

Security Testing using SonarQube

Download SonarQube:

<https://www.sonarsource.com/products/sonarqube/downloads/>

The screenshot shows the SonarQube website's download page. The navigation bar includes links for Deploy, What's new, Why upgrade, Docs, Download (active), Pricing, and a Request trial button. The main content area is divided into four columns representing different editions: Community Build, Developer Edition, Enterprise Edition, and Data Center Edition. Each column has a description, a download button, and a 'Learn more' or 'Download only' link. The Community Build section highlights 'Release 25.6.0.109173' and lists supported languages. The Developer and Enterprise editions list additional languages like C, C++, and Swift. The Data Center Edition mentions high availability and scalability. A chat widget is visible in the bottom right corner.

Community Build	Developer Edition	Enterprise Edition	Data Center Edition
Free and open source for productivity & code quality	Essential capabilities for small teams & businesses	Designed to meet Enterprise-level requirements	For high availability, scalability, & performance
Download for free	Download & try	Download & try	Download & try
Learn more	Download only	Download only	Download only
Release 25.6.0.109173 Static code analysis for 21 languages and frameworks	Community Build, plus: Additional languages: C, C++, Obj-C, Dart/Flutter, Swift, ABAP, T-SQL, PL/SQL and Ansible	Developer Edition, plus: Additional languages: Apex, COBOL, JCL, PL/I, RPG and VB6	En Welcome! Would you like to learn more about additional features in SonarQube Server Developer or Enterprise editions? By using chat, you understand all chats may be

Download for free.

Extract the downloaded folder and then open the folder sonarqube/bin/windows where you can see

