

Configuring default setup for code scanning

In this article

About default setup

Configuring default setup for a repository

Next steps

You can quickly secure code in your repository with default setup for code scanning.

Who can use this feature

People with admin permissions to a repository, or the security manager role for the repository, can configure code scanning for that repository.

Code scanning is available for all public repositories on GitHub.com. Code scanning is also available for private repositories owned by organizations that use GitHub Enterprise Cloud and have a license for GitHub Advanced Security. For more information, see "[About GitHub Advanced Security](#)."

About default setup

Default setup for code scanning is the quickest, easiest, most low-maintenance way to enable code scanning for your repository. Based on the code in your repository, default setup will automatically create a custom code scanning configuration. After enabling default setup, the code in your repository will be scanned:

- on each push to the repository's default branch, or any protected branch. For more information on protected branches, see "[About protected branches](#)."
- when creating or committing to a pull request based against the repository's default branch, or any protected branch.
- on a weekly schedule.

Note: If no pushes and pull requests have occurred in a repository with default setup enabled for 6 months, the weekly schedule will be disabled to save your GitHub Actions minutes.

You can enable the automatically selected configuration of default setup to start scanning your code as soon as possible, or you can customize aspects of the configuration to better meet your code scanning needs. If you choose to customize the configuration yourself, you can select:

- the languages default setup will analyze.
- the query suite default setup will run. For more information, see "[Built-in CodeQL query suites](#)."

You can also enable default setup for multiple or all repositories in an organization at the same time. For information on bulk enablement, see "[Configuring default setup for code](#)

[scanning at scale](#)."

If you need more granular control over your code scanning configuration, you should instead configure advanced setup. For more information, see "[Configuring advanced setup for code scanning](#)."

Requirements for using default setup [↗](#)

Your repository is eligible for default setup for code scanning if:

- it includes at least one CodeQL-supported language.
- GitHub Actions are enabled.
- it is publicly visible.


You can use default setup if your repository includes languages that aren't supported by CodeQL, such as R. For more information on CodeQL-supported languages, see "[About code scanning with CodeQL](#)."

Configuring default setup for a repository [↗](#)

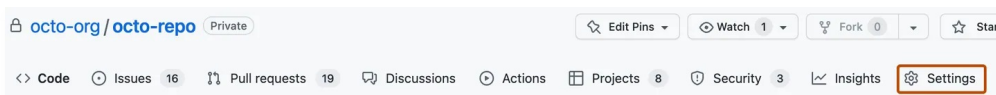
When you initially configure default setup for code scanning for a repository, all CodeQL-supported languages in the repository will be analyzed automatically. The languages that are analyzed successfully will be retained in the new default setup configuration. Languages that are not analyzed successfully will be automatically deselected from the default setup configuration.


Note: At least one CodeQL-supported language's analysis in a repository must succeed, or else default setup will not be successfully enabled in that repository.

- 1 On GitHub.com, navigate to the main page of the repository.

Note: If you are configuring default setup on a fork, you must first enable GitHub Actions. To enable GitHub Actions, under your repository name, click  **Actions**, then click **I understand my workflows, go ahead and enable them**. Be aware that this will enable all existing workflows on your fork.

- 2 Under your repository name, click  **Settings**. If you cannot see the "Settings" tab, select the ... dropdown menu, then click **Settings**.



- 3 In the "Security" section of the sidebar, click  **Code security and analysis**.
- 4 In the "Code scanning" section, select **Set up** ▾, then click **Default**.

Code scanning

Automatically detect common vulnerabilities and coding errors.

Tools

CodeQL analysis
Identify vulnerabilities and errors in your code with [CodeQL](#). Set up ▾

Other tools
Add any third-party code scanning tool.

Protection rules

Pull request check failure

Default
CodeQL will automatically find the best configuration for your repository.

Advanced
Customize your CodeQL configuration via a YAML file checked into the repository.

You will then see a "CodeQL default configuration" dialog summarizing the code scanning configuration automatically created by default setup.

- a. Optionally, in the "Query suites" section of the "CodeQL default configuration" modal dialog, select the **Default** ▾ dropdown menu, then click the CodeQL query suite you would like to use.

CodeQL default configuration

Languages to analyze
Detected on this repository. ● JavaScript ● TypeScript

Query suites
Set of queries run in the analysis. Default ▾

Events
These events will trigger a new scan. On push and pull requests to `main` and 0 protected branches.

Cancel Enable CodeQL

If you choose the **Extended** query suite, your code scanning configuration will run lower severity and precision queries in addition to the queries included in the **Default** query suite. For more information on the available query suites, see "[Built-in CodeQL query suites](#)."

Note: If you configure code scanning to use the **Extended** query suite, you may experience a higher rate of false positive alerts.

- 5 Review the settings for default setup on your repository, then click **Enable CodeQL**. This will trigger a workflow that tests the new, automatically generated configuration.

Note: If you are switching to default setup from advanced setup, you will see a warning informing you that default setup will override existing code scanning configurations. This warning means default setup will disable the existing workflow file and block any CodeQL analysis API uploads.

- 6 Optionally, to view your default setup configuration after enablement, select ⋮, then click **View CodeQL configuration**.

Next steps

After you configure default setup for code scanning, and your configuration runs successfully at least once, you can start examining and resolving code scanning alerts. For more information on code scanning alerts, see "[About code scanning alerts](#)" and "[Managing code scanning alerts for your repository](#)."

You can find detailed information about your code scanning configuration, including timestamps for each scan and the percentage of files scanned, on the tool status page. For more information, see "[About the tool status page for code scanning](#)."

When you configure default setup, you may encounter an error. For information on troubleshooting specific errors, see "[Troubleshooting code scanning](#)."

Legal

© 2023 GitHub, Inc. [Terms](#) [Privacy](#) [Status](#) [Pricing](#) [Expert services](#) [Blog](#)