

Cloud Audit Logs overview

This document provides a conceptual overview of Cloud Audit Logs.

Audit Logs: Querying Logs, P...

Google Cloud services write audit logs that record administrative activities and accesses within your Google Cloud resources. Audit logs help you answer "who did what, where, and when?" within your Google Cloud resources with the same level of transparency as in on-premises environments.



Enabling audit logs helps your security, auditing, and compliance entities monitor Google Cloud data and systems for possible vulnerabilities or external data misuse.

Note: Data Access audit logs help the Support team troubleshoot issues with your account. Therefore, we recommend keeping them enabled. For more Cloud Audit Logs best practices, see [Cloud Audit Logs best practices](/logging/docs/audit/best-practices) (/logging/docs/audit/best-practices).

Google Cloud services producing audit logs

For a list of Google Cloud services that provide audit logs, see [Google Cloud services with audit logs](/logging/docs/audit/services) (/logging/docs/audit/services). All Google Cloud services will eventually provide audit logs.

For an overview of Google Workspace audit logs, see [Audit logs for Google Workspace](/logging/docs/audit/gsuite-audit-logging) (/logging/docs/audit/gsuite-audit-logging).

Required roles

To view audit logs, you must have the appropriate [Identity and Access Management \(IAM\)](/iam/docs) (/iam/docs) permissions and roles:

- To get the permissions that you need to get read-only access to Admin Activity, Policy Denied, and System Event audit logs, ask your administrator to grant you the [Logs Viewer](#)

(<https://cloud.google.com/iam/docs/roles-permissions/logging#logging.viewer>)
(`roles/logging.viewer`) IAM role on your project.

If you have only the Logs Viewer role (`roles/logging.viewer`), then you cannot view Data Access audit logs that are in the `_Default` bucket.

- To get the permissions that you need to get access to all logs in the `_Required` and `_Default` buckets, including Data Access logs, ask your administrator to grant you the Private Logs Viewer

(<https://cloud.google.com/iam/docs/roles-permissions/logging#logging.privateLogViewer>)
(`roles/logging.privateLogViewer`) IAM role on your project.

The Private Logs Viewer role (`roles/logging.privateLogViewer`) includes the permissions contained in the Logs Viewer role (`roles/logging.viewer`), and those necessary to read Data Access audit logs in the `_Default` bucket.

For more information about the IAM permissions and roles that apply to audit logs data, see [Access control with IAM](/logging/docs/access-control) (`/logging/docs/access-control`).

Types of audit logs

Cloud Audit Logs provides the following audit logs for each Google Cloud project, folder, and organization:

- Admin Activity audit logs (`#admin-activity`)
- Data Access audit logs (`#data-access`)
- System Event audit logs (`#system-event`)
- Policy Denied audit logs (`#policy_denied`)

Note: Log entries written by Cloud Audit Logs are immutable.

Admin Activity audit logs

Admin Activity audit logs contain log entries for API calls or other actions that modify the configuration or metadata of resources. For example, these logs record when users create VM instances or change Identity and Access Management permissions.

Admin Activity audit logs are always written; you can't configure, exclude, or disable them. Even if you disable the Cloud Logging API, Admin Activity audit logs are still generated.

For a list of services that write Admin Activity audit logs and detailed information about which activities generate those logs, see [Google Cloud services with audit logs](/logging/docs/audit/services) (/logging/docs/audit/services).

Data Access audit logs

Data Access audit logs contain API calls that read the configuration or metadata of resources, as well as user-driven API calls that create, modify, or read user-provided resource data.

Publicly available resources that have the Identity and Access Management policies [**allAuthenticatedUsers**](/iam/docs/principals-overview#allauthenticatedusers) (/iam/docs/principals-overview#allauthenticatedusers) or [**allUsers**](/iam/docs/principals-overview#allusers) (/iam/docs/principals-overview#allusers) don't generate audit logs. Resources that can be accessed without logging into a Google Cloud, Google Workspace, Cloud Identity, or Drive Enterprise account don't generate audit logs. This helps protect end-user identities and information.

