

# LOGRHYTHM SQL INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validates that security tools are writing log events to LogRhythm SQL to ensure compliance with security policies and regulations
- Collects events generated by security tools that write to LogRhythm SQL 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

The LogRhythm SQL Integration uses SQL to directly query LogRhythm.

- Any calls which return `varbinary` datatypes must be converted in the query:
  - `CONVERT(varchar(max),field_name,1)`
  - See the default queries for examples

## Supported Versions

- LogRhythm 7.2.x
- LogRhythm 7.3.x
- Logrhythm 7.7.x

## Before You Begin

To configure this integration, you need:

- A valid username and password for a user with permissions to sign in to the Microsoft SQL Database. (Read-Only)
- The hostname or IP address of your LogRhythm SQL instance

## Configure Security Validation

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



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. For the **Host**, enter the hostname of your LogRhythm SQL instance instance.
6. Enter a **Port** value. The default is **1433**.
7. Enter the **Database Type**. The default is **mssql**.
8. Optional: Change the **Database Name**, preset to **LogRhythm\_Events**.
9. Enter the **Username** and **Password** for the account that can sign into the SQL database with read-only

permissions.

10. Optional: Add or remove **Queries**, as needed. Default values are provided for **IP Query**, **Email Query**, **DNS Query**, and **Hostname Query**.
11. 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.

12. 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. Configure correlation queries:
    - i. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
    - ii. Modify the **Correlation Query Interval**, if necessary (minutes).
  - d. 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.

- e. Select **Save Suspicious Events**.
    - f. Modify the **Event Time Adjustment** (seconds). The default is **0**.
    - g. 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.

13. Click **Save**.

#### Verify connectivity


1. Go to **Settings > Integrations**.

- 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 \(https://docs.mandiant.com/home/msv-managing-integrations\)](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 \(https://docs.mandiant.com/home/msv-integrations-overview\)](https://docs.mandiant.com/home/msv-integrations-overview).

 This integration is not remote capable.

## Update LogRhythm SQL

- Verify you have the latest LogRhythm Knowledge Base updates added to your instance. These updates contain rules and identifiers for various actors and actions.
- Disable LogMart on any log sources where it is not explicitly required. The resources used by LogMart can cause delays when Actions are run.

## Update the Validation Platform

### Prerequisites

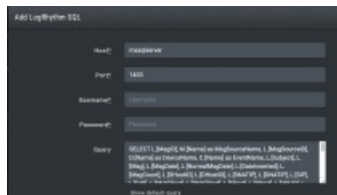
Information to gather before you start:

- Identify the host (name or IP) and Port information.
- Have a valid account for LogRhythm SQL.

### Configuration

#### **TO ADD THE LOGRHYTHM SQL INTEGRATION**

- Go to **Settings > Integrations**.
- Click **Add Integration > LogRhythm SQL**.



(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e0c9cba0017c2f7e34/n/logrhythm-sql.png>)

LogRhythm SQL Integration

- Enter information for the **Host**, **Port**, **Username**, and **Password**.
- Expand **Advanced options**.



(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12dfc9cba0017c2f7e2e/n/logrhythm-sql-adv.png>)

LogRhythm SQL Integration

5. (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 Action 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.

6. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
7. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will only be used when you run Email Actions.
8. (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.



If you find that LogRhythm SQL is matching too many noisy logs, we recommend you add `MsgSourceID` to the WHERE clause in the Host CLI Actions query. For example, `WHERE L.[NormalMsgDate] = '%START_TIME%' AND L.[MsgSourceID] = 1`. If the events are still too noisy, consider adjusting your Risk Based Priority (RBP) settings in LogRhythm.

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

Verify Connectivity

**TO VERIFY CONNECTIVITY**



Click **Test** to verify that:

- The Director can communicate with the LogRhythm SQL host on the port specified.
- The LogRhythm SQL credentials are valid and working.