Authorization

Table of Contents

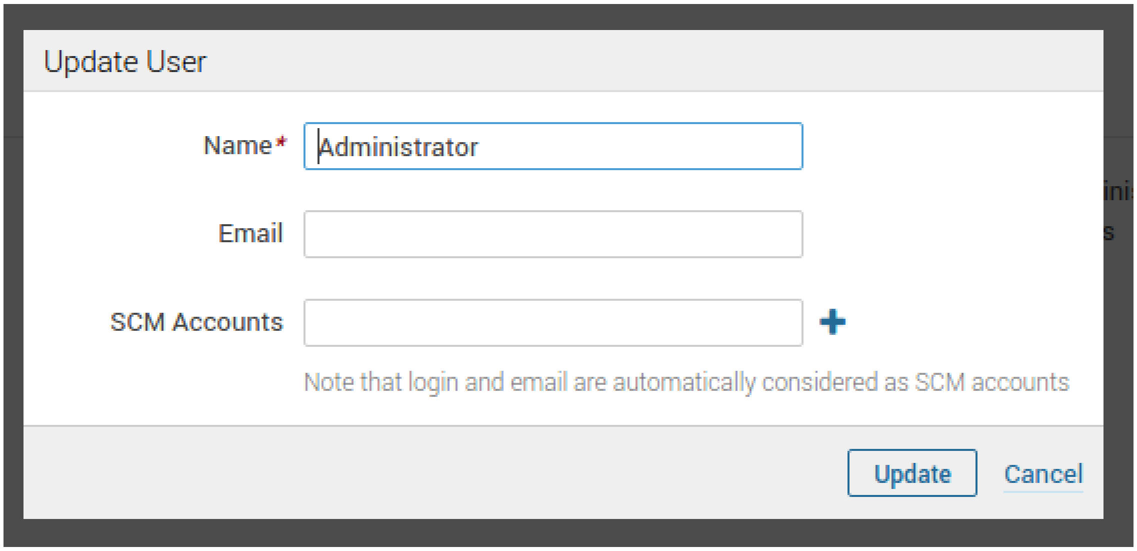
The way authorization is implemented in SonarQube is pretty standard. It is possible to create as many users and groups of users as required in the system. The users can then be attached (or not) to (multiple) groups. Groups and / or users are then given (multiple) permissions. The permissions grant access to projects, services and functionalities.

To administer groups and users, choose **Administration > Security**, and use the sub-menu items.

User

Multiple integrations that allow the delegation of authentication are available (see Plugin Library and Other Plugins), but you can manually create and edit users at **Settings > Security > Users**. For manually-created users, login and password can be set at creation, but not edited afterward by administrators. Manually-created users can edit their passwords.

During both user creation and edit, you can set an account's screen name, email address. User login and email address will be implicitly recognized by the **Issue Assignment** feature as SCM accounts if applicable, but you can set additional SCM accounts explicitly.



Name* Administrator

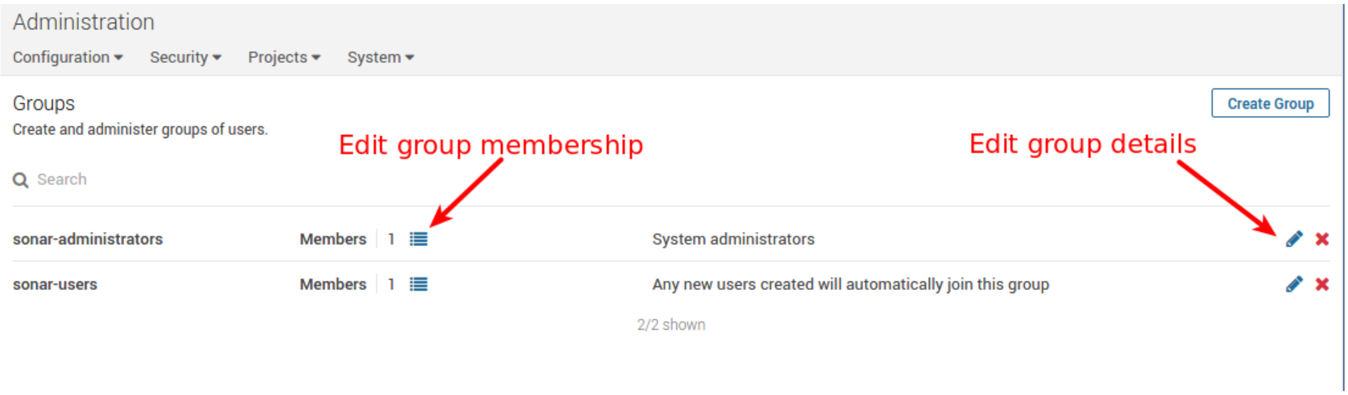
Note that login and email are automatically considered as SCM accounts

Group

A group is a set of users.

