step 4. Choose to "Save public key" and "Save private key" which is to be used in the later sections, as shown in the image here.



Step 5. Open the public key with Notepad as the format needs to be modified in order for it to be accepted in AMP Private Cloud Administration Portal.



Step 6. Remove the first 2 lines that start with "----BEGIN" and the final line that starts with "----END"

Step 7. Remove all the line breaks to make the public key content as a single continuous line.

Step 8. Enter the word "ssh-rsa" at the beginning of the file. Save the file.

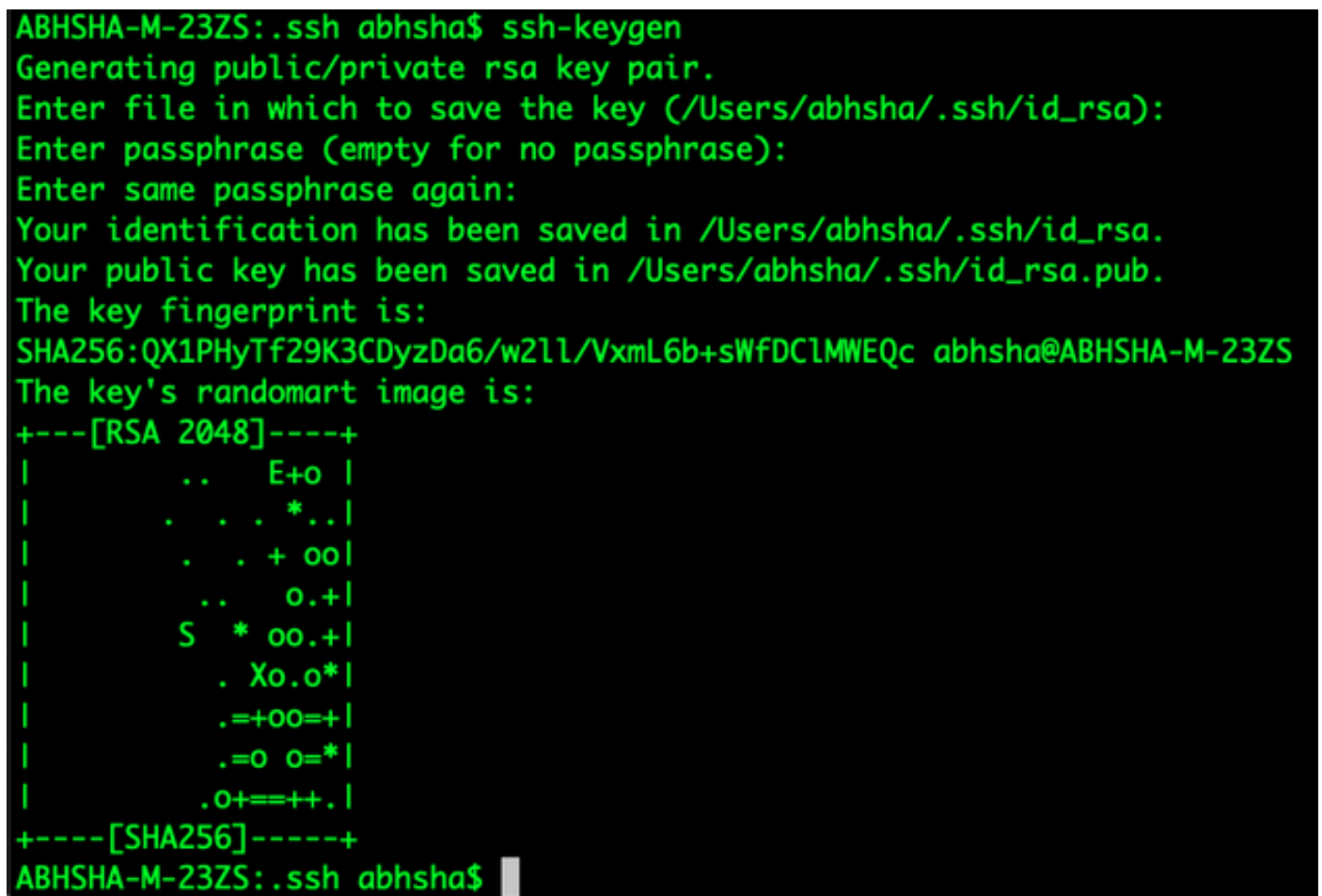


```
AMP-VPC - Notepad
File Edit Format View Help
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQBan/DDbg8zkYwHaMfq011V1GcLL7cFgvj8aj1pbK3+2mXor1nr4YP8S+oDsxl/b6QV899kC7z3sQevpXxc9sC1Guh+nv8WAunF+16912K71DuVyqhfLH/vv5WPHJKaC47BqdWs
+AuDrcCUqoDW0rHREWY+ShZ8GI0vxxenIIn5yY3IUjme889xmsPY/norzyt
m+Wh6h0HdQtfgyBAj6TxGbcdK5vcLFaxb|BCR8cEMx2yW61Ub2DSUwL78e0kfRhf1Vwey07HbQ5zm/KPk1jNIXFCrk98AmVXvPW4w5FZSKKYQJgns1pjggcmpPbR8791b1xz7neUG+ktj16T4G3p
```

