

Searching the audit log for your enterprise

In this article

- About search for the enterprise audit log
- Search query filters
- Search query syntax
- Searching the audit log

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

Who can use this feature

Enterprise owners 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](#)."

Note: Git events are not included in search results.

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 Cloud. For more information, see "[About searching on GitHub](#)."

Note: 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](#)."

Search query filters

Filter	Description
--------	-------------

Yesterday's activity	All actions created in the past day.
----------------------	--------------------------------------

Enterprise account management	All actions in the <code>business</code> 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
Billing updates	All actions concerning how your enterprise pays for GitHub and for when your billing email address was changed.
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
<code>action</code>	Name of the audited action.
<code>actor</code>	Name of the user account that initiated the action.
<code>created</code>	Time at which the action occurred.
<code>country</code>	Name of the country where the actor was when performing the action.
<code>country_code</code>	Two-letter short code of the country where the actor was when performing the action.
<code>hashed_token</code>	The token used to authenticate for the action (if applicable, see " Identifying audit log events performed by an access token ").
<code>ip</code>	IP address of the actor.
<code>operation</code>	Operation type that corresponds with the action. Operation types are <code>create</code> , <code>access</code> , <code>modify</code> ,

remove , authentication , transfer , and restore .

repository

Name with owner of the repository where the action occurred (such as octocat/octo-repo).

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 Cloud 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
account	Contains activities related to an organization account.
advisory_credit	Contains activities related to crediting a contributor for a security advisory in the GitHub Advisory Database. For more information, see " About repository security advisories ."
artifact	Contains activities related to GitHub Actions workflow run artifacts.
audit_log_streaming	Contains activities related to streaming audit logs for organizations in an enterprise account.
billing	Contains activities related to an organization's billing.
business	Contains activities related to business settings for an enterprise.
business_advanced_security	Contains activities related to GitHub Advanced Security in an enterprise. For more information, see " Managing GitHub Advanced Security features for your enterprise ."
business_secret_scanning	Contains activities related to secret scanning in an enterprise. For more information, see " Managing GitHub Advanced Security features for your enterprise ."
business_secret_scanning_automatic_validity_checks	Contains activities related to enabling or disabling automatic validity checks for secret scanning in an enterprise. For more information, see " Managing GitHub Advanced Security features for your enterprise ."
business_secret_scanning_custom_pattern	Contains activities related to custom patterns for secret scanning in an enterprise.
business_secret_scanning_custom_pattern_push_protection	Contains activities related to push protection of a custom pattern for secret scanning in an enterprise. For more information, see " Defining custom patterns for secret scanning ."
business_secret_scanning_push_protection	Contains activities related to the push protection feature of secret scanning in an enterprise. For more information, see " Managing GitHub Advanced Security features for your enterprise ."
business_secret_scanning_push_protection_custom	Contains activities related to the custom

business_secret_scanning_push_protection_custom_message	Contains activities related to the custom message displayed when push protection is triggered in an enterprise. For more information, see " Managing GitHub Advanced Security features for your enterprise ."
checks	Contains activities related to check suites and runs.
codespaces	Contains activities related to an organization's codespaces.
commit_comment	Contains activities related to updating or deleting commit comments.
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 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.
enterprise_domain	Contains activities related to verified enterprise domains.
enterprise_installation	Contains activities related to GitHub Apps associated with an GitHub Connect enterprise connection.
environment	Contains activities related to GitHub Actions environments.
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.
ip_allow_list	Contains activities related to enabling or disabling the IP allow list for an organization.
ip_allow_list_entry	Contains activities related to the creation, deletion, and editing of an IP allow list entry for an 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.
marketplace_agreement_signature	Contains activities related to signing the GitHub Marketplace Developer Agreement.
marketplace_listing	Contains activities related to listing apps in GitHub Marketplace.
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.
members_can_view_dependency_insights	Contains organization-level configuration activities allowing organization members to view dependency insights.
migration	Contains activities related to transferring data from a <i>source</i> location (such as a GitHub.com organization or a GitHub Enterprise Server instance) to a <i>target</i> GitHub Enterprise Server instance.
oauth_access	Contains activities related to OAuth access tokens.
oauth_application	Contains activities related to OAuth apps.
oauth_authorization	Contains activities related to authorizing OAuth apps.

apps.

org	Contains activities related to organization membership.
org_credential_authorization	Contains activities related to authorizing credentials for use with SAML single sign-on.
org_secret_scanning_automatic_validity_checks	Contains activities related to enabling or disabling automatic validity checks for secret scanning in an organization. For more information, see " Managing security and analysis settings for your organization ."
org_secret_scanning_custom_pattern	Contains activities related to custom patterns for secret scanning in an organization. For more information, see " Defining custom patterns for secret scanning ."
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.
pages_protected_domain	Contains activities related to verified custom domains for GitHub Pages.
payment_method	Contains activities related to how an organization pays for GitHub.
prebuild_configuration	Contains activities related to prebuild configurations for GitHub Codespaces.
private_repository_forking	Contains activities related to allowing forks of private and internal repositories, for a repository, organization or enterprise.
profile_picture	Contains activities related to an organization's profile picture.
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.

comments.

repo	Contains activities related to the repositories owned by an organization.
repository_advisory	Contains repository-level activities related to security advisories in the GitHub Advisory Database. For more information, see " About repository security advisories ."
repository_content_analysis	Contains activities related to enabling or disabling data use for a private repository. For more information, see " Managing security and analysis settings for your repository ."
repository_dependency_graph	Contains repository-level activities related to enabling or disabling the dependency graph for a private repository. For more information, see " About the dependency graph ."
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_secret_scanning_automatic_validity_checks	Contains activities related to enabling or disabling automatic validity checks for secret scanning in a repository. For more information, see " Managing security and analysis settings for your repository ."
repository_secret_scanning_custom_pattern	Contains activities related to secret scanning custom patterns in a repository. For more information, see " Defining custom patterns for secret scanning ."
repository_secret_scanning_custom_pattern_push_protection	Contains activities related to push protection of a custom pattern for secret scanning in a repository. For more information, see " Defining custom patterns for secret scanning ."
repository_secret_scanning_push_protection	Contains activities related to the push protection feature of secret scanning in a repository. For more information, see " Push protection for repositories and organizations ."
repository_visibility_change	Contains activities related to allowing organization members to change repository visibilities for the organization.
repository_vulnerability_alert	Contains activities related to Dependabot alerts .
repository_vulnerability_alerts	Contains repository-level configuration activities for Dependabot alerts.
required_status_check	Contains activities related to required status

checks for protected branches.

restrict_notification_delivery	Contains activities related to the restriction of email notifications to approved or verified domains for an enterprise.
role	Contains activities related to custom repository roles .
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.
sponsors	Contains events related to sponsor buttons (see " Displaying a sponsor button in your repository ").
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.
sso_redirect	Contains activities related to automatically redirecting users to sign in (see " Enforcing policies for security settings in your enterprise ").
staff	Contains activities related to a site admin performing an action.
team	Contains activities related to teams in an organization.
team_sync_tenant	Contains activities related to team synchronization with an IdP for an enterprise or organization.
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.

Search based on the token that performed the action [↗](#)

Use the `hashed_token` qualifier to search based on the token that performed the action. Before you can search for a token, you must generate a SHA-256 hash. For more information, see "[Identifying audit log events performed by an access token](#)."

Legal

© 2023 GitHub, Inc. [Terms](#) [Privacy](#) [Status](#) [Pricing](#) [Expert services](#) [Blog](#)