

Integration Guide for FireEye Network Security and Forensics (NX) EventTracker v9.x and later

Publication Date: April 30, 2020

Abstract

This guide provides instructions to retrieve the **FireEye Network Security and Forensics (NX)** events by syslog. Once **EventTracker** is configured to collect and parse these logs, dashboard and reports can be configured to monitor **FireEye Network Security and Forensics (NX)**.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x or above and **FireEye Network Security and Forensics (NX).**

Audience

Administrators who are assigned the task to monitor **FireEye Network Security and Forensics (NX)** events using EventTracker.

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

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright FireEye Network Security and Forensics (NX) is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion 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 Netsurion, 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.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

1.	Ove	erview
2.	Pre	requisites
3.	Inte 3.1	egrating FireEye NX with EventTracker
4.	Eve 4.1	ntTracker Knowledge Packs
	4.2	Alerts
	4.3	Reports5
	4.4	Dashboards
5.	Imp 5.1	orting knowledge pack into EventTracker
	5.2	Alerts
	5.3	Token Template
	5.4	Reports15
	5.5	Knowledge Objects
	5.6	Dashboards
6.	Ver 6.1	ifying knowledge pack in EventTracker
	6.2	Alerts
	6.3	Token Template
	6.4	Reports
	6.5	Knowledge Objects
	6.6	Dashboards



1. Overview

The FireEye Network Security and Forensics (NX) is an effective cyber threat protection solution. It helps organizations minimize the risk of costly breaches by accurately detecting and immediately stopping advanced, targeted and other evasive attacks hiding in Internet traffic.

EventTracker, when integrated with FireEye NX, collects log from FireEye NX and creates detailed reports, alerts, dashboards and saved searches. These attributes of EventTracker help users to view the critical and important information on a single platform.

Reports contain a detailed overview of events such as, malware object, indicating the presence of a file attachment with a malicious executable payload.

It will also show web infection indicating an outbound connection to a website initiated by a web browser that was determined to be malicious.

Alerts are provided as soon as any critical event is triggered by the FireEye NX. With alerts, users will be able to get notifications about real time occurrences of events such as, suspicious file hash detection, or suspicious web URL detection, and any such activities.

Dashboards will display a graphical overview of all the malwares detected by FireEye NX, or Command and Control server connection, etc. These services will include information such as suspicious source IP address, source port, destination IP address, destination port, anomaly type, malware name, etc.

2. Prerequisites

- VCP (virtual collection point) syslog port should be opened.
- Port 514 should be allowed in Firewall (if applicable).

3. Integrating FireEye NX with EventTracker

FireEye NX can be integrated with EventTracker using syslog forwarding.

3.1 Configuring a Syslog Forwarding

Follow the below steps to configure syslog.

- 1. Login to FireEye NX Web UI with an admin account.
- 2. Navigate to Settings > Notifications.
- 3. Click rsyslog and Check the "Event type" check box.
- 4. Make sure Rsyslog settings are:



Default format: CEF

Default delivery: Per event

Default send as: Alert

ttings: Notification	ns							
Data and Time								
Date and time	Notification Setting	js: Select a proi	tocol type b	elow to dis	play and ed	lit its parar	meters	
User Accounts		Protocol	email	http	rsyslog	somo		Settings
Email							Rsyslog Settings	aaranga
MDC Notestal	Event Type	Global	U		1	0	Default format: CEF	
PATER AND TRACESPECT							Carlos and C	
MPC Network							Default delivery: Per event	•
Notifications	Domain Match					1	Default delivery: Per event Default send as: Alert	•

Figure 1

- Next to the "Add Rsyslog Server" button, type "EventTracker". And, click on "Add Rsyslog Server" button.
- 6. Enter the EventTracker server IP address in the "IP Address" field. (Public IP, if hosted in cloud)
- 7. Check off the Enabled check box.
- 8. Select Per Event in the "Delivery" drop-down list.
- 9. Select All Events from the "Notifications" drop-down list.
- 10. Select CEF as the "Format" drop-down list.
- 11. Select UDP from the "Protocol" drop-down list. (Default port is 514)
- 12. Now, click **Update**. And click the "Test-Fire" button to send the test events to EventTracker server.

