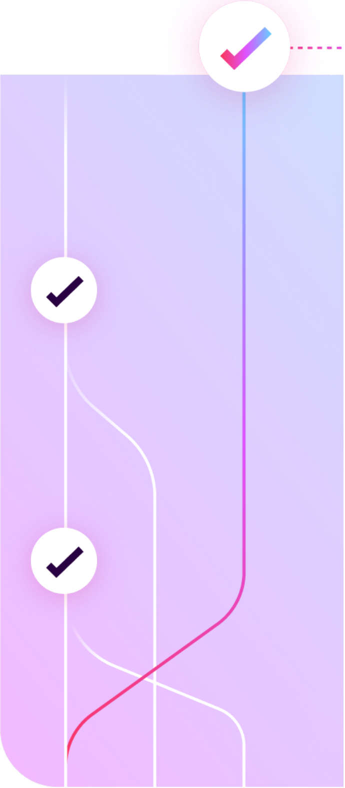
SonarQube Evaluation Guide

SonarQube is a tool that continuously analyzes code to find and guide you in fixing quality and security issues as you develop. You can deploy it in a location you choose: on-premises or in the cloud. It integrates seamlessly into your DevOps workflow and displays clear pass/fail results as you code to ensure only the highest-quality code, free of security vulnerabilities, is built and released to production.

SonarQube is a server with code-scanning engines that you integrate with your build pipeline. Your build automation automatically triggers the scanners as you commit new code changes. The scanners then send the code analysis data to the SonarQube server for final processing. The analysis results are stored in a database linked with SonarQube and displayed in SonarQube's UI and your DevOps workflow with quality gates that only allow the highest-standard code to be built and released to production.



Expectation for evaluation
We recommend you start with a few representative projects to gain an understanding of the project's code quality and security. This will simplify configuration, and you will see how SonarQube displays the analysis results across all your projects. This will save you time!

What to focus on
The following are best practices for the evaluation:

- Involve personnel on your side who are capable of:
  - Installing server software in the infrastructure you prefer
  - Installing a database or configuring a new schema in an existing database
  - Adding scanner invocation configuration to the project build automation
  - Understanding software code quality analysis and evaluating what they see
- If you wish to keep from polluting your production environment with test data while you perform the evaluation, keep your initial evaluation SonarQube server separate from any existing production platform(s).
- Perform a fresh SonarQube server installation.
- Set up and configure your SonarQube evaluation instance.
- If you are evaluating an upgrade to the Enterprise Edition or Data Center Edition of SonarQube, you can export and import projects from an existing instance.

During evaluation, these can be skipped

- Do not configure IDP authentication using LDAP, SAML, or OAuth. Instead, create basic accounts in the SonarQube server.
- Do not set up HTTPS communication to SonarQube. Basic HTTP connectivity is sufficient during evaluation.
- Do not add third-party or custom plugins to the platform. These are more advanced and not needed for evaluation purposes.

Installation and configuration

- Prepare the database
- Install the SonarQube server
- Configure triggering analysis automatically from the build pipeline, following specific setup appropriate for your DevOps platform and project's language

Explore important features

- Security Rules
- Security Reports (Enterprise and Data Center Editions only)
- Branch Analysis
- Pull Request Analysis
- Portfolios (Enterprise and Data Center Editions only)
- Applications (Developer, Enterprise, and Data Center Editions)

For the most efficient technical assistance, please consult our documentation and community.