Kaspersky CyberTrace with McAfee Enterprise Security Manager

Implementation guide

Dear User,

Thank you for choosing Kaspersky as your security software provider. We hope that this document will help you to use our product.

Attention! This document is the property of AO Kaspersky Lab (herein also referred to as Kaspersky): all rights to this document are reserved by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction and distribution of this document or parts hereof incur civil, administrative, or criminal liability under applicable law.

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky.

This document, and graphic images related to it, may be used for informational, non-commercial, and personal purposes only.

Kaspersky reserves the right to amend this document without additional notification.

Kaspersky assumes no liability for the content, quality, relevance, or accuracy of any materials used in this document to which rights are held by third parties, or for any potential harms associated with use of the document.

Document revision date: 2/1/2021

© 2021 AO Kaspersky Lab

https://www.kaspersky.com https://help.kaspersky.com https://support.kaspersky.com

About Kaspersky: (https://www.kaspersky.com/about/company)

Contents

References	4
About this document	5
Integrating with McAfee Enterprise Security Manager	6
Configuring Kaspersky CyberTrace for integration with McAfee Enterprise Security Manager	6
Forwarding events from McAfee Enterprise Security Manager to Kaspersky CyberTrace	8
Parsing Kaspersky CyberTrace service events in McAfee Enterprise Security Manager	12
Parsing Kaspersky CyberTrace detection events in McAfee Enterprise Security Manager	20
Browsing Kaspersky CyberTrace events in McAfee Enterprise Security Manager	23
Configuring the aggregation of Kaspersky CyberTrace events	24
Adding a widget for Kaspersky CyberTrace events to McAfee Enterprise Security Manager	25
AO Kaspersky Lab	27
Trademark notices	28

References

This chapter contains the description of documents that can be used as references. You can also use other McAfee® ESM documentation.

Reference	Description
https://docs.mcafee.com/bundle/enterprise-security-m anager-10.4.x-product-guide/page/GUID-88473528-B 9BD-4799-B3A7-BC7A8C22B55D.html	McAfee Enterprise Security Manager 10 Product Guide
https://docs.mcafee.com/bundle/enterprise-security-m an- ag- er-11.1.x-product-guide/page/GUID-88473528-B9BD- 4799-B3A7-BC7A8C22B55D.html	McAfee Enterprise Security Manager 11 Product Guide

About this document

This document contains instructions for integrating Kaspersky CyberTrace with such security information and event management (SIEM) software as McAfee Enterprise Security Manager 10/11 (hereinafter also "McAfee ESM").

Use Kaspersky CyberTrace for Log Scanner (https://support.kaspersky.com/13858) for integration with McAfee Enterprise Security Manager.

The application contains a certificate for the demo version of Kaspersky Threat Data Feeds. Demo feeds provide lower detection rates in comparison with their corresponding commercial versions. To obtain a certificate for the commercial version of Kaspersky Threat Data Feeds, contact the Kaspersky CyberSecurity Service team (intelligence@kaspersky.com).

Integrating with McAfee Enterprise Security Manager

This chapter describes how to integrate Kaspersky CyberTrace with McAfee Enterprise Security Manager.

In this chapter

Configuring Kaspersky CyberTrace for integration with McAfee Enterprise Security Manager	<u>6</u>
Forwarding events from McAfee Enterprise Security Manager to Kaspersky CyberTrace	<u>8</u>
Parsing Kaspersky CyberTrace service events in McAfee Enterprise Security Manager	<u>12</u>
Parsing Kaspersky CyberTrace detection events in McAfee Enterprise Security Manager	<u>20</u>
Browsing Kaspersky CyberTrace events in McAfee Enterprise Security Manager	<u>23</u>
Configuring the aggregation of Kaspersky CyberTrace events	<u>24</u>
Adding a widget for Kaspersky CyberTrace events to McAfee Enterprise Security Manager	<u>25</u>

Configuring Kaspersky CyberTrace for integration with McAfee Enterprise Security Manager

This section describes how to configure Kaspersky CyberTrace for integration with McAfee ESM.

To configure Kaspersky CyberTrace for integration with McAfee ESM:

- 1. Download Kaspersky CyberTrace for LogScanner (hereinafter referred to as Kaspersky CyberTrace) from https://support.kaspersky.com/13858.
- 2. Install Kaspersky CyberTrace as described at https://support.kaspersky.com/CyberTrace/1.0/en-US/162489.htm.
- 3. When you login to Kaspersky CyberTrace Web UI for the first time, the **Initial Setup Wizard** window opens. Make the following settings:.
 - a. Select Other in the SIEM field and click Next.
 - b. In the Connection Settings window that opens, specify the following:
 - IP address and port on which Kaspersky CyberTrace will listen for incoming events
 - IP address and port of McAfee ESM to which Kaspersky CyberTrace will send detection events and alert events

For McAfee ESM, the port is 514.

