Netsurion™ | EventTracker

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.

Table of Contents

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**.

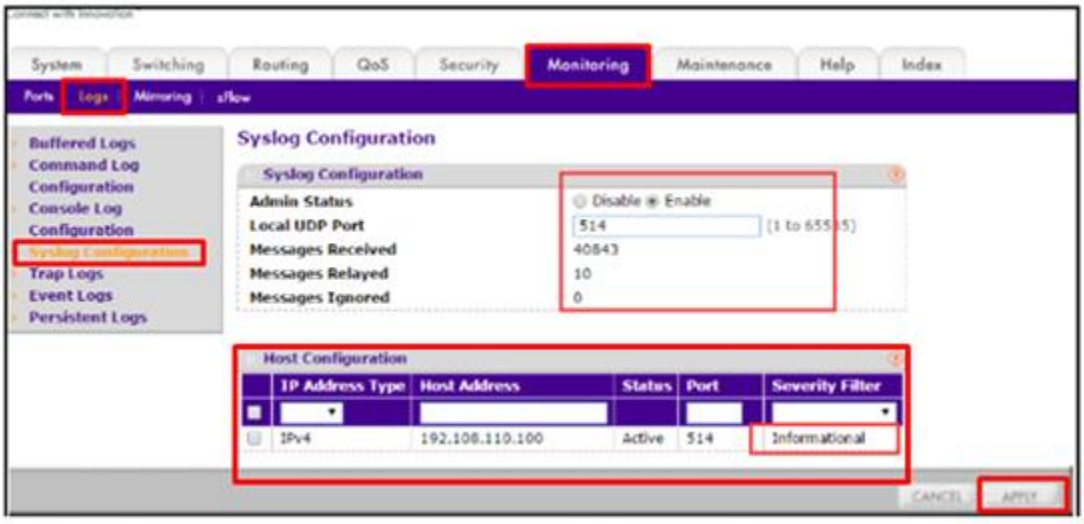


Figure 1

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.**

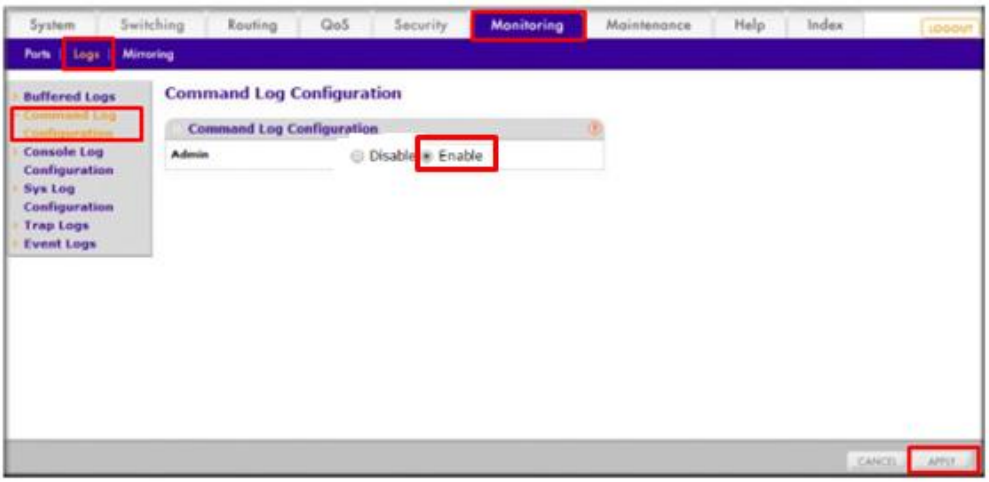


Figure 2

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**.

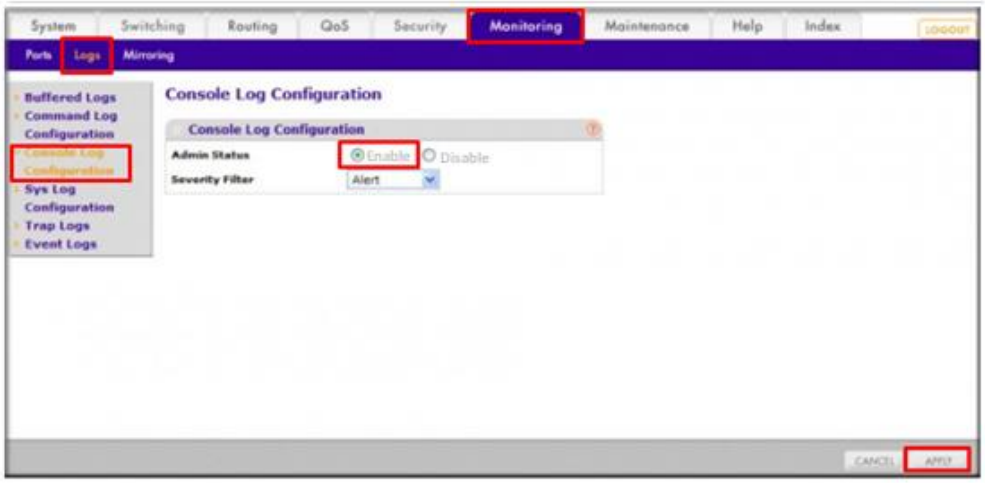


Figure 3

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**.

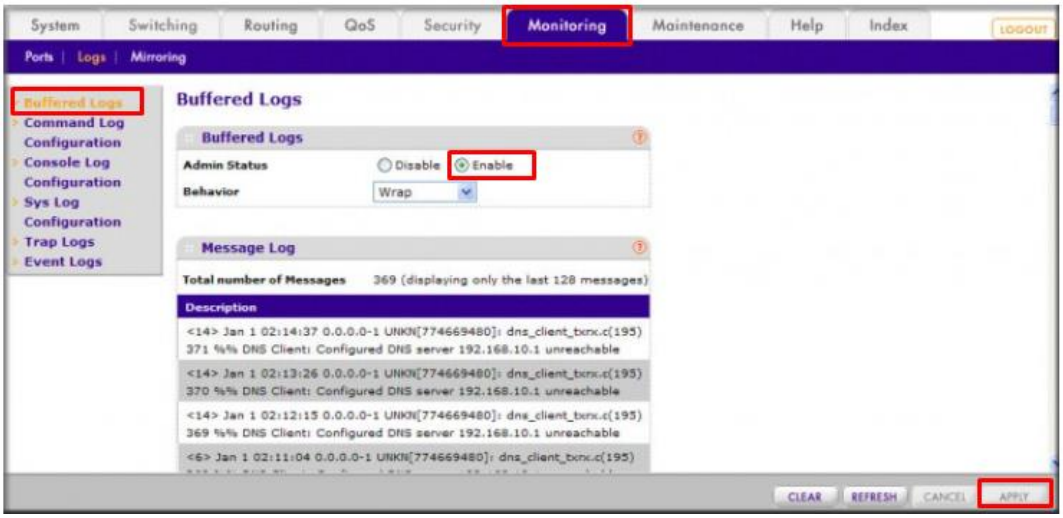


Figure 4

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 IP-address 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	
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

