What is Sticky Bit, SUID and SGID in Linux

Written by [Rahul](https://tecadmin.net/author/myadmin/), Updated on October 25, 2017

[Linux Tutorials](https://tecadmin.net/category/linux-tutorials/) [SGID](https://tecadmin.net/tag/sgid/), [Sticky Bit](https://tecadmin.net/tag/sticky-bit/), [SUID](https://tecadmin.net/tag/suid/), [SUID and SGID in Linux](https://tecadmin.net/tag/suid-and-sgid-in-linux/)

This tutorial will help you to under thae Sticky bit, SUID and SGID file permissions under Linux system.

**What is Sticky Bit?**

The sticky bit is used to indicate special permissions for files and directories. If a directory with sticky bit enabled will restrict deletion of the file inside it. It can be removed by root, owner of the file or who have to write permission on it. This is useful for publically accessible directories like /tmp.

Here is the implementation of Sticky bit on file on Linux system.  
**Method 1:**

$ chmod +t tecadmin.txt

$ ls -l tecadmin.txt

-rw-r--r-**T** 1 root root 0 Mar 8 02:06 tecadmin.txt

**Mothod 2:**

# chmod 1777 tecadmin.txt

# ls -l tecadmin.txt

-rwxrwxrw**t** 1 root root 0 Mar 8 02:06 tecadmin.txt

In above output it showing sticky bit is set with character t or T in permissions filed. Small t represent that execute permission also enable and capital T represent that execute permission are not enabled.

**What is SUID (setuid)?**

If SUID bit is set on a file and a user executed it. The process will have the same rights as the owner of the file being executed.

For example: **passwd** command have SUID bit enabled. When a normal user changes his password this script update few system files like /etc/passwd and /etc/shadow which can’t be updated by non-root account. So that **passwd** command process always run with root user rights.

Here is the implementation of SUID on file under Linux system.

**Mehtod 1:**

# chmod u+s tecadmin.txt

# ls -l tecadmin.txt

-rw**s**r-xr-x 1 root root 0 Mar 8 02:06 tecadmin.txt

**Method 2:**

# chmod 4655 tecadmin.txt

# ls -l tecadmin.txt

-rw**S**r-xr-x 1 root root 0 Mar 8 02:06 tecadmin.txt

**What is SGID (setgid)?**

Same as SUID, The process will have the same group rights of the file being executed. If SGID bit is set on any directory, all subdirectories and files created inside will get same group ownership as the main directory, it doesn’t matter who is creating.

Here is the implementation of SGID on directory on Linux system.

# chmod g+s /test/

# ls -ld /test

drwxrw**s**rwx 2 root root 4096 Mar 8 03:12 /test

Now swich to other user and create a file in /test directory.

# su - tecadmin

$ cd /test/

$ touch tecadmin.net.txt

$ ls -l tecadmin.net.txt

-rw-rw-r-- 1 tecadmin root 0 Mar 8 03:13 tecadmin.net.txt

In above example tecadmin.net.txt is created with root group ownership.

Thanks for reading this article, I hope it will help you to understand the sticky bit, SUID, and SGID in Linux.