## Generate an RSA key pair using Linux/Mac

Step 1. On the Linux/Mac CLI, enter the command "ssh-keygen"

Step 2. Enter the required parameters and this generates the RSA key pair at the folder "~/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$
```

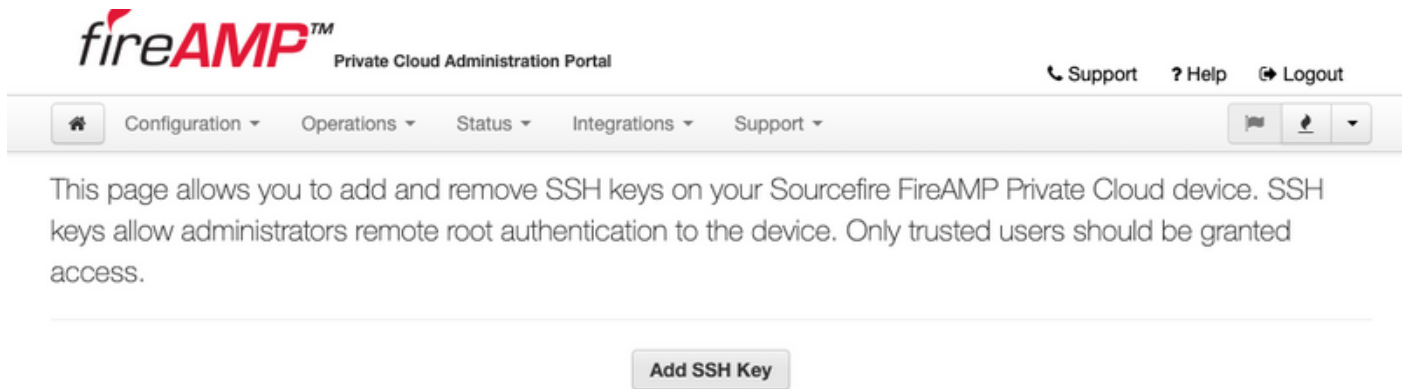
Step 3. If you open the contents of id\_rsa.pub which is the public key, you can see that it is already in the required format.

```
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$
```

## Adding the generated public keys to the AMP Private Cloud Administration Portal

Step 1. Navigate to the AMP Private Cloud Administration Portal > Configuration > SSH

Step 2. Click "Add SSH Key"



Step 3. Add the contents of the public key and save this.

### SSH Key

Name

AMP-TEST

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
```

✓ Save    ✕ Cancel

Step 4. After this has been saved, ensure that you're "Reconfiguring" the appliance.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

