Mandiant

TRELLIX NETWORK SECURITY (NX) INTEGRATION WITH SECURITY VALIDATION

This integration collects events generated by Trellix Network Security to test the efficacy and configuration of the security control using Security Validation jobs. In V2, pagination and OS changes are also provided.

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
`/wsapis/v2.0.0/alerts`	Collect alerts from Trellix Network Security
`/wsapis/v2.0.0/events`	Collect events from Trellix Network Security
`/wsapis/v2.0.0/smartvision/alert`	Collect smartvision alerts from Trellix Network Security
`/wsapis/v2.0.0/auth/login`	login to Trellix Network Security
`/wsapis/v2.0.0/auth/logout`	logout from Trellix Network Security

Supported Versions

Trellix Network Security 9.0.2+

Before You Begin

To configure this integration, you need:

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

Configure Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > Trellix Network Security (NX)**.

   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 Security (NX) instance.
7. Enter a **Port** value. The default is **443**.
8. Enter the **Username** and **Password** for the account with permission to use 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: Change the Include **Oschanges** value, depending on whether you want to include or exclude OS changes in the API call.
12. Optional: Modify the **TrellixNetworkSecurityInfoLevelV2**, as needed, to change the filter on alert info level. The default is **Normal**.
13. Optional: Change the alert **Offset**. The default is **0**.
14. Optional: Modify the **Page Size** to change the request for the upstream server. The default is **200**.
15. Optional: Select either or both **Ips Enabled** and **Smartvision Enabled**. See the Trellix documentation for more information.
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: 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. 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.

18. 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 Network Security (NX) integration enables the Validation Platform Director to pull events from many of Trellix's products, including Central Management (CM Series), Network Security (NX Series), and Email Security (EX Series).

This integration is remote capable.

Update Trellix

1. Enable the Trellix API.
   a. In a terminal window, log in to the command-line interface (CLI) on the appliance where you will run the Web Services API.
   b. Enable the CLI configuration mode:

```
hostname > enable
hostname # configure terminal
```

   c. Enable the Web Services API:

```
hostname (config) # wsapi enable
```

   d. Verify that the Web Service API is enabled.
   For example, if you run the `show wsapi` command on the Trellix CM 4400 and the Web Services API is enabled, the Server Enabled status should be **yes**.

```
Hostname (config) # show wsapi
wsapi status:
Server Enabled:yes
Current State:running
Max Alerts:200
Max Minute Threshold:1000
Max Day Threshold:1000000
OS Changes:no
```

2. Create a Web Services API User Account (api_analyst or api_monitor) that has monitor/read access.
    - api_analyst can read and update alerts, read reports and statistics, and submit objects.
    - api_monitor can read alerts and read reports.

    For full details on setting up user accounts, see the appropriate Trellix Administration Guide.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Login for a token	`/wsapis/v2.0.0/auth/login`
Logout	`/wsapis/v2.0.0/auth/logout`
Alerts query	`/wsapis/v2.0.0/alerts?start_time='%Y-%m-%dT%H:%M:%S.%L%:z'`
SmartVision Alerts	`/wsapis/v2.0.0/smartvision/alert`
IPS Events	`/wsapis/v2.0.0/events`

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Identify the Trellix Host and Port information.
2. Have a monitor/read Web Services API User Account.

