通过SSH访问AMP私有云的CLI，并通过SCP传输文件

目录

简介

本文档介绍使用PuTTY和Linux外壳生成SSH密钥对、将其添加到AMP，然后访问CLI的过程。AMP私有云设备使用基于证书的身份验证通过SSH连接到设备。此处详细介绍快速生成密钥对以访问CLI和通过SCP(WinSCP)与文件系统交互的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- PuTTY
- WinSCP
- Linux/Mac外壳

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

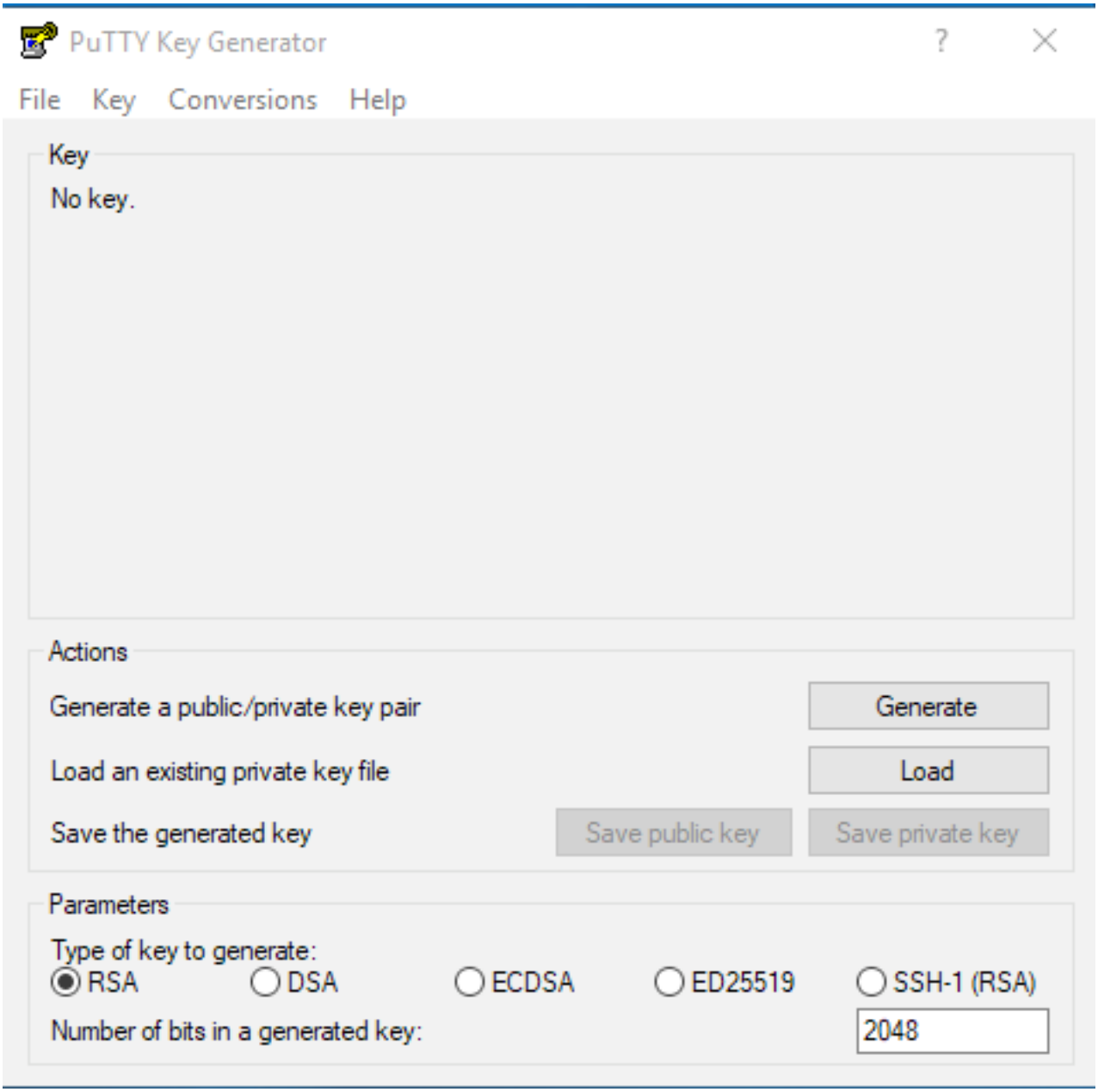
配置

第一步是使用PuTTY或Linux外壳生成RSA密钥对。此后，需要添加公钥并由AMP私有云设备信任。

