Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configuring TrapX DeceptionGrid to Forward Logs with EventTracker

EventTracker v9.2x and above

Author: Marketing

February 10, 2022

Abstract

This guide provides instructions to configure the **TrapX DeceptionGrid Syslog** to send its logs to EventTracker.

Scope

The configuration details in this guide are consistent with the EventTracker version v9.2x or above and TrapX DeceptionGrid v6.1.

Audience

The Administrators who are assigned the task to monitor the TrapX DeceptionGrid events using EventTracker.

Table of Contents

1. Overview

TrapX is a new generation of deception technology that provides real-time breach detection and prevention. Its field-proven solution deceives would-be attackers with turn-key decoys (traps) that imitate true assets. Traps can be deployed creating a virtual minefield for cyberattacks, alerting you to any malicious activity with actionable intelligence immediately.

EventTracker integrates with TrapX DeceptionGrid and helps you monitor crucial events such as threats detected and malicious traffic events.

EventTracker provides insights about the TrapX DeceptionGrid scan events and connection events. EventTracker reports TrapX DeceptionGrid scan events and connection events which provide a detailed summary for various events like the scan hosts, device connected, etc.

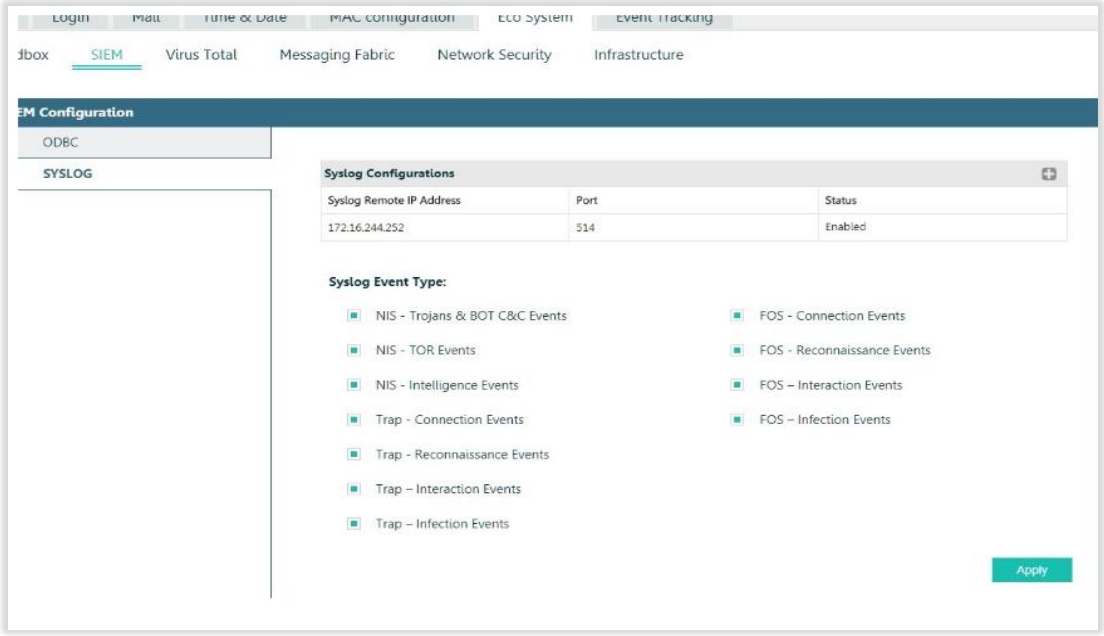
2. Prerequisites

- **Admin** access to the **TrapX DeceptionGrid** console.
- **EventTracker** Manager/Sensor should be installed and running.

3. Configuring TrapX DeceptionGrid Syslog Logging

Refer to the following steps to configure the TrapX DeceptionGrid Syslog to send the logs to EventTracker.

1. Go to the portal and navigate to **Settings** > **General** > **Eco System** > **SIEM** > **Syslog**.
2. Under Syslog server, click , Remote IP enter the **EventTracker** IP address and port to 514.
3. Click **Add**.
4. Check all the Event types.
5. Click **Apply**.



About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both. Netsurion Managed Threat Protection combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion Secure Edge Networking delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all 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 netsurion.com or follow us on Twitter or LinkedIn.

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