Vanguard
Network Cyber Management
Vanguard Plugin installation Guide

Document Version 1.0

December 2019

Important Notice

Table of Contents

1. Introduction

This manual describes how to install and perform initial configure of the Vanguard plugin in Milestone XProtect system.

The manual is intended for system administrators and installers of the Vanguard system.

1.1 Document Scope

This manual consists of the following sections:

- Section 1 - Introduction
- Section 2 - Product Overview
- Section 3 - Vanguard Plugin Installation
- Section 4 - Milestone XProtect Plugin Setup
- Section 5 - Vanguard Alerts Notification
- Section 6 - Vanguard Plugin

1.2 Conventions

Bold is used for the names of interface items.

Note:
Provides important information for the user.

Warning:
Provides important warning information for the user.

1.3 Technical Support

For services and support for Nelysis products, contact your regional representative, or Nelysis's Technical Support Center at:

support@nelysis.com

2. Product Overview

Vanguard NCM is a non-intrusive cyber solution. Through its Vanguard System Collectors components, it connects to mirror ports on network switches in security and control systems networks.

Through this method, network switches in the site send a copy of traffic to Vanguard System Collectors, which convert it into metadata (Vanguard System Collectors produce flows that summarizes the information from the traffic it obtained, without the actual content).

This information is transferred to Vanguard NCM (Core) for analysis.

After completing the data analysis and assessing the risk level, the system sends control commands through Vanguard NGS to site network switches for management and prevention.

2.1 Main System Features

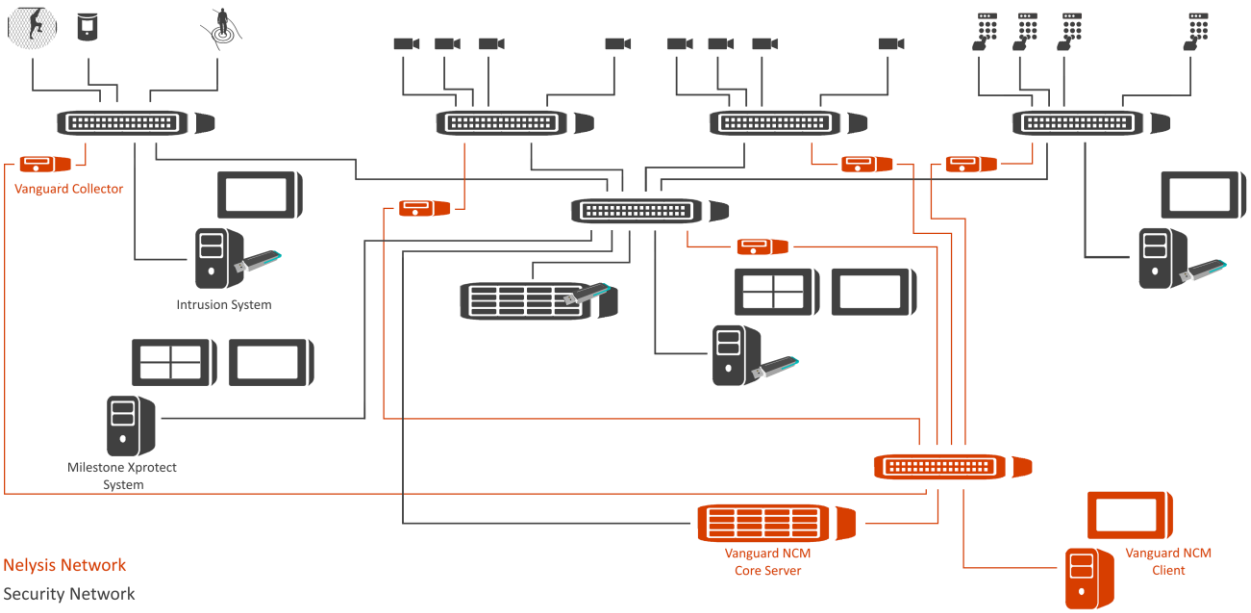
- Constant scrutiny for behavior pattern deviations.
- Element profiles
- Alerts monitoring
- Centralized dashboard
- Traffic recording & historical analysis
- Rule customization
- Real-time reaction
- Reduced system down-time
- Forensic search capabilities
- Monitoring of unauthorized USB memory cards insertion

2.2 Vanguard Components

Vanguard consists of the following components, as shown in the figure below:

- **Vanguard NCM Core** - a server that runs the Vanguard NCM and performing traffic analysis with historical and forensic storage.
- **Vanguard NCM Cyber Management** - NCM's Client Utility that provides a system configuration interface with a day-to-day tools for investigations and analysis.
- **Vanguard NGS** - the Vanguard NGS (Network Gateway Server) provides the system with the ability to control and manage the monitored network switches for immediate prevention purposes, as well as the ability to support Vanguard Protector & Vanguard Monitoring modules.
- **Vanguard Collectors** - collectors are units installed in the monitored networks that collect the network traffic from network switches and send metadata of the information to Vanguard NCM Core for analysis.

Vanguard System Architecture:

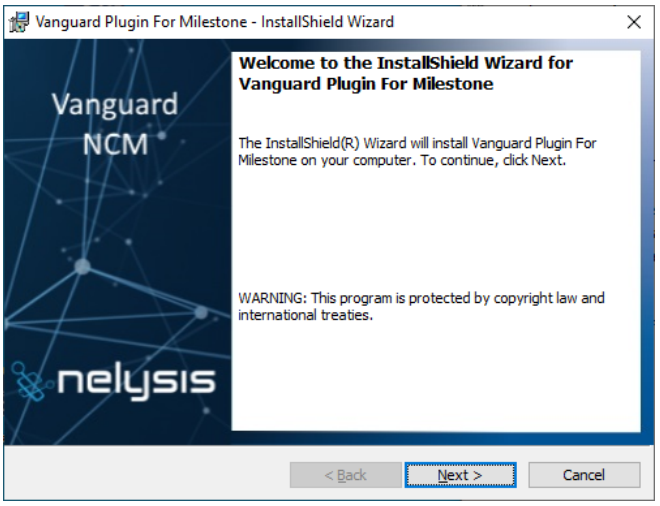


3. Vanguard Plugin Installation

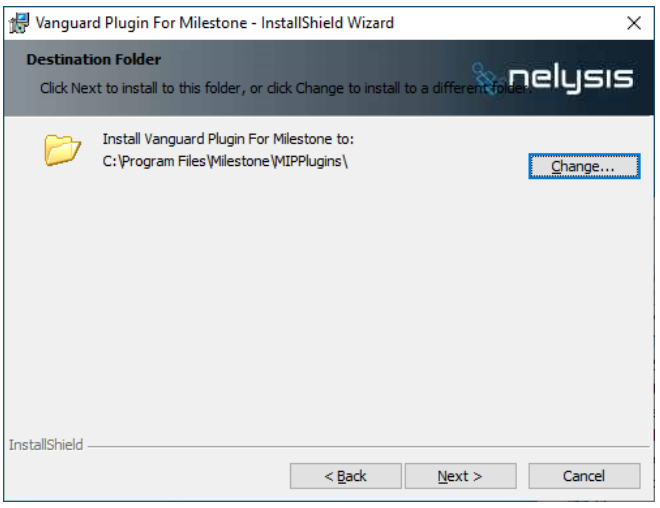
Note:
Vanguard Plugin shall be installed on any computer running Milestone XProtect Management server & Milestone XProtect Smart Client.

