Using Linux as your operating system allows you to easily provide access to many users simultaneously. However, that access also presents potential security risks. Understanding the variety and types of Linux file permissions for users and groups will ensure that your system is optimally secure.

**What are the three permission groups?**

There are three options for permission groups available to you in Linux. These are

* **owners**: these permissions will only apply to owners and will not affect other groups.
* **groups**: you can assign a group of users specific permissions, which will only impact users within the group.
* **all users**: these permissions will apply to all users, and as a result, they present the greatest security risk and should be assigned with caution.

**What are the three kinds of file permissions in Linux?**

There are three kinds of file permissions in Linux:

* **Read (r)**: Allows a user or group to view a file.
* **Write (w)**: Permits the user to write or modify a file or directory.
* **Execute (x)**: A user or grup with execute permissions can execute a file or view a directory.

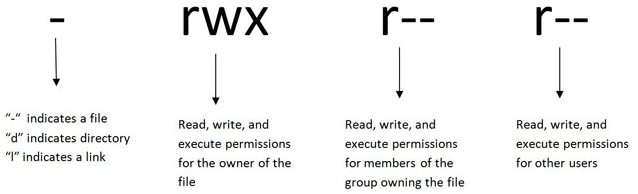
**How do I change directory permissions in Linux?**

To change directory permissions in Linux, use the following:

* **chmod +rwx** filename to add permissions
* **chmod -rwx** directoryname to remove permissions.
* **chmod +x** filename to allow executable permissions.
* **chmod -wx** filename to take out write and executable permissions.

Note that “r” is for read, “w” is for write, and “x” is for execute.

This only changes the permissions for the owner of the file.



To change directory permissions for everyone, use “u” for users, “g” for group, “o” for others, and “ugo” or “a” (for all).