


# Package permissions

By default, all packages in the project can be reviewed and modified by any Teamwork Cloud user.

There are two levels of permissions:

- The **Global permission** specifies which permission is applied for all project packages for all users:
  - Select **Read-Write** as the **Global permission** to allow editing of the entire model.
  - Select **Read-Only** as the **Global permission** to restrict editing of the entire model.


 Global permissions can be overridden by package permissions:

- **Package permissions** specify the permissions applied to a particular package for a particular user. If no permission is specified for the package, the global permission is used. If the global permission is **Read-Only**, the package permissions can be overridden by a package with **Read-Write** permission. This allows the user/group to edit the package, whereas editing the rest of the model is restricted.

If you want to restrict editing of a package for a specific user or user group, you can easily do this by [modifying the package permissions](#). You can modify package permissions if you have the **Manage model permissions** permission on that project. Select:

- **Read-Only** to restrict editing of the package for the selected user.
- **Read-Write** to allow editing of the package for the selected user.

By default, **Read-Write** as the **Global permission** is assigned to the project and the **Read-Only** permission is assigned to the package.

 **Project-level and package-level permissions**  
The TWCloud project-level **Read-Write Permissions** can be overridden by package permissions. For example, if a user was granted project-level **Read-Write** permissions, but was assigned **Read-Only** permissions for a particular package, that user will not be allowed to make changes to the elements owned by the package and the package itself.

## Permissions conflict logic

There are some cases when **Read-Only** permissions or package permissions conflict, and these cases and the final outcome are described below:

1. If the user belongs to two groups and one group is granted Read-Only permission, while another group - Read-Write permission. In this permission conflict, the user will be granted with higher permission, which is Read-Write permission.
2. User is granted different permissions through the Users and Groups tabs, if permissions are different, User permission wins.
3. If permission is granted simultaneously for both users and groups, then this permission will be granted for standalone users and for users within the selected groups.
4. In case of nested packages with each having different permissions (Read-Only/Read-Write), owned element modification mode is decided from the closest root package permissions in the tree.

### Related pages

- [Setting package permissions](#)