To Start Sonar JDK 17 is Required

start sonar

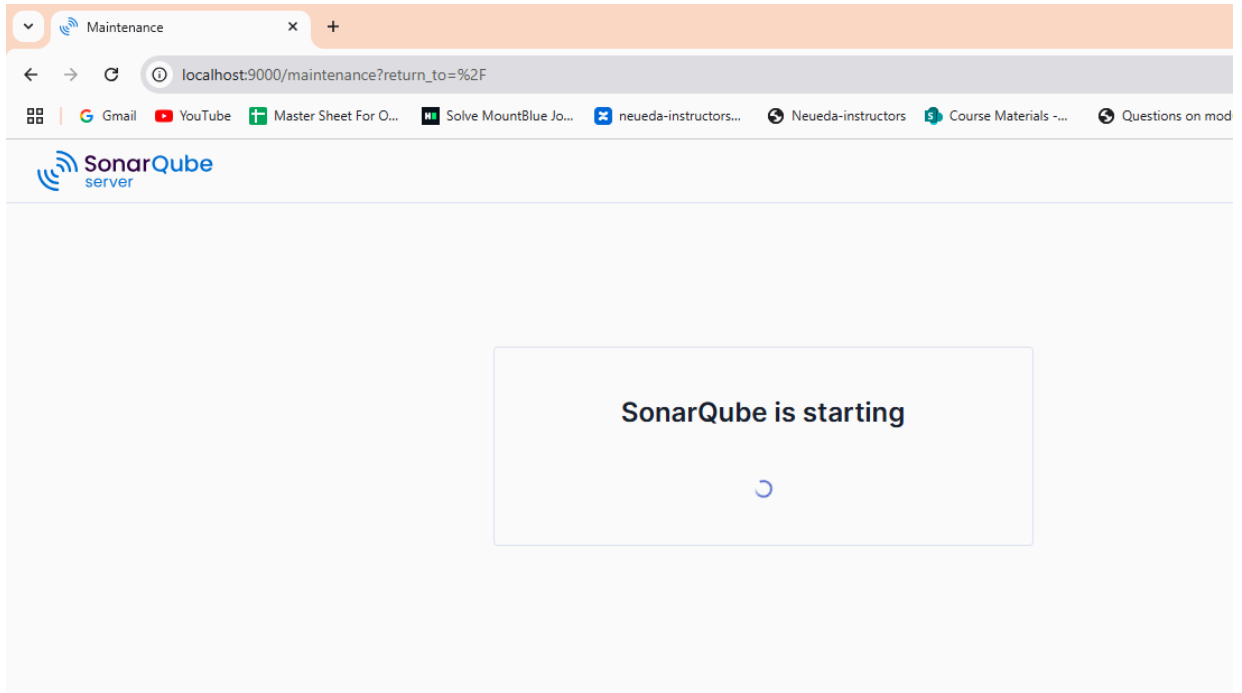
click on startsonar

The screenshot shows a Windows command prompt window with the title 'C:\WINDOWS\system32\cmd'. The output shows the SonarQube server starting. It logs the cleaning or creating of a temporary directory, the Elasticsearch listening on port 127.0.0.1, the launch of the Elasticsearch process from the SonarQube bin directory, and the waiting for Elasticsearch to be up and running. It also mentions the Standard Commons Logging discovery in action with spring-jcl.

```
C:\WINDOWS\system32\cmd. x + v
Starting SonarQube...
2025.06.08 09:35:35 INFO app[][o.s.a.AppFileSystem] Cleaning or creating temp directory C:\User
e-25.6.0.109173\sonarqube-25.6.0.109173\temp
2025.06.08 09:35:35 INFO app[][o.s.a.es.EsSettings] Elasticsearch listening on [HTTP: 127.0.0.1
]
2025.06.08 09:35:36 INFO app[][o.s.a.ProcessLauncherImpl] Launch process[ELASTICSEARCH] from [C
narqube-25.6.0.109173\sonarqube-25.6.0.109173\elasticsearch]: C:\Program Files\Java\jdk-17\bin\j
UseSerialGC -Dcli.name=server -Dcli.script=./bin/elasticsearch -Dcli.libs=lib/tools/server-cli -
EW\Downloads\sonarqube-25.6.0.109173\sonarqube-25.6.0.109173\elasticsearch -Des.path.conf=C:\Use
be-25.6.0.109173\sonarqube-25.6.0.109173\temp\conf\es -Des.distribution.type=tar -cp C:\Users\NE
.6.0.109173\sonarqube-25.6.0.109173\elasticsearch\lib\*;C:\Users\NEW\Downloads\sonarqube-25.6.0.
109173\elasticsearch\lib\cli-launcher\* org.elasticsearch.launcher.CliToolLauncher
2025.06.08 09:35:36 INFO app[][o.s.a.SchedulerImpl] Waiting for Elasticsearch to be up and runn
Standard Commons Logging discovery in action with spring-jcl: please remove commons-logging.jar
to avoid potential conflicts
```

Wait for sometime to startup your sonarqube server

open <http://localhost:9000>





Log in to SonarQube

Login *

Password *

[Go back](#)

[Log in](#)

By default you need to enter admin as username and admin as password.

You will be redirected to update password screen, here you need to set the password with some rules.

