

Configuring secret scanning for your repositories

In this article

Enabling secret scanning alerts for users

Excluding directories from secret scanning alerts for users

Further reading

You can configure how GitHub scans your repositories for leaked secrets and generates alerts.

Who can use this feature

People with admin permissions to a repository can enable secret scanning for the repository.


Secret scanning alerts for partners runs automatically on public repositories and public npm packages to notify service providers about leaked secrets on GitHub.com. Secret scanning alerts for users are available for free on all public repositories. Organizations using GitHub Enterprise Cloud with a license for GitHub Advanced Security can also enable secret scanning alerts for users on their private and internal repositories. For more information, see "[About secret scanning](#)" and "[About GitHub Advanced Security](#)." For information about how you can try GitHub Advanced Security for free, see "[Setting up a trial of GitHub Advanced Security](#)."

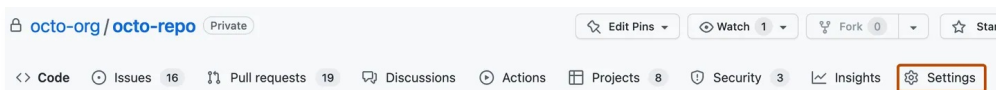
Enabling secret scanning alerts for users


You can enable secret scanning alerts for users for any repository that is owned by an organization. Once enabled, secret scanning scans for any secrets in your entire Git history on all branches present in your GitHub repository. Secret scanning also searches issue descriptions and comments for secrets.

You can also enable secret scanning for multiple repositories in an organization at the same time. For more information, see "[Securing your organization](#)."

Note: If your organization is owned by an enterprise account, an enterprise owner can also enable secret scanning at the enterprise level. For more information, see "[Managing GitHub Advanced Security features for your enterprise](#)."

- 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 If Advanced Security is not already enabled for the repository, to the right of "GitHub Advanced Security", click **Enable**.
- 5 Review the impact of enabling Advanced Security, then click **Enable GitHub Advanced Security for this repository**.
- 6 When you enable Advanced Security, secret scanning may automatically be enabled for the repository due to the organization's settings. If "Secret scanning" is shown with an **Enable** button, you still need to enable secret scanning by clicking **Enable**. If you see a **Disable** button, secret scanning is already enabled.

Secret scanning

Receive alerts on GitHub for detected secrets, keys, or other tokens.

GitHub will always send alerts to partners for detected secrets in public repositories. [Learn more about partner patterns](#).

Enable

- 7 Optionally, if you want to enable push protection, click **Enable** to the right of "Push protection." When you enable push protection for your organization or repository, secret scanning also checks pushes for high-confidence secrets (those identified with a low false positive rate). Secret scanning lists any secrets it detects so the author can review the secrets and remove them or, if needed, allow those secrets to be pushed. For more information, see "[Push protection for repositories and organizations](#)."

Secret scanning

Receive alerts on GitHub for detected secrets, keys, or other tokens.

Disable

Push protection

Block commits that contain [supported secrets](#).

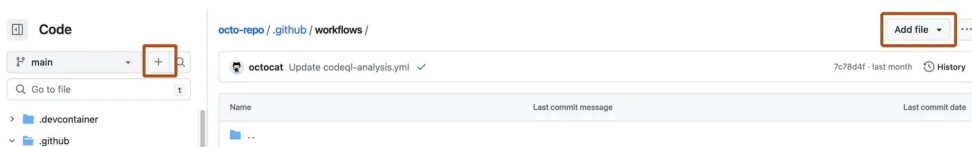
Enable

Excluding directories from secret scanning alerts for users

You can configure a `secret_scanning.yml` file to exclude directories from secret scanning, including when you use push protection. For example, you can exclude directories that contain tests or randomly generated content.

- 1 On GitHub.com, navigate to the main page of the repository.
- 2 Above the list of files, select the **Add file** ▾ dropdown menu, then click + **Create new file**.

Alternatively, you can click + in the file tree view on the left.



- 3 In the file name field, type `.github/secret_scanning.yml`.
- 4 Under **Edit new file**, type `paths-ignore:` followed by the paths you want to exclude from secret scanning.

```
paths-ignore:  
- "foo/bar/*.js"
```

You can use special characters, such as `*` to filter paths. For more information about filter patterns, see "[Workflow syntax for GitHub Actions](#)."

Notes:

- If there are more than 1,000 entries in `paths-ignore`, secret scanning will only exclude the first 1,000 directories from scans.
- If `secret_scanning.yml` is larger than 1 MB, secret scanning will ignore the entire file.

You can also ignore individual alerts from secret scanning. For more information, see "[Managing alerts from secret scanning](#)."

Further reading

- "[Managing security and analysis settings for your organization](#)"
- "[Defining custom patterns for secret scanning](#)"

Legal

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