Mandiant

GOOGLE CLOUD LOGGING INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validates that security tools are writing log events to Google Cloud Logging to ensure compliance with security policies and regulations
- Collects events generated by security tools that write to Google Cloud Logging to test the efficacy and configuration of security controls using Security Validation jobs

Use this document to configure the integration using one of the following methods:

- MSI (Supported and recommended for new integration configurations)
- Legacy (Supported for existing integration configurations)

Configure MSI Integration

This method is the recommended approach for configuring new integrations in Security Validation.

This requires the Cloud Validation license.

To configure an integration, this document walks you through the following high-level steps:

1. Configure the third-party technology
2. Configure Security Validation
3. Verify connectivity

API Calls

API	Usage
`https://logging.googleapis.com/v2/projects`	Used to test connectivity and authentication settings
`https://logging.googleapis.com/v2/projects/{project_id}/queries`	Query for events in Google Cloud Logging

Supported Versions

- Google Cloud Logging API v2

Before You Begin

To configure this integration, you need the JSON-formatted keys to a Google Cloud Service Account with access to the Google Cloud Logging API

Create a Service Account and Generate Keys

1. Log into the Google Cloud Console
2. Navigate to the IAM & Admin section, then navigate to Service Accounts
3. Click "Create Service Account", then fill in the form with the appropriate data.
4. Click "Create and Continue", then grant access to the project and roles as required.
5. Click "Continue", then click "Done" to finish creating the Service Account.

6. Click the e-mail address for the new Service Account in the Cloud Console
7. Navigate to the "Keys" tab and click "Add Key"
8. Click "Create", and a JSON file containing the keys for the service account will be downloaded to your computer

Configure Security Validation

1. Go to **Settings** > **Integrations**.
2. From the Integrations table, click **Add Integration > Google BigQuery**.

   You can add this as either a Direct or Remote Integration.
3. Enter a meaningful **Integration Name**.
4. Optional: From the **Proxy** drop-down, choose a proxy profile if one is available. If one isn't available and all outbound connections go through a proxy, first, set up a **Proxy Rule** (https://docs.mandiant.com/home/msv-proxy-rules).
5. Enter the **Service Account Info** in valid JSON format, or read the credentials from the exported JSON file by clicking **Browse** and selecting the file that you generated.
6. Enter the **Project ID**, which is the Google Cloud project for the service account.
7. Optional: Add or remove **Queries**, as needed. A default is provided for **IP Query**.
8. Optional: Modify the **Field Map** values, as necessary.

   - Each field map box can hold a JSON-formatted comma-separated list of columns returned by the API to be considered for each field when translating into the normalized event object format. Example: description could be configured to be 'msg_s' or 'SyslogMessage' in some environments. The field map tries both if set to: ['msg_s','SyslogMessage'] and whichever matches first is the column that is used.
   - When configuring an integration in Security Validation, you can assign additional host values in the Field Map settings. If none of the assigned fields return a valid host name, Network Actions may miss matched events from the third-party technology. Additional hosts values helps ensure the likelihood of a match between the two environments.
9. Optional: Change the **Page Size** value to change the page size request per upstream server. The default is **500**.
10. Optional: Expand **Advanced options** and update the information as necessary.
    a. Update **Query Time** and **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.

    b. Update **Query Interval** (seconds).
    c. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
    d. Modify the **Correlation Query Interval**, if necessary (minutes).
    e. Select **Discover network devices automatically**, the default and recommended option.

> If unselected, reported events won't include product information for any matching network security technology.

f. Select **Save Suspicious Events**.
g. Modify the **Event Time Adjustment** (seconds). The default is **0**.
h. Modify the **Limit** value if you need to prevent a flood of results. This value is set to **10000** by default. This limit applies to both events and alerts individually, so if you set it to **10**, you can still see a maximum of 10 events and 10 alerts.

11. Click **Save**.

Verify connectivity

1. Go to **Settings > Integrations**.
2. From the Direct Integrations table, click ⋮ **> Test** to verify that:
   - The Director can communicate with the integration host on the port and protocol specified.
   - The integration credentials are valid and working.