To install Vanguard Plugin:

1. **Logon** to the computer, where the Milestone XProtect server is installed, as administrator account.
2. **Stop** Milestone XProtect Event Server service.
3. **Copy** the installation file to the computer.
4. **Double-click** on the Installtion file to start installation.
5. Click **Install** to start installation process.

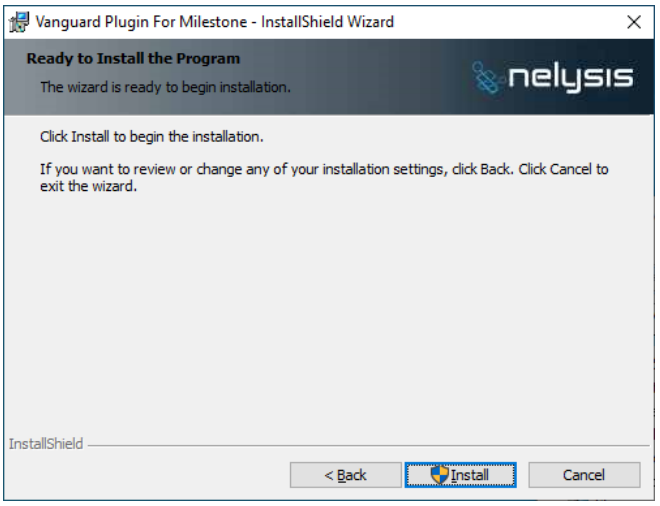


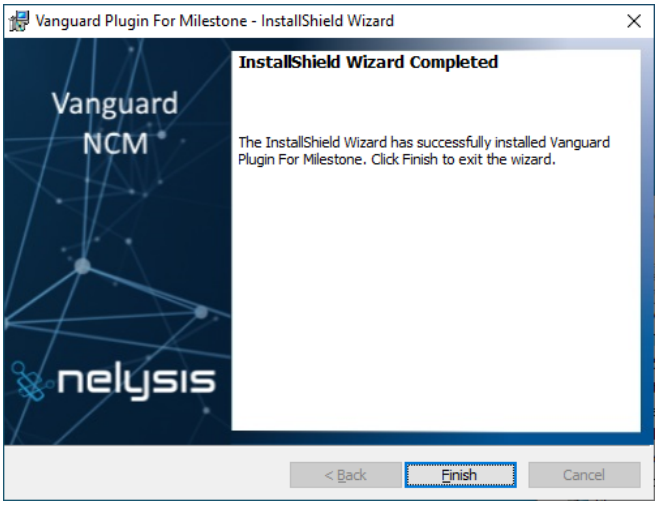
6. Read the license agreement, accept it and click **Next**.
7. **Confirm** installation path and click **Next**.



Note:
Make sure to select Milestone XProtect MIPPlugins folder per XProtect working Path. Default path C:\Program Files\Milestone\MIPPlugins\Nelysis\Vanguard Plugin\.

Click **Install** to start the installation process.

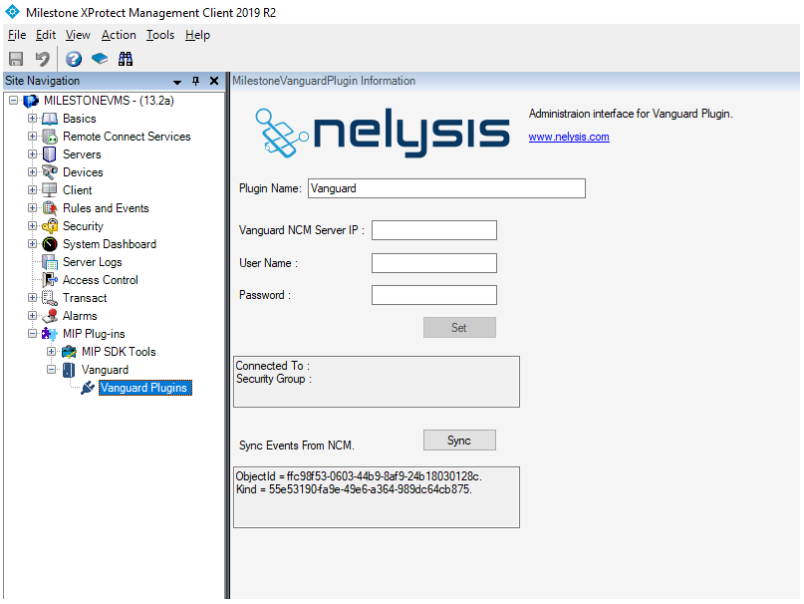




4. Milestone XProtect Plugin Setup

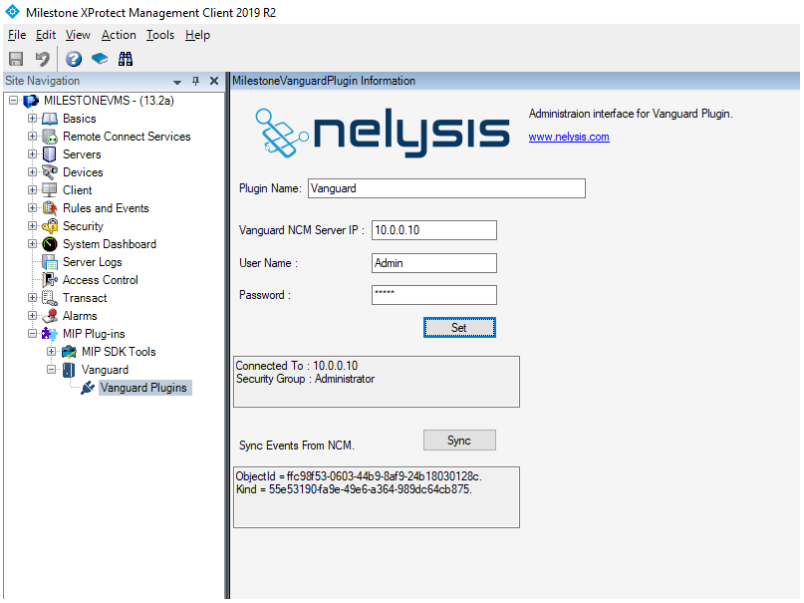
To Configure Vanguard NCM Core:

1. **Logon** to the computer, where the Milestone XProtect server is installed, as administrator account.
2. **Login** to XProtect Management Client.
3. Use Site Navigation tree menu and navigate to **Vanguard Plugin** menu.



