Monitor usage patterns for service accounts and keys

Archived: 2026-04-05 14:22:17 UTC

This page explains how to use Cloud Monitoring to view usage metrics for your service accounts and service account keys. These metrics let you view and track usage patterns, which can help you identify anomalies, either automatically or manually.

Service accounts and service account keys appear in these metrics if they are used to call any Google API, including APIs that are not part of Google Cloud. The metrics include both successful and failed API calls. For example, if an API call fails because the caller is not authorized to call that API, or because the request referred to a resource that does not exist, the service account or key that was used for that API call appears in the metrics.

Service account keys also appear in these metrics if a system lists the keys while attempting to authenticate a request, even if the system doesn't use the key to authenticate the request. This behavior is most common when using signed URLs for Cloud Storage or when authenticating to third-party applications. As a result it is possible to see usage metrics for keys that have not been used for authentication.

The following don't appear in either service account or service account key metrics:

- Cloud Storage HMAC authentication keys
- Requests authenticated by API keys bound to service accounts

Monitoring retains service account metrics for 6 weeks. If you need to access data for a longer time period, you can periodically export the results to BigQuery. For more information, see Monitoring metric export in the Solutions documentation.

After you use a service account or service account key, usage metrics are usually available within a few minutes.

Before you begin

- Enable the IAM and Cloud Monitoring APIs.

  Roles required to enable APIs

  To enable APIs, you need the Service Usage Admin IAM role (`roles/serviceusage.serviceUsageAdmin`), which contains the `serviceusage.services.enable` permission. Learn how to grant roles.

  Enable the APIs

Required roles

To get the permissions that you need to view recent usage for service accounts and keys, ask your administrator to grant you the Monitoring Viewer (`roles/monitoring.viewer`) IAM role on the project. For more information about granting roles, see Manage access to projects, folders, and organizations.

You might also be able to get the required permissions through custom roles or other predefined roles.

View usage metrics for all service accounts or keys

To view the usage metrics for your service accounts or service account keys, follow these steps:

To view the metrics for a monitored resource by using the Metrics Explorer, do the following:

1. In the Google Cloud console, go to the **Metrics explorer** page:

   Go to **Metrics explorer**

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

2. In the toolbar of the Google Cloud console, select your Google Cloud project. For App Hub configurations, select the App Hub host project or the app-enabled folder's management project.
3. In the **Metric** element, expand the **Select a metric** menu, enter `IAM Service Account` in the filter bar, and then use the submenus to select a specific resource type and metric:
   1. In the **Active resources** menu, select **IAM Service Account**.
   2. In the **Active metric categories** menu, select **Service_account**.
   3. In the **Active metrics** menu, select a service account metric. The following metrics are available within your selected time interval:
      - For service account usage metrics, select **Service account authentication events**.
      - For service account key usage metrics, select **Service account key authentication events**.
   4. Click **Apply**.
4. To add filters, which remove time series from the query results, use the **Filter** element.
5. To combine time series, use the menus on the **Aggregation** element. For example, to display the CPU utilization for your VMs, based on their zone, set the first menu to **Mean** and the second menu to **zone**.

   All time series are displayed when the first menu of the **Aggregation** element is set to **Unaggregated**. The default settings for the **Aggregation** element are determined by the metric type you selected.
6. For quota and other metrics that report one sample per day, do the following:
   1. In the **Display** pane, set the **Widget type** to **Stacked bar chart**.
   2. Set the time period to at least one week.

The Cloud Monitoring API API's `timeSeries.list` method allows you to access usage metrics programmatically.

Before using any of the request data, make the following replacements:

- *`PROJECT_ID`* : Your Google Cloud project ID. Project IDs are alphanumeric strings, like `my-project` .
- *`METRIC_TYPE`* : The type of metric you want to check. Use one of the following values:
  - For service account usage metrics, use `iam.googleapis.com%2Fservice_account%2Fauthn_events_count` .