Data Access audit logs—except for BigQuery Data Access audit logs—are disabled by default because audit logs can be quite large. If you want Data Access audit logs to be written for Google Cloud services other than BigQuery, you must explicitly enable them. Enabling the logs might result in your Google Cloud project being charged for the additional logs usage. For instructions on enabling and configuring Data Access audit logs, see [**Enable Data Access audit logs**](/logging/docs/audit/configure-data-access) (/logging/docs/audit/configure-data-access).

For a list of services that write Data Access audit logs and detailed information about which activities generate those logs, see [Google Cloud services with audit logs](/logging/docs/audit/services) (/logging/docs/audit/services).

Data Access audit logs are stored in the [**_Default**](/logging/docs/store-log-entries#default-bucket) (/logging/docs/store-log-entries#default-bucket) log bucket unless you've routed them elsewhere. For more information, see the [**Storing and routing audit logs**](#storing_and_routing_audit_logs) (#storing_and_routing_audit_logs) section of this page.

System Event audit logs

System Event audit logs contain log entries for Google Cloud actions that modify the configuration of resources. System Event audit logs are generated by Google Cloud systems; they aren't driven by direct user action.

System Event audit logs are always written; you can't configure, exclude, or disable them.

For a list of services that write System Event audit logs and detailed information about which activities generate those logs, see [Google Cloud services with audit logs](/logging/docs/audit/services) (/logging/docs/audit/services).

Policy Denied audit logs

Policy Denied audit logs are recorded when a Google Cloud service denies access to a user or [service account](/iam/docs/service-accounts) (/iam/docs/service-accounts) because of a security policy violation.

Policy Denied audit logs are generated by default and your Google Cloud project is charged for the logs storage. You can't disable Policy Denied audit logs, but you can use [exclusion filters](/logging/docs/routing/overview#exclusions) (/logging/docs/routing/overview#exclusions) to prevent Policy Denied audit logs from being stored in Cloud Logging.

For a list of services that write Policy Denied audit logs and detailed information about which activities generate those logs, see [Google Cloud services with audit logs](/logging/docs/audit/services) (/logging/docs/audit/services).

Audit log entry structure

Every audit log entry in Cloud Logging is an object of type [LogEntry](/logging/docs/reference/v2/rest/v2/LogEntry) (/logging/docs/reference/v2/rest/v2/LogEntry). What distinguishes an audit log entry from other log entries is the `protoPayload` field; this field contains an [AuditLog](/logging/docs/audit/api/ref/rest/Shared.Types/AuditLog) (/logging/docs/audit/api/ref/rest/Shared.Types/AuditLog) object that stores the audit logging data.

To understand how to read and interpret audit log entries, and for a sample of an audit log entry, see [Understanding audit logs](/logging/docs/audit/understanding-audit-logs) (/logging/docs/audit/understanding-audit-logs).

Log name

Cloud Audit Logs log names include the following:

- Resource identifiers indicating the Google Cloud project or other Google Cloud entity that owns the audit logs.
- The string `cloudaudit.googleapis.com`.

- A string that indicates whether the log contains Admin Activity, Data Access, Policy Denied, or System Event audit logging data.

The following are the audit log names, including variables for the resource identifiers:

```
projects/PROJECT_ID /logs/cloudaudit.googleapis.com%2Factivity
projects/PROJECT_ID /logs/cloudaudit.googleapis.com%2Fdata_access
projects/PROJECT_ID /logs/cloudaudit.googleapis.com%2Fsystem_event
projects/PROJECT_ID /logs/cloudaudit.googleapis.com%2Fpolicy
```

```
folders/FOLDER_ID /logs/cloudaudit.googleapis.com%2Factivity
folders/FOLDER_ID /logs/cloudaudit.googleapis.com%2Fdata_access
folders/FOLDER_ID /logs/cloudaudit.googleapis.com%2Fsystem_event
folders/FOLDER_ID /logs/cloudaudit.googleapis.com%2Fpolicy
```

```
billingAccounts/BILLING_ACCOUNT_ID /logs/cloudaudit.googleapis.com%2Factivity
billingAccounts/BILLING_ACCOUNT_ID /logs/cloudaudit.googleapis.com%2Fdata_ac
billingAccounts/BILLING_ACCOUNT_ID /logs/cloudaudit.googleapis.com%2Fsystem_
billingAccounts/BILLING_ACCOUNT_ID /logs/cloudaudit.googleapis.com%2Fpolicy
```

```
organizations/ORGANIZATION_ID /logs/cloudaudit.googleapis.com%2Factivity
organizations/ORGANIZATION_ID /logs/cloudaudit.googleapis.com%2Fdata_access
organizations/ORGANIZATION_ID /logs/cloudaudit.googleapis.com%2Fsystem_event
organizations/ORGANIZATION_ID /logs/cloudaudit.googleapis.com%2Fpolicy
```

