

# File permissions in Linux

## Project description

[Describe what you accomplish through Linux commands.]

```
[ cd ./researcher2/projects ]
```

## Check file and directory details

```
[ ls -la ]
```

## Describe the permissions string

```
[ -rw-rw-rw- Research Team ##### ..... project_k.txt ]  
[ -rw-r----- Research Team ##### ..... project_m.txt ]  
[ -rw-rw-r-- Research Team ##### ..... project_r.txt ]  
[ -rw-rw-r-- Research Team ##### ..... project_t.txt ]  
[ -rw--w---- Research Team ##### ..... .project_x.txt ]  
[ drwx--x--- Research Team ##### ..... drafts ]
```

*The 10 character string is used to describe the file/directory permissions for each user-group; the user groups are as follows: 'user', 'group', 'other' -- the 'user' group defines the individual user, the 'group' group defines the workgroup or several users and the 'other' group defines every user that has access to the network system. The 10-character string defines permissions for each user group. The first character defines whether the item is a file or directory with a 'd' for directory or a '-' for a file. The remaining nine characters of the string, represent the user group permissions -- the first three characters describe the read, write and executable permissions for the user with an r/w/x or a '-', the next three characters describe the group permissions and the last three characters represent the other permissions.*

## Change file permissions

```
[ chmod o-rw ./project_k.txt ] //removes read and write permissions from project_k.txt
```

## Change file permissions on a hidden file

```
[ chmod g-w ./project_x.txt ]
```

## Change directory permissions

```
[ chmod g-x ./drafts ]
```

## Summary

[ The above commands show how access authorization can be changed using the bash shell in Linux. Using the **ls -l** command to view the permissions of all files and directories within the current directory; whereas the command **ls -la** includes hidden files and directories. As shown above, the **chmod** command allows for changing authorization modes with shorthand syntax called symbology, the arguments being u for user, g for group and o for other an analyst is able to add to or take away permissions or even set the permissions definitely with the =operator. ]