GOOGLE CLOUD LOGGING

> This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview (https://docs.mandiant.com/home/msv-integrations-overview)**.

This requires the Cloud Validation license.

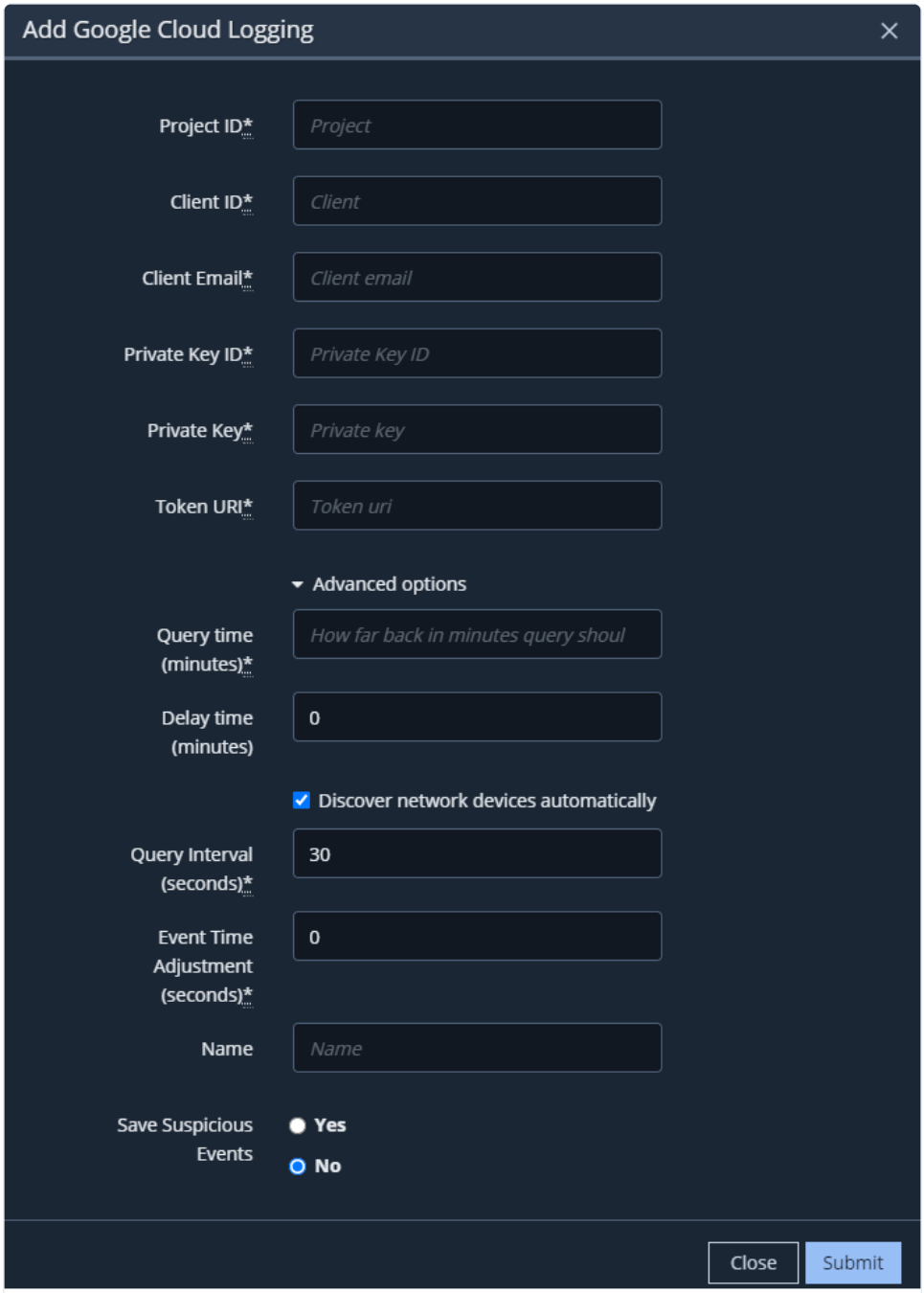
The Google Cloud Logging integration provides events to help you validate security controls of the Google Cloud environment when running Cloud Validation Actions.

Google Cloud Requirements

- Google Cloud does not support API keys, you must use a service account.
- Create a key for your service account in the Google Cloud console.
- After the key is created, you can use a JSON file containing the Service Account Credentials to create this integration.
- The service account must have access to the following minimum permissions:
  - `logging.logEntries.list`
  - `logging.privateLogEntries.list`
  - `logging.views.access`
- These permissions can be provided by the Private Logs Viewer role, though this role might contain a few extra permissions.

Configure Google Cloud Logging Integration

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Google Cloud Logging**.



Configuration Page for Google Cloud Logging

3. Enter the following required values:
    - **Project ID**
    - **Client ID**
    - **Client Email**
    - **Private Key ID** and **Private Key**
    - **Token URI**
4. (Optional) Expand Advanced options and configure the following, as needed:

- Set the **Query time**.
- Set the **Delay time**.