Caller identities in audit logs

Audit logs record the identity that performed the logged operations on the Google Cloud resource. The caller's identity is held in the `AuthenticationInfo` field of `AuditLog` (`/logging/docs/audit/api/ref/rest/Shared.Types/AuditLog`) objects.

Audit logging doesn't redact the caller's principal email address for any access that succeeds or for any write operation.

For read-only operations that fail with a "permission denied" error, Audit Logging might redact the caller's principal email address unless the caller is a service account.

In addition to the conditions listed above, the following applies to certain Google Cloud services:

- [Legacy App Engine API](/appengine/docs/) (/appengine/docs): Identities aren't collected.
- [BigQuery](/bigquery/docs/reference/auditlogs#ids) (/bigquery/docs/reference/auditlogs#ids): Caller identities and IP addresses, as well as some resource names, are redacted from the audit logs, unless certain conditions are met.
- [Cloud Storage](/storage/docs/access-logs) (/storage/docs/access-logs): When Cloud Storage usage logs are enabled, Cloud Storage writes usage data to the Cloud Storage bucket, which generates Data Access audit logs for the bucket. The generated Data Access audit log has its caller identity redacted.
- [Firestore](/firestore/docs/audit-logging) (/firestore/docs/audit-logging): If a JSON Web Token (JWT) was used for third-party authentication, the `thirdPartyPrincipal` field includes the token's header and payload. For example, audit logs for requests authenticated with [Firebase Authentication](https://firebase.google.com/docs/auth) (https://firebase.google.com/docs/auth) include that request's [auth token](https://firebase.google.com/docs/auth/users#auth_tokens) (https://firebase.google.com/docs/auth/users#auth_tokens).
- [VPC Service Controls](/vpc-service-controls/docs/audit-logging) (/vpc-service-controls/docs/audit-logging): For Policy Denied audit logs, the following redaction occurs:
 - Parts of the caller email addresses might be redacted and replaced by three period characters
 - Some caller email addresses belonging to the domain `google.com` are redacted and replaced by `google-internal`.
- [Organization Policy](/resource-manager/docs/organization-policy/audit-logging) (/resource-manager/docs/organization-policy/audit-logging): Parts of the caller email addresses might be redacted and replaced by three period characters

IP address of the caller in audit logs

The IP address of the caller is held in the `RequestMetadata.callerIp` field of the [AuditLog](/logging/docs/audit/api/ref/rest/Shared.Types/AuditLog) (/logging/docs/audit/api/ref/rest/Shared.Types/AuditLog) object:

- For a caller from the internet, the address is a public IPv4 or IPv6 address.
- For calls made from inside the internal production network from one Google Cloud service to another, the `callerIp` is redacted to "private".

- For a caller from a Compute Engine VM with a external IP address, the `callerIp` is the external address of the VM.
- For a caller from a Compute Engine VM without a external IP address, if the VM is in the same organization or project as the accessed resource, then `callerIp` is the VM's internal IPv4 address. Otherwise, the `callerIp` is redacted to "gce-internal-ip". For more information, see [VPC network overview](/compute/docs/vpc) (/compute/docs/vpc).

