# Table of Contents

General description2	
Introduction2	
Solution overview2	
Plugin prerequisites2	
Install and Uninstall	
Installation on the Milestone Event Server Computer3	
Installation on the Milestone Smart Client Computers3	
Uninstall on the Milestone Event Server Computer3	
Uninstall on the Milestone Smart Client Computers4	
Setup and Configuration5	
Turn on Syslog Server in the Transition Networks Switch5	
Adding the switches to Milestone6	
Create Alarms7	
Create Rules	
Adding Transition Networks Switches to Maps12	
Smart Client Hot Buttons	
Syslog Messages	

# **General description**

# Introduction

This document describes the integration between Milestone XProtect and Transition Networks Switches. This plugin was developed on the Milestone MIP SDK 2020R1.

The integration supports the following features:

- Milestone will listen for Transition Networks syslog events such as Authentication, Failed-Authentication, Boot, Configuration, Failed-Configuration, Link-Status, Network, and POE events
- Milestone rules may be configured to act on the syslog events form the switches
- Alarms may be defined off of the syslog events
- Control of the network switches through a Milestone Smart Client Workspace Tab
- Hot buttons to take the user to POE Status, POE Reboot, Auto Power Rest, Topology View, Cable Diagnostics, and Detailed Port Statistics

### Solution overview

The plugin will be installed in two locations: on the Milestone Event Server and any computer that needs the hot button links for switch control within the Milestone Smart Client. Both machines use the same installer, but the installer is only required once if the machine is running the event server and smart client features.

Milestone Event Server:

The plugin is installed on the computer running the Milestone Event Server so that the Event Server can listen for syslog events from the Transition Networks Switches. The plugin brings in Syslog events from the switches that can be used as events within the Milestone system. The events may be used to define alarms or create rules to do actions such as logging, alerts, email notifications, or any other action available within Milestone.

All XProtect Smart Clients in the system are capable of seeing alarms without installing the plugin on their computer.

Computers that require hot button links for switch control:

Any computer that needs to control the switches through the hot buttons must be on the same network as the network switches. For security purposes, if a network is segmented then the plugin does not allow users to bypass the network segmentation to access and control the network switches. In some cases, the network control may require that a user remote into the Milestone Server to manage the network switches from the XProtect Smart Client.

Those computers that need to control the network switches through the Milestone Smart Client must have the plugin installed.

### **Plugin prerequisites**

- 1. The system must be running *x* versions of Milestone and meet all of the Milestone perquisites.
- 2. Microsoft Visual C++ 2015 64 bit is required to run the client-side part of the plugin. https://www.microsoft.com/en-us/download/details.aspx?id=48145

# Installation on the Milestone Event Server Computer

 If the Milestone Smart Client will be used for Transition Networks Switch control, then the Visual C++ 2015 prerequisite is required. https://www.microsoft.com/en-us/download/details.aspx?id=48145

2. Launch the TransitionNetworksInstaller.msi

- 3. Click Next
- 4. The Installation folder should be left as default as Milestone typically looks for the plugin in this location. Click Next.
- 5. Click Next to begin the Install.
- 6. Click Close to Exit.
- 7. The Milestone Event Server Service must be restarted to load the plugin. Right click on the tray icon and select "Restart Event Server Service"



# Installation on the Milestone Smart Client Computers

- 1. Visual C++ 2015 64 bit prerequisite is required. https://www.microsoft.com/en-us/download/details.aspx?id=48145
- 2. Launch the TransitionNetworksInstaller.msi
- 3. Click Next
- 4. The Installation folder should be left as default as Milestone typically looks for the plugin in this location. Click Next.
- 5. Click Next to begin the Install.
- 6. Click Close to Exit.

