TRELLIX ENDPOINT SECURITY (HX)

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 Endpoint Security (HX)

Create a Trellix Endpoint Security (HX) API Account for use with the Validation Platform. This must use the API_Analyst role.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Login for a token	`/hx/api/v3/token`
Alerts query	`/hx/api/v3/alerts/?agent. id=(DeviceId)&limit=(PageLimit)&offset=(PageOffset)&filterQuery=(ReportedAtTimestampFilterQuery)`
Hosts Query	`/hx/api/v3/hosts`

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Identify the Trellix Endpoint Security (HX) Host and Port information.
2. Have a Trellix Endpoint Security (HX) API User Account with the API_Analyst role.

Configuration

TO ADD THE TRELLIX ENDPOINT SECURITY (HX) INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Trellix Endpoint Security (HX)**.

   You can add this as either a Local or Remote Integration.

3. Enter information for the **Host**, **Port**, **Username**, and **Password**.

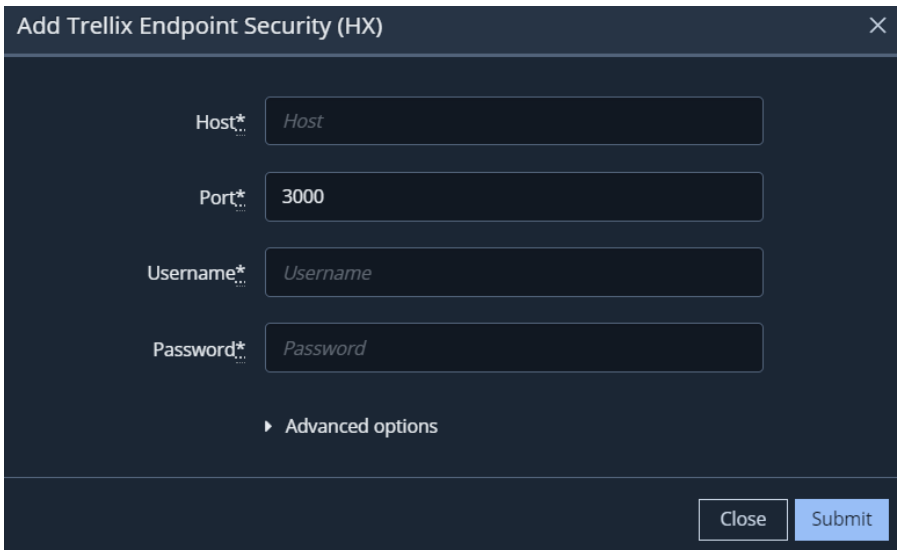
   Port 3000 is required for on-prem HX appliances

4. Expand **Advanced options** and update the information if necessary.
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 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.

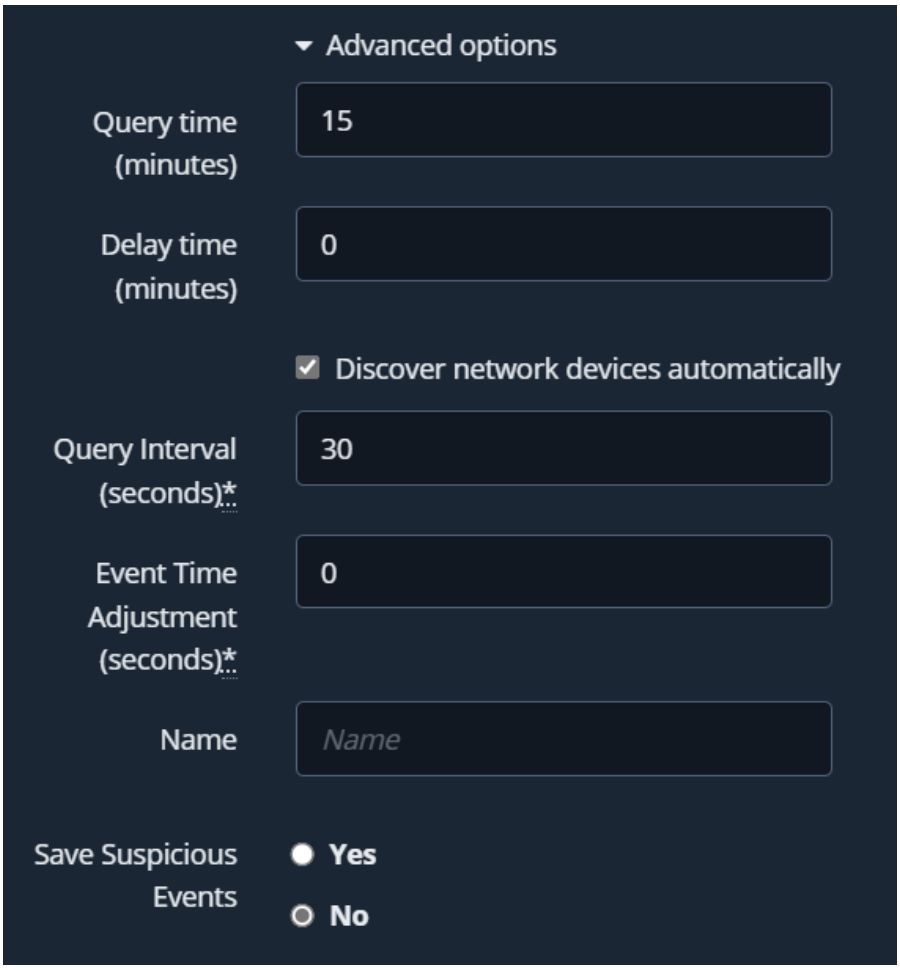
If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

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



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/63ebf667c0da4a6d8947e740/n/trellix-endpoint-security-hx.png)

Trellix Endpoint Security (HX) Integration



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/63ecf34defbf62424e348ffe/n/trellix-endpoint-security-hx-advanced-options.png)

Trellix Endpoint Security (HX) 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 ENDPOINT SECURITY (HX)

Click **Test** to verify that:

- The Director can communicate with the Trellix Endpoint Security (HX) console using the provided host and user information.
- The Webservice API 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.