SSH Tunnelling Guide (Client)

Author: Wayne Pounder

# Putty

## Download

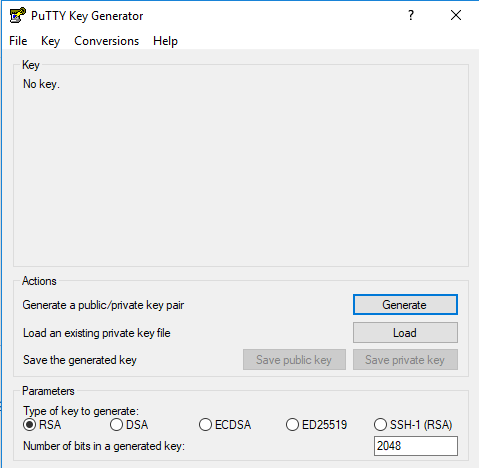
Download the latest release of Putty from here:

<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

## [OPTIONAL] Convert keys to Putty format (ppk)

Keys provided by AWS are in .pem format which are not readable by Putty. We must convert pem keys to Putty compatible ppk keys using “Puttygen” that is installed as part of the downloaded Putty package.

Open “Puttygen” and from the “Conversions” menu select “Import key”. Browse to the .pem format key

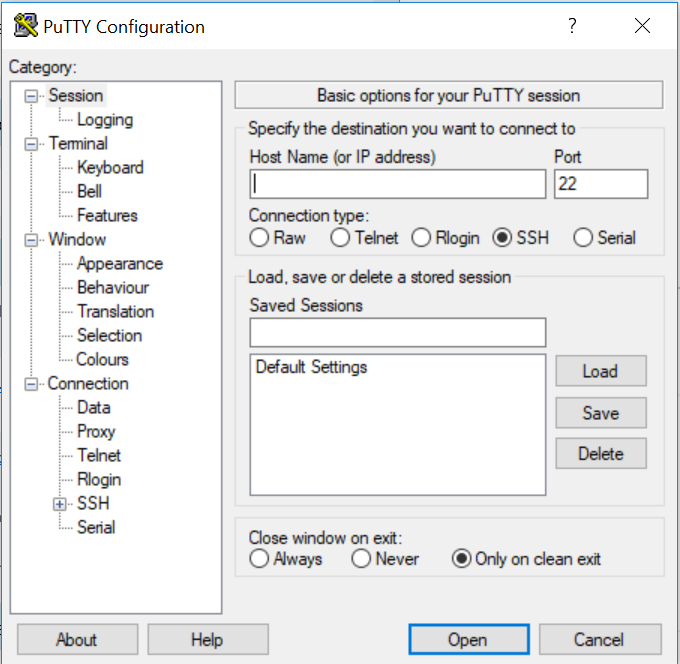


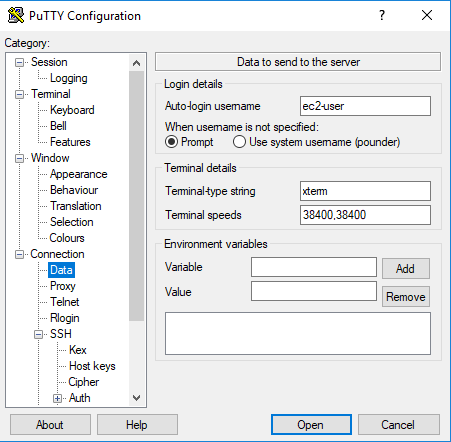
Once imported, click the “Save private key” button and save the key in ppk format.

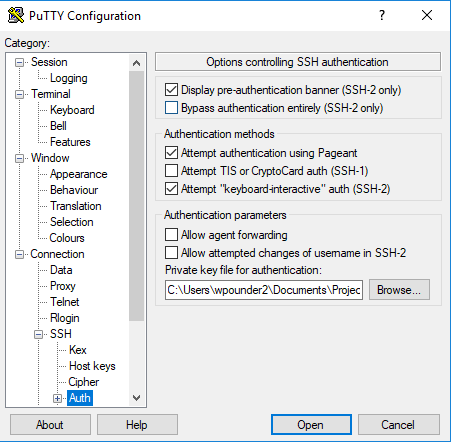
Exit Puttygen

## Create Saved Session for Bastion

Open Putty and enter the IP address of the Bastion host under “Host Name (or IP address)”. Enter a suitable name under “Saved Sessions”



From the “Category:” list expand “Connection” and choose “Data”. Under “Auto-login username” enter YOUR username

From the “Category:” list expand “Connection” and then expand “SSH”. Choose the “Auth” option. Under “Private key file for authentication” set the path to the YOUR private key.

From the “Category:” list choose “Session” and click “Save”.

Click “Open”. As this is your first session you will be prompted to verify the key fingerprint. Click “Yes”.

Exit the connection. You will only need to connect to this host again if your key pair changes.