# Uninstall on the Milestone Event Server Computer

1. Stop the Milestone Event Server Service by right clicking on the icon in the tray and selecting "Stop Event Server Service"



2. Close all open Milestone Smart Client or Milestone Management Client windows

- 3. If any users on this computer are logged into Windows and have left open the Milestone Smart Client or the Milestone Management Client, then the computer will require a reboot. This applies only to users that are running these applications on this computer.
- 4. Open "Apps and Features" or "Programs and Features" depending on the version of your Operating System.
- 5. Select "TransitionNetworksInstaller" and click "Uninstall"
- 6. A dialog box may pop up and ask you to confirm uninstall. Click OK.
- 7. If a reboot is required then you will be prompted to reboot the computer. The Event Server Service will automatically be started after reboot.
- 8. If a reboot was not required, then the Event Server Service must be started. Start the Milestone Event Server Service by right clicking on the icon in the tray and selecting "Start Event Server Service"



# Uninstall on the Milestone Smart Client Computers

- 1. Close all open Milestone Smart Client or Milestone Management Client windows
- 2. If any users on this computer are logged into Windows and have left open the Milestone Smart Client or the Milestone Management Client, then the computer will require a reboot. This applies only to users that are running these applications on this computer.
- 3. Open "Apps and Features" or "Programs and Features" depending on the version of your Operating System.
- 4. Select "TransitionNetworksInstaller" and click "Uninstall"
- 5. A dialog box may pop up and ask you to confirm uninstall. Click OK.
- 6. If a reboot is required then you will be prompted to reboot the computer.

# **Setup and Configuration**

# Turn on Syslog Server in the Transition Networks Switch

- 1. Navigate to the section of the switch to enable Syslog. The location may be different depending on your model of switch.
  - a. Switch > Configuration > System > Log

	VORKS.		
SISPM1040-38	84-LRT-C	System Log Configuration	
Switch	DMS		
Configuration	n v	Server Mode	Enabled 🗸
» System	~	Server Address	192.168.99.95
Information		Server Port	514
> IP			514
> NTP			
> Time		Apply Reset	
> Log			

b. Switch > Event Notification > Syslog > Syslog Configuration

6

SM8TAT2SA	System Log Configuration		
Switch DMS			
System	< Mode	on	
<ul> <li>Port Management</li> </ul>	< Server 1	192.168.99.95	
<ul> <li>PoE Management</li> </ul>	< Server 2		
VLAN Management	< Server 2		
Quality of Service	< Server 3		
Spanning Tree	< Server 4		
MAC Address Table	<		
<ul> <li>Multicast</li> </ul>	< Server 5		
DHCP	< Server 6		
Security	<		
Access Control	< Apply Reset		
▶ SNMP	<		
Event Notification	~		
> SNMP Trap			
» Syslog	~		

- 2. Set the mode to "Enabled" or "on" depending on your switch model.
- 3. Enter the Server's IP address
- 4. If Server Port is an option, then choose 514
- 5. Click apply and save

#### Adding the switches to Milestone

- 6. Open the Milestone Management Client
- 7. On the Site Navigation tree on the left, select "Switches" under TransitionNetworks in the MIP Plug-ins section



8. Right Click on Switches in the middle column and select "Add New ..."



9. Enter the name for the network switch. This will be what is shown in the Milestone system when referencing the network switch.



10. Enter the IP Address, Login, and Password, then click the Save Icon on the upper left File Edit View Action Tools Help



11. Once all of the Transition Networks Switches are added, the Event Server must be rebooted to load the changes and listen for events from the added network switches.

# **Create Alarms**

Alarms can be defined based on desired events coming from the Transition Networks Switches. See Milestone's video tutorials for additional information on Milestone alarms.

https://www.youtube.com/playlist?list=PL6KbBiYxpwh17tQf6u57Hk\_bjOfMDLUsa

1. Navigate to the Alarm Definitions section of the site Navigation in the Milestone XProtect Management Client.



- 2. Right click and select "Add New ..."
- 3. Name the Alarm based on the Syslog Event that the alarm is alerting on. This example will show how to create an alarm for a POE event.
- 4. Select the dropdown under Triggering event and choose "Transition Networks Events"

Alarm Definitions 🚽 🕂	Alarm Definition Information	
Alarm Definitions     Authentication     Bot     Configuration     Failed-Authentication     Failed-Configuration     Failed-Configuration     Inik-Status	Alarm definition Enable: Name: Instructions:	PoE Event
PoE Event	Trigger Triggering event:	Transition Networks Events
	Sources:	Access Control Event Categories Analytics Events Device Events External Events Hardware Events
	Activation period Time profile:	Recording Server Events System Events System Monitor Events Transaction events
	O Event based:	Transition Networks Events

5. In the next dropdown, choose POE. Note: An alarm must be defined for each type of event that should produce an alarm.

Alarm Definitions 🚽 🕂	Alarm Definition Information	
Atarm Definitions Authentication Configuration Configuration Failed-Authentication Failed-Configuration Link-Status Network Restork	Alam definition Enable: Name: Instructions:	PoE Event
- 3 FOC EVAIL	Trigger Triggering event: Sources: Activation period Time profile: Event based:	Transition Networks Events Authentication Boot Configuration Failed-Authentication Failed-Authentication Link-Status Network POE

6. Choose the Source of the alarm by clicking the "Select" button. On the Servers tab, select each network switch that this alarm should be raised or Add the "All Switches" folder to alarm on every switch.

