EventTracker

Actionable Security Intelligence

Integrate Ntopng

EventTracker v8.x and above

Publication Date: March 12, 2018

Abstract

This guide provides instructions to forward syslog generated by Ntopng to EventTracker. EventTracker is configured to collect and parse these logs to generate reports.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.x and later, and Ntopng.

Audience

IT Admins, Ntopng administrators and EventTracker users who wish to forward logs to EventTracker Manager and monitor events using Event Tracker Enterprise.

Table of Contents

Overview

Ntopng is the next generation version of the original ntop. It is 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 and provides reports and knowledge objects using the Alerts generated by Ntopng.

Prerequisites

- EventTracker v8.x or above should be installed.
- Allow port 514.

Configure Ntopng to forward logs to EventTracker

Ntopng supports forwarding logs to EventTracker via syslog.

Configuration to enable Syslog forwarding

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

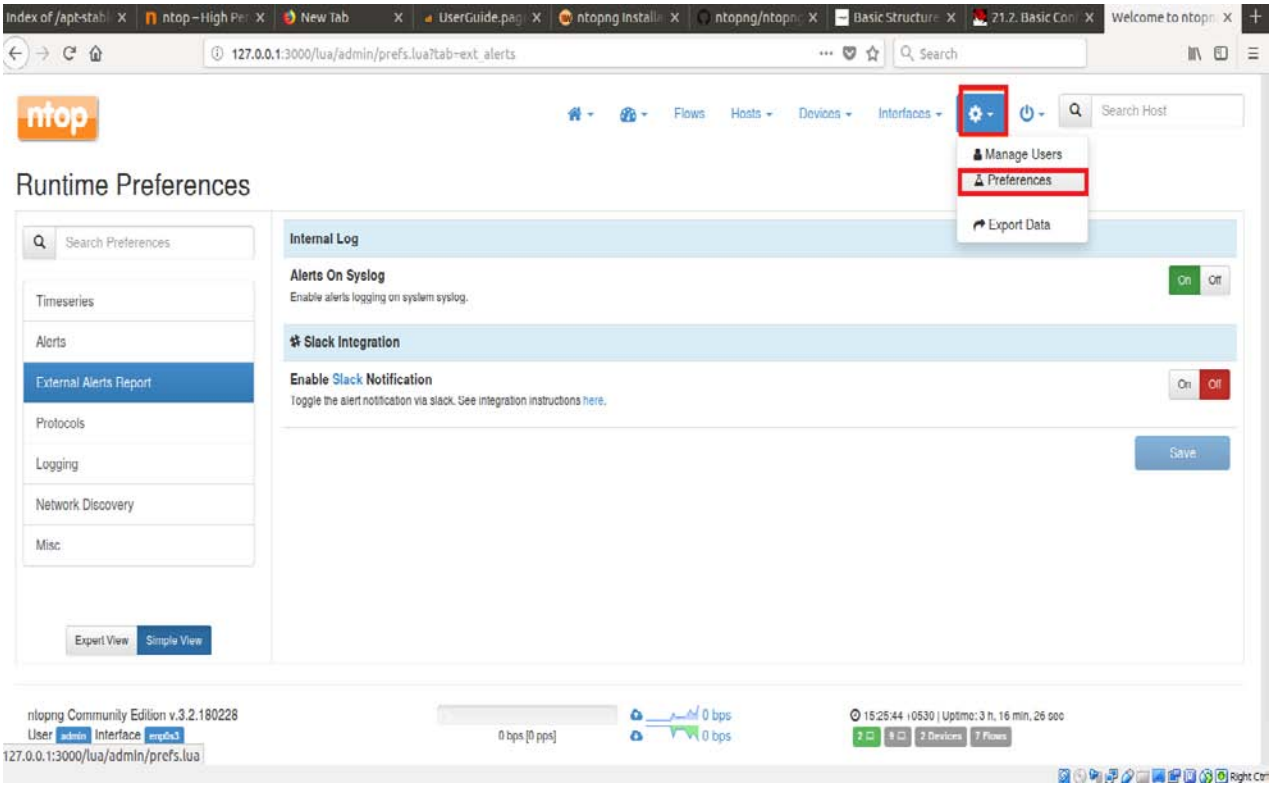

Figure 1

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

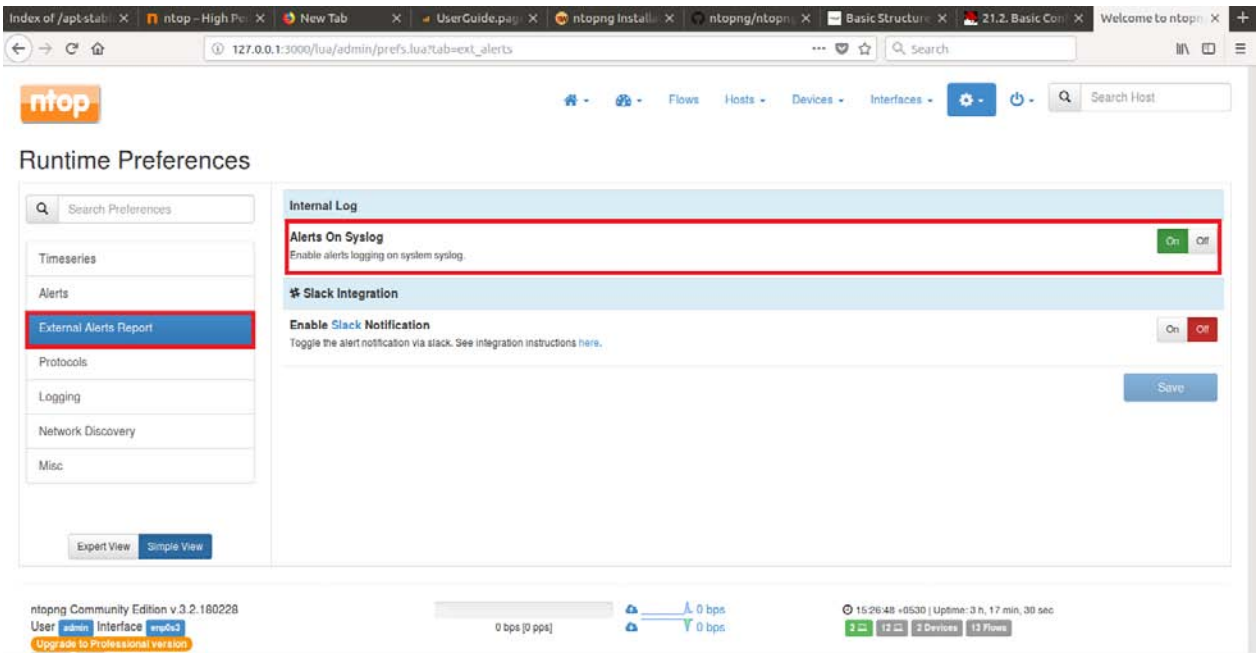

Figure 2

EventTracker Knowledge Pack (KP)