To create a new group, go to **Settings > Security> Groups > Add new group**:

To add/remove users to/from a group, click the icon next to the membership total:



Groups

Create and administer groups of users.

Edit group membership

Edit group details

sonar-administrators	Members	1	System administrators
sonar-users	Members	1	Any new users created will automatically join this group

2/2 shown

Two groups have a special meaning:

- **Anyone** is a group that exists in the system, but that cannot be managed. Every user belongs to this group, including *Anonymous user*.
- **sonar-users** is the default group to which users are automatically added. To change it, go to **Settings > General Settings > Security** and set the *Default user group* property.

Global Permissions

To set global permissions, log in as a System administrator and go to **Administration > Security > Global Permissions**.

- **Administer System:** All administration functions for the instance: global configuration and personalization of default dashboards.
- **Administer Quality Profiles**: Any action on quality profiles.
- **Administer Quality Gates:** Any action on quality gates
- **Share Dashboards and Filters:** Share dashboards, issue filters and measure filters.
- **Execute Analysis:** Execute analyses (project, view, report, developer), and to get all settings required to perform the analysis, even the secured ones like the scm account password, the jira account password, and so on.
- **Create Projects:** Initialize the structure of a new project before its first analysis. This permission is also required when doing the very first analysis of a project that has not already been created via the GUI.

Project Permissions

Five different permissions can be set on project-level resources (projects, views, developers):

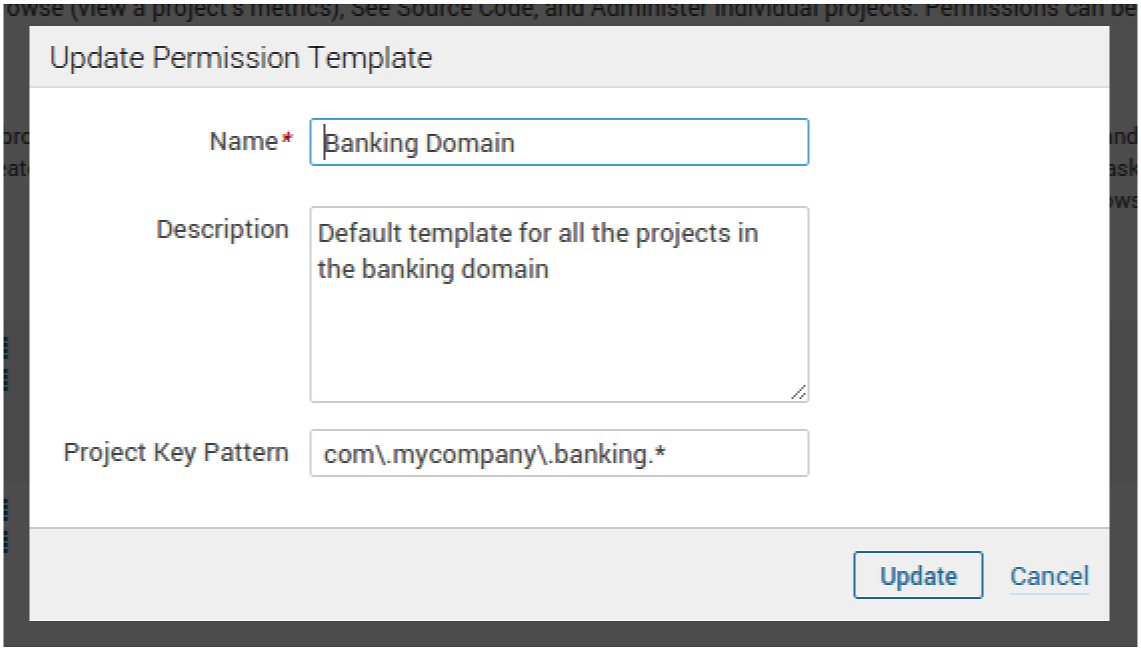
- **Browse:** Access a project, browse its measures, and create/edit issues for it.
- **See Source Code:** View the project's source code.
- **Administer Issues:** Advanced editing on issues: marking an issue False Positive or changing an Issue's severity.
- **Administer:** Access project settings and perform administration tasks.
- **Execute Analysis:** Execute analyses (project, view, report, developer), and to get all settings required to perform the analysis, even the secured ones like the scm account password, the jira account password, and so on.

Note that permissions are not cumulative. For instance, if you want to be able to administer the project, you also have to be granted the *Browse* permission to be able to access the project.

You can either manually grant permissions for each project to some users and groups or apply permission templates to projects.

Creating permission templates

To create a new template, use the "Create" button on **Administration > Security > Permission Templates**. It is possible to provide a **Project key pattern** . By default, every new project matching this key pattern will be granted permissions of this template.