使用PuTTY生成RSA密钥对

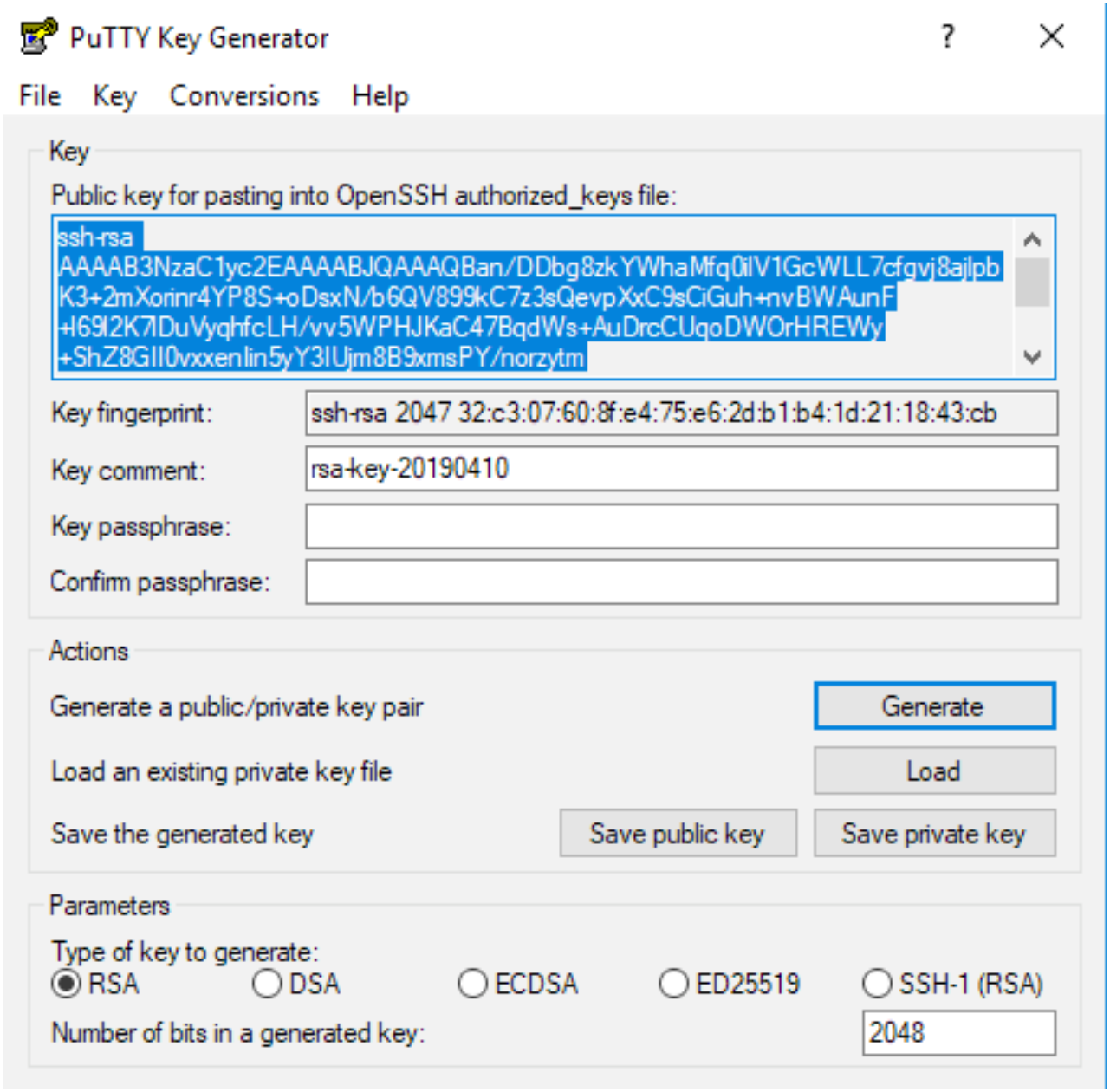
步骤1.确保已完全安装PuTTY。

步骤2.启动与PuTTY一起安装的PuTTYGen以生成RSA密钥对。

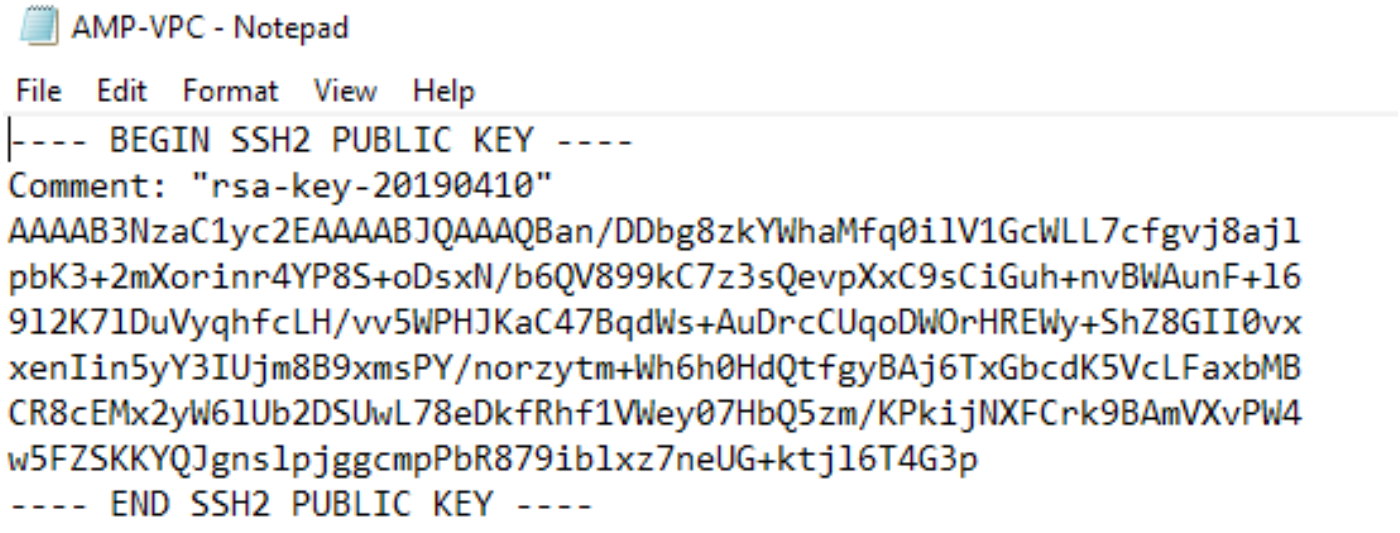


步骤3.点击Generate（生成）以随机移动光标以完成密钥对生成。

步骤4.选择“保存公钥”和“保存私钥”，后面的部分将使用它们，如图所示。



步骤5.使用记事本打开公钥，因为需要修改其格式，以便在AMP私有云管理门户中接受该公钥。



步骤6.删除以“ — BEGIN”开头的前2行和以“ — END”开头的最后2行

步骤7.删除所有换行符，将公钥内容作为一条连续的换行符。