For more information on setting up queries, see **Manage Integrations** (https://docs.mandiant.com/home/msv-managing-integrations).

Configure Legacy Integration

> 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.

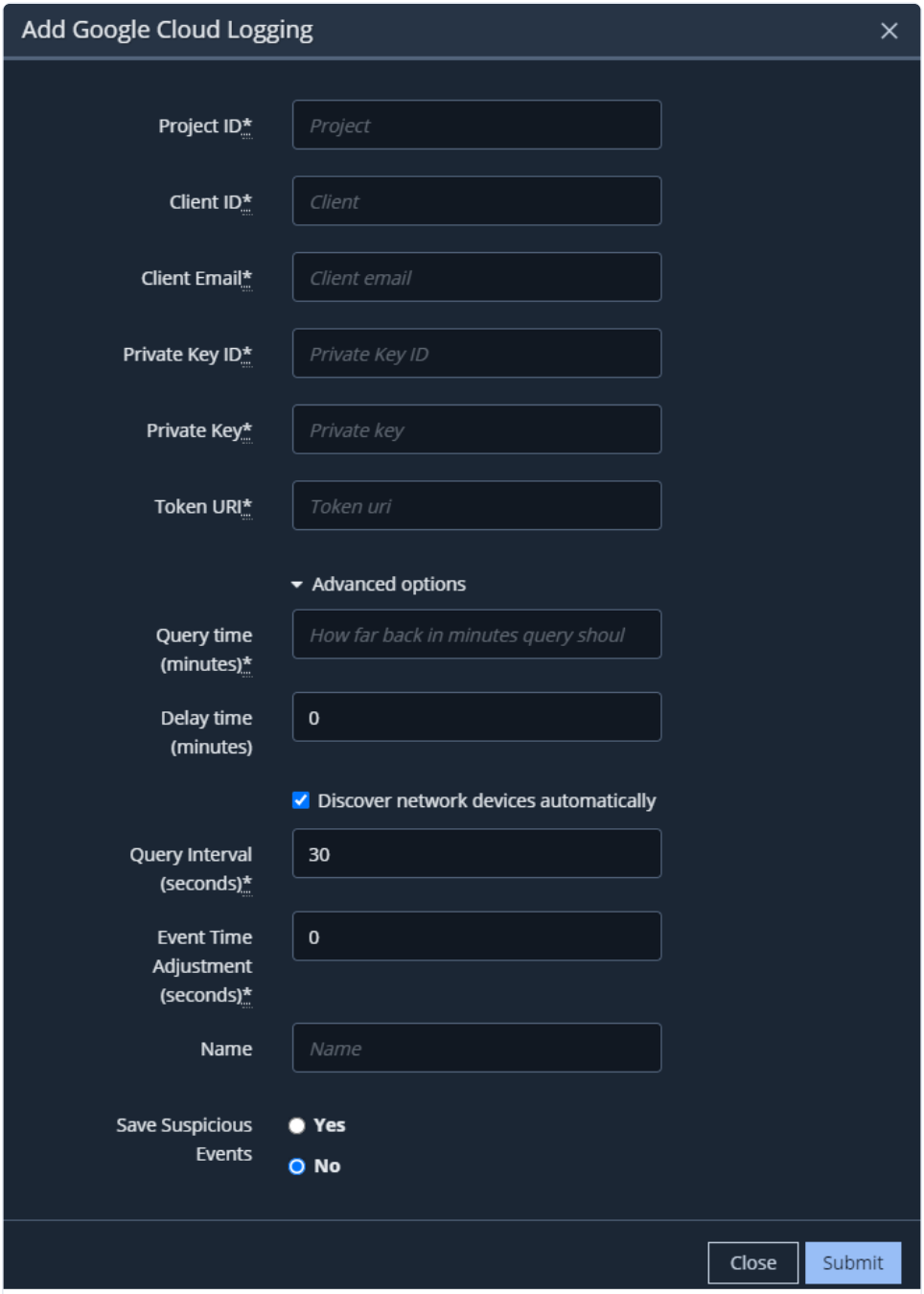
Google Cloud Requirements

- 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:

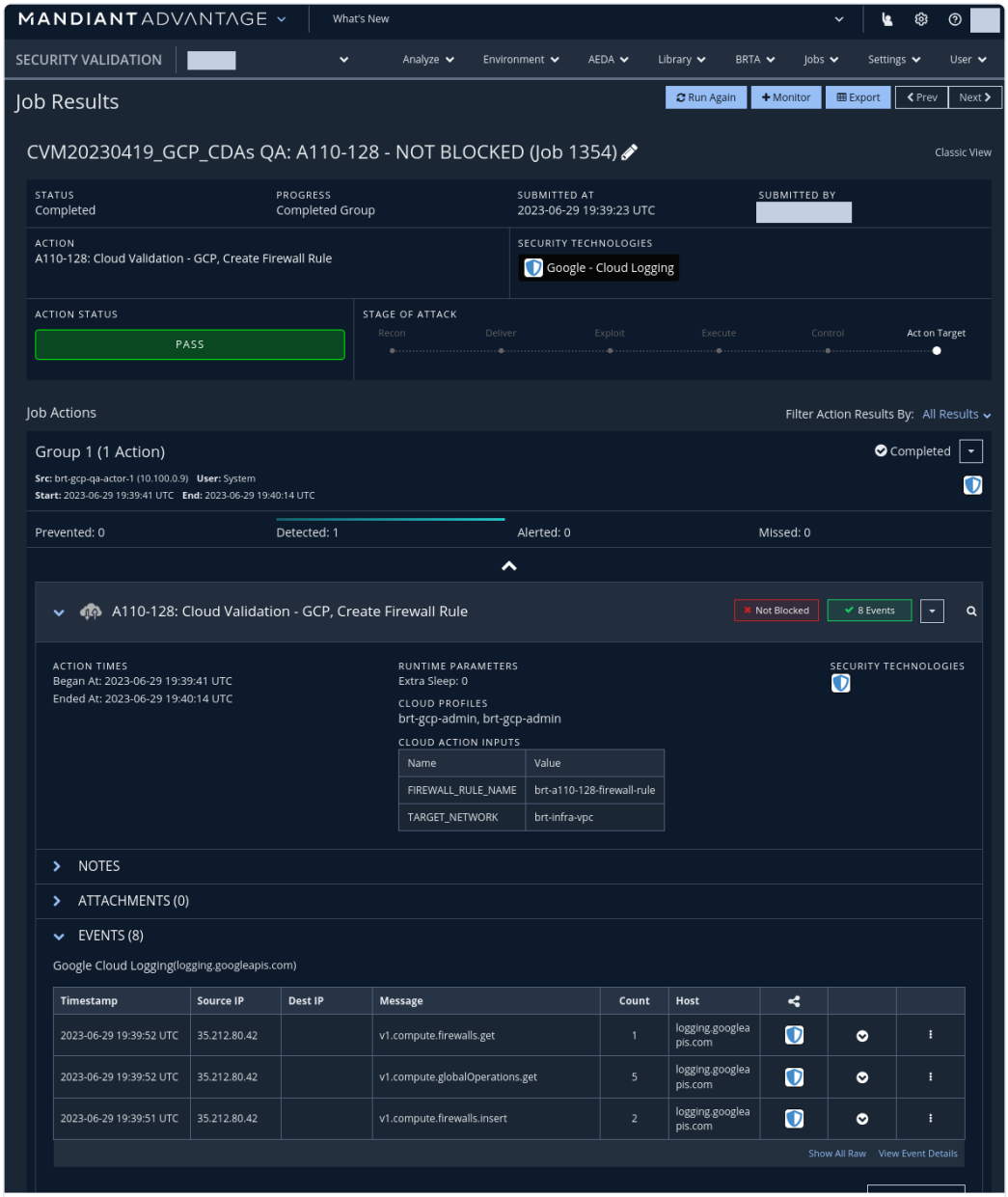
- The Director can communicate with Google Cloud Logging, and the Project ID and Client ID are correct.
- The Service Account Credentials provided can perform queries.

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