

SSH를 통해 AMP 프라이빗 클라우드의 CLI 액세스 및 SCP를 통해 파일 전송

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[PuTTY를 사용하여 RSA 키 쌍 생성](#)

[Linux/Mac을 사용하여 RSA 키 쌍 생성](#)

[생성된 공개 키를 AMP Private Cloud 관리 포털에 추가](#)

[PuTTY를 사용하여 어플라이언스에 SSH를 수행하려면 생성된 키 쌍을 사용합니다.](#)

[구성된 키 쌍을 사용하여 Linux를 사용하여 어플라이언스에 SSH를 적용합니다.](#)

[WinSCP를 사용하여 AMP Private Cloud의 파일 시스템과 상호 작용](#)

소개

이 문서에서는 PuTTY를 사용하여 SSH 키 쌍을 생성하고 Linux 셸을 사용하여 AMP에 추가한 다음 CLI에 액세스하는 절차에 대해 설명합니다. AMP Private Cloud 어플라이언스는 인증서 기반 인증을 사용하여 어플라이언스에 SSH를 적용합니다. CLI에 액세스하고 SCP(WinSCP)를 통해 파일 시스템과 상호 작용하기 위해 키 쌍을 신속하게 생성하는 절차는 여기에서 자세히 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- PuTTY
- WinSCP
- Linux/Mac 셸

