Using the audit log API for your enterprise

In this article

You can programmatically retrieve enterprise events with the REST API.

> **Who can use this feature**
> Enterprise owners and site administrators can use the audit log API.

Using the audit log API

You can interact with the audit log using the REST API. You can use the `read:audit_log` scope to access the audit log via the API.

Timestamps and date fields in the API response are measured in UTC epoch milliseconds.

To ensure your intellectual property is secure, and you maintain compliance for your enterprise, you can use the audit log REST API to keep copies of your audit log data and monitor:

- Access to your organization or repository settings
- Changes in permissions
- Added or removed users in an organization, repository, or team
- Users being promoted to admin
- Changes to permissions of a GitHub App
- Git events, such as cloning, fetching, and pushing (must be enabled, see "Configuring the audit log for your enterprise")

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."

For more information about the audit log REST API, see "GitHub Enterprise administration" and "Organizations."

Example 1: All events in an enterprise, for a specific date, with pagination

You can use page-based pagination. For more information about pagination, see "Using pagination in the REST API."

The query below searches for audit log events created on Jan 1st, 2022 in the `avocado-corp` enterprise, and return the first page with a maximum of 100 items per page using pagination. For more information about pagination, see "Using pagination in the REST API."

```
curl -H "Authorization: Bearer TOKEN" \
--request GET \
"https://api.github.com/enterprises/avocado-corp/audit-log?phrase=created:2022-01-01&page=1&per_page=100"
```

Example 2: Events for pull requests in an enterprise, for a specific date and actor

You can specify multiple search phrases, such as `created` and `actor`, by separating them in your formed URL with the `+` symbol or ASCII character code `%20`.

The query below searches for audit log events for pull requests, where the event occurred on or after Jan 1st, 2022 in the `avocado-corp` enterprise, and the action was performed by the `octocat` user:

```
curl -H "Authorization: Bearer TOKEN" \
--request GET \
"https://api.github.com/enterprises/avocado-corp/audit-log?phrase=action:pull_request+created:>=2022-01-01+actor:octocat"
```