This article is also available in French.

GitHub Docs

Version: Free, Pro, & Team ▾

Search GitHub Docs

Sign up

Repositories / Manage repository settings / Enable features / Security & analysis

Managing security and analysis settings for your repository

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.
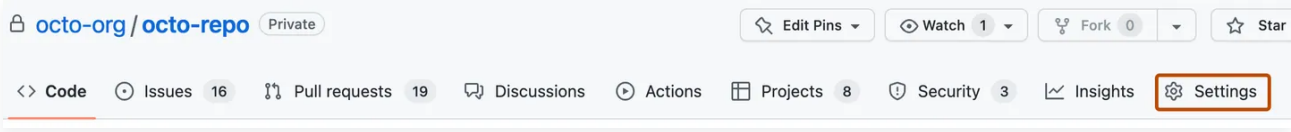
In this article

- 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
- Further reading

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, 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**.
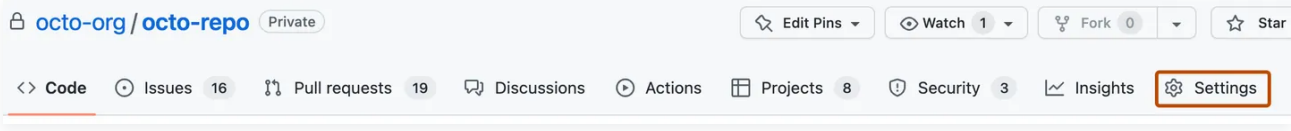

3. In the "Security" section of the sidebar, click 🔍 **Code security and analysis**.

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. Organizations that use GitHub Enterprise Cloud with Advanced Security have extra options available. For more information, see the GitHub Enterprise Cloud documentation.

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

1. On GitHub, 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**.
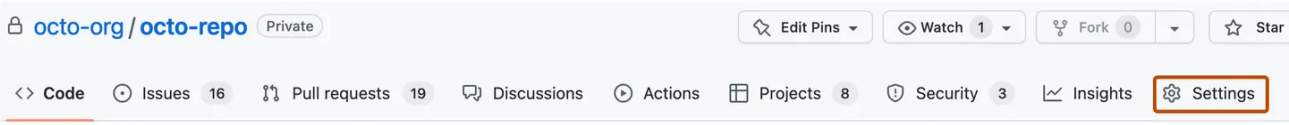
④ Under "Code security and analysis", to the right of the feature, click **Disable** or **Enable**.

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, 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, 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**.
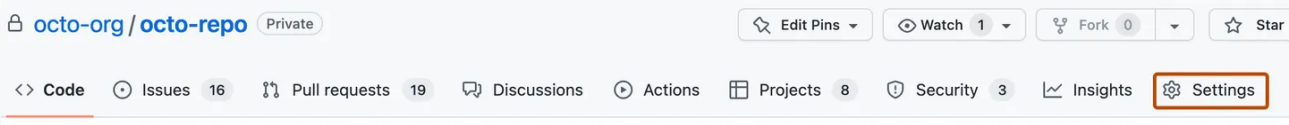
③ In the "Security" section of the sidebar, click ◉ **Code security and analysis**.

④ Under "Access to alerts", to the right of the person or team whose access you'd like to remove, click ✕.
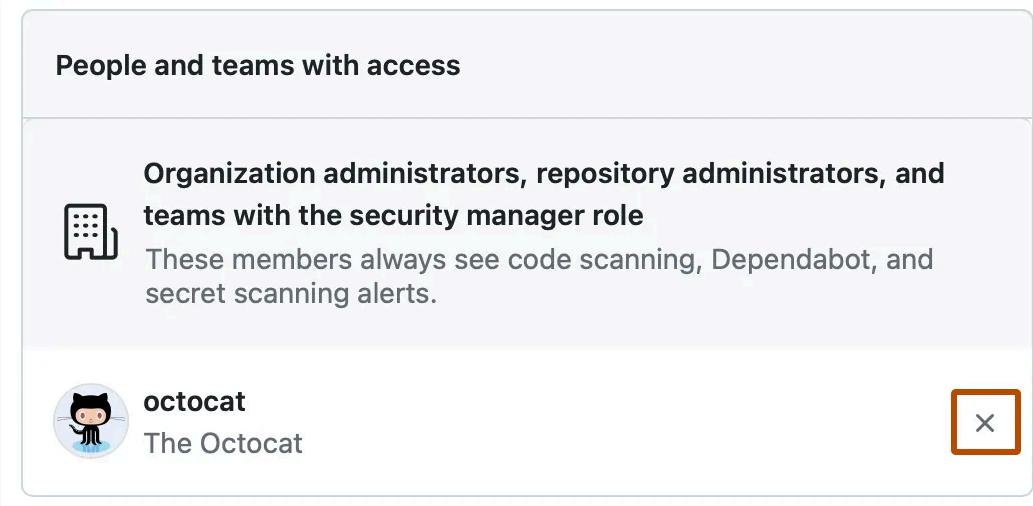
⑤ Click **Save changes**.

Further reading 🔗

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

Help and support

Did you find what you needed?

👍 Yes   👎 No

Privacy policy

Help us make these docs great!

All GitHub docs are open source. See something that's wrong or unclear? Submit a pull request.

⤺ Make a contribution

Learn how to contribute

Still need help?

👥 Ask the GitHub community

💬 Contact support

Legal

© 2024 GitHub, Inc.   Terms   Privacy   Status   Pricing   Expert services   Blog