

# Permissions

On this page

- [Default roles and their permissions](#)
- [Downloading permissions report](#)

Permission in Magic Collaboration Studio 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 permission to edit and 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.

Roles

Role search

Name ↑	Description
Data Markings Manager	Global role. Users who are assigned to this role c...
Index Manager	Resource-specific role. Users who are assigned t...
Resource Contributor	Resource-specific role. Users who are assigned t...
Resource Creator	Category-specific role. Users who are assigned t...
Resource Locks Administrator	Resource-specific role. Users who are assigned t...
Resource Manager	Resource-specific role. Users who are assigned t...
Resource Reviewer	Resource-specific role. Users who are assigned t...
Resource Synchronization Manager	Category-specific role. Users who are assigned t...
Security Audit Manager	Global role. Users who are assigned to this role c...
Security Manager	Global role. Users who are assigned to this role c...
<b>Server Administrator</b>	Global role. Users who are assigned to this role c...
Simulation Manager	Global role. Users who are assigned to this role c...
User Manager	Global role. Users who are assigned to this role c...

Role

**Server Administrator**  
Predefined role

Global role. Users who are assigned to this role can configure server settings, including the ability to configure LDAP integration, secured connection or server licensing.

Permissions

Configure Server

Role assignments (36)

aaE15  
Global scope

ABC  
Global scope

ABE20  
Global scope

ABS8  
Global scope

Administrator  
Global scope

CHANGE

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

## Default roles and their permissions

The table below describes all default roles and their permissions.

Role	Permissions	Description	Scope
------	-------------	-------------	-------

<b>Index Manager</b>	Administer Resources	<p>The user must also have the Edit Resources and Edit Resource Properties permissions to enable listed actions; otherwise, the resources will be read-only.</p> <p>The user with these three permissions can:</p> <ul style="list-style-type: none"> <li>• Use local and server resources</li> <li>• Stop using resources in the resource (including Standard/System Profiles)</li> <li>• Lock/Unlock usages. Change versions of used resources</li> <li>• Update resources from a local file</li> <li>• Reload usages from a local file</li> <li>• Import usage to a resource</li> <li>• Migrate resources to a newer version</li> <li>• Upgrade resources to new versions of Standard/System Profiles</li> <li>• Set a resource as the latest</li> <li>• Export packages to a new resource</li> <li>• Reset element IDs (reset resource IDs)</li> <li>• Create a branch</li> <li>• Remove a branch</li> <li>• Rename a branch</li> </ul>	Global /Resource specific
	List All Resources	The user with this permission can see all resources and access them.	Global /Resource specific
<b>Data Markings Manager</b>	Mark Data	The user with this role can mark or unmark Users, User Groups, Resources, and Categories with predefined clearance and classification levels.	Global
<b>Resource Contributor</b>	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
<b>Resource Creator</b>	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
<b>Resource Locks Administrator</b>	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
<b>Resource Manager</b>	Administer Resources	<p>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.</p> <p>The user with these three permissions can:</p> <ul style="list-style-type: none"> <li>• Use local and server resources</li> <li>• Stop using resources in the resource (including Standard/System Profiles)</li> <li>• Lock/Unlock usages. Change versions of used resources</li> <li>• Update resources from a local file</li> <li>• Reload usages from a local file</li> <li>• Import usage to a resource</li> <li>• Migrate resources to a newer version</li> <li>• Upgrade resources to new versions of Standard/System Profiles</li> <li>• Set a resource as the latest</li> <li>• Export packages to a new resource</li> <li>• Reset element IDs (reset resource IDs)</li> <li>• Create a branch</li> <li>• Remove a branch</li> </ul>	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 includes 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
<b>Resource Synchronization Manager</b>	Create Resource	The user with this permission can create resources. This also includes the ability to add resources to the server.	Category-specific
	Manage Categories	The user with this permission can categorize resources, including the ability to create, delete, or edit existing categories.	Category-specific
	Administer Resources	<p>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.</p> <p>The user with these permissions can:</p> <ul style="list-style-type: none"> <li>• Use local and server resources</li> <li>• Stop using resources in the resource (including Standard/System Profiles)</li> <li>• Lock/Unlock usages. Change versions of used resources</li> <li>• Update resources from a local file</li> <li>• Reload usages from a local file</li> <li>• Import usage to a resource</li> <li>• Migrate resources to a newer version</li> <li>• Upgrade resources to new versions of Standard/System Profiles</li> <li>• Set a resource as the latest</li> <li>• Export packages to a new resource</li> <li>• Reset element IDs (reset resource IDs)</li> <li>• Create a branch</li> <li>• Remove a branch</li> </ul>	Category-specific
<b>Resource Reviewer</b>	Read Resources	The user with this permission can read the resource contents. This includes the ability to open and review models.	Global /Resource specific
<b>Security Audit Manager (global role)</b>	Access Reports	Users with this permission can access the Reports application.	Global
<b>Security Manager (global role)</b>	Configure Data Markings	The user with this permission can see the Data markings menu item in the Settings application.	Global
	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
<b>Server Administrator (global role)</b>	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
<b>User Manager (global role)</b>	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



- 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.
- To work with webhooks, a user needs the following permissions: Read Resources (global or resource-specific), Configure Server, and Administer Resources (global or resource-specific). With resource-specific permissions, the user can create and/or see the webhooks created for the resources that this user can read.

## Downloading permissions report


You can download a user's permission report and view the permissions they were assigned in Excel format.

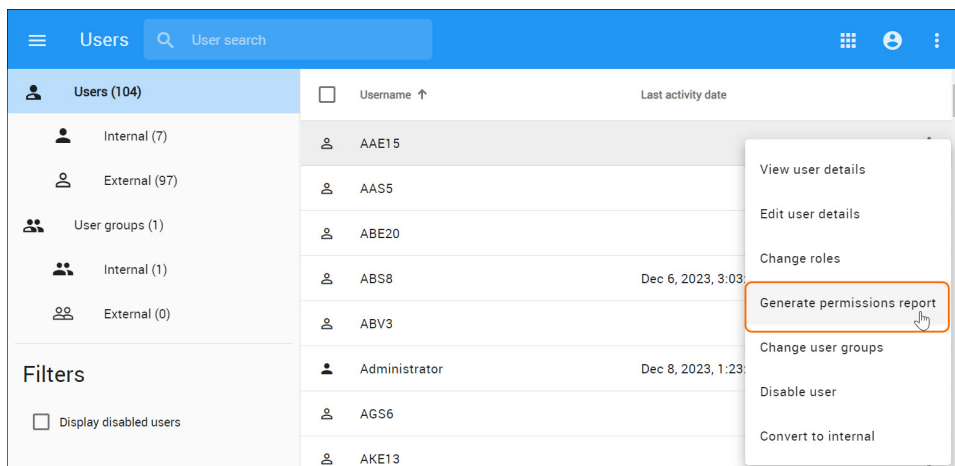



To download the permissions report, you must have the following permissions: **List All Resources**, **Manage Security Roles**, and **Manage User Permissions**.

To download the permissions report

Do one of the following:

- In the **Users** application, click  next to the user and select **Generate permissions report**.



- In the **My account** application, click  at the bottom left corner to download the report.

Related pages

- [Types of roles](#)
- [Scopes of roles](#)