Trigger			
Triggering event:	Transition Networks Events		
	PoE		
Sources:			
Activation period		Select Sources	×
Time profile:	Groups Servers	Selected:	
O Event based:	All Switches	C All Switches	
Operator action required			
Time limit:		Add	
Events triggered:		Bamaya	
Other		Remove	
Related cameras:			
Related map:			
Initial alarm owner:			
Initial alarm priority:		OK	Cancel
Alarm category:		UK	

- 7. Add any additional alarm settings required, then click the save icon in the upper left corner.
- 8. These alarms will now appear in the Smart Client's Alarm Manager

😲 Milesto	one XProtect Smart Clie	ent									
Live	Playback	Sequence Explorer	Search (bet	a) Ala	arm Manager	🧑 Trans	sitionNetworks	System Monitor			
< > €	No map has been	selected					۳Ľ (				
Quick Filter	s	Alarms Custom (filter an	nlied) Y C	lear filter			1				
- 	(64)	Eval Time	Priority Level	State Level	State Name	Alarm	Мексоле		Source	Owner	ID
T New	(04)	11:14:25 AM 6/8/2020	1	1	New	POE	SM16TAT2SA POE-F	PD-OFF: Port 5 PoE PD off	MDF Core	Offici	239
	-ut (0)	11:13:52 AM 6/8/2020			New	POE	SM16TAT2SA POE-	PD-ON: Port 5 PoE PD on	MDF Core		238
T On h	51d (U)	11:13:45 AM 6/8/202			New	POE	SM16TAT2SA POE-	PD-OFF: Port 5 PoE PD off	MDF Core		237
Y Close	ed (0)	11:13:38 AM 6/8/202			New	Authentication	SM16TAT2SA LOGI	N: Login passed for user 'admin'	MDF Core		236
		12:10:14 PM 6/1/202			New	POE	SM16TAT2SA POE-	PD-ON: Port 5 PoE PD on	MDF Core		232

#### **Create Rules**

Rules can be defined based on desired events coming from the Transition Networks Switches. See Milestone's video tutorials for additional information on Milestone rules.

https://www.youtube.com/playlist?list=PL6KbBiYxpwh30ickMGicvvJqDKzn3B-GI

To create a rule on an event coming from a Transition Networks Switch, select the desired Transition Networks Event.



The rule can be configured to do anything possible in rule definitions within the Milestone system. The following is an example to create a rule to log the Link-Status event in the rule log.

- 1. Under Rules and Events, click "Rules"
- 2. Right click on the center pane and select "Add Rule..."
- 3. Name the rule and then click on "event"

	Manage Rule	_ 🗆 X
Name:	Link-Status Log Rule	
Description:		
Active:	✓	
	Step 1: Type of rule	
Perform an action	in a time interval	
Edit the rule descript Perform an action on from <u>devices/re</u>	ion (click ar underlined item) event cording server/management server	
Help	Cancel < Back Next >	Finish

4. Select the "Link-Status" event and click OK Name: Link-Status Log Rule

Description:			
Active:	Select an Event	x	
Select the rule Perform an Perform an	Events     Hardware     Hardware     External Events     External Events     Other     Other     Transition Networks     Transition Networks Events	=	
Edit the rule de Perform an acti from <u>devic</u>	Authentication (Transition Networks Events)     Boot (Transition Networks Events)     Configuration (Transition Networks Events)     Failed-Authentication (Transition Networks Events)     Failed-Status (Transition Networks Events)     Network (Transition Networks Events)	~	

5. Click on the "devices/recording server/management server" link at the bottom

Name:	Link-Status Log Rule
Description:	
Active:	✓
	Step 1: Type of rule
Select the rule type y	you want to create
Perform an action	n on <event></event>
Perform an action	n in a time interval
Edit the rule descript	tion (click an underlined item)
Perform an action on	Link-Status (Transition Networks Events)
from devices/re	ecording server/management server

6. Click on "All Switches" and then Add and OK

	Manage Rule		
	Select Sources		x
Sources:		Selected:	
- Sources - IDF - IDF - IDF2 - IDF3 - IDF4		i All Switches	
	Add  Add		

- 7. Click Next
- 8. The conditions page is where you could set a timeframe for the rule. In this case, leave it blank and select next for an always active rule.

