TRELLIX ENTERPRISE SECURITY MANAGER

> 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).

The Trellix Enterprise Security Manager Integration supports correlation events when using Trellix Enterprise Security Manager v10.x.

> This integration is remote capable.

Update Trellix Enterprise Security Manager

TO UPDATE TRELLIX ENTERPRISE SECURITY MANAGER

1. Identify or create credentials to access Nitro with reporting permissions, at minimum.
2. Ensure that the credentials use Greenwich Mean Time and "YYYY-MM-DD HH:MM:SS" date/time format.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- IP address/host information used to access Trellix (ESM or ePO)
- Port for Trellix (ESM or ePO) communications (default is 443)
- Identify whether the protocol is HTTP or HTTPS for connections to the port (default is HTTPS)

Configuration

TO ADD THE TRELLIX ENTERPRISE SECURITY MANAGER INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Trellix Enterprise Security Manager**.

   > 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. If necessary, modify the **Query**.
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.

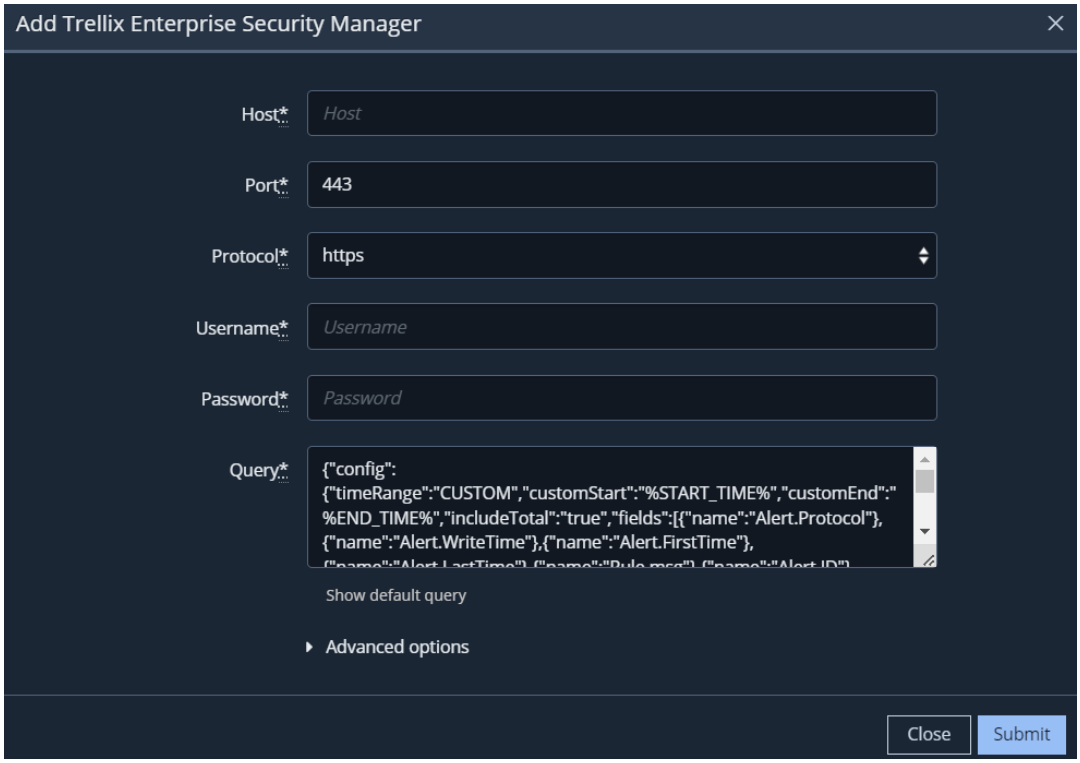
7. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

   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.

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. Verify that the **Device List Refresh Interval** is correct.
11. (Optional) Review and update the **Device Type List** information.
12. Enter the **McAfee version**.

