

Integrate Ntopng

EventTracker v8.x and above

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.

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

This document is for informational purposes only. EventTracker 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 EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker 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 EventTracker, 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.

© 2018 EventTracker Security LLC. 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
Scope	1
Audience	1
Overview	3
Prerequisites	3
Configure Ntopng to forward logs to EventTracker	3
Configuration to enable Syslog forwarding	3
EventTracker Knowledge Pack (KP)	5
Alert	5
Reports-	5
Import Knowledge Pack into EventTracker	5
Import Categories	6
Import Knowledge Objects	7
Import Alerts	8
Import Token Templates	10
Import Flex Reports	10
Verify Knowledge Pack in EventTracker	12
Verify Category	12
Verify Knowledge Object	13
Verify Alerts	14
Verify Token Templates	14
Verify Flex Reports	15

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**.

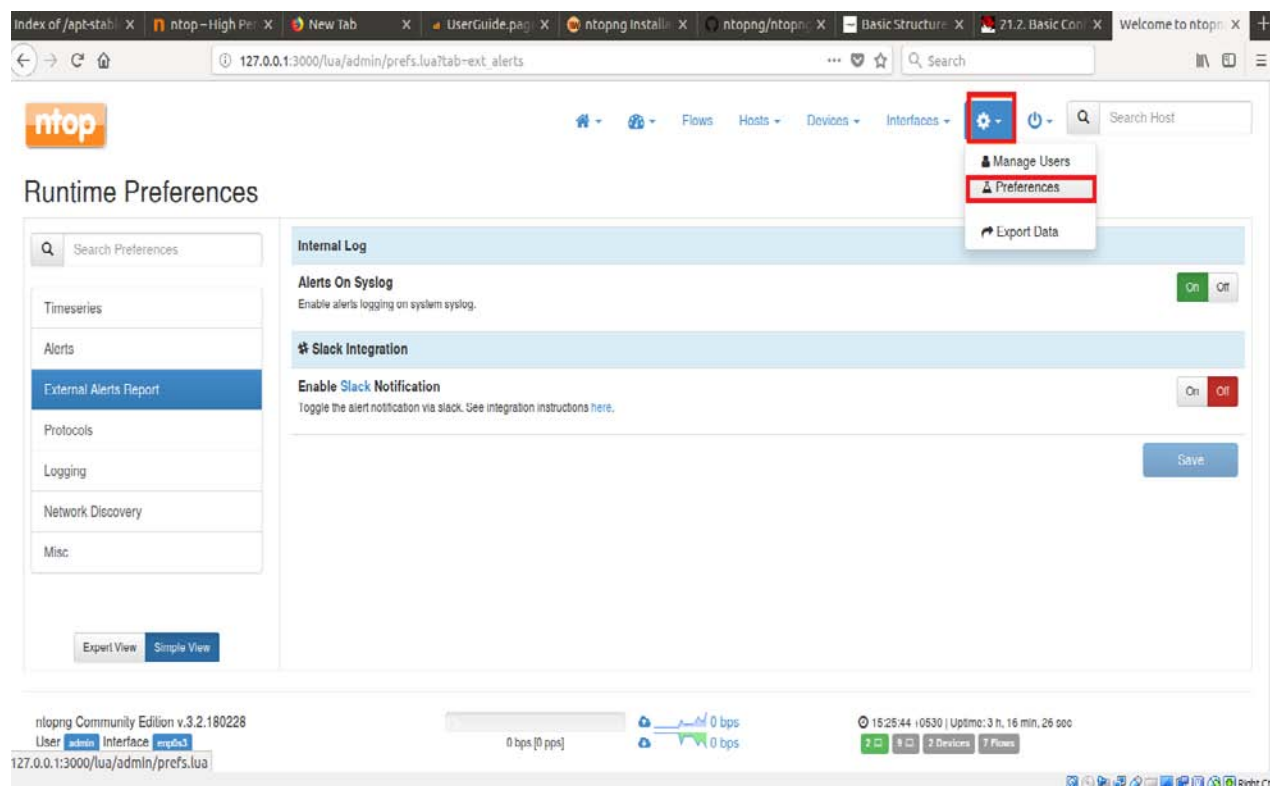


Figure 1

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

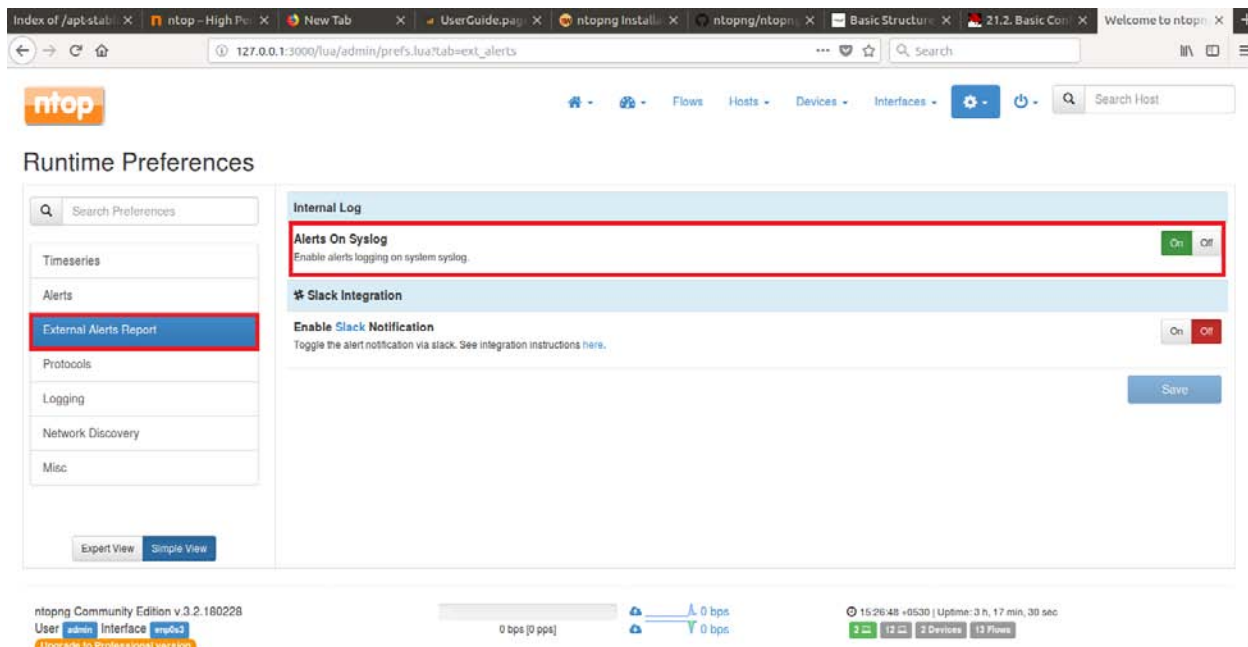


Figure 2

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 triggered 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					
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					
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

Time	Alert Type	Source Name	Source IP	Source Port	Protocol	Destination Name	Destination IP	Destination Port
Feb 20 03:55:46 PM								
Feb 08 02:33:30								
Feb 8 02:21:00								
ntopng: [[Alert]] [[RELEASED]] Host ... is a Flooder (25 flows...								
event_log_type	Application							
event_type	Information							
event_id	3333							
event_source	syslog							
event_user_domain	N/A							
event_computer	ntopng							
event_user_name	N/A							
event_description	Feb 08 02:33:30 Feb 8 02:21:00 ntopng: [[Alert]] [[RELEASED]] Host ... is a Flooder (25 flows s... ent in 3 sec)							

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**.