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

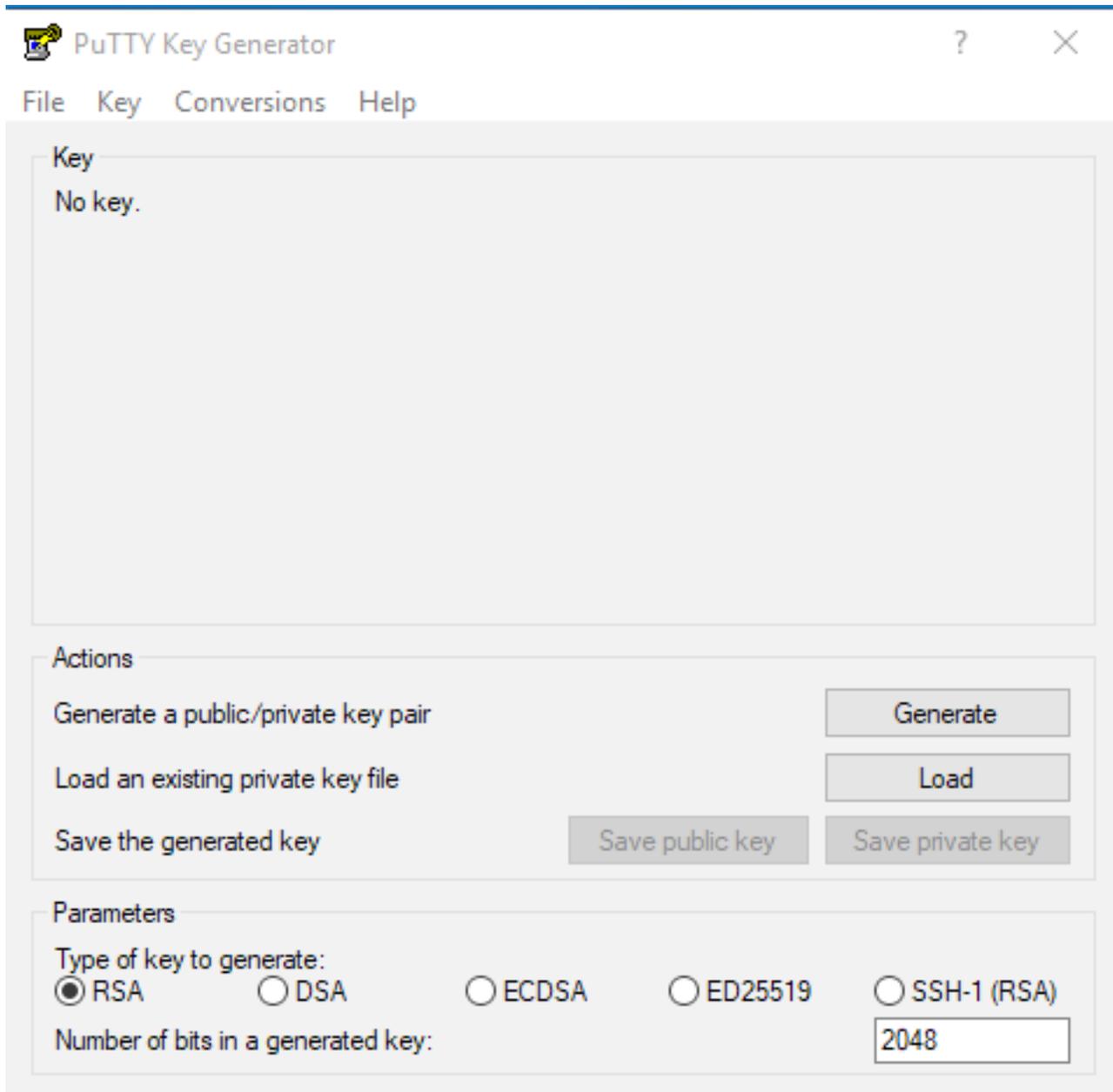
구성

첫 번째 단계에서는 PuTTY 또는 Linux 셸을 사용하여 RSA 키 쌍을 생성합니다.그런 다음 AMP Private Cloud Appliance에서 공개 키를 추가하고 신뢰해야 합니다.

PuTTY를 사용하여 RSA 키 쌍 생성

1단계. PuTTY를 완전히 설치했는지 확인합니다.

2단계. PuTTY와 함께 설치된 PuTTYGen을 실행하여 RSA 키 쌍을 생성합니다.



3단계. Generate(생성)를 클릭하여 커서를 임의로 이동하여 키 쌍 생성을 완료합니다.

4단계. 아래 이미지에 표시된 대로 다음 섹션에서 사용할 "공개 키 저장" 및 "개인 키 저장"을 선택합니다.



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

5단계. AMP Private Cloud Administration Portal에서 수락하려면 형식을 수정해야 하므로 Notepad를 사용하여 공개 키를 엽니다.



