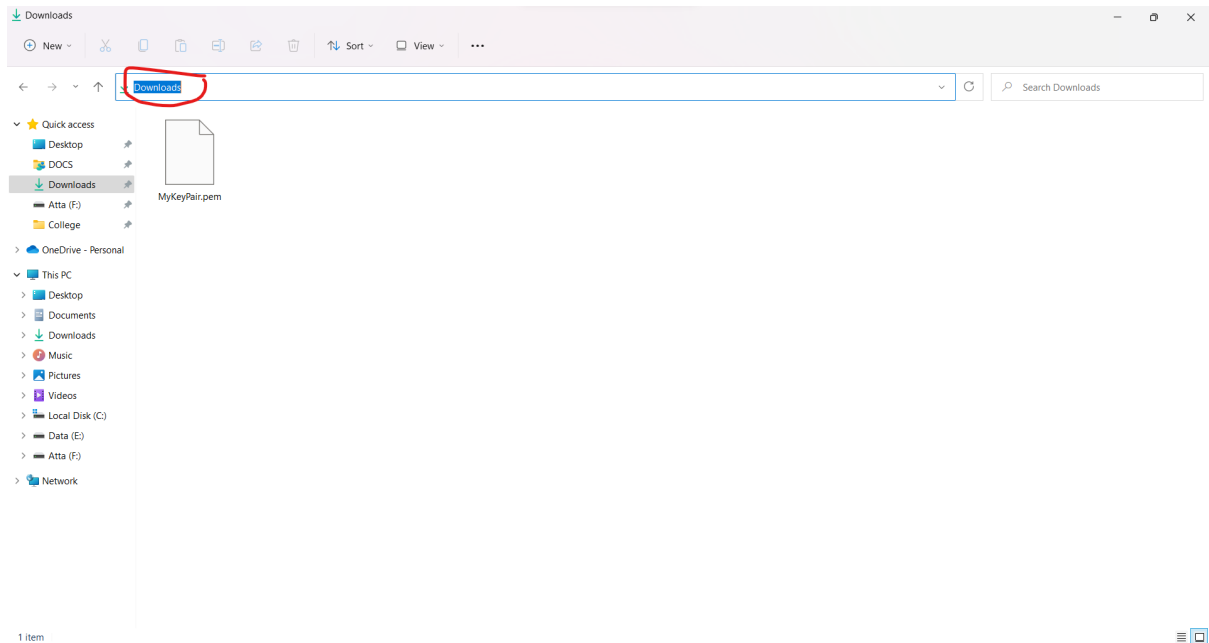
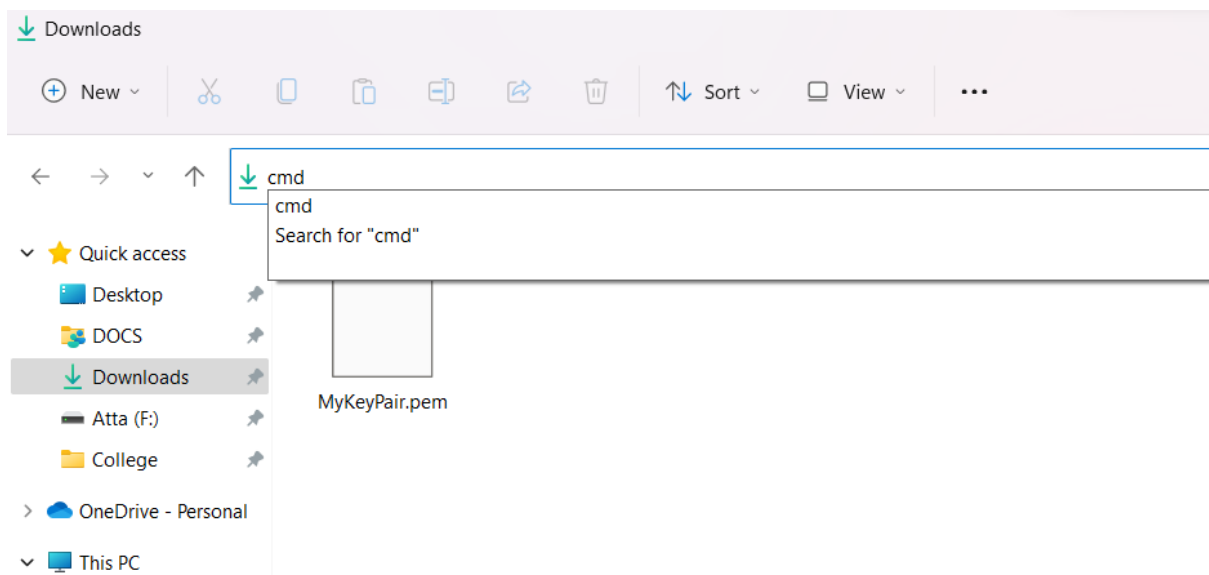


