



Vanguard Network Cyber Management Vanguard Plugin installation Guide

Document Version 1.0 December 2019

Important Notice

All information included in this document, such as text, graphics, photos, logos and images, is the exclusive property of Nelysis and protected by United States and international copyright laws. Permission is granted to view and photocopy (or print) materials from this document for personal, non-commercial use only. Any other copying, distribution, retransmission or modification of the information in this document, whether in electronic or hard copy form, without the express prior written permission of Nelysis Ltd., is strictly prohibited. In the event of any permitted copying, redistribution or publication of copyrighted material, no changes in, or deletion of, author attribution, trademark legend or copyright notice shall be made.

© 2019 Nelysis All rights reserved.

Table of Contents

	Table of Contents								
1.	Intro	oduction	1						
	1.1	Document Scope	1						
	1.2	Conventions	1						
	1.3	Technical Support	1						
2.	Proc	luct Overview	5						
	2.1	Main System Features	5						
	2.2	Vanguard Components	5						
3.	Van	guard Plugin Installation	7						
4.	Mile	stone XProtect Plugin Setup	Э						
5.	Van	guard Alerts Notification12	L						
6.	Van	guard Plugin16	õ						
	6.1	Viewing Vanguard General Info17	7						
	6.2	PSNAC	Э						
	6.3	Viewing Vanguard Alerts	L						
	6.4	Logical MAP24	1						
6.5		Physical MAP							

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.





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\.

3

🐙 Vanguard Plugin For Milestone - InstallShield Wizard	Х
Ready to Install the Program The wizard is ready to begin installation.	5
Click Install to begin the installation.	
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.	
InstallShield < Back Install Cancel	
Vanguard NCM He InstallShield Wizard Completed The InstallShield Wizard has successfully installed Vanguard Plugin For Milestone. Click Finish to exit the wizard.	
& nelysis	

< <u>B</u>ack <u>Finish</u> Cancel

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.
- Use Site Navigation tree menu and navigate to Vanguard Plugin menu.



 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*.

 Click Sync to import all Vanguard Alerts as Analytics Events.

Milestone XProtect Management Client	nt 2019 R2
<u>File Edit View Action Tools H</u> elp	
🗏 🦻 🚱 🗢 🛱	
Site Navigation 🚽 🕈 🗙	Analytics Events
MULESTONEVMS - (132a) MulesTONEVMS - (132a) Barics Bernote Connect Services Servers Client Rules and Events Mules and Events Mode Security Generic Events System Dashboard Farsact Arams Alarms MILP Plug-ins	Analytics Events Output Set Command was sent to Access Control Element Bypass command was sent to Intrusion Panel Coil Set OFF command was sent to Access Control Element Coil Set OFF command was sent to Access Control Element Device with unsultorized protocol has connected to an element Disarm command was sent to Access Control Element Device with unsultorized protocol has connected to an element Device with unsultorized protocol has connected to an element Device with unsultorized protocol has connected to an element Device with unsultorized protocol has connected to an element Device with unsultorized protocol has connected to an element Device with unsultorized protocol has connected to an element Element is offline for 60 min File was ocpied from USB Device High data traffic was detected on various elements - Flooding attempt. High data traffic was detected on various elements - Flooding attempt. High data traffic was detected on various elements - Flooding attempt. High data traffic was mands were sent to one or more Intrusion Panels Multiple Coil Set OFF commands were to one or more Access Control Elements Multiple Coil Set OFF commands were to one or more Access Control Elements Multiple Gaisar Commands were sent to one or more Intrusion Panels Multiple Gaisar Col commands were to one or more Access Control Elements Multiple Gaisar Col commands were to one or more Access Control Elements Multiple Gaisar Col commands were to one or more Access Control Elements Multiple Gaisar Col commands were to one or more Access Control Elements Multiple Gaisar Col commands were to one or more Access Control Elements Multiple Massace Col commands were to one or more Intrusion Panels Multiple Gaisar Col commands were to one or more Access Control Elements Multiple Gaisar Col commands were to one or more Access Control Elements Multiple Massace Col commands were to one or more Access Control Elemen

© 2019 Nelysis All rights reserved.