步骤8.在文件开头输入“ssh-rsa”一词。保存文件。

使用Linux/Mac生成RSA密钥对

步骤1.在Linux/Mac CLI上，输入命令“ssh-keygen”

步骤2.输入所需参数，并在文件夹“~/.ssh”中生成RSA密钥对

```
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/w2ll/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$
```

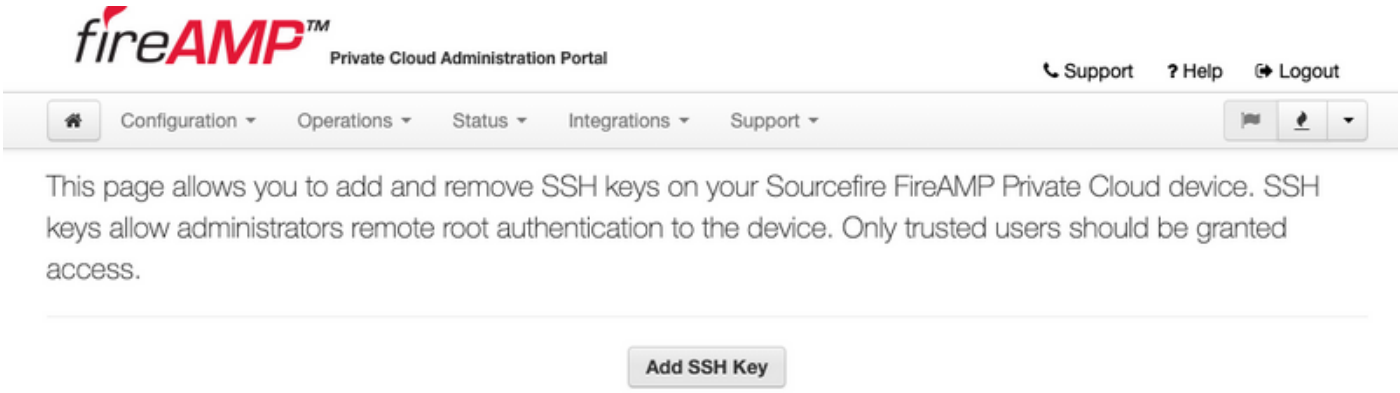
步骤3.如果打开公钥id_rsa.pub的内容，您可以看到它已采用所需的格式。

```
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$
```

