

Integrate Netgear prosafe

EventTracker v9.x and above

Publication Date: August 12, 2019

Abstract

This guide provides instructions to retrieve Netgear prosafe event logs and integrate it with EventTracker. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Netgear prosafe GS748Tv5 switches.

Audience

The configurations detailed in this guide are consistent with EventTracker version v9.x or above and Netgear prosafe GS748Tv5 switches.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

Abstract	1
Audience	1
Overview	3
Prerequisites	3
Configuring Netgear prosafe to forward log to EventTracker Configuring the syslog.	3 3
Configuring the command log	4
Configuring the console log	4
Configuring the buffer logs	5
EventTracker Knowledge Pack Alerts	5 5
Flex Reports	6
Dashboards	9
Saved Searches	11
Importing Netgear prosafe knowledge pack into EventTracker Alerts	11 12
Importing Netgear prosafe knowledge pack into EventTracker Alerts Knowledge object	11 12 13
Importing Netgear prosafe knowledge pack into EventTracker Alerts Knowledge object Token template	11 12 13 14
Importing Netgear prosafe knowledge pack into EventTracker Alerts Knowledge object Token template Flex Reports	11 12 13 14 16
Importing Netgear prosafe knowledge pack into EventTracker Alerts Knowledge object Token template Flex Reports Category	11 12 13 14 16 17
Importing Netgear prosafe knowledge pack into EventTracker	11 12 13 14 16 17 18
Importing Netgear prosafe knowledge pack into EventTracker Alerts Knowledge object Token template Flex Reports Category Dashboard Verifying Netgear prosafe knowledge pack in EventTracker Alerts	11 12 13 14 16 17 18 20 20
Importing Netgear prosafe knowledge pack into EventTracker Alerts Knowledge object Token template Flex Reports Category Dashboard Verifying Netgear prosafe knowledge pack in EventTracker Alerts Knowledge object	11 12 13 14 16 17 18 20 20 20 20
Importing Netgear prosafe knowledge pack into EventTracker	11 12 13 14 16 17 18 20 20 20 20 21
Importing Netgear prosafe knowledge pack into EventTracker	11 12 13 14 16 17 18 20 20 20 20 21 22
Importing Netgear prosafe knowledge pack into EventTracker	11 12 13 14 16 17 18 20 20 20 21 22 22

Netsurion... EventTracker

Overview

Netgear prosafe Web Managed Switches (previously called Prosafe Unmanaged Plus Switches) are an upgrade from unmanaged switches. Prosafe Web Managed Switches are plug-and-play for easy deployment, but also support additional configuration and monitoring features using a web browser-based GUI.

EventTracker collects the event logs delivered from Netgear prosafe for creating a reports, dashboard and alerts. Among the event types, we are considering: Login failure, Login success, Link up/down and authentication failure etc. EventTracker helps you to visualize the Netgear prosafe activities in the dashboard. EventTracker triggers alert whenever a user login attempt failed and the authentication failed by user.

Prerequisites

- Admin access permissions required to make configuration changes on the Netgear prosafe.
- Make sure the exception for port 514 in firewall of EventTracker Manager system.

Configuring Netgear prosafe to forward log to EventTracker

Configuring the syslog.

- 1. Login to Netgear prosafe switch user interface.
- 2. From the main menu, select Monitoring > Logs > Syslog Configuration.

System Switchur	ig kouting Go	5 Security	Monitoring	Mainten	once Help	Index
forte Logs Minoring	shew					
Buffered Logs	Syslog Configu	ration				
Command Log	Syslog Configu	ration	-			30
Console Log	Admin Status		Oisable	# Enable		
Configuration	Local UDP Port		514		(1 to 65515)	
Systep Configuration	Messages Receiv	ed	40543		-	
Trap Logs	Messages Relaye	d	10			
Event Logs	Messages Ignore	d	0			
Persistent Logs						
	Host Configura	tion			24	22
	1P Address T	ype Host Address	SI	atus Port	Severity Filter	
	10 10-4	192,106,110,1	00 Ac	tive 514	Informational	T

Figure 1



- 3. In the syslog Configuration, next to the Admin Status, select the Enable radio button.
- 4. In the Host configuration, provide IP Address type, Host addresss and Port number.
- 5. Click Apply.

