Mandiant

SUMO LOGIC INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validate that security tools are writing log events to Sumo Logic to ensure compliance with security policies and regulations
- Collects events generated by security tools that write to Sumo Logic 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.

API Calls

API	Usage
`/api/v1/search/jobs`	Start an asynchronous query job in Sumo Logic
`/api/v1/search/jobs/{search_id}`	Poll the status of a query job in Sumo Logoic
`/api/v1/search/jobs/{search_id}/messages`	Retrieve a list of events from a query job in Sumo Logic

Supported Versions

Sumo Logic API v1

Before You Begin

To configure this integration, you need:

- API Key
- API ID
- The hostname or IP address of your Sumo Logic instance

Create an API Key and ID

1. Log into Sumo Logic
2. Navigate to "Preferences", then click "Add Access Key" (in the "My Access Keys" section)
3. Enter a name for the new API Key
4. Click "Create Key", then make note of the API Key (Access Key) and API ID (Access ID)

Configure Security Validation

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

   

   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. Change the **HttpProtocols** to use for requests. (**Https** or **Http**.)
6. For the **Host**, enter the hostname of your LogRhythm Elastic instance.
7. Enter a **Port** value. The default is **443**.
8. Enter **API Id** and **Api Key** that you generated.
9. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
10. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
11. Optional: Add or remove **Queries**, as needed. Default values are provided.
12. 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.

13. 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.

14. 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 integration is remote capable.

Update Sumo Logic

TO UPDATE SUMO LOGIC

1. Generate a Sumo Logic API Access ID/Key pairing specifically for the Validation Platform's use. Refer to the **Sumo Logic Documentation (https://help.sumologic.com/Manage/Security/Access-Keys)** for instructions.

    Sumo Logic may not recognize the `validation.cloud` FQDN extension. When you configure your API Access ID/Key in Sumo Logic's admin console, you do not need to specify the domain.

2. Create a Sumo Logic account with sufficient permissions. Read permissions are required, at minimum.
3. (Optional) Create a custom field for the event_time field Security Validation uses. The default time in Sumo Logic may be incorrect because it is based on ingest time, not detect time. If you are concerned about this, you can create a new field, such as timestamp, to capture the required info. An example of this is shown in the code below. For additional details, see Sumo Logic's documentation on formatDate.

    ```
    | formatDate(toLong(timestamp*1000),"MM-dd-yyyy'T'HH:mm:ss'Z'") as event_time
    ```

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Identify the Sumo Logic host used to access the Sumo Logic cloud. The host is visible in the URL after logging in to the Sumo Logic web user interface.
2. API Access ID/Key.
3. Sumo Logic credentials.
4. Identify the field name mappings for the following (there could be multiple of each, depending on log sources and

configuration):

a. Source IP
b. Destination IP
c. Source Port
d. Destination Port
e. Event Signature ID
f. Event Name
g. Event Source Host
h. Event Time

Configuration

TO ADD THE SUMO LOGIC INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Sumo Logic**.
3. Select the Host.
3. Enter the **API Access ID** and **Key**.
4. Review and update the **Query** to include instance-specific field names.

   The default queries can be viewed by clicking **Show default query**.

5. Expand **Advanced options**.
6. (Optional) 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.

7. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

   If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

8. (Optional) Select **Discover network devices automatically**.
9. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
10. (Optional) Assign a **Name**.
11. (Optional) Choose **Yes** to save suspicious events.

12. Click **Submit**.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12dbc9cba0017c2f7e05/n/sumo.png)

Sumo Logic Integration

Set up Proxy Assignment

If all outbound connections go through a proxy, you may want to set up a proxy definition and assignment for your integration. For information on setting up your proxy rules, see **Proxy Rules (https://docs.mandiant.com/home/msv-proxy-rules)**.

Verify connectivity

TO VERIFY CONNECTIVITY TO SUMO LOGIC

Click **Test** to verify that:

- The Director can communicate with Sumo Logic using the API access information on the port and protocol specified.
- User credentials are working.