## Connecting to Amazon Linux EC2 Instance using Command Prompt/Windows PowerShell

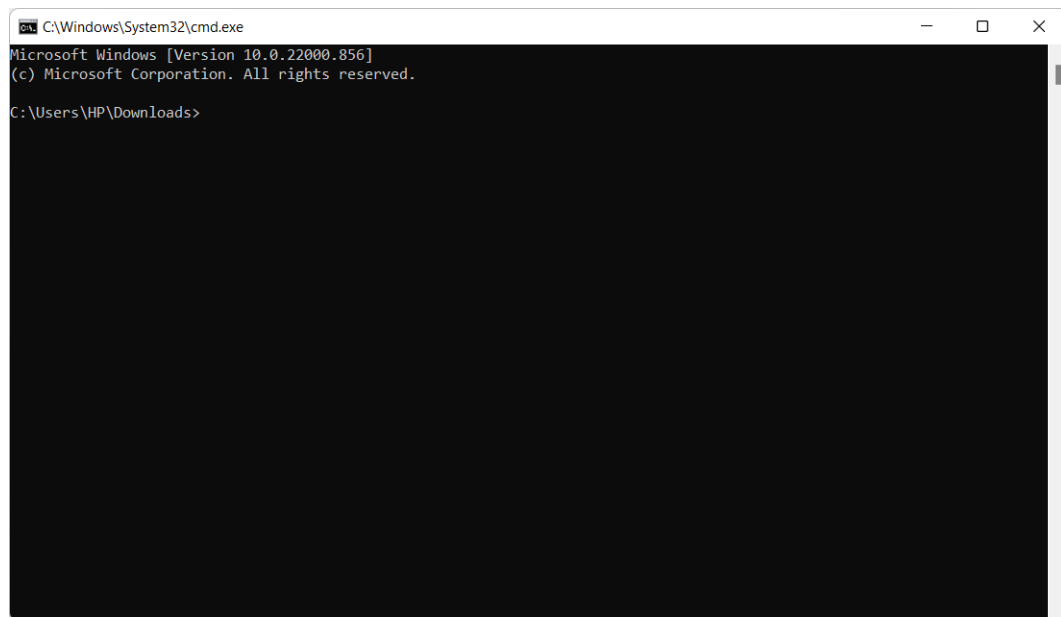
1. Upon creating a new instance, browse to the folder where the Key pair file was downloaded using Windows File Explorer. Click on the address bar.



