

# Using PuTTY to Connect to vFXTs on AWS

## Process Overview

1. [Download and Install PuTTY](#)
2. [Configure Keys for PuTTY](#)
3. [Setup SSH session using PuTTY](#)
4. [Connect to Avere vFXT](#)

This process assumes that an instance with a public IP address (like a NAT) is in the VPC.

## Part 1: Download and Install PuTTY and Puttygen

Download and install PuTTY and puttygen from [the download page](#). This requires admin permissions on the local machine.

<b>putty.exe (the SSH and Telnet client itself)</b>			
32-bit:	<a href="#">putty.exe</a>	<a href="#">(or by FTP)</a>	<a href="#">(signature)</a>
64-bit:	<a href="#">putty.exe</a>	<a href="#">(or by FTP)</a>	<a href="#">(signature)</a>
<b>pscp.exe (an SCP client, i.e. command-line secure file copy)</b>			
32-bit:	<a href="#">pscp.exe</a>	<a href="#">(or by FTP)</a>	<a href="#">(signature)</a>
64-bit:	<a href="#">pscp.exe</a>	<a href="#">(or by FTP)</a>	<a href="#">(signature)</a>
<b>psftp.exe (an SFTP client, i.e. general file transfer sessions much like FTP)</b>			
32-bit:	<a href="#">psftp.exe</a>	<a href="#">(or by FTP)</a>	<a href="#">(signature)</a>
64-bit:	<a href="#">psftp.exe</a>	<a href="#">(or by FTP)</a>	<a href="#">(signature)</a>
<b>puttytel.exe (a Telnet-only client)</b>			
32-bit:	<a href="#">puttytel.exe</a>	<a href="#">(or by FTP)</a>	<a href="#">(signature)</a>
64-bit:	<a href="#">puttytel.exe</a>	<a href="#">(or by FTP)</a>	<a href="#">(signature)</a>
<b>plink.exe (a command-line interface to the PuTTY back ends)</b>			
32-bit:	<a href="#">plink.exe</a>	<a href="#">(or by FTP)</a>	<a href="#">(signature)</a>
64-bit:	<a href="#">plink.exe</a>	<a href="#">(or by FTP)</a>	<a href="#">(signature)</a>
<b>pageant.exe (an SSH authentication agent for PuTTY, PSCP, PSFTP, and Plink)</b>			
32-bit:	<a href="#">pageant.exe</a>	<a href="#">(or by FTP)</a>	<a href="#">(signature)</a>
64-bit:	<a href="#">pageant.exe</a>	<a href="#">(or by FTP)</a>	<a href="#">(signature)</a>
<b>puttygen.exe (a RSA and DSA key generation utility)</b>			
32-bit:	<a href="#">puttygen.exe</a>	<a href="#">(or by FTP)</a>	<a href="#">(signature)</a>
64-bit:	<a href="#">puttygen.exe</a>	<a href="#">(or by FTP)</a>	<a href="#">(signature)</a>

## Part 2: Configure Keys for PuTTY

The AWS keys are in a .pem file format and they need to be converted into a .ppk format.

Open puttygen.

Ensure that one of the RSA options is selected at the bottom like SSH-2 RSA.

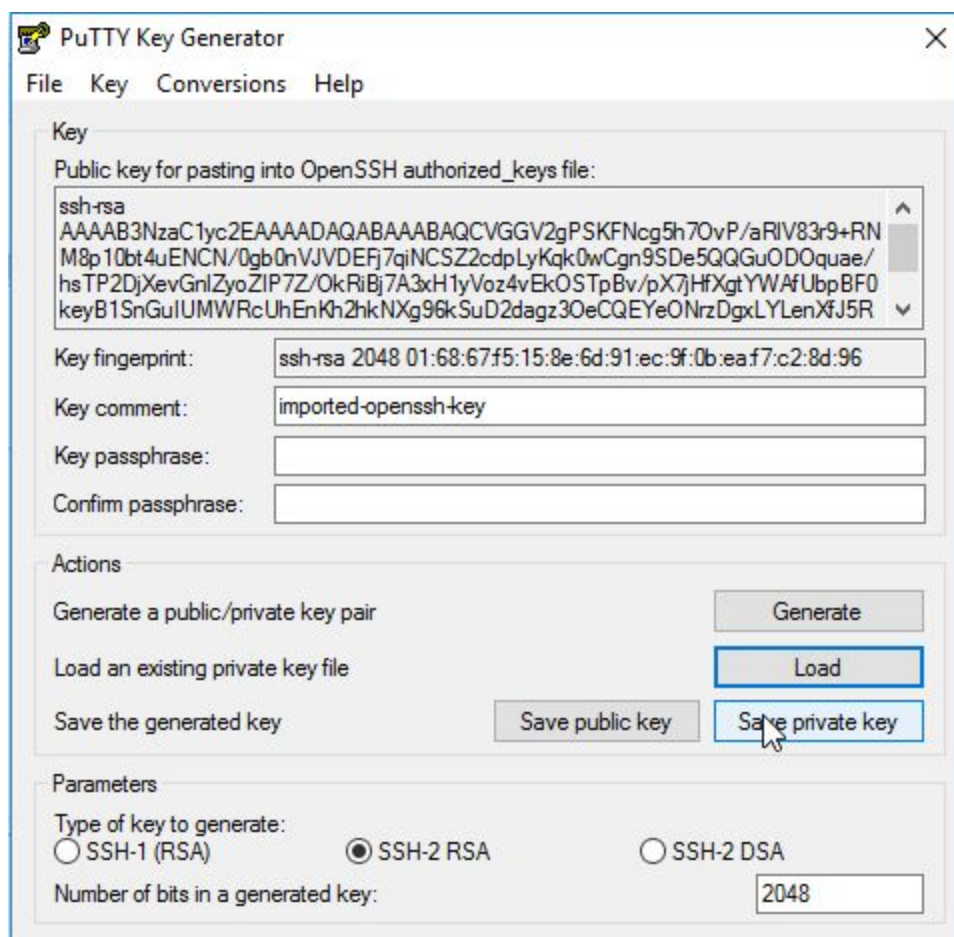
Click **Load**.