5. Vanguard Alerts Notification

To Set Notification Method:

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

$\mathbf{H} \otimes \mathbf{H}$					Search by IP		Q,		<u>e</u> 1
ystem Configuration Ev	ents Configuration User Defin	ed Events Alert	Rule Engine Se	ecurity M	onitoring Mainten	ance			
General Settings	Email Server								
system Collectors	Email Server		Email Use	rname		Port			
Internal Contine						587	/	Edit	
letwork Setting	TCP Communica	tion							
Notification	Protocol Type	Description	Host Name	Port	User Name	Active	44	Add	
IGS Monitoring								Edit	1
ISB Protectors									
	Serial Communic	ation							
	Protocol Type	Description	COM F	Port	User Name	Active	44	Add	
								Edit	

- 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.
- TCP Communication Properties

 Host Name:

 10.0.109

 Description:

 Milestone

 User Name:

 nelysis

 Password:

 Protocol Type:

 MILESTONE_XPROTEC •

 Port:

 9090

 NGS:

 Local •

 Save

 Cancel
- **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.

Options					×
Access Control Settings	Analytics Events	Customer Dashboard	Alarms and Events	Generic Events	K ->
Analytics events Analytics events Security Security All network addresses All network addresses Import	s Idresses:				
Help			0	К	Cancel

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.
- From
 Configuration
 menu select Alert
 Rule Engine.
- 7. Select & Edit the Alert to be sent as Analytics Event.





5

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

Alert Properties		×
Alert Name: Network Discovery		
Alert Type: Elements = () Severity: High =		
Alert Rules		
Event Type: Rule Condition: Event Repetition: Within Duration:		
Aliu		Ð
And		
Notification		
Sound		
Message		
Application		
TCP All Elements Type Selected		
Serial Rect Att		
Select All Milestone		
	Savo	Cancel
	Save	Cancer



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.

Milestone XProtect Management	Client 2019 R2			-		>
Eile Edit View Action Tools Help						
🗏 🦻 🕑 🗢 🛍						
šite Navigation 👻 👎	× Alarm Definitions -	# Properties				•
MILESTONEVMS - (13.2a)	Alarm Definitions	Alarm definition				
Basics Benote Connect Services	RelyTest	Enable:	Y			
Servers	🕘 VanguardAlert	Name:	Alarm Definition			
🗄 🐺 Devices	1	lasta ati ana	Management Ry Naturia			5
🗉 💷 Client	1	instructions.	What to do in case of Vanguard event		· · · · · ·	
Rules and Events	1				~	v
Time Profiles	1	Trigger				
Notification Profiles	1	Trianation event:	Applytics Events			
👰 User-defined Events	1	inggoing even.	Analysics Events			
Analytics Events	1		Milestone Notification Test - port state		`	4
Generic Events Generic Events	1	Sources:	Vanguard	Sele	ed	
🗉 🕥 System Dashboard	1	Activation period				
Server Logs	1	Time profile:	Alwave .			
R C Transact	1					2
🗄 🌏 Alarms	1	O Event based:	Start:	Sele		5
Alarm Definitions	1		Stop:	Sele		
- 3 Alarm Data Settings	1	Operator action required				
MIP Plug-ins	1	Time limit:	1 minute		`	~
	1	Events triggered:		Sele	he	
	1					
	1	Other				
	1	Related cameras:		Sele	oct	
	1	Related map:			`	~
	1	Initial alarm owner:				~
	1	Initial alarm originty:	Hab			5
	1		1191			
		/warm category:			`	-
	1	Events triggered by alarm:		Sele	ect	
	1	Auto-close alarm:				
	_1	Alarm assignable to Administrators:				
Sta Manipartian Endorsted Site Hierard	vr	· · · · · · · · · · · · · · · · · · ·				

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.

🧔 5920 Milestone Notification Test - port state - Vanguard			– 🗆 X
	3:00 ৰা	4 12/3/2019	3:23:32.000 PM 🕨 🕨
Camera:			Go to Alarm Time
Instructions:		Assigned to:	
Vanguard event By Nelysis		State:	1: New 👻
		Priority:	1: High 🔻
Vanguard Ref Number - 2019120313233502		Category:	
		ID:	5920
		Source:	Vanguard
		Alarm:	Alarm Definition
		Message:	Milestone Notification Test - port
Activities:		Type.	Alarm Definition
Time Activity Owner 3:23 PM Initial state: 1: New		Location:	
3:23 PM Initial priority: 1: High		Tag:	192.168.3.249
		Vendor:	Nelysis LTD.
		Object:	
	Add		
Help Print			ОК

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

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.