Once logs are received into EventTracker, Categories and Reports can be configured into EventTracker. The following Knowledge Packs are available in EventTracker Enterprise.

Alert

- **Ntopng -Alert:** The KO provides details about the alterable events recognized by Ntopng. Alerts are generated by Ntopng usually when suspicious event is detected.

Reports

- **Ntopng -Alert:** This report provides information regarding the activities that trigged the alert.

Time	Alert Type	Source Name	Source IP	Source Port	Protocol	Destination Name	Destination IP	Destination Port
Feb 08 02:33:30	is a Flooder	192.168.1.1	192.168.1.1					
Feb 08 02:32:30	is under flood attack	netflix.com	192.168.1.2					
Feb 06 07:49:29	TCP connection refused	stackoverflow.com	192.168.1.3	55065	TCP	netflix.com	192.168.1.50	23
Feb 08 02:32:30	is under flood attack	192.168.1.6	192.168.1.2					
Feb 06 07:49:29	TCP connection refused	amazon.in	192.168.1.3	55065	TCP	iis.net	192.168.3.2	23
Feb 08 02:32:30	is under flood attack	iis.net	192.168.1.2					

Figure 3

Figure 4

Import Knowledge Pack into EventTracker

Import knowledge pack items in the following sequence:

- Categories
- Knowledge Objects
- Alerts

• Token Templates
• Flex Reports

Import Categories

- Select **Export Import Utility**.

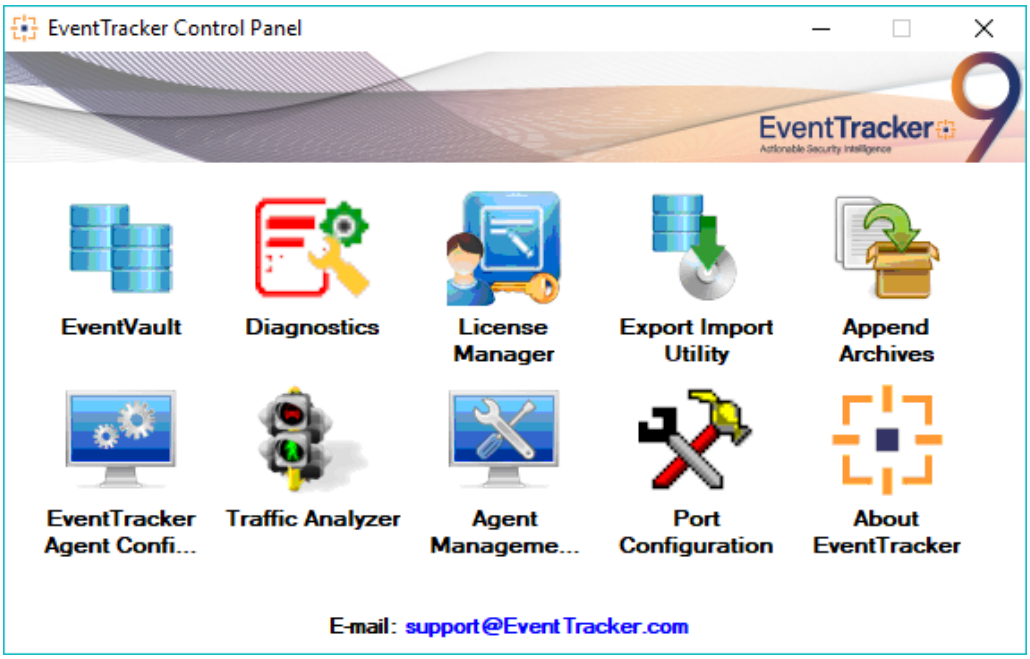

Figure 5

- Click **Category** option, and then click the browse  button.

