kaspersky

Kaspersky CyberTrace with McAfee Enterprise Security Manager

Implementation guide

kaspersky

Dear User,

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

Document revision date: 2/1/2021

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

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

kaspersky

Contents

kaspersky

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-manager-10.4.x-product-guide/page/GUID-88473528-B9BD-4799-B3A7-BC7A8C22B55D.html	McAfee Enterprise Security Manager 10 Product Guide
https://docs.mcafee.com/bundle/enterprise-security-manager-11.1.x-product-guide/page/GUID-88473528-B9BD-4799-B3A7-BC7A8C22B55D.html	McAfee Enterprise Security Manager 11 Product Guide

kaspersky

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).

kaspersky

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

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	DeviceIp	deviceTranslatedAddress\=(.*?)\s	
HASH	RE_HASH	([\da-fA-F]{32,64})	**Extract all**: True
IP	RE_IP	dst\=(.*?)\s	
URL	RE_URL	(?:\:\/\/)((?:\S+(?::\S*)?+@)?(?:(?:(?:[a-z\x{00a1}-\x{ffff}0-9]+-*)*[a-z\x{00a1}-\x{ffff}0-9]*)(?:\.(?:[a-z\x{00a1}-\x{ffff}0-9]+-)*+[a-z\x{00a1}-\x{ffff}0-9]++)*(?:\.(?:[a-z\x{00a1}-\x{ffff}\-0-9]{2,}+)))(?:\.*:\d{2,5})?+(?:\.*\/[^\s\"\<\>]*+)?+)	**Extract all**: True
IP	SRC_IP	src\=(.*?)\s	
CONTEXT	UserName	duser\=(.*?)\s	

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

Figure 1. Replacement rule for integration with McAfee ESM

Save the changes.

5. 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 M**cAfee 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**.

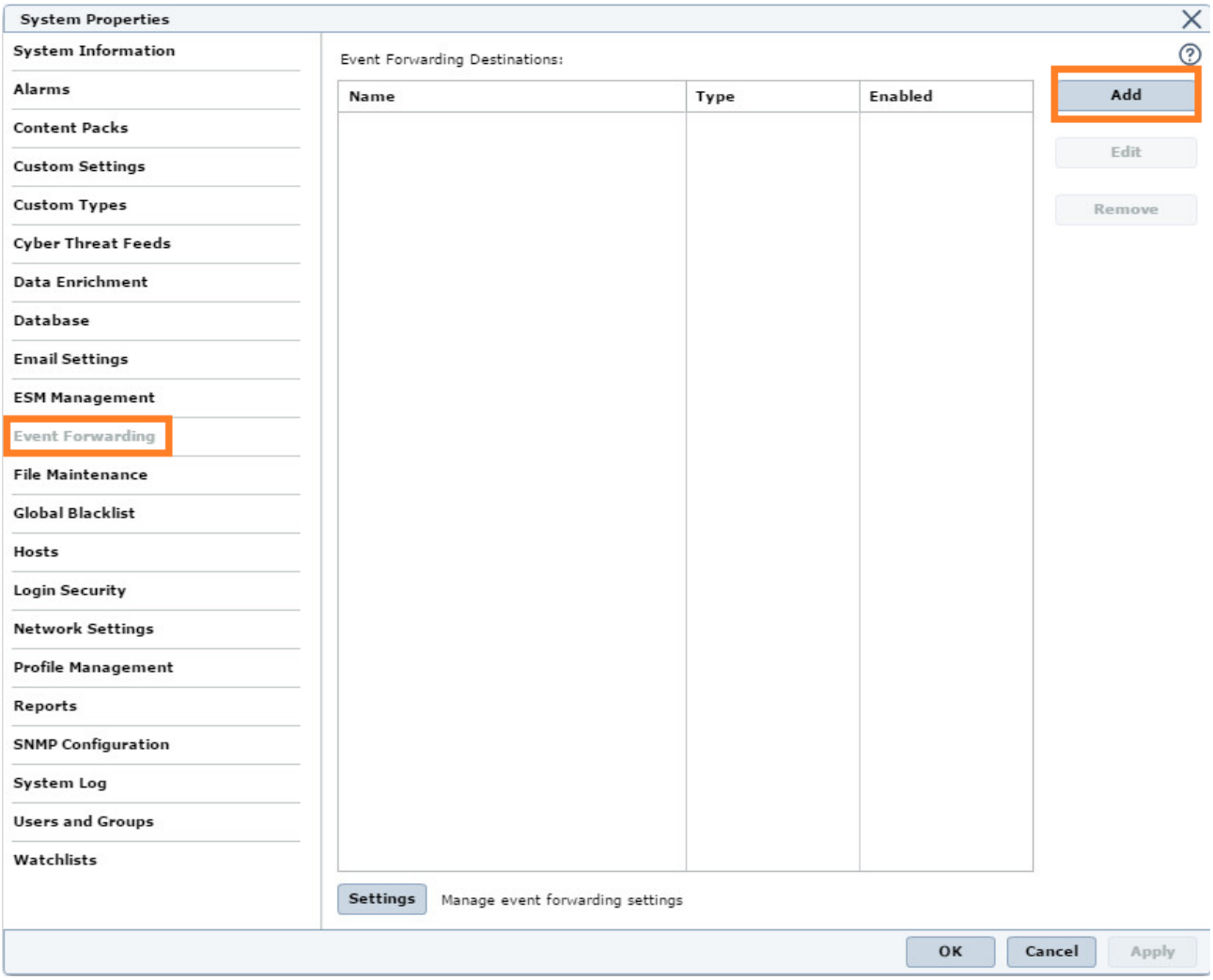


Figure 2. System Properties dialog box

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 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

