# Linux Lab-Giving SSH Access to Users

Create a user with directory location and check that user directory is created.

```
root@ip-172-31-83-123:~# useradd -m -d /home/aravind aravind
root@ip-172-31-83-123:~# passwd -d aravind
passwd: password expiry information changed.
root@ip-172-31-83-123:~# cd /home/
root@ip-172-31-83-123:/home# ls -lrt
total 8
drwxr-xr-x 5 ubuntu  ubuntu  4096 May  6 09:17 ubuntu
drwxr-xr-x 2 aravind aravind 4096 May  6 12:03 aravind
root@ip-172-31-83-123:/home#
```

Login as user giving su comand from root and create ssh keygen and .ssh directory will be created.

```
root@ip-172-31-83-123:~/.ssh# su aravind
aravind@ip-172-31-83-123:/root/.ssh$ cd
aravind@ip-172-31-83-123:~$ pwd
/home/aravind
aravind@ip-172-31-83-123:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/aravind/.ssh/id_rsa):
Created directory '/home/aravind/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/aravind/.ssh/id_rsa.
Your public key has been saved in /home/aravind/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:R491PBJ6bvPiCmT3cPsc2AOjq5GAi18gRn09/II2YM4 aravind@ip-172-31-83-123
The key's randomart image is:
+---[RSA 2048]----+
|              .  |
| .   o    . o    |
| . + . +  o + +  |
|. + o.. o. * o . |
|...E.+..S.= O    |
|.o o. .+.+ * O   |
|. . .    + . = = |
| . .      o o + o|
| .        ..o.. o|
+----[SHA256]-----+
aravind@ip-172-31-83-123:~$
```

