kaspersky

How to integrate Kaspersky Threat Data Feeds with ArcSight ESM

Product version: 1.1

Dear User,

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

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: 09.10.2020

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

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

Contents

About this document

This document explains how to download Kaspersky Threat Data Feeds and import them to ArcSight ESM.

About importing feeds to ArcSight ESM

You can import Kaspersky Threat Data Feeds to ArcSight ESM. After Kaspersky Threat Data Feeds are imported to ArcSight ESM, the fields of events that arrive in ArcSight ESM are matched against indicators from the downloaded feeds. If a field matches a feed record, ArcSight ESM adds a detection event to the Active List.

You can import the following Kaspersky Threat Data Feeds to ArcSight ESM:

- IP Reputation Data Feed—A set of IP addresses with context that cover different categories of suspicious and malicious hosts.
- Botnet CnC URL Data Feed—A set of URLs and hashes with context that cover desktop botnet C&C servers and related malicious objects.
- Malicious URL Data Feed—A set of URLs with context that cover malicious websites and web pages.
- Phishing URL Data Feed—A set of URLs with context that cover phishing websites and web pages.
- Malicious Hash Data Feed—A set of file hashes with context that cover the most dangerous, prevalent, or emerging malware.
- P-SMS Trojan Data Feed—A set of Trojan hashes with context for detecting SMS Trojans that send premium-rate SMS messages to mobile users and enable attackers to steal, delete, and respond to SMS messages.
- Mobile Botnet URL Data Feed—A set of URLs with context that cover mobile botnet C&C servers.
- APT IP Data Feed—A set of IP addresses that belong to the infrastructure used in APT campaigns.
- APT Hash Data Feed—A set of hashes that cover malicious artifacts used by APT actors to conduct APT campaigns.
- APT URL Data Feed—A set of domains that belong to the infrastructure used in APT campaigns.
- Mobile Malicious Hash Data Feed—A set of file hashes with context for detecting malicious objects that infect mobile Google™ Android™ and Apple® iPhone® devices.
- Ransomware URL Data Feed—A set of URLs, domains, and hosts with context that cover ransomware links and websites.
- IoT URL Data Feed—A set of URLs with context covering malicious links used to download malware that infects Internet of Things-enabled (IoT) devices.
- Vulnerability Data Feed—A set of file hashes with context that cover vulnerabilities in applications and cover exploits that use those vulnerabilities.
- ICS Hash Data Feed—A set of file hashes with corresponding context covering the malicious objects that are used to attack Industrial Control Systems infrastructure (ICS).
- Demo IP Reputation Data Feed—Demo version of IP Reputation Data Feed.
- Demo Bonet CnC URL Data Feed—Demo version of Bonet CnC URL Data Feed.
- Demo Malicious Hash Data Feed—Demo version of Malicious Hash Data Feed.
- Demo APT IP Data Feed—Demo version of APT IP Data Feed.
- Demo APT Hash Data Feed—Demo version of APT Hash Data Feed.

- Demo APT URL Data Feed—Demo version of APT URL Data Feed.

To import Kaspersky Threat Data Feeds you use Kaspersky Feed Utility and the kl_feed_for_arcsight.py script. The feeds are downloaded and converted to a format that can be imported to ArcSight ESM.

Alternative way of using Kaspersky Threat Data Feeds in ArcSight ESM

This document describes the process importing of Kaspersky Threat Data Feeds to ArcSight ESM. Alternatively, you can integrate Kaspersky Threat Data Feeds with ArcSight ESM by using Kaspersky CyberTrace.

Kaspersky CyberTrace key features include the following:

- Kaspersky CyberTrace is flexible and can be easily integrated into the existing infrastructure, which allows you to avoid the challenges of integrating threat intelligence feeds with ArcSight ESM.
- Kaspersky CyberTrace does not hinder the performance of existing security controls and does not miss detections. The process of parsing and matching incoming data occurs inside Kaspersky CyberTrace. This reduces the load on the existing SIEM solution.
- Kaspersky CyberTrace helps to reduce the frequency of false positives.

For more information about the integration of Kaspersky CyberTrace with ArcSight ESM, visit https://support.kaspersky.com/13852.

Hardware and software requirements

This section describes the system requirements of Kaspersky Feed Utility and the kl_feed_for_arcsight.py script.

Hardware requirements

Kaspersky Feed Utility and the kl_feed_for_arcsight.py script have the following hardware requirements:

- 300 megabytes (MB) of disk space

Software requirements

Kaspersky Feed Utility and the kl_feed_for_arcsight.py script have the following software requirements:

- Linux® x64
- Python 3 or later version

Network requirements

Kaspersky Feed Utility and the kl_feed_for_arcsight.py script have the following network requirements:

- The Kaspersky Feed Utility binary file (kl_feed_util) must have access to wlinfo.kaspersky.com:443.

ArcSight ESM version and modules

Kaspersky Threat Data Feeds can be imported to ArcSight ESM 6.11 or later version.

ArcSight SmartConnector must be installed and run in Syslog Daemon mode so that it will receive feed records from the kl_feed_for_arcsight.py script and send them to ArcSight ESM using TCP. You can install ArcSight SmartConnector either on the same computer with Kaspersky Feed Utility and kl_feed_for_arcsight.py, or on another computer that belongs to the enterprise network.

Distribution kit

The distribution kit for Kaspersky Feed Utility and the kl_feed_for_arcsight.py script contains the following files:

Table 1. Distribution kit contents

File	Description
bin/feeds.pem	Certificate that allows downloading demo feeds.
bin/kl_feed_util	Kaspersky Feed Utility binary file. It downloads Kaspersky Threat Data Feeds and converts them from JSON format to CSV format.
bin/kl_feed_for_arcsight.py	Script that converts Kaspersky Threat Data Feeds to the format required by ArcSight ESM and sends the feed contents to ArcSight SmartConnector using TCP.
bin/kl_feed_util.conf	Kaspersky Feed Utility configuration file.
bin/kl_feed_util.sh	Script that runs the kl_feed_util file and then the kl_feed_for_arcsight.py file. This script is used for automating the process of downloading and converting Kaspersky Threat Data Feeds and loading them to ArcSight ESM.
doc/Kaspersky_Feed_Utility.html	Kaspersky Feed Utility documentation.
doc/license.txt	End User License Agreement for Kaspersky Threat Data Feeds and Kaspersky Feed Utility.
doc/legal_notices.txt	List of third-party code that is used in Kaspersky Feed Utility.
doc/Importing_Threat_Data_Feeds_in_ArcSight_ESM.pdf	Instructions for importing Kaspersky Threat Data Feeds to ArcSight ESM.
integration/Kaspersky_Threat_Data_Feeds.arb	ARB package that contains rules from importing Kaspersky Threat Data Feeds to ArcSight ESM.

Feeds integration workflow

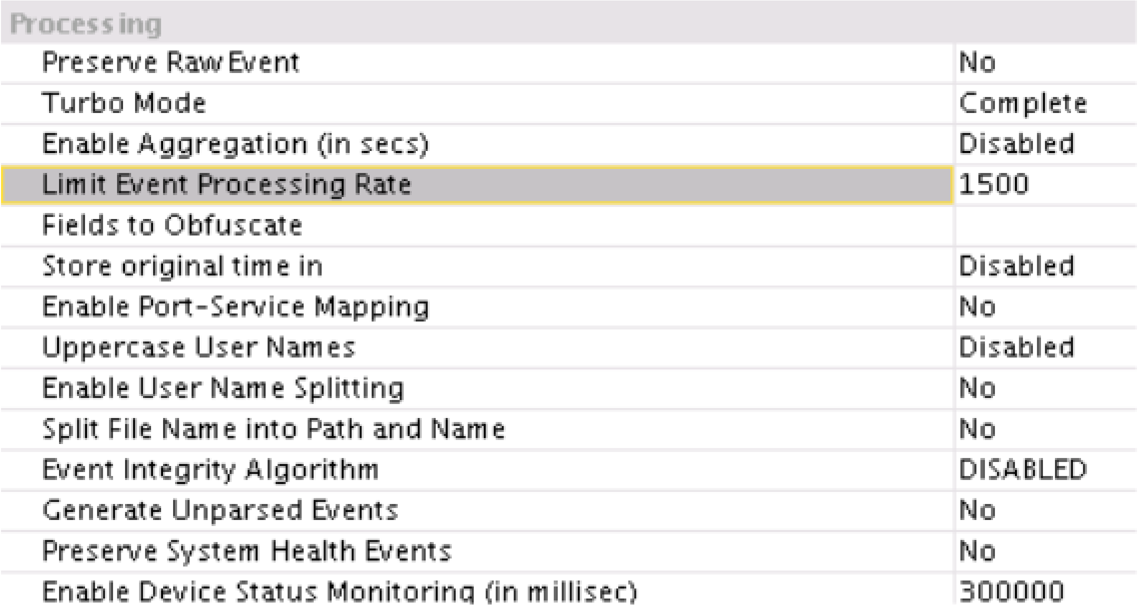
This section describes the scenario to integrate Kaspersky Threat Data Feeds with ArcSight ESM and how the software products interact after integration.

► *To integrate Kaspersky Threat Data Feeds with ArcSight ESM:*

1. Install and configure Kaspersky Feed Utility (see section "Installing and configuring Kaspersky Feed Utility" on page 11).
2. Install ArcSight SmartConnector (see section "Installing ArcSight SmartConnector" on page 13).
3. Import the Kaspersky_Threat_Data_Feeds.arb package in Arcsight ESM.

   The objects that will be added are listed below, in subsection "Objects contained in the ARB package".
4. Optionally, you can set a limit on the processing rate of incoming events by ArcSight SmartConnector.

   To set this limit, in the **Connectors** section of ArcSight Console, open the installed ArcSight SmartConnector and in the **Default** > **Content** tab, in the **Processing** section, specify the desired value of the **Limit Event Processing Rate** setting. We recommend that you specify a value not to exceed 2500.



Processing	
Preserve Raw Event	No
Turbo Mode	Complete
Enable Aggregation (in secs)	Disabled
Limit Event Processing Rate	1500
Fields to Obfuscate	
Store original time in	Disabled
Enable Port-Service Mapping	No
Uppercase User Names	Disabled
Enable User Name Splitting	No
Split File Name into Path and Name	No
Event Integrity Algorithm	DISABLED
Generate Unparsed Events	No
Preserve System Health Events	No
Enable Device Status Monitoring (in millisec)	300000

Figure 1: ArcSight SmartConnector processing settings

Objects contained in the ARB package

The Kaspersky_Threat_Data_Feeds.arb package contains the following objects (see section "The Kaspersky_Threat_Data_Feeds.arb package contents" on page 30):

- Rules for filling in lists with indicators from Kaspersky Threat Data Feeds
- Rules for matching URLs, IP addresses, and hashes from events that arrive in ArcSight ESM against indicators from Kaspersky Threat Data Feeds

Result: Integrated actions

When Kaspersky Threat Data Feeds are integrated with ArcSight ESM, the following actions are performed:

1. The cron utility runs the kl_feed_util.sh script every hour.
2. The kl_feed_util.sh script checks whether the date of the last run of Kaspersky Feed Utility differs from the current date.

   If the dates differ, the kl_feed_util.sh script removes the feeds that were downloaded earlier. If the dates are the same, the script does not remove the earlier feeds.
3. The kl_feed_util.sh script runs Kaspersky Feed Utility that downloads Kaspersky Threat Data Feeds from the web address https://wlinfo.kaspersky.com.
4. If there are feeds downloaded earlier on the working computer, Kaspersky Feed Utility creates files that contain only new records (records not present in the feeds downloaded earlier). Otherwise, Kaspersky Feed Utility creates files that contain all records from Kaspersky Threat Data Feeds.

   Whole feeds will be imported in ArcSight ESM only once a day. At other times, only new and modified records will be imported.
5. On the basis of the files created in the previous step, the kl_feed_for_arcsight.py script generates events in CEF format and sends them to ArcSight SmartConnector by using TCP (see section "The kl_feed_for_arcsight.py script workflow" on page 29).
6. ArcSight SmartConnector receives events from the kl_feed_for_arcsight.py script and sends them to ArcSight ESM.
7. ArcSight ESM receives events from ArcSight SmartConnector and fills the lists with indicators from Kaspersky Threat Data Feeds according to the rules contained in the Kaspersky_Threat_Data_Feeds.arb package.