## Add keys into memory securely using Putty Agent

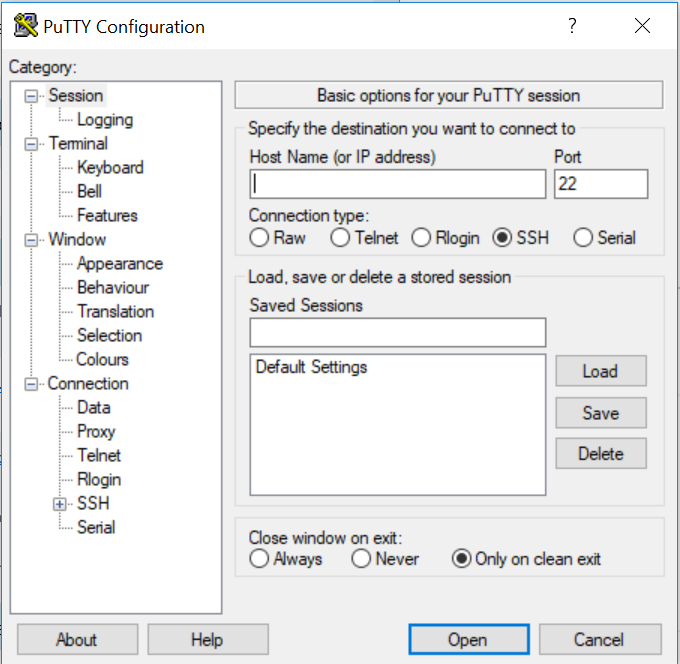
Open “Pageant” that came as part of the Putty package.

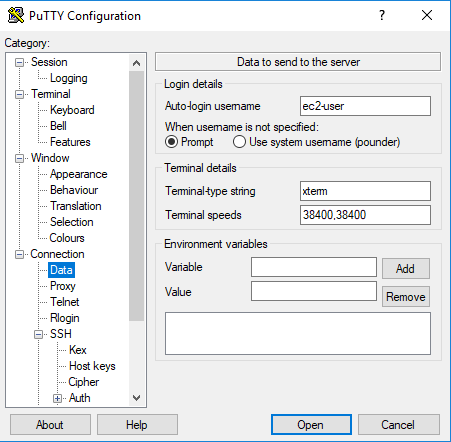
Click “Add key” and browse to the ppk file for YOUR user. Repeat this for the Orchestrator user key.

These keys are now available for use by Putty.

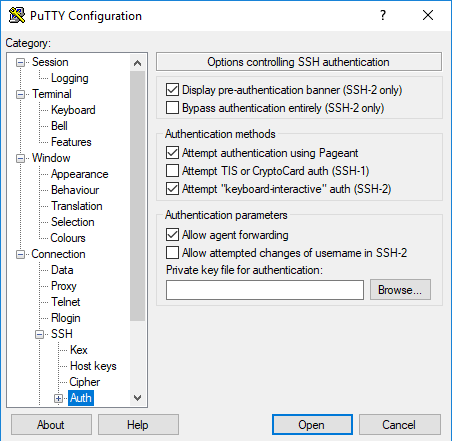
## Create Saved Session for Orchestrator

Open Putty and enter the IP address of the Orchestrator host under “Host Name (or IP address)”. Enter a suitable name under “Saved Sessions”



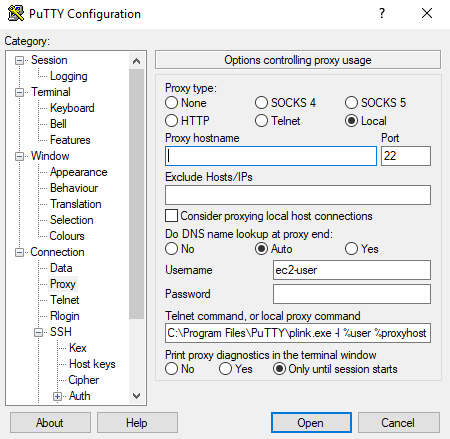
From the “Category:” list expand “Connection” and choose “Data”. Under “Auto-login username” enter “the Orchestrator Admin username”

From the “Category:” list expand “Connection” and then expand “SSH”. Choose the “Auth” option. Check “Allow agent forwarding”. This will utilise the keys stored in memory with Pageant.



From the “Category:” list expand “Connection” and choose “Proxy”. Set the type to “Local”. Enter the Bastion public IP as the “Proxy hostname”. Set the Username to YOUR username. Under “Telnet command, or local proxy command” enter the following string:

C:\Program Files\PuTTY\plink.exe -l %user %proxyhost -agent -nc %host:%port



From the “Category:” list choose “Session” and click “Save”.

Click “Open”. As this is your first session you will be prompted to verify the key fingerprint. Click “Yes”.

