How to Configure and Enable SSH on Debian 12

By Adnan Shabbir. Published on 03/07/2023.

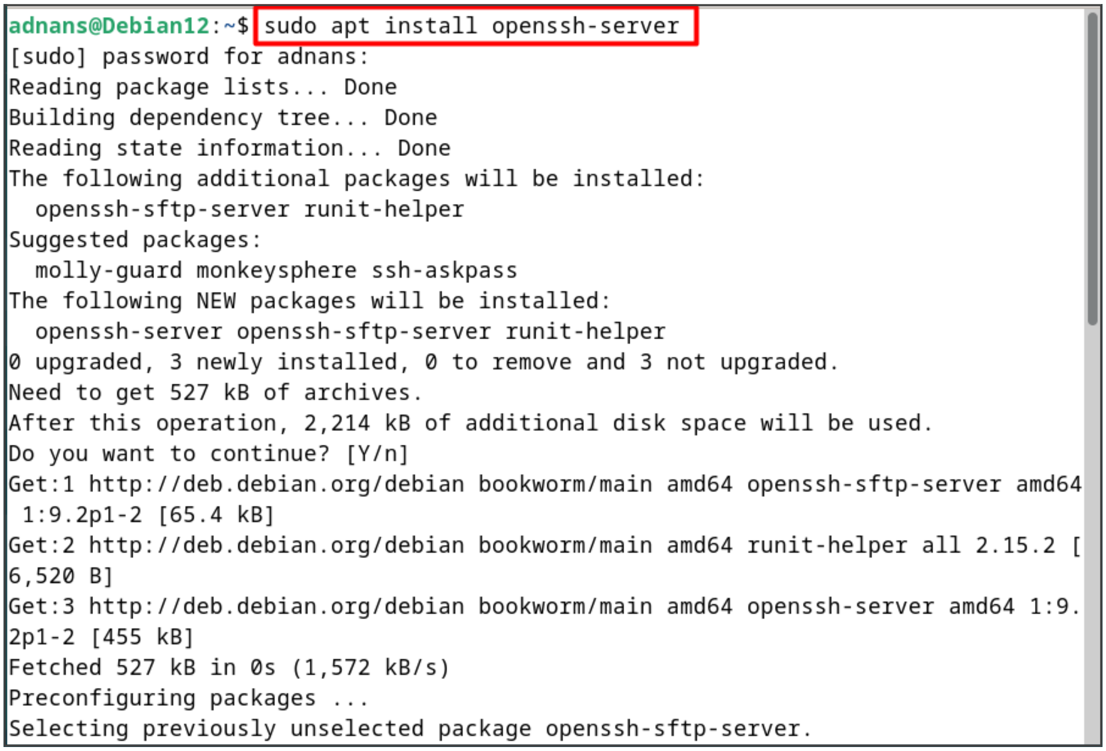
SSH (Secure Shell) is a cryptographic network protocol that provides secure remote access and control over a network. It allows users to log into and manage remote machines or servers securely. SSH plays a vital role in enabling secure remote access, file transfers, and encrypted communication for Debian users, enhancing their systems' overall security and flexibility.

Debian 12, the latest LTS of the Debian distribution, has been released, which offers more advanced security features and an improved user experience. You might be wondering how to configure or enable SSH on Debian 12. Well, it's quite easy and takes no time. We have prepared this guide to teach you how SSH can be enabled and configured on Debian 12.

