

Remote Administration Via SSH

- Set SSH Protocol To 2
- Disable SSH Root Login
- Set SSH `peremptypasswords` to no

Set SSH Protocol To 2

Set SSH protocol to 2

SSH has two protocols it may use, protocol 1 and protocol 2. The older protocol 1 is less secure and should be disabled unless you know that you specifically require it.

1. Open the sshd config

```
|vi /etc/ssh/sshd_config|
```

2. Add or amend as shown below

```
|# Protocol 2,1|  
Protocol 2
```

3. Restart the sshd service

```
|systemctl restart sshd.service|
```

Disable SSH Root Login

Disabling root login via SSH

Disabling SSH root login will add an extra layer of security. It would be more secure to brute force attacks or in case your password is stolen.

1. Create a non-root user

```
adduser username  
passwd username
```

2. Open the ssh configuration file with your editor.

```
vi /etc/ssh/sshd_config
```

3. Add the line "PermitRootLogin no." Or uncomment the line "#PermitRootLogin yes" and change yes to no.

```
#LoginGraceTime 2m  
#PermitRootLogin yes  
#StrictModes yes  
#MaxAuthTries 6  
#MaxSessions 10  
PermitRootLogin no
```

4. Save and exit the file.
5. Restart the ssh service

```
systemctl restart sshd.service
```

Set SSH permitemptypasswords to no

Set SSH permitemptypasswords to no

1. Open the ssh configuration file with your editor.

```
vi /etc/ssh/sshd_config
```

2. Add or amend as shown below

```
|PermitEmptyPasswords no|
```

3. Restart the sshd service

```
|systemctl restart sshd.service|
```