Click Next.

- c. If necessary, specify proxy server connection parameters in the Proxy Settings window.
- d. Perform the remaining steps of the initial setup as required.
- 4. On the Settings > Matching tab, click Edit default rules, select the Regular expressions tab and specify

the following regular expressions (see https://support.kaspersky.com/CyberTrace/1.0/en-US/156534.htm):

Table 1. Regular expressions for integration with McAfee ESM

Indicator type	Rule name	Regular expression	Additional options
CONTEXT	Device	deviceExternalId\=(.*?)\s	
CONTEXT	DeviceAction	act\=(.*?)\s	
CONTEXT	Devicelp	deviceTranslatedAddres s\=(.*?)\s	
HASH	RE_HASH	([\da-fA-F]{32,64})	Extract all: True
IP	RE_IP	dst\=(.*?)\s	
URL	RE_URL	$\begin{array}{l} (?:\\\\\)((?:\\\\)=\\\)(?:\\\))?+\\ @)?(?:(?:[a-z\\\)(a-z\\)(00a1)-\\ \times{ffff}0-9]+-)*[a-z\\\)(?:\\)(?:[a-z\\)(?:[a-z\\)(?:[a-z\\)(?:[a-z\\)(?:[a-z\\)(?:[a-z\\)(?:[a-z\\)(?:\)(?:[a-z\\)(?:\)(?:[a-z\\)(?:\)(?:\)(?:\)(?:\)(?:\)(?:\)(?:\)(?$	Extract all: True
IP	SRC_IP	src\=(.*?)\s	
CONTEXT	UserName	duser\=(.*?)\s	

On the Normalizing rules tab, specify the following replacement rule:

Replacement rules

Regexp to	o replace
-----------	-----------

\u002F

Replace with

Ū

Figure 1. Replacement rule for integration with McAfee ESM

//

Save the changes.

 Select Settings > Events format and specify the following formats (see https://support.kaspersky.com/CyberTrace/1.0/en-US/169253.htm):

Table 2. Events format for integration with McAfee ESM

Field	Value
Alert events format	Kaspersky CyberTrace Service Event date=%Date% alert=%Alert% msg:%RecordContext%
Detection events format	Kaspersky CyberTrace Detection Event date=%Date% reason=%Category% detected=%MatchedIndicator% act=%DeviceAction% dst=%RE_IP% src=%SRC_IP% hash=%RE_HASH% request=%RE_URL% dvc=%DeviceIp% sourceServiceName=%Device% suser=%UserName% msg:%RecordContext%

Field	Value	
Records context format	%ParamName%=%ParamValue%	
	Note the space before %ParamName%.	
Actionable fields context format	%ParamName%:%ParamValue%	
	Note the space before %ParamName%.	

Save the changes.

Forwarding events from McAfee Enterprise Security Manager to Kaspersky CyberTrace

This section contains an instruction for forwarding Kaspersky CyberTrace events from McAfee Enterprise Security Manager to Kaspersky CyberTrace.

- To configure forwarding events from McAfee Enterprise Security Manager to Kaspersky CyberTrace:
 - 1. Open the system properties of McAfee ESM:
 - If you are using McAfee Enterprise Security Manager 10, click System Properties in the main window.
 - If you are using McAfee Enterprise Security Manager 11, click ≡ in the dashboard. In the system navigation tree, select McAfee ESM, and then click Properties.

The System Properties dialog box appears.

2. Click Event Forwarding.

The settings related to event forwarding are displayed.

3. Click Add.

System Properties						X
System Information	Event Forwa	rding Destinations:			_	?
Alarms	Name		Туре	Enabled		Add
Content Packs						
Custom Settings						Edit
Custom Types					1	lemove
Cyber Threat Feeds						
Data Enrichment						
Database						
Email Settings						
ESM Management						
Event Forwarding						
File Maintenance						
Global Blacklist						
Hosts						
Login Security						
Network Settings						
Profile Management						
Reports						
SNMP Configuration						
System Log						
Users and Groups						
Watchlists		· ·				
	Settings	Manage event forwardin	g settings			
				0	K Cancel	Apply

Figure 2. System Properties dialog box

- 4. In the Edit Event Forwarding Destination dialog box, enter the following data:
 - Name: CyberTrace
 - Enable: Selected
 - Use System Profile: Cleared
 - Format: Syslog (Common Event Format)
 - Destination IP: the IP address of the computer on which Kaspersky CyberTrace runs
 - Destination Port: the port that Kaspersky CyberTrace listens on for events

The IP address and port are the same as specified in the **Settings** > **Service** tab of Kaspersky CyberTrace Web (see section "Configuring Kaspersky CyberTrace for integration with McAfee Enterprise Security Manager (on page $\underline{6}$)").