To add the Trellix Network Security (NX) integration

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

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

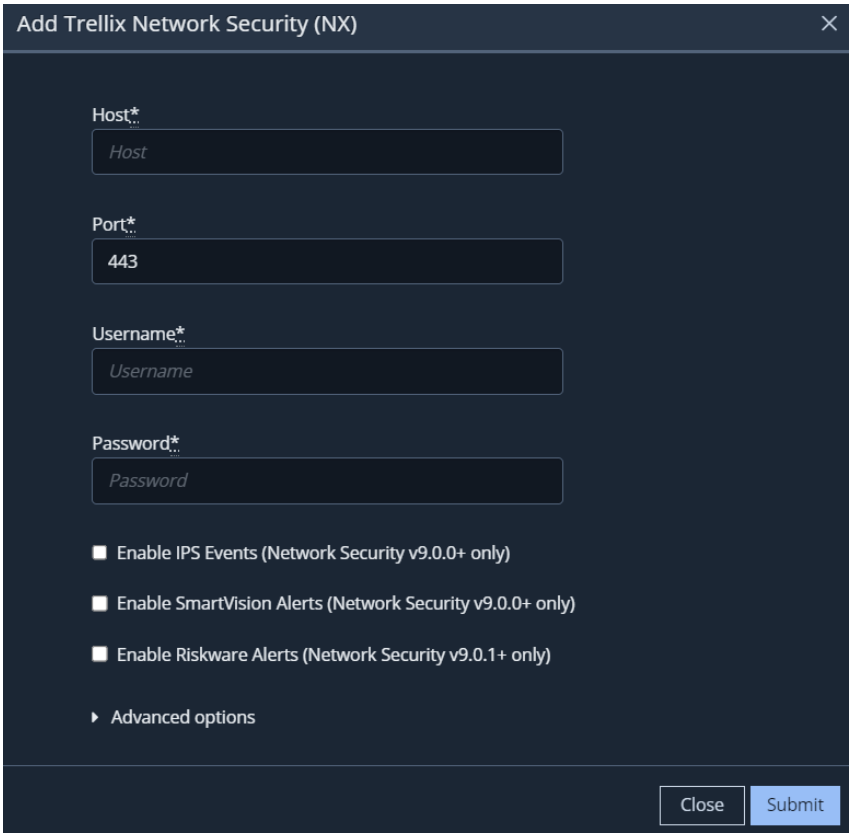
3. Enter information for the **Host**, **Port**, **Username**, and **Password**.
4. (Optional) **Enable IPS Events**, **Enable SmartVision Alerts**, or **Enable Riskware Alerts**, as necessary.

    Events correlated to Network Security IPS Events and SmartVision Alerts include "IPS Event" and "SmartVision Alert" in the event message section, respectively.

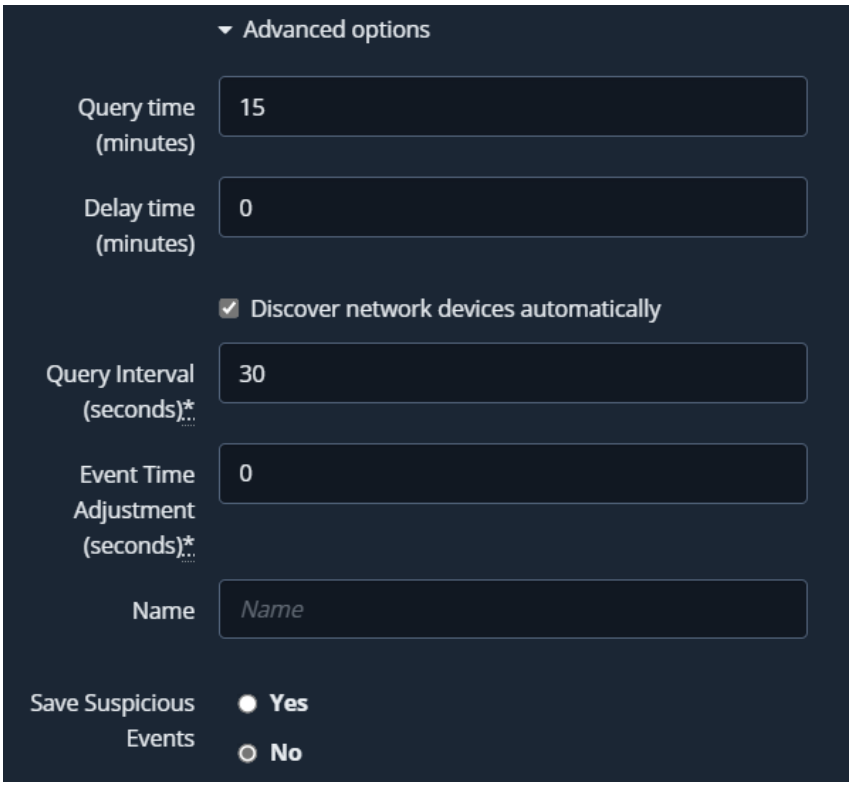
5. Expand **Advanced options** and update the information if necessary.

6. Click **Submit**.

> The query includes information that allows event matching based on any file hashes included in an Action.



Trellix Network Security (NX) Integration



Trellix Network Security (NX) 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

Click **Test** to verify that:

- The Director can communicate with the Trellix 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.