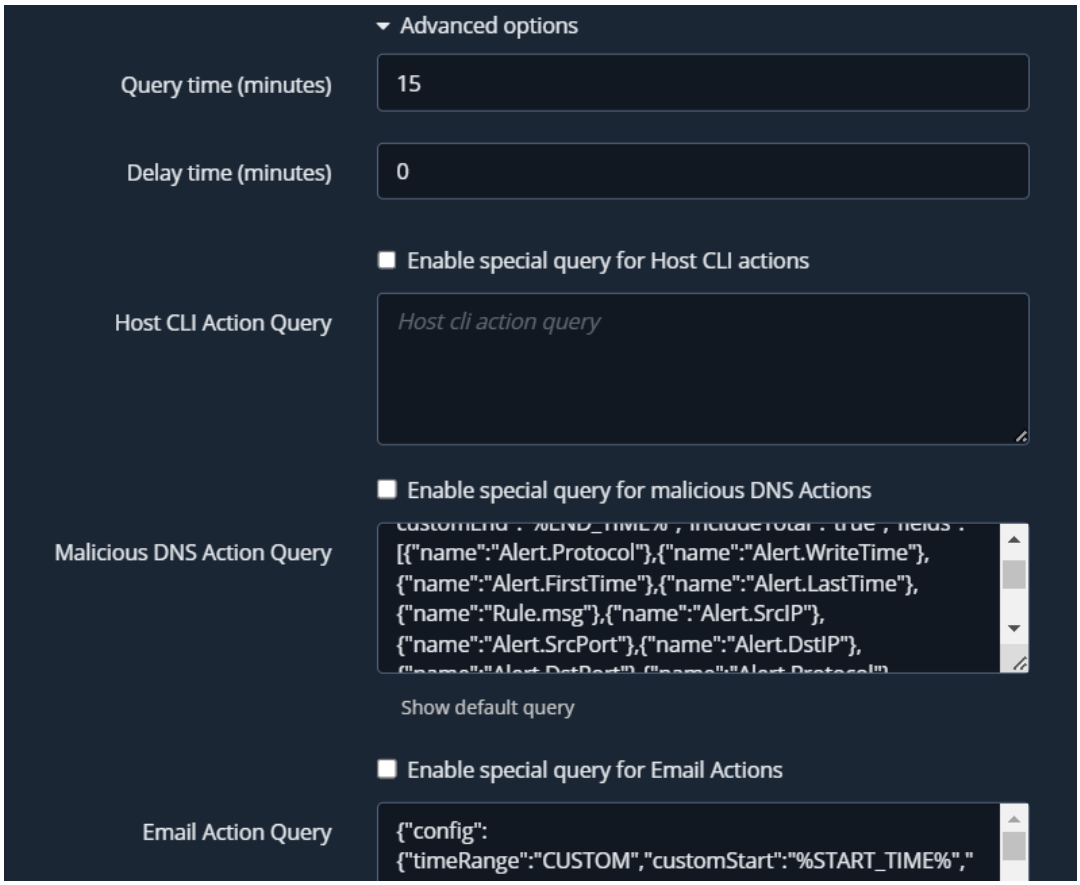
    If you are using version 11.0 or greater, you must enter your version number in this field to use the current version of Trellix Enterprise Security Manager's API. By default, version 10 is assumed.