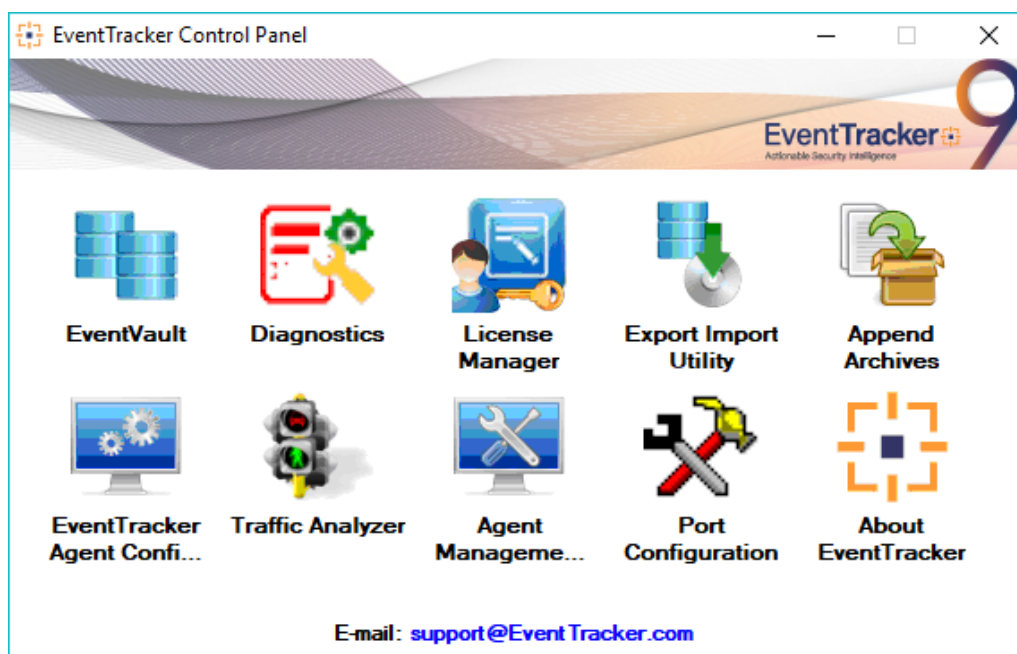



Figure 5

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

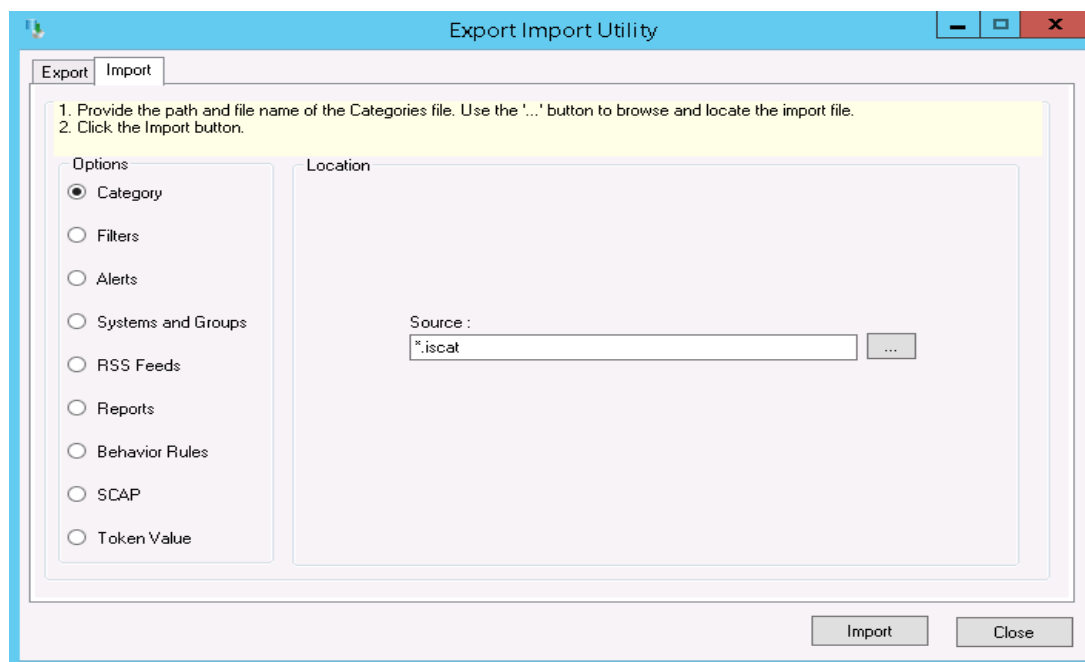


Figure 6

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

EventTracker displays success message.

