

Managing security and analysis settings for your repository

In this article

- Enabling or disabling security and analysis features for public repositories
- Enabling or disabling security and analysis features for private repositories
- Granting access to security alerts
- Removing access to security alerts
- Allowing validity checks for partner patterns in a repository
- Further reading

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

Who can use this feature

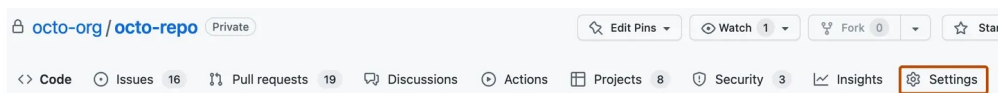
People with admin permissions to a repository can manage security and analysis settings for the repository.

Note: When Dependabot alerts are enabled or disabled at the enterprise level, it overrides the repository level settings for Dependabot alerts. For more information, see "[Configuring Dependabot alerts](#)."

Enabling or disabling security and analysis features for public repositories [↗](#)

You can manage a subset of security and analysis features for public repositories. Other features are permanently enabled, including dependency graph and secret scanning alerts for partners.

- 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 Under "Code security and analysis", to the right of the feature, click **Disable** or **Enable**.

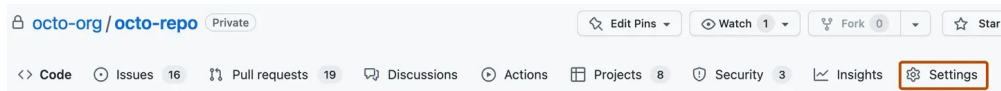
Enabling or disabling security and analysis features

for private repositories [↗](#)

You can manage the security and analysis features for your private or internal repository. If your organization belongs to an enterprise with a license for GitHub Advanced Security then extra options are available. For more information, see "[About GitHub Advanced Security](#)."

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

- 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 Under "Code security and analysis", to the right of the feature, click **Disable** or **Enable**. The control for "GitHub Advanced Security" is disabled if your enterprise has no available licenses for Advanced Security.

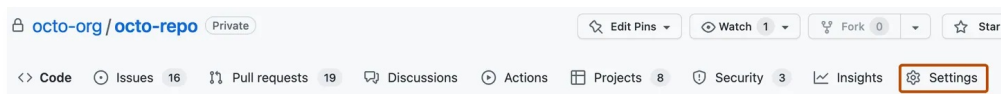
Note: If you disable GitHub Advanced Security, dependency review, secret scanning alerts for users and code scanning are disabled. Any workflows, SARIF uploads, or API calls for code scanning will fail. If GitHub Advanced Security is re-enabled, code scanning will return to its previous state.

Granting access to security alerts [↗](#)

Security alerts for a repository are visible to people with write, maintain, or admin access to the repository and, when the repository is owned by an organization, organization owners. You can give additional teams and people access to the alerts.

Organization owners and repository administrators can only grant access to view security alerts, such as secret scanning alerts, to people or teams who have write access to the repo.

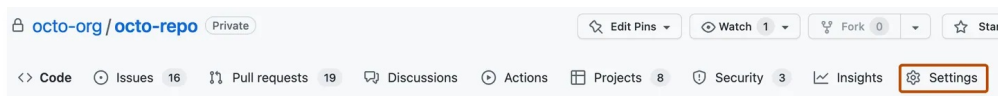
- 1 On GitHub.com, navigate to the main page of the repository.
- 2 Under your repository name, click ⚙️ **Settings**. If you cannot see the "Settings" tab, select the ... dropdown menu, then click **Settings**.



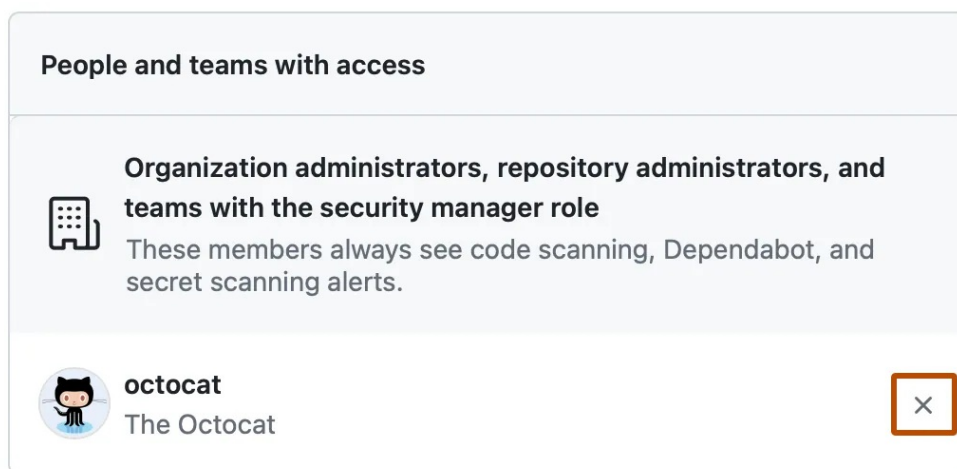
- 3 In the "Security" section of the sidebar, click 🔒 **Code security and analysis**.
- 4 Under "Access to alerts", in the search field, start typing the name of the person or team you'd like to find, then click a name in the list of matches.
- 5 Click **Save changes**.

Removing access to security alerts [🔗](#)

- 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 Under "Access to alerts", to the right of the person or team whose access you'd like to remove, click ✕.



- 5 Click **Save changes**.

Allowing validity checks for partner patterns in a repository [🔗](#)

Note: Validity checks for partner patterns is currently in beta and subject to change.

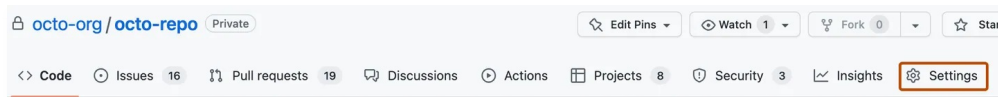
Validity checks for partner patterns is available on all types of repositories on GitHub.com. To use this feature, you must have a license for GitHub Advanced Security.


You can allow secret scanning to automatically check the validity of a secret found in your repository by sending it to the relevant partner. Alternatively, organization owners and enterprise administrators can enable the feature for all repositories in the organization or enterprise settings. For more information, see "[Allowing validity checks for partner patterns in an organization](#)" and "[Managing GitHub Advanced Security features for your enterprise](#)."

Note: When you enable automatic validity checks for a repository, you also allow on-demand validity checks to be performed for patterns detected in that repository.

- 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 Under Secret scanning, select the checkbox next to "Automatically verify if a secret is valid by sending it to the relevant partner".

Further reading

- ["Securing your repository"](#)
- ["Managing security and analysis settings for your organization"](#)

Legal

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