

SSH INTO AN EC2 INSTANCE FROM WINDOWS USING PUTTY

Video Walkthrough:

<https://www.youtube.com/watch?v=bi7ow5NGC-U>

DOWNLOAD & Install PuTTY

If you don't have the PuTTY software installed on your system, you will need to download it from www.putty.org. Be sure to select the entire package as shown below, as it will include all the needed utilities such as puttygen and pageant.

Download PuTTY: latest release (0.69)

[Home](#) | [FAQ](#) | [Feedback](#) | [Licence](#) | [Updates](#) | [Mirrors](#) | [Keys](#) | [Links](#) | [Team](#)
Download: [Stable](#) · [Snapshot](#) | [Docs](#) | [Changes](#) | [Wishlist](#)

This page contains download links for the latest released version of PuTTY. Currently this is 0.69, released on 2017-04-29.

When new releases come out, this page will update to contain the latest, so this is a good page to bookmark or link to. Alternatively, here is a [permanent link to the 0.69 release](#).

Release versions of PuTTY are versions we think are reasonably likely to work well. However, they are often not the most up-to-date version of the code available. If you have a problem with this release, then it might be worth trying out the [development snapshots](#), to see if the problem has already been fixed in those versions.

Package files

You probably want one of these. They include all the PuTTY utilities.
(Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

MSI ('Windows Installer')

32-bit:	putty-0.69-installer.msi	(or by FTP)	(signature)
64-bit:	putty-64bit-0.69-installer.msi	(or by FTP)	(signature)

DOWNLOAD YOUR EC2 KEY PAIR FILE

If you have not already downloaded (or cannot locate) your key pair (i.e my_key_pair.pem) you will need to create a new EC2 instance and download a new one. A key pair consists of a public key that AWS stores and a private key file that you store (downloaded as PEM file). PEM stands for Privacy Enhanced Mail and is a widely used X.509 encoding format used for security certificates. Together, the two keys enable you to securely connect to your EC2 instance using SSH.

Select an existing key pair or create a new key pair ×

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

Key pair name
my_key_pair

Download Key Pair

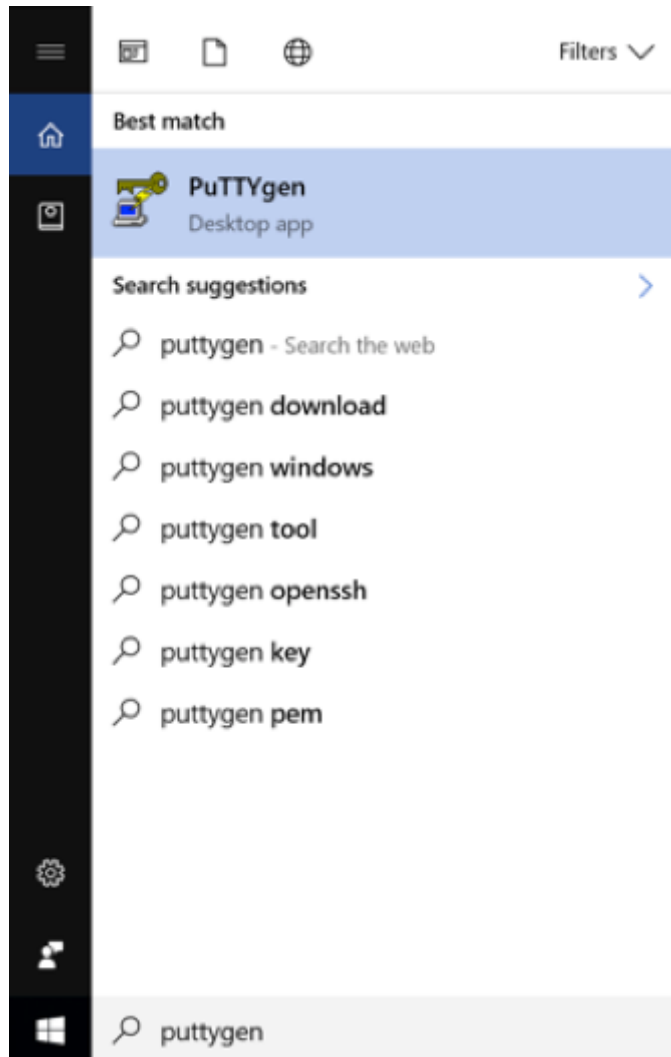
... You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel

Launch Instances

CONVERT YOUR PEM FILE TO PPK FORMAT

PuTTY does not natively support the PEM format that AWS uses, so you need to first convert your PEM file to a PPK file (PPK = PuTTY Private Key). To do this, you use the PuTTYgen utility. To start the utility you can type puttygen in the Windows start dialog box:

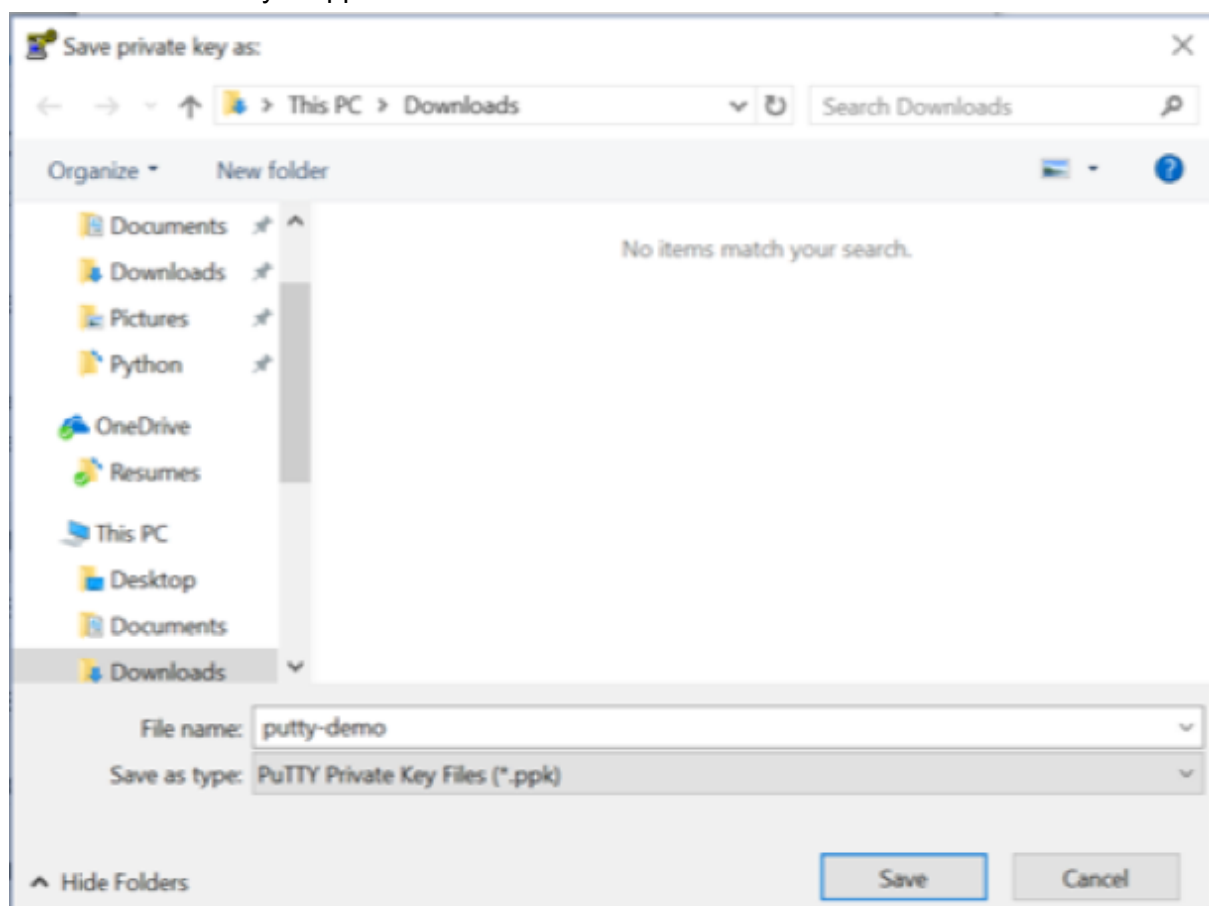


On the PuTTYgen dialog box, click the Load Button and then select the .pem file that you downloaded from AWS. Note: when browsing for your pem file be sure to select All Files in the dropdown list