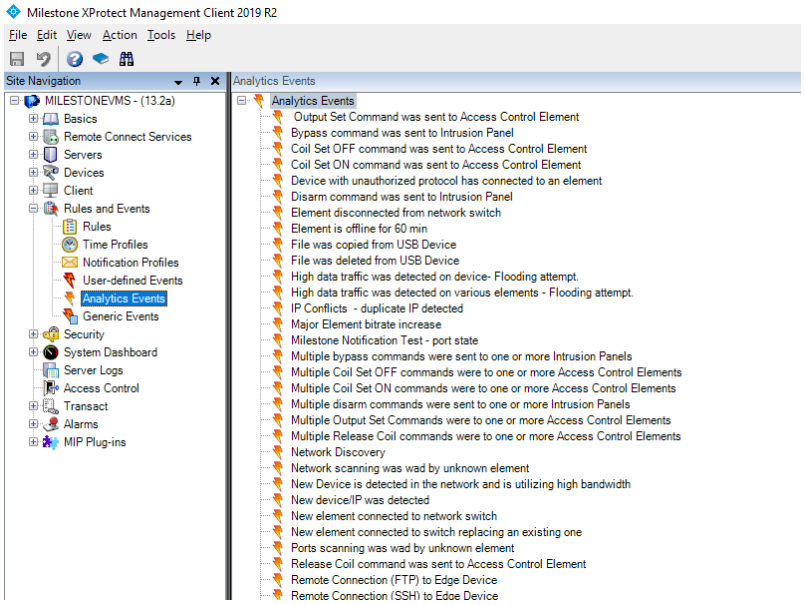
4. **Type** Vanguard NCM Core Server IP, specified a valid user credentials and then click **Set**.

   The connection details appear in Connection Info area.



Note:
For more information regarding Vanguard Alerts please refer to *Vanguard Network Cyber Management Admin Guide*.

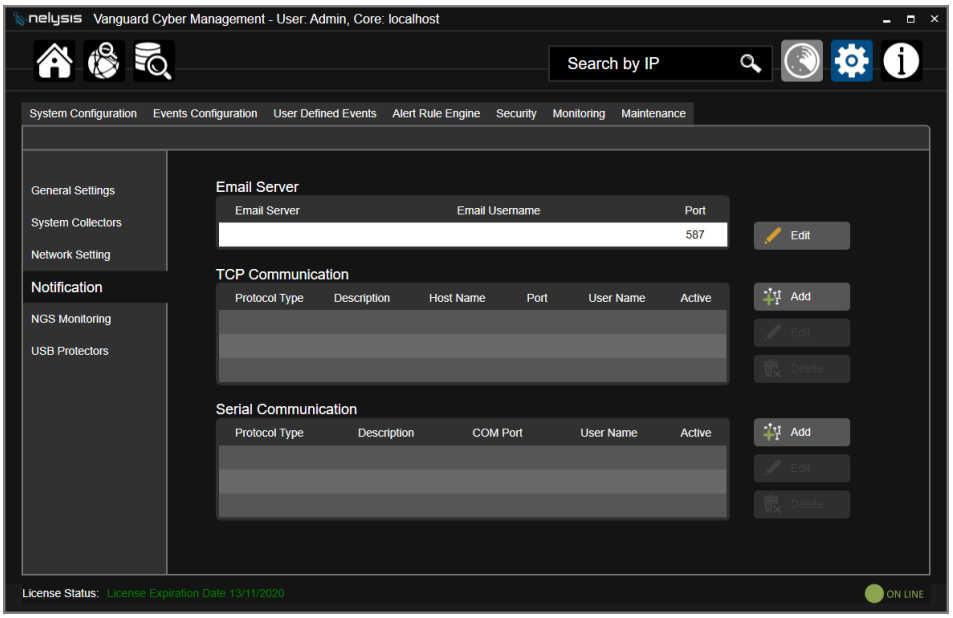
5. Click **Sync** to import all Vanguard Alerts as Analytics Events.



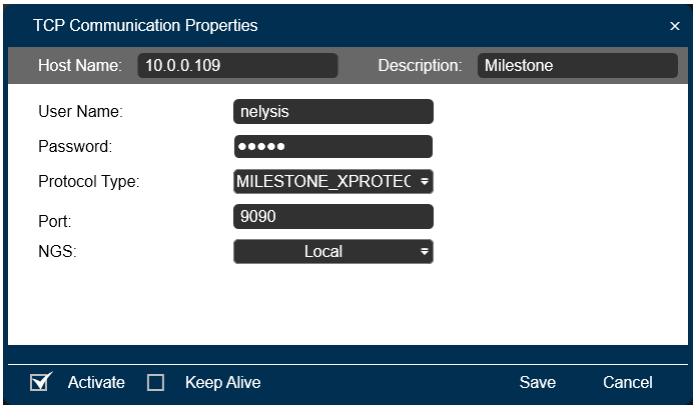
5. Vanguard Alerts Notification

To Set Notification Method:

1. **Logon** to the Vanguard NCM Client application.
2. From **Configuration menu** select **System Configuration** and then select **Notification**.



3. In **TCP Communication**, click **Add** and then add the following parameters:



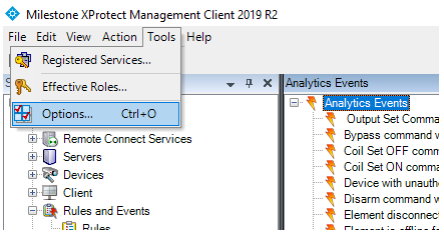
- **Host Name** – Milestone XProtect Server IP.
- **User Name & password** – credential to communicate with Milestone XProtect Server (if needed).
- **Protocol Type** – select Milestone_XProtect.
- **Port** – Analytics Events port
- **NGS** – Vanguard NGS server that communicate with Milestone XProtect Server.

Note:
For more information regarding Vanguard Notification and Vanguard NGS, please refer to *Vanguard Network Cyber Management Admin Guide*.

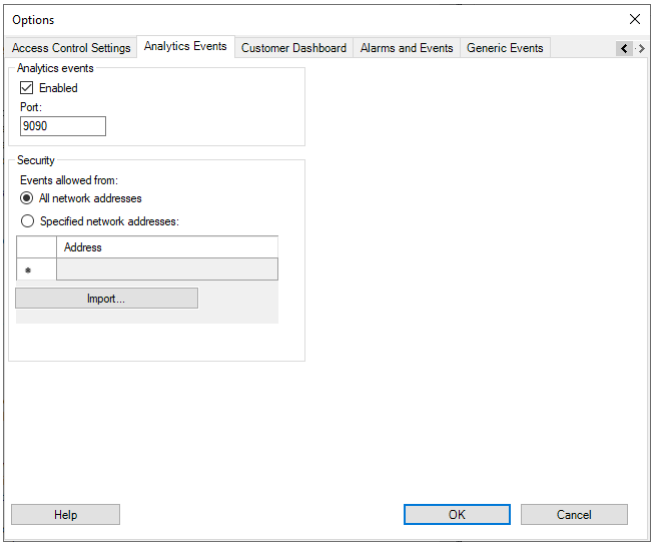
To Verify Analytics Events port:

1. **Login** to XProtect Management Client.
2. On XProtect Management Client menu, select **Tools** and then select **Options**.

   Option menu is displayed.



