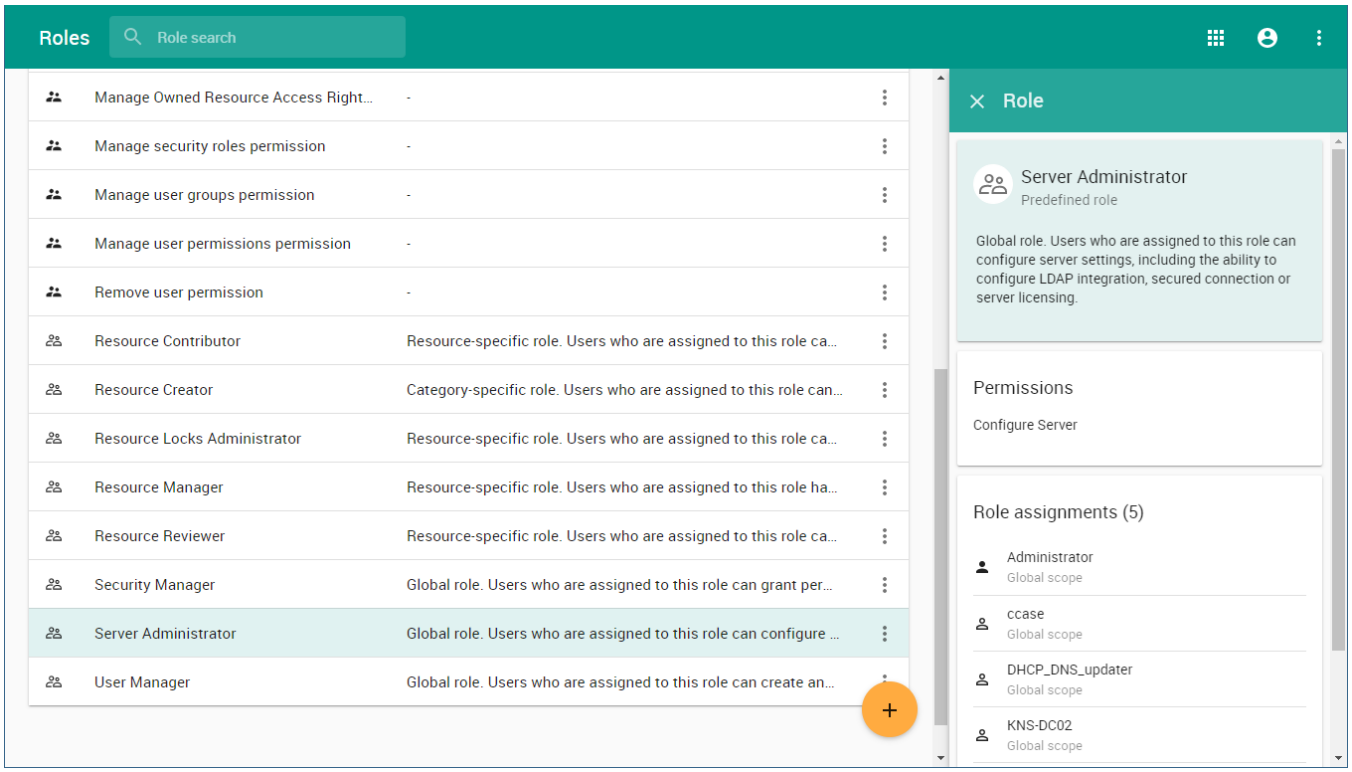
Permissions

A permission in Teamwork Cloud 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 a 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.

> **Assigning permissions**
>
> You cannot directly assign permissions to a user. You must assign permissions to a role first and then assign the role to a user.

When you select a role in the Roles application, you can see its details and the permissions assigned to it. The figure below shows the permissions of the **Server Administrator** role.



The details of the selected role are displayed on the right-hand pane of the Roles application.

The table below describes all default roles and their permissions.

Role	Permissions	Description	Scope
Resource Contributor	Edit Resources	The user with this permission can edit the resource contents. This includes the ability to change or augment the model.	Global /Resource specific
	Edit Resource Properties	The user with this permission can edit resource properties, or change the name or description of the resource.	Global /Resource specific
	Read Resources	The user with this permission can read the resource contents. This includes the ability to open and review models.	Global /Resource specific
Resource Creator	Create Resource	The user with this permission can create resources. This also includes the ability to add resources to the server.	Global /Category specific
	Manage Categories	The user with this permission can categorize resources, including the ability to create, delete, or edit existing categories.	Global /Category specific
Resource Locks Administrator	Read Resources	The user with this permission can read the resource contents. This includes the ability to open and review models.	Global /Resource specific

	Release Resource Locks	The user with this permission can release other users' locks in a resource.	Global /Resource specific
Resource Manager	Administer Resources	The user is required to also have the Edit Resources and Edit Resource Properties permissions to enable listed actions, otherwise the resources 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 • Update resources from a local file • 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 specific
	Edit Resources	The user with this permission can edit the resource contents. This includes the ability to change or augment the model.	Global /Resource specific
	Edit Resource Properties	The user with this permission can edit resource properties, or change the name or description of the resource.	Global /Resource specific
	List All Users	The user with this permission can see all users.	Global
	Manage Model Permissions	The user with this permission can manage model-level permissions. This permission automatically includ es the List All Users permission.	Global /Resource specific
	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 List All Users permission.	Global /Resource specific
	Read Resources	The user with this permission can read the resource contents. This includes the ability to open and review models.	Global /Resource specific
	Remove Resource	The user with this permission can delete resources.	Global /Resource specific
Resource Reviewer	Read Resources.	The user with this permission can read the resource contents. This includes the ability to open and review models.	Global /Resource specific
Security Manager (global role)	List All Resources	The user with this permission can see all resources and access them.	Global
	List All Users	The user with this permission can see all users.	Global
	Manage Security Roles	The user with this permission can manage roles, including the ability to create, edit, or delete roles.	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
Server Administrator (global role)	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
User Manager (global role)	Create User	The user with this permission can create new server users.	Global
	Edit User Properties	The user with this permission can edit user details.	Global
	List All Users	The user with this permission can see all users.	Global
	Manage User Groups	The user with this permission can manage user groups, including the ability to create, edit, or delete user groups.	Global
	Remove User	The user with this permission can delete users.	Global

Important

- If a user with the Resource Creator role creates a resource, that user will be assigned as the Resource Manager for that particular resource.
- To be able to read-write resources, the user must have the Read Resources, Edit Resources, and Edit Resource Properties permissions. Otherwise, the user will see resources as read-only.

Related pages:

- Types of roles
- Scopes of roles