Configuring the command log.

1. Select Monitoring > Logs > Command Log.

System Sv	ritching	Routing	Qo5	Security	Monitoring	Maintenance	Help	Index	LOOOVI
Parts Logs M	moning								
Buffered Logs Communication Configuration Sys Log Configuration Trap Logs Event Logs	Comr Cou Admin	nand Log C	onfigura mfiguratio	tion a Ofsable • Ena	Die				
								CAN	COL CARRY



- 2. Under Command Log, for Admin Status, select the Enable radio button.
- 3. Click Apply.

Configuring the console log.

1. Select Monitoring > Logs > Console Log.

Buffered Logs Command Log	Console Log Config	uration	_	
Configuration Configuration Sys Log Configuration Trap Logs Event Logs	Admin Status Severity Filter	Cnable Disable Alert		





- 2. Under **Console Log** Configuration, for **Admin Status**, select the **Enable** radio button.
- 3. Click Apply.

Configuring the buffer logs.

1. Select Monitoring > Logs > Buffer Logs.

Ports Logs Min	oring		
Rufferred Loge Command Log Configuration Console Log Configuration Sys Log	Buffered Logs Buffered Logs Admin Status Behavior Wrap) Enable	
Trap Logs Event Logs	Message Log Total number of Messages 369 (displaying) g only the last 128 messages)	
	Description		
	<14> Jan 1 02:14:37 0.0.0.0-1 UNKN[774665 371 %% DNS Client: Configured DNS server 1	9480]: dns_client_bcrc.c(195) 192.168.10.1 unreachable	
	<14> Jan 1 02:13:26 0.0.0.0-1 UNKN[774665 370 %% DNS Client: Configured DNS server 1	9480]: dns_client_txrx.c(195) 192.168.10.1 unreachable	
	<14> Jan 1 02:12:15 0.0.0.0-1 UNKN[774665 369 %% DNS Client: Configured DNS server 1	9480]: dns_client_txnx.c(195) 192.168.10.1 unreachable	
	<6> Jan 1 02:11:04 0.0.0-1 UNKN[7746694	480)r dns_client_txnc.c(195)	

Figure 4

- 2. Under Buffer Logs, for Admin Status, select the Enable radio button.
- 3. Click Apply.

EventTracker Knowledge Pack

Once logs are received by EventTracker manager, Knowledge Packs can be configured into EventTracker. The following Knowledge Packs are available in EventTracker to support **Netgear prosafe**.

Alerts

- **Netgear prosafe: Authentication failed** This alert is generated when user is unable to pass authentication. Using this alert, we can track authentication failure and account compromise detection, abnormal authentication attempts, off hour authentication attempts etc.
- **Netgear prosafe: Login failed** This alert is generated when user fails to login. We can identify brute force attack when any an IP or any host has multiple login failures within half an hour.



Flex Reports

 Netgear prosafe – Login success - This report provides detailed information related to user login success. Using this report, we can find out username, login time, computer name and from which IPaddress user is connected.

LogTime	Computer	Source IP	Source User
08/05/2019 06:35:39 PM	NETGEAR1	192.16.0.55	
08/05/2019 05:29:32 PM	NETGEAR	172.16.166.231	
08/05/2019 05:30:00 PM	NETGEAR	172.16.166.231	8
08/06/2019 10:30:16 AM	NG1	192.108.10.20	admin
08/06/2019 10:30:15 AM	NG1	192.108.10.10	admin
08/06/2019 10:30:15 AM	NG1	192.108.100.50	admin
08/05/2019 06:42:54 PM	NG1	192.108.110.100	admin



