Acesso ao CLI da nuvem privada da AMP via SSH e transferência de arquivos via SCP

Contents

Introduction

Este documento descreve o procedimento para gerar um par de chaves SSH usando PuTTY e usando um shell Linux, adicioná-lo ao AMP e, em seguida, acessar o CLI. O dispositivo AMP Private Cloud usa autenticação baseada em certificado para SSH no dispositivo. O procedimento para gerar um par de chaves rapidamente, a fim de acessar a CLI e interagir com o sistema de arquivos via SCP (WinSCP) é detalhado aqui.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- PuTTY
- WinSCP
- shell Linux / Mac

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

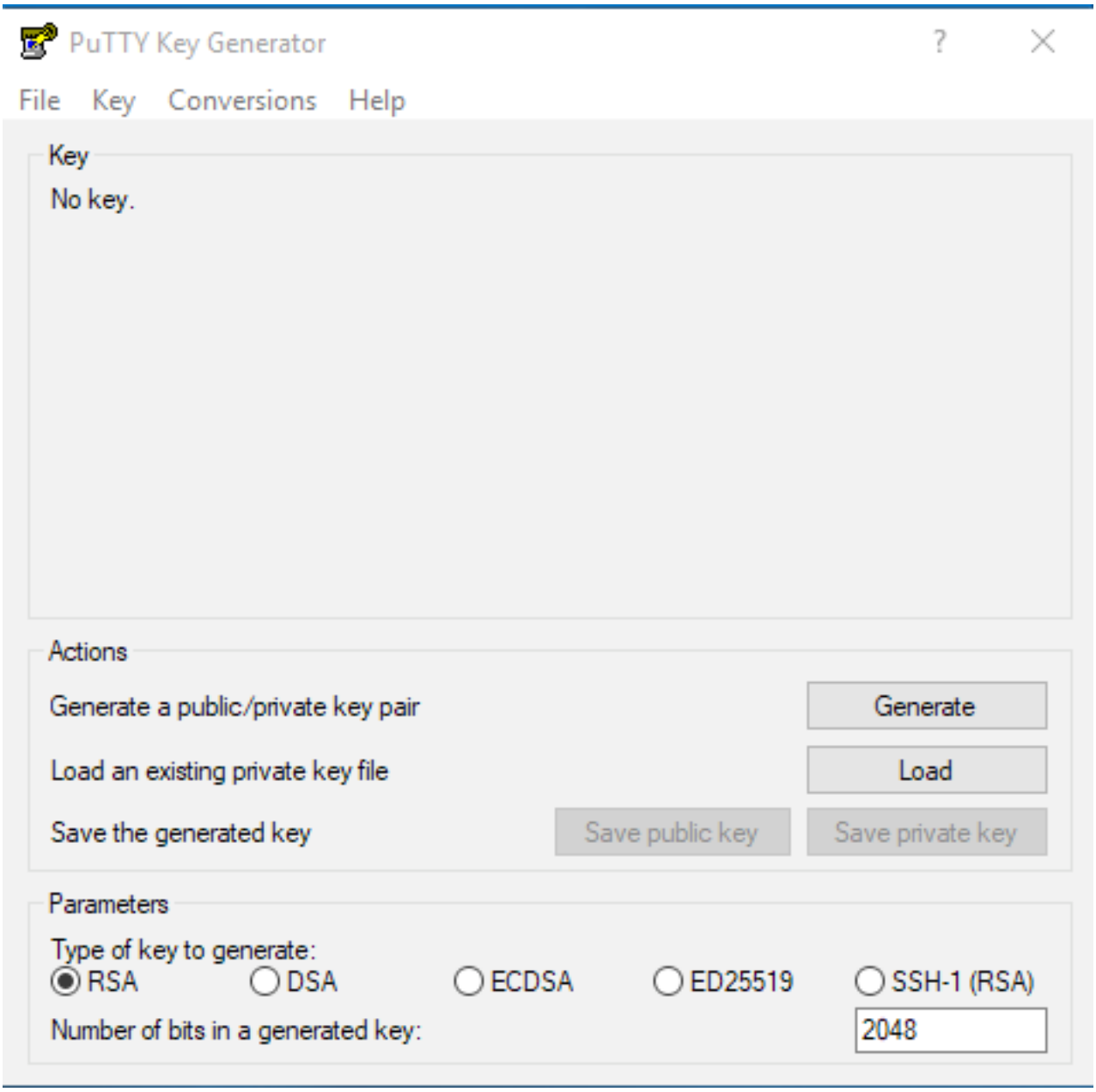
Configurar

A primeira etapa envolve a geração de um par de chaves RSA usando PuTTY ou shell Linux. Depois disso, a chave pública precisa ser adicionada e confiável pelo AMP Private Cloud Appliance.