### Configuration Changed

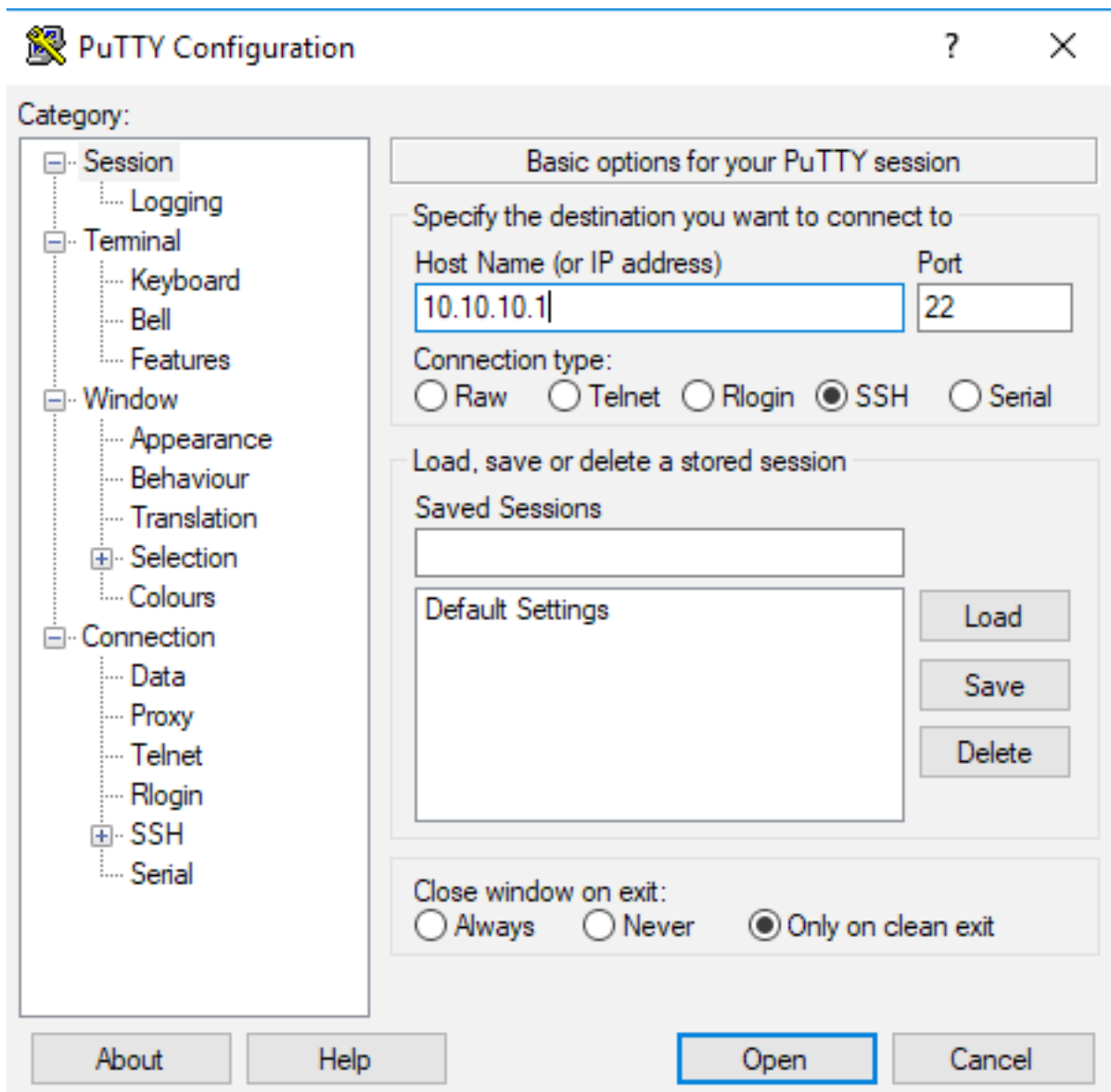
Configuration changes do not take effect until reconfiguration is performed.

 [Reconfigure Now](#)

[Reconfiguration](#)

