

Managing alerts from secret scanning

In this article

- Managing secret scanning alerts
- Reviewing GitHub token metadata
- Securing compromised secrets
- Configuring notifications for secret scanning alerts
- Auditing responses to secret scanning alerts


You can view and close alerts for secrets checked in to your repository.

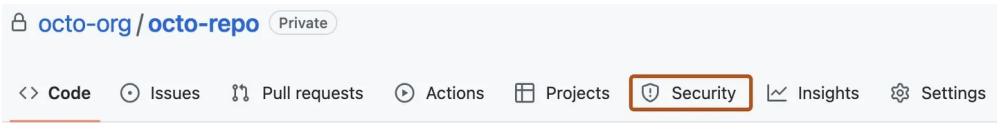
Who can use this feature

People with admin access to a repository can view and dismiss secret scanning alerts for the repository.

Secret scanning is available for organization-owned repositories in GitHub Enterprise Server if your enterprise has a license for GitHub Advanced Security. For more information, see "[About secret scanning](#)" and "[About GitHub Advanced Security](#)."

Managing secret scanning alerts

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



- 3 In the left sidebar, under "Vulnerability alerts", click **Secret scanning**.
- 4 Under "Secret scanning" click the alert you want to view.
- 5 Optionally, if the leaked secret is a GitHub token, check the validity of the secret and follow the remediation steps.

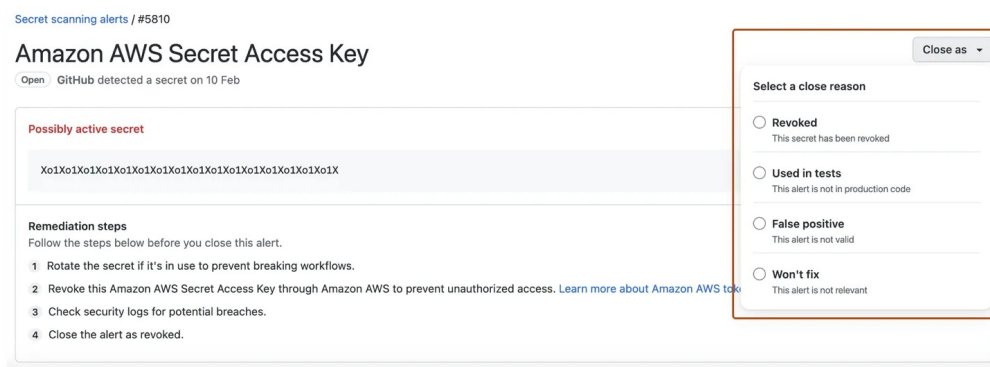
Note: Validity check for GitHub tokens is currently in public beta and subject to change.

GitHub provides information about the validity of the secret, for GitHub tokens only.

Validity	Result
Active secret	GitHub confirmed this secret is active

Active secret	GitHub checked with this secret's provider and found that the secret is active
Possibly active secret	GitHub does not support validation checks for this token type yet
Possibly active secret	GitHub could not verify this secret
Secret appears inactive	You should make sure no unauthorized access has already occurred

- 6 Optionally, if the leaked secret is a GitHub token, you can also review the token metadata. For more information on reviewing token metadata, see "[Reviewing GitHub token metadata](#)."
- 7 To dismiss an alert, select the "Close as" dropdown menu and click a reason for resolving an alert.



- 8 Optionally, in the "Comment" field, add a dismissal comment. The dismissal comment will be added to the alert timeline and can be used as justification during auditing and reporting. You can view the history of all dismissed alerts and dismissal comments in the alert timeline. You can also retrieve or set a comment by using the Secret scanning API. The comment is contained in the `resolution_comment` field. For more information, see "[Secret scanning](#)" in the REST API documentation.
- 9 Click **Close alert**.

Reviewing GitHub token metadata [↗](#)

Note: Metadata for GitHub tokens is currently in public beta and subject to change.

In the view for an active GitHub token alert, you can review certain metadata about the token. This metadata may help you identify the token and decide what remediation steps to take. For more information on viewing individual alerts, see "[Managing secret scanning alerts](#)."

Tokens, like personal access token and other credentials, are considered personal information. For more information about using GitHub tokens, see [GitHub's Privacy Statement](#) and [Acceptable Use Policies](#).

Active secret

GitHub confirmed this secret is active.

github_pat



Secret Details

Secret name

repo permissions only

Secret owner



octo-mona

Creation date

March 10, 2023

Expiration date

March 17, 2023

Last used date

March 10, 2023

Organization Access

Access to mona-test-org

Remediation steps

Follow the steps below before you close this alert.

