TRELLIX HELIX INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validate that security tools are writing log events to Trellix Helix to ensure compliance with security policies and regulations
- Collect events generated by security tools that write to Trellix Helix 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 document covers the the MSI method of creating an integration. This method is the recommended approach for configuring new integrations in Security Validation.

This feature is released as a Public Preview.
Pre-GA products and features are available "as is" and might have limited support. For more information, please contact your TSC, your CSM, or go to **Support.**
(https://docs.mandiant.com/home/mandiant-support-cases)

API calls

API	Usage
`/v1/search`	Query for events from Trellix Helix
`/v3/alerts`	Query for events from Trellix Helix

Supported versions

Trellix Helix API v1 (Legacy & Unified IAM)

Preparation

Authentication & IAM System

This integration supports the migration from the legacy FireEye IAM to the unified Trellix IAM (OAuth 2.0). You must configure the integration according to the IAM system your tenant is currently using.

IAM System Selection

In the configuration, you will find a selector for IAM System:

- FireEye (Legacy): Use this if your tenant still authenticates via apps.fireeye.com using static API Keys.
- Trellix (Modern): Use this if your tenant has been migrated to iam.cloud.trellix.com and requires OAuth 2.0 Client Credentials.

Before You Begin

To configure this integration, you will need the Helix ID (e.g., hexnrv555) and the authentication credentials corresponding to your selected system.

For FireEye IAM (Legacy)

- **API Key**: A valid x-fireeye-api-key.
- **Required Entitlements**:
  - **tap.search.browse** (for event search)
  - **tap.alerts.read** (for alert retrieval)

For Trellix IAM (Modern / OAuth 2.0)

- **Client ID**: The unique application identifier.
- **Client Secret**: The secret key (note: this is shown only once upon creation).
- **Auth URL**: (Optional) The OAuth2 token endpoint. Default: **https://iam.cloud.trellix.com/iam/v1.1/token**.
- **Required Scopes**: Ensure the following scopes are assigned to your Client Credentials to allow the integration to function:
  - **hlx.srh.r** (Replaces tap.search.browse)
  - **hlx.alr.r** (Replaces tap.alerts.read)

Configure Security Validation

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

   
   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. Optional: Change the **HttpProtocols** value to determine what protocol is used for requests (**Http** or **Https**).
6. Enter the **Host** value for the Trellix instance as a hostname or IP address.
7. Enter a **Port** value. The default is **443**.
8. For **IAM System**, choose a value, depending on your environment:
   - **FireEye**: if you authenticate with API keys, choose this option.
   - **Trellix**: if you authenticate with OAuth 2.0 client credentials, choose this option.
9. Enter the **Helix Id**. The format looks similar to this example: hexnrv555.
10. Optional: If you chose **FireEye** in the previous step, enter the **Legacy API Key** value.
11. Optional: If you chose **Trellix** in the previous step, follow these steps:
    a. Enter the **Auth URL**.
    b. Enter the **Client ID** and **Client Secret** values.
12. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
13. Optional: Change the default **Alert State** option to search, if needed. Options include **Open**, **Closed**, or **Open|Closed**.
14. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
15. Optional: Add or remove **Queries**, as needed. Defaults are provided: **IP Query**, **Domain Query**, **Email Query**, and **Hostname Query**.
16. 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.

17. Optional: Change the value for **Page Size** (default **500**) if needed.
18. 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. If supported by your integration, 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.
19. 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 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