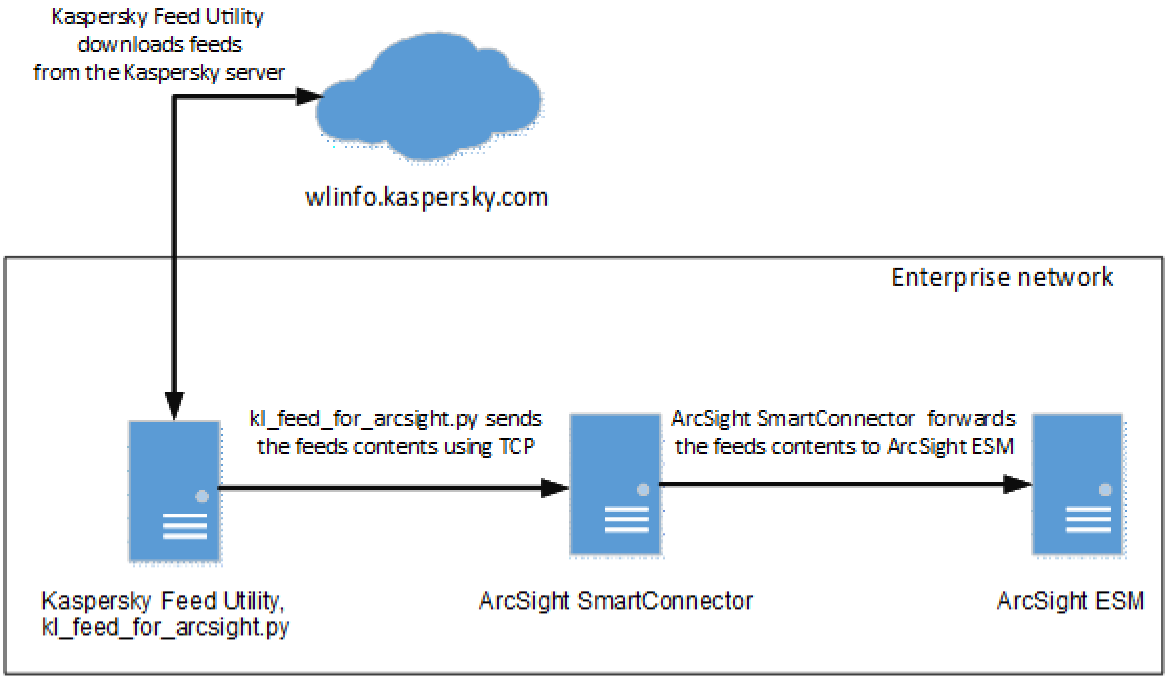

Kaspersky Feed Utility downloads feeds from the Kaspersky server
wlinfo.kaspersky.com
Enterprise network
kl_feed_for_arcsight.py sends the feeds contents using TCP
ArcSight SmartConnector forwards the feeds contents to ArcSight ESM
Kaspersky Feed Utility, kl_feed_for_arcsight.py
ArcSight SmartConnector
ArcSight ESM

Figure 2: Feeds integration workflow

Installing and configuring Kaspersky Feed Utility

This section explains how to install and configure Feed Utility for downloading Kaspersky Threat Data Feeds.

► *To install and configure Kaspersky Feed Utility for downloading Kaspersky Threat Data Feeds:*

1. On the working computer, create the `/opt/kaspersky/feed_util` directory.

   > By default, only the owner has permissions to access all executable and configuration files. It is recommended that none but the owner has rights for accessing the objects listed in this section (directories, executable files, etc.).

2. Unpack the archive containing Kaspersky Feed Utility and the kl_feed_for_arcsight.py script to this directory.
3. Copy the certificate for downloading Kaspersky Threat Data Feeds to the `/opt/kaspersky/feed_util/bin` directory. Make sure that the certificate name is feeds.pem. If there is already a feeds.pem file in this directory, you can either remove or rename it (for example, rename it to demo_feeds.pem).
4. Open the `/opt/kaspersky/feed_util/bin/kl_feed_util.conf` configuration file for editing.
5. Read the End-User License Agreement (EULA), which is provided in the `doc/license.txt` file. Agree to its terms by specifying the `accepted` value in the `EULA` element in the Kaspersky Feed Utility configuration file. If you do not accept the EULA, Kaspersky Feed Utility will not work.
6. For every feed you want to use, set the value of the `enabled` attribute to `true`. For every feed you do not want to use, set the value of the `enabled` attribute to `false`.

   > Do not use a commercial feed and its demo version simultaneously.

7. In the `ArcSightConnectorAddr` element, specify the IP address and port of ArcSight SmartConnector, to which the kl_feed_for_arcsight.py script will send the contents of Kaspersky Threat Data Feeds.

   The IP address and port must be specified in the format `<IP>:<PORT>`. For example: `127.0.0.1:9000`.

8. In the `ArcSightEPS` element, specify the maximum number of feed records per second that the kl_feed_for_arcsight.py script will send to ArcSight Smart Connector.

   > Note that the high rate of transferring events can hurt the performance of ArcSight ESM. For information on how to increase the resource consumption threshold in ArcSight ESM, see section "Configuring ArcSight ESM in different cases (see section "Configuring ArcSight ESM in certain cases" on page 41)".

9. Save the configuration file and close it.
10. If necessary, specify proxy settings for Kaspersky Feed Utility so that it has access to the web address

https://wlinfo.kaspersky.com.

To specify the proxy settings, run the kl_feed_util file with the `--set-proxy username:password@host:port` parameter. Here, `username:password` constitutes the user name and password for authentication on the proxy server (if necessary), and `host:port` constitutes the address and port of the proxy server.

For example:

```
./kl_feed_util --set-proxy 'user:pass@proxy.example.com:3128'
```

This must be done only once. The entered credentials will be encrypted and stored in the Feed Utility configuration file.

11. On the working computer, perform the following commands to set up regular updating of Kaspersky Threat Data Feeds:

    ```
    crontab -l > /tmp/crontab_list
    ```

    ```
    echo "* */1 * * * /opt/kaspersky/feed_util/bin/kl_feed_util.sh" >>
    /tmp/crontab_list
    ```

    ```
    crontab /tmp/crontab_list
    ```

    Kaspersky Threat Data Feeds will be updated every 15 minutes.

12. Run the `/opt/kaspersky/feed_util/bin/kl_feed_util.sh` script. If no errors have occurred, the following message will be printed to the console:

    ```
    [   OK   ]
    ```

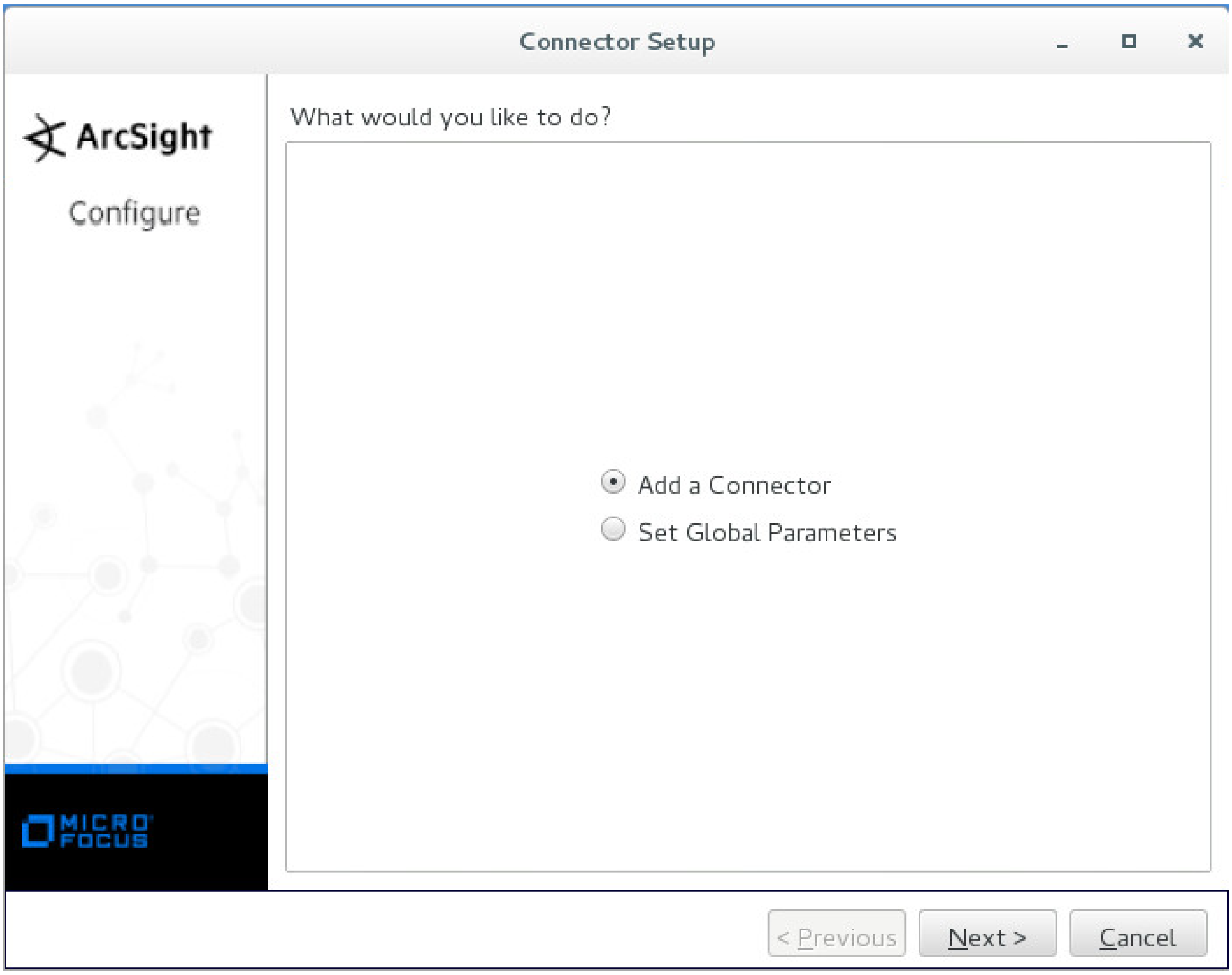
Make sure that no errors occur during the feeds update and Kaspersky Threat Data feeds download. The feeds are downloaded to the directory specified in the `FeedsDir` element of the kl_feed_util.conf configuration file. If errors occur, they will be printed to the console.

Installing ArcSight SmartConnector

This section describes how to install ArcSight SmartConnector.

► *To install ArcSight SmartConnector:*

1. Run the ArcSight SmartConnector installation application.
2. Select the ArcSight SmartConnector installation directory (hereinafter referred to as `%ARCSIGHT_HOME%`).
3. Instruct the installer not to create links.
4. After the contents of the binary file are unpacked, select **Add a Connector**.



What would you like to do?

● Add a Connector
○ Set Global Parameters

Figure 3: Adding a connector

If this window is not displayed, configure ArcSight SmartConnector manually. For this purpose, run the following command:

```
%ARCSIGHT_HOME%/current/bin/runagentsetup.sh
```

