AWS CLOUDWATCH

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.

Update AWS CloudWatch

Identify or create credentials to access CloudWatch with read access and CloudWatchLogsFullAccess permission, at minimum.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Create query	Ruby Aws::CloudWatchLogs::Client.start_query
Get query results	Ruby Aws::CloudWatchLogs::Client. get_query_results

Update the Security Validation Platform

Prerequisites

Information to gather before you start:

- CloudWatch Access Key ID

  An AWS admin can generate this for you.

- CloudWatch Secret Access Key
- The Amazon region associated with your account.
  The following regions are supported:
  - ap-northeast-1
  - ap-northeast-2
  - ap-northeast-3
  - ap-southeast-1
  - ap-southeast-2
  - ap-south1
  - ca-central-1
  - eu-central-1
  - eu-west-1
  - eu-west-2
  - eu-west-3

- sa-east-1
- us-east-1
- us-east-2
- us-west-1
- us-west-2
- us-gov-east-1
- us-gov-west-1

> See the **AWS documentation (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html)** for information on the different regions and their full names.

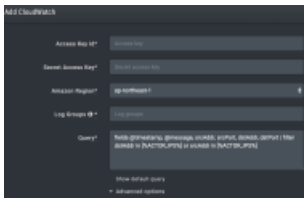
Configuration

TO ADD THE AWS CLOUDWATCH INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **CloudWatch**.

> You can add this as either a Local or Remote Inetgration.

3. Enter the **Access key Id** and the **Secret Access Key**.
4. Select an **Amazon Region**.
5. Enter the **Log Groups** from CloudWatch.
6. (Optional) Configure the **Query**.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e3c9cba0017c2f7e54/n/aws-cloudwatch.png)

AWS Cloudwatch Integration

7. Expand **Advanced options**.
8. (Optional) Update **Query time** and **Delay time**.

> The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. 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, it will impact the pass/fail results for AEDA monitors.

9. (Optional) Select **Enable query for Malicious DNS Actions**, then
    a. Enter the Log Groups to use with Malicious DNS Actions
    b. Configure the **Query**.

    This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.

10. (Optional) Select **Enable query for Email Actions**, then
    a. Enter the Log Groups to use with Email Actions.
    b. Configure the **Query**.

    This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.

11. (Optional) Select **Enable query for Host CLIActions** and:
    a. Enter the Log Groups to use with Host CLI Actions
    b. Configure the **Query**.

    This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.

12. Identify the field name mappings for the following (there could be multiple of each, depending on log sources and configuration): **Verify full list and order in UI**
    - Source IP
    - Destination IP
    - Source Port
    - Destination Port
    - Event Source Host
    - Event Start Time (timestamp)
    - Unique ID
    - Event Signature ID
    - Event Description
    - Email Sender
    - Email Recipient
    - Email Subject
    - URL
    - Username
13. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
14. (Optional) Assign a **Name**.
15. (Optional) Choose **Yes** to save suspicious events.
16. Click **Submit**.

AWS CloudWatch Integration (Advanced Options)

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 AWS CLOUDWATCH

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.