

# CREATING A KEY PAIR

Open below URL to open AWS login landing page.

<https://console.aws.amazon.com/>

Please fill your email address in the E-mail or mobile number box.

Select I am a returning user as show in the above picture.

Click on Sign in using our secure server.

## Sign In or Create an AWS Account

What is your email (phone for mobile accounts)?

E-mail or mobile number:

XXXXXXXXXXXXXXXXXXXX

Specify your email address

☐ I am a new user.

☒ I am a returning user and my password is:

.....

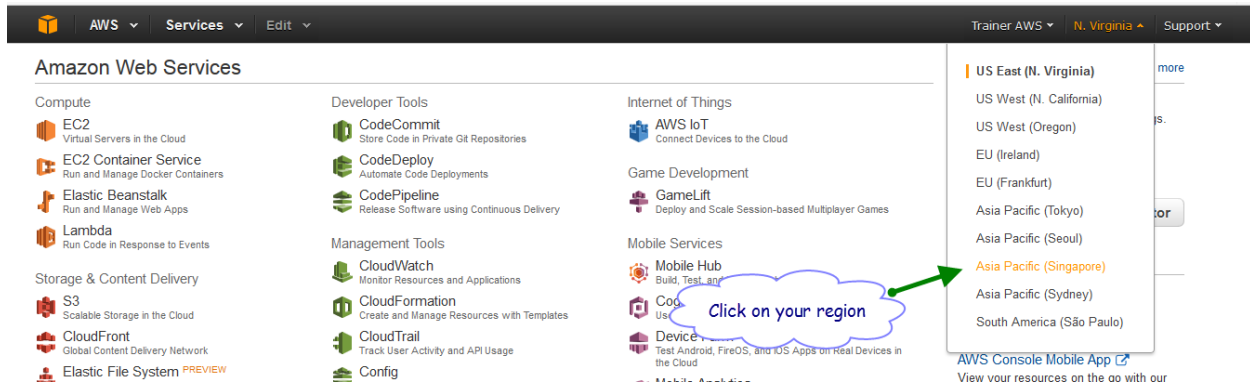
Select this as your a existing user

Sign in using our secure server

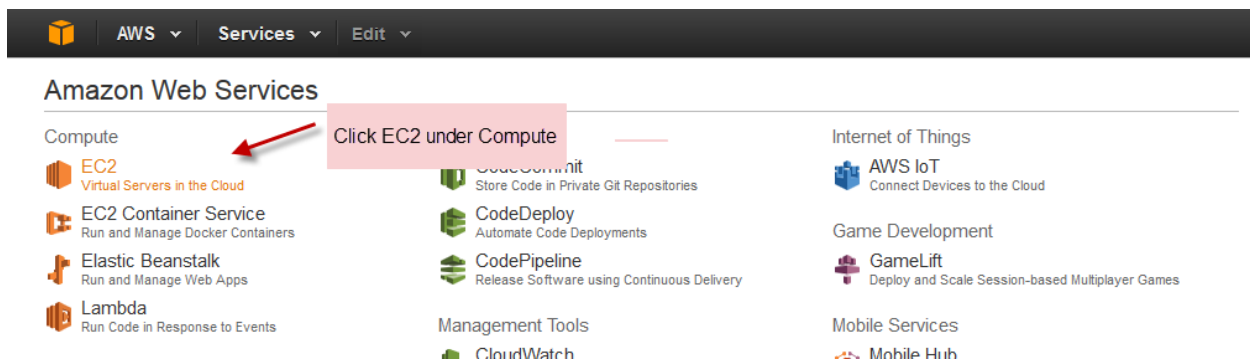
[Forgot your password?](#)

