

Integration Guide

Integrating ntopng with EventTracker

EventTracker v9.2 and later

Publication Date:

April 30, 2021

© Copyright Netsurion. All Rights Reserved.

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

Tab	ole of	f Contents	3
1.	Ov	erview	4
2.	Pre	erequisites	4
3.	Int	egrating ntopng events to EventTracker server	4
4.	Eve	entTracker Knowledge Pack	5
4	ł.1	Categories	5
4	1.2	Alerts	5
4	1.3	Reports	5
4	1.4	Dashboards	7
5.	Im	porting Knowledge Pack into EventTracker	8
ŗ	5.1	Categories	9
ŗ	5.2	Alerts	10
ŗ	5.3	Token Template	11
ŗ	5.4	Flex Reports	12
ŗ	5.5	Knowledge Objects	13
ŗ	5.6	Dashboards	14
6.	Ve	rifying Knowledge Pack in EventTracker	15
(5.1	Categories	15
(5.2	Alerts	16
(5.3	Token Template	16
(5.4	Flex Reports	16
(5.5	Knowledge Objects	17
(5.6	Dashboards	17
1	٩bou	t Netsurion	18
(Conta	act Us	18

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

- 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
- 3. Launch ntopng Web Interface.
- 4. Hover over setting and select Preferences.

Index of /apt-stable 🗙 👖 ntop – High Per 🛪	🛛 ຢ New Tab 🛛 🗙 🖬 UserGuide.pag: 🗙	t 🛛 📾 ntopi	ng Install	a x O	ntopng/nto	png X 🛛 🛁 Ba	asic Structure 🗙	🎘 21.2. Basic Conf 🗲	Welcome to ntopr	× +
← → C ² ŵ ① 127.0	0.1:3000/lua/admin/prefs.lua?tab=ext_alerts					🖾	☆ Q Search		lif\	▣ ≡
Runtime Preferences		# -	£8 ~	Flows	Hosts -	Devices +	Interfaces -	 ✿ - Q ▲ Manage Users ▲ Preferences 	Search Host	
Q Search Preferences	Internal Log							A Export Data		
Timeseries	Alerts On Syslog Enable alerts logging on system syslog.								On C	ж
Alerts	Slack Integration									
External Alerts Report	Enable Slack Notification Toggle the alert notification via slack. See integration ins	structions here.							On C	я
Logging									Save	
Network Discovery										
Misc										
Expert View Simple View										
User admin Interface enplas	0 bps [0 p	ops]	۵ <u>–</u>		ops bps	2	15:25:44 +0530 Upt 9 💷 2 Device:	100:3 h, 16 min, 26 sec 7 Flows		
127.0.0.1:3000/lua/admin/prefs.lua								S	4 # Ø = = = 0 0	💿 Right Ctrl



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

Image: Community Eddition vs. 22.180228	of/apt-stable 🗙 📔 ntop –	High Per X 🔰 New Tab X 🍃 User Guide, pagi: X 🚭 ntopng Installio: X 🔍 ntopng/ntopng X 🔚 Basic Structure: X 💐 21.2. Basic Cont X 🛛 Welcome to ntopng X
Image: Community Eddion v3.2.18028	→ C' û	🛈 127.0.0.1:3000/lua/admin/prefs.lua?tab=ext_alerts 🗸 🖓 Search 🕅 🖸
Search Preferences Internal Log Timeseries Alerts External Alerts Report Protocols Logging Network Discovery Misc Expert View Emple View Tomps Community Edition v3.2.180228 Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log Internal Log	ntop	★ - A Flows Hosts - Devices - Interfaces - O - Q Search Host
Sarch Preferences Intenai Log Intenseries Alerts On Sysiog Con Alerts Report Protocols Constructions here. Togle the alert notification via stack. See integration instructors here. Sarce Constructions here. Constructions here. <td>untime Prefere</td> <td>nces</td>	untime Prefere	nces
Image:	Q Search Preferences	Internal Log
Alerts	Timeseries	Alerts On Syslog Enable alerts logging on system syslog. Of
External Aleris Report Enable Slack Notification on Protocols Toggle the alert notification via slack. See integration instructions here. Save Network Discovery Misc Save	Alerts	拳 Slack Integration
Protocols Save Logging Network Discovery Misc Expert View Simple View Simple View	External Alerts Report	Enable Slack Notification Toggle the alert notification via slack. See integration instructions here.
Logging Network Discovery Misc Expert View Simple View Nopog Community Edition v.3.2.180228	Protocols	
Network Discovery Misc Expert View Simple View topg Community Edition v.3.2.180228 © 15.26.48 +0530 Uptime: 3 h, 17 min, 30 sec	Logging	Save
	Network Discovery	
Expert View Simple View toppg Community Edition v.3.2.180228 <u> <u> </u></u>	Misc	
Itoping Community Edition v.3.2.180228		
topng Community Edition v.3.2.180228 O 1526:48 +0530 Uptime: 3 h, 17 min, 30 sec	Expert View Simple View	
topng Community Edition v.3.2.180228		
Jser admin Interface engos 0 bps [0 pps] 🛆 V 0 bps 2 💷 12 💷 2 Devices 13 Flows	opng Community Edition v.3.2.1 ser admin Interface enp0s3	80228 0 bps [0 pps] 0 bps