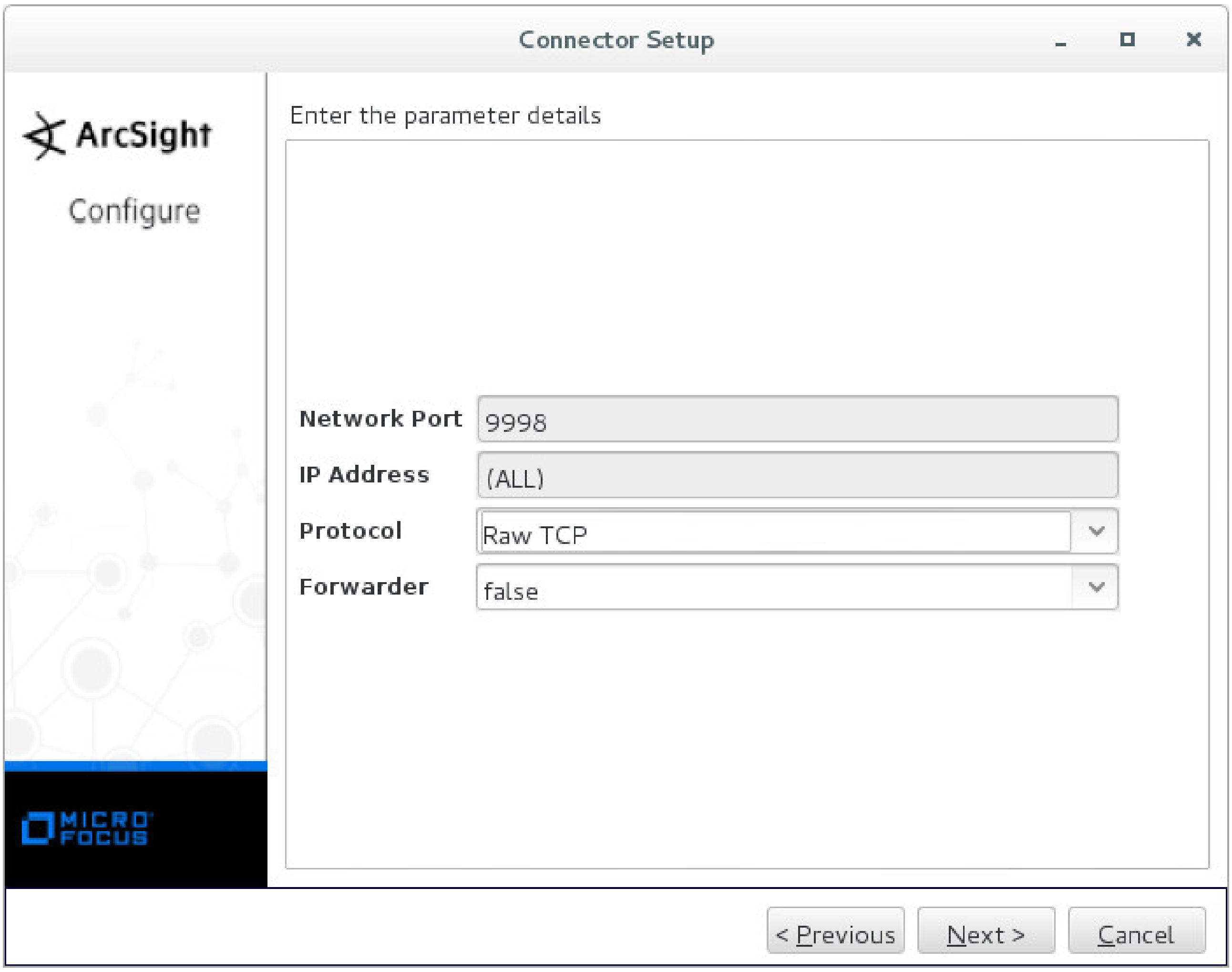
5. Select **Syslog Daemon** as the connector type.

6. On the **Enter the parameter details** form, specify the following data:

   - **Network Port**—Port to which the kl_feed_for_arcsight.py script will send events.
   - **IP Address**—IP address to which the kl_feed_for_arcsight.py script will send events.

     > You can specify `(ALL)` if you want Arcsight SmartConnector to receive events from all network interfaces of the computer on which it runs.

   - **Protocol**—Specify `Raw TCP`.
   - **Forwarder**—Specify `false`.



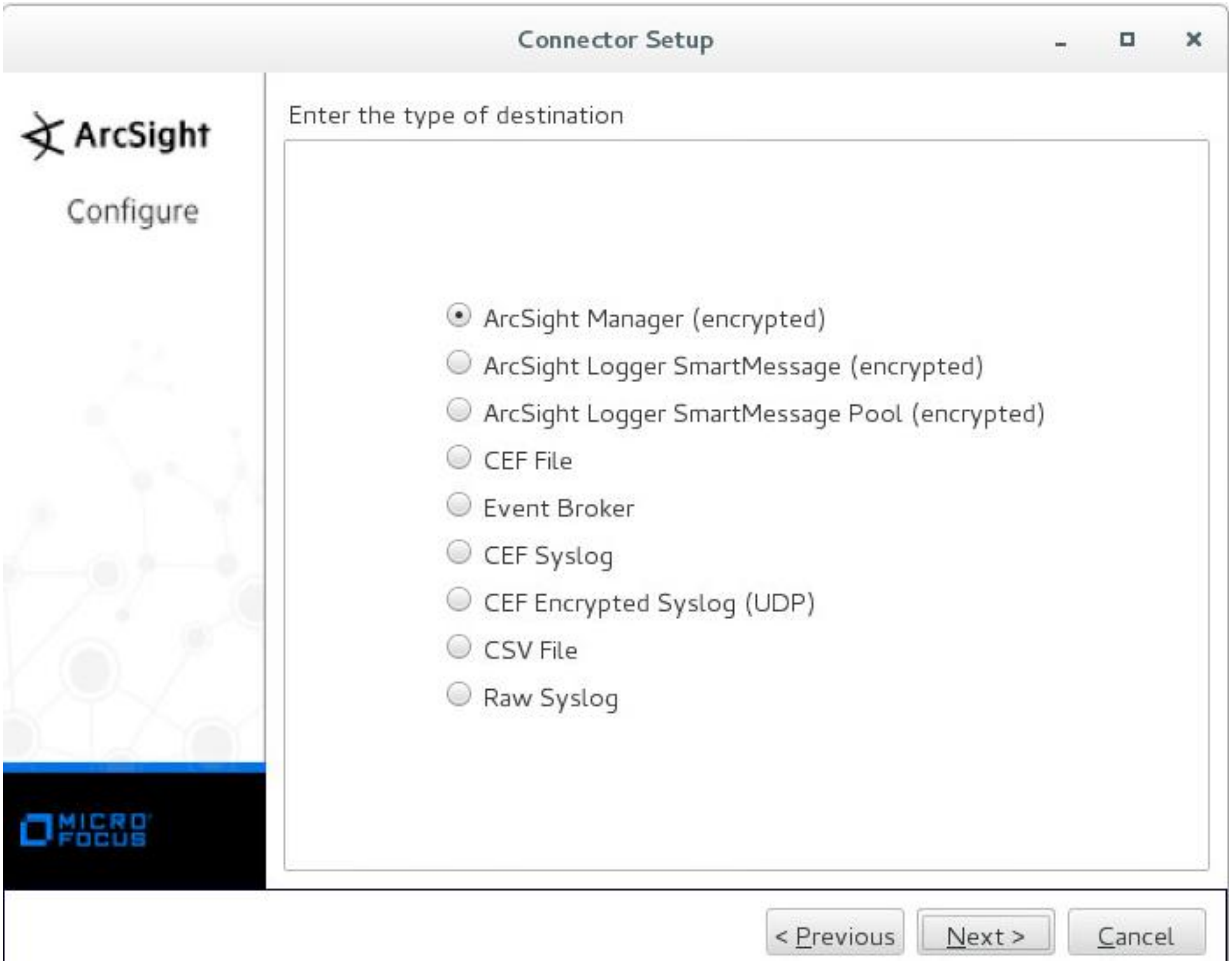
Enter the parameter details

Network Port	9998
IP Address	(ALL)
Protocol	Raw TCP
Forwarder	false

Figure 4: Parameters for sending events

Click **Next**.

7. Specify **ArcSight Manager (encrypted)** as the type of destination.



Enter the type of destination

● ArcSight Manager (encrypted)
○ ArcSight Logger SmartMessage (encrypted)
○ ArcSight Logger SmartMessage Pool (encrypted)
○ CEF File
○ Event Broker
○ CEF Syslog
○ CEF Encrypted Syslog (UDP)
○ CSV File
○ Raw Syslog

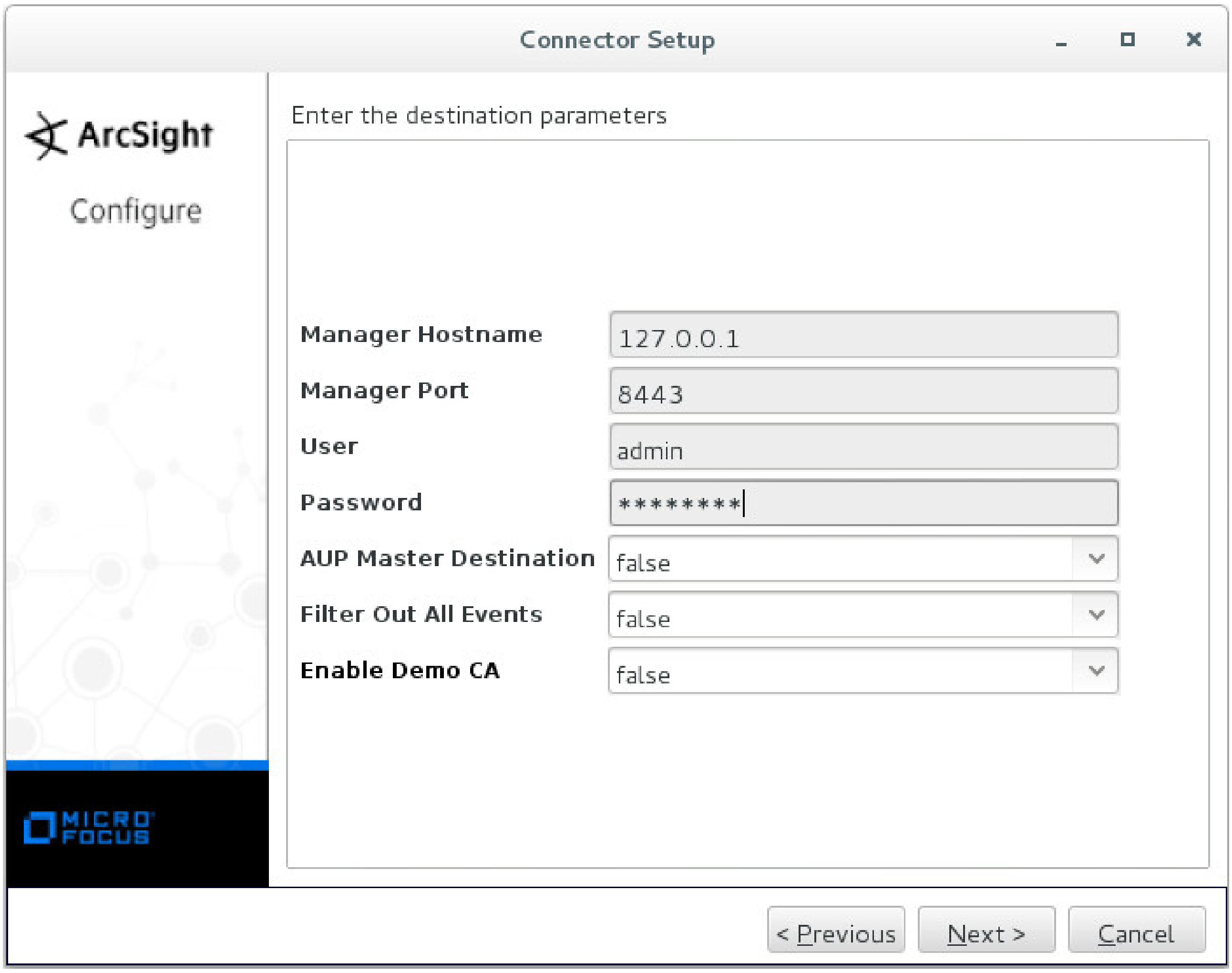
Figure 5: Type of destination

Click **Next**.

8. Specify other destination settings:
   - **Manager Hostname**—Host where ArcSight Manager is running.
   - **Manager Port**—Port where ArcSight Manager is available.

     By default, it is 8443.
   - **User**—Name of the ArcSight ESM user that has rights for registering the connector.
   - **Password**—Password of the ArcSight ESM user.
   - **AUP Master Destination**—Specify **false**.
   - **Filter Out All Events**—Specify **false**.

- **Enable Demo CA**—Specify **false**.



