

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 organization-owned repositories in GitHub Enterprise Server. This feature requires 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.

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 aside from Swift.
- GitHub Actions are enabled.
- GitHub Advanced Security is enabled.

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](#)."

About adding compiled languages to your default setup [🔗](#)

Compiled languages are not automatically included in default setup configuration because they often require more advanced configuration, but you can manually select any CodeQL-supported compiled language other than Swift for analysis.

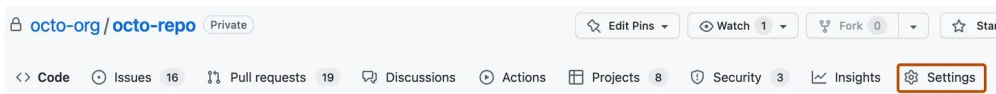
Configuring default setup for a repository [🔗](#)

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 your GitHub Enterprise Server instance, 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.

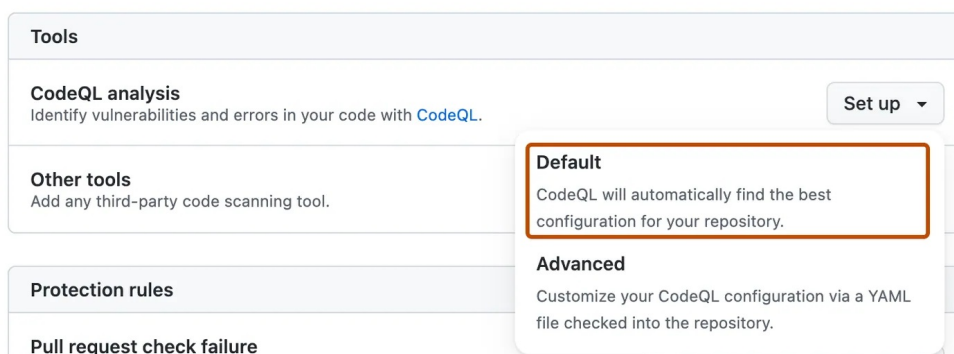
- 2 Under your repository name, click **Settings**. If you cannot see the "Settings" tab, select the ... dropdown menu, then click **Settings**.



- 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.



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



Note: If your repository contains *only* compiled CodeQL-supported languages (for example, Java), you will be taken to the settings page to select the languages you want to add to your default setup configuration.

5 Optionally, to customize your code scanning setup, click  **Edit**.

- To add or remove a language from the analysis performed by default setup, select or deselect that language in the "Languages" section. If you would like to analyze a CodeQL-supported compiled language with default setup, select that language here.
- To specify the CodeQL query suite you would like to use, select your preferred query suite in the "Query suites" section.

6 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.

7 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](#)