

Back to project

Project settings
Details
Summary
People
Permissions
Notifications
Automation
Features
Toolchain
Workflows
Issues
Components
Apps
Development tools

Report settings

Resource Key
es.excentia:hispasat-jira-plugin:IMeter

This is the key of the SonarQube resource where you are going to retrieve the quality metrics. You can get this key from your SonarQube project dashboard or your sonar-project analysis parameters. You can setup more than one resource/project key by providing a comma separated list of resource keys. Measures will be aggregated into a unique view of all the projects together.

**** Only on SonarQube Enterprise Edition:** You can setup a portfolio key as a resource and all the related projects keys will be retrieved automatically. This feature is only available for commercial edition.

Tags
confluence-apps:utility

These are the tags of the SonarQube/SonarCloud resource where you are going to retrieve the quality metrics. You can get this tags from your SonarQube project dashboard or your sonar-project analysis parameters. You can setup more than one tag by providing a comma separated list of tags. Measures will be aggregated into a unique view of all the projects together.

Custom metrics
pantacemetric

List of custom metric keys to display in the dashboard, you can specify 1 or a list of metric keys separated by commas. For example: blocker_violations, major_violations, classes. Check with your SonarQube administrator to find out the keys to the available metrics

Create Jira Issue settings

Issue type for bugs
Bug

This is the issue type to create jira issues for new SonarQube Bugs issues. Issue types with mandatory fields are not displayed.

Issue type for vulnerabilities
Task

This is the issue type to create jira issues for new SonarQube Vulnerabilities issues. Issue types with not mandatory fields are not displayed.

Issue type for code smells
Story

This is the issue type to create jira issues for new SonarQube Code Smells issues. Issue types with not mandatory fields are not displayed.

Issue type for security hotspots
Task

This is the issue type to create new jira issues for SonarQube Security Hotspots. Issue types with not mandatory fields are not displayed.

Save

Maintenance options

Clear issues references
Clear

Removes internal references to completed or deleted Jira issues created by the app

Connection settings:

- SonarQube Server URL:** this is server base URL for your SonarQube Cloud installation
 - Note :** the base URL for SonarQube Cloud is <https://sonarcloud.io>
- Token:** this field is optional. If your SonarQube cloud instance is not public, then you will need to setup this field with the security token from a SonarQube user. You can find more information about SonarQube tokens here: <https://docs.sonarqube.org/display/SONAR/User+Token>

Visualization settings:

- Show history charts :** Check this option if you want to display measures history charts for each sonarqube project in Sonarqube Connector Panel Report.
- Group project's cards :** Select this option to set number of project cards per page that will be displayed in Sonarqube Connector Panel Report.

Filter settings:

- Show bugs, vulnerabilities or code smells :** Check these options if you want to filter sonarqube findings by Bugs, Vulnerabilities or Code Smells.

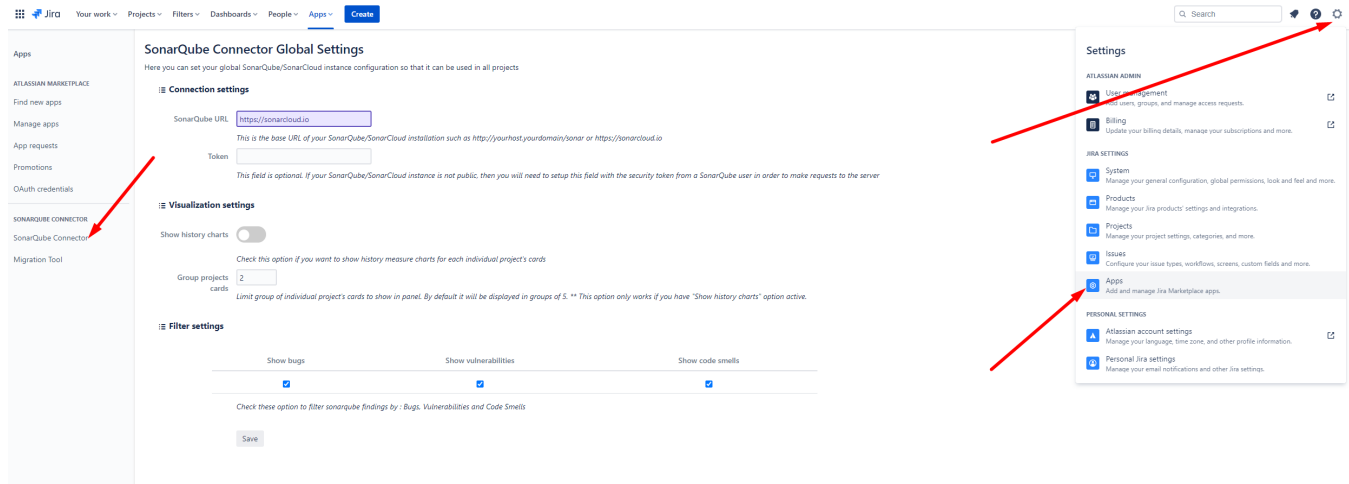
Report settings:

- Resource ID:** this is the key of the SonarQube resource where you are going to retrieve the quality metrics. You can get this key from your SonarQube project dashboard or your sonar-project analysis parameters.
 - Note:** since version 1.4 you can setup more than one resource/project key by providing a comma separated list of resource keys. Measures will be aggregated into a unique view of all the projects together. See [section linking multiple projects](#) to Jira.
- Tags :** This is an optional field. You can get the projects through the tags associated with them in SonarQube/SonarCloud. These tags can be obtained from your project page in SonarQube/SonarCloud or from the analysis properties. You can configure more than one tag by specifying a comma separated list of tags. The results will be aggregated in a single view with all the resources together.
- Custom metrics:** List of custom metric keys to display in the dashboard, you can specify 1 or a list of metric keys separated by commas. For example: blocker_violations, major_violations, classes. Check with your SonarQube administrator to find out the keys to the available metrics

Create Jira Issue Settings:

- Issue type For Bugs:** this is the default issue type to create new Jira issues based on SonarQube Bugs.
- Issue type For Vulnerabilities:** this is the default issue type to create new Jira issues based on SonarQube Vulnerabilities.
- Issue type For Code Smells:** this is the default issue type to create new Jira issues based on SonarQube Code Smells.
- Issue type For Hotspots:** this is the default issue type to create new Jira issues based on SonarQube Security Hotspots.

Global Settings Configuration



You can configure a global server to share the configuration on all Jira projects. This is very useful if your Sonar instance is the same for all your Jira projects.

Connection settings:

- **SonarQube Server URL:** this is server base URL for your installation
 - **Note :** the base URL for SonarCloud is <https://sonarcloud.io>
- **Token:** this field is optional. If your SonarQube instance is not public, then you will need to setup this field with the security token from a SonarQube user. You can find more information about SonarQube tokens here: <https://docs.sonarqube.org/display/SONAR/User+Token>

Visualization settings:

- **Show history charts :** Check this option if you want to display measures history charts for each sonarqube project in Sonarqube Connector Panel Report.
- **Group project's cards :** Select this option to set number of project cards per page that will be displayed in Sonarqube Connector Panel Report.

Filter settings:

- **Show bugs, vulnerabilities or code smells :** Check these options if you want to filter sonarqube findings by Bugs, Vulnerabilities or Code Smells.