**SSH passwordless multiple login**

**I've already written about howto log in, on your local system, and** [**make passwordless ssh connections**](http://www.cyberciti.biz/tips/ssh-public-key-based-authentication-how-to.html) **using ssh-keygen command. However, you cannot just follow these instructions over and over again, as you will overwrite the previous keys.**

**It is also possible to upload multiple public keys to your remote server, allowing one or more users to log in without a password from different computers.**

**Step # 1: Generate first ssh key**

**Type the following command to generate your first public and private key on a local workstation. Next provide the required input or accept the defaults. Please do not change the filename and directory location.**

**workstation#1 $ ssh-keygen -t rsa**

**Finally, copy your public key to your remote server using scp**

**workstation#1 $ scp ~/.ssh/id\_rsa.pub user@remote.server.com:.ssh/authorized\_keys**

**Step # 2: Generate next/multiple ssh key**

**a) Login to 2nd workstation**

**b) Download original the authorized\_keys file from remote server using scp:**

**workstation#2 $ scp user@remote.server.com:.ssh/authorized\_keys ~/.ssh**

**c) Now create the new pub/private key:**

**workstation#2 $ ssh-keygen -t rsa**

**d) Now you have new public key. APPEND this key to the downloaded authorized\_keys file using cat command:**

**workstation#2 $ cat ~/.ssh/id\_rsa.pub >> ~/.ssh/authorized\_keys**

**e) Finally upload authorized\_keys to remote server again:**

**workstation#2 $ scp ~/.ssh/authorized\_keys user@remote.server.com:.ssh/**

**You can repeat step #2 for each user or workstations for remote server.**

**Step #3: Test your setup**

**Now try to login from Workstation #1, #2 and so on to remote server. You should not be asked for a password:**

**workstation#1 $ ssh user@remote.server.com**

**workstation#2 $ ssh user@remote.server.com**

**Updated for accuracy.**