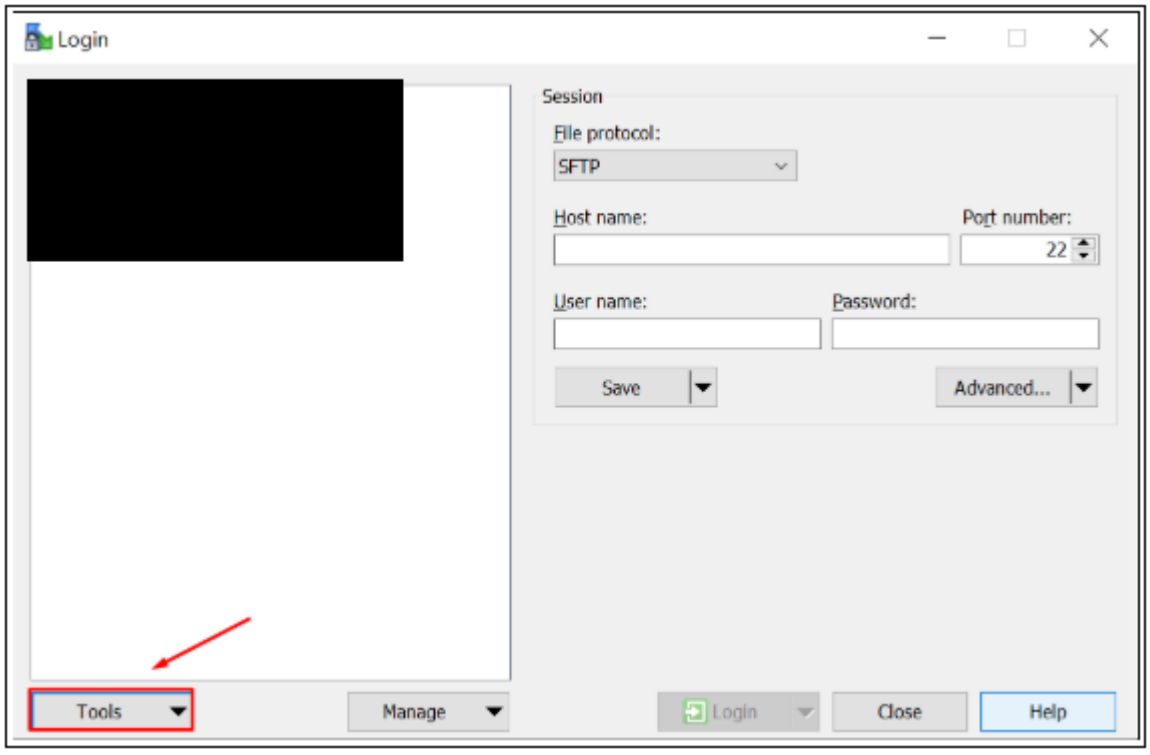
Setting Up SFTP and Creating SSH Keys

This document will walk you through the process of creating public and private key pairs. To Navigate to operating system specific instructions for creating SSH keys, please click one of the links below.

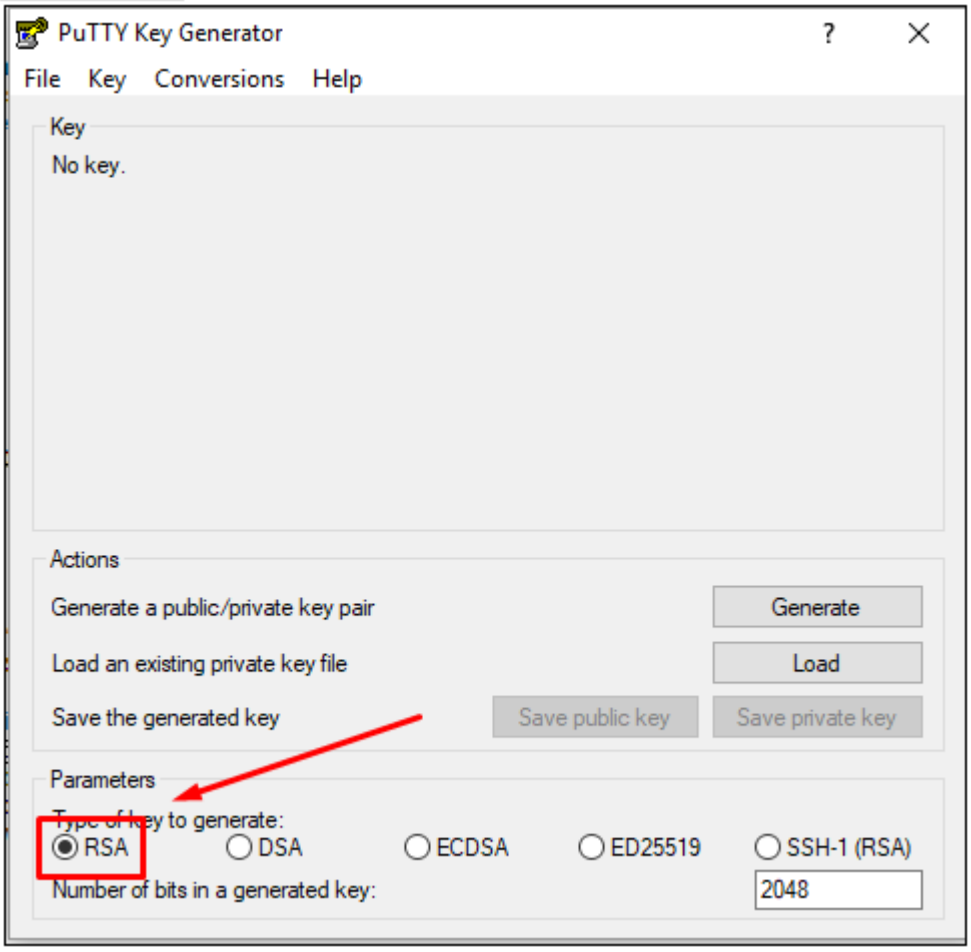
- Creating SSH keys in Windows
- Creating SSH Keys on a Mac

