Mandiant

TRELLIX ENTERPRISE SECURITY MANAGER INTEGRATION WITH SECURITY VALIDATION

This integration collects events generated by Trellix Enterprise Security Manager to test the efficacy and configuration of the security control 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 method is the recommended approach for configuring new integrations in Security Validation.

API Calls

API	Usage
`/rs/esm/v2/qryExecuteDetail`	Execute a query for alerts from Trellix Enterprise Security Manager
`/rs/esm/v2/qryGetStatus`	Retrieve the status of a query from Trellix Enterprise Security Manager
`/rs/esm/v2/qryGetResults`	Retrieve the results of a query from Trellix Enterprise Security Manager
`/rs/esm/v2/ipsGetCorrRawEvents`	Retrieve events correlated to a given alert from Trellix Enterprise Security Manager
`/rs/esm/v2/login`	Authenticate against Trellix Enterprise Security Manager and retrieve an auth token
`/rs/esm/v2/logout`	Log out of the Trellix Enterprise Security Manager session
`/rs/esm/v2/getVersion`	Used to test connectivity and authentication settings

Supported Versions

Trellix Enterprise Security Manager API v2

Before You Begin

To configure this integration, you need:

- A valid username and password for a user with permissions to use the API endpoints described in the previous step
- The hostname or IP address of your Trellix Enterprise Security Manager instance

Configure Security Validation

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

   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. Change the **HttpProtocols** to use for requests. (**Https** or **Http**.)
6. For the **Host**, enter the hostname of your Trellix Enterprise Security Manager instance. The default is **httpbin.org**.
7. Enter a **Port** value. The default is **443**.
8. Enter the **Username** and **Password** for the account the can access the API endpoints.
9. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
10. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
11. Optional: Add or remove **Queries**, as needed. Default values are provided.
12. Optional: Change the **Query Check Interval**, the number of seconds between each check for query execution completion. The default is **5**.
13. Optional: Change the Max Query Checks, the maximum number of times a query is checked for completion before terminating. The default is **3**.
14. Optional: Modify the **Page Size** to change the request for the upstream server. The default is **500**.
15. 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.

16. 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. 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.

17. 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)**.

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.

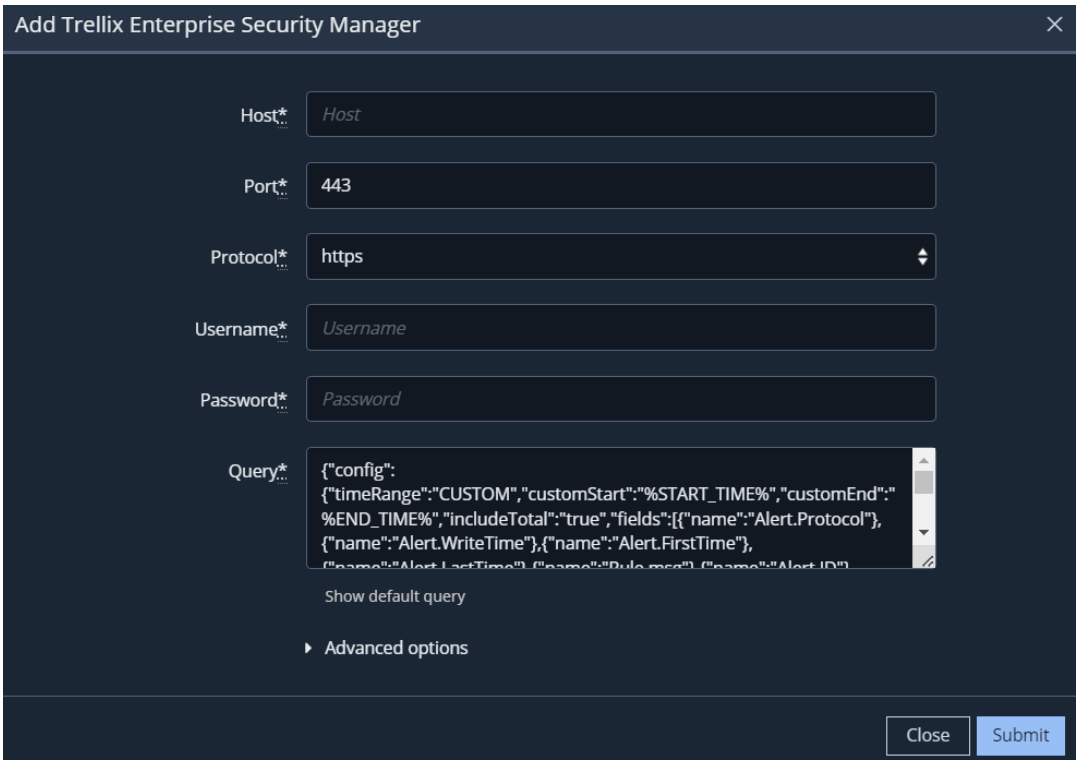
   If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