Update Permission Template

Name* Banking Domain

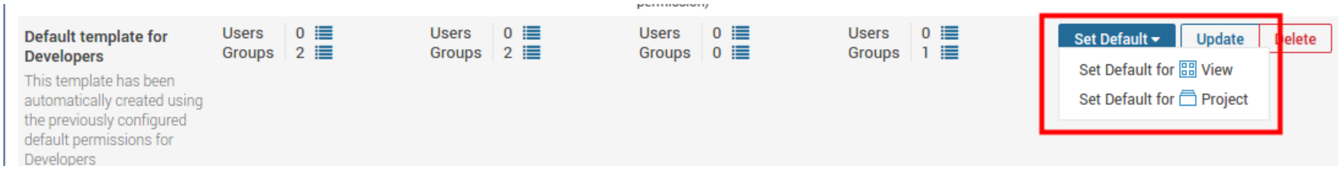
Description Default template for all the projects in the banking domain

Project Key Pattern com\.mycompany\.banking.*

Default project permissions

It is possible to configure the system so that when a new project (project, view, developer) is created, some users/groups are automatically granted permissions on this project.

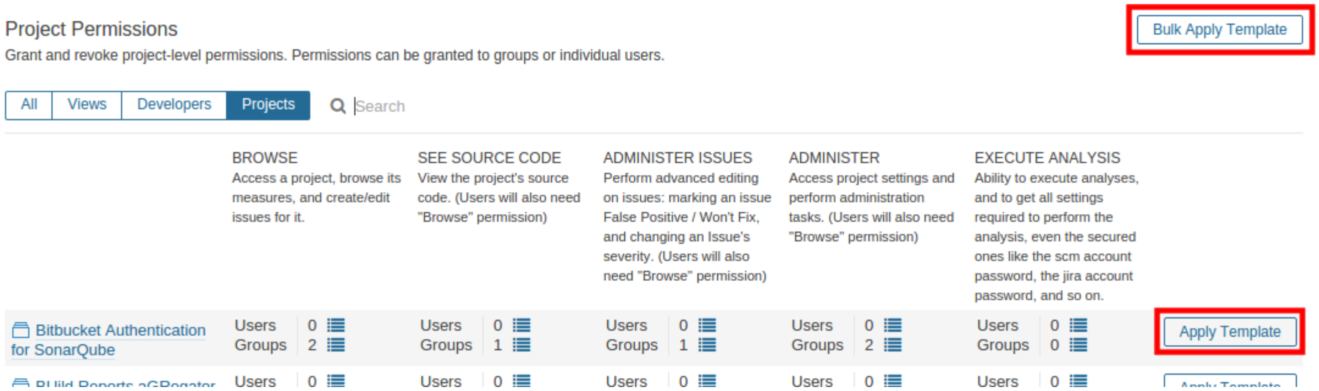
This is done through permission templates. Go to **Settings > Project Permissions > Permission Templates > Set default templates**:



Default template for Developers This template has been automatically created using the previously configured default permissions for Developers	Users 0 Groups 2	Users 0 Groups 2	Users 0 Groups 0	Users 0 Groups 1	Set Default ▾ Update Delete Set Default for View Set Default for Project

Apply permission templates to projects

To apply permission templates to projects to to the Project Permissions page, **Administration > Security > Project Permissions**. You can either apply a template to a specific project through the **Apply Template** link or do some bulk changes through the **Bulk Apply Template** button.



Project Permissions

Grant and revoke project-level permissions. Permissions can be granted to groups or individual users.

	BROWSE Access a project, browse its measures, and create/edit issues for it.	SEE SOURCE CODE View the project's source code. (Users will also need "Browse" permission)	ADMINISTER ISSUES Perform advanced editing on issues: marking an issue False Positive / Won't Fix, and changing an Issue's severity. (Users will also need "Browse" permission)	ADMINISTER Access project settings and perform administration tasks. (Users will also need "Browse" permission)	EXECUTE ANALYSIS Ability to execute analyses, and to get all settings required to perform the analysis, even the secured ones like the scm account password, the jira account password, and so on.	
Bitbucket Authentication for SonarQube	Users 0 Groups 2	Users 0 Groups 1	Users 0 Groups 1	Users 0 Groups 2	Users 0 Groups 0	Apply Template
BUild Reports aGRegator	Users 0	Users 0	Users 0	Users 0	Users 0	Apply Template

Note that there is no relation between a project and a permission template, meaning that:

- the permissions of a project can be modified after a permission template has been applied to this project
- none of the project permissions is changed when a permission template is modified

FAQ

I have locked myself out

To recreate a System administrator:

```
INSERT INTO user_roles(user_id, role) VALUES ((select id from users where login='mylogin'), 'admin');
```