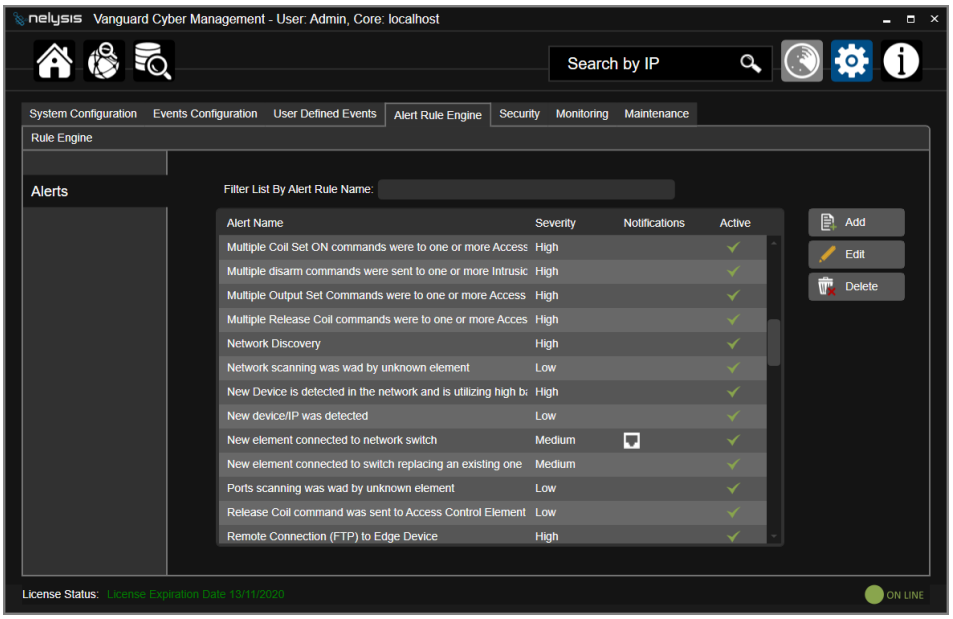
3. Use menu navigation pickers to select **Analytics Events** Menu.
4. Verify Analytics Events is enabled and the TCP port in use.

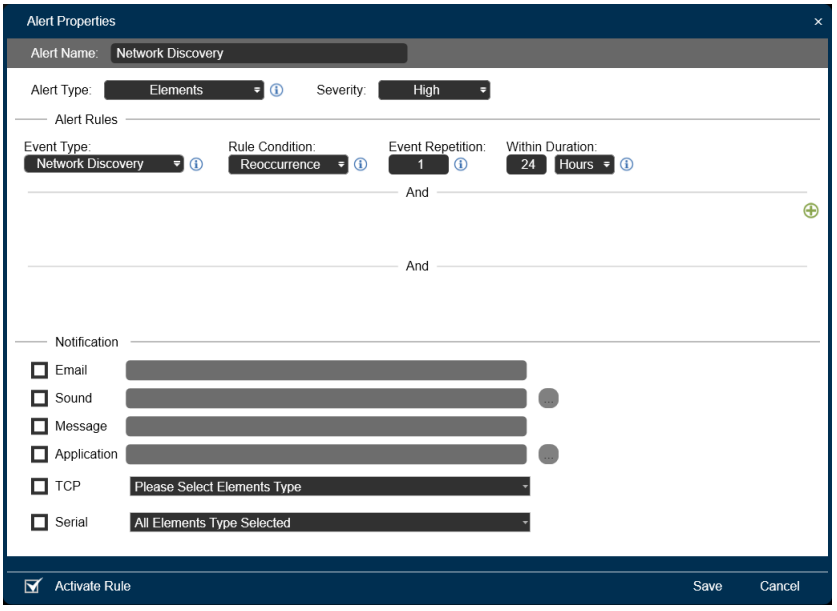


To Set Alerts Notification:

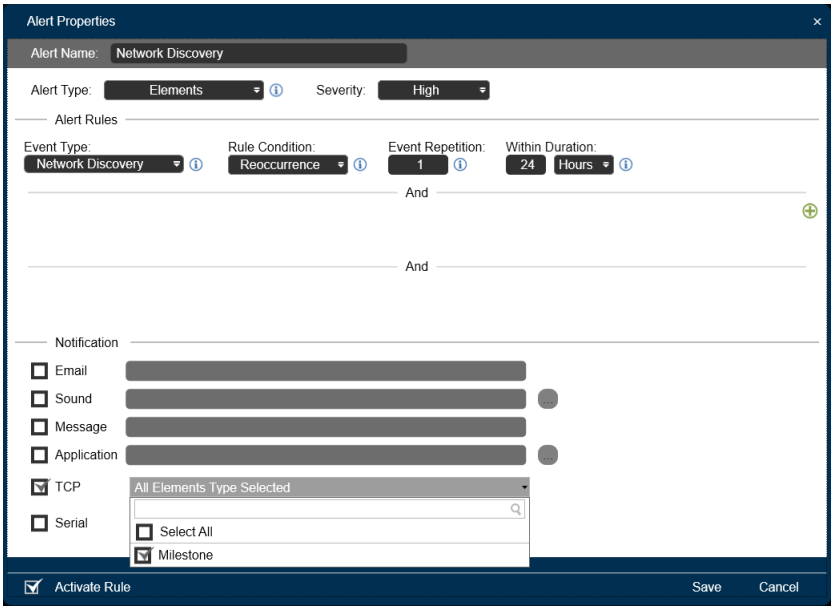
The administrator of the Vanguard system can control the Alerts that will be sent to the Milestone XProtect server as Analytics Events.

5. **Logon** to the Vanguard NCM Client application.
6. From **Configuration** menu select **Alert Rule Engine**.
7. **Select** & **Edit** the Alert to be sent as Analytics Event.





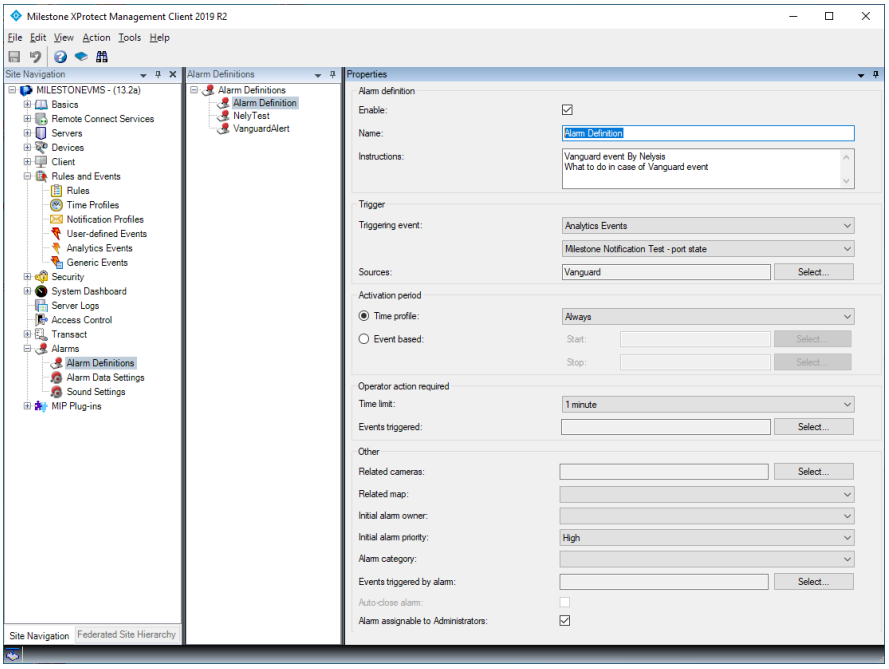
8. In **Notification** Area Select **TCP** and then select the **Notification Method** that have been configured in the previous step.