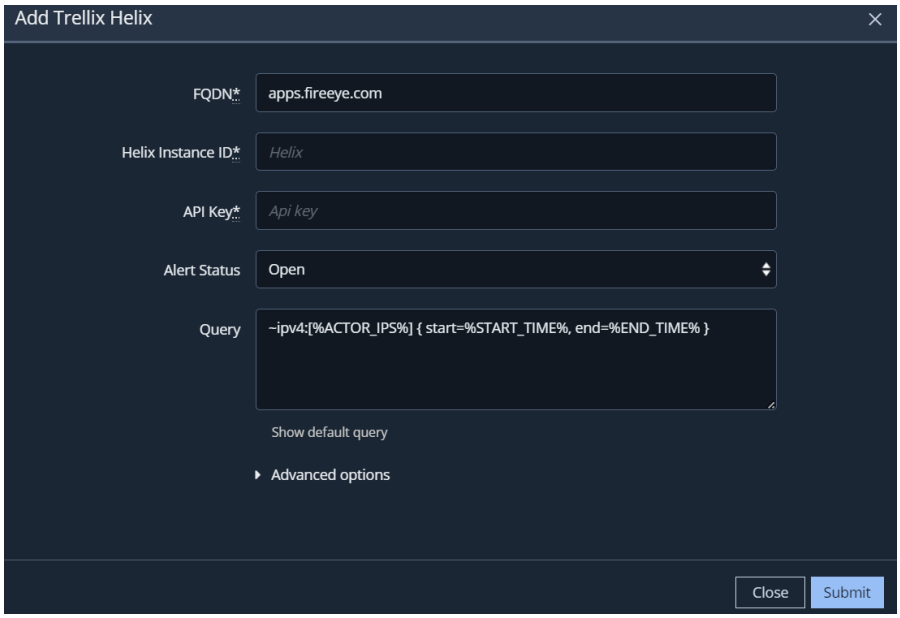
1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Trellix Helix**.

   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.

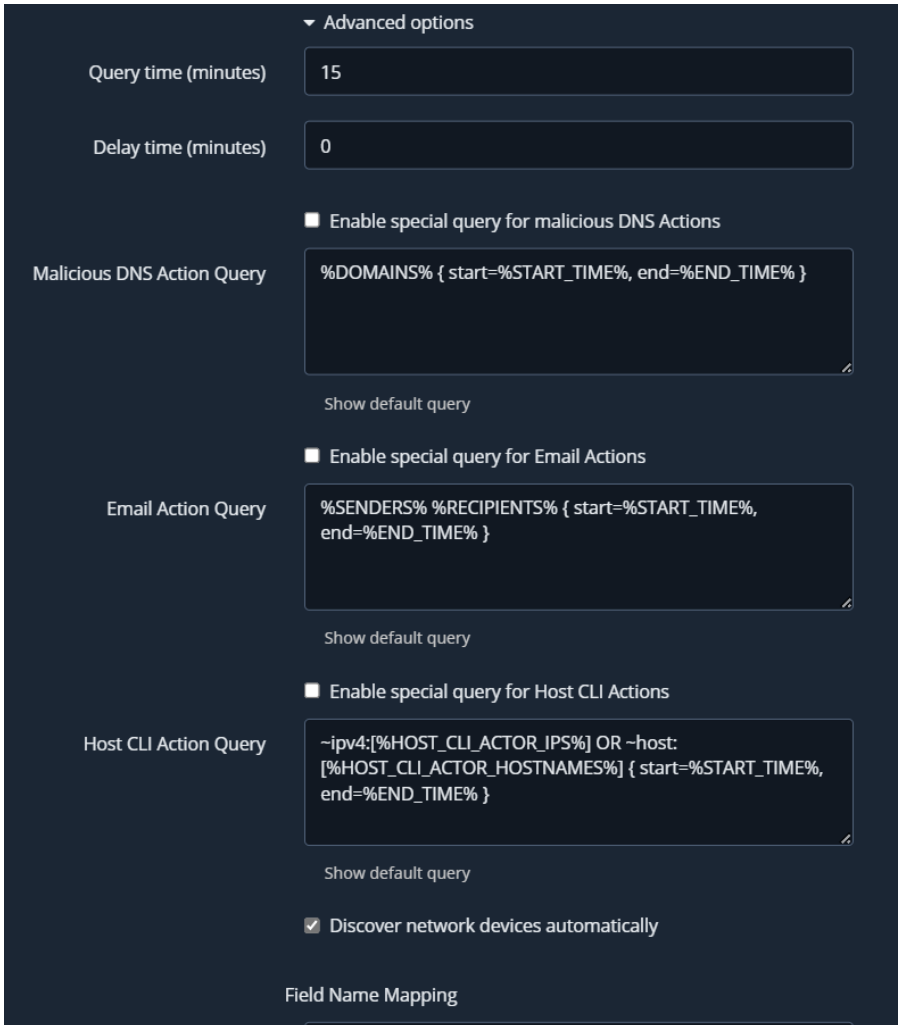
   If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.
8. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.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

