Google Cloud

Contact Us   Start free

Google Cloud Observability > Logging > Documentation > Guides

Audit logs for Google Workspace

Send feedback

This document provides a conceptual overview of the audit logs that Google Workspace provides as a part of Cloud Audit Logs.

For information about managing your Google Workspace audit logs, see View and manage audit logs for Google Workspace.

Overview

Google Cloud services write audit logs to help you answer the questions, "Who did what, where, and when?". You can share your Google Workspace audit logs with Google Cloud to store, analyze, monitor, and alert on your Google Workspace data.

Audit logs for Google Workspace are available for Cloud Identity, Cloud Identity Premium, and all Google Workspace customers.

If you've enabled Google Workspace data sharing with Google Cloud, then audit logs are always enabled for Google Workspace.

Disabling Google Workspace data sharing stops new Google Workspace audit log events from being sent to Google Cloud. Any existing logs remain through their default retention periods, unless you have configured custom retention to retain your logs for a longer period.

If you don't enable Google Workspace data sharing with Google Cloud, then you can't see audit logs for Google Workspace in Google Cloud.

> ⭐ **Note:** Some Enterprise Groups Audit membership changes automatically populate the `principalEmail` field in the audit log with `cloud-support@google.com`. For example, an audit log might show `cloud-support@google.com` as the principal removing a user from the group, when the removal of the user is automatic due to the expiration of a user's membership.

Types of 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 (IAM) permissions.

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. Data Access audit logs don't record the data-access operations on resources that are publicly shared (available to All Users or All Authenticated Users) or that can be accessed without logging into Google Cloud, Google Workspace, Cloud Identity, or Drive Enterprise account.

Google Workspace services forwarding audit logs to Google Cloud

Google Workspace provides the following audit logs at the Google Cloud organization level:

- **Google Workspace Admin Audit**: Admin Audit logs provide a record of actions performed in your Google Admin console. For example, you can see when an administrator added a user or turned on a Google Workspace service. Admin Audit writes Admin Activity audit logs only.

  > ⭐ **Note:** Unless you use the Google Admin console, changes to Group settings are captured in the Google Workspace Enterprise Groups Audit logs. When you use the Google Admin console, changes to Group settings are captured in the Google Workspace Admin Audit logs. For example, if you changed a Group email address

in groups.google.com, then those changes are captured in Google Workspace Enterprise Groups Audit logs.

- **Google Workspace Enterprise Groups Audit**: Enterprise Groups Audit logs provide a record of actions performed on groups and group memberships. For example, you can see when an administrator added a user or when a group owner deleted their group.

  Enterprise Groups Audit writes Admin Activity audit logs only.

- **Google Workspace Login Audit**: Login Audit logs track user sign-ins to your domain. These logs only record the login event. They don't record which system was used to perform the login action.

  Login Audit writes Data Access audit logs only.

- **Google Workspace OAuth Token Audit**: OAuth Token Audit logs track which users are using which third-party mobile or web applications in your domain. For example, when a user opens a Google Workspace Marketplace app, the log records the name of the app and the person using it. The log also records each time a third-party application is authorized to access Google Account data, such as Google Contacts, Calendar, and Drive files (Google Workspace only).

  OAuth Token Audit writes both Admin Activity and Data Access audit logs.

- **Google Workspace SAML Audit**: SAML Audit logs track users' successful and failed sign-ins to SAML applications. Entries usually appear within an hour of the user action.

  SAML Audit writes Data Access audit logs only.

Service-specific information

Details for each Google Workspace service's audit logs are as follows:

Audit log permissions

IAM permissions and roles determine your ability to access audit logs data in the Logging API, the Logs Explorer, and the Google Cloud CLI.

For detailed information about the organization-level IAM permissions and roles you might need, see the Access control with IAM.

Audit log format

Google Workspace audit log entries include the following objects:

- The log entry itself, which is an object of type `LogEntry`. When examining audit logging data, you might find the following useful:

  - `logName` contains the organization ID and audit log type.

  - `resource` contains the target of the audited operation.

  - `timeStamp` contains the time of the audited operation.

  - `protoPayload` contains the Google Workspace audit log in its `metadata` field.