- **Protocol**: TCP
- Facility: User

- Severity: Informational
- Time Format: Standard
- Time Zone: Select the time zone you need
- Obfuscate data: Cleared
- Send Packet: Cleared
- Mode: None

Edit Event Forwarding D	estination		×
Name:	CyberTrace		?
Enabled:		Mode:	None 🗸
Use System Profile:		Local Relay Port:	2000
Format:	syslog (Common Event Forma 🔍	Remote SSH Port:	22
Destination IP:	192.168.0.21	SSH Username:	
Destination Port:	9999	SSH DSA Key:	ssh-dss
Protocol:	тср		phddE1TED26B/MIv/icUrEbH3Qg8naz
Facility:	User		
Severity:	Informational		
Time Format:	💿 Standard 🛛 Legacy		
Time Zone:	(GMT+03:00) Moscow, St. Pel		
Obfuscate data:	Configure		
Send Packet:			
Event Filters	null [TestDev]Device ID [TestDev]		
		<u>.</u>	
			OK Cancel

Figure 3. Edit Event Forwarding Destination dialog box

5. Click Event Filters.

The Event Filters dialog box appears.

Event Filters		×
Enter values to filter t	he event data for this event forwarding destination.	?
Device:	Local Receiver-ELM	7
Destination IP:		
Destination Port:]
Protocol:		1
Source IP:]
Device Type:	387, 169, 172, 270, 132, 397, 14, 137, 46, 50, 263, 456,	7
Normalized ID:		7
Severity:	None V	
Click the button to the	right of this field to choose a specific device.	
	ОК С	ancel
2		

Figure 4. Event Filters dialog box

In the **Event Filters** dialog box you can specify the event sources, the events from which are forwarded to Kaspersky CyberTrace. For example, you can specify the following data:

- The devices, the events from which are forwarded
- The types of devices, the events from which are forwarded
- 6. In the **Event Filters** dialog box, click **OK**.
- 7. In the Edit Event Forwarding Destination dialog box, click OK.
- 8. Make sure that the rule for forwarding events to Kaspersky CyberTrace appears in McAfee Enterprise Security Manager.

Name	Туре	Enabled
cvbertrace	syslog (Common Ev	Yes

Figure 5. The rule for event forwarding to Kaspersky CyberTrace

 Make sure that events arrive from McAfee Enterprise Security Manager. If the events forwarding from McAfee Enterprise Security Manager to Kaspersky CyberTrace has been configured properly, you will see updated indicator statistics on the **Dasboard** tab of Kaspersky CyberTrace Web.

Parsing Kaspersky CyberTrace service events in McAfee Enterprise Security Manager

This section contains an instruction of how to parse Kaspersky CyberTrace service events that have the following format:

```
Kaspersky CyberTrace Service Event| date=%Date% alert=%Alert%
msg:%RecordContext%
```

Note that if you change the service events format, you have to change the parsing service event rules in McAfee Enterprise Security Manager.

To parse a service event, enter the following data in the Advanced Syslog Parser Rule dialog box:

- 1. In the main window of McAfee Enterprise Security Manager, click Configuration.
- 2. In the Physical Display tree, select a Receiver device and click Add Data Source.



Figure 6. Adding a data source

The Add Data Source dialog box appears.

- 3. In the Add Data Source dialog box, enter the following data:
 - Data Source Vendor: Generic
 - Data Source Model: Advanced Syslog Parser
 - Data Format: Default
 - Data Retrieval: SYSLOG (Default)
 - Enabled: Parsing
 - Name: Kaspersky CyberTrace

- IP: The IP address of the computer from which Kaspersky CyberTrace will send events •
- Syslog Relay: None •
- **Mask**: 0 •
- Require syslog TLS: Cleared •
- Port: 514 •
- Support Generic Syslogs: Log "unknown syslog" event •

McAfee Enterprise Security Manager receives all events from Kaspersky CyberTrace. If McAfee Enterprise Security Manager cannot parse an event, the event displays as unknown.

