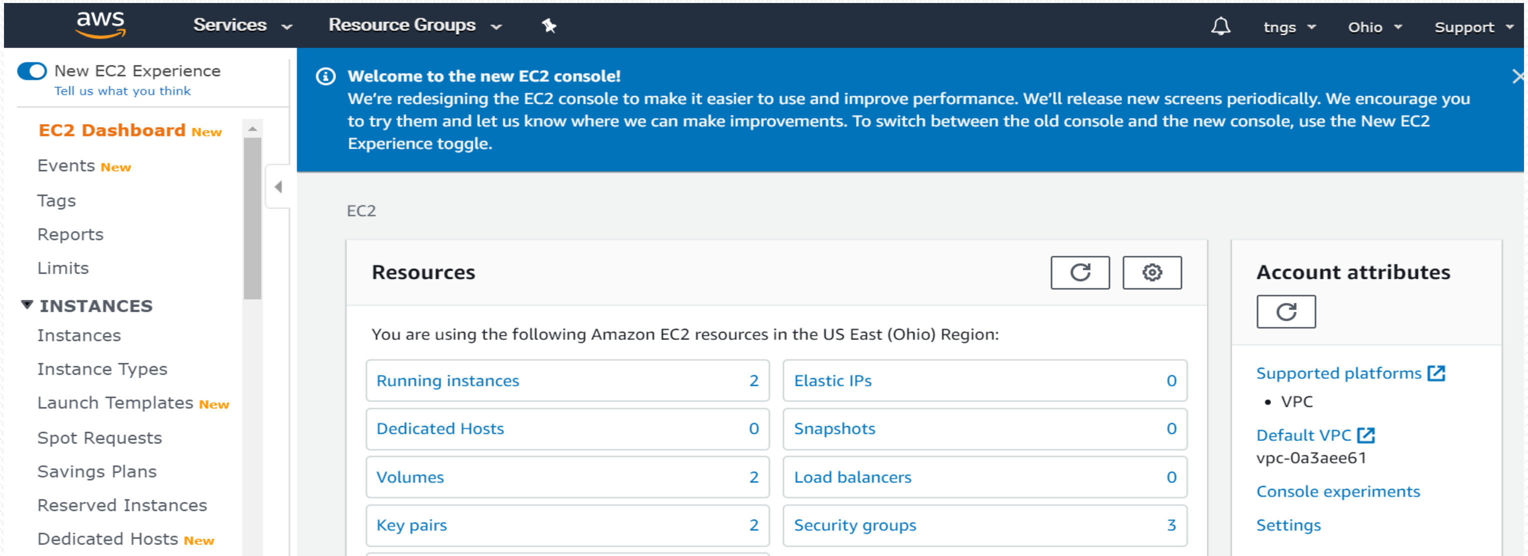
7-Connecting to Instances

CONNECTING TO WINDOWS INSTANCE

Under Services drop down list, choose EC2 from compute section, then make sure you are in the region where you created the instances.



Welcome to the new EC2 console!

We're redesigning the EC2 console to make it easier to use and improve performance. We'll release new screens periodically. We encourage you to try them and let us know where we can make improvements. To switch between the old console and the new console, use the New EC2 Experience toggle.

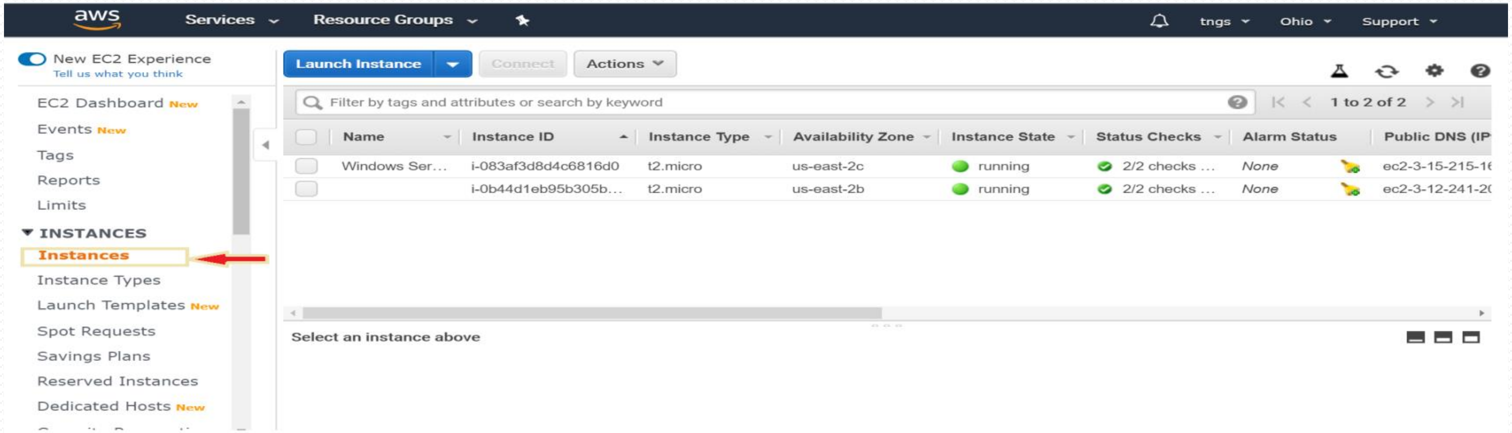
You are using the following Amazon EC2 resources in the US East (Ohio) Region:

Running instances	2	Elastic IPs	0
Dedicated Hosts	0	Snapshots	0
Volumes	2	Load balancers	0
Key pairs	2	Security groups	3

Supported platforms
- VPC

Default VPC
vpc-0a3aee61

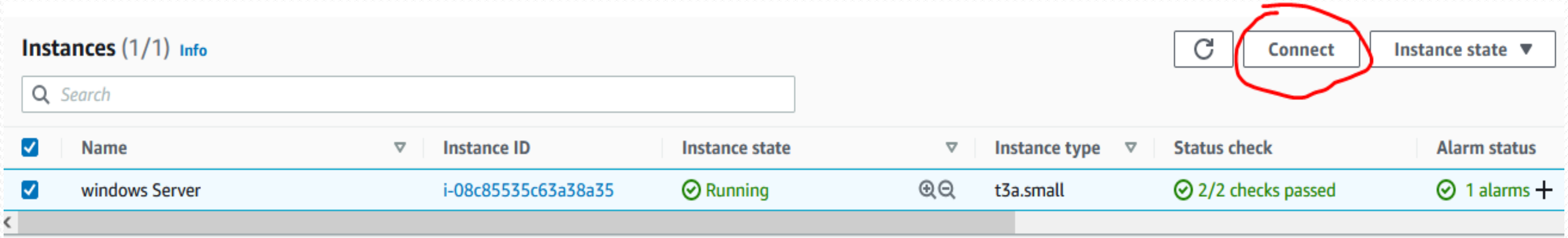
Next, from the left pane select Instances under INSTANCES section to list the instances.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IP
Windows Ser...	i-083af3d8d4c6816d0	t2.micro	us-east-2c	● running	✓ 2/2 checks ...	None	ec2-3-15-215-16
	i-0b44d1eb95b305b...	t2.micro	us-east-2b	● running	✓ 2/2 checks ...	None	ec2-3-12-241-20

Select an instance above

Next, select your windows instance from the instances list then Click on Connect.

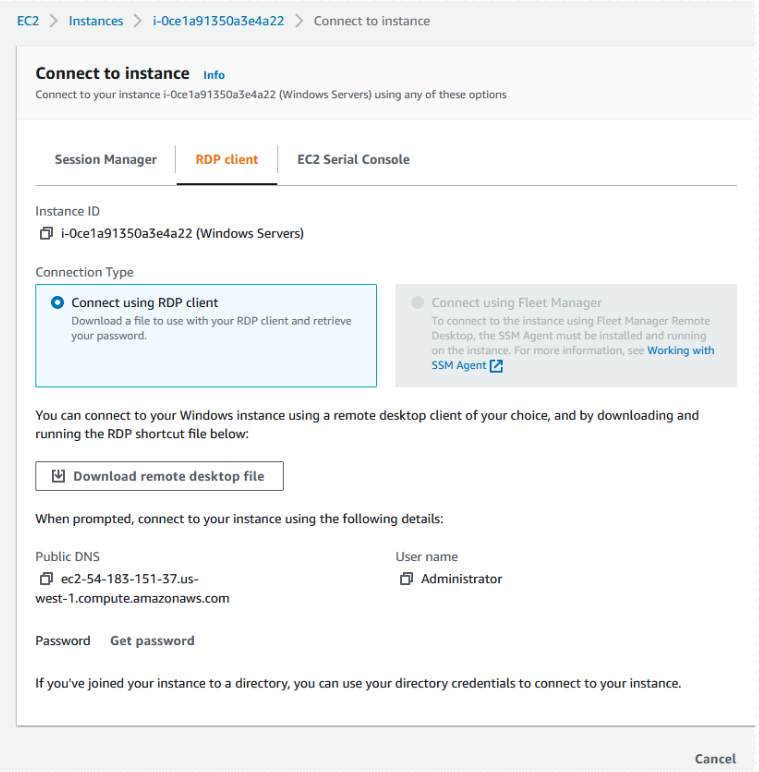


Instances (1/1) Info

Search

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
☑	windows Server	i-08c85535c63a38a35	✓ Running	t3a.small	✓ 2/2 checks passed	✓ 1 alarms +

Select **RDP Client**. Copy username and save on a notepad. Click on **Get password**



EC2 > Instances > i-0ce1a91350a3e4a22 > Connect to instance

Connect to instance Info

Connect to your instance i-0ce1a91350a3e4a22 (Windows Servers) using any of these options

Instance ID

i-0ce1a91350a3e4a22 (Windows Servers)

Connection Type

● Connect using RDP client
Download a file to use with your RDP client and retrieve your password.