2. Clear the text content on the address bar and type 'cmd' and press Enter.

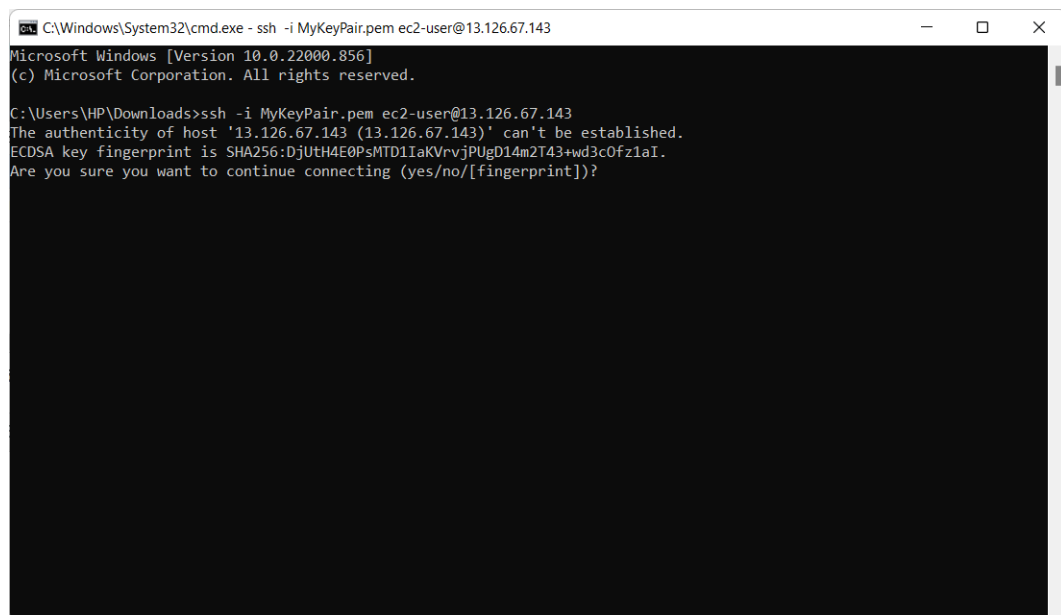


3. A command prompt window of the selected folder (containing the key pair file) looking as follows should open.



4. In the Command prompt window, type in the command –  
`ssh -i <Key-pair-file-name-with-extension.pem> ec2-user@<Public-IP-of-your-instance>`  
and press Enter.

(Refer the command in the following screenshot for example)



You can find the Public IP of your instance for the above command in the Description section with your instance selected in the Instances Dashboard.

Instance: [REDACTED] My Linux EC2 Public DNS: ec2-13-126-67-143.ap-south-1.compute.amazonaws.com

Description Status Checks Monitoring Tags

Instance ID	[REDACTED]	Public DNS (IPv4)	ec2-13-126-67-143.ap-south-1.compute.amazonaws.com
Instance state	running	IPv4 Public IP	13.126.67.143
Instance type	t2.micro	IPv6 IPs	-
Finding	Opt-in to AWS Compute Optimizer for recommendations. <a href="#">Learn more</a>	Elastic IPs	
Private DNS	[REDACTED]	Availability zone	ap-south-1a
Private IPs	[REDACTED]	Security groups	launch-wizard-5. <a href="#">view inbound rules</a> . <a href="#">view outbound rules</a>

### (ALTERNATIVELY)

You can skip steps 1-3 by simply opening Command Prompt and using the command –

```
ssh -i <Path/Key-pair-file-name-with-extension.pem> ec2-user@<Public-IP-of-your-instance>
```

and press Enter.

(It should be noted that in order to select the key pair file without launching Command Prompt in the selected folder, you'll need to specify the path of the folder containing key pair file and then input the file name along with '.pem' file extension after a '/')

5. When prompted,

The authenticity of host '13.126.67.143 (13.126.67.143)' can't be established.

