This version of GitHub Enterprise was discontinued on 2023-03-15. No patch releases will be made, even for critical security issues. For better performance, improved security, and new features, upgrade to the latest version of GitHub Enterprise. For help with the upgrade, contact GitHub Enterprise support.

Searching the audit log for your enterprise

In this article

You can search an extensive list of audited actions in your enterprise.

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

About search for the enterprise audit log

You can search your enterprise audit log directly from the user interface by using the **Filters** dropdown, or by typing a search query.

For more information about viewing your enterprise audit log, see "Accessing the audit log for your enterprise."

You can also use the API to retrieve audit log events. For more information, see "Using the audit log API for your enterprise."

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 Enterprise Server. For more information, see "About searching on GitHub."

> **Note**: 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."

Search query filters

Filter	Description

`Yesterday's activity`	All actions created in the past day.
`Enterprise account management`	All actions in the `business` category.
`Organization membership`	All actions for when a new user was invited to join an organization.
`Team management`	All actions related to team management. - When a user account or repository was added or removed from a team - When a team maintainer was promoted or demoted - When a team was deleted
`Repository management`	All actions for repository management. - When a repository was created or deleted - When the repository visibility was changed - When a team was added or removed from a repository
`Hook activity`	All actions for webhooks and pre-receive hooks.
`Security management`	All actions concerning SSH keys, deploy keys, security keys, 2FA, and SAML single sign-on credential authorization, and vulnerability alerts for repositories.

Search query syntax

You can compose a search query from one or more `key:value` pairs, separated by AND/OR logical operators. For example, to see all actions that have affected the repository `octocat/Spoon-Knife` since the beginning of 2017:

```
repo:"octocat/Spoon-Knife" AND created:>=2017-01-01
```

The `key:value` pairs that can be used in a search query are:

Key	Value
`action`	Name of the audited action.
`actor`	Name of the user account that initiated the action.
`actor_id`	ID of the user account that initiated the action.
`actor_ip`	IP address from which the action was initiated.
`business`	Name of the enterprise affected by the action (if applicable).
`business_id`	ID of the enterprise affected by the action (if applicable).
`ip`	IP address of the actor.
`note`	Miscellaneous event-specific information (in either plain text or JSON format).
`oauth_app_id`	ID of the OAuth app associated with the action.

`operation`	Operation type that corresponds with the action. Operation types are `create`, `access`, `modify`, `remove`, `authentication`, `transfer`, and `restore`.
`org`	Name of the organization affected by the action (if applicable).
`org_id`	ID of the organization affected by the action (if applicable).
`repo_id`	ID of the repository affected by the action (if applicable).
`repository`	Name with owner of the repository where the action occurred (such as `octocat/octo-repo`).
`user_id`	ID of the user affected by the action.
`user`	Name of the user affected by the action.

To see actions grouped by category, you can also use the action qualifier as a `key:value` pair. For more information, see "Search based on the action performed."

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

Searching the audit log

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 Enterprise Server username, not an individual's real name.

Search based on the action performed

To search for specific events, use the `action` qualifier in your query. For example:

- `action:team` finds all events grouped within the team category.
- `-action:hook` excludes all events in the webhook category.

Each category has a set of associated actions that you can filter on. For example:

- `action:team.create` finds all events where a team was created.
- `-action:hook.events_changed` excludes all events where the events on a webhook have been altered.

Actions that can be found in your enterprise audit log are grouped within the following categories:

Category name	Description
`artifact`	Contains activities related to GitHub Actions workflow run artifacts.
`business`	Contains activities related to business settings for an enterprise.
`checks`	Contains activities related to check suites and runs.
`commit_comment`	Contains activities related to updating or deleting commit comments.
`config_entry`	Contains activities related to configuration settings. These events are only visible in the site admin audit log.
`dependabot_alerts`	Contains organization-level configuration activities for Dependabot alerts in existing repositories. For more information, see "[About Dependabot alerts](#)."
`dependabot_alerts_new_repos`	Contains organization-level configuration activities for Dependabot alerts in new repositories created in the organization.
`dependabot_repository_access`	Contains activities related to which private repositories in an organization Dependabot is allowed to access.
`dependabot_security_updates`	Contains organization-level configuration activities for Dependabot security updates in existing repositories. For more information, see "[Configuring Dependabot security updates](#)."
`dependabot_security_updates_new_repos`	Contains organization-level configuration activities for Dependabot security updates for