Figure 5

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 192.108.10.20
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
src_ip_address	192.108.10.20
src_ip_address_geoip.city_name	Virginia Beach
src_ip_address_geoip.continent_name	North America
src_ip_address_geoip.country_iso_code	US
src_ip_address_geoip.region_name	Virginia
src_ip_address_geoip.location.lat	36.9205
src_ip_address_geoip.location.lon	-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

Figure 8

- **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

Figure 9

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

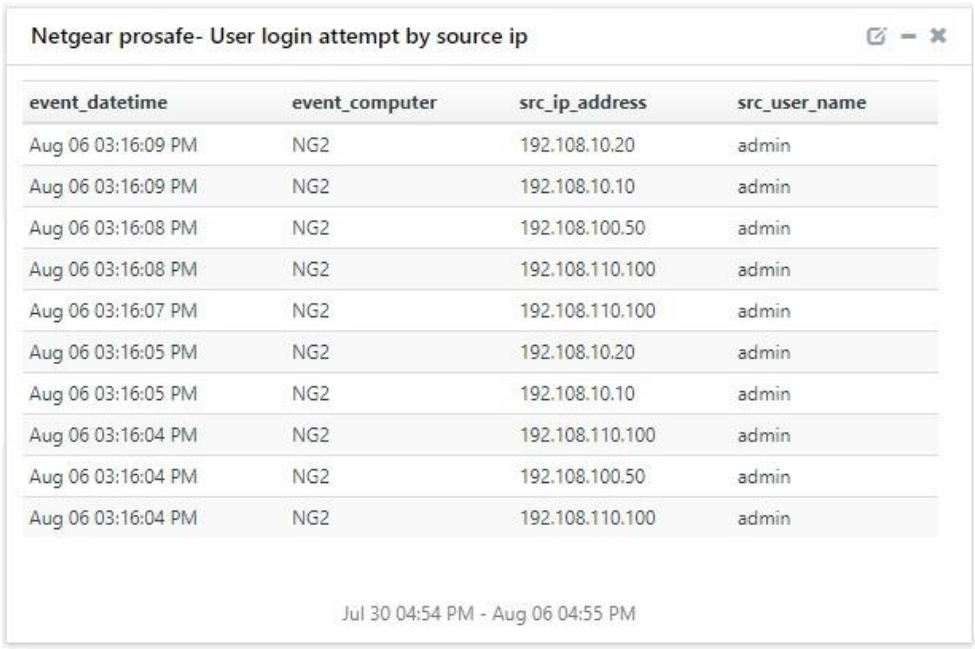
Figure 10

Dashboards

- **Netgear prosafe – Login by geo-location.**

Figure 11

- **Netgear prosafe – User login attempt by source IP.**



event_datetime	event_computer	src_ip_address	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.**

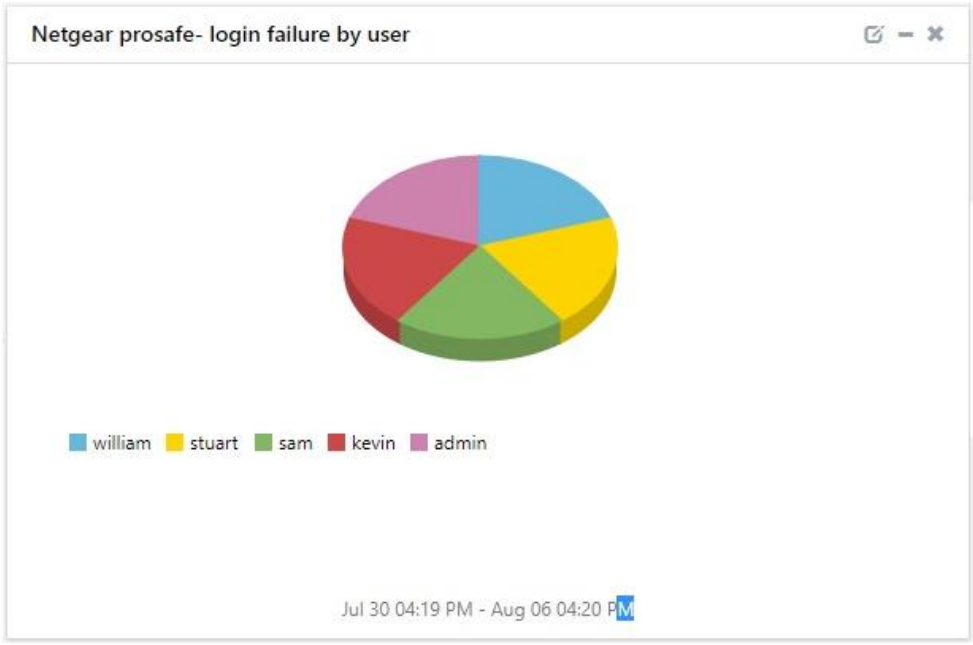
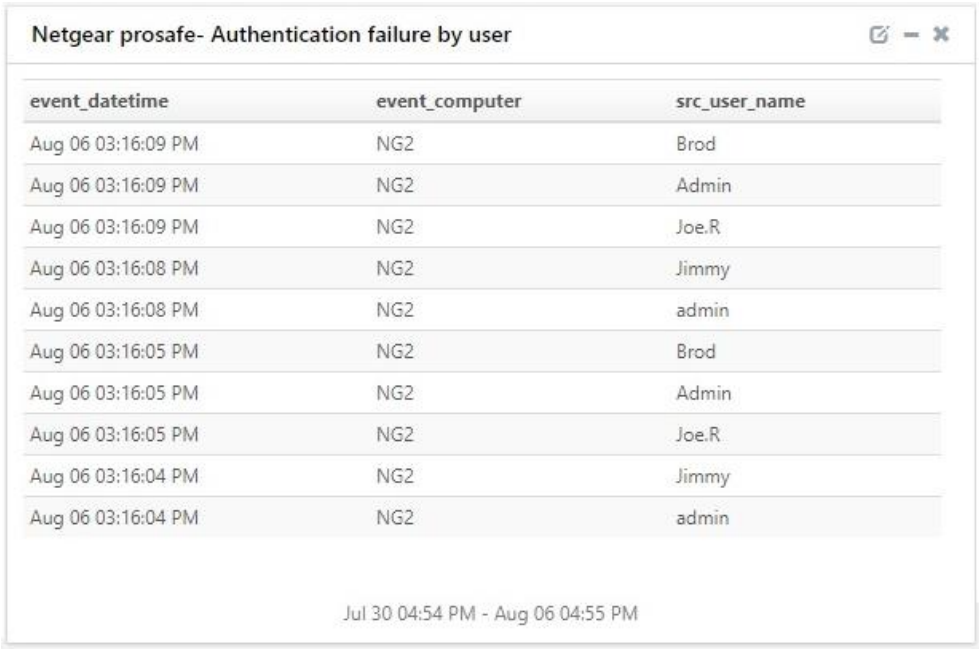