Click here to  
signin

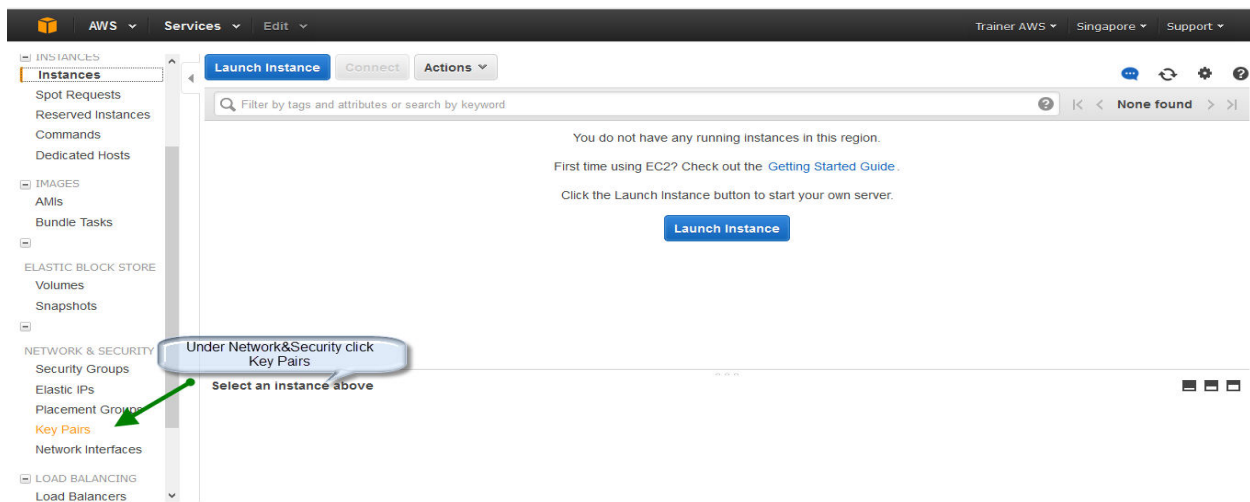
Once logged in select your region from top right side drop down menu as shown below.



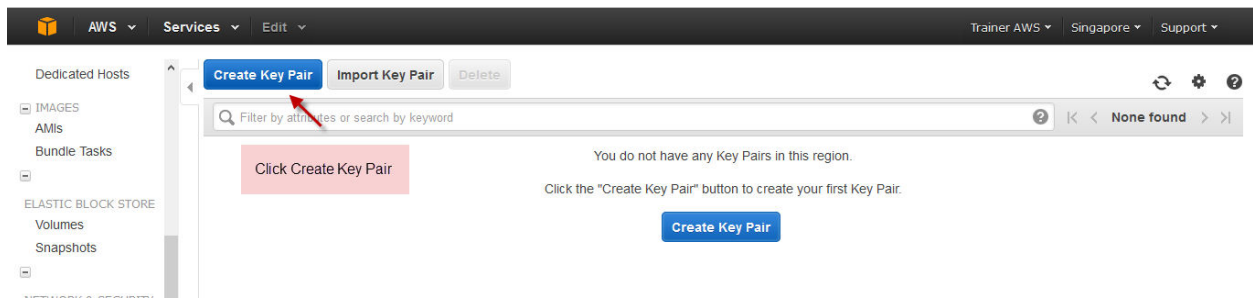
Then Click on EC2 under Compute menu.



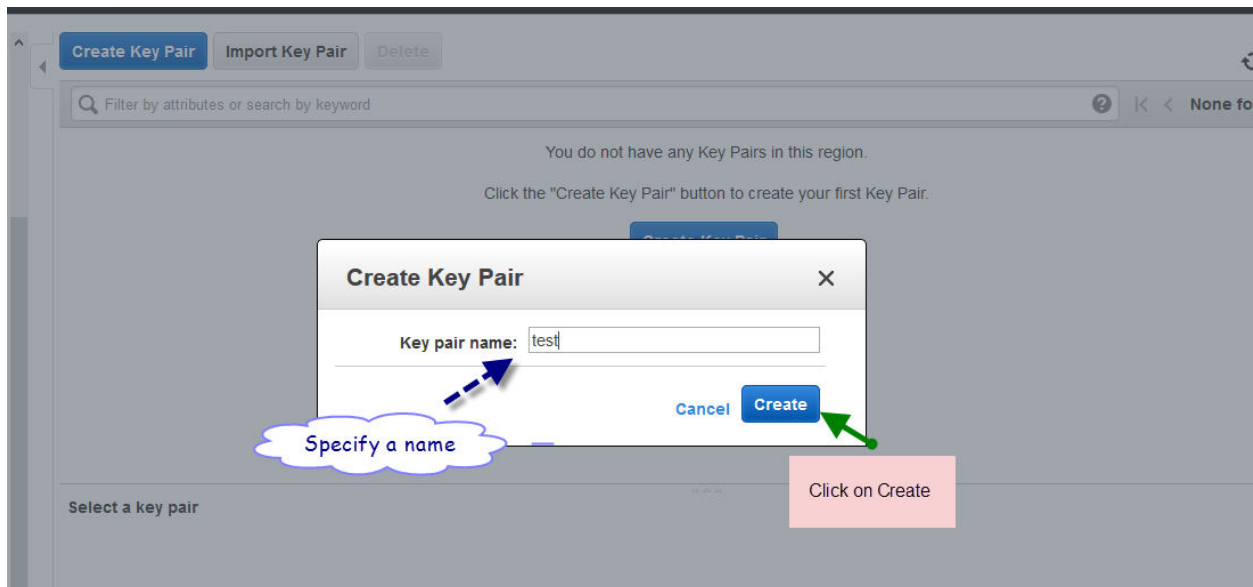
Then Click on Key Pairs under NETWORK & SECURITY menu on the left pane below.