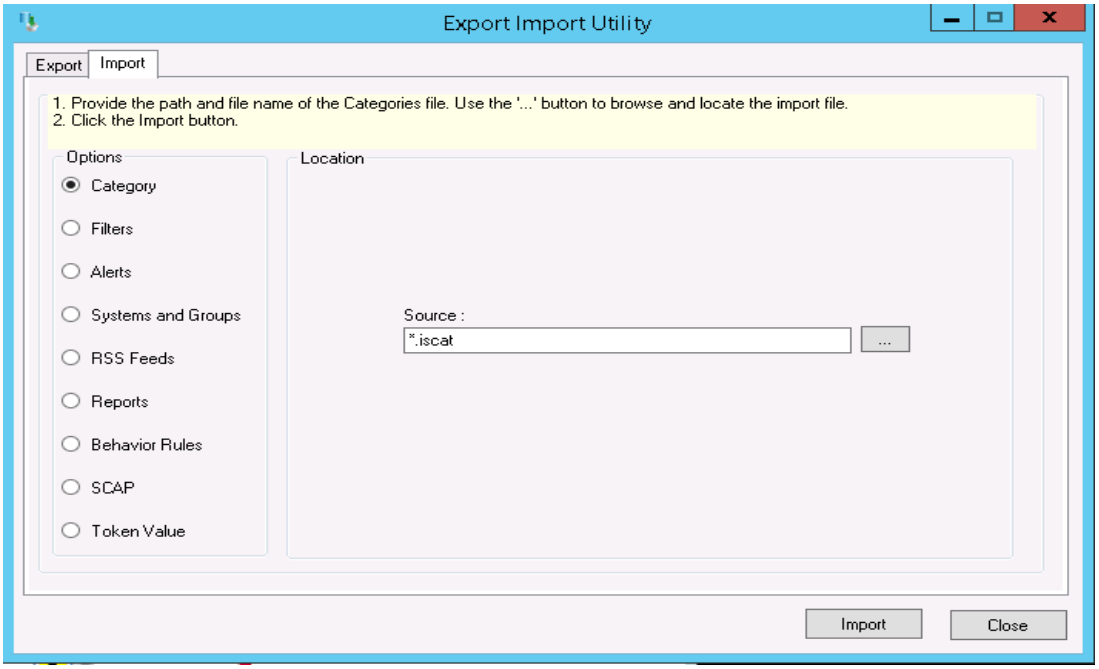

Figure 6

- Locate the .iscat file, and then click the **Open** button.
- To import categories, click the **Import** button.

EventTracker displays success message.

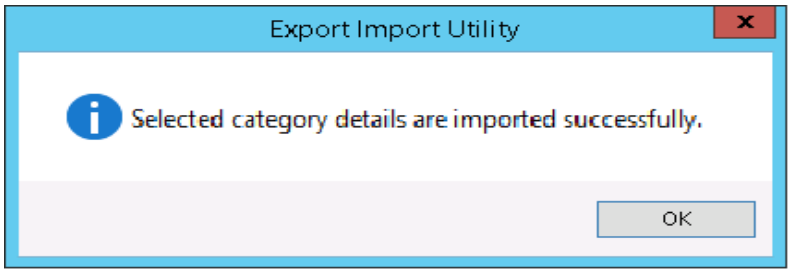

Figure 7

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

Import Knowledge Objects

- Click **Knowledge objects** under **Admin** option in the EventTracker Manager page.
- Click the icon to import Knowledge Objects.
- Locate the **KO_NtopNG syslog.etko** file

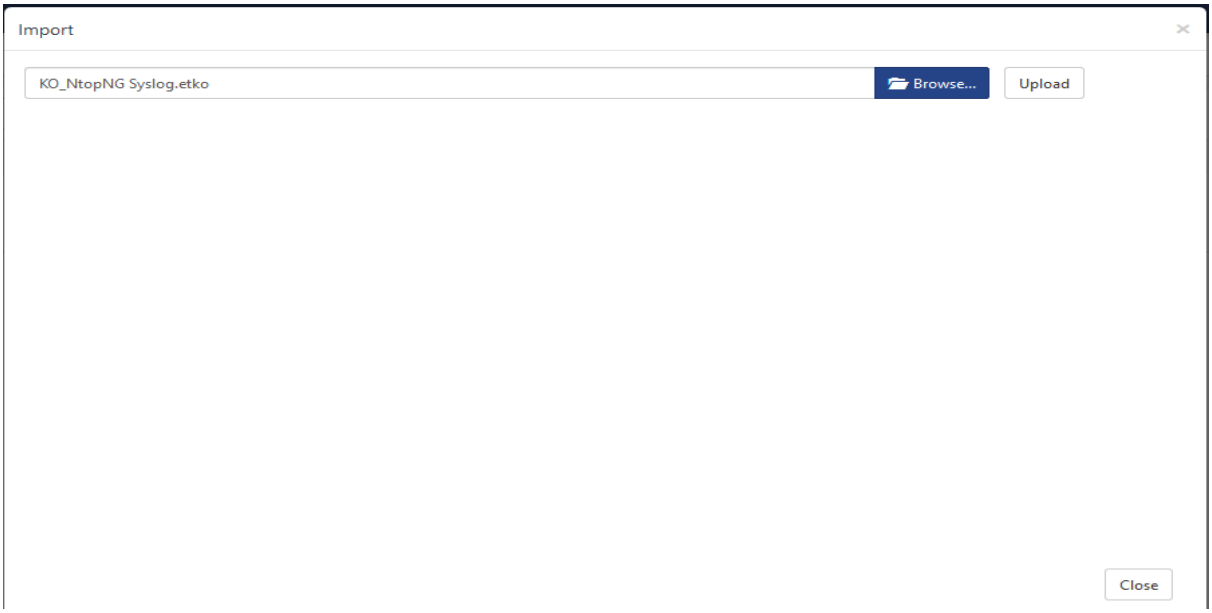

Figure 8

- Now select all the files and then click on **Upload**.

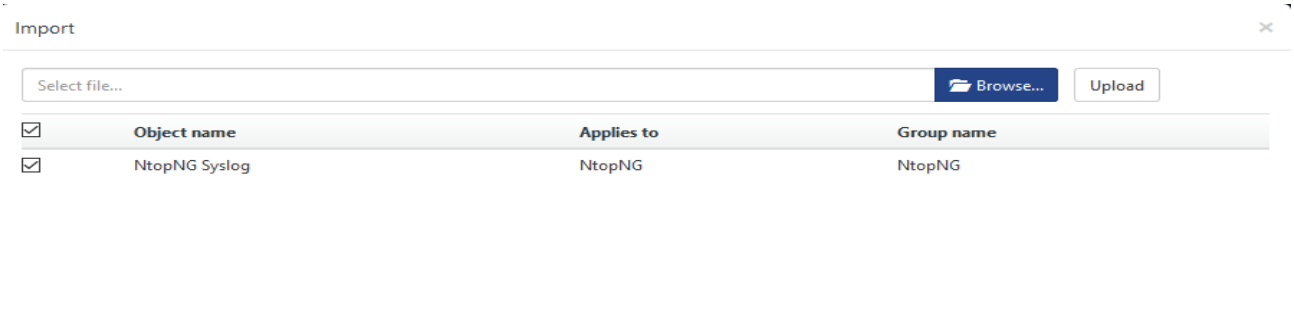

Figure 9

- Knowledge objects are now imported successfully.