Figure 13

- **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.**

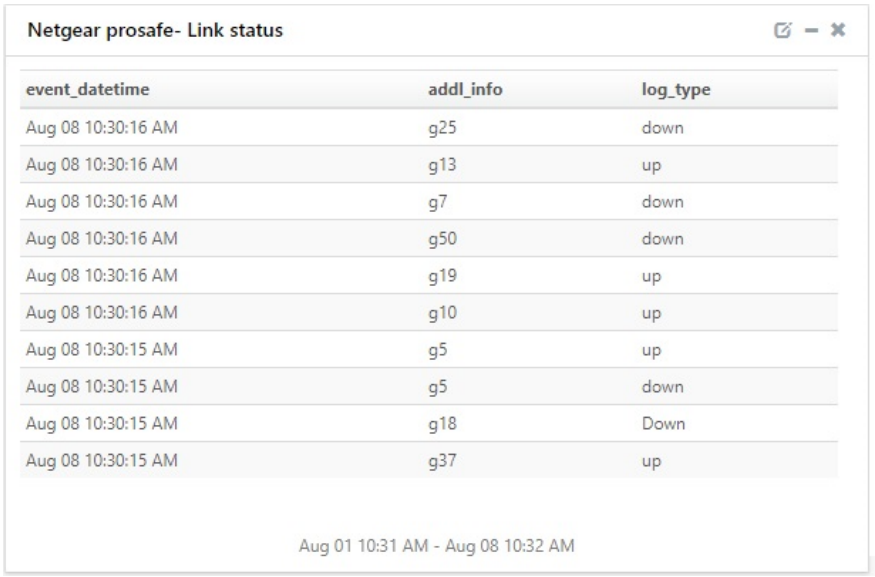


Figure 15

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.

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

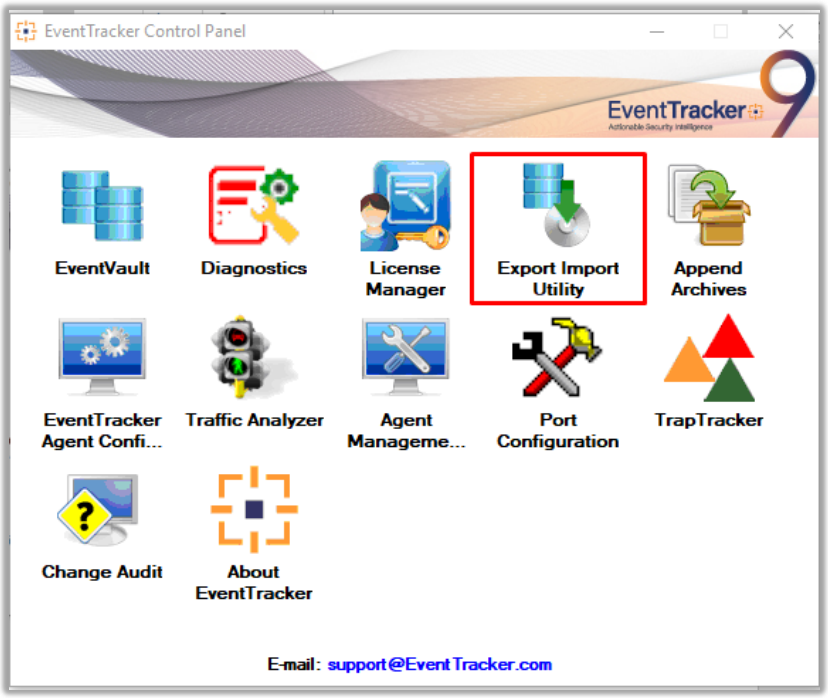


Figure 16

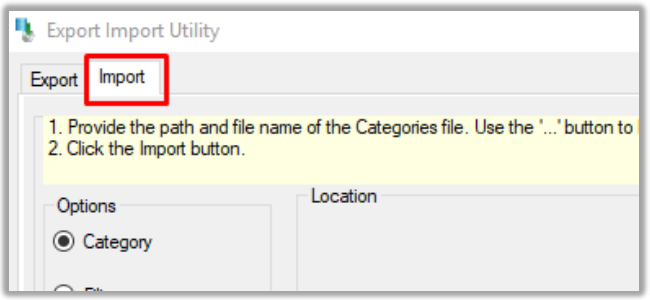


Figure 17

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:

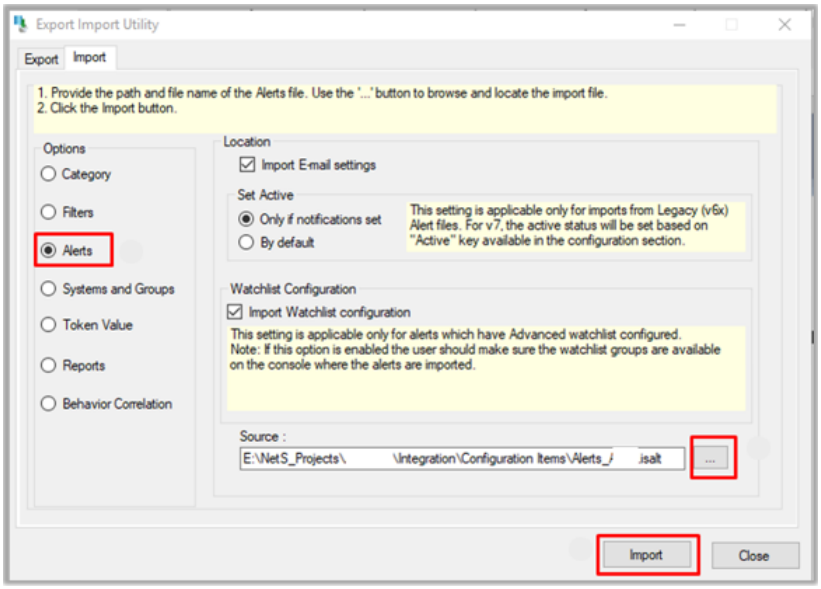


Figure 18

3. EventTracker displays a success message:

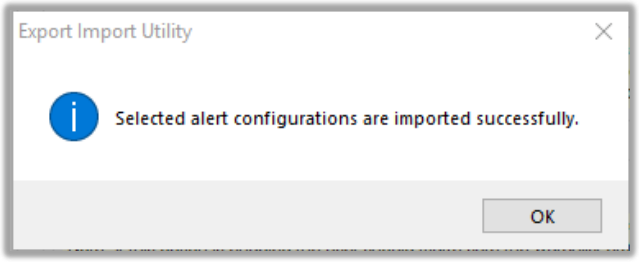


Figure 19

Knowledge object

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

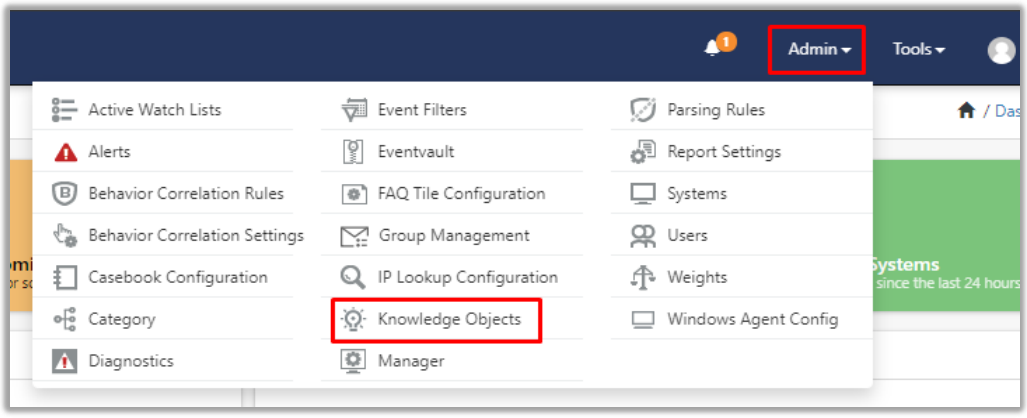


Figure 20

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

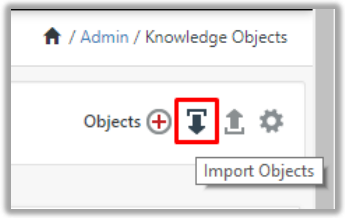


Figure 21

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

Figure 22

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

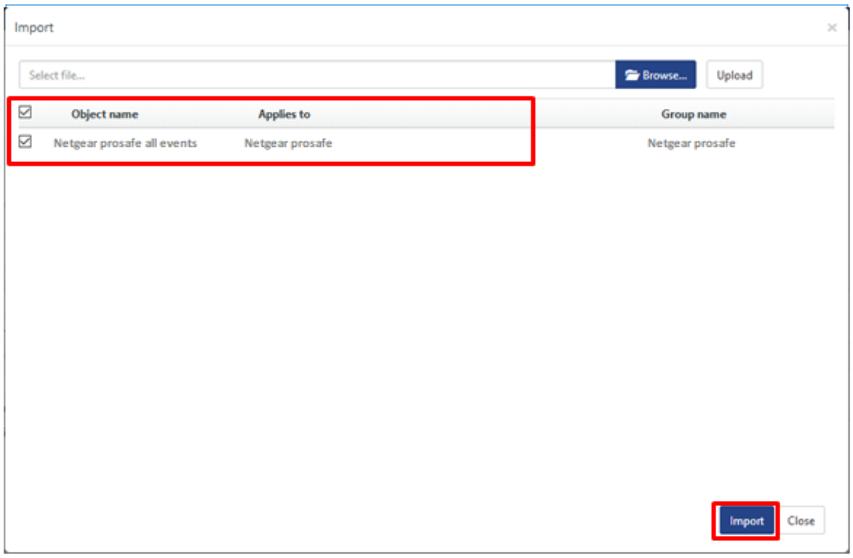


Figure 23

6. A message displays **"file imported successfully".**

Token template

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

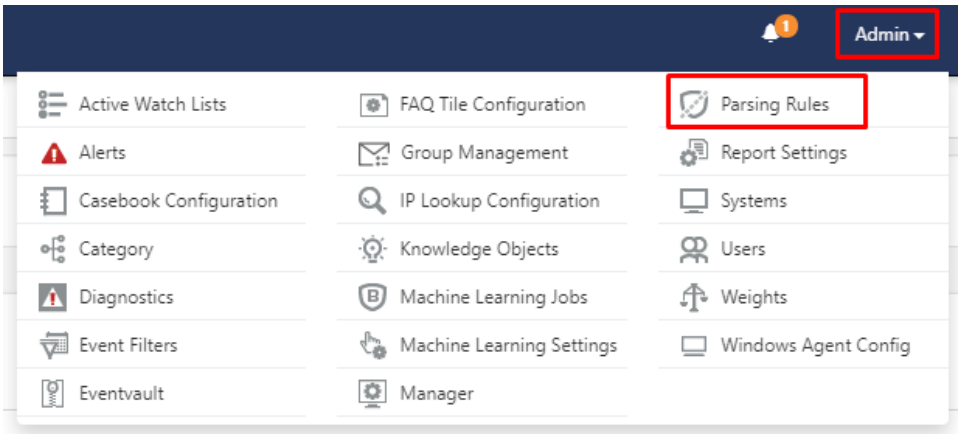