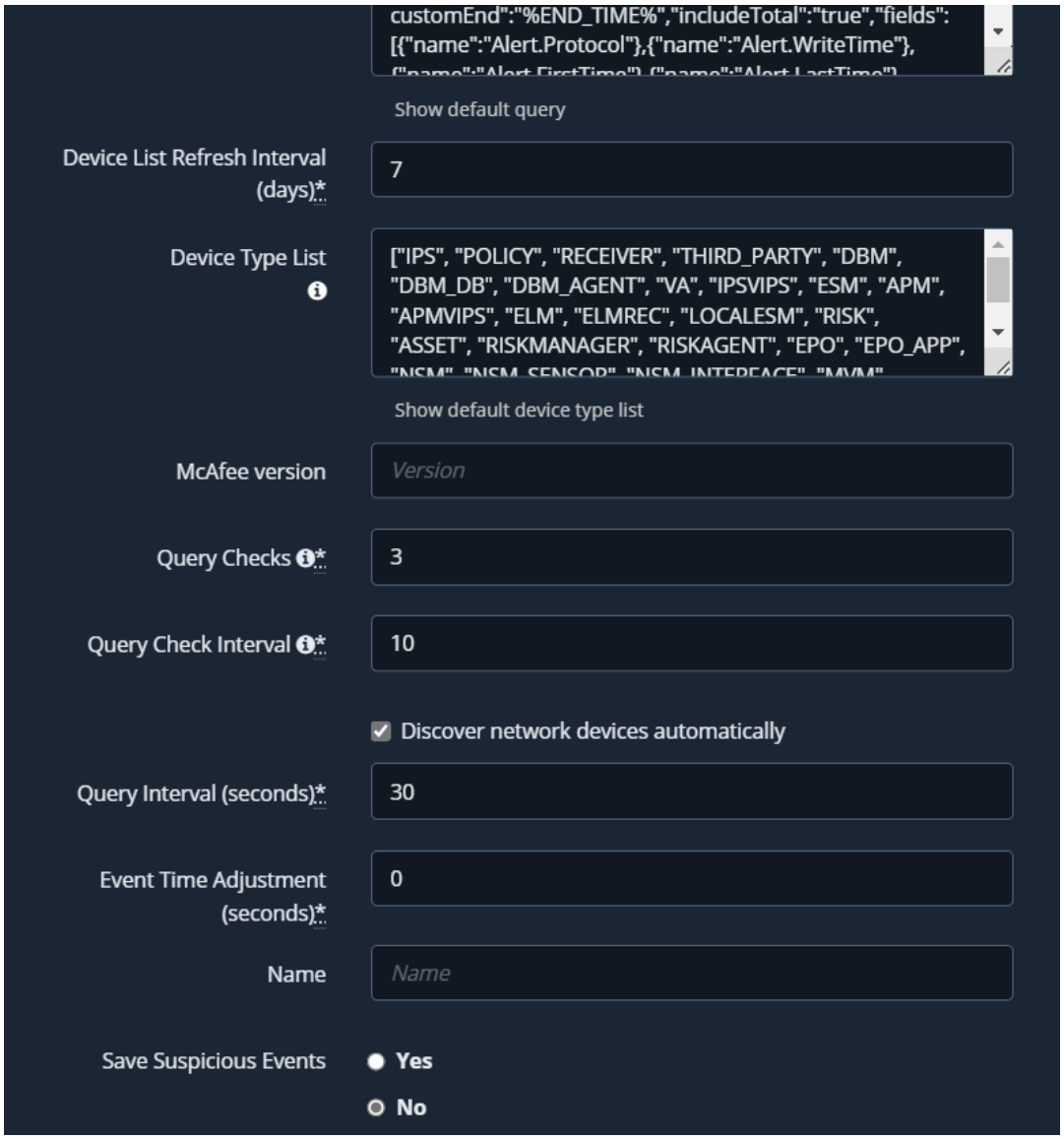
13. Modify the number of **Query Checks** and the **Query Check Interval**, if needed.
14. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
15. (Optional) Assign a **Name**.
16. (Optional) Choose **Yes** to save suspicious events.
17. Click **Submit**.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/63ebf00f2876576d4939b7c6/n/trellix-enterprise-security-manager.png)

Trellix Enterprise Security Manager Integration





(https://dyzz9obi78pm5.cloudfront.net/app/image/id/63ecf2d822231f4e6777d2b7/n/trellix-enterprise-security-manager-advanced-options.png)

Trellix Enterprise Security Manager Integration - Advanced options

Verify Connectivity

TO VERIFY CONNECTIVITY TO TRELLIX ENTERPRISE SECURITY MANAGER

Click **Test** to verify that:

- The Director can communicate with Trellix Enterprise Security Manager IP address on the port specified.
- Credentials are valid and working.