

Toegang tot de CLI van Advanced Malware Protection Private Cloud via SSH en Bestanden overdragen via SCP

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Een RSA-sleutelpaar genereren met PuTTY](#)

[Een RSA-sleutelpaar genereren met Linux/Mac](#)

[De gegenereerde publieke toetsen aan het AMP Private Cloud Management Portal toevoegen](#)

[Gebruik het gegenereerde sleutelpaar om SSH in het apparaat te activeren met PuTTY](#)

[De ingestelde toetsencombinatie met SSH in het apparaat gebruiken met behulp van Linux](#)

[WinSCP gebruiken om te reageren met het bestandssysteem van AMP Private Cloud](#)

Inleiding

Dit document beschrijft de procedure om een SSH-sleutelpaar te genereren met behulp van PuTTY en een Linux-shell, voegt deze toe aan AMP en heeft dan toegang tot de CLI. AMP Private Cloud Appliance maakt gebruik van op certificaten gebaseerde verificatie om SSH in het apparaat te installeren. De procedure om snel een sleutelpaar te genereren, om toegang te hebben tot de CLI en om met het bestandssysteem te communiceren via SCP (WinSCP) is hier gedetailleerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- PuTTY
- WinSCP
- Linux/Mac shell

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

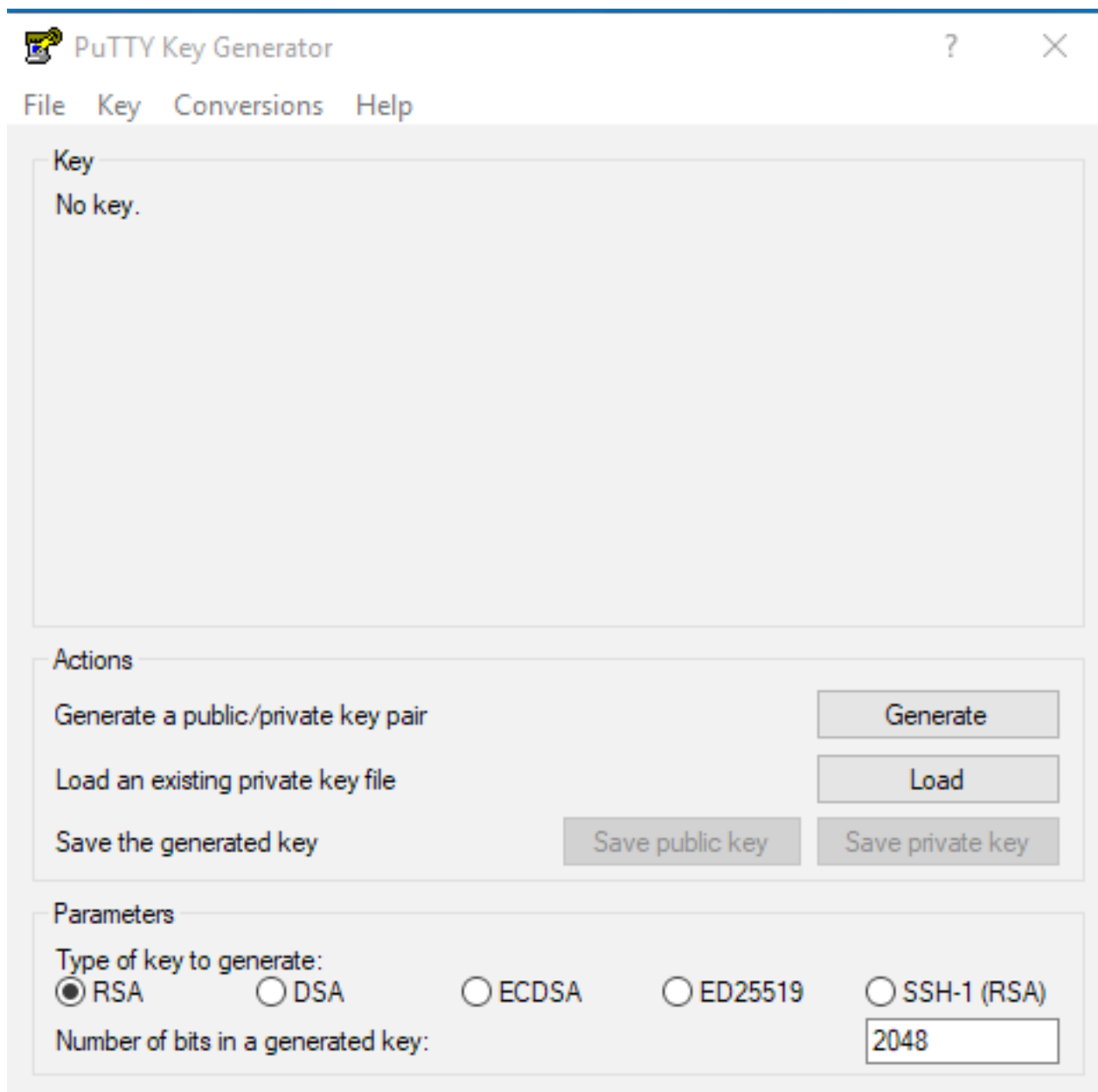
Configureren

De eerste stap bestaat uit het genereren van een RSA-sleutelpaar met behulp van PuTTY of Linux shell. Hierna moet de openbare sleutel worden toegevoegd en vertrouwd door de Advanced Malware Protection Private Cloud Appliance.

Een RSA-sleutelpaar genereren met PuTTY

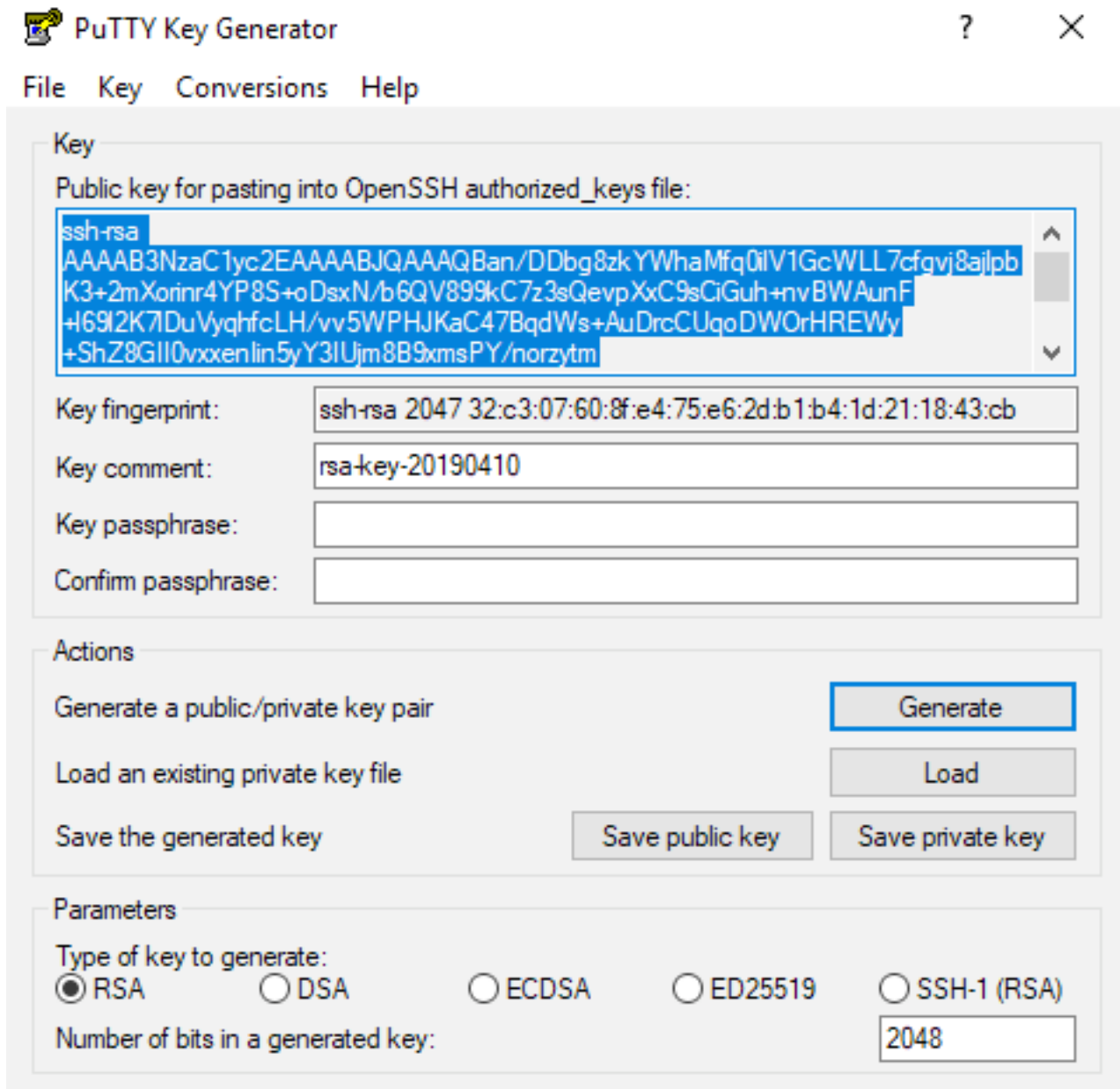
Stap 1. Zorg ervoor dat u PuTTY volledig hebt geïnstalleerd.