Creating SSH keys in Windows

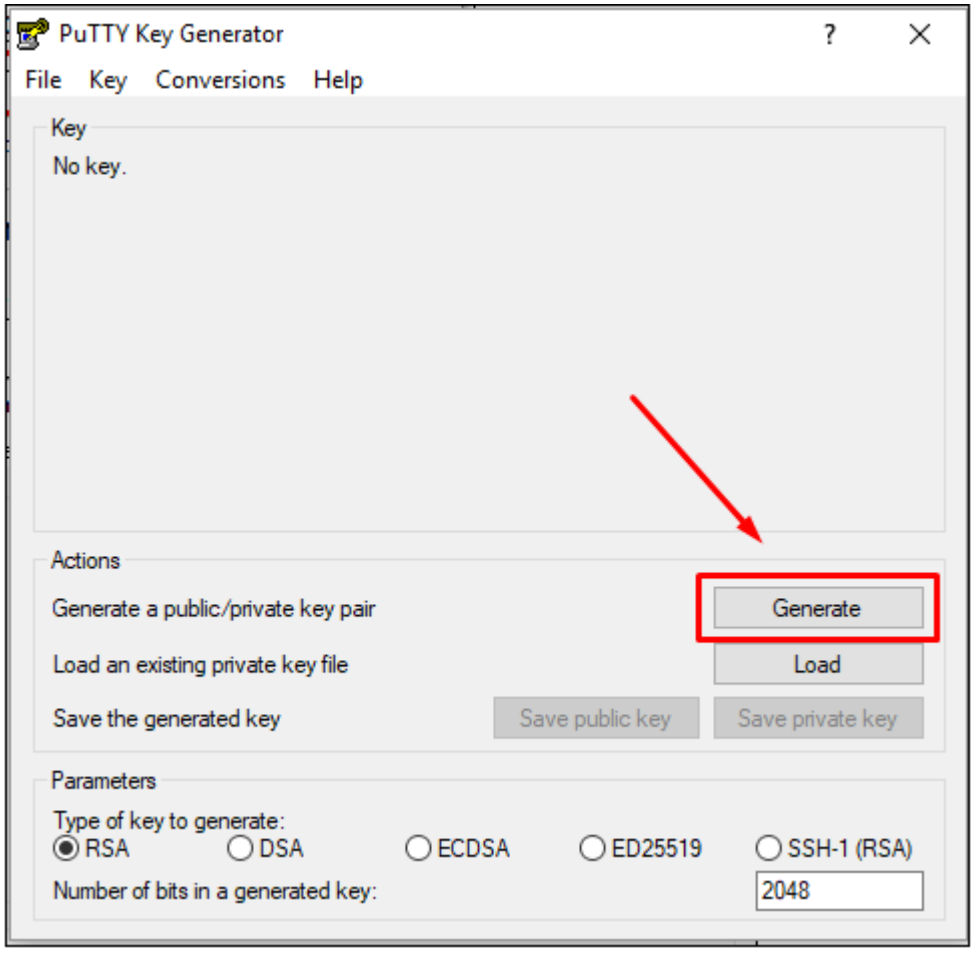
1. Download and run PuTTYGEN. PuTTYGEN is included with WinSCP, but if you're not using WinSCP, you can download a standalone version.
    a. To run PuTTYGEN from WinSCP, click the Tools dropdown box and select Run PuTTYgen.



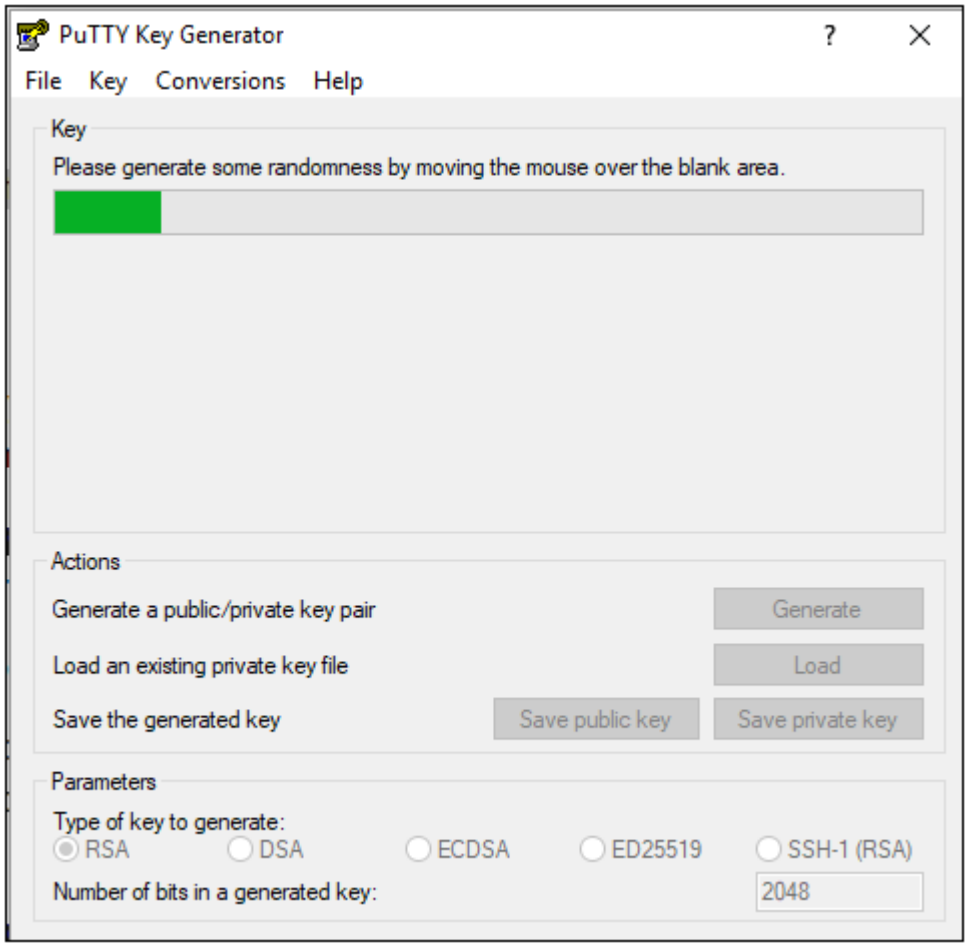
2. Select **RSA**.


