Access Control Lists (ACL) in Linux

**What is ACL?**

Access control list (ACL) provides an additional, more flexible permission mechanism for file systems. It is designed to assist with UNIX file permissions. ACL allows you to give permissions for any user or group to any disc resource.

**Use of ACL :**

Think of a scenario in which a particular user is not a member of group created by you but still you want to give some read or write access, how can you do it without making user a member of group, here comes in picture Access Control Lists, ACL helps us to do this trick.

Basically, ACLs are used to make a flexible permission mechanism in Linux.

From Linux man pages, ACLs are used to define more fine-grained discretionary access rights for files and directories.

**setfacl** and **getfacl** are used for setting up ACL and showing ACL respectively.

For example:

getfacl test/declarations.h

Output:

# file: test/declarations.h

# owner: mandeep

# group: mandeep

user::rw-

group::rw-

other::r--

**List of commands for setting up ACL :**

1) To add permission for user

**setfacl -m "u:user:permissions" /path/to/file**

2) To add permissions for a group

**setfacl -m "g:group:permissions" /path/to/file**

3) To allow all files or directories to inherit ACL entries from the directory it is within

**setfacl -dm "entry" /path/to/dir**

4) To remove a specific entry

**setfacl -x "entry" /path/to/file**

5) To remove all entries

**setfacl -b path/to/file**

For example :

setfacl -m u:mandeep:rwx test/declarations.h

**Modifying ACL using setfacl :**  
To add permissions for a user (user is either the user name or ID):

# setfacl -m "u:user:permissions"

To add permissions for a group (group is either the group name or ID):

# setfacl -m "g:group:permissions"

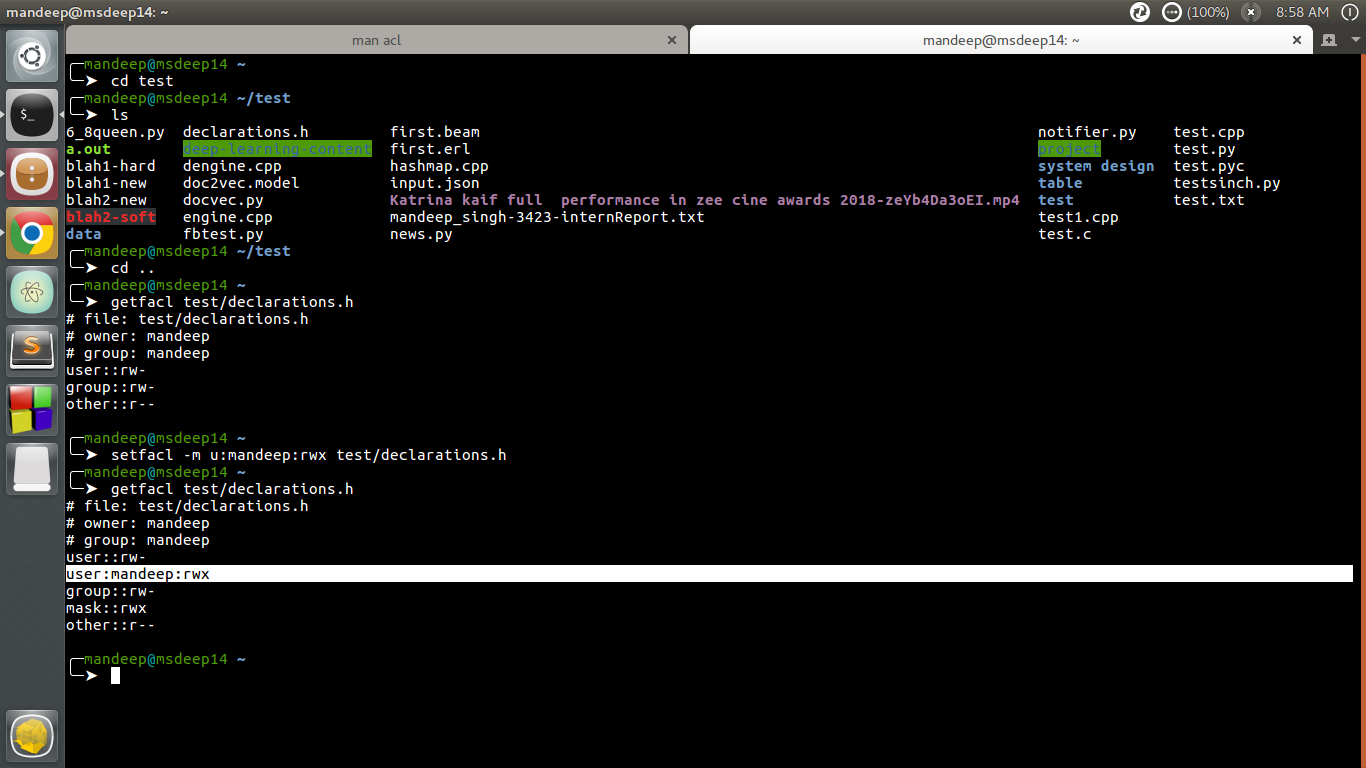
To allow all files or directories to inherit ACL entries from the directory it is within:

# setfacl -dm "entry"

Example :

setfacl -m u:mandeep:r-x test/declarations.h

See below image for output :

[](https://cdncontribute.geeksforgeeks.org/wp-content/uploads/acl1.png)

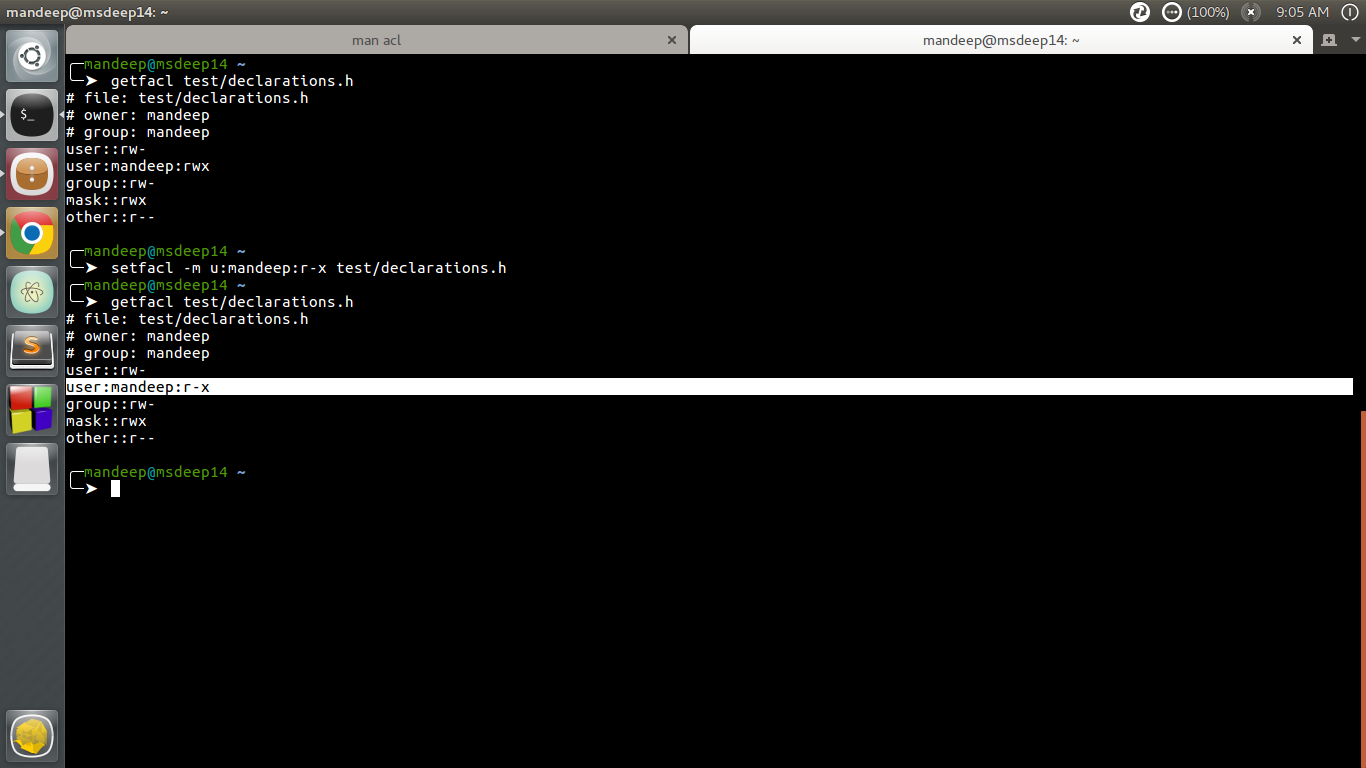
*setfacl and getfacl*

**View ACL :**  
To show permissions :

# getfacl filename

Observe the difference between output of **getfacl** command before and after setting up ACL permissions using **setfacl** command.  
There is one extra line added for user mandeep which is highlighted in image above.