    - For service account key usage metrics, use `iam.googleapis.com%2Fservice_account%2Fkey%2Fauthn_events_count`.
- *`END_TIME`*: The end of the time interval that you want to check, in percent-encoded RFC 3339 format. For example, `2020-06-12T00%3A00%3A00.00Z`.
- *`START_TIME`*: The start of the time interval that you want to check, in percent-encoded RFC 3339 format. For example, `2020-04-12T00%3A00%3A00.00Z`.

HTTP method and URL:

```
GET https://monitoring.googleapis.com/v3/projects/PROJECT_ID/timeSeries?filter=metric.type%3D%22METR
```

To send your request, expand one of these options:

curl (Linux, macOS, or Cloud Shell)

Execute the following command:

```
curl -X GET \
     -H "Authorization: Bearer $(gcloud auth print-access-token)" \
     "https://monitoring.googleapis.com/v3/projects/PROJECT_ID/timeSeries?filter=metric.type%3D%22ME
```

PowerShell (Windows)

Execute the following command:

```
$cred = gcloud auth print-access-token
$headers = @{ "Authorization" = "Bearer $cred" }

Invoke-WebRequest `
    -Method GET `
    -Headers $headers `
    -Uri "https://monitoring.googleapis.com/v3/projects/

PROJECT_ID/timeSeries?filter=metric.type%3D%22METRIC_TYPE%22&interval.endTime=END_TIME&interval.star
```

APIs Explorer (browser)

Open the method reference page. The APIs Explorer panel opens on the right side of the page. You can interact with this tool to send requests. Complete any required fields and click **Execute**.

For more information about programmatically reading usage metrics, see Reading metric data in the Monitoring documentation.

View usage metrics for a single service account

To view usage metrics for a single service account, follow these steps:

1. In the Google Cloud console, go to the **Service Accounts** page.

   Go to Service Accounts

2. Select the project that contains your service account.
3. Click the email address of your service account.
4. Click the **Metrics** tab. The **Authentication traffic** chart shows the usage metrics for the service account.
5. Optional: To view the chart on the **Metrics explorer** page, which offers additional filtering and viewing options, click > **View in Metrics Explorer**.

The Cloud Monitoring API's `timeSeries.list` method , when used with specific filters, allows you to get usage metrics for a single service account. You can then use those metrics to determine when the account was last used.

Before using any of the request data, make the following replacements:

- *`PROJECT_ID`* : Your Google Cloud project ID. Project IDs are alphanumeric strings, like `my-project` .
- *`SERVICE_ACCOUNT_ID`* : The unique numeric ID of your service account. To find your service account's unique numeric ID, follow these steps:

  1. In the Google Cloud console, go to the **Service Accounts** page.

     Go to the Service Accounts page

  2. Click the email address of your service account. Your service account's unique numeric ID is the value in the **Unique ID** field.
- *`END_TIME`* : The end of the time interval that you want to check, in percent-encoded RFC 3339 format. For example, `2020-06-12T00%3A00%3A00.00Z` .
- *`START_TIME`* : The start of the time interval that you want to check, in percent-encoded RFC 3339 format. For example, `2020-04-12T00%3A00%3A00.00Z` .

HTTP method and URL:

```
GET https://monitoring.googleapis.com/v3/projects/PROJECT_ID/timeSeries?filter=metric.type%3D%22iam.
```

To send your request, expand one of these options:

curl (Linux, macOS, or Cloud Shell)

Execute the following command:

```
curl -X GET \
     -H "Authorization: Bearer $(gcloud auth print-access-token)" \
```

```
    "https://monitoring.googleapis.com/v3/projects/PROJECT_ID/timeSeries?filter=metric.type%3D%22ia
```

PowerShell (Windows)

Execute the following command:

```
$cred = gcloud auth print-access-token
$headers = @{ "Authorization" = "Bearer $cred" }

Invoke-WebRequest `
    -Method GET `
    -Headers $headers `
    -Uri "https://monitoring.googleapis.com/v3/projects/

PROJECT_ID/timeSeries?filter=metric.type%3D%22iam.googleapis.com%2Fservice_account%2Fauthn_events_co
```

APIs Explorer (browser)

Open the method reference page. The APIs Explorer panel opens on the right side of the page. You can interact with this tool to send requests. Complete any required fields and click **Execute**.