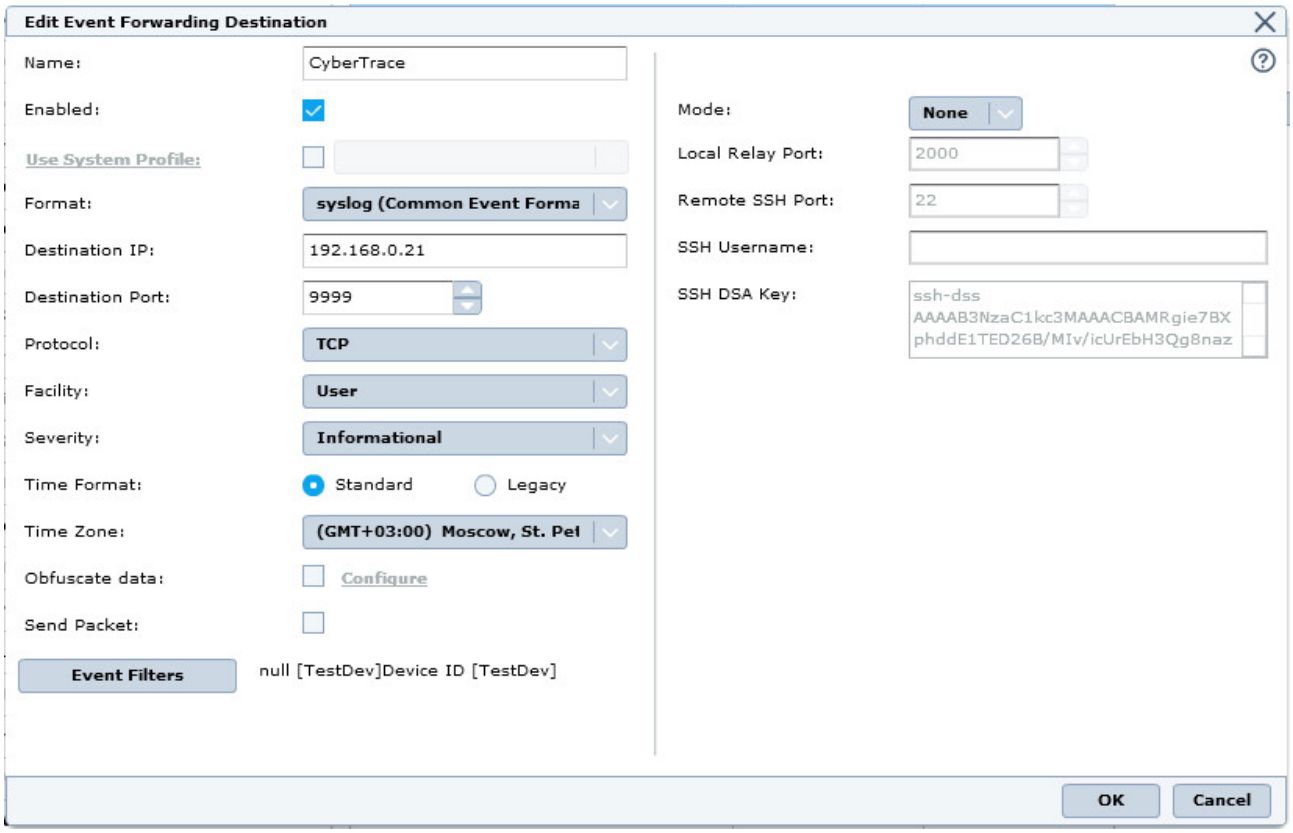


Figure 3. Edit Event Forwarding Destination dialog box

5. Click **Event Filters**.

The **Event Filters** dialog box appears.

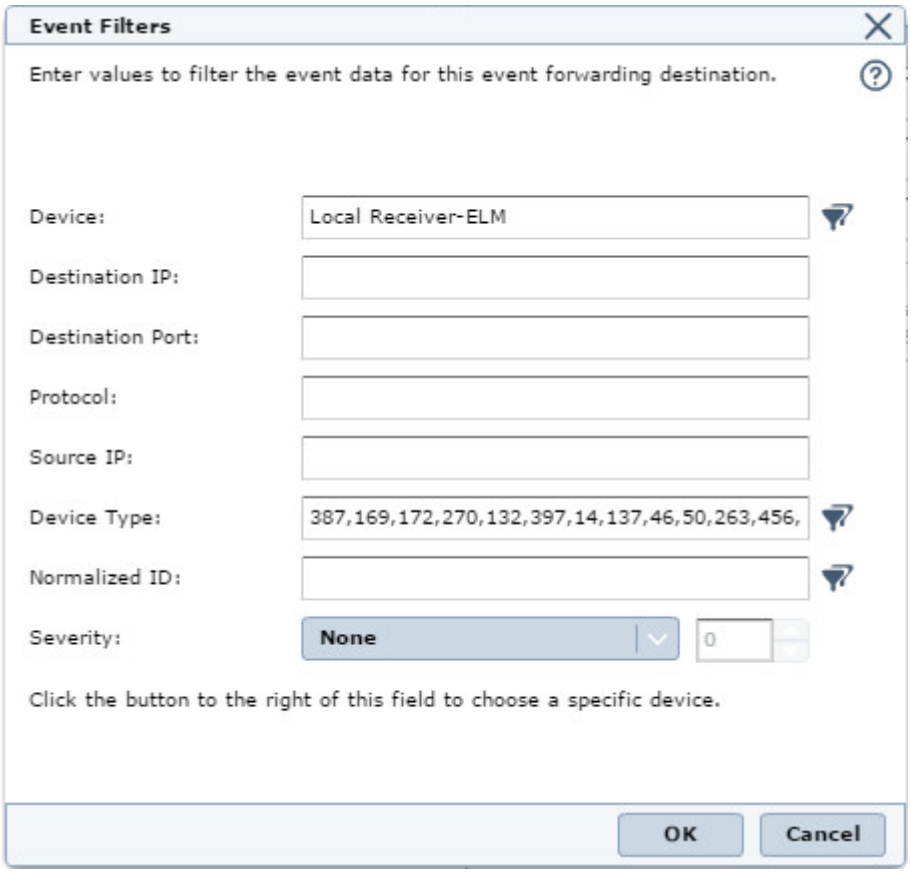


Figure 4. Event Filters dialog box

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.