PuTTY Key Generator
File Key Conversions Help
Key
No key.
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA
DSA
ECDSA
ED25519
SSH-1 (RSA)
Number of bits in a generated key:
2048

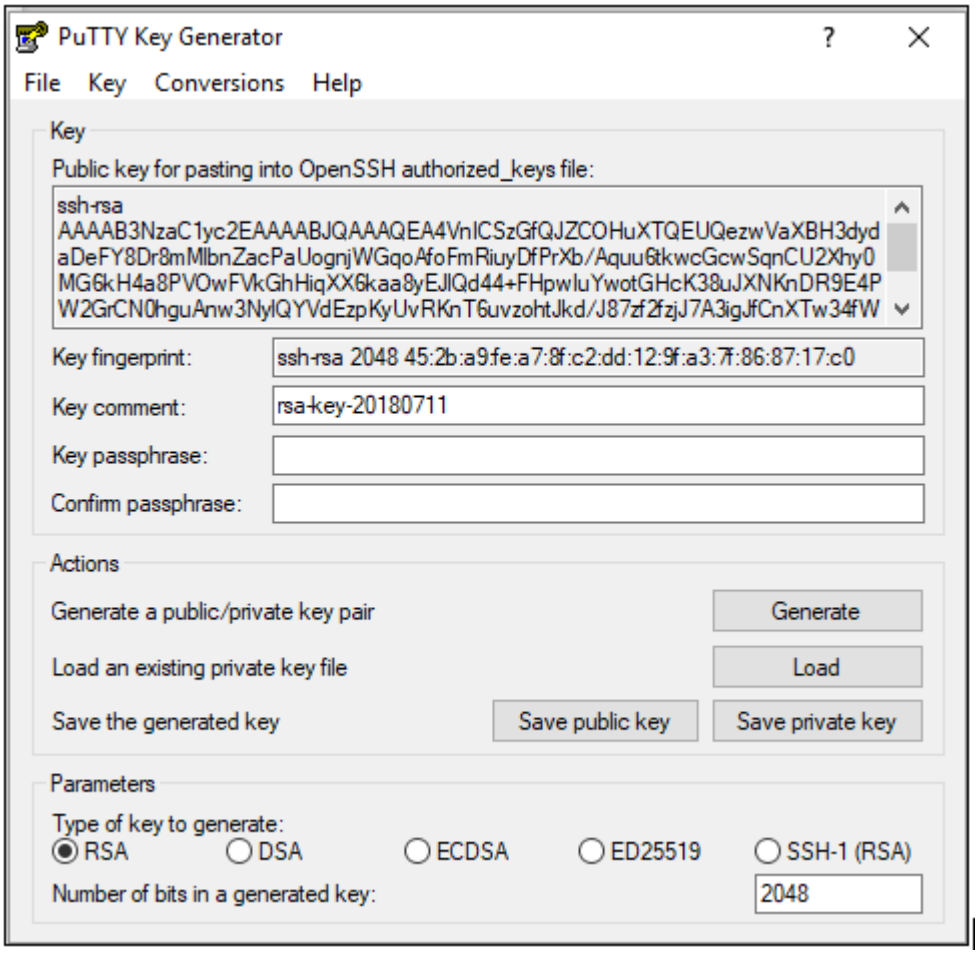
3. Click the **Generate** button.