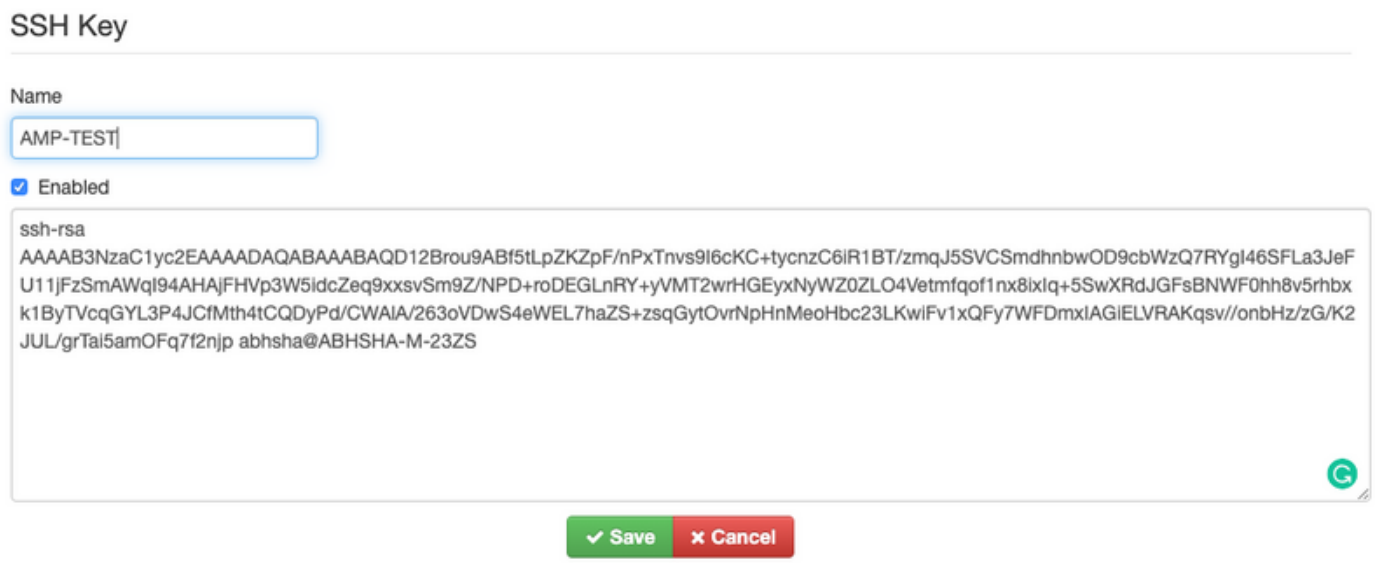
将生成的公钥添加到AMP私有云管理门户

步骤1.导航至AMP私有云管理门户>配置> SSH

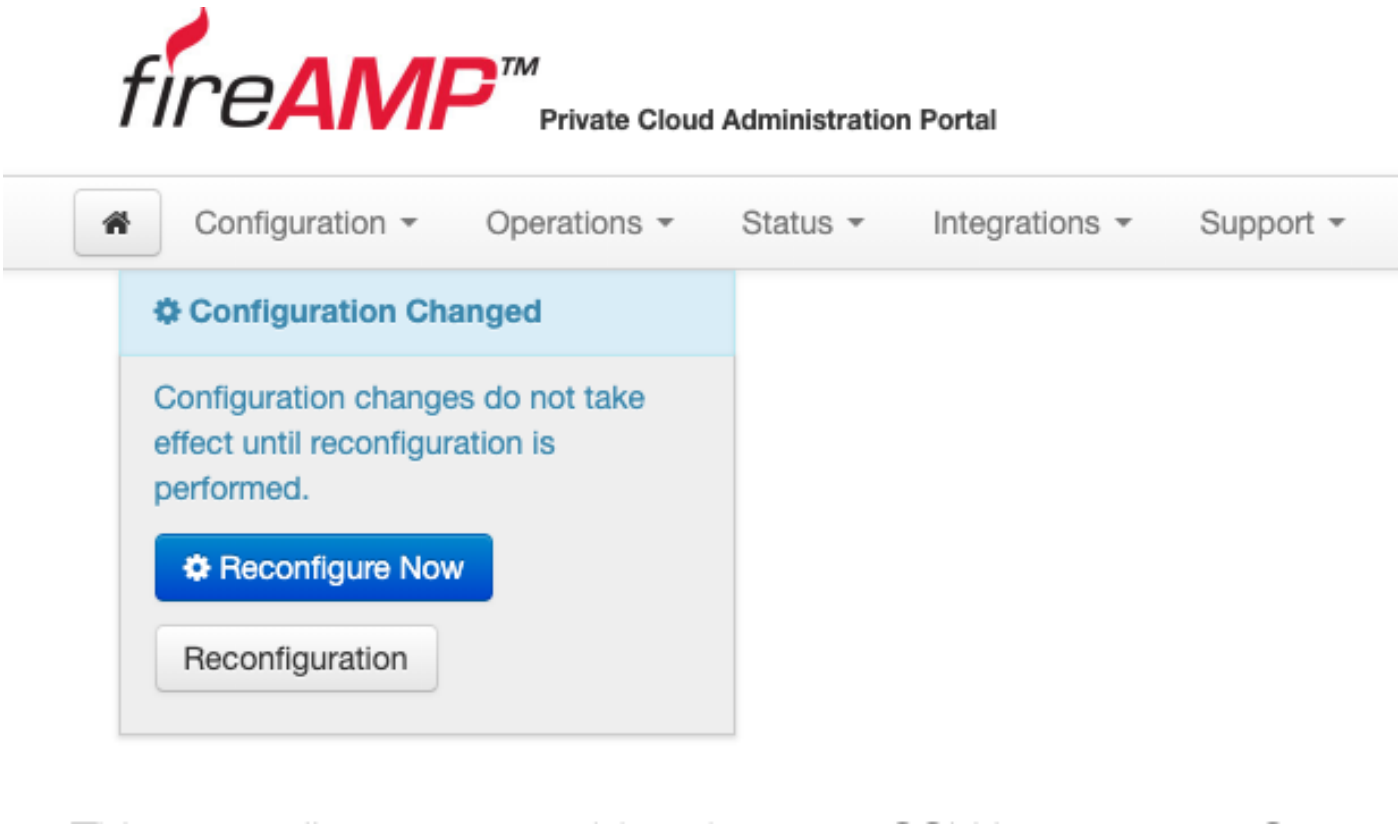
步骤2.点击“添加SSH密钥”