that is located to the right of the File name field. PuTTYgen will then load and convert your file.



As the message indicates, you then need to click on “Save private key”. You will receive a warning message asking if you want to save this key without a passphrase. Be sure to select Yes.

Provide a name for your ppk file and click save.



LAUNCH PuTTY

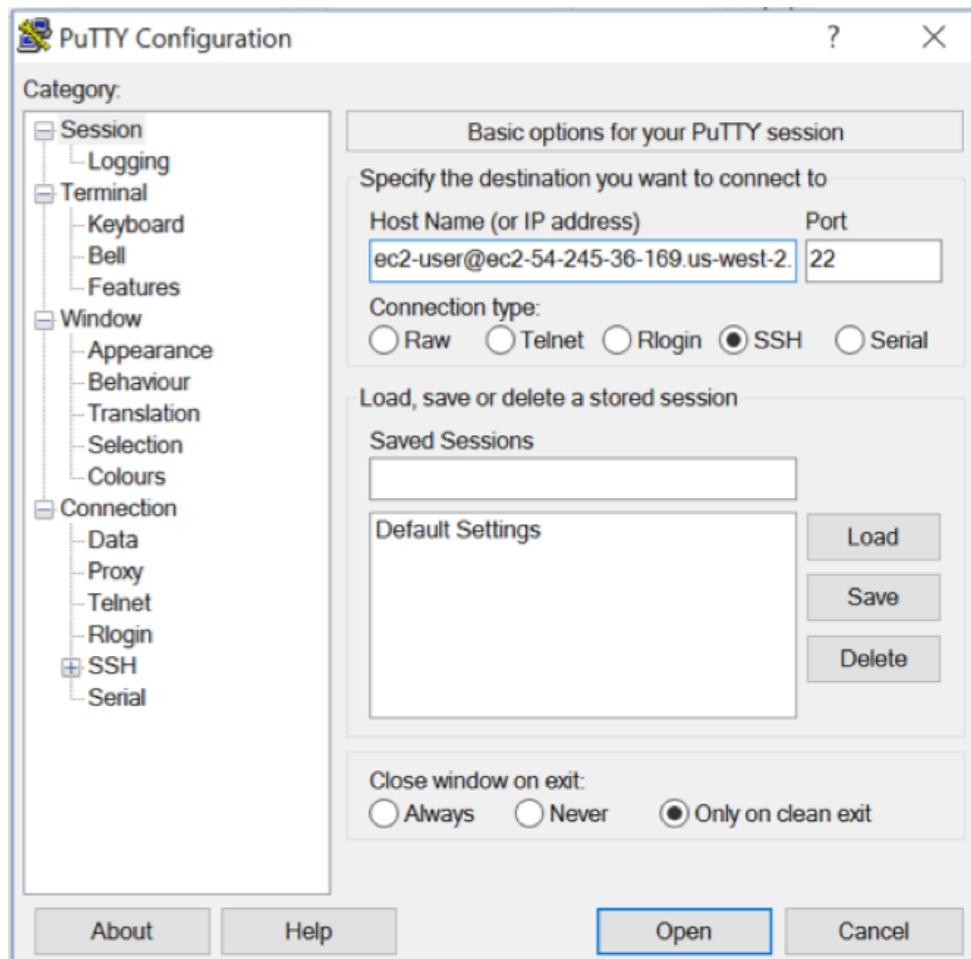
Now that you have converted the pem file to a ppk file, you are ready to use the PuTTY utility. In the Windows start dialog box, type in putty to start the utility.