Sample Logs:

event_category	+- 0
event_computer	+- NG2
event_datetime	+- 8/8/2019 10:30:16 AM
event_datetime_utc	+- 1565240416
event_description	54.100.100-1 General [129997136] : main_login.c(214) 40843 %% HTTP Session 11 initiated for user admin connected from 1
	92.108.10.20
event_id	+- 3230
event_log_type	+- Application
event_source	+- syslog local
event_type	+- Information
event_user_domain	+- N/A
event_user_name	+- N/A
log_source	+- Netgear Prosafe all events
logon_type	+- user admin connected
<pre>src_ip_address</pre>	+- 192.108.10.20
<pre>src_ip_address_geoip.city_name</pre>	+- Virginia Beach
<pre>src_ip_address_geoip.continent_nar</pre>	n t - North America
<pre>src_ip_address_geoip.country_iso_country_</pre>	o de US
<pre>src_ip_address_geoip.region_name</pre>	+- Virginia
<pre>src_ip_address_geoip.location.lat</pre>	+- 36.9205
<pre>src_ip_address_geoip.location.lon</pre>	+76.0192
src user name	+- admin

Figure 6



Netgear prosafe – Login failure – This report provides detailed information related to user login failure.
 Using this report, we can find out which user is failed to login and on which system he/she is trying to login.

LogTime	Computer	User
08/06/2019 10:30:16 AM	NG1	Admin
08/06/2019 10:30:15 AM	NG1	admin
08/06/2019 10:30:15 AM	NG1	Admin
08/05/2019 06:35:06 PM	NETGEAR1	admin
08/05/2019 06:35:06 PM	NETGEAR1	Admin
08/05/2019 05:29:32 PM	NETGEAR	Admin
08/05/2019 06:42:50 PM	NG1	Kevin
08/05/2019 06:35:38 PM	NETGEAR1	Kevin
08/05/2019 06:35:45 PM	NETGEAR1	Kevin
08/05/2019 06:35:43 PM	NETGEAR1	Kevin
08/06/2019 10:30:15 AM	NG1	Maria
08/05/2019 06:35:38 PM	NETGEAR1	Maria
08/06/2019 10:30:15 AM	NG1	Robert

Figure 7

Sample Logs:

event_category	+- 0
event_computer	+- NG2
event_datetime	+- 8/8/2019 10:30:16 AM
event_datetime_utc	+- 1565240416
event_description	54.100.100-1 TRAPMGR[129997136] : traputil.c(658) 40841 %% Failed user login with user ID: Johnson
event_id	+- 3230
event_log_type	+ - Application
event_source	+- syslog local
event_type	+- Information
event_user_domain	+- N/A
event_user_name	+- N/A
log_source	+ - Netgear Prosafe all events
logon_type	+- Failed user login



 Netgear prosafe – Link status - This report provides detailed information related to Interface numbers, link status (up/down) etc.

LogTime	Link Status	Interface Number
08/05/2019 06:35:39 PM	up	g13
08/05/2019 06:35:43 PM	up	g13
08/05/2019 06:35:46 PM	up	g13
08/06/2019 10:30:15 AM	Down	g18
08/05/2019 06:43:11 PM	Down	g18
08/05/2019 06:42:50 PM	up	g19
08/05/2019 06:35:45 PM	down	g25
08/05/2019 06:35:45 PM	up	g37
08/06/2019 10:30:15 AM	up	g5
08/05/2019 06:43:11 PM	down	g5
08/06/2019 10:30:16 AM	down	g50
08/05/2019 06:35:46 PM	down	g50
08/06/2019 10:30:16 AM	down	g7

Sample Logs:

addl_info	+- g7
event_category	+- 0
event_computer	+- NG2
event_datetime	+- 8/8/2019 10:30:16 AM
event_datetime_utc	+- 1565240416
event_description	Jul 15 12:39:43 192.168.1.246 Oct 10 15:25:14 192.168.1.246-1 TRAPMGR[66764860]: traputil.c(696) 1676197
	%% Link down: g7
event_id	+- 3230
event_log_type	+- Application
event_source	+- syslog local
event_type	+- Information
event_user_domain	+- N/A
event_user_name	+- N/A
log_source	+ - Netgear Prosafe all events
log_type	+- down

Figure 10



Dashboards



• Netgear prosafe – Login by geo-location.