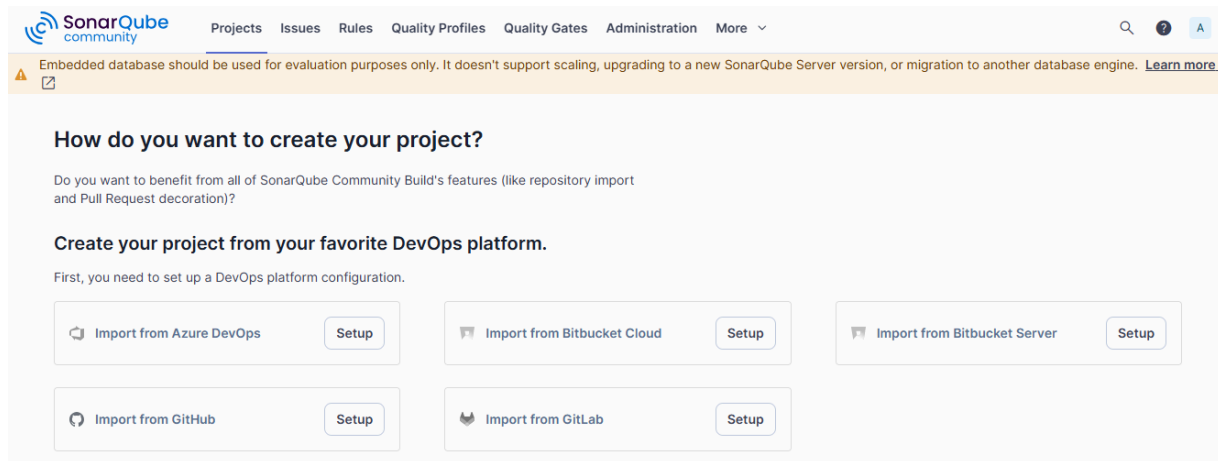
Rules:

Password *

Your password must include at least:

- × 12 characters
- × 1 upper case letter
- × 1 lower case letter
- × 1 number
- × 1 special character

After updating the password you will be redirected to SonarQube Dashboard



Now Let's Create a Project (Node-Project)

create folder node-project

move to that folder, open terminal

npm init -y (create package.json file)

npm install express (install express dependency)

create index.js file

```
const express = require('express')
const app = express() //server
```

```
//api
app.get('/', (req, res) => {
  res.send('Hello From SonarQube!')
})
```

```
//server starting
app.listen(3000, () => console.log('server started'))
```

create sonar-project.properties

```
sonar.projectKey=node-project
sonar.projectName=node-project
sonar.projectVersion=1.0
sonar.sources=.
sonar.exclusions=node_modules/**
sonar.language=js
sonar.sourceEncoding=UTF-8
```

Download Sonar Scanner

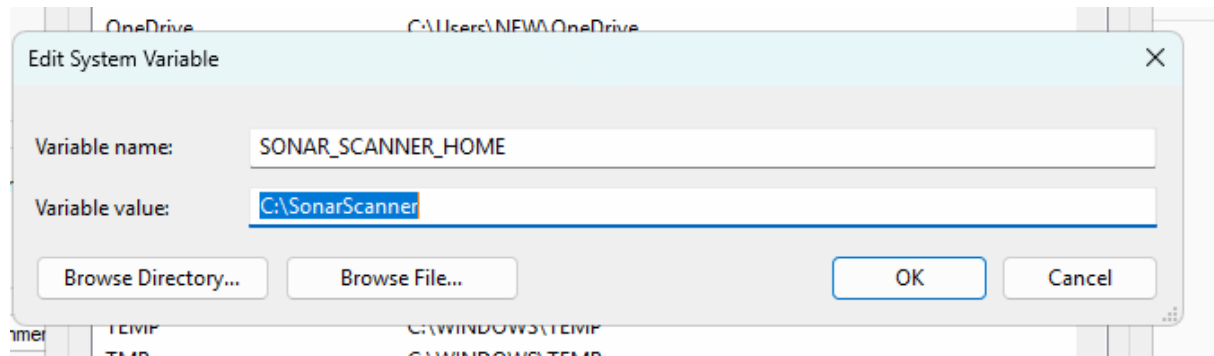
<https://docs.sonarsource.com/sonarqube-server/10.8/analyzing-source-code/scanners/sonarscanner/>

extract the folder

copy the folder and keep it some place and give the folder name like SonarScanner where you can see bin folder and inside that different platform scanner file was there.

for any platform we need to set path

windows:- go to system settings-> advanced system settings --> environment variables --> system variable create variable



and then for user variable above click on path and then add new -->

%SONAR_SCANNER_HOME%\bin

If its added correctly then you can check sonar-scanner -h command if its working path setting done successfully.

```
C:\Users\NEW>sonar-scanner -h

usage: sonar-scanner [options]

Options:
  -D,--define <arg>    Define property
  -h,--help             Display help information
  -v,--version          Display version information
  -X,--debug            Produce execution debug output
```