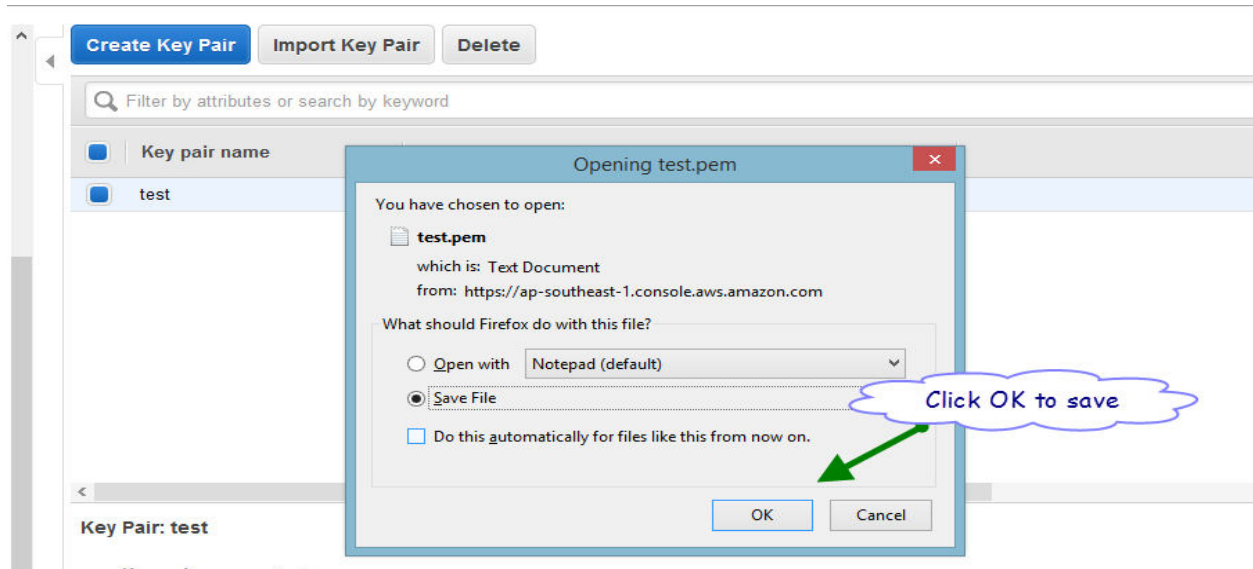
Then Click Create Key Pair.



Specify a name for your Key Pair and click on Create.



A popup window will come and ask you to save the Key pair click on OK to save your key pair.



Place your Key Pair in a secure location, once lost we cannot restore it back.

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 doing anything. We also supply cryptographic signatures for many of our binaries, 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 cryptographic policy, visit the [Keys page](#). If you need a Windows program to compute MD5 checksums, you could try

## Binaries

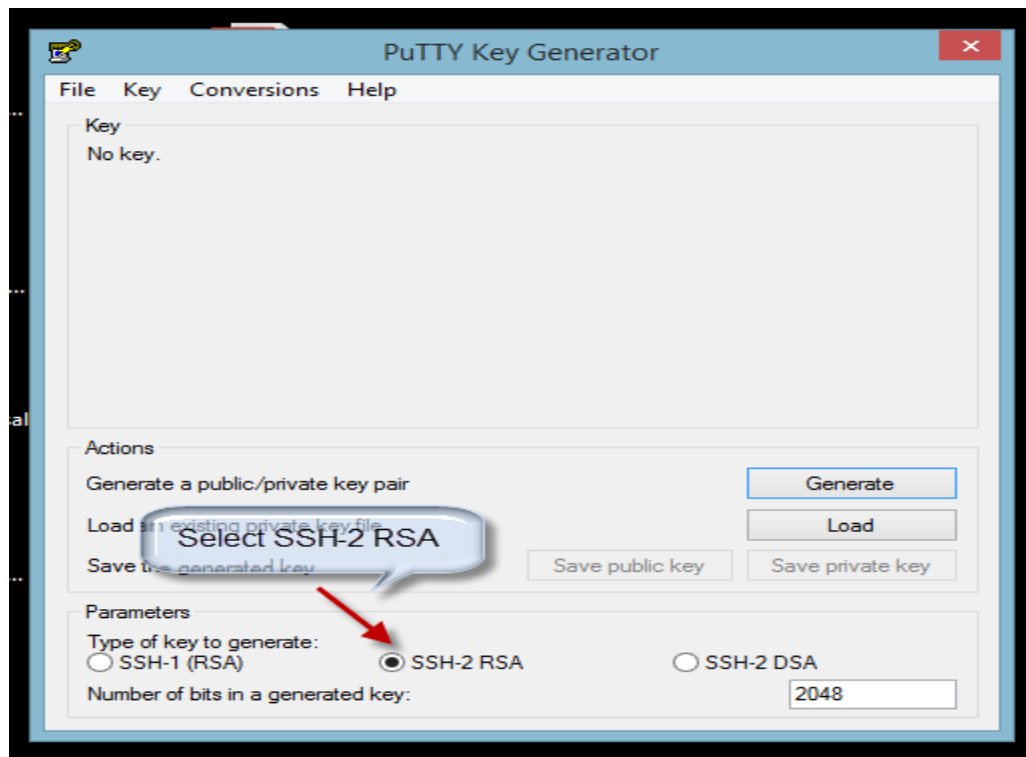
### The latest release version (beta 0.67)