○ Connect using Fleet Manager
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see Working with SSM Agent

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

When prompted, connect to your instance using the following details:

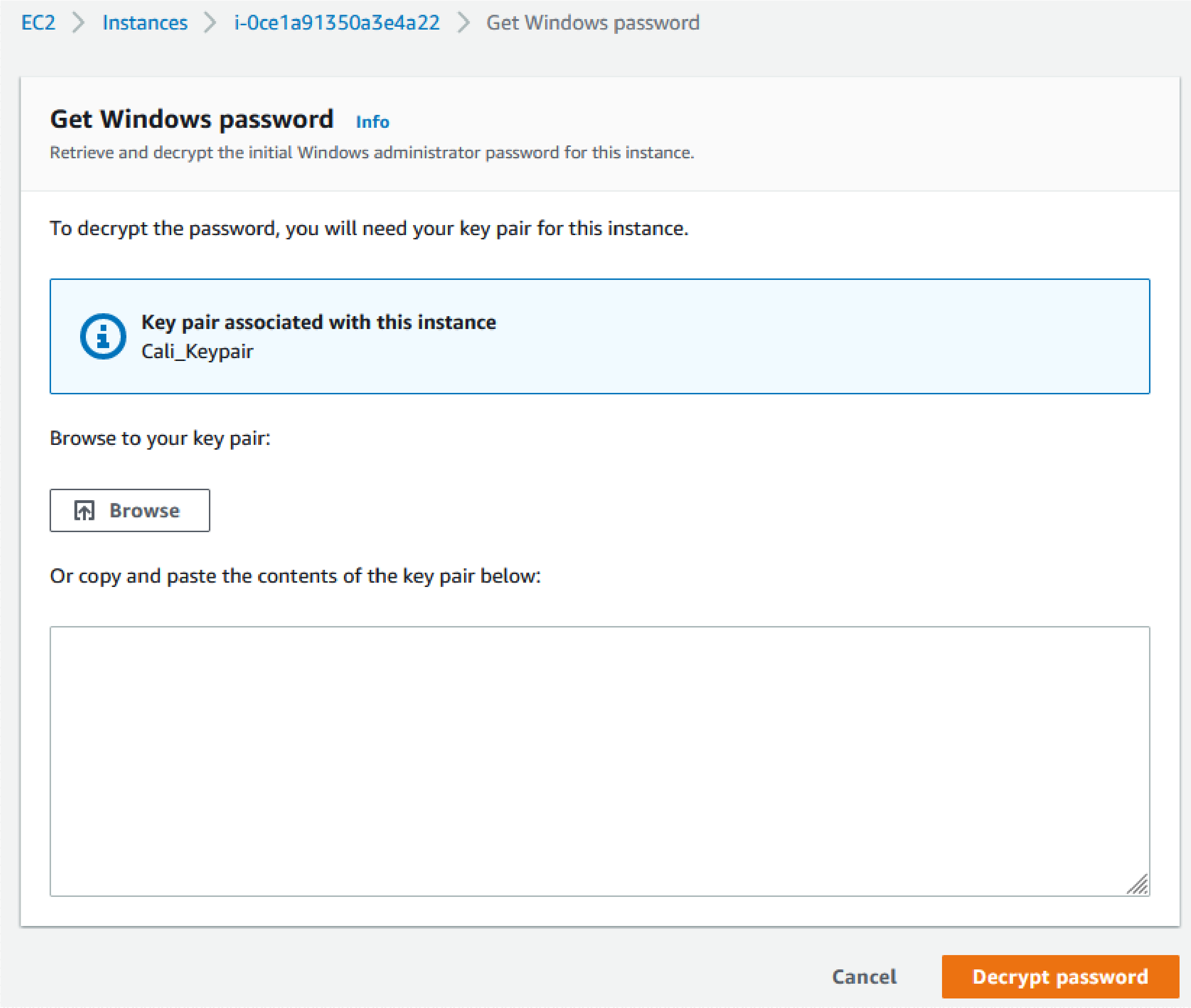
Public DNS
ec2-54-183-151-37.us-west-1.compute.amazonaws.com

User name
Administrator

Password Get password

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

Click on Browse and select your PEM key pair.



EC2 > Instances > i-0ce1a91350a3e4a22 > Get Windows password

Get Windows password

Info

Retrieve and decrypt the initial Windows administrator password for this instance.

To decrypt the password, you will need your key pair for this instance.

Key pair associated with this instance
Cali_Keypair

Browse to your key pair:

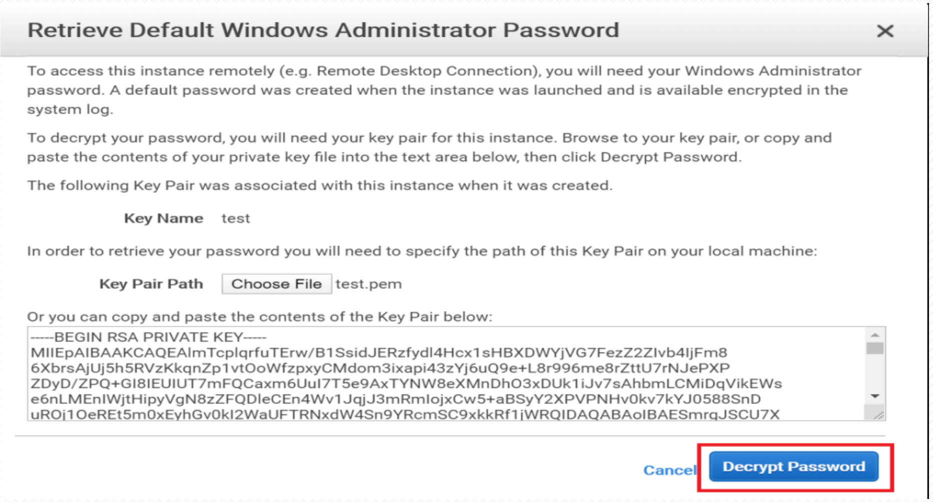
Browse

Or copy and paste the contents of the key pair below:

Cancel

Decrypt password

Next, click on Decrypt Password to get the password.



Retrieve Default Windows Administrator Password

To access this instance remotely (e.g. Remote Desktop Connection), you will need your Windows Administrator password. A default password was created when the instance was launched and is available encrypted in the system log.

To decrypt your password, you will need your key pair for this instance. Browse to your key pair, or copy and paste the contents of your private key file into the text area below, then click Decrypt Password.

The following Key Pair was associated with this instance when it was created.

Key Name test

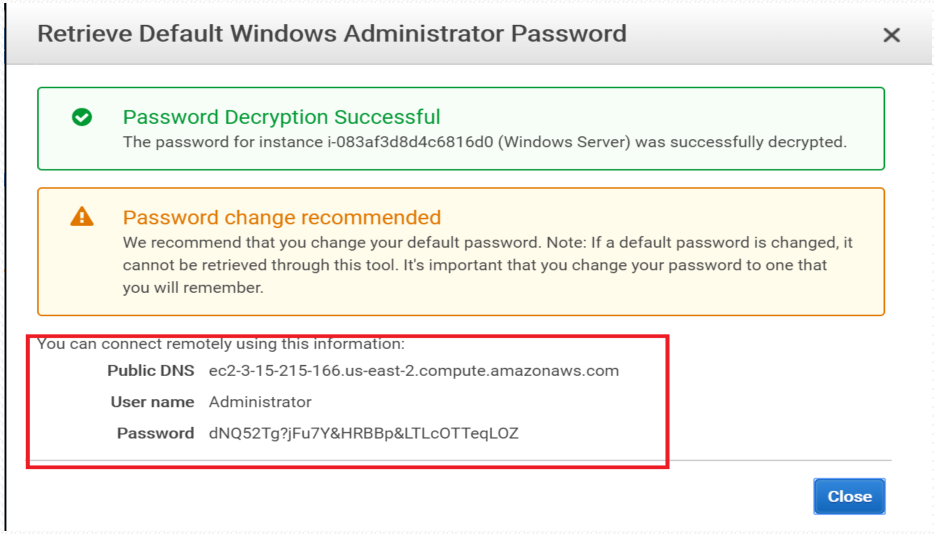
In order to retrieve your password you will need to specify the path of this Key Pair on your local machine:

Key Pair Path Choose File test.pem

Or you can copy and paste the contents of the Key Pair below:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAlmTcplqrfuTErw/B1SsidJERzfydl4Hcx1sHBXDWYjVG7FezZ2Zlvb4IjFm8
6XbrsAjUj5h5RVzKkqnZp1vtOoWfzpxyCMdom3ixapi43zYj6uQ9e+L8r996me8rZttU7rNJePXP
ZDyD/ZPQ+GI8IEUIUT7mFQCaxm6UuI7T5e9AxTYNW8eXMnDhO3xDUk1iJv7sAhbmLCMiDqVikEWs
e6nLMEnIWjtHipyVgN8zZFQDleCEn4Wv1JqjJ3mRmlojxCw5+aBSyY2XPVPNHv0kv7kYJ0588SnD
uROj1OeREt5m0xEyhGv0kI2WaUFTRNxdW4Sn9YRcmSC9xkkRf1jWRQIDAQABAoIBAESmrqJSCU7X
```

You will get the credential information to connect to the windows instance.



Retrieve Default Windows Administrator Password

Password Decryption Successful
The password for instance i-083af3d8d4c6816d0 (Windows Server) was successfully decrypted.

Password change recommended
We recommend that you change your default password. Note: If a default password is changed, it cannot be retrieved through this tool. It's important that you change your password to one that you will remember.

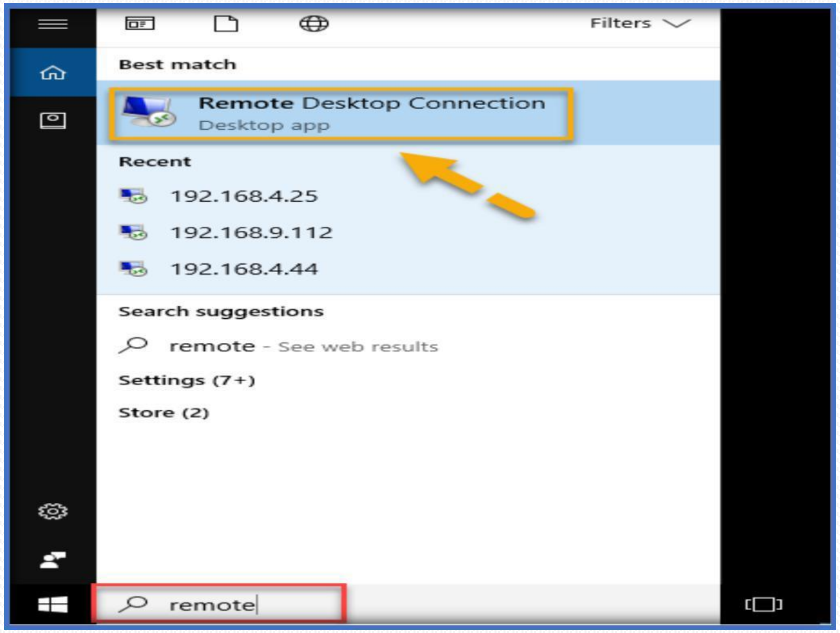
You can connect remotely using this information:

Public DNS ec2-3-15-215-166.us-east-2.compute.amazonaws.com

User name Administrator

Password dNQ52Tg?jFu7Y&HRBBp&LTLcOTTeqLOZ

Now open remote desktop app in your desktop to connect to the windows instance on AWS. To open the remote desktop app, search for remote desktop in the windows search like below.



Filters

Best match

Remote Desktop Connection
Desktop app

Recent

192.168.4.25

192.168.9.112

192.168.4.44

Search suggestions

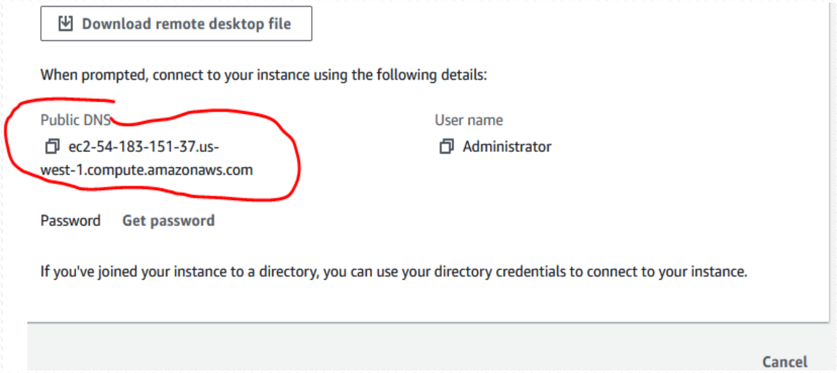
remote - See web results

Settings (7+)

Store (2)

remote

Once remote desktop app opened, copy and paste the public DNS in the computer text box and click on connect to connect to the instance.



Download remote desktop file

When prompted, connect to your instance using the following details:

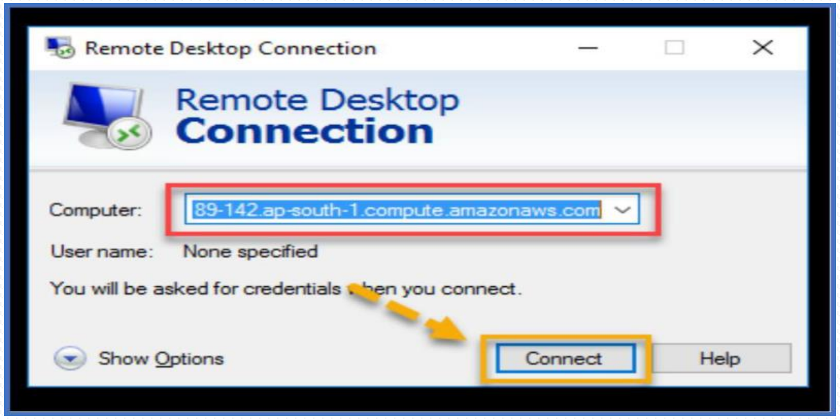
Public DNS
ec2-54-183-151-37.us-west-1.compute.amazonaws.com

User name
Administrator

Password Get password

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

Cancel



Remote Desktop Connection

Remote Desktop
Connection

Computer: 89-142.ap-south-1.compute.amazonaws.com

User name: None specified

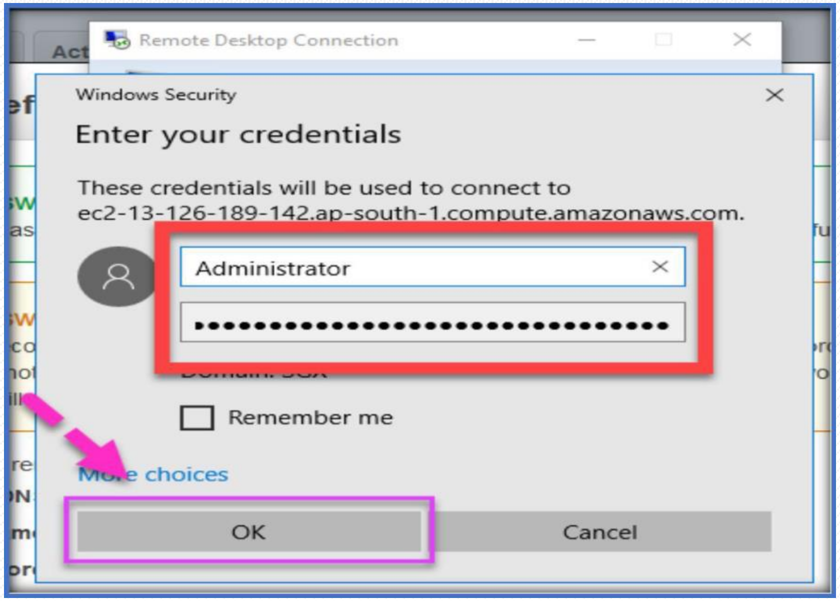
You will be asked for credentials when you connect.

Show Options

Connect

Help

Specify the username and password in the respective fields and choose OK to connect.



Windows Security

Enter your credentials

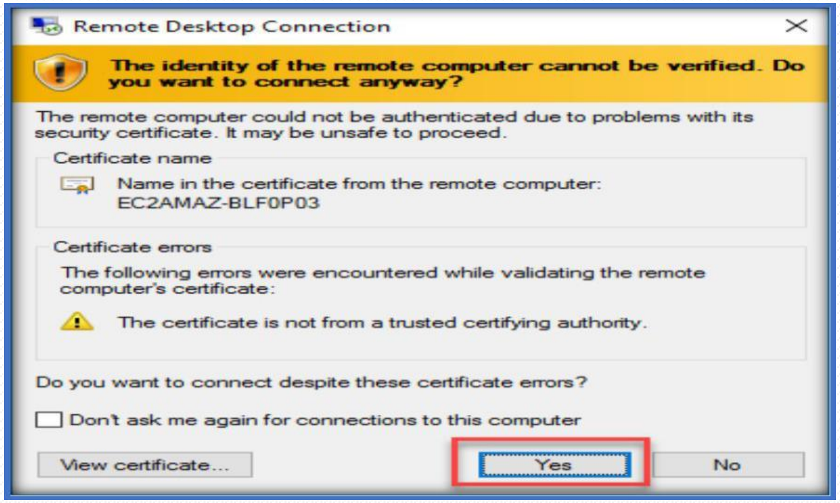
These credentials will be used to connect to ec2-13-126-189-142.ap-south-1.compute.amazonaws.com.

Administrator

••••••••••••••••••••••••••••••••

□ Remember me

Then choose yes to connect.



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
EC2AMAZ-BLF0P03

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

CONNECTING TO LINUX INSTANCE

To connect to Linux instance, we need an app like remote desktop for windows. There are two applications called putty or mobaxterm, we can use any one to access the Linux instances.

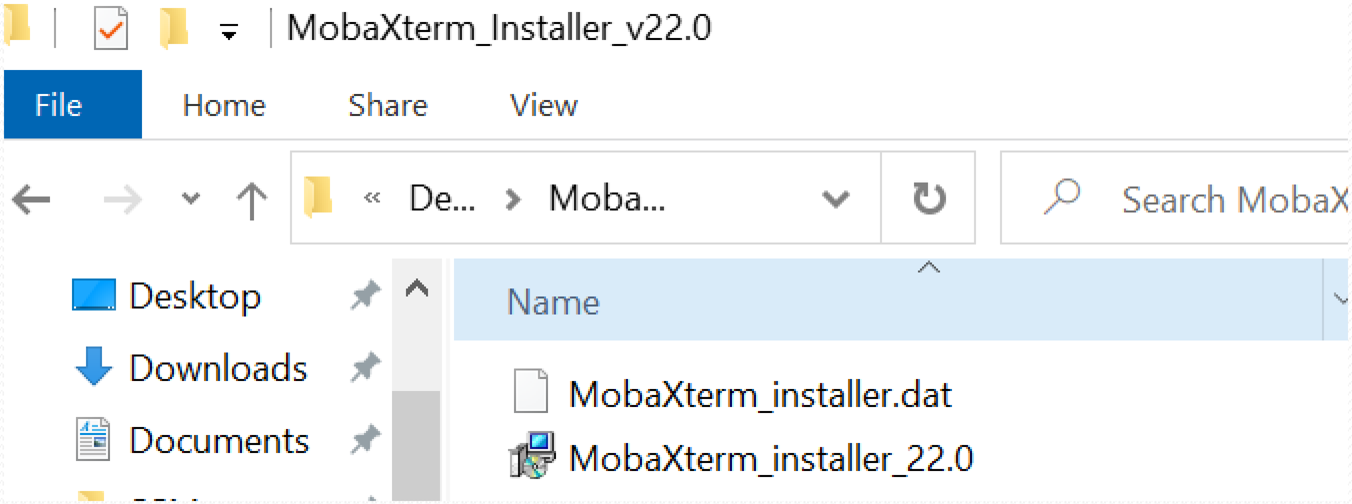
ACCESSING USING MOBAXTERM:

You can download the mobaxterm app from below link.

Download MobaxTerm

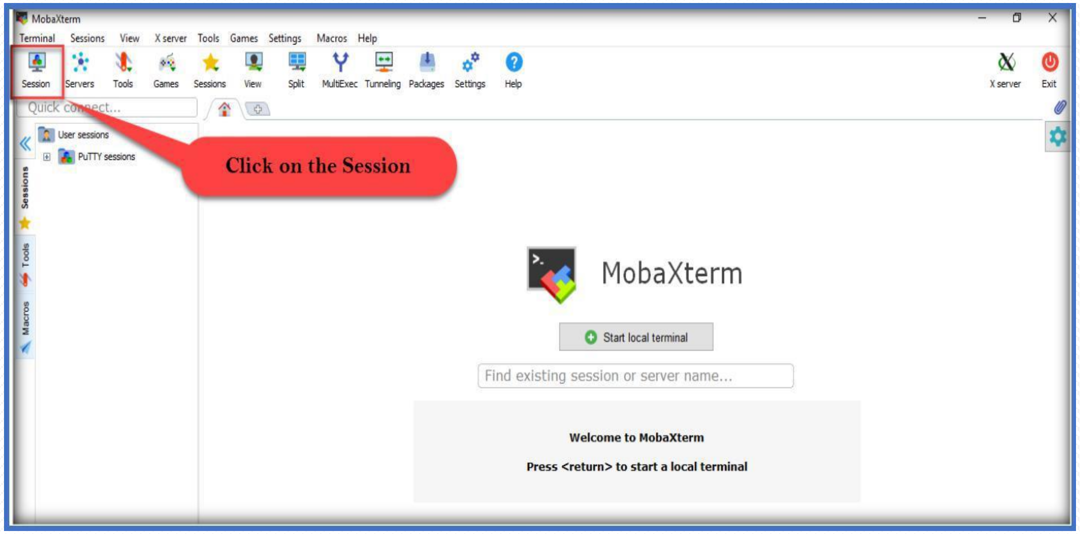
Once opened click on download, unzip the file to desktop and click into the unzipped folder.

Double Click on MobaXterm_installer_22.0 and follow the instructions on the screen to install



Once installation is completed, Search for Mobaxterm on your PC and open

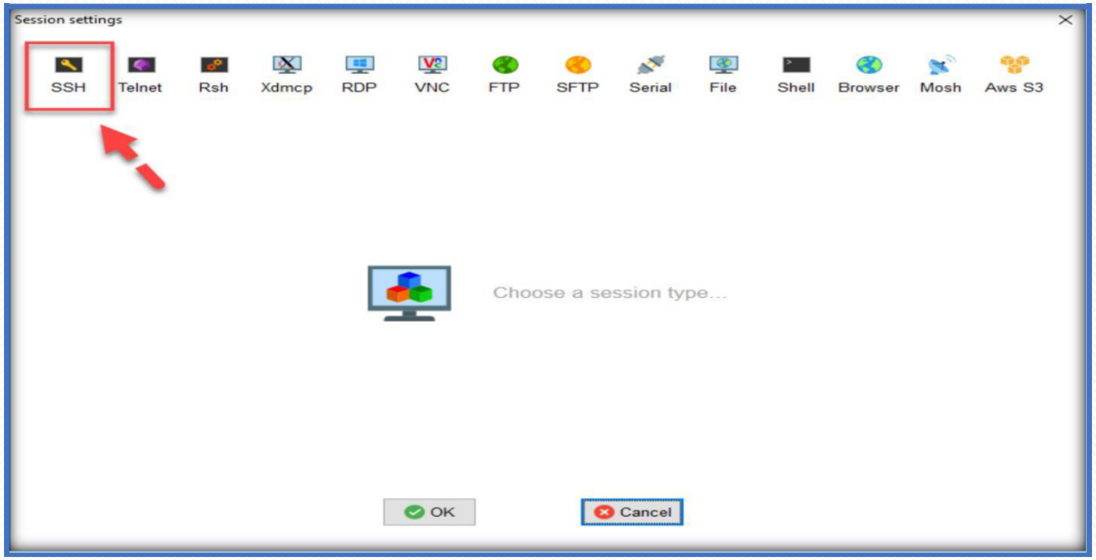
Once app opened, click on the Session on the left side top corner of app.


Click on the Session

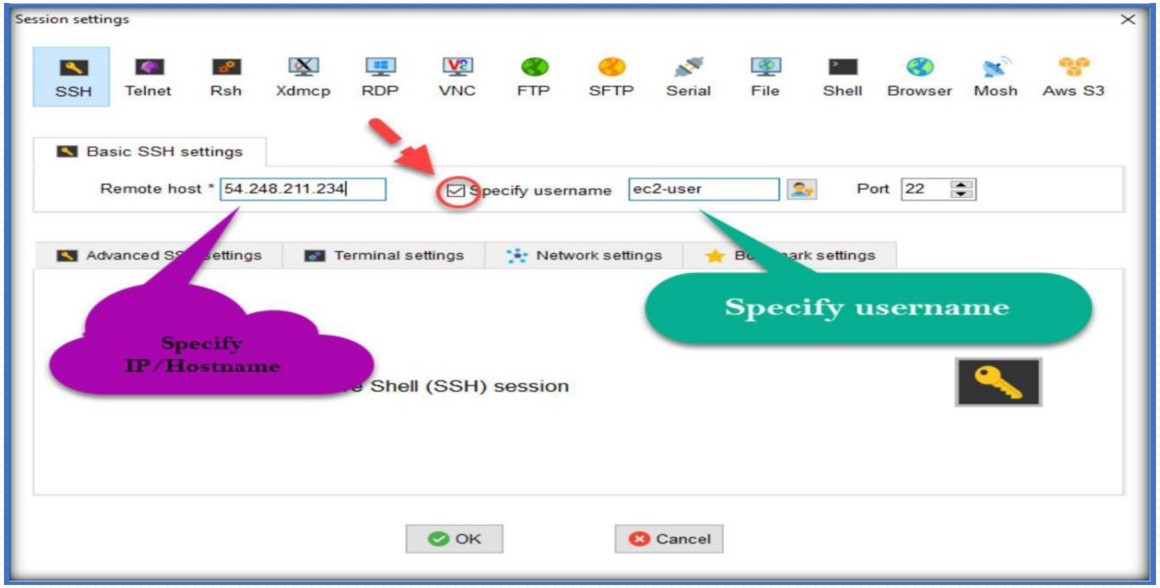
Welcome to MobaXterm

Press <return> to start a local terminal

Choose SSH from the session settings wizard.