Prerequisites: Install SSH Server

The purpose of the guide is to enable and configure SSH on Debian 12. Thus, before proceeding, you must ensure that the SSH is installed on your system. The command to install SSH on Debian 12 is as follows:

```
$ sudo apt install openssh-server
```



```
adnans@Debian12:~$ sudo apt install openssh-server
[sudo] password for adnans:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  openssh-sftp-server runit-helper
Suggested packages:
  molly-guard monkeysphere ssh-askpass
The following NEW packages will be installed:
  openssh-server openssh-sftp-server runit-helper
0 upgraded, 3 newly installed, 0 to remove and 3 not upgraded.
Need to get 527 kB of archives.
After this operation, 2,214 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://deb.debian.org/debian bookworm/main amd64 openssh-sftp-server amd64
 1:9.2p1-2 [65.4 kB]
Get:2 http://deb.debian.org/debian bookworm/main amd64 runit-helper all 2.15.2 [
6,520 B]
Get:3 http://deb.debian.org/debian bookworm/main amd64 openssh-server amd64 1:9.
2p1-2 [455 kB]
Fetched 527 kB in 0s (1,572 kB/s)
Preconfiguring packages ...
Selecting previously unselected package openssh-sftp-server.
```

How to Configure and Enable SSH on Debian 12?

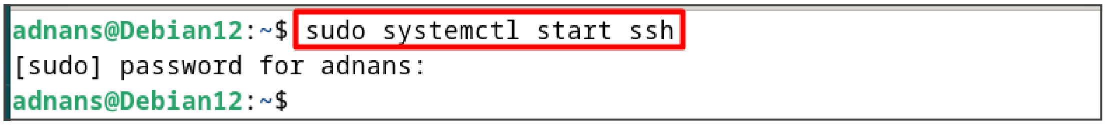
Enabling and configuring SSH on Debian 12 is of utmost importance as it allows for secure remote access and administration of Debian servers. By enabling SSH, administrators gain the ability to manage their systems from any location remotely, eliminating the need for physical access. Let’s do it on Debian 12:

Note: The SSH server is associated with the service named “**ssh**” on Debian 12. So, here the SSH keyword in commands will refer to the service that manages the SSH server on Debian 12.

Step 1: Activate the SSH Server

Right after the installation, the SSH service will be started automatically. However, if it is not. You can start the SSH service as follows:

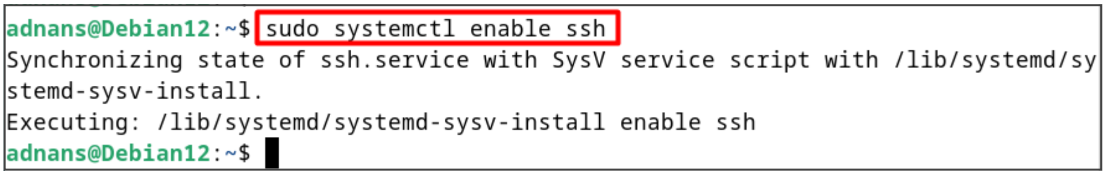
```
$ sudo systemctl start ssh
```



```
adnans@Debian12:~$ sudo systemctl start ssh
[sudo] password for adnans:
adnans@Debian12:~$
```

Meanwhile, it is recommended to enable the SSH service as well to keep functioning the SSH after every restart:

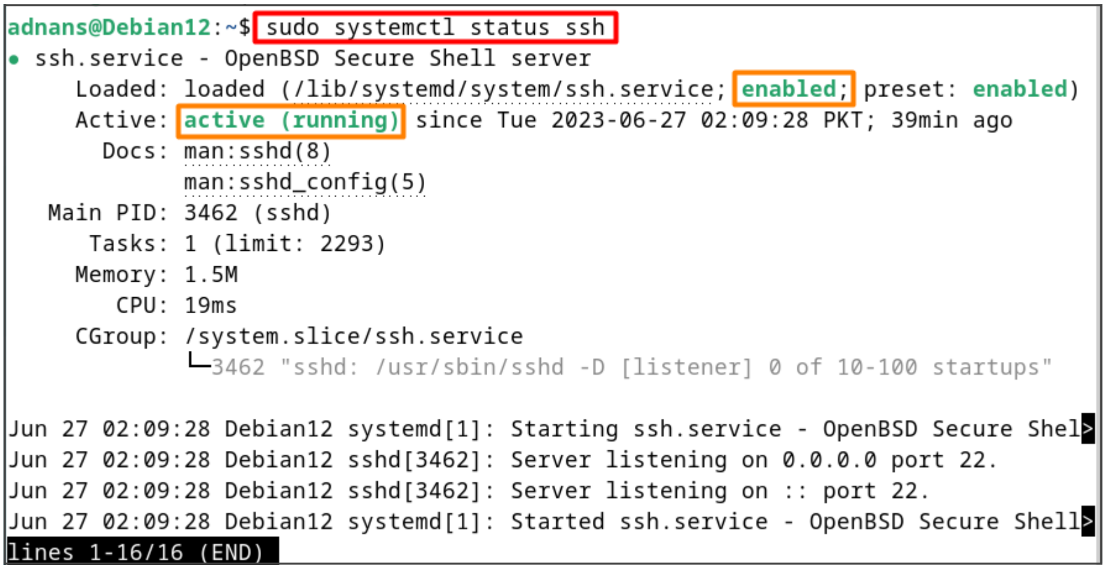
```
$ sudo systemctl enable ssh
```



```
adnans@Debian12:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/sy
stemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
adnans@Debian12:~$ 
```

To verify these, you need to check the status of the SSH service using the command:

```
$ sudo systemctl status ssh
```



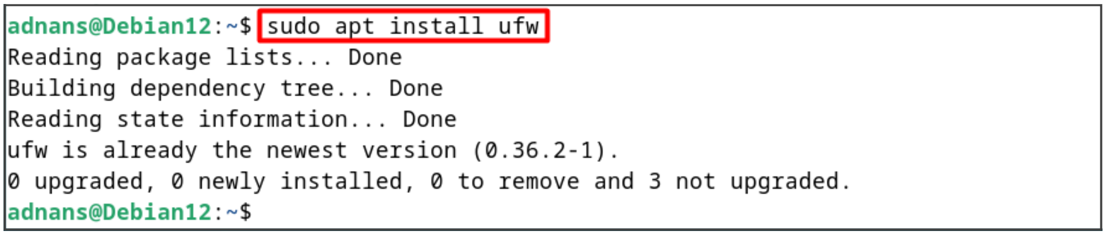
```
adnans@Debian12:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Tue 2023-06-27 02:09:28 PKT; 39min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 3462 (sshd)
      Tasks: 1 (limit: 2293)
     Memory: 1.5M
        CPU: 19ms
     CGroup: /system.slice/ssh.service
             └─3462 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jun 27 02:09:28 Debian12 systemd[1]: Starting ssh.service - OpenBSD Secure Shel>
Jun 27 02:09:28 Debian12 sshd[3462]: Server listening on 0.0.0.0 port 22.
Jun 27 02:09:28 Debian12 sshd[3462]: Server listening on :: port 22.
Jun 27 02:09:28 Debian12 systemd[1]: Started ssh.service - OpenBSD Secure Shell>
lines 1-16/16 (END)
```

The output of the command shows that the SSH is also running in an active state and is enabled.

Step 2: Add the Firewall Rules

The SSH server listens to port 22, which depends on the approval of your system's firewall. Here, the ufw utility will allow SSH over the firewall. To install the ufw on Debian 12, use the command:

```
$ sudo apt install ufw
```

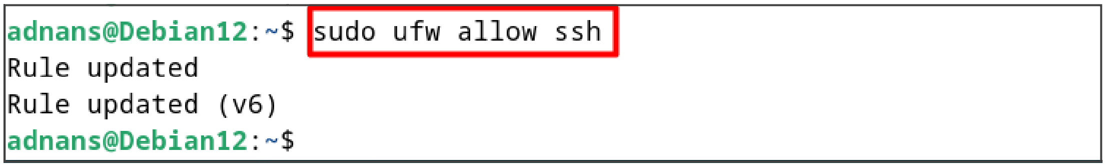


```
adnans@Debian12:~$ sudo apt install ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.2-1).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
adnans@Debian12:~$
```