- Time Zone: Select the time zone you need •
- Encoding: None •

Edit Data Source	>
Use System Profiles:	No Profiles Defined
Data Source Vendor:	Generic
Data Source Model:	Advanced Syslog Parser 🗸 🗸
Data Format:	Default
Data Retrieval:	SYSLOG (Default)
Enabled:	Parsing Logging SNMP Trap
Name:	Kaspersky CyberTrace
IP Address:	127.0.0.1
Host Name:	Look up
Syslog Relay:	None
Mask:	0
Require syslog TLS:	
Port:	514 🗸
Support Generic Syslogs:	Log "unknown syslog" event
Generic Rule Assignment:	User Defined 1
Time Zone:	(GMT,00:00) Greenwich Mean Time
Encoding:	None
Interface	e the network interface for the parent Receiver.
manage	

- Figure 7. Configuration of the data source
- 4. (Optional) Click Advanced to specify parameters for the data source in the Advanced options dialog box.
- 5. Click OK.



McAfee ESM suggests that you roll out the policy you have set.

Rollout		<u> </u>
Click on the label in the Rollout to rollout an individual device, or	Time column to change the device rollout method. Click the i therwise choose OK to process all rollout requests.	icon to the left of the device name 🤅
Device	Rollout Time	Edit
↔ Kaspersky CyberTrace	Roll this policy out now.	
 Local Receiver-ELM 	Koll this policy out now.	
Rollout policy to all devices r	IOW	OK Cancel

Figure 8. Rollout dialog box

6. Select Kaspersky CyberTrace and then click the Policy Editor toolbar button.



7. In the Policy Editor window, select the Advanced Syslog Parser Rules rule type.



8. Click New > Advanced Syslog Parser Rule.



- 9. To create a parser for parsing feed updating events, enter the following data in the **Advanced Syslog Parser Rule** dialog box:
 - In the **General** tab enter the following data:
 - Name: Kaspersky CyberTrace ServiceEvent
 - Tags: Select the tags that define the rule (that is, they will be used while filtering events)
 - Rule Assignment Type: User Defined 1 or another user defined type
 - Description: The Kaspersky Lab CyberTrace service event
 - In the **Parsing** tab enter the following data:
 - Provide content strings: Kaspersky CyberTrace Service Event
 - **Sample Log Data**: Provide an example of a feed updating event. For example (in a single line, without newline symbols):

Kaspersky CyberTrace Service Event| date=Apr 17 19:08:28 alert=KL_ALERT_UpdatedFeed msg:feed=Demo_Botnet_CnC_URL_Data_Feed.json records=3907

• Add the following regular expressions in the **Parsing** tab:

Name	Regular Expression
ct_service_name	alert = (S+) (?=s)
ct_context	(msg.*) (?=\$)
ct_date	date = (S+sd+sS+)

Provide content strings to be matched on incoming log data. Content strings are faster than regular expressions and are used to filter out incoming log data based on matching results. Quotes within a string must be escaped by using a backslash (\).

Enter one or m	ore regular expressions to mate	h on incoming log data.	+ / -	Key	Value
Name		Regular Expression	Target Key	ct_context:1	msg: feed=Demo_B
ct_service_n ct_context	alert\=(\S+)(?=\s) (msg.*)(?=\$)		ct_date:1 ct_service_name:1	Apr 17 19:08:28 KL_ALERT_UpdatedF	
_ ct_date	date\=(\S+\s\d+\s\S+)				
Include sys	log header in regular expressior	n match.			
Sample Log D	ata Transformed Log Data	Format: Ger	ieric 🛛 🗸 🗸		

In the Field Assignment tab enter the following data:

Field	Expression
Action	"0"
Description	Drag ct_context in this field
Severity	"60" or another value you choose
Return_Code	Drag ct_service_name in this field
First Time	Drag ct_date in this field

٠

File	Tools	Help				
neral	Parsing	Field Assignment	Mapping			
atch the ne desir '+' sigr	e following ed field exp n (e.g. 1, 1	fields on the left with pressions. You can co +2, 1+"test"+2 etc	n a group on the right by oncatenate grouping fields .).	entering the group id within each of and string literals together by using + -	Drag and drop a value	below onto an expression to the left.
	Fiel	d	Expression	Sample Value	Key	Value
- Acti	on	"0	n.	0	ct_context:1	feed=Demo_BotnetCnC_URL_D.
Des	cription	ct_	_context:1	feed=Demo_BotnetCnC_URL_Data_I	ct_date:1	Apr 17 19:11:11
Des	tination GU	ID			ct_service_name:1	KL_ALERT_UpdatedFeed
- Des	tination IP					
Des	tination Ma	c Address				
Des	tination Por	rt				
- Eve	nt Count					
Firs	t Time	ct_	_date:1	Apr 17 19:11:11		
Las	t Time				=	
Prot	ocol					
Ret	urn_Code	ct	_service_name:1	KL_ALERT_UpdatedFeed		
- Ses	sion ID					
 Sev 	erity	"6	0"	60		
Sigr	nature Desc	ription				
Sigr	nature ID					
- Sou	rce GUID					
- Sou	rce IP					
Sou	rce Mac Ad	dress				
- Sou	rce Port					

Figure 12. Field Assignment tab

You can add other fields here by clicking the + button.

