About the audit log for your enterprise

In this article

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

About audit logs 🔗

The audit log lists events triggered by activities that affect your enterprise. Audit logs for GitHub Enterprise Server are retained indefinitely, unless an enterprise owner configured a different retention period. For more information, see "Configuring the audit log for your enterprise."

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 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 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

In addition to viewing your audit log, you can monitor activity in your enterprise in other ways, such as viewing push logs and 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 or site administrator, 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. For more information, see "Searching the audit log for your enterprise".
- You can configure settings, such as the retention period for audit log events. For more information, see "Configuring the audit log for your enterprise."
- You can forward audit and system logs, from your enterprise to an third-party hosted monitoring system. For more information, see "Log forwarding."
- 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"
- "About system logs"