Integration Guide

Integrating ntopng with EventTracker

EventTracker v9.2 and later

Publication Date:

April 30, 2021

Abstract

This guide helps you in configuring ntopng with EventTracker to receive ntopng events. In this guide, you will find the detailed procedures required for monitoring Ntopng.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 and later, ntopng v4.2.

Audience

Administrators who are assigned the task to monitor and manage ntopng events using EventTracker.

Table of Contents

1. Overview

ntopng is the next-generation version of the original ntop. It is a passive network monitoring tool focused on flows and statistics that can be obtained from the traffic captured by the server.

EventTracker integrates with ntopng using syslog. ntopng sends events information like alerts, web traffic activities, etc. EventTracker generates a detail reports for ,suspicious traffic activities, web traffic activities, etc. Its graphical representation shows web traffic activities source IP address, destination IP address, top accessed URL, etc.

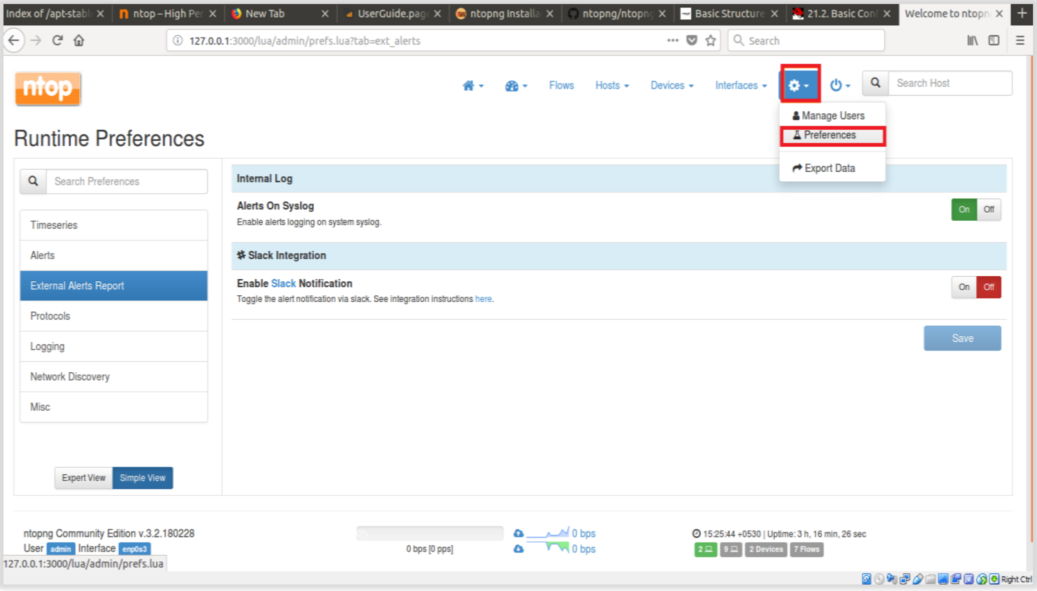
EventTracker triggers alerts in the event when suspicious traffic is detected by ntopng.

2. Prerequisites

- Admin access to ntopng web interface.
- Collect EventTracker IP address for log integration.
- Allow syslog server port 514 if any firewall exists between ntopng and EventTracker.

3. Integrating ntopng events to EventTracker server

1. Edit the rsyslog.conf file using the following command.
   vi /etc/rsyslog.conf
2. In the rsyslog.conf file scroll to the bottom and add the following line.
   If $programname == 'ntopng' then @eventtracker_ip:514
3. Launch ntopng Web Interface.
4. Hover over setting and select **Preferences**.



127.0.0.1:3000/lua/admin/prefs.lua?tab=ext_alerts

Runtime Preferences

Internal Log

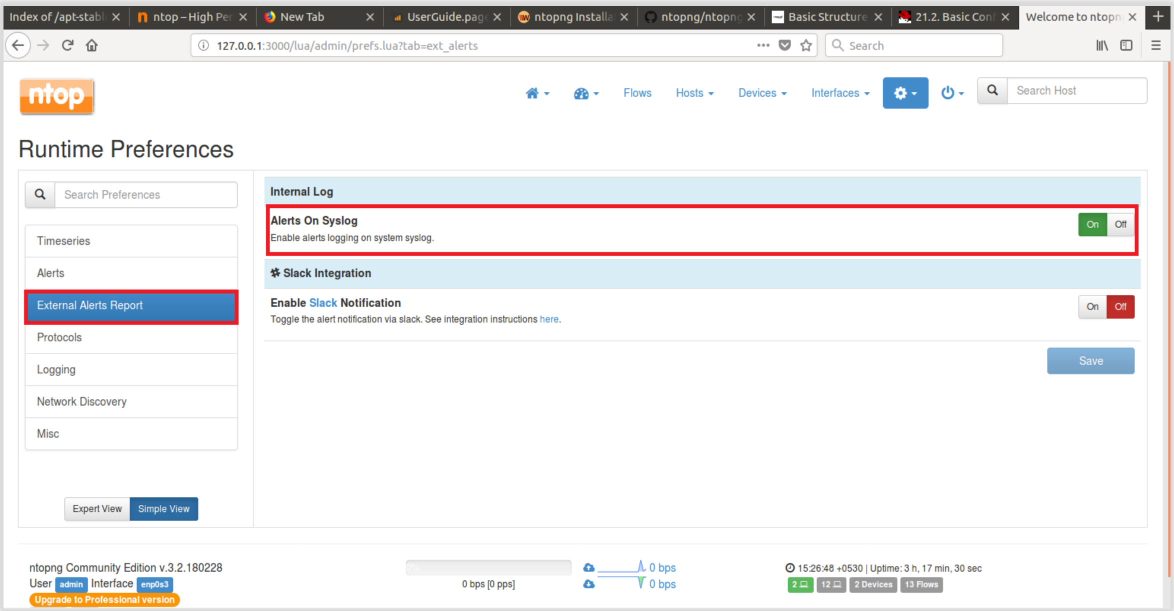
Alerts On Syslog: On
Enable alerts logging on system syslog.

Slack Integration

Enable Slack Notification: Off
Toggle the alert notification via slack. See integration instructions here.

ntopng Community Edition v.3.2.180228
User admin Interface enp0s3
0 bps [0 pps]
15:25:44 +0530 | Uptime: 3 h, 16 min, 26 sec
127.0.0.1:3000/lua/admin/prefs.lua

5. On the left-hand pane, select **External Alerts Report**.
6. Enable **Alerts on Syslog** option.



Runtime Preferences

Internal Log

Alerts On Syslog — On Off
Enable alerts logging on system syslog.

