

Integrate Kaspersky Security Center EventTracker v9.0 and above

Publication Date: September 30, 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.

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.	Int	roduction	3
	1.1.	Pre-requisites	3
	1.2.	Enabling Kaspersky Event Logs and Sending logs to EventTracker	3
2.	Ev	entTracker Knowledge Pack	6
	2.1.	Categories	6
	2.2.	Alerts	7
	2.3.	Report	7
3.	Im	porting Kaspersky Security Center knowledge pack into EventTracker	9
	3.1.	Category	9
	3.2.	Alerts	. 10
	3.3.	Flex Reports	. 11
	3.4.	Token Templates	. 12
4.	Ve	rifying Kaspersky Security Center knowledge pack in EventTracker	. 15
	4.1.	Categories	. 15
	4.2.	Alerts	. 15
	4.3.	Reports	. 16
	4.4.	Token Template	. 17
5.	Sa	mple Dashboards	. 18



1.Introduction

Kaspersky Lab offers consumer security products, such as anti-virus, anti-malware and firewall applications, in addition to security systems designed for small businesses, corporations and large enterprises. Corporate solutions include protection for workstations, file servers, mail servers, payment gateways, banking servers, mobile devices, and internet gateways managed through a centralized administration kit. These applications are also available in bundled security suites scaled to fit the requirements of organizations of varying sizes.

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 Sending 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.

Ka	spersky Security Center 1	0			X	
Administration Serv	er WIN-94FGL6QSL9P (\	WIN	-94FGL6Q5	dministrator)		
Monitoring	Statistics Reports	L	Events	Server s	ettings	
Selection events Selection properties	Recent events	Im	Configure n	otifications and event exp	Refresh	
Add/Remove columns				Search by text columns	Q	
Time	Device	~				
 27/10/2017 17:53:05 27/10/2017 15:53:21 27/10/2017 01:42:13 27/10/2017 01:42:13 	Administration Server <w Administration Server <w WSP-WIN10-NEW WSP-WIN10-NEW</w </w 		Audit (connection to the server) User "WIN-94FGL6QSL9P\Administrator" has connected to Administration Server from "127.0.0.1"			
25/10/2017 17:08:53 25/10/2017 11:36:32	Administration Server <w Administration Server <w< td=""><td>Ξ</td><td colspan="4">Properties</td></w<></w 	Ξ	Properties			

Figure 2

4. Select Configure export to the SIEM system.

5						
Sections						
Notification						
SMS senders						
Exporting events						

Figure 3



5. Select the check box Automatically export events to the SIEM system database.

	Properties: Events
Sections	Exporting events
Notification SMS senders	Automatically export events to SIEM system database
Exporting events	SIEM system:
	(CEF format)
	SIEM system server address:
	SIEM system server port:



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

	Properties: Events	_ _ ×			
Sections	Exporting events				
Notification SMS senders	Automatically export events to SIEM sys	stem database			
Exporting events	SIEM system: (CEF format)				
	SIEM system server address:	1			
	SIEM system server port:	514			
	Protocol:	TCP/IP V			
	Maximum message size, bytes:	2048			
	To export listed events starting from the s	specified date, dick the Export archive button. Export archive			
		2			
<u>Help</u>		OK Cancel Apply			

Figure 5



2.EventTracker Knowledge Pack

Once Kaspersky Security Center events are enabled and Kaspersky Security Center events are received in EventTracker, Alerts, and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support the Kaspersky Security Center monitoring.

2.1. Categories

- **Kaspersky Security Center: Report management:** This category provides information related to report management when a report is added, deleted or modified on Kaspersky Security Center.
- **Kaspersky Security Center: Task management**: This category provides information related to task management when a task is added, deleted or modified on Kaspersky Security Center.
- **Kaspersky Security Center: Policy management:** This category provides information related to policy management when a policy is added, deleted or modified on Kaspersky Security Center.
- Kaspersky Security Center: Group task management: This category provides information related to group task management when a group task is added, deleted or modified on Kaspersky Security Center.
- Kaspersky Security Center: Administrative group management: This category provides information related to administrative group management when an administrative group is added, deleted or modified on Kaspersky Security Center.
- **Kaspersky Security Center: Malicious object scan status:** This category provides information related to the malicious object which has been detected and untreated on Kaspersky Security Center.
- **Kaspersky Security Center: Application privilege management:** This category provides information related to applications that have been added to the trusted group on Kaspersky Security Center.
- **Kaspersky Security Center: Application settings change:** This category provides information related to applications where their settings are changed on Kaspersky Security Center.
- **Kaspersky Security Center: Blocked files**: This category provides information related to files which are being blocked by Kaspersky Security Center.