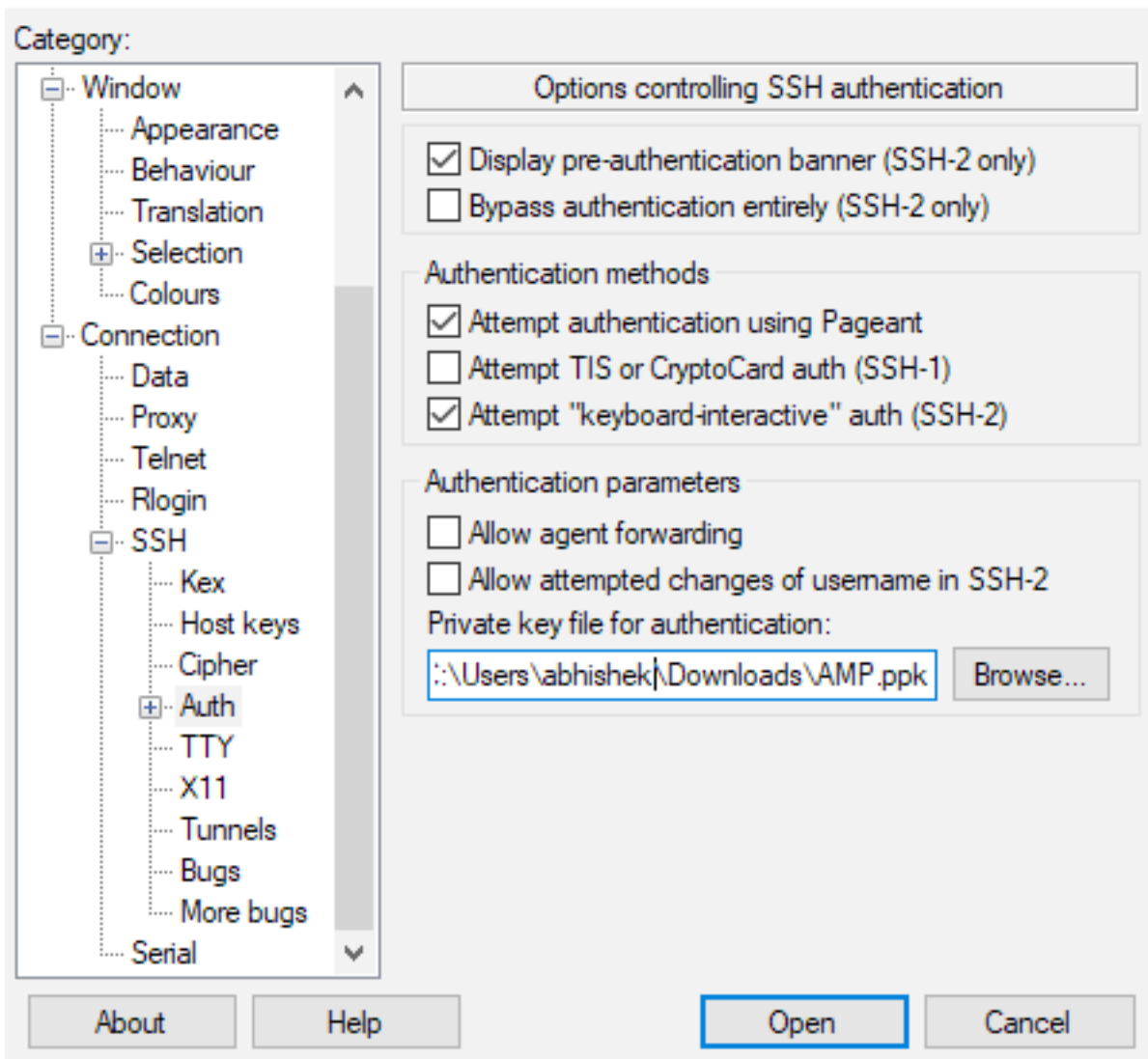
## Use the generated key pair to SSH into the appliance using PuTTY

Step 1. Open the PuTTY and enter the IP address of the AMP Private Cloud Administration portal.



Step 2. On the left pane, select Connection > SSH and click on Auth.

Step 3. Select the Private Key which was generated by PuTTYGen. This is a PPK file.



Step 4. Click on Open and when it prompts for a username, enter "root" and you should land at the CLI of the AMP Private Cloud.

## Using the configured key pair to SSH into the appliance using Linux

Step 1. If the private and public key pairs are stored correctly at `~/.ssh` path, then you should be able to SSH to the AMP Private Cloud appliance by simply issuing the `ssh` command without prompting you for any password.