步骤3.添加公钥的内容并保存此内容。

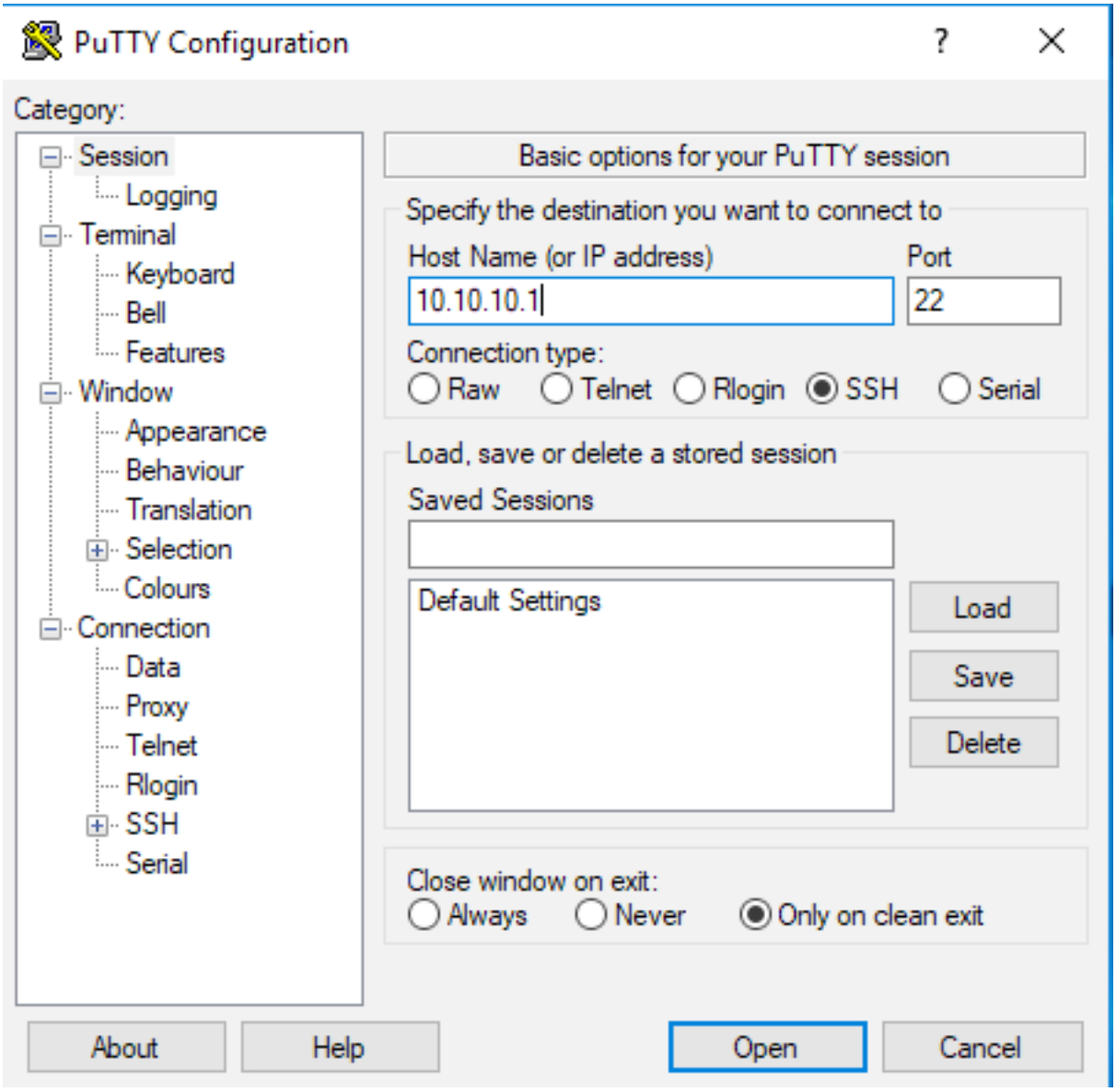


步骤4.保存完此信息后，请确保正在“重新配置”设备。



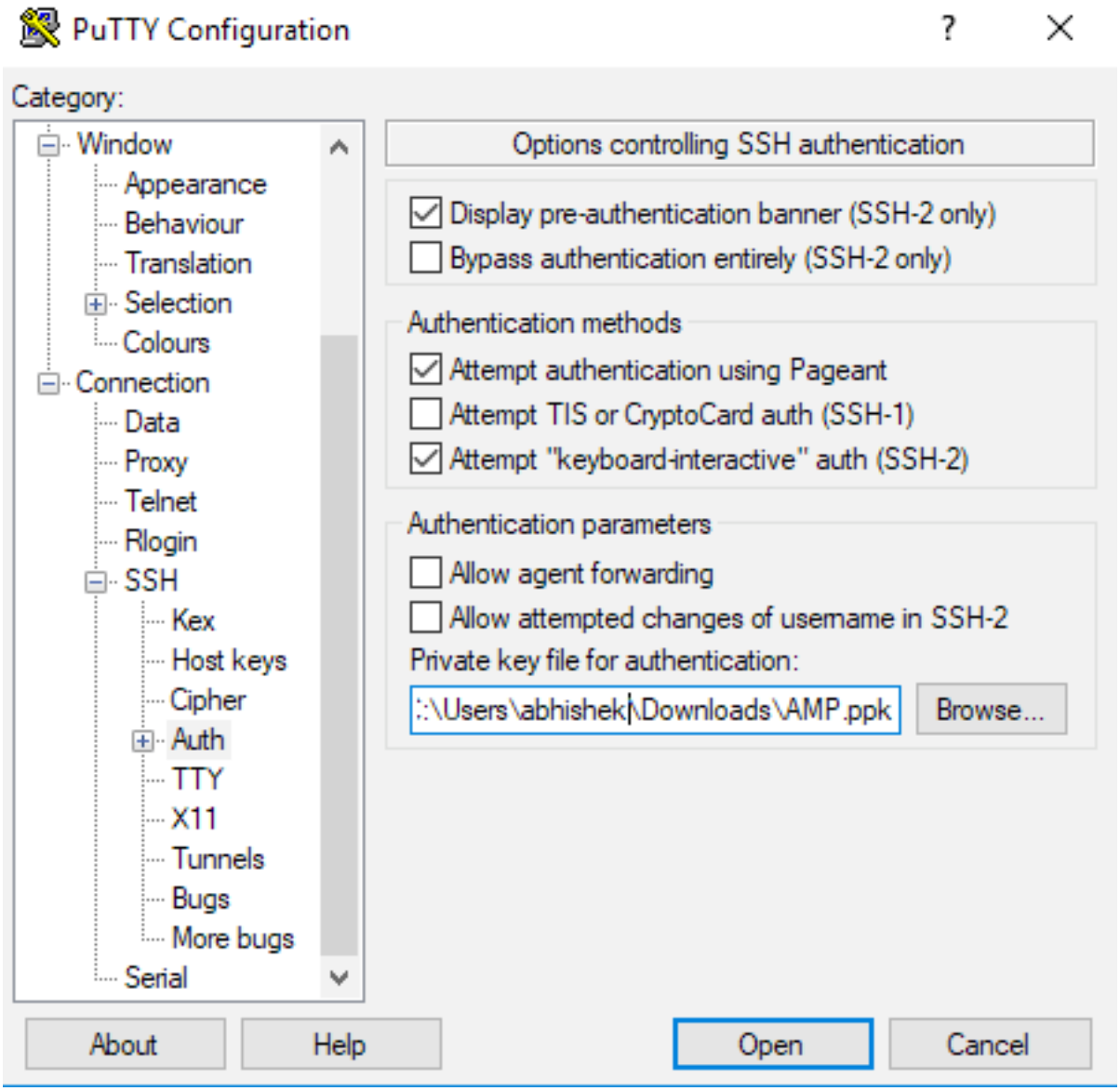
使用生成的密钥对使用PuTTY SSH连接到设备

步骤1.打开PuTTY并输入AMP私有云管理门户的IP地址。