ENTER HOST NAME

Enter your Host Name into the appropriate field. This will be in the format of: user_name@public_dns_name. Be sure to specify the appropriate user name for your AMI type. For example:

- For an Amazon Linux AMI, the user name is ec2-user.
- For a RHEL AMI, the user name is ec2-user or root.
- For an Ubuntu AMI, the user name is ubuntu or root.
- For a Centos AMI, the user name is centos.
- For a Fedora AMI, the user name is ec2-user.
- For SUSE, the user name is ec2-user or root.
- Otherwise, if ec2-user and root don't work, check with the AMI provider.

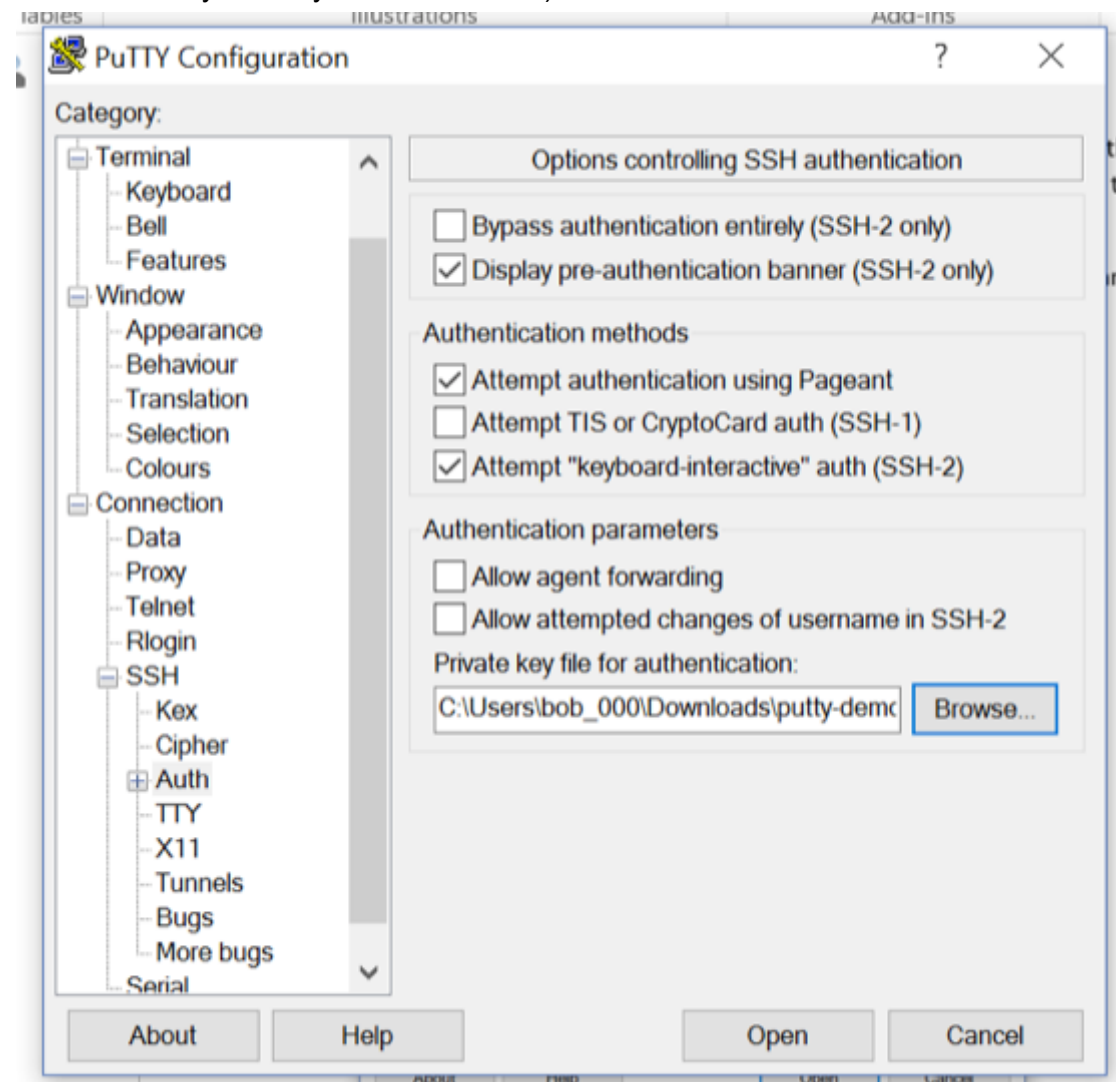
Here is an example for connecting to an Amazon Linux AMI:



SELECT YOUR PPK FILE

Next, click on the + button next to the SSH field to expand this section. Then click on Auth (which stands for authenticate) and enter the name of your private key file (i.e. the ppk file)

where it says Private key file for authentication (if you click on browse you can easily search for the directory where you have stored it).

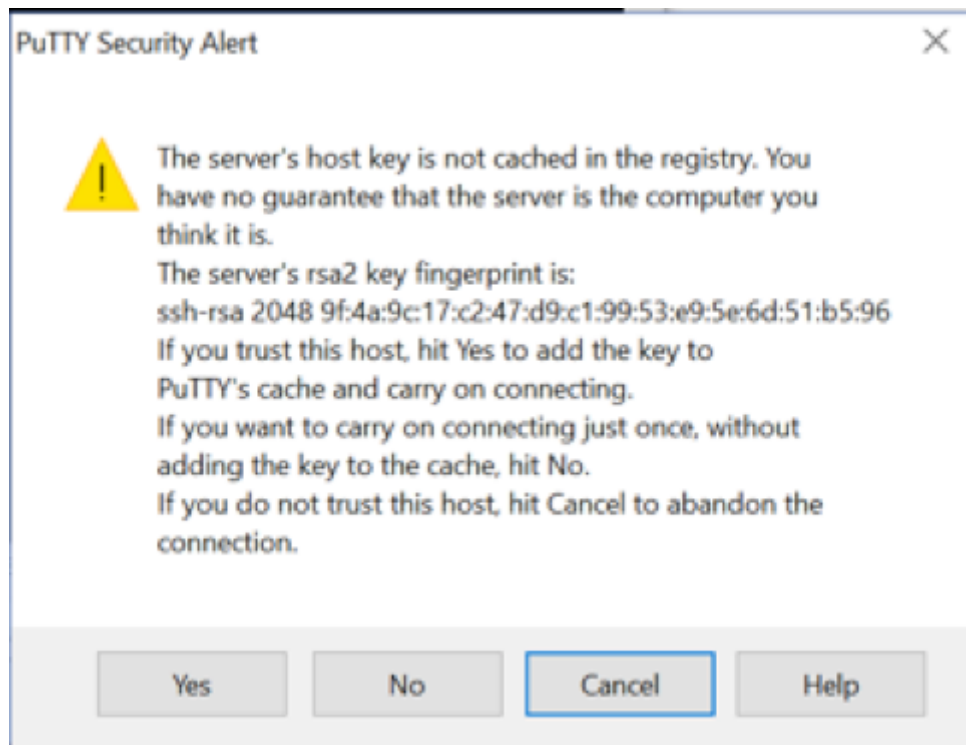


OPEN YOUR TERMINAL SESSION

Lastly, click on Open to start your SSH session.

Note: if this is the first time that you are logging into the instance, you will receive the following alert.

Click on Yes to continue.



If you did everything correctly, you will see a new window appear displaying your command line SSH session (troubleshooting hint: if the window appears but fails to connect, a common issue is that you likely have not created a rule to enable SSH inbound traffic on Port 22 in the Security Group that is attached to this instance.....so double check that first).