Figure 24

2. Select **Template** and click on **import** icon in top right corner.

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** icon

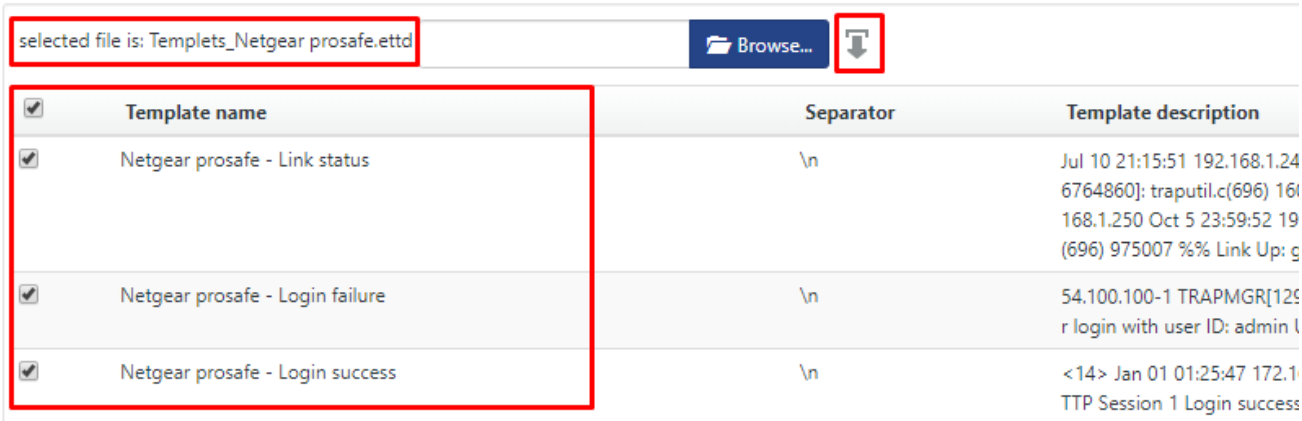


Figure 25

6. Template(s) imported successfully.

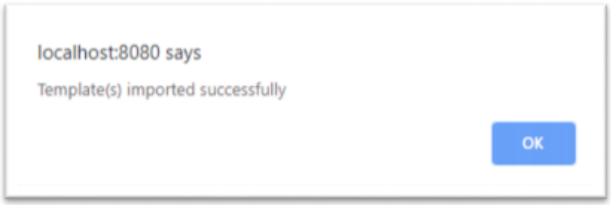


Figure 26

Flex Reports

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

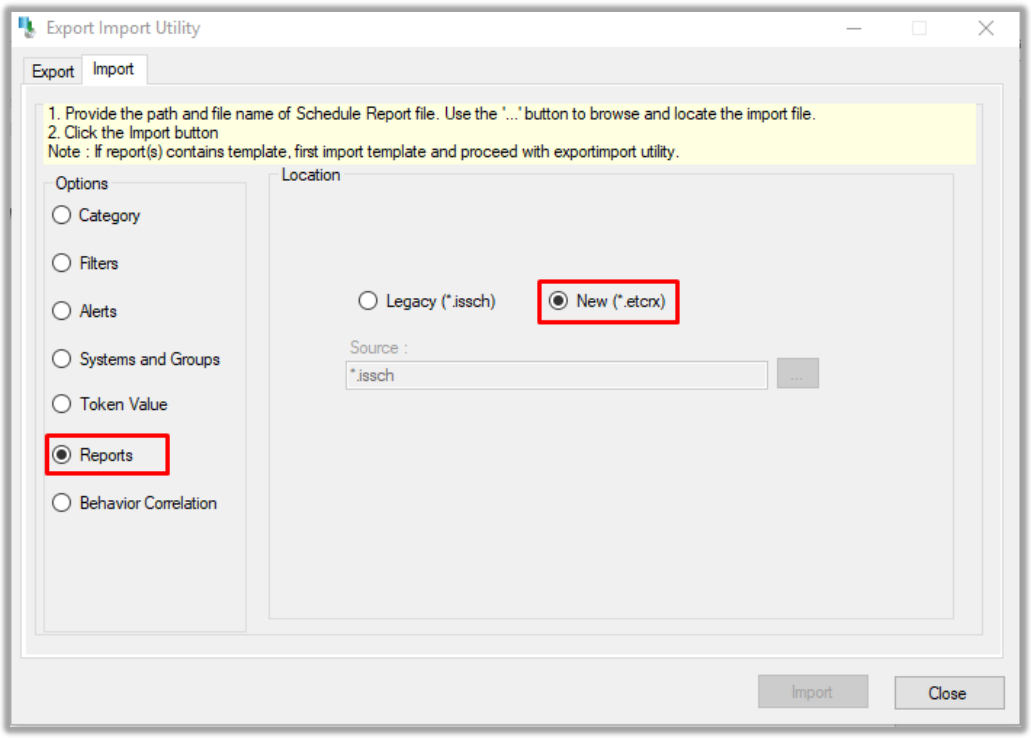


Figure 27

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:

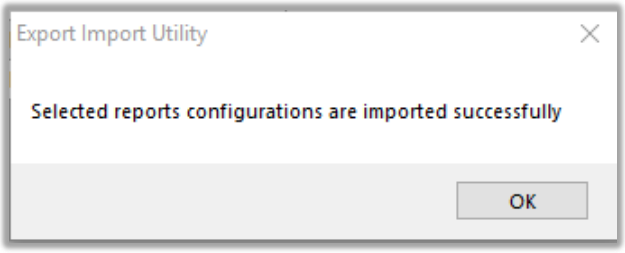


Figure 28

Category

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

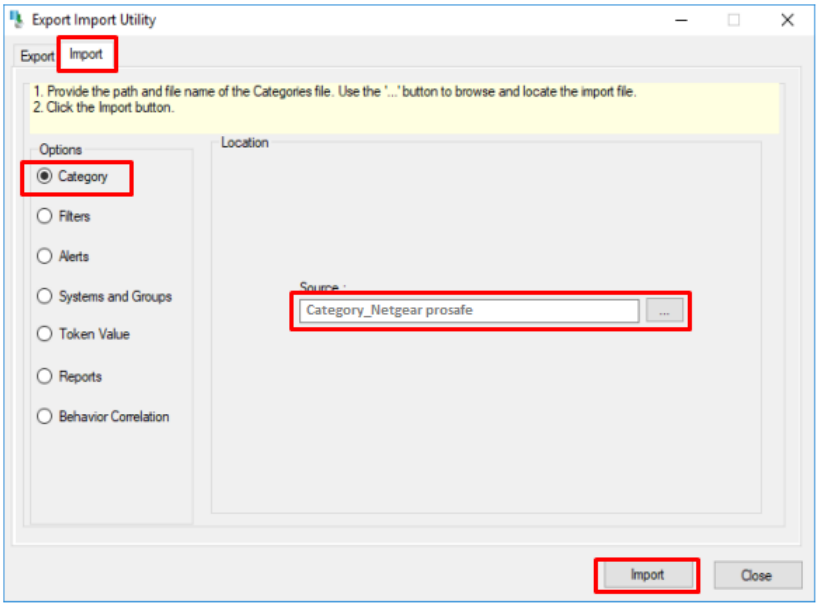


Figure 29

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.

