

Managing Project Permissions

Project permissions are created within [Permission Schemes](#), which are then assigned to specific projects.

Project permissions are able to be granted based on:

- Individual users
- [Groups](#)
- [Project roles](#)
- Issue roles such as 'Reporter', 'Project Lead' and 'Current Assignee'
- 'Anyone' (e.g. to allow anonymous access)
- A (multi-)user picker [custom field](#).
- A (multi-)group picker [custom field](#). This can either be an actual group picker custom field, or a (multi-)select-list whose values are group names.

The following table lists the different types of project permissions and the functions they secure. Note that project permissions can also be used in [workflow conditions](#).

On this page:

- [Permission Schemes](#)
- [Creating a Permission Scheme](#)
- [Associating a Permission Scheme with a Project](#)
- [Deleting a Permission Scheme](#)
- [Copying a Permission Scheme](#)
- [Global Permissions](#)

Project Permissions	Explanation
Administer Projects	Permission to administer a project in JIRA. This includes the ability to edit project role membership , project components , project versions and some project details ('Project Name', 'URL', 'Project Lead', 'Project Description').
Browse Projects	Permission to browse projects, use the Issue Navigator and view individual issues (except issues that have been restricted via Issue Security). Many other permissions are dependent on this permission , e.g. the 'Work On Issues' permission is only effective for users who also have the 'Browse Projects' permission.
View Development Tools	
View (Read-Only) Workflow	Permission to view the project's 'read-only' workflow when viewing an issue. This permission provides the 'View Workflow' link against the 'Status' field of the 'View Issue' page .
Issue Permissions	Explanation
Assign Issues	Permission to assign issues to users. Also allows autocompletion of users in the Assign Issue drop-down. (See also Assignable User permission below)
Assignable User	Permission to be assigned issues. (Note that this does not include the ability to assign issues; see Assign Issue permission above).

Close Issues	Permission to close issues. (This permission is useful where, for example, developers resolve issues and testers close them). Also see the Resolve Issues permission.
Create Issues	Permission to create issues in the project. (Note that the Create Attachments permission is required in order to create attachments.) Includes the ability to create sub-tasks (if sub-tasks are enabled).
Delete Issues	Permission to delete issues. Think carefully about which groups or project roles you assign this permission to; usually it will only be given to administrators. Note that deleting an issue will delete all of its comments and attachments, even if the user does not have the Delete Comments or Delete Attachments permissions. However, the Delete Issues permission does not include the ability to delete individual comments or attachments.
Edit Issues	Permission to edit issues (excluding the 'Due Date' field — see the Schedule Issues permission). Includes the ability to convert issues to sub-tasks and vice versa (if sub-tasks are enabled). Note that the Delete Issue permission is required in order to delete issues. The Edit Issue permission is usually given to any groups or project roles who have the Create Issue permission (perhaps the only exception to this is if you give everyone the ability to create issues — it may not be appropriate to give everyone the ability to edit too). Note that all edits are recorded in the Issue Change History for audit purposes.
Link Issues	Permission to link issues together. (Only relevant if Issue Linking is enabled).
Modify Reporter	Permission to modify the 'Reporter' of an issue. This allows a user to create issues 'on behalf of' someone else. This permission should generally only be granted to administrators.
Move Issues	Permission to move issues from one project to another, or from one workflow to another workflow within the same project. Note that a user can only move issues to a project for which they have Create Issue permission.
Resolve Issues	Permission to resolve and reopen issues. This also includes the ability to set the 'Fix For version' field for issues. Also see the Close Issues permission.
Schedule Issues	Permission to schedule an issue — that is, to edit the 'Due Date' of an issue. In older versions of JIRA this also controlled the permission to view the 'Due Date' of an issue.
Set Issue Security	Permission to set the security level on an issue to control who can access the issue. Only relevant if issue security has been enabled .
Transition Issues	Permission to transition (change) the status of an issue.
Voters & Watchers Permissions	Explanation
Manage Watcher List	Permission to manage (i.e. view/add/remove users to/from) the watcher list of an issue.
View Voters and Watchers	Permission to view the voter list and watcher list of an issue. Also see the Manage Watcher List permission.
Comments Permissions	Explanation
Add Comments	Permission to add comments to issues. Note that this does not include the ability to edit or delete comments.
Delete All Comments	Permission to delete any comments , regardless of who added them.