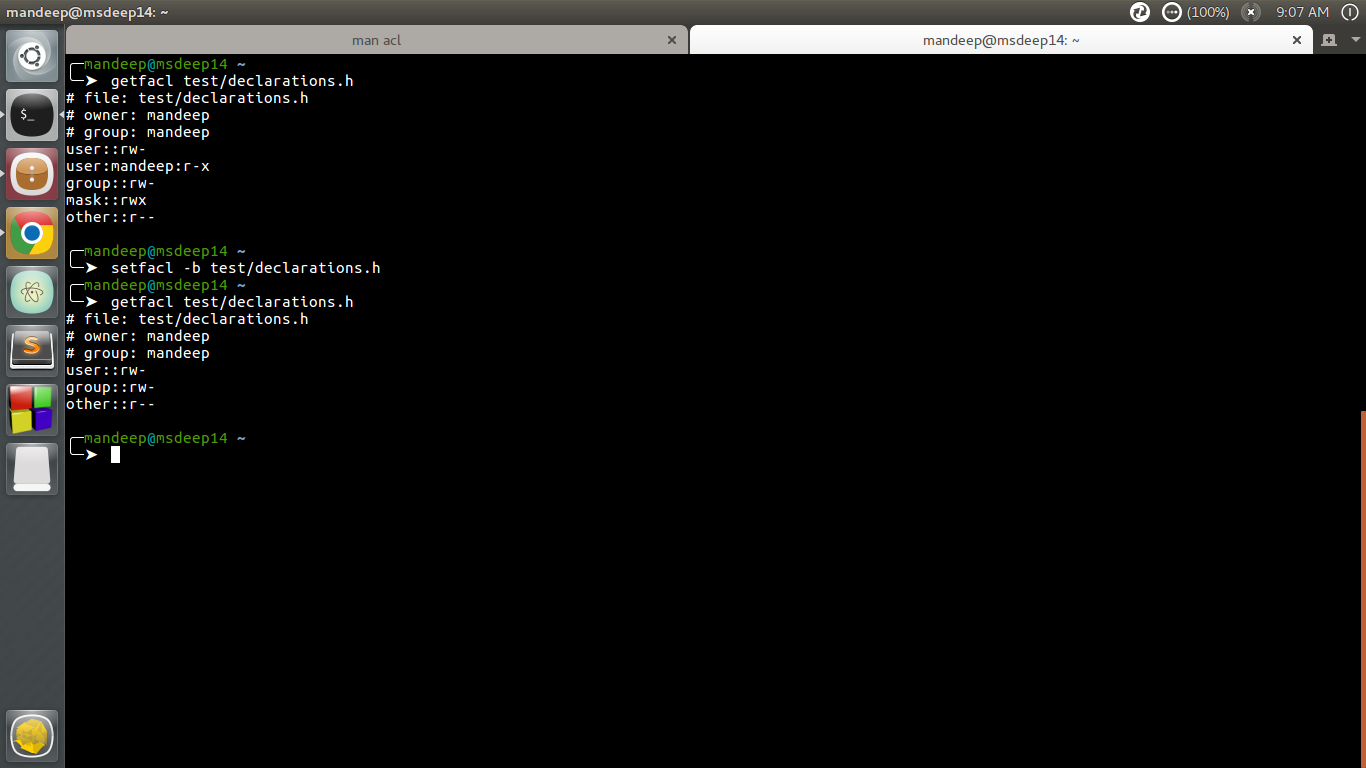
Output:

[](https://cdncontribute.geeksforgeeks.org/wp-content/uploads/acl2.png)

