Convert your private key using PuTTYgen

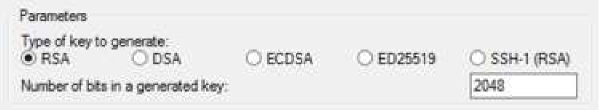
Locate the private key (.pem file) for the key pair that you specified when you launched the instance. Convert the .pem file to a .ppk file for use with PuTTY. For more information, follow the steps in the next section.

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**.

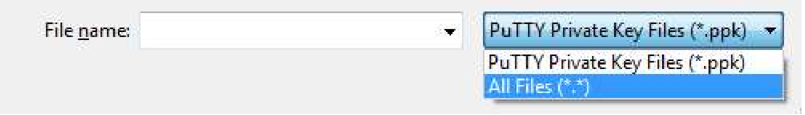


Parameters

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

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.


File name:
PuTTY Private Key Files (*.ppk)
PuTTY Private Key Files (*.ppk)
All Files (*.*)

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. 579) 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:

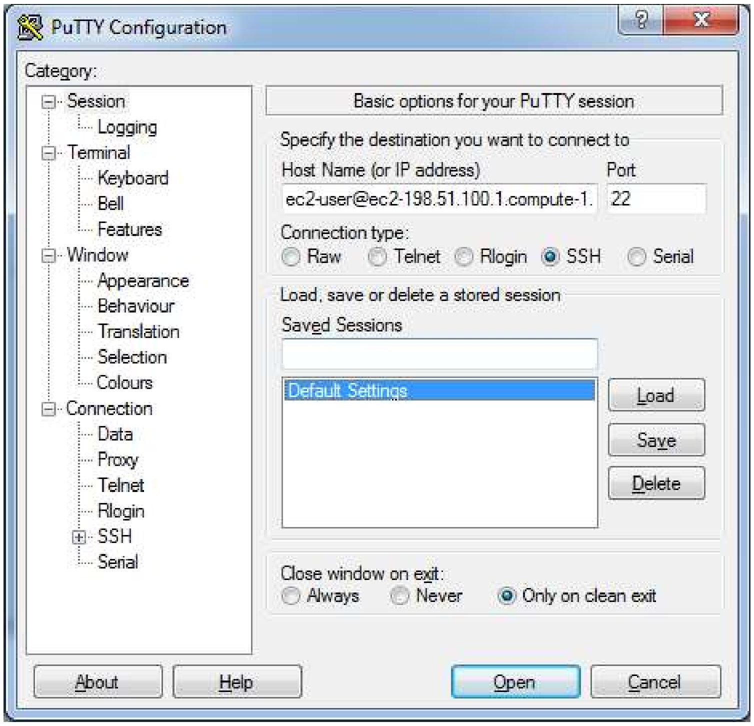
   a. In the **Host Name** box, do one of the following:

- (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. 563).

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

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



Host Name (or IP address): ec2-user@ec2-198.51.100.1.compute-1.
Port: 22
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial
Saved Sessions: Default Settings
Close window on exit: ○ Always ○ Never ● Only on clean exit

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. 565). 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.

   Note
   If you specified a passphrase when you converted your private key to PuTTY's format, you must provide that passphrase when you log in to the instance.

If you receive an error while attempting to connect to your instance, see Troubleshooting Connecting to Your Instance.

Transferring files to your Linux instance using the PuTTY Secure Copy client

The PuTTY Secure Copy client (PSCP) is a command line tool that you can use to transfer files between your Windows computer and your Linux instance. If you prefer a graphical user interface (GUI), you can use an open source GUI tool named WinSCP. For more information, see Transferring files to your Linux instance using WinSCP (p. 581).

To use PSCP, you need the private key you generated in Convert your private key using PuTTYgen (p. 579). You also need the public DNS name of your Linux instance, or the IPv6 address if your instance has one.

The following example transfers the file `Sample_file.txt` from the C:\ drive on a Windows computer to the `my-instance-user-name` home directory on an Amazon Linux instance. To transfer a file, use one of the following commands.