Slack Integration

Enable Slack Notification — On Off
Toggle the alert notification via slack. See integration instructions here.

ntopng Community Edition v.3.2.180228
User admin Interface enp0s3

15:26:48 +0530 | Uptime: 3 h, 17 min, 30 sec

4. EventTracker Knowledge Pack

Once logs are received into EventTracker; alerts, reports can be configured into EventTracker.

The following knowledge packs are available in EventTracker to support Windows.

4.1 Categories

Ntopng: Alert – This category provides information related to suspicious traffic activities like syn flood attack, syn flood victim, etc.

Ntopng: Web traffic activities – This category provides information related to web traffic activities accessed by user.

4.2 Alerts

Ntopng: Alert – This alert is generated whenever suspicious traffic activities are detected by Ntopng.

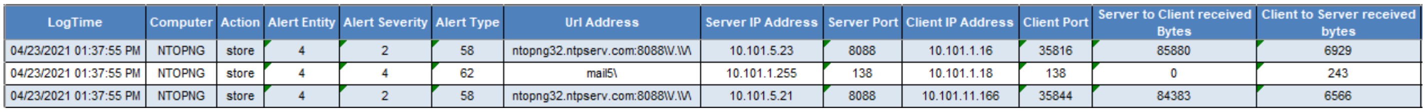
4.3 Reports

ntopng - Web traffic activities – This report provides information related to user accessed web traffic activities. It contains the field information like, source IP, source port, destination IP, destination port, URL, total bytes count bidirectional client and server, etc.

Log_Sample

```
Apr 16 07:25:09  vasdemo Apr 16 11:25:09  10.10.1.16  ntopng[12357]: {"alert_entity":4,"is_flow_alert":true,"flow_status":30,"cli_port":41486,"ifid":1,"srv_localhost":false,"pool_id":0,"cli_os":"Windows 10","alert_severity":2,"srv_blacklisted":false,"srv2cli_bytes":55859,"alert_tstamp":1618572309,"cli_asn":0,"srv_os":"","proto.ndpi":"HTTP","first_seen":1618572308,"l7_master_proto":7,"cli_localhost":true,"alert_json":"{\"info\":\"ntong32.pmusa.com:8088\\/.\\/.\\/\",\"status_info\":\"{\\\"ntopng.key\\\":348827202,\\\"cli2srv.packets\\\":30,\\\"srv.localhost\\\":false,\\\"cli.ip\\\":\\\"10.10.1.16\\\",\\\"srv2cli.packets\\\":50,\\\"srv.port\\\":8088,\\\"hash_entry_id\\\":2135264,\\\"cli.port\\\":41486,\\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\\"proto.ndpi\\\":\\\"HTTP\\\",\\\"proto.l4\\\":\\\"TCP\\\",\\\"info\\\":\\\"r1p1s3vm10.prismusa.com:8088\\/.\\/.\\/\\\",\\\"alert_generation\\\":{\\\"script_key\\\":\\\"flow_risks\\\",\\\"confset_id\\\":0,\\\"subdir\\\":\\\"flow\\\"},\\\"proto.ndpi_cat\\\":\\\"Web\\\",\\\"cli.localhost\\\":true,\\\"duration\\\":1,\\\"srv2cli.bytes\\\":55859,\\\"cli2srv.bytes\\\":4411,\\\"srv.ip\\\":\\\"10.10.5.21\\\"}\"}","score":150,"srv_addr":"10.101.5.213","action":"store","cli2srv_packets":30,"cli_addr":"10.10.1.16","cli_blacklisted":false,"alert_type":58,"cli2srv_bytes":4411,"l7_proto":7,"vlan_id":0,"srv_port":8088,"cli_country":"","srv_asn":0,"proto":6,"alert_entity_val":"flow","srv_country":"","srv2cli_packets":50}
```

Sample_report



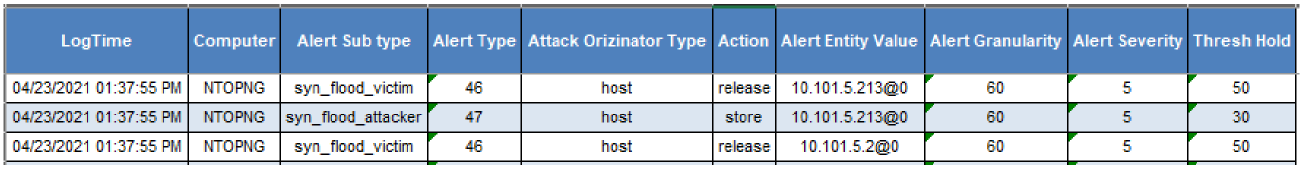
LogTime	Computer	Action	Alert Entity	Alert Severity	Alert Type	Url Address	Server IP Address	Server Port	Client IP Address	Client Port	Server to Client received Bytes	Client to Server received bytes
04/23/2021 01:37:55 PM	NTOPNG	store	4	2	58	ntopng32.ntpserv.com:8088\\/.\\/\	10.101.5.23	8088	10.101.1.16	35816	85880	6929
04/23/2021 01:37:55 PM	NTOPNG	store	4	4	62	mail5\	10.101.1.255	138	10.101.1.18	138	0	243
04/23/2021 01:37:55 PM	NTOPNG	store	4	2	58	ntopng32.ntpserv.com:8088\\/.\\/\	10.101.5.21	8088	10.101.11.166	35844	84383	6566

ntopng – Alerts details – This report provides information related to suspicious traffic detected on hosts. It contains the fields information like, attack type, alert type, action, entity value, alert severity, etc.

