

Managing security and analysis settings for your repository

In this article

- Enabling or disabling security and analysis features
- Granting access to security alerts
- Removing access to security alerts
- Further reading

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

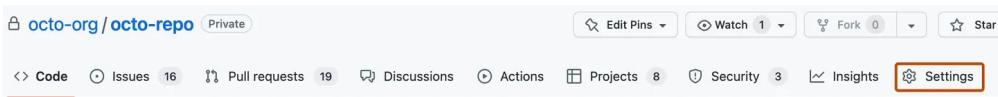
Who can use this feature

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

Enabling or disabling security and analysis features

You can manage the security and analysis features for your 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](#)."

- 1 On your GitHub Enterprise Server instance, 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.

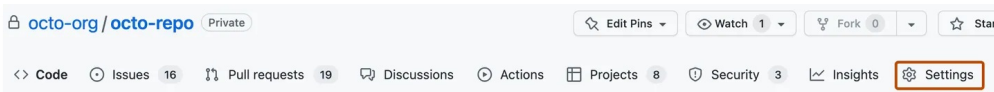
Note: If you disable GitHub Advanced Security, secret scanning and code scanning are disabled. Any workflows, SARIF uploads, or API calls for code scanning will fail. If GitHub Advanced Security is re-enabled, code scanning will return to its previous state.


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.

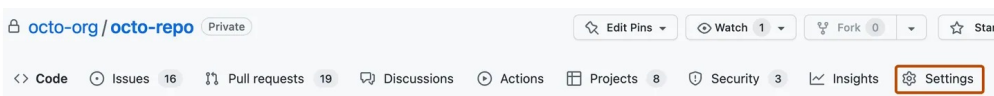
- 1 On your GitHub Enterprise Server instance, navigate to the main page of the repository.
- 2 Under your repository name, click  **Settings**. If you cannot see the "Settings" tab, select the ... dropdown menu, then click **Settings**.




- 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 your GitHub Enterprise Server instance, 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 **x**.

People and teams with access



Organization administrators, repository administrators, and teams with the security manager role

These members always see code scanning, Dependabot, and secret scanning alerts.



octocat
The Octocat



5 Click **Save changes**.

Further reading [↗](#)

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

Legal

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