- 1 Rotate the secret if it's in use to prevent breaking workflows.
- 2 Revoke this GitHub Personal Access Token through GitHub to prevent unauthorized access. [Learn more about GitHub tokens.](#)
- 3 Check security logs for potential breaches.
- 4 Close the alert as revoked.

Metadata for GitHub tokens is available for active tokens in any repository with secret scanning enabled. If a token has been revoked or its status cannot be validated, metadata will not be available. GitHub auto-revokes GitHub tokens in public repositories, so metadata for GitHub tokens in public repositories is unlikely to be available. The following metadata is available for active GitHub tokens:

Metadata

Description

Secret name

The name given to the GitHub token by its creator

Secret owner

The GitHub handle of the token's owner

Created on

Date the token was created

Expired on

Date the token expired

Last used on

Date the token was last used

Access

Whether the token has organization access

Securing compromised secrets 🔑

Once a secret has been committed to a repository, you should consider the secret compromised. GitHub recommends the following actions for compromised secrets:

- For a compromised GitHub personal access token, delete the compromised token, create a new token, and update any services that use the old token. For more information, see "[Managing your personal access tokens.](#)"
 - Identify any actions taken by the compromised token on your enterprise's resources. For more information, see "[Identifying audit log events performed by an access token.](#)"
- For all other secrets, first verify that the secret committed to GitHub Enterprise Server is valid. If so, create a new secret, update any services that use the old secret, and then delete the old secret.

Configuring notifications for secret scanning alerts

Notifications are different for incremental scans and historical scans.

Incremental scans


When a new secret is detected, GitHub Enterprise Server notifies all users with access to security alerts for the repository according to their notification preferences. These users include:

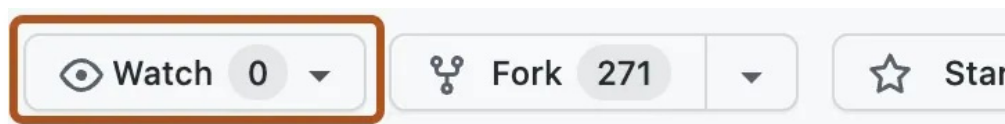
- Repository administrators
- Security managers
- Users with with custom roles with read/write access
- Organization owners and enterprise owners, if they are administrators of repositories where secrets were leaked

Note: Commit authors who've accidentally committed secrets will be notified, regardless of their notification preferences.

You will receive an email notification if:

- You are watching the repository.
- You have enabled notifications for "All Activity", or for custom "Security alerts" on the repository.
- In your notification settings, under "Subscriptions", then under "Watching", you have selected to receive notifications by email.

- 1 On your GitHub Enterprise Server instance, navigate to the main page of the repository.
- 2 To start watching the repository, select  **Watch**.



- 3 In the dropdown menu, click **All Activity**. Alternatively, to only subscribe to security alerts, click **Custom**, then click **Security alerts**.
- 4 Navigate to the notification settings for your personal account. These are available at <https://github.com/settings/notifications>.
- 5 On your notification settings page, under "Subscriptions", then under "Watching", select the **Notify me** dropdown.
- 6 Select "Email" as a notification option, then click **Save**.

Subscriptions

Watching

Notifications for all repositories, teams, or conversations you're watching. [View watched repositories](#)

Notify me: on GitHub ▾

☒ On GitHub

☒ Email

Cancel

Save

and custom

tions you are participating in, or if someone cites you with an @mention. Also for all

pecific events.

Ignored repositories

You'll never be notified. [View ignored repositories](#)

For more information about setting up notification preferences, see "[Managing security and analysis settings for your repository](#)" and "[Configuring your watch settings for an individual repository](#)."

Historical scans [↗](#)

For historical scans, GitHub Enterprise Server notifies the following users:

- Organization owners, enterprise owners, and security managers—whenever a historical scan is complete, even if no secrets are found.
- Repository administrators, security managers, and users with custom roles with read/write access—whenever a historical scan detects a secret, and according to their notification preferences.

We do *not* notify commit authors.

For more information about setting up notification preferences, see "[Managing security and analysis settings for your repository](#)" and "[Configuring your watch settings for an individual repository](#)."

Auditing responses to secret scanning alerts [↗](#)

You can audit the actions taken in response to secret scanning alerts using GitHub tools. For more information, see "[Auditing security alerts](#)."

Legal

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