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 -----

6단계. "—BEGIN"으로 시작하는 처음 2개 행과 "— END"로 시작하는 마지막 줄을 제거합니다.

7단계. 모든 줄 바꿈을 제거하여 공개 키 콘텐츠를 단일 연속 줄로 만듭니다.

8단계. 파일의 시작 부분에 "ssh-rsa"라는 단어를 입력합니다.파일을 저장합니다.



Linux/Mac을 사용하여 RSA 키 쌍 생성

1단계. Linux/Mac CLI에서 "ssh-keygen" 명령을 입력합니다.

2단계. 필요한 매개변수를 입력하면 "~/.ssh" 폴더에 RSA 키 쌍이 생성됩니다.

```
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$
```

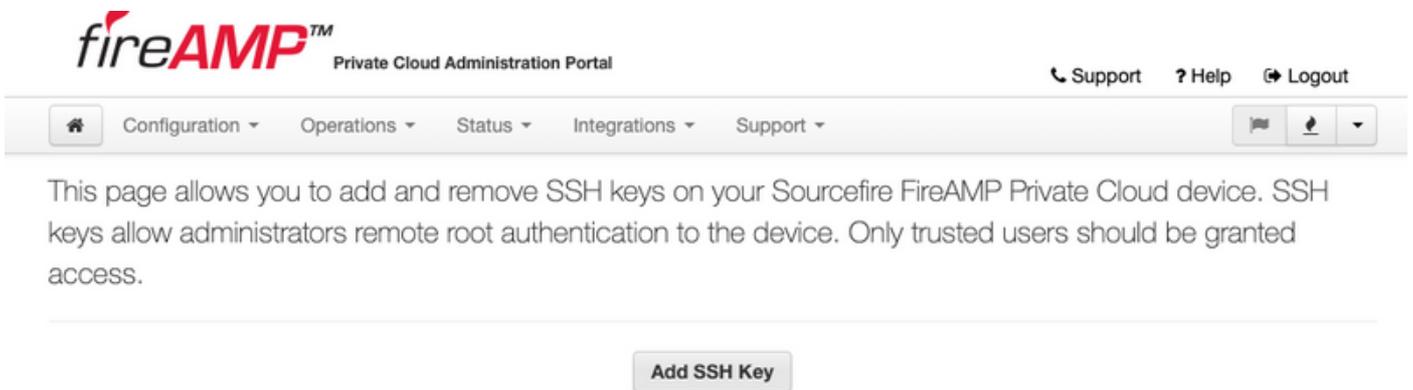
3단계. 공개 키인 id_rsa.pub의 내용을 열면 해당 내용이 이미 필수 형식임을 확인할 수 있습니다.

```
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
JL/grTai5amOFq7f2njp abhsha@ABHSHA-M-23ZS
ABHSHA-M-23ZS: .ssh abhsha$
```

