**Setup SSH Passwordless Login**

To set up a passwordless SSH login in Linux all you need to do is to generate a public authentication key and append it to the remote hosts ~/.ssh/authorized\_keys file.

**First Check for existing SSH key pair.**

ls -al ~/.ssh/id\_\*.pub

If Key exist you can use existing one

or

**Generate a new SSH key pair**

ssh-keygen -t rsa -b 4096 -C your\_email@domain.com

**To be sure that the SSH keys are generated you can list your new private and public keys with:**

ls ~/.ssh/id\_\*

**Ouput Should be**

/home/yourusername/.ssh/id\_rsa /home/yourusername/.ssh/id\_rsa.pub

**Copy the public key to Remote server**

ssh-copy-id remote\_username@server\_ip\_address

**Login to your server using SSH keys**

ssh remote\_username@server\_ip\_address

**Disabling SSH Password Authentication**

ssh sudo\_user@server\_ip\_address

**Open the SSH configuration file /etc/ssh/sshd\_config, search for the following directives and modify as it follows:**

PasswordAuthentication no

ChallengeResponseAuthentication no

UsePAM no

Once you are done save the file and restart the SSH service.

On Ubuntu or Debian servers, run the following command:

sudo systemctl restart ssh

On CentOS or Fedora servers, run the following command:

sudo systemctl restart sshd