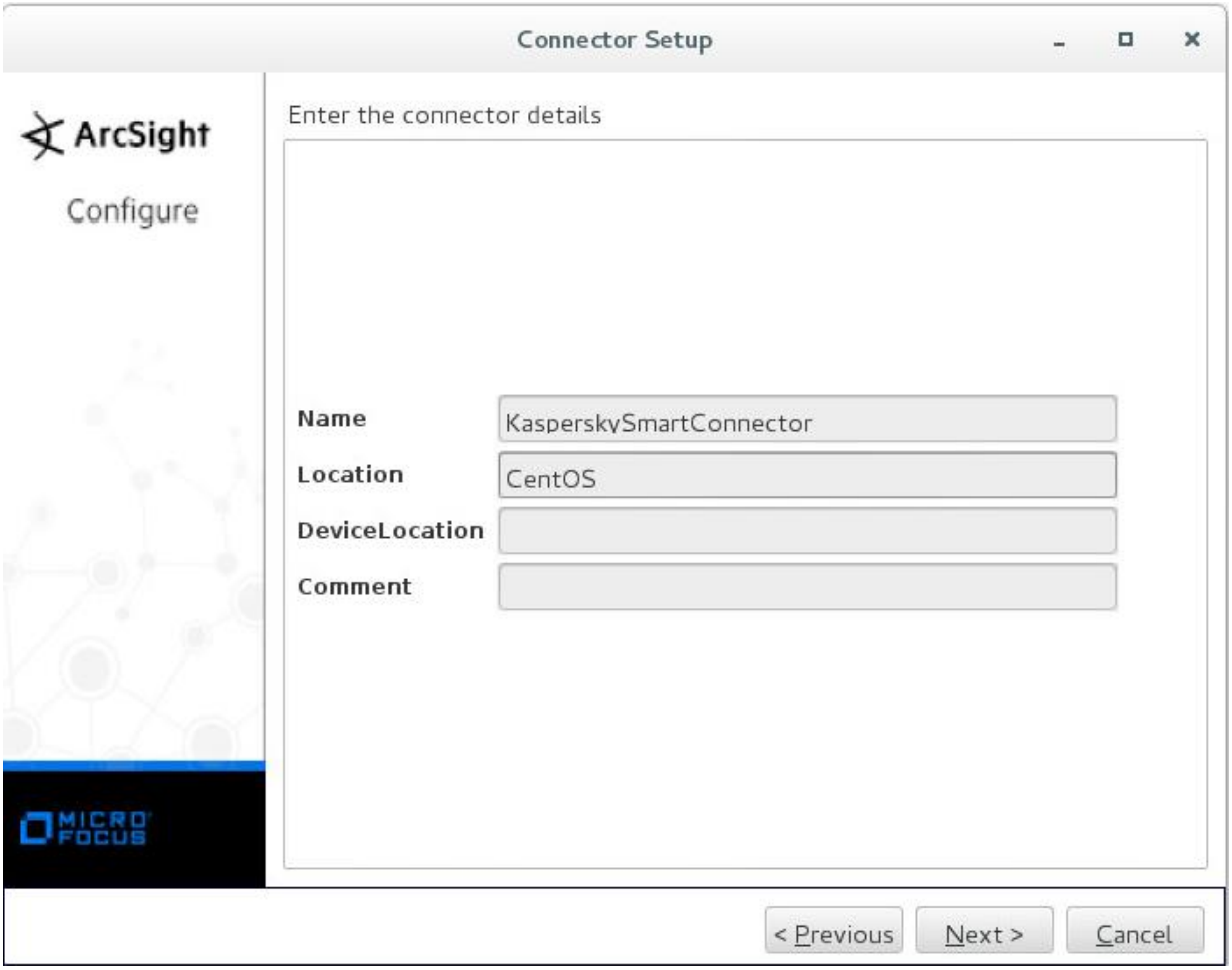
Enter the destination parameters

Manager Hostname	127.0.0.1
Manager Port	8443
User	admin
Password	********
AUP Master Destination	false
Filter Out All Events	false
Enable Demo CA	false

Figure 6: Destination parameters

Click **Next**.

9. Specify the connector details: the name (arbitrary value permitted), location (arbitrary value permitted), location of the device that will send events to the connector (arbitrary value permitted, can be empty), and comment about the connector (arbitrary value permitted, can be empty).



Enter the connector details

Name: KasperskySmartConnector

Location: CentOS

DeviceLocation:

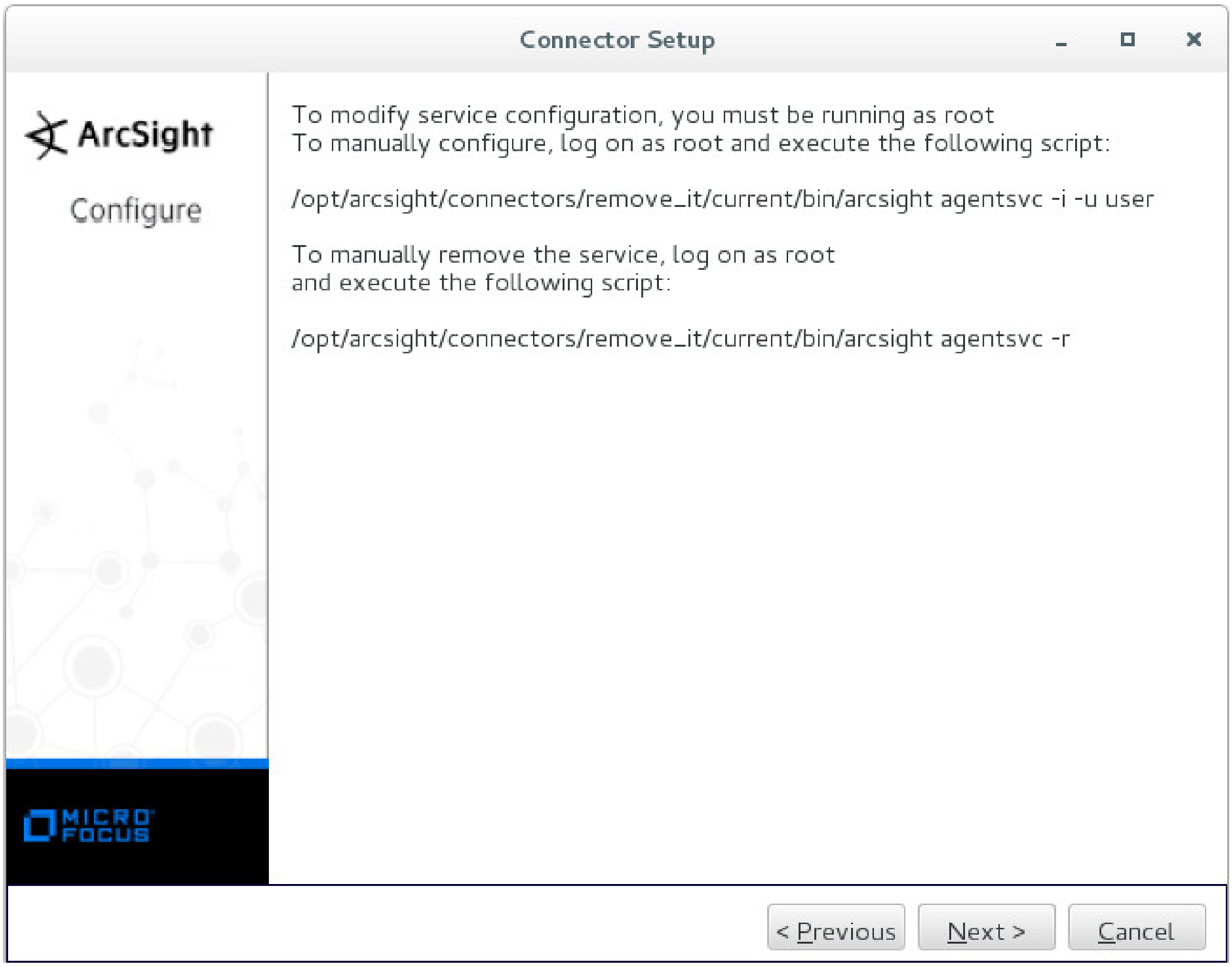
Comment:

Figure 7: Connector details

Click **Next**.

10. If the ArcSight Manager parameters are valid, accept importing the certificate from the destination.
11. If the certificate is imported successfully, install the ArcSight SmartConnector service.

- If you do not run the installation as root, a warning will be displayed.



To modify service configuration, you must be running as root
To manually configure, log on as root and execute the following script:

```
/opt/arcsight/connectors/remove_it/current/bin/arcsight agentsvc -i -u user
```

To manually remove the service, log on as root
and execute the following script:

```
/opt/arcsight/connectors/remove_it/current/bin/arcsight agentsvc -r
```

Figure 8: Warning about user privileges

You can either run the Connector Setup Wizard as root, or run the following command as root:

```
%ARCSIGHT_HOME%/current/bin/arcsight agentsvc -i -u $username -sn
$service_name
```

Here

- `$username` is the name of the operating system user that will run the service.
- `$service_name` is the service name.

  We recommend that you set the service name to be the same as the connector name.

The `%ARCSIGHT_HOME%/current/logs/agent.log` log file will contain messages about the installation process.

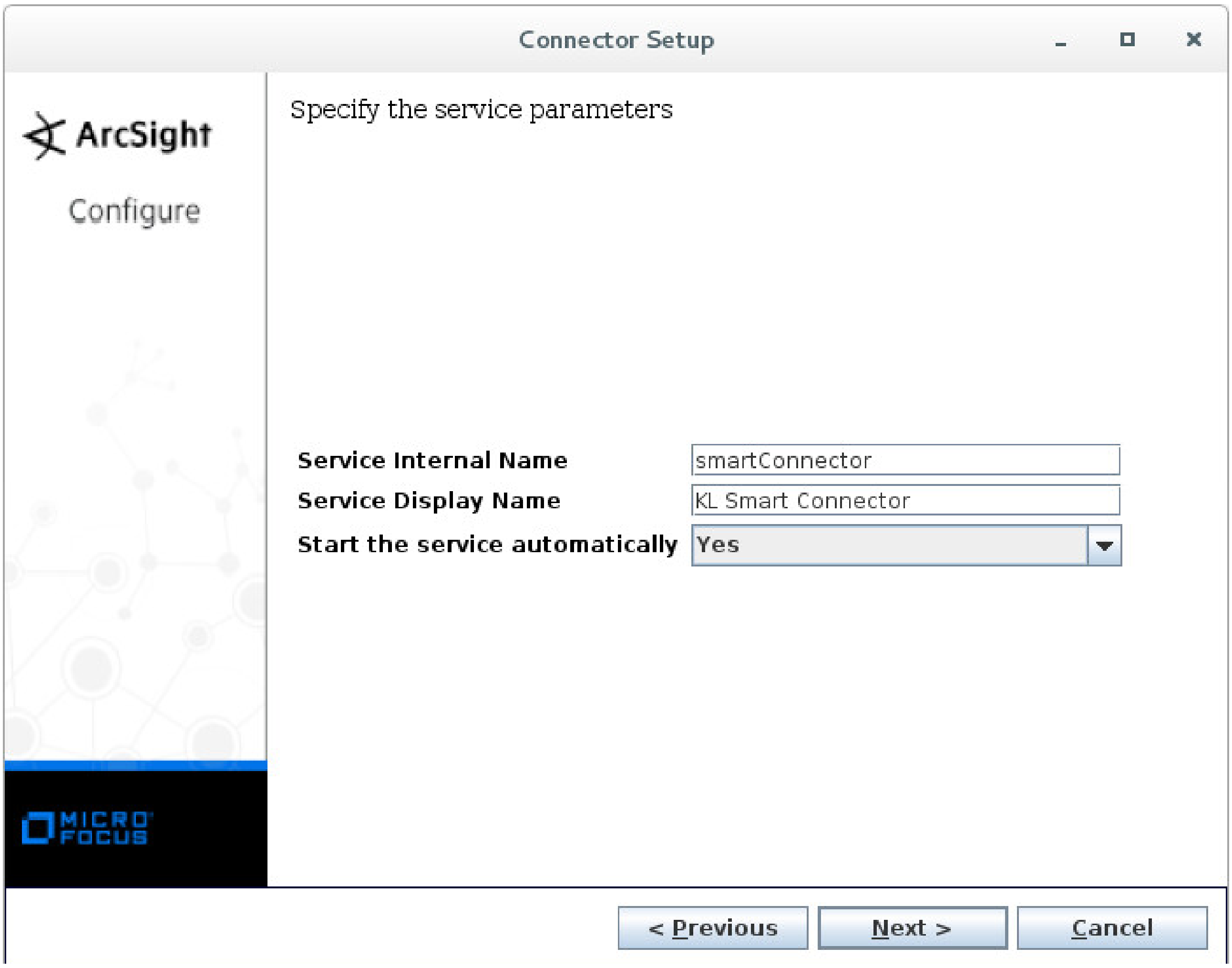
Skip the next step that describes how to specify the service parameters.

- If you run the installation as root, select **Install as a service**.

Click **Next**.

12. Specify the service parameters.

We recommend that you set the service name to be the same as the connector name.



Specify the service parameters

Service Internal Name: smartConnector

Service Display Name: KL Smart Connector

Start the service automatically: Yes

Figure 9: Specifying service parameters

Click **Next**.

13. Start ArcSight SmartConnector by calling the following command:

```
/etc/init.d/arc_$service_name start
```

In this command, `$service_name` is the service name.

Updating Kaspersky Threat Data Feeds

To update Kaspersky Threat Data Feeds, use Kaspersky Feed Utility.

Configure Kaspersky Feed Utility so that it will save the feed fields and apply filters specified in the following table:

Table 2. Feed fields to save and filters to apply

Feed	Fields to save	Filters to apply

Malicious URL Exact Data Feed	`id`
	`urls/url`
	`domains/domain`
	`hosts/host`
	`popularity`
	`last_seen`
	`first_seen`
	`category`
	`files/MD5`
	`files/threat`
		First 100 000 feed records.

