# Standard Access

Standard access is granted by default on the projects, these are the base roles. These Custom are created at org level once, whenever a new project is provisioned these roles will be inherited from org. Even if the roles are inherited and available in the projects, they won't be assigned to users unless we do. Roles can be granted to an individual user, group or a service account.

These 3 are the roles,

1. Admin Role
2. Developer Role
3. Viewer Role

## Admin Role

Admin role grants full access to all fedramp approved services. This role lets users create, update and delete resources.

## Developer Role

This role grants the same access as the admin role except that it won’t let users delete the resources. This roles is suitable for developers

## Viewer Role

As the name suggests this role grants access to readonly access. It is suitable for the users that need to monitor something, validate resources and their configurations.

# Ad Hoc Access

Ad Hoc access is granted on a need only basis. There may be situations where the base roles are not enough for the users. They may be exploring something, doing research etc. as such, they would want higher permissions or permissions on a different service.

In these cases, if the user gets an approval from their manager/project owner, access can be provided.