Mandiant

TRELLIX HELIX

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 Trellix Helix

Using your IAM account, create an API key for use with the Validation Platform. Verify your key has the following Helix entitlements, at a minimum:

- tap.events.browse
- tap.events.read
- tap.alerts.browse
- tap.alerts.read
- tap.lists.browse
- tap.lists.read
- tap.search.*

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Get Events	`/v1/search`
Alerts query	`/v3/alerts`

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Identify your Trellix FQDN. Trellix FQDNs are based on the region associated with your instance:
   - US: apps.fireeye.com
   - EU: helix.eu.fireeye.com
   - AP: helix.ap.fireeye.com
2. Identify your Helix Instance ID.
3. Check whether your Helix instance is configured to leave alerts open, close alerts, or a combination of both.

Configuration

TO ADD THE TRELLIX HELIX INTEGRATION

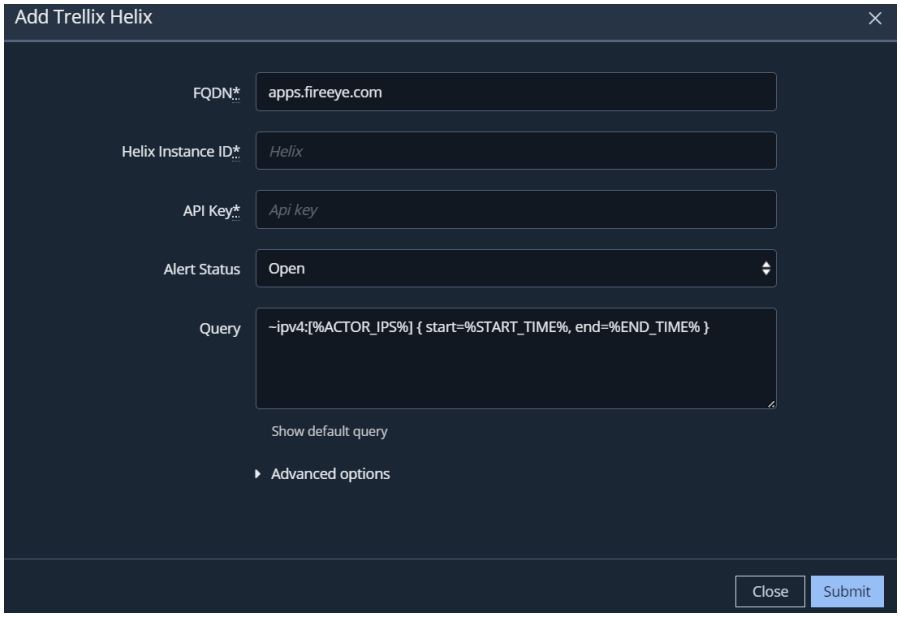
1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Trellix Helix**.

   You can add this as either a Local or Remote Integration.
3. Enter information for the **FQDN**, **Helix Instance ID**, and **API Key**.
4. Select whether the Validation Platform should look for open Helix alerts, closed Helix alerts, or both.
5. Update the **Query**, as necessary.
6. Expand **Advanced options**.
7. (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.

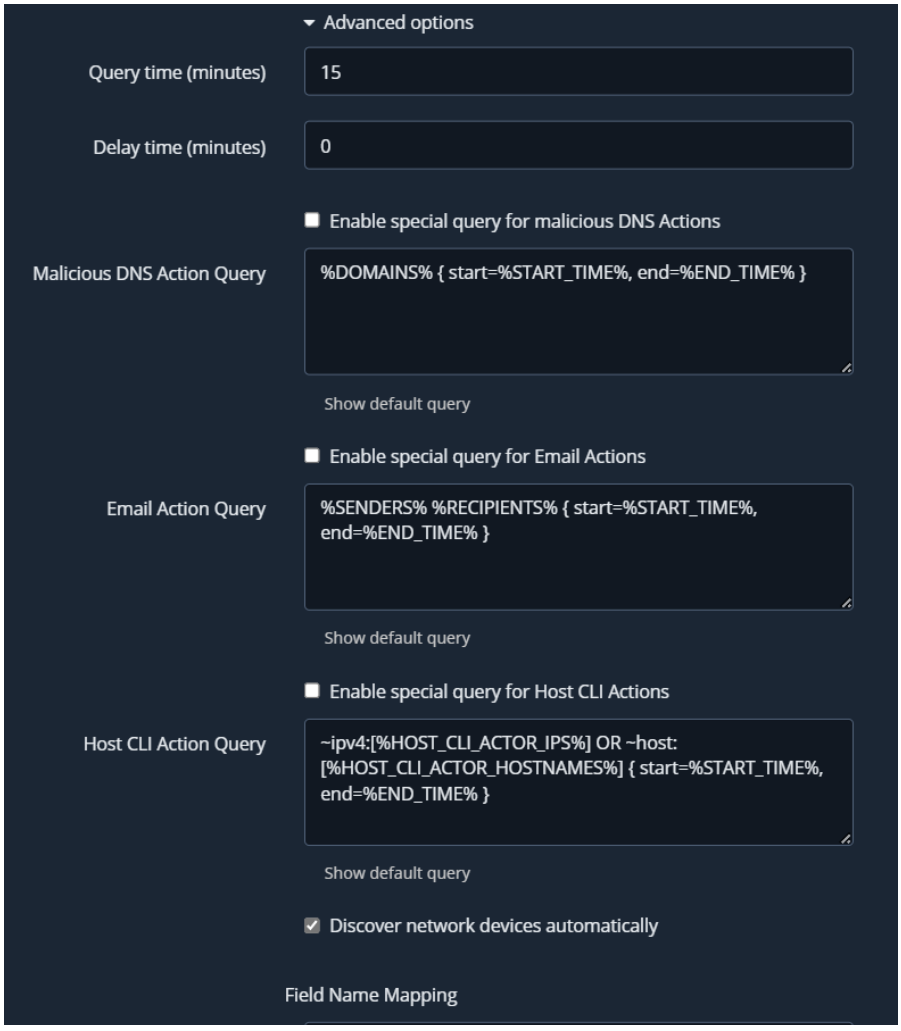
   If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.
8. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
9. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will be only be used when you run Email Actions.
10. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

