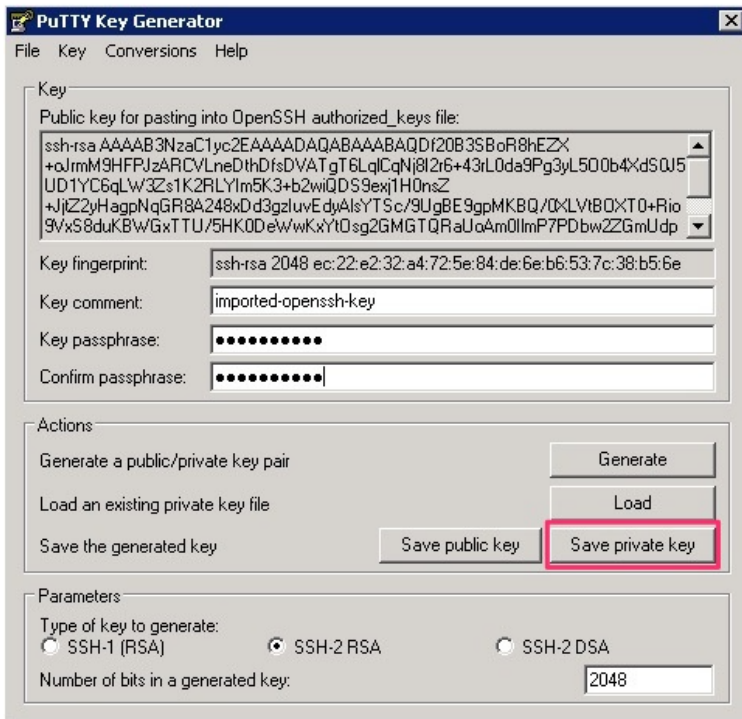


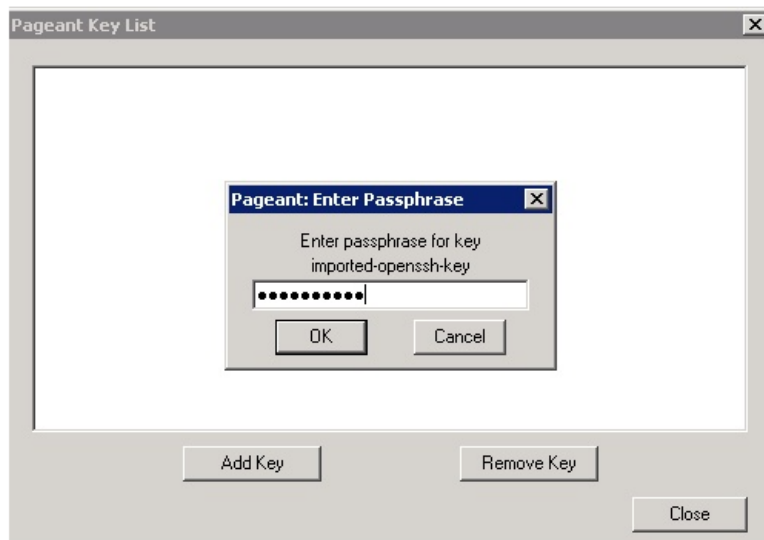
Configuring ssh-agent on Windows

In Windows, you can connect to Linux VPC instances using PuTTY. To get SSH agent functionality, you can use Pageant, which is available from the PuTTY [download page](#). When Pageant is installed, you can use the agent forwarding option in PuTTY to connect to instances in private subnets.

To use Pageant, you need to convert your private key from PEM format to PuTTY format using PuTTYGen (available from the PuTTY [download page](#)). In PuTTYGen, choose **Conversions > Import Key** and select your PEM-formatted private key. Enter a passphrase and then click **Save private key**, as shown in the following screenshot. Save the key as a .ppk file.



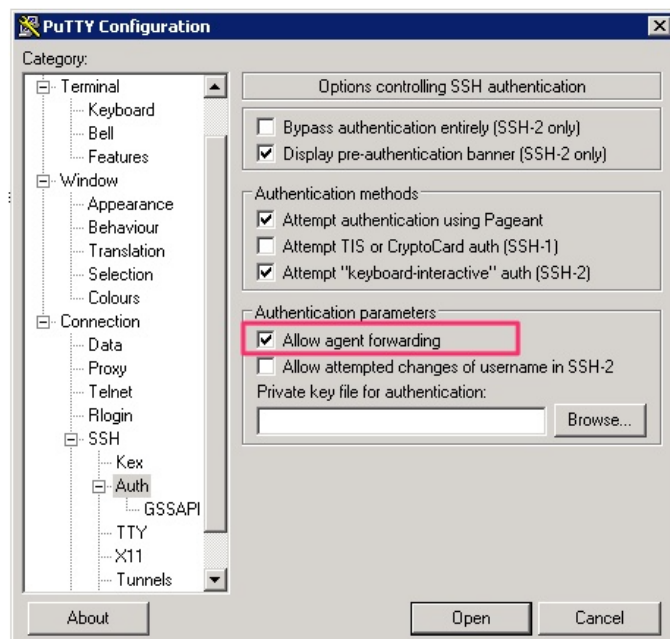
After you convert the private key, open Pageant, which runs as a Windows service. To import the PuTTY-formatted key into Pageant, double-click the Pageant icon in the notification area and then click **Add Key**. When you select the .ppk file, you're prompted to enter the passphrase you chose when you converted the key, as shown in the following screenshot.



After you add the key, close the **Pageant Key List** window.

Finally, when you are configuring the connections for SSH in PuTTY, check the **Allow agent forwarding** box and leave the **Private key file for authentication** field empty.

When you use PuTTY to connect to the public IP address of your bastion, you will see that the Pageant PuTTY component provides the SSH key for authentication, as shown in the following screenshot.



With agent forwarding enabled in the PuTTY configuration, you can connect from the bastion to any other instance in the VPC without having the SSH private key on the bastion. To connect to other instances, use the following command:

```
ssh ec2-user@private ip
```

As long as the matching private key for the instance is loaded into Pageant, the connection will be successful, as shown in the following screenshot.