The `protoPayload.metadata` field holds the audited Google Workspace information. The following is an example of a Login Audit log:

```
{
  "protoPayload": {
    "@type": "type.googleapis.com/google.cloud.audit.AuditLog",
    "authenticationInfo": {
      "principalEmail": "test-user@example.net"
    },
    "requestMetadata": {
      "callerIp": "2001:db8:ffff:ffff:ffff:ffff:ffff:ffff",
      "requestAttributes": {},
      "destinationAttributes": {}
    },
    "serviceName": "login.googleapis.com",
    "methodName": "google.login.LoginService.loginFailure",
```

```
      "resourceName": "organizations/123",
      "metadata": {
        "event": [
          {
            "eventName": "login_failure",
            "eventType": "login",
            "parameter": [
              {
                "value": "google_password",
                "type": "TYPE_STRING",
                "name": "login_type",
              },
              {
                "name": "login_challenge_method",
                "type": "TYPE_STRING",
                "label": "LABEL_REPEATED",
                "multiStrValue": [
                  "password",
                  "idv_preregistered_phone",
                  "idv_preregistered_phone"
                ]
              },
            ]
          }
        ],
        "activityId": {
          "uniqQualifier": "358068855354",
          "timeUsec": "1632500217183212"
        },
        "@type": "type.googleapis.com/ccc_hosted_reporting.ActivityProto"
      }
    },
    "insertId": "-nahbepd4l1x",
    "resource": {
      "type": "audited_resource",
      "labels": {
        "method": "google.login.LoginService.loginFailure",
        "service": "login.googleapis.com"
      }
    },
    "timestamp": "2021-09-24T16:16:57.183212Z",
    "severity": "NOTICE",
    "logName": "organizations/123/logs/cloudaudit.googleapis.com%2Fdata_access",
```

```
    "receiveTimestamp": "2021-09-24T17:51:25.034361197Z"
}
```

For information about service-specific audit logging fields, and how to interpret them, select from the services listed in Available audit logs.

View logs

For information on viewing your Google Workspace audit logs, see View and manage audit logs for Google Workspace.

Route audit logs

You can route Google Workspace audit logs from Cloud Logging to supported destinations, including other Logging buckets.

Here are some applications for routing audit logs:

- To use more powerful search capabilities, you can route copies of your audit logs to Cloud Storage, BigQuery, or Pub/Sub. Using Pub/Sub, you can route to other applications, other repositories, and to third parties.

- To manage your audit logs across an entire organization, you can create aggregated sinks that combine and route logs from all the Google Cloud projects, billing accounts, and folders contained by your organization. For instance, you might aggregate and route audit log entries from an organization's folders to a Cloud Storage bucket.

For instructions on routing logs, see Route logs to supported destinations.

Regionalization

You can't choose a region where your Google Workspace logs are stored. Google Workspace logs aren't covered by the Google Workspace Data Region Policy.

Retention periods

The following retention periods apply to your audit logs data:

- Data retention policy in Google Workspace.

- Data retention policy in Google Cloud Cloud Logging.

For each organization, Cloud Logging automatically stores logs in two buckets: a `_Default` bucket and a `_Required` bucket. The `_Required` bucket holds Admin Activity audit logs, System Event audit logs, and Access Transparency logs. The `_Default` bucket holds all other log entries that aren't stored in the `_Required` bucket. For more information on Logging buckets, see Routing and storage overview.

You can configure Cloud Logging to retain the logs in the `_Default` logs bucket for a period ranging from 1 day to 3650 days.

To update the retention period for the `_Default` logs bucket, see Custom retention.

You can't change the retention period on the `_Required` bucket.

Quotas and limits

The same quotas apply to audit logs for Google Workspace and Cloud Audit Logs.

For details about these usage limits, including the maximum sizes of audit logs, see Quotas and limits.

Pricing

Google Workspace's organization-level logs are free.

What's next

- Learn how to configure and manage Google Workspace audit logs.

- Review best practices for Cloud Audit Logs.

- Learn how to view and understand Access Transparency logs for Google Workspace.

Send feedback

Why Google

Choosing Google Cloud

Trust and security

Modern Infrastructure Cloud

Multicloud

Global infrastructure

Customers and case studies

Analyst reports

Whitepapers

Blog

Products and pricing

Google Cloud pricing

Google Workspace pricing

See all products

Solutions

Infrastructure modernization

Databases

Application modernization

Smart analytics

Artificial Intelligence

Security

Productivity & work transformation

Industry solutions

DevOps solutions

Small business solutions

See all solutions

Resources

Google Cloud Affiliate Program

Google Cloud documentation

Google Cloud quickstarts

Google Cloud Marketplace

Learn about cloud computing

Support

Code samples

Cloud Architecture Center

Training

Certifications

Google for Developers

Google Cloud for Startups

System status

Release Notes

Engage

Contact sales

Find a Partner

Become a Partner

Events

Podcasts

Developer Center

Press Corner

Google Cloud on YouTube

Google Cloud Tech on YouTube

Follow on X

Join User Research

We're hiring. Join Google Cloud!

Google Cloud Community

About Google | Privacy | Site terms | Google Cloud terms

🌿 Our third decade of climate action: join us

Sign up for the Google Cloud newsletter

Subscribe