Navigate to the location where the .pem file is stored. This is the key file from Part 1.

Double click the .pem file.

PuTTYgen will indicate a successful import. Click **OK**.

Click **Save private key**.



Click **Yes**.

Name the file and note its location.

Press Enter or click the **Save** button.

## Part 3: Setup SSH session using PuTTY

This part requires the public IP address of an instance, a local port for tunneling, and the vFXT management IP address. If internet access requires a proxy server, you will need that information.

Copy the public IP address of the instance.

Run putty.

Paste the public IP address of the instance in PuTTY's "Host Name (or IP address)" field.

Enter a name for this stored session. Example: Avere vFXT

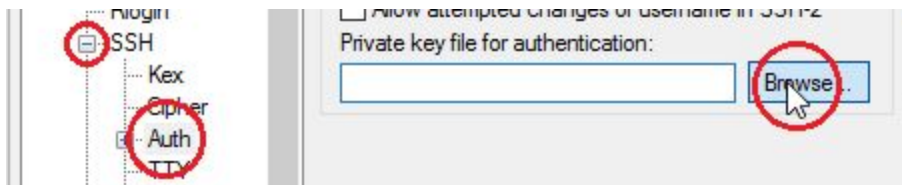
Click **Save**.

To add any proxy settings for your company's proxy server, click **Proxy** on the left.

In the left navigation, click the **+** next to SSH.

Click **Auth**.

Click **Browse**.



Navigate to the .ppk file from Part 3.

Double click the .ppk file.

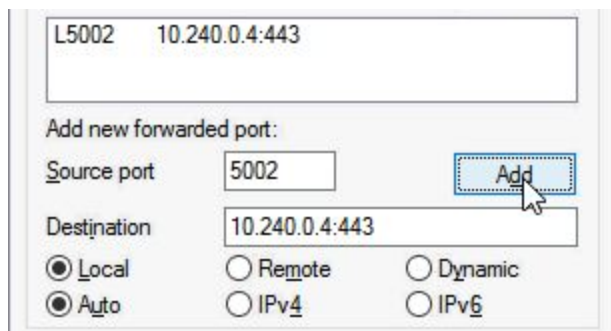
Click **Tunnels** on the left.

Enter a port, like 8443, that you can use for tunneling in the Source port field. If this port is not available, please choose another port like 5002. To see what ports are available, run `netstat -p TCP -an | find "127.0.0.1"` to see local ports being used.

For the Destination, copy and paste the vFXT management IP address (example: 10.240.0.4).

Add **:443** to the end of the Destination.

Click **Add**.



Scroll to the top left and click **Session**.

Click the **Save** button on the right. This second Save session is required to keep your changes.

## Part 4: Connect to Avere vFXT

From putty, click **Open** in the lower right.

Enter the username for the instance, typically ec2-user, and press Enter.

```
login as: ec2-user
Authenticating with public key "imported-openssh-key"

  _|  _|_ )
  _| ( _|_ /  Amazon Linux AMI
  _|\_|_|_|

https://aws.amazon.com/amazon-linux-ami/2014.09-release-notes/
40 package(s) needed for security, out of 169 available
Run "sudo yum update" to apply all updates.
Amazon Linux version 2016.09 is available.
[ec2-user@ip-192-168-2-148 ~]$ █
```

If ec2-user doesn't work, it will often be root or admin. Navigate to EC2 > Instances > click the instance with the public IP address > click Connect > find the username under Example.