Delete Own Comments	Permission to delete comments that were added by the user.
Edit All Comments	Permission to edit any comments , regardless of who added them.
Edit Own Comments	Permission to edit comments that were added by the user.
Attachments Permissions	Explanation
Create Attachments	Permission to attach files to an issue. (Only relevant if attachments are enabled). Note that this does not include the ability to delete attachments.
Delete All Attachments	Permission to delete any attachments , regardless of who added them.
Delete Own Attachments	Permission to delete attachments that were added by the user.
Time Tracking Permissions	Explanation
Work On Issues	Permission to log work against an issue, i.e. create a worklog entry. (Only relevant if Time Tracking is enabled).
Delete All Worklogs	Permission to delete any worklog entries , regardless of who added them. (Only relevant if Time Tracking is enabled). Also see the Work On Issues permission.
Delete Own Worklogs	Permission to delete worklog entries that were added by the user. (Only relevant if Time Tracking is enabled). Also see the Work On Issues permission.
Edit All Worklogs	Permission to edit any worklog entries , regardless of who added them. (Only relevant if Time Tracking is enabled). Also see the Work On Issues permission.
Edit Own Worklogs	Permission to edit worklog entries that were added by the user. (Only relevant if Time Tracking is enabled). Also see the Work On Issues permission.

Permission Schemes

What is a Permission Scheme?

A permission scheme is a set of user/group/role assignments for the project permissions listed above. Every project has a permission scheme. One permission scheme can be associated with multiple projects.

Why Permission Schemes?

In many organisations, multiple projects have the same needs regarding access rights. (For example, only the specified project team may be authorised to assign and work on issues).

Permission schemes prevent having to set up permissions individually for every project. Once a permission scheme is set up it can be applied to all projects that have the same type of access requirements.

Creating a Permission Scheme

1. Log in as a user with the '[JIRA Administrators](#)' [global permission](#).

- Choose **> Issues**. Select **Permission Schemes** to open the Permission Schemes page, which displays a list of all permission schemes in your JIRA system and the projects that use each scheme.
 - Keyboard shortcut: 'g' + 'g' + start typing 'permission schemes'
- Click the 'Add Permission Scheme' link.
- In the 'Add Permission Scheme' form, enter a name for the scheme, and a short description of the scheme. Click the 'Add' button.

Screenshot: The 'Add Permission Scheme' form

- You will return to the 'Permission Schemes' page which now contains the newly added scheme.

Adding Users, Groups or Roles to a Permission Scheme

- Log in as a user with the 'JIRA Administrators' [global permission](#).
- Choose **> Issues**. Select **Permission Schemes** to open the Permission Schemes page, which displays a list of all permission schemes in your JIRA system and the projects that use each scheme.
 - Keyboard shortcut: 'g' + 'g' + start typing 'permission schemes'
- Locate the permission scheme of interest and click its name (or click the 'Permissions' link in the 'Operations' column) to show a list of permissions.

Screenshot: Project Permissions

Project Permissions	Users / Groups / Project Roles	Operations
Administer Projects Ability to administer a project in JIRA.		Add
Browse Projects Ability to browse projects and the issues within them.	• Group (Anyone) (Delete)	Add
View Development Tools Allows users to view development-related information on the view issue screen, like commits, reviews and build information.	• Group (Anyone) (Delete)	Add
View Read-Only Workflow Users with this permission may view a read-only version of a workflow.		Add
Issue Permissions	Users / Groups / Project Roles	Operations
Create Issues Ability to create issues.	• Group (Anyone) (Delete)	Add
Edit Issues Ability to edit issues.	• Group (Anyone) (Delete)	Add
Transition Issues Ability to transition issues.	• Group (Anyone) (Delete)	Add
Schedule Issues Ability to view or edit an issue's due date.	• Group (Anyone) (Delete)	Add
Move Issues Ability to move issues between projects or between workflows of the same project (if applicable). Note the user can only move issues to a project he or she has the create permission for.		Add
Assign Issues Ability to assign issues to other people.	• Group (Anyone) (Delete)	Add

- Click the 'Add' link in the 'Operations' column, which displays the 'Add Permission' page.
- After selecting one or more permissions to add and who to add the selected permissions to, click the 'Add' button. The users/groups/roles will now be added to the selected permissions. Note that [project roles](#) are useful for defining specific team members for each project. Referencing project roles (rather than users or

groups) in your permissions can help you minimise the number of permission schemes in your system.
Screenshot: Add Users To Permissions

Add New Permission

Permission Scheme: **Demo permission scheme**

Please select the type of permission you wish to add to this Permission Scheme

Permissions

- Administer Projects
- Browse Projects
- View Issue Source Tab
- View Read-Only Workflow
- Create Issues
- Edit Issues
- Schedule Issues

(Select the permissions that you want to assign).

Reporter

Group Anyone

Single User Start typing to get a list of possible matches.

Project Lead

Current Assignee

User Custom Field Value Choose a custom field

Project Role Choose a project role

Group Custom Field Value Choose a custom field

- Repeat the last 2 steps until all required users/groups/roles have been added to the permissions.

Deleting Users, Groups or Roles from a Permission Scheme

- Log in as a user with the [JIRA Administrators global permission](#).
- Choose **> Issues**. Select **Permission Schemes** to open the Permission Schemes page, which displays a list of all permission schemes in your JIRA system and the projects that use each scheme.
 - ✔ **Keyboard shortcut:** **g + g +** start typing **permission schemes**
- Locate the permission scheme of interest and click its name (or click the **Permissions** link in the 'Operations' column) to show the list of 'Project Permissions' ([above](#)).
- Click the **Delete** link in the "Users / Groups / Roles" column next to the name of the user, group or project role you wish to delete.