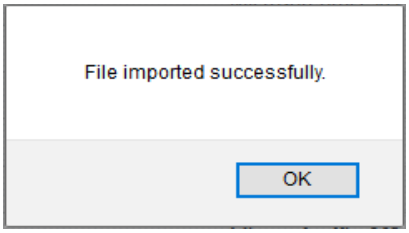

Figure 10

Import Alerts

- Select **Export Import Utility**.

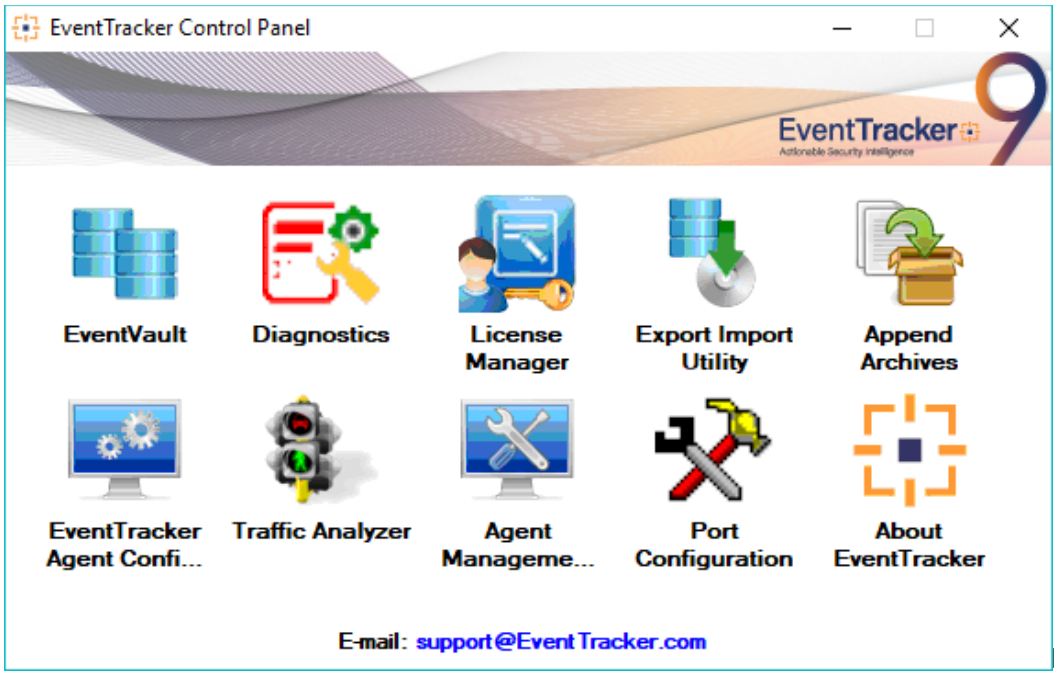

Figure 11

- In the **Import** tab,select **Alerts** in the Left pane.
- Now browse and locate the **NtopNG.isat** and click **Import** .

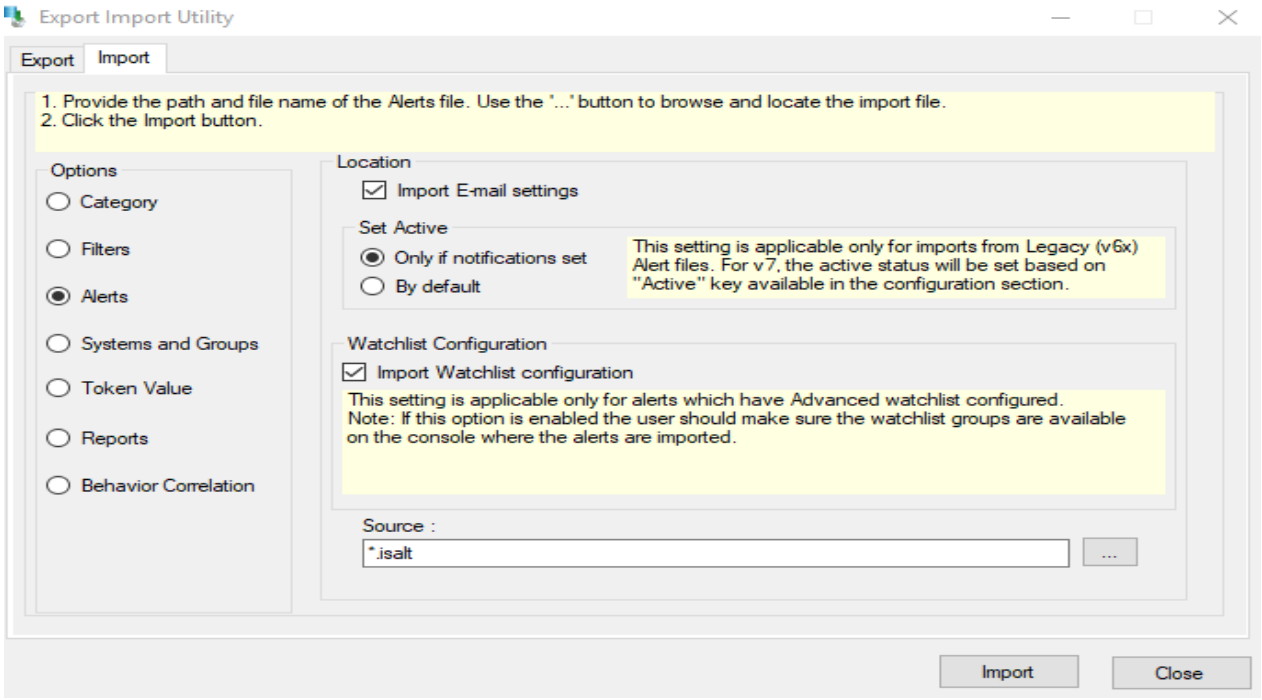

Figure 12

- Alerts are now imported successfully.