생성된 공개 키를 AMP Private Cloud 관리 포털에 추가

1단계. AMP Private Cloud Administration Portal(AMP 프라이빗 클라우드 관리 포털) > Configuration(컨피그레이션) > SSH로 이동합니다.

2단계. "SSH 키 추가"를 클릭합니다.



3단계. 공개 키의 내용을 추가하고 저장합니다.

SSH Key

Name

AMP-TEST

Enabled

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQD12Brou9ABf5tLpZKZpF/nPxTnvs9I6cKC+tycnzC6iR1BT/zmqJ5SVCSmdhnbwOD9cbWzQ7RYgI46SFLa3JeF
U11jFzSmAWqI94AHAjFHVp3W5idcZeq9xxsvSm9Z/NPD+roDEGLnRY+yVMT2wrHGEyxNyWZ0ZL04Vetmfqof1nx8ixIq+5SwXRdJGFsBNWF0hh8v5rhbX
k1ByTVcqGYL3P4JCfMth4tCQDyPd/CWAIA/263oVDwS4eWEL7haZS+zsqGytOvrNpHnMeoHbc23LKwiFv1xQFy7WFDmxIAGiELVRAKqsv//onbHz/zG/K2
JL/grTai5amOFq7f2njp abhsha@ABHSHA-M-23ZS
```

✓ Save ✕ Cancel