Gerar um par de chaves RSA usando PuTTY

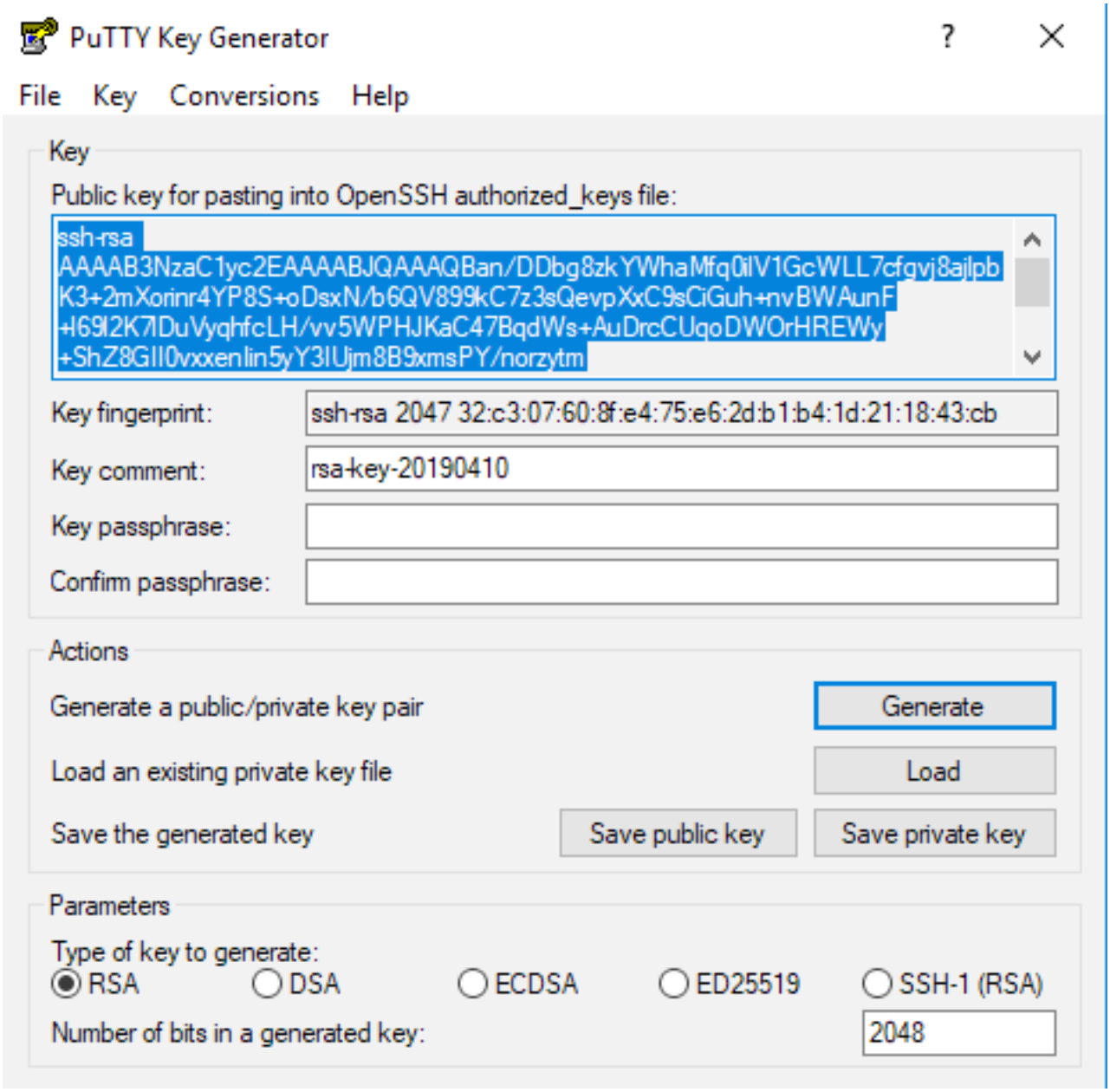
Etapa 1. Verifique se você instalou o PuTTY completamente.

Etapa 2. Inicie o PuTTYGen instalado junto com o PuTTY para gerar o par de chaves RSA.

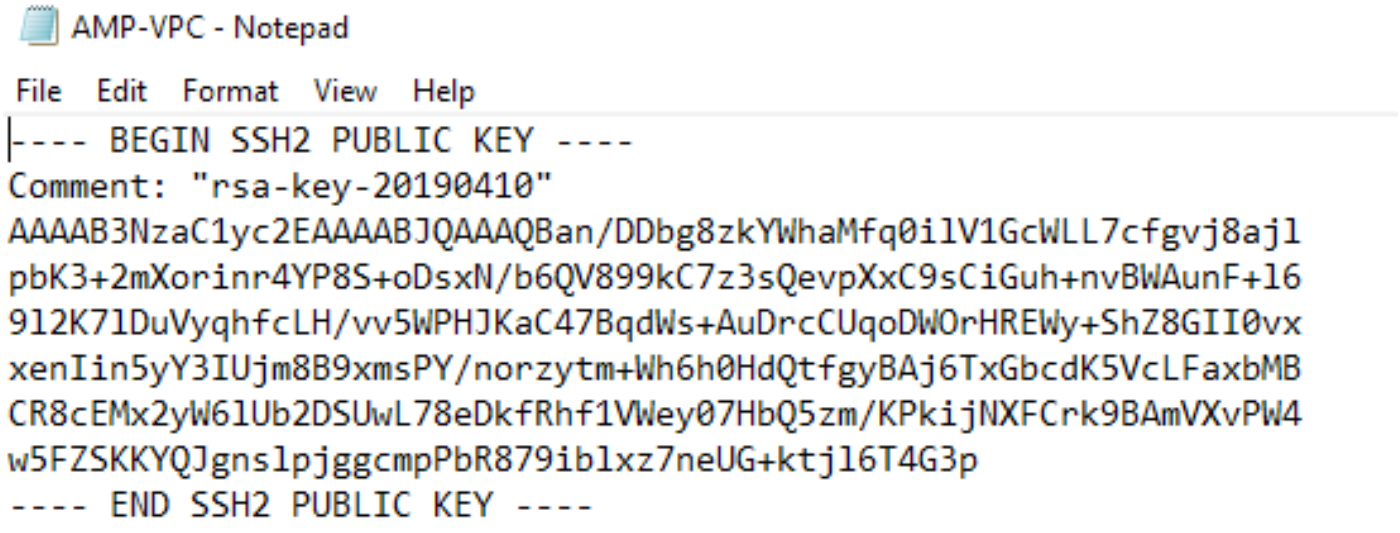


Etapa 3. Clique em Gerar para e mova o cursor aleatoriamente para concluir a geração do par de chaves.