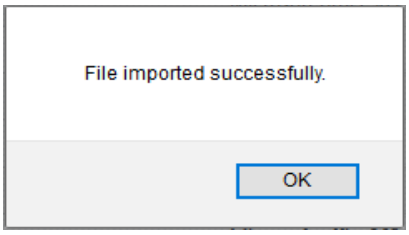

Figure 13

Import Token Templates

- Logon to **EventTracker Enterprise**.
- Click the **Admin** menu, and then click **Parsing Rules**.
- Select **Template** tab, browse and select the **NtopNG.ettd** file
- Click on the **Import** icon.

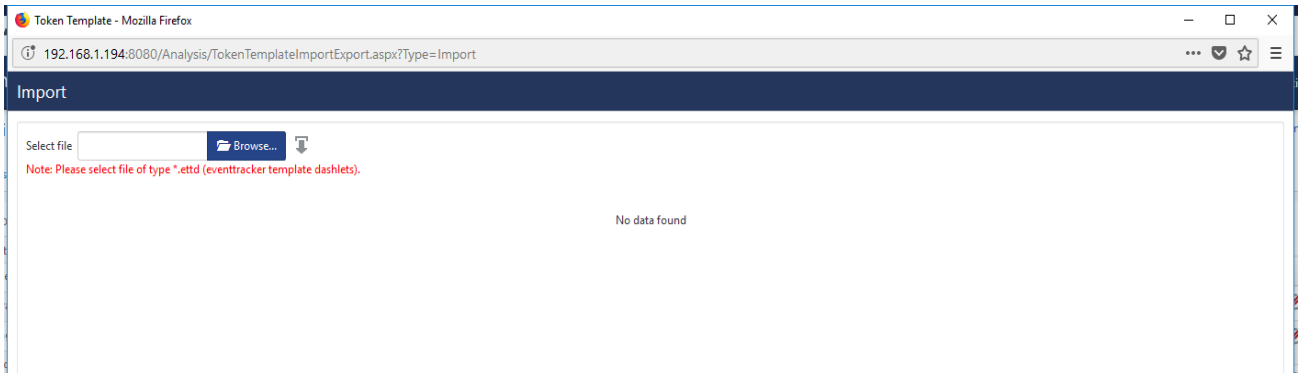

Figure 14

- Templates are now imported successfully.

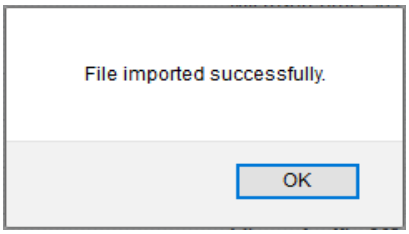

Figure 15

Import Flex Reports

- Select **Export Import Utility**.

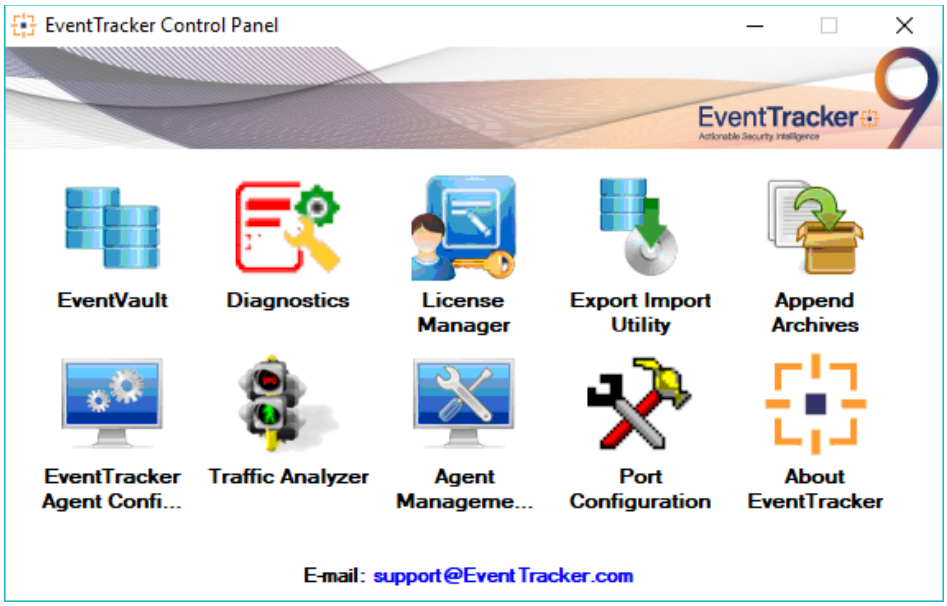

Figure 16

- Click **Reports** option, and select new (.etcrx) from the option.