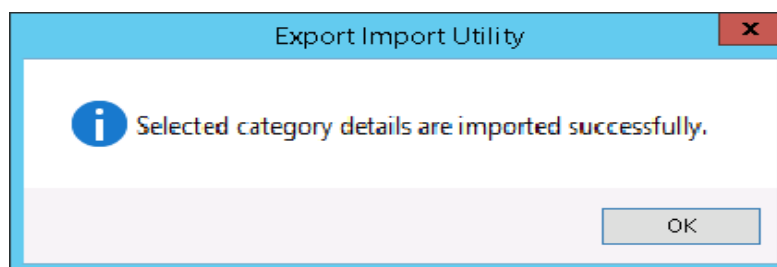



Figure 7

- 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

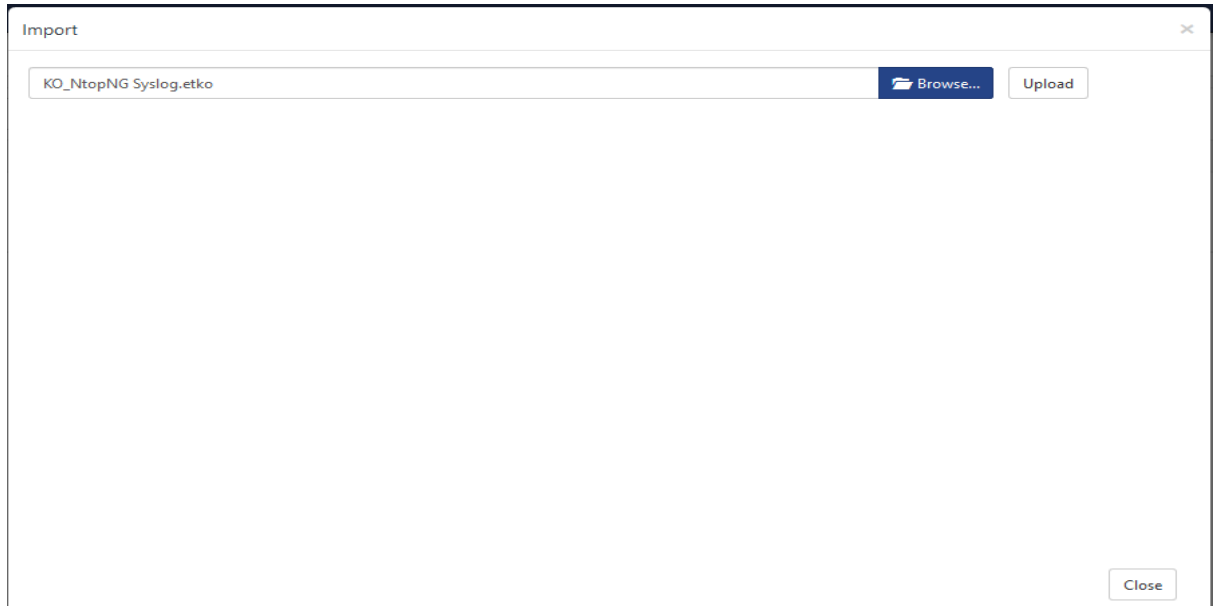


Figure 8

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

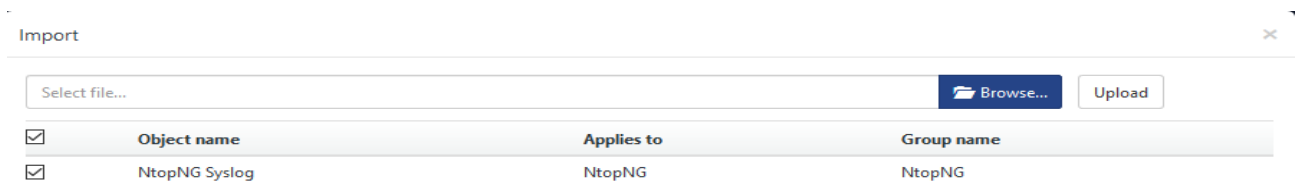


Figure 9

- Knowledge objects are now imported successfully.

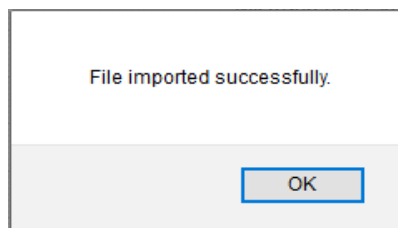


Figure 10

Import Alerts

- Select **Export Import Utility**.