		Protocol	email	http	rsyslog	snmp				1	Settings		
ivent T	уре	Global			۷		Rsyslog Se Default form	at:	CEF Per event		:		
omain	Match	۲		V	۲	đ	Default send Apply Settin	as: (Alert	;)		
Infection Match		•		1	۲	1							
Malware	Callback	2		V	۲	S.							
Malware	Object	2		1	۲	2							
Web Infe	ection	۲	۲	V	۲	1							
syslog	Server Listing	Add Rsy	slog Serv	ar: Name:		Ad	Rsyslog Sen	/er					
lemove	Name	Enabled	đ	IP Address		Delivery		Notifica	ation		Format		Send as
	UserInsight- Collector	۲		172.16.75.2	50	Per even	:	All Ev	ents	:)	CEF	:	Default
				Account	1	Protocol							
						UDP :							

Figure 2



4. EventTracker Knowledge Packs

4.1 Saved Searches

Saved searches are designed to quickly parse logs and allow user to see only specific events related to:

- FireEye: Suspicious Domain Match This category of saved search allows user to filter and view the events specific to website domain that has been identified as the source of malicious behavior.
- FireEye: Initial Web Infection Identification this category of saved search allows user to filter and view events specific to the process of identifying a URL pointing to the initial web infection.
- FireEye: Command and Control Connections This category of saved search allows user to filter and view events specific to situation where there is an established connection between the infected endpoint and a command and control (CnC) server.
- **FireEye:** Suspicious File Attachments This category of saved search allows user to filter and view events that indicates presence of a file attachment with a malicious executable payload.
- FireEye: Outbound Connections established with Malicious Website This category of saved search allows user to filter and view events that indicates a web browser initiated an outbound connection to a website that was ultimately determined to be malicious.

4.2 Alerts

Alerts are triggered when an event received is identified as critical and requires immediate notification. Such as,

- FireEye NX: A command and Control connection has been blocked This alert is triggered when the FireEye MVX engine detects an established command and control server connection with an endpoint in the network.
- FireEye NX: A website with malicious contents has been discovered This alert is triggered when the FireEye detects a user visited website is infected with malicious contents.
- **FireEye NX: File attachment with a malicious executable payload detected** This alert is triggered when the FireEye detects a presence of a file attachment with a malicious executable payload.

4.3 Reports

• FireEye NX – Malicious File detected – This report for FireEye includes events that indicates the presence of a file attachment with a malicious executable payload. The report contains the file hash of the malicious payload along with relevant information such as source and destination IP.



LogTime	Computer	Source IP	Source Port	Destination IP	Destination Port	File Hash	Malware
04/22/2020 06:00:20 PM	NTPLDTBLR48-SYSLOG	169.250.0.4	10	127.0.0.20	20	dfcc0ebba834870c2860296cdc96 c644	FireEye-TestEvent-SIG
04/23/2020 01:01:16 PM	NTPLDTBLR48-SYSLOG	169.250.0.4	10	127.0.0.20	20	dfcc0ebba834870c2860296cdc96 c644	FireEye-TestEvent-SIG

 FireEye NX - Outbound connections with malicious websites – This report for FireEye includes events that indicates that a web browser initiated an outbound connection to a website that was ultimately determined to be malicious. This report contains the infected website URL, along with relevant information such as, source and destination IP.

Computer	Source IP	Source Port	URL	Anomaly Type	Destination IP	Destination Port
NTPLDTBLR48-SYSLOG	169.250.0.1	10	compl_0_2- someurl.x1y2z3.com	anomaly-tag datatheft keylogger	127.0.0.20	20
NTPLDTBLR48-SYSLOG	169.250.0.1	10	compl_0_2- someurl.x1y2z3.com	anomaly-tag datatheft keylogger	127.0.0.20	20

Figure 4

FireEye NX - Successful Command and Control Activities – This report for FireEye includes events that
indicates there is an established connection between the infected endpoint and a command and control
(CnC) server. This report contains the information on Command and control server IP address and to
which system it has connected, i.e. source IP.