Etapa 4. Escolha "Save public key" (Salvar chave pública) e "Save private key" (Salvar chave privada), que serão usadas nas seções posteriores, como mostrado na imagem aqui.



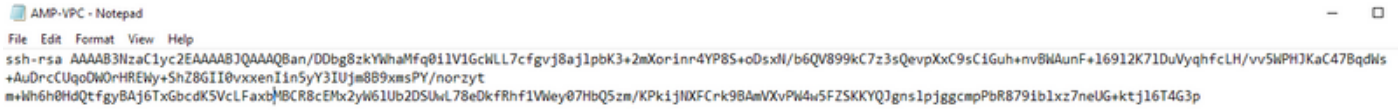
Etapa 5. Abra a chave pública com o Notepad, pois o formato precisa ser modificado para que seja aceito no AMP Private Cloud Administration Portal.



Etapa 6. Remova as duas primeiras linhas que começam com "—BEGIN" e a última linha que começa com "— END"

Passo 7. Remova todas as quebras de linha para tornar o conteúdo da chave pública como uma única linha contínua.

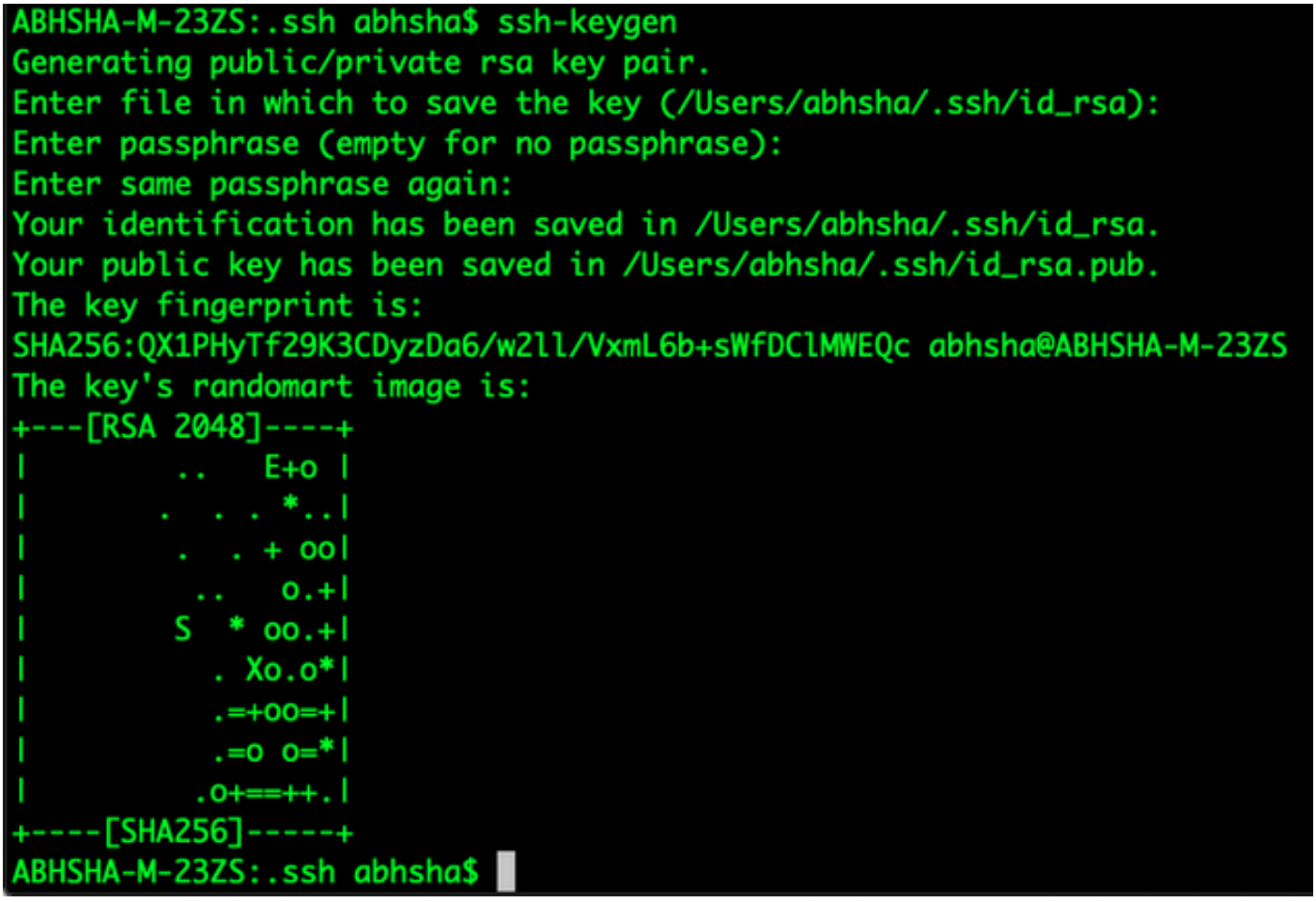
Etapa 8. Digite a palavra "ssh-rsa" no início do arquivo. Salve o arquivo.



