Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configuring Cisco ISE to Forward Logs to EventTracker

EventTracker v9.3 and above

Publication Date:

September 06, 2021

Abstract

This guide helps you in configuring **Cisco Identity Service Engine (ISE) with** EventTracker to receive **Cisco Identity Service Engine (ISE)** events.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or above and Cisco Identity Service Engine (ISE).

Audience

Administrators who are assigned the task to monitor Cisco Identity Service Engine (ISE) events using EventTracker.

Table of Contents

1. Overview

Cisco Identity Services Engine (ISE) is a network administration product (which is either a Cisco ISE appliance or Virtual Machine) that helps in creating and enforcing security and access policies for endpoint devices of the company's routers and switches.

EventTracker helps to monitor events from **Cisco ISE**. Its dashboard, alerts and reports will help you to track authentication activities, endpoint compliance status, admin, and operations activity, to keep you informed about its activities. It will trigger alert whenever user authenticate fails, receive invalid or bad HTTP request or ERS xml input suspect for XSS or Injection attack.

2. Prerequisites

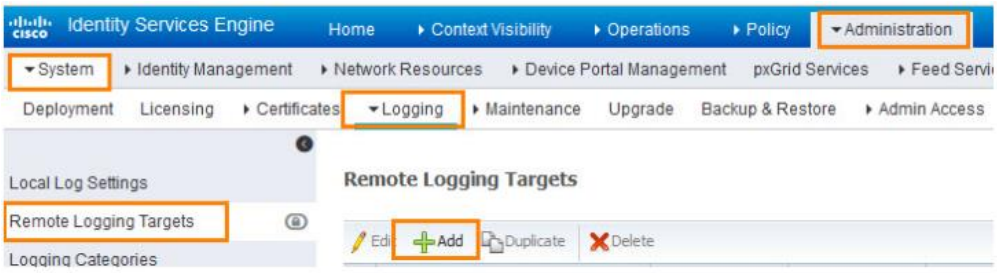
- A user who is global administrator.
- EventTracker manager IP address. (Public IP, if ISE hosted in VMware cloud offering in AWS)
- Syslog port (e.g., 514) should be allowed in firewall.

3. Configuring Cisco Identity Services Engine (ISE) to Forward Logs to EventTracker

Cisco ISE can be integrated with EventTracker by forwarding the syslog to EventTracker manager.

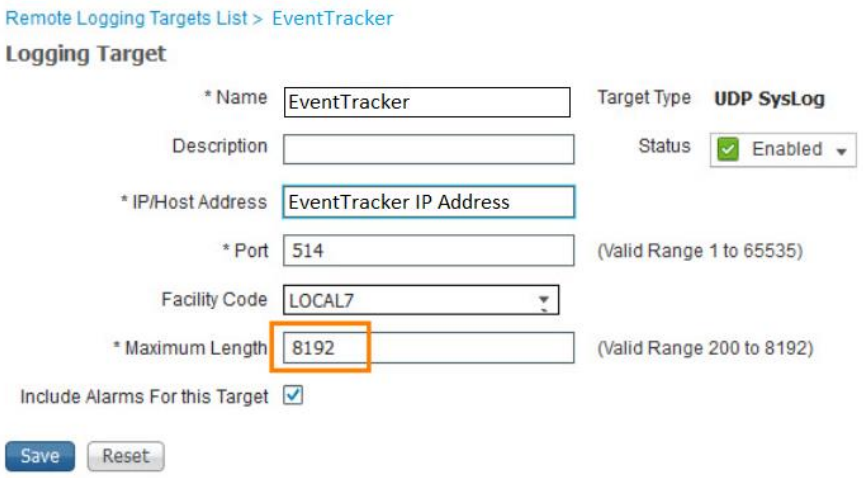
3.1 Forwarding syslog data to EventTracker

1. Login to your Cisco ISE Administration Interface.
2. Navigate to **Administration > System > Logging > Remote Logging Targets**.
3. Click **Add**.

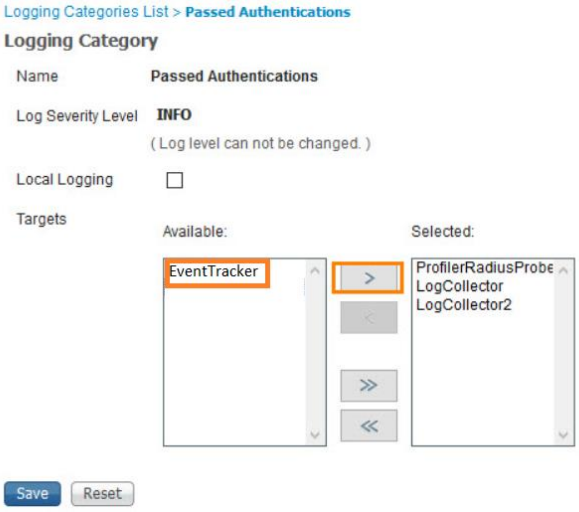


4. Configure the below fields.

Fields	Value
Name	EventTracker
IP Address	<EventTracker public IP>
Port	<EventTracker port. e.g., 514>
Target Type	UDP
Maximum Length	8192



5. Click **Save**.
6. Additional Configuration of Logging categories. Navigate to **Administration > System > Logging > Logging** Categories.
7. You will be presented with list of available logging categories. Select a logging category and click **Edit**.
8. For **Log Severity**, select a severity for the logging category.
9. In the **Target** field, add your remote logging target for EventTracker (as created in previous steps).



10. Click **Save**. (Repeat these steps for all categories)

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