Log_Sample:

```
Apr 16 07:25:09  etvasdemo Apr 16 11:25:09  10.10.1.16 ntopng[12357]: {"alert_tstamp_end":1618572307,"alert_type":46,"alert_subtype":"syn_flood_victim","alert_granularity":60,"alert_entity_val":"10.101.15.21@0","alert_json":"{\"value\":386,\"operator\":\"gt\",\"alert_generation\":{\"confset_id\":0,\"script_key\":\"syn_flood_victim\",\"subdir\":\"host\"},\"threshold\":50,\"metric\":\"syn_flood_victim\"}","alert_entity":1,"alert_severity":5,"pool_id":0,"alert_tstamp":1618572307,"ifid":1,"action":"engage"}
```

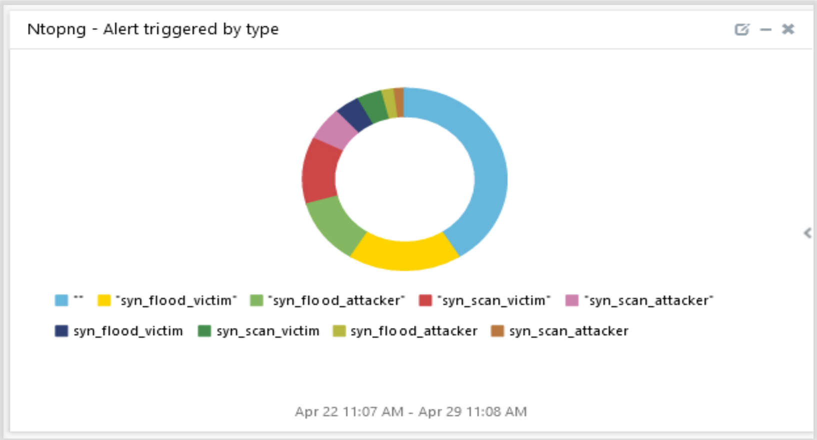
Sample_Report:



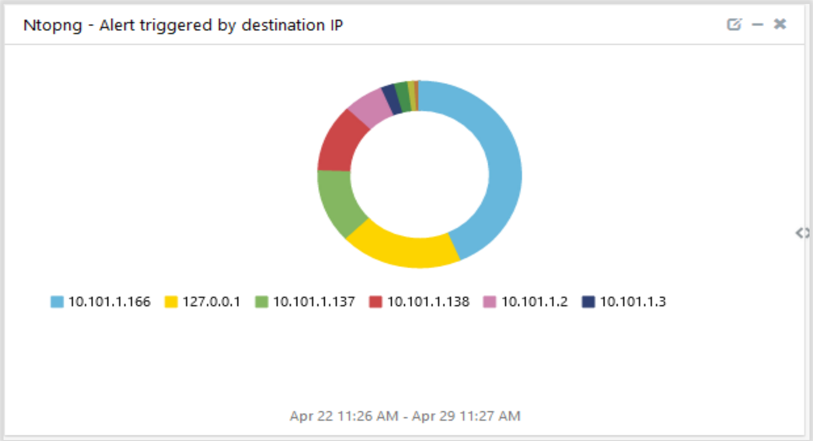
LogTime	Computer	Alert Sub type	Alert Type	Attack Orizinator Type	Action	Alert Entity Value	Alert Granularity	Alert Severity	Thresh Hold
04/23/2021 01:37:55 PM	NTOPNG	syn_flood_victim	46	host	release	10.101.5.213@0	60	5	50
04/23/2021 01:37:55 PM	NTOPNG	syn_flood_attacker	47	host	store	10.101.5.213@0	60	5	30
04/23/2021 01:37:55 PM	NTOPNG	syn_flood_victim	46	host	release	10.101.5.2@0	60	5	50

4.4 Dashboards

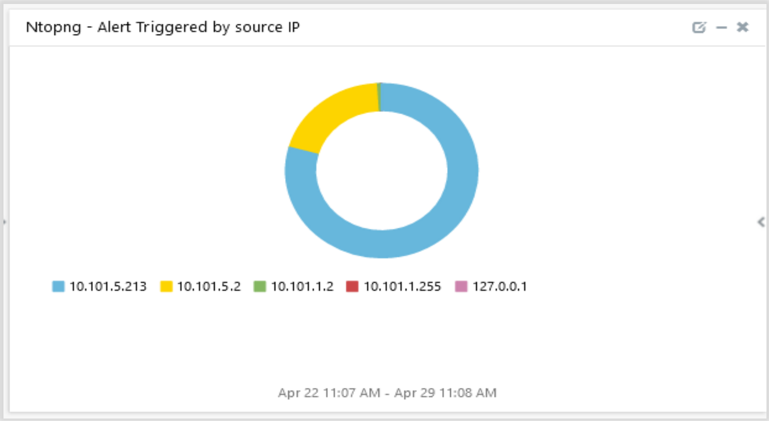
- **ntopng - Alert triggered by type**



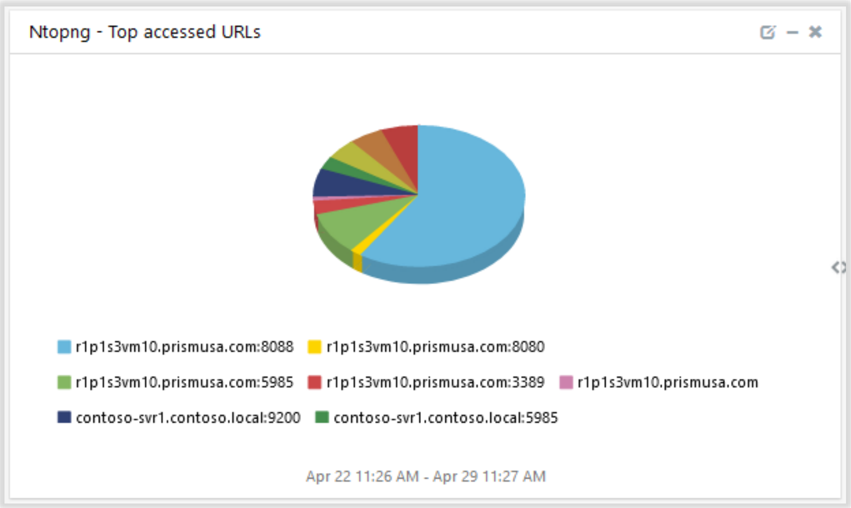
- **ntopng - Alert triggered by destination IP**