*change permissions*

The above command change permissions from **rwx** to **r-x**

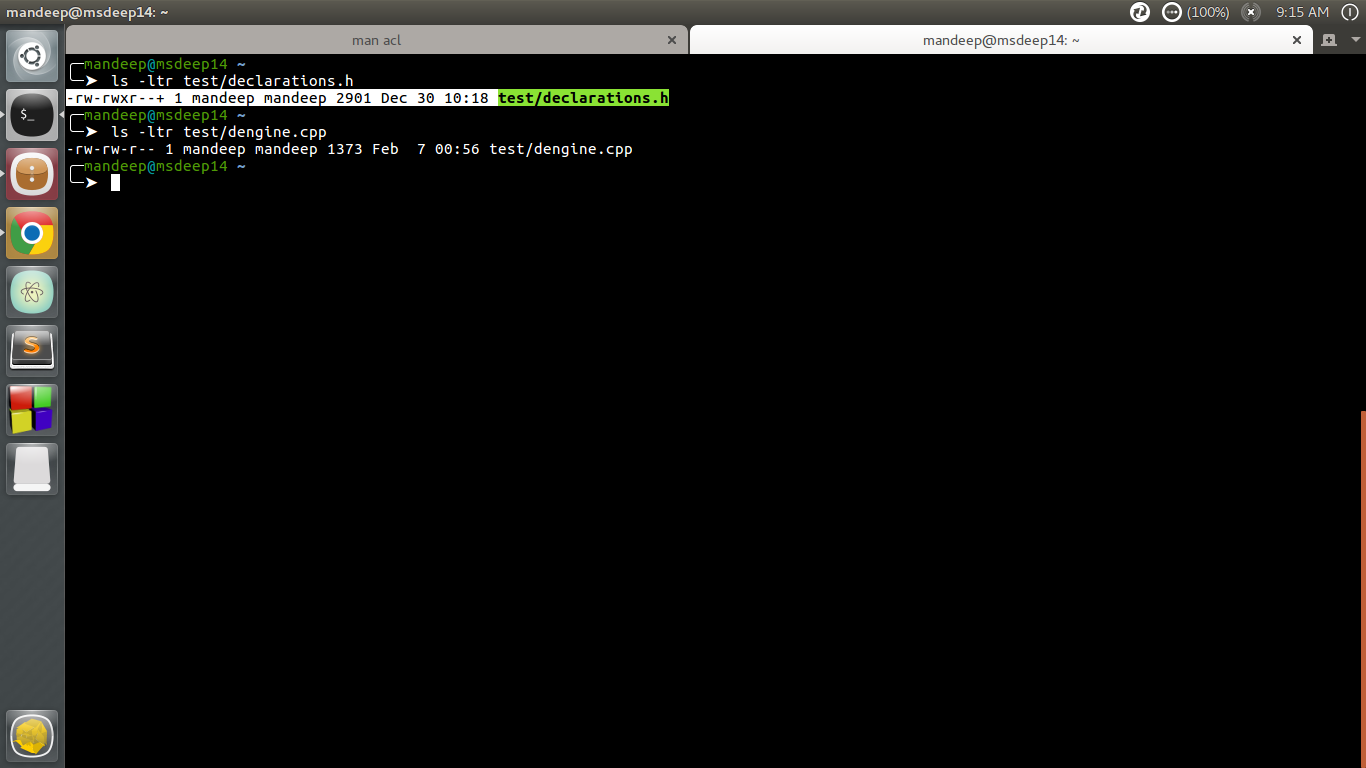
**Remove ACL :**  
If you want to remove the set ACL permissions, use setfacl command with -b option.  
For example :

[](https://cdncontribute.geeksforgeeks.org/wp-content/uploads/acl3.png)

*remove set permissions*

If you compare output of getfacl command before and after using setfacl command with -b option, you can observe that there is no particular entry for user mandeep in later output.

You can also check if there are any extra permissions set through ACL using ls command.

[](https://cdncontribute.geeksforgeeks.org/wp-content/uploads/acl4.png)

*check set acl with ls*

Observe the first command output in image, there is extra “+” sign after the permissions like **-rw-rwxr–+**, this indicates there are extra ACL permissions set which you can check by getfacl command.

**Using Default ACL :**  
The default ACL is a specific type of permission assigned to a directory, that doesn’t change the permissions of the directory itself, but makes so that specified ACLs are set by default on all the files created inside of it. Let’s demonstrate it : first we are going to create a directory and assign default ACL to it by using the -d option:

$ mkdir test &&setfacl -d -m u:dummy:rw test