Figure 11

• Netgear prosafe – User login attempt by source IP.

event_datetime	event_computer	<pre>src_ip_address</pre>	src_user_name
Aug 06 03:16:09 PM	NG2	192.108.10.20	admin
Aug 06 03:16:09 PM	NG2	192.108.10.10	admin
Aug 06 03:16:08 PM	NG2	192.108.100.50	admin
Aug 06 03:16:08 PM	NG2	192.108.110.100	admin
Aug 06 03:16:07 PM	NG2	192.108.110.100	admin
Aug 06 03:16:05 PM	NG2	192.108.10.20	admin
Aug 06 03:16:05 PM	NG2	192.108.10.10	admin
Aug 06 03:16:04 PM	NG2	192.108.110.100	admin
Aug 06 03:16:04 PM	NG2	192.108.100.50	admin
Aug 06 03:16:04 PM	NG2	192.108.110.100	admin

Figure 12





• Netgear prosafe – Login failure by user.

Figure 13

• Netgear prosafe – Authentication failure by user.

event_datetime	event_computer	src_user_name
Aug 06 03:16:09 PM	NG2	Brod
Aug 06 03:16:09 PM	NG2	Admin
Aug 06 03:16:09 PM	NG2	Joe.R
Aug 06 03:16:08 PM	NG2	Jimmy
Aug 06 03:16:08 PM	NG2	admin
Aug 06 03:16:05 PM	NG2	Brod
Aug 06 03:16:05 PM	NG2	Admin
Aug 06 03:16:05 PM	NG2	Joe.R
Aug 06 03:16:04 PM	NG2	Jimmy
Aug 06 03:16:04 PM	NG2	admin

Figure 14



• Netgear prosafe – Link status.

Netgear prosafe- Link status		C - >
event_datetime	addl_info	log_type
Aug 08 10:30:16 AM	g25	down
Aug 08 10:30:16 AM	g13	up
Aug 08 10:30:16 AM	g7	down
Aug 08 10:30:16 AM	g50	down
Aug 08 10:30:16 AM	g19	up
Aug 08 10:30:16 AM	g10	up
Aug 08 10:30:15 AM	g5	up
Aug 08 10:30:15 AM	g5	down
Aug 08 10:30:15 AM	g18	Down
Aug 08 10:30:15 AM	g37	up
	Aug 01 10:31 AM - Aug 08 10:32 AN	л



Saved Searches

- 1. **Netgear prosafe: Authentication failure** This saved search will display events specific to the "Authentication failure" activity.
- 2. Netgear prosafe: Link status This saved search will display events specific to the "Link status" activity.
- 3. Netgear prosafe: Login failed This saved search will display events specific to the "Login failed" activity.
- 4. Netgear prosafe: Login success This saved search will display events specific to the "Login success" activity.

Importing Netgear prosafe knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Alerts.
- Knowledge Object.
- Token templates.
- Flex Reports.
- Categories.
- Dashboard.

Netsurion... EventTracker

- 1. Launch the EventTracker Control Panel.
- 2. Double click Export-Import Utility.



🥾 Ехро	rt Import	Utility	
Export	Import		
1. Pro 2. Cli	ovide the p ck the Imp	ath and file nar ort button.	ne of the Categories file. Use the '' button to
Opti	ons		Location
•	Category		



3. Click the **Import** tab.

Alerts

- 1. Click Alert option, and then click the browse ____button.
- 2. Navigate to the location having a file with the **extension ".isalt**" and then click on the "**Import**" button:

Options	Location	
Category	Import E-mail settings	
Filters	Set Active Only if notifications set Dev default	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.
 Alerts 	0 0,000	
 Systems and Groups 	Watchlist Configuration	
O Token Value	Import Watchlist configurat This setting is applicable only f Note: If this option is enabled t	ion for alerts which have Advanced watchlist configured. the user should make sure the watchlist croups are available
Reports	on the console where the alert	ts are imported.
O Behavior Correlation		
	Source : E:\NetS_Projects\	\Integration\Configuration items\Alerts_F isait

Figure 18

3. EventTracker displays a success message:



Figure 19

Knowledge object

- 1. Logon to EventTracker console.
- 2. Click **Knowledge objects** under the **Admin** option in the EventTracker manager page.