> The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

> If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

- Select **Discover network devices automatically**.
- Specify the **Query Interval**.
- Set the **Event Time Adjustment**.
- Assign a **Name**.
- Choose whether to save suspicious events.

5. Click **Submit**.

Verify connectivity

Click **Test** to verify that:

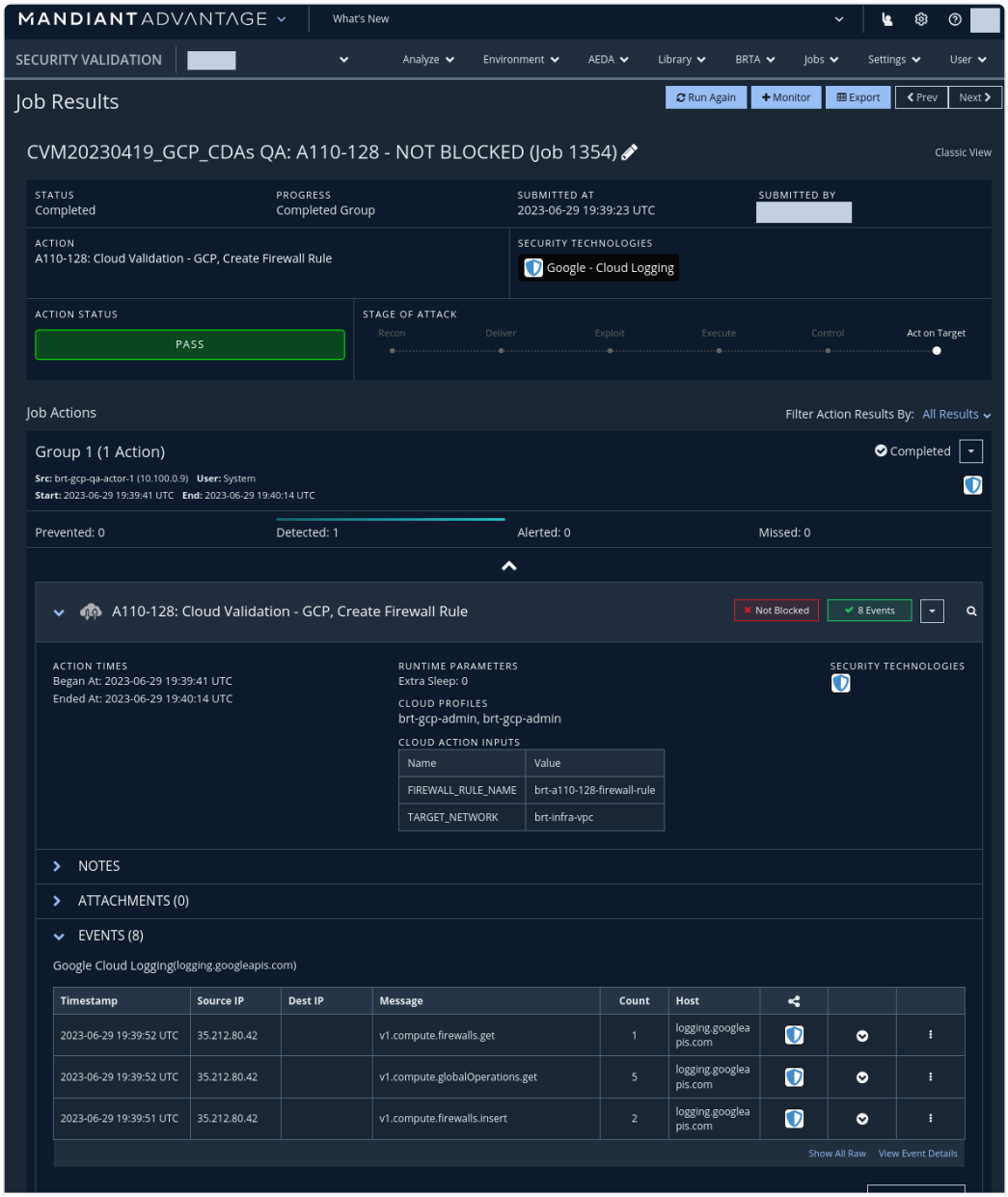
- The Director can communicate with Google Cloud Logging, and the Project ID and Client ID are correct.
- The Service Account Credentials provided can perform queries.

Audit logs

Audit logs are used and require setup in your Google Cloud environment. Data Access audit logs are disabled by default for every Google Cloud Service except BigQuery. For events to be created for Cloud Actions concerned with data access (such as Cloud Validation - GCP, List Firewall Rules (A300-004)), you need to follow the **Enable Data Access audit logs (https://cloud.google.com/logging/docs/audit/configure-data-access)** guide.

Sample Action

The following image shows an example of Job Results for a Cloud Action. The Job Results show events that are retrieved through the Google Cloud Logging integration:



Cloud Action for Google Cloud Logging Events