Users, Groups and Roles

Your content management system requires different types of users. You need to create a different group for each type of user and then assign those groups different roles within your system.

- Web content management roles
  You define the access of a user or group for a library to determine who has access to a library, and to define access to the different views within the authoring portlet.
- User roles and access
  Different users will have different access to items and functions in your system depending on the role they are assigned. Roles can be assigned at the library level, and also assigned on individual items.
- Security architecture
  The security architecture describes what groups are required for your site and what access is required for different groups to the authoring portlet and rendered website.

User roles and access

Different users will have different access to items and functions in your system depending on the role they are assigned. Roles can be assigned at the library level, and also assigned on individual items.

Assigning access to items

There are two methods that are used to assign roles to access controls on items:

- Selecting users or groups directly in the access section of an item.
- Allowing assigned roles to be inherited from parent items up to and including the library. Access roles are inherited in the following hierarchies:
  - Library/site area/content item
  - Library/taxonomy/category
  - Library/folder/component
  - Library/folder/authoring template
  - Library/folder/presentation template
  - Library/workflow
  - Library/workflow stage
  - Library/workflow action

  You can stop inheritance at any point in an inheritance hierarchy. For example, you might allow inheritance down to a site area, but assign access roles manually for each content item under that site area.

  Inheritance from a library is based on the role that is assigned to the overall library, not on the role that is assigned to specific item types. For example, you might not have access to the presentation template view on a library, but if you inherit the role of editor to a presentation template, you are able to view and edit that presentation template from the All Items view.

  Inheritance does not apply to draft items.

Note

By default, inheritance is enabled for all roles and items.

Viewing an item's security settings

The following sections are displayed on the security section of each item.

Table 1. Security settings

Section	Details
User Defined	If the item is not participating in a workflow, the user can edit access under user-defined.
Workflow	If an item is participating in a workflow, then the user-defined option does not appear and the workflow settings are displayed. This cannot be edited. Workflow-defined access is set in workflow stages. Published items and workflow defined item security • If you grant a user editor access to an item in a workflow stage that uses a publish action, then those users are able to edit the published item directly. No draft is created. The same is true for administrator defined security when applied to published items. • If you grant a user manager access to an item in a workflow stage that uses a publish action, then those users are able to edit and delete the published item directly. No draft is created. The same is true for administrator defined security when applied to published items. • If you grant a user reviewer access to an item in a workflow stage that uses a publish action, then those users are able to create drafts of the published item.
Administrator Defined	Administrators can edit user access to an item at any time by changing the administrator defined settings.
Inheritance	You can also choose to inherit access that is assigned in the current web content library, or from an item's parent. Inheritance for all user roles is enabled by default.

How security is set

When a new item is created, the creator is automatically given manager access to the item. Extra user and group security can be added in the user-defined and system defined settings.

If an item is participating in a workflow, the creator is given manager access to the item only in the first workflow stage. As the item progresses through a workflow, the item security is determined by the combined workflow and system defined security.

Table 2. Security matrix

Security level	No workflow	First workflow stage	Extra workflow stages
User	• User defined • Administrator defined • Inherited	• Administrator defined • Workflow defined	• Administrator defined • Workflow defined
Contributor			
Editor			
Manager			
Reviewer			

Security level	No workflow	First workflow stage	Extra workflow stages
Draft Creator			
Administrator	If you are assigned the administrator role to a library, you automatically inherit all administration access down to the item-level. It cannot be turned off.	If you are assigned the administrator role to a library, you automatically inherit all administration access down to the item-level. It cannot be turned off.	If you are assigned the administrator role to a library, you automatically inherit all administration access down to the item-level. It cannot be turned off.

Deleting items

When a new item is created, the creator can also delete the item. If an item is participating in a workflow, the creator can delete the item in the first workflow stage only.

Assigning access to different types of users or groups

When you access a website or rendering portlet, users login as either anonymous users, or authenticated portal users.

The following user and groups can be used to grant access to items.

Table 3. Users and groups

User or group	Details
anonymous portal user	Select this user to grant access to anonymous users
[all users]	Select this group to grant access to all users, anonymous and authenticated.
[all authenticated portal users]	Select this group to grant access to all authenticated users.
[all portal user groups]	Select this group to grant access to all user groups.
[creator]	Select this group to grant access to the creator of the item.
[authors]	Select this group to grant access to users who are selected as an "author" of the item.
[owners]	Select this group to grant access to users who are selected as an "owner" of the item.

The access required to view a rendered item

To view an item on a rendered page, you need the following:

1. You need at least user access to the library the item is stored in.
2. You need at least user access to the presentation template used to display the current content item.
3. There must be a valid template map.
4. You must have sufficient access to view the item itself.

   Rendered item behavior varies depending on how you specify the `wcm.path.traversal.security` property in the `WCM WCMConfigService` service. If the property is not specified, the default value is `false`.

   If set to `false`:

   - Menus display content regardless of whether a user has access to all site areas in the content path.

- Navigators do not display site areas a user does not have access to, but can show content under these site areas in specific circumstances such as within breadcrumb navigators.
- URLs are only checked for content access, not site area access.

If set to `true`:

- Menus and navigators do not display content under secure site areas if the user does not have access to all site areas in the content path.
- Directly accessing content under secure site areas using a URL fails if the user does not have access to all site areas in the content path.

Rendering performance is slower if set to true.

Button access

You assign item-level access by assigning users and groups different roles for each item. The role that you assign determines what actions a user has access to for each item. The following table describes the minimum access that is required for access to each button in the user interface. If you enable inheritance at the library level, the library access level is inherited by item level access by default. For example, giving a user editor access to a library is automatically applied to new items they create if inheritance is enabled.