Name:	Link-Status Log Rule				
Description:					
Active:					
	Step 2: Conditions				
Select conditions to a	apply				
Outside selected ti	time in <time profile=""></time>				
Within the time pe	ariod <start time=""> to <end time=""></end></start>				
Day of week is <c< td=""><td>Jay&gt;</td></c<>	Jay>				
Edit the rule descript	ion (click an underlined item)				
Perform an action on	Link-Status (Transition Networks Events)				
nom <u>Air Switches</u>					
1					
Help	Cancel < Back Next> Finish				

9. In the "Step 3: Actions" page, you can choose what you want the XProtect System to do on this event. This example is "Make new <log entry>", but you could also do Send notification to <profile> for an email alert or a sender the sender the

any other action allowed in the XProtect System.

	Manage Rule
Name: Description: Active:	Link-Status Log Rule
Select actions Start patrol Pause patro Move date Set device Create boo Play audio Send notifi V Make new Start plug-i	Step 3: Actions           to perform         Ining on cdevices> using <profile> with PTZ <priority>           olling on cdevices&gt;         state            cs&gt; to <preset> position with PTZ <priority>         fault preset on <devices>           fault preset on <devices> with PTZ <priority>         output to <state>           kmark on <devices> <message> on <devices> with <priority>         state            colspan="2"&gt;advices&gt;           adog entry&gt;         n on <devices></devices></priority></devices></message></devices></state></priority></devices></devices></priority></preset></priority></profile>
Edit the rule de Perform an acti from <u>All Sw</u> Create log entry	escription (click an underlined item) on on <u>Link-Status (Transtion Networks Events)</u> I <del>ches</del> /* <mark>Tog entry</mark> /

10. Click on "log entry" link at the bottom and choose how to display the log entry. Click on "Event name", "Triggering time", "Rule name", and then "Recording server name" all with spaces in between.

Name:	Link-Status Log Rule	
Description:		
Active:	$\checkmark$	
Select acti	Select a Log Entry	
Start re	Text to log:	^
Start fe	\$EventName\$ \$TriggerTime\$ \$RuleName\$ \$RecorderName\$	_
Set <sr< td=""><td>Add system information (click links to insert variables in log text)</td><td>-</td></sr<>	Add system information (click links to insert variables in log text)	-
Set <sr< td=""><td>Device name</td><td></td></sr<>	Device name	
Remov	Event name	
Set rec	Triggering time	
Set rec	Kule name Recording server name	
Start pa		~
Edit the rul	OK Const	
Perform an	OK	
Create log er	III IIIV. LIIK-Status Spevicenames Seventnames Smidder nines Smithames Smecolde	Name\$"

- 11. Click finish to end the rule setup
- 12. Go to "Server Logs"



13. Click on "Rule-triggered logs" to see rule log events

		00	0			
Tools Help						
?a)	<b>→</b> # ×	System logs	Audit logs	Rule-triggered logs		
rmation tion		₩ 5/22/20	20 9:06 AM	- 6/22/2020 9:06 AM	~	Source name

# Adding Transition Networks Switches to Maps

1. Click on setup in the Smart Client in Live or Playback to create a map.



2. Drag Map over to a view



3. Select your background image

ct video management software. The triz Organize 👻 New folder	-				1= - 🔟
📕 SDK 2019R2 🔿	Name	Date modified	Туре	Size	
SDK 2019R3 SDK 2020R1	퉬 Icons	7/16/2020 1:20 PM	File folder		
Selenium	El Icons-Switch-Whitebackground.jpg	7/16/2020 12:24 PM	JPEG image	49 KB	
ServerMIDM	Map.jpg	7/22/2020 4:14 PM	JPEG image	22 KB	
Schweimer Mit					
Sopu					
Souther BE					
Stentofon					
Test2016-10					
Test2016-10					
Map Test2016-10					
Test2018-09					
Create new map					
Name: Demails					
lcons					
🗌 Lise existing man					
File na	me: Maning			y Imag	e files (* hmn * aif * ina
► M iis-85	[wap,jpg				emes (tomp, ign, ijpg,
▶ 劉 Map				0	ipen 💌 Cancel
▶ Mitest - Copy					
OK Cancel					