			🔎 🛛 Admin 🗸	Tools 🗕 🌔
	Active Watch Lists	Event Filters	🧭 Parsing Rules	🔒 / Das
	Alerts	Sector Eventvault	Report Settings	
	Behavior Correlation Rules	FAQ Tile Configuration	Systems	
	🗞 Behavior Correlation Settings	Group Management	Q Users	
o <mark>mi</mark> prisc	Casebook Configuration	🔍 IP Lookup Configuration	r Weights	since the last 24 hours
	eeeory	·☆ Knowledge Objects	Windows Agent Config	
	Diagnostics	Manager		





3. Next, click on the "import object" icon.





4. A pop-up box will appear, click "**Browse**" in that and navigate to the file path with extension ".etko" button".

Import	×
Ko_Netgear prosafe.ekto 😂 Browse Upload	
Figure 22	

5. List of available Knowledge object will appear. Select the relevant files and click on "**Import**" button:

Impo	ort			×
Se	lect file		🖀 Browse	Upload
	Object name	Applies to	Group	ame
	Netgear prosafe all events	Netgear prosafe	Netgear p	rosafe
				Import Close



6. A message displays "file imported successfully".

Token template

1. Click on **Parsing rule** under the **Admin** option in the EventTracker manager page.



		🔎 🛛 Admin 🗸
Active Watch Lists	FAQ Tile Configuration	🧭 Parsing Rules
Alerts	Group Management	Report Settings
Casebook Configuration	Q IP Lookup Configuration	Systems
● Category	·☆ Knowledge Objects	Q Users
▲ Diagnostics	Machine Learning Jobs	T Weights
Event Filters	🗞 Machine Learning Settings	Windows Agent Config
Eventvault	D Manager	

2. Select **Template** and click on **import**

icon in top right corner.

Event Tracker ⊕			1	Admin -	Tools -	🚯 Adarsh Pandey -
Parsing Rules					A	/ Admin / Parsing Rule
Parsing Rule Template						
Groups	(+)					CIT
Default						
ABC	Ē Ø			Active		

Figure 25

- 3. Select the file of type *.ettd(eventtracker template dashlets.)
- 4. Select all the Netgear prosafe template name.
- 5. And click on **import i**con

selecte	d file is: Templets_Netgear prosafe.ettd	🗁 Browse 😱	
	Template name	Separator	Template description
✓	Netgear prosafe - Link status	١n	Jul 10 21:15:51 192.168.1.24 6764860]: traputil.c(696) 16 168.1.250 Oct 5 23:59:52 19 (696) 975007 %% Link Up: g
•	Netgear prosafe - Login failure	\n	54.100.100-1 TRAPMGR[129 r login with user ID: admin l
	Netgear prosafe - Login success	\n	<14> Jan 01 01:25:47 172.1 TTP Session 1 Login success

Figure 25

6. Template(s) imported successfully.

ок



Flex Reports

 In EventTracker control panel, select "Export/ Import utility" and select the "Import tab". Then, click Reports option, and choose "New (*.etcrx)":

Export Import Utility	- 0	×
Export Import		
1. Provide the path and file nam 2. Click the Import button Note : If report(s) contains templ	e of Schedule Report file. Use the '' button to browse and locate the import file. ate, first import template and proceed with exportimport utility.	
Options	Location	
Category		
⊖ Filters		
◯ Alerts	O Legacy (*.issch) New (*.etcrx)	
Systems and Groups	Source :	
◯ Token Value	ISSCN	
Reports		
Behavior Correlation		
	Import Close	



