How To Generate & Set Up SSH Keys On Linux

Step 1: Create SSH Key Pair

Step 1: Create SSH Key Pair

Start by logging into the source machine (local server) and creating a **2048-bit RSA key pair** using the command:

```
ssh-keygen -t rsa
```

If you want to tighten up security measures, you can create a **4096-bit key** by adding the -b 4096 flag

```
ssh-keygen -t rsa -b 4096
```

2. After entering the command, you should see the following prompt:

```
Generating public/private rsa key pair.

Enter file in which to save the key (home/your_username
/.ssh/id_rsa):
```

3. To save the file in the suggested directory, press Enter**.**
Alternatively, you can specify another location.

4. Next, the prompt will continue with:

```
Enter passphrase (empty for no passphrase):

Enter same passphrase again:
```

Although creating a passphrase isn't mandatory, it is highly advisable.

5. Finally, the output will end by specifying the following information:

```
Your identification has been saved in home/your_username/.ssh/id_rsa.

Your public key has been saved in home/your_username/.ssh/id_rsa.pub.

The key fingerprint is:

KYg355:gKotTeU5NQ-5m296q55Ji57F8iO6c0K6GUr5:PO1iRk

username@hostname

The key's randomart image is:

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

|       .oo.            |

|        +o+.           |

|      + +.+            |

| o  +          S .     |

|      .    E  .   . =.o|

|    .  +       .   B+@o|

|        +   .     oo*=O|

|   oo            . .+o+|

|                 o=ooo=|
+------ [SHA256] ------+
```

Now you need to add the public key to the remote CentOS server.

2. Copy Public Key to CentOS Server

You can copy the public SSH key on the remote server using several different methods:

- Using ssh-copy-id script
- Using Secure Copy (scp)
- Manually Copying the key

The fastest and easiest method is by utilizing `ssh-copy-id`. If the option is available, we recommend using it. Otherwise, try any of the other two noted.

Copy Public Key Using ssh-copy-id

1.Start by typing the following command, specifying the SSH user account, and the IP address of the remote host:

```
ssh-copy-id username@remote_host
```

If it is the first time your local computer is accessing this specific remote server you will receive the following output:

```
The authenticity of host '104.0.316.1 (104.0.316.1)' ca
n't be established.

ECDSA key fingerprint is KYg355:gKotTeU5NQ-5m296q55Ji57
F8iO6c0K6GUr5:PO1iRk.
Are you sure you want to continue connecting (yes/no)?
yes
```

2. Confirm the connection – type yes **and hit Enter**.
3. Once it locates the `id_rsa.pub key` created on the local machine, it will ask you to provide the password for the remote account. Type in the password and hit **Enter**.

4. Once the connection has been established, it adds the public key on the remote server. This is done by copying the `~/.ssh/id_rsa.pub` file to the remote server's `~/.ssh` directory. You can locate it under the name `authorized_keys`.

5. Lastly, the output tells you the number of keys added, along with clear instructions on what to do next:

```
Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'username@
192.168.0.115'"
and check to make sure that only the key(s) you wanted
were added.
```