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.

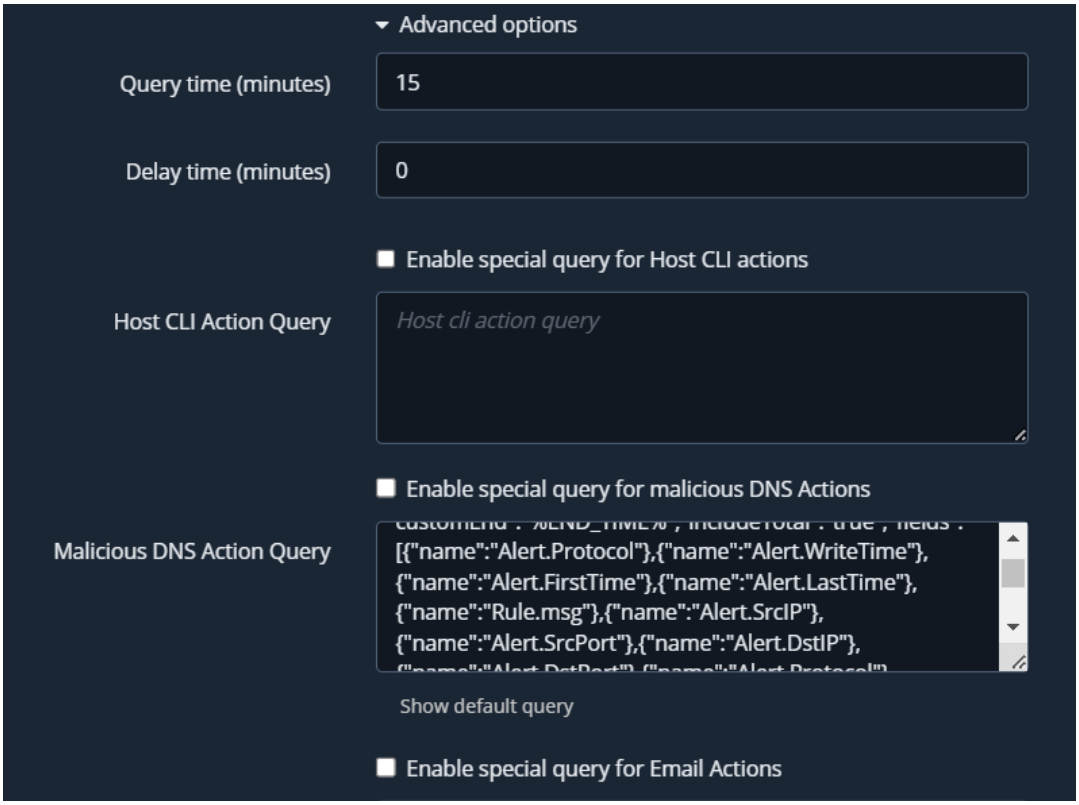
13. Modify the number of **Query Checks** and the **Query Check Interval**, if needed.
14. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
15. (Optional) Assign a **Name**.
16. (Optional) Choose **Yes** to save suspicious events.