Specify the IP/Hostname at the Remote host text box, Select the Specify username option and fill the username.



Session settings

Basic SSH settings

Remote host * 54.248.211.234

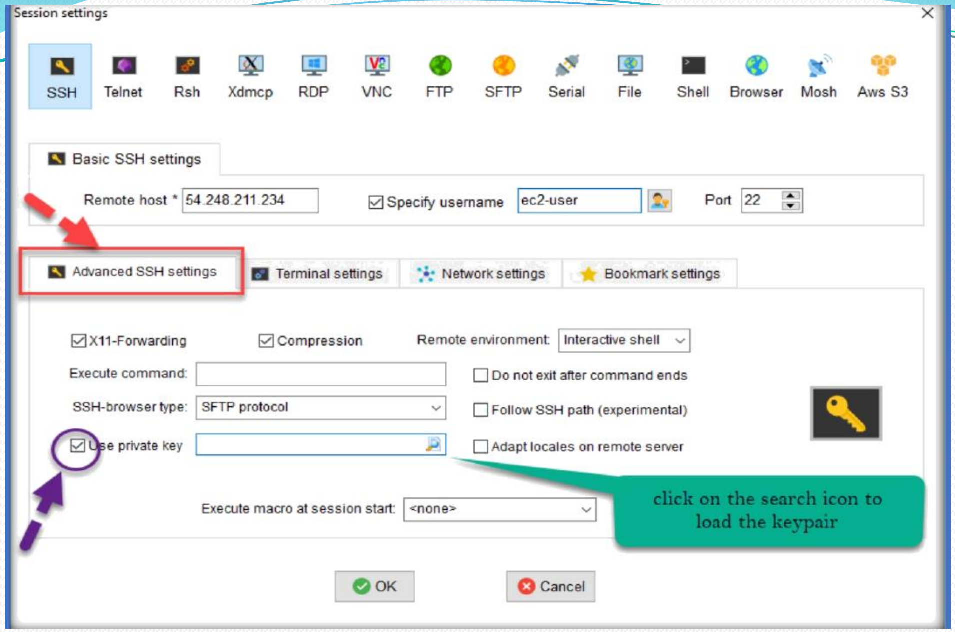
☑ Specify username ec2-user

Port 22

Specify username

Specify IP/Hostname

Select advanced SSH Settings bar, select use private key, then mouse over to the end of the text box, you will find a search icon click on it to load the key pair.



Remote host * 54.248.211.234 ☑ Specify username ec2-user Port 22

☑ X11-Forwarding ☑ Compression Remote environment: Interactive shell

Execute command:

□ Do not exit after command ends

SSH-browser type: SFTP protocol

□ Follow SSH path (experimental)

☑ Use private key

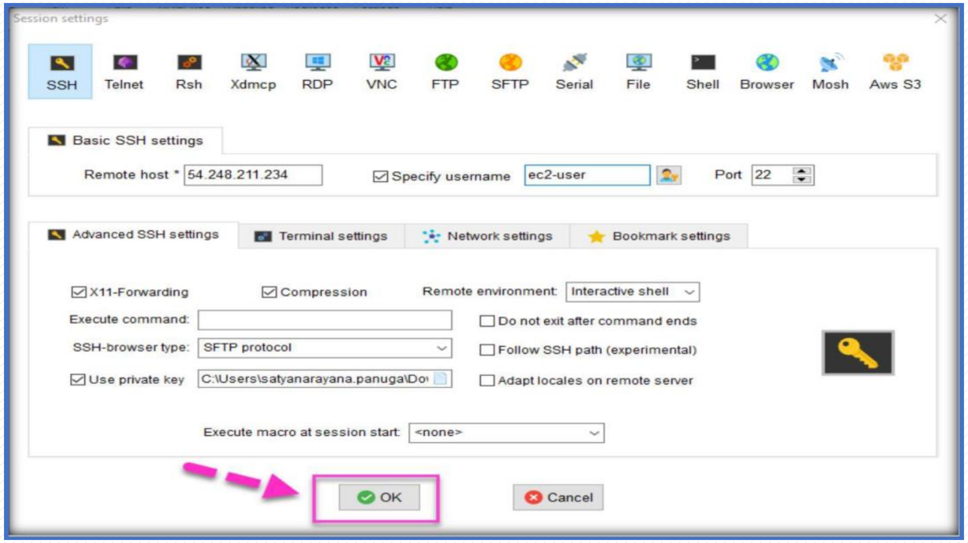
□ Adapt locales on remote server

Execute macro at session start: <none>

click on the search icon to load the keypair

Choose the PEM file click on open

Next, click on OK to connect to the Linux server



Remote host * 54.248.211.234 ☑ Specify username ec2-user Port 22

☑ X11-Forwarding ☑ Compression Remote environment: Interactive shell

Execute command:

□ Do not exit after command ends

SSH-browser type: SFTP protocol

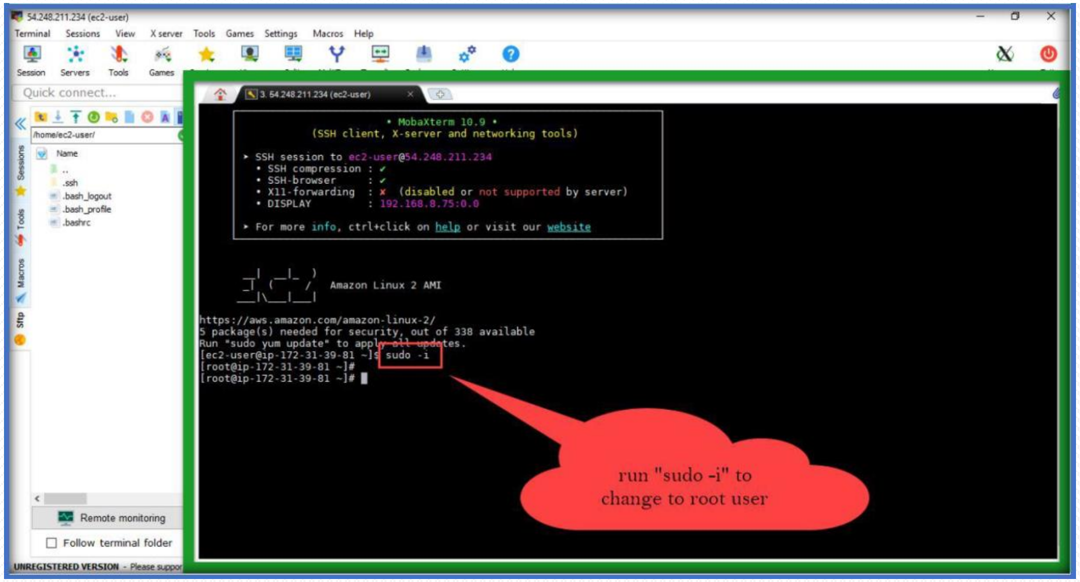
□ Follow SSH path (experimental)

☑ Use private key C:\Users\satyanarayana.panuga\Do

□ Adapt locales on remote server

Execute macro at session start: <none>

Once clicked on OK, you will be connected to Linux server, then use “sudo -i” command to log in to root user.



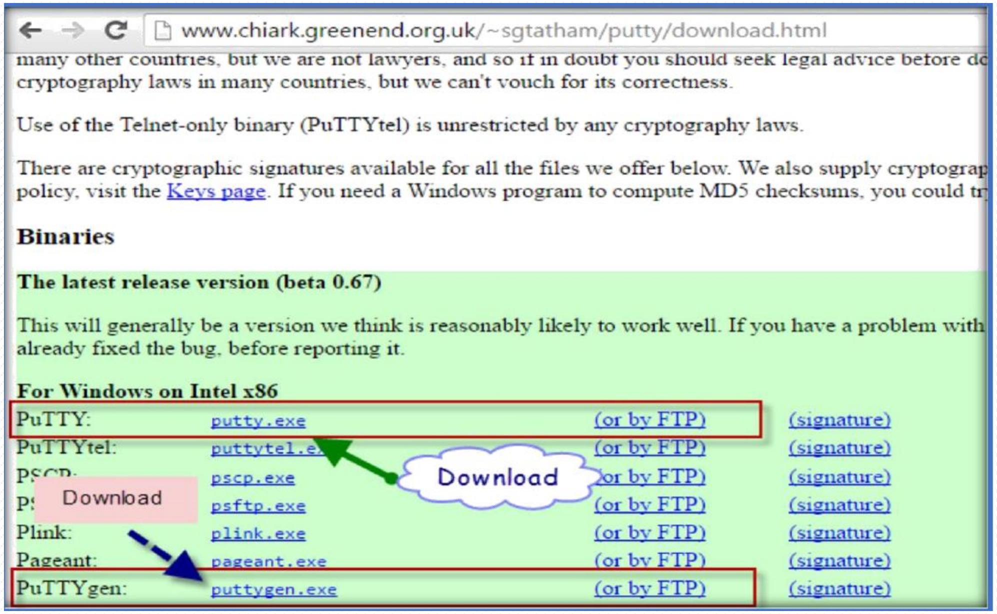
54.248.211.234 (ec2-user)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games
Quick connect...
/home/ec2-user/
Name
..
.ssh
.bash_logout
.bash_profile
.bashrc
Sessions Tools Macros Sftp
3. 54.248.211.234 (ec2-user)
Remote monitoring
□ Follow terminal folder
UNREGISTERED VERSION - Please suppor