4단계. 저장된 후 어플라이언스를 "재구성"하는지 확인합니다.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

⚙ Configuration Changed

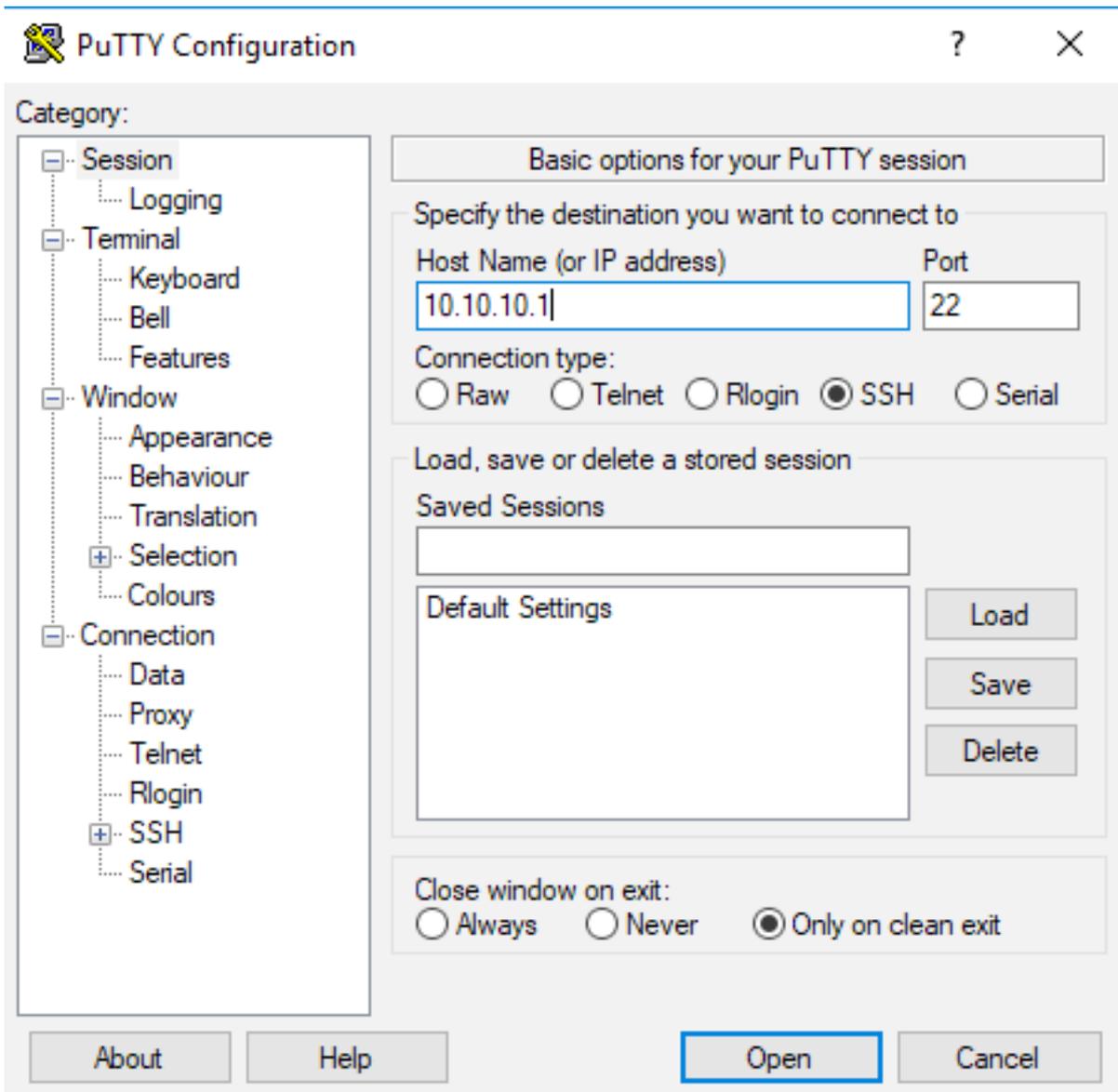
Configuration changes do not take effect until reconfiguration is performed.

⚙ Reconfigure Now

Reconfiguration

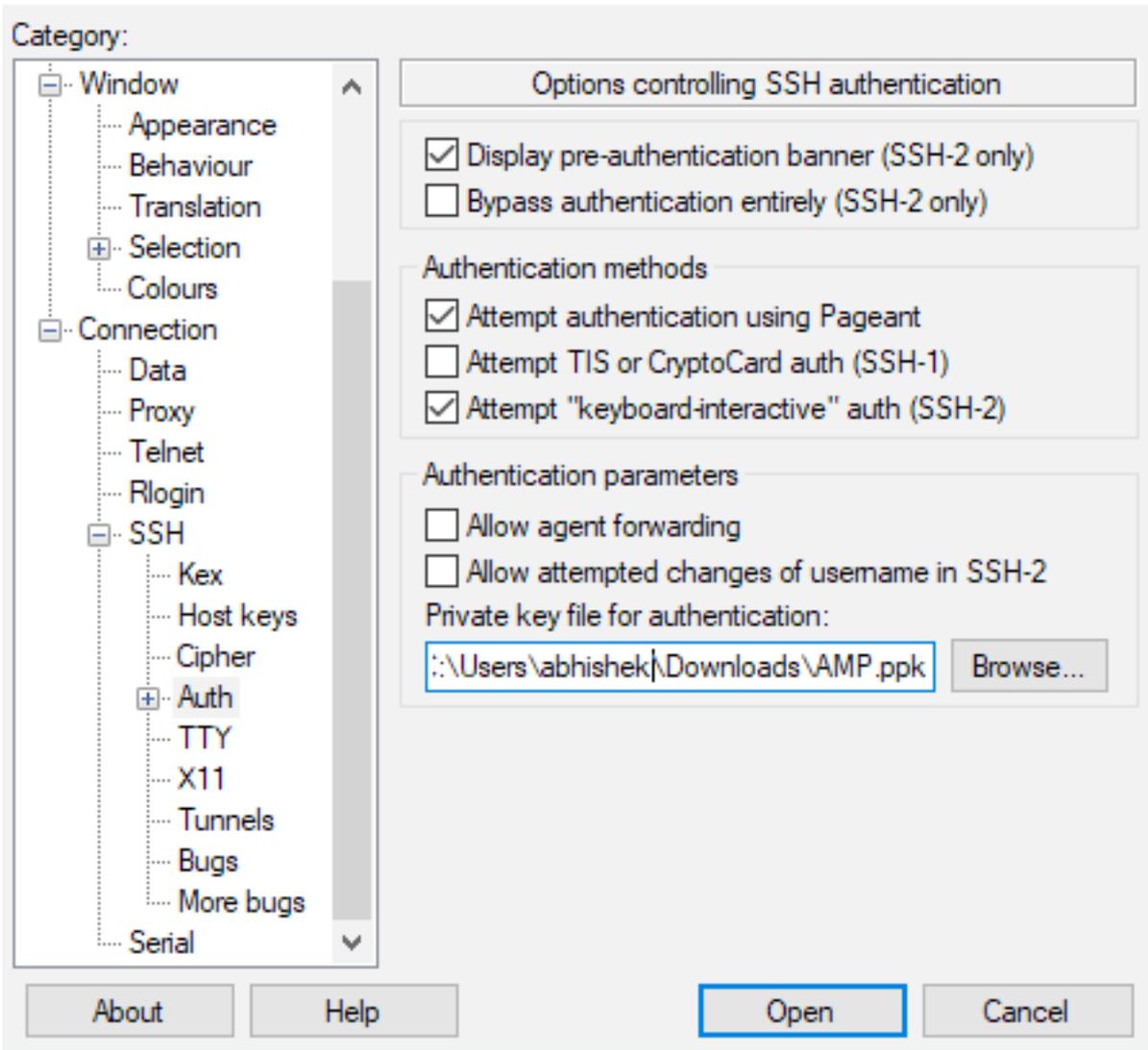
PuTTY를 사용하여 어플라이언스에 SSH를 수행하려면 생성된 키쌍을 사용합니다.

1단계. PuTTY를 열고 AMP Private Cloud Administration 포털의 IP 주소를 입력합니다.



2단계. 왼쪽 창에서 Connection(연결) > SSH를 선택하고 Auth(인증)를 클릭합니다.

3단계. PuTTYGen에서 생성된 Private Key(개인 키)를 선택합니다.PPK 파일입니다.



4단계. Open(열기)을 클릭하고 사용자 이름을 묻는 메시지가 나타나면 "root(루트)"를 입력하고 AMP Private Cloud의 CLI에 있어야 합니다.

구성된 키 쌍을 사용하여 Linux를 사용하여 어플라이언스에 SSH를 적용합니다.