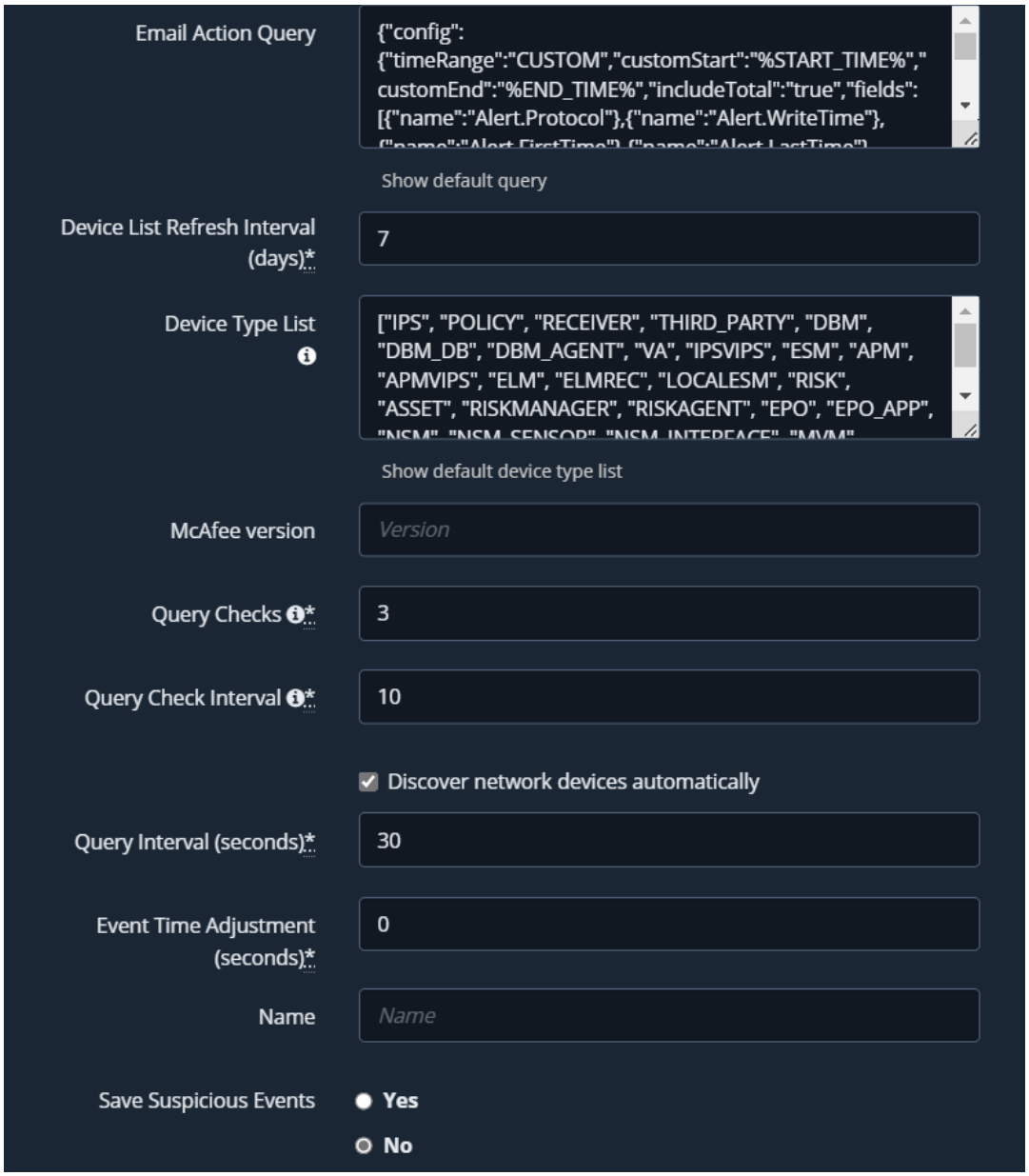
17. Click **Submit**.



(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.