Stap 2. Start PuTYGen die samen met PuTTY is geïnstalleerd om het RSA-sleutelpaar te genereren.



Stap 3. Klik op Generate to en verplaats de cursor om de sleutelgeneratie te voltooien.

Stap 4. Klik op "Save public key" en "Save private key", die in de latere secties moet worden gebruikt, zoals in de afbeelding hier.



Stap 5. Open de openbare toets met Kladblok omdat het formaat moet worden gewijzigd zodat deze in AMP Private Cloud Administration Portal kan worden geaccepteerd.

AMP-VPC - Notepad

File Edit Format View Help

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: "rsa-key-20190410"  
AAAAB3NzaC1yc2EAAAABJQAAAQBan/DDbg8zkYWhaMfq0ilV1GcWLL7cfgvj8ajl  
pbK3+2mXorinr4YP8S+oDsxN/b6QV899kC7z3sQevpXxC9sCiGuh+nvBWAunF+16  
912K71DuVyqhfcLH/vv5WPHJKaC47BqdWs+AuDrcCUqoDWOrHREWy+ShZ8GII0vx  
xenIin5yY3IUjm8B9xmsPY/norzytm+Wh6h0HdQtfgyBAj6TxGbcdK5VcLFaxbMB  
CR8cEMx2yW61Ub2DSUwL78eDkFRhf1Vwey07HbQ5zm/KPkijNXFCrk9BAmVXvPW4  
w5FZSKKYQJgns1pjggcmpPbR879ib1xz7neUG+ktj16T4G3p  