1	Aruba 2530-8	192.168.3.247	HP
	Cisco IE2000	192.168.3.246	Cisco Systems
	Catylyet	102 169 2 249	Cieco Svetome

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

6.3 Viewing Vanguard Alerts

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

Milestone XProtect Smart Clin	ient			_			12/3/2019 1:37:52 PM — 🗗 🗙			
Live Playback	Sequence Explorer	Alarm Manager 📢	Vanguar	d System M	nitor		+ 0 Y ~			
							Setup 🔀			
General Info 📃 P	PSNAC	🛞 Logical MAP	• Phys	sical Map			ON LINE	Alerts Filtering		
Time Selection Method. Time Range Aukk Time Range										
Last 24 Hours										
Status: New + Open	- Severity: All		IP: AI		Search By Text:		Show List			
_										
Time	Ref Number	Seventy	Status	IP	Alert Name					
12/3/2019 1:29:47 PM	2019120311294714		New	192.168.3.249	New element connected to network switch					
12/3/2019 1:29:32 PM	2019120311293212		New	192.168.3.249	New element connected to network switch					
12/3/2019 1:29:30 PM				192.168.3.251	New element connected to network switch					
12/3/2019 1:29:27 PM	2019120311292709		New	192.168.3.249	New element connected to network switch					
12/3/2019 1:29:27 PM	2019120311292710		New	192.168.3.249	Element disconnected from network switch					
12/3/2019 1:29:27 PM	2019120311292711		NCW	192.168.3.249	Milestone Notification Test - port state					
12/3/2019 1:28:43 PM	2019120311284307			192.168.3.251	New element connected to network switch					
12/3/2019 1:28:41 PM	2019120311284108		New	192.168.3.249	New element connected to network switch					
12/3/2019 1:28:08 PM	2019120311280804			192.168.3.251	New element connected to network switch					
12/3/2019 1:28:08 PM	2019120311280805		New	192.168.3.251	Milestone Notification test - port state					
12/3/2019 1:28:08 PM	2019120311280806			192.168.3.251	Milestone Notification lest - port state					
12/3/2019 1:25:05 PM	2019120311250501		New	192.168.3.249	New element connected to network switch			Alerts		
12/3/2019 1:25:05 PM	2019120311250502			192.168.3.249	Milestone Notification test - port state					
12/3/2019 1:24:58 PM	2019120311245899		New	192.168.3.251	New element connected to network switch			Information		
12/3/2019 1:24:50 PM				192.168.3.249	Milestone Notification Test - port state					
12/3/2019 1:24:45 PM	2019120311244598		New	192.168.3.249	New element connected to network switch					
12/3/2019 1:24:35 PM	2019120311243595			192.168.3.249	New element connected to network switch					
12/3/2019 1:24:35 PM	2019120311243596		New	192.168.3.249	Milestone Notification Test - port state					
12/3/2019 1:24:35 PM	2019120311243597		New	192.168.3.249	Milestone Notification test - port state					
12/3/2019 1:24:25 PM	2019120311242592		New	192.168.3.249	New element connected to network switch					
12/3/2019 1:24:25 PM			New	192.168.3.249	Element disconnected from network switch					
12/3/2019 1:24:25 PM	2019120311242594		New	192.168.3.249	Milestone Notification Test - port stale					
12/3/2019 1.23:43 PM			New	192.168.3.251	New element connected to network switch					
12/3/2019 1.23:39 PM	2019120311233990		New	192.168.3.249	New element connected to network switch					
12/3/2019 1:20:06 PM	2019120311200688	Medium	New	192.168.3.251	New element connected to network switch		•			
Total Results: 3179 Disp	layed Results: 200				Show More					

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.



Show List

To perform additional actions on individual alerts:

 Right-click the required alert and click the required action.
 NM
 2019 (10009 (2004)
 New
 192
 Alert Details
 Victor Mas detected

 NM
 20191(10309412585
 Low
 New
 192
 Close Alert
 elements disconnection were detected on network switch

 NM
 20191(10309412586
 Low
 New
 192
 Filter
 new elements disconnection were detected to network switch in the last 1 hour

 NM
 20101(0309412586
 Low
 New
 192
 Filter
 new elements were connected to network switch in the last 1 hour

 NM
 20104(0300901770
 Low
 100 4000 201710
 Counter the last 1 hour

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:

 Right-click the required alert and click Alert Details.