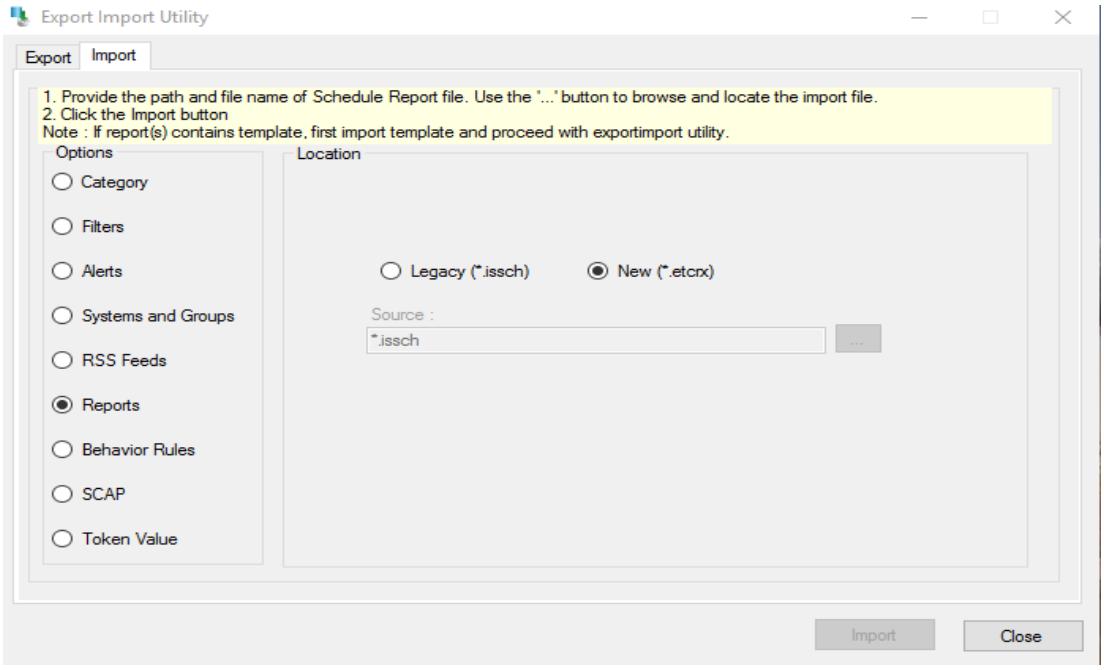

Figure 17

- And then click the browse  button.

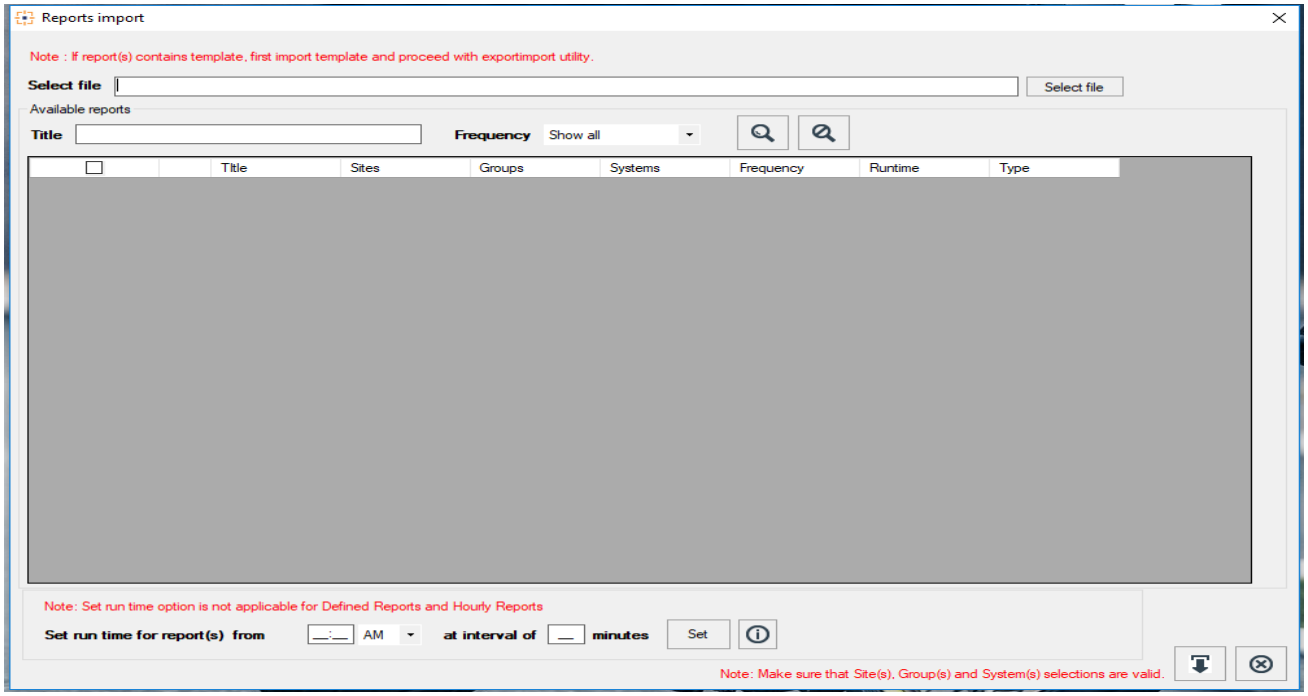

Figure 18

- Locate the file named **FlexReports_Ntopng.etcrx** and select all the check box.
- Click the **Import** button to import the reports. EventTracker displays success message.

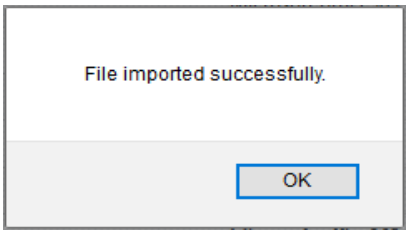

Figure 19

Verify Knowledge Pack in EventTracker

Verify Category

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Category**.
3. In **Category Group Tree** to view imported category, scroll down and click **Ntopng** group folder.

Category are displayed in the pane.

