

Using the Root Account on Debian

By *srlinuxx*

Created *05/12/2005 - 1:37am*

Submitted by srlinuxx on Monday 5th of December 2005 01:37:33 AM Filed under [HowTos](#) [1]

There is one user account on your Debian system that has the power to change anything: the root account. By power, I mean absolute power. The root user account can read, replace, or remove any file. It can read or write to any attached device. It can read or write to any part of the computer's memory. If there's even a mere suspicion that a piece of software is buggy or poses a security risk, there's no way you should run it as root.

Because of the power of the root account, sensible system administrators take a good deal of care when using it. The best rule of thumb is to do only the bare minimum of operations as root. Different users take different views on how to minimize root usage. Increasingly, Unix-like operating systems take the approach of going as far as to disable the root account and to use privilege-gaining tools such as sudo to give normal users the ability to run programs as the root user when required.

This article introduces using sudo to restrict superuser privileges. It is a good idea for you to get used to sudo now, as the rest of this series will use it wherever you need root access to perform a task.

[Full Article](#) [2].

[HowTos](#)

Source URL: <http://www.tuxmachines.org/node/3844>

Links:

[1] <http://www.tuxmachines.org/taxonomy/term/98>

[2] http://www.linuxdevcenter.com/pub/a/linux/2005/12/01/linux_root.html