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

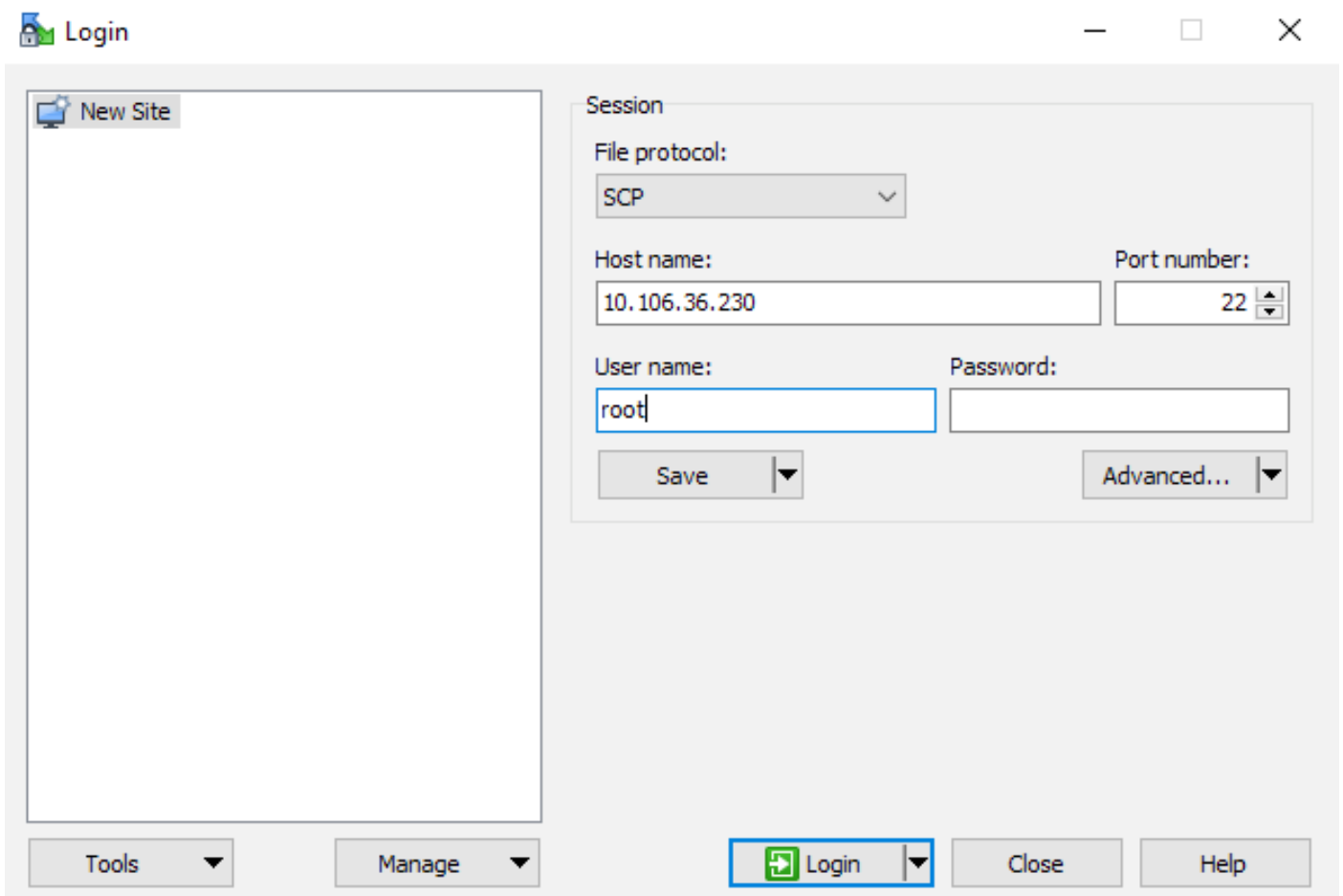


```
[abhishek@supecomputer .ssh]$ ssh root@10.106.36.230
The authenticity of host '10.106.36.230 (10.106.36.230)' can't be established.
RSA key fingerprint is SHA256:mvHHLqnMJhPBBBpPankbdXV7pJxBha5NE1h1GdBs1fg.
RSA key fingerprint is MD5:27:78:7c:39:de:b9:b7:d8:45:87:8e:09:96:33:b6:db.
Are you sure you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

## Using WinSCP to interact with the file system of AMP Private Cloud

Step 1. Install WinSCP on your machine and launch it.

Step 2. Enter the IP address of the AMP Private Cloud Administration Portal, and select the File Protocol as SCP. Enter the username as root and leave the password field.



Step 3. Select Advanced > Advanced > SSH > Authentication

Step 4. Select the PPK file which was generated as a private key by 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

Step 5. Click OK, and then Login. You should be able to log in successfully after accepting the prompt.