

SonarTSQL

By [SonarSource](#) – [SonarSource](#) – [Issue Tracker](#) – Supported by [SonarSource](#)

[More versions](#)

SonarTSQL 1.3.1 – Dec 13, 2018 – SonarQube 6.7+ (Compatible with LTS)

19 new syntaxes supported to increase the number of analyzed files

I accept the [Terms and Conditions](#) – [Download](#) – [Release notes](#)

Description

[SonarTSQL](#) detects bugs, vulnerabilities and code smells in Transact-SQL (TSQL) code.

First Analysis of a T-SQL Project

1. Install SonarQube Server (see [Setup and Upgrade](#) for more details)
2. Install [SonarQube Scanner](#) and be sure you can call `sonar-scanner` from the directory where you have your source code
3. Install SonarTSQL (see [Installing a Plugin](#) for more details)
4. Run your analysis with the [SonarQube Scanner](#) by executing the following command from the root directory of the project:

```
sonar-scanner -Dsonar.projectKey=xxx -Dsonar.sources=.
```

5. Follow the link provided at the end of the analysis to browse your project's quality in SonarQube UI

Further Analyses

Assuming steps 1-3 above have already been completed, you'll want to encapsulate your analysis parameters in a `sonar-project.properties` file at the root of your project (see a sample project on GitHub: <https://github.com/SonarSource/sonar-scanning-examples/tree/master/sonarqube-scanner>). Then subsequent analyses can simply be run with:

```
sonar-scanner
```

Advanced Use

With SonarTSQL, you can:

- change the files to analyze by configuring the property `sonar.tsq1.file.suffixes` in [Settings > General Settings > T-SQL > File Suffixes](#)

Important Note

With the default configuration, SonarTSQL only analyses files with the `.tsq1` file extension (since SonarTSQL 1.2), and files with the `.sql` file extension are analysed by SonarPLSQL. This behavior is defined through analysis properties: `sonar.tsq1.file.suffixes` and `sonar.plsql.file.suffixes`. You can override these properties either at server level or at project level in order to have SonarTSQL analyse `.sql` files.