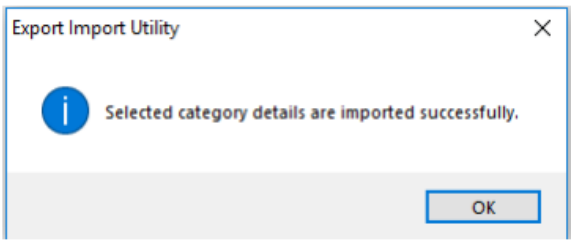


Figure 30

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

Dashboard

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

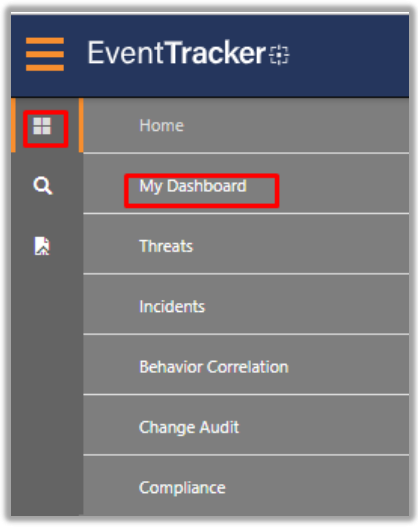


Figure 31

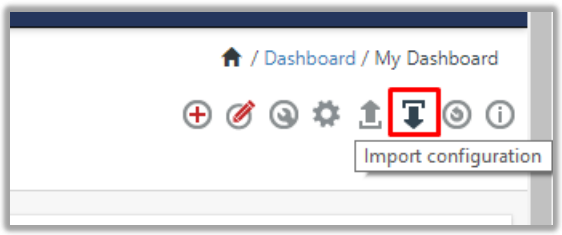


Figure 32

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

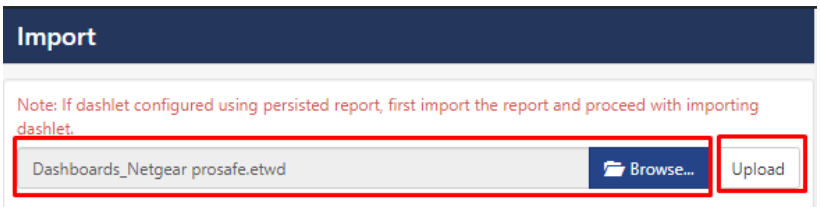


Figure 33

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

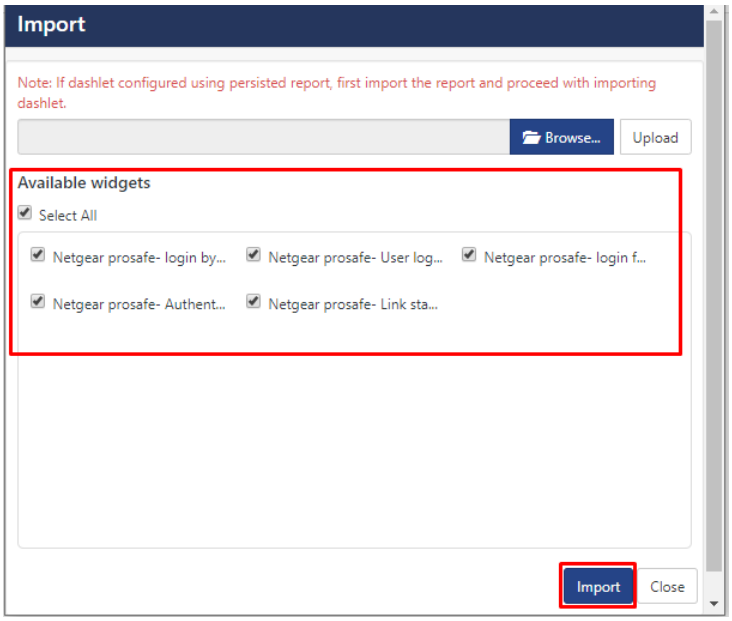


Figure 34

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

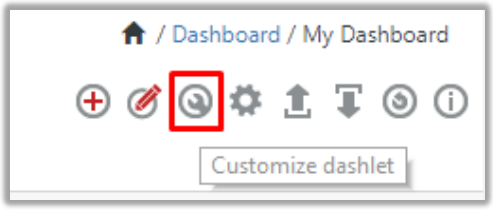


Figure 35

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

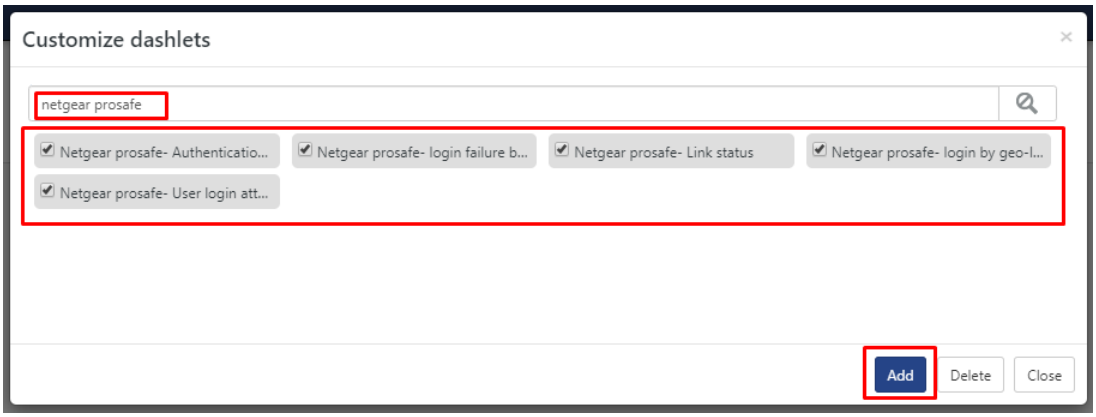


Figure 36