## Connect To Your Instance



I would like to connect with

- A standalone SSH client
- A Java SSH Client directly from my browser (Java required)

### To access your instance:

1. Open an SSH client. (find out how to [connect using PuTTY](#))
2. Locate your private key file (test.pem). The wizard automatically detects the key you used to launch the instance.
3. Your key must not be publicly viewable for SSH to work. Use this command if needed:

```
chmod 400 test.pem
```

4. Connect to your instance using its Public IP:

```
54.87.207.81
```

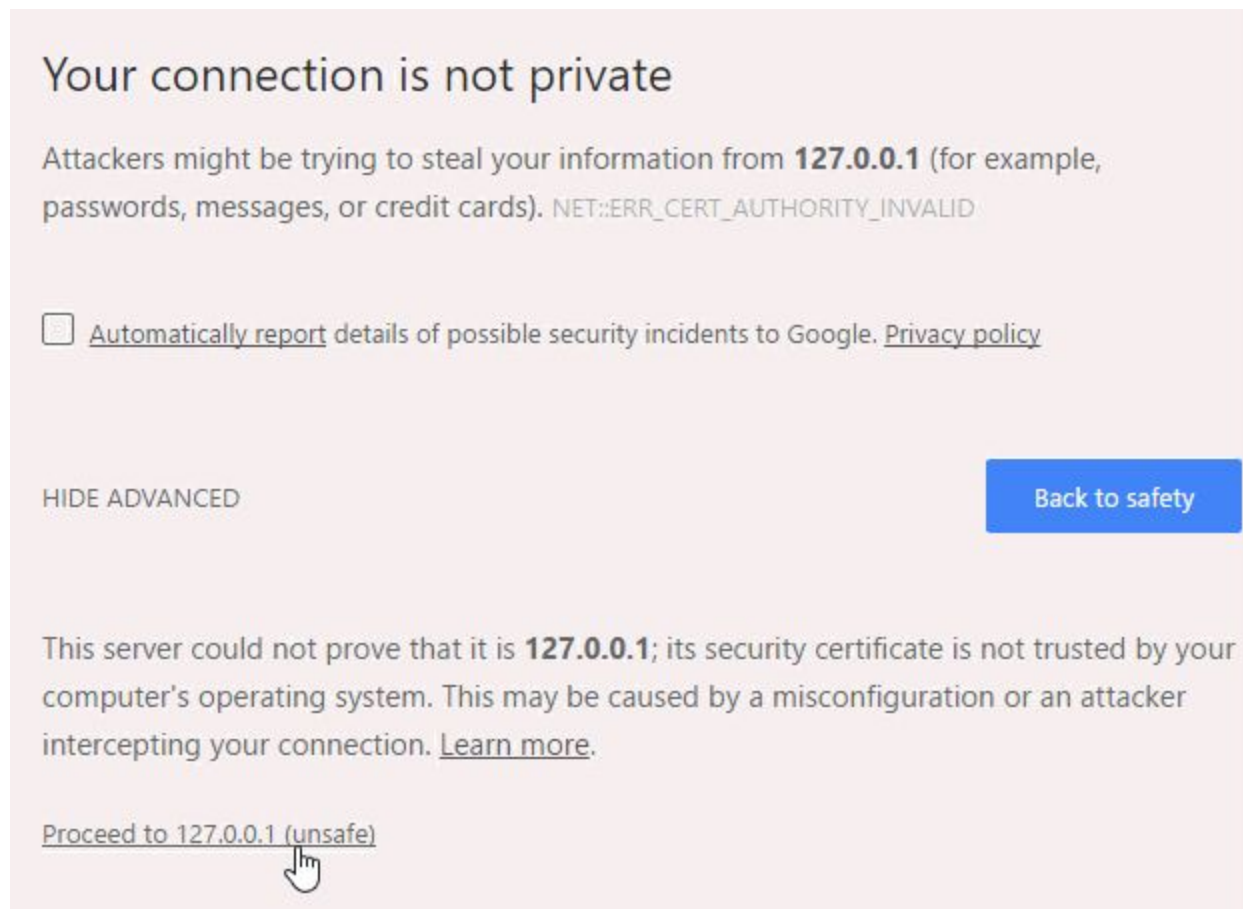
### Example:

```
ssh -i "test.pem" ec2-user@54.87.207.81
```

Please note that in most cases the username above will be correct, however please ensure that you read your AMI usage instructions to ensure that the AMI owner has not changed the

In your browser, navigate to <https://127.0.0.1:8443>. Change the port if you used a different port. The browser will show that the session is not private. Indicate that you understand and navigate to it. In Chrome, for example, click **Advanced** in the lower left and then **Proceed to 127.0.0.1**.

At the Avere Control Panel, enter **admin** for the username and provide the password.



The screenshot shows a browser security warning page with a light pink background. At the top, the heading reads "Your connection is not private". Below this, a message states: "Attackers might be trying to steal your information from **127.0.0.1** (for example, passwords, messages, or credit cards). NET::ERR\_CERT\_AUTHORITY\_INVALID". There is a checkbox with the text "Automatically report details of possible security incidents to Google. [Privacy policy](#)". Below the checkbox is the text "HIDE ADVANCED" and a blue button labeled "Back to safety". Further down, a paragraph explains: "This server could not prove that it is **127.0.0.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. [Learn more.](#)". At the bottom, there is a link "Proceed to 127.0.0.1 (unsafe)" with a mouse cursor pointing to it.

## Reconnecting

Virtual machines receive new IP addresses after each restart. When reconnecting to your cluster, you will need to provide the new public IP address in putty.

Open putty.

Select the Avere vFXT session that was previously saved.

Click **Load**.

Paste the new, public IP address in the "Host Name (or IP address)" field of putty.

Click **Save**.