Reviewing your security log

You can review the security log for your personal account to better understand actions you've performed and actions others have performed that involve you.

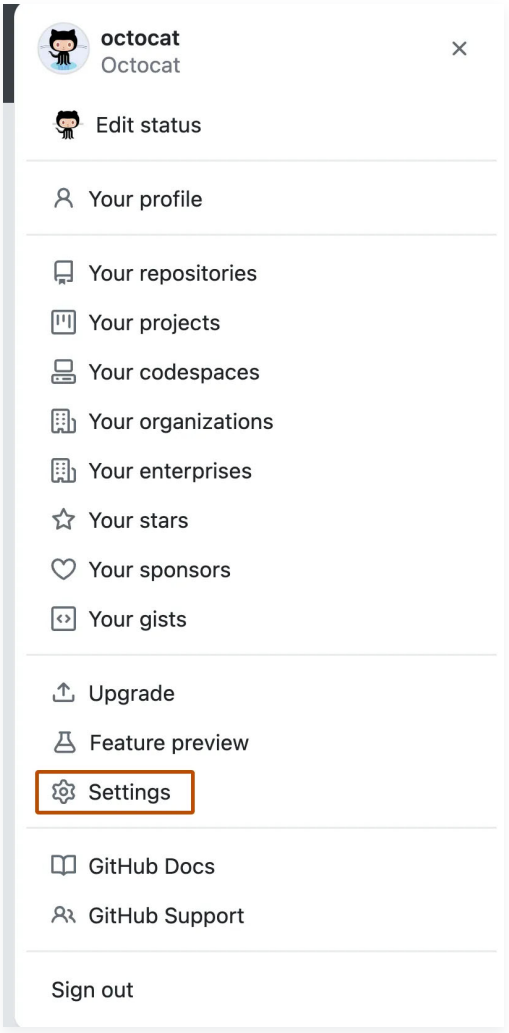
In this article

Accessing your security log
Searching your security log
Exporting your security log

Accessing your security log

The security log lists all actions performed within the last 90 days.

1. In the upper-right corner of any page, click your profile photo, then click **Settings**.



2 In the "Archives" section of the sidebar, click **Security log**.

Searching your security log

The name for each audit log entry is composed of the `action` object or category qualifier, followed by an operation type. For example, the `repo.create` entry refers to the `create` operation on the `repo` category.

Each audit log entry shows applicable information about an event, such as:

- The organization an action was performed in
- The user (actor) who performed the action
- The user affected by the action
- Which repository an action was performed in

- The action that was performed
- Which country the action took place in
- The date and time the action occurred

Note that you cannot search for entries using text. You can, however, construct search queries using a variety of filters. Many operators used when querying the log, such as `-`, `>`, or `<`, match the same format as searching across GitHub. For more information, see "About searching on GitHub."

Search based on operation

Use the `operation` qualifier to limit actions to specific types of operations. For example:

- `operation:access` finds all events where a resource was accessed.
- `operation:authentication` finds all events where an authentication event was performed.
- `operation:create` finds all events where a resource was created.
- `operation:modify` finds all events where an existing resource was modified.
- `operation:remove` finds all events where an existing resource was removed.
- `operation:restore` finds all events where an existing resource was restored.
- `operation:transfer` finds all events where an existing resource was transferred.

Search based on repository

Use the `repo` qualifier to limit actions to a specific repository. For example:

- `repo:my-org/our-repo` finds all events that occurred for the `our-repo` repository in the `my-org` organization.
- `repo:my-org/our-repo repo:my-org/another-repo` finds all events that occurred for both the `our-repo` and `another-repo` repositories in the `my-org` organization.
- `-repo:my-org/not-this-repo` excludes all events that occurred for the `not-this-repo` repository in the `my-org` organization.

Note that you must include the account name within the `repo` qualifier; searching for just `repo:our-repo` will not work.

Search based on the user

The `actor` qualifier can scope events based on who performed the action. For example:

- `actor:octocat` finds all events performed by `octocat`.

- `actor:octocat actor:hubot` finds all events performed by `octocat` or `hubot`.
- `-actor:hubot` excludes all events performed by `hubot`.

Note that you can only use a GitHub username, not an individual's real name.

Search based on the action performed

The events listed in your security log are triggered by your actions. Actions are grouped into different categories. For the full list of events in each category, see "Security log events."

Category name	Description
`billing`	Contains all activities related to your billing information.
`codespaces`	Contains all activities related to GitHub Codespaces. For more information, see "GitHub Codespaces overview."
`marketplace_agreement_signature`	Contains all activities related to signing the GitHub Marketplace Developer Agreement.
`marketplace_listing`	Contains all activities related to listing apps in GitHub Marketplace.
`oauth_access`	Contains all activities related to OAuth access tokens.
`oauth_authorization`	Contains all activities related to authorizing OAuth apps. For more information, see "Authorizing OAuth apps."
`passkey`	Contains activities related to your passkeys. For more information, see "About passkeys."
`payment_method`	Contains all activities related to paying for your GitHub subscription.
`personal_access_token`	Contains activities related to fine-grained personal access tokens. For more information, see "Managing your personal access tokens."
`profile_picture`	Contains all activities related to your profile picture.
`project`	Contains all activities related to project boards.
`public_key`	Contains all activities related to your public SSH keys.

Category name	Description
`repo`	Contains all activities related to the repositories you own.
`sponsors`	Contains all events related to GitHub Sponsors and sponsor buttons (see "About GitHub Sponsors" and "Displaying a sponsor button in your repository")
`two_factor_authentication`	Contains all activities related to two-factor authentication.
`user`	Contains all activities related to your account.

Exporting your security log

You can export the log as JSON data or a comma-separated value (CSV) file with the **Export** dropdown menu.

To filter the results in your export, search by one or more of these supported qualifiers before using the **Export** dropdown menu.

Qualifier	Example value
`action`	team.create
`actor`	octocat
`user`	codertocat
`org`	octo-org
`repo`	octo-org/documentation
`created`	2019-06-01

After you export the log, you'll see the following keys and values in the resulting file.

Key	Example value
`action`	team.create

Key	Example value
`actor`	octocat
`user`	codertocat
`actor_location.country_code`	US
`org`	octo-org
`repo`	octo-org/documentation
`created_at`	1429548104000 (Timestamp shows the time since Epoch with milliseconds.)
`data.email`	octocat@nowhere.com
`data.hook_id`	245
`data.events`	["issues", "issue_comment", "pull_request", "pull_request_review_comment"]
`data.events_were`	["push", "pull_request", "issues"]
`data.target_login`	octocat
`data.old_user`	hubot
`data.team`	octo-org/engineering

Legal

© 2023 GitHub, Inc. Terms Privacy Status Pricing Expert services Blog