

Configure SSH Keys for GitHub on Windows

In these instructions, you will configure your ssh keys for Github on Windows. This is necessary if you change your home directory to be on the Windows subsystem (as in, if you run “cd ~”, and “pwd”, the output starts with “/mnt/c/Users/...”

To fix permission issues with we will create your ssh keys on the original Linux subsystem and tell ssh to on the Linux subsystem, rather than your home directory (which is now on the Windows subsystem)

Remove any pre-existing .ssh folder in your Windows home directory:

```
cd ~
rm -rf .ssh
```

Go to to your Linux home directory, and create the .ssh folder:

```
cd /home/<username>/
mkdir .ssh
pwd
```

Generate the key:

```
ssh-keygen
```

ssh-keygen will ask where to create your id_rsa file. Enter what is written below:

```
/home/<username>/.ssh/id_rsa
```

```
Enter #No passphrase
```

```
Enter #No passphrase
```

```
sliakat@DESKTOP-UAA2PC0:/home/sliakat$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/mnt/c/Users/sl/.ssh/id_rsa): /home/sliakat/.ssh/id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/sliakat/.ssh/id_rsa
Your public key has been saved in /home/sliakat/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:xUPKjojTBRctDrayz7SCpBkNudeN14cn4z9XcTJJWpQ sliakat@DESKTOP-UAA2PC0
The key's randomart image is:
+---[RSA 3072]---+
|  . oo . . . |
|  oo...+   E |
|  . . +..O +  + |
| O .O.O.O . . = .|
| +O+oo..S.    = |
| O.+ + O = O  . |
| O= + O . =   . |
| + . +   . . . |
|  .   ..O      |
+---[SHA256]-----+
```

Once your id_rsa and id_rsa.pub are generated, run the following commands:

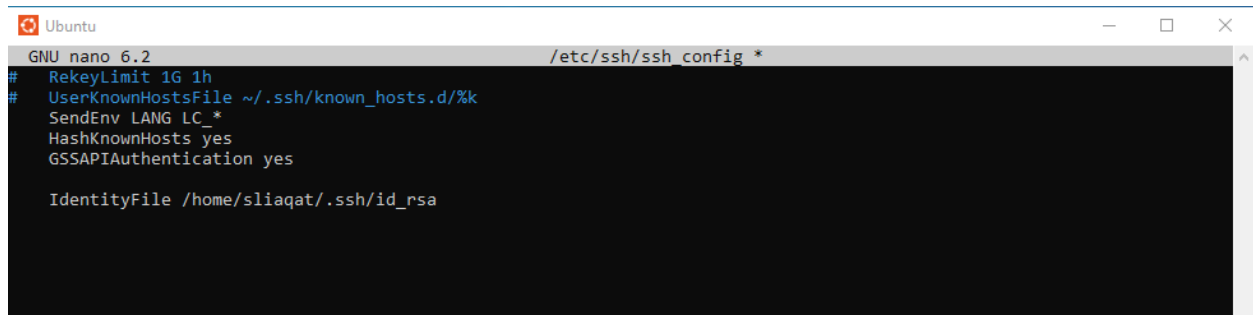
```
chmod 600 /home/<username>/.ssh/id_rsa.pub
chmod 600 /home/<username>/.ssh/id_rsa
```

Next we will tell SSH about this id_rsa file:

```
sudo nano /etc/ssh/ssh_config
```

Then go to the end of the file and paste the following line (with four spaces in the front so it's aligned with the previous line, see image below):

```
IdentityFile /home/<username>/.ssh/id_rsa
```



Then to exit, press:

Ctrl-x - initiate exit

Y - save file

Enter - set name

Then run:

```
sudo service ssh restart # (It might output "no hostkeys available, exiting". This is fine)
```

```
cat /home/<username>/.ssh/id_rsa.pub
```

Then copy the contents of the id_rsa.pub (make sure it's the id_rsa.pub file not id_rsa) file, and add them to GitHub.

1. Log into www.github.com
2. Click your avatar on the top right, and select settings.
3. On the left, open the tab that says "SSH and GPG keys"
4. Click the "New SSH key" button
5. Give it any name, and in the box, paste your id_rsa.pub file contents.
6. Click the "Add SSH key" button

After doing all this, the following command should work (you may need to type yes if it prompts you with a question):

```
ssh -T git@github.com
```

The output should say you're successfully authenticated:

```
sliqat@DESKTOP-UAA2PCO:/home/sliaqat$ ssh -T git@github.com
The authenticity of host 'github.com (140.82.112.3)' can't be established.
ED25519 key fingerprint is SHA256:+DiY3wvvV6TuJJhbpZisF/zLDA0zPMSvHdkr4UvCOQU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'github.com' (ED25519) to the list of known hosts.
Hi saliaqat! You've successfully authenticated, but GitHub does not provide shell access.
```