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_i d":0,"cli_os":"Windows

 $10","alert_severity":2,"srv_blacklisted":false,"srv2cli_bytes":55859,"alert_tstamp":1618572309,"cli_asn":0," srv_os":"","proto.ndpi":"HTTP","first_seen":1618572308,"l7_master_proto":7,"cli_localhost":true,"alert_jso n":"{\"info\":\"ntong32.pmusa.com:8088\\.\\\.\\/\\",\"status_info\":\"{\\"ntopng.key\\\":348827202,\\\"cli2srv.packets\\\":30,\\\"srv.localhost\\\":false,\\\"cli.ip\\\":\\\"10.10.1.16\\\",\\\"srv2cli.packets\\\":50,\\\"srv.port\\\":8088,\\\"hash_entry_id\\\":2135264,\\\"cli.port\\\":41486,\\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\\"proto.ndpi\\\":\\\"HTTP\\\",\\\"proto.ndpi\\\":\\\"HTTP\\\",\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\"proto.ndpi_app\\\":\\\"HTTP\\\",\\"proto.ndpi_sv_localhost\\":su bdir\\\":\\\"flow_risks\\\",\\\"confset_id\\\":0,\\"su bdir\\\":\\\"flow\\\",\\"score":150,"srv_addr": "10.101.5.21\\\"}\",score":150,"srv_addr": "10.101.5.21\\\"}\",score":150,"srv_asn":0,"proto":6, "alert_entity_val":"flow","srv_country":"","srv2cli_packets":50}$

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\V.\V	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\V.\V	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

Ntopng - Top accessed URLs	ß	- :	×
			<>>
r1p1s3vm10.prismusa.com:8088 r1p1s3vm10.prismusa.com:8080			
📕 r1p1s3vm10.prismusa.com:5985 🛛 📕 r1p1s3vm10.prismusa.com:3389 🖉 r1p1s3vm10.prismusa.co	m		
contoso-svr1.contoso.local:9200 contoso-svr1.contoso.local:5985			
Apr 22 11:26 AM - Apr 29 11:27 AM			

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.

💺 Export Import Utility	
Export Import	
1. Provide the path and file n 2. Click the Import button.	ame of the Categories file. Use the '' button to
Options Category	Location

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.

Click the Import button.	ane of the categorie:	s nie. Ose une but	ton to biowse and loc	ate the import ne.		
Options Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation	Location S	ource : .iscat]	
Behavior Correlation						

EventTracker displays a success message.





5.2 Alerts

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

💺 Export Import Utility			×
Export Import			
 Provide the path and file nar Click the Import button. 	ne of the Alerts file. Use the '' butt	on to browse and locate the import file.	
Options	Location		
Category	Import E-mail settings		
) Filters	Set Active Only if notifications set	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on	
Alerts	O By default	Active key available in the conliguration section.	
O Systems and Groups	Watchlist Configuration		
O Token Value	✓ Import Watchlist configurat		
◯ Reports	Note: If this option is enabled t on the console where the alert	or alerts which have Advanced watchlist configured. he user should make sure the watchlist groups are available s are imported.	
O Behavior Correlation			
	Source :		
	*.isalt		
		Import	
		import	se

EventTracker displays a success message.





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.