	activities for Dependabot security updates for new repositories created in the organization.
`dependency_graph`	Contains organization-level configuration activities for dependency graphs for repositories. For more information, see "[About the dependency graph](#)."
`dependency_graph_new_repos`	Contains organization-level configuration activities for new repositories created in the organization.
`dotcom_connection`	Contains activities related to GitHub Connect.
`enterprise`	Contains activities related to enterprise settings.
`hook`	Contains activities related to webhooks.
`integration`	Contains activities related to integrations in an account.
`integration_installation`	Contains activities related to integrations installed in an account.
`integration_installation_request`	Contains activities related to organization member requests for owners to approve integrations for use in the organization.
`issue`	Contains activities related to pinning, transferring, or deleting an issue in a repository.
`issue_comment`	Contains activities related to pinning, transferring, or deleting issue comments.
`issues`	Contains activities related to enabling or disabling issue creation for an organization.
`members_can_create_pages`	Contains activities related to managing the publication of GitHub Pages sites for repositories in the organization. For more information, see "[Managing the publication of GitHub Pages sites for your organization](#)."
`members_can_create_private_pages`	Contains activities related to managing the publication of private GitHub Pages sites for repositories in the organization.
`members_can_create_public_pages`	Contains activities related to managing the publication of public GitHub Pages sites for repositories in the organization.
`members_can_delete_repos`	Contains activities related to enabling or disabling repository creation for an organization.
`oauth_access`	Contains activities related to OAuth access tokens.
`oauth_application`	Contains activities related to OAuth apps.
`org`	Contains activities related to organization membership.
`org_credential_authorization`	Contains activities related to authorizing credentials for use with SAML single sign-on.

`organization_default_label`	Contains activities related to default labels for repositories in an organization.
`organization_domain`	Contains activities related to verified organization domains.
`organization_projects_change`	Contains activities related to organization-wide project boards in an enterprise.
`pre_receive_environment`	Contains activities related to pre-receive hook environments.
`pre_receive_hook`	Contains activities related to pre-receive hooks.
`private_instance_encryption`	Contains activities related to enabling private mode for an enterprise.
`private_repository_forking`	Contains activities related to allowing forks of private and internal repositories, for a repository, organization or enterprise.
`project`	Contains activities related to project boards.
`project_field`	Contains activities related to field creation and deletion in a project board.
`project_view`	Contains activities related to view creation and deletion in a project board.
`protected_branch`	Contains activities related to protected branches.
`public_key`	Contains activities related to SSH keys and deploy keys.
`pull_request`	Contains activities related to pull requests.
`pull_request_review`	Contains activities related to pull request reviews.
`pull_request_review_comment`	Contains activities related to pull request review comments.
`repo`	Contains activities related to the repositories owned by an organization.
`repository_image`	Contains activities related to images for a repository.
`repository_invitation`	Contains activities related to invitations to join a repository.
`repository_projects_change`	Contains activities related to enabling projects for a repository or for all repositories in an organization.
`repository_secret_scanning`	Contains repository-level activities related to secret scanning. For more information, see "About secret scanning."
`repository_vulnerability_alert`	Contains activities related to Dependabot alerts.

`restrict_notification_delivery`	Contains activities related to the restriction of email notifications to approved or verified domains for an enterprise.
`secret_scanning`	Contains organization-level configuration activities for secret scanning in existing repositories. For more information, see "[About secret scanning](#)."
`secret_scanning_new_repos`	Contains organization-level configuration activities for secret scanning for new repositories created in the organization.
`security_key`	Contains activities related to security keys registration and removal.
`ssh_certificate_authority`	Contains activities related to a SSH certificate authority in an organization or enterprise.
`ssh_certificate_requirement`	Contains activities related to requiring members use SSH certificates to access organization resources.
`staff`	Contains activities related to a site admin performing an action.
`team`	Contains activities related to teams in an organization.
`team_discussions`	Contains activities related to managing team discussions for an organization.
`two_factor_authentication`	Contains activities related to two-factor authentication.
`user`	Contains activities related to users in an enterprise or organization.
`user_license`	Contains activities related to a user occupying a licensed seat in, and being a member of, an enterprise.
`workflows`	Contains activities related to GitHub Actions workflows.

Search based on time of action

Use the `created` qualifier to filter events in the audit log based on when they occurred.

Date formatting must follow the [ISO8601](#) standard, which is `YYYY-MM-DD` (year-month-day). You can also add optional time information `THH:MM:SS+00:00` after the date, to search by the hour, minute, and second. That's `T`, followed by `HH:MM:SS` (hour-minutes-seconds), and a UTC offset (`+00:00`).

When you search for a date, you can use greater than, less than, and range qualifiers to further filter results. For more information, see "[Understanding the search syntax](#)."

For example:

- `created:2014-07-08` finds all events that occurred on July 8th, 2014.
- `created:>=2014-07-08` finds all events that occurred on or after July 8th, 2014.
- `created:<=2014-07-08` finds all events that occurred on or before July 8th, 2014.

- `created:2014-07-01..2014-07-31` finds all events that occurred in the month of July 2014.

Search based on location

Using the qualifier `country`, you can filter events in the audit log based on the originating country. You can use a country's two-letter short code or full name. Countries with spaces in their name will need to be wrapped in quotation marks. For example:

- `country:de` finds all events that occurred in Germany.
- `country:Mexico` finds all events that occurred in Mexico.
- `country:"United States"` all finds events that occurred in the United States.