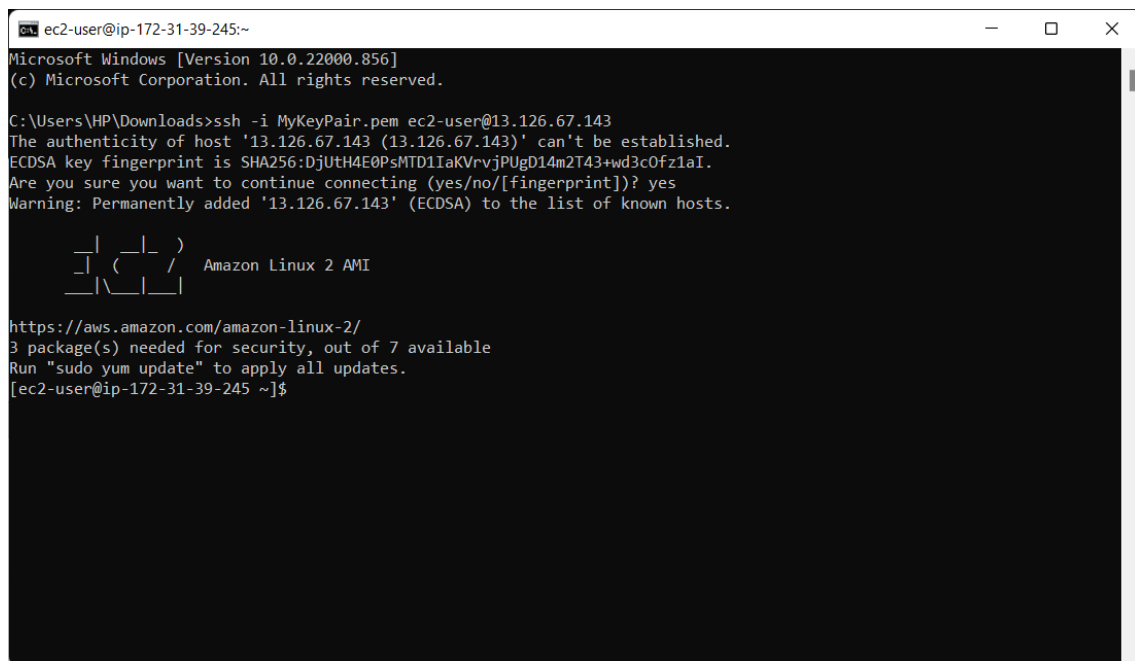
ECDSA key fingerprint is

SHA256:DjUtH4E0PsMTD1IaKVrvjPUgD14m2T43+wd3cOfz1aI.

Are you sure you want to continue connecting (yes/no/[fingerprint])?

Type **yes** and press Enter.

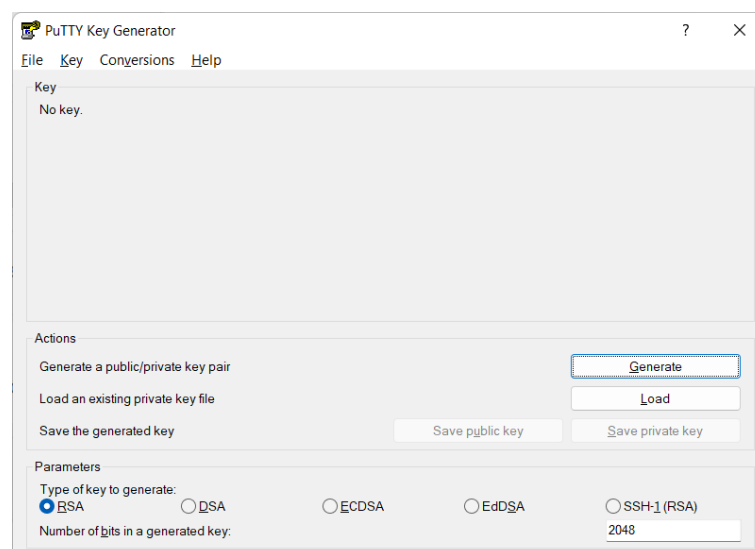
Your Amazon Linux EC2 instance should be launched.



```
ec2-user@ip-172-31-39-245:~  
Microsoft Windows [Version 10.0.22000.856]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\HP\Downloads>ssh -i MyKeyPair.pem ec2-user@13.126.67.143  
The authenticity of host '13.126.67.143 (13.126.67.143)' can't be established.  
ECDSA key fingerprint is SHA256:DjUth4E0PsMTD1IaKVrvjPUgD14m2T43+wd3c0fz1aI.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '13.126.67.143' (ECDSA) to the list of known hosts.  
  
 _ | _ | )  
 _ | ( _ / Amazon Linux 2 AMI  
 _ | \ _ |  
  
https://aws.amazon.com/amazon-linux-2/  
3 package(s) needed for security, out of 7 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-172-31-39-245 ~]$
```

## Connecting to Amazon Linux EC2 Instance using PuTTY SSH Client

1. Install PuTTY SSH Client on your PC. You can download the latest version here:  
<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>
2. Open PuTTYgen (included with PuTTY Client installation).