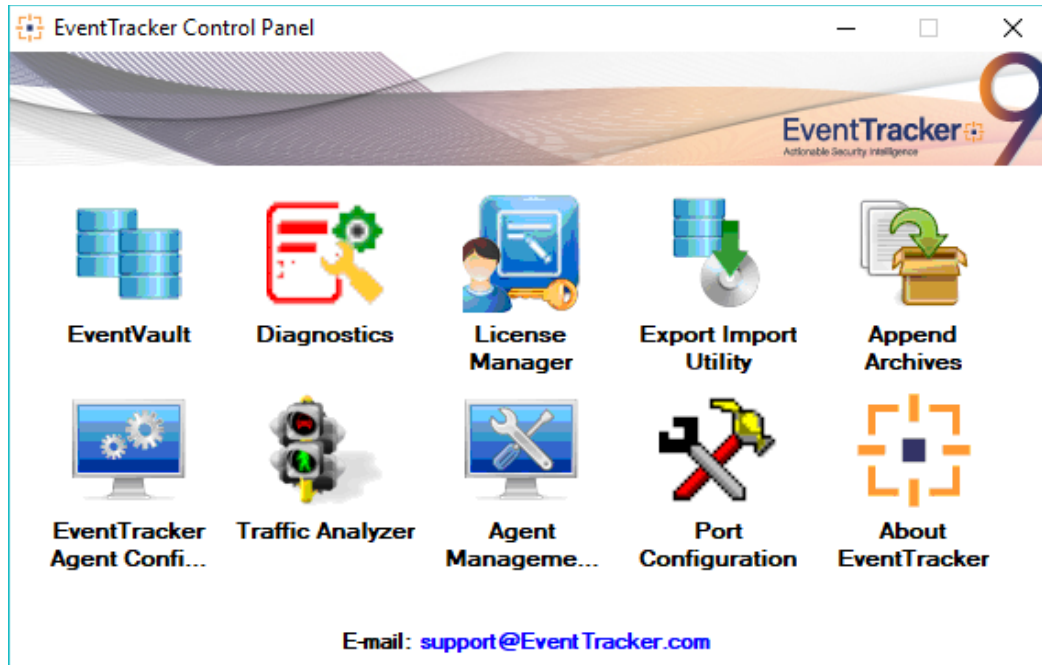


Figure 11

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

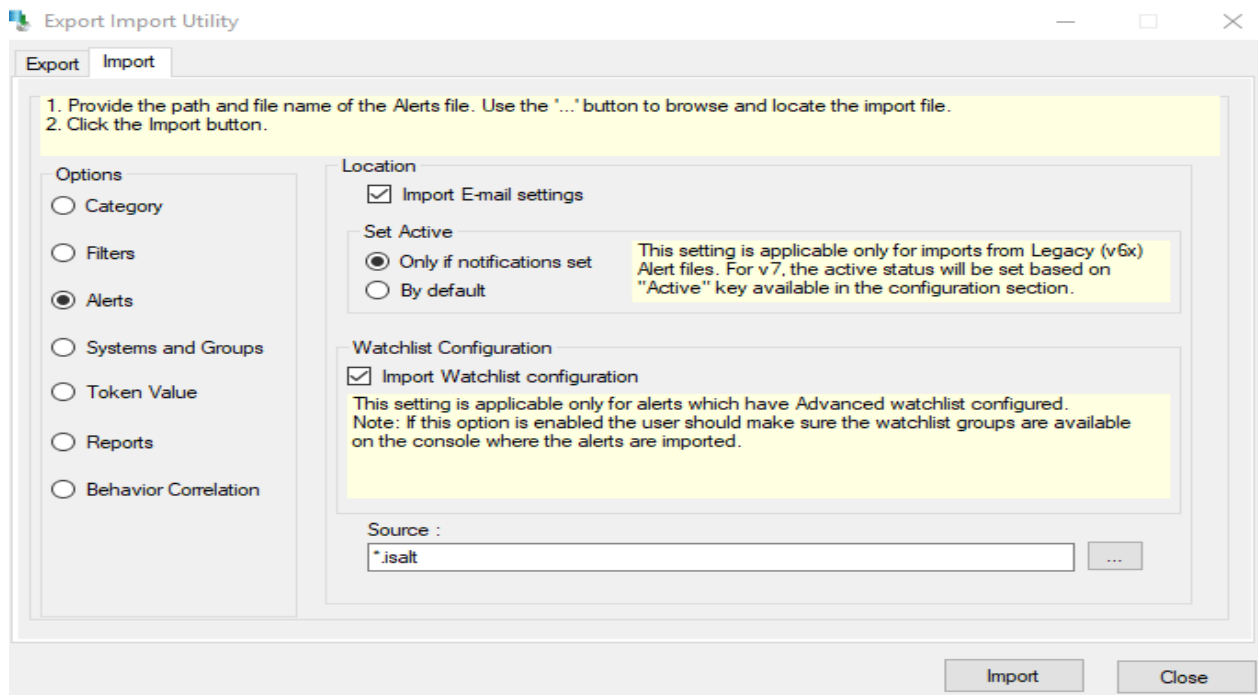


Figure 12

- Alerts are now imported successfully.

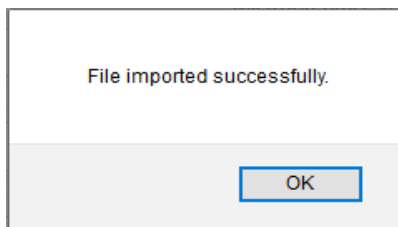


Figure 13

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.

