How to Configure FortiNAC with EventTracker

EventTracker v9.x and above

Publication Date: July 19, 2019

Abstract

This guide provides instructions to retrieve FortiNAC event logs and integrate it with EventTracker. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor FortiNAC.

Audience

The configurations detailed in this guide are consistent with EventTracker version v9.x or above and FortiNAC v8.3 and v8.5.

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

Overview

Network Access Control (NAC) is an approach to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), the user or system authentication and network security enforcement. FortiNAC provides visibility to all administrators to see everything connected to their network, as well as the ability to control those devices and users, including dynamic, automated responses.

EventTracker collects the event logs delivered from FortiNAC and filters them out to get some critical event types for creating reports, dashboard, and alerts. Among the even types, we are considering: Admin user login success/ failure, rogue MAC address detection, switch interface up/ down and host session login/ logout.

Prerequisites

- EventTracker agents should be installed in a host system/ server.
- PowerShell 5.0 should be installed on the host system/ server.
- User should have administrative privilege on the host system/ server to run PowerShell.
- User must have root-level access to FortiNAC console.

Configuring FortiNAC to forward the log to EventTracker

The logs can be forwarded to EventTracker via configuring "**syslog**", **SNMP trap** or **API to an external server**. In this documentation, we will use **syslog "CEF"** format.

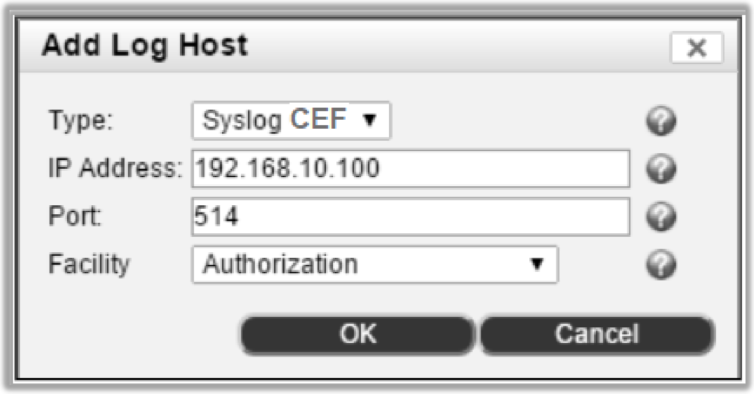
Integration is divided into 2 steps. STEP 1 for enabling **"External" logging**, and STEP 2 for adding "**Log Host server**".

STEP 1: Enable "External" Logging

1. Click **Logs>Event Management**.
2. Use the filters to locate the appropriate event.
3. For each event that should be logged externally, select one or more events and click the **Options** button. Select one of the following:
    - **External**—Logs only to an external host.
    - **Internal & External**—Logs both to an internal events database and an external host.

STEP 2: Adding “Log Host” server

1. Click **System > Settings**.
2. In the tree on the left select System **Communication > Log Receivers**.
3. Click **Add** to add a log host.
4. Select “**Type**” field as “**Syslog Command Event Format (CEF)**”
5. Enter the IP address of the EventTracker server.
6. Enter the configuration parameters for the type of log host. The standard port information for each host type is automatically entered.
7. Click **OK**.



Add Log Host

Type: Syslog CEF

IP Address: 192.168.10.100

Port: 514

Facility: Authorization

Figure 1

Field	Definition
Type	Type of server that will receive Event and Alarm messages. Options include: Syslog CSV, SNMP Trap, and **Syslog Command Event Format (CEF)**.
IP Address	IP Address of the server that will receive event and alarm messages.
Port	Connection port on the server. For syslog CSV and syslog CEF servers, the default=514. For SNMP Trap servers the default=162
Facility	Displays only when syslog is selected as the Type. It allows you to configure the message type. The default is 4. Options include: 0 Kernel messages 1 User-level messages 2 Mail system 3 System daemons 4 Security/authorization messages 5 Messages generated internally by syslog 6 Line printer subsystem 7 Network news subsystem 8 UUCP subsystem 9 Clock daemon 10 Security/authorization messages 11 FTP daemon

Field	Definition
	12 NTP subsystem 13 Log audit 14 Log alert 15 Clock daemon 16 Local use 0 (local0) 17 Local use 1 (local1) 18 Local use 2 (local2) 19 Local use 3 (local3) 20 Local use 4 (local4) 21 Local use 5 (local5) 22 Local use 6 (local6) 23 Local use 7 (local7)
Security String	Displays only when SNMP is selected as the type. The security string sent with the Event and Alarm message.