- **ntopng - Alert triggered by server IP**



- **ntopng - Top accessed URLs**

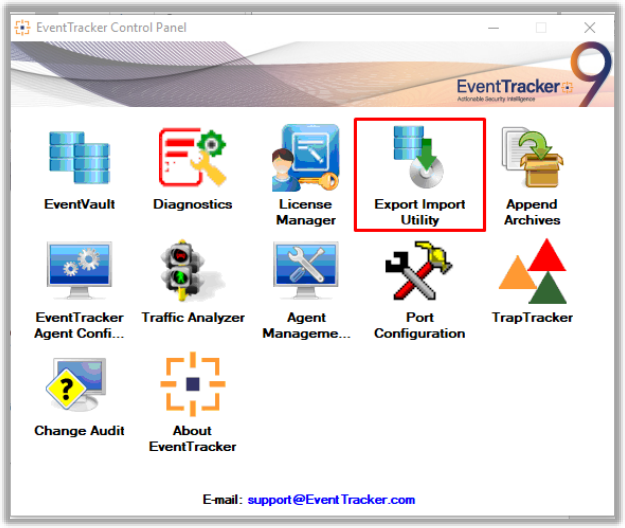


5. Importing Knowledge Pack into EventTracker

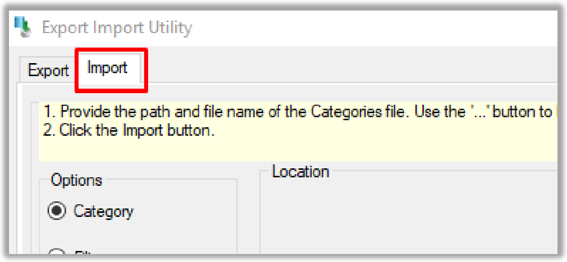
NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Template/Parsing Rule
- Flex Reports
- Knowledge Objects
- Dashboards

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



Export-Import Utility window opens.

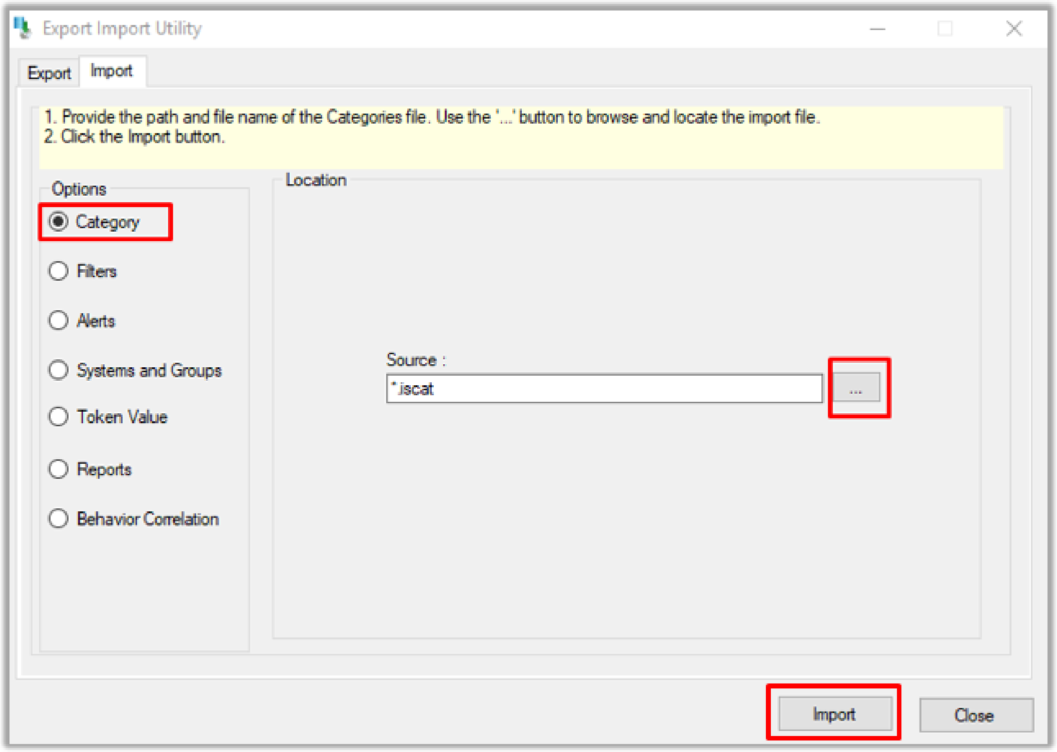


1. Provide the path and file name of the Categories file. Use the '...' button to
2. Click the Import button.

3. Click the **Import** tab.

5.1 Categories

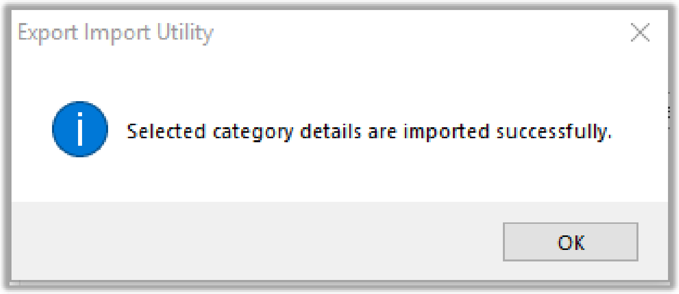
1. In **Export-Import Utility** window, select the **Category** option, and click **Browse** . ...
2. Navigate to the knowledge pack folder and select the file with the extension **".iscat",** like **Categories_Ntopng. iscat** and click **Import**.



1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Source : *.iscat

EventTracker displays a success message.

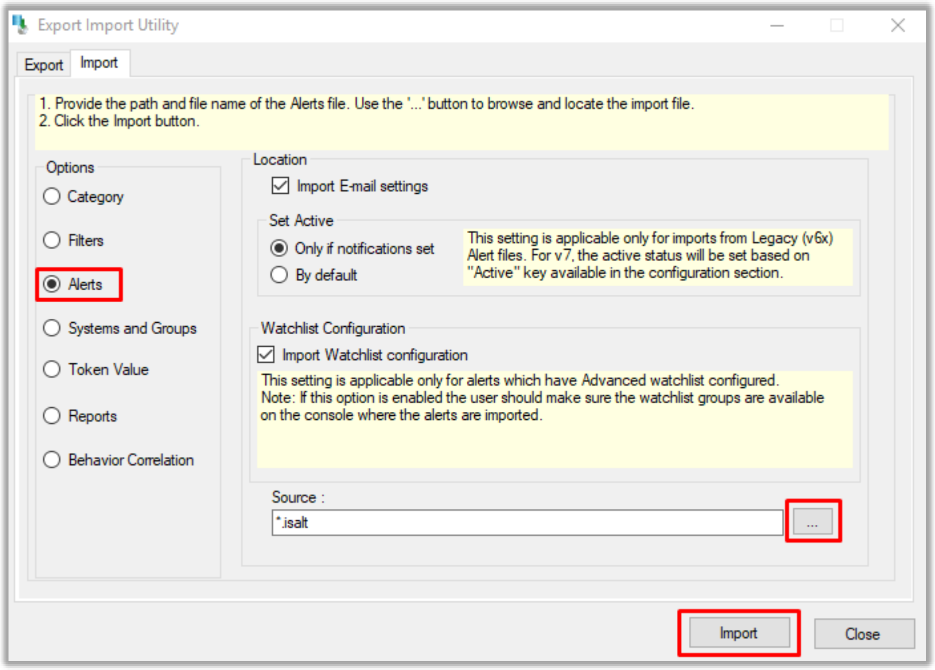


Export Import Utility

Selected category details are imported successfully.