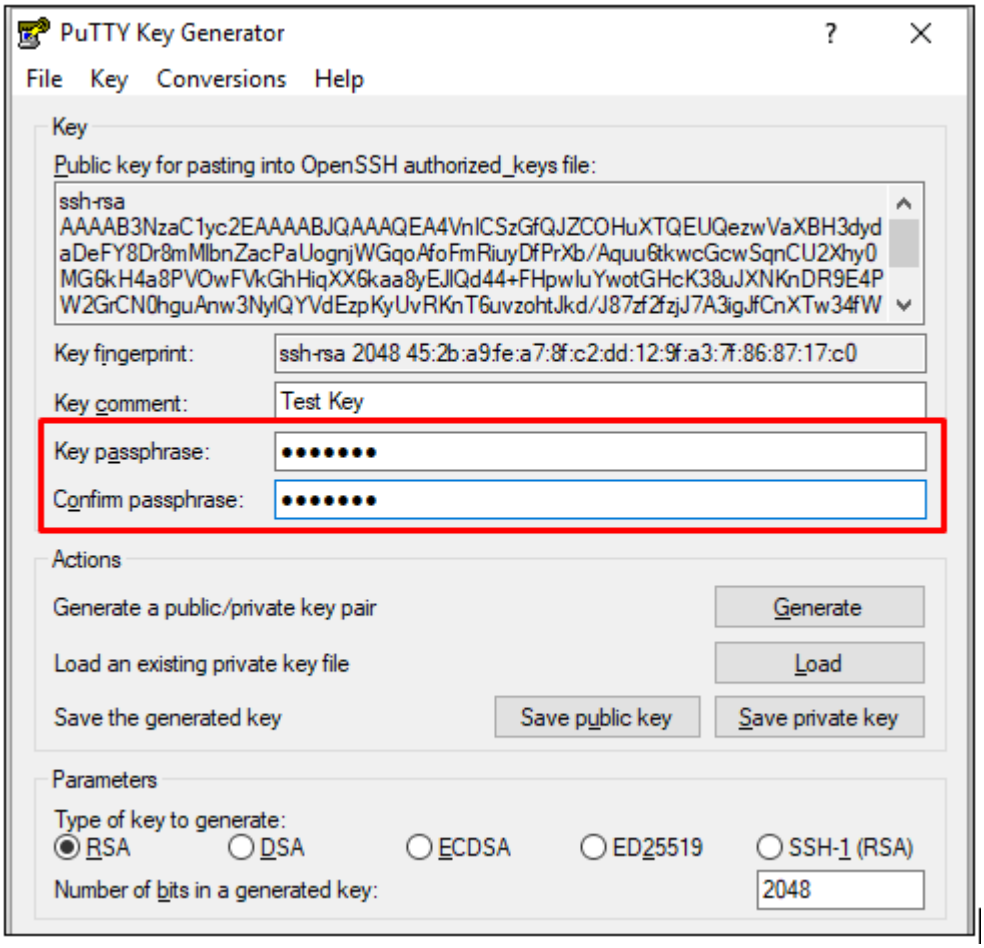
4. Move your mouse pointer around in the blank area of the **Key** section, until the progress bar is full.



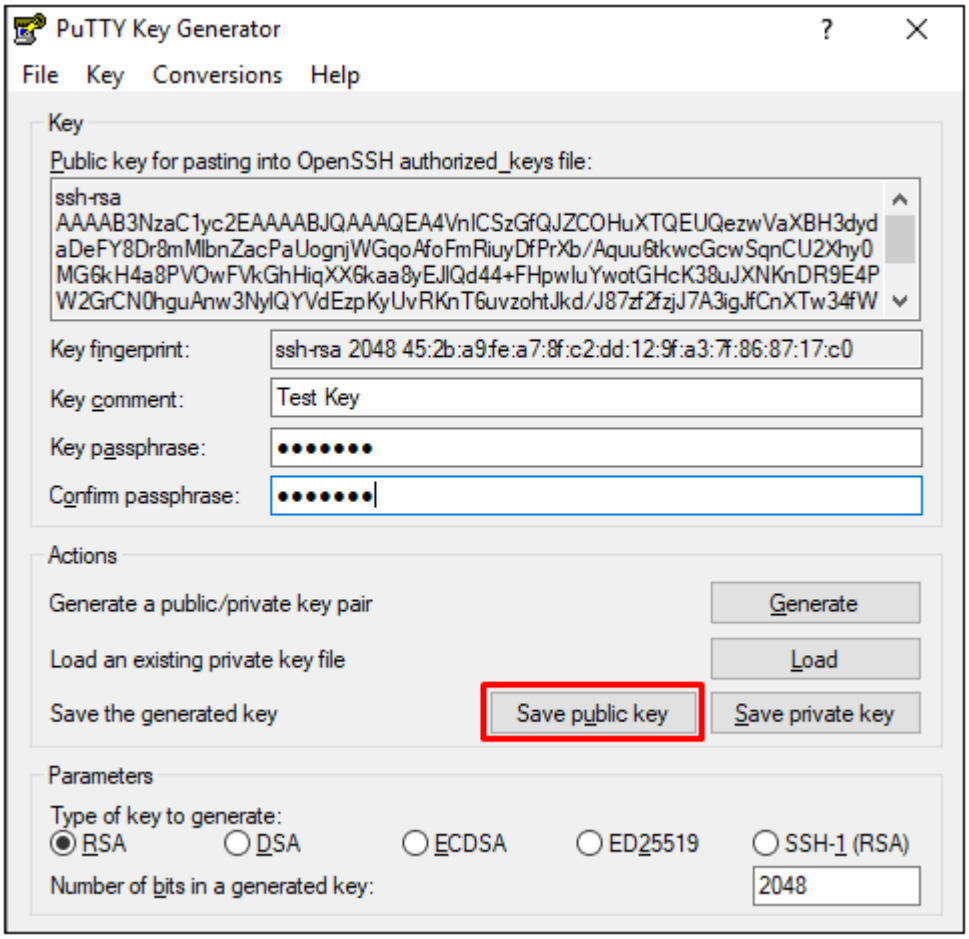
5. Once the progress bar fills, the key is generated and displayed.



6. You can enter a password into the **Key Passphrase** and **Confirm Passphrase** boxes for added security but it is not required. You will have to enter this password whenever you log into the SFTP server.

