



Howto setup SSH keys between machines

by [Daniel Owen](#) on February 13, 2004 (updated February 19,2004)

SSH keys can provide a relief to system administrators. Are you tired of typing in strong passwords over and over again to connect machines you admin? Using SSH keys and ssh-agent allows you to type in a passphrase only once on your workstation. SSH generates a private and a public key. The public key can be put on the machines you wish to communicate with. SSH will then connect to those machines with keys instead of your standard password. Using ssh-agent can automate this by automatically sending your key to the machines you connect to.

Let's get started by creating a pair of keys for your workstation from which you'll be connecting to your various servers.

```
[daniel@linuxone][daniel]# ssh-keygen -t dsa
Generating public/private dsa key pair.
```

ssh-keygen will prompt you for the file where you wish to save your private key. This is the key that will only be on your machine and not given out to others. It can be called id_dsa or also identity. The file should be located in the .ssh directory inside your home directory.

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

Next it will prompt for the passphrase you wish to use. This is basically the password for your key. This is the password ssh-agent will use to authenticate to all your machines that have your public key.

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/daniel/.ssh/id_dsa.
Your public key has been saved in /home/daniel/.ssh/id_dsa.pub.
The key fingerprint is:
XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX daniel@linuxone.
shsu.edu
```

Now if you list the contents of your .ssh directory you should see your private and public key.

```
[daniel@linuxone][.ssh]# ls
id_dsa id_dsa.pub
```

Now that you have generated your keys you need to put your public keys in the authorized keys file on all the machines you wish to connect to using ssh. In this example I will use an example machine called linuxtwo.

```
[daniel@linuxone][daniel]# scp .ssh/id_dsa.pub daniel@linuxtwo:
```

scp will prompt you for the password to the remote machine. After entering that, the public key will be sitting in your home directory on the remote machine.

Connect to the remote machine and cat the contents of the public key to a file called authorized_keys in

your `.ssh` directory of your home directory.

```
[daniel@linuxtwo][daniel]# cat id_dsa.pub >> .ssh/authorized_keys
```

Be sure to use the double ">>" so you do not overwrite any other authorized keys you may have added to the `authorized_keys` file. Remove the `id_dsa.pub` file from your home directory.

```
[daniel@linuxtwo][daniel]# rm -f id_dsa.pub
```

Before you go any further, we need to check some permissions; or SSH may not act correctly. The `.ssh` folder should have permissions of 700, and the `authorized_keys` file should have permissions of 644. SSH will totally ignore the keys if the permissions aren't correct.

```
[daniel@linuxtwo][daniel]# chmod 700 .ssh
```

```
[daniel@linuxtwo][daniel]# chmod 644 .ssh/authorized_keys
```

On the machine you started with, in our example `linuxone`, try to SSH to the remote machine. It should now prompt you to enter your passphrase instead of your password.

To automate the sending of keys with `ssh-agent` see my tip on this [here](#).

-Daniel Owen

Copyright © 2003-2004 FedoraNEWS.ORG. All rights reserved.

FedoraNEWS.ORG is not sponsored by Red Hat, Inc.

[Legal](#) | [License](#) | [Right](#)

Site Manager: [Thomas Chung](#)

WE PROUDLY SUPPORT

