

Table Of Contents

Table Of Contents ..... 1

How Do I Keep Track Of All Users In Admin Group? ..... 2

See Also: ..... 3

[Home](#) > [Faq](#) > [CentOS](#)

## CentOS / Red Hat: Sudo Allows People In Group Admin To Run All Commands

Posted by [Vivek Gite](#) <[vivek@nixcraft.com](mailto:vivek@nixcraft.com)>

I like the way Ubuntu Linux works - all people in admin groups should be able to run all commands after running it via sudo "command-name". How do I setup [sudo under CentOS or Red Hat Enterprise Linux](#) [2] to allow all members of the 'admin' group to run all commands?



[1]

/etc/sudoers file allows particular users or groups to run various commands as the root user, without needing the root password. This is useful for delegating roles and permissions to other users without sharing the root password. This file must be edited with the visudo command. Login as the root user and enter:



[3]



[4]

```
# visudo
```

Append the following line:

```
## Allows people in group admin to run all commands
%admin  ALL=(ALL)        ALL
```

Save and close the file. Finally, add a group called admin:

```
# groupadd admin
```

Add a user called [vivek \(existing user\) to group admin](#) [5]:

```
# usermod -a -G admin vivek
```

Verify group membership:

```
# id vivek
```

Sample Outputs:

```
uid=5001(vivek) gid=5001(vivek) groups=5001(vivek),10(admin)
```

Login as user vivek and to run any command as the root type:

```
$ sudo /etc/init.d/httpd restart
```

To gain root shell, enter:

```
$ sudo -s
```

When prompted for a password, enter vivek's password.

## How Do I Keep Track Of All Users In Admin Group?

sudo can log both successful and unsuccessful attempts (as well as errors) to syslog (default is /var/log/secure), a log file, or both. By default sudo will log via syslog but this is changeable at [configure time or via the sudoers file](#) [6].

```
# tail -f /var/log/secure
# grep something /var/log/secure
```

Please note that sudo will normally only log the command it explicitly runs. If a user runs a command such as `sudo su` or `sudo sh`, subsequent commands run from that shell will not be logged, nor will sudo's access control affect them. The same is true for commands that offer shell escapes (including most editors).

**See Also:**

- [Allow a normal user to run commands as root under Linux / UNIX operating systems](#) <sup>[2]</sup>

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our [daily email](#) newsletter or [weekly newsletter](#) to make sure you don't miss a single tip/tricks. Alternatively, subscribe via [RSS/XML](#) feed.

Article printed from Frequently Asked Questions About Linux / UNIX: <http://www.cyberciti.biz/faq/>

URL to article: <http://www.cyberciti.biz/faq/linux-sudo-allows-people-in-group-admin/>

URLs in this post:

[1] Image: <http://www.cyberciti.biz/faq/category/redhat-and-friends/>

[2] sudo under CentOS or Red Hat Enterprise Linux: <http://www.cyberciti.biz/tips/allow-a-normal-user-to-run-commands-as-root.html>

[3] Image: <http://www.cyberciti.biz/faq/category/centos/>

[4] Image: <http://www.cyberciti.biz/faq/category/fedora-linux/>

[5] vivek (existing user) to group admin: <http://www.cyberciti.biz/faq/howto-linux-add-user-to-group/>

[6] configure time or via the sudoers file: <http://www.cyberciti.biz/faq/sudo-send-e-mail-sudo-log-file/>