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

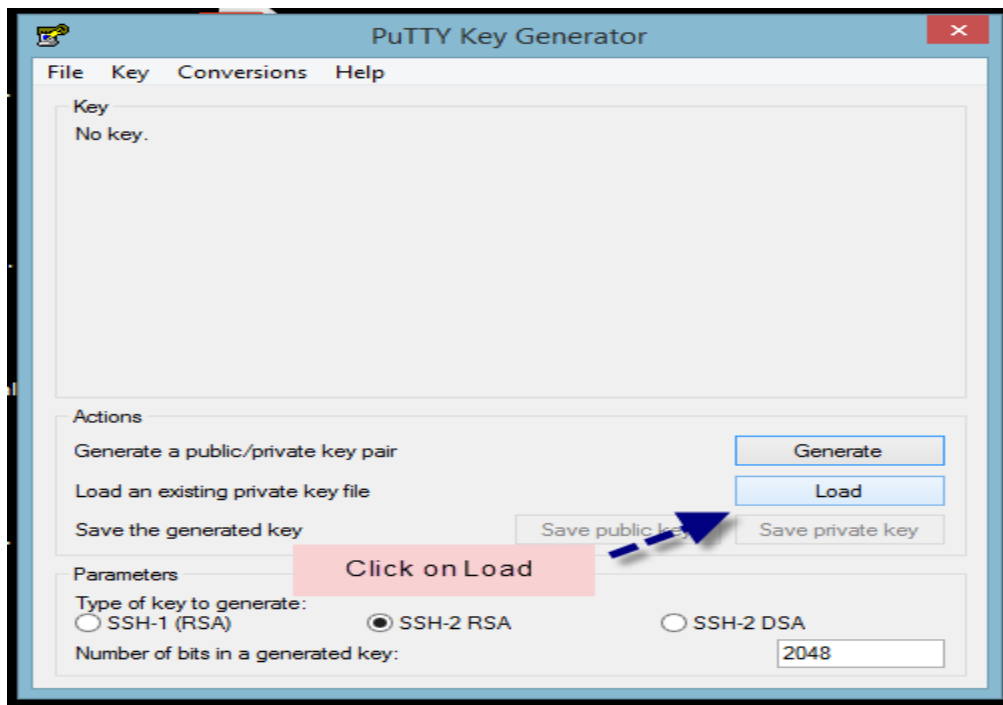
#### For Windows on Intel x86

PuTTY:	<a href="#">putty.exe</a>	(or by FTP)	(signature)
PuTTYtel:	<a href="#">puttytel.exe</a>	(or by FTP)	(signature)
pSCP:	<a href="#">pscp.exe</a>	(or by FTP)	(signature)
psFTP:	<a href="#">psftp.exe</a>	(or by FTP)	(signature)
Plink:	<a href="#">plink.exe</a>	(or by FTP)	(signature)
Pageant:	<a href="#">pageant.exe</a>	(or by FTP)	(signature)
PuTTYgen:	<a href="#">puttygen.exe</a>	(or by FTP)	(signature)

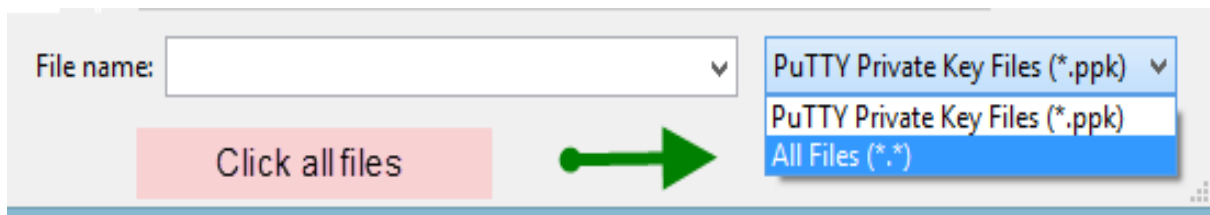
Open Puttygen.exe and select SSH-2 RSA in the below.



