

Configuring advanced setup for code scanning

In this article

About advanced setup for code scanning

Configuring advanced setup for a repository

Next steps

You can configure advanced setup for a repository to find security vulnerabilities in your code using a highly customizable code scanning configuration.

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. People with write permissions to a repository can also configure code scanning, but only by creating a workflow file or manually uploading a SARIF file.

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 advanced setup for code scanning

Advanced setup for code scanning is helpful when you need more granular control over your code scanning configuration. By creating and editing a CodeQL workflow file, you can change the scan schedule, scan any CodeQL-supported language, use a matrix build, and more.

You can also configure code scanning with third-party tools. For more information, see "[Configuring code scanning using third-party actions](#)."

If you run code scanning using multiple configurations, the same alert will sometimes be generated by more than one configuration. If an alert comes from multiple configurations, you can view the status of the alert for each configuration on the alert page. For more information, see "[About code scanning alerts](#)."

If you do not need a highly customizable code scanning configuration, consider using default setup for code scanning. For more information on eligibility for default setup, see "[Configuring default setup for code scanning](#)."

Prerequisites

Your repository is eligible for advanced setup if:

- it uses CodeQL-supported languages or you plan to generate code scanning results with a third-party tool.
- GitHub Actions are enabled.

- it is publicly visible.

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


Advanced setup for code scanning is helpful when you need to customize your code scanning. By creating and editing a workflow file, you can choose which queries to run, change the scan schedule, select the languages to scan, use a matrix build, and more.

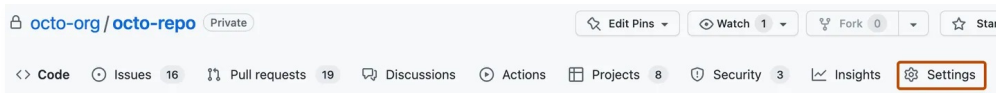
Configuring advanced setup for code scanning with CodeQL [🔗](#)


You can customize your code scanning by creating and editing a workflow file. Selecting advanced setup generates a basic workflow file for you to customize.


Using actions to run code scanning will use minutes. For more information, see "[About billing for GitHub Actions](#)."

Note: You can configure code scanning for any public repository where you have write access.

- 1 On GitHub.com, navigate to the main page of the repository.
- 2 Under your repository name, click  **Settings**. If you cannot see the "Settings" tab, select the ... dropdown menu, then click **Settings**.

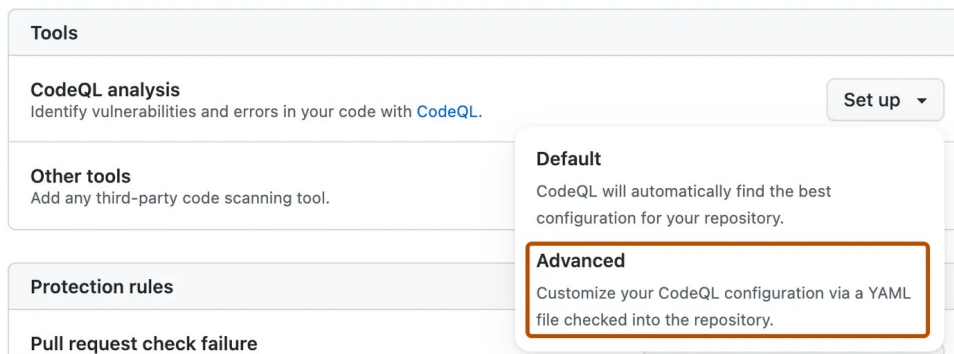


- 3 In the "Security" section of the sidebar, click  **Code security and analysis**.
- 4 Scroll down to the "Code scanning" section, select **Set up** ▾, then click **Advanced**.

Note: If you are switching from default setup to advanced setup, in the "Code scanning" section, select ..., then click  **Switch to advanced**. In the pop-up window that appears, click **Disable CodeQL**.

Code scanning

Automatically detect common vulnerabilities and coding errors.



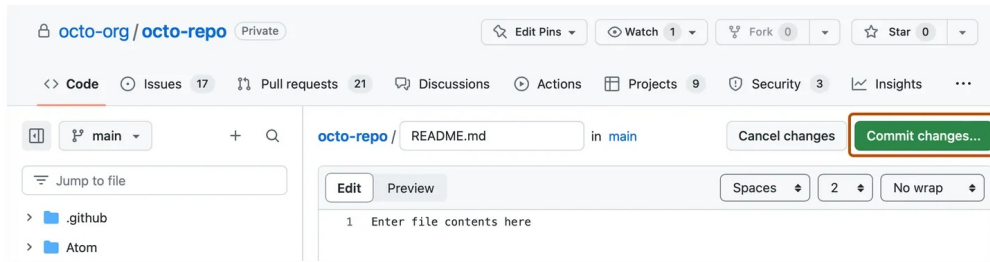
- 5 To customize how code scanning scans your code, edit the workflow.

Generally, you can commit the CodeQL analysis workflow without making any changes to it. However, many of the third-party workflows require additional configuration, so read the comments in the workflow before committing.

For more information, see "[Customizing your advanced setup for code scanning](#)"

and "[CodeQL code scanning for compiled languages](#)."

- 6 Click **Commit changes...** to display the commit changes form.



- 7 In the commit message field, type a commit message.
- 8 Choose whether you'd like to commit directly to the default branch, or create a new branch and start a pull request.
- 9 Click **Commit new file** to commit the workflow file to the default branch or click **Propose new file** to commit the file to a new branch.
- 10 If you created a new branch, click **Create pull request** and open a pull request to merge your change into the default branch.