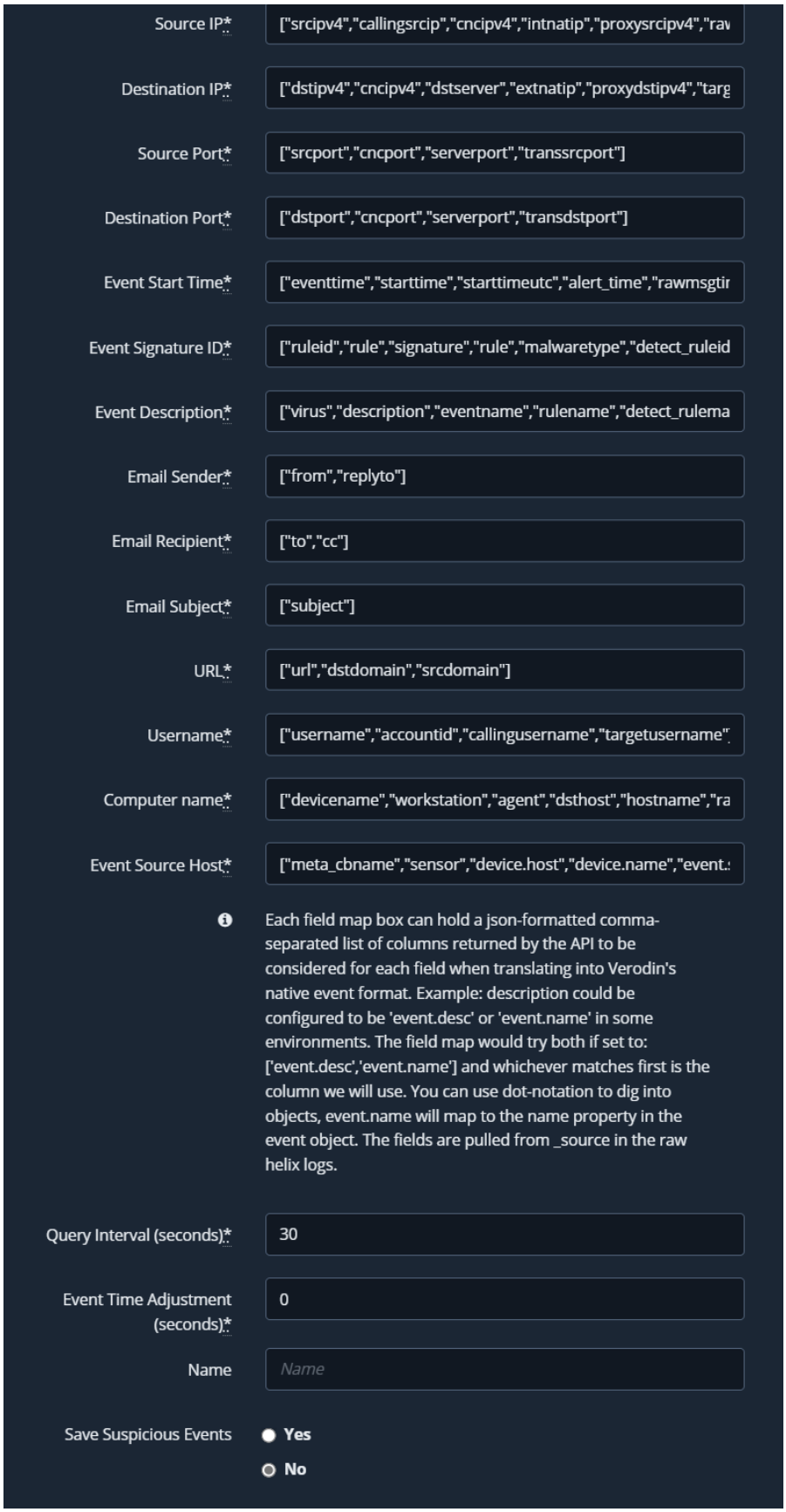
    If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.
11. (Optional) Select **Discover network devices** automatically.
12. Review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