Netsurion | EventTracker®

# How to-Configure Kaspersky Security Center to send logs to EventTracker

## EventTracker v9.0 and above

Publication Date: December 5, 2019

# Abstract

This guide will facilitate a **Kaspersky Security Center** user to send logs to **EventTracker.**

# Scope

The configurations detailed in this guide are consistent with **EventTracker 9.x or later and Kaspersky Security Center 10 and later.**

# Audience

Administrators who want to monitor the **Kaspersky Security Center** using **EventTracker**.

# Table of Contents

# 1. Introduction

Kaspersky Security Center offers consumer security products, such as anti-virus, anti-malware and firewall applications. Besides, to the security systems designed for small businesses, corporations, and large enterprises.

Kaspersky Security Center can be integrated with EventTracker via syslog. EventTracker can fetch the device management, object management, virus detected, vulnerabilities detected events on endpoints.

Dashboards provide a view of unmanaged endpoints, inactive endpoints and threat detected on the endpoint.

By using a detailed report, we can understand which endpoint is infected by malware, endpoints which are inactive for more than seven days and provide information about the unmanaged endpoint in the environment. Alerts are triggered whenever malware is detected, device blocked on endpoints, etc.

## 1.1 Pre-requisites

- **EventTracker 9.x or later** should be installed.
- **EventTracker Agent** to be installed on Kaspersky Security Center administrative server.
- **Advance licensed Kaspersky** is required to forward the syslog.

## 1.2 Enabling Kaspersky Event Logs and Send logs to EventTracker

1. Open Kaspersky Security Center 10 and Go to **Administration Server.**

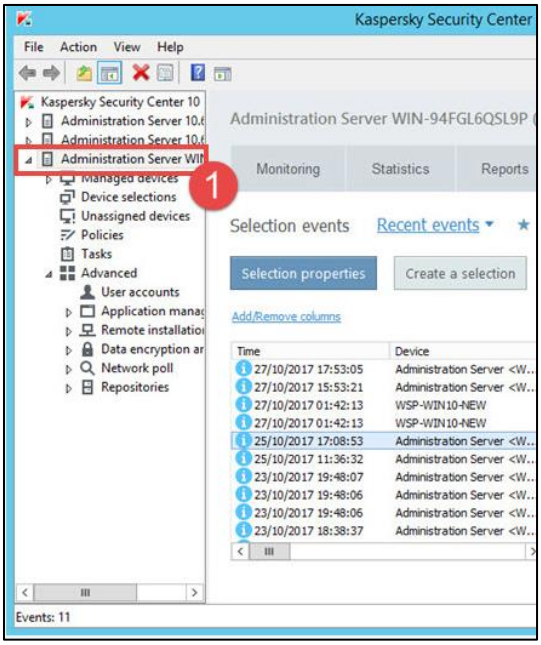


Figure 1

2. In Admin **Administration Server**, select **Events** in the right frame.
3. Click on **Configure notifications and event export.**