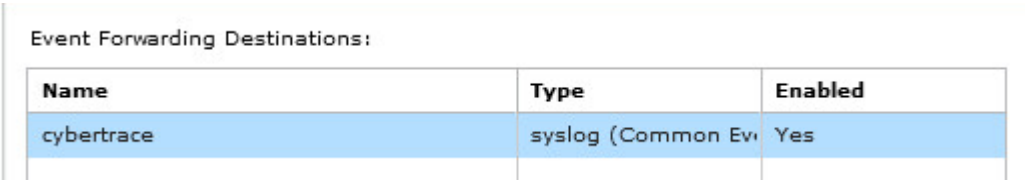


Figure 5. The rule for event forwarding to Kaspersky CyberTrace

9. 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**.

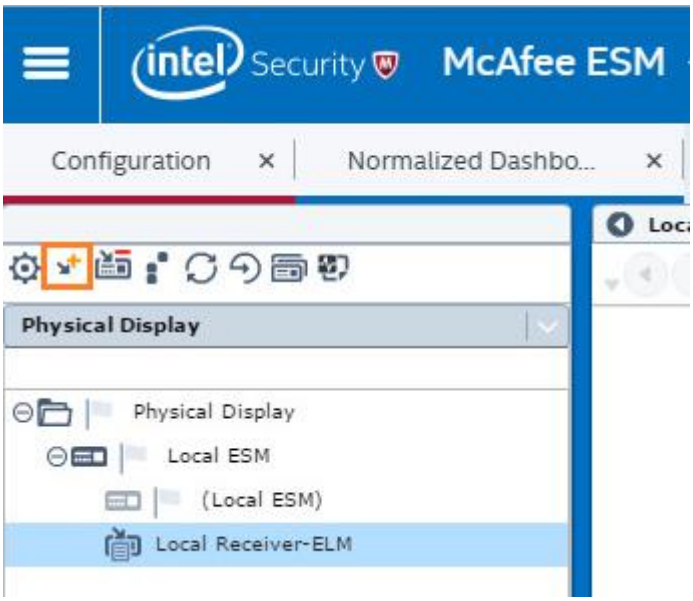


Figure 6. Adding a data source

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

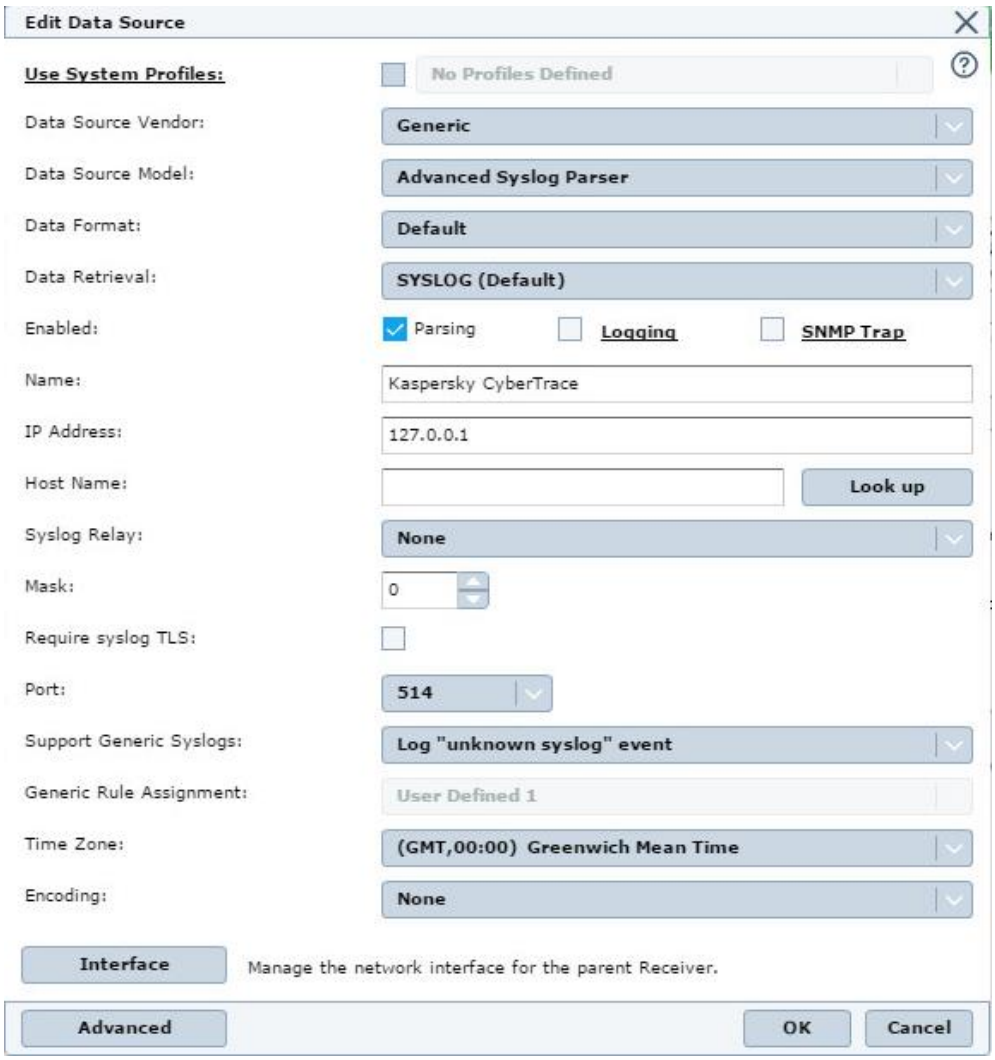


Figure 7. Configuration of the data source

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.