- In the **Mapping** tab enter the following data:
 - In the time data table:

Time Format	Time Fields			
%b %d %H:%M:%S	First time			

• In the actions table:

Action Key	Action Value
0	Success



• In the severity table:

Severity Key	Severity Value
60	60

File	Tools	Help											
neral	Parsing	Field Assignment	Mapping										
ll out the orticular	e desired o way that i	ustom fields below. s beyond the norm.	Custom fiel	ds are used in ra	are cases that	you might ha	ive with	regards to i	ncoming lo	g data that ei	ther needs to	be mapped or	parsed a
ime Fo	rmat			Time Fields		1 2							
%b %d 9	%H:%M:%	5		First Time			5						
tch the incomin	desired ac ng log data	tion fields on the left to the right by enter	to the diffe ing values i	rent kinds of act nto the action m	tions that cou apping colum	ld occur base n.	d off						
ction K	(ey		A	ction Value									
			a	ert									
			e	ror									
			su	iccess									
	v second a		fa	ilure									
Use th	ne followin	g action for the defau	lt if one is	not specified	pass		$ \cdot $						
everity N	Mapping:					+ 2							
everity	Key			Severity Value			-						
50				50			2						
] Use th	ne followin	g severity for the defa	ault if one i	s not specified	60	B	-02						
										Cancel	< Back	Next >	Finis

10. Click **Finish** to save the policy.

Kaspersky CyberTrace

11. In the Default Policy list select the Kaspersky CyberTrace device and enable the Kaspersky CyberTrace ServiceEvent rule.

Advanced Syslog Parser Rules		•	Filters/
Name	Actio	n Severity	Filter
Kaspersky_CyberTrace_ServiceEvent	disable	d 25	
		Inherit parent value Block inheritance above th	is point
		enabled	
		📲 disabled	

- Figure 14. Enabling a rule
- 12. Select **File > Save** menu to save the current state.
- 13. Select **Operations** > **Rollout** to roll out the policy.

File New Edit	Operations	Tools	Help	
Default Policy Rule Types Variable Receiver Filter	Rollout Clear Upda Create new Append to Modify Agg Event Aggr	ted Rule S watchlist watchlist regation S egation Ex	tatus ettings ceptions	•
Advanced Syslog Parse Data Source Windows Events Normalization	Order ASP Order Filte	Rules r Rules		_

- 14. When prompted, agree to reinitialize the Kaspersky CyberTrace device in McAfee ESM.
- 15. Select the Operations > Modify Aggregation Settings menu item to change Kaspersky CyberTrace service events aggregation rules.

16. In Modify Aggregation Settings in Field 2 set value Return Code and click OK.



17. Confirm the rollout request.

Parsing Kaspersky CyberTrace detection events in McAfee **Enterprise Security Manager**

This section contains an instruction of how to parse Kaspersky CyberTrace detection events that have the following format:

Kaspersky CyberTrace Detection Event | date=%Date% reason=%Category% detected=%MatchedIndicator% act=%DeviceAction% dst=%RE IP% src=%SRC IP% hash=%RE HASH% request=%RE URL% dvc=%DeviceIp% sourceServiceName=%Device% suser=%UserName% msg:%RecordContext%

Note that if you change the format of Kaspersky CyberTrace detection events, you have to change the Kaspersky CyberTrace parser rules in McAfee Enterprise Security Manager.