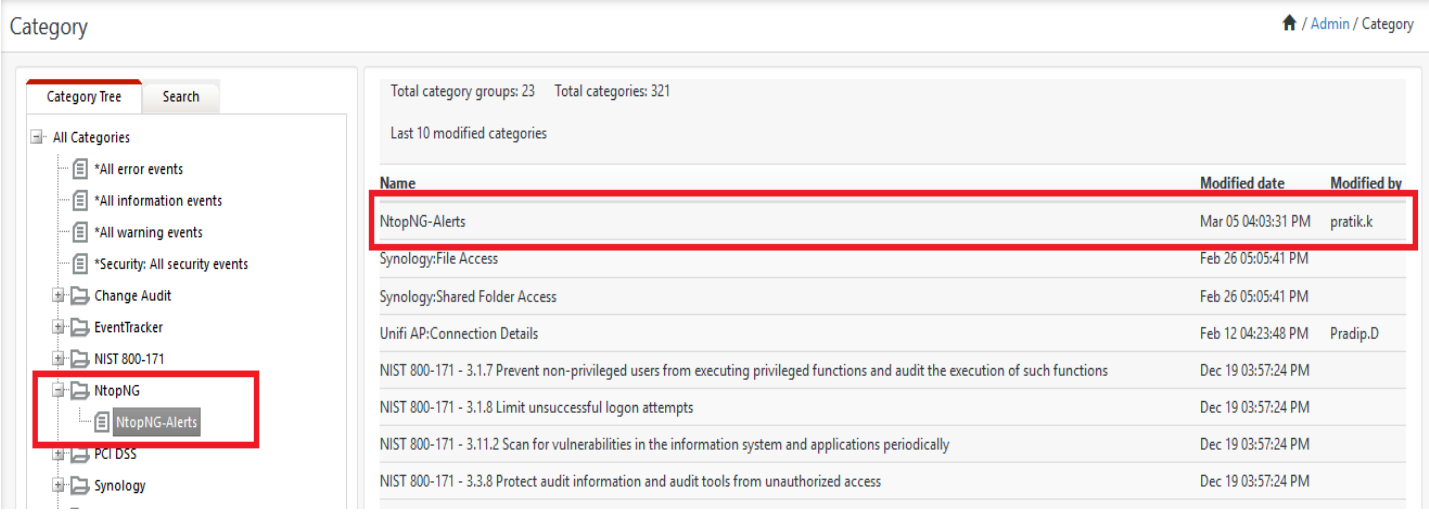

Figure 20

Verify Knowledge Object

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Knowledge Object**.
3. In **Knowledge Object Group Tree** to view imported knowledge object, scroll down and click **Ntopng** group folder.

Knowledge Object are displayed in the pane.

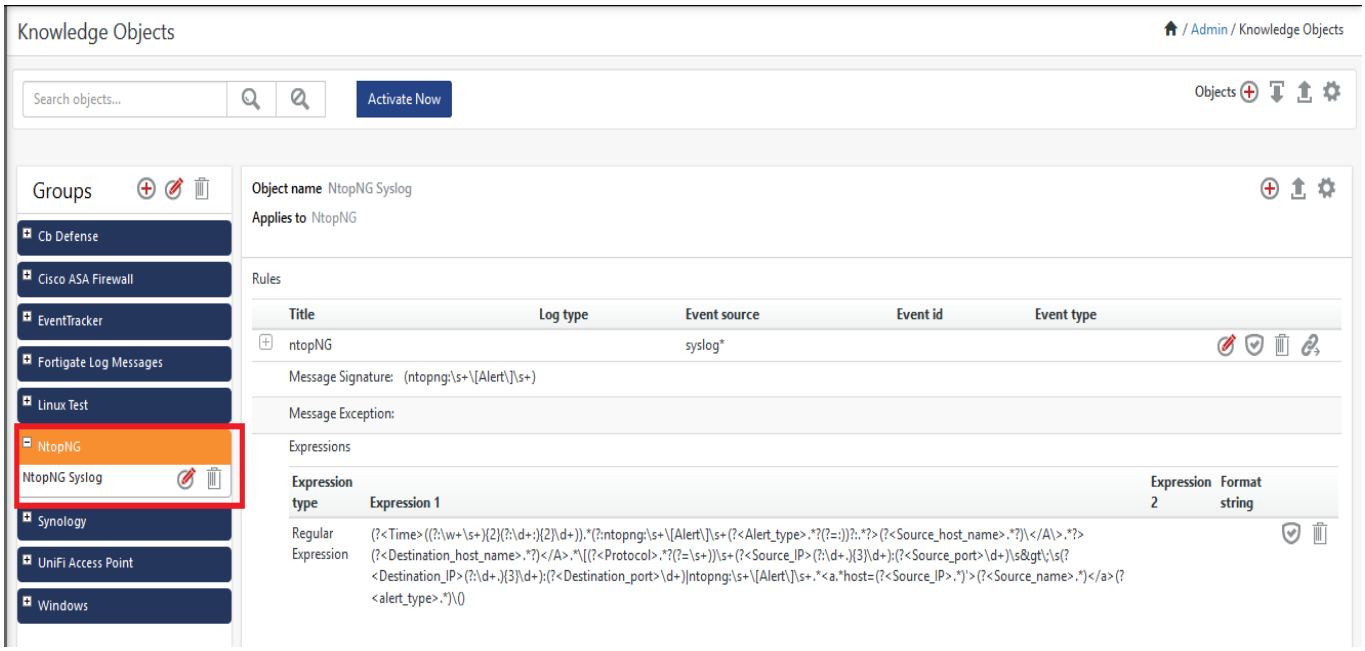

Figure 21

Verify Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**. Alerts are displayed in the pane.