Gerar um par de chaves RSA usando Linux/Mac

Etapa 1. Na CLI do Linux/Mac, digite o comando "ssh-keygen"

Etapa 2. Insira os parâmetros necessários e isso gera o par de chaves RSA na pasta "~/.ssh"



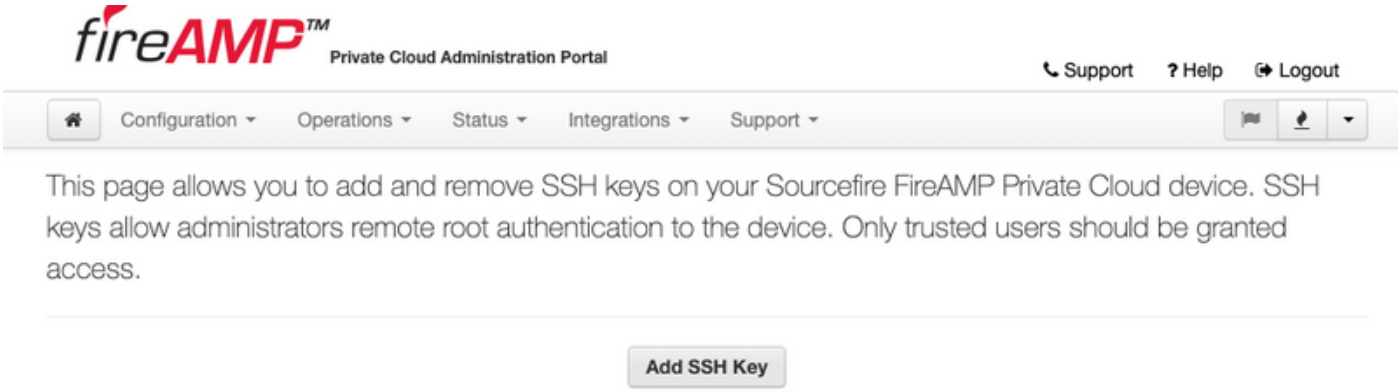
Etapa 3. Se você abrir o conteúdo de id_rsa.pub, que é a chave pública, poderá ver que ele já está no formato necessário.

```
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 AAAAB3NzaC1yc2EAAAADAQABAAABAQD12Brou9ABf5tLpZKZpF/nPxTnvs9I6cKC+tycnzC6iR1BT/zmqJ
5SVCSmdhnbwOD9cbWzQ7RYgI46SFLa3JeFU11jFzSmAWqI94AHAjFHVp3W5idcZeq9xxsvSm9Z/NPD+roDEGLnRY+y
VMT2wrHGEyxNyWZ0ZLO4Vetmfqof1nx8ixIq+5SwXRdJGFsBNWF0hh8v5rhbxk1ByTVcqGYL3P4JCfMth4tCQDyPd/
CWAlA/263oVDwS4eWEL7haZS+zsqGytOvrNpHnMeoHbc23LKwiFv1xQFy7WFDmxIAGiELVRAKqsv//onbHz/zG/K2J
JUL/grTai5amOFq7f2njp abhsha@ABHSHA-M-23ZS
ABHSHA-M-23ZS:.ssh abhsha$
```

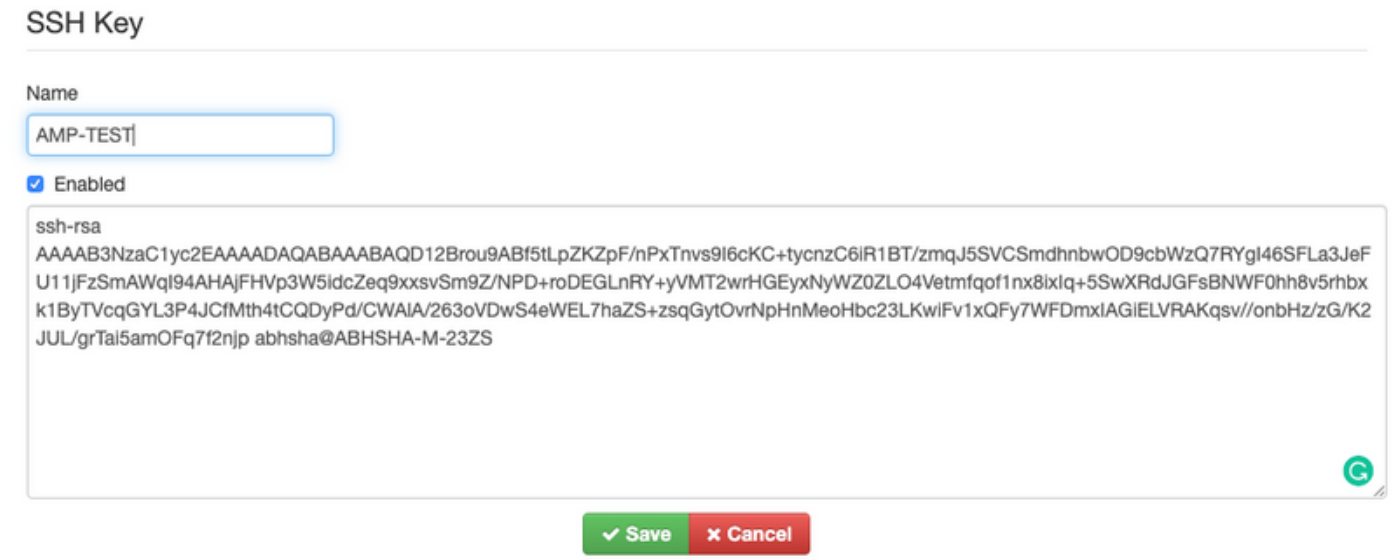
Adição das chaves públicas geradas ao portal AMP Private Cloud Administration