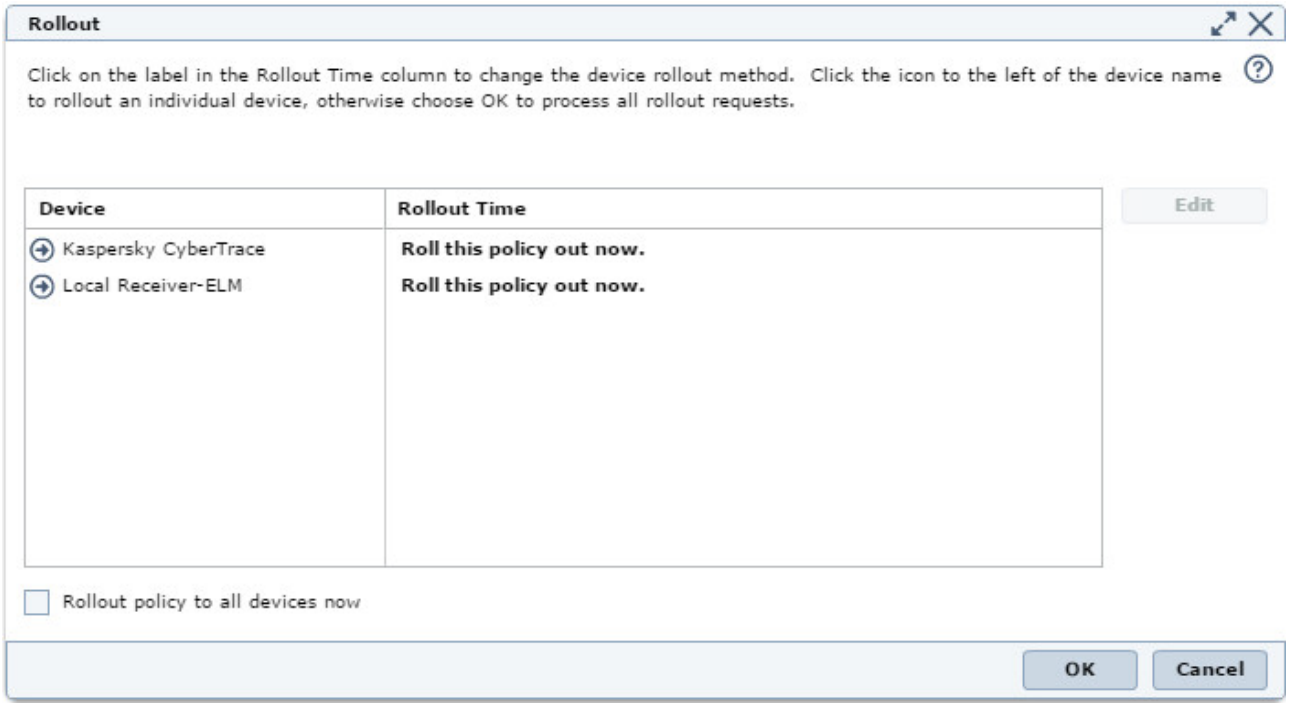


Figure 8. Rollout dialog box

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

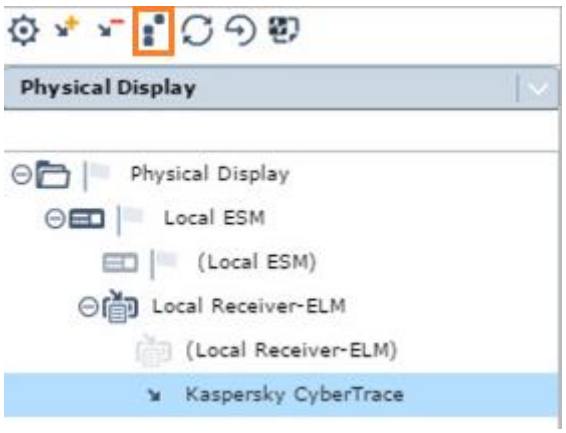


Figure 9. Selecting Policy editor

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

8. Click **New > Advanced Syslog Parser Rule**.

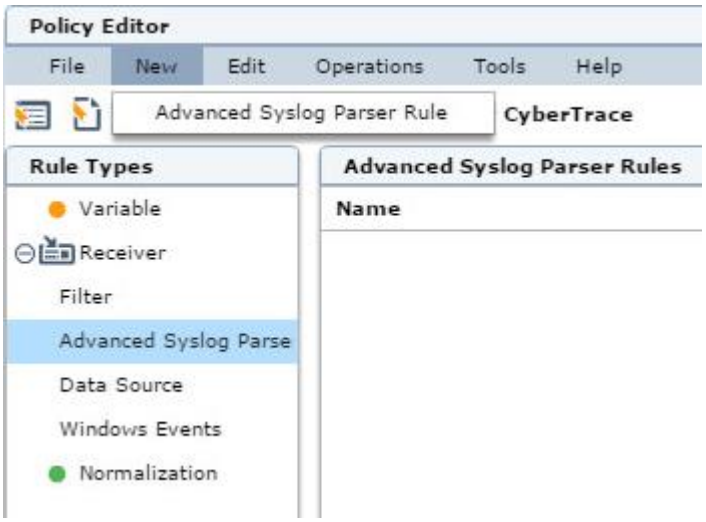


Figure 10. Policy Editor window

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+\s\d+\s\S+)