LogTime	Computer	Source IP	Source Port	CnC_Host	Protocol	Destination IP	Destination Port
04/23/2020 05:31:53 PM	NTPLDTBLR48-SYSLOG	192.168.25.2	28941	172.65.203.203	tcp	172.65.203.203	80
04/23/2020 05:31:53 PM	NTPLDTBLR48-SYSLOG	192.168.26.142	Ó	3.3.3.3	tcp	2.2.2.2	80

Figure 5

• FireEye NX - Suspicious Domain match Activities – This report for FireEye includes events that indicates the website domain has been identified as the source of malicious behavior.

LogTime	Computer	Source IP	Source Port	Protocol	CnC_Host	Malware	Destination IP	Destination Port
04/23/2020 05:31:53 PM	NTPLDTBLR48-SYSLOG	169.250.0.1	10	tcp	FireEye-TestEvent.example.com	FireEye-TestEvent-SIG-DM	127.0.0.20	20
04/23/2020 05:31:53 PM	NTPLDTBLR48-SYSLOG	169.250.0.1	10	tcp	FireEye-TestEvent.example.com	FireEye-TestEvent-SIG-DM	127.0.0.20	20

Figure 6

• FireEye NX - URL pointing to the initial web infection – This report for FireEye includes events indicates to the process of identifying a URL pointing to the initial web infection.

LogTime	Computer	Source IP	Source Port	Protocol	Malware	Destination IP	Destination Port
04/23/2020 05:36:47 PM	NTPLDTBLR48-SYSLOG	192.168.10.23	123	tcp	nam	192.0.2.2	123
04/24/2020 04:47:39 PM	NTPLDTBLR48-SYSLOG	192.168.10.24	123	tcp	nam	192.0.2.2	123

4.4 Dashboards

• FireEye - Command and Control connection By Action type

FireEye - Command and Control connection By Action type
blocked 172.65.203.203



• FireEye - Command and Control connection By client application





Figure 9

• FireEye - Suspicious File Hashes



Figure 10



• FireEye - Suspicious URLs



Figure 11



• FireEye - Security event types

Figure 12



• FireEye - Malwares by anomaly type

FireEye - Malwares types and signature discovered





Figure 14



5. Importing knowledge pack into EventTracker

How to get Knowledge Packs

To get the knowledge packs, locate the knowledge pack folder. Follow the below steps:

- 1. Press "₩ + R".
- Now, type "%et_install_path%\Knowledge Packs" and press "Enter".
 (Note If, not able to locate the file path as mentioned above, please contact EventTracker support to get the assistance).

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Template/ Parsing Rules
- Flex Reports
- Knowledge Objects
- Dashboards
- 1. Launch the EventTracker Control Panel.
- 2. Double click Export-Import Utility.



Figure 15

🥾 Export Import Utility	
Export Import	
1. Provide the path and file n 2. Click the Import button.	name of the Categories file. Use the '' button to
Options	Location
 Category 	
0.5	

Figure 16

3. Click the **Import** tab.

5.1 Saved Searches

- 1. Once you have opened "Export Import Utility" via "EventTracker Control Panel", click the Category option, and then click Browse
- Navigate to the knowledge pack folder and select the file with extension ".iscat", e.g. "Categories_FireEye NX.iscat" and then click "Import":

Export Import	Export Import Utility	_		\times
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. Options Location Image: Options Location Image: Options Image: Options Image: Options Image: Options Image: Options Location Image: Options Image: Options Image: Options Image: Options Image: Options Image: Options Image: Options Image: Options Image: Options Image: Options Source : Image: Options Image: Options Image: Option Option Image: Option Option Image: Option Option Image: Option Option Image: Option Option Image: Option Option Image: Option Option Image: Option Option Image: Option Option Option Image: Option Option Image: Option Option Option Image: Option Option Option Image: Opti	Export Import			
Options Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation	1. Provide the path and file name of the Categories file. Use the '' button to brow 2. Click the Import button.	rse and locate the import file.		
Systems and Groups Source : Token Value Reports Behavior Correlation	Options Location			
	Alerts Source : Source :			
Import		Import	Close	

Figure 17



EventTracker displays a success message:





5.2 Alerts

- 1. Once you have opened "Export Import Utility" via "EventTracker Control Panel", click Alert option, and then click browse.
- 2. Navigate to the knowledge pack folder and select the file with extension ".isalt", e.g. "Alerts_ FireEye NX.isalt" and then click "Import".