Create a new key pair uisng puttygen copy the public key and paste in **authorised_keys** in **/home/user/.ssh/**
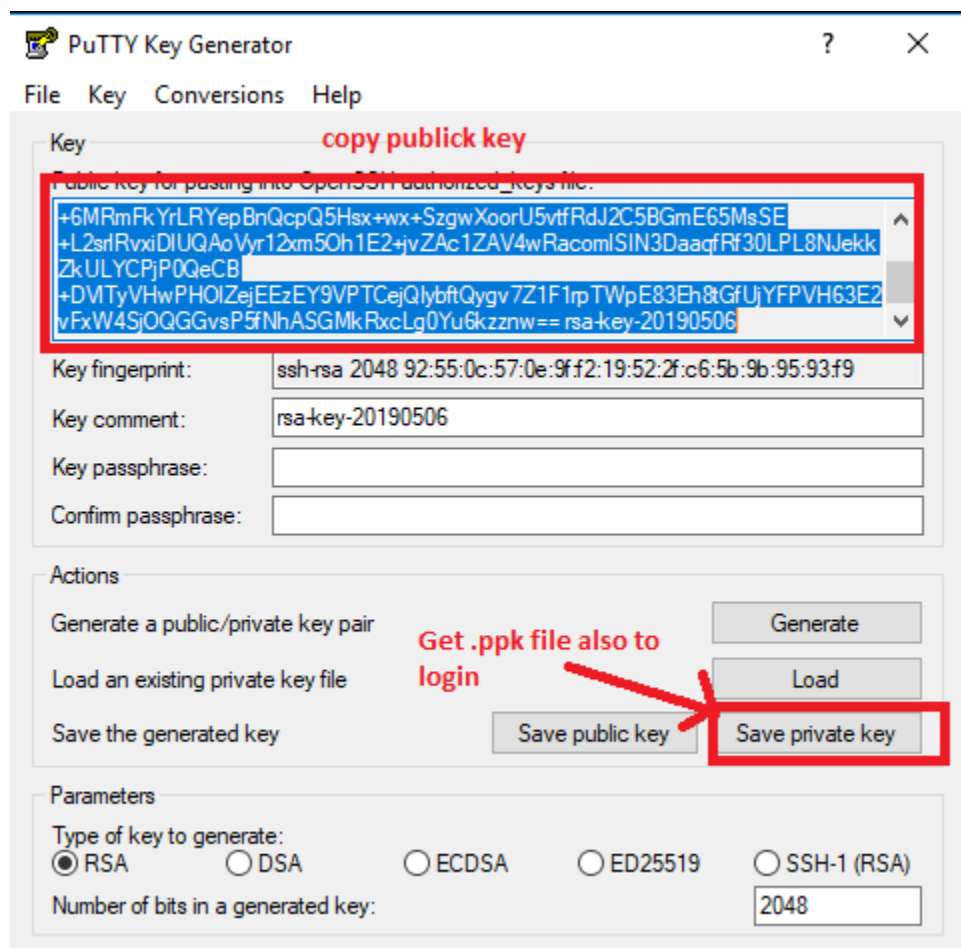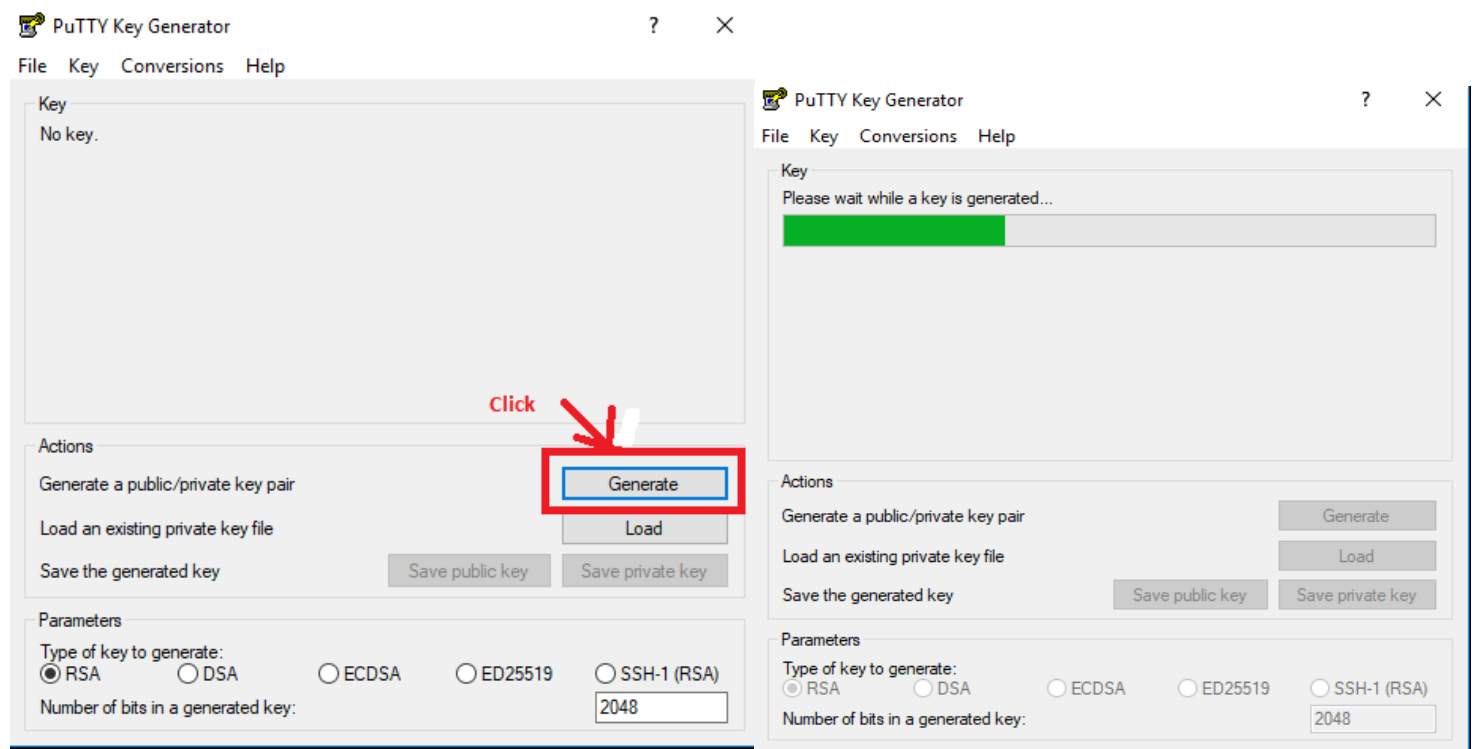
Paste in **authorised_keys (**if not there create it)

```
aravind@ip-172-31-83-123:~$ cd .ssh/
aravind@ip-172-31-83-123:~/.ssh$ vi authorized_keys
aravind@ip-172-31-83-123:~/.ssh$ vi authorized_keys
aravind@ip-172-31-83-123:~/.ssh$ █
```

To give sudo permission (if Required)

Go to /etc

root@ip-172-31-83-123:/etc# chmod 777 sudoers

root@ip-172-31-83-123:/etc# vi sudoers

root@ip-172-31-83-123:/etc# chmod 440 sudoers

Change the full permission for **sudoers** file then add the user name with No Password in the list and save

$USER ALL=(ALL) NOPASSWD: ALL

```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
aravind ALL=(ALL) NOPASSWD: ALL
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
~
~
~
~
~
~
~
~
~
~
~
~
~
:wq█
```

Now you can try from your end

```
login as: aravind
Authenticating with public key "rsa-key-20190506"
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-1075-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud

79 packages can be updated.
40 updates are security updates.

New release '18.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

$ sudo -i
root@ip-172-31-83-123:~#
```