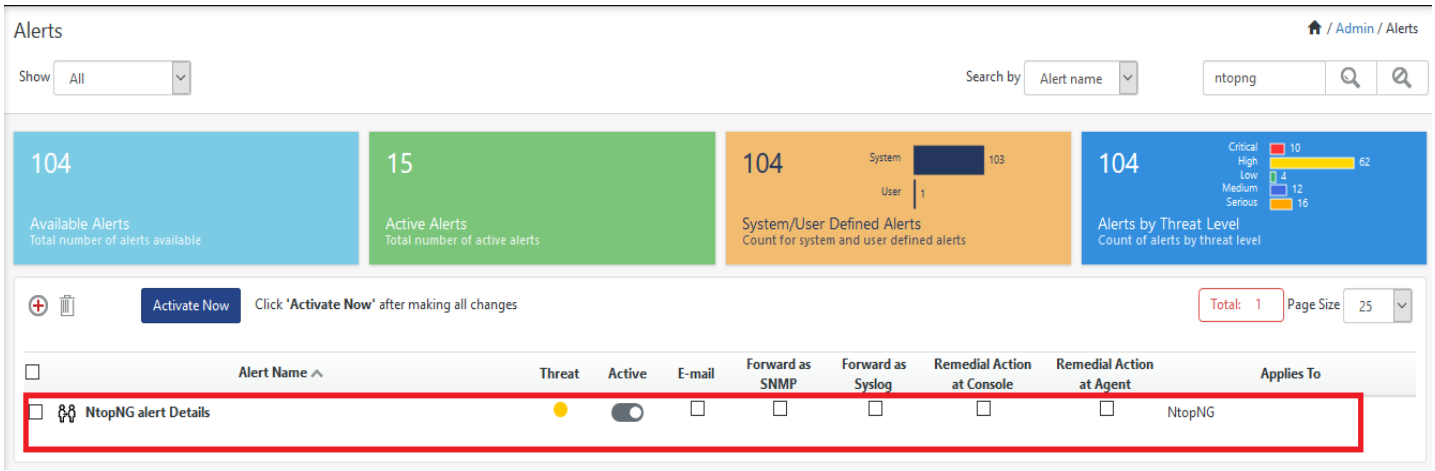

Figure 22

Verify Token Templates

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Parsing Rules**.
3. In **Parsing Rules** select **Template**, scroll down and click **Ntopng** group folder.

Token template are displayed in the pane.

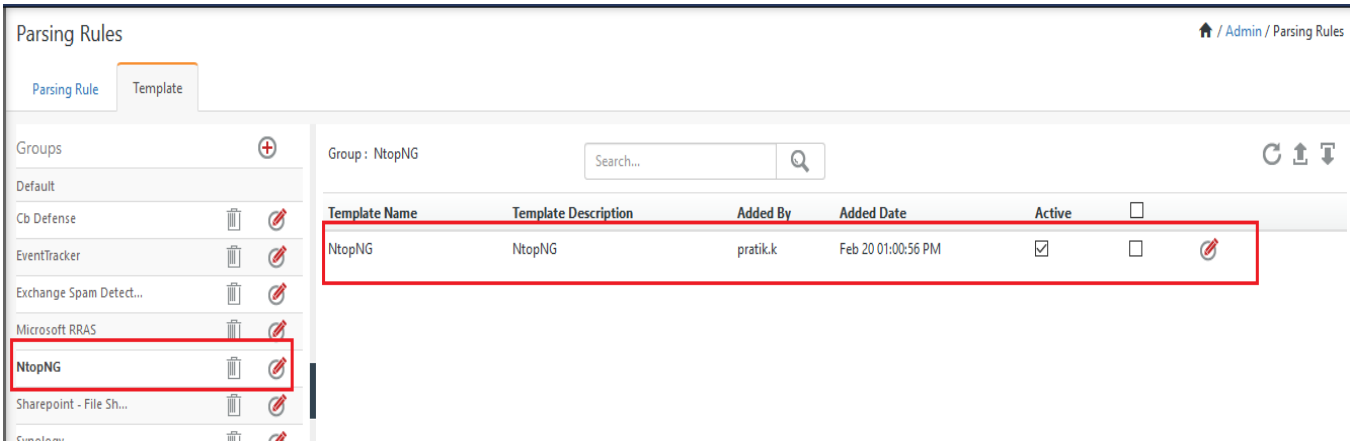

Figure 23

Verify Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu, and then **Configuration**.
3. Select **Defined** in report type.
4. In **Report Groups Tree** to view imported Scheduled Reports, scroll down and click **Ntopng** group folder.

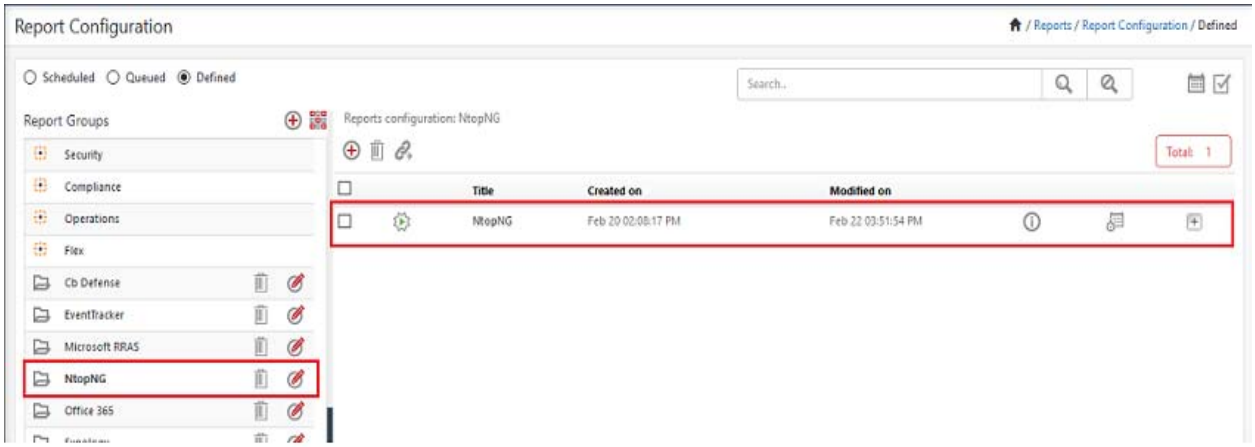

Figure 24

Reports are displayed in the Reports configuration pane.