- (Public DNS) To transfer a file using your instance's public DNS name, enter the following command.

```
pscp -i C:\path\my-key-pair.ppk C:\path\Sample_file.txt my-instance-user-name@my-
instance-public-dns-name:/home/my-instance-user-name/Sample_file.txt
```

- (IPv6) Alternatively, if your instance has an IPv6 address, to transfer a file using your instance's IPv6 address, enter the following command. The IPv6 address must be enclosed in square brackets (`[ ]`).

```
pscp -i C:\path\my-key-pair.ppk C:\path\Sample_file.txt my-instance-user-name@[my-
instance-IPv6-address]:/home/my-instance-user-name/Sample_file.txt
```

Transferring files to your Linux instance using WinSCP

WinSCP is a GUI-based file manager for Windows that allows you to upload and transfer files to a remote computer using the SFTP, SCP, FTP, and FTPS protocols. WinSCP allows you to drag and drop files from your Windows computer to your Linux instance or synchronize entire directory structures between the two systems.

To use WinSCP, you need the private key that you generated in Convert your private key using PuTTYgen (p. 579). You also need the public DNS name of your Linux instance.

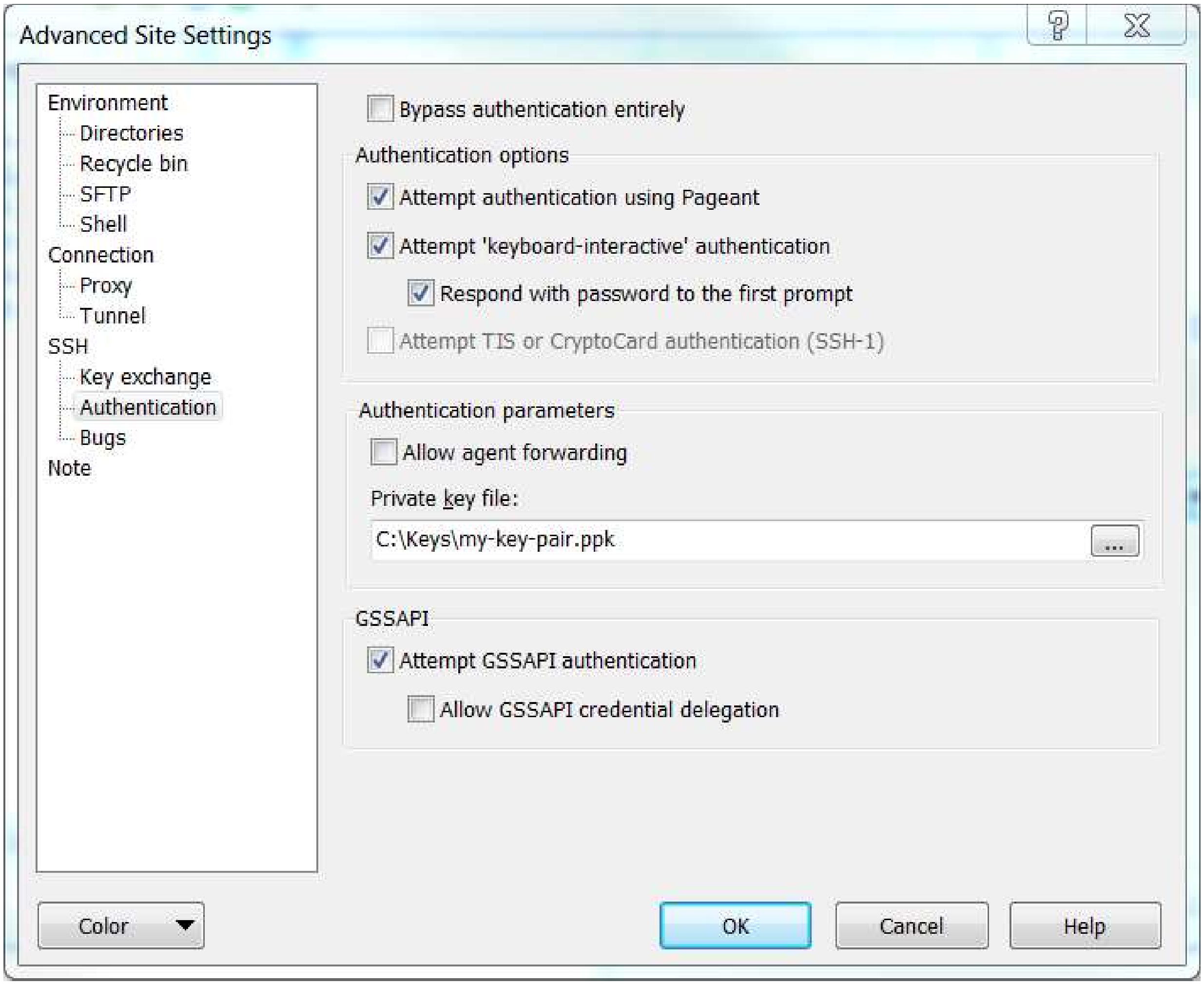
1. Download and install WinSCP from http://winscp.net/eng/download.php. For most users, the default installation options are OK.
2. Start WinSCP.
3. At the **WinSCP login** screen, for **Host name**, enter one of the following:
   - (Public DNS or IPv4 address) To log in using your instance's public DNS name or public IPv4 address, enter the public DNS name or public IPv4 address for your instance.
   - (IPv6) Alternatively, if your instance has an IPv6 address, to log in using your instance's IPv6 address, enter the IPv6 address for your instance.

