Permissions

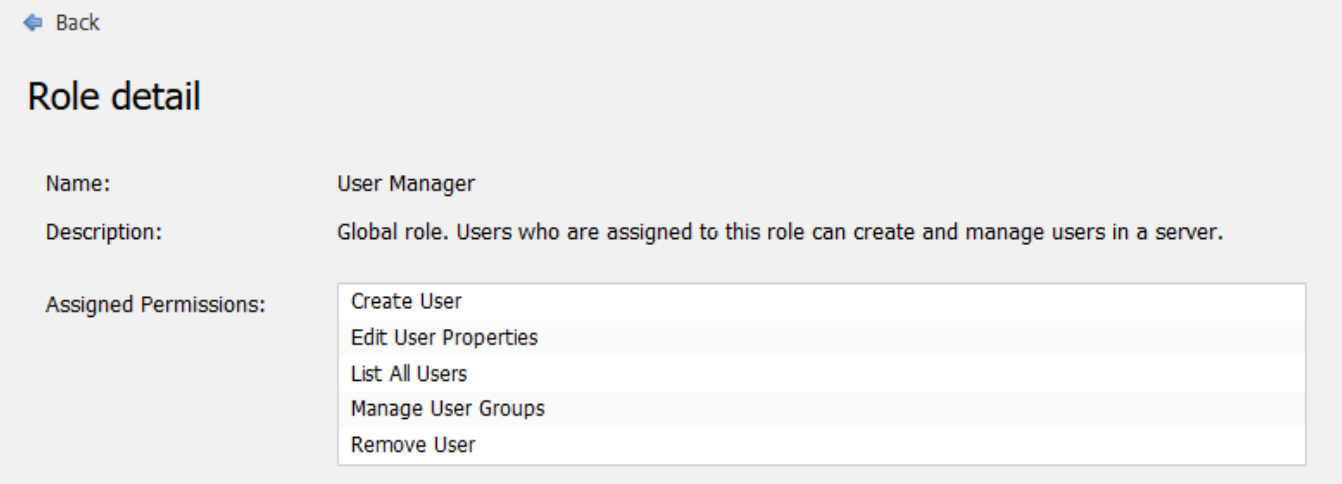
On this page

A permission in Teamwork Cloud Admin (TWAdmin) is an approval to perform a particular task or access one or more data or resource objects in the system. Permissions are associated with roles. A role contains a set of permissions allowing the user with that role to perform specific tasks or work on a resource. For example, a Resource Contributor (Role) has permissions to edit, read resources, or edit resource properties. The permissions enable that role to perform specific operations that are forbidden to other users.

Some permissions can only be used once a role has been assigned a resource, such as a resource reviewer role whose permission allows him to view or read data in a resource. If no resource is assigned to this role, the resource reviewer cannot access the data. You can assign one or more permissions to a custom role.

Note
You cannot directly assign the permissions to the user. You must assign permissions to a role first and then assign the role to a user.

The **Role detail** page in TWAdmin allows you to see all permissions for each role. As an example, the figure below shows the permissions of the User Manager role, which include creating, editing, listing, and removing users.



The role's permissions on the Role detail page of TWAdmin.

Some types of permission do not require you to specify which protected objects you want to assign them to. For example:

- **Read Resources** either specifies which resource to read or assigns resources by selecting **Global** as the scope of the role.
- **Create Resources** does not require a specific resource to create because this permission belongs in the **Global** role scope by default. This permission can be used to create any resource.

For more information about the scopes of role, see Scopes of roles.

Role's permission

We use permissions to protect data such as files or information in TWAdmin and to limit what a user can read, write, and execute within the system. A user can have many roles and a role can have many users. The table below lists all permission types that belong in each preexisting role in the TWCloud system.

Role	Permissions
Resource Contributor	• Edit Resource Properties. • Edit Resources. • Read Resources.

Resource Creator	• Categorize Resources. • Create Resources. • List All Resources.
Resource Locks Administrator	• Read Resources. • Release Resource Locks.
Resource Manager	• Administer Resources. • Edit Resource Properties. • Edit Resources. • List All Users. • Manage Model Permissions. • Manage Owned Resource Right. • Read Resources. • Remove Resource.
Resource Reviewer	• Read Resources.
Security Manager (Global role)	• List All Resources. • List All Users. • Manage Security Roles. • Manage User Permissions.
Server Administrator (Global role)	• Configure Server.
User Manager (Global role)	• Create Users. • Edit User Properties. • List All Users. • Manage User Groups. • Remove User.

If a user has more than one permission type, the permission types will be merged to the user's assigned permissions. For example, if you assign the following:

- role_A to read resource_A only.
- role_B to edit resource_A only.

This user will be able to read and edit resource_A.

> **Note**
> If a user with the Resource Creator role creates a resource, that user will be assigned as the Resource Manager for that particular resource.

Permission description

The following table describes predefined permissions and the possible role scope for each permission type.

> To be able to read-write resources, the user must have the Edit Resources and Edit Resource Properties permissions, otherwise user will see resources as read-only.

Permission	Description	Scope

Administer Resources	The user is required to have also the Edit Resources and Edit Resource Properties permissions to enable listed actions, otherwise resource will be read-only. The user with these three permissions can: • Use local and server resources • Stop using resources in the resource (including Standard/System Profiles) • Lock/Unlock usages. Change versions of used resources • Reload usages from a local file • Import usage to a resource • Migrate resources to a newer version • Upgrade resources to new versions of Standard/System Profiles • Set a resource as the latest • Export packages to a new resource • Reset element IDs (reset resource IDs) • Create a branch • Remove a branch • Rename a branch	Global /Resource
Edit Resources	The user with this permission can edit the resource contents. This includes the ability to change or augment the model.	Global /Resource
Edit Resource Properties	The user with this permission can edit resource properties, change the name or description of the resource.	Global /Resource
List All Resources	The user with this permission can see all resources and access them.	Global
Read Resources	The user with this permission can read the resource contents. This includes the ability to open resources and review the models.	Global /Resource
Release Resource Locks	The user with this permission can release other users locks in a resource.	Global /Resource
Create Resource	The user with this permission can create resources. This also includes the ability to add the resources to the server.	Global
Remove Resource	The user with this permission can delete resources.	Global /Resource
Manage Model Permissions	The user with this permission can manage model-level permissions. This permission automatically includes the permission List all users.	Global /Resource
Manage Owned Resource Access Right	The user with this permission can manage resource-specific access rights, including the ability to grant or revoke user roles in the limited resource scope. This permission automatically includes the permission List all users.	Global /Resource
Categorize Resources	The user with this permission can categorize resources, including the ability to create, delete, or edit existing categories.	Global
Create User	The user with this permission can create new server users.	Global
List All Users	The user with this permission can see all Users.	Global
Remove User	The user with this permission can delete users.	Global
Edit User Properties	The user with this permission can edit user details.	Global
Manage User Permissions	The user with this permission can manage user-level permissions, including the ability to grant or revoke roles in unlimited scope.	Global
Configure Server	The user with this permission can configure server settings, including the ability to configure a secured connection, LDAP connection, and manage server licenses.	Global
Manage User Groups	The user with this permission can manage User groups, including the ability to create, edit, or delete user groups.	Global
Manage Security Roles	The user with this permission can manage security roles, including the ability to create, edit, or delete security roles.	Global

Related pages

- User categories