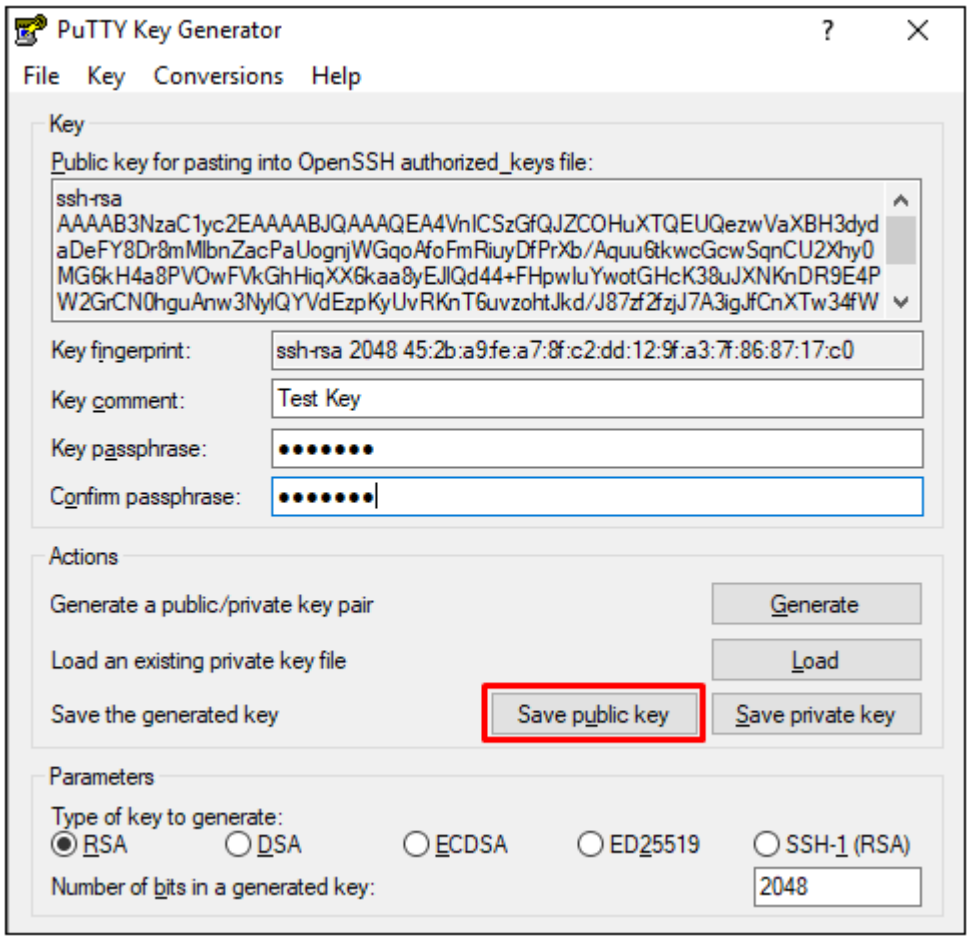


7. Click the **Save public key** button and name your file. You can use any name you want, but you will want to use a descriptive name like “Conversica Public Key.”

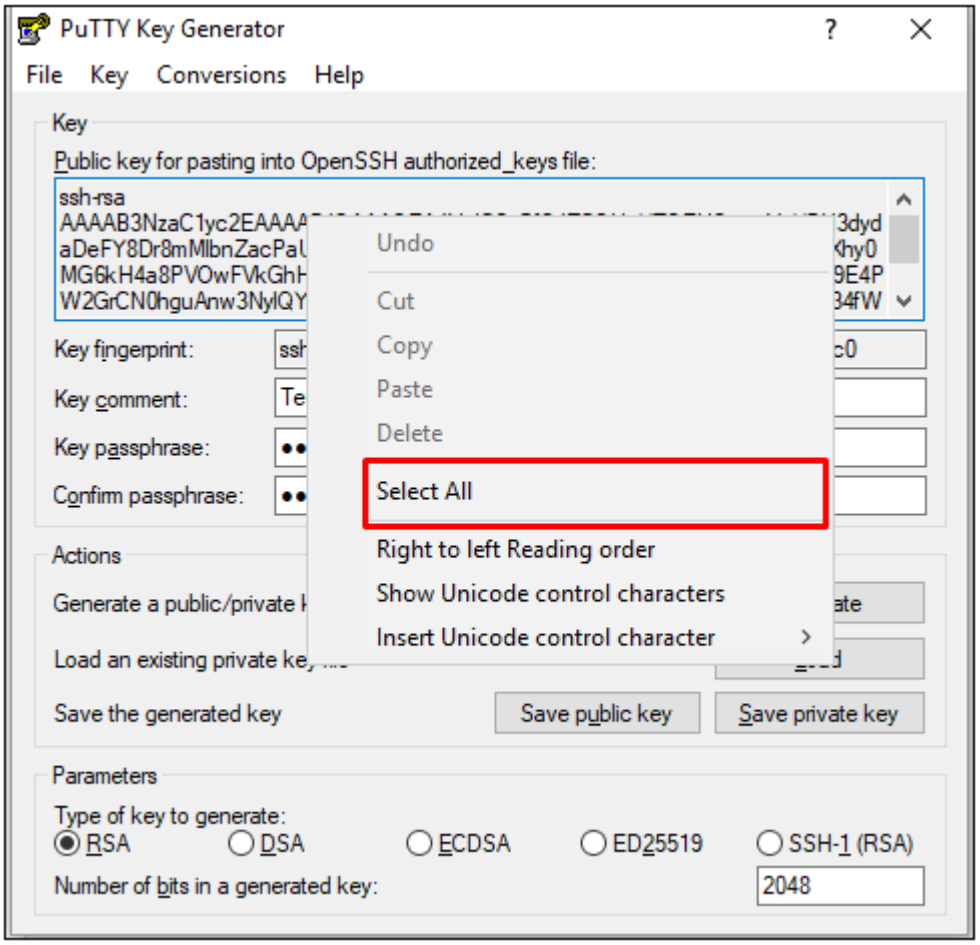


8. Click the **Save private key** button and choose a file name. Make sure this private key is stored somewhere safe and it will not get lost. If something happens to this file, it will result in loss of access until a new public