If the Port is Default (22):

Now, use the allow option of the ufw utility to allow SSH on the firewall as follows:

```
$ sudo ufw allow ssh
```



```
adnans@Debian12:~$ sudo ufw allow ssh
Rule updated
Rule updated (v6)
adnans@Debian12:~$
```

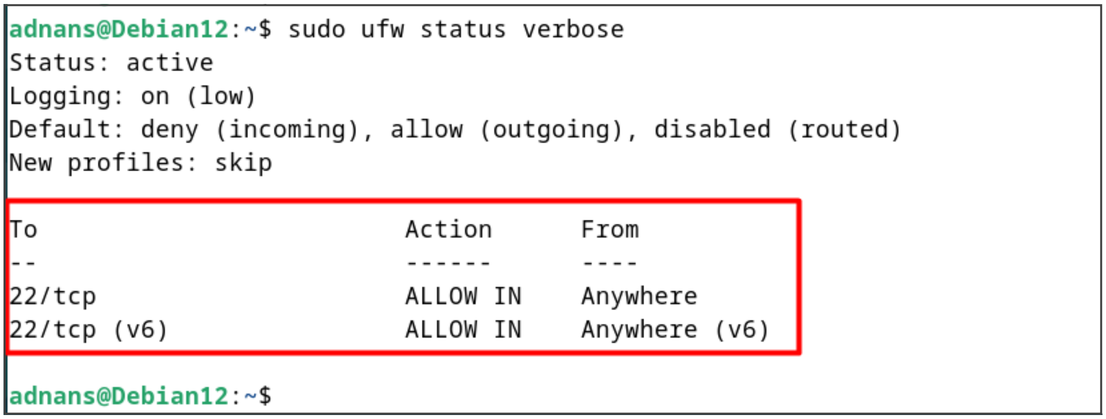
If the Port is Other Than Default:

What if the SSH is listening to a port other than 22? Then, you have to specify the port number in the command:

```
$ sudo ufw allow <port-no>
```

To verify it, check the status of the ufw utility in verbose mode as follows:

```
$ sudo ufw status verbose
```



```
adnans@Debian12:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)

adnans@Debian12:~$
```

Test the SSH Server on Debian 12

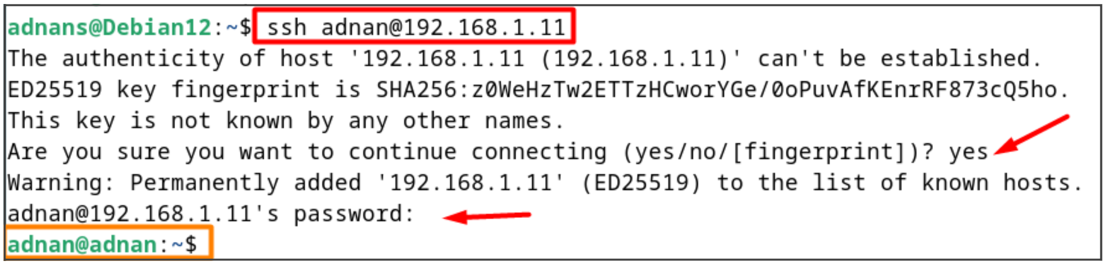
Once you have done the above-listed steps, you can make a new SSH connection. The command's syntax to connect to the machine via SSH is:

Syntax:

```
$ ssh <username> @<Server-IPAddress>
```

Enter the username and the IP address of the server to whom you are establishing the connection. For example, we have created an SSH connection with a Linux server. You have to write “yes” to continue connecting and then insert the password of the server’s username that you entered in the command. Once the connection is established, you can see that the username and the hostname have been changed to the machine you are connected to.