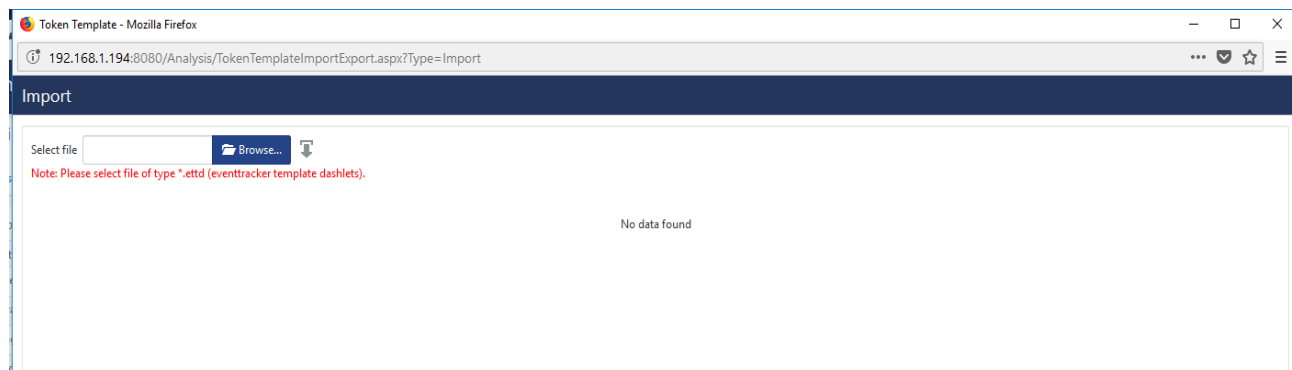


Figure 14

- Templates are now imported successfully.

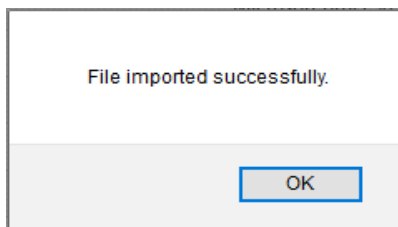


Figure 15

Import Flex Reports

- Select **Export Import Utility**.

