Role permission reference

March 28, 2023 • Jan Cerman and Martina Farkasova • 5 min read

When setting up your team in Kontent.ai, you create roles in your project and choose from several permissions. Each permission defines what your users can do within a project.

This reference explains what each permission enables users to do.

Content production

The *View* permission allows users to:

- View content items in the project.
- Move content items through their workflow (also depends on your workflow setup).
  - Publish content items.
  - Unpublish and archive content.
  - Cancel scheduled content items.
- View and compare older versions of content items.
- Assign contributors to content items.
- Set due dates for content items.
- Add notes.
- Add comments and suggestions.
- Add, edit, and resolve tasks.
- Access Your content, Project overview, and Editorial calendar tabs.
- Access the Relations tab.

The *Edit* permission allows users to:

- Edit content items.
- Work with item versions (also depends on your workflow setup).
  - Create new versions of content items.
  - Restore older versions of content items.
  - Discard the latest versions of content items.
- Work with custom elements used in content items.
- Insert components to content items.
- Approve suggestions.
- View all assets in the project.
- Add, modify, and delete assets.
- Assign taxonomy terms to assets.

The *Create* permission allows users to:

- Create new content items.
- Duplicate content items.

- Create new language variants of content items.
- Convert components to items.

The *Delete* permission allows users to:

- Delete content items.

Restrict access to specific content

You can allow users to work with all content or only the content items assigned to them. The role can be further defined by setting which specific content types and content groups the role can work with.

If there are specific content types and content groups that you don't want the role to work with, **exceptions** can be added to the role.

Active permissions and workflows

The content capabilities of a given role can be further restricted by your project's content workflows setup. For each workflow step, you can limit which roles can work on content in the given step and move it to the following steps.

For example, if you want only Project managers to be able to publish content:

1. Set up your workflow steps so that only a single step transitions to the *Published* step; for example, a step named *Approved*.
2. Limit the *Approved* workflow step to the *Project manager* user role.

For a more thorough example of using roles and workflow together, see the example of setting up a common production flow.

Multiple workflows and restrictions on the first workflow step

If you have multiple workflows enabled in your project, role restrictions on the first workflow step work a bit differently.

When a user creates a content item in a workflow where they can't work with the first step, the item gets created in the first step anyway but the user can't work with the item because of their role permissions.

In case you don't have multiple workflows enabled, users whose role can't work with the first workflow step create content items in the first step they can work with.

Content model

The *Manage content types, asset type, and snippets* permission allows users to:

- View content types, content type snippets, and asset type.
- Add, modify, and delete content types.
- Add, modify, and delete content type snippets.

- Duplicate content types.
- Add, modify, and delete the asset type.

The *Manage taxonomy* permission allows users to:

- View taxonomy groups and terms.
- Add, modify, and delete taxonomy groups and terms.

The *Manage sitemap* permission allows users to:

- Add, modify, and delete sitemap items.

Settings

The *Manage environment* permission allows users to:

- Create new environments.
- Manage environments.
- Delete the environments in which the users are active.

The *Invite and manage project members* permission allows users to:

- Invite and deactivate users.
- Assign roles to users.

The *Manage custom roles* permission allows users to:

- Add, modify, and delete custom roles.

The *Manage workflow steps* permission allows users to:

- View the project's content workflow settings.
- Add, modify, and delete workflows and their workflow steps.
- Reorder steps in workflows.

The *Manage spaces* permission allows users to:

- Add, modify, and delete spaces.

The *Manage collections* permission allows users to:

- View and configure the project's collection settings.

The *Manage localization* permission allows users to:

- View the project's localization settings.
- Add and configure project languages.

The *Manage APIs* permission allows users to:

- View API keys and use the Kontent.ai APIs.

The *Manage development settings* permission allows users to:

- View and modify the codenames of content items.
- View and modify preview URLs.
- View, add, modify, and delete webhooks.
- Set a default Home item in the Relations tab for every user in the environment.

The *Access audit log* permission allows users to:

- View activity logs in the audit log.

What's next?

Set up a common production flow for your project and see how roles and content workflows can work together to your team's benefit.