5.2 Alerts

1. In **Export-Import Utility** window , select the **Alert** option and click **Browse**.
2. Navigate to the knowledge pack folder and select the file with the extension **".isalt**", **e.g.**, "**Alerts_ Ntopng.isalt**" and click **Import**.



1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options
○ Category
○ Filters
● Alerts
○ Systems and Groups
○ Token Value
○ Reports
○ Behavior Correlation

Location
☑ Import E-mail settings

Set Active
● Only if notifications set
○ By default

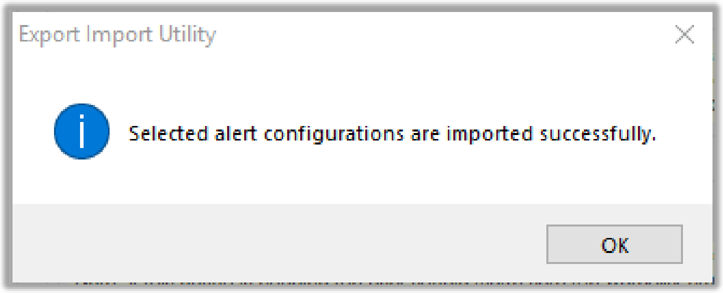
This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Watchlist Configuration
☑ Import Watchlist configuration

This setting is applicable only for alerts which have Advanced watchlist configured.
Note: If this option is enabled the user should make sure the watchlist groups are available on the console where the alerts are imported.

Source : *.isalt

EventTracker displays a success message.



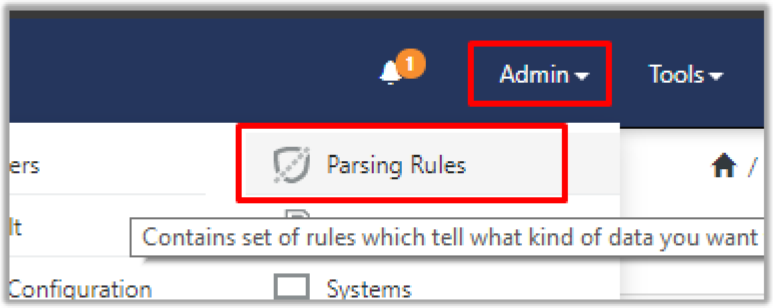
Export Import Utility

Selected alert configurations are imported successfully.

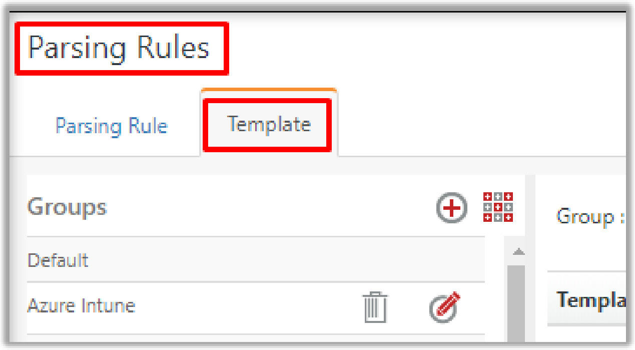
5.3 Token Template

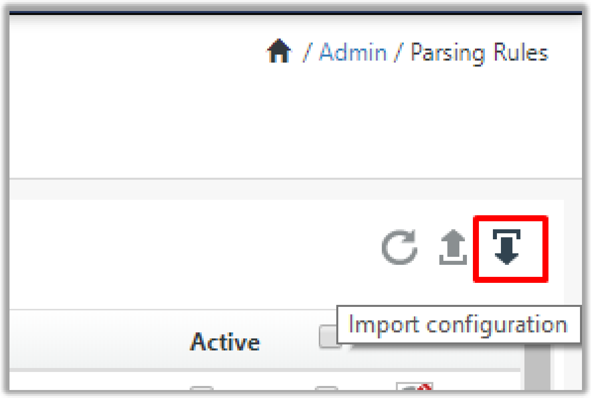
For importing **Token Template**, navigate to the **EventTracker manager** web interface.

1. Click **Parsing Rules** under the **Admin** option in the EventTracker manager web interface.

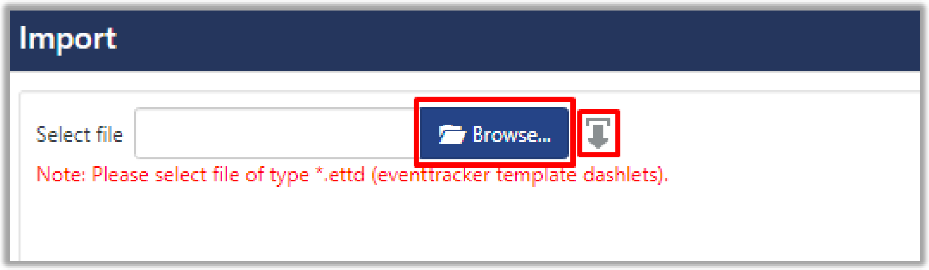


2. Click the **Template** tab and then click the **Import Configuration** button.





3. Click the **Browse** button and navigate to the knowledge packs folder (type **C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs**” in the navigation bar) where **“.ettd”, e.g., “Templates_Ntopng.ettd”** file is located. Wait for a few seconds, as templates will be loaded. Once you see the templates, click desired templates, and click **Import** button:

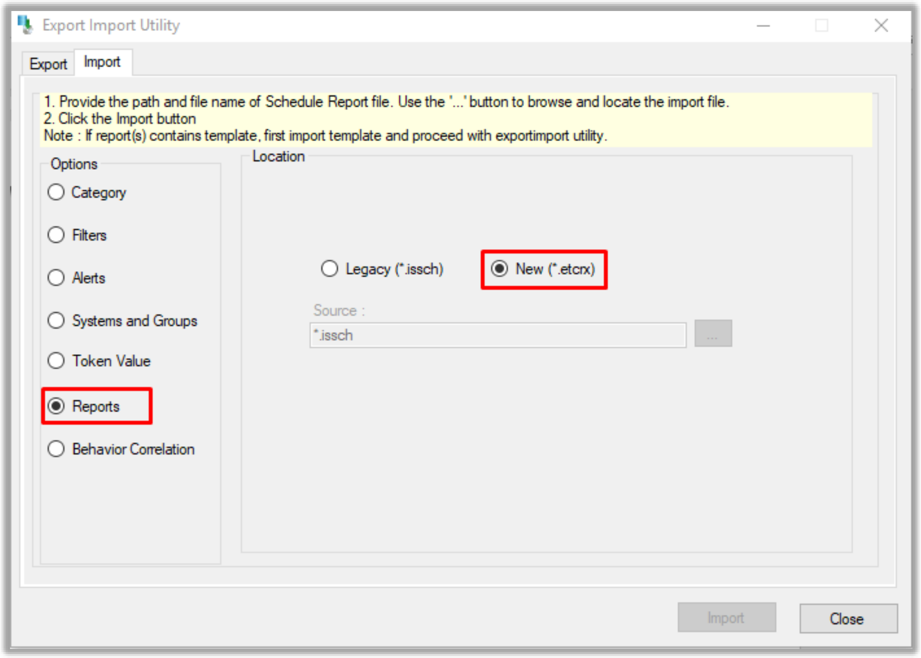


Select file

Note: Please select file of type *.ettd (eventtracker template dashlets).

5.4 Flex Reports

1. In **Export-Import Utility** window, select the **Import tab**. Click the **Reports** option, and choose **New (*.etcrx)**.



1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

Options

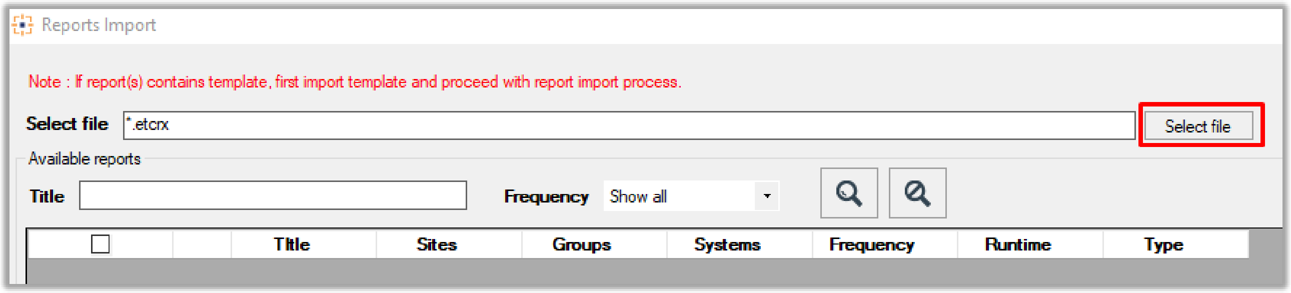
○ Category
○ Filters
○ Alerts
○ Systems and Groups
○ Token Value
● Reports
○ Behavior Correlation

Location

○ Legacy (*.issch) ● New (*.etcrx)

Source : *.issch

2. A new pop-up window appears. Click the **Select File** button and navigate to the knowledge pack folder and select file with the extension **".etcrx", e.g., "Reports_Ntopng.etcrx".**



Note : If report(s) contains template, first import template and proceed with report import process.

Select file *.etcrx

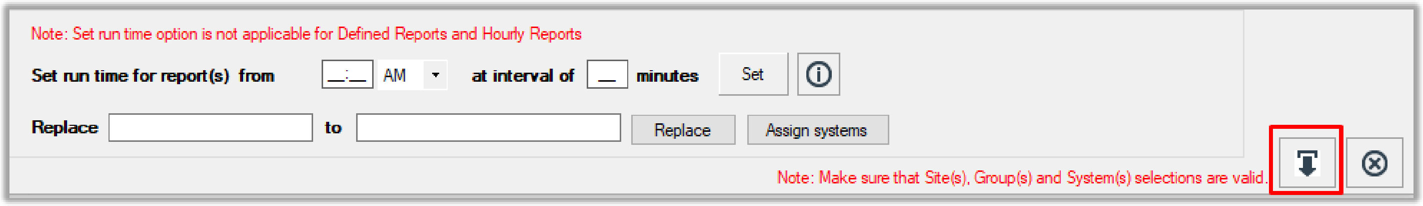
Available reports

Title

Frequency Show all

□	Title	Sites	Groups	Systems	Frequency	Runtime	Type

3. Wait while reports populate. Select all the relevant reports and click **Import** .



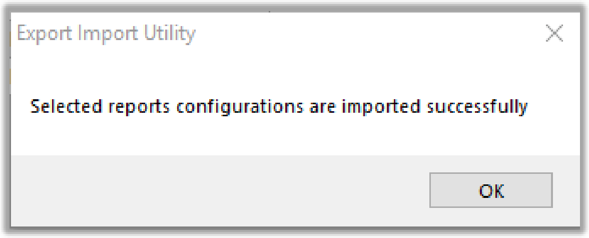
Note: Set run time option is not applicable for Defined Reports and Hourly Reports

Set run time for report(s) from __:__ AM at interval of __ minutes

Replace __ to __

Note: Make sure that Site(s), Group(s) and System(s) selections are valid.

EventTracker displays a success message.

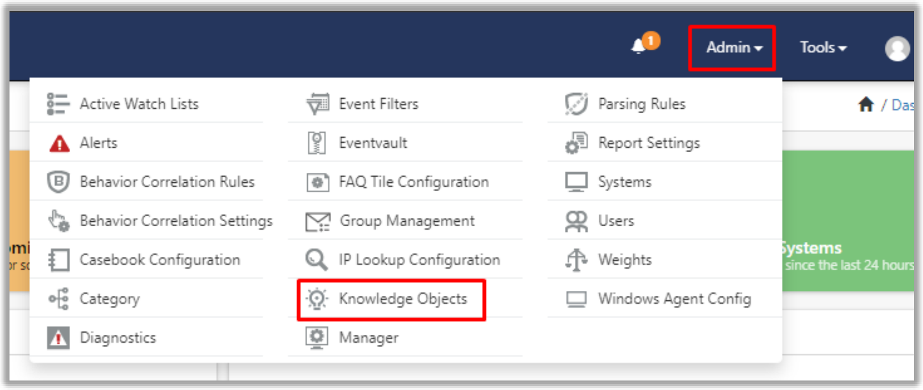


Export Import Utility

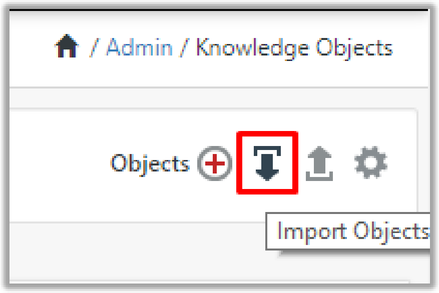
Selected reports configurations are imported successfully

