Netsurion | EventTracker®

How to- Configure Cisco Expressway to forward logs to EventTracker

EventTracker v9.x and above

Publication Date: April 21, 2020

Abstract

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

Scope

The configurations detailed in this guide are consistent with EventTracker version v9.x or above and **Cisco Expressway.**

Audience

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

Table of Contents

1. Overview

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

EventTracker helps to monitor events from **Cisco Expressway**. It's dashboard, alerts and reports will help you to detect security related attack and authentication failures detected in Cisco Expressway.

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

Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems long before a disastrous failure occurs.

2. Prerequisites

- **EventTracker v9.x** or **above** should be installed.
- **Cisco Expressway** should be configured.
- **Local Admin permission** for the workstation.

3. Integration of Cisco Expressway with EventTracker

3.1 Enabling Syslog

1. Go to Maintenance > Logging and enter the IP addresses or Fully Qualified Domain Names (FQDNs) of the EventTracker Manager to which this system will send log messages.
2. Click on the **Options** for each server.
3. Specify the Transport protocol and Port you wish to use. If you choose to use TLS, you will see the option to enable Certificate Revocation List (CRL) checking for the syslog server.
4. In the Message Format field, select the writing format for remote syslog messages. The default is Legacy BSD.
5. Use the Filter by Severity option to select how much detail to send. The Expressway sends messages of the selected severity and more severe messages.
6. Use the Filter by Keywords option if you only want to send messages with certain keywords.
7. Click Save.

   Note:
   - The Filter by Keywords option is applied to messages already filtered by severity.
   - You can use up to five keywords, which includes groups of words (for example 'login successful'), separated by commas.
   - You can use a maximum of 256 characters in the keyword search.

- We recommend that you search for the most relevant keywords first to avoid any impact on system performance. This ensures the system pushes the relevant log messages to the syslog server at the earliest opportunity.