Etapa 1. Navegue até AMP Private Cloud Administration Portal > Configuration > SSH

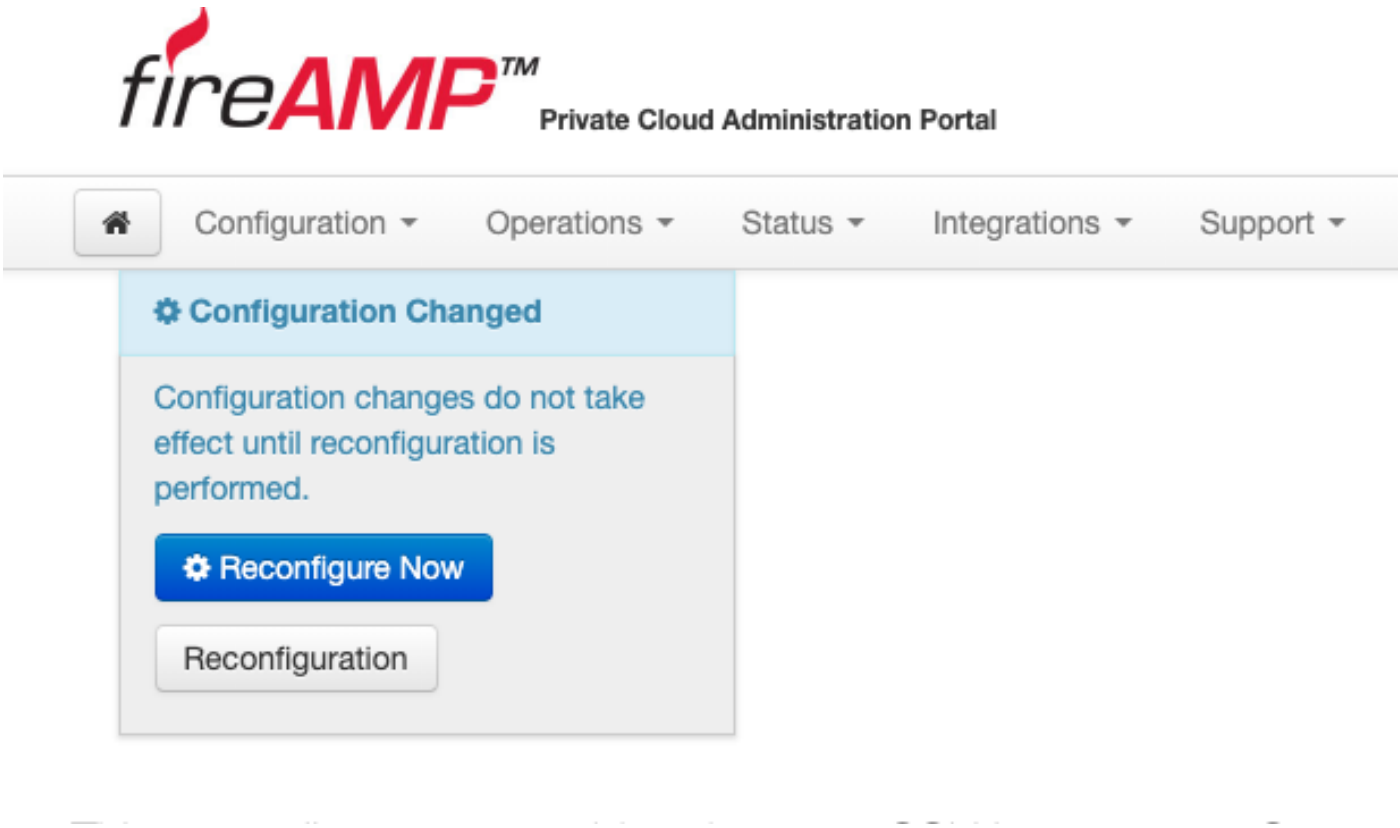
Etapa 2. Clique em "Add SSH Key" (Adicionar chave SSH)



Etapa 3. Adicione o conteúdo da chave pública e salve-o.