4. For **User name**, enter the default user name for your AMI.

   - For Amazon Linux 2 or the Amazon Linux AMI, the user name is `ec2-user`.
   - For a CentOS AMI, the user name is `centos`.
   - For a Debian AMI, the user name is `admin`.
   - For a Fedora AMI, the user name is `ec2-user` or `fedora`.
   - For a RHEL AMI, the user name is `ec2-user` or `root`.
   - For a SUSE AMI, the user name is `ec2-user` or `root`.
   - For an Ubuntu AMI, the user name is `ubuntu`.
   - Otherwise, if `ec2-user` and `root` don't work, check with the AMI provider.

5. Specify the private key for your instance. For **Private key**, enter the path to your private key, or choose the "**...**" button to browse for the file. To open the advanced site settings, for newer versions of WinSCP, choose **Advanced**. To find the **Private key file** setting, under **SSH**, choose **Authentication**.

   Here is a screenshot from WinSCP version 5.9.4:



☐ Bypass authentication entirely

Authentication options

☑ Attempt authentication using Pageant

☑ Attempt 'keyboard-interactive' authentication

☑ Respond with password to the first prompt

☐ Attempt TIS or CryptoCard authentication (SSH-1)

Authentication parameters

☐ Allow agent forwarding

Private key file:

C:\Keys\my-key-pair.ppk ...