Verifying Netgear prosafe knowledge pack in EventTracker

Alerts

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

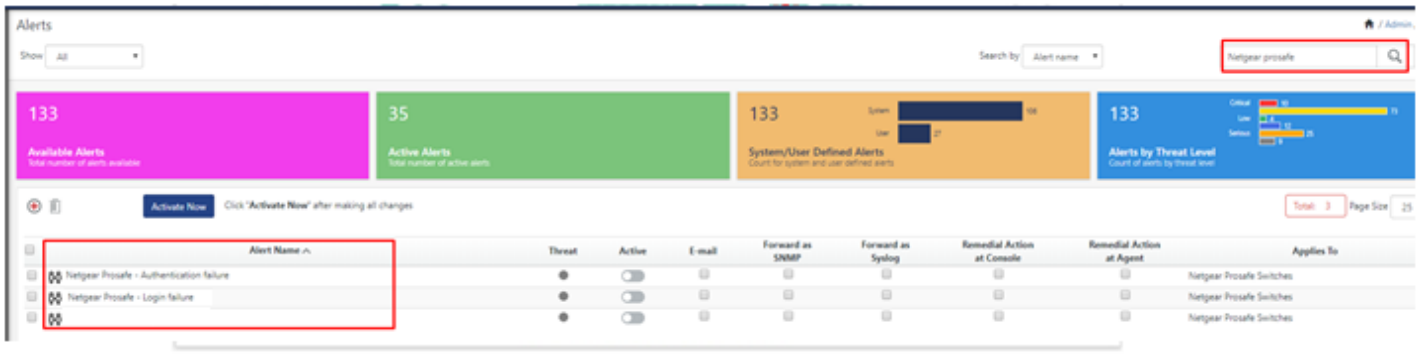


Figure 37

Knowledge object

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

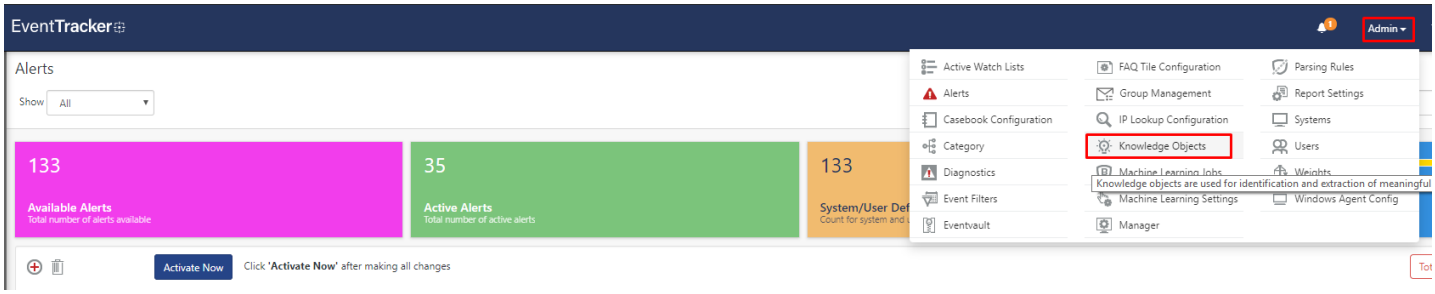


Figure 38

2. In the group section **Netgear prosafe** is present.

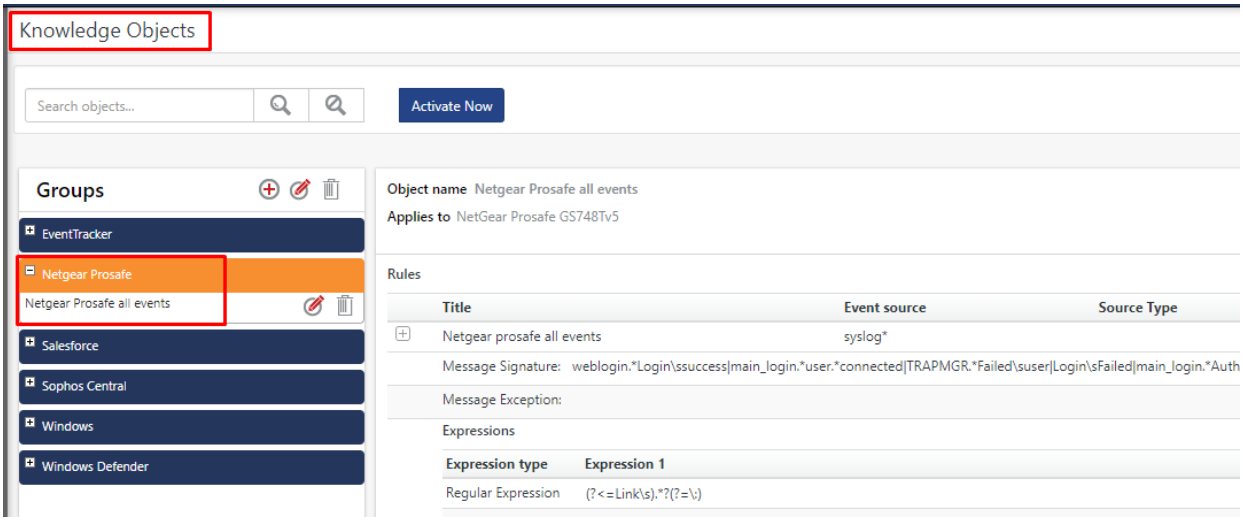


Figure 39

Token template

1. Click on **Parsing rules** under **Admin** .

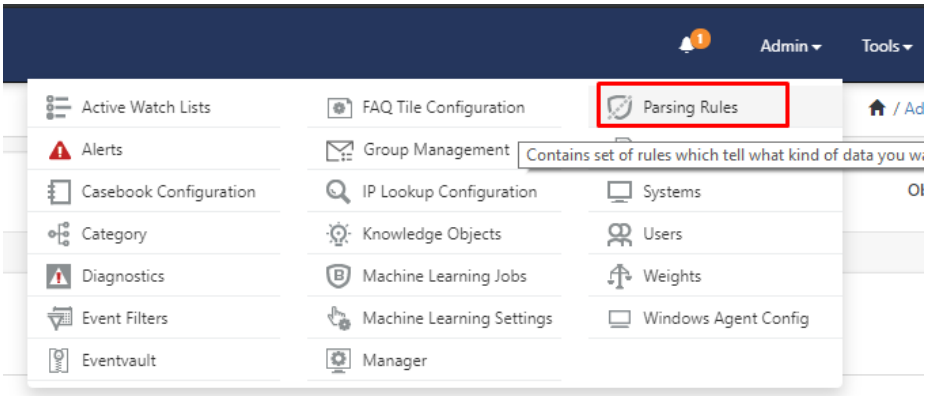


Figure 40

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

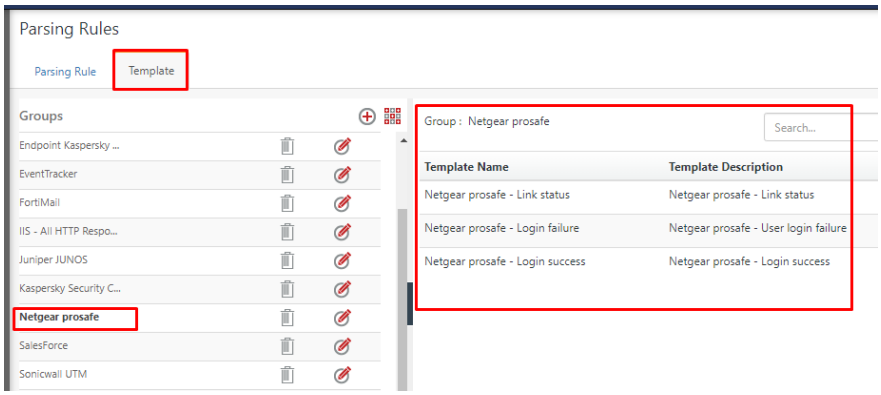


Figure 41

Flex Reports

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

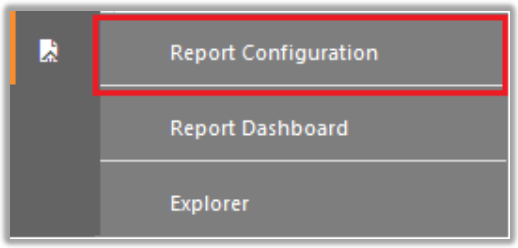