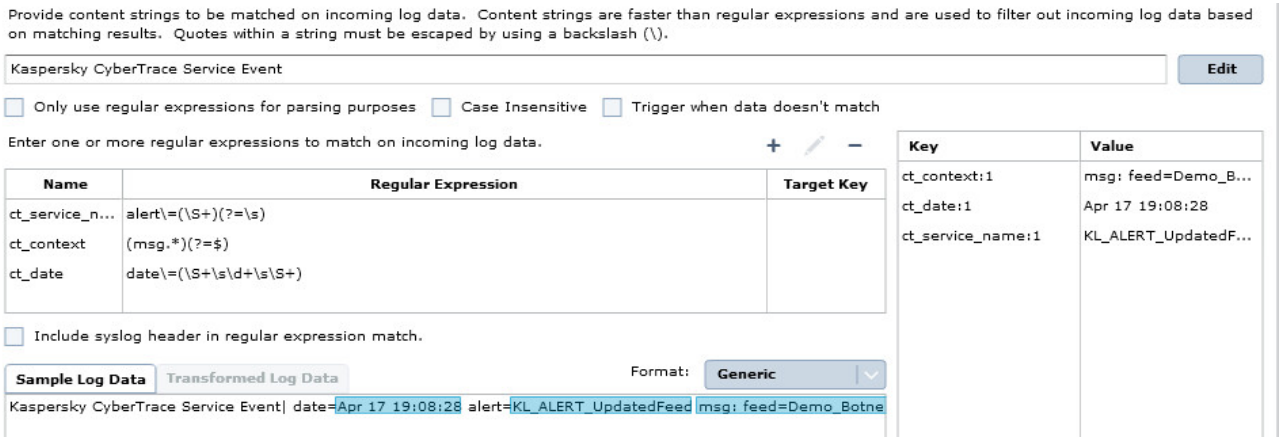


Figure 11. Parsing tab

- 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

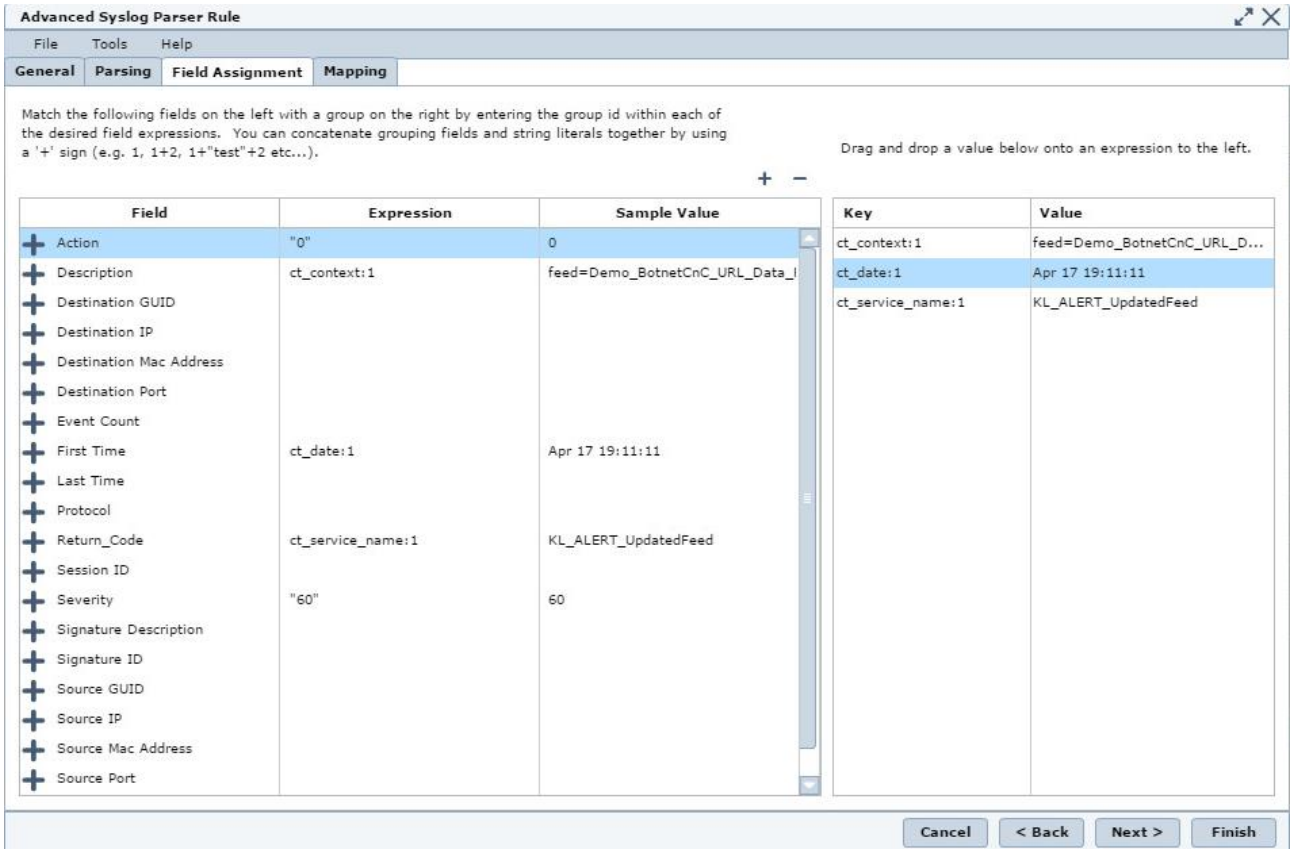


Figure 12. Field Assignment tab

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

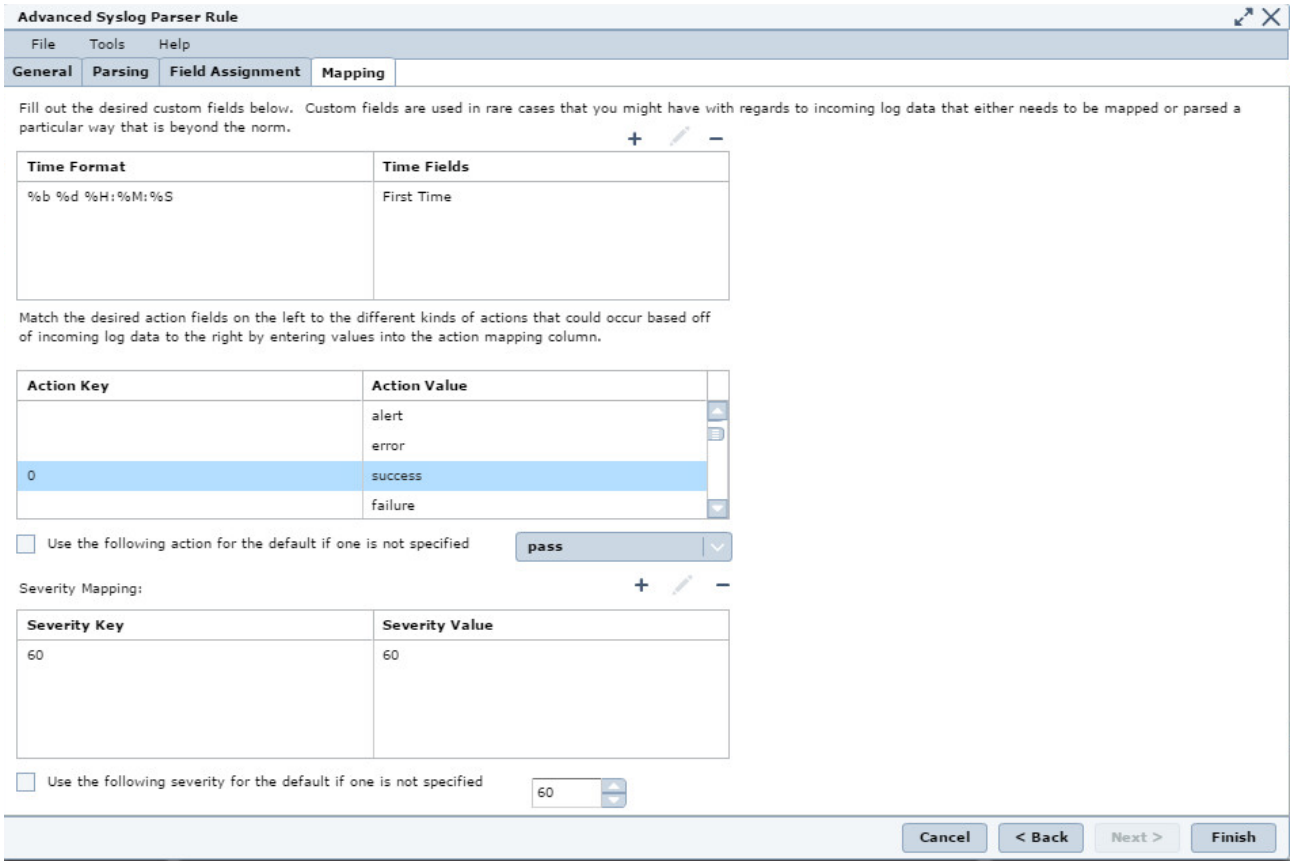


Figure 13. Mapping tab

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