4. Use your mouse scroll button to set the zoom level so the portion of the map that is desired is visible (you can right click and choose zoom in/out via the right click context menu)

- 5. Click on the plugin icon in the Tools menu to get access to the Transition Networks Switches.
- 6. Drag the switch onto the map and adjust the size and position of the image and text.



- 7. Click Setup to Exit Map Configuration
- 8. The map and any nearby cameras can be associated with alarms to see events in the alarm manager. This is done in the Alarm Definitions section of the Management Client.

Security	O Event based:	Start: Select Stop: Select
System Dashboard  Current Tasks  System Monitor  System Monitor Thr  Evidence Lock	Operator action required Time limit: Events triggered:	1 minute V Select
Configuration Repo Server Logs Access Control € , Transact ≡	Other Related cameras:	IDF Camera Select
Transaction source Transaction definiti Alarms	Initial alarm owner: Initial alarm priority:	High V
Alarm Data Setting Sound Settings MIP Plug-ins	Alam category: Events triggered by alam: Auto-close alam:	Select

9. In the Smart Client, the Alarm Manager will display the alarm with the map and associated camera. The red circle around the switch icon means that there is an alarm for that switch.



10. Right click on the switch and select Acknowledge Alarms to clear the alarms associated with this switch. The alarms with that device will change state to "In Progress" and no longer appear in the "New" alarm filter.



11. The Switch's Topology view in DMS Graphical Monitoring could be used as a map background for placing the switches on a map.



# **Smart Client Hot Buttons**

The plugin for the XProtect Smart Client creates a Workspace tab that give the user the ability to control the network switches through their web interface via Hot Buttons. The computer that runs the smart client must be on the same network as the switches with the ability to talk to the desired switch. The user may need to log into the recording server so access the switches.

When the plugin is installed on the computer running the Smart Client, you should see the Transition Networks Tab.

💠 Milesto	ne XProtect Smart	Client				
Live	Playback	Sequence Explorer	Search (beta)	Alarm Manager 🌀	TransitionNetworks	System Monitor
Transition N	letworks Switches:			Please select a switch on	the left.	
Cornwall S IDF1 Uplink Swit Main MDF	ite tch					

Click on a switch to see the hot buttons. You'll see the switch name and IP address in the upper left corner.



Click on the "Quick Links" button to get back to the page with the hot buttons.

Live	Playback	Sequence Explorer	Search (beta)	Alarm Manager 🌀	TransitionN	letworks	System Mon	itor
Transition N	etworks Switches:		Quick Links	TDANCI	IN		NSITION -	1 3 5
Cornwall Si IDF1	te			NETW	/ORKS®	=	°0	2 4 6
Uplink Swit	ch							
Main MDF				SM8TAT:	2SA	Pow	er Over Etł	hernet (
				Switch	DMS			

The hot buttons available are:

PoE Status - This link opens up the Power Over Ethernet Status page on the network switch's web interface.

rer Search (beta)	Alarm Manager	😡 Transition	letworks	Syster	n Monitor						
Quick Links	TRANS	SITION ETWORKS.	=	TRANSITION	•						
	SM8T	Po	Power Over Ethernet Status								
	Switch	DMS	Aut	Auto refreeb Off Defreeb							
	<ul> <li>System</li> </ul>	<	Aut	to-renesh v	Keire	511					
	Port Management     PoE Management			ocal Port	PD Class	Power Allocated	Power Override	Power Used	Current Used		
					-	0 [W]	0	0 [W]	0 [mA]		
	> PoE Config	uration	2		-	0 [W]	0	0 [W]	0 [mA]		
	> PoE Status	3		-	0 [W]	0	0 [W]	0 [mA]			
	> PoE Power	ower Reset	4		-	0 [W]	0	0 [W]	0 [mA]		
	> PoE Schedu	uling Profile	5		-	0 [W]	0	0 [W]	0 [mA]		
	<ul> <li>VLAN Mana</li> </ul>	agement <	6		-	0 [W]	0	0 [W]	0 [mA]		
	▶ Quality of S	Service <	7			0 [W]	0	0 [W]	0 [mA]		
	<ul> <li>Spanning T</li> </ul>	Tree <	1				0	0 [W]			
	▶ MAC Addre	ss Table 🗸	8		-	0 [W]	0	0 [W]	0 [mA]		
	▶ Multicast	<	To	otal		0 [W]		0 [W]	0 [mA]		
	▶ DHCP	<	Ba	alance PoE I	Power Availabl	le	130 [W]				
	<ul> <li>Security</li> </ul>	<									