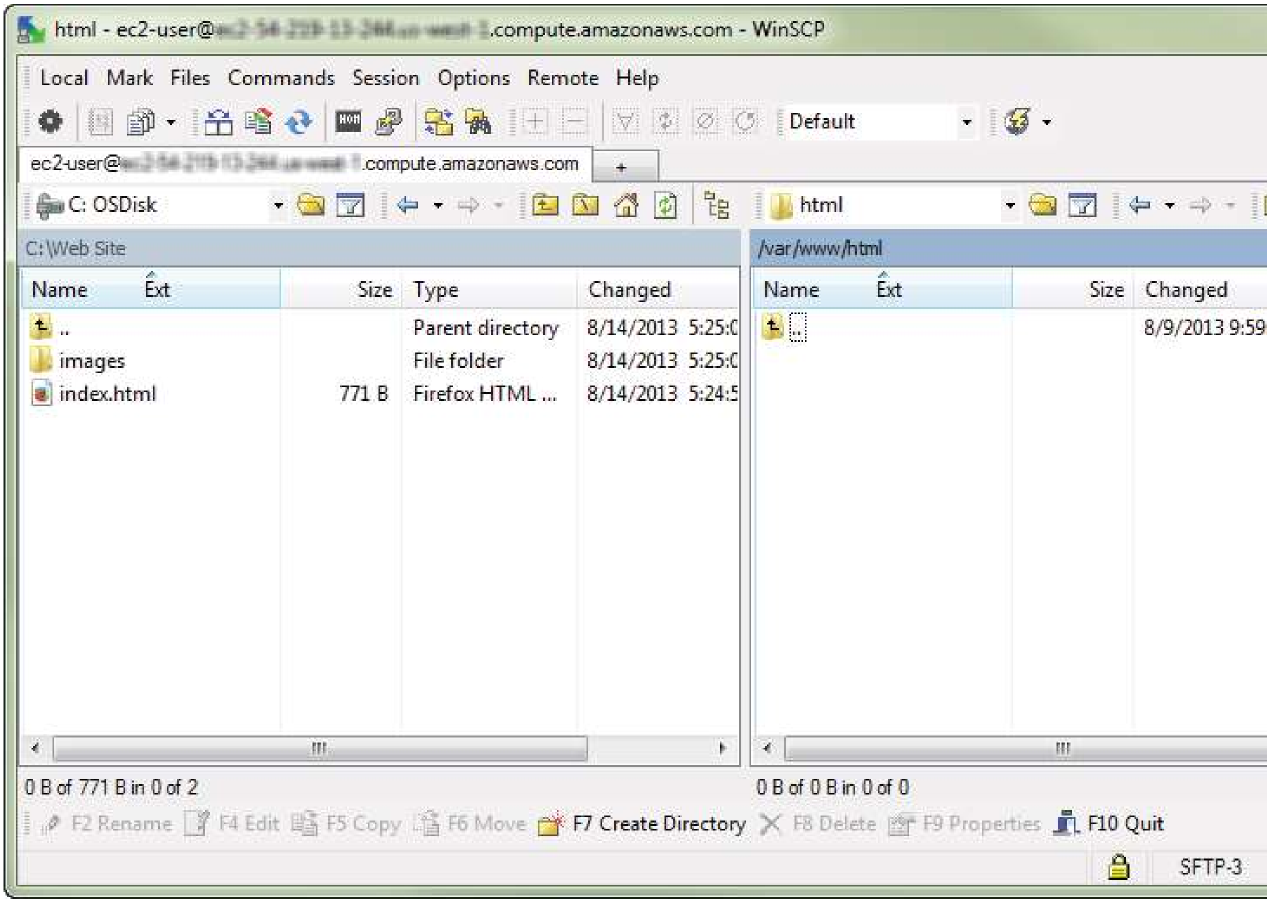
GSSAPI

☑ Attempt GSSAPI authentication

☐ Allow GSSAPI credential delegation

   WinSCP requires a PuTTY private key file (`.ppk`). You can convert a `.pem` security key file to the `.ppk` format using PuTTYgen. For more information, see Convert your private key using PuTTYgen (p. 579).

6. (Optional) In the left panel, choose **Directories**. For **Remote directory**, enter the path for the directory to which to add files. To open the advanced site settings for newer versions of WinSCP, choose **Advanced**. To find the **Remote directory** setting, under **Environment**, choose **Directories**.
7. Choose **Login**. To add the host fingerprint to the host cache, choose **Yes**.



html - ec2-user@[redacted].compute.amazonaws.com - WinSCP

C:\Web Site

Name	Ext	Size	Type	Changed
..			Parent directory	8/14/2013 5:25:(
images			File folder	8/14/2013 5:25:(
index.html		771 B	Firefox HTML ...	8/14/2013 5:24:5

/var/www/html

Name	Ext	Size	Changed
..			8/9/2013 9:59

0 B of 771 B in 0 of 2

0 B of 0 B in 0 of 0

8. After the connection is established, in the connection window your Linux instance is on the right and your local machine is on the left. You can drag and drop files directly into the remote file system from your local machine. For more information on WinSCP, see the project documentation at http://winscp.net/eng/docs/start.

   If you receive a "Cannot execute SCP to start transfer" error, you must first install **scp** on your Linux instance. For some operating systems, this is located in the `openssh-clients` package. For Amazon Linux variants, such as the Amazon ECS-optimized AMI, use the following command to install **scp**.

```
[ec2-user ~]$ sudo yum install -y openssh-clients
```

Connecting to your Linux instance from Windows using Windows Subsystem for Linux

After you launch your instance, you can connect to it and use it the way that you'd use a computer sitting in front of you.

The following instructions explain how to connect to your instance using a Linux distribution on the Windows Subsystem for Linux (WSL). WSL is a free download and enables you to run native Linux