Netsurion. | EventTracker®

How to- Configure AudioCodes to forward logs to EventTracker

EventTracker v9.2 and above

Publication Date: August 31, 2020

Abstract

This guide will facilitate an AudioCodes user to send logs to EventTracker.

Scope

The configuration details in this guide are consistent with EventTracker 9.2 or later and AudioCodes SBC's (VE) v7.2.

Audience

Administrators who want to monitor the AudioCodes 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. Introduction

AudioCodes Ltd is a leading vendor of advanced voice networking and media processing solutions for the digital workplace. AudioCodes's SBC is a device that protects data and voice over a VoIP network. It has multiple deployment methods, one of which is, Mediant VE (built for deployment in virtualized data centers, public clouds, and NFV environments).

EventTracker can be integrated with AudioCodes using its syslog. It helps you to monitor the outgoing and incoming call activities by the client based on user geolocation, username, and login attributes which helps you to find the unauthorized access attempt to the login page.

EventTracker also alerts you if any unauthorized access attempts to the login page and IP address are added to the blacklist.

EventTracker generates a schedule report for user login activities, incoming and outgoing calls in AudioCodes. It displays incoming and outgoing calls by location and call activities by source and destination IP address, etc.

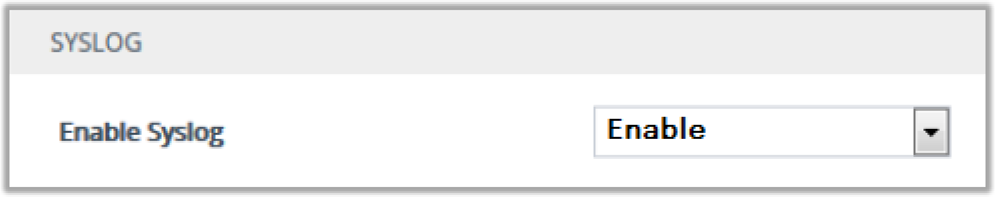
1.1 Pre-requisites

- The host machine should have installed the **EventTracker agent**.
- Administrator privilege for AudioCodes web interface.
- AudioCodes SBC's (VE) v7.2 should be installed.

1.2 Integration of AudioCodes events to EventTracker

1.2.1 Enabling syslog

1. Connect to the SBC Web interface, and then log in using the default credentials.
2. Open the Logging Settings page (**TROUBLESHOOT > Logging > Logging Settings**).
3. Configure the following parameters.
   a. From the '**Enable Syslog**' drop-down list, select "**Enable".**


SYSLOG

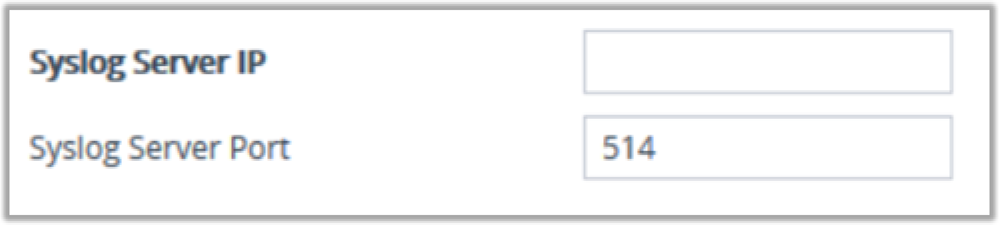
Enable Syslog: Enable

Figure 1

   b. Please fill the below information.

In the **'Syslog Server IP**' field, enter the “**EventTracker IP address”**.

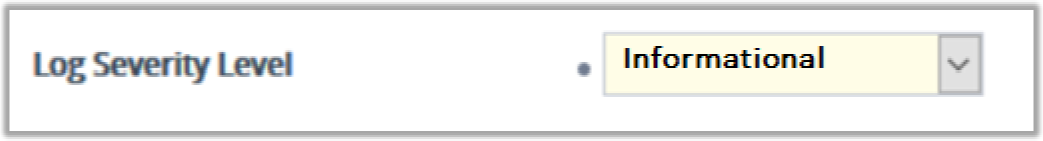
In the **‘Syslog Server Port’** field, enter the port number **514.**



Syslog Server IP	
Syslog Server Port	514

Figure 2

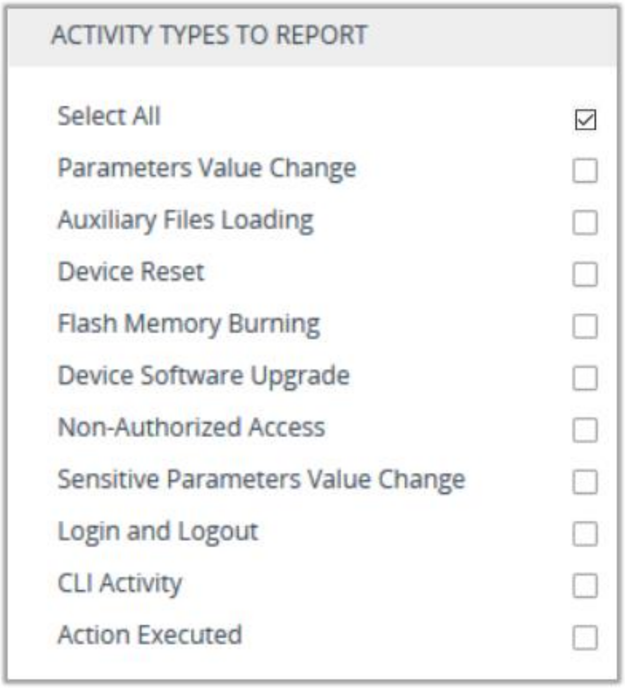
c. In the ‘**Log Severity Level**’ drop-down list, select the severity level, “**Informational”.**



Log Severity Level • Informational

Figure 3

d. To configure reporting of management user activities, under the “**Activity Types to Report group**”, select the actions to report to the syslog server. Choose, “**Select All**”:



ACTIVITY TYPES TO REPORT

- Select All ☑
- Parameters Value Change □
- Auxiliary Files Loading □
- Device Reset □
- Flash Memory Burning □
- Device Software Upgrade □
- Non-Authorized Access □
- Sensitive Parameters Value Change □
- Login and Logout □
- CLI Activity □
- Action Executed □

Figure 4

4. Click **Apply** to apply your settings.