3. Make sure the checkbox “RSA” is selected.

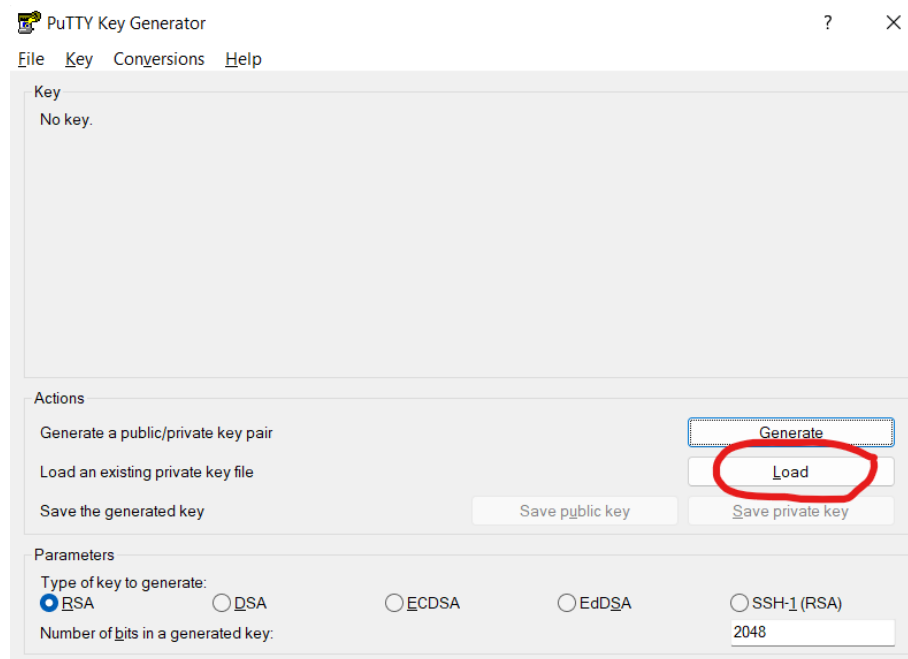
Parameters

Type of key to generate:

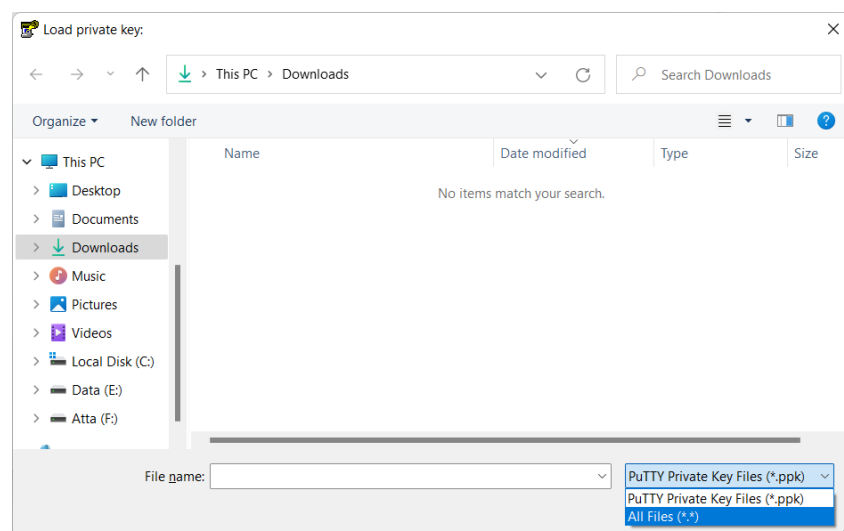
☒ RSA ☐ DSA ☐ ECDSA ☐ EdDSA ☐ SSH-1 (RSA)