**PoE Reboot** – Displays the ports that have PoE power enabled. Select a number of ports and then click "Reboot Selected" to reboot those PoE devices on the ports.

Live	Playback	Sequence Explorer	Search (beta)	Alarm Manager 🧑	TransitionNetworks	System Monitor
Transition N	etworks Switches:		Quick Links	Please select from the list	of PoE enabled ports to rebo	ot PoE.
Cornwall Si	te			1		Reboot Selected
IDF1 Uplink Swit	ch			3	1	Clear Selections
Main MDF				4		
				5		Select All
				6		

Search (beta)	Alarm Manager 🎯 🛛 Transit	ionNetworks	System Monitor				
Quick Links	TRANSITION						
	SM8TAT2SA	PoE	Auto Power Rese	et Configuration			
	Switch DMS						
	<ul> <li>System</li> </ul>	< Ping	g Check	off			
	<ul> <li>Port Management</li> </ul>	<	Dent Conformuli				
	PoE Management	Pot	Port Configuration				
	> PoE Configuration	Por	Ping IP Address	Startup Time	Interval Time(sec)	Retry Time	Fa
	> PoE Status						
	> PoE Power Delay	1	0.000	60	20	2	er
	> PoE Auto Power Reset	1	0.0.0.0	00	50	3	tc
	> PoE Scheduling Profile	2	0.000	60	20	2	er
	<ul> <li>VLAN Management</li> </ul>	< 2	0.0.0.0	00		3	tc
	<ul> <li>Quality of Service</li> </ul>	< 2	0.0.0.0	60	30	2	er
	<ul> <li>Spanning Tree</li> </ul>	< 3	0.0.0.0	00	50	3	tc
	<ul> <li>MAC Address Table</li> </ul>	< _	0.0.0.0	60	30	3	er
	<ul> <li>Multicast</li> </ul>	<					tc
	▶ DHCP	< 5	0.0.0.0	60	30	3	er to
	<ul> <li>Security</li> </ul>	<					
	<ul> <li>Access Control</li> </ul>	< 6	0.0.0.0	60	30	3	er tc

#### Auto Power Reset – Opens the PoE Auto Power Reset Configuration page on the switch.

**Topology View** – Opens the Topology View page on the switch's browser interface. This allows you to see a graphical layout of your network.



**Cable Diagnostics** – Opens the cable diagnostics status page that allows you to run cable tests on each network cable.

Search (beta)	Alarm Manager 🎯 🛛 TransitionN	etworks System Monitor		
Quick Links	TRANSITION NETWORKS.	TRANSITION		17 18
	SM16TAT2SA	Cable Diagnostics	S	
	Switch DMS			
	▶ System <	Port 1 V Start		
	▶ Port Management <	Cable Diagnostics S	Status	
	▶ PoE Management <	Port	Link Status	Test Result
	► VLAN Management <	1	-	
	Quality of Service <	2		
	Spanning Tree     <	2		
	MAC Address Table	5		
	▶ Multicast <	4	-	
	► DHCP <	5		
	► Security <	6		
	<ul> <li>Access Control</li> </ul>	7		
	► SNMP <	8		
	► Event Notification <	9		
	<ul> <li>Diagnostics </li> <li>Ping</li> </ul>	10	-	

Detailed Port Statistics – Opens the Port Statistics Overview page. This is useful to determine if any packet errors are occurring.