```
                  • MobaXterm 10.9 •
      (SSH client, X-server and networking tools)

 ➤ SSH session to ec2-user@54.248.211.234
   • SSH compression : ✓
   • SSH-browser     : ✓
   • X11-forwarding  : ✗  (disabled or not supported by server)
   • DISPLAY         : 192.168.8.75:0.0

 ➤ For more info, ctrl+click on help or visit our website


       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
5 package(s) needed for security, out of 338 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-39-81 ~]$ sudo -i
[root@ip-172-31-39-81 ~]#
[root@ip-172-31-39-81 ~]#
```

run "sudo -i" to
change to root user

CONNECT USING PUTTY APPLICATION:

Download Putty.exe and Puttygen.exe from below URL and open it.
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html



www.chiark.greenend.org.uk/~sgtatham/putty/download.html

many other countries, but we are not lawyers, and so if in doubt you should seek legal advice before do
cryptography laws in many countries, but we can't vouch for its correctness.

Use of the Telnet-only binary (PuTTYtel) is unrestricted by any cryptography laws.

There are cryptographic signatures available for all the files we offer below. We also supply cryptograp
policy, visit the Keys page. If you need a Windows program to compute MD5 checksums, you could tr

Binaries

The latest release version (beta 0.67)

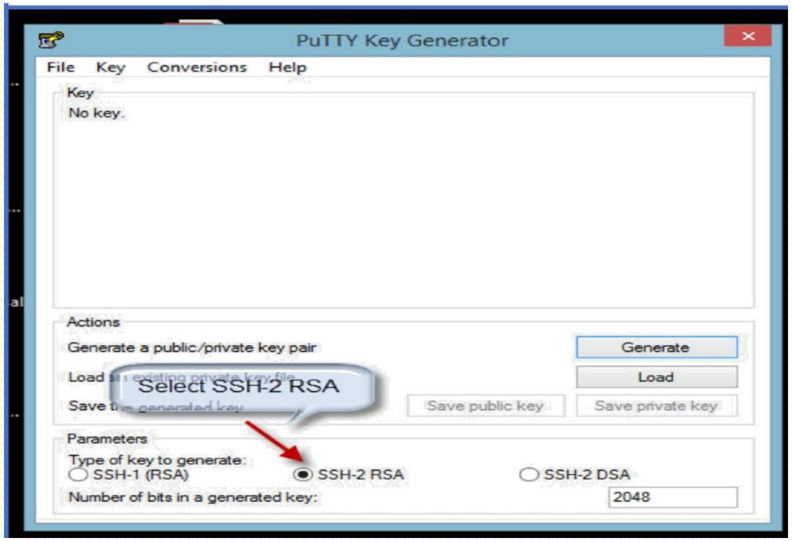
This will generally be a version we think is reasonably likely to work well. If you have a problem with
already fixed the bug, before reporting it.

For Windows on Intel x86

PuTTY:	putty.exe	(or by FTP)	(signature)
PuTTYtel:	puttytel.e	(or by FTP)	(signature)
PSCP:	pscp.exe	or by FTP)	(signature)
PS	psftp.exe	(or by FTP)	(signature)
Plink:	plink.exe	(or by FTP)	(signature)
Pageant:	pageant.exe	(or by FTP)	(signature)
PuTTYgen:	puttygen.exe	(or by FTP)	(signature)

Then, putty does not support PEM file authentication, so we have to convert PEM to PPK by using a app called PuTTYgen, as we have already downloaded. Once downloaded double click on the app will open, no need to install.

Open Puttygen.exe and select SSH-2 RSA in the below.



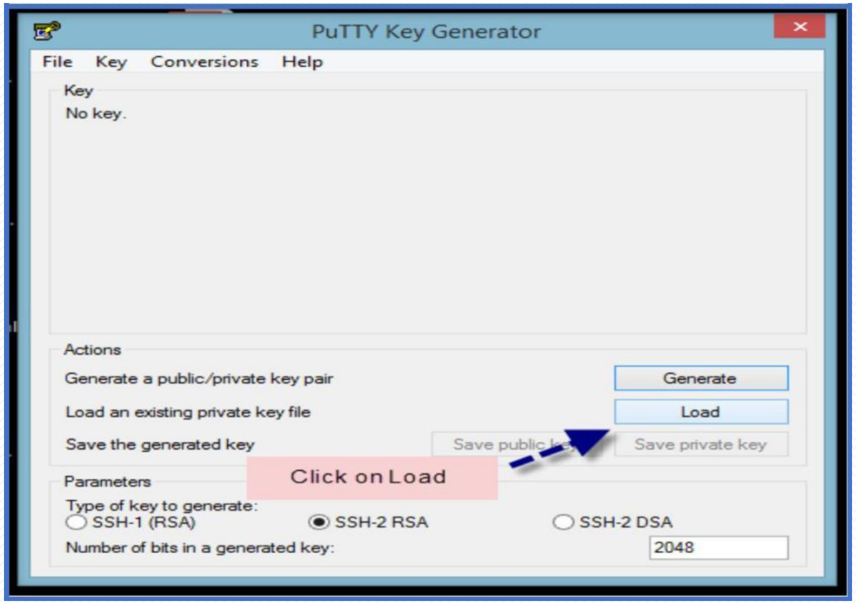
PuTTY Key Generator

Key
No key.

Actions
Generate a public/private key pair
Load an existing private key file
Save the generated key

Parameters
Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA
Number of bits in a generated key: 2048

Click on Load to load the PEM file.

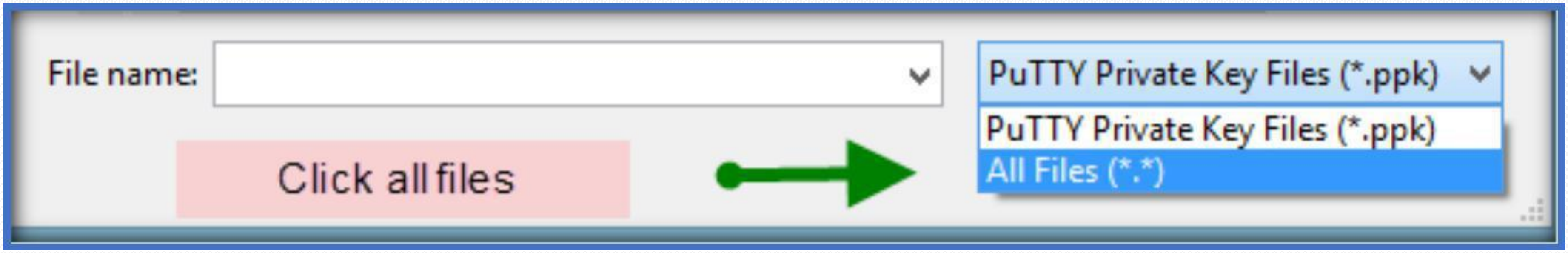


Key
No key.

Actions
Generate a public/private key pair
Load an existing private key file
Save the generated key

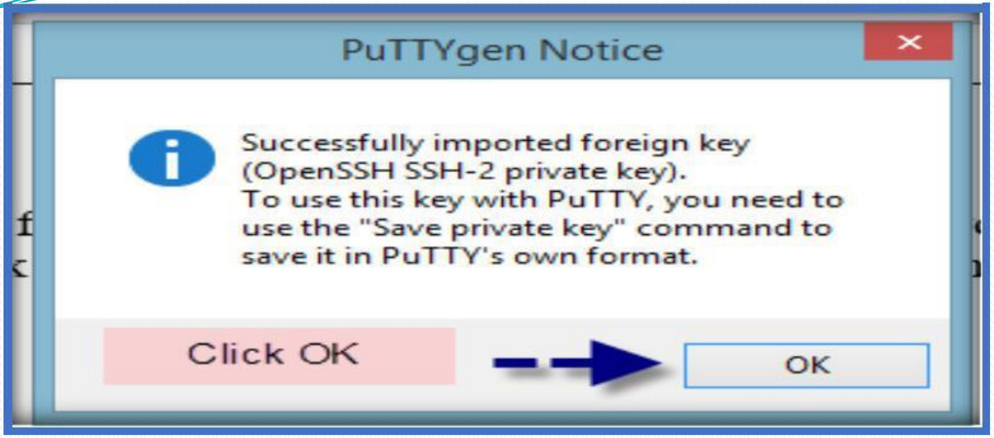
Parameters
Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA
Number of bits in a generated key: 2048

Once you click on Load, by default, Puttygen displays only files with extension. ppk. To locate your .pem file, select the option to display files of all types


PuTTY Private Key Files (*.ppk)
PuTTY Private Key Files (*.ppk)
All Files (*.*)
Click all files

File name:

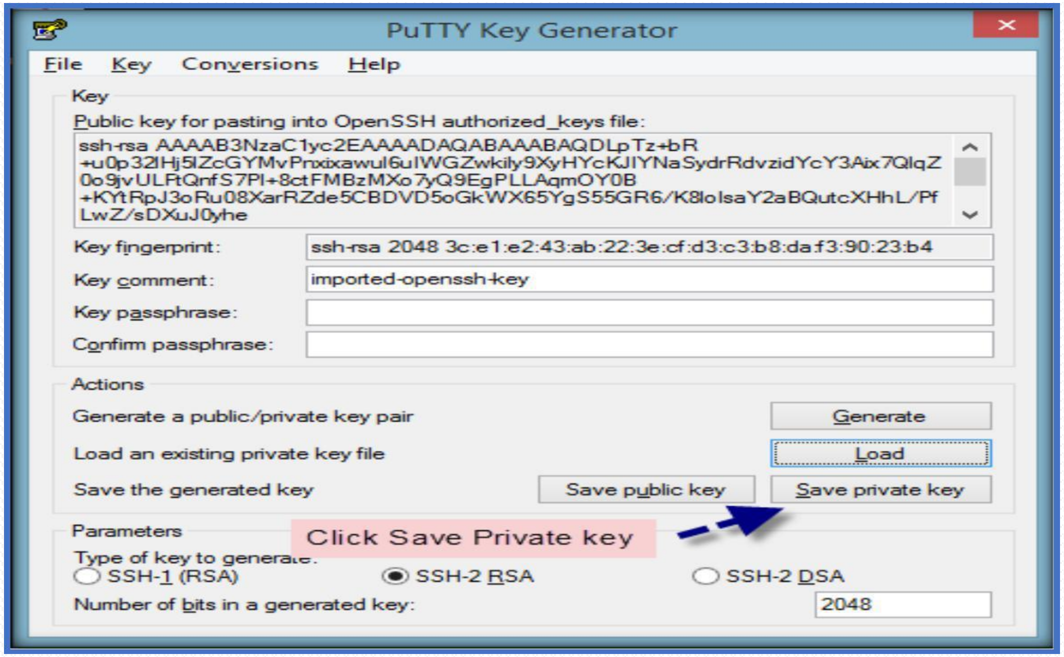
Select your .pem file for the key pair that you specified when you launch your instance, and then click Open. Click OK to dismiss the confirmation dialog box



Successfully imported foreign key (OpenSSH SSH-2 private key).
To use this key with PuTTY, you need to use the "Save private key" command to save it in PuTTY's own format.

Click OK

Click Save private key to save the key in the format that PuTTY can use. PuTTYgen displays a warning about saving the key without a passphrase. Click Yes



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDLpTz+bR
+u0p32lHj5lZcGYMvPnxixawul6uIWGZwkily9XyHYcKJIYNaSydrRdvzidYcY3Aix7QlqZ
0o9jvULRtQnfS7Pl+8ctFMBzMXo7yQ9EgPLLAqmOY0B
+KYtRpJ3oRu08XarRZde5CBDVD5oGkWX65YgS55GR6/K8loIsaY2aBQutcXHhL/Pf
LwZ/sDXuJ0yhe
```