**NOTE:** You must add your keys to Pageant each time you restart your laptop as the keys are only held in memory.

# Mobaxterm

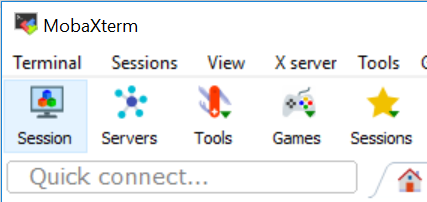
## Download

Download the latest release of Mobaxterm here:

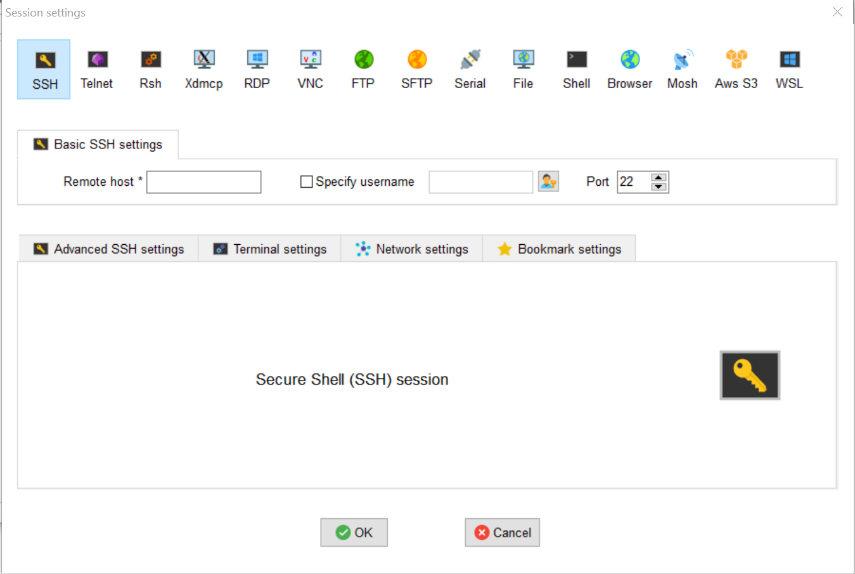
<https://mobaxterm.mobatek.net/download.html>

## Create Saved Session

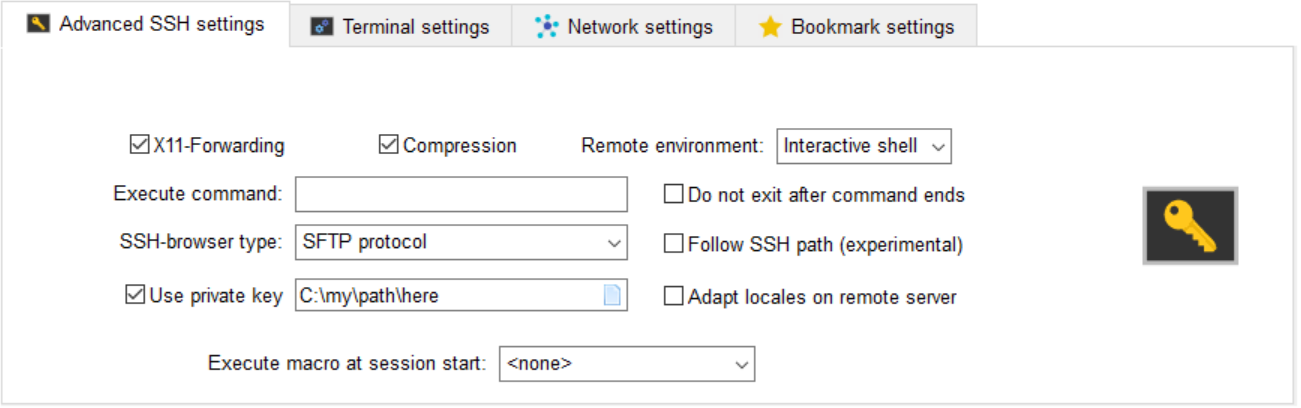
Open Mobaxterm and select “Session”



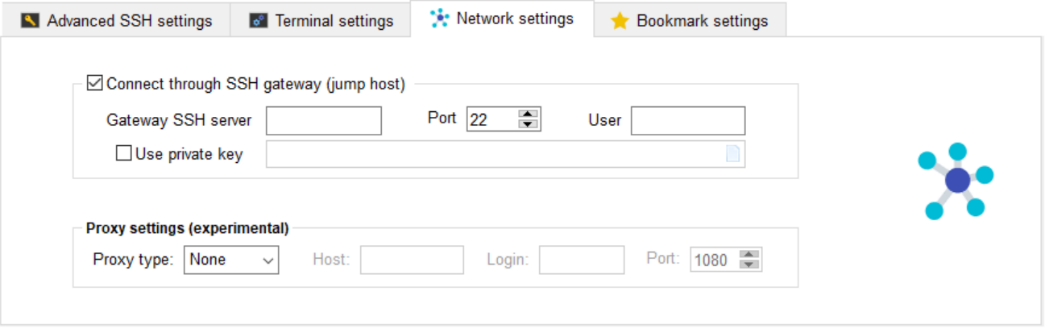
In the Session Settings dialog enter the IP address of the Orchestrator Host under “Remote host”, check the “Specify username” box and set the username as the Orchestrator Admin username.



Under the “Advanced SSH settings” tab check “Use private key” and enter the path to the private key for the Orchestrator Admin user.



Under the “Network settings” tab check “Connect through SSH gateway (jump host)”. Enter the public IP address of the Bastion host under “Gateway SSH server”. Set “User” to YOUR username. Check “Use private key” and enter the path to YOUR Bastion host private key.



Done.