Netsurion | EventTracker®

# How to – Configure FireEye Network Security and Forensics (NX) to forward logs to EventTracker

## 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.

# Table of Contents

1. Overview ..... 3
2. Prerequisites ..... 3
3. Integrating FireEye NX with EventTracker ..... 3
   3.1 Configuring a Syslog Forwarding ..... 3

# 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

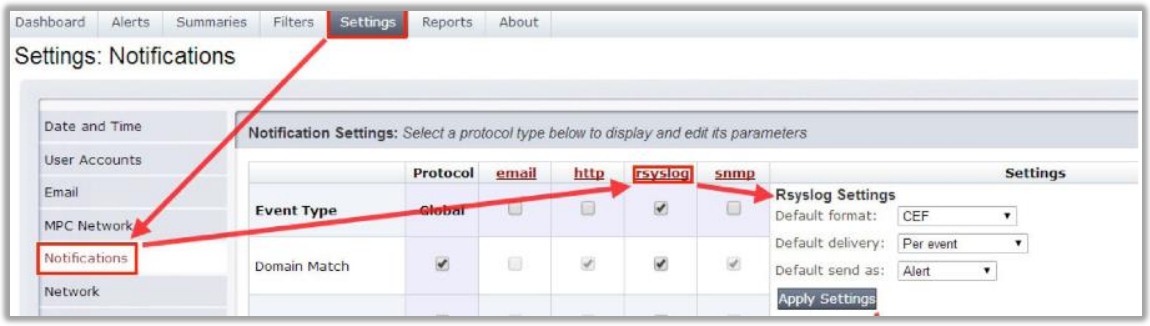


Figure 1

5. 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.

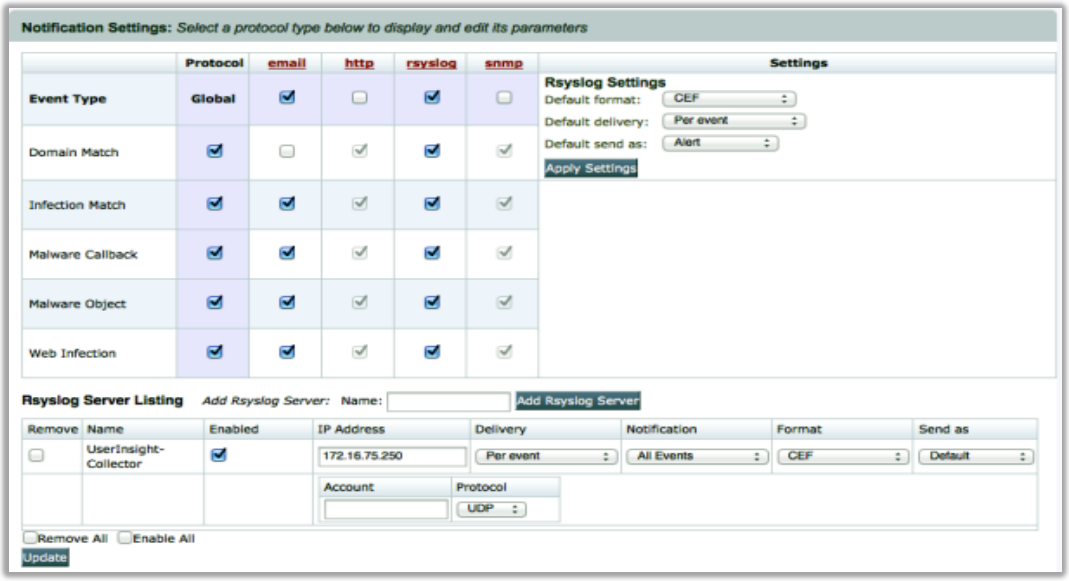


Figure 2