Table 4. Item access controls

Actions	Minimum item access	Minimum role access to library resources	Minimum library access	Item status
Add or move children	Contributor access or higher.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.
Add or remove child links	Contributor access or higher.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.
Add or remove workflows	Manager access or higher.	When first created, you require manager access to the library resource in any library. When saved, you require manager access to both the item and library resource in the library the item is stored in.	Contributor access or higher.	N.A.
Add to project (Non-workflowed items or existing draft) You will also need read access to the project, and access to at least one draft or	Editor access or higher.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.

Actions	Minimum item access	Minimum role access to library resources	Minimum library access	Item status
published item.				
Add to project (Workflowed items) You will also need read access to the project, and access to at least one draft or published item.	Draft Creator access on the current stage required to create a draft, and editor access or higher on the first stage of the workflow required to add the draft to project.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.
Apply authoring template (authoring portlet)	N.A.	Manager access or higher to the authoring template library resource. Note This default behavior can be changed to allow all users to apply authoring templates to items they have edit access to. See Web content authoring options for further information.	Manager access or higher.	N.A.
Apply authoring template (content form)	Editor access or higher.	Contributor access or higher to the authoring template library resource.	Contributor access or higher.	N.A.
Approve	Reviewer or administrator.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.
Approve Project	Reviewer.	Not required.	Contributor access or higher.	N.A.
Batch-edit access controls	Editor access or higher.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.
Cancel draft	Manager access or higher. Editor access or higher for system workflow.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.
Copy	Contributor access or	Editor access or	Contributor	N.A.

Actions	Minimum item access	Minimum role access to library resources	Minimum library access	Item status
	higher.	higher to the library resource type.	access or higher.	
Create draft (Workflowed items)	Draft Creator access or higher.	Editor access or higher to the library resource type.	Contributor access or higher.	Only published or expired items.
Create draft (Non-workflowed items)	Editor access or higher.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.
Delete	Manager access or higher.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.
Edit	Editor access or higher.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.
Expire	Reviewer access.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.
Generate	Contributor access or higher.	Editor access or higher to the library resource types of Components, Authoring Templates, Presentation Templates, Content, and Site Areas.	Contributor access or higher.	N.A.
Link to	Contributor access or higher, or Reviewer access.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.
Manage elements (In site areas and content items, not authoring templates.)	Administrator access If the Allow elements to be managed by editors option is selected on the authoring template that is used by an item, then this button is enabled for users with Editor access or higher. This option is enabled by default on Site Areas that are created by using the default Site Area	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.

Actions	Minimum item access	Minimum role access to library resources	Minimum library access	Item status
	template.			
Move	Editor access or higher.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.
Next Stage	Reviewer access.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.
Preview item and view rendered item	User access or higher, or Reviewer access.	Not required.	Contributor access or higher.	N.A.
Previous Stage	Manager access or higher, or on workflow stages that have been configured to enable Reviewers access to the previous stage button.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.
Process now	N.A.	Not required.	Administrator access	N.A.
Publish Project	Editor access or higher.	Not required.	Not required.	Only when a project is in pending state.
Purge	Manager access or higher.	Not required.	Manager access or higher.	N.A.
Read	User access or higher, or Reviewer access.	Not required.	Contributor access or higher.	N.A.
Reference	User access or higher, or Reviewer access.	Not required.	Contributor access or higher.	N.A.
Reject	Reviewer or administrator access.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.
Reject Project	Reviewer.	Not required.	Contributor access or higher.	N.A.
Restart workflow	Draft Creator access.	Manager access or higher to the library resource type.	Contributor access or higher.	Only published or expired items.
Restore	Editor access or higher.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.
Save version	Editor access or higher.	Editor access or	Contributor	N.A.

Actions	Minimum item access	Minimum role access to library resources	Minimum library access	Item status
		higher to the library resource type.	access or higher.	
Show hidden fields	N.A.	Not required.	Administrator access	N.A.
Submit for review(Workflows)	Reviewer access.	Editor access or higher to the library resource type.	Contributor access or higher.	N.A.
Submit for review (Projects)	Editor access or higher.	Editor access or higher to the library resource type.	Contributor access or higher.	Only when a project is in an active state.
System security	N.A.	Not required.	Administrator access	N.A.
Unlock	Manager access or higher.	Not required.	Manager access or higher.	N.A.
Validate (Projects)	User access or higher.	Not required.	Not required.	Only when a project is in active, review, pending, or publish failed states.
View references	User access or higher, or Reviewer access.	Not required.	Contributor access or higher.	N.A.
View versions	User access or higher, or Reviewer access.	Not required.	Contributor access or higher.	N.A.
Withdraw approval	Reviewer.	Not required.	Contributor access or higher.	Only when a project is in the review state. Only when Joint Approval is selected.
Withdraw from review	Reviewer.	Not required.	Contributor access or higher.	Only when a project is in the review state.

Creating new items

The ability to create new items is set at the library level, not item level. You must have at least contributor access to a library and editor access to an item-type to create a new item. If you have access to create any item type, you can also create folders and projects.

Button access on content items

You can choose to hide selected buttons on content item forms when you create an authoring template. This means that a user may not have access to all buttons on a content item form regardless of their role. Administrators can choose to display hidden buttons if required.

Profiling versus security

Using profiling to personalize a site is different from using security to limit what items a user can access. In a profile-based personalized site, although a user might not be able to access all the pages by using personalized menus, they might still be able to access other pages by using navigators, or by searching for content. In a secured site, a user can only view items that they are granted access to.