For Mac and Linux users you can set Path

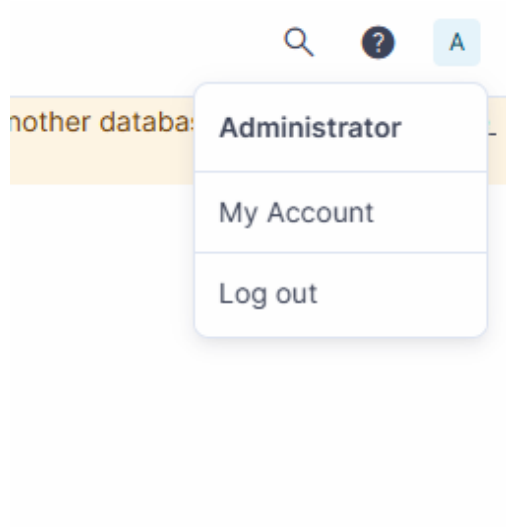
export PATH=\$PATH:/give/path/to/sonar-scanner

To scan Project We need to execute one command.

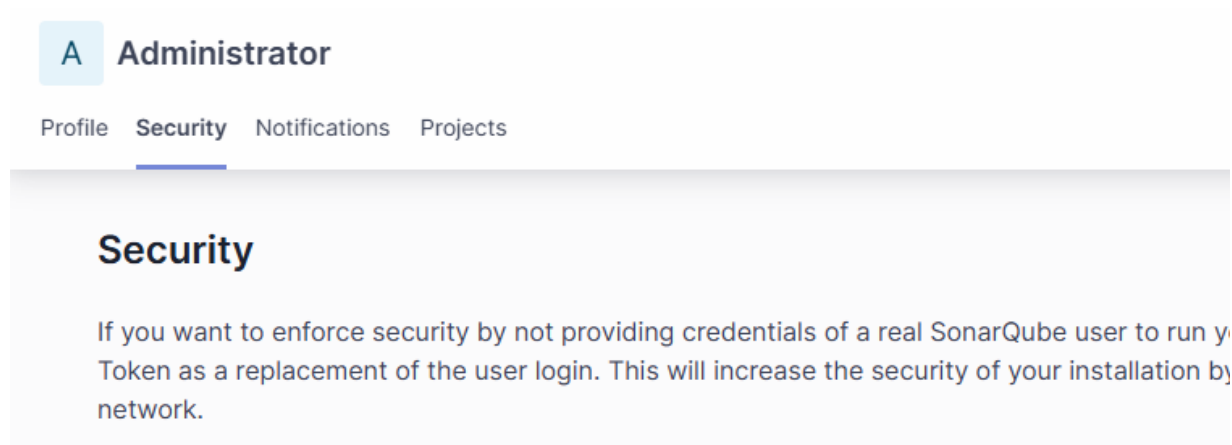
sonar-scanner -Dsonar.projectBaseDir=%cd% -Dsonar.host.url=http://localhost:9000 -Dsonar.token=YOUR-TOKEN