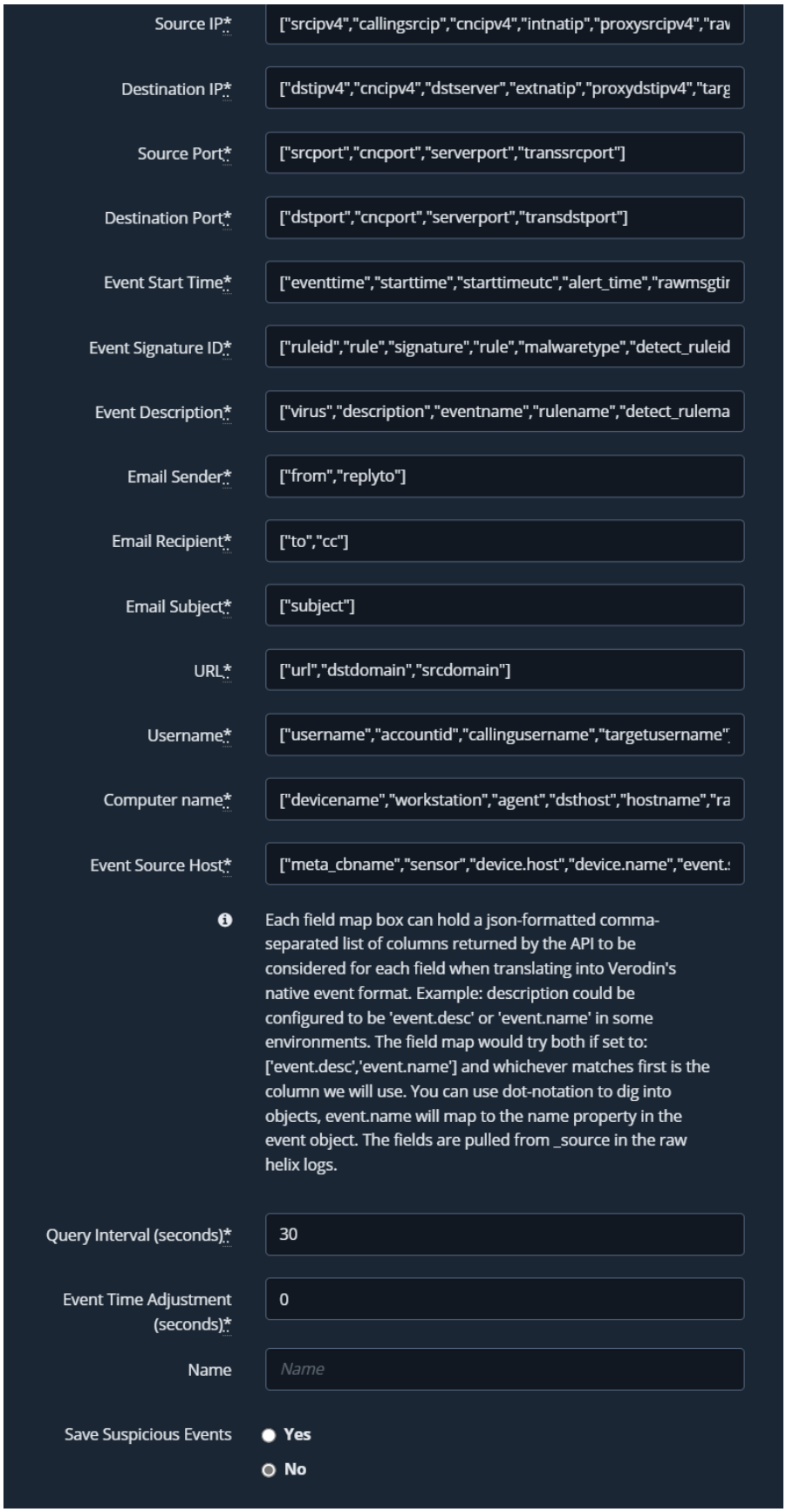
    If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.
11. (Optional) Select **Discover network devices** automatically.
12. Review and update the **Field Name Mapping** fields.
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**.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/63ebf77ac9ec1e48182a725a/n/trellix-helix.png)

Trellix Helix Integration





(https://dyzz9obi78pm5.cloudfront.net/app/image/id/63ecf3409427d260527efc4d/n/trellix-helix-advanced-options.png)

Trellix Helix 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 TRELLIX HELIX

Click **Test** to verify that:

- The Director can communicate with the Trellix Helix console using the provided host and user information.
- The API Server is enabled and allowing communication.

If the test is not successful, messages will be displayed to help identify possible issues, such as no connection to the API server.