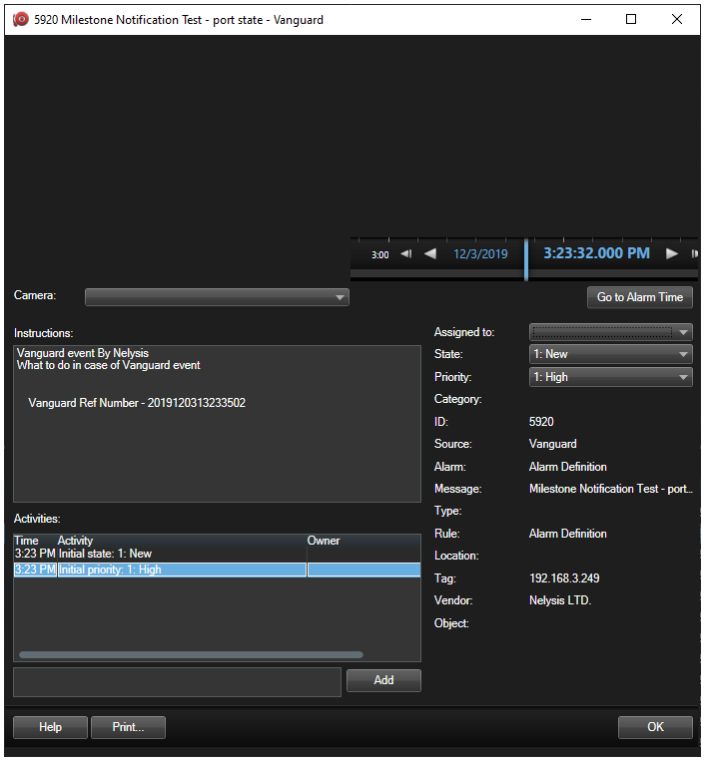
Note:
For more information regarding Vanguard Alerts Rules, please refer to *Vanguard Network Cyber Management Admin Guide*.

Alarm Manager:

Use Milestone XProtect Manager to set Alarm Definitions for the Vanguard events.



Per the Alarm rules, configured in the Milestone XProtect Alarm Definitions, Vanguard Alerts are displayed in the Alarm Manager, containing all relevant information for monitoring.



6. Vanguard Plugin

After you setup your Vanguard system and added Vanguard Plugin to Milestone XProtect, you can start monitoring your network for any unusual activity, as detected by the Vanguard system.

The Vanguard plugin displays high-level information relating to alerts, events, elements and elements conversations.

Login to Milestone XProtect Smart Client then select Vanguard Plugin

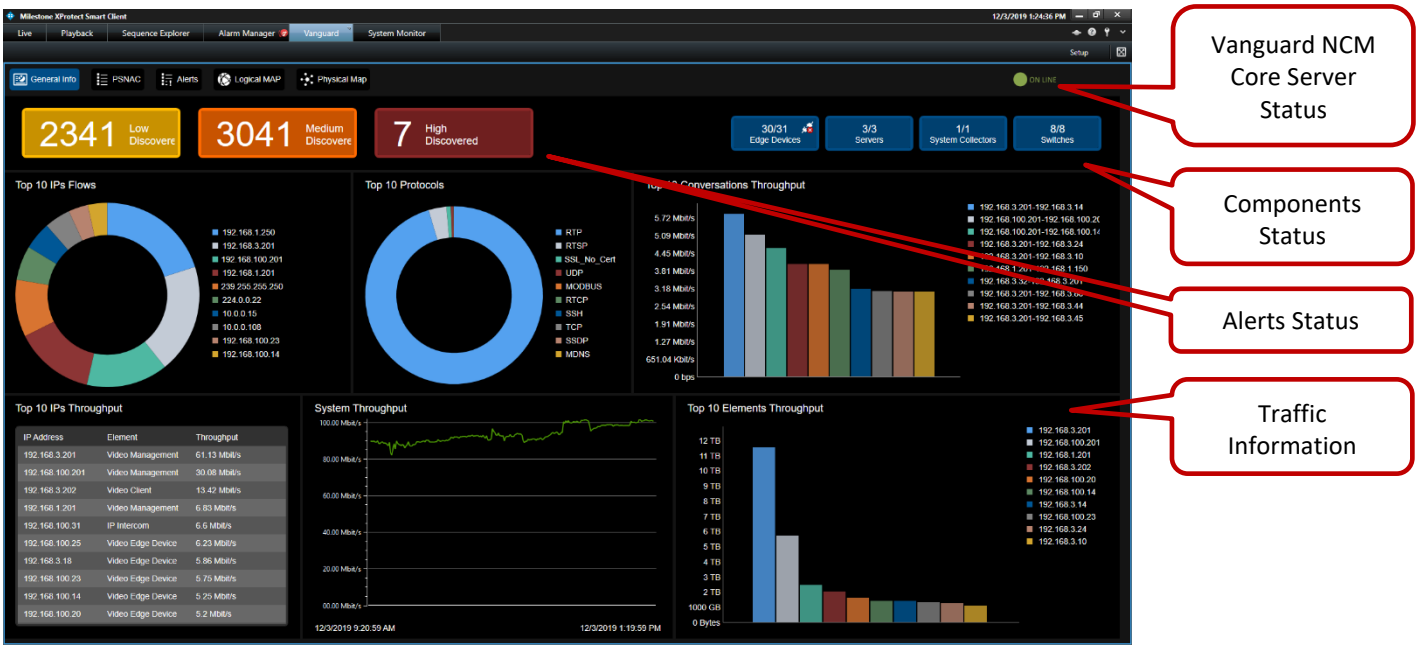
Note:
For more information regarding Vanguard System please refer to *Vanguard Network Cyber Management Admin Guide*.

Vanguard plugin provides several monitoring screens:

- **General Info -** displays general information for the "Top 10" items of interest on the monitored network.
- **Alerts -** displays information on alerts that occurred in the system.
- **PSNAC -** displays information on network switches on the monitored network.
- **Network Map -** displays current logical connections/conversations between elements.
- **Physical Map -** displays current physical connections between the various elements and network switches configured in the system.

6.1 Viewing Vanguard General Info

The **General Info** displays status of various components in the Vanguard system, and general information for the "Top 10" items of interest on the monitored network.



The main sections of this screen include:

- a **Header** with buttons for accessing other functionality in the Vanguard plugin.
- **Alerts Status Buttons** that display alert status and enable quick access to alerts by their severity.
- **Critical Components Status** that display the critical component status.
- **Traffic Information** display general information various “top 10” traffic collections.

