

5.2 SSH Server Configuration

SSH is a secure, encrypted replacement for common login services such as telnet, ftp, rlogin, rsh, and rcp. It is strongly recommended that sites abandon older clear-text login protocols and use SSH to prevent session hijacking and sniffing of sensitive data off the network.

Note: The recommendations in this section only apply if the SSH daemon is installed on the system, if remote access is not required the SSH daemon can be removed and this section skipped.

Note: Once all configuration changes have been made to /etc/ssh/sshd_config, the sshd configuration must be reloaded:

```
# service sshd reload
```

From:

<https://secscan.acron.pl/> - **SecScan**

Permanent link:

<https://secscan.acron.pl/ubuntu1604/5/2>

Last update: **2017/05/04 10:02**

