How To: Setup sudo in Debian

sudo in Debian Linux

Apparently, **[Debian](#)** installer doesn't install or activate **[sudo](#)** by default. This means that [sudo command](#) is not found the only privilege escalation method available is becoming root via su command. Since I like and use **[sudo](#)** daily, I decided to install and setup it on **Debian** VM.

Install sudo package in Debian

That's the very first step you'll need to do: use apt to install sudo. You need to become root before you do it, of course (so you must know root user password for your **Debian** install):

```
greys@debian:~$ su -
Password:
root@debian:~ # apt install sudo
Reading package lists… Done
Building dependency tree
Reading state information… Done
The following NEW packages will be installed:
```

```
  sudo
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/1,245 kB of archives.
After this operation, 3,886 kB of additional disk space will
be used.
Selecting previously unselected package sudo.
(Reading database … 174742 files and directories currently
installed.)
Preparing to unpack …/sudo_1.8.27-1_amd64.deb …
Unpacking sudo (1.8.27-1) …
Setting up sudo (1.8.27-1) …
Processing triggers for man-db (2.8.5-2) …
Processing triggers for systemd (241-5) …
root@debian:~ # sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u
user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U
user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g
group] [-h host] [-p prompt] [-T timeout] [-u user]
[VAR=value] [-i|-s] []
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group]
[-h host] [-p prompt] [-T timeout] [-u user] file …
```

Configure /etc/sudoers File

/etc/sudoers is the main configuration file for [sudo command](). It contains list of users and groups that are allowed to become root (or become other users by invoking su command as root).

Here's the default file in [**Debian 10 Buster**]():

```
root@debian:~ # cat /etc/sudoers
```

```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/
instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults
secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin
:/sbin:/bin"
# Host alias specification


# User alias specification


# Cmnd alias specification


# User privilege specification
root    ALL=(ALL:ALL) ALL


# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL


# See sudoers(5) for more information on "#include"
directives:
#includedir /etc/sudoers.d
```

I've highlighted the 3 most important elements of this file at this early stage:

root   ALL=(ALL:ALL) ALL

This is the line that allows you to debug sudo commands as root user.

At this means that any user that belongs to group sudo will also be allowed to use **[sudo commands](#)**:

%sudo   ALL=(ALL:ALL) ALL

Finally, this part includes additional configuration files from /etc/sudoers.d directory:

#includedir /etc/sudoers.d

… this means you don't have to edit **/etc/sudoers** file but instead can create a specific file in **/etc/sudoers.d** and name it self-descriptively, like:

/etc/sudoers.d/web-server-admins

meaning, that this file will contain usernames and privileges required by web-server admins (usually commands like stopping/starting Apache or nginx webserver).

Since this is a very basic tutorial, we don't have to edit the file at all – just need to add our user (mine is greys, as you remember) to the sudo group and check.

Add user to sudo group

Step 1: let's make sure sudo is not accessible before we begin

This needs to be run as your regular user, not as root:

```
greys@debian:~$ sudo -i
[sudo] password for greys:
greys is not in the sudoers file.  This incident will be
reported.
greys@debian:~$
```

Let's check my groups just to be sure there's no **sudo** among them:

```
greys@debian:~$ id greys
uid=1000(greys)                          gid=1000(greys)
groups=1000(greys),24(cdrom),25(floppy),29(audio),30(dip),44(v
ideo),46(plugdev),108(netdev),112(bluetooth),116(scanner)
```

Step 2: add user to sudo group

Excellent, now it's time to add user greys to the group sudo (we must become root again to run **usermod command**)

```
root@debian:~ # usermod -a -G sudo greys
root@debian:~ # id greys
uid=1000(greys)                          gid=1000(greys)
groups=1000(greys),24(cdrom),25(floppy),27(sudo),29(audio),30(
dip),44(video),46(plugdev),108(netdev),112(bluetooth),116(scan
ner)
```

As you can see, I'm now a member of the **sudo** group!

Step 3: Log out and log back in for group membership to be recognised

Now you need to disconnect from your server or desktop session and log in again, so that your group membersip is recognised. One reconnected, check your groups with **id command** and try **sudo** again:

greys@debian9:~$ id
uid=1000(greys)   gid=1000(greys)
groups=1000(greys),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),108(netdev),112(bluetooth),116(scanner)

so yes, we're a member of sudo group now… This is the moment of truth! Let's try to become root:

greys@debian:~$ **sudo -i**
root@debian:~ # **id**
uid=0(root) gid=0(root) groups=0(root)

Tha'ts it for today!

See Also

- **SUDO reference**
- **sudo command**