

# Step 4: Securing OpenSSH

⚠ Before continuing: This will make login via password impossible. If you lose your SSH key, you will lose access to your server and it will require a reinstallation.

The OpenSSH server configuration should be located at `/etc/ssh/sshd_config` but we aren't going to edit this file. We are going to create a new file at `/etc/ssh/sshd_config.d/hardening.conf`. (add video)

```
X11Forwarding no

AllowAgentForwarding no

PermitEmptyPasswords no

MaxAuthTries 3

# NOTE: this will disable password authentication entirely! Setup SSH keys before applying
this config!
PubkeyAuthentication yes
PasswordAuthentication no
PermitRootLogin no

Protocol 2
```

Now to apply these settings, we need to restart the ssh server with: `sudo systemctl restart sshd`, and voilà!

---

Revision #10

Created 20 October 2025 13:10:23 by seres

Updated 19 December 2025 02:13:24 by seres