----- END SSH2 PUBLIC KEY -----
```

Stap 6. Verwijder de eerste 2 lijnen die beginnen met "—BEGIN" en de laatste regel die begint met "— END"

Stap 7. Verwijder alle regeleinden om de openbare basisinhoud als één doorlopende lijn te maken.

Stap 8. Voer het woord "ssh-rsa" in aan het begin van het bestand. Sla het bestand op.

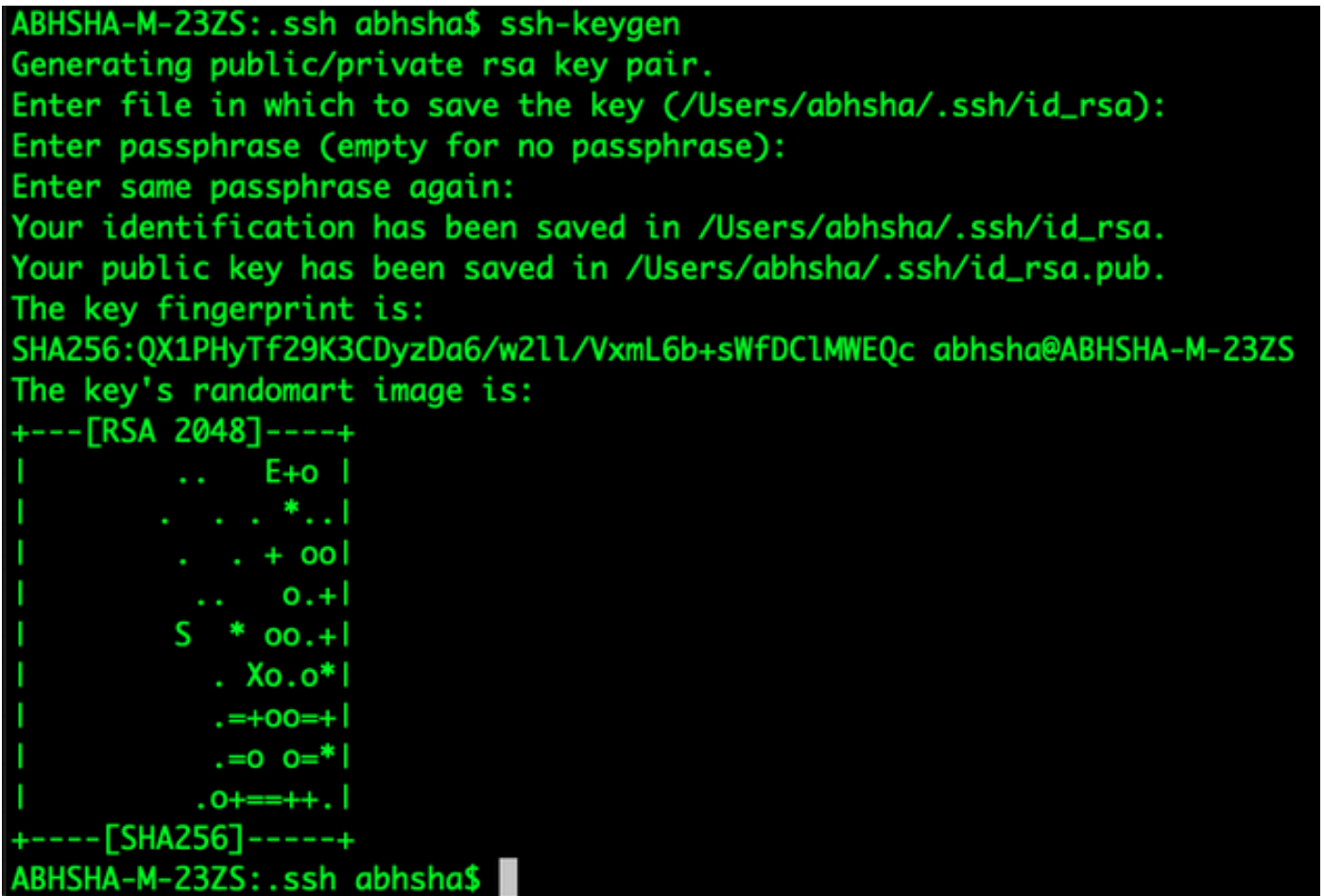


```
AMP-VPC - Notepad
File Edit Format View Help
ssh-rsa AAAAB3NzaC1yc2EAAAQBAn/DObg8zkYwHaMfq0i1V1GcLL7c fgvj8aj1pbK3+2mXon1nr4YP85+oDsxdI/b6QV899kc7z3sQevpXxC9sC1Guh+nv8NAunF+16912K71DuVyqhfcLH/vv5hPHJKaC47BqdWs
+AuDrcUgoDw0rHREHy+ShZ8GII0vxxenIIn5yY3IUj=889xmsPY/norzyt
m+Wh6h0HdQtfgyBAj6TxGbcdK5VcLFaxbHBCRBcEMx2yw61Ub2DSUwL78eDkFRhf1VWey07HbQ5zm/KPk1jIXFCrk9BAmXvPW4w5FZSKKYQJgns1pjggcmpPbR879ib1xz7neUG+ktj16T4G3p
```

Een RSA-sleutelpaar genereren met Linux/Mac

Stap 1. Voer in de Linux/Mac CLI de opdracht "Sh-keygen" in

Stap 2. Voer de gewenste parameters in en hiermee wordt het RSA-sleutelpaar op de map "~/.ssh" gegenereerd



