DOCUMENTATION > REMOTE-ACCESS > SSH > PASSWORDLESS

PASSWORDLESS SSH ACCESS

It is possible to configure your Pi to allow your computer to access it without providing a password each time you try to connect. To do this you need to generate an SSH key:

CHECK FOR EXISTING SSH KEYS

First, check whether there are already keys on your computer (the one you're connecting from):

```
ls ~/.ssh
```

If you see files named `id_rsa.pub` or `id_dsa.pub` you have keys set up already, so you can skip the generating keys step (or delete these files with `rm id*` and make new keys).

GENERATE NEW SSH KEYS

To generate new SSH keys enter the following command (Choose a sensible hostname such as `<YOURNANME>@<YOURDEVICE>` where we have used `eben@pi`):

```
ssh-keygen -t rsa -C eben@pi
```

You can also use a more descriptive comment using quotes if you have spaces, e.g. `ssh-keygen -t rsa -C "Raspberry Pi #123"`

Upon entering this command, you'll be asked where to save the key. We suggest you save it in the default location (`/home/pi/.ssh/id_rsa`) by just hitting `Enter`.

You'll also be asked to enter a passphrase. This is extra security which will make the key unusable without your passphrase, so if someone else copied your key, they could not impersonate you to gain access. If you choose to use a passphrase, type it here and press `Enter`, then type it again when prompted. Leave empty for no passphrase.

Now you should see the files `id_rsa` and `id_rsa.pub` in your `.ssh` directory in your home folder:

```
ls ~/.ssh
```

```
authorized_keys  id_rsa  id_rsa.pub  known_hosts
```

The `id_rsa` file is your private key. Keep this on your computer.

The `id_rsa.pub` file is your public key. This is what you put on machines you want to connect to. When the machine you try to connect to matches up your public and private key, it will allow you to connect.

Take a look at your public key to see what it looks like:

```
cat ~/.ssh/id_rsa.pub
```

It should be in the form:

```
ssh-rsa <REALLY LONG STRING OF RANDOM CHARACTERS> eben@pi
```

COPY YOUR PUBLIC KEY TO YOUR RASPBERRY PI

If your Pi does not have an .ssh directory you will need to set one up so that you can copy the key from your computer.

```
cd ~
install -d -m 700 ~/.ssh
```

To copy your public key to your Raspberry Pi, use the following command to append the public key to your `authorized_keys` file on the Pi, sending it over SSH:

```
cat ~/.ssh/id_rsa.pub | ssh <USERNAME>@<IP-ADDRESS> 'cat >>
.ssh/authorized_keys'
```

Note that this time you will have to authenticate with your password.

Now try `ssh <USER>@<IP-ADDRESS>` and you should connect without a password prompt.

following command:

```
ssh-add
```

If this did not work, delete your keys with `rm ~/.ssh/id*` and follow the instructions again.

You can also send files over SSH using the `scp` command (secure copy). See the SCP guide for more information.

VIEW/EDIT THIS PAGE ON GITHUB

READ OUR USAGE AND CONTRIBUTIONS POLICY