- **Kaspersky Security Center: Device Control:** This category provides information related to devices which have been blocked when inserted into the Kaspersky Security Center system.
- **Kaspersky Security Center: Malware detected:** This category provides information related to malwares which have been detected in the system of Kaspersky Security Center.
- **Kaspersky Security Center: Object quarantine:** This category provides information related to malware objects which are added into the quarantine list in Kaspersky Security Center.
- Kaspersky Security Center: Task management: This category provides information related to task management of Kaspersky Security Center.
- **Kaspersky Security Center: Vulnerability detected:** This category provides information related to a vulnerability which has been detected in Kaspersky Security Center.

2.2. Alerts

- Kaspersky Security Center: Attack Detected: This alert is generated when an Alert is detected in the Kaspersky Security Center.
- Kaspersky Security Center: Suspicious Object Found: This alert is generated when a malicious/Suspicious object is detected in Kaspersky Security Center.
- Kaspersky Security Center: Virus Found: This Alert is generated when one of the files or web Viruses is detected in the Kaspersky Security Center.

2.3. Report

• Kaspersky Security Center- Suspicious Object Found: This report provides information related to malware detected in the web for which the user tries to access an unidentified object.

Logs considered

Jan 14 05:04:28 ccc-app9

CEF:0|KasperskyLab|SecurityCenter|10.3.407|GNRL_EV_SUSPICIOUS_OBJECT_FOUND|Probably infected object detected|4|msg=Result: Detected: not-a-virus:WebToolbar.Win32.Asparnet.gen\r\nUser: CCCNTR\\CCC5055\$ (Initiator)\r\nObject: C:\\Program Files (x86)\\askpartnernetwork\\toolbar\\updater\\tbnotifier.exe\r\n rt=1547463838 dhost=CCC5055 dst=192.168.6.242 cs2=KES cs2Label=ProductName cs3=10.2.4.0 cs3Label=ProductVersion filePath=C:\Program Files (x86)\AskPartnerNetwork\Toolbar\Updater\TBNotifier.exe cs1=not-avirus:WebToolbar.Win32.Asparnet.gen cs1Label=VirusName duser=CCCNTR\CCC5055\$

Sample Report

EventSource	EventDescription	Destination Host	Destination IP	Product Name	Product Version
* syslog	Jan 13 12:53:54 coc-app9 CEF:0 KasperskyLab SecurityCenter 10.3.407 KLPR CL_TaskState Completed 11tt=1547405610 dhost=CCC5352 dst=132.168.10.190 cs2=KES cs2Label=ProductVersion cs5=10.2.4.0 cs3Labe =ProductVersion cs5=Database Update cs5Labe =TaskName cs4=324 cs4Labe =TaskId cs24_cs2 _abe =TaskIdew=State_cs1=1	CCC5352	192.168.10.190	KES	10.2.4.0
syslog	Jan 13 12:54:24 coc-app9 CEF:0IK asperskyLabl SecurityCenter[10:3:407 KLPR CL_TaskState Completed]11tr=1547405643 dhost=CCC5358 dst=192.168.11:243 cs2=KES cs2Label=ProductName cs3=10.2;4.0 cs3Label=ProductVersion cs5=Database Update cs5Label=TaskName cs4=324 cs4Label=TaskId cn2=4 cn21 ahel=TaskNamitate cn1=1	CCC5358	192.168.11.243	KES	10.2.4.0

• Kaspersky Security Center-Task Status Updated: This report provides information related to task management where the task is started or stopped.