Botnet CnC URL Exact Data Feed	`id`
	`urls/url`
	`domains/domain`
	`hosts/host`
	`popularity`
	`last_seen`
	`first_seen`
	`threat`
	`files/MD5`
		First 100 000 feed records.

Demo Botnet CnC URL Data Feed	`id`
	`mask`
	`type`
	`popularity`
	`last_seen`
	`first_seen`
	`threat`
	`files/MD5`
		First 100 000 feed records.

Phishing URL Exact Data Feed	id urls/url domains/domain hosts/host last_seen first_seen popularity industry	First 100 000 feed records.
IP Reputation Data Feed Demo IP Reputation Data Feed	ip threat_score category last_seen first_seen popularity files/MD5 files/threat	Records whose threat_score field is equal to or more than 75.
Malicious Hash Data Feed Demo Malicious Hash Data Feed	id md5 last_seen first_seen popularity threat	First 100 000 feed records.
P-SMS Trojan Data Feed	MD5 Date AV Verdict	First 100 000 feed records.
Mobile Botnet URL Data Feed	id mask type files/MD5 threat popularity last_seen first_seen files/Behaviour	First 100 000 feed records.
APT IP Data Feed Demo APT IP Data Feed	id ip detection_date publication_name	First 100 000 feed records.

APT Hash Data Feed
Demo APT Hash Data Feed
	`id`
	`MD5`
	`detection_date`
	`publication_name`
		First 100 000 feed records.

APT URL Data Feed
Demo APT URL Data Feed
	`id`
	`mask`
	`type`
	`detection_date`
	`publication_name`
		First 100 000 feed records.

Mobile Malicious Hash Data Feed	`id`
	`md5`
	`last_seen`
	`first_seen`
	`popularity`
	`threat`
		First 100 000 feed records.

Ransomware URL Data Feed	`id`
	`mask`
	`type`
	`last_seen`
	`first_seen`
	`popularity`
	`files/MD5`
	`files/threat`
		First 100 000 feed records.

IoT URL Data Feed	`id`
	`mask`
	`type`
	`last_seen`
	`first_seen`
	`port`
	`popularity`
	`files/MD5`
	`files/threat`
		First 100 000 feed records.

Vulnerability Data Feed	`kla_id`
	`detection_date`
	`severity`
	`vulnerable_files/md5`
	`exploits/md5`
	`exploits/threat`
		First 100 000 feed records.

ICS Hash Data Feed	`MD5`
	`first_seen`
	`last_seen`
	`popularity`
	`threat`
		First 100 000 feed records.

Saving feed fields in CEF fields

Every `Feed` element of the kl_feed_util.conf configuration file must have a `CEFFileds` nested element. The `CEFFileds` element specifies the correspondence between the feed fields and CEF fields to which the values of the feed fields must be saved. This correspondence is specified in the following format:

```
<%CEF_FIELD_NAME%>%FEED_FIELD_NAME%</%CEF_FIELD_NAME%>
```

Here `%CEF_FIELD_NAME%` is the name of CEF field, and `%FEED_FIELD_NAME%` is the name of the feed field whose value is saved to the CEF field. For example:

```
<cs3>file_size</cs3>
```

You can also list several feed fields for a single CEF field, separating them by semicolons (`;`).

Save the feed fields that are interpreted as malicious indicators, in the `cs1` CEF field.

A feed field cannot be specified for more than one CEF field.

The following CEF fields are provided for use:

- `reason`
- `message`
- `deviceCustomNumber3`
- `deviceCustomString3`
- `deviceCustomString4`

In this chapter

Default correspondence between feed fields and CEF fields

The following table shows the default correspondence between the feed fields and CEF fields to which the values of the feed fields are saved.

Note that in the kl_feed_util.conf configuration file the `deviceCustomString` and `deviceCustomNumber` fields are shortened to `cs` and `cn` respectively.

Table 3. Default correspondence between feed fields and CEF fields

Feed	Feed fields	CEF fields
Malicious URL Exact Data Feed	urls/url domains/domain hosts/host popularity last_seen first_seen category files/MD5 files/threat	deviceCustomString1 deviceCustomString1 deviceCustomString1 deviceCustomNumber1 flexString1 flexString2 deviceCustomString5 deviceCustomString1 deviceCustomString2
Botnet CnC URL Exact Data Feed	urls/url domains/domain hosts/host popularity last_seen first_seen threat files/MD5	deviceCustomString1 deviceCustomString1 deviceCustomString1 deviceCustomNumber1 flexString1 flexString2 deviceCustomString2 deviceCustomString1
Demo Botnet CnC URL Data Feed	mask popularity last_seen first_seen threat files/MD5	deviceCustomString1 deviceCustomNumber1 flexString1 flexString2 deviceCustomString2 deviceCustomString1
Phishing URL Exact Data Feed	urls/url domains/domain hosts/host last_seen first_seen popularity industry	deviceCustomString1 deviceCustomString1 deviceCustomString1 flexString1 flexString2 deviceCustomNumber1 deviceCustomString6

IP Reputation Data Feed Demo IP Reputation Data Feed	ip threat_score category last_seen first_seen popularity files/MD5 files/threat	deviceCustomString1 deviceCustomNumber2 deviceCustomString5 flexString1 flexString2 deviceCustomNumber1 deviceCustomString1 deviceCustomString2
Malicious Hash Data Feed Demo Malicious Hash Data Feed	md5 last_seen first_seen popularity threat	deviceCustomString1 flexString1 flexString2 deviceCustomNumber1 deviceCustomString2
P-SMS Trojan Data Feed	MD5 Date AV Verdict	deviceCustomString1 flexString2 deviceCustomString2
Mobile Botnet URL Data Feed	mask files/MD5 threat popularity last_seen first_seen files/Behaviour	deviceCustomString1 deviceCustomString1 deviceCustomString2 deviceCustomNumber1 flexString1 flexString2 deviceCustomString3
APT IP Data Feed Demo APT IP Data Feed	ip detection_date publication_name	deviceCustomString1 flexString2 deviceCustomString2
APT Hash Data Feed Demo APT Hash Data Feed	MD5 detection_date publication_name	deviceCustomString1 flexString2 deviceCustomString2
APT URL Data Feed Demo APT URL Data Feed	mask detection_date publication_name	deviceCustomString1 flexString2 deviceCustomString2
Mobile Malicious Hash Data Feed	md5 last_seen first_seen popularity threat	deviceCustomString1 flexString1 flexString2 deviceCustomNumber1 deviceCustomString2

Ransomware URL Data Feed	mask last_seen first_seen popularity files/MD5 files/threat	deviceCustomString1 flexString1 flexString2 deviceCustomNumber1 deviceCustomString1 deviceCustomString2
IoT URL Data Feed	mask last_seen first_seen popularity files/MD5 files/threat	deviceCustomString1 flexString1 flexString2 deviceCustomNumber1 deviceCustomString1 deviceCustomString2
Vulnerability Data Feed	detection_date severity vulnerable_files/md5 exploits/md5 exploits/threat	flexString2 deviceCustomString4 deviceCustomString1 deviceCustomString1 deviceCustomString2
ICS Hash Data Feed	md5 last_seen first_seen popularity threat	deviceCustomString1 flexString1 flexString2 deviceCustomNumber1 deviceCustomString2

Adding and removing context fields

The feed fields to import to ArcSight ESM are listed in the `RequiredFields` elements (that are nested in the `Feed` elements) of the kl_feed_util.conf configuration file. You can add fields to these elements or remove fields from them.

Removal of the following fields is not allowed:

- `type` (for Ransomware URL Data Feed, Mobile Botnet URL Data Feed, Demo Botnet CnC URL Data Feed, APT URL Data Feed, IoT URL Data Feed)
- `mask` (for Ransomware URL Data Feed, Mobile Botnet URL Data Feed, Demo Botnet CnC URL Data Feed, Botnet CnC URL Data Feed, APT URL Data Feed, IoT URL Data Feed)
- `MD5`
- `ip`
- `id`

- `kla_id`

However, if you remove a mandatory field from the `RequiredFields` element of a feed, ArcSight ESM will contain the value `'-'` in the field that contains the information about this feed.

> Note that adding fields to ArcSight lists or removing fields from them leads to re-creating the lists from scratch and altering the matching rules. After a list is re-created, all information that was stored in it is lost. If you need re-creating a list, contact your technical account manager (TAM).

If you have added a field to the `RequiredFields` element of a feed, specify the CEF field (see section "Saving feed fields in CEF fields" on page 24) in which the feed field value will be saved in ArcSight ESM. We do not recommend that you add new CEF fields that are not specified in the kl_feed_util.conf configuration file.

The kl_feed_for_arcsight.py script workflow

The kl_feed_for_arcsight.py script imports Kaspersky Threat Data Feeds to ArcSight ESM as follows:

1. The kl_feed_for_arcsight.py script reads the files of the feeds.

   The feeds are stored in the directory specified in the FeedsDir element of the kl_feed_util.conf configuration file. The kl_feed_util.conf file resides in the same directory as the kl_feed_for_arcsight.py file.

2. From the feed records that are read, the kl_feed_for_arcsight.py script creates strings of the following format:

   ```
   CEF:0|Kaspersky Lab|Kaspersky Threat Data
   Feed|1.0|%INDICATOR_TYPE%|%FEED_NAME%|3|%FEED_RECORD%
   ```

   Here `%FEED_NAME%` is the feed name, `%FEED_RECORD%` are the fields of the feed record in CEF format, and `%INDICATOR_TYPE%` takes one of the following values:

   - 1—If the event contains an IP address.
   - 2—If the event contains a URL.
   - 3—If the event contains a domain.
   - 4—If the event contains a host.
   - 5—If the event contains a hash.

3. The kl_feed_for_arcsight.py script, using TCP, sends generated strings to the address specified in the `ArcSightConnectorAddr` element of the kl_feed_service.conf configuration file.

   The script sends feed records at the rate specified in the `ArcSightEPS` element of the kl_feed_service.conf configuration file.

4. After all indicators from Kaspersky Threat Data Feeds are sent to ArcSight SmartConnector, the kl_feed_for_arcsight.py script sends the following event:

   ```
   CEF:0|Kaspersky Lab|Kaspersky Threat Data Feed|1.0|9|FEEDS_UPDATED|3|
   msg=Uploaded indicators from feeds:%INDICATORS_COUNT%
   ```

   Here `%INDICATORS_COUNT%` is the number of indicators sent to ArcSight SmartConnector.

The Kaspersky_Threat_Data_Feeds.arb package contents

This section describes the contents of the Kaspersky_Threat_Data_Feeds.arb package contained in the distribution kit.

The Kaspersky_Threat_Data_Feeds.arb package contains objects of the following types:

- Lists
- Rules
- Filters
- Reports
- Active channels
- Dashboards

Lists contained in Kaspersky_Threat_Data_Feeds.arb

The Kaspersky_Threat_Data_Feeds.arb package contains the following lists:

- `Kaspersky IP indicators`

  The list contains the IP addresses and context from IP Reputation Data Feed and APT IP Data Feed. This list stores data for a day.

- `Kaspersky URL indicators`

  The list contains the URLs and context from Kaspersky Threat Data Feeds. This list stores data for a day.

- `Kaspersky Domain indicators`

  The list contains the domains and context from Kaspersky Threat Data Feeds. This list stores data for a day.

- `Kaspersky Host indicators`

  The list contains the hosts and context from Kaspersky Threat Data Feeds. This list stores data for a day.

- `Kaspersky Hash indicators`

  The list contains the hashes and context from Kaspersky Threat Data Feeds. This list stores data for a day.

- `Kaspersky detection events`

  The list contains events, indicators from which matched some feed records, and the context of the matched feed records. This list stores data for a year.

  The list contains the following fields:

  - `Device Custom String1`—Contains the indicator involved in the detection process.
  - `Reason`—Contains the name of the feed involved in the detection process.
  - `Device Custom Number1`—Contains the value of the `popularity` field from the feed record (if

any).

- Device Custom Number2—Contains the value of the threat_score field from IP Reputation Data Feed.
- Device Custom String2—Contains the value either of the threat field or the publication_name field (depending on the feed involved in the detection process).
- Flex String1—Contains the value of the last_seen field from the feed record (if any).
- Flex String2—Contains the value of the first_seen field from the feed record.
- Device Product—Name of the product, the event from which is involved in the detection process.
- Device Address—Address of the product, the event from which is involved in the detection process.
- Source Address—Identifies the source that an event refers to in an IP network.
- Source User Name—Identifies the source user by name.
- Destination Address—Identifies the destination address that the event refers to in an IP network.
- File Hash—File hash (if it contains in the original event).
- Request Url—URL requested (if it contains in the original event).
- Device Custom String5—Contains the value of the category, Behaviour, or severity field (depending on the feed involved in the detection process).
- Device Custom String6—Contains the value of the Industry field of Phishing URL Data Feed.
- Device Custom String3, Device Custom String4, Device Custom Number3, Message—Contain no values. These fields can be used for expanding the context from Kaspersky Threat Data Feeds.

