For the most part, SSH works reasonably well when it’s first installed, so you may not need  
to make any changes to its configuration. If you do need to make changes, though, these  
are mostly handled through the main SSH configuration file, /etc/ssh/sshd\_config. You  
can also edit some additional files to limit access to the SSH server or to change how SSH  
manages the login process.

The /etc/ssh/sshd\_config file consists mainly of option lines that take the  
following form:  
option value

Don’t confuse the sshd\_config file with the ssh\_config file. The former  
controls the OpenSSH server, whereas the latter controls the SSH client  
program, ssh.

**Protocol** This option specifies the protocol levels OpenSSH understands. Possible values  
are 1 and 2. You can configure OpenSSH to support both protocols by separating them by  
a comma, as in 1,2 or 2,1, which are equivalent. OpenSSH protocol level 1 is no longer  
considered secure. Therefore, the safest configuration is to set Protocol 2. This limits the  
server’s ability to communicate with older clients, though.  
**PermitRootLogin** By default, this option is set to yes, which enables OpenSSH to accept  
direct logins by root. This is safer than a similar configuration under Telnet, but for a bit  
of added security, set this value to no. The result will be that anybody wanting to perform  
remote work using superuser privileges will need first to log in as an ordinary user.  
**X11Forwarding** This option specifies whether OpenSSH’s X tunneling features should  
be active. If you want to enable remote users to run GUI programs via SSH, you must set  
this option to yes. Doing so can slightly degrade security of the client’s X display, though,  
depending on certain other options, hence the conservative default value of no.