About the audit log for your enterprise

In this article

To support debugging and internal and external compliance, GitHub Enterprise Cloud provides logs of audited user, organization, and repository events.

About audit logs

The audit log lists events triggered by activities that affect your enterprise within the current month and up to the previous six months. The audit log retains Git events for seven days.

By default, only events from the past three months are displayed. To view older events, you must specify a date range with the `created` parameter. For more information, see "Understanding the search syntax."

The name for each audit log entry is composed of a category of events, 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 enterprise or 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
- The SAML SSO identity of the user (actor) who performed the action (public beta)
- For actions outside of the web UI, how the user (actor) authenticated
- Optionally, the source IP address for the user (actor) who performed the action

In addition to viewing your audit log, you can monitor activity in your enterprise in other ways, such as managing global webhooks. For more information, see "Exploring user activity in your enterprise." You can also use the audit log, and other tools, to monitor the actions taken in response to security alerts. For more information, see "Auditing security alerts."

Using your audit logs

As an enterprise owner, you can interact with the audit log data for your enterprise in several ways:

- You can view the audit log for your enterprise. For more information, see "Accessing the audit log for your enterprise."
- You can search the audit log for specific events and export audit log data. For more information, see "Searching the audit log for your enterprise" and "Exporting audit log activity for your enterprise".
- You can identify all events that were performed by a specific access token. For more information, see "Identifying audit log events performed by an access token."
- You can display the IP address associated with events in the audit log. For more information, see "Displaying IP addresses in the audit log for your enterprise."
- You can stream audit and Git events data from GitHub to an external data management system. For more information, see "Streaming the audit log for your enterprise."
- You can use the Audit log API to view actions performed in your enterprise. For more information, see "Using the audit log API for your enterprise."

For a full list of audit log actions that may appear in your enterprise audit log, see "Audit log events for your enterprise."

Further reading

- "Reviewing the audit log for your organization"