In the suggested CodeQL analysis workflow, code scanning is configured to analyze your code each time you either push a change to the default branch or any protected branches, or raise a pull request against the default branch. As a result, code scanning will now commence.

The `on:pull_request` and `on:push` triggers for code scanning are each useful for different purposes. For more information, see "[Customizing your advanced setup for code scanning](#)."

For information on bulk enablement, see "[Configuring advanced setup for code scanning with CodeQL at scale](#)."

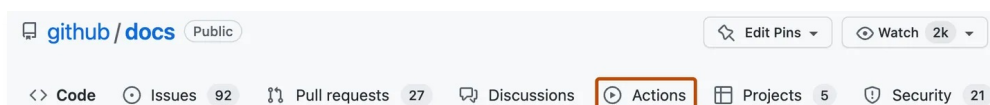
Configuring code scanning using third-party actions [🔗](#)

Note: Starter workflows for Advanced Security have been consolidated in a "Security" category in the **Actions** tab of a repository. This new configuration is currently in beta and subject to change.

GitHub provides starter workflows for security features such as code scanning. You can use these suggested workflows to construct your code scanning workflows, instead of starting from scratch.

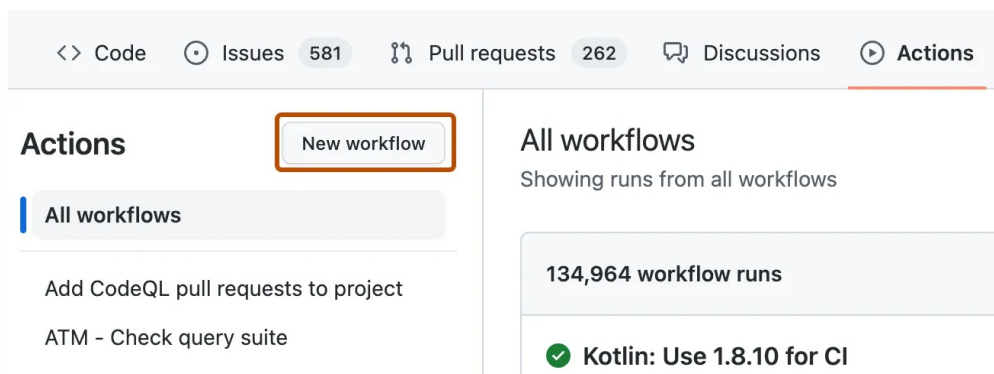
Using actions to run code scanning will use minutes. For more information, see "[About billing for GitHub Actions](#)."

- 1 On GitHub.com, navigate to the main page of the repository.
- 2 Under your repository name, click **Actions**.

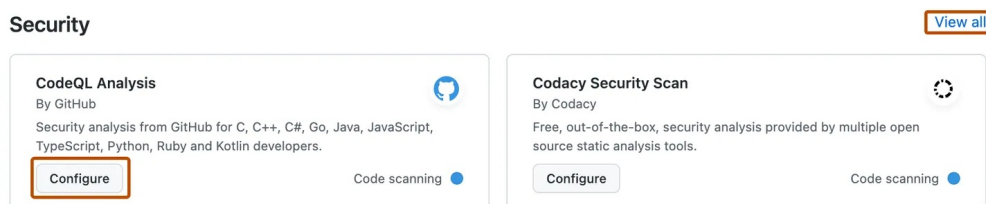


- 3 If the repository has already at least one workflow configured and running, click

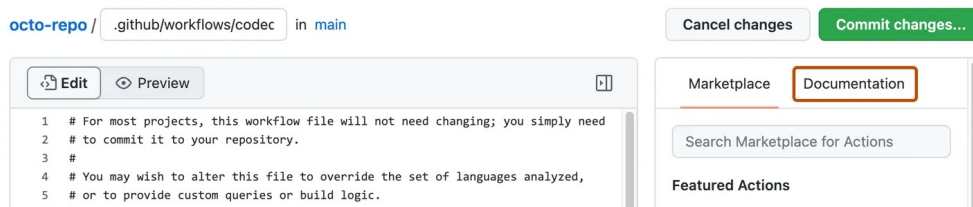
New workflow to display starter workflows. If there are currently no workflows configured for the repository, go to the next step.



- 4 In the "Choose a workflow" or "Get started with GitHub Actions" view, scroll down to the "Security" category and click **Configure** under the workflow you want to configure. You may need to click **View all** to find the security workflow you want to configure.



- 5 Follow any instructions in the workflow to customize it to your needs. For more general assistance about workflows, click **Documentation** on the right pane of the workflow page.



For more information, see "[Using starter workflows](#)" and "[Customizing your advanced setup for code scanning](#)."

Next steps

After configuring code scanning, and allowing its actions to complete, you can:

- View all of the code scanning alerts generated for this repository. For more information, see "[Managing code scanning alerts for your repository](#)."
- View any alerts generated for a pull request submitted after you configure code scanning. For more information, see "[Triaging code scanning alerts in pull requests](#)."
- Configure notifications for completed runs. For more information, see "[Configuring notifications](#)."
- Learn about code scanning checks on pull requests. For more information, "[Triaging code scanning alerts in pull requests](#)."
- View the logs generated by the code scanning analysis. For more information, see "[Viewing code scanning logs](#)."

- Investigate any problems that occur with the initial configuration of code scanning. For more information, see "[Troubleshooting code scanning](#)."
- Customize how code scanning scans the code in your repository. For more information, see "[Customizing your advanced setup for code scanning](#)."

Legal

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