11. In the **Default Policy** list select the `Kaspersky CyberTrace` device and enable the `Kaspersky_CyberTrace_ServiceEvent` rule.

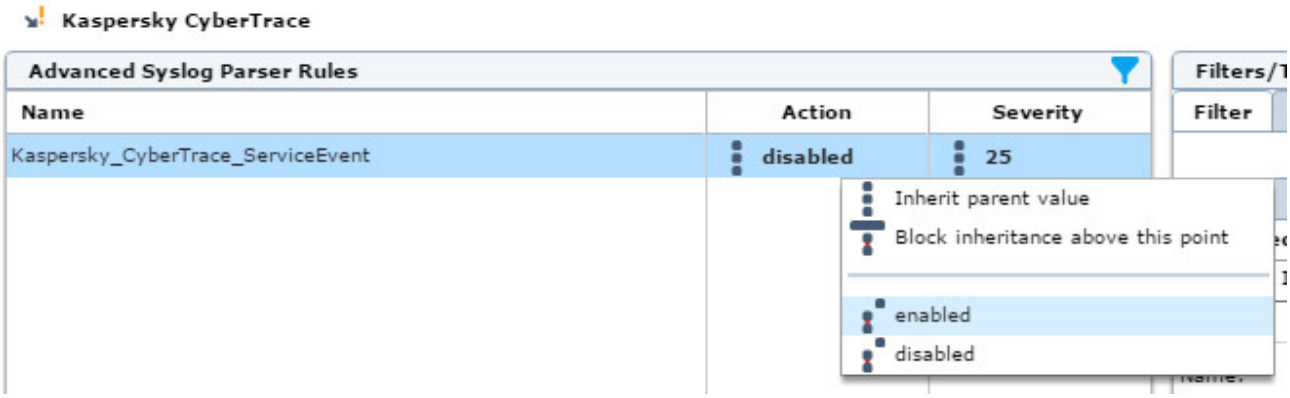


Figure 14. Enabling a rule

12. Select **File** > **Save** menu to save the current state.
13. Select **Operations** > **Rollout** to roll out the policy.

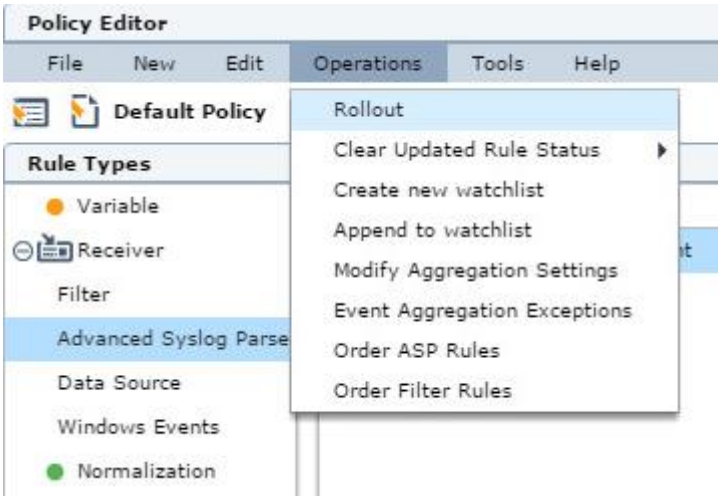


Figure 15. Rolling out a policy

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**.