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

2013	110003400201	r ngri	non.	152.10	0.0.201 001	crui existing cierra	and more reprint	acca on neuro	in omen in me		
				192	Alert Details	vice/IP was de					
2019	9110309412585		New	192	Close Alert	elements disc	elements disconnection were detected on network switch				
2019	9110309412586		New	192	Filter	new elements	were connec	ted to network	switch in the las	t 1 hour	
2040	440200204770	Low	Nour	400.40	0.0.40 Cou	varal aviating along	noto wara rant	aaad an natur	dcowitab in the	laat d bour	
Ak	ert Summary										
(Alert New eleme Ref Number: 201912	nt connected t	o network switch		Alert Time: 1 Status: N Severity: V	12/3/2019 1:33:37 PM New Varning	Element IP: Element Type:	192.168.3.249 Router/Switch	Last Update: Last Handled By:	12/3/2019 1:33:37 PM	
Ever	nts:										
	Time	IP	Туре	Status	Last Update Use	er Event Data					
	12/3/2019 1:33:37 PM	100 100 0 010	Involted MAC on Coultab		1.14	de a de la seconda de la seconda de				1110 0 00 00 00 00 00 00	
	1202010 1.00.0711	192.100.3.249	Invalid MAC on Switch		N/A	C violation was detected	on switch 192.168	s.3.249- port numbe	r 2 - Fa-0/0/2.0 - New	MAC : 00.22.30.02.32.20 - C	
		192.100.3.249	Invalid MAC on Switch		ine.	C volation was detected	on switch 192.168	s.3.249- port numbe	r 2 - Fa-0/0/2.0 - New	MAC : 00.22.30.02.32.20 - C	
	120201011000011	132.100.3.245	Invalid MAC ON SWICH		108	c volation was detected	on switch 192.168	s.3.249- port numbe	r 2 - Fa-0/0/2.0 - New	MAC : 00.22.30.02.32 20 - C	
		192.196.3.249	Invalid MAC ON SWICH		108	C Wolation was detected	on switch 192.168	s.s.249- port numbe	r 2 - Fa-UrUr2.0 - New	MAC : 00.2230 023220 - 0	
l		132.100.3.249	IIIValo MAC OI SWICH		Titles	C Wolation was detected	on switch 192,168	3.3.249- pon numbe	r 2 - Fal-0r012.0 - New	MAC : 00.22.30 02.32.20 - 0	
		132.100.3.249			109	c volation was detected	on switch 192,168	3.3.249- pon numbe	r 2 - Fa-Uru 2 U - New	MAC - 00-22 30 02 32 20 - 0	
		192.160.3.249			109	c. volation was detected	on switch 192, 166	3.249- por numbe	12 - Fa-UKI2U - New	MAC - 00-22-30 02-32-29 - 0	
		192.160.3,249			104	 woranon was detected 	on switch 152, 168	3.249- por numbe	2 - F8-002 0 - New	MAC , 002230023220-C	
		192.160.3.249			105	cc volation was detected	on switch 152, 168	3.249- por numbe	2 - F8-002 0 - New	IIAC . 002230023226-0	
		192.186.3.2.19			104	ic volation was detected	on switch 152, 168	3.249- por nume	2 - F8-002 0 - New	IIAC . 002230023226-0	
		192.186.3.2.19			104	ic volation was before	on switch 152, 168	3.249- por nume	2 - F8-0020 - New	IIAC . 002230023226-C	

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, Rightclick the required Event and click Locate Element on Map.

ted to	o network switch		Alert Time: Status: Severity:	12/3/2019 2:08:41 PM New Warning	Element IP: Element Type:	192.168.3.249 Router/Switch
	Туре	Status	Last Update	User Event Data		
249	Invalid MAC on Switch			MAC violation was detected	d on switch 192.168	3.3.249- port number
				Locate element	on MAP	
	249	ted to network switch Type 249 Invalid MAC on Switch	ted to network switch Type Status 249 Invalid MAC on Switch	Alert Time: Status: Severity: Type Status Last Update 249 Invalid MAC on Switch	Alert Time: 12/3/2019 2:08:41 PM ted to network switch Status: New Severity: Warning Type Status Last Update User Event Data 249 Invalid MAC on Switch MAC violation was detected	Alert Time: 12/3/2019 2:08:41 PM Element IP: Status: New Element Type: Severity: Warning Type Status Last Update User Event Data 249 Invalid MAC on Switch MAC violation was detected on switch 192.166 Locate element on MAP

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



6

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.