Viewing audit logs

You can query for all audit logs or you can query for logs by their audit log name. The audit log name includes the [resource identifier](#)

(/resource-manager/docs/creating-managing-projects#identifying_projects) of the Google Cloud project, folder, billing account, or organization for which you want to view audit logging information. Your queries can specify indexed [LogEntry](#)

(/logging/docs/reference/v2/rest/v2/LogEntry) fields. For more information about querying your logs, see [Build queries in the Logs Explorer](#) (/logging/docs/view/building-queries)


The Logs Explorer lets you view filter individual log entries. If you want to use SQL to analyze groups of log entries, then use the **Log Analytics** page. For more information, see:

- [Query and view logs in Log Analytics](#) (/logging/docs/analyze/query-and-view).
- [Sample queries for security insights](#) (/logging/docs/analyze/analyze-audit-logs).
- [Chart query results](#) (/logging/docs/analyze/charts).

Most audit logs can be viewed in Cloud Logging by using the Google Cloud console, the Google Cloud CLI, or the Logging API. However, for audit logs related to billing, you can only use the Google Cloud CLI or the Logging API.

[Console](#) (#gcloud)[REST](#) (#rest)
(#console)

In the Google Cloud console, you can use the Logs Explorer to retrieve your audit log entries for your Google Cloud project, folder, or organization:

 **Note:** You can't view audit logs for Cloud Billing accounts in the Google Cloud console. You must use

the API or the gcloud CLI.

1. In the Google Cloud console, go to the **Logs Explorer** page:

Go to Logs Explorer (<https://console.cloud.google.com/logs/query>)

If you use the search bar to find this page, then select the result whose subheading is **Logging**.

2. Select an existing Google Cloud project, folder, or organization.
3. To display all audit logs, enter either of the following queries into the query-editor field, and then click **Run query**:

```
logName:"cloudaudit.googleapis.com"
```

```
protoPayload."@type"="type.googleapis.com/google.cloud.audit.AuditLog"
```

4. To display the audit logs for a specific resource and audit log type, in the **Query builder** pane, do the following:

- In **Resource type**, select the Google Cloud resource whose audit logs you want to see.
- In **Log name**, select the audit log type that you want to see:
 - For Admin Activity audit logs, select **activity**.
 - For Data Access audit logs, select **data_access**.
 - For System Event audit logs, select **system_event**.
 - For Policy Denied audit logs, select **policy**.
- Click **Run query**.

If you don't see these options, then there aren't any audit logs of that type available in the Google Cloud project, folder, or organization.

If you're experiencing issues when trying to view logs in the Logs Explorer, see the [troubleshooting](/logging/docs/view/logs-explorer-interface#troubleshooting) (/logging/docs/view/logs-explorer-interface#troubleshooting) information.

For more information about querying by using the Logs Explorer, see [Build queries in the Logs Explorer](/logging/docs/view/building-queries) (/logging/docs/view/building-queries).

Storing and routing audit logs

Cloud Logging uses [log buckets](/logging/docs/store-log-entries) (/logging/docs/store-log-entries) as containers that store and organize your logs data. For each billing account, Google Cloud project, folder, and organization, Logging automatically creates two log buckets, `_Required` and `_Default`, and correspondingly named [sinks](/logging/docs/routing/overview#sinks) (/logging/docs/routing/overview#sinks).

Cloud Logging `_Required` buckets store Admin Activity audit logs and System Event audit logs. You can't prevent Admin Activity or System Event audit logs from being stored. You also can't configure the sink that routes log entries to the `_Required` buckets.

Admin Activity audit logs and System Event audit logs are always stored in the `_Required` bucket in the project where the logs were generated.

If you route Admin Activity audit logs and System Event audit logs to a different project, then those logs don't pass through the `_Default` or `_Required` sink of the destination project. Therefore, these logs aren't stored in the `_Default` log bucket or the `_Required` log bucket of the destination project. To store these logs, create a log sink in the destination project. For more information, see [Route logs to supported destinations](/logging/docs/export/configure_export_v2) (/logging/docs/export/configure_export_v2).

The `_Default` buckets, by default, store any enabled Data Access audit logs as well as Policy Denied audit logs. To prevent Data Access audit logs from being stored in the `_Default` buckets, you can disable them. To prevent any Policy Denied audit logs from being stored in the `_Default` buckets, you can exclude them by modifying their sinks' filters.

