

TRELLIX NETWORK DLP WITH SECURITY VALIDATION

This integration collects events generated by Trellix Network DLP 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
<code>/remote/core.executeQuery</code>	Query for events from Trellix Network DLP
<code>/remote/core.help</code>	Used to test connectivity and authentication settings

Supported Versions

Trellix Data Loss Prevention (DLP) Endpoint 11.x

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 Network DLP instance

Configure Security Validation

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



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 Network DLP instance.
7. Enter a **Port** value. The default is **443**.
8. Enter the **Username** and **Password** for the account that 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. A default is provided for **Hostname Query**.
12. 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.

13. 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 Action 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. Select **Correlation Query Enabled** and fill in the **Correlation Query**.

d. Modify the **Correlation Query Interval**, if necessary (minutes).

e. 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.

f. Select **Save Suspicious Events**.

g. Modify the **Event Time Adjustment** (seconds). The default is **0**.

h. 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.

14. 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-](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 \(https://docs.mandiant.com/home/msv-integrations-overview\)](https://docs.mandiant.com/home/msv-integrations-overview).



This integration is remote capable.

Update Trellix Network DLP

Identify or create credentials to access ePO with read permissions, at minimum.

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

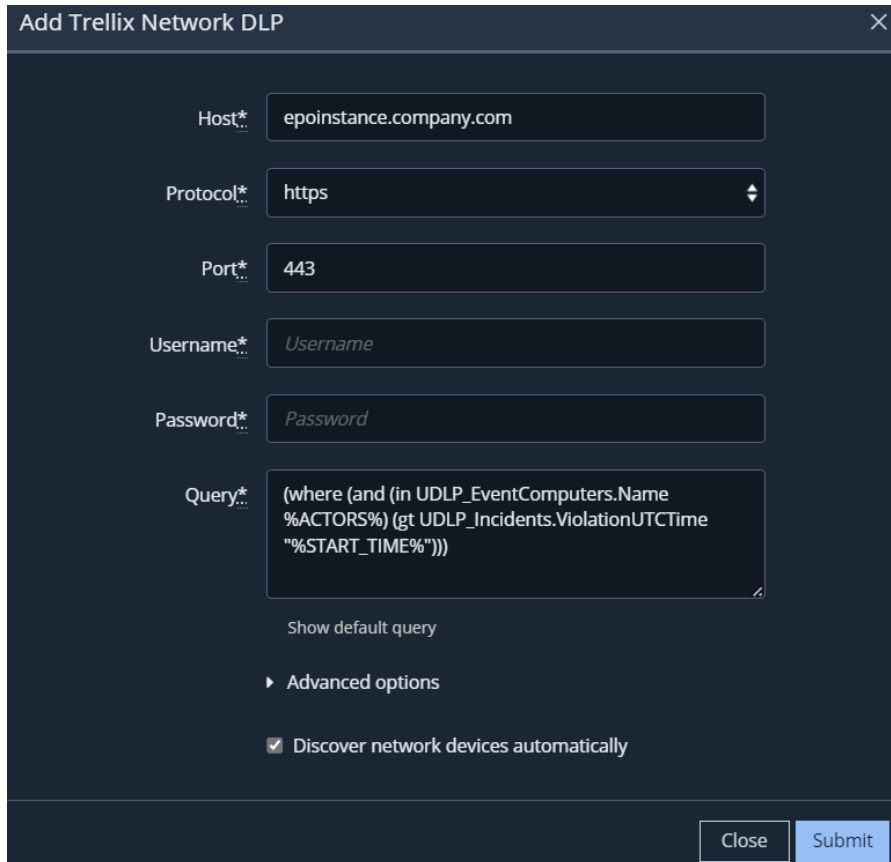
TO ADD THE TRELIX NETWORK DLP INTEGRATION

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



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

3. Enter information for the **Host, Protocol, Port, Username** and **Password** or **API Token**.
4. If necessary, modify the **Query**.
5. Expand **Advanced options** and update the information, if necessary.
6. Click **Submit**.



(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/63ebee4e298e17f0819260b/n/trellix-network-dlp.png>)

Trellix Network DLP Integration

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 \(https://docs.mandiant.com/home/msv-proxy-rules\)](https://docs.mandiant.com/home/msv-proxy-rules).

Verify Connectivity

TO VERIFY CONNECTIVITY TO TRELIX NETWORK DLP

Click **Test** to verify that:

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