

Managing security and analysis settings for your personal account

In this article

About management of security and analysis settings

Enabling or disabling features for existing repositories

Enabling or disabling features for new repositories

Further reading

You can control features that secure and analyze the code in your projects on GitHub.

About management of security and analysis settings



GitHub can help secure your repositories. This topic tells you how you can manage the security and analysis features for all your existing or new repositories.

You can still manage the security and analysis features for individual repositories. For more information, see "[Managing security and analysis settings for your repository](#)."

You can also review the security log for all activity on your personal account. For more information, see "[Reviewing your security log](#)."

Note: You can't disable some security and analysis features that are enabled by default for public repositories.

If you enable security and analysis features, GitHub performs read-only analysis on your repository.


For an overview of repository-level security, see "[Securing your repository](#)."

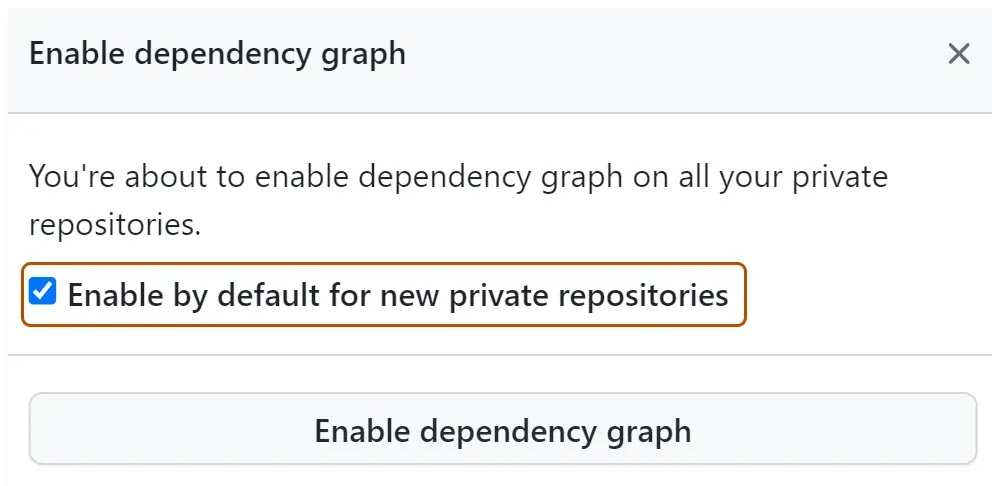
Enabling or disabling features for existing repositories



1 In the upper-right corner of any page, click your profile photo, then click **Settings**.



- 2 In the "Security" section of the sidebar, click  **Code security and analysis**.
- 3 Under "Code security and analysis", to the right of the feature, click **Disable all** or **Enable all**.
- 4 Optionally, enable the feature by default for new repositories that you own.



- 5 Click **Disable FEATURE** or **Enable FEATURE** to disable or enable the feature for all the repositories you own.

When you enable one or more security and analysis features for existing repositories, you will see any results displayed on GitHub within minutes:

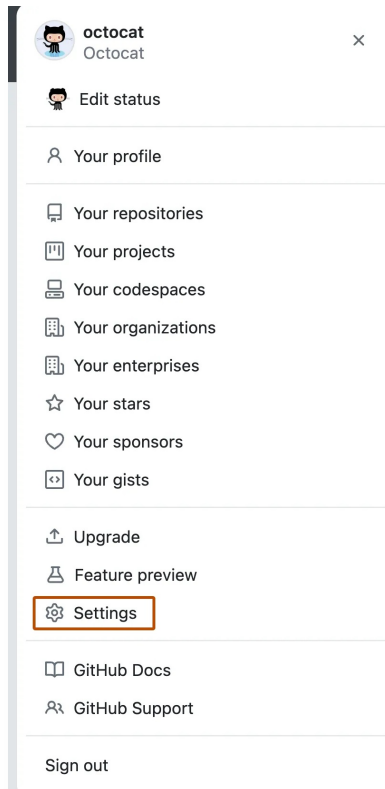
- All the existing repositories will have the selected configuration.
- New repositories will follow the selected configuration if you've enabled the checkbox for new repositories.
- We use the permissions to scan for manifest files to apply the relevant services.
- If enabled, you'll see dependency information in the dependency graph.
- If enabled, GitHub will generate Dependabot alerts for vulnerable dependencies or

malware.

- If enabled, Dependabot security updates will create pull requests to upgrade vulnerable dependencies when Dependabot alerts are triggered.

Enabling or disabling features for new repositories [↗](#)

- 1 In the upper-right corner of any page, click your profile photo, then click **Settings**.



- 2 In the "Security" section of the sidebar, click **Code security and analysis**.
- 3 Under "Code security and analysis", to the right of the feature, enable or disable the feature by default for new repositories that you own.

Further reading [↗](#)

- ["About the dependency graph"](#)
- ["About Dependabot alerts"](#)
- ["Keeping your dependencies updated automatically with Dependabot version updates"](#)

Legal

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