Number of bits in a generated key: 2048

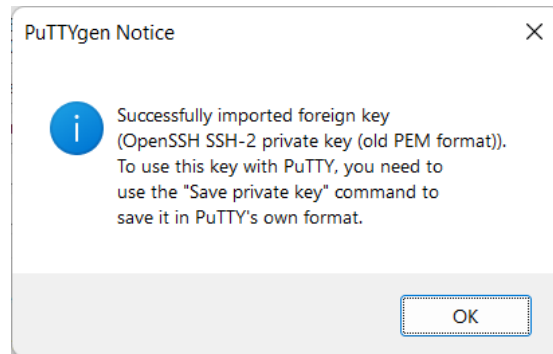
4. Click Load and browse to the folder where your Key pair file is stored. There, select the .pem file and click Open.



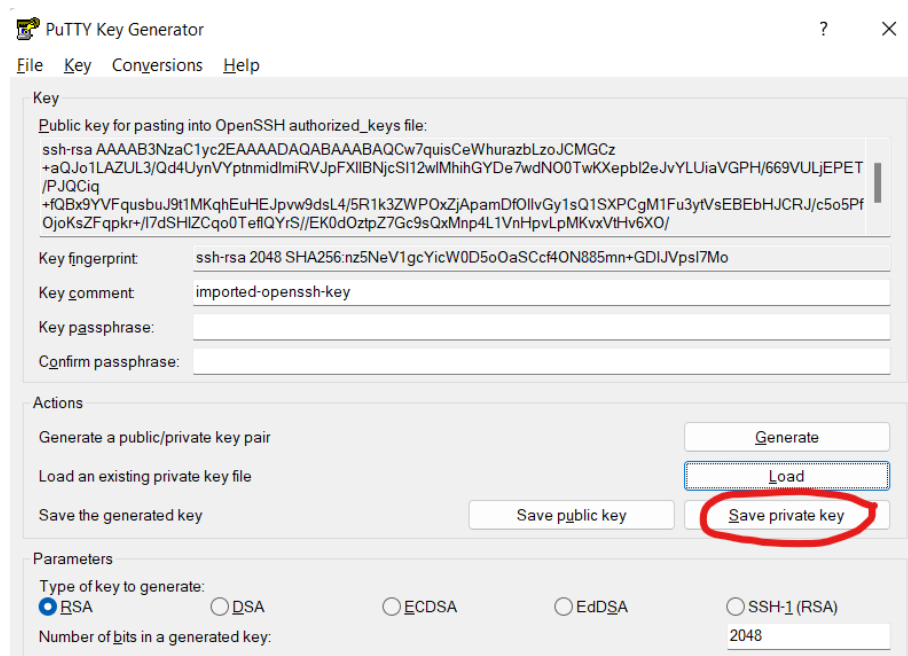
If you are unable to see your file, click on the dropdown list next to File name bar and select All Files (\*.\*). Now, select your file and click Open.



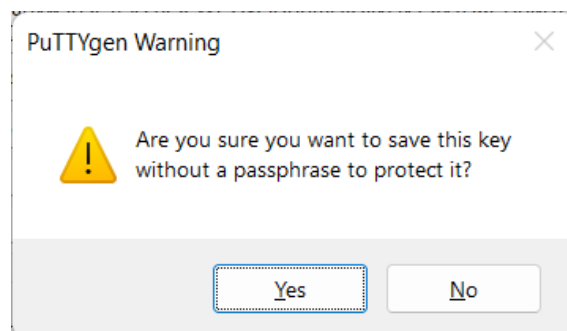
- Click 'Ok' when you see the following pop-up.



- After the Key is loaded, click on Save private key.



The following message will prompt, select Yes.