6.1.1 Alerts Status Buttons

Each Alerts Status button displays the status according to alarm severity, and provides quick access to alert panes that are pre-filtered according to the selected severity.

The levels of severity are:

- **Low Discovered**
- **Medium Discovered**
- **High Discovered**

6.1.2 Critical Components Status

Each Critical Components Status displays the status according to the components type as monitored by Vanguard as follows:

- **Edge Devices** - displays the status for Edge Device elements.
- **Servers** - displays the status for Server elements.
- **System Collectors** - displays the status for the Vanguard **System Collectors**.
- **Switches** - displays the status of the monitored switches.

6.1.3 Traffic Information

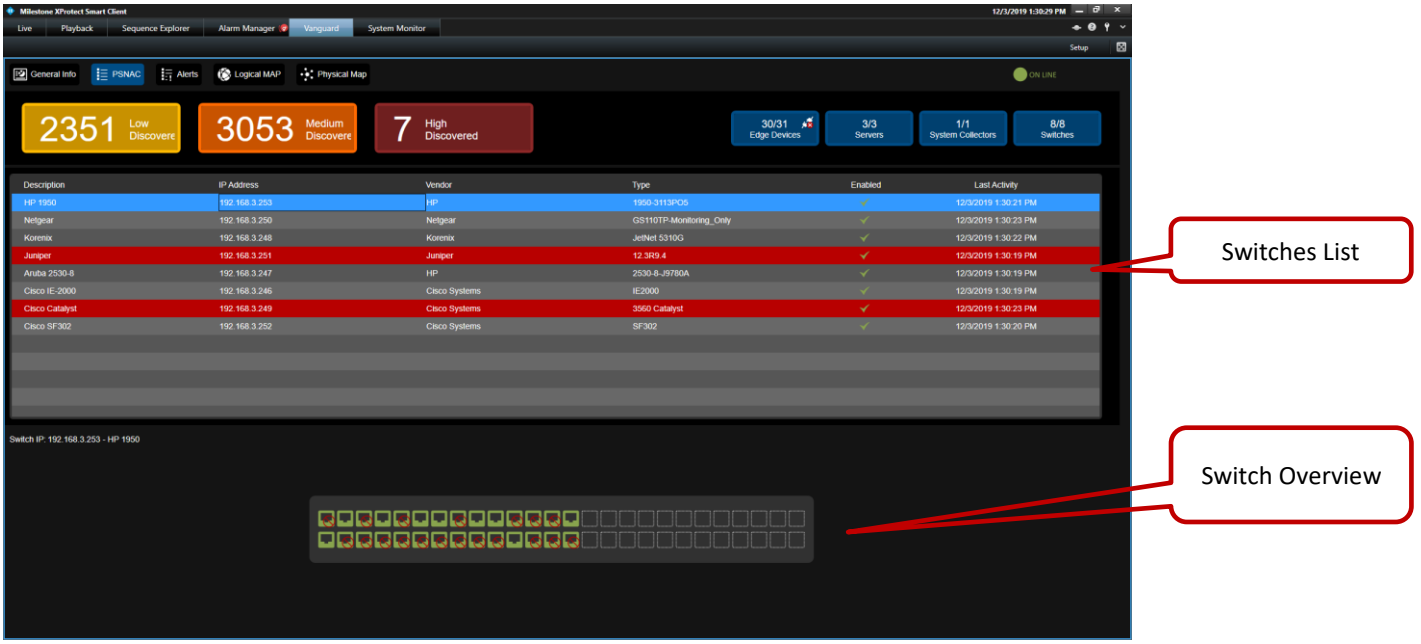
The Traffic Information section provides a visual overview of the "Top 10" items of interest according to the following categories:

- **Top 10 IP Flows**
- **Top 10 Protocols**
- **Top 10 Conversations Throughput**
- **Top 10 IPs Throughput**
- **System Throughput**
- **Top 10 Element Throughput**

You can view additional information by hovering on the graphs.

6.2 PSNAC

The **PSNAC** menu enables you to view detailed information about the network switches on the monitored network.

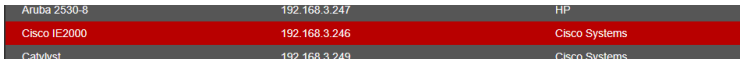


The main sections of this screen include:

- **Switches List** – a list of the monitored.
- **Switch Overview & Ports Status** - Each Port Status displays the current status, and provides quick admin control on the selected port.

To view system alerts:

1. In the header, click **PSNAC Dashboard**.
2. Switches with violations are marked red.



3. Select switch you want to view, selected switch is marked blue, and switch port status appears in switch overview.

Switch preview:

You can view additional information by hovering on the switch ports.

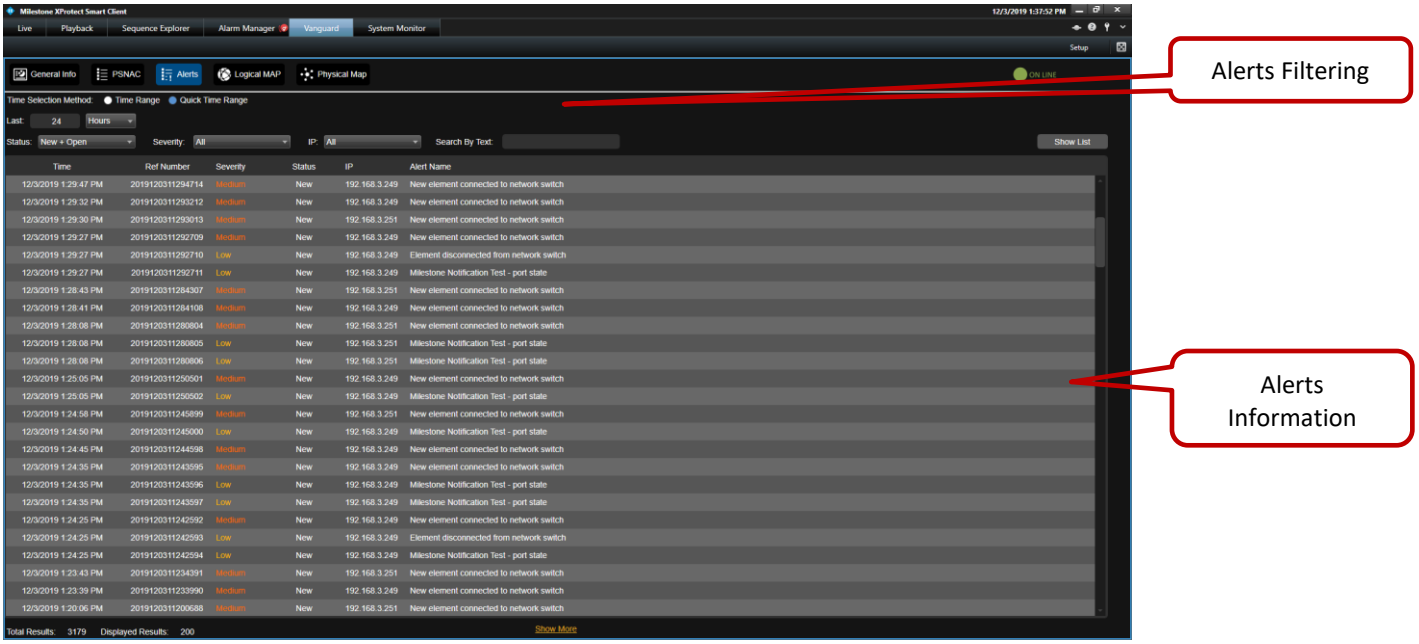
- Port link down.
- Port link down.
- Alerted port.
- Port is shutdown.