The response contains a `timeSeries` object with all of the recent authentication events for the specified service account.

View usage metrics for a single service account key

To view usage metrics for a single service account key, follow these steps:

1. In the Google Cloud console, go to the **Service Accounts** page.

   Go to Service Accounts

2. Select the project that contains the service account associated with your key.
3. Click the email address of the service account associated with your key.
4. Click the **Metrics** tab. The **Authentication traffic per key** chart shows usage metrics for all keys associated with the service account.
5. In the chart legend, click the ID of the service account key that you want to view usage metrics for. The chart updates to show metrics for only that service account key.
6. Optional: To view the chart on the **Metrics explorer** page, which offers additional filtering and viewing options, click > **View in Metrics Explorer**.

First, get the service account key's ID.

1. List the service account keys:

   The `projects.serviceAccounts.keys.list` method lists all of the service account keys for a service account.

   Before using any of the request data, make the following replacements:

   - *`PROJECT_ID`* : Your Google Cloud project ID. Project IDs are alphanumeric strings, like `my-project` .
   - *`SA_NAME`* : The name of the service account whose keys you want to list.
   - *`KEY_TYPES`* : Optional. A comma-separated list of key types that you want to include in the response. The key type indicates whether a key is user-managed (`USER_MANAGED`) or system-managed (`SYSTEM_MANAGED`). If left blank, all keys are returned.

   HTTP method and URL:

   ```
   GET https://iam.googleapis.com/v1/projects/PROJECT_ID/serviceAccounts/SA_NAME@PROJECT_ID.iam.g
   ```

   To send your request, expand one of these options:

   curl (Linux, macOS, or Cloud Shell)

   Execute the following command:

   ```
   curl -X GET \
        -H "Authorization: Bearer $(gcloud auth print-access-token)" \
        "https://iam.googleapis.com/v1/projects/PROJECT_ID/serviceAccounts/SA_NAME@PROJECT_ID.iam
   ```

   PowerShell (Windows)

   Execute the following command:

   ```
   $cred = gcloud auth print-access-token
   $headers = @{ "Authorization" = "Bearer $cred" }

   Invoke-WebRequest `
       -Method GET `
       -Headers $headers `
       -Uri "https://iam.googleapis.com/v1/projects/

   PROJECT_ID/serviceAccounts/SA_NAME@PROJECT_ID.iam.gserviceaccount.com/keys?keyTypes=KEY_TYPES"
   ```

APIs Explorer (browser)

Open the method reference page. The APIs Explorer panel opens on the right side of the page. You can interact with this tool to send requests. Complete any required fields and click **Execute**.

You should receive a JSON response similar to the following:


```
{
  "keys": [
    {
      "name": "projects/my-project/serviceAccounts/my-service-account@my-project.iam.gservicea
      "validAfterTime": "2020-03-04T17:39:47Z",
      "validBeforeTime": "9999-12-31T23:59:59Z",
      "keyAlgorithm": "KEY_ALG_RSA_2048",
      "keyOrigin": "GOOGLE_PROVIDED",
      "keyType": "USER_MANAGED"
    },
    {
      "name": "projects/my-project/serviceAccounts/my-service-account@my-project.iam.gservicea
      "validAfterTime": "2020-03-31T23:50:09Z",
      "validBeforeTime": "9999-12-31T23:59:59Z",
      "keyAlgorithm": "KEY_ALG_RSA_2048",
      "keyOrigin": "GOOGLE_PROVIDED",
      "keyType": "USER_MANAGED"
    },
    {
      "name": "projects/my-project/serviceAccounts/my-service-account@my-project.iam.gservicea
      "validAfterTime": "2020-05-17T18:58:13Z",
      "validBeforeTime": "9999-12-31T23:59:59Z",
      "keyAlgorithm": "KEY_ALG_RSA_2048",
      "keyOrigin": "GOOGLE_PROVIDED",
      "keyType": "USER_MANAGED",
      "disabled": true
      "disable_reason": "SERVICE_ACCOUNT_KEY_DISABLE_REASON_EXPOSED"
      "extended_status": "SERVICE_ACCOUNT_KEY_EXTENDED_STATUS_KEY_EXPOSED"
      "extended_status_message": "exposed at: https://www.github.com/SomePublicRepo"
    }
  ]
}
```