Key fingerprint: ssh-rsa 2048 3c:e1:e2:43:ab:22:3e:cf:d3:c3:b8:da:f3:90:23:b4

Key comment: imported-openssh-key

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

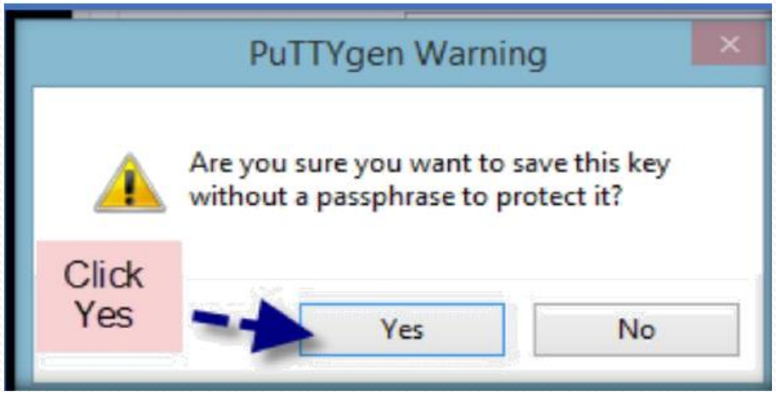
Click Save Private key

Parameters

Type of key to generate:

○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

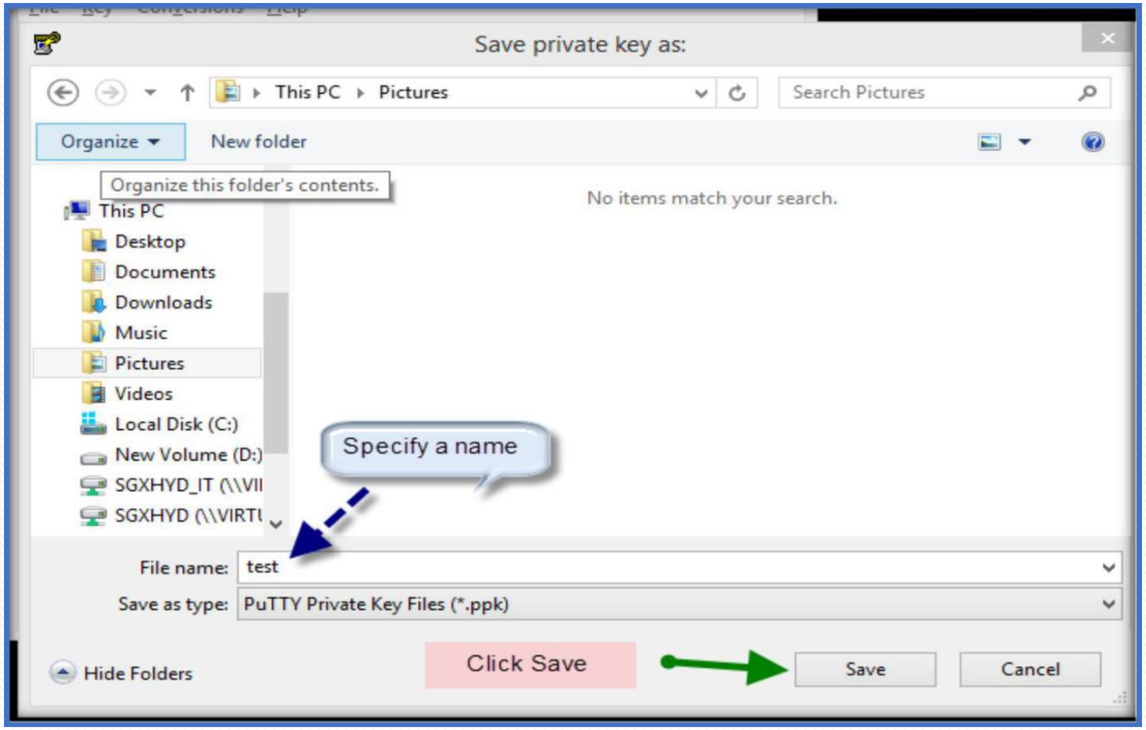
Number of bits in a generated key: 2048



PuTTYgen Warning

Are you sure you want to save this key without a passphrase to protect it?

Then specify a name to the ppk file and click save.



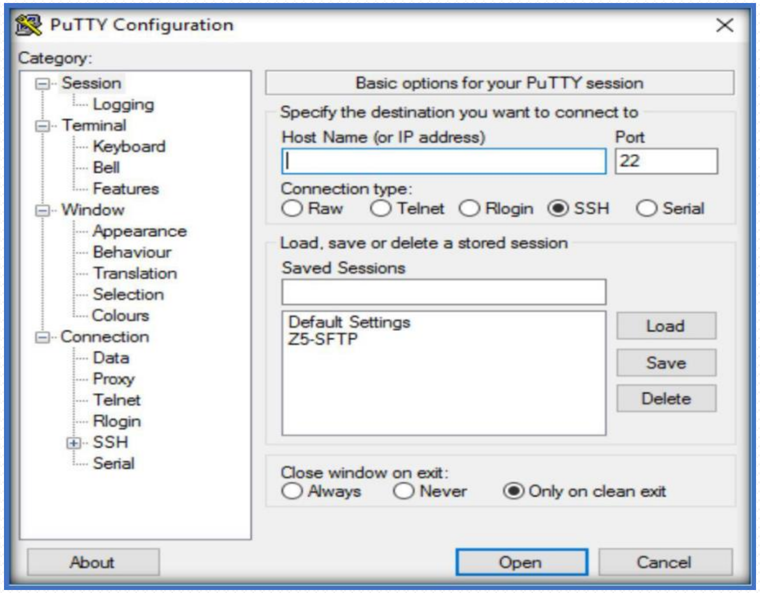
Save private key as:

No items match your search.

File name: test

Save as type: PuTTY Private Key Files (*.ppk)

Now open the PuTTY app to start connecting to Linux instance, by double click on it.



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

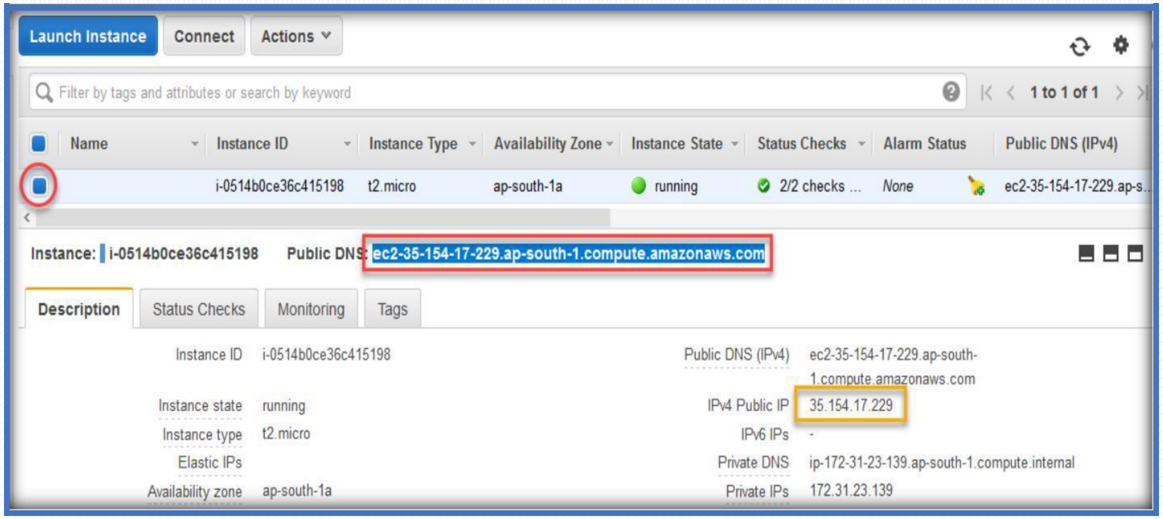
Load, save or delete a stored session

Saved Sessions

Default Settings
Z5-SFTP

Close window on exit:
○ Always ○ Never ● Only on clean exit

Then go to AWS management console, select the instance and copy either Public DNS or Public IP.

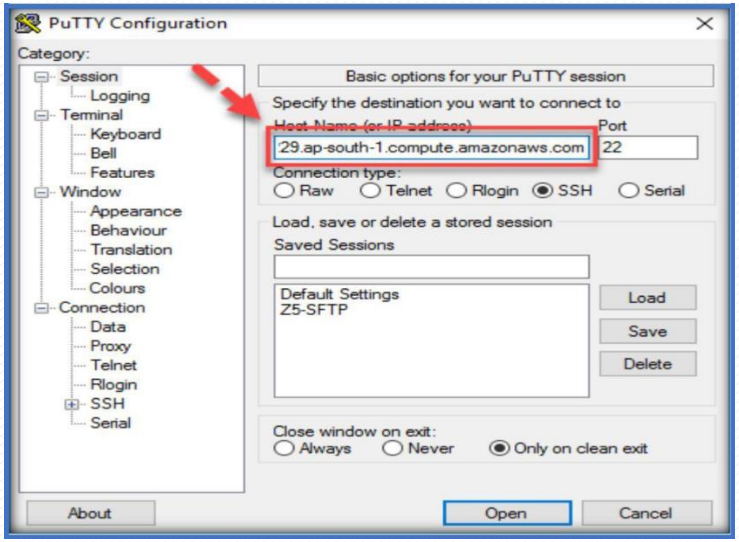


☐	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
☐		i-0514b0ce36c415198	t2.micro	ap-south-1a	● running	✓ 2/2 checks ...	None	ec2-35-154-17-229.ap-s...