- To parse a detection event, enter the following data in the Advanced Syslog Parser Rule dialog box:
 - In the **General** tab enter the following data:
 - Name: Kaspersky CyberTrace DetectionEvent •

- Tags: Select the tags that define the rule (that is, they will be used while filtering events)
- Rule Assignment Type: User Defined 1
- Description: The Kaspersky CyberTrace detection event
- In the **Parsing** tab enter the following data:
 - Provide content strings: Kaspersky CyberTrace Detection Event
 - Sample Log Data: Provide an example of a URL detection event. For example:

```
Kaspersky CyberTrace Detection Event| date=Oct 12 16:13:23
reason=KL_BotnetCnC_URL detected=http://fakess123bn.nu act=REQUEST_URL
dst=192.168.1.0 src=192.168.2.0 hash=776735A8CA96DB15B422879DA599F474
request=http://fakess123bn.nu dvc=192.168.3.0
sourceServiceName=FireWall suser=UserName msg:popularity=5 geo=vn,
in, mx threat=Trojan.Win32.Waldek
```

• Add the following regular expressions for parsing events:

Name	Regular Experssion
ct_date	date = (S+s/d+s/s)
ct_reason	reason\=(.*)\sdetected
ct_indicator	<pre>detected\=(.*) \sact</pre>
ct_dev_action	<pre>act\=(.*) \sdst</pre>
ct_dst	dst = (S+)
ct_src	src\=(\S+)
ct_hash	$hash = (\S+)$
ct_request	request\=(.*)\sdvc
ct_dev_ip	dvc = (S+)
ct_serviceName	<pre>sourceServiceName\=(.*)\ssuser</pre>
ct_username	<pre>suser\=(.*?)\smsg</pre>
ct_context	msg\:(.*)\$

• In the Field Assignment tab enter the following data:

Field	Expression
Action	" 0 "
First Time	Drag ct_date in this field
URL	Drag ct_request in this field
Destination IP	Drag ct_dst in this field

Field	Expression
Device_Action	Drag ct_dev_action in this field
Hash	Drag ct_hash in this field
Host	Drag ct_dev_ip in this field
Message_Text	Drag ct_context in this field
Object	Drag ct_indicator in this field
Return_Code	Drag ct_reason in this field
Service_Name	Drag ct_serviceName in this field
Severity	"80"
Source IP	Drag ct_src in this field
Source User	Drag ct_username in this field

McAfee ESM renames the Object field to ObjectID.

- In the **Mapping** tab enter the following data:
 - In the time data table use the following data:

Time Format	Time Fields
%b %d %H:%M:%S	First time

• In the actions table use the following data:

Action Key	Action Value
0	Success

In the severity table use the following data:

Severity Key	Severity Value
80	80

- After specifying the above values do the following:
 - In the Default Policy list select the Kaspersky CyberTrace device and enable the Kaspersky_CyberTrace_DetectionEvent rule.
 - 2. Select **File** > **Save** to save the current state.
 - 3. Select **Operations** > **Rollout** to roll out the policy.
 - 4. Reinitialize the Kaspersky CyberTrace device.
 - 5. Select Operations > Modify Aggregation Settings to change the aggregation rules for Kaspersky

CyberTrace service events.

The Modify Aggregation Settings dialog box appears.

- 6. Specify the following values:
 - Set Field 2 to Object.
 - Set Field 3 to Return_Code.
- 7. Click OK.
- 8. Confirm the rollout request.

Browsing Kaspersky CyberTrace events in McAfee Enterprise Security Manager

This section contains an instruction of how to browse Kaspersky CyberTrace events in McAfee ESM.

- ► To browse the events from Kaspersky CyberTrace:
 - 1. Select the **Normalized Dashboard** tab and in the **Event Summary** table find rows with text that start with **Kaspersky_CyberTrace_**.

Normalized Dashbo ×							/
Physical Display	Type to begin filterin	8	Q Q.	Advanced Search		◯ Refresh マ ③ Current Day	~
Normalized Groups	2.1	Normalized Sub-Groups	o 2 i	Event Summary			
100%	105	100%	105	100%			
Normalized Total Event Count		Normalized Total Event Count		Rule Message	Total Event Count		
Uncategorized	94	Uncategorized	94	Kaspersky_CyberTrace_DetectionEvent		4	9
System 6		File Status 6		unknown event		28	
Authentication 🚦 3		Policy 2		Kaspersky_CyberTrace_ServiceEvent	17		
Application 2		Data Status 2		File Deleted	6		
		Login 1		Policy Modify	2		
				Rule Add	2		

Figure 17. Browsing event summary

2. Select a desired row in the Event Summary table.

The Events table will contain events from Kaspersky CyberTrace.