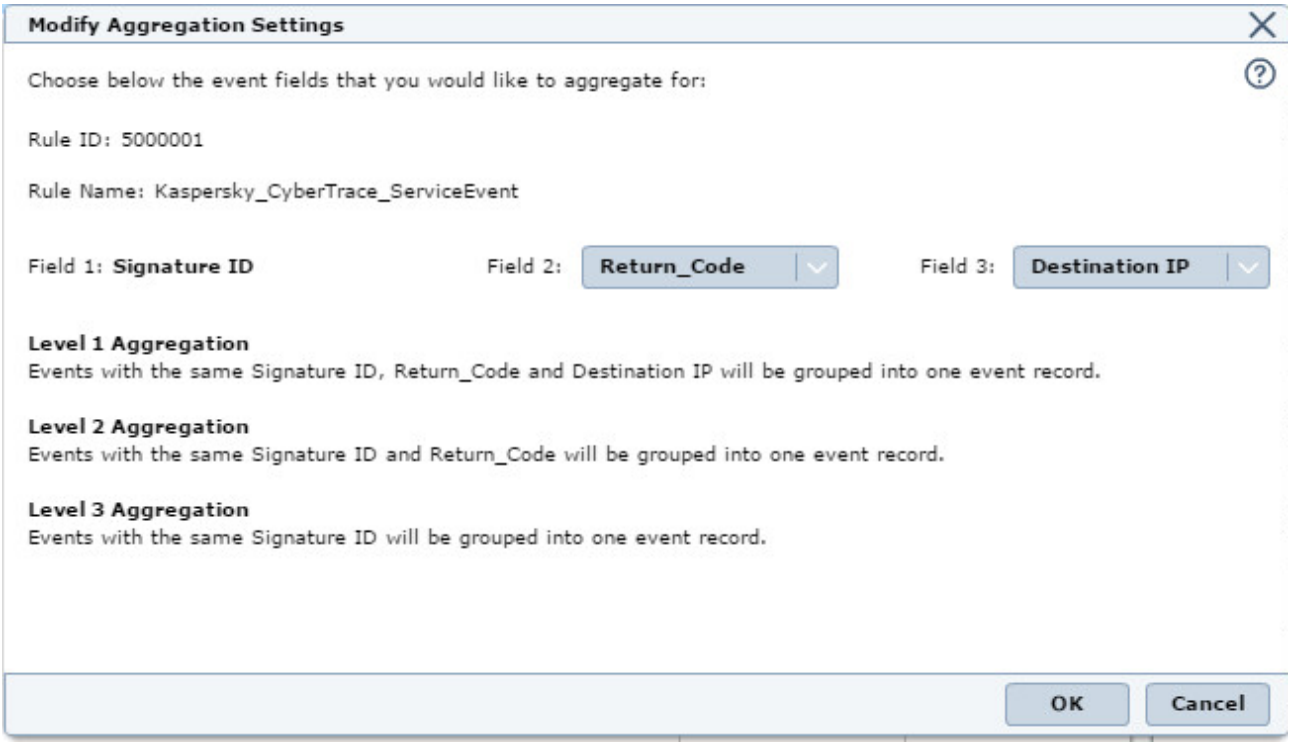


Figure 16. Modify Aggregation Settings

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	detected\=(.*)\sact
ct_dev_action	act\=(.*)\sdst
ct_dst	dst\=(\S+)
ct_src	src\=(\S+)
ct_hash	hash\=(\S+)
ct_request	request\=(.*)\sdvc
ct_dev_ip	dvc\=(\S+)
ct_serviceName	sourceServiceName\=(.*)\ssuser
ct_username	suser\=(.*?)\smsg
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:*

1. 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_**.

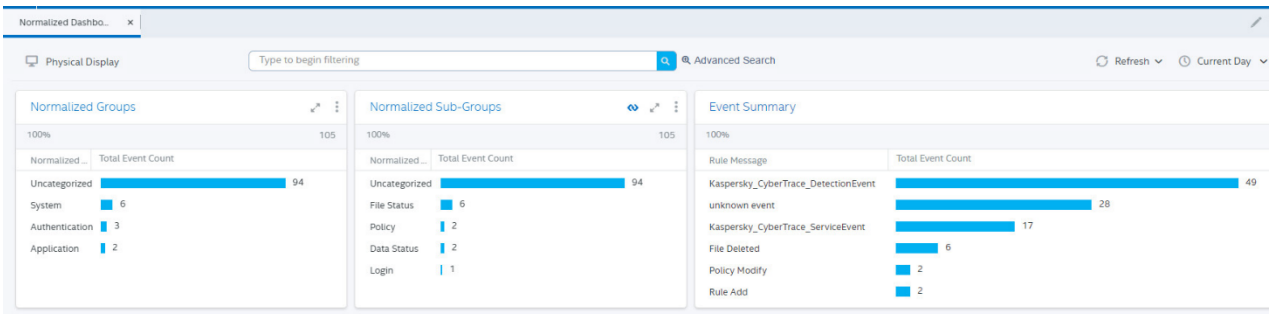


Figure 17. Browsing event summary

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

   The **Events** table will contain events from Kaspersky CyberTrace.