To perform additional actions on individual port:

1. Right-click the required port and click the required action.

6.3 Viewing Vanguard Alerts

The **Alerts** menu enables you to view detailed information about system alerts and filter the information as required.

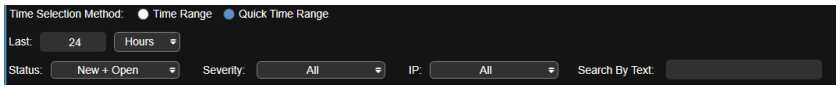


The main sections of this screen include:

- **Alerts Filtering** Use the filters to narrow down the list as required.
- **Alerts Information** that display the critical component status.

To view system alerts:

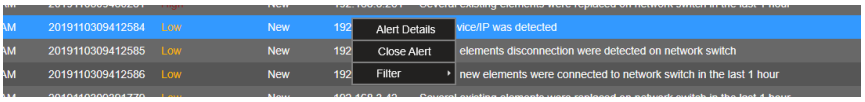
1. In the header, click **Alerts**.
2. Use the filters to narrow down the list as required.



3. Click **Show List**.

To perform additional actions on individual alerts:

1. Right-click the required alert and click the required action.



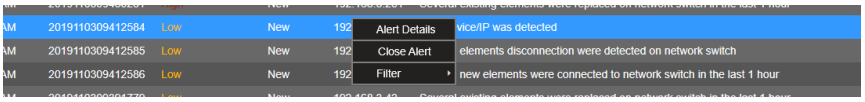
The main options of this menu:

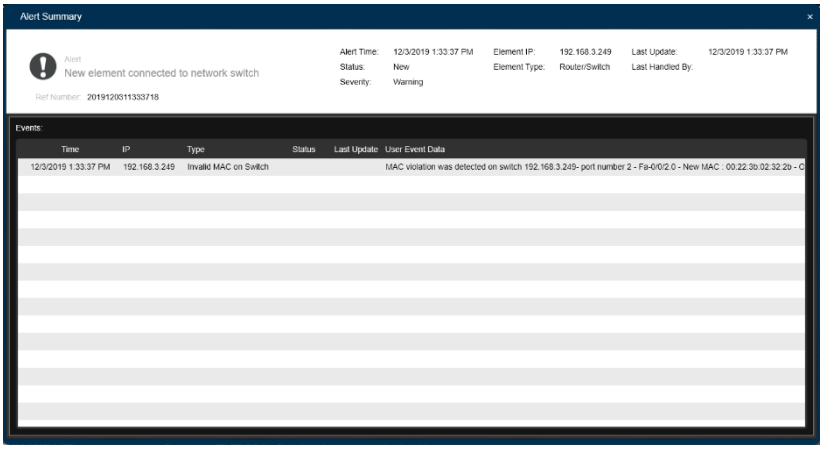
- **Alert Details** provide information about the events triggered the selected alert.
- **Close Alert** close current alert.
- **Filter** quick filtering functions

To view Alert details:

1. **Right-click** the required alert and click **Alert Details**.

   Alert Summary is opened, displaying list of events triggered the alert.

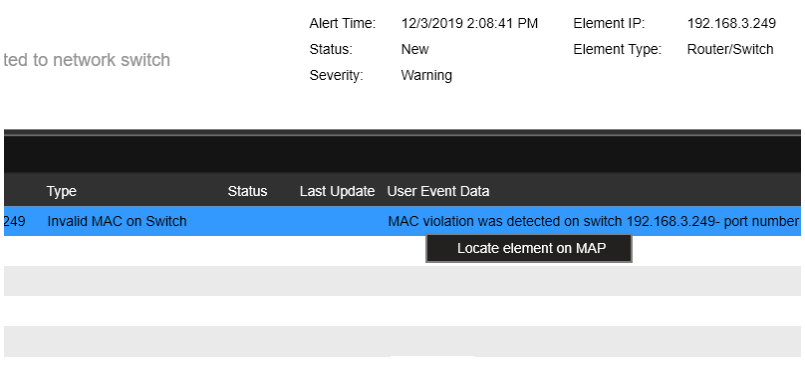




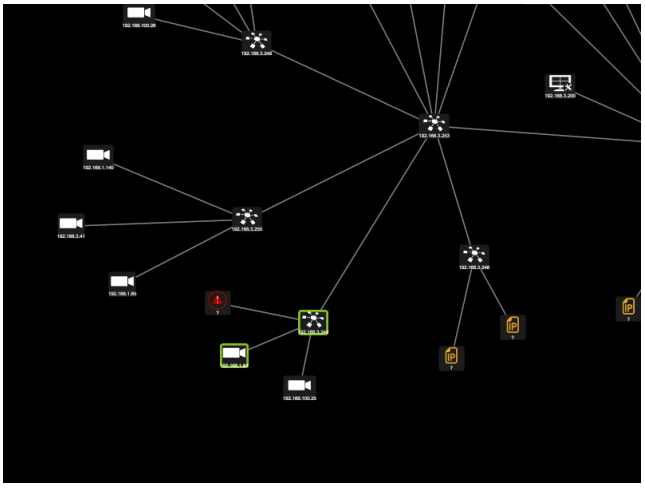
To locate a Physical connection:

The Vanguard system enables the user to identify the physical connection of an element that has triggered an Alert.