1단계. 프라이빗 및 퍼블릭 키 쌍이 ~/.ssh 경로에 올바르게 저장되어 있는 경우 비밀번호를 입력하지 않고 ssh 명령을 실행하여 AMP Private Cloud 어플라이언스에 SSH를 실행할 수 있어야 합니다.

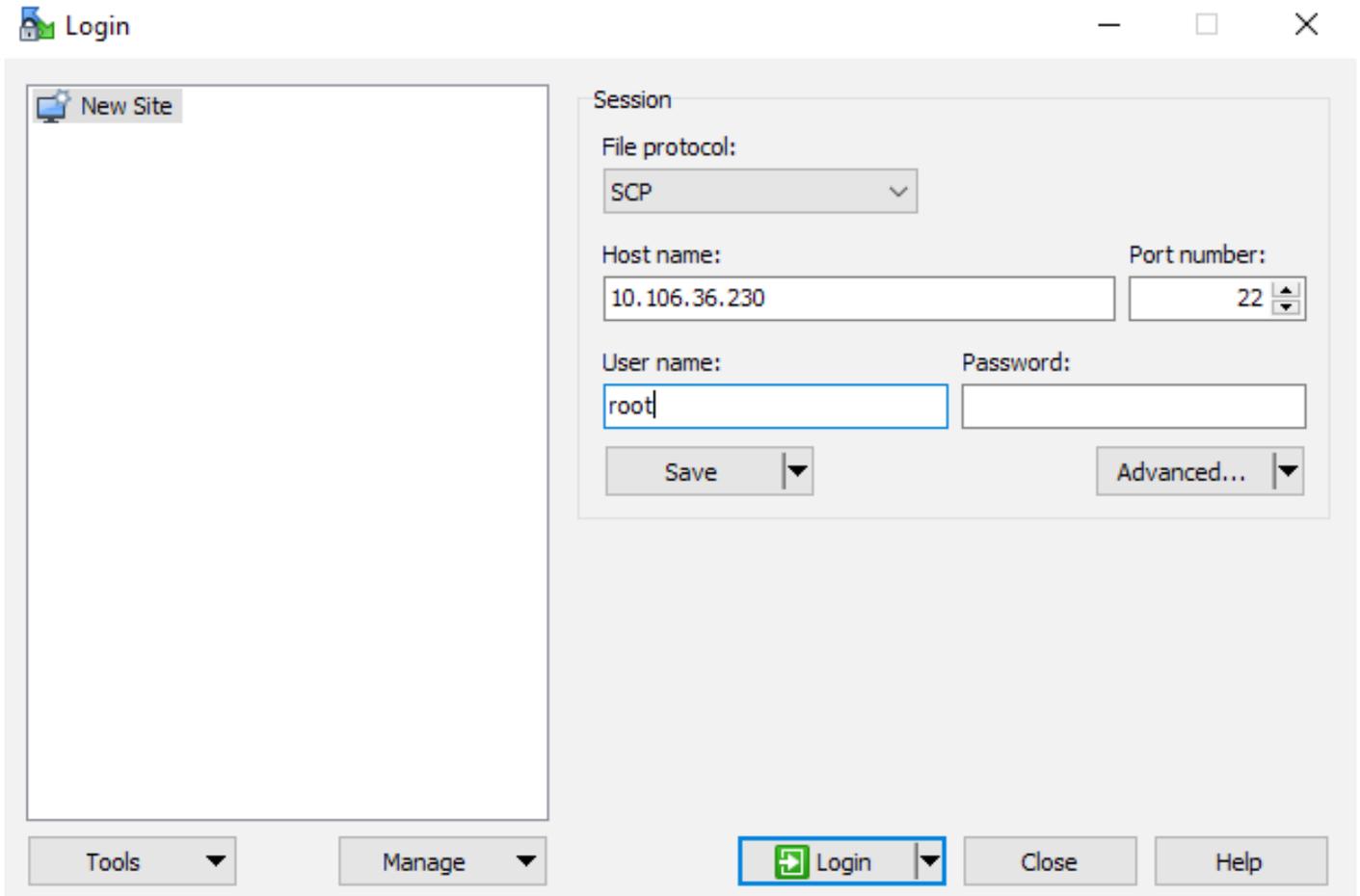
```
ssh root@<AMP-IP-ADDRESS>
```

```
[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 ~]#
```

WinSCP를 사용하여 AMP Private Cloud의 파일 시스템과 상호 작용

1단계. 컴퓨터에 WinSCP를 설치하고 시작합니다.

2단계. AMP Private Cloud Administration Portal의 IP 주소를 입력하고 File Protocol(파일 프로토콜)을 SCP로 선택합니다. 사용자 이름을 root로 입력하고 비밀번호 필드를 그대로 둡니다.



3단계. Advanced > Advanced > SSH > Authentication을 선택합니다.

4단계. PuTTYgen에서 개인 키로 생성된 PPK 파일을 선택합니다.

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

5단계. OK(확인)를 클릭한 다음 Login(로그인)을 클릭합니다.프롬프트를 수락한 후 성공적으로 로그인할 수 있어야 합니다.