```
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$
```

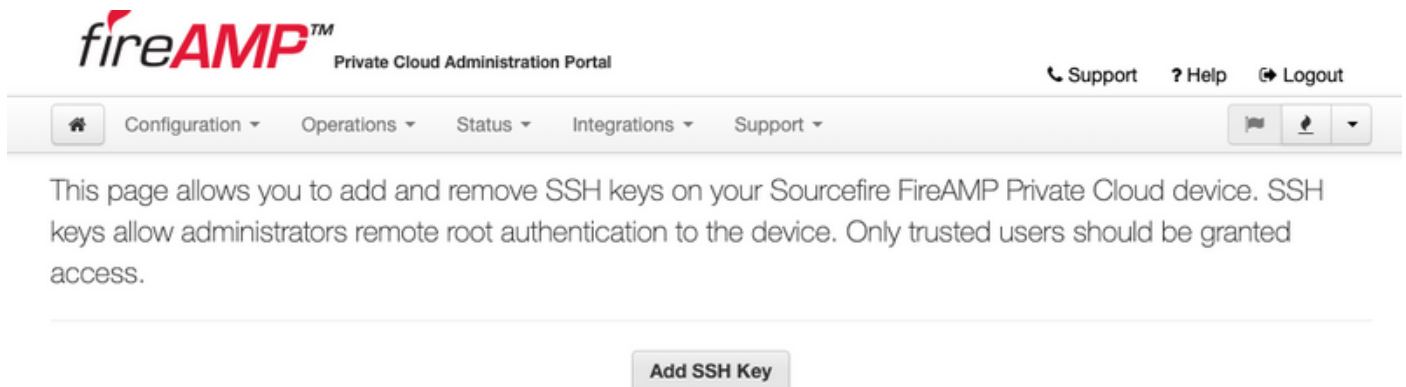
Stap 3. Als u de inhoud van id_rsa.pub opent, wat de openbare sleutel is, kunt u zien dat deze al in het vereiste formaat zit.

