Netsurion™ | EventTracker

How to- Configure FortiSandbox to forward logs to EventTracker

EventTracker v8.0 and above

Publication Date: October 8, 2019

Abstract

This guide helps you in configuring **FortiSandbox v3.1.0** and **EventTracker** to receive FortiSandbox events. You will find the detailed procedures required for monitoring FortiSandbox v3.1.0.

Scope

The configurations detailed in this guide are consistent with **EventTracker v8.x** and later, **FortiSandbox v3.1.0.**

Audience

FortiSandbox users, who wish to forward Events to EventTracker and monitor events 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.

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Netsurion™ | EventTracker

1.Overview

FortiSandbox Cloud is a cloud-based managed option for businesses looking for a turnkey solution. It delivers the same rapid detection and automated response as the physical FortiSandbox appliance, but is accessed through the cloud, and provides unlimited flexibility to complement entry and mid-range FortiGates.

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

- Admin privileges for **FortiSandbox v3.1.0** and should be installed.
- If Firewall existed between **EventTracker** and **FortiSandbox** appliance, please allow for port number 514.

3.Integration of FortiSandbox with EventTracker using syslog

FortiSandbox logs we can get by using syslog.

To create a syslog server:

1. Please login into the FortiSandbox admin portal.
2. Go to **Log & Reports > Log Servers**.
3. Select **+** Create New from the toolbar.
4. Enter the following information.
    - **Name**: Enter a name for the syslog server on **FortiSandbox**.
    - **Type**: Select Log Server Type from the drop-down list as **syslog**.
    - **Log Server Address**: Enter **EventTracker IP** address.
    - **Port**: Enter the syslog server port number **514**.
    - **Status**: Select to **enable** sending logs to the EventTracker.
    - **Log Level**: Please select **Alert logs**, **Critical logs**, **error logs**, **warning logs**, and **information logs.**

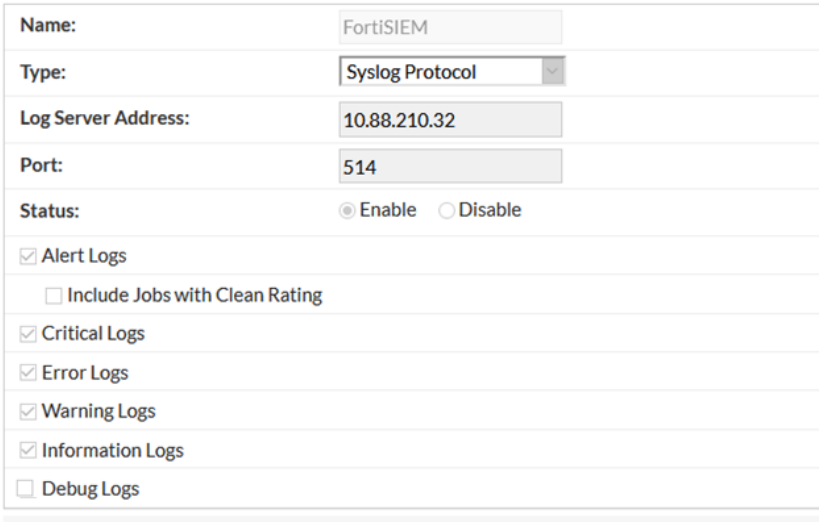

Figure 1

5. Select **OK** to save the entry.