SSH into your Synology DiskStation with SSH Keys

https://chainsawonatireswing.com/2012/01/15/ssh-into-your-synology-diskstation-with-ssh-keys/

The Synology DiskStation supports both `telnet` & `SSH`, but all right-thinking people know that you should never use `telnet`, as it is completely insecure, & should instead use SSH, as it is very secure. It's easy to enable SSH on your DiskStation by going to Control Panel > Terminal & checking the box next to Enable SSH Service. You can now log in with your username & password.

But that's not enough. Logging in with a username & password isn't nearly as secure as requiring SSH keys. With that method, you have a private key on your computer & a public key on the SSH server (the Synology DiskStation in this case). When a computer tries to log in via SSH, the server looks at the public key & asks for the corresponding private key. No private key, no login.

NOTE: I'm assuming that you have already generated or possess SSH keys. If you haven't, I've written a section in *Linux Phrasebook* that covers how to do so, or you can easily find instructions on the Web.

To start the process, you need to edit the SSH daemon's config file to allow access via keys. Edit `/etc/ssh/sshd_config` using vim & change these lines:

```
#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile .ssh/authorized_keys
```

To this:

```
#RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_keys
```

Allow Root Login:

Change this line:

`PermitRootLogin No` `(or whateger else)`

To this:

`PermitRootLogin Yes`

Save the file.

Time to create the necessary `.ssh` directory & file on your Synology DiskStation:

```
> cd /root
> mkdir .ssh
> touch .ssh/authorized_keys
```

Now get your permissions set correctly on that directory & file:

```
> chmod 700 .ssh
> chmod 644 .ssh/authorized_keys
```

Note: Do not use Midnight Commander to create folders and files, as well as to assign access rights. Everything is done through the console. But you can insert a Public Key already using Midnight Commander
If you changed the host, but left the previous IP address, then do not forget to clear the cache of the old key `[HKEY_CURRENT_USER\SOFTWARE\SimonTatham\PuTTY\Ssh Host Keys]`

Now you need to edit the `authorized_keys` file. Do so remotely with vim, or FTP (with SSL enabled!) into the server, grab the file, edit it on your machine, & then FTP it back to the DiskStation—your choice. Put your public SSH key into the `authorized_keys` file, so it will look something like this:

```
ssh-dss
AAVLyQ9TYW7rKzUQJV9akeEaQjkVeERVaGvaLXnmg3PCIUaJd2tZTvQvdXHgtUfJdCJcKjTF2RdYFDO5weeoTtdaYl1cGYIWT+nfOhqs9+EG
mwwkM1MKoibRzIcu2EEkidBhAE4Ahya+iKbTzwk7VNgprAXA61j39SazZW2LkdHtlsHFloCqcHPXlakEj2JlAAAAFQDRBQ+l7v2rwhwFPKux
ucM834AqYzU4HzAbv0AgqLFsC4ZBwPEw+3HFwJX/Xkv3V67Sug8JKDbprbZct9c3TSYq24IDYRmVBsewj714qCeafZKdo3SRAVzB/6/rMKFa
5LkY5dOBfQuExSj9mTHMT9BkeeQnacld76OxxQiMej+bVLyQ9TYW7rKzUQJV9akeEaQjkVeERVaGvaLXnmg3PCIUaJd2tZJputa0TEpg5Gyq
enhQ6LE0B5ebjN/fVi7yuzRKqHrQUZVnziVgIMKpSJtqYoKW+3L0/L2rwhwFPKuxucM834AqYzU4Hz+q28Ss1HDEUrrQGR+D5xWISskUnH2o
PY0d5A8/phnH8FQp/gEwh3YIq3dLapOxpAZtg== johncarter@barsoom.local
```

Save the file, & try logging in to your Synology DiskStation:

```
ssh root@IP
BusyBox v1.16.1 (2011-11-26 14:58:46 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

>
```