步骤2.在左窗格中，选择Connection > SSH，然后点击Auth。

步骤3.选择由PuTTYGen生成的私钥。这是PPK文件。



步骤4.点击Open，当提示输入用户名时，输入“root”，您应该登录AMP私有云的CLI。

使用已配置的密钥对使用Linux SSH连接到设备

步骤1.如果私钥对和公钥对正确存储在~/.ssh路径中，则您应该能够通过发出ssh命令而不提示输入任何密码，从而对AMP私有云设备执行SSH。

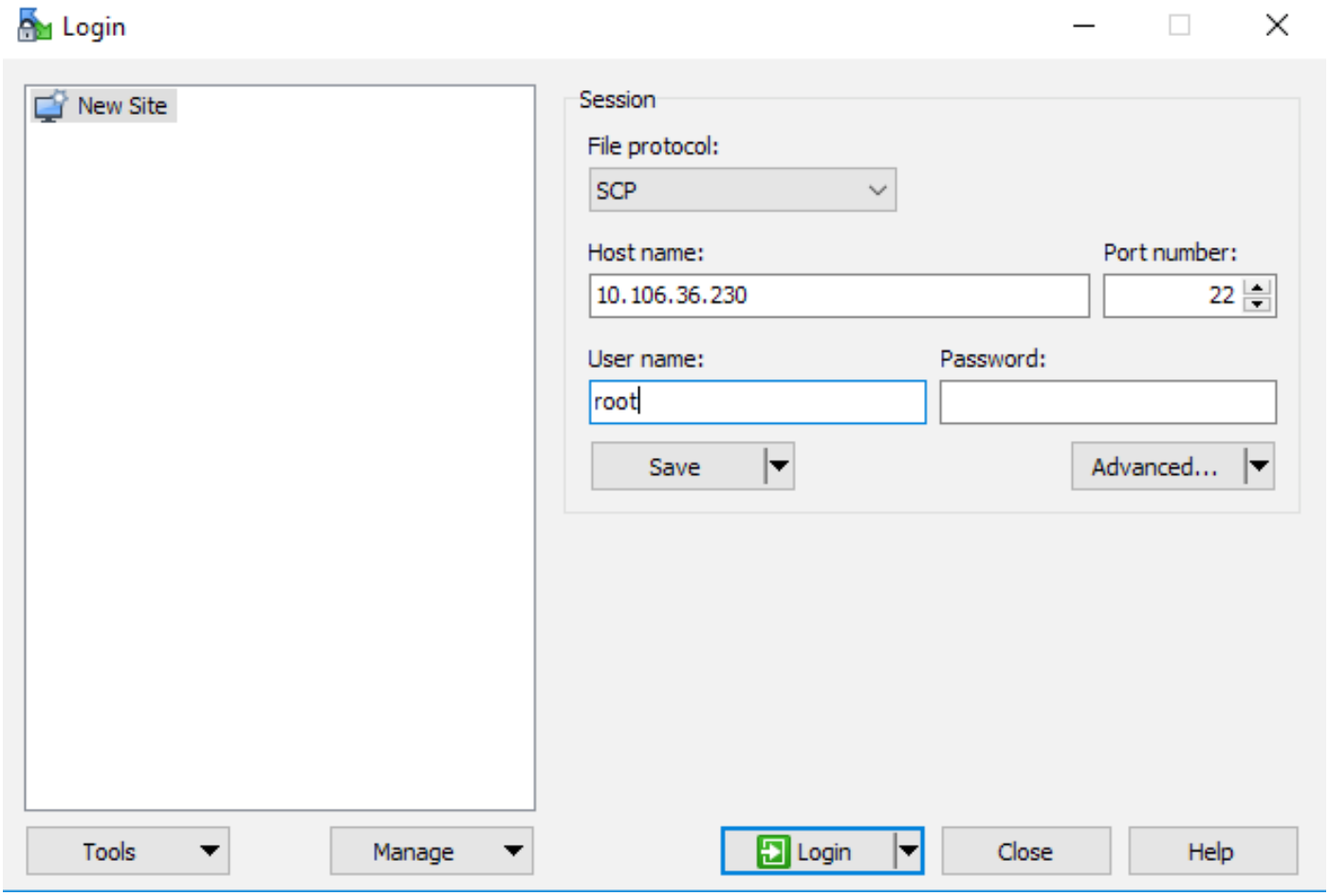
ssh root@<AMP-IP-ADDRESS>

```
[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 ~]#
```