	🔎 Admin	n ✔ Tools ✔
ers	🧭 Parsing Rules	† /
lt Contains	s set of rules which tell what kind	d of data you want
Configuration	Systems	

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

Parsing Rule	S				
Parsing Rule	Template				
Groups			⊕ #		Group :
Default				*	
Azure Intune		Ē	1		Templa
	n / Ad	dmin /	Parsing F	Rules	5
	n / Ad	dmin /	Parsing F	Rules	5
	n / Ad	dmin /	Parsing F	Rules	5

 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:



Import						
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).

 Provide the path and file nan Click the Import button 	ie of Schedule Report file. Use the "' button to browse and locate the import file.	
Note : If report(s) contains temp Options	Late, first import template and proceed with exportimport utility.	
Category		
Filters		
 Alerts 	O Legacy (*issch) New (*.etcrx)	
 Systems and Groups 	Source :	
O Token Value	.155C1	
Reports		

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".

段 Reports Import	
Note : if report(s) contains template, first import template and proceed with report import process	
Select file *.etorx	Select file
Available reports	
Title Frequency Show all • Q Q	
Title Sites Groups Systems Frequency Runtime	Туре

Ţ



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

Note: Set run time option is not applicab	le for Defined Reports and Hourly Reports			
Set run time for report(s) from	AM • at interval of _ minutes	Set D		
Replace	to Replace	Assign systems		
		Note: Make sure that Site(s), $Group(s)$ and $System(s)$ selections are v	alid.	\otimes

EventTracker displays a success message.

Export Import Utility	×
Selected reports configurations are imported successfully	
ОК	

5.5 Knowledge Objects

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

			斗 🛛 Admin 🗸	Tools 🕶 📀
Π.	Active Watch Lists	Event Filters	🧭 Parsing Rules	🔒 / Das
1	Alerts	Eventvault	Report Settings	
	Behavior Correlation Rules	FAQ Tile Configuration	Systems	
	🗞 Behavior Correlation Settings	Group Management	🗙 Users	
or so	Casebook Configuration	Q IP Lookup Configuration	r Weights	since the last 24 hours
	● Category	·☆ Knowledge Objects	Windows Agent Config	
	Diagnostics	Manager		

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





 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.

Import	
KO_ <product name="">.etko</product>	🗁 Browse 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** \rightarrow **My Dashboard**.
- 3. In My Dashboard, Click the Import button.

≡	Event Tracker 🖶
	Home
٩	My Dashboard
	Threats
	Incidents
	Behavior Correlation
	Change Audit
	Compliance

Import

Close





- 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.
Available widgets Select All
Import Close

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.

ategory	
Category Tree Search	
ntop	ର୍ ଷ୍
Category	
✓Ntopng: Alerts	
Ntoppg: 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 v							Search by Alert name	¥	ntop	Q	Q
318	115				318	System	200	318	Cristical 17 Low 10 Services 17	161	
Available Alerts Total number of alerts available	Active Alerts Total number of active alerts				System/User Defined a Count for system and user define	Alerts ed alerts		Alerts by Threat Level Count of alerts by threat level	a 7		
Activate Now Click 'Activate Now' after making all	changes								Total: 1 Pa	age Size 25	v
Alert Name ^	1	Threat	Active	Email	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To		
្រ ក្ខិភ្លឺ NtopNG: Alert		•				0		Ntop	ong 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.

Parsing Rules				
Parsing Rule	Template			
Groups				(+)
Ntopng		Ē	Ø	^

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.

Netstrion®

Report Configuration			
O Scheduled O Queued Defined			
Report Groups			+
NtopNG	Ē	Ø	^

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.

ର୍ ଝ୍
🕀 🏉 🗓
Ø 🗓

6.6 Dashboards

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

	Home
Dashb	My Dashboard
R	Threats
	Incidents

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

Available dashlets			>
ntop			Q
□ Ntopng - Alert triggered by d	🗆 Ntopng - Alert Triggered by s	🗌 Ntopng - Alert triggered by t	Ntopng - Top accessed URLs
			Export Close



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 <u>EventTracker</u> 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 <u>BranchSDO</u> delivers purpose-built technology with optional levels of managed services to multilocation 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 <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>. Netsurion is #19 among <u>MSSP Alert's 2020 Top 250 MSSPs</u>.

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