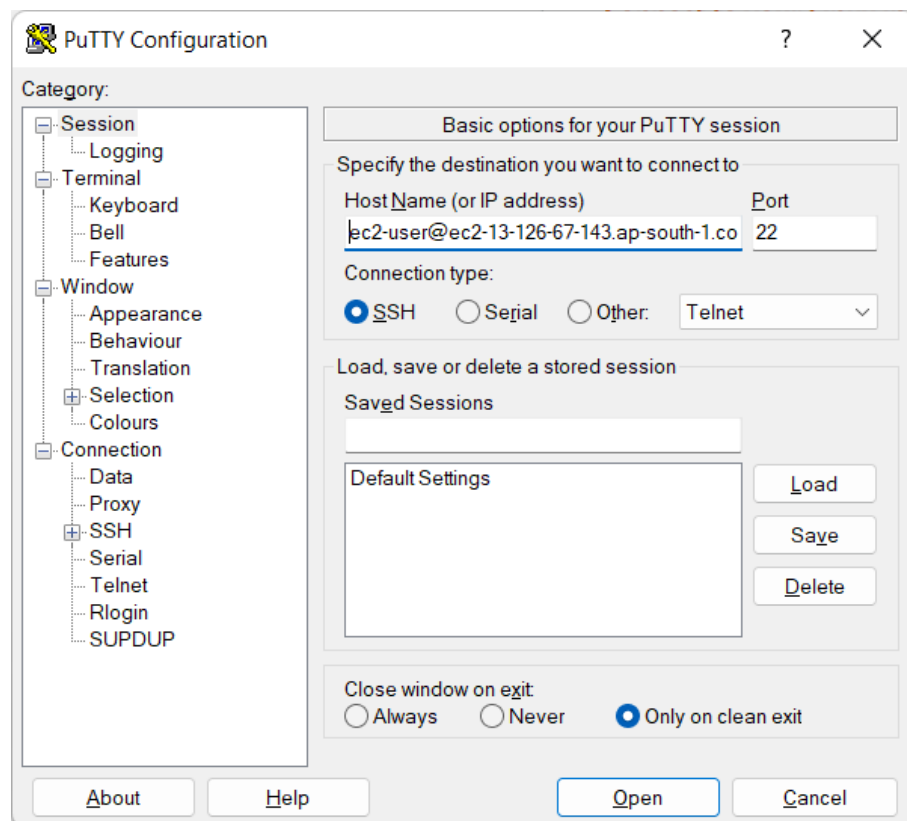


7. Now, type a name for your key, which will then be saved with a file extension *.ppk* and select a path where you want this file to be saved. Click Save.
8. Close PuTTYGen program and open PuTTY application.
9. In the Category pane, choose Session. In the Host Name box enter

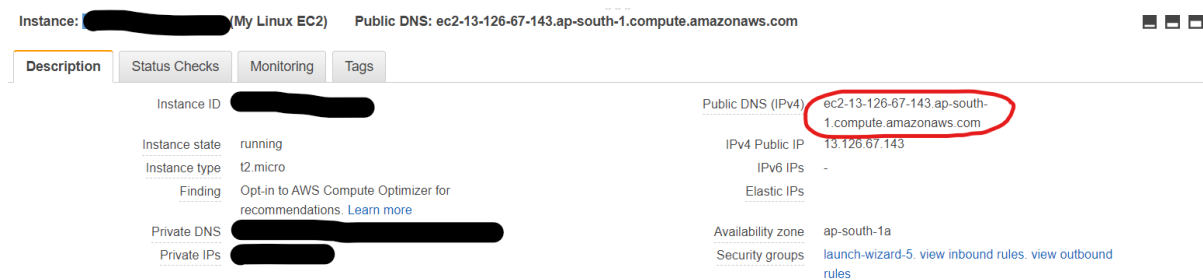
`ec2-user@<instance-public-dns-name>`

Ensure that the Port value is 22. Under Connection type, select SSH.