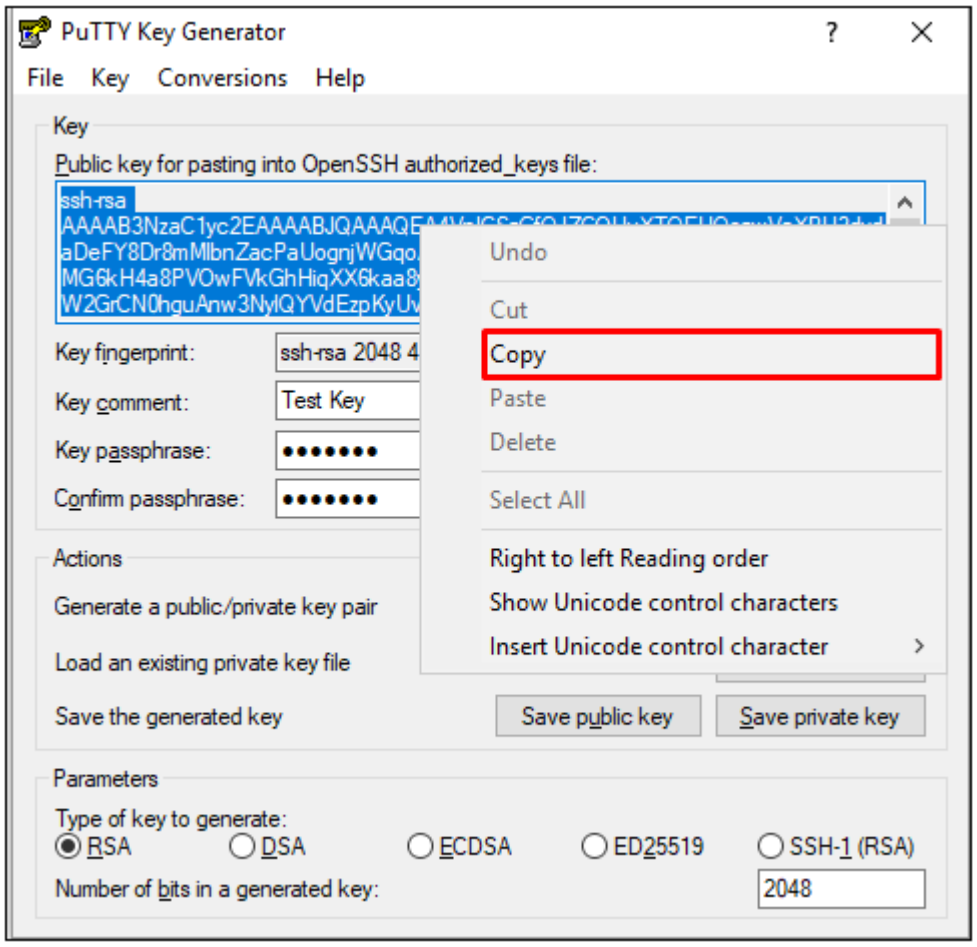
and private key pair can be made and the Conversica system can be reconfigured for the new credentials.



9. Right-click in the text field labeled Public **key for pasting into OpenSSH authorized_keys file** and choose **Select All**.