使用WinSCP与AMP私有云的文件系统交互

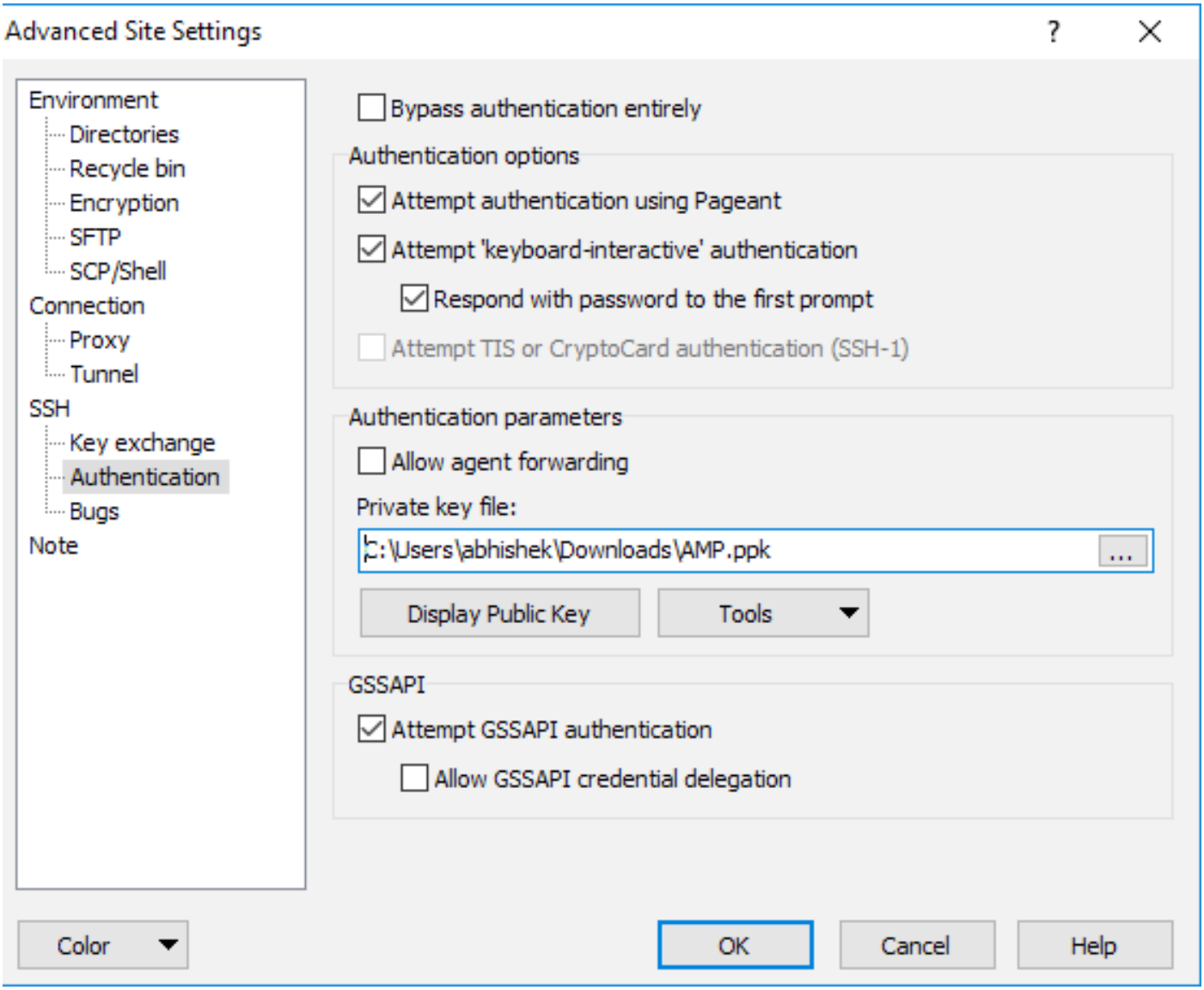
步骤1.在您的计算机上安装WinSCP并启动它。

步骤2.输入AMP私有云管理门户的IP地址，并选择File Protocol作为SCP。输入用户名为root并保留密码字段。



步骤3.选择Advanced > Advanced > SSH > Authentication

步骤4.选择由PuTTYgen生成为私钥的PPK文件。



步骤5.单击OK，然后单击Login。在接受提示后，您应该能够成功登录。