Figure 42

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

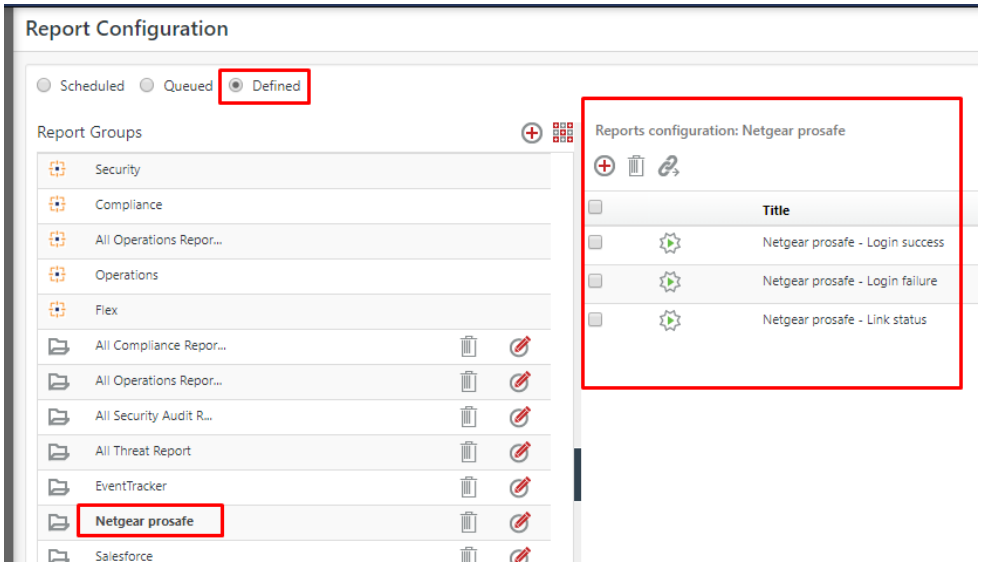


Figure 43

Category

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

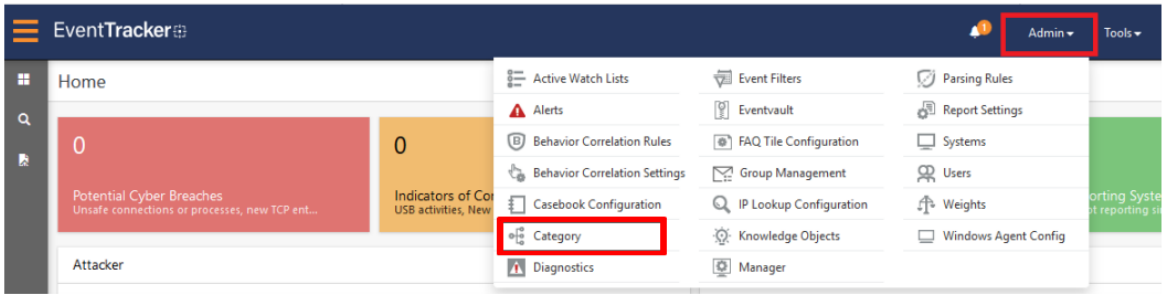


Figure 44

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

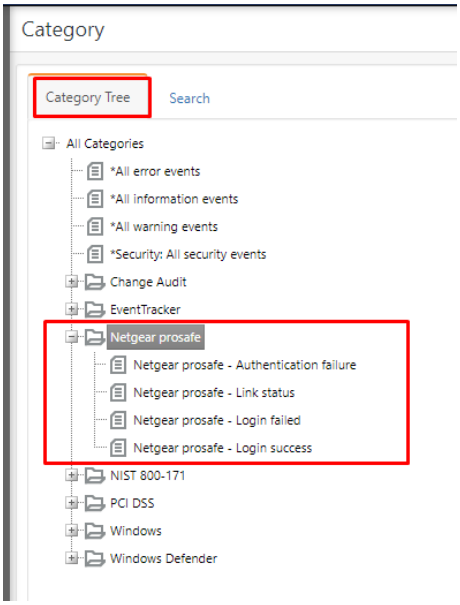


Figure 45

Dashboard

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

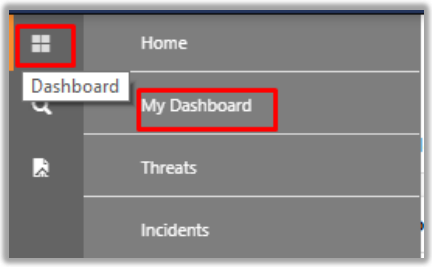


Figure 46

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

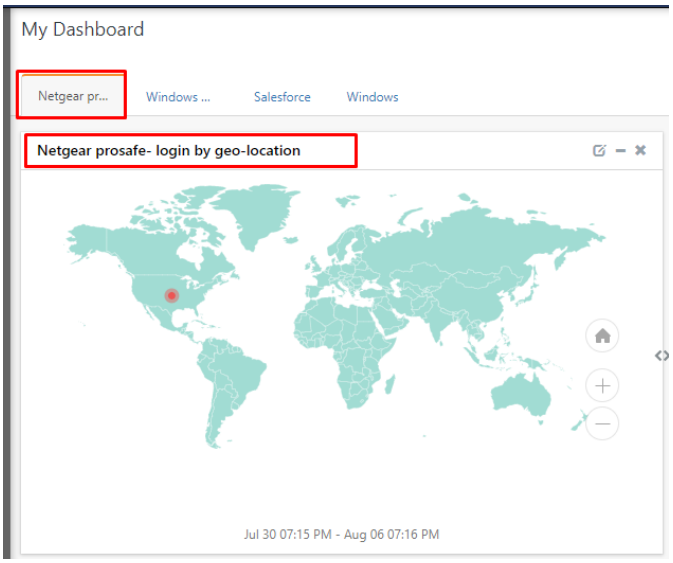

My Dashboard
Netgear pr...
Windows ...
Salesforce
Windows
Netgear prosafe- login by geo-location
Jul 30 07:15 PM - Aug 06 07:16 PM

Figure 47