2. Use the metadata in the response to identify the key you want to track. Then, copy the key's unique ID from the end of the `name` field.

   The `name` field has the following format:

```
"name": "projects/PROJECT_ID/serviceAccounts/SERVICE_ACCOUNT_EMAIL/keys/KEY_ID"
```

The key's unique ID is everything after `keys/`.

For example, the unique ID in the following key name is `0f561cc41650ff521899de2fd653bd3de08e2da4`:

```
"name": "projects/my-project/serviceAccounts/my-account@my-project.iam.gserviceaccount.com/key
```

Then, use the ID to view usage metrics for the service account key.

The Cloud Monitoring API's `timeSeries.list` method , when used with specific filters, allows you to get usage metrics for a single service account key. You can then use those metrics to determine when the key was last used.

Before using any of the request data, make the following replacements:

- *PROJECT_ID* : Your Google Cloud project ID. Project IDs are alphanumeric strings, like `my-project`.
- *KEY_ID* : The unique ID of your service account key.
- *END_TIME* : The end of the time interval that you want to check, in percent-encoded RFC 3339 format. For example, `2020-06-12T00%3A00%3A00.00Z`.
- *START_TIME* : The start of the time interval that you want to check, in percent-encoded RFC 3339 format. For example, `2020-04-12T00%3A00%3A00.00Z`.

HTTP method and URL:

```
GET https://monitoring.googleapis.com/v3/projects/PROJECT_ID/timeSeries?filter=metric.type%3D%22iam.
```

To send your request, expand one of these options:

curl (Linux, macOS, or Cloud Shell)

Execute the following command:

```
curl -X GET \
     -H "Authorization: Bearer $(gcloud auth print-access-token)" \
     "https://monitoring.googleapis.com/v3/projects/PROJECT_ID/timeSeries?filter=metric.type%3D%22ia
```

PowerShell (Windows)

Execute the following command:

```
$cred = gcloud auth print-access-token
$headers = @{ "Authorization" = "Bearer $cred" }
```

```
Invoke-WebRequest `
    -Method GET `
    -Headers $headers `
    -Uri "https://monitoring.googleapis.com/v3/projects/

PROJECT_ID/timeSeries?filter=metric.type%3D%22iam.googleapis.com%2Fservice_account%2Fkey%2Fauthn_eve
```

APIs Explorer (browser)

Open the method reference page. The APIs Explorer panel opens on the right side of the page. You can interact with this tool to send requests. Complete any required fields and click **Execute**.

The response contains a `timeSeries` object with all of the recent authentication events for the specified service account key.

Export metrics

You can use Monitoring to export your metrics to BigQuery. Exporting metrics is useful for performing long-term analysis because Monitoring only retains metrics for a limited time.

For instructions, see Monitoring metric export in the Solutions documentation.

What's next

- Discover how to export metric data to BigQuery.
- Use Activity Analyzer to view only the most recent authentication events for your service accounts and keys.
- Use service account insights to identify service accounts that have not been used in the past 90 days.
- Learn how to disable service accounts or delete service accounts.
- Learn how to delete service account keys.
- Explore the features offered by Monitoring.