```
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$
```

De gegenereerde publieke toetsen aan het AMP Private Cloud Management Portal toevoegen

Stap 1. Navigeer naar het Advanced Malware Protection Private Cloud Management Portal > Configuration > SSH

Stap 2. Klik op "SSH-toets toevoegen"



Stap 3. Voeg de inhoud van de openbare toets toe en bewaar deze.

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

Stap 4. Zorg ervoor dat u het apparaat "opnieuw configureren" hebt nadat u dit hebt opgeslagen.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

Configuration Changed

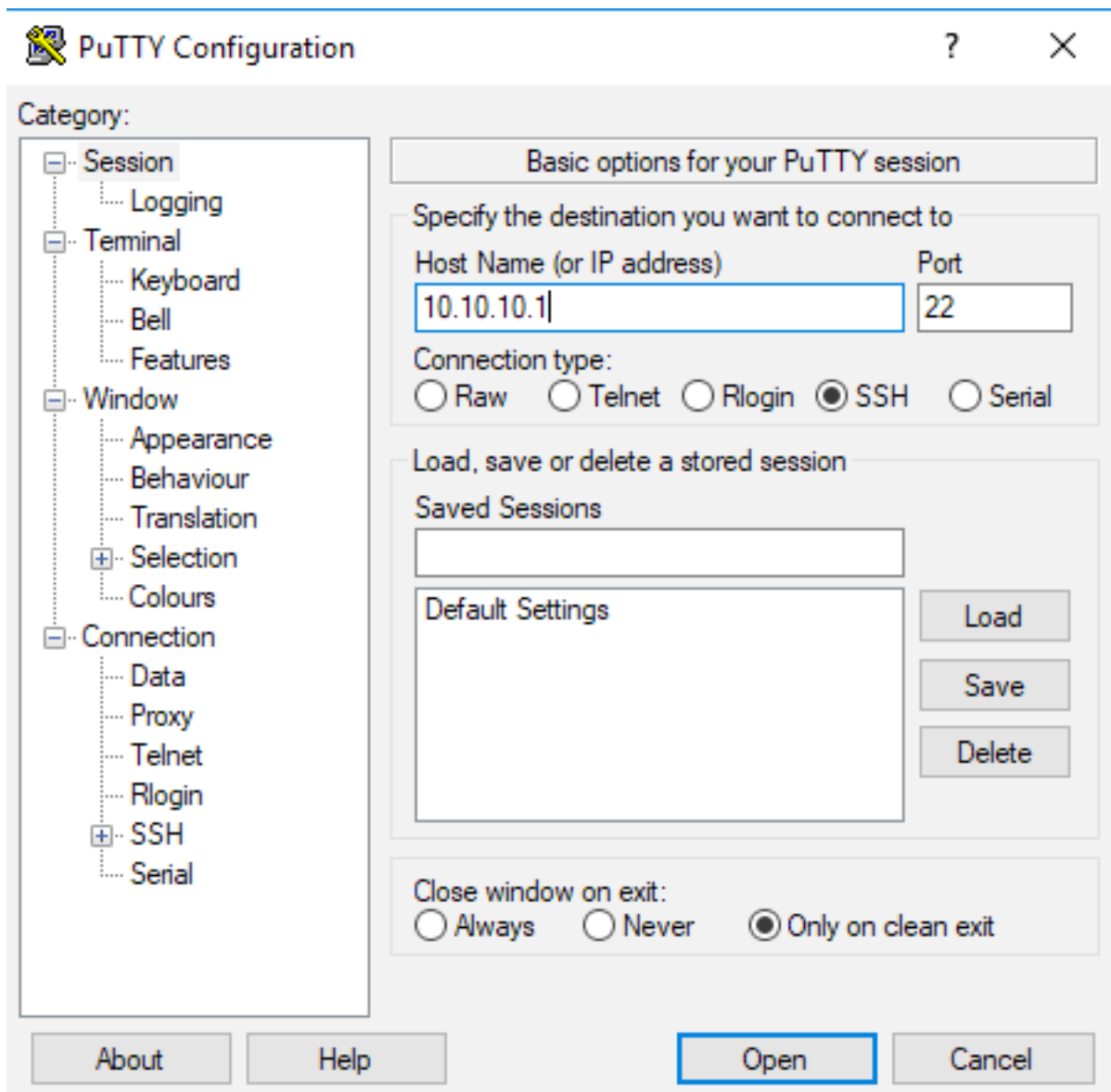
Configuration changes do not take effect until reconfiguration is performed.

 **Reconfigure Now**

Reconfiguration

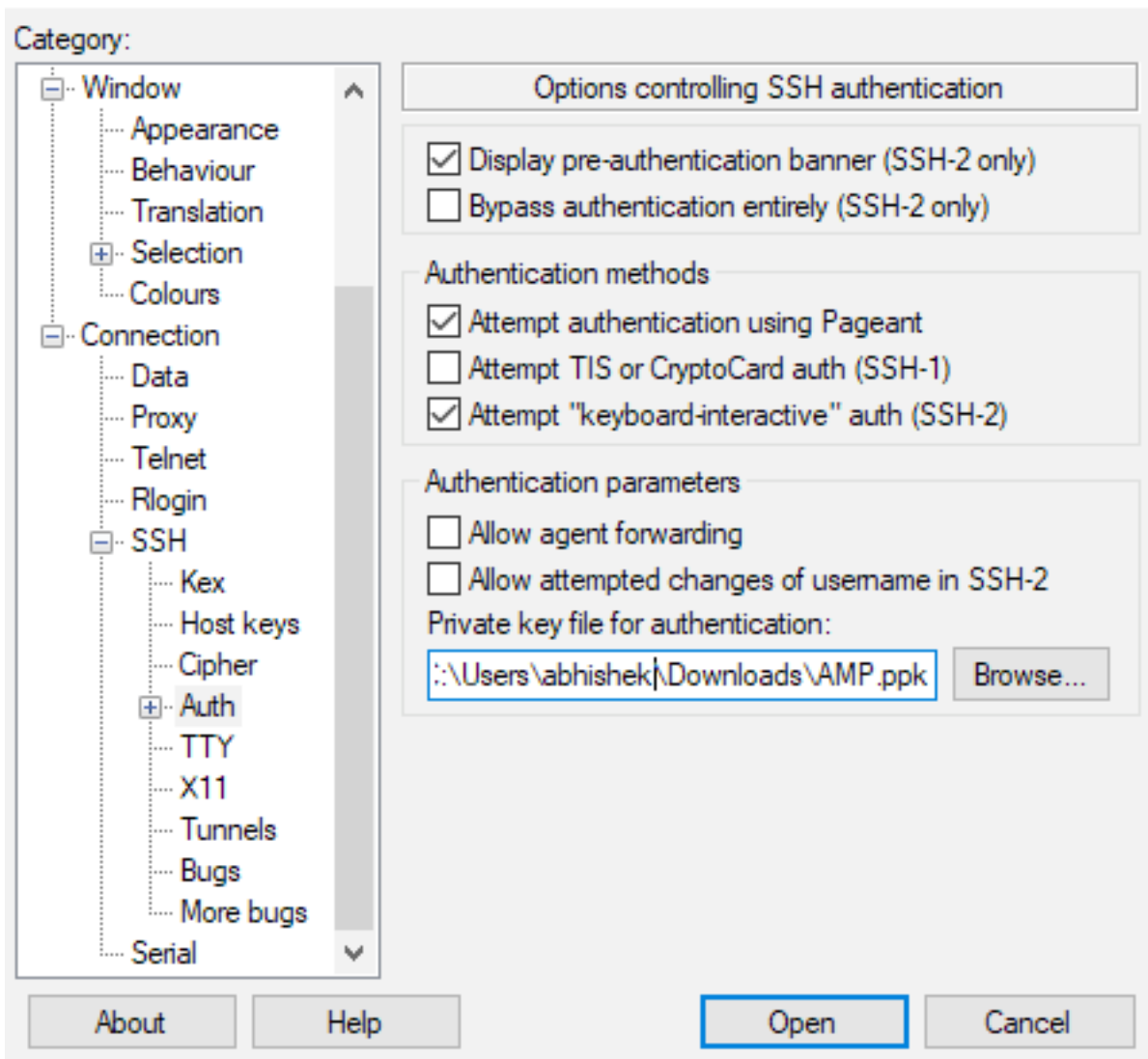
