Jira Configuring permissions

When configuring security for your Jira application instance, there are two areas to address:

- permissions within Jira applications themselves
- security in the external environment

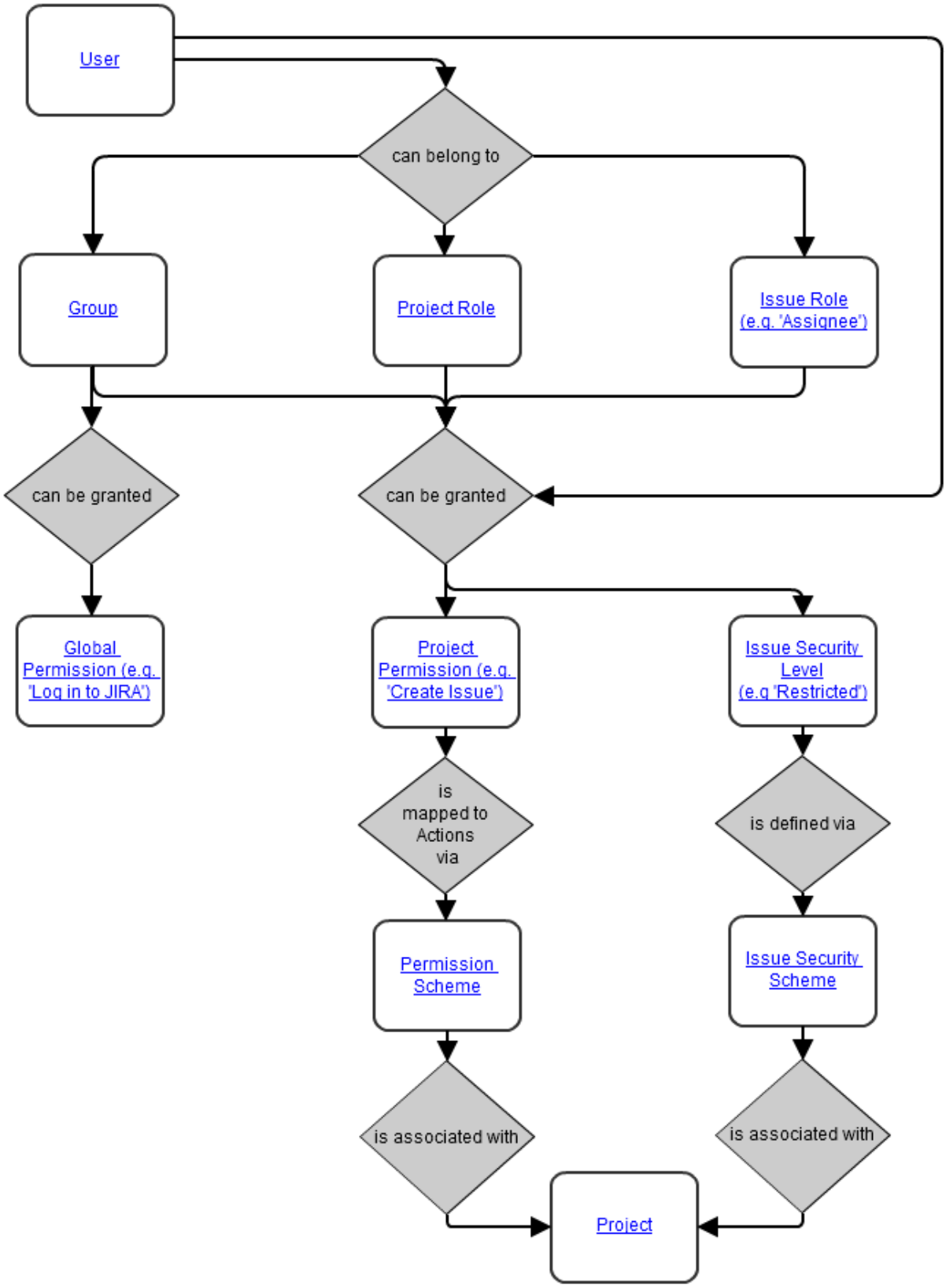
Configuring permissions within Jira applications

Jira applications have a flexible security system which allows you to configure who can access Jira applications, and what they can do/see within them.

There are five types of security levels within Jira applications:

1. Global permissions — these apply to Jira applications as a whole.
2. Project permissions — organized into permission schemes, these apply to projects as a whole (e.g. who can see the project's issues ('Browse' permission), create, edit and assign them).
3. Issue security levels — organized into security schemes, these allow the visibility of individual issues to be adjusted, within the bounds of the project's permissions.
4. Comment visibility — allows the visibility of individual comments (within an issue) to be restricted.
5. Work-log visibility — allows the visibility of individual work-log entries (within an issue) to be restricted. Does not restrict visibility of progress bar on issue time tracking.

Diagram: People and permissions



Configuring security in the external environment

If your Jira application instance contains sensitive information, you may want to configure security in the environment in which your instance is running. Some of the main areas to consider are:

- File system — you should restrict access to the following directories (but note that the user which your instance is running as will require full access to these directories):
    - Index directory
    - Attachments directory
- Database:
    - If you are using an external database as recommended for production systems (i.e. you are not using Jira's internal/bundled H2 database), you should restrict access to the database that your Jira instance uses.
    - If you are using Jira's internal/bundled H2 database, you should restrict access to the directory in which you installed Jira. (Note that the user which your Jira instance is running as will require full access to this directory.)
- SSL — if you are running your Jira instance over the Internet, you may want to consider using SSL.