Netsurion. | EventTracker®

How to – Configure EventTracker Endpoint Security to forward logs to EventTracker

EventTracker v9.2x and above

Publication Date: January 15, 2021

Abstract

This guide provides instructions to configure EventTracker Endpoint Security to send its logs to EventTracker.

Scope

The configuration details in this guide are consistent with EventTracker version v9.2x or above and **EventTracker Endpoint Security**

Audience

Administrators who are assigned task to monitor EventTracker Endpoint Security 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 laws 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.

Table of Contents

1. Overview

EventTracker Endpoint Security provides a predictive threat prevention platform by applying deep learning with its advanced artificial intelligences to cybersecurity.
Its on-device solution protects against zero-day threats and APT attacks with unmatched accuracy. It safeguards the enterprise's endpoints and mobile devices against threats on any infrastructure and provides protection against unknown and evasive cyber-attacks.

EventTracker helps to monitor events from EventTracker Endpoint Security. Its dashboard displays information for EventTracker Endpoint Security and Endpoint Security. Dashboard shows any threat detected and prevented on hosts, login activities, top high-risk users and hosts, malware family detected.

EventTracker reports will provide threat activity, administrator activity and login activity information containing username, hostname, Ip, virus/malware and other important details.

EventTracker's built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

2. Prerequisites

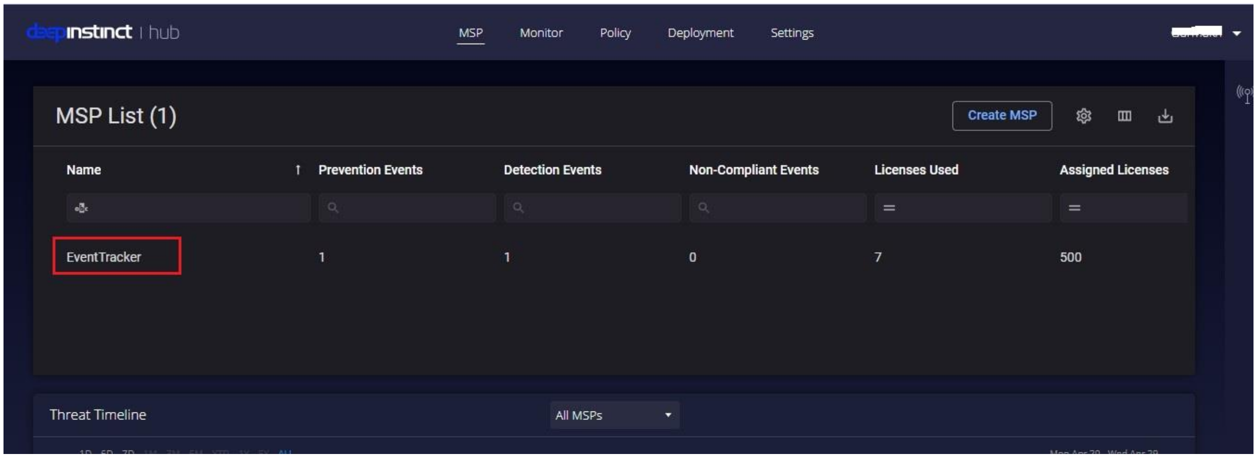
- Admin privileges for **EventTracker Endpoint Security**.
- **EventTracker agent** should be installed in the system.

3. Integration of EventTracker Endpoint Security with EventTracker

3.1 Integration can be performed via syslog configuration

Follow the below steps to configure syslog.

1. Login to the EventTracker Endpoint Security console.
2. Click on the MSP Name.



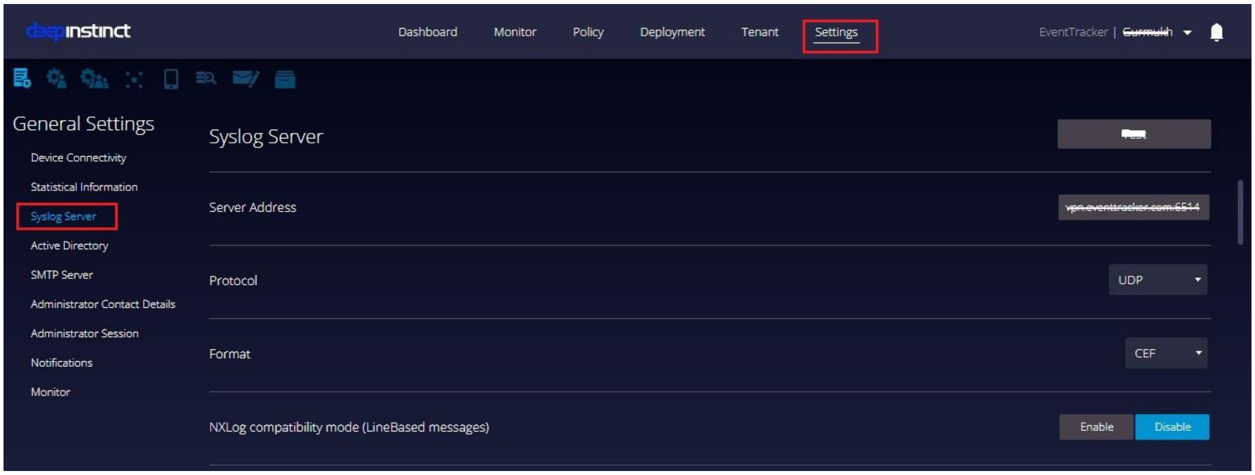
MSP List (1)

Name	Prevention Events	Detection Events	Non-Compliant Events	Licenses Used	Assigned Licenses
EventTracker	1	1	0	7	500

Threat Timeline — All MSPs

Figure 1

3. A new page opens, go to **setting > syslog server.**
4. Fill in the required details:



Syslog Server: [redacted]

Server Address: [redacted]

Protocol: UDP

Format: CEF

NXLog compatibility mode (LineBased messages): Enable [✓ Disable]

Figure 2

- Syslog Server as **Manager Name**
- Server Address as **EventTracker Manager IP**
- Protocol as **UDP**.
- Format as **CEF**.

Integration is complete, EventTracker will receive EventTracker Endpoint Security logs.