10. Right-click again once the text is highlighted in the same text field and choose **Copy**.

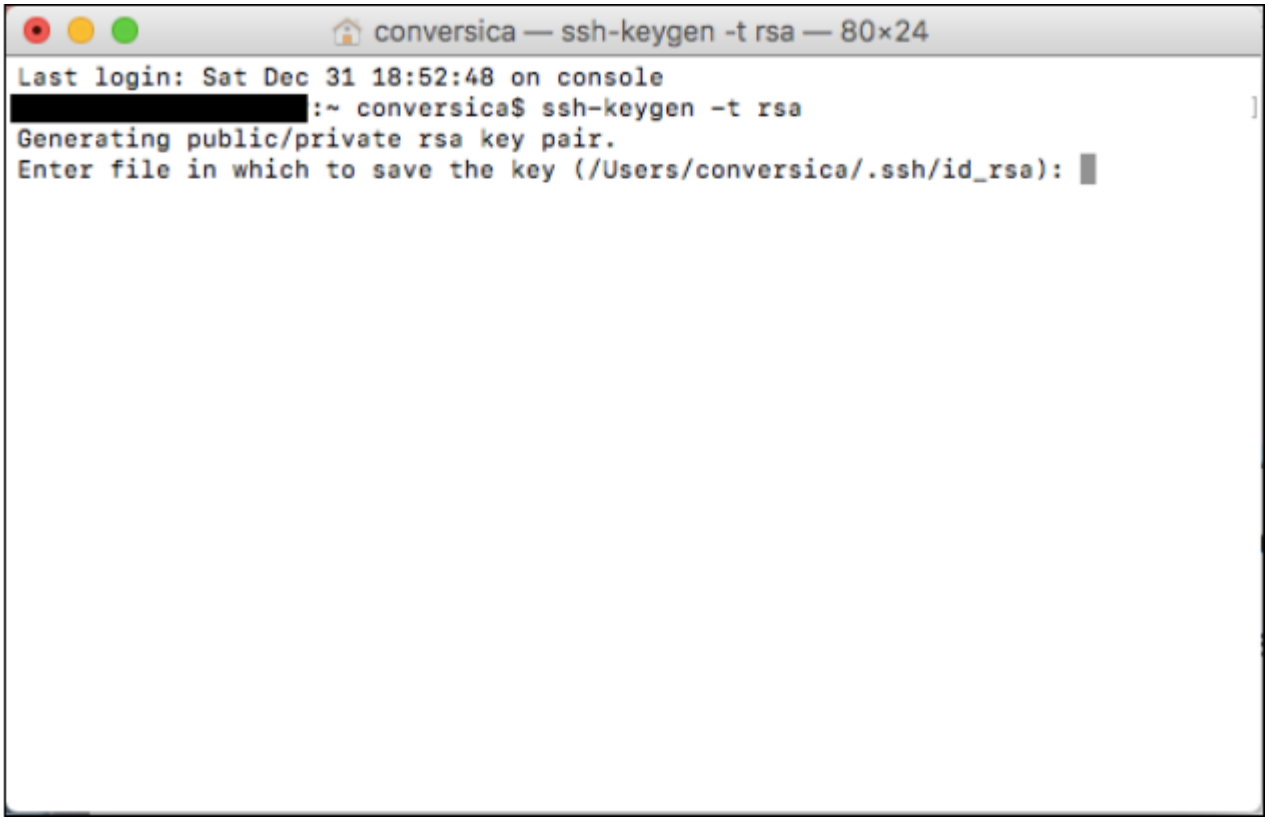


11. Send the copied value to your TAM. The key should all be on one line and begin with "ssh-rsa AAAA ...."

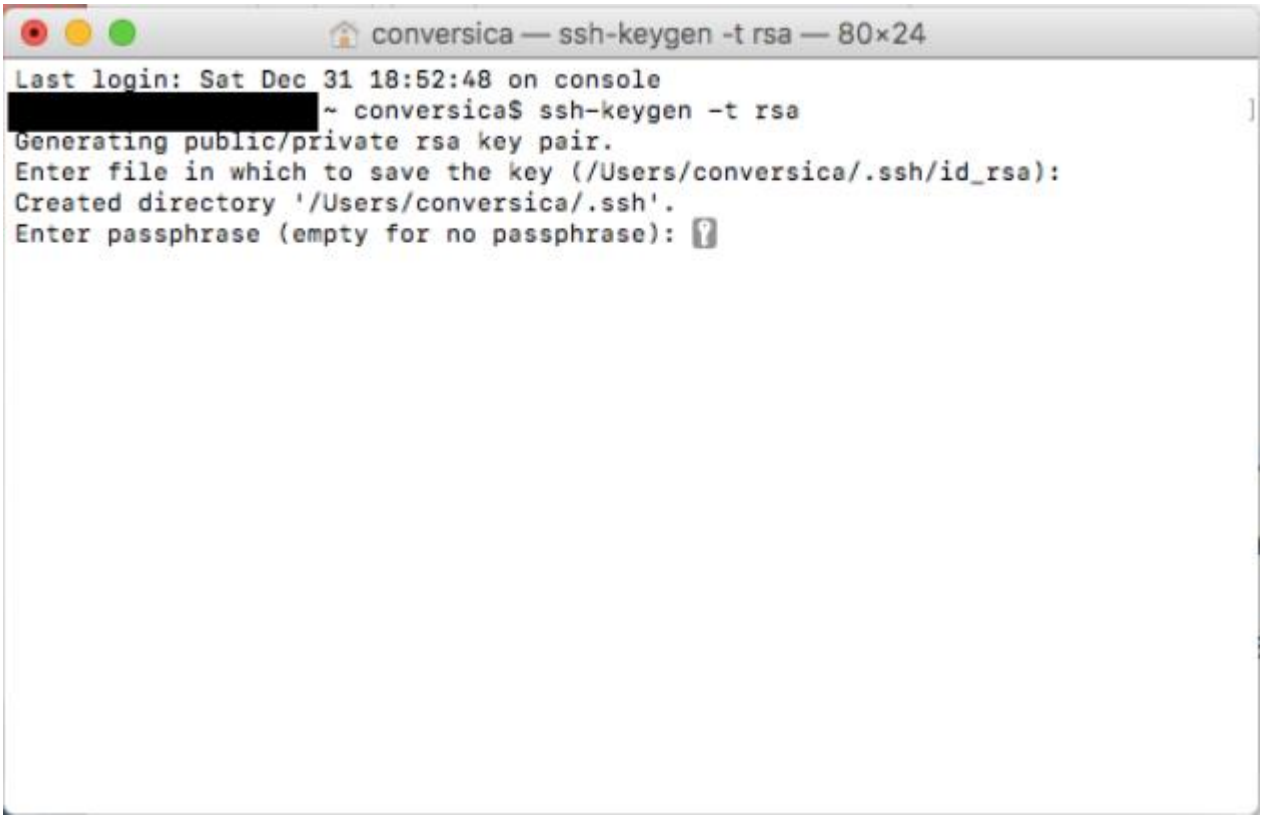
Creating SSH Keys on a Mac

1. Select **Launchpad** and type “terminal” and then click on the terminal icon.

2. Type “ssh-keygen -t rsa” without the quotes.

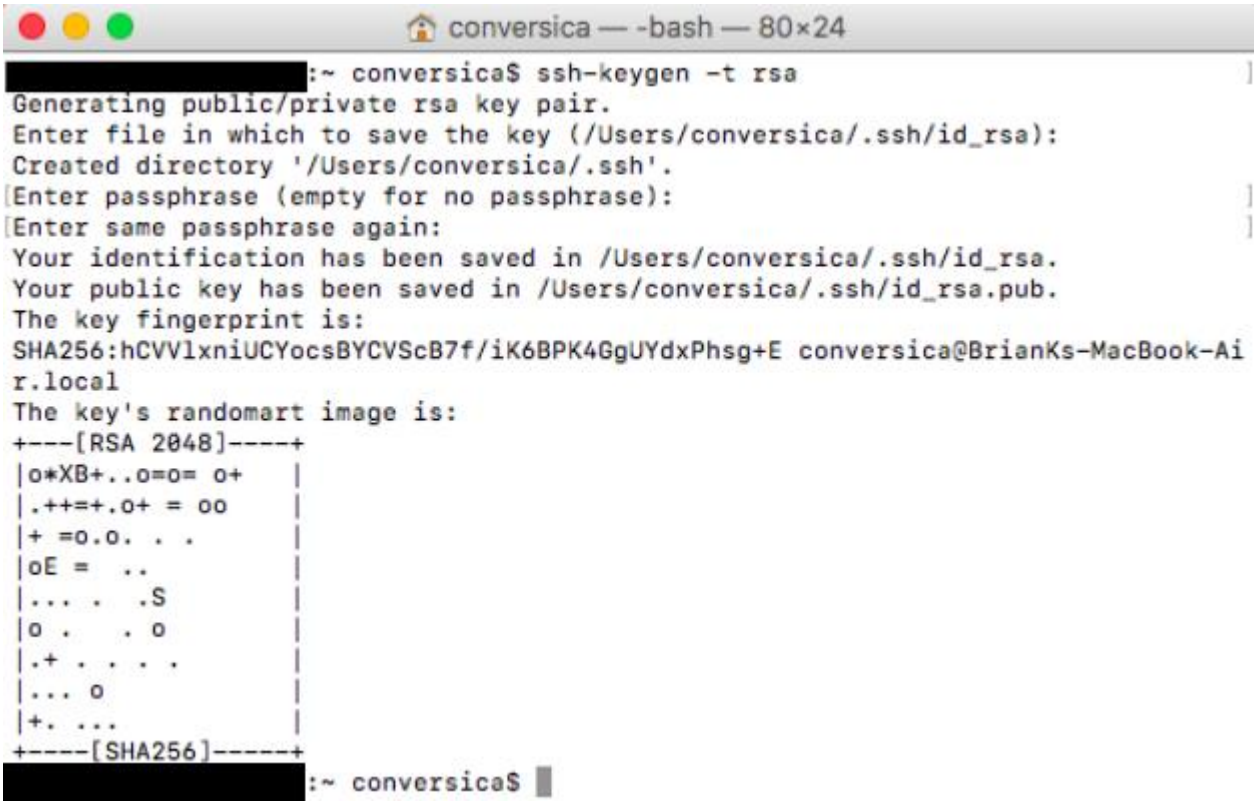


3. You will be prompted for a location to save the key files. If you just press Enter it will save in the default location. The rest of these instructions are written as though you saved to the default location.