You can also route your audit log entries to user-defined Cloud Logging buckets at the Google Cloud project level or to supported destinations outside of Logging using sinks. For instructions on routing logs, see [Route logs to supported destinations](/logging/docs/export/configure_export_v2) (/logging/docs/export/configure_export_v2).

When configuring your log sinks' filters, you need to specify the audit log types you want to route; for filtering examples, see [Security logging queries](#) (/logging/docs/view/query-library#security-filters).

If you want to route audit log entries for a Google Cloud organization, folder, or billing account, see [Collate and route organization-level logs to supported destinations](#) (/logging/docs/export/aggregated_sinks).

Audit log retention

For details on how long log entries are retained by Logging, see the retention information in [Quotas and limits: Logs retention periods](#) (/logging/quotas#logs_retention_periods).

Access control

IAM permissions and roles determine your ability to access audit logs data in the [Logging API](#) (/logging/docs/reference/v2/rest), the [Logs Explorer](#) (/logging/docs/view/logs-explorer-interface), and the [Google Cloud CLI](#) (/logging/docs/reference/tools/gcloud-logging).

For detailed information about the IAM permissions and roles you might need, see [Access control with IAM](#) (/logging/docs/access-control).

Quotas and limits

For details on logging usage limits, including the maximum sizes of audit logs, see [Quotas and limits](#) (/logging/quotas).

Pricing

Cloud Logging doesn't charge to route logs to a supported destination; however, the destination might apply charges. With the exception of the `_Required` log bucket, Cloud Logging charges to stream logs into log buckets and for storage longer than the default retention period of the log bucket.

Cloud Logging doesn't charge for copying logs, for creating [log scopes](/logging/docs/log-scope/create-and-manage) (</logging/docs/log-scope/create-and-manage>) or [analytics views](/logging/docs/analyze/about-analytics-views) (</logging/docs/analyze/about-analytics-views>), or for queries issued through the **Logs Explorer** or **Log Analytics** pages.

For more information, see the following documents:

- [Cloud Logging pricing summary](/stackdriver/pricing#logs-pricing-summary) (</stackdriver/pricing#logs-pricing-summary>)
- Destination costs:
 - [Cloud Storage pricing](/storage/pricing) (</storage/pricing>)
 - [BigQuery pricing](/bigquery/pricing#data_ingestion_pricing) (/bigquery/pricing#data_ingestion_pricing)
 - [Pub/Sub pricing](/pubsub/pricing) (</pubsub/pricing>)
 - [Cloud Logging pricing](/stackdriver/pricing#logging-cost) (</stackdriver/pricing#logging-cost>)
- [VPC flow log generation charges](/vpc/network-pricing#network-telemetry) (</vpc/network-pricing#network-telemetry>) apply when you send and then exclude your Virtual Private Cloud flow logs from Cloud Logging.

What's next

- Learn how to [read and understand audit logs](/logging/docs/audit/understanding-audit-logs) (</logging/docs/audit/understanding-audit-logs>).
- Learn how to [enable Data Access audit logs](/logging/docs/audit/configure-data-access) (</logging/docs/audit/configure-data-access>).
- Review [best practices](/logging/docs/audit/best-practices) (</logging/docs/audit/best-practices>) for Cloud Audit Logs.
- Learn about [Access Transparency](/assured-workloads/access-transparency/docs/overview) (</assured-workloads/access-transparency/docs/overview>), which provides logs of actions taken by Google Cloud staff when accessing your Google Cloud content.

Except as otherwise noted, the content of this page is licensed under the [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/) (<https://creativecommons.org/licenses/by/4.0/>), and code samples are licensed under the [Apache 2.0 License](https://www.apache.org/licenses/LICENSE-2.0) (<https://www.apache.org/licenses/LICENSE-2.0>). For details, see the [Google Developers Site Policies](https://developers.google.com/site-policies) (<https://developers.google.com/site-policies>). Java is a registered trademark of Oracle and/or its affiliates.

Last updated 2025-05-16 UTC.