Logs considered

Jan 14 05:07:58 ccc-app9 CEF:0|KasperskyLab|SecurityCenter|10.3.407|KLPRCI_TaskState|Completed|1|rt=1547464052 dhost=CCC-RD-HOST11 dst=192.168.0.101 cs2=WSEE cs2Label=ProductName cs3=10.0.0.0 cs3Label=ProductVersion cs5=Server Database Update cs5Label=TaskName cs4=204 cs4Label=TaskId cn2=4 cn2Label=TaskNewState cn1=1 cn1Label=TaskOldState

Sample Report

EventId	EventUser	Computer	EventSource	EventDescription
123458	N/A	KASPERSKY	Syslog	Jan 14 04:57:58 ccc-app9 CEF:0 KasperskyLab SecurityCenter 10.3.407 GNRL_EV_ SUSPICIOUS_OBJECT_FOUND Probably infected object detected 4 msg=Result: Detected: not-a- virus:WebToolbar.Win32.Asparnet.gen User: CCCNTR\CCC5055\$ (Initiator) Object: C:\Program Files (x86)\askpartnernetwork\toolbar\updater\tbnotifier.exe rt=1547463462 dhost=CCC5055 dst=192.168.6.242 cs2=KES cs2Label=ProductName cs3=10.2.4.0 cs3Label=ProductVersion filePath=C:\Program Files (x86)\AskPartnerNetwork\Toolbar.Updater\tBNotifier.exe cs1=not-a-virus:WebToolbar.Win32.Asparnet.gen cs1Label=VirusName duser=CCCNTR\CCC5055\$



3.Importing Kaspersky Security Center knowledge pack into EventTracker

- 1. Launch the EventTracker Control Panel.
- 2. Double click Export Import Utility, and then click the Import tab.

Import Token Templates/Category/Alert/Tokens/ Flex Reports as given below.

Note: Importing should be in the same order as mentioned above.



Figure 6

3.1. Category

1. Click the **Category** option, and then click the browse button.

Netsurion... EventTracker

	Export Import Utility
port Import	
Provide the path and file na	me of the Categories file. Use the '' button to browse and locate the import file.
2. Click the Import button.	
Options	Location
 Category 	
O Filters	
O Alerts	
O Systems and Groups	Source :
	".iscel
O HSS Feeds	
O Reports	
O Behavior Rules	
O SCAP	
O Token Value	
	Import Close

Figure 7

- 2. Locate All Kaspersky Security Center group of Categories.iscat file, and then click the Open button.
- 3. To import categories, click the **Import** button.

EventTracker displays a success message.





4. Click **OK**, and then click the **Close** button.

3.2. Alerts

1. Click **Alerts** option, and then click the **browse** button.



2. Click the Import button. Options	Location	
 Category Filters 	The second firm of the Winese	
Alerts	Set Active	This setting is applicable only for imports from Legacy
Systems and Groups	 By default 	(v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.
RSS Feeds		
Reports	Source : * isalt	
Behavior Rules	- North	
SCAP		
Token Value		



- 2. Locate All Kaspersky Security Center group of Alerts.isalt file, and then click the Open button.
- 3. To import alerts, click the **Import** button.

EventTracker displays a success message.



Figure 10

4. Click **OK**, and then click the **Close** button.

3.3. Flex Reports

1. Click the **Report** option, and then click the **browse** button.

Vote : If report(s) contains tem Options Category	plate, first import template and proceed with exportimport utility. Location	
Alerts	O Legacy (*.issch) New (*.etcrx)	
Systems and Groups	Source :	_
RSS Feeds	"Jssch	
Reports		
O Behavior Rules		
⊖ SCAP		
O Token Value		

Figure 11

- 2. Locate All Kaspersky Security Center group of Flex Report.issch file, and then click the Open button.
- 3. To import reports, click the **Import** button.

EventTracker displays a success message.



Figure 12

4. Click **OK**, and then click the **Close** button.

3.4. Token Templates

- 1. Click the Admin menu, and then click Parsing rule.
- 2. Select the **Template** tab, and then click on **T 'Import'** option.

PARSING RULE									
Parsing Rule Te	mplate	^							
Default			Group : All					C1	11
A10 ADC	Ē 🏈	=	TEMPLATE NAME	TEMPLATE DESCRIPTION	GROUP NAME	ADDED BY	ADDED DATE	ACTIVE	EDIT
Amazon Web Services	Ū Ø		A10 ADC Authenticat	A10 Application Delivery C	Default	ETAdmin	9/25/2015 07:56:59 PM		Ø
ApacheWeb Server	11 🧭		A10 ADC Traffic	A10 Application Delivery C	Default	ETAdmin	9/25/2015 07:56:59 PM	v) 🧭
Centrify Server Suit	Ū Ø		Cisca IOS-Access Den		Cisco IOS	ETAdmin	10/17/2015 03:32:42] 🧭
CheckPaint	Ū Ø	1.	Cisco IOS-Configurati		Cisca IOS	ETAdmin	10/17/2015 06:4B:45	V	
Cisco ACS	Ū Ø		Cisco IOS-Port Status		Cisco 105	ETAdmin	10/16/2015 06:27:54		
Cisco ASA	Ē 🏉								
Cisco IOS	Ū 🧭		HP ProCurve-Port Sta	HP 2520G,HP 2520,HP 253	Default	ETAdmin	9/16/2015 04:16:51 PM	v	Ø
Cisco IranPart ESA	İ 🧭		HP ProCurve-Security	HP 2520G,HP 2520,HP 253	Default	ETAdmin	9/16/2015 05:33:25 PM		Ø
CISCO Iranpart WSA	Ē Ø								
Cisco ISE	1						DELETE	VE TO GRO	JUP
Clavister firewall	Ü 🧭	Ŧ							