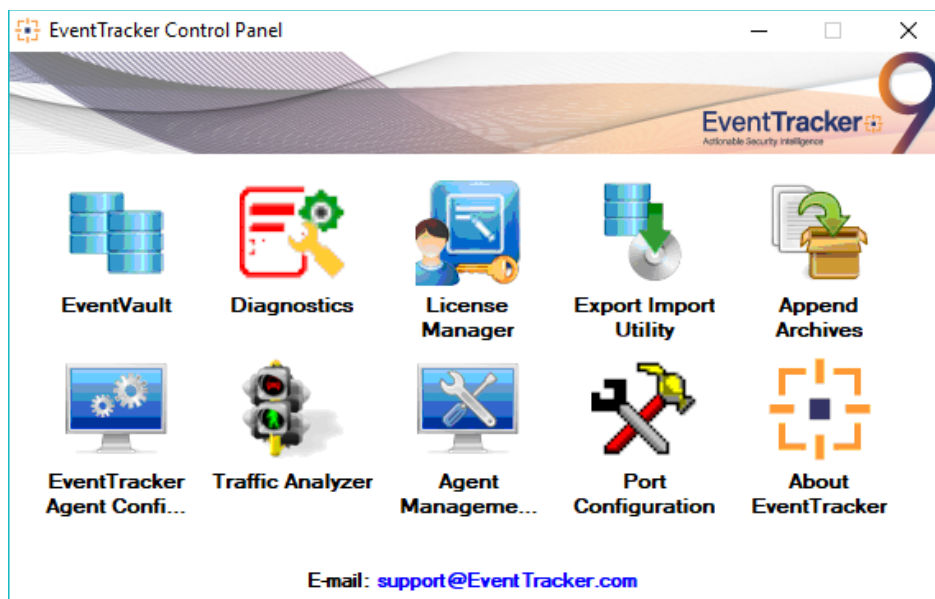


Figure 16

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

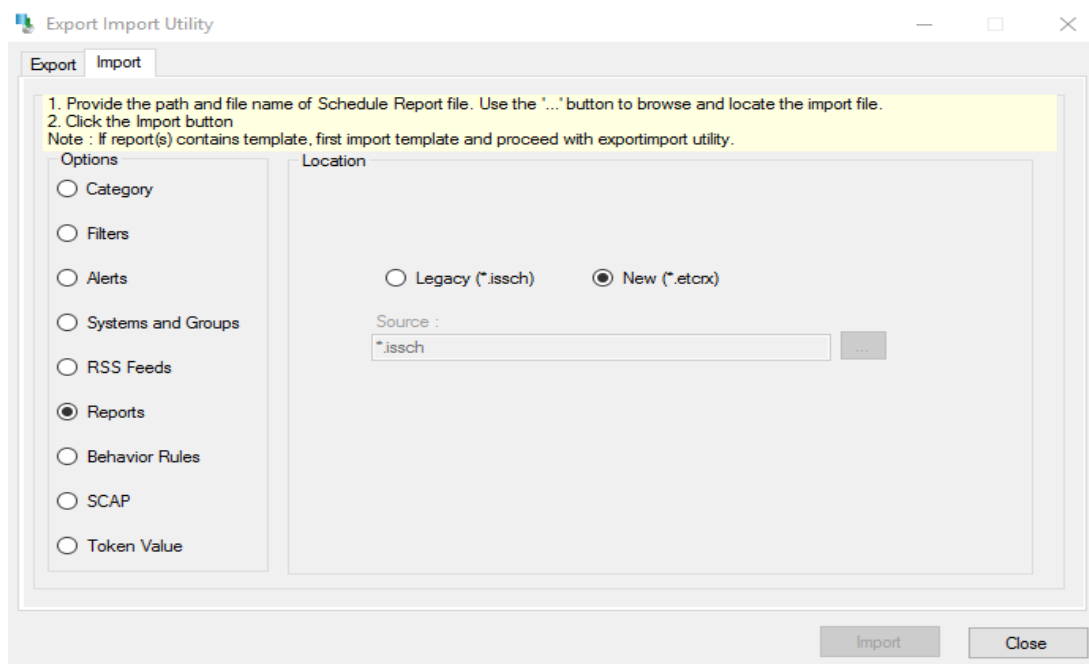



Figure 17

- And then click the browse  button.

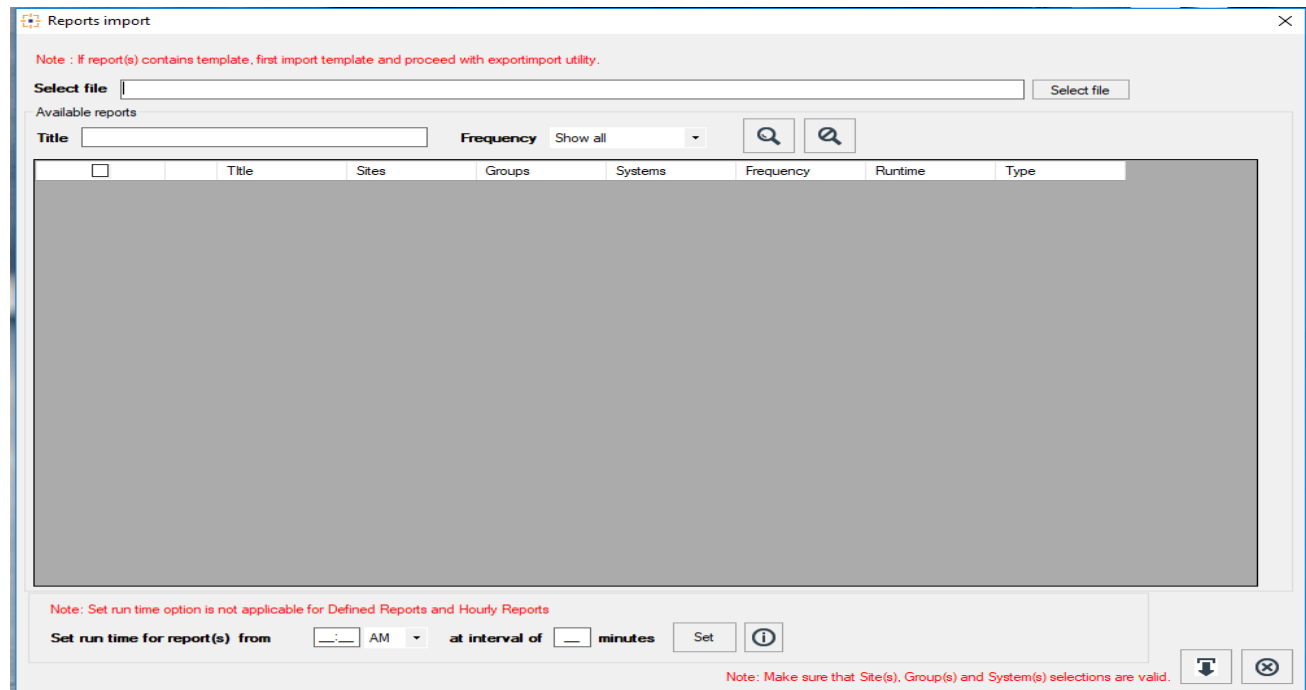


Figure 18

- 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.

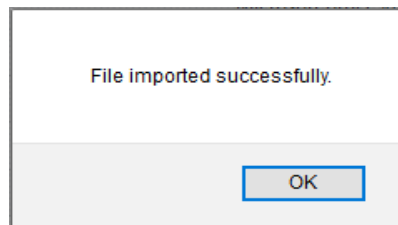


Figure 19

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.