- 2. Once you have selected "**New (*.etcrx)**", a new pop-up window will appear. Click "**Select File**" button and navigate to the file path with a file having extension ".etcrx".
- 3. Select all the relevant files and then click **Import** button.
- 4. EventTracker displays a success message:





Figure 28

Category

1. Click the category option, and then click the browse ____ button.

Export Import Utility	-		\times
Export Import			
1. Provide the path and file nam 2. Click the Import button.	ne of the Categories file. Use the '' button to browse and locate the import file.		
Options Category Fiters Alerts Systems and Groups Token Value Reports Behavior Correlation	Location Source - Category_Netgear prosafe		
	Import	(Jose



- 2. Locate the **Category_Netgear prosafe.iscat** file, and then click the open button.
- 3. To import category, click the Import button.

EventTracker displays a success message.





4. Click the OK button, and then click the **Close** button.



Dashboard

- 1. Login to EventTracker.
- 2. Navigate to **Dashboard** \rightarrow **My Dashboard**.
- 3. In "My Dashboard", Click Import Button:







4. Select the **browse** button and navigate to file path where Dashboard file is saved and click on "**Upload**" button.





5. Once completed, choose "Select All" and click on "Import" Button.



shlet.	🗁 Browse Upload
vailable widgets	
Select All	
Netgear prosafe- login by	✓ Netgear prosafe- User log ✓ Netgear prosafe- login f
Netgear prosafe- Authent	✓ Netgear prosafe- Link sta

6. Next, click "Customize dashlet" button as shown below:





7. Now, put a text on **Search bar: "Netgear prosafe"** and then select the Netgear prosafe Dash-lets and the click **"Add"** button.

Customize dashlets			×
netgear prosafe			Q
🗹 Netgear prosafe- Authenticatio	✓ Netgear prosafe- login failure b	🗹 Netgear prosafe- Link status	☑ Netgear prosafe- login by geo-l
☑ Netgear prosafe- User login att			
			Add Delete Close

Figure 36



Verifying Netgear prosafe knowledge pack in EventTracker

Alerts

- 1. In the EventTracker web interface, click the Admin dropdown, and then click Alerts.
- In search box enter "Netgear prosafe" and then click the Search button.
 EventTracker displays an alert related to "Netgear prosafe":

Alerts Show All •						Search by Alert name	•	★ / Admin. Netgear prosafe
133 Available Alerts Vale nuester of auch sectate	35 Active Alerts Intel number of active elerts			133 System/User Defi Court for system and a	Igner Der 1 ned Alerts ar defind sierts	, ,	133 Alerts by The Court of seek by	Conce a a a a a a a a a a a a a a a a a a a
Activate Now Cick "Activate New" sher making at	changes							Total 3 Page Size 25
Aiert Name A	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
B Son Netgear Prosale - Authentication failure	•		- 10	0	0	0	0	Netgear Prosafe Switches
topin falure	0		8	0	0	0		Netgear Prosafe Switches
0	•		0	0	0	0		Netgear Procafe Switches

Figure 37

Knowledge object

1. In the EventTracker web interface, click the Admin dropdown, and then click Knowledge object.

Event Tracker ⊕					🔎 Admin v
Alerts			Active Watch Lists	FAQ Tile Configuration	🧭 Parsing Rules
Show All Y			Alerts	Group Management	Report Settings
			Casebook Configuration	Q IP Lookup Configuration	Systems
			eleo Category	·泣:· Knowledge Objects	🛱 Users
133	35	133	▲ Diagnostics	Machine Learning Jobs	A Weights
Available Alerts	Active Alerts	System/User Def	Event Filters	Machine Learning Settings	Windows Agent Config
Total number of alerts available	Total number of active alerts	Count for system and o	👰 Eventvault	🖉 Manager	
Activate Now Click 'Activate Now' after m	aking all changes				1