Here we need to generate Token from Sonar Server

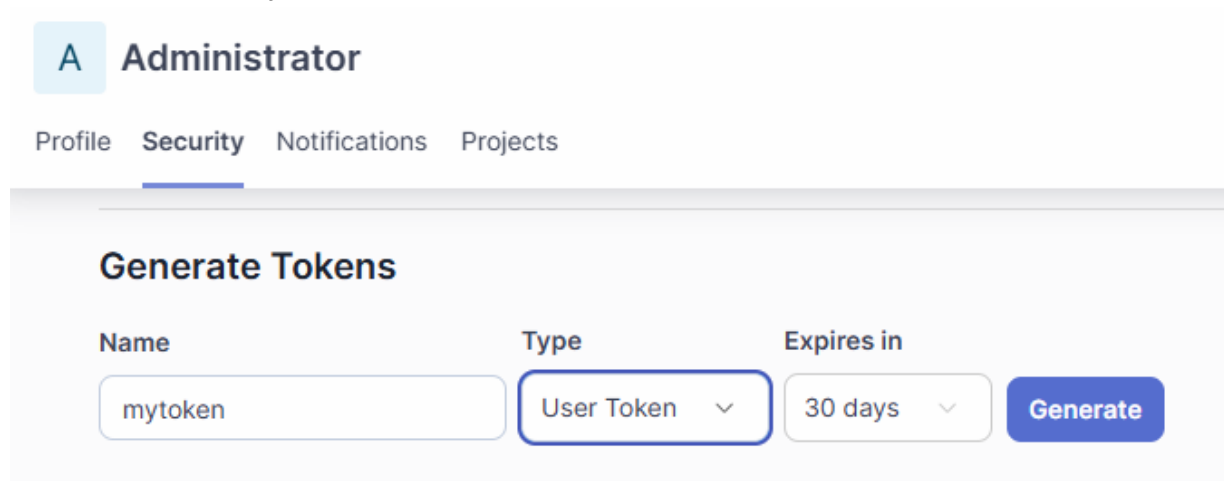
click on user



click on My Account



then click on security Tab





click on generate

A Administrator

Profile **Security** Notifications Projects

Name	Type	Expires in	
<input type="text" value="Enter Token Name"/>	<input type="text" value="Select Token Type"/>	<input type="text" value="30 days"/>	<input type="button" value="Generate"/>

 New token "mytoken" has been created. Make sure you copy it now, you won't be able to see it again!