Category

Home / Admin / Category

Category Tree Search

All Categories

- *All error events
- *All information events
- *All warning events
- *Security: All security events
- Change Audit
- EventTracker
- NIST 800-171
- NtopNG**
 - NtopNG-Alerts**
- PCI DSS
- Synology

Total category groups: 23 Total categories: 321

Last 10 modified categories

Name	Modified date	Modified by
NtopNG-Alerts	Mar 05 04:03:31 PM	pratik.k
Synology:File Access	Feb 26 05:05:41 PM	
Synology:Shared Folder Access	Feb 26 05:05:41 PM	
Unifi AP:Connection Details	Feb 12 04:23:48 PM	Pradip.D
NIST 800-171 - 3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions	Dec 19 03:57:24 PM	
NIST 800-171 - 3.1.8 Limit unsuccessful logon attempts	Dec 19 03:57:24 PM	
NIST 800-171 - 3.11.2 Scan for vulnerabilities in the information system and applications periodically	Dec 19 03:57:24 PM	
NIST 800-171 - 3.3.8 Protect audit information and audit tools from unauthorized access	Dec 19 03:57:24 PM	

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.

Knowledge Objects

Home / Admin / Knowledge Objects

Search objects... Activate Now

Objects + - < > ⚙

Groups + - 🗑

- Cb Defense
- Cisco ASA Firewall
- EventTracker
- Fortigate Log Messages
- Linux Test
- NtopNG**
 - NtopNG Syslog**
- Synology
- UniFi Access Point
- Windows

Object name: NtopNG Syslog

Applies to: NtopNG

Rules

Title	Log type	Event source	Event id	Event type
ntopNG		syslog*		

Message Signature: (ntopng:\s+\[Alert\]\s+)

Message Exception:

Expressions

Expression type	Expression 1	Expression 2	Format string
Regular	(?<Time>(?:[w+ s+](2)(?:d+)(2)d+).*(?:ntopng:\s+\[Alert\]\s+(?:<Alert_type>.*(?:= :)?.*(?:<Source_host_name>.*?)\.*(?:<Destination_host_name>.*?)\.*(?:<Protocol>.*(?:= :)+)\s+(?:<Source_IP>(?:\d+)(3)d+)(?:<Source_port>\d+)\s>\s(?:<Destination_IP>(?:\d+)(3)d+)(?:<Destination_port>\d+)\sntopng:\s+\[Alert\]\s+.*<a.*host=(?:<Source_IP>.*?)(?:<Alert_type>.*?)\()		

Figure 21

Verify Alerts

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

Alerts

Show: All

Search by: Alert name

ntopng

104 Available Alerts
Total number of alerts available

15 Active Alerts
Total number of active alerts

104 System/User Defined Alerts
Count for system and user defined alerts

104 Alerts by Threat Level
Count of alerts by threat level

Activate Now

Click 'Activate Now' after making all changes

Total: 1 Page Size: 25

Alert Name	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
NtopNG alert Details	●	☑	☐	☐	☐	☐	☐	NtopNG

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.

Parsing Rules

Parsing Rule Template

Groups

Group: NtopNG

Template Name	Template Description	Added By	Added Date	Active		
NtopNG	NtopNG	pratik.k	Feb 20 01:00:56 PM	☑	☐	✎

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.

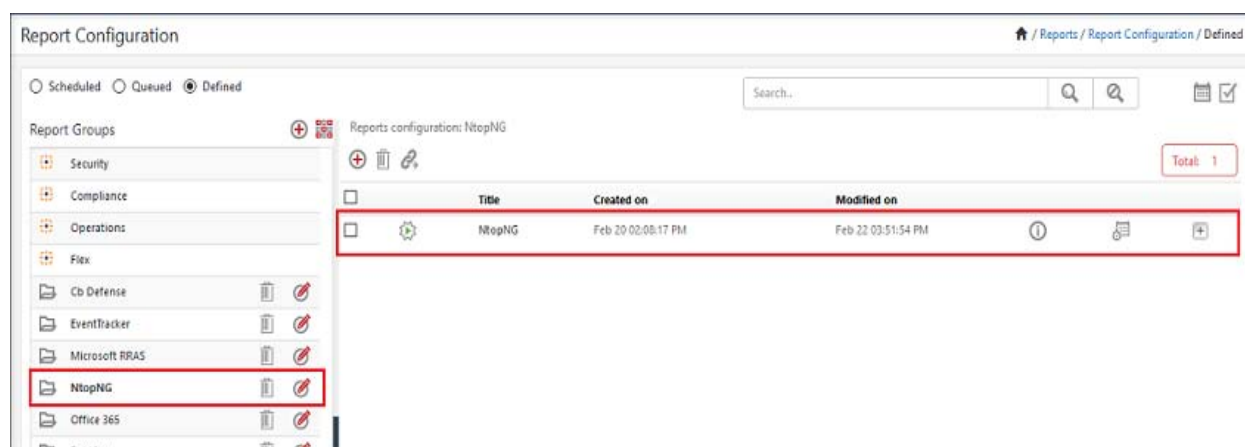


Figure 24

Reports are displayed in the Reports configuration pane.