Figure 13

3. Click on the Browse button.

SELECT FILE Browse No file selected. Note: Please select file of type *.ettd (eventtracker template das	lets).
	No data found

Figure 14

4. Locate All Kaspersky Security Center group of template.ettd file, and then click the Open button.



TEMPLATE NAME	SEPARATOR	TEMPLATE DESCRIPTION	ADDED DATE	ADDED BY	GROUP NAME
Kaspersky Security Centre	١n	PNPL-TESTLAB7 [Thursday, April 21, 2016 3:27:20 PM (GMT+05:-30)] (): Result: Detected: EICAR-Test-File User: TOONS\ETAdmin (Active user) Object: C:\Users\ ETAdmin\Downloads\eicar_com (4).zip/eicar.com	4/21/2016 5:09:37 PM	ETAdmin	Kaspersky Security Centre
Kaspersky Security Centre- Application privilege control	١n	PNPL-TESTLAB7 [Thursday, April 21, 2016 8:15:06 PM (GMT+05:-30)] (Applicati on Privilege Control): Event type: Application placed in the trusted group Appli cation\Name: AppX Deployment Bytecode Generator EXE Application\Path: c.\ windows\system32\ Application\Process ID: 7796 User: NT AUTHORITVSYSTE M (System user) Component: Application Privilege Control Result\Threat level: Low Result\Precision: Exactly Action: Application placed in group Object: Trust ed Object\Type: Group of applications Object\Name: Trusted Reason: Signed b y the digital signature of trusted manufacturers	4/22/2016 12:35:16 PM	ETAdmin	Kaspersky Security Centre

Figure 15

5. Now select the check box and then click on ^T 'Import' option. EventTracker displays a success message.

Template(s) imported successfully	
ОК	



6. Click on the **OK** button.



4.Verifying Kaspersky Security Center knowledge pack in EventTracker

4.1. Categories

- 1. Logon to EventTracker.
- 2. Click the Admin menu, and then click Categories.
- 3. In **Category Tree** to view imported categories, scroll down and expand the **Kaspersky Security Center** group folder to view the imported categories.

tegory Tree Search			
I 🔁 Juniper JUNOS	 Total category groups: 351 Total categories: 3,134 Last 10 modified categories 		
LDAP Server	NAME	MODIFIED DATE	MODIFIED BY
i 🔁 Linux	Kaspersky Security Centre- Malicious object detected	3/29/2016 5:19:38 PM	ETAdmin
🗄 🕞 Linux Cracking	Kaspersky Security Centre: Administrative group management	3/29/2016 3:17:52 PM	ETAdmin
Unux Violation	Kaspersky Security Centre: Group task management	3/29/2016 3:04:03 PM	FTAdmin
- Call Locializer SP	Kaspersky Security Centre: Report management	3/29/2016 12:33:29 PM	ETAdmin
C McAfee IntruShield	Parameter Parameter Parlameter Parlameter and	ACRONAL TABLE	FTAdmin
McAfee Sidewinder Firewall	Kaspersky Security Centre: Poicy management	3/28/2016 7:01:26 PM	ETAdmin
Microsoft Forefront	Trend Micro InterScan: User Jogon	3/21/2016 5:42:57 PM	FTAdmin
Microsoft Windows RRA5	Trend Micro InterScar: URL filter	3/21/2016 5:42:42 PM	ETAdmin
- Motorola	Trend Mirm InterScar (10) access control	3/31/2016 5-42-38 PM	FTAdmin
A MySQL	II	JETEVIO JALEO FM	CTAUNIT
D Netscreen	Trend Micro InterScan: HTTP CPU utilization	3/21/2016 5:42:00 PM	ELAdmie
C OKTA SSO			
DenDNS Umbrella Insights and Platfo			
G Oracle			
Paloalto			

Figure 17

4.2. Alerts

- 1. Logon to EventTracker.
- 2. Click the Admin menu, and then click Alerts.
- 3. In the Search field, type 'Kaspersky Security Center', and then click the Go button.