Export Import Utility		—	\times
Export Import			
1. Provide the path and file na 2. Click the Import button.	ame of the Alerts file. Use the '' butt	on to browse and locate the import file.	
Options	Location		
Category	Import E-mail settings		
· · ·	Set Active		
 Filters 	 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 configuration section.	
Systems and Groups	Watchlist Configuration		
	Import Watchlist configuration	ion	
	This setting is applicable only f	or alerts which have Advanced watchlist configured.	
Reports	on the console where the alert	ne user should make sure the watchlist groups are available s are imported.	
Behavior Correlation			
0			
	Source :		
	isait		
		Import	ose

Figure 19



EventTracker displays a success message:





5.3 Token Template

For importing "Token Template", please navigate to EventTracker manager web interface.

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





2. Next, click the "Template" tab and then click "Import Configuration".

Parsing Rule	s			
Parsing Rule	Template			
Groups			(Group :
Default			^	
Azure Intune		Ē	۲	Templa





A	/ Admin / Parsing Rules
	C 1 I
Active	Import configuration



3. Now, click "Browse" and navigate to the knowledge packs folder (type "%et_install_path%\Knowledge Packs" in navigation bar) where ".ettd", e.g. "Templates_FireEye NX.ettd" file is located. Wait for few seconds, as templates will be loaded. Once you see the templates, click desired templates and click "Import":

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

Figure 24

5.4 Reports

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



🐁 Export Import Utility		_		\times
Export Import				
1. Provide the path and file name 2. Click the Import button Note : If report(s) contains template	of Schedule Report file. Use the '' button to browse and locate the import file e, first import template and proceed with exportimport utility. Location	÷.		
Category				
○ Filters				
) Alerts	◯ Legacy (*.issch)			
O Systems and Groups	Source :			
O Token Value	19901			
Reports				
O Behavior Correlation				
		_		
	Im	port	Clos	e

Figure 25

 Once you have selected "New (*.etcrx)", a new pop-up window will appear. Click "Select File" and navigate to knowledge pack folder and select file with extension ".etcrx", e.g. "Reports_ FireEye NX.etcrx".

다 Reports Import				
Note : If report(s) contains template, first import ter	nplate and proceed with report import p	rocess.		Calastila
				Select file
Title	Frequency Sh	ow all 🔻	Q Q	
	Sites Groups	Systems	Frequency	Runtime Type

Figure 26

Wait while reports are being populated in below tables. Now, select all the relevant reports and then click Import .

Note: Set run time option is not applicat	ole for Defined Reports and Hourly Reports	
Set run time for report(s) from	AM • at interval of _ minutes	Set
Replace	to Replac	e Assign systems
		Note: Make sure that Site(s), Group(s) and System(s) selections are valid.

Figure 27

EventTracker displays a success message:



Figure 28

5.5 Knowledge Objects

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

		🔎 🛛 Admin 🗸	Tools 🕶 📀
Active Watch Lists	Event Filters	🧭 Parsing Rules	📌 / Da
Alerts	Ventvault	Report Settings	
Behavior Correlation Rules	FAQ Tile Configuration	Systems	
🗞 Behavior Correlation Settings	Group Management	QQ Users	
yr sc Casebook Configuration	Q IP Lookup Configuration	r Weights	Systems since the last 24 hours
eter Category	·☆ Knowledge Objects	Windows Agent Config	
Diagnostics	O Manager		

Figure 29

2. Next, click the "import object" icon:





 A pop-up box will appear, click "Browse" in that and navigate to knowledge packs folder (type "%et_install_path%\Knowledge Packs" in navigation bar) with the extension ".etko", e.g. "KO_ FireEye NX.etko" and then click "Upload".