Instance: i-0514b0ce36c415198   Public DNS: ec2-35-154-17-229.ap-south-1.compute.amazonaws.com

Instance ID	i-0514b0ce36c415198	Public DNS (IPv4)	ec2-35-154-17-229.ap-south-1.compute.amazonaws.com
Instance state	running	IPv4 Public IP	35.154.17.229
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-172-31-23-139.ap-south-1.compute.internal
Availability zone	ap-south-1a	Private IPs	172.31.23.139

Then paste that in the Hostname or IP Address text box in the PuTTY app.



PuTTY Configuration

Category:

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 29.ap-south-1.compute.amazonaws.com

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

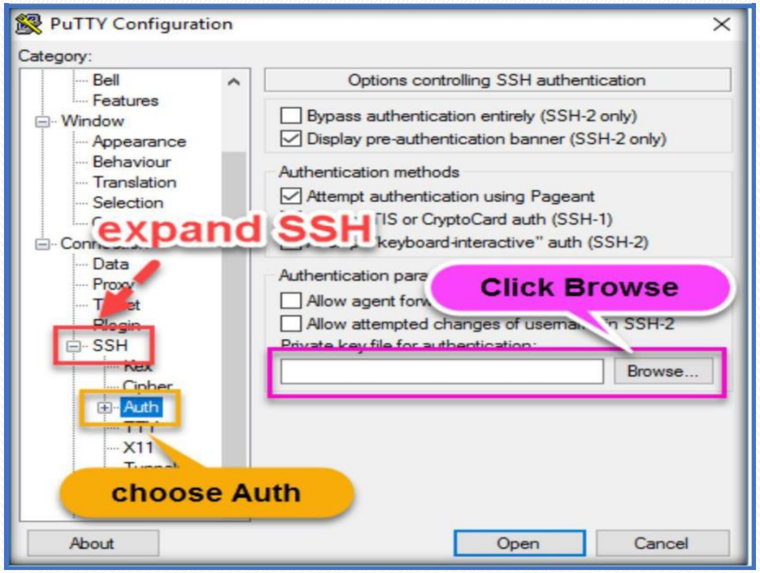
Load, save or delete a stored session

Saved Sessions

Default Settings
Z5-SFTP

Close window on exit: ○ Always ○ Never ● Only on clean exit

Then expand SSH under Connection, Choose Auth, then click on Browse from left



PuTTY Configuration

Category:

Options controlling SSH authentication

☐ Bypass authentication entirely (SSH-2 only)

☑ Display pre-authentication banner (SSH-2 only)

Authentication methods

☑ Attempt authentication using Pageant

TIS or CryptoCard auth (SSH-1)

keyboard-interactive" auth (SSH-2)

Authentication para

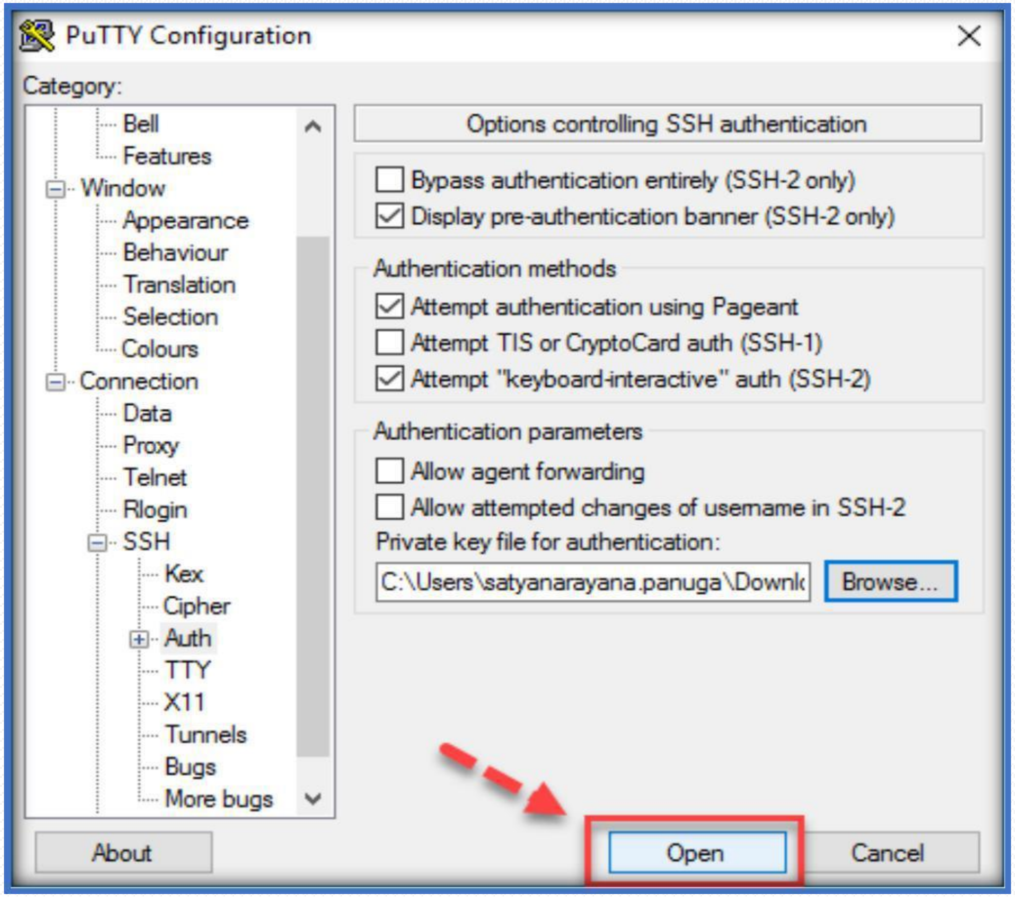
☐ Allow agent forw

☐ Allow attempted changes of userna in SSH-2

Private key file for authentication:

Choose the PPK file which we converted and click on open.

Next, choose Open on the PuTTY app, to connect to the Linux instance.



Options controlling SSH authentication

□ Bypass authentication entirely (SSH-2 only)
☑ Display pre-authentication banner (SSH-2 only)

Authentication methods

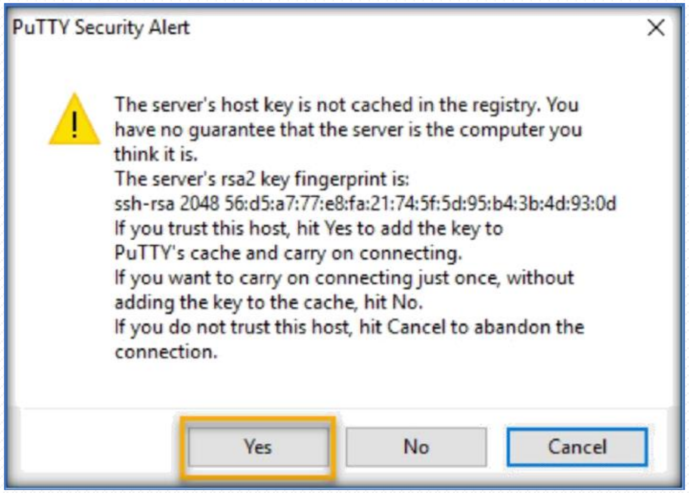
☑ Attempt authentication using Pageant
□ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding
□ Allow attempted changes of username in SSH-2

Private key file for authentication:
C:\Users\satyanarayana.panuga\Downk
Browse...

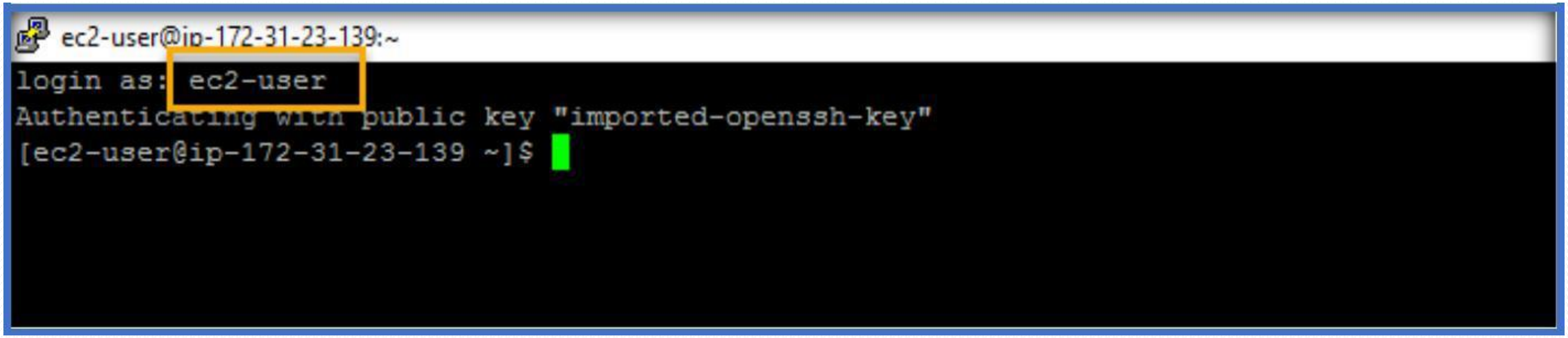
Next, choose yes.



PuTTY Security Alert

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 56:d5:a7:77:e8:fa:21:74:5f:5d:95:b4:3b:4d:93:0d
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

Now enter the username based on the Linux distro and enter to connect.



ec2-user@ip-172-31-23-139:~

```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
[ec2-user@ip-172-31-23-139 ~]$
```

Find the below default usernames for the different Linux distributions.

LINUX DISTRO	DEFAULT USERNAME
AMAZON LINUX	ec2-user
REDHAT	ec2-user
CENTOS	root
UBUNTU	ubuntu
SUSE	ec2-user
DEBIAN	admin