Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configuring Cisco Catalyst Syslog with EventTracker

EventTracker v9.2 and above

Publication Date:

April 12, 2021

Abstract

This guide helps you in configuring **Cisco Catalyst** with EventTracker to receive **Cisco Catalyst** events. In this guide, you will find the detailed procedures required for monitoring **Cisco Catalyst.**

Scope

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

Audience

Administrators, who are assigned the task to monitor and manage **Cisco Catalyst** events using **EventTracker.**

Table of Contents

1. Overview

This guide helps you in configuring **Cisco Catalyst** with EventTracker to receive activity logs via syslog. In this guide, you will find the detailed procedures required for monitoring **Cisco Catalyst.**

EventTracker helps to monitor events from **Cisco Catalyst**. Its dashboard, alerts and reports will help you to detect attacks, suspicious host and accounts.

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

2. Prerequisites

Prior to configuring Cisco Catalyst and the EventTracker, ensure that you meet the following prerequisites:

- EventTracker v9.x or above should be installed.
- Cisco Catalyst should be installed and proper access permissions to make configuration changes.
- Administrative access on the EventTracker.

2.1 Integration of Cisco Catalyst with EventTracker

Cisco Catalyst can be integrated with EventTracker via syslog configuration.
To configure Cisco Catalyst to forward the log to EventTracker:

1. Log in to your Cisco CatOS user interface.
2. Type the following command to access privileged EXEC mode:
   Enable
3. Configure the system to timestamp messages:
   Set logging timestamp enable.
4. Type the IP address of EventTracker:
   Set logging server <IP address>
5. Limit messages that are logged by selecting a severity level:
   Set logging server severity.
6. Configure the facility level that should be used in the message. The default is local7.
   Set logging server facility.
7. Enable the switch to send syslog messages to the EventTracker.
   Set logging server enable.

Events forwarded to EventTracker by Cisco Catalyst are displayed on the **Log Search** tab of EventTracker.

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

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