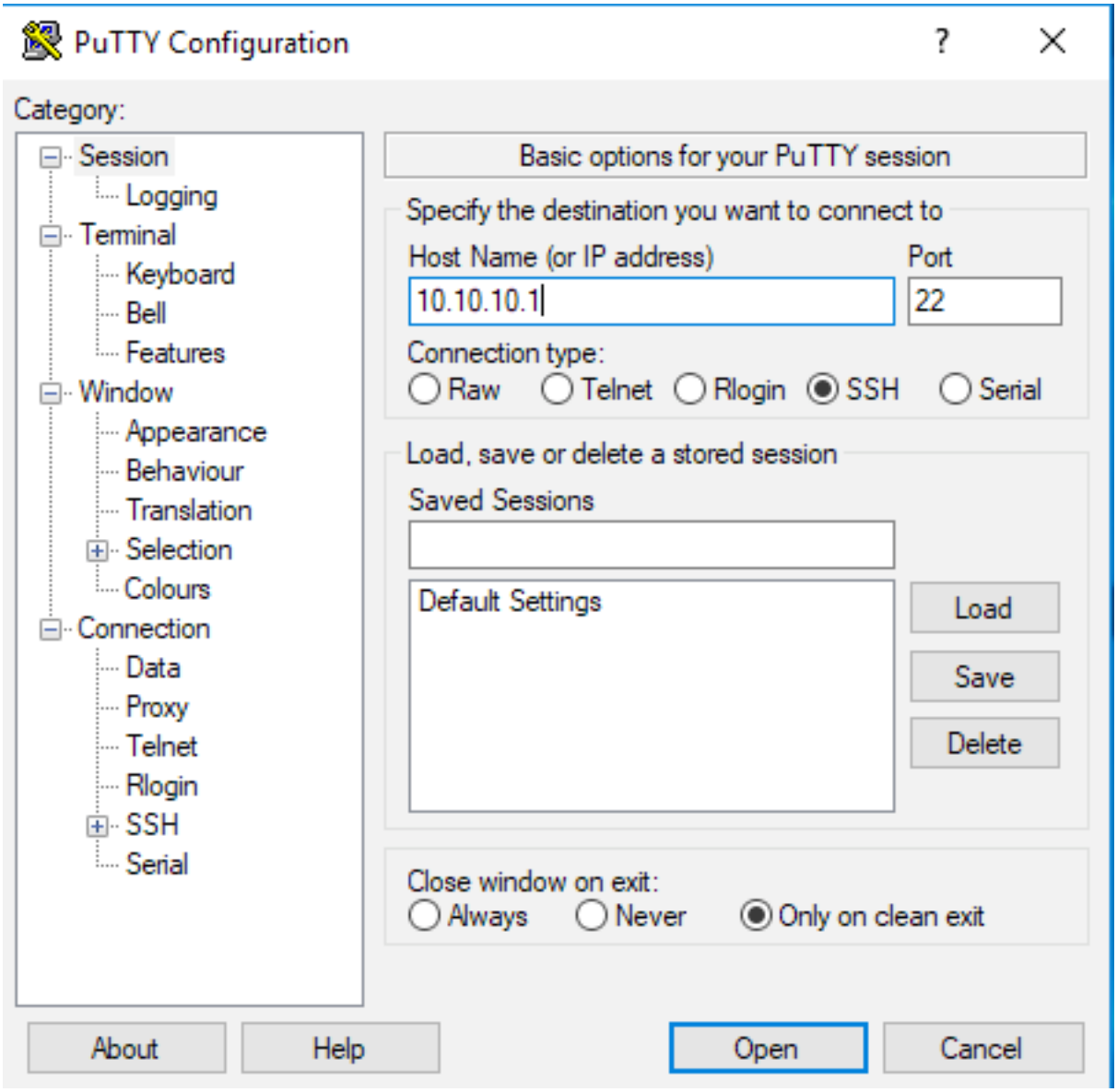


Etapa 4. Depois que isso for salvo, verifique se você está "Reconfigurando" o dispositivo.



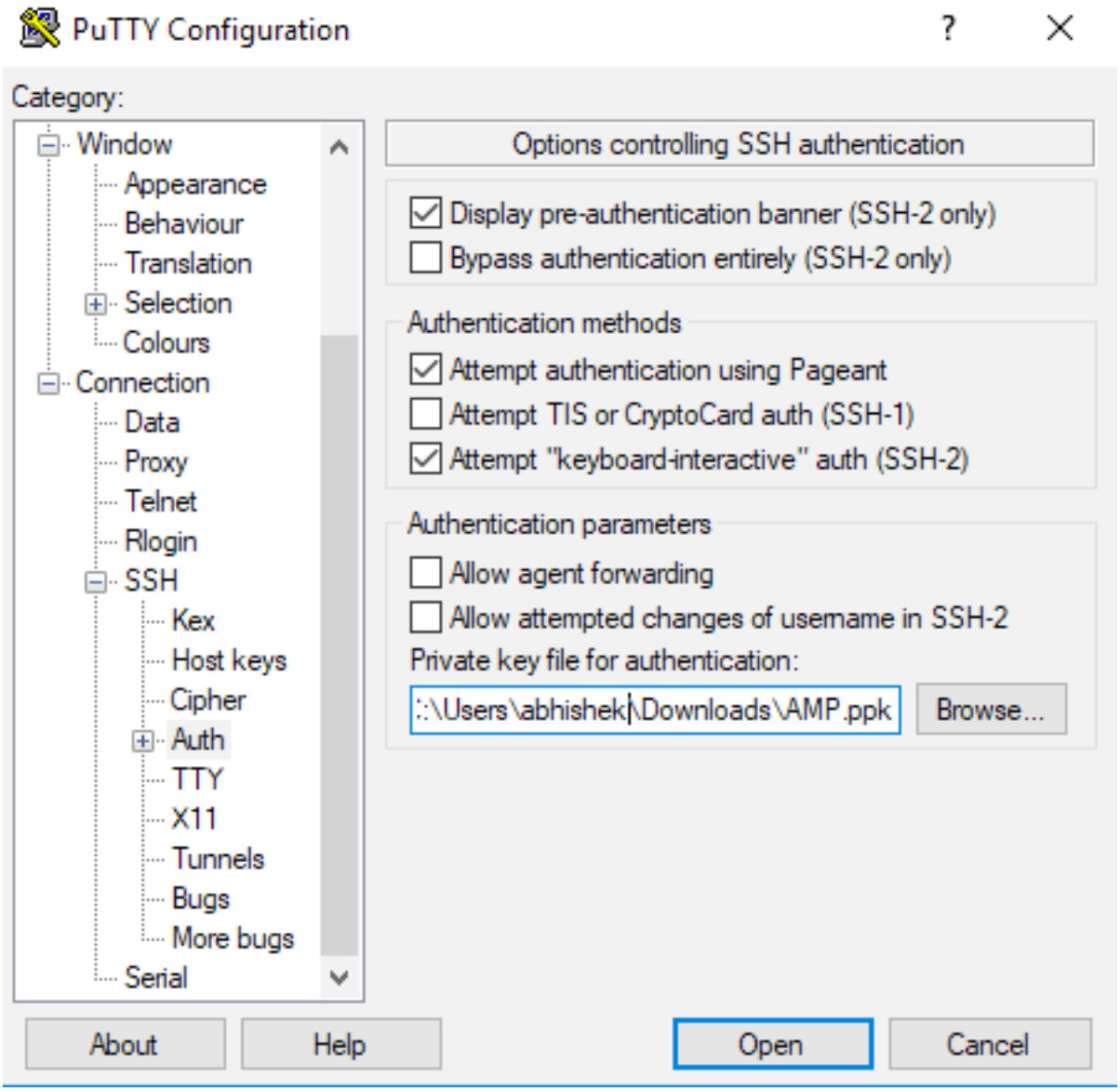
Usar o par de chaves gerado para SSH no dispositivo usando PuTTY