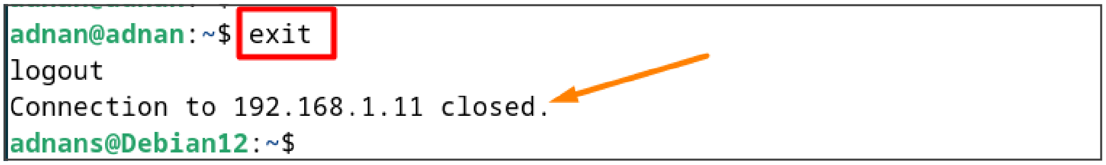
```
$ ssh adnan@192.168.1.11
```



```
adnans@Debian12:~$ ssh adnan@192.168.1.11
The authenticity of host '192.168.1.11 (192.168.1.11)' can't be established.
ED25519 key fingerprint is SHA256:z0WeHzTw2ETTzHCworYGe/0oPuvAfKEnrRF873cQ5ho.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.11' (ED25519) to the list of known hosts.
adnan@192.168.1.11's password:
adnan@adnan:~$
```

To break the connection, type exit and hit enter. The connection will be terminated instantly, as seen in our case:

```
$ exit
```



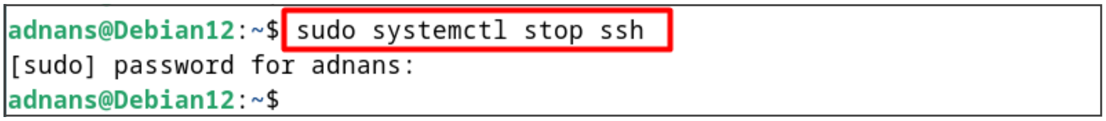
```
adnan@adnan:~$ exit
logout
Connection to 192.168.1.11 closed.
adnans@Debian12:~$
```

How to Disable SSH on Debian 12?

What if you are now done with the SSH but still think some penetration can occur? Well, Linux is well-known for its security. However, this may happen on extremely exposed servers. You can avoid such cases by disabling the SSH and disallowing the SSH over the firewall.

Stop the SSH Server's service:

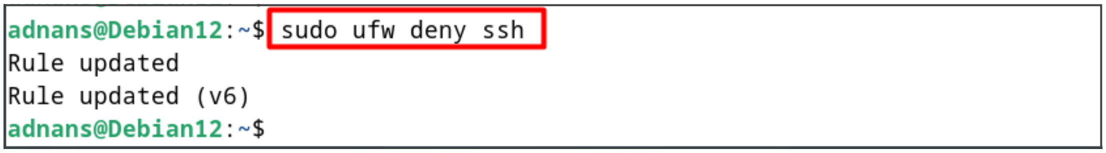
```
$ sudo systemctl stop ssh
```



```
adnans@Debian12:~$ sudo systemctl stop ssh
[sudo] password for adnans:
adnans@Debian12:~$
```

Deny the SSH Over Firewall

```
$ sudo ufw deny ssh
```



```
adnans@Debian12:~$ sudo ufw deny ssh
Rule updated
Rule updated (v6)
adnans@Debian12:~$
```

That's how you can configure the SSH on Debian 12.

Wrap Up

Being a Linux administrator, you must be aware of the importance of SSH, which is used to establish a remote connection. As you know, Debian 12 has just been released, and if you are an administrator working on Debian 12, then this guide is purely for you to configure/enable SSH on your Debian 12.

The systemctl and the ufw utilities play a vital role in managing the SSH services on the system and on the firewall. We have listed all the steps with commands to configure and enable SSH on Debian 12. Moreover, the process to disable (just for security reasons) the SSH server is also demonstrated. Want more tips for system/network administrators? keep visiting Linux-Genie for daily updates.

← PREVIOUS POST

How to Configure Firewall on Debian 12?

NEXT POST →

How to Install Cinnamon Desktop Environment (DE) on Debian 12