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 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
- API requests (must be enabled)
- Git events, such as cloning, fetching, and pushing

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."

Each audit log API endpoint has a rate limit of 1,750 queries per hour for a given combination of user and IP address. To avoid rate limiting, integrations that query the audit log API should query at a maximum frequency of 1,750 queries per hour. Additionally, if your integration receives a rate limit error (typically a 403 or 429 response), it should wait before making another request to the API. For more information, see "Resources in the REST API" and "Best practices for using the REST API."

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 cursor 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 returns 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." The `--include` flag causes the headers to be returned along with the response.

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

If there are more than 100 results, the `link` header will include URLs to fetch the next, first, and previous pages of results.

```
link: <https://api.github.com/enterprises/13827/audit-log?%3A2022-11-
01=&per_page=100&after=MS42NjQzODMzNTk5MjdlKzEyfDloQzBxdURzaFdVbVlLWjkxRU9mNXc%3D&be
 rel="next",
<https://api.github.com/enterprises/13827/audit-log?%3A2022-11-
01=&per_page=100&after=&before=>; rel="first",
<https://api.github.com/enterprises/13827/audit-log?%3A2022-11-
01=&per_page=100&after=&before=MS42Njc4NDA2MjM4MzNlKzEyfExqeG5sUElvNEZMbG1XZHA5akdK
 rel="prev"
```

Copy the corresponding pagination link into your next request. For example:

```
curl -I -H "Authorization: Bearer TOKEN" \
--request GET \
"https://api.github.com/enterprises/13827/audit-log?%3A2022-11-
01=&per_page=100&after=MS42Njc4NDA2MjM5NDFlKzEyfHRYa3AwSkxUd2xyRjA5bWxfOS1RbFE%3D&be
```

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"
```