Events 💊 🖉						
Q Search current table o	lata					Displaying 21 of 21 Rows
First Time	SF-Return_Code	Object	Event C	Source IP	Destination IP	Message_Text
04/26/2019 09:48:11	KL_IP_Reputation	192.0.2.1	3	192.168.0.0	192.0.2.1	category=malware first_seen=01.01.20
04/26/2019 09:48:11	KL_IP_Reputation	192.0.2.3	3	192.168.0.0	192.0.2.3	category=malware first_seen=15.01.20
04/26/2019 09:48:11	KL_BotnetCnC_URL	fakess123bn.nu	15	192.168.0.0		first_seen=10.07.2015 23:53 id=0 last_
04/26/2019 09:49:48	KL_BotnetCnC_URL	fakess123bn.nu	4	192.168.0.0	-	first_seen=10.07.2015 23:53 id=0 last_
04/26/2019 09:49:48	KL_BotnetCnC_URL	5a015004f9fc05290d87e86d69c4b237.com	4	192.168.0.0		first_seen=10.07.2015 23:53 id=99999
04/26/2019 09:49:48	KL_IP_Reputation	192.0.2.1	4	192.168.0.0	192.0.2.1	category=malware first_seen=01.01.20
04/26/2019 09:49:48	KL_IP_Reputation	192.0.2.3	4	192.168.0.0	192.0.2.3	category=malware first_seen=15.01.20
04/26/2019 09:49:48	KL_Malicious_Hash_MD5	44D88612FEA8A8F36DE82E1278ABB02F	4	192.168.0.0		MD5=44D88612FEA8A8F36DE82E127
04/26/2019 09:49:48	KL_Malicious_Hash_MD5	776735A8CA96DB15B422879DA599F474	4	192.168.0.0		MD5=776735A8CA96DB15B422879D
04/26/2019 09:49:48	KL_Malicious_Hash_MD5	FEAF2058298C1E174C2B79AFFC7CF4DF	4	192.168.0.0	2	MD5=FEAF2058298C1E174C2B79AFF

Figure 18. Kaspersky CyberTrace events list

3. Select a row in the **Events** table.

The full information about the selected event will be displayed below the **Events** table.

First Time	SF-Return_Code	Object		Event C	Source IP	Destination IP
04/26/2019 09:48:11	KL IP Reputation	192.0.2.1		3	192.168.0.0	192.0.2.1
04/26/2019 09:48:11	KL_IP_Reputation	192.0.2.3		3	192.168.0.0	192.0.2.3
			_			
DETAILS GEOLO	CATION DESCRIPTION	N NOTES CUSTOM	TYPES PACKET			
DETAILS GEOLC	CATION DESCRIPTION	N NOTES CUSTOM	TYPES PACKET			
DETAILS GEOLC	CATION DESCRIPTION	N NOTES CUSTOM	TYPES PACKET	192.0.2.3		
DETAILS GEOLC HostID UserIDSrc	CATION DESCRIPTION 127.0.0.0 EvalTestUserName	N NOTES CUSTOM	TYPES PACKET ObjectID URL	192.0.2.3		
DETAILS GEOLC HostID UserIDSrc Message_Text	ICATION DESCRIPTION 127.0.0.0 EvalTestUserName category=malware first_seen=15	N NOTES CUSTOM	TYPES PACKET ObjectID URL Return_Code	192.0.2.3 - KL_IP_Rep	utation	
DETAILS GEOLC HostID UserIDSrc Message_Text Device_Action	CATION DESCRIPTION 127.0.0.0 EvalTestUserName category=malware first_seen=15 VerificationTest	N NOTES CUSTOM	TYPES PACKET ObjectID URL Return_Code Service_Name	192.0.2.3 - KL_IP_Rep Kaspersky	utation Lab]CyberTrace Verifica	tion Kit

Please refer to the McAfee ESM documentation on the instructions for creating dashboards and alerts.

Configuring the aggregation of Kaspersky CyberTrace events

Once you have configured the integration of Kaspersky CyberTrace with McAfee ESM, you may notice that McAfee ESM aggregates service or detection events from Kaspersky CyberTrace. In this case the value in the **Event Count** field of the Kaspersky CyberTrace event will be greater than 1.



- ► To view each Kaspersky CyberTrace event separately, perform the following steps:
 - 1. Open Configuration.
 - 2. Select the Kaspersky CyberTrace device and click I to open Policy Editor.
 - 3. In the window that opens, select **Data Source**.

Do not remove the value in the **Device Type Id** field, which is assigned automatically when **Policy Editor** opens.

4. The two rules for parsing Kaspersky CyberTrace events will be displayed.



For each rule, perform the following:

- a. Select Operations > Modify Aggregation Settings.
- b. In the Modify Aggregation Settings dialog box that opens, select the fields to be used for aggregation. These fields must be similar to the fields that you specified in the aggregation rules for Kaspersky CyberTrace events (see sections "Parsing Kaspersky CyberTrace service events in McAfee Enterprise Security Manager (on page <u>12</u>)" and "Parsing Kaspersky CyberTrace detection events in McAfee Enterprise Security Manager (on page <u>20</u>)").
- 5. Select **Operations** > **Rollout** to roll out the policy.

