

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

EventTracker v9.0 and above

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**.

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

1. Introduction.....	3
1.1 Pre-requisites.....	3
1.2 Enabling Kaspersky Event Logs and Send logs to EventTracker	3

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**.

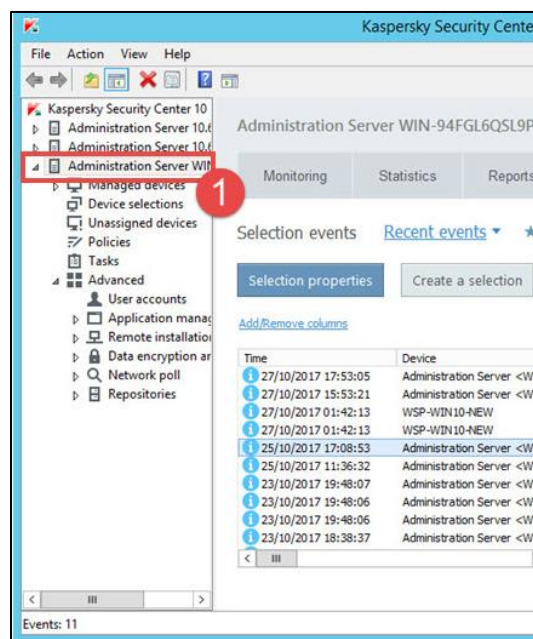


Figure 1