Alert Management page will display all the imported Kaspersky Security Center alerts.



Alerts							Search by	Alert name 🔻	Type here
106 Available Alerts Total number of alerts available	17 Active Alerts Total number of active alerts				106 System/Use Count for system	System User r Defined Al n and user define	3 erts ed alerts	106 Alerts t Count of A	Critical High Low 4 Medium Serious by Threat Level slerts by threat level
Î Activate Now Click 'Activate N	ow' after making all changes								Total: 3 Pag
Alert Name A		Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	n Remedial Action at Agent	Applies
🔲 🖗 Kaspersky Security Center Attack Detected		•							Kaspersky Security Cen
🔲 🚱 Kaspersky Security Center Suspicious Object F	ound	•							Kaspersky Security Cen
β & Kaspersky Security Center Virus Found		•							Kaspersky Security Cen

Figure 18

4. To activate the imported alerts, select the respective checkbox in the **Active** column.

EventTracker displays a message box.

Successfully saved co	nfiguration.



5. Click **OK**, and then click the **Activate Now** button.

NOTE:

You can select alert notification such as Email, and Message, etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

4.3. Reports

- 1. Logon to EventTracker.
- 2. Click the Reports menu, and then select Configuration.
- 3. In **Reports Configuration** pane, select the **Defined** option.



EventTracker displays the **Defined** page.

4. In search box enter 'Kaspersky Security Center', and then click the Search button.

EventTracker displays Flex reports of Kaspersky Security Center.

	Repo	rt Configuration					
۹	⊖ Sc	heduled 🔘 Queued 🖲 Def	ined				Search
R	Repo	rt Groups		+	Reports o	onfiguration: Kaspersky Security Center -New	
	0	Security			🕀 🗓	<i>д</i> ,	
	0	Compliance				Title	Created on
	0	Operations			🗉 🄅	Kaspersky Security Center Suspicious Object Found	Feb 13 10:50:12 AM
	Ð	Flex			🗉 🄅	Kaspersky Security Center-Task Status Update	Feb 06 01:01:59 PM
		1111Kaspersky	Ē	1			
		21313Kapersky	Ē	1			
		EventTracker	Ű	Ø			
		Kaspersky Security C	Ű	Ø			
		Windows	Ü	0			

Figure 20

4.4. Token Template

- 1. Logon to EventTracker.
- 2. Click the Admin menu, and then click Parsing Rules.

Parsing Rules									🕈 / Adr
Parsing Rule Templ	late	()	Group : Kaspersky Security	Search	Q				
Default	前	<u> </u>	Center -New						
ABC	10		Template Name	Template Description	Added By	Added Date	Active		
Cisco ASA	前	8	12234		EventTrackerAdmin	Feb 13 11:09:12 AM	2	8	Ø
CISCO ASA VPN	Î	1	Kasperesky Security Center	kaspersky security center	EventTrackerAdmin	Feb 12 05:27:31 PM			Ø
Clavister firewall	Ű	1	suspicious object found						-
Endpoint Kaspersky	Ē	0	Kaspersky Security Center - Task Status	Kaspersky Security Center	EventTrackerAdmin	Feb 12 04:59:33 PM		0	Ø
EventTracker	面	1	Suspicious	Kaspersky Security Center	EventTrackerAdmin	Feb 13 10:57:24 AM	2		Ø
Forcepoint Test	Ē	1							
Kaspersky SC	1Û)	1							
Kaspersky Security C	Ű	1							

Figure 21



5.Sample Dashboards



• Kaspersky Security Center- Suspicious object Found by Host



• Kaspersky Security Center- Suspicious object Found on IP Address



Figure 23





• Kaspersky Security Center- Suspicious object Found by Threat



• Kaspersky Security Center- Suspicious object Found by user



Figure 25





• Kaspersky Security Center- Suspicious object Found by Task Status

Figure 26

• Kaspersky Security Center- Suspicious object Found by System



Figure 27