Etapa 1. Abra o PuTTY e insira o endereço IP do portal AMP Private Cloud Administration.



Etapa 2. No painel esquerdo, selecione Connection > SSH e clique em Auth.

Etapa 3. Selecione a chave privada gerada por PuTTYGen. Este é um arquivo PPK.



Etapa 4. Clique em Open (Abrir) e, quando solicitar um nome de usuário, digite "root" (raiz) e você deve pousar na CLI da nuvem privada da AMP.

Usando o par de chaves configurado para SSH no dispositivo usando Linux

Etapa 1. Se os pares de chave privada e pública estiverem armazenados corretamente no caminho ~/.ssh, você deverá conseguir SSH para o dispositivo AMP Private Cloud simplesmente emitindo o comando ssh sem solicitar qualquer senha.

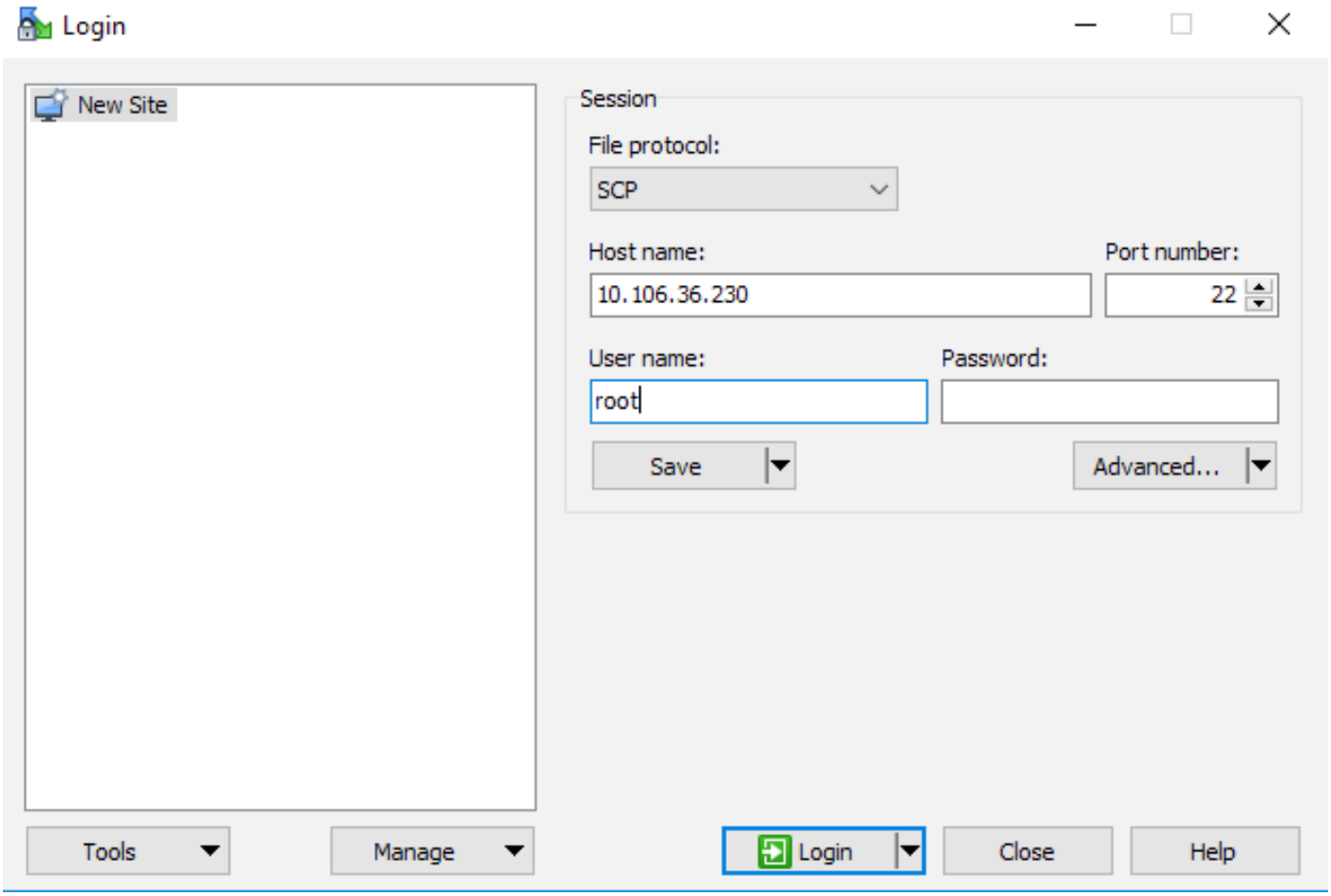
ssh root@<AMP-IP-ADDRESS>

```
[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 ~]#
```