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

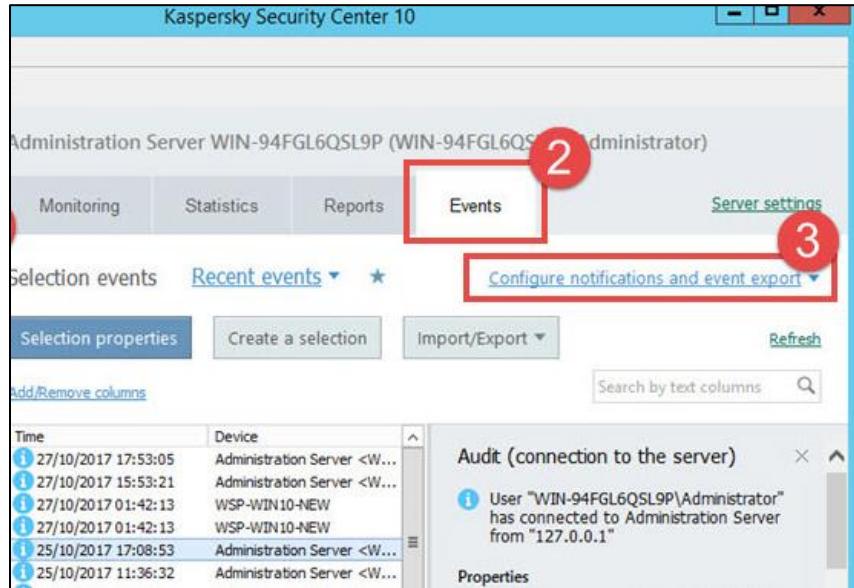


Figure 2

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

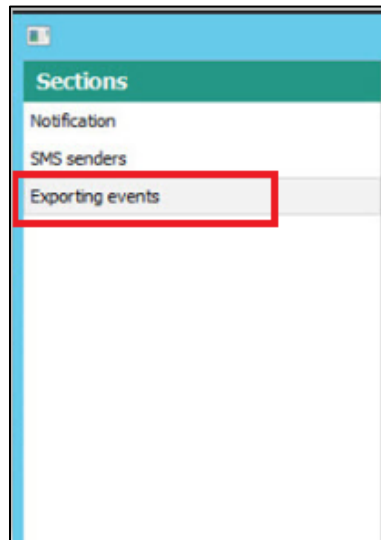


Figure 3

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

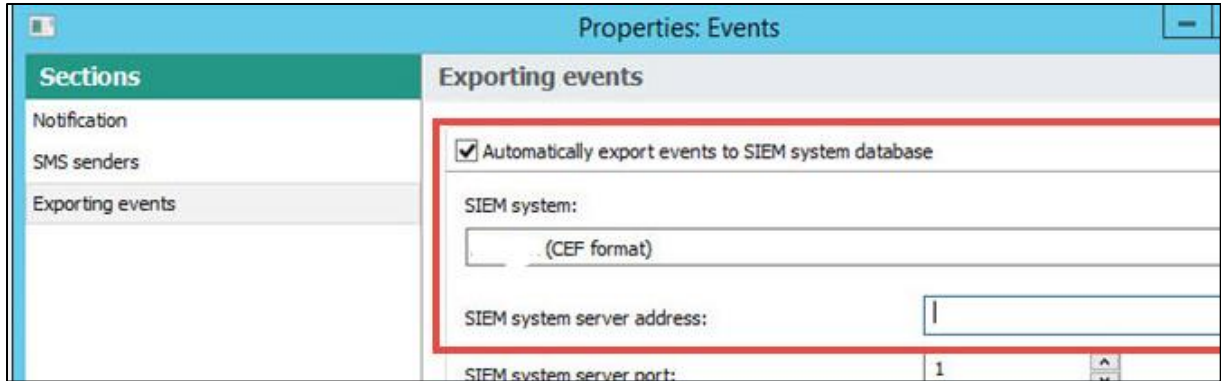


Figure 4

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

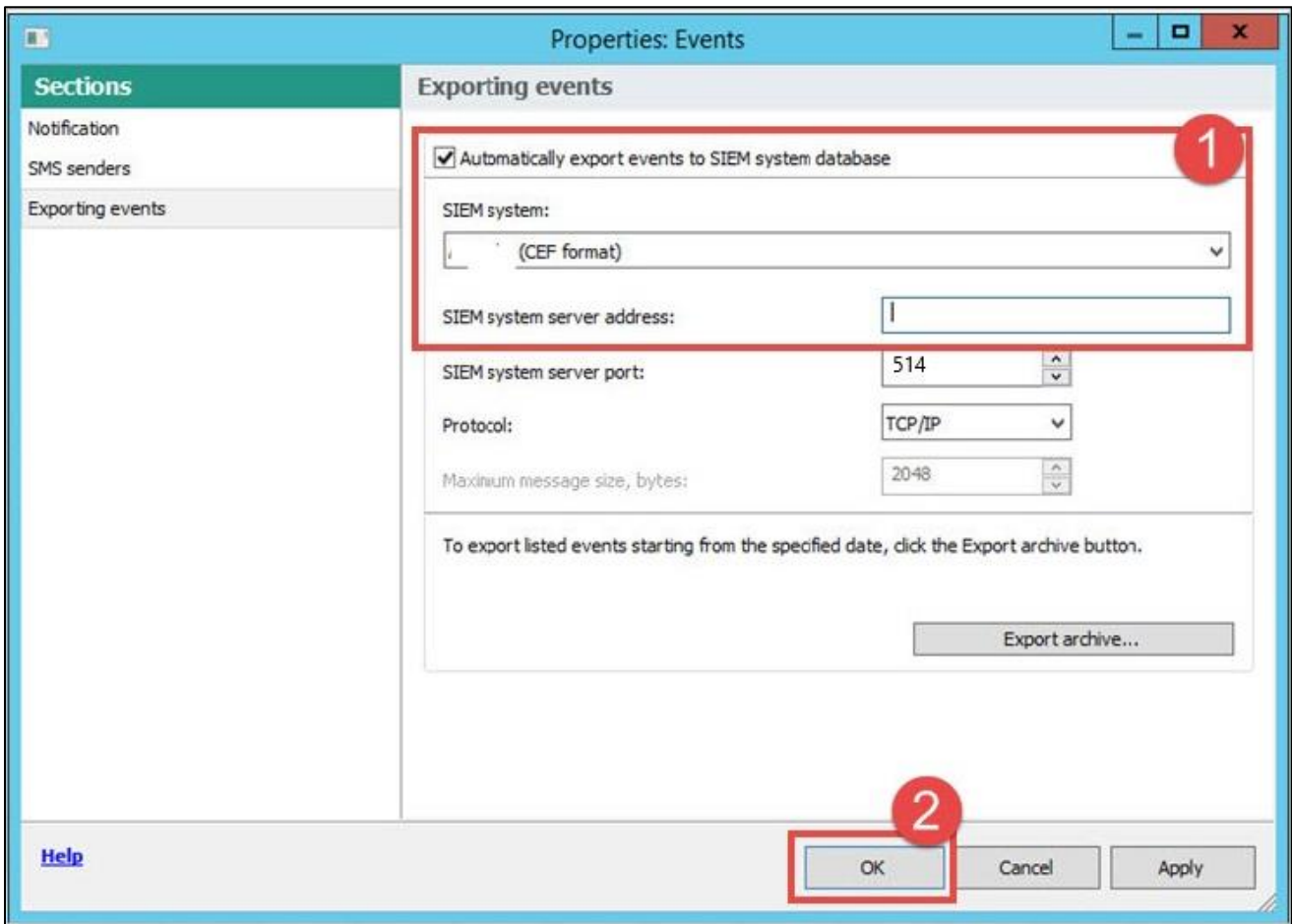


Figure 5