Search (beta)	Alarm Manager 🎯 🛛 Tra	ansitionNet	works	System Monitor							
Quick Links	TRANSITIO	N.s.		NSITION NETWORKS.	* • •						
	SM16TAT2SA	Ą	Port S	ort Statistics Overview &Home							
	Switch DM	٨S		off							
	System      Port Management		Auto-ret	resn	Refresh						
				Packets		Bytes		Errors		Drops	
	> Port Configuration		Port	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	
	> Port Statistics		1	0	0	0	0	0	0	0	
	> SFP Port Information	1	2	0	0	0	0	0	0	0	
	> Energy Efficient Ethe	rnet	2	0	0	0	0	0	0	0	
	» Link Aggregation	<	3	0	0	0	0	0	0	0	
	» Loop Protection	<	4	0	0	0	0	0	0	0	
	<ul> <li>PoE Management</li> </ul>	<	5	15768301	35611439	19746763506	2968810416	41	0	2	
	<ul> <li>VLAN Management</li> </ul>	<		-	-		-	-			
	<ul> <li>Quality of Service</li> </ul>	<	6	0	0	0	0	0	U	0	
	Snanning Tree	<	7	0	0	0	0	0	0	0	

Group Name	Description	Event Name
Login	Login passed for user username through TELNET from ip_address and authenticated by [no   local   radius   tacacs   redirect] method	Authentication
Login	Login passed for user [username] through [CONSOLE] and authenticated by [no   local   radius   tacacs   redirect] method	Authentication
Login	Login passed for user [username] through [SSH] from [ip_address] and authenticated by [ no   local   radius   tacacs   redirect] method	Authentication
Logout	User [username] logout through [TELNET] from [ip_address]	Authentication
Logout	User [username] logout through [SSH] from [ip_address]	Authentication
Logout	User [username] logout through [WEB] from [ip_address]	Authentication
Password-Change	Password of user [ username] was changed	Authentication
Mgmt-IP-Change	Management IP address was changed\nby user [username] from [address:port (address represent ipv4 or ipv6)]	Authentication
ACCESS-MGMT	Access management filter reject [SSH   TELNET   HTTP   SNMP   HTTPS] access from IP address [ipv4 or ipv6]	Failed- Authentication
Auth-Failed	Bad password attempt for user [username] through [TELNET SSH SNMP] from [ip_address] and authenticated by [no   local   radius   tacacs   redirect] method"	Failed- Authentication
NAS	RADIUS-assigned VLAN: Invalid character found in decimal ASCII string	Failed- Authentication
NAS	NAS (Port [ uport ]): RADIUS timeout while authenticating user	Failed- Authentication
Port-Security	Port Security Limit Control (Port [1~port_num], MAC=[mac_address]): Limit exceeded.	Failed- Authentication
Cold-Start	Switch just made a cold boot	Boot
Warm-Start	Switch just made a warm boot	Boot
Config-Info	User [username] saved running config as startup config	Configuration
Config-Info	User [username] restored default configuration	Configuration
Config-Info	User [username] restored backup configuration	Configuration
Import-Export	User [username] succeed to download configuration	Configuration
Import-Export	User [username] succeed to download configuration	Configuration
Import-Export	User [username] succeed to upload configuration	Configuration
Import-Export	User [username] failed to download configuration	Failed- Configuration
Firmware-Upgrade	Firmware Upgrade Failed	Failed- Configuration
Link-Status	Link [up   down] on port [1 ~ port_num]	Link-Status
Loop-Protect	Interface GigabitEthernet 1/ <port num=""> is shutting down because of loop detected.</port>	Network
Loop-Protect	A loop is detected on Interface GigabitEthernet 1/ <port num="">.</port>	Network
I LACP	LACP was enabled on port [1 ~ port_num] with key [conf.port_key]	Network

The Syslog message events that the plugin is listening for are in the table below:

Module-Change	SFP module inserted on port [1~port_num ]	Network
Module-Change	SFP module removed on port [1~port_num ]	Network
Over-Max-PoE-	Port [1~port_num] over max PoE power limitation	PoE
Power-Limitation		
PoE-Auto-Check	PoE Auto Checking Reboot PD Failure, Port [1~port_num] IP: [ipv4 or	PoE
	ipv6]	
PoE-PD-Off	Port [ 1~port_num ] PoE PD off	PoE
PoE-PD-On	Port [ 1~port_num ] PoE PD on	PoE
PoE-PD-Over-	Port [ 1~port_num ] PoE PD over current	PoE
Current		