Rules contained in Kaspersky_Threat_Data_Feeds.arb

Note that the use of the rules contained in the Kaspersky_Threat_Data_Feeds.arb package can impact the CPU of the computer on which ArcSight ESM runs; ArcSight ESM can deactivate one or several rules if it consumes more CPU resources than specified in its configuration files. You can monitor the deactivation of rules in the Kaspersky Rules monitor active channel (for more information, see subsection "Active channels contained in Kaspersky_Threat_Data_Feeds.arb").

The Kaspersky_Threat_Data_Feeds.arb package contains the following rules:

- Kaspersky add ip indicator

  Rule for filling the Kaspersky IP indicators list with IP addresses from Kaspersky Threat Data Feeds.

- Kaspersky add url indicator

  Rule for filling the Kaspersky URL indicators list with URLs from Kaspersky Threat Data Feeds.

- Kaspersky add domain indicator

  Rule for filling the Kaspersky Domain indicators list with domains from Kaspersky Threat Data Feeds.

- `Kaspersky add host indicator`

  Rule for filling the `Kaspersky Host indicators` list with hosts from Kaspersky Threat Data Feeds.

- `Kaspersky add hash indicator`

  Rule for filling the `Kaspersky Hash indicators` list with hashes from Kaspersky Threat Data Feeds.

- `Kaspersky check ip`

  Rule for matching IP addresses from events that arrive in Arcsight ESM, against the `Kaspersky IP indicators` list. In case of a match, the incoming event and the context from the feed record are added to the `Kaspersky detection events` list.

- `Kaspersky check url`

  Rule for matching URLs from events that arrive in Arcsight ESM, against the `Kaspersky URL indicators` list. In case of a match, the incoming event and the context from the feed record are added to the `Kaspersky detection events` list.

- `Kaspersky check domain`

  Rule for matching domains from events that arrive in Arcsight ESM, against the `Kaspersky Domain indicators` list. In case of a match, the incoming event and the context from the feed record are added to the `Kaspersky detection events` list.

- `Kaspersky check host`

  Rule for matching hosts from events that arrive in Arcsight ESM, against the `Kaspersky Host indicators` list. In case of a match, the incoming event and the context from the feed record are added to the `Kaspersky detection events` list.

- `Kaspersky check hash`

  Rule for matching hashes from events that arrive in Arcsight ESM, against the `Kaspersky Hash indicators` list. In case of a match, the incoming event and the context from the feed record are added to the `Kaspersky detection events` list.

- `Kaspersky check update status`

  Rule for checking whether Kaspersky Threat Data Feeds were updated in the last 24 hours. This rule is activated after the first successful update of the feeds.

  If no update has occurred in the last 24 hours, the rule creates a `Kaspersky Threat Data Feeds are not updated` case in the **Cases** > **Shared** > **All Cases** > **Public** > **Kaspersky Threat Data Feeds** tree item. We recommend that you add the `Send Notification` action in the **Actions** tab of the rule so that the rule will notify the ArcSight ESM administrator about a problem with the update of the feeds.

After you import the ARB package to ArcSight ESM, specify that the rules must be triggered in real time.

► *To set real-time rules triggering:*

1. Open ArcSight Console.
2. Open the **Active Channels** drop-down list and select **Rules** (or press **Ctrl**+**Alt**+**L**).
3. In the tree, select **Rules** > **Shared** > **All Rules** > **Public** > **Kaspersky Threat Data Feeds**.

4. For every rule, right-click it and select **Deploy Real Time Rule(s)**.

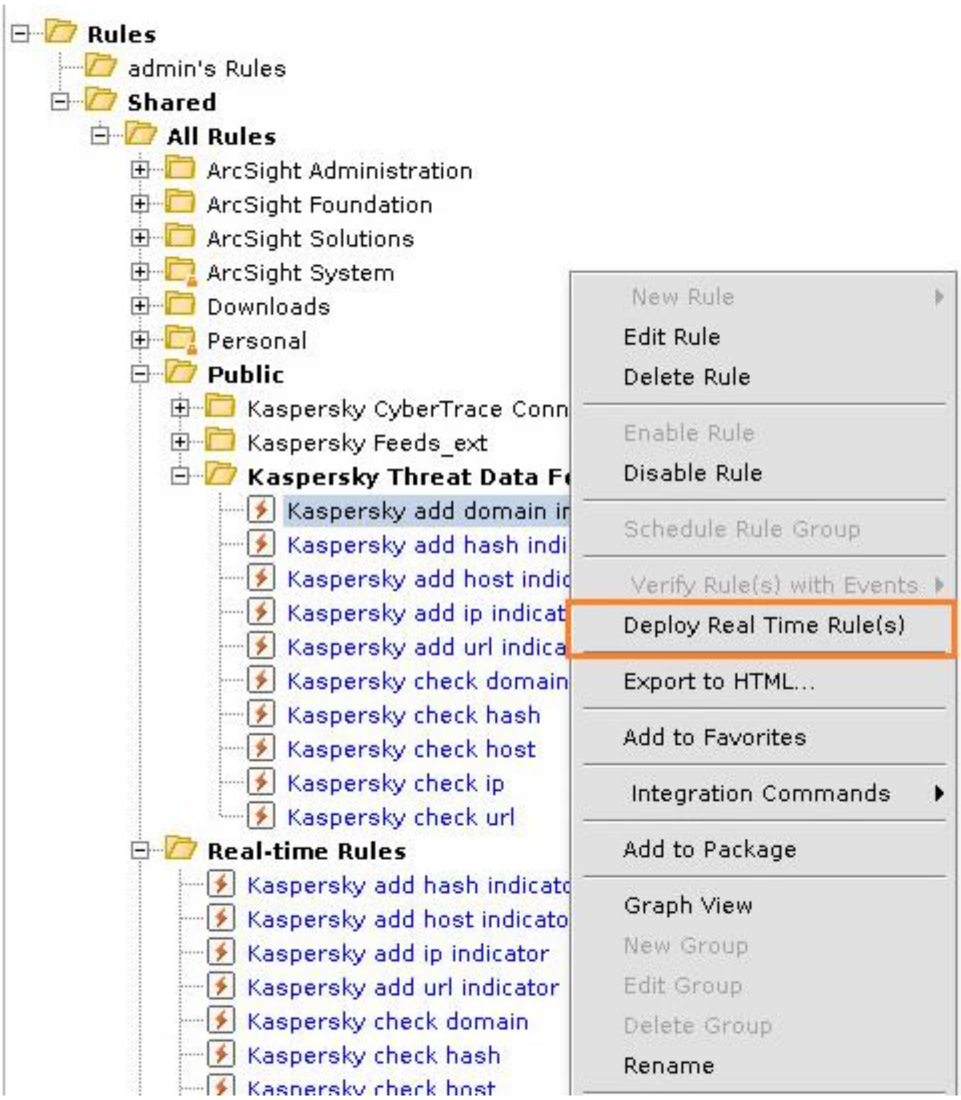


Figure 10: Making rules real-time

If you do not need to keep the hashes or URLs from feeds in ArcSight ESM, do not select **Deploy Real Time Rule(s)** for the relevant rules (for example, `Kaspersky add hash indicator` and `Kaspersky check hash`).

Filters contained in Kaspersky_Threat_Data_Feeds.arb

The Kaspersky_Threat_Data_Feeds.arb package contains the following filters:

- `Kaspersky detection events`

  Filter for finding detection events related to Kaspersky Threat Data Feeds among events that arrive in ArcSight ESM.

- `Kaspersky feeds records input`

  Filter for finding, among the events that arrive in ArcSight ESM, those events that contain records of Kaspersky Threat Data Feeds.

- `Kaspersky url checking`

  Filter for finding, among the events that arrive in ArcSight ESM, those events that contain URLs which are matched against indicators from Kaspersky Threat Data Feeds.

  The filter contains the following conditions that must be met simultaneously:

  - The `Request Url` field of the event contains some value.
  - The event has arrived from one of the following vendors: Palo Alto Networks, Cisco®, Microsoft®, Juniper Networks®, Trend Micro™, McAfee®, Imperva®, CheckPoint, Blue Coat®, Apache®, Fortinet, Sourcefire®, F5 Networks®, FireEye®, Squid.

- `Kaspersky ip checking`

  Filter for finding, among the events that arrive in ArcSight ESM, those events that contain IP addresses which are matched against indicators from Kaspersky Threat Data Feeds.

  The filter contains the following conditions that must be met together:

  - The `Destination Address` field or the `Source Address` field is not empty and its value is an address that does not belong to the inner network.
  - The event has arrived from one of the following vendors: Palo Alto Networks, Cisco, Microsoft, Juniper Networks, Trend Micro, McAfee, Imperva, CheckPoint, Blue Coat, Apache, Fortinet, Sourcefire, F5 Networks, FireEye, Squid.

- `Kaspersky hashes checking`

  Filter for finding, among the events that arrive in ArcSight ESM, those events that contain hashes which are matched against indicators from Kaspersky Threat Data Feeds.

  The filter contains the following conditions that must be met together:

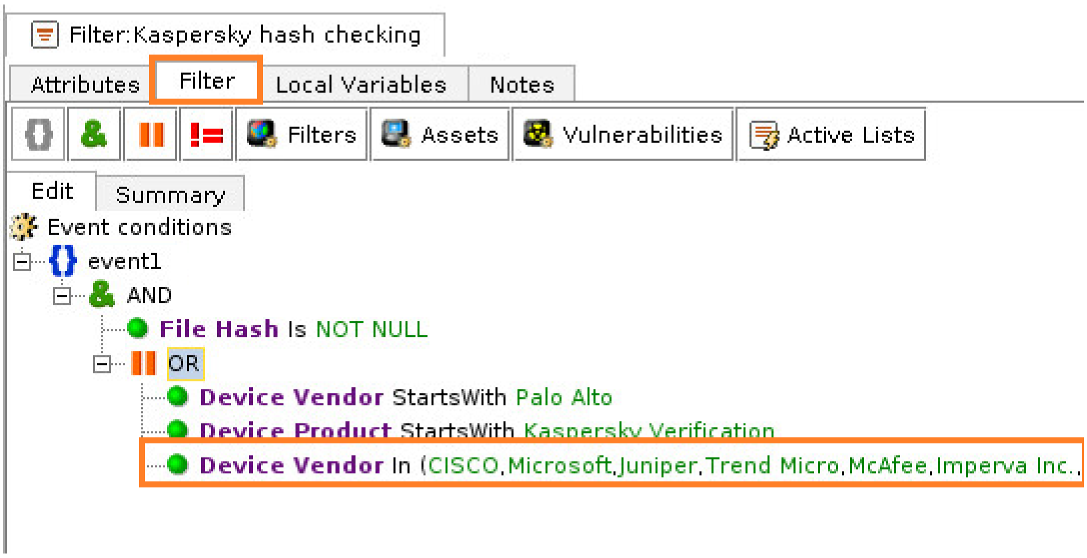
  - The `File Hash` field of the event contains some value.
  - The event has arrived from one of the following vendors: Palo Alto Networks, Cisco, Microsoft, Juniper Networks, Trend Micro, McAfee, Imperva, CheckPoint, Blue Coat, Apache, Fortinet, Sourcefire, F5 Networks, FireEye, Squid.

You can edit a filter and add other vendors, the events from which you want to check against Kaspersky Threat Data Feeds.

► *To add other vendors to the filter:*

1. Open ArcSight Console.
2. Open the **Active Channels** drop-down list and select **Filters**.
3. In the tree, select **Filters** > **Shared** > **All Filters** > **Public** > **Kaspersky Threat Data Feeds**.
4. Right-click the filter you want to edit.
5. Select **Edit Filter**.
6. In the right pane, select the **Filter** tab.
7. Edit the list of vendors.

8. Click **Apply**.



Filter:Kaspersky hash checking

```
Event conditions
event1
  AND
    File Hash Is NOT NULL
    OR
      Device Vendor StartsWith Palo Alto
      Device Product StartsWith Kaspersky Verification
      Device Vendor In (CISCO,Microsoft,Juniper,Trend Micro,McAfee,Imperva Inc.,
```

Figure 11: Editing a filter

Reports contained in Kaspersky_Threat_Data_Feeds.arb

- `Kaspersky detection statistics`

  Report that contains detection events related to Kaspersky Threat Data Feeds. You can specify the desired period for data to be analyzed.