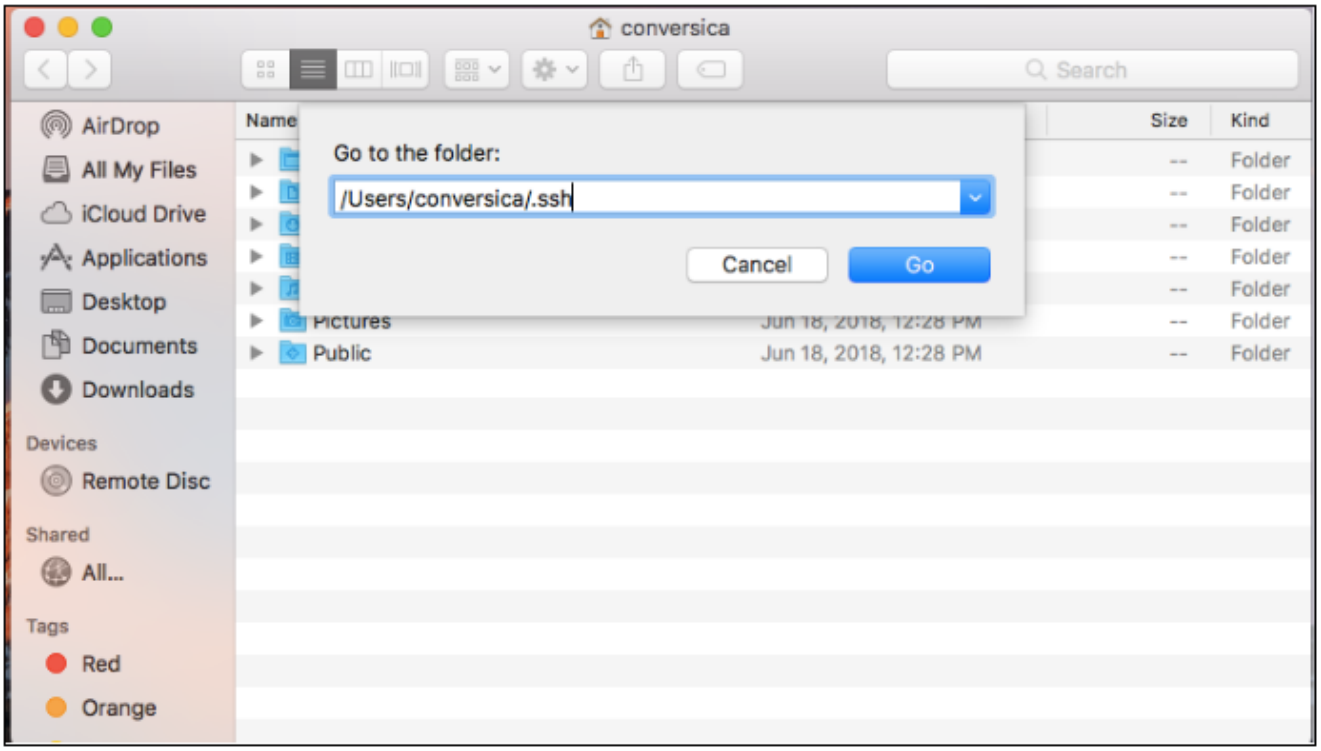


4. You will be prompted for a passphrase. You can enter one or leave it empty. If you enter a password, you will need to enter it twice and the passphrase will need to be entered every time you log into the SFTP directory.

5. Terminal will display a message giving the location of the new files and it will provide a key fingerprint and random art. You do not need the fingerprint or random art.



6. **Press Command + Shift + G** and enter the location that terminal says the file was stored to go to the location where the key file was saved.



7. Copy the .pub file to an email and send it to your TAM.

You are now ready to log into your directory. Please contact your TAM for the next steps.