5.5 Knowledge Objects

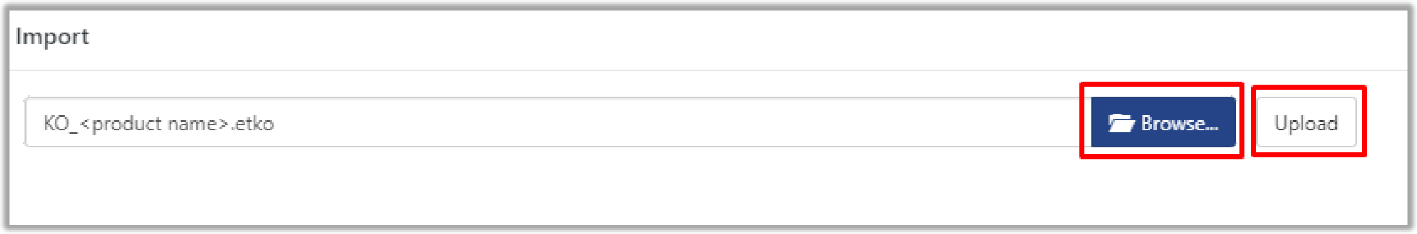
1. Click **Knowledge objects** under the **Admin** option in the EventTracker web interface.



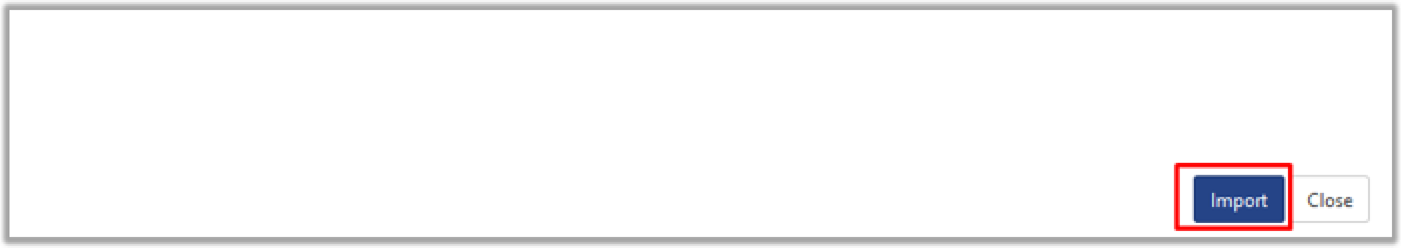
2. Click the **import object** icon.



3. A pop-up box appears, click **Browse** and navigate to the knowledge packs folder (type "**C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs**" in the navigation bar) with the extension **".etko", e.g., "KO_Ntopng.etko"** and click **Upload**.

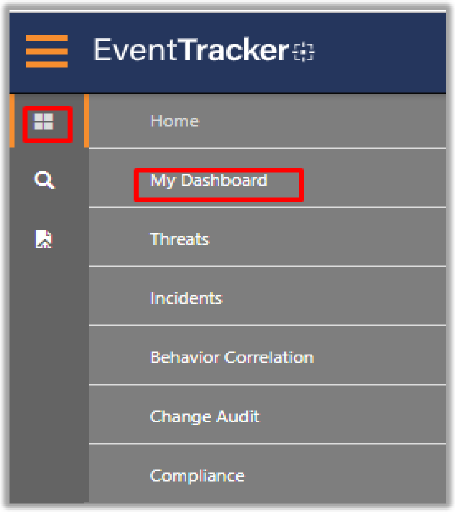


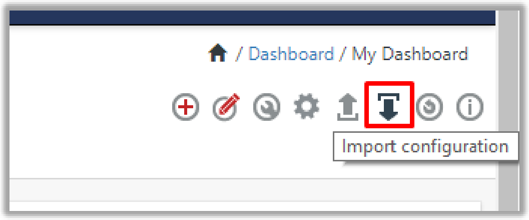
4. Wait while EventTracker populates all the relevant knowledge objects. Once the objects are displayed, select the required ones, and click **Import**.



5.6 Dashboards

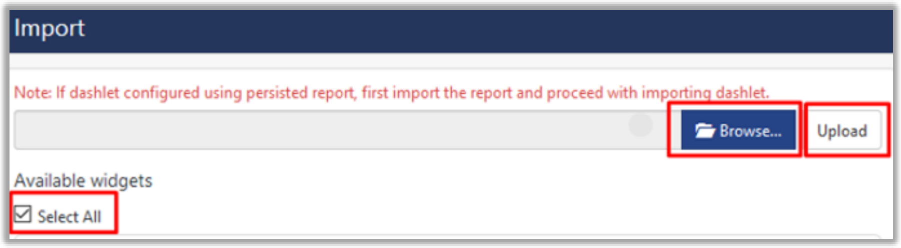
1. Login to the **EventTracker web interface**.
2. Navigate to **Dashboard** → **My Dashboard**.
3. In **My Dashboard**, Click the **Import** button**.**



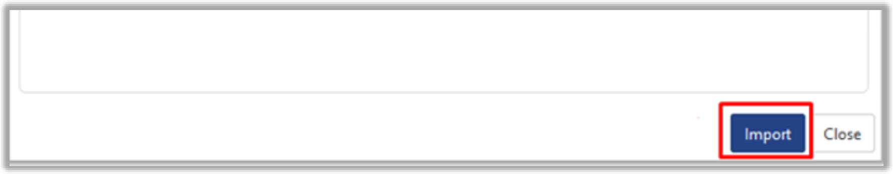


4. Click **Browse** and navigate to the knowledge pack folder (type **"C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs"** in the navigation bar) where "**.etwd**", **e.g.,** "**Dashboard_Ntopng.etwd**" is saved and click **Upload**.

5. Wait while EventTracker populates all the available dashboards. Enable **Select All** and click **Import**.


Import

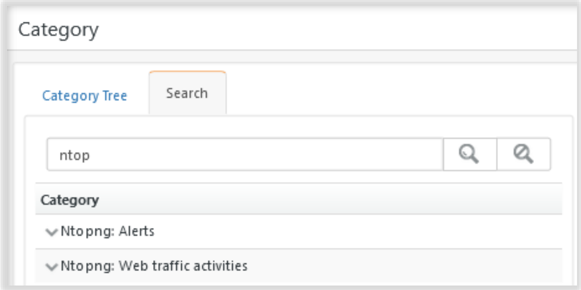
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.



