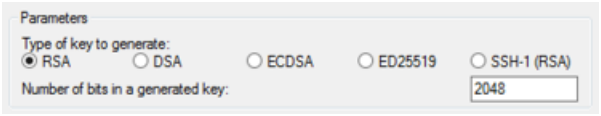
Convert your private key using PuTTYgen

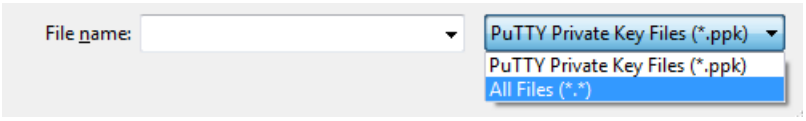
PuTTY does not natively support the private key format for SSH keys. PuTTY provides a tool named PuTTYgen, which converts keys to the required format for PuTTY. You must convert your private key (.pem file) into this format (.ppk file) as follows in order to connect to your instance using PuTTY.

To convert your private key

1. From the **Start** menu, choose **All Programs**, **PuTTY**, **PuTTYgen**.
2. Under **Type of key to generate**, choose **RSA**. If you're using an older version of PuTTYgen, choose **SSH-2 RSA**.



3. Choose **Load**. By default, PuTTYgen displays only files with the extension `.ppk`. To locate your `.pem` file, choose the option to display files of all types.



4. Select your `.pem` file for the key pair that you specified when you launched your instance and choose **Open**. PuTTYgen displays a notice that the `.pem` file was successfully imported. Choose **OK**.
5. To save the key in the format that PuTTY can use, choose **Save private key**. PuTTYgen displays a warning about saving the key without a passphrase. Choose **Yes**.

   Note
   A passphrase on a private key is an extra layer of protection. Even if your private key is discovered, it can't be used without the passphrase. The downside to using a passphrase is that it makes automation harder because human intervention is needed to log on to an instance, or to copy files to an instance.
6. Specify the same name for the key that you used for the key pair (for example, `my-key-pair`) and choose **Save**. PuTTY automatically adds the `.ppk` file extension.

Your private key is now in the correct format for use with PuTTY. You can now connect to your instance using PuTTY's SSH client.

Connecting to your Linux instance

Use the following procedure to connect to your Linux instance using PuTTY. You need the `.ppk` file that you created for your private key. For more information, see Convert your private key using PuTTYgen (p. 545) in the preceding section. If you receive an error while attempting to connect to your instance, see Troubleshooting Connecting to Your Instance.

To connect to your instance using PuTTY

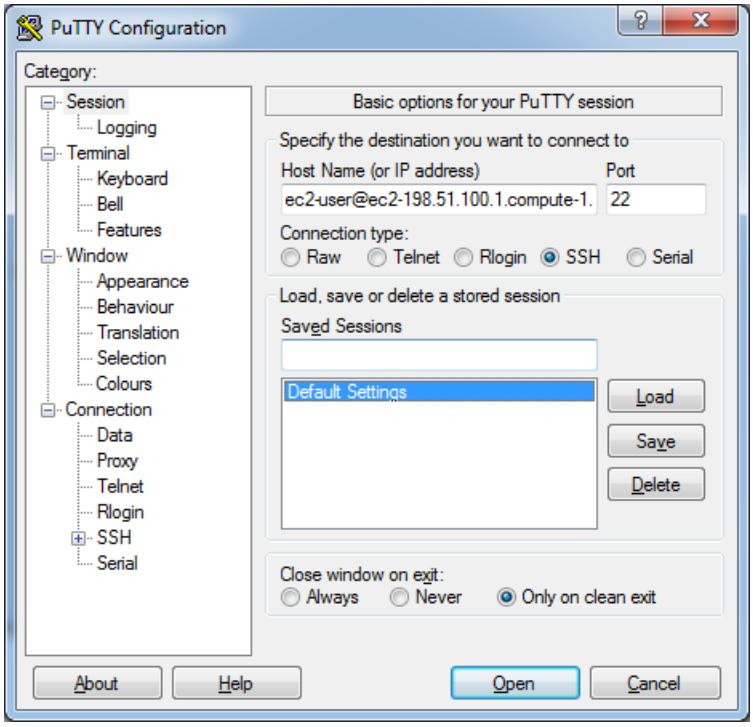
1. Start PuTTY (from the **Start** menu, choose **All Programs, PuTTY, PuTTY**).
2. In the **Category** pane, choose **Session** and complete the following fields:

   a. In the **Host Name** box, do one of the following:
   - (Public DNS) To connect using your instance's public DNS name, enter *my-instance-user-name*@*my-instance-public-dns-name*.
   - (IPv6) Alternatively, if your instance has an IPv6 address, to connect using your instance's IPv6 address, enter *my-instance-user-name*@*my-instance-IPv6-address*.

For information about how to get the user name for your instance, and the public DNS name or IPv6 address of your instance, see Get information about your instance (p. 530).

b. Ensure that the **Port** value is 22.

c. Under **Connection type**, select **SSH**.



3. (Optional) You can configure PuTTY to automatically send 'keepalive' data at regular intervals to keep the session active. This is useful to avoid disconnecting from your instance due to session inactivity. In the **Category** pane, choose **Connection**, and then enter the required interval in the **Seconds between keepalives** field. For example, if your session disconnects after 10 minutes of inactivity, enter 180 to configure PuTTY to send keepalive data every 3 minutes.
4. In the **Category** pane, expand **Connection**, expand **SSH**, and then choose **Auth**. Complete the following:

   a. Choose **Browse**.

   b. Select the `.ppk` file that you generated for your key pair and choose **Open**.

   c. (Optional) If you plan to start this session again later, you can save the session information for future use. Under **Category**, choose **Session**, enter a name for the session in **Saved Sessions**, and then choose **Save**.

   d. Choose **Open**.
5. If this is the first time you have connected to this instance, PuTTY displays a security alert dialog box that asks whether you trust the host to which you are connecting.

   a. (Optional) Verify that the fingerprint in the security alert dialog box matches the fingerprint that you previously obtained in (Optional) Get the instance fingerprint (p. 531). If these fingerprints don't match, someone might be attempting a "man-in-the-middle" attack. If they match, continue to the next step.

   b. Choose **Yes**. A window opens and you are connected to your instance.