TRELLIX NETWORK SECURITY (NX) 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)**.

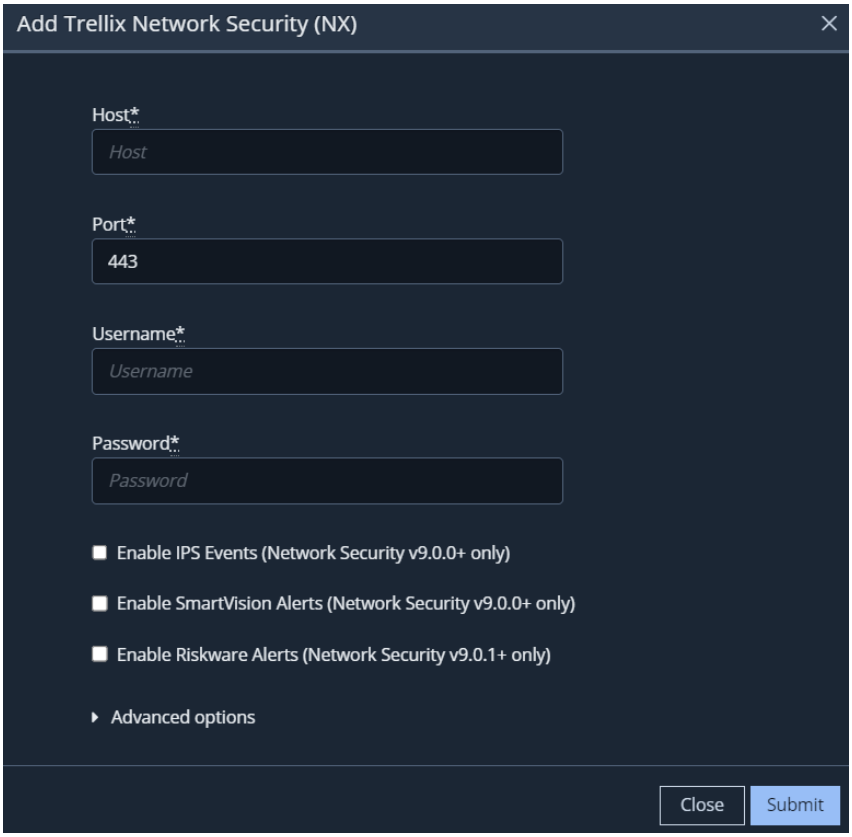
   You can add this as either a Local or Remote Integration.

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

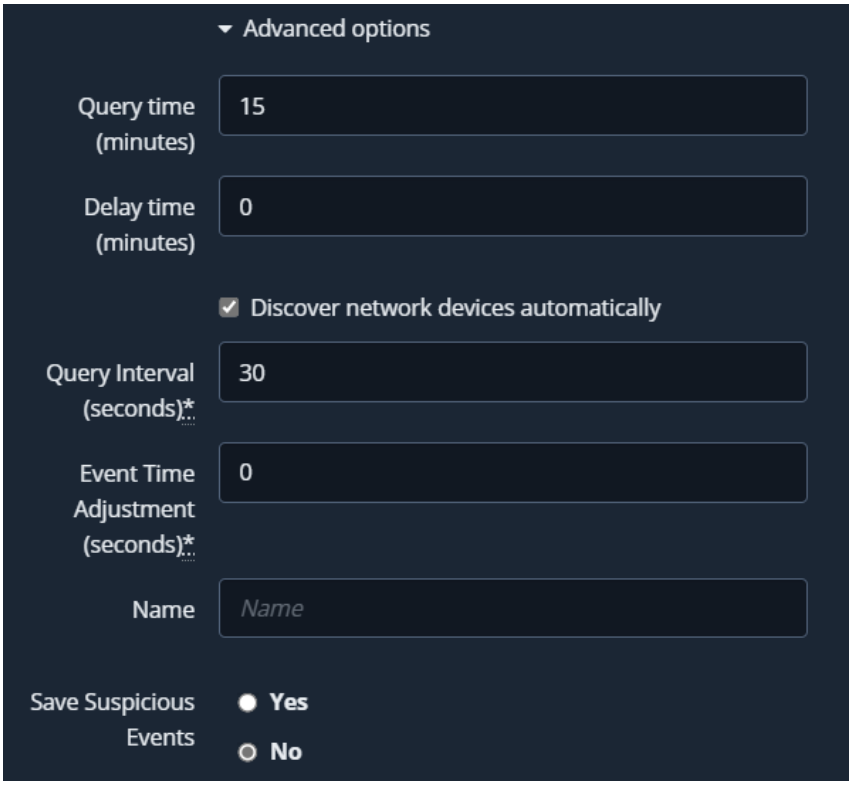
   Events correlated to Network Security IPS Events and SmartVision Alerts include "IPS Event" and "SmartVision Alert" in the event message section, respectively.

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.