6. Verifying Knowledge Pack in EventTracker

6.1 Categories

1. Login to the **EventTracker web interface**.
2. Click **Admin** dropdown and click **Categories**.
3. In **Category Tree** to view imported categories, click the **Search** tab and enter **ntopng** in the search**.**


Category

ntop

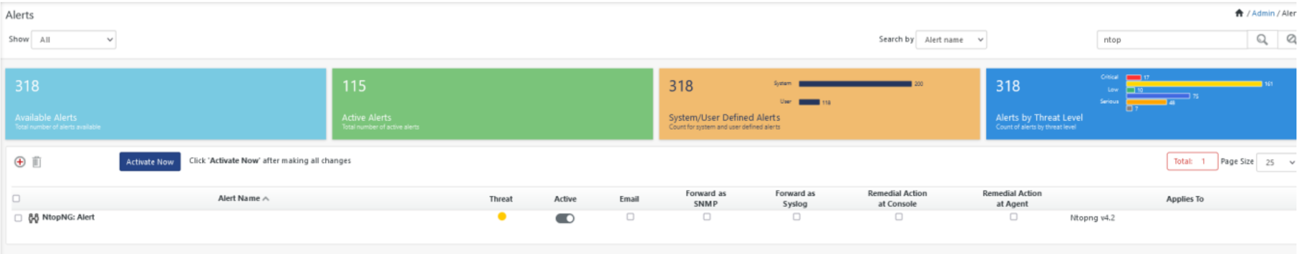
Category

Ntopng: Alerts

Ntopng: Web traffic activities

6.2 Alerts

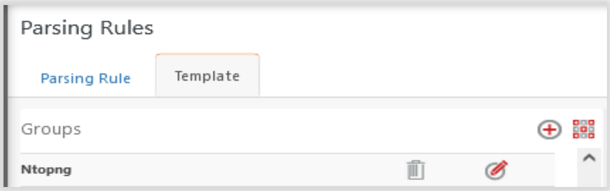
1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Alerts.**
2. In search box enter **ntopng** and click **Search**.
   EventTracker displays an alert related to Ntopng**.**


Alerts
/ Admin / Aler
Show All
Search by Alert name
ntop
318
Available Alerts
Total number of alerts available
115
Active Alerts
Total number of active alerts
318
System/User Defined Alerts
Count for system and user defined alerts
System 200
User 118
318
Alerts by Threat Level
Count of alerts by threat level
Critical 17
161
Low 10
75
Serious 48
7
Activate Now
Click 'Activate Now' after making all changes
Total: 1
Page Size 25

□	Alert Name	Threat	Active	Email	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
□	NtopNG: Alert	●	●	□	□	□	□	□	Ntopng v4.2

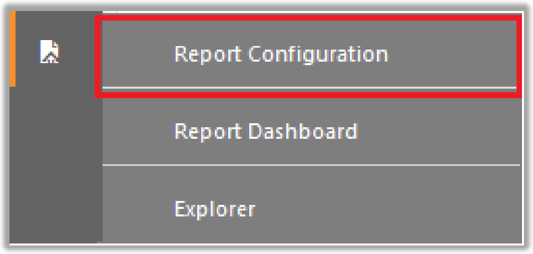
6.3 Token Template

1. In the EventTracker web interface, click the Admin dropdown, and then click **Parsing Rules**.
2. In the **Template** tab, click on the **ntopng** group folder to view the imported Token.

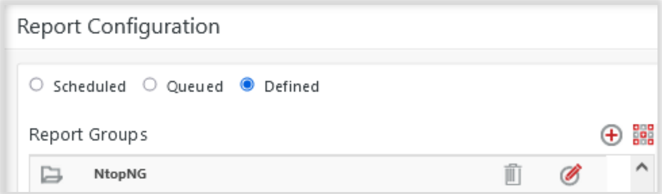


6.4 Flex Reports

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



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



Report Configuration

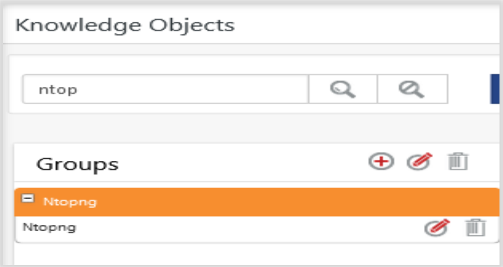
○ Scheduled ○ Queued ● Defined

Report Groups

NtopNG

6.5 Knowledge Objects

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects.**
2. In the **Knowledge Object** tree, expand the **ntopng** group folder to view the imported Knowledge objects.



Knowledge Objects

ntop

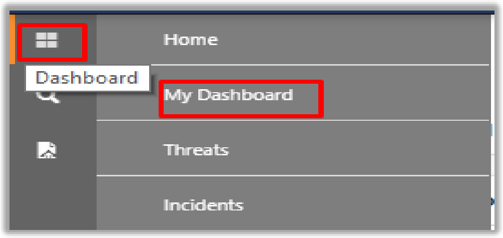
Groups

Ntopng

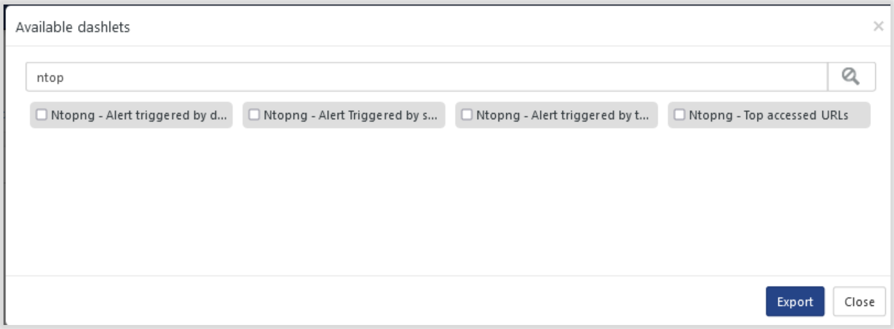
Ntopng

6.6 Dashboards

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



2. In the **ntopng** dashboard you see the following screen.



Available dashlets

ntop

□ Ntopng - Alert triggered by d... □ Ntopng - Alert Triggered by s... □ Ntopng - Alert triggered by t... □ Ntopng - Top accessed URLs

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #19 among MSSP Alert's 2020 Top 250 MSSPs.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support