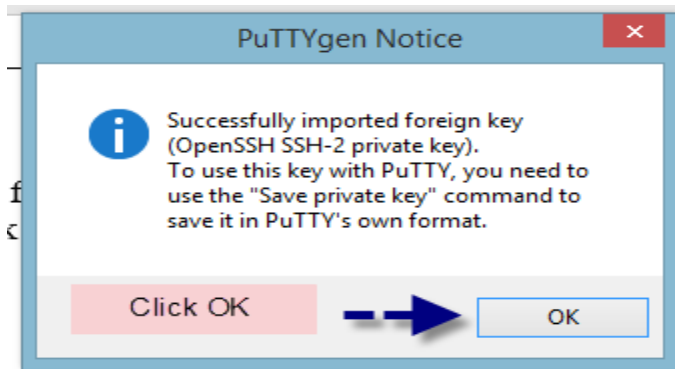
Click on Load to load the PEM file.



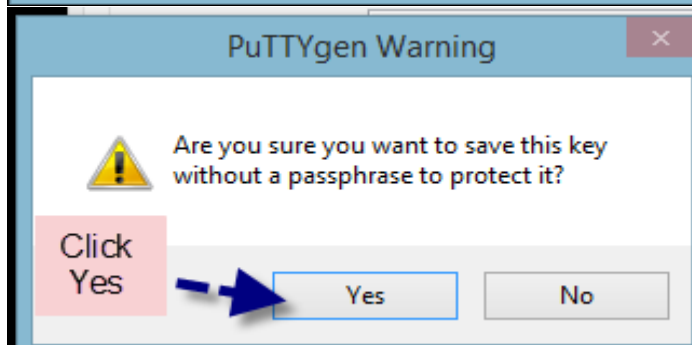
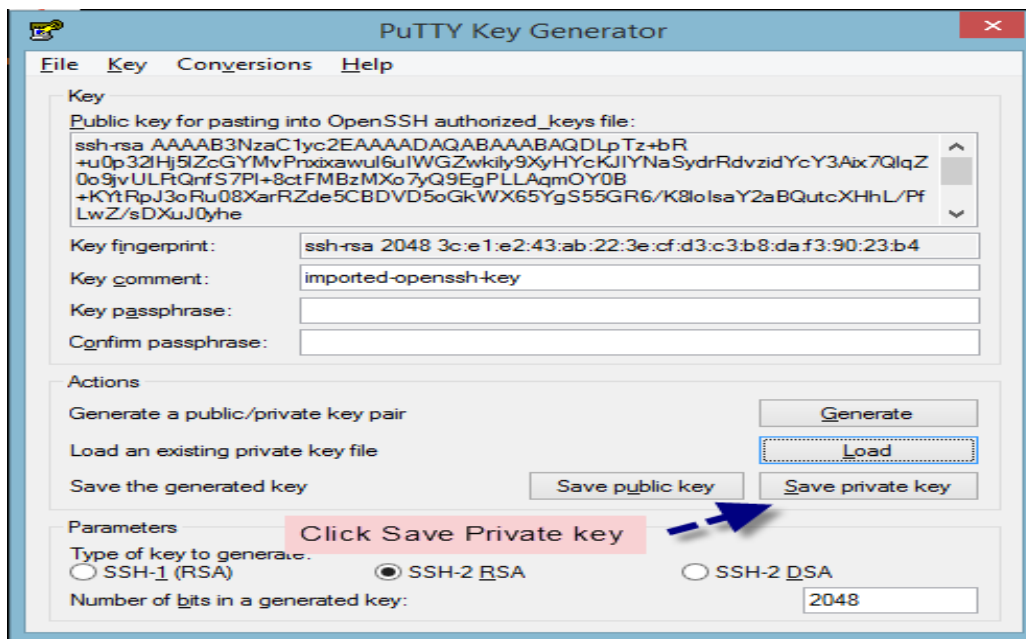
Once you click on Load, by default, Puttygen displays only files with extension **.ppk**. To locate your **.pem** file, select the option to display files of all types.



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.



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.





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

