## **Step 1 — Creating SSH Keys**

The first step to configure SSH key authentication to your server is to generate an SSH key pair on your local computer.

To do this, we can use a special utility called ssh-keygen, which is included with the standard OpenSSH suite of tools. By default, this will create a 3072 bit RSA key pair.

On your local computer, generate a SSH key pair by typing:

“ssh -keygen”

Accept all the prompts by pressing enter till you get the below output:

Output

Your identification has been saved in /home/username/.ssh/id\_rsa.

Your public key has been saved in /home/username/.ssh/id\_rsa.pub.

The key fingerprint is:

SHA256:CAjsV9M/tt5skazroTc1ZRGCBz+kGtYUIPhRvvZJYBs username@hostname

The key's randomart image is:

+---[RSA 3072]----+

|o ..oo.++o .. |

| o o +o.o.+... |

|. . + oE.o.o . |

| . . oo.B+ .o |

| . .=S.+ + |

| . o..\* |

| .+= o |

| .=.+ |

| .oo+ |

+----[SHA256]-----+

You now have a public and private key that you can use to authenticate. The next step is to place the public key on your server so that you can use SSH key authentication to log in.

### 

### **STEP-2 Copying Your Public Key Manually**

If you do not have password-based SSH access to your server available, you will have to do the above process manually.

The content of your id\_rsa.pub file will have to be added to a file at ~/.ssh/authorized\_keys on your remote machine somehow.

To display the content of your id\_rsa.pub key, type this into your local computer:

cat ~/.ssh/id\_rsa.pub

You will see the key’s content, which may look something like this:

~/.ssh/id\_rsa.pub

ssh-rsa  username@hostname

Login to your remote machine using the pem key you have available.

Open the authorized key file on the remote server using the below command

sudo nano ~/.ssh/authorized\_keys

Paste the key of your local machine into the server’s authorized\_key file, press ctrl+o, then Enter, press ctrl+x to exit the file.

Now login to the server using the below command.

ssh username@ip-address