Disallow logging in to a Synology DiskStation with passwords & only allow logging in via SSH keys

https://chainsawonatireswing.com/2012/01/23/disallow-logging-in-to-a-synology-diskstation-with-passwords-only-allow-logging-in-via-ssh-keys/

In a previous post—SSH into your Synology DiskStation with SSH Keys—I covered how to log in to your DiskStation using SSH keys instead of a password. After you know your keys work, it's a good idea to configure the SSH daemon on the DiskStation to disallow passwords so you *only* log in via keys. This adds a nice layer of security, but it also means that you'd better keep backups of your SSH keys, or you are hosed! If you're ready to do it, edit `/etc/ssh/sshd_config` & change these lines:

```
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
```

To this:

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
```

Save the file & restart the SSH daemon. Theoretically, you can do this on the command line—`/usr/syno/etc.defaults/rc.d/S95sshd.sh restart`–but I've found that this doesn't always work, which is troubling. Instead, use the GUI. Click on the Control Panel on the "Desktop" of the DiskStation, & then click on Terminal. Uncheck Enable SSH Service, check it again, and press OK.

Try logging in now, but use a username that doesn't exist on the server. You won't be prompted for a password; instead, you'll see:

```
Permission denied (publickey).
```

No key, no admittance. No passwords accepted. Excellent.