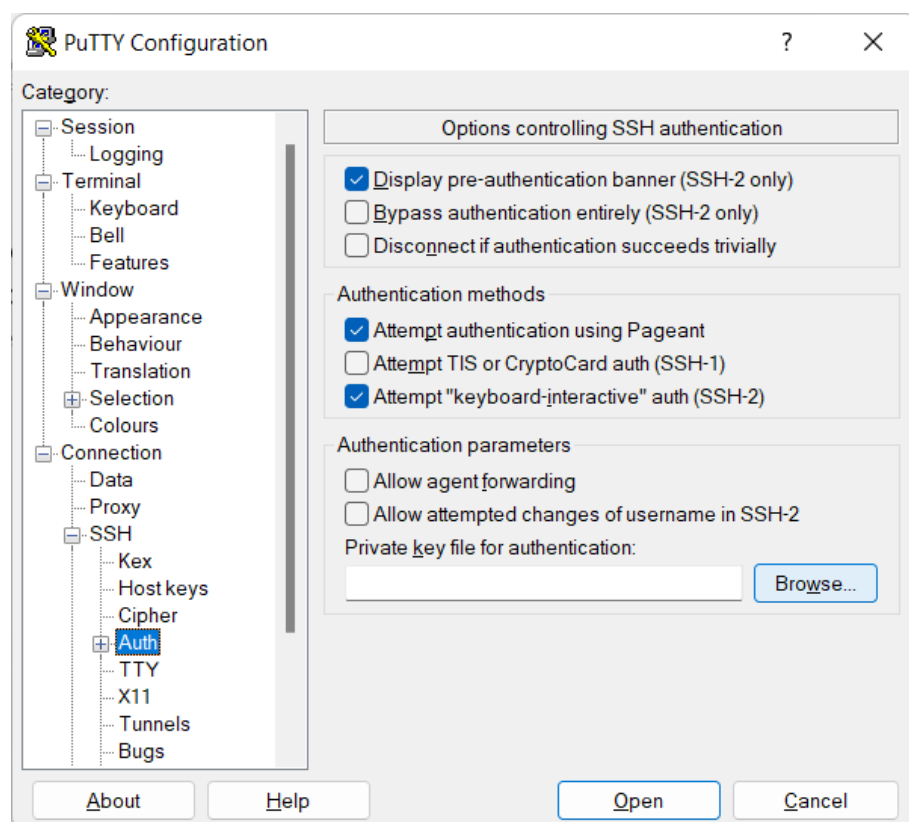
It should look like following –



You can find the Public DNS of your instance in the Description section with your instance selected in the Instances Dashboard.

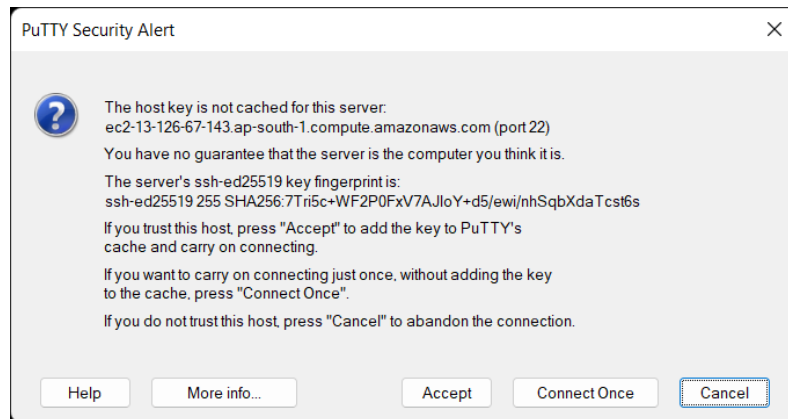


10. In the Category pane, expand Connection, expand SSH, and then choose Auth. Choose Browse for Private key file for authentication. Select the *.ppk* file that you generated for your key pair and choose Open.





If this is the first time you have connected to this instance, PuTTY displays a security alert dialog box that asks whether you trust the host to which you are connecting.



Choose Accept.

A window opens and you are connected to your instance.