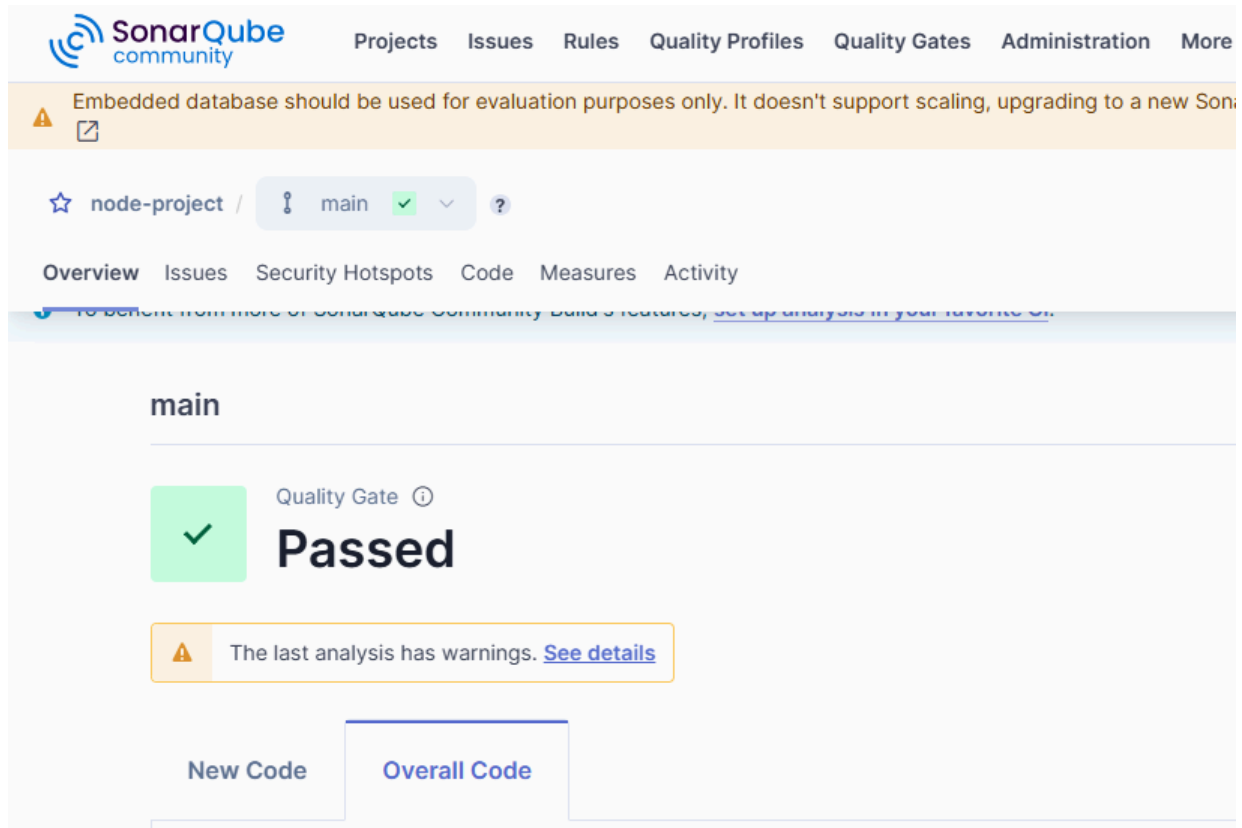


This token you need to use for scanner command.

Once the command executed you can see below message in terminal

```
10:54:17.614 WARN    * node_modules/iconv-lite/.idea/codeStyles/Project.xml
10:54:17.617 WARN    * node_modules/iconv-lite/.idea/vcs.xml
10:54:17.620 WARN    This may lead to missing/broken features in SonarQube
10:54:17.624 INFO    CPD Executor 1 file had no CPD blocks
10:54:17.628 INFO    CPD Executor Calculating CPD for 0 files
10:54:17.634 INFO    CPD Executor CPD calculation finished (done) | time=0ms
10:54:17.664 INFO    SCM revision ID '4916b372e5596f30430dee4bbb4a9b38fdaa5be1'
10:54:19.271 INFO    Analysis report generated in 921ms, dir size=246.2 kB
10:54:19.399 INFO    Analysis report compressed in 80ms, zip size=33.0 kB
10:54:22.598 INFO    Analysis report uploaded in 3199ms
10:54:22.605 INFO    ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard
10:54:22.614 INFO    Note that you will be able to access the updated dashboard once the server has p
itted analysis report
10:54:22.623 INFO    More about the report processing at http://localhost:9000/api/ce/task?id=e946159
b68db6bfbbc5
10:54:23.295 INFO    Analysis total time: 1:10.458 s
10:54:23.315 INFO    SonarScanner Engine completed successfully
10:54:24.055 INFO    EXECUTION SUCCESS
10:54:24.058 INFO    Total time: 1:32.481s
```

Below information on your sonar dashboard



If you want to set up the entire things in Linux/ubuntu follow the below mentioned steps
open wsl

move to the sonarqube folder

cd /bin/linux

execute below command

```
sonam@DESKTOP-4F8ELLU:/mnt/c/Users/NEW/
in/linux-x86-64$ ./sonar.sh start
/usr/bin/java
Starting SonarQube...
Started SonarQube.
sonam@DESKTOP-4F8ELLU:/mnt/c/Users/NEW/
in/linux-x86-64$ ./sonar.sh status
/usr/bin/java
sonam@DESKTOP-4F8ELLU:/mnt/c/Users/
sonam@DESKTOP-4F8ELLU:/mnt/c/Users/
in/linux-x86-64$ ./sonar.sh status
/usr/bin/java
SonarQube is running (919).
sonam@DESKTOP-4F8ELLU:/mnt/c/Users/
```


then you can access inside browser: <http://localhost:9000>

you will be redirected to login screen then continue with the same process for login mentioned above.