Active channels contained in Kaspersky_Threat_Data_Feeds.arb

Note that the active channels contained in Kaspersky_Threat_Data_Feeds.arb do not work in real time by default. This is done to reduce the load on ArcSight ESM. If you want the data in the active channels to be continually updated, do the following:

1. Open ArcSight Console.
2. Select the **Active Channels** tab.
3. In the tree, select **Active Channels** > **Shared** > **All Active Channels** > **Public** > **Kaspersky Threat Data Feeds**.

4. Right-click the active channel whose properties you want to edit and select **Edit Active Channel**.

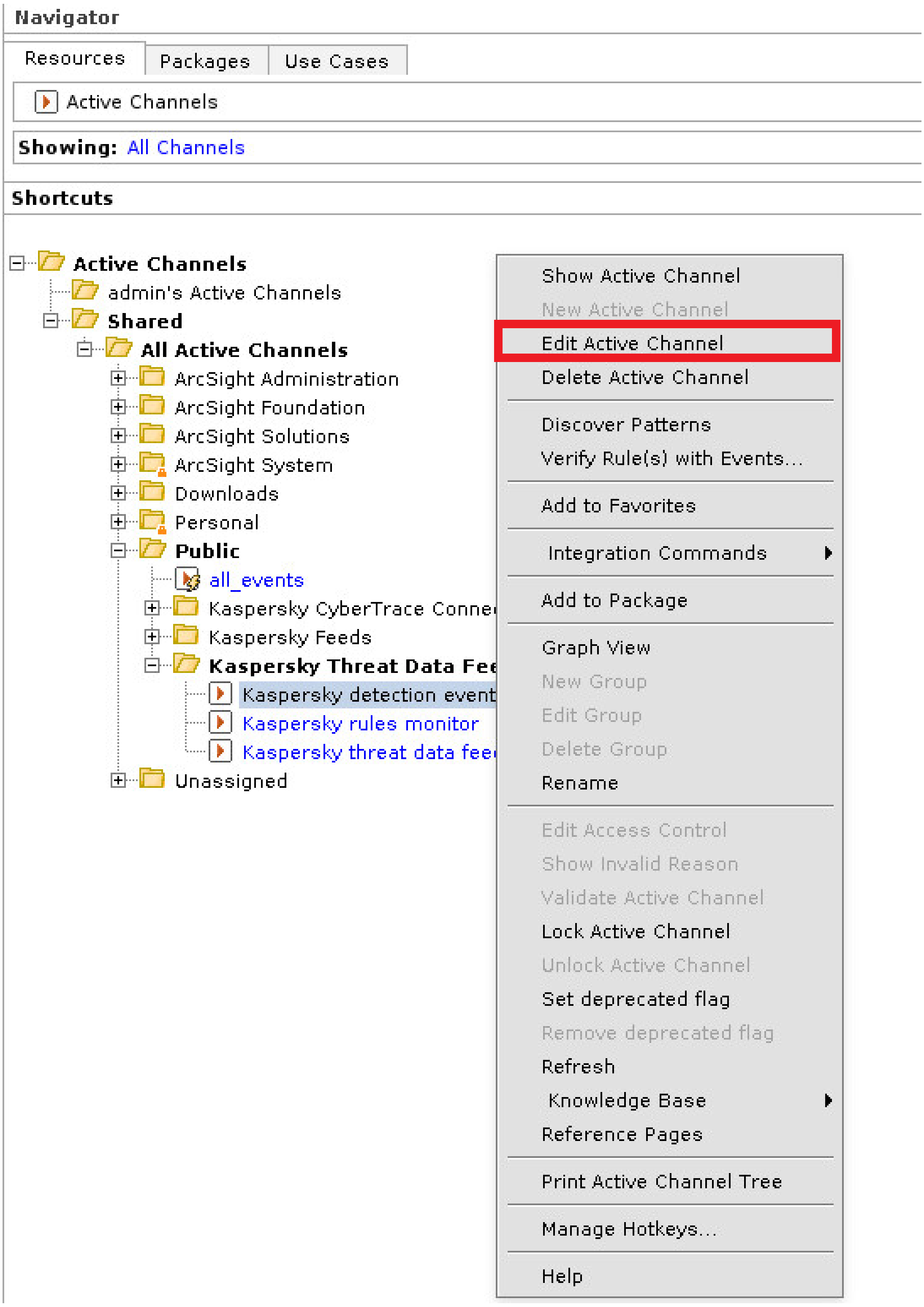
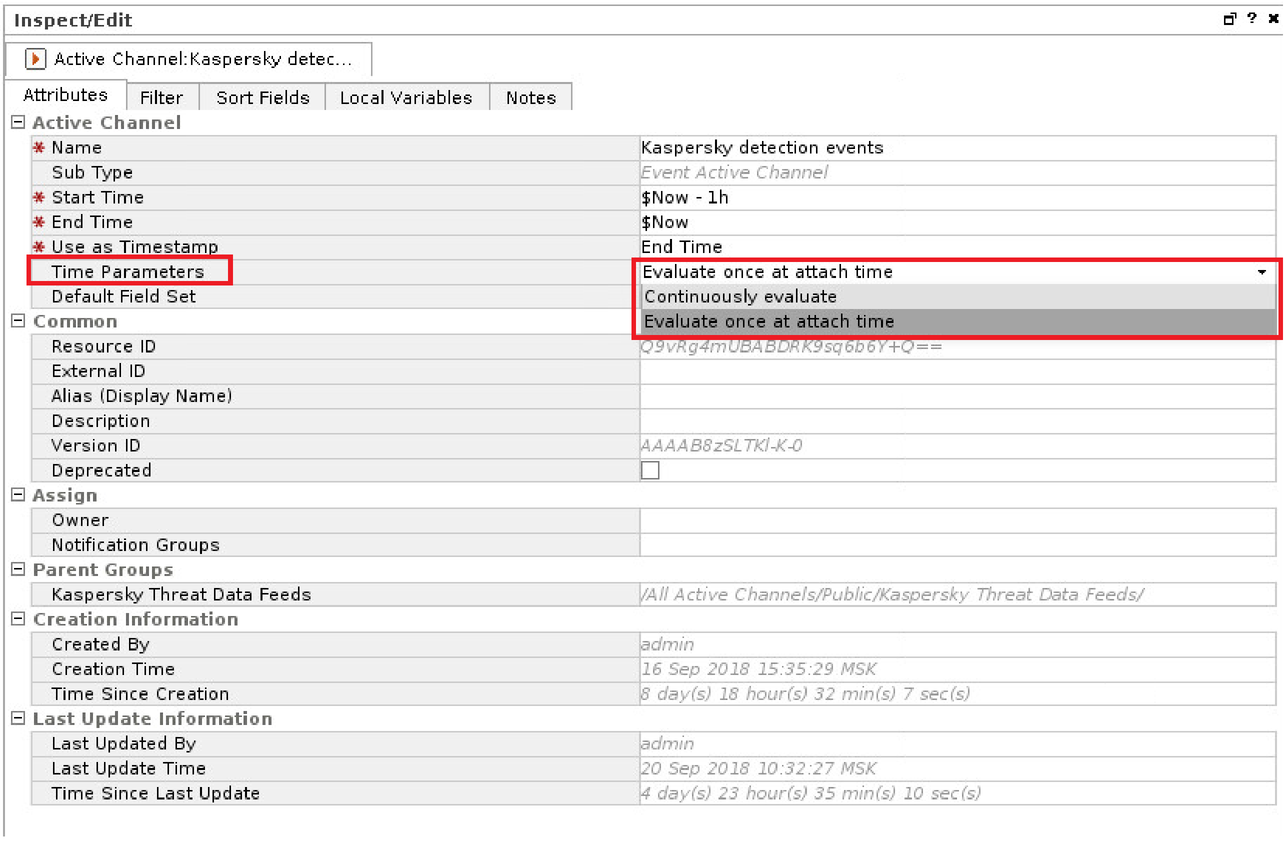


Figure 12: Editing an active channel

5. In the **Time Parameters** field, specify **Continuously evaluate**.



⊟ Active Channel

* Name	Kaspersky detection events
Sub Type	Event Active Channel
* Start Time	$Now - 1h
* End Time	$Now
* Use as Timestamp	End Time
Time Parameters	Evaluate once at attach time Continuously evaluate Evaluate once at attach time
Default Field Set	

⊟ Common

Resource ID	Q9vRg4mUBABDRK9sq6b6Y+Q==
External ID	
Alias (Display Name)	
Description	
Version ID	AAAAB8zSLTKl-K-0
Deprecated	□

⊟ Assign

Owner	
Notification Groups	

⊟ Parent Groups

Kaspersky Threat Data Feeds	/All Active Channels/Public/Kaspersky Threat Data Feeds/

⊟ Creation Information

Created By	admin
Creation Time	16 Sep 2018 15:35:29 MSK
Time Since Creation	8 day(s) 18 hour(s) 32 min(s) 7 sec(s)

⊟ Last Update Information

Last Updated By	admin
Last Update Time	20 Sep 2018 10:32:27 MSK
Time Since Last Update	4 day(s) 23 hour(s) 35 min(s) 10 sec(s)

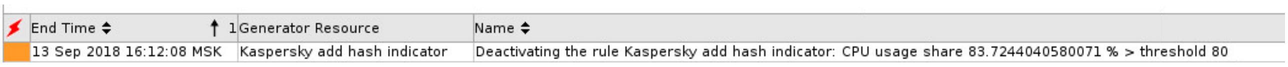
Figure 13: Active channel properties

6. Apply the settings.

The Kaspersky_Threat_Data_Feeds.arb package contains the following active channels:

- `Kaspersky Rules monitor`

  Active channel that displays rules from the ARB package that have been deactivated by ArcSight ESM due to usage of computer resources in excess of the established threshold.



	End Time ⬍ ↑ 1	Generator Resource	Name ⬍
🟧	13 Sep 2018 16:12:08 MSK	Kaspersky add hash indicator	Deactivating the rule Kaspersky add hash indicator: CPU usage share 83.7244040580071 % > threshold 80

Figure 14: Deactivated rule

  If you have discovered such an event in the active channel, find the deactivated rule on the **Rules** tab in ArcSight Console and perform the following actions in sequence on the rule:

  1. Deactivate a rule.
  2. Activate a rule.

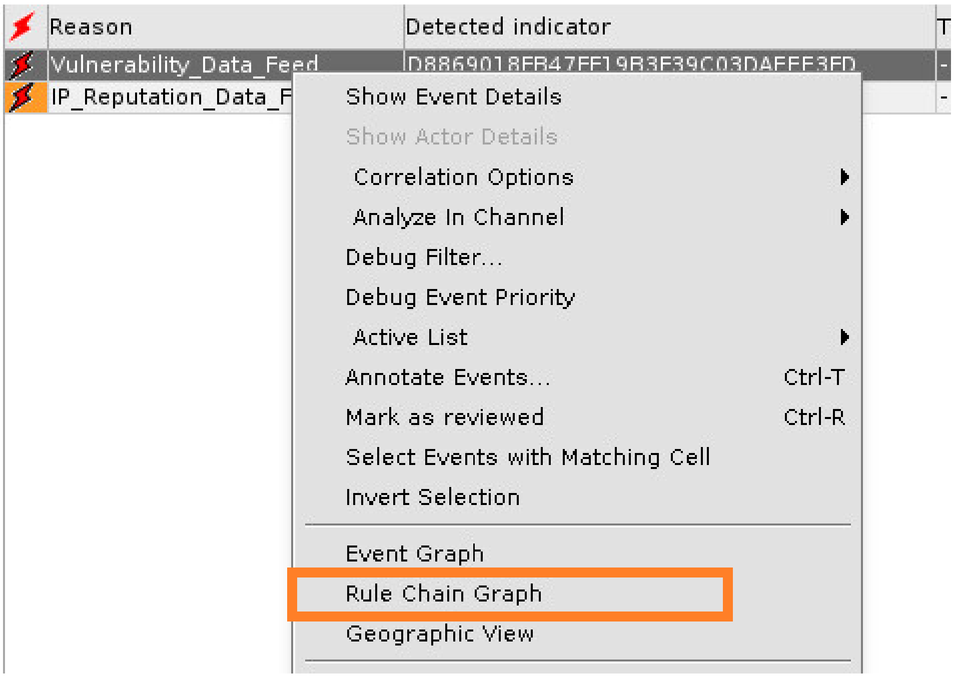
  Also, we recommend that you edit the ArcSight ESM configuration file and increase the resource consumption threshold (see section "Configuring ArcSight ESM in certain cases" on page 41).

- `Kaspersky threat data feeds input`

  Active channel that displays feed records that arrive in Arcsight ESM.

