

Passwordless SSH

To set up password-less ssh/scp between two accounts on two different machines :

1. Install SSH on each machine, and in each of the two accounts, run `ssh-keygen` with an empty passphrase :

```
bob@pluto:/export/home/bob> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/export/home/bob/.ssh/identity):
Created directory '/export/home/bob/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /export/home/bob/.ssh/identity.
Your public key has been saved in /export/home/bob/.ssh/identity.pub.
The key fingerprint is:
48:bc:98:6a:9b:dc:8d:ee:a5:66:02:45:ce:6e:db bob@pluto
bob@pluto:/export/home/bob>
```

2. then on each machine, add the contents of `$HOME/.ssh/identity.pub` from the OTHER machine to `$HOME/.ssh/authorized_keys` on the local machine (`authorized_keys` is a bit like a `.rhosts` file) (`identity.pub` should look something like

```
1024 35 160113598328315770347757629917900809305107052156577
35309230295215401023914018627645367660366634152222008662730523500914536747457721973246144
4305418708539664884348021852629799444102754790417057317676624046572566499195728210728140
74215982344694643792671 bob@europa
```

(all that is on one line!)

Then you should be able to run `'ssh other_host'` or `'scp myfile other_host:myfile.bak'` from each and not get a password prompt.

N.B. The first time you connect to a new remote machine you will get a warning :

```
Warning: Permanently added the RSA1 host key for IP address 'a.b.c.d' to the list
of known hosts.
```

and it adds the remote machine's key to `$HOME/.ssh/known_hosts`

You should only set this up for situations where automated remote copying needs to be done, not just to avoid typing passwords..

If you have any problems you can use `'ssh -v other_host'` and you will see verbose messages as it proceeds, which usually pinpoints where the problem lies.