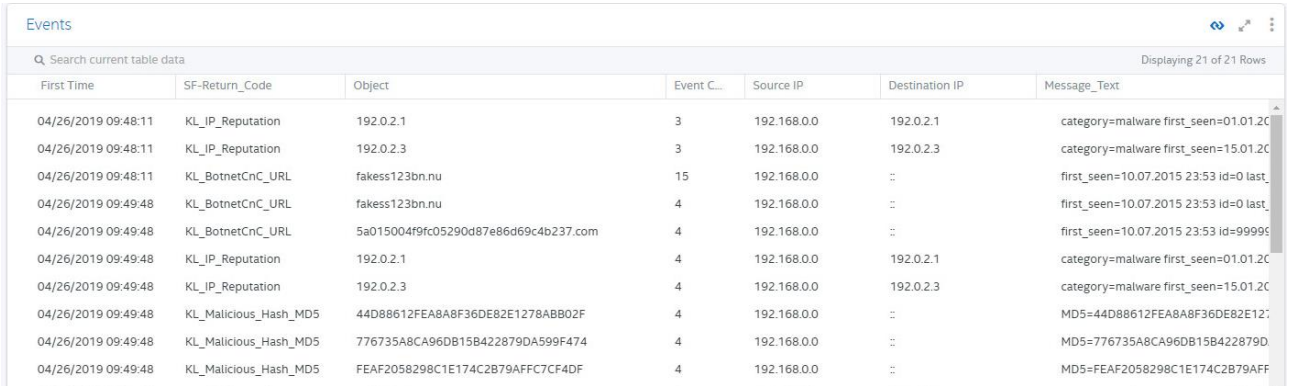


Figure 18. Kaspersky CyberTrace events list

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

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

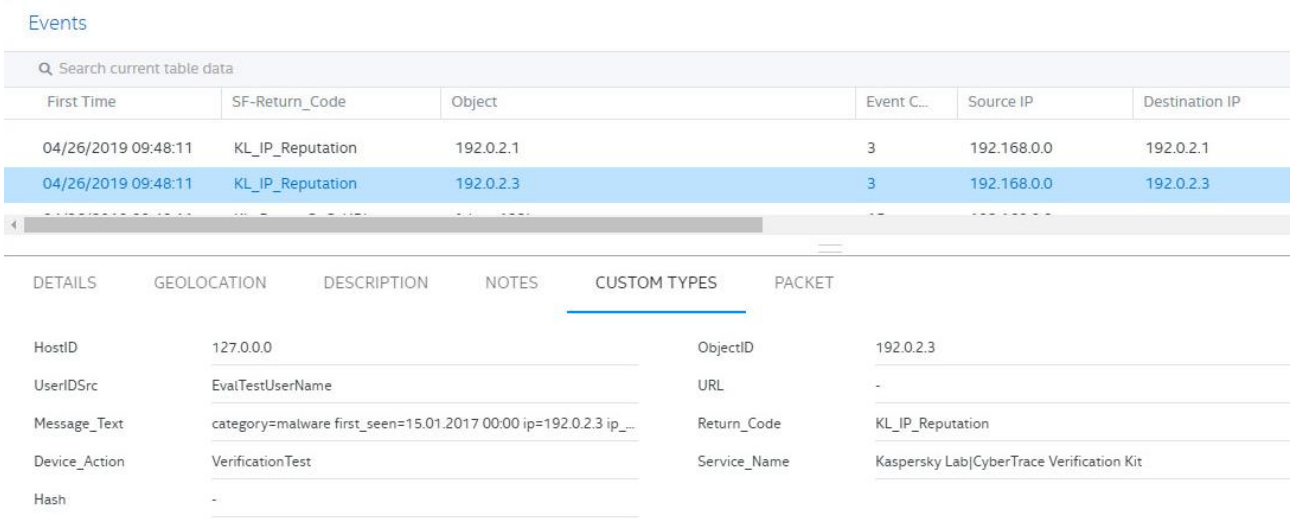


Figure 19. Browsing the event information

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.

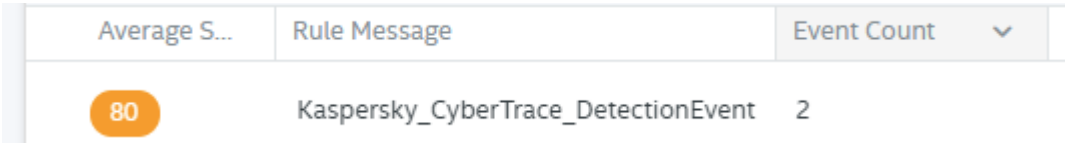


Figure 20. An aggregated Kaspersky CyberTrace detection event

► *To view each Kaspersky CyberTrace event separately, perform the following steps:*

1. Open **Configuration**.
2. Select the `Kaspersky CyberTrace` device and click  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 12)" and "Parsing Kaspersky CyberTrace detection events in McAfee Enterprise Security Manager (on page 20)").

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**.

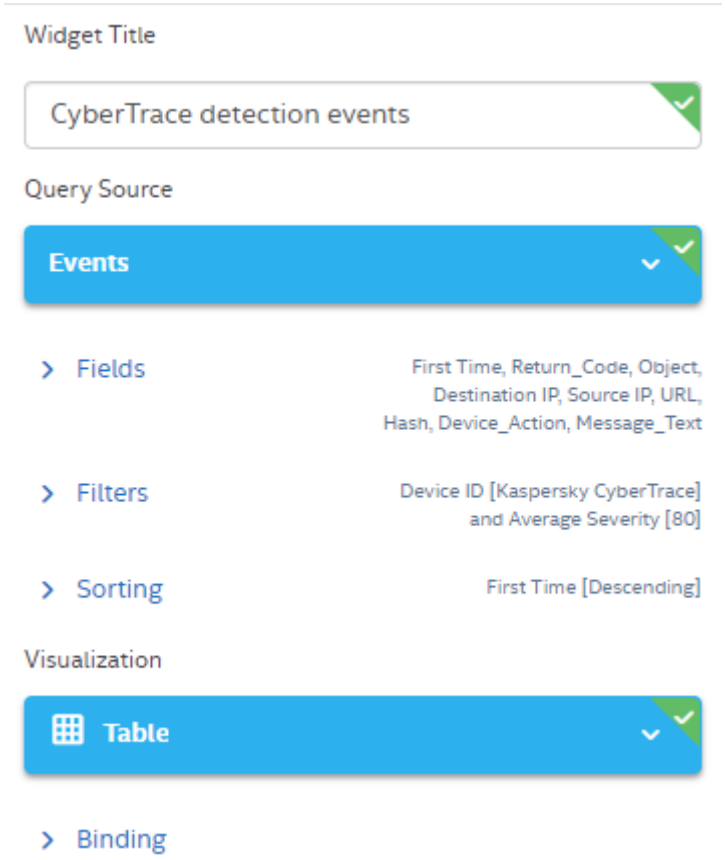
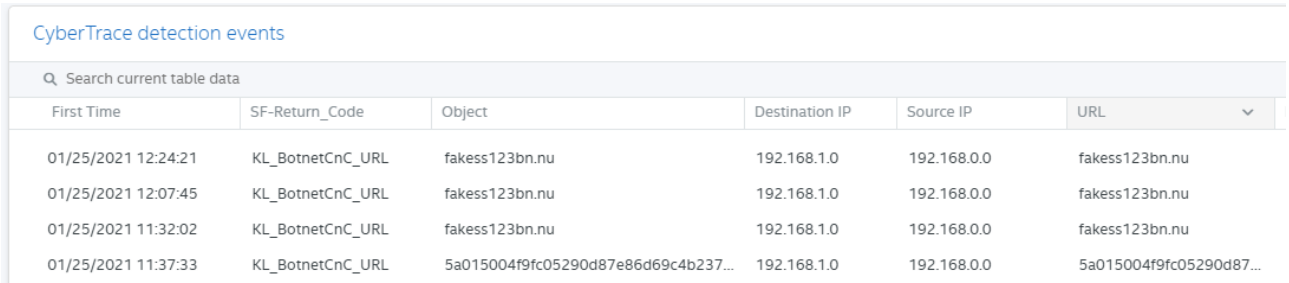


Figure 21. Widget parameters

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.



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

kaspersky

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.