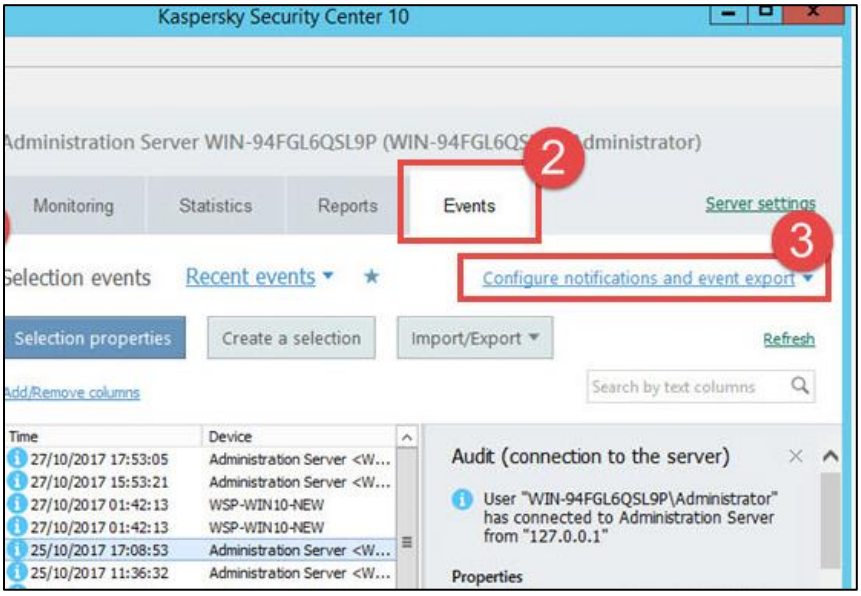


Figure 2

4. Select **Configure export to the SIEM system**.

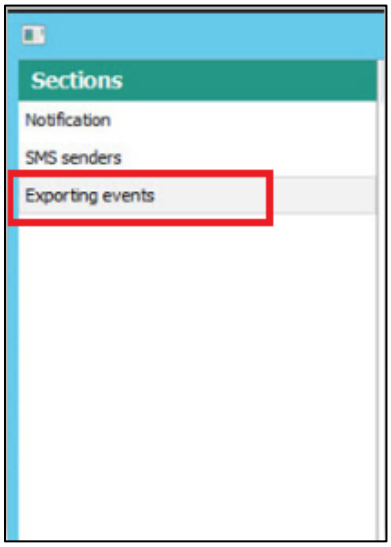


Figure 3

5. Select the checkbox **Automatically export events to the SIEM system database**.

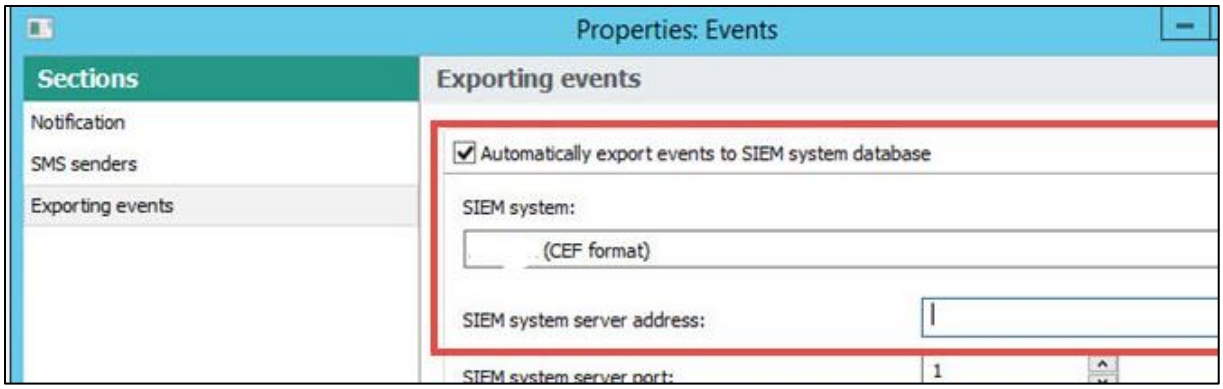


Figure 4

6. Choose the **SIEM** system. Specify the EventTracker Manager address.
7. Click **OK**.

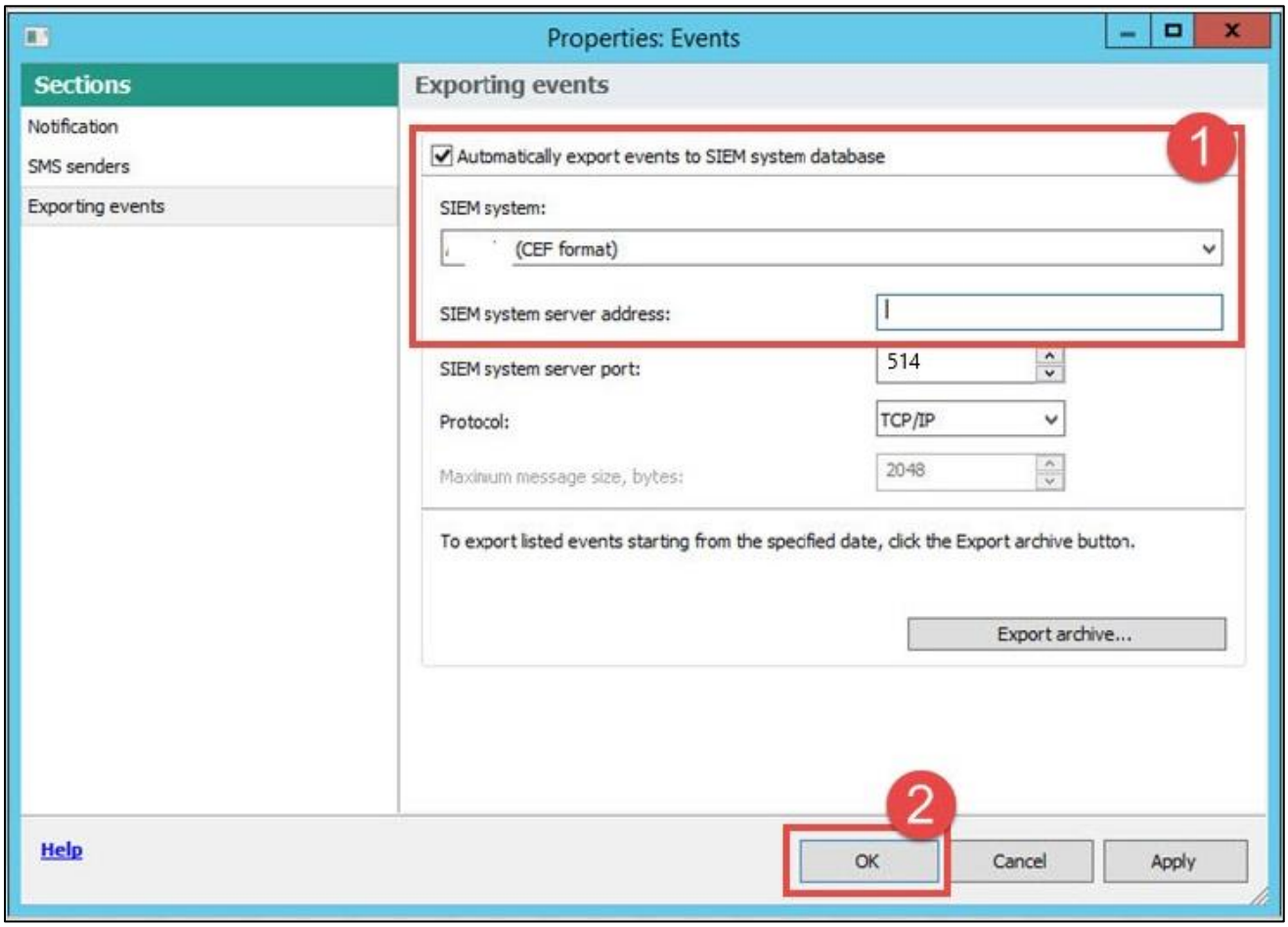


Figure 5