Gebruik het gegenereerde sleutelpaar om SSH in het apparaat te activeren met PuTTY

Stap 1. Open de PuTTY en voer het IP-adres van het Advanced Cloud Management-portal in.



Stap 2. Selecteer in het linker deelvenster een optie Connection > SSH en klik op in augustus.

Stap 3. Selecteer de particuliere sleutel die door PuTTYGen gegenereerd is. Dit is een PPK-bestand.



Stap 4. Klik op Open en wanneer u een gebruikersnaam voor de gebruiker vraagt, voer dan "wortel" in en u moet landen bij de CLI van de Advanced Malware Protection Private Cloud.

De ingestelde toetsencombinatie met SSH in het apparaat gebruiken met behulp van Linux

Stap 1. Als de privaat- en publieke sleutelparen correct zijn opgeslagen op `~/.ssh-pad`, dan dient u in staat te zijn SSH aan het Advanced Malware Protection Private Cloud Appliance te leveren door de ssh-opdracht eenvoudig uit te geven zonder u om een wachtwoord te vragen.

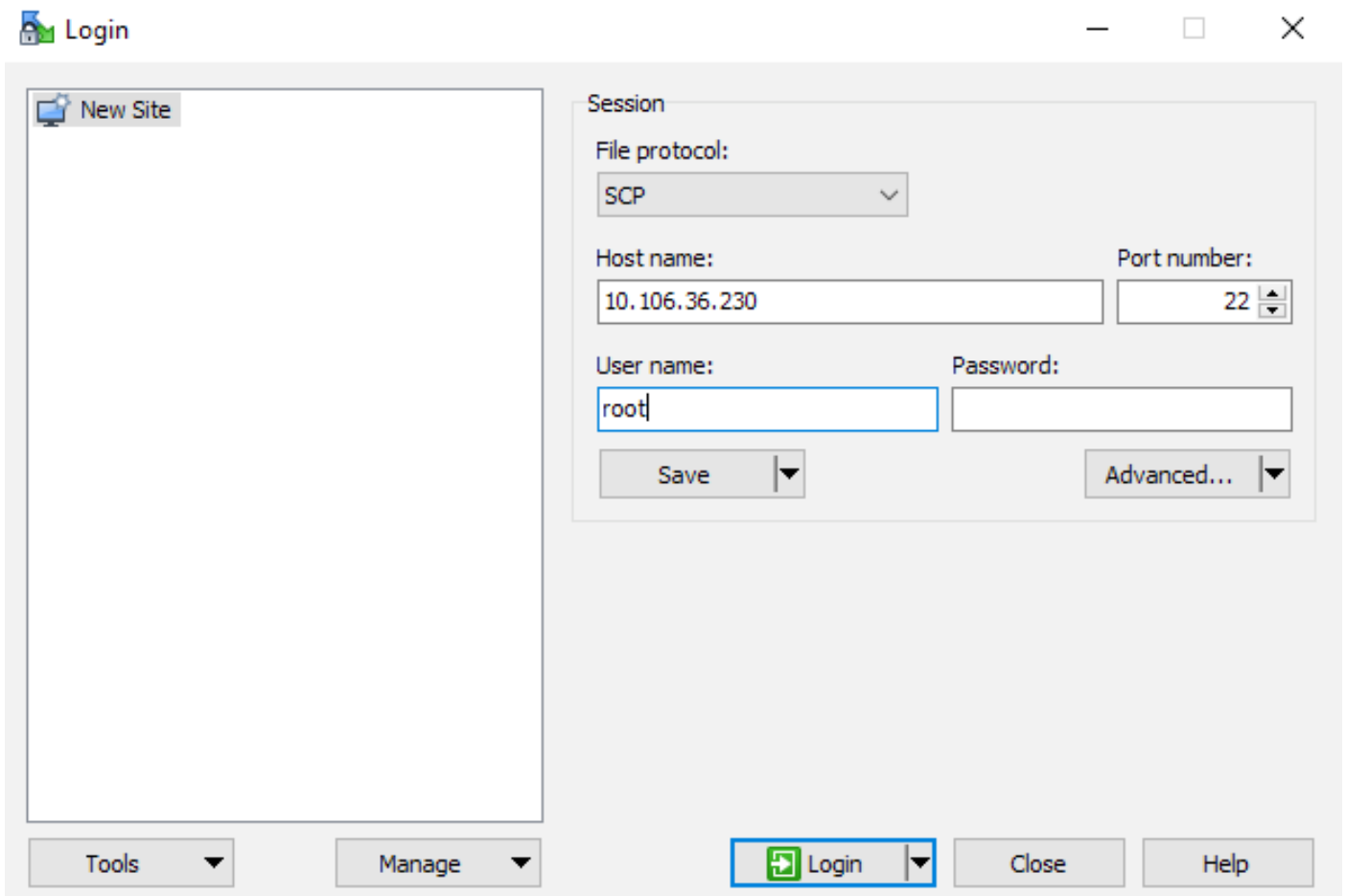
Bron: @<AMP-IP-ADRES>


```
[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 ~]#
```

WinSCP gebruiken om te reageren met het bestandssysteem van AMP Private Cloud

Stap 1. Installeer WinSCP op uw computer en start het programma.

Stap 2. Voer het IP-adres in van het Advanced Malware Protection Private Cloud Management Portal en selecteer het File Protocol als SCP. Typ de gebruikersnaam als wortel en laat het wachtwoordveld achter.



Stap 3. Selecteer Geavanceerd > Geavanceerd > SSH > Verificatie

Stap 4. Selecteer het PPK-bestand dat door PuTTYgen als privésleutel is gegenereerd.

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

Stap 5. Klik op OK en vervolgens op Aanmelden. U kunt pas inloggen nadat u de melding hebt geaccepteerd.