Mandiant

GRAYLOG

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 Graylog

Identify or create credentials to access Graylog with read access, at minimum.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Search raw logs	/api/search/universal/absolute
Search alert events	/api/events/search

Due to a limitation in the Graylog API, the Validation Platform alert correlations are only populated by Graylog filter alerts.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Identify the hostname/IP used to access Graylog.
- Identify the Port used for Graylog communication (this defaults to 443).
- Identify whether the protocol is HTTP or HTTPS for connections to the Graylog port.
- Obtain the username and password of a Graylog account with appropriate access permissions.

Configuration

TO ADD THE GRAYLOG INTEGRATION

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

   You can add this as either a Local or Remote Integration.
3. Enter information for the **Host**, **Port**, **Protocol**, **Username** and **Password** or **API Token**.
4. Review and update the **Query**.

   The %ACTOR_IPS% variable can be used in all queries. This improves event matching.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12efc9cba0017c2f7ec5/n/graylog.png)

Graylog Integration

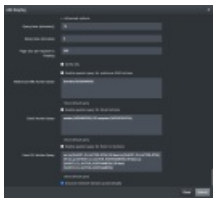
5. Expand **Advanced options**.
6. (Optional) Update **Query time** and **Delay time**.

> 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 Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
8. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will only be used when you run Email Actions.
9. (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.



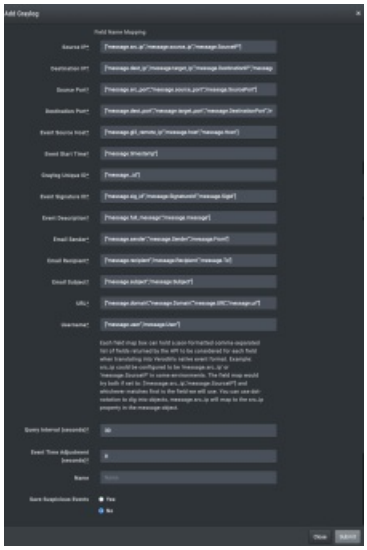
(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12dbc9cba0017c2f7e03/n/graylog-adv-1.png)

Graylog Integration (Advanced Options)

10. Identify the field name mappings for the following (there could be multiple of each, depending on log sources and configuration):
    - Source IP
    - Destination IP

- Source Port
- Destination Port
- Event Source Host
- Event Start Time (timestamp)
- Graylog Unique ID
- Event Signature ID
- Event Description
- Email Sender
- Email Recipient
- Email Subject
- URL
- Username

11. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
12. (Optional) Assign a **Name**.
13. (Optional) Choose **Yes** to save suspicious events.
14. Click **Submit**.



Graylog 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 GRAYLOG

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.