Import	
KO_ <product name="">.etko</product>	🗁 Browse Upload

Figure 31

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 EventTracker manager web interface.
- 2. Navigate to **Dashboard** \rightarrow **My Dashboard**.
- 3. In "My Dashboard", Click Import:



≡	EventTracker 🕀						
	Home						
٩	My Dashboard						
	Threats						
	Incidents						
	Behavior Correlation						
	Change Audit						
	Compliance						



🟫 / Dashboard / My Dashboard
- 🖉 🕸 🏚 🗊
Import configuration



- 4. Click **Browse** and navigate to knowledge pack folder (type **"%et_install_path%\Knowledge Packs**" in navigation bar) where **".etwd**", **e.g. "Dashboards_ FireEye NX.etwd**" is saved and click **"Upload**".
- 5. Wait while EventTracker populates all the available dashboards. Now, choose "Select All" and click "Import".

Import	
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.	
🗁 Browse	Upload
Available widgets	
Select All	









6. Verifying knowledge pack in EventTracker

6.1 Saved Searches

- 1. Login to EventTracker manager web interface.
- 2. Click Admin dropdown, and then click Categories.
- 3. In **Category Tree** to view imported categories, scroll down and expand "**FireEye NX**" group folder to view the imported categories:



Figure 37



6.2 Alerts

- 1. In the EventTracker manager web interface, click the Admin dropdown, and then click Alerts.
- In search box enter "<search criteria> e.g. "FireEye" and then click Search.
 EventTracker displays an alert related to "FireEye":

Alerts									📌 / Admin / Aler
Show All							Search by	Alert name 🔻	FireEye 🔍 🦉
142 Available Alerts Total number of alerts available	26 Active Alerts Total number of active a	lerts			142 System/Use	System User r Defined Aler m and user defi	113 29 ts ned alerts	142 Alerts by Count of a	Critical 14 High Serous 18 Serous 18 Threat Level
Activate Now Click 'Activate	Now' after making all change	5							Total: 3 Page Size 25 🔻
Alert Name 🔨		Threat	Active	Email	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
🔲 🖗 FireEye: A command and Control connectio	n has been blocked	•							FireEye Network Security and Forensics
βδ FireEye: A website with malicious contents	has been discovered.	•							FireEye Network Security and Forensics
βŷ FireEye: File attachment with a malicious ex	ecutable payload detected	•							FireEye Network Security and Forensics



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 **"<product name/ report group name>"** e.g. "**FireEye NX**" group folder to view the imported Templates.

Parsing Rules							
Parsing Rule	Template						
Groups			(+)	Group : FireEye			
Default							
FireEye		Ī	1	Template Name			
Windows		Ē	٢	FireEye			

Figure 39



6.4 Reports

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





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

Report Configuration					
Scheduled Queued I D	efined				
Report Groups		+ ***	Rep	orts config	guration: FireEye
🖕 Security			\oplus	Ü 🕗	
Compliance					Title
Gerations				£\$3	FireEye - Infection match Activities
🔓 Flex				£3	FireEye - Domain match Activities
🔁 FireEye	Ē	1		£3	FireEye - Malware Callback Activities
🔁 Windows		1		£\$3	FireEye - Web Infection Activities
				£\$3	FireEye - Malware Object Activities



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 "**FireEye**" group folder to view the imported Knowledge objects.



Knowledge Objects								
Search objects	Q Q Activate Now							
Groups 🕂 🖉 🗓 Object name FireEye Events Applies to FireEye Network Security and Forensics								
FireEye	Rules							
FireEye Events 🧭 🔟	Title	Event source						
	🛨 🛛 FireEye Events	syslog						
Message Signature: (?i)CEF\:\d\ FireEye\ MPS\								
	Message Exception:							

6.6 Dashboards

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





2. Select "**Customize daslets**" And (a) type "**FireEye**" in the search bar.









Figure 45