1. From **Alert Summary, Right-click** the required Event and click **Locate Element on Map**.

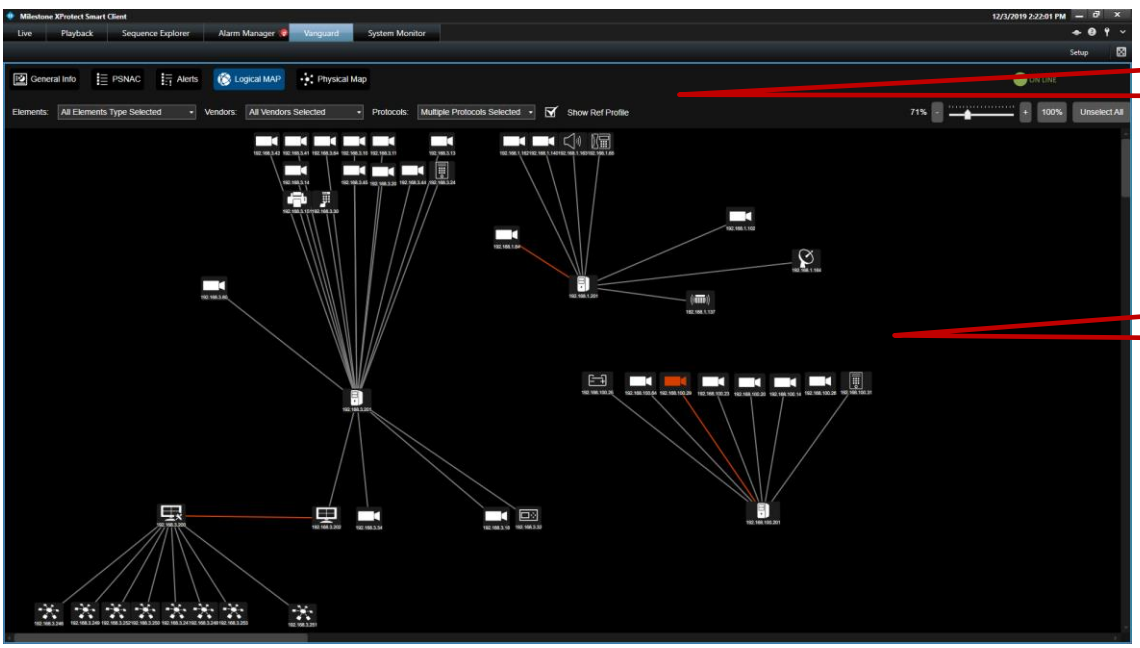


The **Physical Map** is displayed, and the relevant element is marked marking with a green border.



6.4 Logical MAP

The **Logical MAP** menu enables you a visualization of the current logical connections/conversations between elements detected by the Vanguard System.

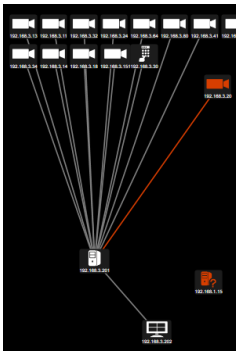


The main sections of this screen include:

- **Components Filtering** Use the filters to narrow down the list as required.
- **MAP Overview** displays the current elements status and the logical connections/conversations between the different element.

To view Logical Map:

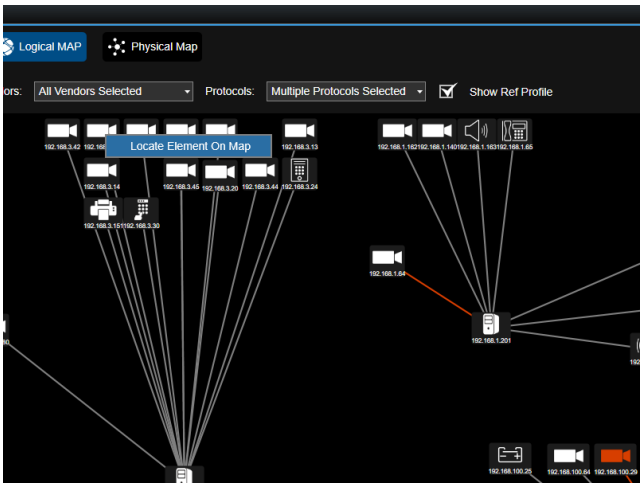
1. In the header, click **Logical MAP**.



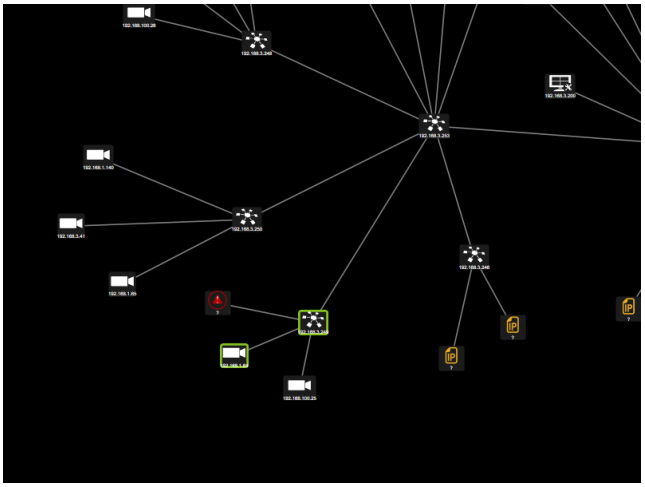
To locate an Element connection:

The Vanguard system enables the user to identify the physical connection of an element.

1. From **Logical Map, Right-click** the required Element and click **Locate Element on Map**.

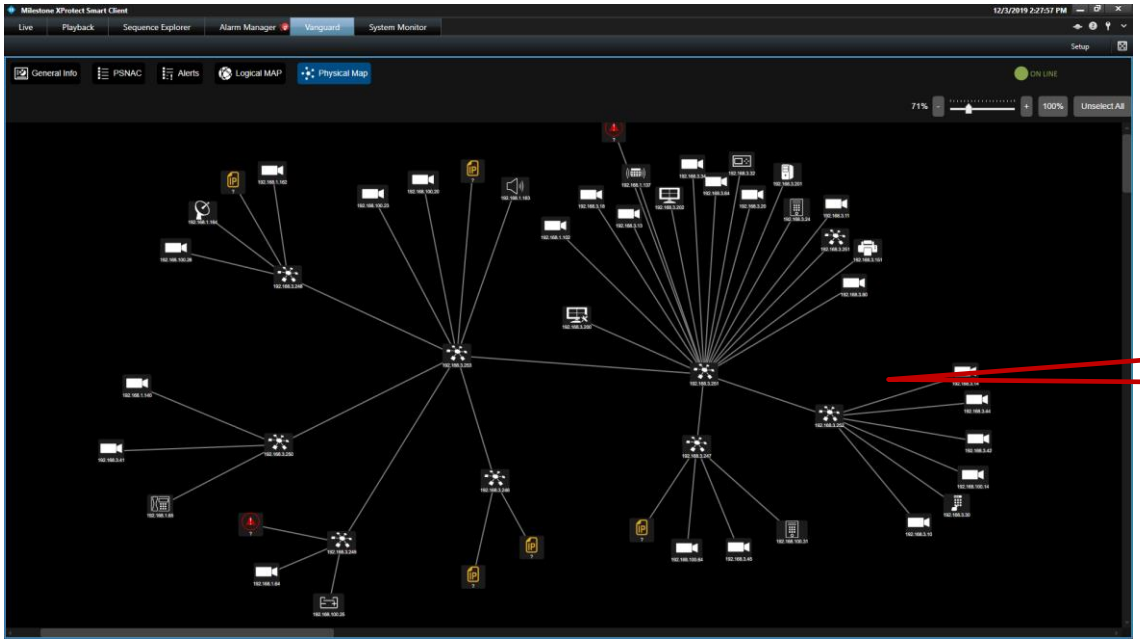


The **Physical Map** is displayed, and the relevant element is marked marking with a green border.



6.5 Physical MAP

The **Physical MAP** menu enables you a visualization of the current physical connections between elements & the network switches monitoring by the Vanguard System.



To view system alerts:

1. In the header, click **Physical MAP**.
2. **MAP Overview** displays the current status and the physical connections between elements and switches.