- `Kaspersky detection events`

Active channel that displays detection events. To view the original event, right-click the detection event and select **Rule Chain Graph**.



	Reason	Detected indicator	T
	Vulnerability_Data_Feed	D8869018FB47FE19B3F39C03DAEEE3FD	-
	IP_Reputation_Data_F		-

Figure 15: Getting the original event

ArcSight Console will display the original event in a gray box and the detection event in a red box. You can double-click the gray box to display the event contents in the **Inspect/Edit** panel.

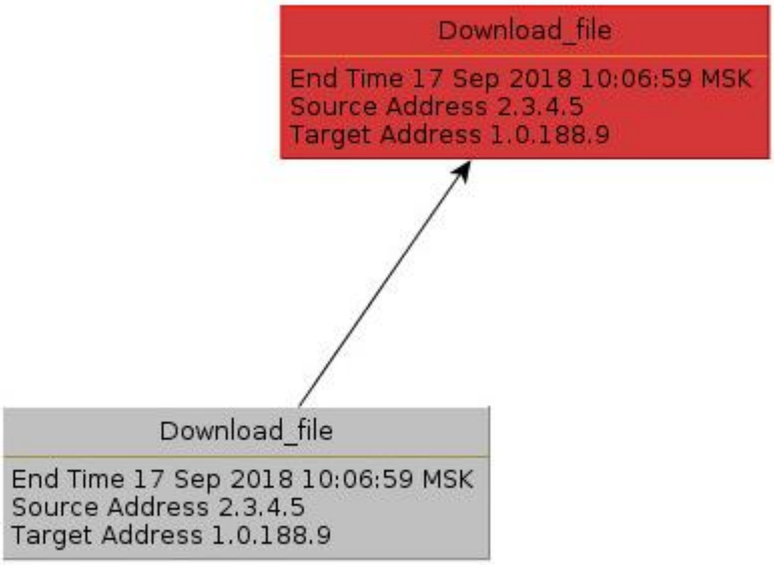


Figure 16: Rule chain graph

Dashboards contained in Kaspersky_Threat_Data_Feeds.arb

Note that the dashboard contained in Kaspersky_Threat_Data_Feeds.arb is disabled by default. This is done to reduce the load on ArcSight ESM. If you want to display data on the dashboard, enable the data monitors.

► *To enable data monitors:*

1. Open ArcSight Console.
2. Select the **Dashboards** tab and then the **Data Monitors** tab.
3. In the tree, select **Data Monitors** > **Shared** > **All Data Monitors** > **Public** > **Kaspersky Threat Data Feeds**.
4. Right-click each data monitor nested in this tree node and select **Enable Data Monitor**.

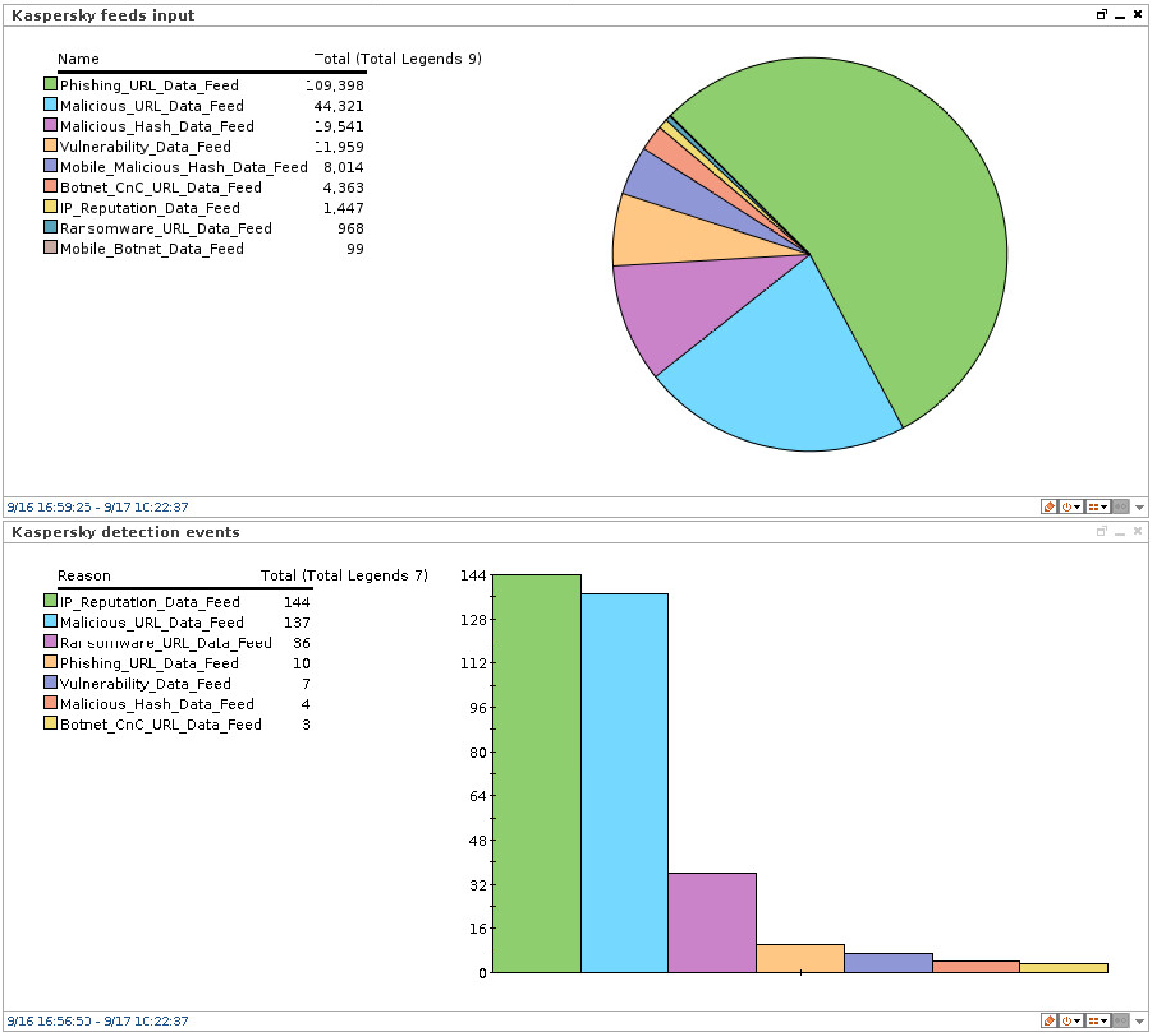
The Kaspersky_Threat_Data_Feeds.arb package contains the following dashboards:

- `Kaspersky Threat Data Feeds statistics`

  This dashboard displays the following data:

  - Number of indicators that are imported in ArcSight ESM in the last 24 hours

- Number of detections related to Kaspersky Threat Data Feeds in the last 24 hours



Kaspersky feeds input

Name	Total (Total Legends 9)
🟩 Phishing_URL_Data_Feed	109,398
🟦 Malicious_URL_Data_Feed	44,321
🟪 Malicious_Hash_Data_Feed	19,541
🟧 Vulnerability_Data_Feed	11,959
🟦 Mobile_Malicious_Hash_Data_Feed	8,014
🟥 Botnet_CnC_URL_Data_Feed	4,363
🟨 IP_Reputation_Data_Feed	1,447
🟦 Ransomware_URL_Data_Feed	968
🟫 Mobile_Botnet_Data_Feed	99

9/16 16:59:25 - 9/17 10:22:37

Kaspersky detection events

Reason	Total (Total Legends 7)
🟩 IP_Reputation_Data_Feed	144
🟦 Malicious_URL_Data_Feed	137
🟪 Ransomware_URL_Data_Feed	36
🟧 Phishing_URL_Data_Feed	10
🟦 Vulnerability_Data_Feed	7
🟥 Malicious_Hash_Data_Feed	4
🟨 Botnet_CnC_URL_Data_Feed	3

9/16 16:56:50 - 9/17 10:22:37

Figure 17: Kaspersky Threat Data Feeds statistics

Configuring ArcSight ESM in certain cases

This section explains how to configure ArcSight ESM in some cases.

Increasing the number of indicators imported to ArcSight ESM

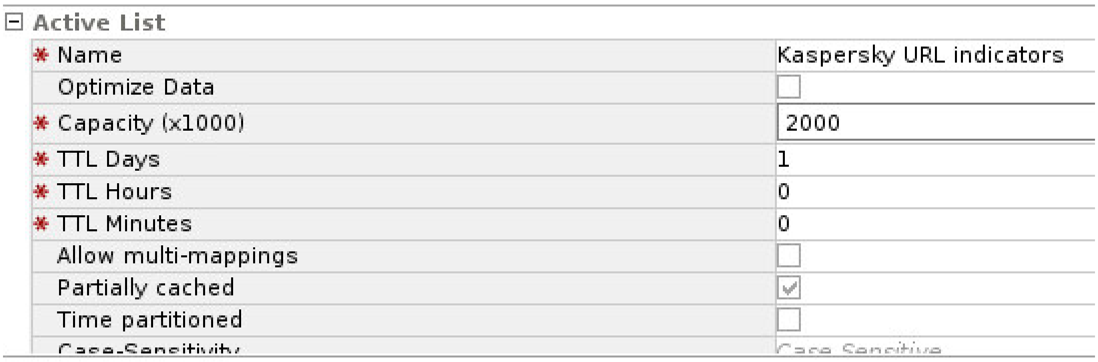
By default, ArcSight ESM allows the storage of no more than 1 000 000 indicators in the lists. You can enlarge the storage—for example, if you have increased the value of the `RecordsCount` element of the kl_feed_util.conf configuration file or increased the number of the fields to detect that must be imported from the feed.

► *To increase the capacity of the ArcSight ESM storage for indicators (for example, to 2 000 000):*

1. Open the server.properties configuration file of ArcSight ESM for editing. (By default, the file is located in the `/opt/arcsight/manager/config` directory.)
2. Add the following line to the server.properties file:

   ```
   activelist.max_capacity=2000000
   ```
3. Save the server.properties file and close it.
4. Restart ArcSight ESM to apply the settings by running the following command:

   ```
   /etc/init.d/arcsight_services restart manager
   ```
5. In ArcSight Console, open the **Lists** section.
6. Edit the properties of the list (see section "The Kaspersky_Threat_Data_Feeds.arb package contents" on page 30) that will store more feed records than were stored earlier.
7. In the `Capacity` field, specify `2000`.
8. Apply the settings.



⊟ Active List

* Name	Kaspersky URL indicators
Optimize Data	□
* Capacity (x1000)	2000
* TTL Days	1
* TTL Hours	0
* TTL Minutes	0
Allow multi-mappings	□
Partially cached	☑
Time partitioned	□
Case-Sensitivity	Case Sensitive

Figure 1. Рисунок 18: List properties

Increasing the resource consumption threshold

A large number of Kaspersky Threat Data Feeds indicators can arrive in ArcSight ESM—for example, if you assigned a large value to the `ArcSightEPS` (see section "`Installing and configuring Kaspersky Feed Utility`" on page 11) setting in the kl_feed_util.conf file. The use of rules that save the indicators in the lists (see section "The Kaspersky_Threat_Data_Feeds.arb package contents" on page 30) can lead to consumption of more CPU resources than specified in ArcSight ESM. When that specified threshold is exceeded, ArcSight ESM automatically deactivates the rule without notifying the user. To prevent the deactivation, you can increase the resource consumption threshold.

► *To increase the resource consumption threshold:*

1. Open the server.properties configuration file of ArcSight ESM for editing. (By default, the file is located in the `/opt/arcsight/manager/config` directory.)
2. Add the following line to the server.properties file:

   ```
   rules.max.fractional.cpu=80
   ```
3. Save the server.properties file and close it.
4. Restart ArcSight ESM to apply the settings by running the following command:

   ```
   /etc/init.d/arcsight_services restart manager
   ```

Information about third-party code

Information about third-party code is contained in the legal_notices.txt file in the `doc` subdirectory of the distribution kit.

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.

Android, Google are trademarks of Google, Inc.

Apache and the Apache feather logo are trademarks of The Apache Software Foundation.

Apple, iPhone are trademarks of Apple Inc., registered in the U.S. and other countries.

Blue Coat is a trademark of Blue Coat Systems, Inc. in the United States and/or other countries.

Cisco, Sourcefire are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

F5 and F5 Networks are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries.

FireEye is a registered trademark of FireEye, Inc.

Imperva is a trademark of Imperva, Inc. and its subsidiaries.

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

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

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

Microsoft is a registered trademark of Microsoft Corporation in the United States and other countries.

Trend Micro is a trademark of Trend Micro.