Usando o WinSCP para interagir com o sistema de arquivos da AMP Private Cloud

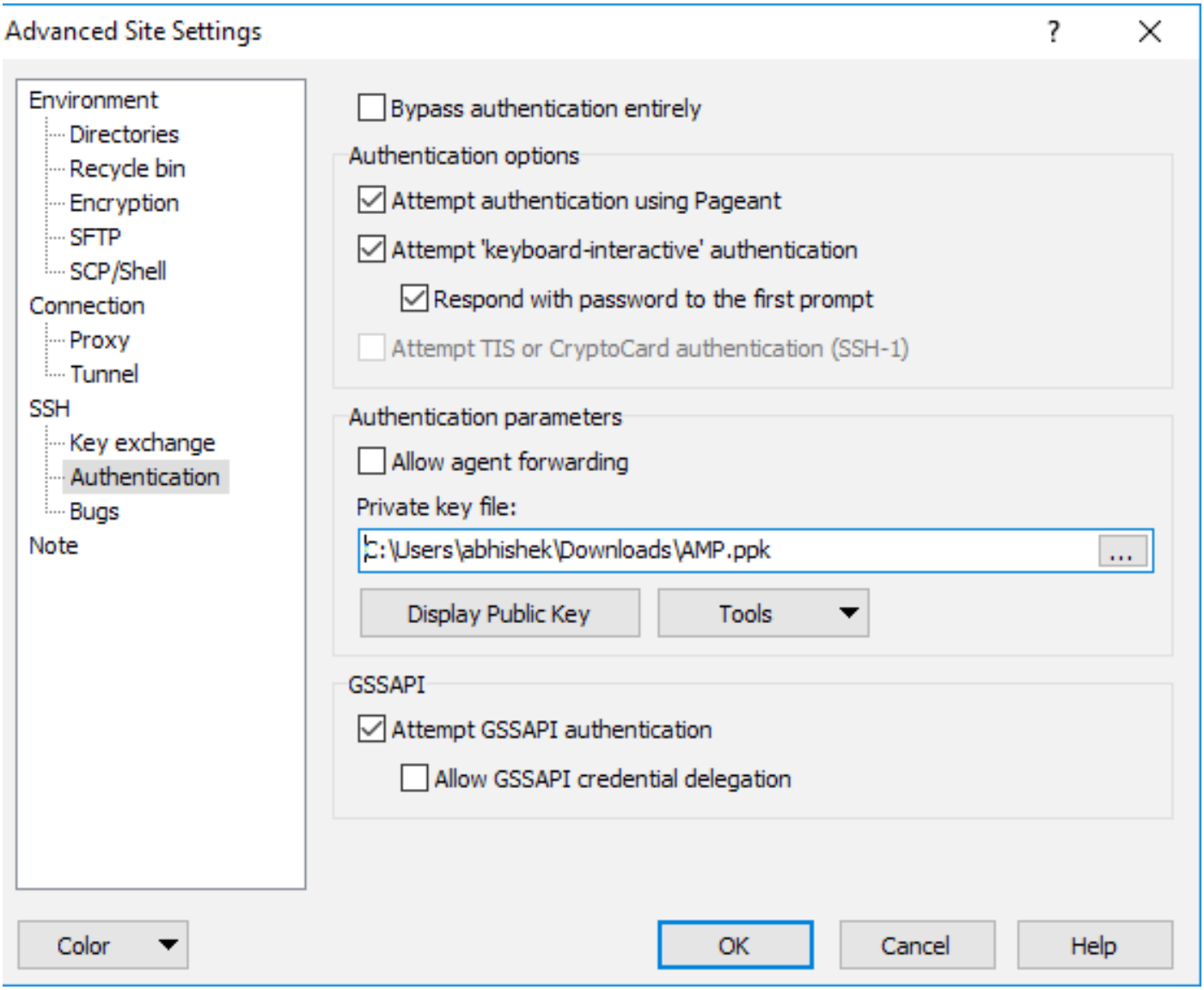
Etapa 1. Instale o WinSCP na sua máquina e inicie-o.

Etapa 2. Insira o endereço IP do AMP Private Cloud Administration Portal e selecione File Protocol como SCP. Digite o nome de usuário como raiz e deixe o campo senha.



Etapa 3. Selecione Avançado > Avançado > SSH > Autenticação

Etapa 4. Selecione o arquivo PPK que foi gerado como chave privada pelo PuTTYgen.



Etapa 5. Clique em OK e em Login. Você deve conseguir fazer login com êxito após aceitar o prompt.