Adding a widget for Kaspersky CyberTrace events to McAfee Enterprise Security Manager

This section contains an instruction of how to add a widget for Kaspersky CyberTrace events to the McAfee ESM dashboard.

- To add a widget for Kaspersky CyberTrace events:
 - 1. Select the Normalized Dashboard tab.
 - 2. Select the tab on which you want to display Kaspersky CyberTrace events and click Edit.
 - 3. Select Add Widget.
 - 4. In the dialog box that opens, specify the following:
 - a. In Widget Title, type the name of the widget (for example, CyberTrace detection events).
 - b. In Query Source, select Events.
 - c. In **Fields**, specify the fields that will be displayed in the widget.

Example:

- i. First time
- ii. Return Code
- iii. Object
- iv. Destination IP
- V. Source IP
- vi. URL
- vii. Hash
- viii. Device Action
- ix. Message Text
- d. In Filters, specify Kaspersky CyberTrace as Device ID and add the Average Severity filter:
 - If you want to display only detection events, set Average Severity to 80.
 - If you want to display only service events, set Average Severity to 60.

- e. In Sorting, select First Time.
- f. In Visualization, select Table.



- 5. Save the widget.
- 6. Click Save As to save the changes to the tab.

Below, you can view an example of a widget which displays Kaspersky CyberTrace events.

CyberTrace detection events						
Q Search current table data						
First Time	SF-Return_Code	Object	Destination IP	Source IP	URL	-
01/25/2021 12:24:21	KL_BotnetCnC_URL	fakess123bn.nu	192.168.1.0	192.168.0.0	fakess123bn.nu	
01/25/2021 12:07:45	KL_BotnetCnC_URL	fakess123bn.nu	192.168.1.0	192.168.0.0	fakess123bn.nu	
01/25/2021 11:32:02	KL_BotnetCnC_URL	fakess123bn.nu	192.168.1.0	192.168.0.0	fakess123bn.nu	
01/25/2021 11:37:33	KL_BotnetCnC_URL	5a015004f9fc05290d87e86d69c4b237	192.168.1.0	192.168.0.0	5a015004f9fc05290d87	

Figure 22. A widget with Kaspersky CyberTrace events

AO Kaspersky Lab

Kaspersky is a world-renowned vendor of systems protecting computers against digital threats, including viruses and other malware, unsolicited email (spam), and network and hacking attacks.

In 2008, Kaspersky was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky is the preferred vendor of computer protection systems for home users in Russia (IDC Endpoint Tracker 2014).

Kaspersky was founded in Russia in 1997. It has since grown into an international group of companies with 38 offices in 33 countries. The company employs more than 3,000 skilled professionals.

Products. Kaspersky products provide protection for all systems, from home computers to large corporate networks.

The personal product range includes security applications for desktop, laptop, and tablet computers, smartphones and other mobile devices.

The company offers protection and control solutions and technologies for workstations and mobile devices, virtual machines, file and web servers, mail gateways, and firewalls. The company's portfolio also features specialized products providing protection against DDoS attacks, protection for industrial control systems, and prevention of financial fraud. Used in conjunction with centralized management tools, these solutions ensure effective automated protection for companies and organizations of any size against computer threats. Kaspersky products are certified by major test laboratories, compatible with software from diverse vendors, and optimized to run on many hardware platforms.

Kaspersky virus analysts work around the clock. Every day they uncover hundreds of thousands of new computer threats, create tools to detect and disinfect them, and include their signatures in databases used by Kaspersky applications.

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky. It is no coincidence that many other developers use the Kaspersky Anti-Virus engine in their products, including: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, and ZyXEL. Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky has won hundreds of awards for its services in combating computer threats. Following tests and research conducted by the reputed Austrian test laboratory AV-Comparatives in 2014, Kaspersky ranked among the top two vendors by the number of Advanced+ certificates earned and was ultimately awarded the Top Rated certificate. But Kaspersky's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

Kaspersky website:	https://www.kaspersky.com
Virus encyclopedia:	https://securelist.com
Kaspersky VirusDesk:	https://virusdesk.kaspersky.com (for analyzing suspicious files and websites)
Kaspersky Community:	https://community.kaspersky.com

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

McAfee is a trademark or registered trademark of McAfee, Inc. in the United States and other countries.