Figure 38

2. In the group section Netgear prosafe is present.

Knowledge Objects				
Search objects	ର୍ ଷ୍	Activate Now		
Groups	🕀 🏈 🗓	Object name Netgear Prosafe all events		
EventTracker		Applies to NetGear Prosate G5748105		
Netgear Prosafe		Rules		
Netgear Prosafe all events	Ø 🗓	Title	Event source	Source Type
■ Salesforce		Hetgear prosafe all events	syslog*	
Sophos Central		Message Signature: weblogin.*Login\ssu	ccess main_login.*user.*connected TRAPMGR.*Failed	\suser Login\sFailed main_login.*Auth
Windows		Message Exception: Expressions		
Windows Defender		Expression type Expression 1		
		Regular Expression (?<=Link\s).*?(?=\;)	

Token template

1. Click on Parsing rules under Admin .

		📣 Admin v	Tools +
Active Watch Lists	FAQ Tile Configuration	🧭 Parsing Rules	🔒 / Ad
Alerts	Group Management Contai	ns set of rules which tell what kind of	data you w
Casebook Configuration	Q IP Lookup Configuration	Systems	O
ele Category	☆ Knowledge Objects	QQ Users	
Diagnostics	B Machine Learning Jobs	∯ Weights	-
Event Filters	🐁 Machine Learning Settings	Windows Agent Config	
Eventvault	Manager		



- 2. Select template under parsing rules and select Netgear prosafe group.
- 3. All the templates are present under Netgear prosafe.

Parsing Rules				
Parsing Rule Template				
Groups		(+)	Group : Netgear prosafe	Search
Endpoint Kaspersky	Ű	<i>i</i>		
EventTracker	Ĩ	1	Template Name	Template Description
FortiMail	Ű	1	Netgear prosafe - Link status	Netgear prosafe - Link status
IIS - All HTTP Respo	Ē	1	Netgear prosafe - Login failure	Netgear prosafe - User login failure
Juniper JUNOS	Ĩ	1	Netgear prosafe - Login success	Netgear prosafe - Login success
Kaspersky Security C	Ű	0		
Netgear prosafe	Ũ	1		
SalesForce	Ű	1		
Sonicwall UTM	Ē	1		





Flex Reports

1. In the EventTracker web interface, click the Reports menu, and then select the Report Configuration.





- 2. In Reports Configuration pane, select the Defined option.
- 3. Click on the Netgear prosafe group folder to view the imported reports.

epor							
Sch	eduled 🔘 Queued	Defined					
Report	t Groups			+ #	Repor	ts configuration	on: Netgear prosafe
£(3	Security				⊕ į́	і д	
{]}	Compliance						Title
£3	All Operations Repor					2.23	Netgear prosafe - Login succes
[]]	Operations					1	Netgear prosafe - Login failure
{]}	Flex					2003	Netgear prosafe - Link status
	All Compliance Repor		Ē	Ø		~	
	All Operations Repor		Ē	Ø	<u> </u>		
	All Security Audit R		iii ii	0			
	All Threat Report			1			
	EventTracker		Ē	0			
	Netgear prosafe		Ē	1			
ם	Salesforce		ΠĪ.	Ø			

Category

- 1. Login to EventTracker.
- 2. Click the Admin menu, and then click Category.

≡	Event Tracker ⊕				🔎 🛛 Admin v	Tools 🕶
	Home		Active Watch Lists	Event Filters	Ø Parsing Rules	
٩		_	Alerts	Eventvault	Report Settings	_
	0	0	Behavior Correlation Rules	FAQ Tile Configuration	Systems	
			behavior Correlation Settings	Group Management	Q Users	
	Potential Cyber Breaches Unsafe connections or processes, new TCP ent	Indicators of Cor USB activities, New	Casebook Configuration	Q IP Lookup Configuration	Heights	orting Syste
			● Category	·☆· Knowledge Objects	Windows Agent Config	
	Attacker		Diagnostics	💇 Manager		





3. Click the search, and then search with Netgear prosafe.





Dashboard

1. In the EventTracker web interface, Click on Home 🔠 Button and select "My Dashboard".





2. In "Netgear prosafe" dashboard you should be now able to see something like this:





Figure 47

Netsurion EventTracker