Associating a Permission Scheme with a Project

- Log in as a user with the [JIRA Administrators global permission](#).
- Choose **> Projects**.
 - ✔ **Keyboard shortcut:** **g + g +** start typing **projects**
- Select the project of interest to open the **Project Summary** administration page for that project. See [Defining a Project](#) for more information.
- On the lower right, in the **Permissions** section, click the name of the current scheme (e.g. 'Default Permission Scheme') to display the details of the project's current permission scheme.
- Click the **'Actions'** dropdown menu and choose **'Use a different scheme'**.
- On the 'Associate Permission Scheme to Project' page, which lists all available permission schemes, select the permission scheme you want to associate with the project.
- Click the **'Associate'** button to associate the project with the permission scheme.

Deleting a Permission Scheme

- Log in as a user with the [JIRA Administrators global permission](#).
- Choose **> Issues**. Select **Permission Schemes** to open the Permission Schemes page, which displays a list of all permission schemes in your JIRA system and the projects that use each scheme.
 - ✔ **Keyboard shortcut:** **g + g +** start typing **permission schemes**

3. Click the **Delete** link (in the **Operations** column) for the scheme that you want to delete.
4. A confirmation screen will appear. To delete click **Delete** otherwise click **Cancel**.
5. The scheme will be deleted and all associated projects will be automatically associated with the Default Permission Scheme. (Note that you cannot delete the Default Permission Scheme.)

Copying a Permission Scheme

1. Log in as a user with the **JIRA Administrators** [global permission](#).
2. Choose **> Issues**. Select **Permission Schemes** to open the Permission Schemes page, which displays a list of all permission schemes in your JIRA system and the projects that use each scheme.
 🟢 **Keyboard shortcut:** **g + g** + start typing **permission schemes**
3. Click the **Copy** link (in the **Operations** column) for the scheme that you want to copy.
4. A new scheme will be created with the same permissions and the same users/groups/roles assigned to them.

Global Permissions

This table lists the different global permissions and the functions they secure:

Global Permission	Explanation
JIRA System Administrators	<p>Permission to perform all JIRA administration functions.</p> <p>⚠️ The number of users that count towards your JIRA license is the sum of all users (including users in groups) that have the JIRA System Administrators permission, even if they do not also have the JIRA Administrators or JIRA Users permissions. A user with JIRA System Administrators will be able to log in to JIRA without the JIRA Users permission, but may not be able to perform all regular user functions (e.g. edit their profile) unless they also belong to a group that has the JIRA Users permission.</p>
JIRA Administrators	<p>Permission to perform most JIRA administration functions (see list of exclusions below).</p> <p>⚠️ The number of users that count towards your JIRA license is the sum of all users (including users in groups) that have the JIRA Administrators permission, even if they do not also have the JIRA System Administrators or JIRA Users permissions. A user with JIRA Administrators will be able to log in to JIRA without the JIRA Users permission, but may not be able to perform all regular user functions (e.g. edit their profile) unless they also belong to a group that has the JIRA Users permission.</p>
JIRA Users	<p>Permission to log in to JIRA.</p> <p>⚠️ The number of users that count towards your JIRA license is the sum of all users (including users in groups) that have this permission. If you want to reduce this count, see Updating your JIRA License Details.</p> <p>📘 Granting the JIRA Users permission to a group results in all newly created users being automatically added to that group. The exception to this are groups that also have either the JIRA System Administrators or JIRA Administrators permissions, since JIRA prevents groups with these administrative-level global permissions from being granted the JIRA Users permission. Furthermore, it would be unwise to automatically grant these administrative-level global permissions to all new users.</p>
Browse Users	<p>Permission to view a list of all JIRA user names and group names. Used for selecting users /groups in popup screens. Enables auto-completion of user names in most 'User Picker' menus and popups.</p> <p>Note that the Assign User permissions also allows a limited version of this on a per-project basis.</p>

Create Shared Objects	Permission to share a filter or dashboard globally or with groups of users. Also used to control who can create a JIRA Agile board .
Manage Group Filter Subscriptions	Permission to manage (create and delete) group filter subscriptions.
Bulk Change	<p>Permission to execute the bulk operations within JIRA:</p> <ul style="list-style-type: none"> - Bulk Edit * - Bulk Move * - Bulk Workflow Transition - Bulk Delete * <p>(* subject to project-specific permissions.)</p> <p> The decision to grant the Bulk Change permission should be considered carefully. This permission grants users the ability to modify a collection of issues at once. For example, in JIRA installations configured to run in Public mode (i.e. anybody can sign up and create issues), a user with the Bulk Change global permission and the Add Comments project permission could comment on <i>all</i> accessible issues. Undoing such modifications may not be possible through the JIRA application interface and may require changes made directly against the database (which is not recommended).</p>